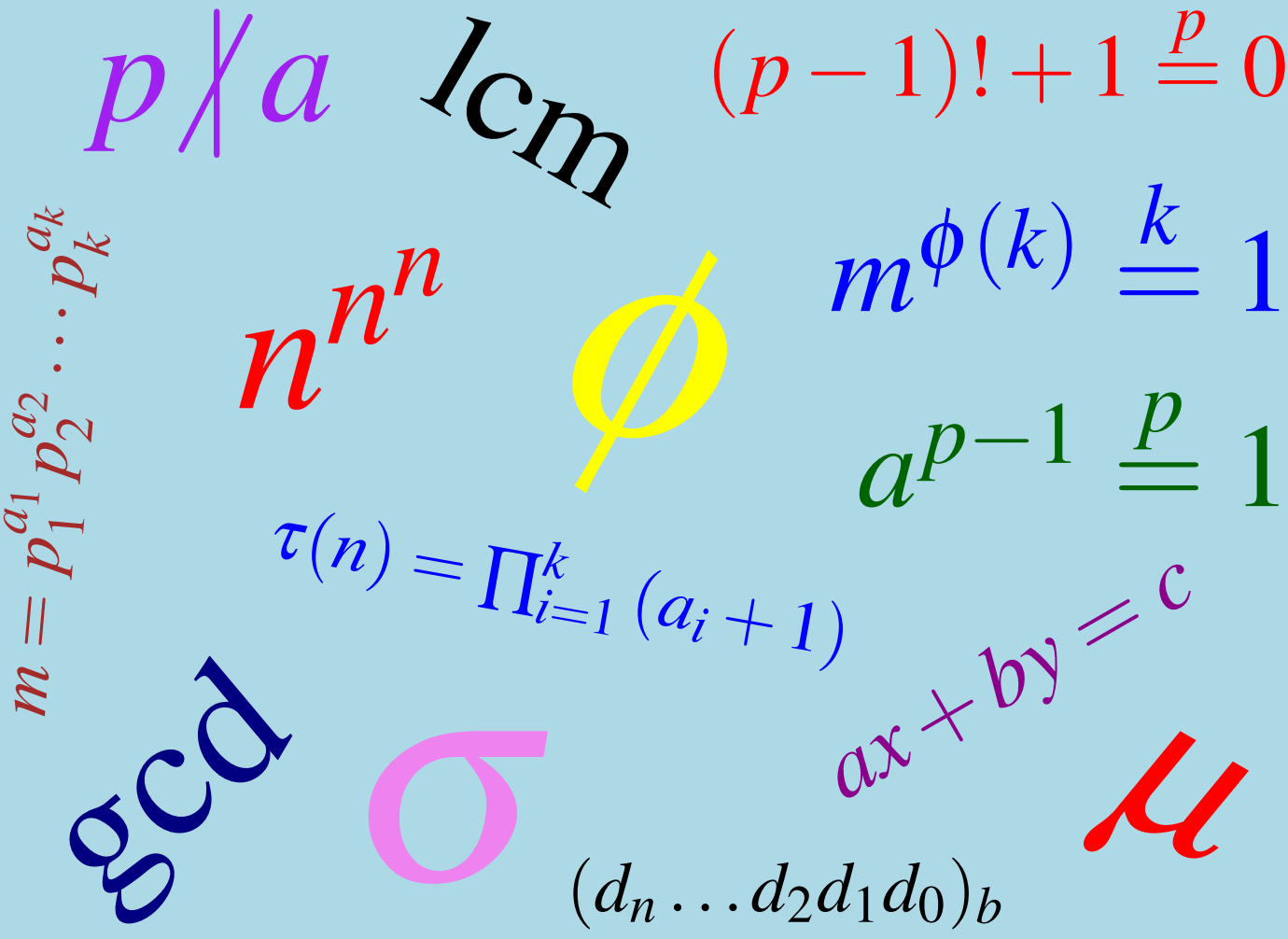
Notes and Problems in Number Theory

Volume I: Introduction



Taha Sochi

Preface

This book is a collection of notes and problems in number theory. It is important to note the following about this book (as well as about this volume):

• Number theory is very big subject and hence it is difficult to investigate properly in one volume (even at basic level). Therefore, this book (unlike my previous books) is designed to be multi-volume.

• The book (at least in its first volume) is about elementary number theory. The present volume introduces the basics of number theory for the beginners who are not familiar with the topics, methods and techniques of number theory. In the following volumes we intend to build on the material of this volume and extend the investigated topics. So, our plan is to expand and elaborate (gradually) the subject of number theory horizontally and vertically as we progress and add more volumes. We may also investigate during this long journey other subjects (or rather topics of other subjects) related to number theory (such as abstract algebra) from the perspective of number theory and as much as they are related to it. So, the book is likely to become open ended. In fact, there are many uncertainties about the future development of this book apart from being about number theory.

• The book is planned to contain (in its volumes in general but not necessarily in each volume) both solved problems and unsolved (or open) problems. The inclusion of unsolved problems is to make the readers aware of these problems and hence encourage them to think about them and try to make these problems "solved" or solvable. We may also try to investigate these unsolved problems from various perspectives and angles to improve their general understanding which may contribute to their subsequent solution in the future. So, in this regard the book is especially useful to the young "mathematicians" (or rather the future generation of mathematicians) to help them in digesting and searching for solutions to these problems (as well as other problems).

• The solved problems in this volume range from very simple to rather difficult. However, they are generally within the intended and prescribed level of the book. We usually use the simple problems for purposes like highlighting essential points and preparing for the more difficult problems, while we use the medium and difficult problems for presenting and illustrating the main contents of number theory as well as preparing for the more advanced topics and difficult problems. We also use solved problems to provide necessary notes or theorems which we generally need in the subsequent parts of the book.

• Although the book does not contain detailed and systematic theoretical background about number theory (apart from a basic introduction in chapter 2), we provide (as we progress) a collection of short comments and explanatory notes within and around the problems and solutions and as much as needed so that the reader will not struggle to understand or need to consult other books or references. So, the book (and this volume) is generally self contained.

• The required background of the reader is A-level (or college level) of general mathematics or at most the level of first year of undergraduate general mathematics.

• As in my previous books, my topmost priority in the structure and presentation is clarity and graduality so that the readers have the best chance of understanding the content with minimum effort and with maximum enjoyment. For this purpose (as well as for other obvious purposes) the book is full of cross references (which are hyperlinked in the electronic versions although the hyperlinks are not highlighted with color or other marking techniques to avoid distortion and ugliness).

• The book can be used as a text or as a reference for an introductory course on number theory and may also be used for general reading in mathematics (especially by those who have the hobby of problem solving). The book may also be adopted as a source of pedagogical materials which can supplement, for instance, tutorial sessions (e.g. in undergraduate courses on mathematics or computing or cryptography or related subjects).

Taha Sochi
London, July 2023

Contents

Nomenclature

In the following list, we define the common symbols, notations and abbreviations which are used in the book as a quick reference for the reader.

$\forall$	for all
$\times$, $\cdot$	multiplication sign
$\{\cdots\}$	set
$!$	factorial
$\in$	in (or belong to)
$\ni$	(backward) in (or belong to)
$\notin$	not in
$\lvert a\rvert$	absolute value of a
$\overline{a}$	negation of a
$\mathbb{C}$	the set of complex numbers
C_m^n	binomial coefficient (number of combinations of m in n with no repetition)
$C_{n_1,n_2,\ldots,n_k}^n$	multinomial coefficient
$\mathbb{E}$	the set of even numbers
Eq., Eqs.	Equation, Equations
$\mathrm{floor}(a)$	floor function (the greatest integer less than or equal to a)
$\gcd(m,n)$	greatest common divisor of m and n
iff	if and only if
$\mathrm{lcm}(m,n)$	least common multiple of m and n
$m \lvert n$	m divides n
$m \not\rvert n$	m does not divide n
$m \uparrow n$	tetration of m to n
$(m)_n$	the number m in base n
$m \overset{k}{=} n$	m and n are congruent modulo k
$m \overset{k}{\neq} n$	m and n are not congruent modulo k
$m, n, k, \ldots$	integers
m^*	modular multiplicative inverse of m
m_k^*	modular multiplicative inverse of m modulo k
$\max(a,b)$	the maximum of a and b
$\min(a,b)$	the minimum of a and b
mod	modulo (or modulus)
M_p	Mersenne prime
$\widehat{n}$	factorial power of n
$\mathbb{N}$	the set of natural numbers (i.e. $1, 2, 3, \ldots$)
$\mathbb{N}^0$	the set of non-negative integers (i.e. $0, 1, 2, 3, \ldots$)
$\mathbb{O}$	the set of odd numbers
p	prime number
$\mathbb{P}$	the set of prime numbers
P_e	even perfect number
P_m^n	number of permutations of m in n (with no repetition)
$\mathbb{Q}$	the set of rational numbers
$\mathbf{r}, \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3$	position vectors (in 3D space)

$\mathbb{R}$	the set of real numbers
$s(n)$	the restricted divisor function
S_c	complete residue system
S_r	reduced residue system
x, y, z	variable integers
$\mathbb{Z}$	the set of integers
$\mu(n)$	the Mobius function
Π	the product symbol (for repeated multiplication)
$\sigma(n)$	the divisor function
Σ	the summation symbol
$\tau(n)$	the tau function
$\phi(n)$	the totient (or phi or Euler) function

Chapter 1
Preliminaries

In this chapter we present and discuss a number of subjects and issues in preparation for the forthcoming investigations.

1.1 Introductory Remarks

In this section we present some short remarks about number theory and some of its basic terminology and concepts which will be needed in the future investigations (mainly for the purpose of avoiding dependence on later parts of the book). We also present a number of general remarks related to the conventions, terminology and commonly occurring issues in this book. All these are outlined in the following points:

1. **Number Theory** is the branch of mathematics that investigates integers and their properties.
2. "**Natural numbers**" in this book (symbolized as $\mathbb{N}$) means the set of positive integers (i.e. $1, 2, 3, \ldots$).
3. "**Divisible**" in number theory means "without remainder" (noting that number theory is about integers and hence "divisible" in number theory is an attribute of integers). For example, 8 is divisible by 4 because $8 \div 4 = 2$ without remainder but not by 6 because $8 \div 6 = 1$ with remainder 2 (noting that fractions do not exist in the set of integers). Similarly, "**divisibility**" means being divisible (i.e. without remainder). More clearly, **divisibility** in number theory means the property of integers to be divisible (i.e. by each other) with no residue (i.e. without remainder). In technical terms, if m, n, k are integers such that $m = n \times k$ then we say: n divides m, or n is a **divisor** or a **factor** of m, or m is a **multiple** of n, and write $n|m$. Otherwise (i.e. if m is not a multiple of n) we write $n \not| m$.[1]
4. **Proper divisor** of a given integer n is a positive divisor of n excluding n itself.[2]
5. "**Prime number**" (or "**prime**" for short) is a natural number greater than 1 that is divisible only by 1 and itself (considering only the positive divisors), while "**composite number**" (or "**composite**") is a natural number greater than 1 that is not prime.
6. Two integers (or natural numbers) are described as **coprime** or **relatively prime** if there is no integer greater than 1 that divides them both.
7. "**Trailing digit**" or "**last digit**" refer to the unit digit (i.e. the digit of least value), e.g. the trailing or last digit of 12**34** is 4. Similar expressions (like "number ending in digit") may also be used.
8. The **greatest common divisor** (symbolized as gcd) of two or more integers (which are not all zero) is the largest natural number that divides each one of these integers. The **least common multiple** (symbolized as lcm) of two or more integers (none of which is zero) is the smallest natural number that is divisible by each one of these integers. For example, $\gcd(18, 24) = 6$ and $\mathrm{lcm}(18, 24) = 72$.
9. A function whose domain is the set of natural numbers is called **arithmetic** (or **arithmetical**) **function**. Regrading its range, it depends on the purpose and author but we generally assume it is the set of numbers (which usually, in the context of elementary number theory, is the set of integers).
10. An arithmetic function f is **multiplicative** *iff* $f(mn) = f(m)f(n)$ where m and n are (positive) coprime numbers.[3]
11. For a **conditional statement** $a \to b$ (i.e. the **if statement**: if a then b), the **converse** is $b \to a$, and the **contrapositive** is $\overline{b} \to \overline{a}$, while the **inverse** is $\overline{a} \to \overline{b}$ (where the bar means negation). The truth of contrapositive follows the truth of the statement (i.e. if $a \to b$ is true/false then $\overline{b} \to \overline{a}$ is also true/false) but this does not apply to the converse (i.e. if $a \to b$ is true/false then $b \to a$ is not

[1] To be more clear, if m, n, k are integers such that $m \div n = k$ then m is the **dividend**, n is the **divisor**, and k is the **quotient**.

[2] We follow the literature in this definition, but we think what should be excluded is $|n|$.

[3] There is some difference in convention between authors (and hence more or less conditions may be attached to this definition). However, these details are irrelevant to us in this book.

necessarily true/false). Similarly, the truth of inverse does not follow the truth of the statement (i.e. if $a \to b$ is true/false then $\overline{a} \to \overline{b}$ is not necessarily true/false).

12. Based on point 11, an if statement is equivalent to two statements: $a \to b$ and $\overline{b} \to \overline{a}$. Now, if we note that an *iff* statement (i.e. $a \leftrightarrow b$) is a combination of an if statement (i.e. $a \to b$) and its converse (i.e. $b \to a$) then we can conclude that an *iff* statement is equivalent to four statements: $a \to b$, $\overline{b} \to \overline{a}$, $b \to a$ and $\overline{a} \to \overline{b}$. In more simple terms, the *iff* statement $a \leftrightarrow b$ means: either a and b are true or a and b are false (i.e. it is impossible that one of them is true and the other is false).
13. A **conjecture** is an unproven proposition that is supported by partial evidence or indication and hence it is believed (tentatively) to be correct. An **open problem** or **open question** is a proposition that is not supported or contradicted by a conclusive evidence and hence it is equally likely to be correct or incorrect.
14. Because this book is about number theory (whose prime subject is integers and their properties), we are interested only in the set of integer numbers and its subsets like natural numbers or non-negative integers or prime numbers or perfect numbers. So, in general we have no interest in rational numbers $\mathbb{Q}$ or real numbers $\mathbb{R}$ or complex numbers $\mathbb{C}$. Accordingly, in this book "number" with no other qualification should mean "integer" or one of its subsets (depending on the context and circumstances). Yes, in very exceptional circumstances we refer to types of numbers other than integers in which case we state this explicitly.
15. Due to the huge extension and versatility of number theory and its methods and techniques, most problems in number theory can be solved by several (and possibly many) methods. However, due to the restrictions on the size of the book we cannot demonstrate all these methods in our solved Problems. Nevertheless, we generally do our best to demonstrate a sample of these methods in different Problems and usually select the more common, accessible and intuitive of these methods (considering in particular the level of the book and its intended readers). We also tried deliberately (when possible) to use different methods (or techniques or notations or methods of formulation and presentation) to tackle similar types of problems for the purpose of diversity and to expose the readers to a range of experiences which helps to diversify and enrich their base knowledge and skills and improve their ability to recognize, understand and deal with similar problems (to become more flexible in thinking and acting).

1.2 Characteristics of Number Theory

Like any other discipline, number theory has certain characteristics and properties. In the following points we list and discuss (briefly) some of these characteristics:

1. **Richness**: this branch of mathematics is one of the richest (and possibly the richest) in all mathematics. It is so big and extended that it contains many subbranches and fields. This should come as no surprise since numbers (and hence their theory) are the essence and soul of mathematics.
2. **Interconnections**: this subject is strongly connected to many other branches and subjects of mathematics like abstract algebra and group theory. In fact, some of these branches and subjects are so mixed with number theory that they are commonly treated and regarded as topics in number theory (at least within their connections to number theory).
3. **History**: number theory is the oldest branch of mathematics. In fact, we can find many examples of sophisticated and complex theorems and propositions in number theory even in the old ages as well as in very early stages during the time of European renaissance. So, it is not only the oldest branch of mathematics but it is the oldest branch that progressed to high and advanced levels and accomplished significant achievements even before the birth of most other branches of mathematics. This should be no surprise given that the subject of number theory is the integers and their subsets (notably the "natural" numbers) which are the first and most intuitive entity in mathematics (or rather arithmetic which is the first stage and product of mathematical thinking).
4. **Entertainment**: working on number theory is generally an entertaining and gratifying experience because solving a number theory problem (at least at elementary level) is like solving a challenging puzzle which generates excitement and motivation. Hence, this branch of mathematics apparently embraces

the largest number of amateur "mathematicians" who crave for excitement and joy in pondering and solving challenging number theory problems.

5. **Open problems and conjectures**: one of the characteristics of this subject is that it embraces some of the most famous and challenging open and unsolved problems in mathematics as well as conjectures. It also embraces more open problems and conjectures than any other branch in mathematics (and possibly most of the conjectures and open problems in mathematics). Hence, it is especially attractive to young and ambitious mathematicians who want to rise to glory through tackling and solving these challenges.
6. **Research**: number theory contains some of the most active research areas in mathematics. This in part is due to its inclusion of many open problems and conjectures (which we discussed in the previous point) and hence it attracts a lot of attention and interest for investigation and research.
7. **Intuitivity**: considerable part of elementary number theory is based on intuition, common sense and logic, and this is one reason for making this subject attractive to many mathematicians (especially the amateurs) and hence making it one of the most popular branches of mathematics. This should be explained in part by its arithmetic roots which represent the entry point of humanity to mathematics. It should also be attributed to its heavy reliance on logic and rational thinking.

1.3 Computers and Computing in Number Theory

The use of calculators, computers and computing equipment in general (as well as their accessories like computer algebra systems and programming languages) in number theory is not only useful but it is a necessity in many cases and areas of application and research. However, like using any other tool, certain rules and procedures should be observed and followed to avoid making mistakes or wasting or misusing resources. In the following subsections we briefly investigate a few issues related to the use of computers and computing in number theory.

1.3.1 Dealing with Large Numbers

Dealing with very large numbers is very common in number theory. It is tempting to use basic calculators and ordinary computer programs to solve such problems or check their solutions which were already obtained by other means. However, we should always be careful about this because the accuracy of such calculators and programs is limited to a certain number of digits (e.g. 15 digits). For example if we calculate 234257^4 using a basic calculator we may get something like 3011412916678850000000 and hence we may conclude wrongly that 234257^4 is divisible by 10^7 or it is even. However, the exact value of 234257^4 is 3011412916678845518401 and hence it is neither divisible by 10^7 nor even.

Accordingly, when using any calculator (or computational tool or method) to solve or test a large-number problem (or indeed any number theory problem) the user should be aware of (and consider) the limitations of the calculator to see if it can cope with the problem or not. In fact, even when we have access to "competent calculators" (i.e. calculators that supposedly can cope) we recommend using more than one competent calculator to double check the result because no calculator (or software or computing library or method) is infallible.

We also recommend using the analytical methods as the first choice because the analytical methods are more robust and easier to check (and discover) if an error is committed in their use. So, in tackling number theory problems calculators and computational methods should be considered and used as a second choice (to check the results obtained already for instance) because most of them are not designed for dealing with the type of problems met in number theory (especially large numbers). Moreover, they are mostly "black boxes" and hence it is not easy to discover their mistakes if they contain bugs or limitations even when they are supposed to be competent (i.e. designed to deal with the given problem). In fact, some types of number theory problems can be tackled only by analytical methods.

1.3.2 Numeric Libraries, Software Packages and Internet

There are many dedicated and undedicated **computing libraries** for doing number theory problems and facilitating their management and solution. These libraries come in different shapes and forms and for various purposes and capabilities using many different programming languages and computing procedures. However, most of these libraries are not user friendly at all and they require not only considerable knowledge and skill in programming languages (and related computing skills like installation of libraries using scripting languages) but they also require technical and specialized knowledge in number theory which is not usually available for the novice users. Also, many (or most) of these packages are designed for certain operating systems and platforms (which are mostly distributions of Linux) and hence they are not available (at least in their optimized and reliable form) for other types of operating systems, platforms and distributions.

However, the advantages of these libraries include many aspects such as:
• Versatility and flexibility (being mostly open source and hence they can be modified, adapted and further developed according to the purposes and needs of the user).
• Capability of being incorporated and embedded within other packages and computing resources or interacting with them (e.g. by using a programming or scripting mediator).
• Being free of charge and hence they are affordable to everyone.
• Being clean of parasitic additives which are commonly attached to commercial packages.
• Protection of privacy as they do not require personal data which are usually collected and used (and even misused) by vendors of commercial packages.
• Being resource-effective as they are usually optimized by design for their functionalities and hence they require the minimum of resources (unlike commercial packages which usually require considerable overhead). This is reflected as an advantage in performance (i.e. speedy operations with less memory consumption).

The alternative to these libraries is the **commercial software packages** whose main virtue is their relative ease of use as they are designed for general users and not only specialists. However, they have many cons and disadvantages such as:[4]
• Expensive license or registration fees.
• Availability to certain operating systems and platforms but not to others.
• Lack of efficiency as they usually require considerable computing overhead and consume a lot of resources (in terms of processor time, required memory and disk space).
• Violation of privacy as well as parasitic behavior. In fact, commercial packages have full access to the user data and have almost complete control over his system, and hence they usually feel free to change the system according to their wishes and needs and gather the data they want noting that many commercial vendors have very limited, if any, moral or ethical code. Moreover, the regulations in this regard do not exist or very vague or impractical to impose or verify or prosecute (in case of violation). The end result is that when we install a commercial software package we actually hand over our system to the vendor and hence we rely on his good will and practices.

We may also mention in this regard **non-commercial software packages** which are usually offered on certain operating systems and platforms (especially on Linux distributions). The main advantage of these packages is being free of charge. However, they have many disadvantages such as being limited in capability and functionality (as they are usually less capable and versatile than their commercial counterparts), having no access to customer services (unlike commercial ones), being less user friendly than their commercial counterparts, and being limited to certain operating systems and platforms. They also have limited liability (if any at all) and some may even be dangerous (maliciously or non-maliciously).[5]

[4] For more about these cons and disadvantages (as well as others) we refer the readers to the Internet using some keywords related to well known commercial packages. So, we generally discourage heavy reliance on (and trust in) commercial packages and favor using other methods and tools (especially developing our own tools and techniques if possible).

[5] A few years ago I installed such a non-commercial software package for some purpose on my computer. On doing a routine cleaning job I discovered that this program wiped off everything in the directory of installation (which cost me considerable amount of time and effort to restore). However, I was lucky not to install this program in the root directory because I would have lost everything (data and work) and suffered a crippling disaster.

Another alternative to these libraries (as well as to commercial and non-commercial software packages) is the **Internet sites** which offer various functionalities related directly or indirectly to number theory (e.g. prime factorization calculators, gcd and lcm calculators, modular arithmetic calculators, congruence equation solvers, etc.). This could be the best available option for most novice "number theorists" who have limited knowledge, skills and resources. These sites are generally very easy to use and they are designed specifically to their declared functionalities. However, Internet sites also have their cons and disadvantages such as violation of privacy, potential hacking and malware infection, limited functionality (e.g. most sites put limitations on the size of the input data), and even non-availability (e.g. some functionalities may not be offered by any site on the Internet at least in its complete and direct form). They also have (seemingly more than others) the problem of reliability since some of these sites may provide wrong results.[6]

Anyway, anyone who works on number theory these days (at any level and for whatever reason and purpose) needs access to some sort of computing facilities and capabilities to deal with various aspects and issues (e.g. related to solving problems and verifying the obtained solutions) especially when dealing with exotic and eccentric problems (such as solving systems of large number of equations or dealing with very big numbers). Therefore, the issue of choosing and accessing proper computing tools and facilities should be considered carefully and thoughtfully before and during the engagement in number theory activities so that the work will be easier and more enjoyable and the success will be more plausible.

We therefore recommend investigating this issue and thinking about it carefully (as well as spending some time and effort on preparing the tools and facilities such as installing programming libraries which may require considerable amount of time and effort) before setting off and starting the work on number theory. This is especially important for those who work on big and long term projects (such as postgraduate students) who should not leave this issue to chance and coincidence. The time and effort spent on this issue will be well compensated and well rewarded later on since preparation in this regard (by having access to effective, efficient and reliable computing tools and facilities) will eventually save a lot of time and effort and provide more chances for success and progress.

1.3.3 Artificial Intelligence in Number Theory

Despite the recent achievements and progress, artificial intelligence is still in its infancy or childhood and hence it is not expected to offer much to number theory at this stage of development. For example, no one should expect artificial intelligence to be of use in proving theorems (beyond very basic level at most)[7] or solving open problems in number theory at this stage. However, it is useful to consider this as a potential tool during number theory investigations even at this early stage to be prepared for the future and to introduce this important tool to the areas of application and research related to number theory. For example, artificial intelligence could be useful in suggesting theorems or conjectures or proposing methods and approaches for tackling number theory problems and issues. It can also be useful at this early stage in complementary tasks and activities such as by helping in identifying patterns or gathering relevant information or testing and assessing possibilities.

A quick search on the Internet suggests that so far there are very few and primitive activities in this field. However, we may expect this situation to change in the near future due to the very quick advance in the field of artificial intelligence and its relentless invasion to many fields and areas which were beyond its reach just a few years ago, as well as the huge need for machine help to tackle perplexing problems in number theory which are so colossal that there is very little hope to be solved with the bare human intelligence of individuals and groups. The exponential growth and advancement in artificial intelligence

[6] I have (from my personal experience) many examples of wrong results obtained from such sites. For example, some sites use numerical routines to search for integers and because of limited accuracy they may provide incorrect integer solutions to Diophantine equations (for instance). So, the users of these sites should be vigilant and should always double check the obtained results.

[7] We mean "proving theorems" by analytic and direct ways using logical arguments. In fact, proving theorems by computers (even without use of artificial intelligence) is common for certain types of proof. For example, computers are used systematically to search for an example to prove a statement of existence or to search for a counterexample to disprove the generality of a statement (see § 1.5.4).

and the great need for its help in number theory (especially in the extreme and exotic areas of number theory) should justify the call for spending more resources on introducing artificial intelligence to number theory as soon as possible so that number theorists can benefit from this important tool and they are not left behind in the race for progress and achievement which is accelerated these days by artificial intelligence.

1.4 Solution of Mathematical Problems

There are many aspects related to solving mathematical problems in general and number theory problems in particular. In the following subsections we investigate some of these aspects.

1.4.1 Types of Solution

There are several types of "solution" to an unsolved mathematical problem. For example, a problem related to a suggested mathematical proposition or statement can be "solved" by:

1. Proving the statement is **right**.
2. Proving the statement is **wrong**.
3. Proving the problem is **unsolvable unconditionally** because of ambiguity or lack of sensibility or internal inconsistency or some other reason.
4. Proving the problem is **unsolvable conditionally**. For example, we may prove that a given mathematical theorem is unprovable by the existing mathematics (or the available tools and methods such as the required computing resources) although we cannot rule out the possibility of being solved in the future due to advancement and progress in mathematics (as well as methods, tools and technologies).[8]

These types could (and should) provide some criteria and conditions (as well as motivations and directions of research) about solving mathematical problems.

1.4.2 Existence of Solution

Based on the types and criteria which we set in § 1.4.1 about solving mathematical problems, it may be sensible to propose a principle which simply state: any problem in mathematics must have a solution (in the extended sense of solution as outlined in § 1.4.1). This should provide the basis and motivation for our search for a solution to any mathematical problem. In other words, we should believe (or convince ourselves) that we are capable of solving any mathematical problem in the extended sense of "solution". This principle is vital to justify our relentless attempts to solve any mathematical problem (even the most difficult and challenging ones) and keep our hope alive that we can find some sort of solution to any mathematical problem.

Restricting the meaning of "solution" to its direct sense will limit our opportunities for finding a solution. It will also diminish our hope and motivation and limit our direction of research and our awareness of potential existence of other types and possibilities of solution that we should always consider during our search for solutions. So in brief, when we start our investigation about a mathematical problem (especially the perplexing ones such as those recognized by the global mathematical community as open problems) we should consider (from the beginning to the end) all the possible types of solution and routes of investigation not only the direct ones. Awareness of this fact will open many new possibilities and increase the chance of success and reduce the chance of frustration and failure.

1.4.3 Partial Solution

There are many problems in mathematics (as well as in other fields) which have only partial solutions, e.g. by having solutions only in special cases or under certain conditions. For example, an unsolved

[8] Probably proving Fermat's last theorem is of this type where great mathematicians failed in the past to prove this theorem because mathematics in their time was not developed sufficiently to be able to tackle and solve this type of problems. In general, the possibility of non-existence of solution within the existing mathematics should provide the drive and motivation for the invention of new mathematical branches (or at least new mathematical methods and techniques within the existing mathematical branches) and hence it is hugely beneficial to mathematics.

number theory problem related to integers or prime numbers may be proved for certain types of integers or certain groups of prime numbers. In fact, many problems which have complete solutions have been solved gradually and stage by stage until their solution is completed. So, obtaining a partial solution is likely to be the first stage for obtaining a complete solution. Sometimes, the partial solution may prove to be the complete and final solution in the sense that the original proposition will be shown to be valid only for the specific cases which have already been proved.

1.4.4 The Role of Technology in the Search for Solution

In the old days, solving a mathematical problem is almost entirely dependent on bare human intelligence of individual mathematicians. However, these days solving mathematical problems is commonly aided by machines and technology mostly in the form of computers and computing in their diverse forms and capabilities (as well as being a group activity). For example, computers are commonly used to search for an example to prove an existence statement or to search for a counterexample to disprove a negation conjecture. In fact, these days some of such projects are done on a large scale involving many research groups (of professional mathematicians as well as amateurs) around the world.[9] As indicated earlier, we expect an increase in the future in our dependency on the help of machines and technology in our search for solutions to open problems in mathematics (as in other subjects and fields) especially with the expected rise and dominance of artificial intelligence (see § 1.3.3).

1.4.5 Learning from Previously-Solved Problems

It is very useful to keep in mind that many unsolved problems can be solved by learning from similar problems which were solved previously. So, it is a good investment of time (when tackling an unsolved problem) to search for and investigate previously solved problems to see if it is possible to apply the same or similar method of solution (possibly with some adaptation) to the unsolved problem.

1.5 Proof in Mathematics

We investigate in the following subsections some issues about the nature and use of proof in mathematics in general (including number theory which is the focus of our interest).

1.5.1 Importance of Proof in Mathematics

Mathematical proof is a painstaking business (especially when the target is a high quality and clear proof), and this could discourage some young mathematicians to go through proofs during their reading, or avoid creating their own proofs when they are asked to do so (and hence they just copy what they find in the books or on the Internet). However, it is important to know that mathematical proof is the spirit and soul of mathematics, and hence the "mathematicians" who avoid reading and creating proofs will miss a great deal of mathematical knowledge and mathematical skill that can be learned and acquired only through reading and practicing proofs. In fact, problem solving in most cases is no more than a form of mathematical proof, and hence any one who wants to be a proficient problem solver must learn to be a devotee proof reader and a competent proof creator.

1.5.2 Quality and Correctness of Proof

Not all proofs (whether individuals or types) are the same in quality. So, some proofs are stronger and more decisive or conclusive than others. In fact, mathematical proofs are (like anything else) susceptible to errors and mistakes (e.g. because of illusion or vagueness in definitions or bad symbolism or typo errors). So, being a mathematical proof is not a guarantee that it is correct (as beginners may think). In fact, the

[9] We should also mention distributed computing projects on the Internet which involve many amateur mathematicians and even ordinary people who participate through offering their support in non-specialist operations or by allowing the use of their machines in massive world-wide computing operations (e.g. in search for Mersenne primes; see § 2.2.2).

history of mathematics is full of examples of errors and mistakes committed even by great mathematicians in their proofs and arguments (as well as in their final products). Moreover, there are many controversies and differences in opinion between mathematicians about many things including proofs. So, it is always useful (and important) to inspect, examine and assess any given proof (whether old or novel) to see if it is robust and tight enough to be accepted or not.

1.5.3 Correctness of Proof and Correctness of Result

It is important to note that the correctness of proof and the correctness of result are correlated but not identical. Although the correctness of proof implies the correctness of result, the opposite is not true in general, i.e. the correctness of the result does not guarantee the correctness of the proof that is created to establish it. In fact, any correct result can be "proved" by a wrong argument. So, we should not be tolerant about the quality and rigor of our proof when we try to prove a result that we already know (or feel) it is correct. The correctness of the proof and the correctness of the results should be seen as two separate issues from this perspective, and hence the mistake in the proof should be considered to be as serious as the mistake in the final result. In fact, we can find many examples in the literature of wrong proofs or arguments used to establish statements which are known to be correct (e.g. they are proved already by other methods) where the laxity of the proof originates from the confidence about the correctness of the result.

Problems

1. Justify the above statement: any correct result can be "proved" by a wrong argument.
   Solution: This is because the correctness of the result is more general than the correctness of its proof. In fact, this is similar to the relation between cause (representing proof) and effect (representing result) where the existence of cause (corresponding to correctness of proof) leads to the existence of effect (corresponding to the correctness of result) but the absence of cause (corresponding to incorrectness of proof) does not necessarily lead to the absence of effect (corresponding to the incorrectness of result) because the effect can have another cause (corresponding to the result having another proof which is correct). For example, the existence of fire leads to the existence of heat but the absence of fire does not necessarily lead to the absence of heat because heat can be generated by causes other than fire such as friction. We may also find a (non-rigorous) analogy in the technicalities of conditional statement (see point 11 of § 1.1) where the correctness of the proof is a and the correctness of the result is b and hence $a \to b$ and $\overline{b} \to \overline{a}$ but not necessarily $\overline{a} \to \overline{b}$ or $b \to a$.

1.5.4 Methods of Proof

Anyone trying to solve a mathematical problem should be fully aware of the methods of proof so that he considers what is possible and relevant to use for solving the problem in hand. In this subsection we briefly investigate the main methods and types of proof which are commonly used in mathematics, and hence they should be considered when trying to tackle an unsolved mathematical problem. In fact, all these types and methods of proof are used in number theory which is the subject of our book (and hence they will be met in various places in this book).

Accordingly, it is important when tackling a number theory problem (involving proofs or arguments) to keep all these methods in mind so that they can be considered systematically (depending on the nature of the problem) to get the required proof. Being aware of the possible and available methods of proof may provide a hint or clue or insight about how to tackle the problem and could be the first step towards solving the problem.

In the following points we list and discuss briefly some of the methods which are commonly used by mathematicians to prove mathematical statements and propositions:[10]

[10] As indicated above, these methods will be met (in action) in our future investigations. We also note that these types and methods generally belong to different classifications and categorizations. Moreover, in many cases they are used in combination.

1. Proof by **direct method** is an argument made of a series of given or previously proved statements that lead eventually to the final result (which is what is required to prove). This (or some of its variations which are subject to more strict formalities) may be called proof by **deduction** which is directly based on logic (usually the rules of syllogism) to prove the truthfulness of the claimed statement.
2. Proof by **induction** is a method in which it is shown first that the proposition holds for a given integer m (usually 1), and it is shown second that if the proposition holds for an unidentified integer k then it also holds for $(k+1)$. The obvious result of these two steps is that the proposition holds for all integers $\geq m$ (and possibly for all integers).[11]
3. Proof by **contrapositive** (or **contraposition**) is a method in which a hypotheses (a) is shown to be false because its conclusion (b) is false.[12] This type of proof is based on the dependency of the truthfulness of contrapositive on the truthfulness of the corresponding conditional statement, i.e. if $a \to b$ then $\overline{b} \to \overline{a}$ (or rather $a \to b$ *iff* $\overline{b} \to \overline{a}$). Also see point 11 of § 1.1 and Problem 1 of § 1.5.3.
4. Proof by **contradiction** is a method in which the falsehood/truthfulness of a proposition is established by showing that the assumption that the proposition is true/false leads to contradiction. In fact, this type of proof (or some of its variants) may be seen as being based ultimately on the proof by contrapositive (which we investigated in point 3).[13]
5. Proof by **example** is a method used for proving a statement about existence. For example, if we want to prove the statement "there exists an odd number which is a perfect square" (or "there exists a perfect square which is odd" or "some odd numbers are perfect squares" or "some perfect squares are odd") then we can simply prove this by giving an example of such a number like 9.
6. Proof by **counterexample** is a method usually used for disproving the generality of a statement (i.e. proving that a given general statement is false in its generality). For example, if we want to disprove the statement "no perfect square is odd" (or "all perfect squares are even") then we can simply prove the falsehood of this claim by giving an example of an odd perfect square like 9.[14]
7. Proof by **exhaustion** (which may also be called **proof by cases**) is a method in which we consider all the possible cases of the proposition and prove the correctness (or otherwise) of the proposition in all these cases. For example, if we want to prove the proposition that the polynomial $(n^5 - n)$ is divisible by 5 for all $n \in \mathbb{Z}$, then we consider all the possible forms of n with regard to their divisibility by 5 (i.e. $5k$, $5k+1$, $5k+2$, $5k+3$, $5k+4$ where $k \in \mathbb{Z}$) and hence we prove that this polynomial is divisible by n for each one of these five possible forms.

Finally, it is worth noting the following points:

• The above types and methods of proof represent general classes and categories and hence we may find different variants (or "flavors") inside these classes and categories. Also, the distinction between some of these types and methods may not be clear cut and hence some proofs may be classified differently based on different criteria, considerations and formulations. So in brief, these types and methods of proof should be seen as generic prototypes rather than strict and rigorous species of proof.

• There are many types and methods of proof which are more specific or specialized and they mostly go under one of the main types and methods which we listed above (e.g. proof by infinite descent which may be classified as a special type of proof by contradiction; see Problem 3).

• In many mathematical proofs more than one method of proof are used in combination or in association

---

[11] In fact, there are many variations for the proof by induction (e.g. proving the proposition holds for $k+c$ instead of $k+1$ where c is a given constant integer). However, all these variations rest on the same logical foundation.

[12] Proof by contrapositive may also refer to the inference of a conditional statement from its contrapositive. For example, the statement $a \to b$ may be proved by proving its contrapositive $\overline{b} \to \overline{a}$ (noting that the contrapositive of $\overline{b} \to \overline{a}$ is $a \to b$ since $\overline{\overline{a}} = a$ and $\overline{\overline{b}} = b$ and hence if $\overline{b} \to \overline{a}$ is true/untrue then $a \to b$ is true/untrue due to the equivalence in truth between any statement and its contrapositive).

[13] We note that some variants of the proof by contradiction can be seen as a form or an instance of the direct method (which we investigated in point 1). In fact, we can identify many types and variants of proof by contradiction where the common feature of all these types and variants is the use of contradiction in the proof (see for instance the proof by infinite descent which will be mentioned in the end of this preamble and outlined in Problem 3).

[14] In fact, the proof by counterexample can be seen as a variant of the proof by example (which we investigated in point 5) because the negation of a general statement is an existence statement of its opposite (e.g. "no perfect square is odd" is negated by "there exists an odd perfect square").

to reach the final result.
• Many mathematical propositions and theorems can be proved by more than one method (i.e. independently). For example, a mathematical proposition can be proved by mathematical induction as well as by exhaustion. In fact, the topic of mathematical proof is very diverse and it has a strong element of art (rather than being a precise "science") and this should encourage the search for novel and improved versions of proof to old mathematical propositions (as well as to new propositions).

Problems

1. Give some examples for the use of some of the above methods of proof in this book.
   Solution: For example:
   • Proof by induction: see for instance Problem 1 of § 2.9.3 and Problem 1 of § 2.9.4.
   • Proof by contradiction: see for instance part (d) of Problem 12 of § 2.2 and Problem 3 of § 2.2.3.
   • Proof by counterexample: see for instance Problem 4 of § 2.7.
   • Proof by exhaustion: see for instance part (a) of Problem 12 of § 2.2,[15] point 5 of Problem 1 of § 2.6.4, point 1 of Problem 1 of § 2.6.5, and part (a) of Problem 5 of § 6.2.
2. Give an example for the use of combinations of some of the above methods of proof in this book.
   Solution: In part (a) of Problem 12 of § 2.2 we use a combination of proof by exhaustion and proof by contradiction.
3. Outline the method of infinite descent.
   Solution: The method of infinite descent (which is commonly used in the proofs related to the subject of Diophantine equations) is a special type of the proof by contradiction (which we outlined in point 4 in the preamble). The essence of this method is based on a simple idea (although the technical details of the method are usually very messy) whose essence is to start with an assumption of the existence of a minimal solution to a given equation within the domain of natural numbers where the subsequent arguments based on this assumption lead to the conclusion that we have a smaller solution to that equation than the presumed minimal solution, and this conclusion contradicts our earlier assumption of minimality.
   The method is usually used to prove that an equation has no solution. However, it may also be used to prove the existence of a solution smaller than a given solution of an equation (and even to find and construct this smaller solution). We refer the readers to the Problems of § 4.1.6 for some examples for the use of the method of infinite descent to prove the non-existence of solution to some types of non-linear Diophantine equations.

1.5.5 Conditional Proof

Sometimes a proposition P_2 can be proved if an unproven proposition P_1 is accepted (i.e. assumed true). This type of conditional proving is important for a number of reasons such as:
• It can be used when P_1 is proved later.
• It can lead to falsification of P_1 (by contradiction) if P_2 or some of its implications proved later to be false.
• It can help to draw the implications and consequences of P_1 and P_2.
• It can help to clarify the situation of P_1 and P_2 and their relation and hence it can lead to proving or disproving them (for instance).
So, this type of conditional proving should always be considered as an option (when applicable).

1.5.6 Partial Proof

In many cases a theorem (or statement or proposition) can be proved partly, i.e. its validity is established under certain conditions and restrictions or in special cases. In fact, this sort of partial proof usually lead to complete proof (if the theorem is actually correct unconditionally and in its generality). So, this type of partial proving should always be considered as an option (when applicable).

[15] In fact, this is also an example of proof by contradiction.

1.5.7 Proof Before and Proof After

The title of this subsection sounds odd and vague (which we do deliberately to draw the attention, especially of young mathematicians, to this important issue). Our intention here is that the usual way of using proof and the general conception about it is that it follows the creation or formation of a specific statement, i.e. we have a ready-made statement (e.g. obtained by a guess or a collection of examples or special cases) and we search for a proof to establish this statement. However, there is a more creative and aggressive way of using proof which is by trying to synthesize a proof to non-existing statement, and hence the creation of the proof will inevitably lead to the creation of a new statement (or theorem).

In fact, this sort of "preemptive" or "anticipatory" or "backward" proof is not only the most clever and "deceptive" (and possibly easy) way of creating proof but it is also an important method for creating new mathematics (i.e. by creating a new theorem or a new problem for instance as a result of the created proof). I believe that considerable part of mathematics is not created by an ingenious insight (i.e. into the result directly) but by certain tricks of creation one of which is this way of "proof before" or "proof first" (through trial and error for example). I also believe that prolific mathematicians are those who have discovered (or developed) and used some imaginative ways of inventing theorems using such indirect methods of creation such as by searching for (or rather synthesizing) proof before having any ready-made statement or result to prove.

1.6 Representation of Integers

The notation for representing integers in number theory depends on the base used in the representation (noting that the default notation is decimal, i.e. using base 10). Subscripts are usually used to indicate the base, e.g. $(251)_{16}$ means hexadecimal while $(251)_{10}$ means decimal (noting that the subscript, which represents the base, is always in decimal notation). However, because the default notation is decimal subscripts are generally ignored for decimal representation and hence 251 for instance means $(251)_{10}$ when other bases are not under consideration.

We list in the following some common rules and facts related to the representation of integers in various bases:

1. The digits used in the representation of integers in base b are $0, 1, \ldots, b-1$. For example, the digits $0, 1, 2, 3, 4$ are used in base 5 while the digits $0, 1, 2, \ldots, 9$ are used in base 10 (i.e. decimal).
2. If the base exceeds 10 then the uppercase Latin letters (i.e. $\mathrm{A}, \mathrm{B}, \mathrm{C}, \ldots$) are used to represent the digits exceeding 9. For example, in base 16 (i.e. hexadecimal) the letters $\mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}, \mathrm{E}, \mathrm{F}$ are used to represent the digits corresponding to $10, 11, 12, 13, 14, 15$ in decimal.
3. The most used bases (other than base 10, i.e. decimal, which is the mostly used base) are base 2 (binary), base 8 (octal) and base 16 (hexadecimal). This is because of their use in digital computers which are based on binary system (i.e. 0 and 1 bits) and its natural powers (i.e. 2^3 for octal and 2^4 for hexadecimal).
4. The conversion from one (non-decimal) base system to another (non-decimal) base system is usually done through the mediation of the decimal system due to the familiarity of decimal and its wide use which makes working in decimal "intuitive". For example, converting a base-7 number to a base-13 number is usually done by converting the base-7 number to decimal followed by converting the obtained decimal to the base-13 number. Yes, the conversion between systems of common basic base (e.g. octal and hexadecimal whose bases are natural powers of the basic base 2) can be done directly in a rather straightforward way.
5. A number expressed in base b represents a sum of its digits as multiples of integer powers of the base. For example, the number $d_n \ldots d_2 d_1 d_0$ in base b (where $d_n, \ldots, d_2, d_1, d_0$ are digits in base b) represents the following sum:

$$(d_n \ldots d_2 d_1 d_0)_b = (d_n \times b^n) + \cdots + (d_2 \times b^2) + (d_1 \times b^1) + (d_0 \times b^0)$$

6. The number $d_n \ldots d_m d_{m-1} \ldots d_2 d_1 d_0$ in any base can be written as a sum of a number trailing in m

zeros plus a number represented by its last m digits, that is:

$$d_n \dots d_m d_{m-1} \dots d_2 d_1 d_0 = d_n \dots d_m 0 \dots 000 + d_{m-1} \dots d_2 d_1 d_0$$

More generally, a number n can be decomposed into a sum of two or more numbers where the digits of n are distributed on these numbers (while keeping their positions) with the replacement of these digits by zeros in the other number(s). For example, we may decompose the number 123456 into the following 3 forms:

$$123456 = 103050 + 020406 = 120056 + 003400 = 120000 + 003400 + 000056$$

This "trick" (and its alike) can be useful in tackling and solving certain number theory problems (see for instance Problems 1 and 3 of § 6.15).

7. A number (represented in base b) has m trailing zeros (or more) *iff* it has a factor of b^m. For example, a binary number that has m trailing zeros (or more) should have a factor of 2^m, and a decimal number that has m trailing zeros (or more) should have a factor of 10^m. See Problem 15 of § 1.9.

Most of these rules and facts will become more clear by studying the following Problems (as well as the upcoming sections and chapters).

Problems

1. Express the following binary and hexadecimal numbers in decimal notation:[16]

   (**a**) $(110101)_2$. (**b**) $(1001110)_2$. (**c**) $(9367)_{16}$. (**d**) $(\text{C09BA1})_{16}$.

   Solution:

   (**a**)

   $$(110101)_2 = (1 \times 2^5) + (1 \times 2^4) + (0 \times 2^3) + (1 \times 2^2) + (0 \times 2^1) + (1 \times 2^0) = (53)_{10}$$

   (**b**)

   $$(1001110)_2 = (1 \times 2^6) + (0 \times 2^5) + (0 \times 2^4) + (1 \times 2^3) + (1 \times 2^2) + (1 \times 2^1) + (0 \times 2^0) = (78)_{10}$$

   (**c**)

   $$(9367)_{16} = (9 \times 16^3) + (3 \times 16^2) + (6 \times 16^1) + (7 \times 16^0) = (37735)_{10}$$

   (**d**)

   $$(\text{C09BA1})_{16} = (12 \times 16^5) + (0 \times 16^4) + (9 \times 16^3) + (11 \times 16^2) + (10 \times 16^1) + (1 \times 16^0) = (12622753)_{10}$$

2. Construct the octal expression of the decimal number $(267)_{10}$.

   Solution:

   $$\begin{aligned} 267 &= (33 \times 8) + 3 \\ 33 &= (4 \times 8) + 1 \\ 4 &= (0 \times 8) + 4 \\ \text{Hence:} \quad (267)_{10} &= (413)_8 \end{aligned}$$

3. Construct the hexadecimal expression of the octal number $(74105)_8$.

   Solution:

   $$\begin{aligned} (74105)_8 &= (7 \times 8^4) + (4 \times 8^3) + (1 \times 8^2) + (0 \times 8^1) + (5 \times 8^0) \\ &= (7 \times 2^{12}) + (4 \times 2^9) + (1 \times 2^6) + (0 \times 2^3) + (5 \times 2^0) \\ &= (7 \times 16^3) + (8 \times 16^2) + (4 \times 16^1) + 5 \\ \text{Hence:} \quad (74105)_8 &= (7845)_{16} \end{aligned}$$

[16] As we noted earlier, A, B, C, D, E, F in hexadecimal correspond to $10, 11, 12, 13, 14, 15$ in decimal. Also, when we do not use subscripts to indicate the base of the number it means it is decimal. For example, $(324)_{16}$ means hexadecimal while $(324)_{10}$ or (324) or 324 means decimal.

4. Find the base $b \in \mathbb{N}$ such that: $(5602)_b = (12001)_{10}$.
Solution:[17] From the notation of 5602 (i.e. it contains less digits than 12001) it is obvious that $b > 10$. On trying the few integers just above 10 (using for instance a spreadsheet) we get:

$$(5 \times 13^3) + (6 \times 13^2) + (0 \times 13^1) + (2 \times 13^0) = (12001)_{10}$$

i.e. $b = 13$.

1.7 Estimating the Magnitude of Big Integers

Estimating the magnitude of big integers means calculating them in an approximate fractional scientific form and not in their exact integer form. In other words, estimating their value and size rather than obtaining them as they are in their full-digit form. Although this is not a number theory problem or issue, it can be useful and even necessary in some number theory situations and contexts. For example, we may obtain (by using the methods and techniques of number theory) an integer in its exact integer form and we want to check that we did not make a big mistake in our procedures and calculations. In this case it is more easy (and is usually more reliable) to have an estimate of the magnitude of the number to see if it is reasonably close to the obtained integer value (which gives us confidence about our results and rules out the possibility of a big blunder although it does not prove that our result is correct) or not (which should indicate that we have made some big mistake and hence we need to redo our calculations). As an example, let us assume that we used the techniques of number theory (implemented, for instance, within some complicated computer algorithms and codes) to calculate the exact integer value of 23^{35} and we found that:

$$23^{35} = 45758761418148553734248853700452577779671963200 7 \simeq 4.5758761418 \times 10^{47}$$

To check this roughly, we use the techniques of logarithms to calculate this number approximately, that is:

$$\log_{10}(23^{35}) = 35 \log_{10}(23) \simeq 47.660474260616$$

and hence:

$$23^{35} = 10^{\log_{10}(23^{35})} \simeq 10^{47.660474260616} = 10^{0.660474260616} \times 10^{47} \simeq 4.5758761418 \times 10^{47}$$

As we see, this approximate result is of the same magnitude as the exact integer result and this should give us more confidence in our exact result although it cannot confirm the exact result entirely because the exact result contains more information about this number since it gives the exact value of each one of its digits and not only the magnitude of the number.

As the approximate non-integer calculations are usually much easier and simpler than their exact integer counterparts, such approximate calculations usually enjoy very high level of certainty and hence they provide reliable checks. Also see § 5.2.

We should finally note that those who have reasonable programming skills can (almost) always check the exact result of their calculations (obtained, for instance, by using certain algorithms or theorems or shortcuts) by writing rather simple computer codes that can manage and manipulate the individual digits of big numbers with the use of basic arithmetic operations. For example, if we want to calculate the exact value of 23^{35} then we can deal with this by writing a computer code that performs repetitive multiplication operations, i.e.

$$\overbrace{(((23 \times 23) \times 23) \times \cdots \times) \times 23}^{34 \text{ multiplications}}$$

where the result of each stage of multiplication is stored and used in the next stage of multiplication with 23 (applying arithmetic operations on the individual digits as done at elementary school level). This similarly applies to many other calculations of extreme enormity and nature. Of course, we can also use high-level

[17] We deliberately use a simple method of solution (noting that there are more formal methods).

computer languages that offer such capabilities or employ specialized numeric libraries or software for instance, although most of these tools and methods have certain limitations (e.g. on availability or on the size of the problem at hand) which are not usually encountered (or encountered less severely) when using the aforementioned basic method of writing simple computer codes. Moreover, the basic method should (in principle) provide a higher level of confidence since numeric libraries or software packages (for instance) are not as transparent and flexible as our own codes.[18]

Problems

1. Calculate the magnitude of the following numbers:

(**a**) 279^{562}. (**b**) $927!$. (**c**) C_{639}^{1362}. (**d**) P_{194}^{429}. (**e**) $13^{13^{13}}$.

Solution:

(**a**)

$$279^{562} = 10^{\log_{10}(279^{562})} = 10^{562\log_{10}(279)} = 10^{562\log_{10}(279)} \simeq 10^{1374.42956224} \simeq 2.68882316 \times 10^{1374}$$

(**b**)

$$927! = 10^{\log_{10}(927!)} = 10^{\sum_{k=1}^{927}\log_{10}(k)} \simeq 10^{2349.77459767} \simeq 5.95110578 \times 10^{2349}$$

(**c**)

$$\begin{aligned} C_{639}^{1362} &= \frac{1362!}{639!(1362-639)!} = \frac{1362!}{639!\,723!} \\ \log_{10} C_{639}^{1362} &= \log_{10}(1362!) - \log_{10}(639!) - \log_{10}(723!) \\ \log_{10} C_{639}^{1362} &= \sum_{k=1}^{1362}\log_{10}(k) - \sum_{k=1}^{639}\log_{10}(k) - \sum_{k=1}^{723}\log_{10}(k) \simeq 407.21278213 \\ C_{639}^{1362} &= 10^{\log_{10} C_{639}^{1362}} \simeq 10^{407.21278213} \simeq 1.63223292 \times 10^{407} \end{aligned}$$

(**d**)

$$\begin{aligned} P_{194}^{429} &= \frac{429!}{(429-194)!} = \frac{429!}{235!} \\ \log_{10} P_{194}^{429} &= \log_{10}(429!) - \log_{10}(235!) \\ \log_{10} P_{194}^{429} &= \sum_{k=1}^{429}\log_{10}(k) - \sum_{k=1}^{235}\log_{10}(k) \simeq 488.00072630 \\ P_{194}^{429} &= 10^{\log_{10} P_{194}^{429}} \simeq 10^{488.00072630} \simeq 1.00167376 \times 10^{488} \end{aligned}$$

(**e**)

$$\begin{aligned} \log_{10} 13^{13^{13}} &= 13^{13}\log_{10}(13) = 302875106592253\log_{10}(13) \simeq 337385711567664.82323 \\ 13^{13^{13}} &= 10^{\log_{10} 13^{13^{13}}} \simeq 10^{337385711567664.82323} \simeq 6.6563 \times 10^{337385711567664} \end{aligned}$$

1.8 General Rules

We list in the following some general rules which we use (mostly) in our future investigations (noting that some of these rules are obvious or trivial and some are useful as general knowledge that everyone interested in number theory should know):

1. Any linear combination of integers is integer, e.g. if $a, b, c, d \in \mathbb{Z}$ then $(ac \pm bd) \in \mathbb{Z}$. A product of integers can be seen as a special case of linear combination of integers.

[18] In fact, the level of confidence should also depend on our experience and skill in coding as well as the level of confidence in the other tools (e.g. numeric libraries) according to our past experience or public opinion.

2. Every prime number (other than 2) is odd.
3. If a prime number p divides a product (say mn) then p must divide at least one of the two factors (i.e. m or n).[19]
4. The rules of **addition and subtraction of odd and even numbers** are as follows:

$$\text{odd} \pm \text{odd} = \text{even} \qquad \text{odd} \pm \text{even} = \text{odd} \qquad \text{even} \pm \text{even} = \text{even} \tag{1}$$

   The rules of adding/subtracting more than two odd/even numbers can be obtained simply by carrying the operations in stages considering a pair in each stage,[20] e.g. odd±odd±even = (odd±odd)±even = even ± even = even.
5. From rule 4 we can conclude that two integers have the same parity *iff* their algebraic sum is even and have opposite parity *iff* their algebraic sum is odd.
6. The rules of **multiplication of odd and even numbers** are as follows:

$$\text{odd} \times \text{odd} = \text{odd} \qquad \text{odd} \times \text{even} = \text{even} \qquad \text{even} \times \text{even} = \text{even} \tag{2}$$

   The rules of multiplying more than two odd/even numbers can be obtained simply by carrying the operations in stages considering a pair in each stage,[21] e.g. odd × odd × even = (odd × odd) × even = odd × even = even.[22] It is obvious that the positive powers of integers are subject to the rules of multiplication (since $m^n = m \times \cdots \times m$), and hence the parity of the power is the same as the parity of its base (i.e. the positive powers of odd/even are odd/even; also see point 10).
7. The rules of **division of odd and even numbers** (assuming divisibility) are:

$$\frac{\text{odd}}{\text{odd}} = \text{odd} \qquad \frac{\text{even}}{\text{odd}} = \text{even} \tag{3}$$

   No specific rules can be set for the division of even by even (e.g. 16/4 is even while 12/4 is odd). No odd number is divisible by an even number.
8. From rule 6 we can conclude that any odd number can be written only as a product of odd numbers (i.e. no odd number can be written as a product of odd × even or as a product of even × even). On the other hand (noting that 1 is odd), we can conclude that any even number can be written as a product of odd × even. Now, if we note that all even numbers must contain factors of 2, we can conclude that all non-zero even numbers can be written as $2^n \times$ odd ($n \in \mathbb{N}$).
9. If two integer quantities (i.e. numbers, variables, etc.) are equal then they must have the same parity (i.e. both odd or both even), and hence (by contraposition) if two integer quantities are of different parity then they cannot be equal (i.e. no even can be equal to odd).[23]
10. Raising an integer to a non-negative integer power does not change its parity except if the number is non-zero even and the power in 0 (noting that any non-zero integer raised to zero is 1). On the other hand, taking the n^{th} root ($\mathbb{N} \ni n > 1$) of an integer (when the n^{th} root is an integer) does not change its parity.
11. If a number ending in $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ is squared it ends in $0, 1, 4, 9, 6, 5, 6, 9, 4, 1$. As a result, no perfect square ends in $2, 3, 7, 8$.[24]
12. All natural powers of integers ending in 1 end in 1.
13. Natural odd powers of 4 end in 4 and natural even powers of 4 end in 6.

[19] This is because p is prime and hence it cannot be split between the two factors. Therefore, it must be contained (in its entirety) in one of these factors (at least) which means that p divides one of these factors.

[20] This is based on what we may consider as: "associativity of addition with regard to parity".

[21] This is based on what we may consider as: "associativity of multiplication with regard to parity".

[22] A simpler approach to determine the parity of a product of integers is to use the fact that: a product of integers is even *iff* (at least) one of the multiplicands is even (and hence it is odd otherwise).

[23] This is based on the fact that the parity of an integer is unique, i.e. every integer has exactly one parity and hence any integer is either odd or even (but not none or both). This is because any integer is either divisible by 2 (and hence it is even) or not divisible by 2 (and hence it is odd) noting that the remainder of the division of an integer by 2 is either 0 or 1.

[24] This can be used as a test to exclude non-perfect squares.

14. All natural powers of 5 end in 5. All natural powers > 1 of 5 end in 25.
15. All natural powers of integers ending in 5 end in 5. Natural even powers of integers ending in 5 end in 25.
16. All natural powers of 6 end in 6.
17. All natural powers of integers ending in 6 end in 6.
18. Natural odd powers of 9 end in 9 and natural even powers of 9 end in 1.
19. The last digit of the sum of two natural numbers is the last digit of the sum of their last digits. For example, the last digit of $2378 + 495$ is 3 because $8 + 5 = 13$ whose last digit is 3.
20. The last digit of the difference $(m - n)$ of two (distinct) natural numbers $(m, n \in \mathbb{N})$ is determined as follows (where d is the last digit of the difference, d_m is the last digit of m, and d_n is the last digit of n):
    • If $m > n$ and $d_m \geq d_n$ then $d = d_m - d_n$. For example, the last digit of $(5-2)$ or $(55-2)$ or $(55-32)$ is 3 because $5 - 2 = 3$.[25]
    • If $m > n$ and $d_m < d_n$ then $d = (10 + d_m) - d_n$. For example, the last digit of $(55 - 7)$ or $(55 - 37)$ is 8 because $15 - 7 = 8$.
    • If $m < n$ then the last digit is the same as the last digit of $(n - m)$, and hence it can be obtained from the first two points (with reversing of labels).
21. The last digit of the product of two integers is the last digit of the product of their last digits (e.g. the last digit of 23×16 is 8 because $3 \times 6 = 18$ which ends in 8). In fact, rules 11-18 (related to last digit) are no more than (direct or indirect) results and applications of this principle. For instance, rule 12 is because natural powers are no more than repetitive multiplications where each multiplication preserves 1 (as a last digit of the product) since 1 is the last digit of its multiplicands (noting that $1 \times 1 = 1$) and hence 1 is preserved (as a last digit) in the final product (i.e. the natural power). This logic similarly applies to rules 14-17 (related to last digit).
22. If $m = \mu k + r_m$ and $n = \nu k + r_n$ (where $m, n, k, \mu, \nu, r_m, r_n \in \mathbb{Z}$, $0 \leq r_m < |\mu|$ and $0 \leq r_n < |\nu|$) then the remainder of $(m + n) \div k$ is equal to the remainder of $(r_m + r_n) \div k$ $(k > 0)$.
23. All factorials are integers.
24. All factorials are even numbers (excluding 0! and 1!).
25. The **number of permutations**[26] given by:

$$P_m^n = \frac{n!}{(n-m)!} = n \times (n-1) \times \cdots \times (n-m+1) \qquad (n, m \in \mathbb{Z} \text{ and } 0 \leq m \leq n) \qquad (4)$$

    is always integer.
26. The **binomial coefficient**[27] given by:

$$C_m^n = \frac{n!}{m!(n-m)!} = \frac{n \times (n-1) \times \cdots \times (n-m+1)}{m!} \qquad (n, m \in \mathbb{Z} \text{ and } 0 \leq m \leq n) \qquad (5)$$

    is always integer.
27. The **multinomial coefficient**[28] given by:

$$C_{n_1, n_2, \ldots, n_k}^n = \frac{n!}{n_1!\, n_2! \ldots n_k!} \qquad (n, n_1, n_2, \ldots, n_k \in \mathbb{N}^0 \text{ and } n = n_1 + n_2 + \cdots + n_k) \qquad (6)$$

    is always integer.

[25] For the determination of relative size (or order) of m and n (i.e. whether $m > n$ or $m < n$) when dealing with very big numbers (e.g. $m = 7^{4523}$ and $n = 69^{1891}$) especially when they are of different formats (e.g. $m = 245!$ and $n = 348^{99}$), we can use the methods of estimating the magnitude of big integers (some of which were investigated in § 1.7).

[26] The number of permutations P_m^n is the number of distinct arrangements (or configurations) of m objects that can be formed (separately) from a set of n different objects.

[27] The binomial coefficient C_m^n is the number of combinations of sets, i.e. the number of distinct m-size sets that can be obtained (separately) from a set of n different objects.

[28] The multinomial coefficient $C_{n_1, n_2, \ldots, n_k}^n$ is the number of possible partitions of a set of size n into k sets of size $n_1, n_2, \ldots, n_k$. It can also be defined as the number of distinct permutations of n objects with repetitions (i.e. repetition of n_1 objects, repetition of n_2 objects, ..., repetition of n_k objects).

28. The n^{th} root ($\mathbb{N} \ni n > 1$) of an integer (when such a root exists in $\mathbb{R}$) is either an integer (i.e. when the integer is an n^{th} power of an integer) or irrational.

Problems

1. Show that the number of permutations P_m^n is always integer.
   Solution: This can be seen from the second equality of Eq. 4 since P_m^n is a product of integers (see rule 1 in the preamble).
2. Show that the binomial coefficient C_m^n and the multinomial coefficient $C_{n_1,n_2,\ldots,n_k}^n$ are always integers.
   Solution: Regarding the binomial coefficient, we can prove this formally in several ways, but we do not need to do this. Instead, we can use its combinatorial meaning by arguing that C_m^n represents the number of combinations of sets (i.e. the number of m-size sets in an n-size set) and hence by definition it is an integer.[29]
   Regarding the multinomial coefficient, we can prove this formally but we do not need to do this. Instead, we can use its combinatorial meaning (see footnote [28]) to show that it is an integer by definition (as we did for the binomial coefficient). We may also argue that $C_{n_1,n_2,\ldots,n_k}^n$ can be expanded as a product of binomial coefficients (which are integers according to rule 26) and hence it must be an integer.
3. Show that C_m^n divides P_m^n.
   Solution: From Eqs. 4 and 5 we have $P_m^n/C_m^n = m!$ and hence C_m^n divides P_m^n (since $m!$ is an integer).
4. Show that if n is odd then n^2 has remainder 1 on division by 4, while if n is even then n^2 is divisible by 4 (i.e. it has remainder 0 on division by 4).
   Solution: If n is odd then it has the form $n = 2k + 1$ ($k \in \mathbb{Z}$), and hence:

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$$

   So, n^2 has remainder 1 on division by 4 since it is a multiple of 4 plus 1.
   If n is even then it has the form $n = 2k$ ($k \in \mathbb{Z}$), and hence:

$$n^2 = (2k)^2 = 4k^2$$

   So, n^2 is divisible by 4 since it is a multiple of 4.
5. Determine if it is possible to have m, n such that:
   (**a**) $m^2 - 11m - 19 = n^4 + 3n^2 - 2 \quad (m, n \in \mathbb{Z})$. (**b**) $17^m - 36^m = 13^n - 45^n \quad (m, n \in \mathbb{N}^0)$.
   Solution:
   (**a**) It is impossible because $(m^2 - 11m - 19)$ is odd for all $m \in \mathbb{Z}$, while $(n^4 + 3n^2 - 2)$ is even for all $n \in \mathbb{Z}$ (see the rules of parity in the preamble of this section).
   (**b**) If $m \neq 0$ and $n \neq 0$ then $(17^m - 36^m)$ is odd and $(13^n - 45^n)$ is even, i.e. for all $m, n \in \mathbb{N}$ (see the rules of parity in the preamble of this section). If $m = 0$ and $n \neq 0$ or $m \neq 0$ and $n = 0$ then the equality is obviously not true (because zero cannot equal non-zero). Yes, if $m = n = 0$ then the equality is true because $1 - 1 = 1 - 1$. So, the only m, n that satisfy this equation is $m = n = 0$.
6. Show that 2^{2k} ends either in 4 or in 6 where $k \in \mathbb{N}$.
   Solution: We have $2^{2k} = (2^2)^k = 4^k$. Hence, by rule 13 (see the preamble) 2^{2k} ends either in 4 or in 6 (i.e. 2^{2k} ends in 4 when k is odd and 2^{2k} ends in 6 when k is even).

1.9 Divisibility Rules

We list in the following some divisibility rules which we use in the future investigations (noting that $m, n, k, r \in \mathbb{Z}$):
1. $m|0$ when $m \neq 0$, i.e. 0 is divisible by any other integer.[30]
2. $\pm 1|m$, i.e. any integer is divisible by ± 1.
3. $m| \pm 1 \leftrightarrow m = \pm 1$.
4. $m|m \quad (m \neq 0)$.

[29] See our book "Introduction to the Probability Theory" for further details about these issues.
[30] Some may add to this: $0|m$ *iff* $m = 0$.

5. $m|m^n \quad (m \neq 0, n \in \mathbb{N})$.
6. $m|n \to m|n^k \quad (m \neq 0, k \in \mathbb{N})$.
7. $m^k|n \to m|n \quad (m \neq 0, k \in \mathbb{N})$.
8. $m|n$ and $k|r \to mk|nr$.[31]
9. $m|n$ and $n|m \to m = \pm n$.
10. $m|n$ and $n|k \to m|k$.
11. $m|n \to |m| \leq |n| \quad (m, n \neq 0)$.
12. $m|n$ *iff* $(-m)|n$.
13. $m|n$ *iff* $m|(-n)$.
14. $k|m$ and $k|n \to k|(m \pm n)$. More generally, $k|m$ and $k|n \to k|(cm \pm dn)$ (where $c, d \in \mathbb{Z}$).
15. $k\not|(m \pm n) \to k\not|m$ or $k\not|n$.[32]
16. $k|m$ and $k|(m \pm n) \to k|n$.
17. $k|m$ and $k\not|n \to k\not|(m \pm n)$.
18. $m|n \to m|kn$.
19. $mn|k \to m|k$ and $n|k$.
20. $m|k$ and $n|k \leftrightarrow mn|k$ (m and n are coprime).
21. $m|nk \to m|k$ (m and n are coprime).
22. $p|(n_1 n_2 \dots n_k) \leftrightarrow p|n_i$ for some $1 \leq i \leq k$ (p is prime).
23. $m|n \leftrightarrow m^t|n^t$ ($m, n \in \mathbb{Z}$ and $t \in \mathbb{N}$).
24. An integer is divisible by 2 *iff* its last digit (i.e. unit digit) is divisible by 2 (i.e. it is 0,2,4,6, or 8).[33]
25. An integer is divisible by 3 *iff* the sum of its digits is divisible by 3.
26. An integer is divisible by 4 *iff* its last two digits are divisible by 4.
27. An integer is divisible by 5 *iff* its last digit is divisible by 5 (i.e. it is 0 or 5).
28. An integer is divisible by 6 *iff* it is divisible by 2 and 3.
29. An integer is divisible by 7 *iff* the difference between twice its last digit and its remaining part is divisible by 7.
30. An integer is divisible by 8 *iff* its last three digits are divisible by 8.[34]
31. An integer is divisible by 9 *iff* the sum of its digits is divisible by 9.
32. An integer is divisible by 10 *iff* its last digit is divisible by 10 (i.e. it is 0). Alternatively, an integer is divisible by 10 *iff* it is divisible by 2 and 5.
33. An integer is divisible by 11 *iff* the alternating sum (i.e. $+-$) of its digits is divisible by 11.
34. An integer is divisible by 12 *iff* it is divisible by 3 and 4.
35. An integer is divisible by 13 *iff* 4 times its last digit plus its remaining part is divisible by 13.[35]
36. An integer is divisible by 14 *iff* it is divisible by 2 and 7.
37. An integer is divisible by 15 *iff* it is divisible by 3 and 5.
38. An integer is divisible by 16 *iff* its last four digits are divisible by 16.
39. For the previous rules that include a test, the procedure of the test can be repeated when the number is large to obtain a small number (eventually) that is easy to determine its divisibility.[36]
40. An integer is divisible by 10^n *iff* its last n digits are 0.
41. An integer is divisible by 2^n *iff* its last n digits are divisible by 2^n.
42. An integer is divisible by 5^n *iff* its last n digits are divisible by 5^n.

---

[31] This is trivially generalized to more than two cases by repeated application of this rule. This note also applies to similar rules (e.g. rules 14 and 20).

[32] This is the contrapositive of rule 14.

[33] We note that this rule (and the following rules) are generally based on assuming the number to be in its decimal representation (see § 1.6).

[34] If the number is less than three digits then we add zeros to the left to complete three. This applies to similar rules (e.g. rules 26, 38 and 41).

[35] There are other variants of this method as well as other methods for testing the divisibility by 13.

[36] For example, to determine the divisibility of 5494 by 13 we do the following:

$$549 + (4 \times 4) = 565 \qquad 56 + (4 \times 5) = 76 \qquad 7 + (4 \times 6) = 31$$

and hence we conclude that 5494 is not divisible by 13 because 31 is not divisible by 13.

43. An integer whose digits are identical is divisible by 11 *iff* it has an even number of digits.[37]
44. A product of m consecutive integers is divisible by m.
45. A product of m consecutive integers is divisible by $m!$.
46. If $0 < m \leq n$ then m divides $n!$ and $m!$ divides $n!$ (i.e. $n! = Km$ and $n! = m!\,k$ where $m, n, K, k \in \mathbb{N}$).
47. If $p > n$ then $p \not| n!$ (where $p \in \mathbb{P}$ and $n \in \mathbb{N}$). This is because p cannot be a factor of $n!$ since it is greater than n.
48. For a number to be divisible by b^m (where b is the base in its representation), the number must have at least m trailing zeros in that representation (see rule 7 of § 1.6 as well as Problem 15 of this section).
49. The difference of two integers ends in m zeros (and hence it is divisible by 10^m) *iff* the last m digits of these integers are identical.
50. In any three consecutive odd numbers exactly one of them is divisible by 3.
51. The remainder of the division of the polynomial expression $P(x)$ by the linear expression $(x - a)$ is equal to $P(a)$.

Problems

1. Justify rule 24.[38]
   Solution: This rule is obvious because a number is divisible by 2 *iff* it is even which requires its last digit to be one of the even digits.
2. Justify rules 25 and 31.
   Solution: Let us represent the number (i.e. in its decimal form) as $d_k \ldots d_2 d_1 d_0$ where $d_k, \ldots, d_2, d_1, d_0$ are the digits of the number. Now, if we expand this number (i.e. in powers of 10 since it is in decimal) then we have:

$$\begin{aligned} d_k \ldots d_2 d_1 d_0 &= d_k(10^k) + \ldots + d_2(10^2) + d_1(10^1) + d_0 \\ &= d_k(9 \cdots 9 + 1) + \ldots + d_2(99 + 1) + d_1(9 + 1) + d_0 \\ &= (9 \cdots 9 d_k + \ldots + 99 d_2 + 9 d_1) + (d_k + \ldots + d_2 + d_1 + d_0) \\ &= \Big[9(1 \cdots 1 d_k + \ldots + 11 d_2 + d_1)\Big] + (d_k + \ldots + d_2 + d_1 + d_0) \end{aligned}$$

   As we see, the sum inside the first (square) brackets is obviously divisible by 3 (and 9) because of the common factor of 9, so the number is divisible by 3 (and 9) *iff* the sum inside the second brackets is divisible by 3 (and 9), as required by rule 25 (and rule 31).[39]
3. Justify rules 28, 32, 34, 36, and 37.
   Solution: These rules are justified by rule 20 noting that $(2, 3)$, $(2, 5)$, $(3, 4)$, $(2, 7)$ and $(3, 5)$ are coprime.
4. Justify rule 40.
   Solution: If we represent the number as $d_k \ldots d_n d_{n-1} \ldots d_2 d_1 d_0$ then we have:

$$d_k \ldots d_n d_{n-1} \ldots d_2 d_1 d_0 = d_k \ldots d_n 0 \ldots 000 = (d_k \ldots d_n) \times 10^n$$

   and hence it is divisible by 10^n (which is a factor of it). The converse is proved by reversing the argument.
5. Justify rule 41 (and hence rules 26, 30 and 38).
   Solution: If we represent the number as $d_k \ldots d_n d_{n-1} \ldots d_2 d_1 d_0$ and split it as a sum then we have:

$$d_k \ldots d_n d_{n-1} \ldots d_2 d_1 d_0 = (d_k \ldots d_n 0 \ldots 000) + (d_{n-1} \ldots d_2 d_1 d_0)$$

[37] This rule is about multi-digit non-zero integer.

[38] Before we start working on these Problems we draw the attention of the readers that some of the proofs and justifications of the divisibility rules (which we will investigate in the following Problems) are generally based on an implicit assumption that the numbers are positive (i.e. $\in \mathbb{N}$). However, this does not affect the generality of these rules in their applicability to all integers (i.e. to all numbers $\in \mathbb{Z}$) because the divisibility of an integer is independent of its sign and the sign of its divisor (see rules 12 and 13 in the preamble) and noting as well that 0 is divisible by any other integer.

[39] We are implicitly using rules 14 and 16 in this argument.

Now, the first term ends in n zeros and hence (by rule 40) it is divisible by $10^n = 2^n \times 5^n$, i.e. it is divisible by 2^n. So, the number is divisible by 2^n *iff* the second term is divisible by 2^n (see rules 14 and 16). This should also justify rules 26, 30 and 38 which are instances of this rule.

6. Justify rule 42.
   Solution: The justification is identical to the justification of Problem 5 (with 2^n being replaced by 5^n).
7. Justify rule 29.
   Solution: Let us represent the number (i.e. in its decimal form) as $d_k \dots d_2 d_1 d_0$ where $d_k, \dots, d_2, d_1, d_0$ are the digits of the number. Now, if we expand this number (i.e. in powers of 10 since it is in decimal) then we have:
   $$d_k \dots d_2 d_1 d_0 = d_k(10^k) + \dots + d_2(10^2) + d_1(10^1) + d_0$$
   So, if this number is divisible by 7 then it must be a multiple of 7, i.e.
   $$\begin{aligned}
   7n &= d_k(10^k) + \dots + d_2(10^2) + d_1(10^1) + d_0 && (n \in \mathbb{N})\\
   7n &= \big[d_k(10^k) + \dots + d_2(10^2) + d_1(10^1) + d_0\big] + 20d_0 - 20d_0 && (\pm 20d_0)\\
   7n &= \big[d_k(10^k) + \dots + d_2(10^2) + d_1(10^1) - 20d_0\big] + 21d_0\\
   7n - 21d_0 &= \big[d_k(10^k) + \dots + d_2(10^2) + d_1(10^1) - 20d_0\big]\\
   7(n - 3d_0) &= 10\,\big[d_k(10^{k-1}) + \dots + d_2(10^1) + d_1(10^0) - 2d_0\big]\\
   7(n - 3d_0) &= 10\big[d_k \dots d_2 d_1 - 2d_0\big] && (\text{decimal representation})
   \end{aligned}$$
   Now, 7 must divide the right hand side (since it is a factor on the left hand side), and since it is coprime to 10 it must divide the difference inside the square brackets (see rule 21). However, the difference inside the square brackets is just the difference between twice the last digit of the number and its remaining part. This means that the divisibility of the number by 7 (as expressed by $7n$) and the divisibility of the difference inside the square brackets by 7 are equivalent, as required.
8. Justify rule 33.
   Solution: Let us represent the number (i.e. in its decimal form) as $d_k \dots d_2 d_1 d_0$ where $d_k, \dots, d_2, d_1, d_0$ are the digits of the number. Now, if we expand this number (i.e. in powers of 10 since it is in decimal) then we have:
   $$\begin{aligned}
   d_k \dots d_2 d_1 d_0 &= d_k(10^k) + \dots + d_2(10^2) + d_1(10^1) + d_0 = \sum_{i=0}^{k} 10^i d_i\\
   &= \left[\sum_{i \text{ even}} (10^i - 1)d_i + d_i\right] + \left[\sum_{i \text{ odd}} (10^i + 1)d_i - d_i\right]\\
   &= \left[\sum_{i \text{ even}} (10^i - 1)d_i\right] + \left[\sum_{i \text{ odd}} (10^i + 1)d_i\right] + \left[\sum_{i=0}^{k} (-1)^i d_i\right]
   \end{aligned}$$
   Now, the sum inside the first and second (square) brackets in the last equality is divisible by 11 (see the upcoming note). So, the divisibility of this number (i.e. $d_k \dots d_2 d_1 d_0$) by 11 and the divisibility of the algebraic sum inside the third (square) brackets by 11 are equivalent (see rules 14 and 16). However, the algebraic sum inside the third brackets is just the alternating sum of its digits. This means that the divisibility of the number by 11 and the divisibility of the alternating sum of its digits by 11 are equivalent, as required.
   Note: for **even** i, $(10^i - 1)$ is a number made of i 9's (e.g. for $i = 0, 2, 4, 6$ we have $10^i - 1 = 0, 99, 9999, 999999$ respectively) and hence it can be expressed as:[40]
   $$99 \cdots 99 = 09 \cdots 09 + 90 \cdots 90 = 11 \times 09 \cdots 09$$

[40] We note that any number in any base can be written as a sum of two numbers made of consecutive zero and non-zero digits (see point 6 of § 1.6). For example, 123456 can be written as $123456 = 103050 + 020406$.

For example, for $i = 0, 2, 4, 6, \ldots$ we have:

$$10^0 - 1 = 11 \times 0 \qquad 10^2 - 1 = 11 \times 9 \qquad 10^4 - 1 = 11 \times 909 \qquad 10^6 - 1 = 11 \times 90909$$

and so on. So, $(10^i - 1)$ is divisible by 11 and hence the sum $\sum_{i \text{ even}}(10^i - 1)d_i$ is divisible by 11.
For **odd** i, we have $(10^i + 1) = 10^i - 10 + 11 = 10(10^{i-1} - 1) + 11$ which is divisible by 11 $\big[$noting that $(10^{i-1} - 1)$ is divisible by 11 since $(i - 1)$ is even and hence the proof of the even i (which we already presented) applies$\big]$. Hence, the sum $\sum_{i \text{ odd}}(10^i + 1)d_i$ is divisible by 11.

9. Justify rule 35.
Solution: Let us represent the number (i.e. in its decimal form) as $d_k \ldots d_2 d_1 d_0$ where $d_k, \ldots, d_2, d_1, d_0$ are the digits of the number. Now, if we expand this number (i.e. in powers of 10 since it is in decimal) then we have:
$$d_k \ldots d_2 d_1 d_0 = d_k(10^k) + \ldots + d_2(10^2) + d_1(10^1) + d_0$$
So, if this number is divisible by 13 then it must be a multiple of 13, i.e.
$$\begin{aligned}
13n &= d_k(10^k) + \ldots + d_2(10^2) + d_1(10^1) + d_0 && (n \in \mathbb{N}) \\
13n &= \big[d_k(10^k) + \ldots + d_2(10^2) + d_1(10^1) + d_0\big] + 40d_0 - 40d_0 && (\pm 40d_0) \\
13n &= \big[d_k(10^k) + \ldots + d_2(10^2) + d_1(10^1) + 40d_0\big] - 39d_0 \\
13n + 39d_0 &= \big[d_k(10^k) + \ldots + d_2(10^2) + d_1(10^1) + 40d_0\big] \\
13(n + 3d_0) &= 10\,\big[d_k(10^{k-1}) + \ldots + d_2(10^1) + d_1(10^0) + 4d_0\big] \\
13(n + 3d_0) &= 10\,[d_k \ldots d_2 d_1 + 4d_0] && \text{(decimal representation)}
\end{aligned}$$
Now, 13 must divide the right hand side (since it is a factor on the left hand side), and since it is coprime to 10 it must divide the sum inside the square brackets (see rule 21). However, the sum inside the square brackets is just the sum of 4 times the number's last digit plus its remaining part. This means that the divisibility of the number by 13 (as expressed by $13n$) and the divisibility of the sum inside the square brackets by 13 are equivalent, as required.

10. Justify rule 39.
Solution: If the divisibility rule applies to the original number then it should also apply to the number obtained from the prescribed procedure (which implements the rule) noting that the two numbers supposedly have the same divisibility property (e.g. being divisible by 7). This argument should also apply to the other numbers which are obtained consecutively from applying the procedure repeatedly.

11. Justify rule 43.
Solution: This is a direct result of rule 33 because if the number of digits is even then the alternating sum is 0 (which is divisible by 11), while if the number of digits is odd then the alternating sum is a single-digit non-zero number (noting that the rule is about multi-digit non-zero integers) and hence it is not divisible by 11 (since $1, 2, \ldots, 9$ are not divisible by 11).

12. Justify rule 44.
Solution: This is because m successive integers must include a multiple of m and hence their product must be divisible by m.
Note: rule 44 is weaker than rule 45 and hence the argument of rule 45 (which will be given in Problem 13) should also justify rule 44.

13. Justify rule 45.
Solution: This is because the product of m successive integers (ignoring their sign which does not affect divisibility and assuming they do not include 0) divided by $m!$ is a binomial coefficient which is an integer (see rule 26 of § 1.8). If the m successive integers include zero then the product is zero which is divisible by any other number.

14. Justify rule 46.
Solution: If $m = n$ then this is obvious because m divides $m!$ (since m is a factor of $m!$) and $m!$ divides $m!$ (by rule 4).[41] If $m < n$ then m divides $m!$ and $m!$ divides $m!$ (which we already justified) and

[41] In fact, if $m = n$ then this rule is a special case for rules 44 and 45 (which we already justified in the last two Problems) noting that $n!$ (which is equal to $m!$) is a product of m consecutive integers.

hence m divides $n!$ and $m!$ divides $n!$ because $m!$ is a factor of $n!$ (see rule 18).

15. Show the following:
(**a**) A number expressed in base b is divisible by b *iff* its last digit (in base b) is zero.
(**b**) A number expressed in base b is divisible by b^n *iff* its representation in base b ends in n zeros.
Solution:
(**a**) This is because a number in base b can be written as:

$$\begin{aligned}(d_k \dots d_2 d_1 d_0)_b &= d_k(b^k) + \dots + d_2(b^2) + d_1(b^1) + d_0 \\ &= b\left[d_k(b^{k-1}) + \dots + d_2(b^1) + d_1\right] + d_0\end{aligned}$$

and hence it is divisible by b *iff* d_0 is divisible by b (see rules 14 and 16). Now, if we note that in base b we have $0 \leq d_0 < b$ then the divisibility of d_0 by b means $d_0 = 0$.[42]
(**b**) This is because if a number in base b ends in n zeros then it can be written as:

$$\begin{aligned}(d_k \dots d_n d_{n-1} \dots d_2 d_1 d_0)_b &= (d_k \dots d_n 0 \dots 000)_b \\ &= d_k(b^k) + \dots + d_n(b^n) + 0(b^{n-1}) + \dots + 0(b^2) + 0(b^1) + 0 \\ &= d_k(b^k) + \dots + d_n(b^n) \\ &= b^n\left[d_k(b^{k-n}) + \dots + d_n\right]\end{aligned}$$

and hence it must be divisible by b^n. The converse of this conditional statement can be proved by reversing the argument.

16. Show that in any three consecutive odd numbers exactly one of them is divisible by 3.
Solution: Let the numbers be k, $k+2$ and $k+4$ (where k is odd). Now, the remainder r of k when it is divided by 3 is either 0 or 1 or 2. If $r = 0$ then k is divisible by 3 while $k+2$ and $k+4$ are not. If $r = 1$ then $k+2$ is divisible by 3 while k and $k+4$ are not. If $r = 2$ then $k+4$ is divisible by 3 while k and $k+2$ are not.

17. Show that the remainder of $(7^n + 7) \div 4$ is 2 for odd n and is 0 for even n ($n \in \mathbb{N}^0$).
Solution: We prove this by induction (see § 1.5.4).
Regarding odd n, the remainder of $(7^1 + 7) \div 4$ is 2. Now, let assume that the remainder of $(7^n + 7) \div 4$ is 2 for a given odd $n = 2k + 1$ ($k \in \mathbb{N}$) and we will show that the remainder of the next odd n [i.e. $n = 2(k+1) + 1 = 2k + 3$] must also be 2, that is:

$$7^{2k+3} + 7 = (7^2 \times 7^{2k+1}) + 7 = (49 \times 7^{2k+1}) + 7 = (48 \times 7^{2k+1}) + (7^{2k+1} + 7)$$

Now, $(48 \times 7^{2k+1})$ is divisible by 4 (since 48 is divisible by 4) and hence the remainder of $(7^{2k+3} + 7) \div 4$ is the same as the remainder of $(7^{2k+1} + 7) \div 4$ which is 2 according to our assumption. So, by mathematical induction the remainder of $(7^n + 7) \div 4$ is 2 for all odd n.
Regarding even n, the remainder of $(7^0 + 7) \div 4$ is 0. Now, let assume that the remainder of $(7^n + 7) \div 4$ is 0 for a given even $n = 2k$ ($k \in \mathbb{N}$) and we will show that the remainder of the next even n [i.e. $n = 2(k+1) = 2k + 2$] must also be 0, that is:

$$7^{2k+2} + 7 = (7^2 \times 7^{2k}) + 7 = (49 \times 7^{2k}) + 7 = (48 \times 7^{2k}) + (7^{2k} + 7) \tag{7}$$

Now, (48×7^{2k}) is divisible by 4 and hence the remainder of $(7^{2k+2} + 7) \div 4$ is the same as the remainder of $(7^{2k} + 7) \div 4$ which is 0 according to our assumption. So, by mathematical induction the remainder of $(7^n + 7) \div 4$ is 0 for all even n.

18. Justify the following proposition: a natural number has an even number of (positive) divisors unless it is a perfect square (in which case it has an odd number of divisors).
Solution: We have three (comprehensive and mutually exclusive) cases to consider:
• The natural number is 1: noting that 1 is a perfect square (since $1 = 1^2$) and it has only one positive

[42] It is worth noting that the statement in part (a) is a special case of the statement in part (b) and hence the proof of (b) should establish (a) as well.

divisor (which is 1), this proposition is true.
• The natural number is prime: noting that a prime number cannot be a perfect square and it has exactly two positive divisors (i.e. 1 and itself), this proposition is also true.
• The natural number is composite: the divisors of any composite number come in pairs because the quotient of the division of the number by any one of its divisors is also a divisor, e.g. if d is a divisor of n then n/d is also a divisor of n because $n/(n/d) = d$. Now, since the divisors come in pairs then their number must be even, i.e. a composite number has an even number of divisors. However, if the number is a perfect square then there is a single divisor (i.e. the square root of the number) which is paired to itself and hence we have a number of pairs plus 1 which means that the number of divisors in this case is odd, i.e. the number of divisors of a perfect square is odd. So, this proposition is also true in this case.
So, this proposition is true in all these three cases and hence it is true in general (i.e. it applies to all natural numbers). Also see Problem 3 of § 2.6.3.

19. Show the following:
(**a**) If $n \in \mathbb{N}$ and $d_1, \ldots, d_k$ are its positive divisors (including 1 and n) in increasing order and $D_1, \ldots, D_k$ are its positive divisors (including 1 and n) in decreasing order then there is a one-to-one correspondence between $d_1, \ldots, d_k$ and $D_1, \ldots, D_k$ such that $d_i D_i = n$ $(i = 1, \ldots, k)$.
(**b**) If $n \in \mathbb{N}$ and d represents the positive divisors of n (including 1 and n) then:

$$\sum_{d|n} d = \sum_{d|n} \frac{n}{d} \tag{8}$$

(**c**) If $n \in \mathbb{N}$ and d represents the positive divisors of n (including 1 and n) then:

$$\sum_{d|n} \frac{1}{d} = \sum_{d|n} \frac{d}{n} \tag{9}$$

Solution:
(**a**) If we note that the quotient of a (non-zero) number by one of its divisors is also a divisor (see Problem 18) then this proposition becomes obvious because of the ordering of $d_1, \ldots, d_k$ and $D_1, \ldots, D_k$ which means that an increase in d's must correspond to a decrease in D's (noting that $n/d_i = D_i$) and hence their product remains constant, i.e. $d_i D_i = n$ $(i = 1, \ldots, k)$.
(**b**) If d on the left hand side of Eq. 8 represents d_i's (of part a) and d on the right hand side of Eq. 8 represents D_i's (of part a) then the proposition is justified by part (a) because $d_i = n/D_i$ $(i = 1, \ldots, k)$ and hence the two sums are equal (and actually have identical terms).
(**c**) Again, if d on the left hand side of Eq. 9 represents d_i's (of part a) and d on the right hand side of Eq. 9 represents D_i's (of part a) then the proposition is justified by part (a) because $1/d_i = D_i/n$ $(i = 1, \ldots, k)$ and hence the two sums are equal (and actually have identical terms).

20. Prove rule 23.
Solution: If $m|n$ then n/m is an integer and hence its t^{th} power is an integer (see rule 1 of § 1.8), i.e. $(n/m)^t = n^t/m^t$ is an integer which means $m^t|n^t$.
If $m^t|n^t$ then $n^t/m^t = (n/m)^t$ is an integer and hence its t^{th} root (which is n/m) must be an integer because it is not irrational (see rule 28 of § 1.8), i.e. $m|n$.

1.10 General Identities

We list in the following a number of mathematical identities which we need to refer to in the future. Most of these identities can be found (with their proofs) in the literature of elementary algebra and calculus and hence we take them for granted (although we will prove some of them as an exercise).

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}) \qquad (n = 2, 3, 4, \ldots) \tag{10}$$

$$x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + \cdots - xy^{n-2} + y^{n-1}) \qquad (n = 3, 5, 7, \ldots) \tag{11}$$

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1) \qquad (n = 2, 3, 4, \ldots) \qquad (12)$$

$$(x+y)^n = \sum_{k=0}^{n} C_k^n x^k y^{n-k} \qquad (n \in \mathbb{N}) \qquad (13)$$

$$(x_1 + \cdots + x_k)^n = \sum_{\forall\ n_1+\cdots+n_k=n} C_{n_1,\ldots,n_k}^n\, x_1^{n_1} \ldots x_k^{n_k} \qquad (n \in \mathbb{N}) \qquad (14)$$

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2} \qquad (n \in \mathbb{N}) \qquad (15)$$

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6} \qquad (n \in \mathbb{N}) \qquad (16)$$

$$\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4} \qquad (n \in \mathbb{N}) \qquad (17)$$

$$\sum_{k=1}^{n} k^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30} \qquad (n \in \mathbb{N}) \qquad (18)$$

$$\sum_{k=1}^{n} k^5 = \frac{n^2(n+1)^2(2n^2+2n-1)}{12} \qquad (n \in \mathbb{N}) \qquad (19)$$

$$\sum_{k=1}^{n} (2k-1)^3 = n^2(2n^2-1) \qquad (n \in \mathbb{N}) \qquad (20)$$

$$\sum_{k=0}^{n} C_k^n = 2^n \qquad (n \in \mathbb{N}^0) \qquad (21)$$

$$\sum_{k=0}^{n} ar^k = a\left(\frac{r^{n+1}-1}{r-1}\right) \qquad (n \in \mathbb{N}^0) \qquad (22)$$

We note that Eqs. 13, 14 and 22 represent (respectively) the binomial theorem, the multinomial theorem and the geometric series, while Eq. 15 represents an instance (or special case) of arithmetic series.

Problems

1. Prove the identities of:
   (**a**) Eq. 10. (**b**) Eq. 11. (**c**) Eq. 12.
   Solution:
   (**a**) We have:

$$\begin{aligned} x(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}) &= x^n + x^{n-1}y + \cdots + xy^{n-1} \\ y(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}) &= x^{n-1}y + \cdots + xy^{n-1} + y^n \end{aligned}$$

   By subtracting the second equation from the first (side by side) we get the identity of Eq. 10.
   (**b**) For $n = 3, 5, 7, \ldots$ we have $x^n + y^n = x^n - (-y)^n$, i.e. this identity is an instance of the identity of Eq. 10 (corresponding to $n = 3, 5, 7, \ldots$ with the replacement of y by $-y$) and hence the proof of part (a) is sufficient.
   (**c**) This identity is a special case of the identity of Eq. 10 (corresponding to $y = 1$) and hence the proof of part (a) is sufficient.
2. Prove the identities of Eqs. 15-17.
   Solution: We use induction noting that all these identities are satisfied for $n = 1$ and hence all we need to do is to show that if they are valid for n then they are valid for $n + 1$.

$$\frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)\big[n+2\big]}{2} = \frac{(n+1)\big[(n+1)+1\big]}{2}$$

$$\begin{aligned}\frac{n(n+1)(2n+1)}{6}+(n+1)^2 &= \frac{n(n+1)(2n+1)+6(n+1)^2}{6}=\frac{(n+1)\big[n(2n+1)+6(n+1)\big]}{6}\\ &= \frac{(n+1)\big[2n^2+7n+6\big]}{6}=\frac{(n+1)(n+2)(2n+3)}{6}\\ &= \frac{(n+1)\big[(n+1)+1\big]\big[2(n+1)+1\big]}{6}\end{aligned}$$

$$\begin{aligned}\frac{n^2(n+1)^2}{4}+(n+1)^3 &= \frac{n^2(n+1)^2+4(n+1)^3}{4}=\frac{(n+1)^2\big[n^2+4(n+1)\big]}{4}\\ &= \frac{(n+1)^2\big[n^2+4n+4\big]}{4}=\frac{(n+1)^2\big[n+2\big]^2}{4}=\frac{(n+1)^2\big[(n+1)+1\big]^2}{4}\end{aligned}$$

As we see, all these relations are valid for $n+1$ if we assume their validity for n, and hence by mathematical induction they are valid for all $n \in \mathbb{N}$.

1.11 Simple Checks and Tests

The calculations and considerations in number theory usually involve unusual operations and attributes as well as eccentric numbers (both as input and as output) and hence they are more likely to be affected by errors (or mistakes or bugs or wrong judgments or ...) than ordinary calculations and considerations. So, it is important to have some simple and general tests (or procedures or regulations) which can be used as initial checks (or guidelines or rules of thumb) to rule out the possibility of big blunders committed during these calculations and considerations and affected the obtained results (or alternatively detecting and identifying such blunders). Although passing these types of checks and tests usually does not guarantee the correctness of the obtained results, it can increase the confidence in the obtained results substantially especially if they are used collectively and in combination (noting that they are usually conclusive in detecting errors and mistakes if they are not passed). We give in the following points some examples of these simple general checks (and will illustrate their use in the Problems):

• Calculating the magnitude of the expected result and compare it to the magnitude of the obtained result (see § 1.7).

• Checking the parity of the obtained result to see if it is correct according to the rules of parity (see § 1.8) or not.

• Conducting simple divisibility checks using basic divisibility rules (see § 1.9). For example, we may apply simple divisibility rules (like the rule of divisibility by 3) to rule out primality (i.e. being prime).

• Counting the number of digits to see if it is commensurate to the expected magnitude of the result.

So, the general advice to anyone working on number theory is to keep such simple tests and rules always in mind and use them systematically before trying any sophisticated tests or approaches as they can save considerable amount of time and effort. In fact, these tests and rules (and their alike) should always be considered (when relevant) as the first attempt to solve number theory problems, and hence they should not be considered only as tests and checks for already-obtained results. For example, if we are asked to find the general solution of the equation $n^4+4n^3-7n^2-12n+7=0$ in integers (i.e. $n \in \mathbb{Z}$) then before we try to solve this problem by using the rules and methods of solving polynomial equations we should simply check the parity of this polynomial, and hence we can easily conclude (by checking the parity) that this equation has no solution because the polynomial is odd and hence it cannot be equal to 0 which is even.[43] So in brief, these tests and rules should always be considered as the first resort when tackling any number theory problem as well as the first resort when checking and testing the validity of the obtained result of any number theory problem.

[43] It is useful to note that $n^4+4n^3-7n^2-12n+7=0$ has a solution in non-integers (e.g. real numbers or complex numbers) because the rules of parity applies only to the set of integers and its subsets (noting that being odd or even is an attribute of integers but not of real numbers or complex numbers).

Problems

1. Conduct initial checks on the following results:
   (**a**) $47^{71} = 52353764298962037499714614674899404237532566015059076993264$.
   (**b**) $12^{39} = 32248096399742387088189629625125355105812 48$.
   (**c**) $5^{4^3} = 54210108624275221700372640043497085571289 0620$.
   Solution: All these results are wrong because:
   (**a**) The obtained result contains much less digits than what we should expect because the number of digits of the obtained result is 59 while the actual number of digits cannot be less that 71 (assuming base 10). Moreover, 47^{71} is odd (see rule 6 of § 1.8) while the obtained result is even.
   (**b**) The magnitude of 12^{39} (using the rules of logarithms; see § 1.7) is 1.2248×10^{42} while the magnitude of the obtained result is 3.2248×10^{42}.
   (**c**) 5^{4^3} must end in 5 (see rule 14 of § 1.8) while the obtained result ends in 0.
2. As a result of a certain argument or assumption, we concluded that 23744612803137 is prime. Assess this conclusion.
   Solution: The sum of digits of this number is 51 and hence it is divisible by 3 (see rule 25 of § 1.9). So, it is not prime.
3. Find all the solutions of the equation: $n^5 - 13n^2 + 1 = m^9 - m$ (where $m, n \in \mathbb{Z}$).
   Solution: According to the rules of parity (see § 1.8), $n^5 - 13n^2 + 1$ is odd while $m^9 - m$ is even and hence the equality cannot be satisfied by any $m, n \in \mathbb{Z}$. So, this equation has no solution in integers.

Chapter 2
The Basics of Number Theory

In this chapter we present a short introduction to number theory at its basic and elementary level. This introduction will provide the necessary background for the majority of our subsequent investigations and applications. More elaborations will follow as we progress in this book.

2.1 The Fundamental Theorem of Arithmetic

The fundamental theorem of arithmetic states: every natural number greater than 1 is either a prime or can be factored as a product of two or more prime numbers in a unique way except for the order of the factors. Accordingly, if m is a positive non-prime number (i.e. composite) then it can be written uniquely as:

$$m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} \tag{23}$$

where $p_1, p_2, \dots, p_k$ are prime numbers and $a_1, a_2, \dots, a_k$ are positive integers. This way of expressing a composite integer m as a product of its powered prime factors $p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ is called **prime factorization** (or **prime decomposition**) of m. An integer $m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ is **square free** if none of $a_1, a_2, \dots, a_k$ in its prime factorization is greater than 1.

It is useful to note the following:

1. In the above statement of the fundamental theorem of arithmetic, "two or more" does not require being distinct, i.e. they can be distinct or non-distinct (totally or in part). Yes, in Eq. 23 we generally assume $p_1, p_2, \dots, p_k$ to be distinct to have a unique form.
2. The above form of prime factorization (as given by Eq. 23 and within the stated conditions) may be called "standard prime factorization" to distinguish it from non-standard prime factorization when some of $a_1, a_2, \dots, a_k$ are allowed to be zero for certain purposes (some of which will be met later on; see for instance point 2 of § 2.4 and point 2 of § 2.5).
3. The proofs of the fundamental theorem of arithmetic that we found in the literature of number theory are generally based on propositions (or assumptions) which are not more obvious or better established than the fundamental theorem itself. Therefore, in our view it may be better to consider the fundamental theorem of arithmetic as an axiom (of number theory) from which other results are derived. However, we will outline in the Problems the essence of the common proof in the literature.
4. Prime factorization (as defined above) is restricted to composite numbers which (by definition) are restricted to non-prime natural numbers > 1. However, in many contexts and arguments we need to extend and widen the concept of prime factorization to include 0, 1, primes and negative integers. So, let us agree (as a convention) that the "prime factorization" of 0 is 0, of 1 is 1, of $p \in \mathbb{P}$ is p, and of $\mathbb{Z} \ni n < 0$ is the same as the prime factorization of $|n|$.

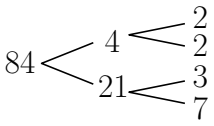
Problems

1. Prove the fundamental theorem of arithmetic.
   Solution: We note first that in this "proof" we need to accept (or assume) rule 22 of § 1.9 (or rather just one part of this rule). So, let n be a natural number > 1.
   If n is prime then that is it.
   If n is composite then we need to show the *existence* of a prime factorization of n and the *uniqueness* of this prime factorization.
   Regarding existence, it should be self-evident because it is a matter of definition (based on the concept of divisibility) since n is presumably composite.[44]

[44] Some try to prove existence by induction which (in our view) is nonsensical or at least superfluous.

Regarding uniqueness, let n have two prime factorizations, i.e. $n = p_1p_2 \dots p_m = q_1q_2 \dots q_k$ where we did not use indicial notation and hence the p's are not necessarily distinct of each other and similarly the q's are not necessarily distinct of each other. Now, by rule 22 of § 1.9 a given p_i $(1 \leq i \leq m)$ must divide a given q_j $(1 \leq j \leq k)$ or vice versa (since $p_i|n = q_1q_2 \dots q_k$ and $q_j|n = p_1p_2 \dots p_m$), and hence they must be identical (since they are prime) which means that they can be canceled from both sides. On repeating this process of cancellation we end up either with $p_ap_f \dots p_s = 1$ or $q_bq_d \dots q_z = 1$ or $1 = 1$. The first and second cases are impossible because the p's and q's are greater than 1 (since they are primes), and hence we must end up with $1 = 1$ which proves that the two prime factorizations are identical except, possibly, for the order of their factors (as required).

2. List some common methods of prime factorization (i.e. how to obtain the prime factorization of a given composite number).
Solution: There are two main methods (which are similar and can be seen as identical in essence):
• The **direct method** (or **upside-down division method**) where we divide the given number repeatedly by the smallest and smallest primes (i.e. 2 then 3 then 5 then 7 and so on, each conducted repetitively if necessary) and record the prime divisors until the result of the division (i.e. the quotient) is prime. For example, if we want to prime-factorize 84 by this method then we divide 84 by 2 (since it is even) to get 42, then we divide 42 by 2 (since it is even) to get 21, then we divide 21 by 3 (since it is divisible by 3) to get 7, and we stop here because 7 is prime and hence it cannot be divided further. Accordingly, $84 = 2^2 \times 3 \times 7$.
• The **factor tree method** where the given number is put at the root of a tree which branches repeatedly to its factors until we reach the prime factors at the end of the tree. For example, if we want to prime-factorize 84 by this method then we produce a tree like the following (where the prime factors of 84 are at the end branches of this tree, i.e. 2,2,3,7 and accordingly $84 = 2^2 \times 3 \times 7$):



Note: the focus of this problem is "generic methods" (outlining the factorization process) not "algorithms".

3. Give a form (or formula) that represents all the positive divisors of a given natural number m.
Solution: If m is given in its prime decomposition as $m = p_1^{a_1}p_2^{a_2} \cdots p_k^{a_k}$ $(a_i \in \mathbb{N},\ 1 \leq i \leq k)$ then all the positive divisors of m are represented by the following form:

$$p_1^{b_1}p_2^{b_2} \cdots p_k^{b_k} \qquad (b_i \in \mathbb{N}^0,\ b_i \leq a_i,\ 1 \leq i \leq k)$$

where we consider all the possible combinations of b_i (also see Problem 3 of § 2.6.1). For example, $1800 = 2^3 \times 3^2 \times 5^2$ and hence its positive divisors are:

$2^0 \times 3^0 \times 5^0 = 1$	$2^1 \times 3^0 \times 5^0 = 2$	$2^0 \times 3^1 \times 5^0 = 3$	$2^0 \times 3^0 \times 5^1 = 5$
$2^1 \times 3^1 \times 5^0 = 6$	$2^1 \times 3^0 \times 5^1 = 10$	$2^0 \times 3^1 \times 5^1 = 15$	$2^1 \times 3^1 \times 5^1 = 30$
$2^2 \times 3^0 \times 5^0 = 4$	$2^0 \times 3^2 \times 5^0 = 9$	$2^0 \times 3^0 \times 5^2 = 25$	$2^2 \times 3^1 \times 5^0 = 12$
$2^2 \times 3^0 \times 5^1 = 20$	$2^1 \times 3^2 \times 5^0 = 18$	$2^0 \times 3^2 \times 5^1 = 45$	$2^1 \times 3^0 \times 5^2 = 50$
$2^0 \times 3^1 \times 5^2 = 75$	$2^2 \times 3^1 \times 5^1 = 60$	$2^1 \times 3^2 \times 5^1 = 90$	$2^1 \times 3^1 \times 5^2 = 150$
$2^2 \times 3^2 \times 5^0 = 36$	$2^2 \times 3^0 \times 5^2 = 100$	$2^0 \times 3^2 \times 5^2 = 225$	$2^2 \times 3^2 \times 5^1 = 180$
$2^2 \times 3^1 \times 5^2 = 300$	$2^1 \times 3^2 \times 5^2 = 450$	$2^2 \times 3^2 \times 5^2 = 900$	$2^3 \times 3^0 \times 5^0 = 8$
$2^3 \times 3^1 \times 5^0 = 24$	$2^3 \times 3^0 \times 5^1 = 40$	$2^3 \times 3^1 \times 5^1 = 120$	$2^3 \times 3^2 \times 5^0 = 72$
$2^3 \times 3^0 \times 5^2 = 200$	$2^3 \times 3^2 \times 5^1 = 360$	$2^3 \times 3^1 \times 5^2 = 600$	$2^3 \times 3^2 \times 5^2 = 1800$

2.2 Prime, Coprime and Composite Numbers

Prime number (or **prime** for short) is a natural number greater than 1 that is divisible only by 1 and itself (considering only the positive divisors). The first few primes are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$. Non-prime natural numbers (excluding 1) are described as **composite**. Two integers (or natural numbers)[45] are described as **coprime** or **relatively prime** if there is no integer > 1 that divides them both. In other words, their greatest common divisor (gcd) is 1. A set of integers $\{m_1, m_2, \ldots, m_k\}$ $(k > 2)$ are described as **pairwise relatively primes** (or **pairwise coprimes**) if each pair in the set are relatively prime, i.e. $\gcd(m_i, m_j) = 1$ for all $1 \leq i < j \leq k$. For example, the numbers $5, 9, 28$ are pairwise relatively primes because $\gcd(5, 9) = \gcd(5, 28) = \gcd(9, 28) = 1$.

In the following points we provide some useful remarks about prime, coprime and composite numbers:

1. All non-negative integers are either prime or composite except 0 and 1 which are neither.[46]
2. There are infinitely many primes (see part a of Problem 12).[47]
3. All primes are odd except 2 (and hence all even numbers greater than 2 are composite). So, "odd primes" means all primes except 2.
4. The numbers 2 and 3 are the only consecutive primes (i.e. all other successive primes must be separated by at least one composite number).
5. Primes become sparser (i.e. less frequent) as we go higher on the ladder of number line. However, the gap between successive primes varies unpredictably.
6. If $n \in \mathbb{N}$ is a composite number then n has a prime divisor $\leq \sqrt{n}$. As a result (i.e. by contraposition), if $n \in \mathbb{N}$ does not have a prime divisor $\leq \sqrt{n}$ then n is prime.
7. A set of integers $\{m_1, m_2, \ldots, m_k\}$ $(k > 2)$ may be described as mutually relatively primes (or mutually coprimes) if there is no integer > 1 that divides them all, i.e. $\gcd(m_1, m_2, \ldots, m_k) = 1$. However, we should note that being mutually relatively prime (according to this convention) is weaker than being pairwise relatively primes (or pairwise coprimes), i.e. pairwise relatively primes are necessarily mutually relatively primes but not vice versa. For instance, $2, 3, 4$ are mutually relatively primes because $\gcd(2, 3, 4) = 1$ but they are not pairwise relatively primes because $\gcd(2, 4) = 2 \neq 1$. In general, if a pair of $\{m_1, m_2, \ldots, m_k\}$ is relatively prime then $\{m_1, m_2, \ldots, m_k\}$ are mutually relatively primes because $\gcd(m_1, m_2, \ldots, m_k) = 1$ (see rules 6 and 11 of § 2.4).
8. From a pedagogical viewpoint, we may describe prime numbers as the "atoms of the chemistry of number theory", and describe composite numbers as the "molecules of this chemistry".[48] In other words, primes are the basic building blocks of the structure of numbers (i.e. integers) which are the subject of number theory. This basic analogy can be easily elaborated (if required).

Problems

1. List some common facts about coprime and pairwise relatively prime numbers.
   Solution: For example (noting that some of these facts are just variants of other facts):
   (**a**) m and n are coprime *iff* their greatest common divisor is 1.
   (**b**) m and n are coprime *iff* their least common multiple is mn (assuming lcm exists, i.e. $mn \neq 0$).
   (**c**) m and n are coprime *iff* there is no prime number that can divide them both.
   (**d**) m and n are coprime *iff* there is no common factor in their prime factorization.[49]
   (**e**) m and n are coprime to k *iff* their product mn is coprime to k.
   (**f**) m and n are coprime *iff* $sm + tn = 1$ for some $s, t \in \mathbb{Z}$ (see § 2.3.4).
   (**g**) 1 is coprime to all numbers (i.e. integers or natural numbers).

[45] Being integers or natural numbers seems to follow different conventions.

[46] This statement means (partly) that a positive integer > 1 must be either prime or composite in the sense that it cannot be neither or both. In fact, this statement represents the essence of the fundamental theorem of arithmetic (see § 2.1) although the fundamental theorem has more content than this.

[47] Of course, there are infinitely many composites. However, this statement is trivial since we can synthesize infinite number of composites from a finite number of primes let alone from an infinite number of primes.

[48] We may also describe primes as "elements" and composites as "compounds" of this chemistry.

[49] We note that prime factorization of a given *composite* number is to express the number as a product of its prime factors, e.g. the prime factorization of 12 is $2^2 \times 3$. However, in this statement (and its alike) we should generalize the concept of "prime factorization" to include prime numbers, e.g. the prime factorization of 3 is 3.

(**h**) Any two consecutive integers are coprime.
(**i**) No two even numbers can be coprime (i.e. coprimes must be either both odd or one odd and one even).
(**j**) Any two (or more) distinct primes are (pairwise) coprimes (but coprimes are not necessarily primes).
(**k**) $p \not| m$ *iff* p and m are coprime (where $p \in \mathbb{P}$ and $m \in \mathbb{Z}$ or $m \in \mathbb{N}$).
(**l**) If coprimality applies to integers (i.e. not only to natural numbers) then 0 is coprime to none of the non-zero integers except ± 1.
(**m**) The natural powers of distinct primes are coprime (see part n of Problem 12).
(**n**) m and n are coprime *iff* m^s and n^t are coprime (where $s, t \in \mathbb{N}$; see part l of Problem 12).

2. List some classifications of primality tests (i.e. tests used to identify that a given number is prime).
Solution: There are many possible classifications for primality tests. For example:[50]
• They can be classified as deterministic versus non-deterministic (i.e. probabilistic or stochastic).
• They can be classified as tests for primality versus tests for non-primality (i.e. to negate primality and hence they are actually composity tests).[51]
• They can be classified as analytical versus computational (or algorithmic).[52]
• They can also be classified according to their individual characteristics and properties. For example, we have **direct test** (or trial division test) which is the simplest primality test where we divide the suspected number n by all the prime numbers between 2 and $\sqrt{n}$ and hence if it is divisible by none of these primes then it must be prime. We also have tests based on **using certain number theoretic theorems** (such as Wilson's theorem or Fermat's little theorem; see § 2.9.1 and § 2.9.3) which give primality conditions or signs that can be used analytically or computationally to test for primality or non-primality.[53]
We should finally note that composity tests can be used as an indirect primality tests and vice versa (i.e. proving/disproving primality/composity leads to disproving/proving composity/primality). So, the classification as primality test or composity test is rather artificial and depends on the contexts and objectives. Also see Problem 3.

3. List some quick composity tests (i.e. simple tests or signs for showing that a given integer is not prime).
Solution: For example:
• An integer whose last digit is $0, 2, 4, 5, 6, 8$ is composite (because it is either even or divisible by 5).[54]
In other words, prime numbers must end in $1, 3, 7, 9$ (and this can be seen as a preliminary "primality test" in the sense of being a necessary but not sufficient condition for primality).
• Simple divisibility tests (such as those given in § 1.9) can be used as quick tests for being composite. For example, the number 1308981471 is obviously composite because the sum of its digits is divisible by 3 (see rule 25 of § 1.9).
• No two consecutive integers (except 2 and 3) can be both prime. So, if we know (or assume) that $m > 3$ is prime then $m - 1$ and $m + 1$ must be composite (because m is odd and hence $m - 1$ and $m + 1$ must be even and greater than 2 and hence they are necessarily composite noting that 2 is the only even prime).

4. Show that the following numbers are composite:
(**a**) $13^{7612} + 23^{3784}$. (**b**) $3176^{238} - 9^{4296}$. (**c**) $73^{1937} + 40^{1937}$. (**d**) $442^{851} - 923^{627}$.
Solution:

[50] We note that these classifications are based on different criteria and hence a single test usually belongs to more than one category corresponding to different classifications.
[51] In fact, composity tests can be tests on their own (i.e. to identify composite numbers) rather than being indirect tests for primality, i.e. to negate primality (see Problem 3).
[52] We note that primality tests of very big numbers are generally programmed and hence conducted by computers (even if they are analytical in nature). We also note that computational tests are usually based on analytical criteria and conditions.
[53] Because Wilson's theorem is an *iff* statement it can be used directly, while because Fermat's little theorem is an if statement it is used indirectly (i.e. its contrapositive is used to negate primality and hence it is actually a composity test). These issues will be clarified further later on.
[54] We note that we should exclude 0 (because it is neither prime nor composite), 2 (because it is prime) and 5 (because it is prime) although their "last" digits are $0, 2, 5$.

(**a**) This is the sum of two odd numbers and hence it is even (> 2) and thus it is composite (see the parity rules in § 1.8).
(**b**) 3176^{238} ends in 6 (see rule 17 of § 1.8) and 9^{4296} ends in 1 (see rule 18 of § 1.8) and hence their difference ends in 5 (see rule 20 of § 1.8), i.e. it is divisible by 5 (see rule 27 of § 1.9) and hence it is composite.
(**c**) According to Eq. 11 this sum has a factor of $(73 + 40) = 113$ and hence it is composite.
(**d**) Both 442 and 923 are divisible by 13 and hence 442^{851} and 923^{627} are divisible by (powers of) 13. So, their difference is divisible by 13 (see rule 14 of § 1.9) and hence it is composite.

5. List some methods for finding primes, i.e. methods to search for and find primes collectively within a given range by sieving primes or composites within that range (such as all primes less than 1000).
Solution: For example:
• The **direct method** by testing the individual numbers for primality or composity using some of the primality or/and composity tests (such as some of the tests listed or mentioned in Problems 2 and 3).
• The **sieve of Eratosthenes** which will be outlined in § 2.3.1.
• The **sieve of Sundaram**.
• The **sieve of Atkin**.
Note: these methods are generally computational in nature (i.e. they are usually programmed and conducted by computers). Accordingly, these methods (and their alike and variants) are beyond the scope of this book (or at least the scope of this volume). So, the interested readers should refer to the literature for details (noting that the purpose of this Problem is general knowledge and awareness which is useful and necessary for anyone interested in number theory and in prime numbers in particular).
6. Show that if n is composite then it mus have a prime divisor $\leq \sqrt{n}$.
Solution: Since n is composite then it must have at least one prime divisor p and hence $n = pm$ ($m \in \mathbb{N}$). Now:
• If $p \leq \sqrt{n}$ then that is it.
• If $p > \sqrt{n}$ then m must be $< \sqrt{n}$ because otherwise $n = pm > (\sqrt{n} \times \sqrt{n}) = n$, i.e. $n > n$ which is impossible. Now, if m is prime then that is it; otherwise m must contain a prime factor which is necessarily $< m$ and hence $< \sqrt{n}$ (noting that any composite number can be factorized as a product of primes; see § 2.1).
7. What is the importance of the fact that: if n is composite then it has a prime divisor $\leq \sqrt{n}$?
Solution: This fact is important for the search of primes and test for primality. In other words, to verify that a given number is prime we need only to establish that it has no prime divisor $\leq \sqrt{n}$ with no need to test for potential prime divisors $> \sqrt{n}$ because by the contraposition of this conditional statement if the number has no prime divisor $\leq \sqrt{n}$ then it is not composite (i.e. it is prime). In fact, the traditional prime sieves use this fact in the search for primes (see for instance § 2.3.1).
8. Determine if the following numbers are primes or composite: 79, 157, 233, 501.
Solution: Referring to point 6 in the preamble of this section (as well as Problems 6 and 7):
• The primes $\leq \sqrt{79}$ are 2,3,5,7. As 79 is not divisible by these primes it must be prime.
• The primes $\leq \sqrt{157}$ are 2,3,5,7,11. As 157 is not divisible by these primes it must be prime.
• The primes $\leq \sqrt{233}$ are 2,3,5,7,11,13. As 233 is not divisible by these primes it must be prime.
• The sum of digits of 501 is 6 which is a multiple of 3 and hence it is divisible by 3. So, it is composite.
9. Show that the square root of any prime number p is irrational.
Solution: There are several elementary proofs to this (most of which are similar to the proof of the irrationality of $\sqrt{2}$ which every reader of this book must know; see the upcoming note). An example of these proofs is: if $\sqrt{p}$ is rational then $\sqrt{p} = m/n$ (where $m, n \in \mathbb{N}$) and hence $n^2 p = m^2$. Now, m^2 and n^2 are obviously composite (because $m^2 = m \times m$ and $n^2 = n \times n$). Moreover, since they are squares then any prime number in their prime factorization must occur an even number of times. This means that we have an odd number of primes on the left hand side and an even number of primes on the right hand side which is impossible according to the fundamental theorem of arithmetic (see § 2.1). In fact, this logic (with minor adaptation) should apply to the n^{th} root of any prime number and not only to the square root.
Note: it is worth noting that there are two main methods for proving the irrationality of $\sqrt{2}$ (and

indeed the irrationality of any n^{th} root of any natural number whose n^{th} root is not an integer): the method of prime factorization and the method by contradiction (noting that both these methods rest on the same logic and they both lead eventually to a sort of contradiction). A third method based on Fermat's last theorem (see § 2.9.5) may also be used for some n^{th} roots (which is legitimate only if the proof of Fermat's last theorem does not depend on these proofs noting that there are claims of circularity in this method of proof which requires a detailed inspection of the proof of Fermat's last theorem).

10. Let $mn = k^s$ where $m, n, k, s \in \mathbb{N}$ and m and n are coprime. What can you conclude from this?
Solution: We can conclude that there are two coprime numbers $\mu, \nu \in \mathbb{N}$ such that $m = \mu^s$ and $n = \nu^s$. The justification of this conclusion is that since m and n are coprime then there is no common factor in their prime factorization (see part d of Problem 1) and hence we can separate their prime factors in their product k^s to those belonging to m and those belonging to n. This means that we can express m and n as $m = \mu^s$ and $n = \nu^s$ where μ and ν have no common prime factor, i.e. μ and ν are coprime.
11. Show that if p, $4p^2 + 1$ and $6p^2 + 1$ are primes then $p = 5$.
Solution: Referring to Problem 3, prime numbers must end in $1, 3, 7, 9$ (excluding 2 and 5). Moreover, the squares of the numbers ending in $1, 3, 7, 9$ must end in $1, 9, 9, 1$ (see rule 11 of § 1.8). Now, if p^2 ends in 1 then $4p^2 + 1$ ends in 5 (which is divisible by 5 and hence $4p^2 + 1$ is not prime), while if p^2 ends in 9 then $6p^2 + 1$ ends in 5 (which is divisible by 5 and hence $6p^2 + 1$ is not prime).[55] So, one of $4p^2 + 1$ and $6p^2 + 1$ must be composite and hence p, $4p^2 + 1$ and $6p^2 + 1$ cannot be primes except if $p = 5$ since 5 is the only prime number that ends in 5 and hence both $4p^2 + 1$ and $6p^2 + 1$ are primes in this case (as well as 5 itself). We finally note that $p = 2$ is not a possibility because $6(2^2) + 1 = 25$ which is composite.
12. Prove or justify the following:
(**a**) There are infinitely many primes.
(**b**) If n is composite then $(2^n - 1)$ is composite.
(**c**) If $(2^n - 1)$ is prime then n is prime.
(**d**) If $m, n \in \mathbb{N}$ and $(m + n) \in \mathbb{P}$ then m and n are coprime.
(**e**) If m and n are coprime then there is no common factor in their prime factorization.
(**f**) If m and n are coprime to k then their product mn is also coprime to k.
(**g**) Any two consecutive integers (or natural numbers) are coprime.
(**h**) No three consecutive natural numbers (> 1) can be all prime (i.e. at least one of them must be composite).[56]
(**i**) A set of pairwise relatively prime numbers contains at most one even number (i.e. either they are all odd or they contain only one even number).
(**j**) No more than three consecutive numbers can be pairwise relatively primes.[57]
(**k**) Any set of more than n numbers taken from the set $\{1, 2, \ldots, 2n\}$ must contain (at least) a pair of coprime numbers (i.e. two of them are coprime).
(**l**) m and n are coprime *iff* m^s and n^t are coprime ($s, t \in \mathbb{N}$).
(**m**) If m and n are coprime and $m = a\mu$ and $n = b\nu$ ($a, \mu, b, \nu \in \mathbb{Z}$) then μ and ν are coprime.
(**n**) The natural powers of distinct primes are coprime.
Solution:
(**a**) Let assume that the number of primes is finite (say n). If $q = (p_1 p_2 \cdots p_n) + 1$ then either q is prime or not. If q is prime then we found another prime (and hence our assumption is false since we have more than n primes noting that the infinity of the number of primes can be judged by repetitive application of this argument). If q is not prime then it must have a prime factor p. Now, if p is not one of the n primes then we found another prime (and hence our assumption is false with the same previous

[55] We refer the reader to rules 19 and 21 of § 1.8.
[56] The condition "> 1" is about "at least one of them must be composite".
[57] Whether or not these numbers must exclude 0 (or even be restricted to natural numbers) requires some details, i.e. with regard to the definition of relatively prime and with regard to the status of 0 in respect of coprimality (see for instance the preamble of this section as well as part l of Problem 1). Anyway, this issue is trivial and hence it should not concern us.

justification). If p is one of the n primes then p must divide both $(p_1 p_2 \cdots p_n)$ and q and hence it must divide their difference which is 1 (see rule 14 of § 1.9). However, no prime can divide 1, and hence p cannot be one of the n primes. This means that we found another prime (and hence our assumption is false). So, our assumption of having a finite number of primes is false in all cases, and hence there must be infinitely many primes.[58]

(**b**) If n is composite then $n = mk$ ($m, k \in \mathbb{N}$ and $m, k > 1$) and hence (see Eq. 12):

$$2^n - 1 = 2^{mk} - 1 = (2^m)^k - 1 = \Big[(2^m) - 1\Big]\Big[(2^m)^{k-1} + (2^m)^{k-2} + \cdots + (2^m) + 1\Big]$$

Now, since $m, k > 1$ then both factors in the square brackets must be greater than 1 and hence $(2^n - 1)$ is composite since it is equal to a product of two factors greater than 1.

(**c**) "Prime" means "not composite" and hence this statement is the contrapositive of the statement of part (b) and thus it is true (see point 11 of § 1.1).

(**d**) If m and n are not coprime then they must have a common divisor $g > 1$, and hence:

$$m + n = g\mu + g\nu = g(\mu + \nu) \qquad\qquad (\mu, \nu \in \mathbb{N})$$

This means that $(m + n)$ is a product of g and $(\mu + \nu)$ both of which are > 1 and hence $(m + n)$ is not prime in contradiction to the given assumption.

(**e**) This should be obvious because if there is a common factor then this factor (which is greater than 1 since it is in their prime factorization) will divide them both and hence they will not be coprime.

(**f**) This is because being coprime to k means that they have no common factor in their prime factorization with k (see part e) and so is their product (noting that multiplication cannot create a new prime factor).

(**g**) This is because if the numbers are m and $m + 1$ and their greatest common divisor is d then $d|m$ and $d|(m + 1)$ and hence (by rule 14 of § 1.9) d divides their difference which is 1, i.e. $d = 1$ (see rule 3 of § 1.9). So, they must be coprime.

(**h**) This is because at least one of these numbers must be even and greater than 2 and hence it must be composite (see point 3 in the preamble of this section).

(**i**) This is because if they contain two (or more) even numbers then the gcd of these even numbers must be greater than 1 since they have a common factor of 2 (and hence the set cannot be of pairwise relatively prime numbers).

(**j**) This is because four (or more) consecutive numbers must include at least two even numbers and hence they cannot be pairwise relatively primes (according to i).

(**k**) This is because a set of more than n numbers must include (at least) two consecutive integers and hence by part (g) they must be coprime.

(**l**) This is because raising a number to a power does not create a new prime factor in its prime factorization (i.e. it just changes the exponents in its prime factorization). Now, coprimality of two numbers means they have no common factor in their prime factorization (see point d of Problem 1). Hence, if there is no common prime factor between m^s and n^t then there is no common prime factor between m and n and vice versa. This proves both **the if part** and **the only if part** of the given statement.

(**m**) Because m and n are coprime then they have no common factor in their prime factorization and hence μ and ν (which contain no prime factors other than those of m and n) must also have no common factor in their prime factorization and hence they must also be coprime.[59]

(**n**) This is obvious because the natural powers of distinct primes cannot have a common prime factor and hence they must be coprime.[60] In fact, this is an instance of the "only if" part of the statement of part (l) noting that any two distinct primes are coprime.

---

[58] As indicated earlier, the essence of this argument is that if the number of primes is finite then it is fixed and since we find in every case a new prime (which means that the number of primes is not fixed) then we conclude by contradiction that the number of primes is not finite. So, the argument is essentially a proof by contradiction (see § 1.5.4).

[59] It should be obvious (as a matter of labeling) that (a, b), (a, ν) and (b, μ) are also coprime.

[60] In fact, we can include even the 0 power, but this is trivial, moreover it extends to non-distinct primes.

13. What is the relation between the primality of n and the primality of (2^n-1)?
Solution: If (2^n-1) is prime then n is prime (see part c of Problem 12), but if n is prime then (2^n-1) is not necessarily prime (e.g. $2^{11}-1=2047\notin\mathbb{P}$). So, the primality of n is a necessary but not sufficient condition for the primality of (2^n-1). In brief, if n is composite then (2^n-1) is composite and hence if (2^n-1) is not composite (i.e. it is prime) then n is not composite. Symbolically, $n\notin\mathbb{P}\rightarrow(2^n-1)\notin\mathbb{P}$ and hence its contrapositive (but not its converse or inverse) is also true (see point 11 of § 1.1).
14. Let m and n be integers of opposite parity. Show that m and n are coprime *iff* $m+n$ and m^2+n^2 are coprime.
Solution: Regarding **the if part**, if m and n are not coprime then $m=p\mu$ and $n=p\nu$ where $\mu,\nu\in\mathbb{Z}$ and $p\in\mathbb{P}$. But then $m+n=p(\mu+\nu)$ and $m^2+n^2=p^2(\mu^2+\nu^2)$ are not coprime (since they have a common factor p) which is a contradiction. This means (by contraposition) that if $m+n$ and m^2+n^2 are coprime then m and n are coprime.
Regarding **the only if part**, if m and n are coprime but $m+n$ and m^2+n^2 are not coprime then $m+n$ and m^2+n^2 must have a common factor $p\in\mathbb{P}$. Now:

$$\begin{aligned}2m^2&=(m^2+n^2)+(m^2-n^2)=(m^2+n^2)+(m+n)(m-n)=pA\\2n^2&=(m^2+n^2)-(m^2-n^2)=(m^2+n^2)-(m+n)(m-n)=pB\end{aligned}$$

where A,B are integers and where we used in the last steps the presumption that $m+n$ and m^2+n^2 have a common factor p.
Now, since m and n are of opposite parity p cannot be 2. This is because p presumably divides $m+n$ which is odd (see the rules of parity in § 1.8). But since $p\neq2$ then p must be a common factor of m^2 and n^2 and hence p must be a common factor of m and n (since raising a number to a power does not create a new prime factor in its prime factorization; see part l of Problem 12) which is a contradiction (since m and n are presumably coprime). This means that if m and n are coprime then $m+n$ and m^2+n^2 are coprime.
15. Let $\mathbb{N}\ni m,n>1$. Show that if (m^n-1) is prime then: (**a**) $m=2$ and (**b**) n is prime.
Solution:
(**a**) From Eq. 12 we have:

$$m^n-1=(m-1)(m^{n-1}+m^{n-2}+\cdots+m^2+m+1)=(m-1)A$$

So, $(m-1)$ is a divisor of (m^n-1), and since (m^n-1) is prime (which is divisible only by 1 and itself) then $(m-1)=1$ (noting that $A>1$), i.e. $m=2$.
(**b**) From part (a) we have $(m^n-1)=(2^n-1)$, and hence from part (c) of Problem 12 (also see Problem 13) n is prime (since 2^n-1 is prime).
16. Show that every prime other than 2 is of the form $(4k+1)$ or $(4k-1)$ where $k\in\mathbb{N}$.
Solution: Let assume that n is a prime and we divide it by 4. The remainder r that we get from this division must be one of the four following cases:
• $r=0$. This case is impossible because n is supposedly prime and hence it cannot be divisible by 4.
• $r=1$. Hence, $n=4k+1$.
• $r=2$. This case is impossible because n is supposedly prime and hence if $n=4k+2$ then it must be even >2 $\big[$i.e. $n=2(2k+1)\big]$ which cannot be prime (see point 3 in the preamble of this section).
• $r=3$. Hence, $n=4k'+3=4k'+4-1=4(k'+1)-1=4k-1$ (noting that $k'\in\mathbb{N}^0$).
So, if n is prime >2 then it can only be of the form $(4k+1)$ or the form $(4k'+3)$ which is equivalent to $(4k-1)$.
17. Show that there are infinitely many primes of the form $(4k+1)$ and $(4k-1)$ (or equivalently $4k'+3$).
Solution: There are infinitely many primes (see part a of Problem 12). Moreover, all primes (except 2) are of the form $4k+1$ or $4k-1$ (see Problem 16). Accordingly, there are infinitely many primes of the form $4k\pm1$ (i.e. considering them together). However, what is required here is to prove that there are infinitely many primes of each one of these forms individually (i.e. there are infinitely many primes of the form $4k+1$ and there are infinitely many primes of the form $4k-1$ which is equivalent to $4k'+3$). This can be established by Dirichlet's theorem (see point 2 of § 2.9.5) noting that 4 and 1 are coprime and 4 and 3 are coprime.

18. Give a condition that makes every number of the form $m^s + n^t$ composite ($m, n, s, t \in \mathbb{N}$).
Solution: The condition "m and n are not coprime" meets this requirement since:

$$m^s + n^t = d\left(\mu m^{s-1} + \nu n^{t-1}\right) \qquad \left[m = d\mu,\ n = d\nu,\ d = \gcd(m, n)\right]$$

which is obviously composite since it is a product of two integers both of which are greater than 1 (noting that $d > 1$ since m and n are not coprime).

19. Show the following (where $m, n, k \in \mathbb{N}$):
(**a**) If m and n are coprime and $n = m \pm k$ then n is also coprime to k.
(**b**) m and n are coprime *iff* m and $(m \pm n)$ are coprime.
Solution:
(**a**) If n is not coprime to k then they should have a common factor $d > 1$ and hence $n = dn'$ and $k = dk'$. Therefore:

$$n = m \pm k \qquad \rightarrow \qquad dn' = m \pm dk' \qquad \rightarrow \qquad d(n' \mp k') = m$$

This means that m also has a factor of d and hence it cannot be coprime to n (which has a factor of d).
(**b**) Regarding the "**if part**": if m and $(m \pm n)$ are coprime but m and n are not coprime then we must have $d > 1$ such that $m = dm'$ and $n = dn'$. But then we have $(m \pm n) = (dm' \pm dn') = d(m' \pm n')$ which means that m and $(m \pm n)$ are not coprime because they have a common factor $d > 1$. This contradiction should establish the "if part" of the statement.
Regarding the "**only if part**": if m and n are coprime but m and $(m \pm n)$ are not coprime then we must have $d|m$ and $d|(m \pm n)$ for some $d > 1$. But then (by rule 14 of § 1.9) we must have $d|n$ which means that m and n are not coprime because they have a common factor $d > 1$. This contradiction should establish the "only if part" of the statement.

20. Show that if $m, n \in \mathbb{Z}$ are coprime and mn is a square (of an integer) then each one of m, n is a square (of an integer).
Solution: Because mn is a square we can write:

$$mn = \left(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}\right)^2 = p_1^{2a_1} p_2^{2a_2} \cdots p_k^{2a_k} \tag{24}$$

where $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the prime factorization of $\sqrt{mn}$.
Also, because m, n are coprime then they have no common factor in their prime factorization (see part d of Problem 1). This means that each one of the factors $p_i^{2a_i}$ $(i = 1, 2, \ldots, k)$ belongs to exactly one of m and n. So, we can separate the factors of m and n in Eq. 24 and write:

$$mn = p_1^{2a_1} p_2^{2a_2} \cdots p_k^{2a_k} = \left(\prod_s p_s^{2a_s}\right)\left(\prod_t p_t^{2a_t}\right) = \left(\prod_s p_s^{a_s}\right)^2 \left(\prod_t p_t^{a_t}\right)^2$$

where $m = \left(\prod_s p_s^{a_s}\right)^2$ and $n = \left(\prod_t p_t^{a_t}\right)^2$, i.e. each one of m, n is a square.

21. Show that the distribution of prime numbers (i.e. the number of primes less than or equal to $n \in \mathbb{N}$ as a function of n) follows a logarithmic pattern.
Solution: There are several theorems (with their proofs) that confirm this logarithmic pattern. However, in this book we demonstrate this visually for $n \leq 10^{20}$ by plotting $\pi(n)$ (i.e. the function representing the number of primes $\leq n$) versus n on a logarithmic scale (see Figure 1). As we see, $\pi(n)$ is (approximately) linear on this log-log plot which illustrates (and verifies up to $n \leq 10^{20}$) the claimed logarithmic pattern.

22. Why 0 and 1 are considered neither prime nor composite?
Solution: Regrading 0, it is not prime because it is divisible by any other number while prime must be divisible only by 1 and itself (considering positive divisors). It is also not composite because it cannot be expressed as a product of primes.
Regrading 1, it is not composite because it cannot be expressed as a product of primes. However, it is like a prime (since it is divisible only by 1 and itself) and hence it seems reasonable to classify it

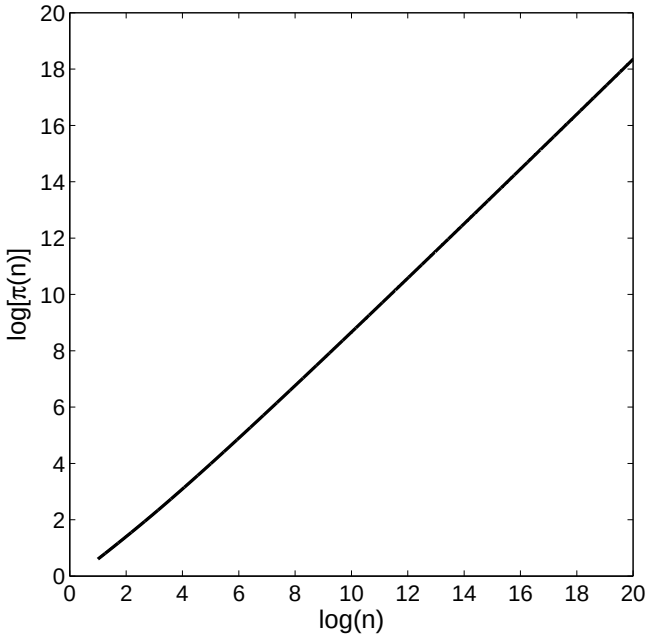


Figure 1: The plot of $\log\left[\pi(n)\right]$ versus $\log(n)$ for $n \leq 10^{20}$. See Problem 21 of § 2.2.

as prime. So, the reason for not considering it prime seems to be the desire to preserve the property of uniqueness of prime factorization (according to the fundamental theorem of arithmetic; see § 2.1). For example, if 1 is prime then 4 can be prime-factorized in infinitely many ways, e.g. 1×2^2, $1^2 \times 2^2$, $1^3 \times 2^2$, etc.

23. Find every prime number p which is the sum and the difference (simultaneously) of (distinct) pairs of primes.
Solution: Since p is the sum of two primes then it is > 2 and hence it is odd.
Since p is the sum (and difference) of two primes and it is odd then one of the primes in the pairs must be even (rule 4 of § 1.8) which can only be 2 because 2 is the only even prime. So, $p = 2 + p_1$ and $p = p_2 - 2$, i.e. $2 + p_1 = p_2 - 2$ and hence $p_2 - p_1 = 4$ which means that p_1, p, p_2 are three consecutive odd numbers and hence exactly one of them is divisible by 3 (see rule 50 and Problem 16 of § 1.9). Now, 3 is the only prime number divisible by 3 and hence $p_1 = 3$ which leads to $p = 5$ and $p_2 = 7$. So, 5 is the only prime number which is the sum and the difference of pairs of primes, i.e. $5 = 2 + 3$ and $5 = 7 - 2$.
24. Show that $(2k^2 + k + 2)$ is not the sum of two primes where $\mathbb{O} \ni k > 1$.
Solution: According to the rules of parity (see § 1.8), $(2k^2 + k + 2)$ is odd (noting that k is odd) and hence if it is the sum of two primes then it can only be the sum of an even prime and an odd prime. Noting that the only even prime is 2, we have:

$$2k^2 + k + 2 = 2 + m \qquad \rightarrow \qquad m = 2k^2 + k = k(2k + 1)$$

So, m must be composite because it is a product of k (which is > 1) and $(2k + 1)$.
Note: for $k = 1$ we have $2k^2 + k + 2 = 5$ and hence it is the sum of two primes, i.e. $5 = 2 + 3$.
25. Show that m and n are coprime *iff* mn and $m + n$ are coprime.
Solution: In this proof we essentially employ the method of contraposition (see § 1.5.4).
Regarding **the if part**, let assume that m and n are not coprime and hence they have a common factor $p \in \mathbb{P}$. So, $m = p\mu$ and $n = p\nu$ where $\mu, \nu \in \mathbb{Z}$. But in this case we will have $mn = p\mu p\nu = p(\mu p\nu)$ and $m + n = p\mu + p\nu = p(\mu + \nu)$, i.e. mn and $m + n$ are not coprime since they have a common factor p. This means that if mn and $m + n$ are coprime then m and n must be coprime.

Regarding **the only if part**, let assume that mn and $m+n$ are not coprime and hence they have a common factor $p \in \mathbb{P}$. Accordingly, $p|(mn)$ and hence (by rule 22 of § 1.9) p must divide m or n (say m). But if p divides m (and p presumably divides $m+n$) then p must divide their difference which is n (see rule 14 of § 1.9). So, p divides both m and n and hence they are not coprime. This means that if m and n are coprime then mn and $m+n$ must be coprime.

2.2.1 Twin Primes

Twin primes are prime numbers which are 2 apart (like 11 and 13). In the following points we provide some useful remarks related to twin primes:

1. It is unknown if there are infinitely many twin primes (although it is conjectured and seems to be supported by partial evidence).
2. Although 2 and 3 are consecutive primes they are not twin primes because their difference is not 2 (see the definition of twin primes above). Hence, the first (or lowest) twin primes are 3 and 5.
3. $(3,5)$ and $(5,7)$ are the only consecutive pairs of twin primes. In other words, 5 is the only prime number that is shared by two different pairs of twin primes.
4. The sum of any twin primes other than $(3,5)$ is divisible by 12.[61]
5. Any twin primes other than $(3,5)$ can be expressed as $(6n-1, 6n+1)$ where $n \in \mathbb{N}$.
6. The number between a twin primes is composite.

Problems

1. Prove or justify the following:
   (**a**) The number between a twin primes is composite.
   (**b**) $(3,5)$ and $(5,7)$ are the only consecutive pairs of twin primes (i.e. they share a number which is 5).
   (**c**) The sum of any twin primes other than $(3,5)$ is divisible by 12.
   (**d**) Any twin primes other than $(3,5)$ can be expressed as $(6n-1, 6n+1)$ where $n \in \mathbb{N}$.
   Solution:
   (**a**) This is justified by part (h) of Problem 12 of § 2.2.
   (**b**) Let $(p, p+2)$ and $(p+2, p+4)$ be another pair of consecutive twin primes (i.e. $p > 3$). Now, if we divide p by 3 then the remainder is either 0 (and hence p is not prime) or 1 (and hence $p+2$ is not prime) or 2 (and hence $p+4$ is not prime). What distinguishes the pair $(3,5)$ and $(5,7)$ from other consecutive pairs (and hence makes this argument does not apply to this pair) is that 3 is the only prime number that is divisible by 3 (and hence for this pair the remainder is 0 despite p being prime).
   (**c**) Let the twin primes be $p_1 = 2k+1$ and $p_2 = 2k+3$ (where $\mathbb{N} \ni k > 1$) noting that all primes are odd except 2. Now, the sum of these primes is $p_1 + p_2 = 4k+4 = 4(k+1)$ which is divisible by 4. Moreover, the remainder of p_1 when it is divided by 3 cannot be 0 (because p_1 is not divisible by 3 since it is a prime greater than 3) and cannot be 1 (because otherwise p_2 will be divisible by 3 which is impossible because it is a prime greater than 3). So, the only possibility is that the remainder of p_1 (when divided by 3) is 2 and hence the remainder of p_2 (when divided by 3) is 1. This means that the remainder of their sum (when divided by 3) is zero (see rule 22 of § 1.8 as well as the upcoming rules of § 2.7), i.e. $p_1 + p_2$ is divisible by 3. So, $p_1 + p_2$ is divisible by 3 and by 4 and hence it must be divisible by 12 (see rule 34 of § 1.9).
   (**d**) This is a consequence of (c) because since they are divisible by 12 then their sum can be written as:

$$p_1 + p_2 = 12n = 6n + 6n = (6n-1) + (6n+1)$$

   Now, if we note the imposed conditions (i.e. $n \in \mathbb{N}$ with p_1 and p_2 being natural numbers which are 2 apart) then we can conclude that $p_1 = 6n-1$ and $p_2 = 6n+1$.

[61] This (and the next) can be used as a test to rule out (but not in) being twin primes. For instance, we can immediately conclude that $(9476869, 9476871)$ are not twin primes because their sum is not divisible by 12, but we cannot conclude that $(9476807, 9476809)$ are twin primes although their sum is divisible by 12.

2.2.2 Mersenne Primes and Mersenne Numbers

Mersenne prime M_p is a prime number that is one less than a power of 2, i.e. $M_p = 2^n - 1$ (for some $\mathbb{N} \ni n > 1$). However, because $2^n - 1$ is composite if n is composite (see part b of Problem 12 of § 2.2), the Mersenne primes can be defined more specifically as $M_p = 2^p - 1$ (for some $p \in \mathbb{P}$). The first few Mersenne primes are $3, 7, 31, 127, 8191, 131071, 524287$.

In the following points we provide some useful remarks and facts about Mersenne primes:[62]

1. Mersenne prime may be defined as $M_p = 2^p - 1$ (for some $p \in \mathbb{P}$). However, it should be noticed that the condition $p \in \mathbb{P}$ in this definition is a necessary but not sufficient condition for being a Mersenne prime. For instance, $2^{11} - 1 = 2047 = 23 \times 89$ which is composite. It is worth noting that the numbers that have the form $(2^n - 1)$ regardless of being prime or not may be described as Mersenne numbers. Accordingly, "Mersenne prime" my be defined as a Mersenne number which is prime.
2. Mersenne primes are closely related to perfect numbers (see § 2.8).
3. It is unknown if there are infinitely many Mersenne primes or not.
4. Currently (February 2023), there are only 51 known Mersenne primes.[63]
5. The largest known prime number (which is $2^{82589933} - 1$) is a Mersenne prime. In fact, the largest known prime numbers are mostly Mersenne primes.
6. Noting that $(2^n - 1)$ in binary is made of n "1" digits $\big[$e.g. $2^3 - 1 = (111)_2$ and $2^4 - 1 = (1111)_2\big]$, Mersenne primes (and numbers) can be represented most easily in this simple binary form, and this simple representation may be exploited in certain computational algorithms for the search and manipulation of Mersenne primes.
7. It seems unknown if $(2^p - 1)$ is composite for infinitely many primes p or not.

We should finally note that because of the close relationship between Mersenne primes and perfect numbers (which we indicated already) as well as their dependency on each other, we defer the Problems about Mersenne primes to § 2.8 (noting that some Problems related to Mersenne primes and numbers have already been given earlier; see for instance parts b and c of Problem 12 of § 2.2).

2.2.3 Fermat Primes and Fermat Numbers

Fermat prime is a prime number of the form $(2^n + 1)$ where $n \in \mathbb{N}$. It can be shown that if $(2^n + 1)$ is prime then n is a power of 2, i.e. $n = 2^k$ where $k \in \mathbb{N}^0$ (see Problem 1). This means that Fermat primes are of the form $(2^{2^k} + 1)$. The first three Fermat primes are $3, 5, 17$ (corresponding to $n = 1, 2, 4$ or $k = 0, 1, 2$).

In the following points we provide some useful remarks and facts about Fermat primes and Fermat numbers (see footnote [62]):

1. Fermat number is a natural number of the form $2^{2^k} + 1$ (where $k \in \mathbb{N}^0$) regardless of being prime or not. Accordingly, Fermat primes is a subset of Fermat numbers.
2. Fermat numbers are generally symbolized as F_k (e.g. $F_3 = 2^{2^3} + 1$).
3. All Fermat numbers are odd (as can be seen from their form).
4. There are infinitely many Fermat numbers (noting that there are infinitely many k's). However, it is unknown if there are infinitely many Fermat primes or not.
5. Currently (February 2023), there are only five known Fermat primes (which are the first five Fermat numbers $3, 5, 17, 257, 65537$ corresponding to $k = 0, 1, 2, 3, 4$).
6. It is unknown if Fermat numbers are composite for all $k > 4$.
7. Fermat numbers can be generated by the recursive formula $F_k = 2 + (F_0 F_1 \dots F_{k-1})$.
8. F_s and F_t are coprime where $s \neq t$ $(s, t \in \mathbb{N}^0)$.

Problems

[62] We note that some "facts" of this sort and in such contexts may require further verification as they are obtained from the Internet and hence they are based on trust (and some can be outdated).

[63] This is what we found on the Internet (seen on February 2023). Because of the relation between Mersenne primes and (even) perfect numbers this is also the number of known perfect numbers (see § 2.8).

1. Show that if (2^n+1) is prime then n is a power of 2 (i.e. $n=2^k$ where $k\in\mathbb{N}^0$).
   Solution: We prove this by contraposition (noting that the given statement is true for $n=1,2$ corresponding to $k=0,1$ and hence we need only to prove it for $n>2$). So, let assume that n in (2^n+1) is not a power of 2. Accordingly, n can be written as $n=mp$ where $m\in\mathbb{N}$ and p is an odd prime (noting that since n is not a power of 2 and it is >2 then it must have an odd prime factor; see § 2.1). So, we have:
   $$2^n+1=2^{mp}+1=(2^m)^p+1^p=(2^m+1)\left[(2^m)^{p-1}-(2^m)^{p-2}+\cdots-2^m+1\right]$$
   where we used the identity of Eq. 11 (noting that p is an odd prime). As we see, (2^n+1) is composite (since it is a product of two integers >1) and hence (by contraposition) if (2^n+1) is prime then n must be a power of 2.
2. Find all $n\in\mathbb{N}$ such that both (2^n-1) and (2^n+1) are primes.
   Solution: Since (2^n-1) is prime then n is prime (see part c of Problem 12 of § 2.2).
   Also, (2^n+1) is a Fermat prime and hence n is a power of 2 (see Problem 1).
   So, n is a prime number and it is a power of 2 at the same time. No prime number meets this condition other than 2 and hence $n=2$ only. Also see part (d) of Problem 9 of § 2.7.
3. Show that no Fermat number F_k $(k\neq 1)$ can be the sum of two primes.
   Solution: For $k=0$ we have $F_0=3$ which is not the sum of two primes. For $k>1$ we prove this by contradiction. So, let assume that a given Fermat number F_k $(k>1)$ is the sum of two primes. Since all Fermat numbers are odd (see point 3 in the preamble) then exactly one of these primes is even (see the rules of parity in § 1.8) which must be 2 because 2 is the only even prime (see point 3 of § 2.2). Accordingly, the other prime must be (F_k-2) and hence we have:
   $$F_k-2=(2^{2^k}+1)-2=2^{2^k}-1=(2^{2^{k-1}})^2-1=(2^{2^{k-1}}-1)(2^{2^{k-1}}+1)$$
   As we see, (F_k-2) is composite (since it is a product of two integers >1) and this contradicts our assumption that (F_k-2) is prime. So, no Fermat number F_k $(k\neq 1)$ can be the sum of two primes.
4. Show that $F_k=(F_{k-1}-1)^2+1$ where $k\in\mathbb{N}$.
   Solution: We have:
   $$F_k=2^{2^k}+1=\left(2^{2^{k-1}}\right)^2+1=\left(2^{2^{k-1}}+1-1\right)^2+1=\left(\left[2^{2^{k-1}}+1\right]-1\right)^2+1=(F_{k-1}-1)^2+1$$
5. Show that $F_k=F_{k-1}^2-2(F_{k-2}-1)^2$ where $k>1$.
   Solution: We have:
   $$\begin{aligned}F_k &= 2^{2^k}+1=2^{2^k}+(2\times 2^{2^{k-1}})+1-(2\times 2^{2^{k-1}})=\left[2^{2^k}+(2\times 2^{2^{k-1}})+1\right]-(2\times 2^{2^{k-1}})\\ &= \left[2^{2^{k-1}}+1\right]^2-2\left[2^{2^{k-1}}\right]=\left[2^{2^{k-1}}+1\right]^2-2\left[2^{2^{k-2}}\right]^2=\left[2^{2^{k-1}}+1\right]^2-2\left[2^{2^{k-2}}+1-1\right]^2\\ &= \left[2^{2^{k-1}}+1\right]^2-2\left[(2^{2^{k-2}}+1)-1\right]^2=F_{k-1}^2-2(F_{k-2}-1)^2\end{aligned}$$
6. Show that $F_k=2+(F_0F_1\ldots F_{k-1})$.
   Solution: We prove this by induction.
   We have $F_0=2^{2^0}+1=3$ and $F_1=2^{2^1}+1=5$, and hence $F_1=2+F_0$. So, the formula is true for $k=1$.[64] Now, let assume that the formula is true for a given $k\in\mathbb{N}$ and hence we have $F_k=2+(F_0F_1\ldots F_{k-1})$, i.e. $F_0F_1\ldots F_{k-1}=F_k-2$. Accordingly:
   $$\begin{aligned}(F_k-2)F_k &= \left[(2^{2^k}+1)-2\right](2^{2^k}+1)=(2^{2^k}-1)(2^{2^k}+1)=\left(2^{2^k}\right)^2-1=2^{2^{k+1}}-1\\ &= \left(2^{2^{k+1}}+1\right)-2=F_{k+1}-2\end{aligned}$$

[64] If this start is not convincing to some, we can add: $17=F_2=2+F_0F_1=2+(3)(5)=17$.

i.e.

$$F_{k+1} = 2 + (F_k - 2)F_k = 2 + (F_0F_1 \dots F_{k-1})F_k = 2 + (F_0F_1 \dots F_{k-1}F_k)$$

As we see, the formula is true for $k+1$ (assuming it is true for k) and hence by mathematical induction the formula is true in general.

7. Show that Fermat numbers are pairwise relatively prime, i.e. F_s and F_t are coprime where $s \neq t$ $(s, t \in \mathbb{N}^0)$.
Solution: We can assume (with no loss of generality) that $s < t$. Let d be a common positive divisor to F_s and F_t, i.e. $d|F_s$ and $d|F_t$. Accordingly, $d|(F_0F_1 \dots F_{t-1})$ because F_s occurs in $(F_0F_1 \dots F_{t-1})$ noting that $s < t$. Now, from the result of Problem 6 we have: $2 = F_t - (F_0F_1 \dots F_{t-1})$. Since $d|F_t$ and $d|(F_0F_1 \dots F_{t-1})$ then $d|2$ (see rule 14 of § 1.9). This means that either $d = 2$ (which is impossible since all Fermat numbers are odd; see rule 7 of § 1.8) or $d = 1$ (which is the only acceptable possibility). So, $d = 1$ which means that the only possible common positive divisor to F_s and F_t is 1 and hence F_s and F_t must be coprime.
Note: the result of this Problem may be used by some to prove that there are infinitely many primes (see part a of Problem 12 of § 2.2). This is because since Fermat numbers are pairwise relatively prime then no two Fermat numbers can have a common prime factor which means that any Fermat number must consist (in its prime decomposition) of prime number(s) which are unique to that Fermat number. Now, since there are infinitely many Fermat numbers then there must be infinitely many prime numbers.
8. Show that $F_k + 1 = 6n$ where $k, n \in \mathbb{N}$.
Solution: From the result of Problem 6 we have:

$$F_k + 1 = 3 + (F_0F_1 \dots F_{k-1}) = 3 + (3F_1 \dots F_{k-1}) = 3(1 + F_1 \dots F_{k-1})$$

Now, if we note that $(1 + F_1 \dots F_{k-1})$ is even (see point 3 in the preamble as well as the rules of parity in § 1.8) then we can see that $(F_k + 1)$ is divisible by 2 and divisible by 3 and hence it is divisible by 6 (see rule 28 of § 1.9), i.e. $F_k + 1 = 6n$ where $k, n \in \mathbb{N}$.
9. Show that F_5 is composite.
Solution: We will show that $641|F_5$ (and hence F_5 is composite). We have:
$(2^7 \times 5) + 1 = 641 \quad \rightarrow \quad 2^7 \times 5 = 641 - 1 \quad \rightarrow \quad (2^7 \times 5)^4 = (641 - 1)^4 \quad \rightarrow$
$2^{28} \times 5^4 = (641 - 1)^4 \quad \rightarrow \quad 2^{28} \times 5^4 = 1 + 641m$
where we used the identity of Eq. 13 in the last step (noting that $m \in \mathbb{Z}$).
We also have: $641 = 2^4 + 5^4$ and hence $5^4 = 641 - 2^4$. On combining these results we get:

$$\begin{aligned} 2^{28} \times 5^4 &= 1 + 641m \\ 2^{28} \times (641 - 2^4) &= 1 + 641m \\ (2^{28} \times 641) - (2^{28} \times 2^4) &= 1 + 641m \\ (2^{28} \times 641) - 2^{32} &= 1 + 641m \\ 2^{32} + 1 &= (2^{28} \times 641) - 641m \\ F_5 &= 641(2^{28} - m) \end{aligned}$$

10. Show that the last digit of F_k is 7 where $k > 1$.
Solution: According to Problem 6 we have $F_k - 2 = (F_0F_1 \dots F_{k-1})$ which means that $F_m|(F_k - 2)$ where $m < k$. Now, since $F_1 = 5$ then we have $5|(F_k - 2)$ where $k > 1$. This means that $F_k = 5n + 2$ $(n \in \mathbb{N})$. Now, if we note that F_k is odd (see point 3 in the preamble) then we can conclude (see rule 19 of § 1.8) that F_k ends in 7 (because otherwise it ends in 2 which means it is even noting that $5n$ ends either in 5 or in 0).
Note: from the result of this Problem we can conclude that no Fermat number can be a perfect square because (according to rule 11 of § 1.8) no perfect square ends in 7 (noting as well that F_0 and F_1, which are 3 and 5, are not perfect squares).

2.3 Common Algorithms and Methods in Number Theory

There are countless algorithms and methods related to number theory and used for various objectives and purposes. Some of these algorithms and methods are analytic in nature (and hence they are supposed to be implemented and employed by humans) while others intrinsically belong to computing and hence they are designed for (and usually conducted by) computers. However, most algorithms and methods these days (whether in number theory or in other subjects) are implemented computationally and conducted by computers. We also note that algorithms and methods in general (including those of number theory) can be deterministic and can be probabilistic (noting that most common algorithms used in number theory are deterministic).

In the following subsections we list a number of mathematical and computing algorithms and methods[65] which are commonly used in elementary number theory for various purposes and which will mostly be needed (or referred to) in the upcoming sections and chapters.

2.3.1 The Sieve of Eratosthenes

The sieve of Eratosthenes is an ancient algorithm for finding all the prime numbers less than a given number $n \in \mathbb{N}$. The algorithm can be outlined as follows (assuming $n > 2$):

- List all the natural numbers that are greater than 1 and less than n.
- Remove all the multiples of 2 from the list.[66]
- If the next remaining number in the list is less than $\sqrt{n}$ remove all its multiples from the list.[67]
- Repeat the process in the previous point until the next remaining number is $\geq \sqrt{n}$.
- The remaining numbers in the list are the required primes.

It is noteworthy that these days the sieve of Eratosthenes is of historical and educational value (rather than practical value) due to the emergence of more efficient algorithms for searching for primes (especially the very large ones) and sieving them. However, the basic principles of this sieve remain embedded in some of the modern sieves and algorithms which can be regarded as improved versions of this sieve.

2.3.2 The Division Algorithm

The division algorithm is actually a "division theorem" which states: if $m, n \in \mathbb{Z}$ (where $|n| \leq |m|$ and $mn \neq 0$) then there exist unique integers $q, r \in \mathbb{Z}$ (where $0 \leq r < |n|$) such that $m = qn + r$.[68] Therefore, the role of the division *algorithm* is to search for q and r whose existence and uniqueness are guaranteed by the division theorem. The existence and uniqueness of q and r (which represent the essence of the division theorem) can be easily proved. It is worth noting that m, n, q, r are called (respectively) **dividend**, **divisor**, **quotient**, and **remainder**. However, "divisor" is also used specifically in the terminology of divisibility (i.e. when $r = 0$) and hence the reader should be aware of this distinction.[69] For example, "n is a divisor of m" means n divides m evenly with no remainder (and this is symbolized by $n|m$).

2.3.3 The Euclidean algorithm

This is an ancient algorithm for calculating the greatest common divisor (gcd) of two integers (m and n). The algorithm is based on the fact that the gcd of two positive integers is unaffected if the bigger integer is replaced by its difference with the smaller integer, i.e. if $m, n \in \mathbb{N}$ and $m < n$ then $\gcd(m, n) =$

[65] "Mathematical" suggests analytical nature, while "computing" suggests computational (or algorithmic) nature.

[66] "Multiple" here does not include the number itself, i.e. the multiples of m are km where $\mathbb{N} \ni k > 1$.

[67] Whether the consideration of $\sqrt{n}$ belongs to the original sieve or not seems controversial, and may be an added improvement to the original sieve.

[68] This means that if $r = 0$ then $n|m$ (i.e. n divides m evenly).

[69] In fact, even "dividend" and "quotient" may also be used specifically in the terminology of divisibility, and this usually depends on the writer and context.

$\gcd(m, n-m)$.[70] The algorithm may also be seen as a repetitive application of the division algorithm (or theorem; see § 2.3.2). The best way of explaining the Euclidean algorithm is by examples where this algorithm is demonstrated through its application in specific cases (instead of giving a formal description of this algorithm), and that is what we will do in the future (see for instance Problem 3 of § 2.4).

2.3.4 The Extended Euclidean Algorithm

The extended Euclidean algorithm is a method for expressing the greatest common divisor (gcd) of two natural numbers (or integers), m and n, as a linear combination of these numbers, i.e. $\gcd(m, n) = sm+tn$ (where $s, t \in \mathbb{Z}$). So, if we are given m and n then with the help of this algorithm we can find s and t. The existence of s and t are guaranteed by the "Bezout theorem" (or rather by a supposed lemma of Bezout theorem) which states: if m and n are positive integers then there exist integers s and t such that $\gcd(m, n) = sm + tn$. In fact, the extended Euclidean algorithm (which we will use in the future; see § 2.4) should reveal the logic of this theorem and hence it can be seen as a form of proof (or rather justification) to this theorem. The best way of explaining the extended Euclidean algorithm is by examples where this algorithm is demonstrated through its application in specific cases (instead of giving a formal description of this algorithm), and that is what we will do in the future (see for instance Problem 5 of § 2.4). The extended Euclidean algorithm has a number of uses and applications; the most common one is apparently in solving linear Diophantine equations (see § 4.1.1). As the names suggest, the extended Euclidean algorithm is intimately linked to the Euclidean algorithm (as will be demonstrated in Problems 3 and 5 of § 2.4).

2.3.5 Other Common Algorithms and Methods

Other common algorithms and methods which are more frequently used or referred to (and hence they deserve to be investigated more thoroughly and systematically as we will do in the future) include: the Chinese remainder method (see § 2.7.3) and the equivalent equation method (see § 2.7.4).

2.4 Greatest Common Divisor

The greatest common divisor (gcd) of two or more integers (which are not all zero)[71] is the largest natural number that divides each of the integers. There are a number of methods (or algorithms) to calculate the greatest common divisor. One of the common methods is based on the **prime factorization** which will be outlined and demonstrated in the following (see point 2 and Problem 2). Another common method is the **Euclidean algorithm** which will be demonstrated by examples in the upcoming Problems (see for instance Problem 3).

We list in the following points some common rules and facts about the greatest common divisor (gcd) which will be used or referred to in the future or are important to know as general background knowledge:
1. By definition, the greatest common divisor is a natural number, i.e. it is always positive integer.
2. If m and n are positive integers whose prime factorizations are:[72]

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \qquad (a_i \in \mathbb{N}^0 \text{ for all } 1 \leq i \leq k) \tag{25}$$

$$n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k} \qquad (b_i \in \mathbb{N}^0 \text{ for all } 1 \leq i \leq k) \tag{26}$$

[70] In fact, we can also say (more strongly): the gcd of two positive integers is unaffected if the bigger integer is replaced by the remainder of the division of the bigger integer by the smaller integer, i.e. if $m, n \in \mathbb{N}$ and $m < n$ then $\gcd(m, n) = \gcd(m, r)$ where r is the remainder. See rules 12 and 13 of § 2.4.

[71] We note that some may exclude zero by restricting the definition of gcd to non-zero integers (i.e. gcd is defined only for integers none of which is zero) and hence gcd becomes like lcm in this regard. However, we do not see any reason for this since the definition of gcd applies in this case sensibly. Yes, this may be accepted in specific contexts and situations (where zero needs to be excluded for specific reasons).

[72] We allow a_i and b_i here to be zero (i.e. $a_i \in \mathbb{N}^0$ and $b_i \in \mathbb{N}^0$ instead of $a_i \in \mathbb{N}$ and $b_i \in \mathbb{N}$) to include the case when some primes are present in the factorization of only one of m and n. See point 2 in the preamble of § 2.1.

then

$$\gcd(m,n) = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k} \qquad \big[c_i = \min(a_i, b_i) \text{ for all } 1 \le i \le k\big] \tag{27}$$

3. The gcd (of given integers which are not all zero) is guaranteed to exist.
4. The gcd (when exists) is unique.
5. The gcd is commutative,[73] i.e. $\gcd(m,n) = \gcd(n,m)$.
6. The gcd is associative, i.e. $\gcd(m,n,k) = \gcd\big[\gcd(m,n),k\big] = \gcd\big[m,\gcd(n,k)\big]$. This can be extended to any number of operands.
7. The gcd scales linearly, i.e. $\gcd(km,kn) = k\gcd(m,n)$ where $k \in \mathbb{N}$.
8. The gcd can be expressed as a linear combination of its operands, i.e. if m and n are integers (having a gcd) then there are integers s and t such that $\gcd(m,n) = sm + tn$. This linear combination is usually obtained by using the **extended Euclidean algorithm** (as will be demonstrated by an example in Problem 5).
9. $k = \gcd(m,n)$ *iff* $\gcd\big[(m \div k),(n \div k)\big] = 1$ ($k \in \mathbb{N}$). In other words, m and n can be expressed as $m = k\mu$ and $n = k\nu$ where μ and ν ($\in \mathbb{Z}$) are coprime.
10. $\gcd(m,n) = \gcd(-m,n) = \gcd(m,-n) = \gcd(-m,-n)$.
11. $\gcd(1,m) = 1 \qquad \gcd(0,m) = |m| \qquad \gcd(m,m) = |m| \qquad \gcd(m,mn) = |m|$.[74]
12. If $m,n \in \mathbb{N}$ and $m < n$ then $\gcd(m,n) = \gcd(m,n-m) = \gcd(n,n-m)$.
13. If $m,n \in \mathbb{N}$ and $m < n$ then $\gcd(m,n) = \gcd(m,r)$ where r is the remainder of the division of n by m.
14. If $m,n \in \mathbb{N}$ then $mn = \gcd(m,n) \times \mathrm{lcm}(m,n)$ where lcm is the least common multiple (see § 2.5).
15. If $m \in \mathbb{N}$ then $\gcd\big[m,\mathrm{lcm}(m,n)\big] = m$.
16. From point 2 we can define the gcd of two integers (m and n) as the product of all the common prime factors in the prime factorizations of m and n.[75]
17. As indicated earlier, there are several methods for finding the gcd; the most common of these methods seems to be the prime factorization and the Euclidean algorithm. These methods differ in efficiency and applicability. For instance, the Euclidean algorithm is restricted to finding the gcd of two numbers (although it can be extended by recursive application using rule 6). We also note that the prime factorization method does not apply if one of the numbers is zero because zero has no prime factorization in the strict sense (see point 4 in the preamble of § 2.1) although this case can be trivially handled by rule 11 (with rule 6 if we have more than two operands).

Problems

1. Justify the prime factorization method for obtaining the greatest common divisor (see point 2 in the preamble of this section).
   Solution: We note first that prime factorization does not apply if one of the numbers is zero (see point 17 in the preamble) and hence we assume here that none of the numbers is zero. Now, from the given definition of gcd we can extract three (necessary and sufficient) conditions that gcd must satisfy:
   (a) $\gcd > 0$.
   (b) $\gcd \,|m$ and $\gcd \,|n$.
   (c) gcd is greater than any other natural number that divides both m and n.
   So, all we need to do is to show that the gcd (as given by Eq. 27) satisfies all these conditions. Now, from Eq. 27 it is obvious that condition (a) and condition (b) are satisfied (see Problem 3 of § 2.1). Regarding condition (c), it is obvious that any divisor to m and n cannot contain any prime factor other than $p_1, p_2, \cdots, p_k$. So, the only possibility for a divisor d that potentially-divides both m and n and it is greater than gcd is to have an extra factor of $p_1, p_2, \cdots, p_k$ in the prime factorization of gcd in Eq. 27, e.g. $d = p_1 \times \gcd = p_1^{c_1+1} p_2^{c_2} \cdots p_k^{c_k}$. However, any extra factor should make d fail to divide (at least) one of the numbers (i.e. m and n) since $c_i = \min(a_i, b_i)$ which means that we have only c_i factors of p_i in the prime factorization of (at least) one of the numbers m and n. So, d cannot be greater than gcd and divides both m and n, and hence condition (c) is also satisfied. Therefore, all the

[73] In this context, adjectives like "commutative" and "associative" should belong to the operation of taking gcd.
[74] We note that $m \in \mathbb{Z}$ (excluding 0 in the second, third and fourth statements).
[75] We note that "all the common prime factors" means "counted individually" (or considered as powered factors and not as base factors) and hence the common prime factors between 8 and 12 are $2 \times 2 = 2^2$ (i.e. not 2).

three (necessary and sufficient) conditions that gcd must satisfy are observed in the prime factorization method (as represented by Eq. 27) and hence this method for obtaining the gcd is justified.
Note: we can put the above argument in a more formal form as follows:[76]

$$\begin{aligned}
\gcd(m,n) &= \gcd\left(p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k},\ p_1^{b_1}p_2^{b_2}\cdots p_k^{b_k}\right) \\
&= p_1^{c_1}p_2^{c_2}\cdots p_k^{c_k} \times \gcd\left(p_1^{a_1-c_1}p_2^{a_2-c_2}\cdots p_k^{a_k-c_k},\ p_1^{b_1-c_1}p_2^{b_2-c_2}\cdots p_k^{b_k-c_k}\right) \\
&= p_1^{c_1}p_2^{c_2}\cdots p_k^{c_k} \times 1 \\
&= p_1^{c_1}p_2^{c_2}\cdots p_k^{c_k}
\end{aligned}$$

where line 2 is justified by rule 7 (see the preamble of this section), while line 3 is justified by the fact that $\left(p_1^{a_1-c_1}p_2^{a_2-c_2}\cdots p_k^{a_k-c_k}\right)$ and $\left(p_1^{b_1-c_1}p_2^{b_2-c_2}\cdots p_k^{b_k-c_k}\right)$ are coprime after taking the common factors $(p_1^{c_1}p_2^{c_2}\cdots p_k^{c_k})$ and hence their gcd is 1.

2. Find $\gcd(168, 28, 380, 88)$.
Solution: We use the prime factorization method:

$$168 = 2^3 \times 3 \times 7 \qquad 28 = 2^2 \times 7 \qquad 380 = 2^2 \times 5 \times 19 \qquad 88 = 2^3 \times 11$$

Hence: $\gcd(168, 28, 380, 88) = 2^2 = 4$.

3. Find $\gcd(372, 268)$.
Solution: We use the Euclidean algorithm:

$$\begin{aligned}
372 &= (268 \times 1) + 104 \\
268 &= (104 \times 2) + 60 \\
104 &= (60 \times 1) + 44 \\
60 &= (44 \times 1) + 16 \\
44 &= (16 \times 2) + 12 \\
16 &= (12 \times 1) + 4 \\
12 &= (4 \times 3) + 0
\end{aligned}$$

Hence: $\gcd(372, 268) = 4$.
Note 1: referring to footnote [70] and rule 13 we can write:

$$\begin{aligned}
\gcd(372, 268) &= \gcd(268, 104) = \gcd(104, 60) = \gcd(60, 44) = \gcd(44, 16) \\
&= \gcd(16, 12) = \gcd(12, 4) = 4
\end{aligned}$$

As we see, these equalities are obviously based on (and justified by) the fact that the gcd of two positive integers is unaffected if the bigger integer is replaced by the remainder of the division of the bigger integer by the smaller integer
Note 2: negative remainders may be used (to speed up the gcd calculations) when the negative remainders are smaller in absolute value than positive remainders. For example:

$$\begin{aligned}
372 &= (268 \times 1) + 104 \\
268 &= (104 \times 3) - 44 \\
104 &= (44 \times 2) + 16 \\
44 &= (16 \times 3) - 4 \\
16 &= (4 \times 4) + 0
\end{aligned}$$

As we see, using negative remainders reduced the number of steps required by the Euclidean algorithm by 2.

[76] In fact, this may be considered as a different argument.

4. Find $\gcd(680, 24)$, $\gcd(565, 75)$, $\gcd(273, 132)$ and $\gcd(804, 126)$.
Solution: We use the brief procedure suggested by note 1 of Problem 3 (with the use of negative remainders when appropriate according to note 2 of Problem 3):

$$\begin{aligned}\gcd(680, 24) &= \gcd(24, 8) = 8\\ \gcd(565, 75) &= \gcd(75, -35) = \gcd(35, 5) = 5\\ \gcd(273, 132) &= \gcd(132{,}9) = \gcd(9, -3) = 3\\ \gcd(804, 126) &= \gcd(126, 48) = \gcd(48, -18) = \gcd(18, -6) = 6\end{aligned}$$

5. Express $\gcd(372, 268)$ as $\gcd(372, 268) = s372 + t268$ where $s, t \in \mathbb{Z}$.
Solution: We use the extended Euclidean algorithm (by reversing the operations in Problem 3):

$$\begin{aligned}4 &= 16 - (12 \times 1) = 16 - 12 = 16 - [44 - (16 \times 2)] = -44 + (16 \times 3)\\ &= -44 + ([60 - \{44 \times 1\}] \times 3) = (-4 \times 44) + (60 \times 3) = (-4 \times [104 - \{60 \times 1\}]) + (60 \times 3)\\ &= (-4 \times 104) + (60 \times 7) = (-4 \times 104) + ([268 - \{104 \times 2\}] \times 7) = (-18 \times 104) + (268 \times 7)\\ &= (-18 \times [372 - \{268 \times 1\}]) + (268 \times 7) = (-18 \times 372) + (25 \times 268)\end{aligned}$$

Thus, $\gcd(372, 268) = 4 = (-18)372 + (25)268$, i.e. $s = -18$ and $t = 25$.
6. Find two integers a and b that satisfy the following equation: $136a + 79b = 1$.
Solution: We note that $\gcd(136, 79) = 1$. So, by using the extended Euclidean algorithm (as we did in Problem 5) we get $1 = (-18)136 + (31)79$. Therefore, a possible solution is $a = -18$ and $b = 31$.
7. Show that there are infinitely many k such that $(m + k)$ and $(n + k)$ are coprime (where $m, n, k \in \mathbb{N}$ and $m < n$).
Solution: Because $(n - m)$ has a finite number of prime factors (while there are infinitely many primes), then there are infinitely many numbers $\mathbb{N} \ni s > n$ such that $(n - m)$ and s are coprime, i.e. $\gcd\big[(n - m), s\big] = 1$. This means that there are infinitely many k such that:

$$\begin{aligned}1 &= \gcd\big[(n - m), s\big]\\ &= \gcd\big[(n - m), (n + k)\big] && (s = n + k)\\ &= \gcd\big[(n + k) - (m + k), (n + k)\big] && (\pm k)\\ &= \gcd\big[(m + k), (n + k)\big] && (\text{rule } 12)\end{aligned}$$

So, $\gcd\big[(m + k), (n + k)\big] = 1$ for infinitely many k, i.e. we have infinitely many k such that $(m + k)$ and $(n + k)$ are coprime.
8. Let $m, n, k \in \mathbb{N}$ and m and n be coprime. Show that $\gcd(mn, k) = \gcd(m, k) \times \gcd(n, k)$.
Solution: Let $m = g_m\mu$ and $n = g_n\nu$ where $\mu, \nu \in \mathbb{N}$ and $g_m = \gcd(m, k)$ and $g_n = \gcd(n, k)$. Now, because m and n are coprime then g_m and g_n are coprime (see part m of Problem 12 of § 2.2).
Also, let $k = g_m\kappa_m$ and $k = g_n\kappa_n$ ($\kappa_m, \kappa_n \in \mathbb{N}$). Since g_m and g_n are coprime then $k = g_mg_n\kappa$ where $\kappa_m = g_n\kappa$ ($\kappa \in \mathbb{N}$).
Now, μ and κ are coprime, and ν and κ are coprime, and hence (by part e of Problem 1 of § 2.2) κ is coprime to $\mu\nu$. Accordingly:

$$\gcd(mn, k) = \gcd(g_mg_n\mu\nu, g_mg_n\kappa) = g_mg_n \gcd(\mu\nu, \kappa) = g_mg_n \times 1 = g_mg_n = \gcd(m, k) \times \gcd(n, k)$$

where the third equality is justified by the fact that $\mu\nu$ and κ are coprime.
9. Let $m, n, k \in \mathbb{N}$ such that m and n are coprime and $k|(mn)$. Prove (or justify) the following:
(**a**) There are unique coprime natural numbers s and t such that $s|m$, $t|n$ and $k = st$.
(**b**) $s = \gcd(k, m)$ and $t = \gcd(k, n)$.
Solution:
(**a**) Because m and n are coprime then they must have no common prime factor in their prime factorization. Now, since $k|(mn)$ then we must have:

$$k = (p_{m_1}^{a_1} \times \ldots \times p_{m_x}^{a_x})(p_{n_1}^{b_1} \times \ldots \times p_{n_z}^{b_z})$$

such that $\left(p_{m_1}^{a_1},\ldots,p_{m_x}^{a_x}\right)$ are all the common prime factors between k and m, and $(p_{n_1}^{b_1},\ldots,p_{n_z}^{b_z})$ are all the common prime factors between k and n [noting that $\left(p_{m_1}^{a_1},\ldots,p_{m_x}^{a_x}\right)$ and $(p_{n_1}^{b_1},\ldots,p_{n_z}^{b_z})$ are coprime since m and n are coprime; see part m of Problem 12 of § 2.2]. It should be obvious that since $k|(mn)$ then k cannot contain any factor other than these (i.e. factors which are not in the prime factorization of mn) because otherwise k cannot divide mn. Hence, if we label $(p_{m_1}^{a_1}\times\ldots\times p_{m_x}^{a_x})$ as s and label $(p_{n_1}^{b_1}\times\ldots\times p_{n_z}^{b_z})$ as t then $k=st$. So in brief, we have unique coprime natural numbers $s=(p_{m_1}^{a_1}\times\ldots\times p_{m_x}^{a_x})$ and $t=(p_{n_1}^{b_1}\times\ldots\times p_{n_z}^{b_z})$ such that $s|m$, $t|n$ and $k=st$, as required.
(**b**) According to part (a), s represents all the common prime factors between k and m, while t represents all the common prime factors between k and n, and hence from the definition of gcd (see point 16 in the preamble as well as the note of Problem 1) we must have $s=\gcd(k,m)$ and $t=\gcd(k,n)$, as required.

10. Show that $\gcd(m,n)$ is divisible by any other common divisor of m and n.
Solution: If we express $\gcd(m,n)$ in its prime factorization as $\gcd(m,n)=p_1^{c_1}p_2^{c_2}\cdots p_k^{c_k}$, then any other common divisor of m and n must be a product of p_1, $p_2,\ldots,p_k$ raised (some or all) to lower powers than $c_1,c_2,\ldots,c_k$ (because $p_1^{c_1}p_2^{c_2}\ldots p_k^{c_k}$ represents all the common factors of m and n; see Problem 3 of § 2.1 as well as Problem 3 of § 2.6.1) and hence any other common divisor must divide $\gcd(m,n)$.
Note: if $\gcd(m,n)=1$ then m and n have no other common divisor (except -1 if we consider negative divisors in which case we also have $-1|1$).
11. Justify (briefly) properties 3-8 (in the preamble of this section).[77]
Solution: Property 3 is because 1 (which divides any integer) does exist, i.e. the existence of gcd in the form of 1 is guaranteed if a common divisor greater than 1 does not exist (noting that having an upper limit to such "greatest" divisor is guaranteed by the finity of the numbers which this greatest divisor is their gcd). The method of prime factorization for obtaining the greatest common divisor (see point 2 as well as Problem 1) can also provide a justification to this property.
Properties 4-7 can be appreciated by considering the method of prime factorization for obtaining the greatest common divisor (see point 2 as well as Problem 1).
Property 8 can be appreciated by considering the extended Euclidean algorithm (see § 2.3.4 as well as Problem 5 of the present section).
12. Justify point 9 (in the preamble of this section).
Solution: Briefly, this is justified by the linear scaling property (see point 7 in the preamble). In detail:
• If $k=\gcd(m,n)$ then:

$$k=\gcd\left[k(m\div k),k(n\div k)\right]=k\gcd\left[(m\div k),(n\div k)\right]$$

where we used linear scaling property in the last step. Hence, by dividing both sides by k we get: $\gcd\left[(m\div k),(n\div k)\right]=1$.
• If $\gcd\left[(m\div k),(n\div k)\right]=1$ then by multiplying both sides by k we get:

$$k=k\gcd\left[(m\div k),(n\div k)\right]=\gcd(m,n)$$

where we used the linear scaling property in the last step.
13. Justify point 10 (in the preamble of this section).
Solution: This is justified by the method of prime factorization for obtaining the greatest common divisor (see point 2 as well as Problem 1) noting that the sign does not affect the prime factors of a given integer, i.e. the prime factorization of a given integer is a property of its magnitude and not of its sign (see point 4 of § 2.1).
14. Justify the properties given in point 11 (in the preamble of this section).
Solution: Regrading $\gcd(1,m)=1$, it is self-evident because 1 is the largest natural number that divides 1. Moreover, 1 divides any integer m (see point 2 of § 1.9). Hence, $\gcd(1,m)=1$.
Regarding $\gcd(0,m)=|m|$, we have:

$$\gcd(0,m)=\gcd(0,|m|)=\gcd(0\times|m|,|m|)=|m|\gcd(0,1)=|m|\gcd(1,0)=|m|\times1=|m|$$

[77] The purpose of this Problem is to show the reader the rationale behind the properties rather than providing formal proofs.

where we used property 10 in equality 1, property 7 in equality 3, property 5 in equality 4, and used $\gcd(1,m)=1$ (which we already justified) in equality 5 (with $m=0$).
Regarding $\gcd(m,m)=|m|$, we have:

$$\gcd(m,m)=\gcd(|m|,|m|)=|m|\gcd(1,1)=|m|\times 1=|m|$$

where similar justifications apply.
Regarding $\gcd(m,mn)=|m|$, we have:

$$\gcd(m,mn)=\gcd(|m|,|m|n)=|m|\gcd(1,n)=|m|\times 1=|m|$$

where similar justifications apply.

15. Show that $\gcd(m,n)=\gcd(m,m+n)$.
Solution: Let $g=\gcd(m,n)$. Now, $g|m$ and $g|n$ and hence $g|(m+n)$ (see rule 14 of § 1.9). So, g is a common divisor of m and $m+n$. Therefore, all we need to do to complete the proof is to show that there is no common divisor of m and $m+n$ greater than g and this is what we will do using the proof by contradiction (see § 1.5.4). So, let assume that we have a common divisor G of m and $m+n$ such that $G>g$. If this is the case then G divides m and G divides $m+n$ and hence (by rule 14 of § 1.9) G divides their difference which is n. This means that G divides both m and n in contradiction to the fact that g is the greatest common divisor of m and n.
16. Justify points 12 and 13 (in the preamble of this section).
Solution: Regarding $\gcd(m,n)=\gcd(m,n-m)$ we have:

$$\gcd(m,n)=\gcd(-m,n)=\gcd(-m,n-m)=\gcd(m,n-m)$$

where we used point 10 in equality 1, used the result of Problem 15 in equality 2 (with $-m$ representing m in that result), and used point 10 in equality 3.
Regarding $\gcd(m,n)=\gcd(n,n-m)$ we have:

$$\gcd(m,n)=\gcd(n,m)=\gcd(n,-m)=\gcd(n,n-m)$$

where we used point 5 in equality 1, used point 10 in equality 2, and used the result of Problem 15 in equality 3.
Regarding $\gcd(m,n)=\gcd(m,r)$, if $n=km+r$ (where $k\in\mathbb{N}$ and $\mathbb{N}^0\ni r<m$) then this result will be obtained by applying $\gcd(m,n)=\gcd(m,n-m)$ (which we already justified) k times.
17. Prove that:

$$\gcd\left(n-1,\frac{n^k-1}{n-1}\right)=\gcd(n-1,k)\qquad\qquad(n,k\in\mathbb{N},n>1)$$

Solution: Let $g=\gcd\left(n-1,\frac{n^k-1}{n-1}\right)$. From Eq. 12 we have:

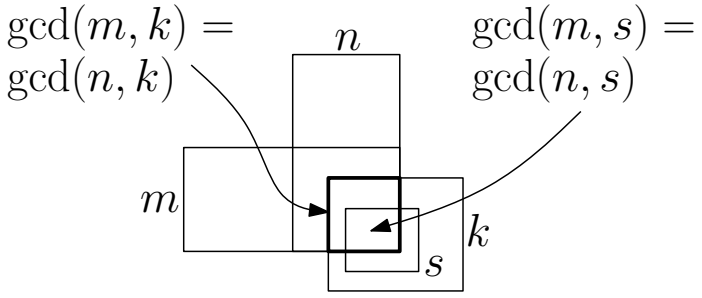
$$\begin{aligned}\frac{n^k-1}{n-1} &= n^{k-1}+n^{k-2}+\cdots+n+1\\ \frac{n^k-1}{n-1} &= (n^{k-1}-1)+(n^{k-2}-1)+\cdots+(n-1)+k \qquad (28)\\ k &= \left[\frac{n^k-1}{n-1}\right]-\left[(n^{k-1}-1)+(n^{k-2}-1)+\cdots+(n-1)\right] \qquad (29)\end{aligned}$$

Now, g divides $\left[\frac{n^k-1}{n-1}\right]$ because $g=\gcd\left(n-1,\frac{n^k-1}{n-1}\right)$.
Also, g divides $(n^{k-1}-1)+(n^{k-2}-1)+\cdots+(n-1)$ because (according to Eq. 12) each bracketed term in this sum is divisible by $(n-1)$ which is divisible by g since $g=\gcd\left(n-1,\frac{n^k-1}{n-1}\right)$.
Therefore, from Eq. 29 we conclude that g divides k (see rule 14 of § 1.9).
So, g is a common divisor of $(n-1)$ and k, and hence all we need to complete the proof is to show that

g is their greatest common divisor.
Now, let assume that $(n-1)$ and k have a common divisor $d > g$. So, from Eq. 28 we conclude that d divides $\left[\frac{n^k-1}{n-1}\right]$ because d divides k and d divides $(n-1)$ which is a common factor to all the other terms on the right hand side of Eq. 28 (see rule 14 of § 1.9). But since d divides $(n-1)$ and d divides $\left[\frac{n^k-1}{n-1}\right]$ then this means that we found a common divisor of $(n-1)$ and $\left[\frac{n^k-1}{n-1}\right]$ that is greater than their gcd (i.e. g) which is impossible. So, we conclude that g is the greatest common divisor of $(n-1)$ and k, and hence:

$$\gcd\left(n-1, \frac{n^k-1}{n-1}\right) = g = \gcd(n-1, k)$$

18. Show that if $\gcd(m,k) = \gcd(n,k)$ and $s|k$ then $\gcd(m,s) = \gcd(n,s)$ where $m, n, k, s \in \mathbb{Z}$.
Solution: Considering prime factorization, $\gcd(m,k)$ represents the common factors of m and k while $\gcd(n,k)$ represents the common factors of n and k. So, $\gcd(m,k) = \gcd(n,k)$ means that the common factors of m and k are the same as the common factors of n and k. Now, since $s|k$ then the factors of s are a subset of the factors of k. So, any factor of s must be either a common factor of k and m (and hence a common factor of k and n) or not a common factor of k and m (and hence not a common factor of k and n). This means that any factor of s must be either a common factor of s and m (and hence a common factor of s and n) or not a common factor of s and m (and hence not a common factor of s and n), i.e. $\gcd(m,s) = \gcd(n,s)$.
Note: the following "Venn diagram" illustrates the given proof (where the sets in this diagram represent the prime factors of m, n, k, s):



2.5 Least Common Multiple

The least common multiple (lcm) of two or more integers (none of which is zero) is the smallest natural number that is divisible by these integers. There are a number of methods (or algorithms) to calculate the least common multiple. The common method seems to be the one based on the **prime factorization** which will be outlined, justified and demonstrated in the following (see point 2 and Problems 1 and 2). The gcd and the lcm can also be obtained from each other by using the relation $\gcd(m,n) \times \text{lcm}(m,n) = mn$ (and hence we can obtain the lcm from the gcd which can be obtained for instance by the Euclidean algorithm).

We list in the following points some common rules and facts about the least common multiple (lcm) which will be used or referred to in the future or are important to know as general background knowledge:
1. By definition, the least common multiple is a natural number, i.e. it is always positive integer.
2. If m and n are positive integers whose prime factorizations are:[78]

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \qquad (a_i \in \mathbb{N}^0 \text{ for all } 1 \le i \le k) \tag{30}$$

$$n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k} \qquad (b_i \in \mathbb{N}^0 \text{ for all } 1 \le i \le k) \tag{31}$$

[78] As indicated earlier, we allow a_i and b_i to be zero to include the case when some primes are present in the factorization of only one of m and n.

then

$$\text{lcm}(m,n) = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k} \qquad \big[d_i = \max(a_i, b_i) \text{ for all } 1 \le i \le k\big] \tag{32}$$

3. The lcm (of given non-zero integers) is guaranteed to exist.
4. The lcm (when exists) is unique.
5. The lcm is commutative,[79] i.e. $\text{lcm}(m,n) = \text{lcm}(n,m)$.
6. The lcm is associative, i.e. $\text{lcm}(m,n,k) = \text{lcm}\big[\text{lcm}(m,n),k\big] = \text{lcm}\big[m,\text{lcm}(n,k)\big]$. This can be extended to any number of operands.
7. The lcm scales linearly, i.e. $\text{lcm}(km,kn) = k\,\text{lcm}(m,n)$ where $k \in \mathbb{N}$.
8. $\text{lcm}(m,n) = \text{lcm}(-m,n) = \text{lcm}(m,-n) = \text{lcm}(-m,-n)$.
9. $\text{lcm}(1,m) = |m| \qquad \text{lcm}(m,m) = |m| \qquad \text{lcm}(m,mn) = |mn|$.
10. If $m,n \in \mathbb{N}$ then $mn = \gcd(m,n) \times \text{lcm}(m,n)$ where gcd is the greatest common divisor (see § 2.4).
11. If $m \in \mathbb{N}$ then $\text{lcm}\big[m,\gcd(m,n)\big] = m$.

Problems

1. Justify the prime factorization method for obtaining the least common multiple (see point 2 in the preamble of this section).
   Solution: The justification is similar to the justification of prime factorization method for obtaining the gcd (which we discussed in Problem 1 of § 2.4). So, in the following we just outline the argument: Referring to Eq. 32, $p_1^{d_1}$ must be a factor of lcm where d_1 is the least positive power such that $p_1^{d_1}$ can be divided by the p_1 factors in both m and n, and this means that d_1 must be the maximum of a_1 and b_1. This argument obviously applies to all $p_i^{d_i}$ $(i = 1,2,\ldots,k)$. So, lcm must be the product of all these $p_i^{d_i}$ factors (which is what is given by Eq. 32).
2. Find $\text{lcm}(168,28,380,88)$.
   Solution: We use the prime factorization method:

   $$168 = 2^3 \times 3 \times 7 \qquad 28 = 2^2 \times 7 \qquad 380 = 2^2 \times 5 \times 19 \qquad 88 = 2^3 \times 11$$

   Hence: $\text{lcm}(168,28,380,88) = 2^3 \times 3 \times 5 \times 7 \times 11 \times 19 = 175560$.
3. Justify (briefly) properties 3-7 (in the preamble of this section).[80]
   Solution: Property 3 is because a common multiple (i.e. the product of the numbers) always exists, i.e. the existence of lcm in the form of this product is guaranteed if a common multiple lower than this product does not exist (noting that having a lower limit to such "least" multiple is guaranteed by the finity of the numbers which this least multiple is their lcm). The method of prime factorization for obtaining the least common multiple (see point 2 as well as Problem 1) can also provide a justification to this property.
   Properties 4-7 can be appreciated by considering the method of prime factorization for obtaining the least common multiple (see point 2 as well as Problem 1).
4. Justify point 8 (in the preamble of this section).
   Solution: This is justified by the method of prime factorization for obtaining the least common multiple (see point 2 as well as Problem 1) noting that the sign does not affect the prime factors of a given integer, i.e. the prime factorization of a given integer is a property of its magnitude and not of its sign (see point 4 of § 2.1).
5. Justify the properties given in point 9 (in the preamble of this section).
   Solution: Regrading $\text{lcm}(1,m) = |m|$, it is self-evident because $|m|$ is the smallest natural number that is divisible by m. Moreover, $|m|$ is divisible by 1. Hence, $\text{lcm}(1,m) = |m|$.
   Regarding $\text{lcm}(m,m) = |m|$, we have:

   $$\text{lcm}(m,m) = \text{lcm}(|m|,|m|) = |m|\,\text{lcm}(1,1) = |m| \times 1 = |m|$$

   where we used property 8 in equality 1, property 7 in equality 2, and used $\text{lcm}(1,m) = |m|$ (which we already justified) in equality 3 (with $m = 1$).

[79] In this context, adjectives like "commutative" and "associative" should belong to the operation of taking lcm.

[80] As before, the purpose of this Problem is to show the reader the rationale behind the properties rather than providing formal proofs.

Regarding $\text{lcm}(m, mn) = |mn|$, we have:

$$\text{lcm}(m, mn) = \text{lcm}(|m|, |m|\, n) = |m|\, \text{lcm}(1, n) = |m|\, |n| = |mn|$$

where we used property 8 in equality 1, property 7 in equality 2, and used $\text{lcm}(1, m) = |m|$ (which we already justified) in equality 3 (with $m = n$).

6. Show the following:
(**a**) $mn = \gcd(m, n) \times \text{lcm}(m, n)$ where $m, n \in \mathbb{N}$.
(**b**) $\gcd\big[m, \text{lcm}(m, n)\big] = m$ where $m \in \mathbb{N}$.
(**c**) $\text{lcm}\big[m, \gcd(m, n)\big] = m$ where $m \in \mathbb{N}$.
(**d**) m and n are coprime *iff* $\text{lcm}(m, n) = mn$ (where $m, n \in \mathbb{N}$).
(**e**) $\gcd\big[m + n, \text{lcm}(m, n)\big] = \gcd(m, n)$.
Solution:
(**a**) We note (with reference to point 2 of § 2.4 and point 2 of the present section) that $c_i + d_i = \min(a_i, b_i) + \max(a_i, b_i) = a_i + b_i$. Hence:

$$\begin{aligned} \gcd(m, n) \times \text{lcm}(m, n) &= \left(p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}\right) \times \left(p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}\right) = p_1^{c_1+d_1} p_2^{c_2+d_2} \cdots p_k^{c_k+d_k} \\ &= p_1^{a_1+b_1} p_2^{a_2+b_2} \cdots p_k^{a_k+b_k} = \left(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}\right) \times \left(p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}\right) = mn \end{aligned}$$

Note: this result cannot be extended to more than two numbers, i.e. $m_1 \times m_2 \times \cdots \times m_r \neq \gcd(m_1, m_2, \ldots, m_r) \times \text{lcm}(m_1, m_2, \ldots, m_r)$ in general. For example, $\gcd(2, 3, 4) = 1$ and $\text{lcm}(2, 3, 4) = 12$ and hence $\gcd(2, 3, 4) \times \text{lcm}(2, 3, 4) = 12$ while $2 \times 3 \times 4 = 24$.
(**b**) $\text{lcm}(m, n)$ is a multiple of m, i.e. $\text{lcm}(m, n) = km$ ($k \in \mathbb{N}$). Hence:

$$\gcd\big[m, \text{lcm}(m, n)\big] = \gcd\big[m, km\big] = m \gcd\big[1, k\big] = m \times 1 = m$$

where we used point 7 of § 2.4 in step 2, and used point 11 of § 2.4 in step 3.
(**c**) $\gcd(m, n)$ is a divisor of m, i.e. $m = k \gcd(m, n)$ where $k \in \mathbb{N}$. Hence:

$$\text{lcm}\big[m, \gcd(m, n)\big] = \text{lcm}\big[k \gcd(m, n), \gcd(m, n)\big] = \gcd(m, n) \times \text{lcm}\big[k, 1\big] = \gcd(m, n) \times k = m$$

where we used point 7 of the present section in step 2, and used point 9 of the present section (with point 5) in step 3.
(**d**) We use the relation $mn = \gcd(m, n) \times \text{lcm}(m, n)$ which we proved already in part (a).
The if part: if $\text{lcm}(m, n) = mn$, then $mn = \gcd(m, n) \times mn$ and hence $\gcd(m, n) = 1$, i.e. m and n are coprime.
The only if part: if m and n are coprime, then $\gcd(m, n) = 1$ and hence $mn = 1 \times \text{lcm}(m, n)$, i.e. $\text{lcm}(m, n) = mn$.
Note: this result can be easily extended to more than two numbers, i.e. $m_1, m_2, \ldots, m_i$ are pairwise coprime *iff* $\text{lcm}(m_1, m_2, \ldots, m_i) = m_1 \times m_2 \times \ldots \times m_i$. This is because if the numbers are pairwise coprime then there is no common prime factor between any two of them and hence their lcm must contain all their prime factors (so that it can be divided by each one of them) which means that their lcm is their product. The converse can be proved by reversing this argument.
(**e**) Let $m = D\mu$ and $n = D\nu$ where $D = \gcd(m, n)$. This means that μ and ν are coprime (see point 9 of § 2.4). Accordingly:

$$\begin{aligned} \gcd\big[\mu + \nu, \mu\nu\big] &= 1 && \text{(see Problem 25 of § 2.2)} \\ \gcd\big[\mu + \nu, \text{lcm}(\mu, \nu)\big] &= 1 && \text{(see part d of the present Problem)} \\ D \gcd\big[\mu + \nu, \text{lcm}(\mu, \nu)\big] &= D && (\times D) \\ \gcd\big[D\mu + D\nu, D\, \text{lcm}(\mu, \nu)\big] &= D && \text{(point 7 of § 2.4)} \\ \gcd\big[D\mu + D\nu, \text{lcm}(D\mu, D\nu)\big] &= D && \text{(point 7 of the present section)} \\ \gcd\big[m + n, \text{lcm}(m, n)\big] &= \gcd(m, n) && \big[m = D\mu,\ n = D\nu,\ D = \gcd(m, n)\big] \end{aligned}$$

7. Find a formula for the smallest natural number that is divisible by all the natural numbers up to and including n (where $n \in \mathbb{N}$).
Solution: We are actually looking for a formula for $\text{lcm}(2, 3, \ldots, n)$. Now, if $p_1, p_2, \ldots, p_k$ are all the primes that are less than or equal to n then each one of the numbers $\{2, 3, \ldots, n\}$ can be prime factorized as $p_1^{c_{i1}} p_2^{c_{i2}} \cdots p_k^{c_{ik}}$ (where $i = 2, 3, \ldots, n$ and the c_i's $\in \mathbb{N}^0$). Now, if:

C_1 is the largest of c_{i1}'s $\quad$ C_2 is the largest of c_{i2}'s $\quad \cdots \quad$ C_k is the largest of c_{ik}'s

then $\text{lcm}(2, 3, \ldots, n) = p_1^{C_1} p_2^{C_2} \cdots p_k^{C_k}$.

2.6 Common Functions in Number Theory

In the following subsections we define and investigate briefly some of the common functions met in number theory. Although these functions (or some of them) may be defined on non-zero integers (by including the negative integers), in the following we consider only natural numbers to avoid some unnecessary complications in the presentation and notation (noting that valid extensions to negative integers are generally obvious).

2.6.1 The Divisor Function

The divisor function $\sigma(n)$ is defined as the sum of the positive divisors of n (including 1 and n). In other words, $\sigma(n)$ is the sum of the proper divisors of n plus n. Accordingly:

$$\sigma(n) = \sum_{d|n} d \qquad\qquad (n, d \in \mathbb{N}) \tag{33}$$

For example:

$$\sigma(23) = 1 + 23 = 24 \qquad \sigma(125) = 1 + 5 + 25 + 125 = 156 \qquad \sigma(203) = 1 + 7 + 29 + 203 = 240$$

We list in the following points some common facts about the divisor function which will be used or referred to in the future or are important to know as general background knowledge:
1. The divisor function is multiplicative, i.e. $\sigma(mn) = \sigma(m)\sigma(n)$ where m and n are coprime.
2. n is prime *iff* $\sigma(n) = 1 + n$.
3. For $p \in \mathbb{P}$ and $a \in \mathbb{N}$ we have:
$$\sigma(p^a) = \frac{p^{a+1} - 1}{p - 1} \tag{34}$$
4. If $\mathbb{N} \ni n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ (where $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ represents the prime factorization of n) then:
$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1} \tag{35}$$
5. The divisor function is many-to-one, i.e. $m = n \;\; \rightarrow \;\; \sigma(m) = \sigma(n)$ but $\sigma(m) = \sigma(n) \;\; \nrightarrow \;\; m = n$. For example, $\sigma(16) = \sigma(25) = 31$.
6. Eq. 34 is a special case of Eq. 35 (corresponding to $k = 1$), while $\sigma(n) = 1 + n$ ($n \in \mathbb{P}$) is a special case of Eq. 34 (corresponding to $a = 1$ noting that $n = p$ in this case).

Problems

1. Prove (or justify) points 1-4 in the preamble.
Solution:
Point 1: we have:
$$\sigma(m)\sigma(n) = \left(\sum_{d_m|m} d_m \right) \left(\sum_{d_n|n} d_n \right) = \sum_{d_m|m} \sum_{d_n|n} d_m d_n = \sum_{d_{mn}|mn} d_{mn} = \sigma(mn)$$

where the first and last equalities are from Eq. 33, while the second and third equalities are because m and n are coprime (and hence all the d_m and d_n which are greater than 1 are different).
Point 2: this is obvious from the definition of prime (see § 2.2) associated with the definition of the divisor function, i.e. 1 and n are the only positive divisors of n *iff* n is prime and hence $\sigma(n) = 1 + n$.
Point 3: this is because the positive divisors of p^a are $1, p^1, p^2, \ldots, p^a$ (see Problem 3 of § 2.1 and Problem 3 of the present subsection) and hence we have (see Eq. 12):

$$\sigma(p^a) = 1 + p^1 + p^2 + \cdots + p^a = \frac{p^{a+1} - 1}{p - 1}$$

Point 4: this is a result of point 3 (noting that the divisor function is multiplicative and the natural powers of distinct primes are coprime), that is:

$$\sigma(n) = \sigma(p_1^{a_1})\sigma(p_2^{a_2}) \cdots \sigma(p_k^{a_k}) = \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1}$$

2. Evaluate the divisor function σ of the following integers:
(**a**) 236. (**b**) 421. (**c**) 37^7. (**d**) 19^{12}. (**e**) 13060498880585. (**f**) 248814740604969.
Solution:
(**a**) We use Eq. 33: $\sigma(236) = 1 + 2 + 4 + 59 + 118 + 236 = 420$.
(**b**) We use Eq. 33: $\sigma(421) = 1 + 421 = 422$.
(**c**) We use Eq. 34:

$$\sigma(37^7) = \frac{37^8 - 1}{36} = 97568873720$$

(**d**) We use Eq. 34:

$$\sigma(19^{12}) = \frac{19^{13} - 1}{18} = 2336276859014281$$

(**e**) We use Eq. 35 (noting that $13060498880585 = 5 \times 13^3 \times 29^4 \times 41^2$):

$$\sigma(13060498880585) = \left(\frac{5^2 - 1}{5 - 1}\right)\left(\frac{13^4 - 1}{13 - 1}\right)\left(\frac{29^5 - 1}{29 - 1}\right)\left(\frac{41^3 - 1}{41 - 1}\right) = 18023761082040$$

(**f**) We use Eq. 35 (noting that $248814740604969 = 3^5 \times 7^2 \times 11^3 \times 17 \times 31^4$):

$$\sigma(248814740604969) = \left(\frac{3^6 - 1}{3 - 1}\right)\left(\frac{7^3 - 1}{7 - 1}\right)\left(\frac{11^4 - 1}{11 - 1}\right)\left(\frac{17^2 - 1}{17 - 1}\right)\left(\frac{31^5 - 1}{31 - 1}\right) = 521767495529280$$

3. Show that all the positive divisors of $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ $(m \in \mathbb{N})$ are of the form $p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ where $0 \leq b_i \leq a_i$ $(i = 1, 2, \ldots, k)$.
Solution: By the fundamental theorem of arithmetic (and using the rules of indices) we can write m uniquely as:

$$m = \left(p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}\right)\left(p_1^{a_1 - b_1} p_2^{a_2 - b_2} \cdots p_k^{a_k - b_k}\right) \qquad (0 \leq b_i \leq a_i, i = 1, 2, \ldots, k)$$

and hence all the divisors are of the form $p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$. Also see Problem 3 of § 2.1.
4. Show that $\sigma(n) = \sum_{d|n} \frac{n}{d}$ where d represents the positive divisors of n (including 1 and n).
Solution: We have:

$$\sigma(n) = \sum_{d|n} d \qquad \text{(Eq. 33)}$$

$$\sigma(n) = \sum_{d|n} \frac{n}{d} \qquad \text{(see part b of Problem 19 of § 1.9)}$$

2.6.2 The Restricted Divisor Function

The restricted divisor function $s(n)$ is defined as the sum of the proper divisors of n. Accordingly:

$$s(n) = \sum_{d|n,\, d\neq n} d = \left(\sum_{d|n} d\right) - n = \sigma(n) - n \qquad (n, d \in \mathbb{N}) \tag{36}$$

For example:

$$s(23) = 1 \qquad s(125) = 1 + 5 + 25 = 31 \qquad s(203) = 1 + 7 + 29 = 37$$

We list in the following points some common facts about the restricted divisor function:
1. The restricted divisor function is multiplicative, i.e. $s(mn) = s(m)s(n)$ where m and n are coprime.
2. n is prime *iff* $s(n) = 1$.
3. The restricted divisor function is many-to-one, i.e. $m = n \quad \rightarrow \quad s(m) = s(n)$ but $s(m) = s(n) \quad \nrightarrow m = n$. For example, $s(n) = 1$ for all primes.
4. The easiest way to calculate the restricted divisor function (in the non-trivial cases) is to use the formula $s(n) = \sigma(n) - n$ (see Eq. 36) where $\sigma(n)$ is calculated by the formulae given in § 2.6.1.

Problems

1. Prove (or justify) points 1 and 2 in the preamble.
   Solution:
   Point 1: we repeat the argument of the divisor function (which we presented in point 1 of Problem 1 of § 2.6.1) but with d_m and d_n standing now for the proper divisors of m and n.
   Point 2: this is obvious from the definition of prime (see § 2.2) associated with the definition of the restricted divisor function, , i.e. 1 is the only proper divisor of n *iff* n is prime and hence $s(n) = 1$.
2. Show that if $s \equiv s(n)$ is a proper divisor of n then n is prime.
   Solution: Since s is the value of the restricted divisor function then $s = s + t$ (where t is the sum of the other proper divisors) and hence $t = 0$. This means that s represents a single divisor which must be 1 because if it is not 1 then n must have 1 as another proper divisor and hence $t \neq 0$. So, we have $s(n) = 1$. Now, if we remember that n is prime *iff* $s(n) = 1$ (see point 2 in the preamble) then we conclude that n is prime.
3. Evaluate the restricted divisor function s of the integers of Problem 2 of § 2.6.1.
   Solution: These can be easily obtained by the formula $s(n) = \sigma(n) - n$ (see Eq. 36) using the values of $\sigma(n)$ that we calculated in Problem 2 of § 2.6.1 (see point 4 in the preamble).

2.6.3 The tau Function

The tau function $\tau(n)$ is defined as the number of positive divisors of n (including 1 and n). Accordingly:

$$\tau(n) = \sum_{d|n} 1 \qquad (n, d \in \mathbb{N}) \tag{37}$$

For example:

$$\tau(23) = 2 \qquad \tau(125) = 4 \qquad \tau(203) = 4$$

We list in the following points some common facts about the tau function:
1. The tau function is multiplicative, i.e. $\tau(mn) = \tau(m)\tau(n)$ where m and n are coprime.
2. n is prime *iff* $\tau(n) = 2$.
3. For $p \in \mathbb{P}$ and $a \in \mathbb{N}$ we have:
$$\tau(p^a) = a + 1 \tag{38}$$
4. If $\mathbb{N} \ni n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ (where $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ represents the prime factorization of n) then:
$$\tau(n) = \prod_{i=1}^{k} (a_i + 1) \tag{39}$$

5. The tau function is many-to-one, i.e. $m = n \quad \rightarrow \quad \tau(m) = \tau(n)$ but $\tau(m) = \tau(n) \quad \nrightarrow \quad m = n$. For example, $\tau(n) = 2$ for all primes.
6. Eq. 38 is a special case of Eq. 39 (corresponding to $k = 1$), while $\tau(n) = 2$ ($n \in \mathbb{P}$) is a special case of Eq. 38 (corresponding to $a = 1$ noting that $n = p$ in this case).

Problems

1. Prove (or justify) points 1-4 in the preamble.
   Solution:
   Point 1: we have:

$$\tau(m)\tau(n) = \left(\sum_{d_m|m} 1\right)\left(\sum_{d_n|n} 1\right) = \sum_{d_m|m}\sum_{d_n|n} 1 = \sum_{d_{mn}|mn} 1 = \tau(mn)$$

   where the first and last equalities are from Eq. 37, while the second and third equalities are because m and n are coprime.
   Point 2: this is obvious from the definition of prime (see § 2.2) associated with the definition of the tau function, i.e. 1 and n are the only positive divisors of n *iff* n is prime and hence $\tau(n) = 2$.
   Point 3: this is because the divisors of p^a are $1, p^1, p^2, \ldots, p^a$ (see Problem 3 of § 2.1 and Problem 3 of § 2.6.1) and hence their number $\big[$which is $\tau(p^a)\big]$ is $(a + 1)$.
   Point 4: this is a result of point 3 (noting that the divisor function is multiplicative and the natural powers of distinct primes are coprime), that is:

$$\tau(n) = \tau(p_1^{a_1})\tau(p_2^{a_2})\cdots\tau(p_k^{a_k}) = \prod_{i=1}^{k}(a_i + 1)$$

2. Evaluate the tau function τ of the integers of Problem 2 of § 2.6.1.
   Solution: Using Eqs. 37, 38 and 39 we get:

$$\begin{aligned}
\tau(236) &= \tau(2^2 \times 59) = (2+1)(1+1) = 6\\
\tau(421) &= \tau(1 \times 421) = 1 + 1 = 2\\
\tau(37^7) &= (7+1) = 8\\
\tau(19^{12}) &= (12+1) = 13\\
\tau(13060498880585) &= \tau(5 \times 13^3 \times 29^4 \times 41^2) = (1+1)(3+1)(4+1)(2+1) = 120\\
\tau(248814740604969) &= \tau(3^5 \times 7^2 \times 11^3 \times 17 \times 31^4) = (5+1)(2+1)(3+1)(1+1)(4+1) = 720
\end{aligned}$$

3. Show that a natural number has an even number of (positive) divisors unless it is a perfect square (in which case it has an odd number of divisors).
   Solution: We note first that this statement is true for 1 (which is a perfect square and has only 1 positive divisor, i.e. 1), so the following is about natural numbers > 1.
   According to Eq. 39 (noting that Eq. 38 is a special case of Eq. 39), τ is even unless all a_i's are even. In more details:
   • If any of the a_i's is odd then (at least) one of the factors $(a_i + 1)$ is even and hence the product (i.e. τ) is even (see rule 6 of § 1.8) which means that the number of divisors (i.e. τ) is even. Now, if any of the a_i's is odd then n cannot be a perfect square (because each prime factor of a perfect square must have an even power noting that if $m = p_1^{b_1}p_2^{b_2}\cdots p_k^{b_k}$ then $m^2 = p_1^{2b_1}p_2^{2b_2}\cdots p_k^{2b_k}$). So, if a natural number is not a perfect square then it must have an even number of divisors.
   • If none of the a_i's is odd then all the factors $(a_i + 1)$ are odd and hence the product (i.e. τ) is odd (see rule 6 of § 1.8) which means that the number of divisors (i.e. τ) is odd. Now, if none of the a_i's is odd then n must be a perfect square (because if $s = p_1^{2c_1}p_2^{2c_2}\cdots p_k^{2c_k}$ then $\sqrt{s} = p_1^{c_1}p_2^{c_2}\cdots p_k^{c_k}$ which means that s is a perfect square). So, if a natural number is a perfect square then it must have an odd number of divisors.
   So in brief, n is a perfect square *iff* $\tau(n)$ is odd (where $n \in \mathbb{N}$). Also see Problem 18 of § 1.9.

2.6.4 The Totient Function

The totient **(**or **phi** or **Euler)** function $\phi(n)$ is defined (for $n \in \mathbb{N}$) as the number of positive integers which are less than or equal to n and are relatively prime to n. Accordingly:

$$\phi(n) = \sum_{k=1}^{n} \text{floor}\left[\frac{1}{\gcd(n,k)}\right] \qquad (n,k \in \mathbb{N}) \tag{40}$$

We may also define the totient function as:

$$\phi(n) = \sum_{c} 1 \qquad \Big[1 \leq c \leq n, \gcd(c,n) = 1\Big] \tag{41}$$

For example:

$$\phi(1) = 1 \qquad \phi(2) = 1 \qquad \phi(3) = 2 \qquad \phi(8) = 4$$

We list in the following points some common facts about the totient function:
1. The totient function is multiplicative, i.e. $\phi(mn) = \phi(m)\phi(n)$ where m and n are coprime.
2. n is prime *iff* $\phi(n) = n - 1$.
3. For $p \in \mathbb{P}$ and $a \in \mathbb{N}$ we have:
$$\phi(p^a) = p^a - p^{a-1} \tag{42}$$
4. If $\mathbb{N} \ni n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ (where $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ represents the prime factorization of n) then:
$$\begin{aligned} \phi(n) &= \left(p_1^{a_1} - p_1^{a_1-1}\right)\left(p_2^{a_2} - p_2^{a_2-1}\right)\cdots\left(p_k^{a_k} - p_k^{a_k-1}\right) &(43)\\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right) &(44)\end{aligned}$$
5. $\phi(n)$ is even for all integers greater than 2.
6. For all $n \in \mathbb{N}$ we have:
$$\sum_{d|n} \phi(d) = n \tag{45}$$
7. For all $n > 1$, $\phi(n) \leq (n-1)$.
8. The totient function is many-to-one, i.e. $m = n \;\; \rightarrow \;\; \phi(m) = \phi(n)$ but $\phi(m) = \phi(n) \;\; \nrightarrow \;\; m = n$. For example, $\phi(3) = \phi(4) = 2$.
9. Eq. 42 is a special case of Eq. 43 (corresponding to $k = 1$), while $\phi(n) = n - 1$ $(n \in \mathbb{P})$ is a special case of Eq. 42 (corresponding to $a = 1$ noting that $n = p$ in this case).

Problems

1. Prove (or justify) points 1-7 in the preamble.
Solution:
Point 1: we have:
$$\phi(m)\phi(n) = \left(\sum_{c_m} 1\right)\left(\sum_{c_n} 1\right) = \sum_{c_m}\sum_{c_n} 1 = \sum_{c_{mn}} 1 = \phi(mn)$$
where the first and last equalities are from Eq. 41, while the second and third equalities are because m and n are coprime.
Point 2: this is because all the numbers $1, 2, \ldots, n$ are relatively prime to n except n (noting that n is prime).
Point 3: this is because the list of numbers $1, 2, \ldots, p^a$ contains p^a entries. Now, the entries in this list that are not coprime to p^a are the multiples of p and we have $p^a/p = p^{a-1}$ of them.[81] Hence, the

[81] This is because $p^a = (p^{a-1})p$ and hence we have p^{a-1} (natural) multiples of p, i.e. $p, 2p, 3p, \ldots, (p^{a-1})p$.

number of entries of relatively primes to p in this list must be $p^a - p^{a-1}$.
Point 4: this is because (noting that the totient function is multiplicative and the natural powers of distinct primes are coprime):

$$\begin{aligned}
\phi(n) &= \phi\left(p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}\right) && \left(n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}\right)\\
&= \phi\left(p_1^{a_1}\right)\phi\left(p_2^{a_2}\right)\cdots\phi\left(p_k^{a_k}\right) && \text{(multiplicativity)}\\
&= \left(p_1^{a_1} - p_1^{a_1-1}\right)\left(p_2^{a_2} - p_2^{a_2-1}\right)\cdots\left(p_k^{a_k} - p_k^{a_k-1}\right) && \text{(Eq. 42)}\\
&= p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right) && \text{(factorizing)}\\
&= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right) && \left(n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}\right)
\end{aligned}$$

Point 5: to justify this we consider the following two cases (which are comprehensive and mutually exclusive):
• If n is prime then (according to point 2) $\phi(n) = (n-1)$ which is even because all primes > 2 are odd.
• If n is composite then (from Eq. 43 noting that Eq. 42 is a special case of Eq. 43) $\phi(n)$ is even because all the factors in the product are even (see rules 4 and 6 of § 1.8).
Point 6: $\sum_{d|n}\phi(d)$ represents the number of pairs (a_i, b_j) (where $a_i, b_j \in \mathbb{N}$) such that b_j divides n, $a_i \le b_j$ and a_i is relatively prime to b_j. Now, if we form the set of fractions: $\{1/n, 2/n, \ldots, n/n\}$ and reduce them to their simplest form then we will have a set of fractions of the form s_k/t_m representing all the pairs (s_k, t_m) such that t_m divides n (because t_m is either equal to n or it is a factor of n), $s_k \le t_m$ (because all the original fractions are ≤ 1 and so is their reduced form) and s_k is relatively prime to t_m (because s_k/t_m are in their reduced form). Now, since we have n unique fractions of the form $\{1/n, 2/n, \ldots, n/n\}$ (and hence n unique fractions of the reduced form) then we must have n pairs of (s_k, t_m) corresponding to n pairs of (a_i, b_j), i.e. $\sum_{d|n}\phi(d) = n$.
Point 7: this is obvious from the definition of $\phi(n)$ noting that n (which is > 1) cannot be coprime to itself. More clearly, the number of positive integers $\le n$ is n, so if we exclude n (because n is not coprime to itself when $n > 1$) then we must have $\phi(n) \le (n-1)$ where $n > 1$.

2. Evaluate the totient function ϕ of the integers of Problem 2 of § 2.6.1.
Solution: Using Eqs. 42 and 43 we get:

$$\begin{aligned}
\phi(236) &= \phi(2^2 \times 59) = (2^2 - 2)(59 - 1) = 116\\
\phi(421) &= \phi(1 \times 421) = (421 - 1) = 420\\
\phi(37^7) &= (37^7 - 37^6) = 92366150724\\
\phi(19^{12}) &= (19^{12} - 19^{11}) = 2096824660167942\\
\phi(13060498880585) &= \phi(5 \times 13^3 \times 29^4 \times 41^2) = (5-1)(13^3 - 13^2)(29^4 - 29^3)(41^2 - 41)\\
&= 9084976642560\\
\phi(248814740604969) &= \phi(3^5 \times 7^2 \times 11^3 \times 17 \times 31^4)\\
&= (3^5 - 3^4)(7^2 - 7)(11^3 - 11^2)(17 - 1)(31^4 - 31^3) = 117726977491200
\end{aligned}$$

3. Show the following (where $p \in \mathbb{P}$ and $n \in \mathbb{N}$):
(**a**) $\sigma(p) + \phi(p) = 2p$. (**b**) $\sigma(p) = \tau(p) + \phi(p)$. (**c**) $\phi(8n^2 + 24n + 18) = \phi\big[(2n+3)^2\big]$.
Solution:
(**a**) Referring to point 2 of § 2.6.1 and point 2 of the present subsection, we have:

$$\sigma(p) + \phi(p) = (p+1) + (p-1) = 2p$$

(**b**) Referring to point 2 of § 2.6.1, point 2 of § 2.6.3 and point 2 of the present subsection, we have:

$$\sigma(p) = p + 1 = 2 + (p-1) = \tau(p) + \phi(p)$$

(**c**) We have:

$$\phi(8n^2+24n+18)=\phi\big[2(2n+3)^2\big]=\phi(2)\times\phi\big[(2n+3)^2\big]=\phi\big[(2n+3)^2\big]$$

where in the second step we use the multiplicativity of the totient function noting that $(2n+3)^2$ is odd (see the rules of parity in § 1.8) and hence it is coprime to 2, while the last step is because $\phi(2)=1$.

4. Show the following:

$$\phi(mn)=g\,\phi(l)\qquad\qquad\big[m,n\in\mathbb{N},\ g=\gcd(m,n),\ l=\mathrm{lcm}(m,n)\big]\tag{46}$$

Solution: p is a prime factor of mn *iff* p is a prime factor of their lcm, i.e. l (see point 2 and Problem 1 of § 2.5). Hence, if we label any such prime factor with p then from Eq. 44 we have $\phi(mn)=mn\prod_p(1-p^{-1})$ and $\phi(l)=l\prod_p(1-p^{-1})$ and hence:

$$\frac{\phi(mn)}{mn}=\prod_p\left(1-p^{-1}\right)=\frac{\phi(l)}{l}\qquad\rightarrow\qquad\frac{\phi(mn)}{mn}=g\frac{\phi(l)}{mn}\qquad\rightarrow\qquad\phi(mn)=g\,\phi(l)$$

where we used the identity $mn=\gcd(m,n)\times\mathrm{lcm}(m,n)$ in the middle step (see part a of Problem 6 of § 2.5).

5. Show the following:

$$\phi(mn)=\frac{g\,\phi(m)\,\phi(n)}{\phi(g)}\qquad\qquad\big[m,n\in\mathbb{N}\text{ and }g=\gcd(m,n)\big]\tag{47}$$

Solution: Let do the following:
- Label any prime factor of m as p_{mg}.
- Label any prime factor of n as p_{ng}.
- Label any prime factor of the product of m and n (i.e. mn) as p_{mn}.
- Label any prime factor that is exclusive to m as p_m.
- Label any prime factor that is exclusive to n as p_n.
- Label any prime factor of both m and n (i.e. belongs to their gcd) as p_g.

Now, we have:

$$\begin{aligned}
\prod_{p_{mn}}\left(1-p_{mn}^{-1}\right)&=\left[\prod_{p_m}\left(1-p_m^{-1}\right)\right]\left[\prod_{p_g}\left(1-p_g^{-1}\right)\right]\left[\prod_{p_n}\left(1-p_n^{-1}\right)\right]\\
\prod_{p_{mn}}\left(1-p_{mn}^{-1}\right)&=\frac{\left[\prod_{p_m}\left(1-p_m^{-1}\right)\right]\left[\prod_{p_g}\left(1-p_g^{-1}\right)\right]\left[\prod_{p_n}\left(1-p_n^{-1}\right)\right]\left[\prod_{p_g}\left(1-p_g^{-1}\right)\right]}{\prod_{p_g}\left(1-p_g^{-1}\right)}\\
\prod_{p_{mn}}\left(1-p_{mn}^{-1}\right)&=\frac{\left[\prod_{p_{mg}}\left(1-p_{mg}^{-1}\right)\right]\left[\prod_{p_{ng}}\left(1-p_{ng}^{-1}\right)\right]}{\prod_{p_g}\left(1-p_g^{-1}\right)}\\
mn\prod_{p_{mn}}\left(1-p_{mn}^{-1}\right)&=\frac{m\left[\prod_{p_{mg}}\left(1-p_{mg}^{-1}\right)\right]n\left[\prod_{p_{ng}}\left(1-p_{ng}^{-1}\right)\right]}{\prod_{p_g}\left(1-p_g^{-1}\right)}\\
\phi(mn)&=\frac{\phi(m)\,\phi(n)}{\prod_{p_g}\left(1-p_g^{-1}\right)}\\
\phi(mn)&=\frac{g\,\phi(m)\phi(n)}{g\prod_{p_g}\left(1-p_g^{-1}\right)}\\
\phi(mn)&=\frac{g\,\phi(m)\,\phi(n)}{\phi(g)}
\end{aligned}$$

where we used Eq. 44 in lines 5 and 7.
Note: when m and n are coprime, Eq. 47 reduces to $\phi(mn) = \phi(m)\phi(n)$ (see point 1 in the preamble). So, $\phi(mn) = \phi(m)\phi(n)$ is a special case of Eq. 47.

6. Show the following:

$$\phi(m)\,\phi(n) = \phi(g)\,\phi(l) \qquad \big[m, n \in \mathbb{N},\ g = \gcd(m, n),\ l = \text{lcm}(m, n)\big]$$

Solution: On comparing Eqs. 46 and 47 we get:

$$g\,\phi(l) = \frac{g\,\phi(m)\,\phi(n)}{\phi(g)} \qquad \rightarrow \qquad \phi(l) = \frac{\phi(m)\,\phi(n)}{\phi(g)} \qquad \rightarrow \qquad \phi(m)\,\phi(n) = \phi(g)\,\phi(l)$$

7. Show that if $p \in \mathbb{P}$ and $n \in \mathbb{N}$ then either $\phi(pn) = (p-1)\,\phi(n)$ or $\phi(pn) = p\,\phi(n)$.
Solution: If p and n are coprime (i.e. p is not a factor of n) then from Eq. 47 we have:

$$\phi(pn) = \phi(p)\,\phi(n) = (p-1)\,\phi(n)$$

where we used property 2 in the last step (see the preamble).
If p and n are not coprime then from Eq. 47 we have (noting that $g = p$):

$$\phi(pn) = \frac{p\ \phi(p)\,\phi(n)}{\phi(p)} = p\ \phi(n)$$

8. Find $p, p_1, p_2 \in \mathbb{P}$ and $n \in \mathbb{N}$ in the following equations:
(**a**) $\phi(3^n) = 54$. (**b**) $\phi(p^3) = 294$. (**c**) $\phi(p^n) = 1210$.
(**d**) $\phi(pn) = \phi(n)$. (**e**) $\phi(p_1 n) = \phi(p_2 n)$. (**f**) $\phi(p_1 p_2) = 20$.
Solution:
(**a**) From Eq. 42 we have: $\phi(3^n) = 3^n - 3^{n-1} = 3^{n-1}(3-1) = 3^{n-1}2$. So, the given equation is equivalent to the equation $3^{n-1}2 = 54$ (i.e. $3^{n-1} = 27$) whose solution is $n = 4$, i.e. $\phi(81) = 54$.
(**b**) From Eq. 42 we have: $\phi(p^3) = p^3 - p^2 = p^2(p-1)$. So, the given equation is equivalent to the equation $p^2(p-1) = 294$. Now, if we prime-factorize 294 we get: $p^2(p-1) = 2 \times 3 \times 7^2 = 7^2(7-1)$. On comparing the two sides of the last equation we can see that $p = 7$, i.e. $\phi(343) = 294$.
(**c**) From Eq. 42 we have: $\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$. So, the given equation is equivalent to the equation $p^{n-1}(p-1) = 1210$. Now, if we prime-factorize 1210 we get: $p^{n-1}(p-1) = 2 \times 5 \times 11^2 = 11^2(11-1)$. On comparing the two sides of the last equation we can see that $p = 11$ and $n = 3$, i.e. $\phi(1331) = 1210$.
(**d**) From the result of Problem 7 we must have $p = 2$ and n is odd, e.g. $\phi(2 \times 9) = \phi(9)$.
(**e**) If $p_1 = p_2$ then this is an identity. So, we need only to consider $p_1 \neq p_2$. We have four cases (where we use the result of Problem 7 in the following analysis):
• If p_1 and n are coprime and p_2 and n are coprime then:

$$(p_1 - 1)\phi(n) = (p_2 - 1)\phi(n) \qquad \rightarrow \qquad p_1 - 1 = p_2 - 1$$

which is impossible since $p_1 \neq p_2$.
• If p_1 and n are not coprime and p_2 and n are not coprime then:

$$p_1\phi(n) = p_2\phi(n) \qquad \rightarrow \qquad p_1 = p_2$$

which is impossible since $p_1 \neq p_2$.
• If p_1 and n are coprime and p_2 and n are not coprime then:

$$(p_1 - 1)\phi(n) = p_2\phi(n) \qquad \rightarrow \qquad p_1 - 1 = p_2 \qquad \rightarrow \qquad p_1 = p_2 + 1$$

Now, the only consecutive primes are 2 and 3 and hence $p_1 = 3$ and $p_2 = 2$. But since p_1 and n are coprime then n is not a multiple of 3, and since p_2 and n are not coprime then n is even. So, we must

have: $p_1 = 3$, $p_2 = 2$ and n is an even number not divisible by 3, i.e. $n \in \mathbb{E}$ and $n \neq 6k$ ($k \in \mathbb{N}$).
• If p_1 and n are not coprime and p_2 and n are coprime then we just relabel p_1 and p_2 and get the same result as in the previous case.
So in brief, we must have $p_1 = 3$, $p_2 = 2$, $2|n$ and $3 \not| n$, e.g. $\phi(3 \times 8) = \phi(2 \times 8)$.
(**f**) If $p_1 = p_2 = p$ then from Eq. 42 we have: $\phi(p^2) = p^2 - p = 20$, i.e. $p^2 - p - 20 = (p+4)(p-5) = 0$ which has a solution $p = 5$ (since $p \in \mathbb{P}$). So, we have $\phi(5^2) = 20$.
If $p_1 \neq p_2$ then from Eq. 43 we have: $\phi(p_1 p_2) = (p_1 - 1)(p_2 - 1) = 20$. Now, if we consider the different factorizations[82] of 20 (i.e. $20 = 1 \times 20$ or $20 = 2 \times 10$ or $20 = 4 \times 5$) we can see that only $p_1 - 1 = 2$ and $p_2 - 1 = 10$ is acceptable, i.e. $p_1 = 3$ and $p_2 = 11$ (or the other way around). So, $\phi(3 \times 11) = 20$.

2.6.5 The Mobius Function

The Mobius function $\mu(n)$ is defined as follows:

$$\mu(n) = \begin{cases} 1 & (n = 1) \\ (-1)^k & (n \text{ is square free}) \\ 0 & (n \text{ is not square free}) \end{cases} \qquad (n, k \in \mathbb{N}) \tag{48}$$

where $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ in its standard prime factorization (noting that "square free" means none of $a_1, a_2, \ldots, a_k$ is greater than 1; see § 2.1). For example:

$$\mu(2) = -1 \qquad \mu(3) = -1 \qquad \mu(4) = 0 \qquad \mu(6) = 1$$

We list in the following points some common facts about the Mobius function:
1. The Mobius function is multiplicative, i.e. $\mu(mn) = \mu(m)\mu(n)$ where m and n are coprime.
2. If n is prime then $\mu(n) = -1$.
3. The Mobius function is many-to-one, i.e. $m = n \;\rightarrow\; \mu(m) = \mu(n)$ but $\mu(m) = \mu(n) \;\nrightarrow\; m = n$. For example, $\mu(n) = -1$ for all primes.
4. If we extend "prime factorization" to include 1 (see point 4 of § 2.1) then we can reduce Eq. 48 to two parts (i.e. square free and not square free) where $\mu(1) = 1$ is included in the square free case (i.e. with $k = 0$).

Problems

1. Prove (or justify) points 1 and 2 in the preamble.
   Solution:
   Point 1: we have five (comprehensive) cases:
   Case 1: $m = n = 1$ and hence we have:
   $$\mu(m)\mu(n) = \mu(1)\mu(1) = 1 \times 1 = 1 = \mu(1) = \mu(1 \times 1) = \mu(mn)$$
   Case 2: either $m = 1$ or $n = 1$ but not both (say $m = 1$ due to the arbitrariness of labeling). Accordingly we have:
   $$\mu(m)\mu(n) = \mu(1)\mu(n) = 1 \times \mu(n) = \mu(n) = \mu(1 \times n) = \mu(mn)$$
   Case 3: $m \neq 1$ and $n \neq 1$ and both m and n are square free. In this case it is obvious that mn is also square free (because m and n are coprime and hence they have no common prime factor) and the number of prime factors of mn is the sum of the number of prime factors of m and n (according to the rules of multiplication). Accordingly we have (noting that k_m, k_n are the number of prime factors of m, n respectively):
   $$\mu(m)\mu(n) = (-1)^{k_m}(-1)^{k_n} = (-1)^{k_m + k_n} = \mu(mn)$$
   Case 4: $m \neq 1$ and $n \neq 1$ and only one of m and n is not square free (say m is not square free). In this case it is obvious that mn is also not square free. Accordingly we have:
   $$\mu(m)\mu(n) = 0 \times (-1)^{k_n} = 0 = \mu(mn)$$

[82] Actually, we are considering only positive factorizations involving two factors only.

Case 5: $m \neq 1$ and $n \neq 1$ and both m and n are not square free. In this case it is obvious that mn is also not square free. Accordingly we have:

$$\mu(m)\mu(n) = 0 \times 0 = 0 = \mu(mn)$$

So, in all these five (comprehensive) cases we have $\mu(mn) = \mu(m)\mu(n)$ and hence the Mobius function is multiplicative.

Point 2: this is because any prime is square free with $k = 1$ and hence $\mu(p) = (-1)^1 = -1$.

2. Evaluate the Mobius function μ of the following integers: 3410, 63278621, 191052 and 16993.
Solution: Using Eq. 48 we get:

$$\begin{aligned}
\mu(3410) &= \mu(2 \times 5 \times 11 \times 31) = (-1)^4 = 1 \\
\mu(63278621) &= \mu(7 \times 37 \times 41 \times 59 \times 101) = (-1)^5 = -1 \\
\mu(191052) &= \mu(2^2 \times 3^3 \times 29 \times 61) = 0 \\
\mu(16993) &= \mu(16993) = (-1)^1 = -1 \qquad (16993 \in \mathbb{P})
\end{aligned}$$

3. Let n be an integer greater than 1 whose prime factorization is $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. Show the following:
(**a**) $\sum_{d|n} \mu(d) = 0$. (**b**) $\sum_{d|n} |\mu(d)| = 2^k$.
Solution:
(**a**) The divisors d of n are of two types: square free whose Mobius function is $(-1)^s$ where $s \in \mathbb{N}^0$,[83] and not square free whose Mobius function is 0. So, in the sum $\sum_{d|n} \mu(d)$ we need to consider only the square free divisors, that is:

$$\begin{aligned}
\sum_{d|n} \mu(d) &= \mu(1) + \left[\sum_{i=1,2,\ldots,k} \mu(p_i)\right] + \left[\sum_{1\leq i<j\leq k} \mu(p_i p_j)\right] + \cdots + \mu(p_1 p_2 \cdots p_k) \\
&= 1 + \left[\sum_{i=1,2,\ldots,k} (-1)\right] + \left[\sum_{1\leq i<j\leq k} \mu(p_i)\mu(p_j)\right] + \cdots + \mu(p_1)\mu(p_2)\cdots(p_k) \\
&= C_0^k(-1)^0 + C_1^k(-1)^1 + C_2^k(-1)^2 + \cdots + C_k^k(-1)^k \\
&= C_0^k(-1)^0\,1^k + C_1^k(-1)^1\,1^{k-1} + C_2^k(-1)^2\,1^{k-2} + \cdots + C_k^k(-1)^k\,1^0 \\
&= (1-1)^k \\
&= 0
\end{aligned}$$

where:
the **second line** is justified by: $\mu(1) = 1$ (see Eq. 48), $\mu(p_i) = -1$ (see point 2 in the preamble), and the multiplicativity of the Mobius function,
the **third line** is justified by the fact that the m^{th} term ($m = 0, 1, \ldots, k$) in the second line represents the number of combinations of m prime factors (in k prime factors) multiplied by $(-1)^m$,
the **fourth line** is justified by the neutrality of multiplication by 1 (raised to any integer power),
and the **fifth line** is justified by the identity of Eq. 13 (with $x = -1$ and $y = 1$).
(**b**) Taking the absolute value of $\mu(d)$ means replacing all the (-1) in the equations of part (a) with $+1$, and hence we have (starting from the third line of the equations of part a):

$$\begin{aligned}
\sum_{d|n} |\mu(d)| &= C_0^k(+1)^0 + C_1^k(+1)^1 + C_2^k(+1)^2 + \cdots + C_k^k(+1)^k \\
&= C_0^k + C_1^k + C_2^k + \cdots + C_k^k \\
&= \sum_{i=0}^{k} C_i^k \;=\; 2^k
\end{aligned}$$

where we used the identity of Eq. 21 in the last line.

[83] We are including $\mu(1) = 1$ in the "square free" case (see point 4 in the preamble).

2.7 Congruence and Modular Arithmetic

We say m and n are congruent modulo k (and write $m \overset{k}{=} n$) if k divides $(m-n)$.[84] In other words, m and n leave the same remainder when divided by k. Accordingly, the congruence relation $m \overset{k}{=} n$ is equivalent to:

$$m - n \overset{k}{=} 0 \qquad k|(m-n) \qquad m - n = sk \qquad m = sk + n \tag{49}$$

where $m, n, k, s \in \mathbb{Z}$ and $k > 1$. For example, the integers 19 and 4 are congruent modulo 5 (i.e. $19 \overset{5}{=} 4$) because 5 divides $(19-4) = 15$, and this can be expressed as:

$$19 - 4 \overset{5}{=} 0 \qquad 5|(19-4) \qquad 19 - 4 = 3 \times 5 \qquad 19 = (3 \times 5) + 4 \tag{50}$$

Similarly, the integers 12 and -2 are congruent modulo 7 (i.e. $12 \overset{7}{=} -2$) because 7 divides $(12-[-2]) = 14$, and this can be expressed as:

$$12 - [-2] \overset{7}{=} 0 \qquad 7|(12-[-2]) \qquad 12 - [-2] = 2 \times 7 \qquad 12 = (2 \times 7) + [-2] \tag{51}$$

Some of the rules and properties of congruence and modular arithmetic (which is based on the rules of congruence) are listed in the following points (noting that $m, n, k, s, t \in \mathbb{Z}$ and $k > 1$):

1. *Congruence* is an **equivalence relation**, i.e. it is **reflexive** ($m \overset{k}{=} m$), **symmetric** ($m \overset{k}{=} n \;\leftrightarrow\; n \overset{k}{=} m$) and **transitive** ($m \overset{k}{=} s$ and $s \overset{k}{=} n \;\rightarrow\; m \overset{k}{=} n$).
2. $m \overset{k}{=} n$ *iff* (m mod k) is *equal* to (n mod k).[85]
3. $m \overset{k}{=} n$ *iff* $m + s \overset{k}{=} n + s$.
4. If $m \overset{k}{=} n$ and $s \overset{k}{=} t$ then $m + s \overset{k}{=} n + t$.
5. If $m \overset{k}{=} n$ and $s \overset{k}{=} t$ then $m - s \overset{k}{=} n - t$.
6. If $m \overset{k}{=} n$ then $sm \overset{k}{=} sn$.
7. If $sm \overset{k}{=} sn$ and k and s are coprime then $m \overset{k}{=} n$.
8. If $g = \gcd(s, k)$ and $sm \overset{k}{=} sn$ then $m \overset{k/g}{=} n$.[86]
9. $m \overset{k}{=} n$ *iff* $sm \overset{sk}{=} sn$ ($s \in \mathbb{N}$).
10. If $m \overset{k}{=} n$ and $s \overset{k}{=} t$ then $ms \overset{k}{=} nt$.
11. If $m \overset{k}{=} n$ then $m^t \overset{k}{=} n^t$ ($t \in \mathbb{N}$).[87]
12. If $m \overset{\phi(k)}{=} n$, then $s^m \overset{k}{=} s^n$ (k and s are coprime).[88]
13. If $m \overset{k}{=} n$ then $P(m) \overset{k}{=} P(n)$ where P represents polynomial with integer coefficients.
14. If $m \overset{k_1}{=} n$, $m \overset{k_2}{=} n$, ..., $m \overset{k_s}{=} n$ then $m \overset{k}{=} n$ where $k = \text{lcm}(k_1, k_2, \ldots, k_s)$.
15. A congruence relation modulo k divides the set of integers to k residue classes[89] which are mutually exclusive and comprehensive (i.e. any integer belongs to one and only one of these k classes).

[84] To indicate the consideration of the modularity of n with respect to the modulo k (or the consideration of the modular arithmetic of n with respect to the modulo k) we write n (modulo k). So, the notations $n \overset{k}{=}$ and n (modulo k) are equivalent or similar where the former is used in congruence equations while the latter is used in textual presentations and explanatory comments and contexts. We should also note that we abbreviate "modulo" as "mod" and hence n (modulo k) is abbreviated as n (mod k).

[85] It is important to note that this "*equal*" is an "ordinary equal" not a "congruence equal".

[86] We note that rule 7 is a special case of this rule. We should also note that for $m \overset{k/g}{=} n$ to be sensible we should have $(k/g) > 1$.

[87] In fact, even $t = 0$ can be included (but this will annihilate m and n since we will have $1 \overset{k}{=} 1$ which is trivial).

[88] See Problem 3 of § 2.9.2.

[89] **Residue class** (or **congruence class**) is the set of integers that leave the same remainder when divided by a given modulo.

16. Negative numbers are generally not congruent to their positive counterparts. For example, $-7 \overset{5}{=} 3$ while $7 \overset{5}{=} 2$ and hence $-7 \overset{5}{\neq} 7$.
17. Although most of the rules and properties of ordinary arithmetic applies to modular arithmetic, we should be careful when dealing with modular arithmetic as mistakes can easily occur by treating congruence equations as ordinary equations (noting that the two types of equations are not entirely identical in their rules and properties; also see § 2.7.6).

Problems

1. Find all $k \in \mathbb{N}$ that satisfy the following congruence equations:

   (**a**) $62 \overset{k}{=} 54$. (**b**) $325 \overset{k}{=} 122$. (**c**) $3295 \overset{k}{=} 3256$.

   Solution: The numbers k that satisfy these equations are the positive divisors ($\mathbb{N} \ni k > 1$) of:
   (**a**) $62 - 54 = 8$ which are $2, 4, 8$.
   (**b**) $325 - 122 = 203$ which are $7, 29, 203$.
   (**c**) $3295 - 3256 = 39$ which are $3, 13, 39$.
2. Find all $n \in \mathbb{Z}$ that satisfy the following congruence equations:

   (**a**) $6n - 13 \overset{5}{=} 0$. (**b**) $14n^2 + 15n - 11 \overset{23}{=} 0$. (**c**) $13n^2 - 17n + 5 \overset{25}{=} 0$.

   Solution:
   (**a**) We have:

   $$\begin{aligned} 6n &\overset{5}{=} 13 && \text{(see rule 3 in the preamble of this section)} \\ 6n &\overset{5}{=} 3 && \text{(see the definition of congruence noting that } 13 = 2 \times 5 + 3) \\ n &\overset{5}{=} 3 && \text{(see the definition of congruence noting that } 6n = 5n + n) \end{aligned}$$

   So, the general solution of $6n - 13 \overset{5}{=} 0$ (i.e. all $n \in \mathbb{Z}$ that satisfy $6n - 13 \overset{5}{=} 0$) is $n = 3 + 5k$ where $k \in \mathbb{Z}$ (i.e. $n = \ldots - 7, -2, 3, 8 \ldots$).
   (**b**) We have $14n^2 + 15n - 11 = (2n - 1)(7n + 11)$ and hence we have $(2n - 1)(7n + 11) \overset{23}{=} 0$. Noting that $14n^2 + 15n - 11 \overset{23}{=} 0$ means the polynomial is divisible by 23, we conclude that since the polynomial is divisible by 23 (which is prime) then 23 must be a divisor of at least one factor of the polynomial (see rule 22 of § 1.9). Thus, all we need to do is to test if 23 divides any of the factors of the polynomial, i.e. if $2n - 1 \overset{23}{=} 0$ or $7n + 11 \overset{23}{=} 0$. So in brief, we need to find the solutions (if any) of $2n - 1 \overset{23}{=} 0$ and $7n + 11 \overset{23}{=} 0$.
   Regarding $2n - 1 \overset{23}{=} 0$, it is equivalent to $2n - 1 = 23k$ (see Eq. 49). Now, if (by inspection) we take $k = 1$ then we get $n = 12$ and hence the general solution of $2n - 1 \overset{23}{=} 0$ is $n = 12 + 23k$ ($k \in \mathbb{Z}$).
   Regarding $7n + 11 \overset{23}{=} 0$, it is equivalent to $7n + 11 = 23k$. Now, if (by inspection) we take $k = 2$ then we get $n = 5$ and hence the general solution of $7n + 11 \overset{23}{=} 0$ is $n = 5 + 23k$ ($k \in \mathbb{Z}$).
   Thus, the general solution of the given congruence equation is $n = m + 23k$ where $m = 5, 12$ and $k \in \mathbb{Z}$ (i.e. $n = \ldots, -18, -11, 5, 12, \ldots$).
   (**c**) The polynomial in this congruence equation does not factorize and hence we cannot use the method of part (b). The easiest way to solve this problem (noting that modulo 25 is relatively small) is to test all the possibilities (representing the residue classes) of n (mod 25) by substituting $n = 0, 1, \ldots, 24$ in the congruence equation to find which value of n satisfies the congruence equation (i.e. makes the polynomial divisible by 25). This can be easily done using, for instance, a spreadsheet or a simple computer code. On testing these possibilities we find that only $n \overset{25}{=} 15$ and $n \overset{25}{=} 19$ satisfy this congruence equation. Hence, the general solution of the given congruence equation is $n = m + 25k$ where $m = 15, 19$ and $k \in \mathbb{Z}$ (i.e. $n = \ldots, -10, -6, 15, 19, \ldots$).
3. Explain why the following congruence equations have no solution in $n \in \mathbb{Z}$.

(**a**) $32n^2+12n-3 \overset{k}{=} 0$ (k even). (**b**) $5n^3-13n+81 \overset{7}{=} 0$.

(**c**) $15n^5-5n^4+3n^3-n^2-12n+4 \overset{759}{=} 0$. (**d**) $10n-17 \overset{5}{=} 0$.

Solution:

(**a**) $(32n^2+12n-3)$ is odd regardless of the parity of n and hence it cannot have an even divisor (see the rules of parity in § 1.8) noting that $32n^2+12n-3 \overset{k}{=} 0$ is equivalent to $k|(32n^2+12n-3)$.

(**b**) By the rules of congruence (see the preamble of this section) the congruence equation $5n^3-13n+81 \overset{7}{=} 0$ is equivalent to $5n^3+n+4 \overset{7}{=} 0$ which means:

$$5\big[n \pmod 7\big]^3+\big[n \pmod 7\big]+4 \overset{7}{=} 0$$

So, all we need to do is to test all the possibilities (representing the residue classes) of $n \pmod 7$ by substituting $n=0,1,2,3,4,5,6$ in the last congruence equation to find if we can get 0 (mod 7). On substituting $n=0,1,2,3,4,5,6$ in the last congruence equation we get (respectively) $4,3,4,2,6,4,5$. This means that there is no n that can make this congruence equation true.

(**c**) We cannot use the method of part (a) because the polynomial is even and hence it can be divisible by an odd number. Also, it is not very practical (or rather it is lengthy) to use the method of part (b) because the modulo 759 is very big (and hence we have 759 possibilities to test). So, in this type of problems it is better to use another method and that is what we will do here.

Now, if we factorize the polynomial and prime-factorize the modulo then we get:

$$15n^5-5n^4+3n^3-n^2-12n+4=(3n-1)(5n^2-4)(n^2+1) \qquad 759=3\times 11\times 23$$

So, if the polynomial is divisible by 759 (as implied by the congruence equation) then (by rule 20 of § 1.9) the polynomial should be divisible by each prime factor of 759 (i.e. $3,11,23$). This implies (see rule 22 of § 1.9) that each factor of 759 (i.e. $3,11,23$) is a divisor of at least one factor of the polynomial. So, if 3 (or 11 or 23) can divide none of the polynomial factors then the polynomial is not divisible by 759. Thus, all we need to do is to test if any one of the factors $3,11,23$ fails to divide any of the factors of the polynomial. Starting with 3 (which is the smallest factor and hence the easiest to test) we get:

$$3n-1 \overset{3}{\neq} 0 \qquad 5n^2-4 \overset{3}{\neq} 0 \qquad n^2+1 \overset{3}{\neq} 0 \qquad (n\in\mathbb{Z})$$

i.e. 3 can divide none of the polynomial factors for any $n\in\mathbb{Z}$. This should be enough (i.e. we do not need to test the factors 11 and 23) to explain and justify why the given congruence equation has no solution in $n\in\mathbb{Z}$.

(**d**) We have $10n \overset{5}{=} 17$ (see rule 3 in the preamble). Now, $10n \overset{5}{=} 0$ (since $10n=5\times 2n$ which is a multiple of the modulo 5), while $17 \overset{5}{=} 2$ (since $17=5\times 3+2$ which is a multiple of the modulo 5 plus 2). So, this congruence equation implies $0 \overset{5}{=} 2$ (i.e. $0=2$ in mod 5) which is impossible (see point 2 in the preamble), and hence this congruence equation has no solution in $n\in\mathbb{Z}$.

4. Is it true that (where $m,n,k,s\in\mathbb{N}$ and $k>1$):

(**a**) If $m^s \overset{k}{=} n^s$ then $m \overset{k}{=} n$. (**b**) If $m \overset{k}{=} n$ then $s^m \overset{k}{=} s^n$.

Solution: We use the method of proof by counterexample (see § 1.5.4).

(**a**) It is not true in general. For example, $3^2 \overset{10}{=} 7^2$ but $3 \overset{10}{\neq} 7$.

(**b**) It is not true in general. For example, $8 \overset{5}{=} 3$ but $2^8 \overset{5}{\neq} 2^3$.

5. Prove (or justify) the following:

(**a**) If $m,n,s\in\mathbb{Z}$, $\mathbb{N}\ni k>1$, $g=\gcd(s,k)$ and $sm \overset{k}{=} sn$ then $m \overset{k/g}{=} n$.[90]

(**b**) If $sm \overset{k}{=} sn$ and k and s are coprime then $m \overset{k}{=} n$.

[90] It is worth noting that for $m \overset{k/g}{=} n$ to be sensible we should have $(k/g)>1$.

(**c**) All odd primes are congruent either to 1 or to 3 (mod 4).
(**d**) For any $n \in \mathbb{Z}$, either $n^2 \overset{3}{=} 0$ or $n^2 \overset{3}{=} 1$ (i.e. $n^2 \overset{3}{\neq} 2$).
(**e**) For $p \in \mathbb{P}$, $C_k^{p-1} \overset{p}{=} (-1)^k$.
(**f**) $n^2 \overset{8}{=} 1$ where n is odd.
(**g**) $(mn)^2 - 1 \overset{8}{=} m^2 + n^2 - 2$ where m and n are odd.
(**h**) $m \overset{nk}{=} r$ *iff* $m \overset{n}{=} r$ and $m \overset{k}{=} r$ ($m, r \in \mathbb{Z}$, $\mathbb{N} \ni n, k > 1$, n and k are coprime).
(**i**) $2^{2^n} + 3 \overset{7}{=} 5$ for even n and $2^{2^n} + 3 \overset{7}{=} 0$ for odd n (where $n \in \mathbb{N}^0$).
(**j**) Rule 13 (in the preamble of this section).
Solution:
(**a**) $sm \overset{k}{=} sn$ implies:

$$k|(sm - sn) \qquad \rightarrow \qquad k|s(m-n) \qquad \rightarrow \qquad s(m-n) = tk$$

where $t \in \mathbb{Z}$. Now, if we divide both sides of the last equation by g we get $(s/g)(m-n) = t(k/g)$. Because $\gcd(s/g, k/g) = 1$ (see point 9 of § 2.4), then (k/g) must be a divisor of $m - n$ (see rule 21 of § 1.9) and hence $m \overset{k/g}{=} n$ (see Eq. 49).
(**b**) This is a corollary of part (a) because if k and s are coprime then $g = 1$.
(**c**) This was shown in Problem 16 of § 2.2. In brief, an odd prime cannot be congruent (mod 4) to 0 (because it is prime and hence it cannot be divisible by 4) and cannot be congruent (mod 4) to 2 (because it is odd), and hence it must be congruent either to 1 or to 3 (mod 4).
(**d**) We have 3 cases for n to consider (where $k \in \mathbb{Z}$):
• $n = 3k$ which leads to $n^2 = 9k^2$ and hence $n^2 \overset{3}{=} 0$.
• $n = 3k + 1$ which leads to $n^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$ and hence $n^2 \overset{3}{=} 1$.
• $n = 3k + 2$ which leads to $n^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$ and hence $n^2 \overset{3}{=} 1$.
As we see, we have only $n^2 \overset{3}{=} 0$ and $n^2 \overset{3}{=} 1$ and hence $n^2 \overset{3}{\neq} 2$ for any $n \in \mathbb{Z}$.
(**e**) We have:

$$\begin{aligned}
&k!\, C_k^{p-1} = (p-1) \times (p-2) \times \cdots \times (p-1-k+1) && \text{(Eq. 5)}\\
&k!\, C_k^{p-1} \overset{p}{=} (-1) \times (-2) \times \cdots \times (-k) && \text{(definition of congruence)}\\
&k!\, C_k^{p-1} \overset{p}{=} (-1)^k k! &&\\
&\quad C_k^{p-1} \overset{p}{=} (-1)^k && \text{(rule 7 in preamble)}
\end{aligned}$$

We note that p and $k!$ are coprime because $p > k$ (since $k \leq p - 1$) and hence p cannot be a factor of $k!$ (see rule 47 of § 1.9).
(**f**) Since n is odd it can be written as $2k + 1$ where $k \in \mathbb{Z}$. Hence:

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$$

Now, whether k is even or odd $(k^2 + k)$ is even (see rules 4 and 6 of § 1.8) and hence $(k^2 + k) = 2m$ for some $m \in \mathbb{Z}$. Hence, $n^2 = 8m + 1$ which is equivalent to $n^2 \overset{8}{=} 1$.
(**g**) If we note that m, n and mn are odd (see rule 6 of § 1.8) then from the result of part (f) we have:

$$(mn)^2 - 1 \overset{8}{=} 1 - 1 = 0 \qquad \text{and} \qquad m^2 + n^2 - 2 \overset{8}{=} 1 + 1 - 2 = 0$$

So, both sides of the given congruence relation are 0 and hence the congruence relation is true (see rule 2 in the preamble).
(**h**) **The if part**: if $m \overset{n}{=} r$ and $m \overset{k}{=} r$ then $m - r = sn$ and $m - r = tk$ ($s, t \in \mathbb{Z}$) and hence $sn = tk$. This means that $k|(sn)$. However, because n and k are coprime then $k|s$ (see rule 21 of § 1.9), i.e. $s = ak$ for some $a \in \mathbb{Z}$. Therefore, $m - r = akn$ which means $m \overset{nk}{=} r$ (as required).

The only if part: if $m \overset{nk}{=} r$ then $m - r = ank$ for some $a \in \mathbb{Z}$. This means that $n|(m-r)$ and $k|(m-r)$ which are equivalent to $m \overset{n}{=} r$ and $m \overset{k}{=} r$ (as required).
(**i**) We prove this by induction.
If n is even then $n = 2k$ ($k \in \mathbb{N}^0$). For $k = 0$ we have $2^{2^0} + 3 = 5 \overset{7}{=} 5$. Now, let assume that $2^{2^{2k}} + 3 \overset{7}{=} 5$ for a given k and hence $2^{2^{2k}} \overset{7}{=} 2$ (see point 3 in the preamble). We will show that this assumption will lead to $2^{2^{2(k+1)}} + 3 = 2^{2^{2k+2}} + 3 \overset{7}{=} 5$, that is:

$$2^{2^{2k+2}} + 3 = 2^{2^{2k} \times 2^2} + 3 = 2^{2^{2k} \times 4} + 3 = \left(2^{2^{2k}}\right)^4 + 3 \overset{7}{=} 2^4 + 3 = 19 \overset{7}{=} 5$$

where we used in step 4 the relation $2^{2^{2k}} \overset{7}{=} 2$ (which we obtained above based on our assumption that $2^{2^{2k}} + 3 \overset{7}{=} 5$). So, by mathematical induction $2^{2^n} + 3 \overset{7}{=} 5$ for all even $n \in \mathbb{N}^0$.
If n is odd then $n = 2k + 1$ ($k \in \mathbb{N}^0$). For $k = 0$ we have $2^{2^1} + 3 = 7 \overset{7}{=} 0$. Now, let assume that $2^{2^{2k+1}} + 3 \overset{7}{=} 0$ for a given k and hence $2^{2^{2k+1}} \overset{7}{=} 4$ (see point 3 in the preamble). We will show that this assumption will lead to $2^{2^{2(k+1)+1}} + 3 = 2^{2^{2k+3}} + 3 \overset{7}{=} 0$, that is:

$$2^{2^{2k+3}} + 3 = 2^{2^{2k+1} \times 2^2} + 3 = 2^{2^{2k+1} \times 4} + 3 = \left(2^{2^{2k+1}}\right)^4 + 3 \overset{7}{=} 4^4 + 3 = 259 \overset{7}{=} 0$$

where we used in step 4 the relation $2^{2^{2k+1}} \overset{7}{=} 4$ (which we obtained above based on our assumption that $2^{2^{2k+1}} + 3 \overset{7}{=} 0$). So, by mathematical induction $2^{2^n} + 3 \overset{7}{=} 0$ for all odd $n \in \mathbb{N}^0$.
(**j**) This is just a combination of property 11, property 6 and property 4.

6. Find the remainder when:

(**a**) $\sum_{k=1}^{100} k!$ is divided by 6!. (**b**) $5^{5^{5^5}}$ is divided by 9. (**c**) 19^{97207} is divided by 6.
(**d**) $129^{362} + 62^{22}$ is divided by 10. (**e**) 7^{921} is divided by 100. (**f**) 3450^{689} is divided by 13.

Solution:
(**a**) We note that $\sum_{k=6}^{100} k!$ is divisible by 6! since each term contains a factor of 6!. So, we only need to consider $\left(\sum_{k=1}^{5} k!\right)$, that is:

$$\left(\sum_{k=1}^{5} k!\right) = 153 \overset{6!}{=} 153 \overset{720}{=} 153$$

So the remainder is 153.
(**b**) We use rule 12 (see the preamble of this section) noting that $\phi(9) = 6$ and $\phi(6) = 2$:

$$\begin{array}{rcll} 5^{5^5} & \overset{\phi(9)}{=} & c_1 & \rightarrow \quad 5^{5^{5^5}} \overset{9}{=} 5^{c_1} \\ 5^5 & \overset{\phi(6)}{=} & c_2 & \rightarrow \quad 5^{5^5} \overset{6}{=} 5^{c_2} \\ 5 & \overset{\phi(2)}{=} & c_3 & \rightarrow \quad 5^5 \overset{2}{=} 1 \qquad (5^5 \text{ is odd}) \end{array}$$

Now, if we work backwards starting from the last equation then we have:

$$\begin{array}{rcll} 5^5 & \overset{\phi(6)}{=} & 1 & \rightarrow \quad 5^{5^5} \overset{6}{=} 5^1 \overset{6}{=} 5 \\ 5^{5^5} & \overset{\phi(9)}{=} & 5 & \rightarrow \quad 5^{5^{5^5}} \overset{9}{=} 5^5 \overset{9}{=} 2 \end{array}$$

So the remainder is 2.
(**c**) We have:

$$\begin{array}{l} 19 \overset{6}{=} 1 \\ 19^{97207} \overset{6}{=} 1^{97207} \qquad \text{(rule 11)} \end{array}$$

$$19^{97207} \overset{6}{=} 1$$

So the remainder is 1.
(**d**) We have $129 \overset{10}{=} -1$ and $62 \overset{10}{=} 2$. Hence, by rule 11 we get:

$$129^{362} \overset{10}{=} (-1)^{362} = 1 \qquad \text{and} \qquad 62^{22} \overset{10}{=} 2^{22} = 4194304 \overset{10}{=} 4$$

So, by rule 4 we get $129^{362} + 62^{22} \overset{10}{=} 1 + 4 = 5$, i.e. the remainder is 5.
(**e**) We have $7^4 = 2401$. Hence:

$$\begin{aligned} 7^4 &\overset{100}{=} 1 && \\ \left(7^4\right)^{230} &\overset{100}{=} 1^{230} && \text{(rule 11)} \\ 7 \times \left(7^4\right)^{230} &\overset{100}{=} 7 \times 1^{230} && \text{(rule 6)} \\ 7^{921} &\overset{100}{=} 7 && \text{(rules of indices)} \end{aligned}$$

So the remainder is 7.
(**f**) We have:

$$\begin{aligned} 3450 &\overset{13}{=} 5 && \\ 3450^{689} &\overset{13}{=} 5^{689} && \text{(rule 11)} \\ 3450^{689} &\overset{13}{=} 5 \times \left(5^4\right)^{172} && \text{(rules of indices)} \\ 3450^{689} &\overset{13}{=} 5 \times (1)^{172} && (5^4 \overset{13}{=} 1) \\ 3450^{689} &\overset{13}{=} 5 && \end{aligned}$$

So the remainder is 5.

7. Find the periodic pattern of the following (where $n \in \mathbb{N}$):
(**a**) n^n modulo 2. (**b**) n^n modulo 3. (**c**) n^n modulo 4.

Solution:
(**a**) If n is odd then n^n is odd and hence $n^n \overset{2}{=} 1$ while if n is even then n^n is even and hence $n^n \overset{2}{=} 0$. So, we have a periodic pattern of $1, 0$ (starting from 1).
(**b**) We have three cases:
• $n \overset{3}{=} 0$ and hence $n^n \overset{3}{=} 0^n = 0$ (see rule 11).
• $n \overset{3}{=} 1$ and hence $n^n \overset{3}{=} 1^n = 1$.
• $n \overset{3}{=} 2$ and hence $n^n \overset{3}{=} 2^n$. Now, if n is odd then $n^n \overset{3}{=} 2^{2k+1} = 2^{2k} \times 2 = 4^k \times 2 \overset{3}{=} 1^k \times 2 = 2$, while if n is even then $n^n \overset{3}{=} 2^{2k} = 4^k \overset{3}{=} 1^k = 1$. If we note that consecutive multiples of 3 alternate in parity (and hence n in the case of $n \overset{3}{=} 2$ alternate in parity) then we can conclude that we have a periodic pattern with a period of 6, i.e. $0, 1, 2, 0, 1, 1$. If we identify the first periodic block of 6 (i.e. corresponding to $n = 1, 2, 3, 4, 5, 6$) we find that the pattern is $1, 1, 0, 1, 2, 0$. So, this pattern repeats itself every 6 consecutive natural numbers (starting from 1).
(**c**) We have four cases:
• $n \overset{4}{=} 0$ and hence $n^n \overset{4}{=} 0^n = 0$ (see rule 11).
• $n \overset{4}{=} 1$ and hence $n^n \overset{4}{=} 1^n = 1$.
• $n \overset{4}{=} 2$ and hence $n^n \overset{4}{=} 2^n$. Now, since $n \overset{4}{=} 2$ then n must be even (since it is a multiple of 4 plus 2) and hence $n^n \overset{4}{=} 2^n = 2^{2k} = 4^k \overset{4}{=} 0$ ($k \in \mathbb{N}$).
• $n \overset{4}{=} 3 \overset{4}{=} -1$ and hence $n^n \overset{4}{=} 3^n \overset{4}{=} (-1)^n$. Now, since $n \overset{4}{=} 3$ then n must be odd (since it is a multiple of 4 plus 3) and hence $n^n \overset{4}{=} (-1)^n = -1 \overset{4}{=} 3$.

Now, if we identify the first periodic block of 4 (i.e. corresponding to $n = 1, 2, 3, 4$) we find that the pattern is $1, 0, 3, 0$. So, this pattern repeats itself every 4 consecutive natural numbers (starting from 1).

8. Find all $n \in \mathbb{N}$ such that n, $n+16$ and $n+20$ are all primes.
Solution: n is prime and hence it must be > 1. Also, if $n = 2$ then neither $n+16$ nor $n+20$ is prime because they are even greater than 2 (see point 3 of § 2.2). However, $n = 3$ is acceptable since $3, 19, 23$ are all primes. So, let see if we have other triples like this.
If n is prime > 3 then it is not divisible by 3 (since 3 is the only prime divisible by 3) and hence $n \overset{3}{=} 1$ or $n \overset{3}{=} 2$. However, if $n \overset{3}{=} 1$ then $n + 20 \overset{3}{=} 1 + 2 = 3 \overset{3}{=} 0$ (i.e. $n + 20$ is divisible by 3 and hence it is not prime), while if $n \overset{3}{=} 2$ then $n + 16 \overset{3}{=} 2 + 1 = 3 \overset{3}{=} 0$ (i.e. $n + 16$ is divisible by 3 and hence it is not prime). So, n, $n + 16$ and $n + 20$ are all primes only for $n = 3$.
9. Show the following:
(**a**) $3p^2 - 1$ is composite except for $p = 2$ ($p \in \mathbb{P}$).
(**b**) $2p^2 + 1$ is composite except for $p = 3$ ($p \in \mathbb{P}$).
(**c**) If p and $2p + 1$ are primes then $4p + 1$ is composite except for $p = 3$.
(**d**) $2^n - 1$ and $2^n + 1$ are primes only if $n = 2$ ($n \in \mathbb{N}$, $n > 1$).
Solution:
(**a**) Since p is prime and $p \neq 2$ then it is odd and hence $3p^2 - 1$ is even (see the parity rules in § 1.8). Thus, $3p^2 - 1$ is composite noting that $(3p^2 - 1) > 2$. What distinguishes 2 is that it is the only even prime number (and hence the above argument does not apply and thus $3p^2 - 1 = 11$ is odd and prime in this case).
(**b**) Since p is prime and $p \neq 3$ then it is not divisible by 3. Hence, either $p \overset{3}{=} 1$ or $p \overset{3}{=} 2$.
Now, if $p \overset{3}{=} 1$ then $p^2 \overset{3}{=} 1$ (by rule 11) and $2p^2 \overset{3}{=} 2$ (by rule 6) and thus $2p^2 + 1 \overset{3}{=} 3 \overset{3}{=} 0$ (by rule 3), i.e. $2p^2 + 1$ is divisible by 3 and hence it is composite (noting that it is > 3).
Similarly, if $p \overset{3}{=} 2$ then $p^2 \overset{3}{=} 4 \overset{3}{=} 1$ (by rule 11) and $2p^2 \overset{3}{=} 2$ (by rule 6) and thus $2p^2 + 1 \overset{3}{=} 3 \overset{3}{=} 0$ (by rule 3), i.e. $2p^2 + 1$ is divisible by 3 and hence it is composite (noting that it is > 3).
So, in both cases $2p^2 + 1$ is composite. What distinguishes 3 is that it is the only prime number divisible by 3 (and hence the above argument does not apply and thus $2p^2 + 1 = 19$ is prime in this case).
(**c**) Since p is prime and $p \neq 3$ then it is not divisible by 3. Hence, either $p \overset{3}{=} 1$ or $p \overset{3}{=} 2$.
Similarly, since $2p + 1$ is prime then it is not divisible by 3 (noting that it is > 3). Hence, either $2p + 1 \overset{3}{=} 1$ (and hence $p \overset{3}{=} 0$ which is impossible since $p \overset{3}{=} 1$ or $p \overset{3}{=} 2$) or $2p + 1 \overset{3}{=} 2$ (and hence $p \overset{3}{=} 2$ which is acceptable). So, we must have $p \overset{3}{=} 2$ and $2p + 1 \overset{3}{=} 2$ and hence:

$$4p + 1 = 2p + (2p + 1) \overset{3}{=} 2(2) + 2 = 6 \overset{3}{=} 0$$

i.e. $4p + 1$ is divisible by 3 and hence it is composite (noting that it is > 3).
As before, 3 is excluded because it is the only prime number divisible by 3 (and hence the above argument does not apply because $p \overset{3}{=} 0$ in this case).
(**d**) If $(2^n - 1)$ is prime and $n \neq 2$ then it is not divisible by 3 (noting that it is > 3 since $n > 2$), and hence either $2^n - 1 \overset{3}{=} 1$ or $2^n - 1 \overset{3}{=} 2$. However, $2^n - 1 \overset{3}{=} 1$ leads (by adding 2 to both sides) to $2^n + 1 \overset{3}{=} 0$, i.e. $2^n + 1$ is composite since it is divisible by 3. Also, $2^n - 1 \overset{3}{=} 2$ leads (by adding 1 to both sides) to $2^n \overset{3}{=} 0$ which is impossible because 2^n has no factor of 3 and hence it cannot be divisible by 3. So, both cases are impossible. Yes, if $n = 2$ then $2^n - 1 \overset{3}{=} 0$ and $2^n + 1 \overset{3}{=} 2$ which is consistent with both being primes (noting that $2^2 - 1 = 3$ and $2^2 + 1 = 5$) since the aforementioned argument does not apply. The culprit of this is that 3 is the only prime number divisible by 3. Also see Problem 2 of § 2.2.3.
10. Find all $m, n \in \mathbb{Z}$ such that $m^4 \overset{5}{=} n^7$.
Solution: The easiest and fastest way to solve this type of problems is to use tables (with help of a spreadsheet or a simple computer code), and this is what we do in the following.

We have $m^4 \overset{5}{=} \big[m \pmod 5\big]^4$ and $n^7 \overset{5}{=} \big[n \pmod 5\big]^7$ (see rules 2 and 11 in the preamble). So, if we consider all the combinations of the 5 possibilities of $m \pmod 5$ with the 5 possibilities of $n \pmod 5$ then we have the following table:

	$\boldsymbol{n \overset{5}{=} 0}$	$\boldsymbol{n \overset{5}{=} 1}$	$\boldsymbol{n \overset{5}{=} 2}$	$\boldsymbol{n \overset{5}{=} 3}$	$\boldsymbol{n \overset{5}{=} 4}$
$\boldsymbol{m \overset{5}{=} 0}$	$0^4 \overset{5}{=} 0,\ 0^7 \overset{5}{=} 0$	$0^4 \overset{5}{=} 0,\ 1^7 \overset{5}{=} 1$	$0^4 \overset{5}{=} 0,\ 2^7 \overset{5}{=} 3$	$0^4 \overset{5}{=} 0,\ 3^7 \overset{5}{=} 2$	$0^4 \overset{5}{=} 0,\ 4^7 \overset{5}{=} 4$
$\boldsymbol{m \overset{5}{=} 1}$	$1^4 \overset{5}{=} 1,\ 0^7 \overset{5}{=} 0$	$1^4 \overset{5}{=} 1,\ 1^7 \overset{5}{=} 1$	$1^4 \overset{5}{=} 1,\ 2^7 \overset{5}{=} 3$	$1^4 \overset{5}{=} 1,\ 3^7 \overset{5}{=} 2$	$1^4 \overset{5}{=} 1,\ 4^7 \overset{5}{=} 4$
$\boldsymbol{m \overset{5}{=} 2}$	$2^4 \overset{5}{=} 1,\ 0^7 \overset{5}{=} 0$	$2^4 \overset{5}{=} 1,\ 1^7 \overset{5}{=} 1$	$2^4 \overset{5}{=} 1,\ 2^7 \overset{5}{=} 3$	$2^4 \overset{5}{=} 1,\ 3^7 \overset{5}{=} 2$	$2^4 \overset{5}{=} 1,\ 4^7 \overset{5}{=} 4$
$\boldsymbol{m \overset{5}{=} 3}$	$3^4 \overset{5}{=} 1,\ 0^7 \overset{5}{=} 0$	$3^4 \overset{5}{=} 1,\ 1^7 \overset{5}{=} 1$	$3^4 \overset{5}{=} 1,\ 2^7 \overset{5}{=} 3$	$3^4 \overset{5}{=} 1,\ 3^7 \overset{5}{=} 2$	$3^4 \overset{5}{=} 1,\ 4^7 \overset{5}{=} 4$
$\boldsymbol{m \overset{5}{=} 4}$	$4^4 \overset{5}{=} 1,\ 0^7 \overset{5}{=} 0$	$4^4 \overset{5}{=} 1,\ 1^7 \overset{5}{=} 1$	$4^4 \overset{5}{=} 1,\ 2^7 \overset{5}{=} 3$	$4^4 \overset{5}{=} 1,\ 3^7 \overset{5}{=} 2$	$4^4 \overset{5}{=} 1,\ 4^7 \overset{5}{=} 4$

As we see, $m^4 \overset{5}{=} n^7$ only in the following five cases:

$m \overset{5}{=} 0$ & $n \overset{5}{=} 0$ $\qquad$ $m \overset{5}{=} 1$ & $n \overset{5}{=} 1$ $\qquad$ $m \overset{5}{=} 2$ & $n \overset{5}{=} 1$ $\qquad$ $m \overset{5}{=} 3$ & $n \overset{5}{=} 1$ $\qquad$ $m \overset{5}{=} 4$ & $n \overset{5}{=} 1$

So, all $m, n \in \mathbb{Z}$ that satisfy the congruence $m^4 \overset{5}{=} n^7$ are given by: $(m, n) = (5k, 5q)$, $(1 + 5k, 1 + 5q)$, $(2 + 5k, 1 + 5q)$, $(3 + 5k, 1 + 5q)$, $(4 + 5k, 1 + 5q)$ where $k, q \in \mathbb{Z}$.

Note: we could have used $m^4 - n^7 \overset{5}{=} 0$ (which is equivalent to $m^4 \overset{5}{=} n^7$) in our analysis and table and hence we would have simpler (or less messy) table and solution (since we do not need to deal with m^4 and n^7 separately). However, we preferred this "messy" way because it better demonstrates the rules and logic which the solution is based on.

11. Show that $m^4 + n^4 \overset{13}{=} 0$ *iff* $m \overset{13}{=} 0$ and $n \overset{13}{=} 0$.
Solution: The easiest and fastest way to solve this type of problems is to use tables (as we did in Problem 10), and this is what we do in the following.[91] As we see, 0 occurs only once in the table corresponding to $m \overset{3}{=} 0$ and $n \overset{13}{=} 0$ and hence we can conclude that $m^4 + n^4 \overset{13}{=} 0$ *iff* $m \overset{3}{=} 0$ and $n \overset{13}{=} 0$.

		$\boldsymbol{n}$ **mod(13)**												
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
$\boldsymbol{m}$ **mod(13)**	**0**	0	1	3	3	9	1	9	9	1	9	3	3	1
	1	1	2	4	4	10	2	10	10	2	10	4	4	2
	2	3	4	6	6	12	4	12	12	4	12	6	6	4
	3	3	4	6	6	12	4	12	12	4	12	6	6	4
	4	9	10	12	12	5	10	5	5	10	5	12	12	10
	5	1	2	4	4	10	2	10	10	2	10	4	4	2
	6	9	10	12	12	5	10	5	5	10	5	12	12	10
	7	9	10	12	12	5	10	5	5	10	5	12	12	10
	8	1	2	4	4	10	2	10	10	2	10	4	4	2
	9	9	10	12	12	5	10	5	5	10	5	12	12	10
	10	3	4	6	6	12	4	12	12	4	12	6	6	4
	11	3	4	6	6	12	4	12	12	4	12	6	6	4
	12	1	2	4	4	10	2	10	10	2	10	4	4	2

12. Show that $m^4 + n^4 \overset{13}{\neq} 7, 8, 11$.
Solution: This type of problems can also be solved easily by tables. Referring to the table of Problem 11 we can see there is no 7 or 8 or 11 entry in the table and hence we can conclude that $m^4 + n^4 \overset{13}{\neq} 7, 8, 11$.
13. Show that $7^m \overset{4}{=} 1$ when m is even and $7^m \overset{4}{=} 3$ when m is odd ($m \in \mathbb{N}^0$).
Solution: We have (where $k \in \mathbb{N}^0$):

$$7^{2k} \overset{4}{=} (7^2)^k \qquad \text{(rules of indices)}$$

[91] In fact, we need to build only half the table because of the symmetry, as seen in the table. It should be obvious that the (non-emboldened) entries in this table represent $m^4 + n^4$ (mod 13) corresponding to m (mod 13) rows (emboldened) and to n (mod 13) columns (emboldened). For more clarity, the reader is referred to the table of Problem 10 which is similar to the table of this Problem (but its structure shows more details).

$$7^{2k} \overset{4}{=} 1^k \qquad (7^2 = 49 \overset{4}{=} 1)$$
$$7^{2k} \overset{4}{=} 1$$

i.e. $7^m \overset{4}{=} 1$ when m is even (i.e. $m = 2k$). Similarly:

$$7^{2k+1} \overset{4}{=} (7^2)^k \times 7 \qquad \text{(rules of indices)}$$
$$7^{2k+1} \overset{4}{=} 1^k \times 7 \qquad (7^2 = 49 \overset{4}{=} 1)$$
$$7^{2k+1} \overset{4}{=} 7$$
$$7^{2k+1} \overset{4}{=} 3 \qquad (7 \overset{4}{=} 3)$$

i.e. $7^m \overset{4}{=} 3$ when m is odd (i.e. $m = 2k + 1$).

Note: we can solve this Problem more simply by noting that $7 \overset{4}{=} -1$ and hence $7^m \overset{4}{=} (-1)^m$ which leads to $7^m \overset{4}{=} 1$ when m is even and to $7^m \overset{4}{=} -1 \overset{4}{=} 3$ when m is odd.

14. Show that for all $\mathbb{N} \ni n > 1$ the numbers 6^n end in $36, 16, 96, 76, 56$.

Solution: We have: $76^k \overset{100}{=} 76$ for all $k \in \mathbb{N}$. This can be proved by induction (as follows). $76^k \overset{100}{=} 76$ is obviously true for $k = 1$. So, let assume it is true for a given $k \in \mathbb{N}$ (i.e. $76^k \overset{100}{=} 76$) and hence:

$$76^{k+1} = 76^k \times 76 \overset{100}{=} 76 \times 76 = 5776 \overset{100}{=} 76$$

where step 2 is justified by our assumption. So, $76^k \overset{100}{=} 76$ for all $k \in \mathbb{N}$.
Now:

$$6^5 \overset{100}{=} 76 \qquad (6^5 = 7776)$$
$$6^{5k} \overset{100}{=} 76^k \qquad (k \in \mathbb{N}, \text{ see rule 11 in the preamble})$$
$$6^{5k} \overset{100}{=} 76 \qquad (76^k \overset{100}{=} 76 \text{ for all } k \in \mathbb{N})$$

Now, for $n = 2, 3, 4, 5, 6$ we have: $6^2 \overset{100}{=} 36$, $6^3 \overset{100}{=} 16$, $6^4 \overset{100}{=} 96$, $6^5 \overset{100}{=} 76$, $6^6 \overset{100}{=} 56$. Moreover, for $n \overset{5}{=} 2, 3, 4, 5, 6$ $(n > 6)$ we have:

$$\begin{aligned}
6^{5k+2} &= 6^{5k} \times 6^2 \overset{100}{=} 76 \times 36 = 2736 \overset{100}{=} 36 \\
6^{5k+3} &= 6^{5k} \times 6^3 \overset{100}{=} 76 \times 16 = 1216 \overset{100}{=} 16 \\
6^{5k+4} &= 6^{5k} \times 6^4 \overset{100}{=} 76 \times 96 = 7296 \overset{100}{=} 96 \\
6^{5k+5} &= 6^{5k} \times 6^5 \overset{100}{=} 76 \times 76 = 5776 \overset{100}{=} 76 \\
6^{5k+6} &= 6^{5k} \times 6^6 \overset{100}{=} 76 \times 56 = 4256 \overset{100}{=} 56
\end{aligned}$$

where $k \in \mathbb{N}^0$ (to include $n = 2, 3, 4, 5, 6$). So, the numbers 6^n end in $36, 16, 96, 76, 56$ for all $\mathbb{N} \ni n > 1$.

2.7.1 Modular Multiplicative Inverse

If m is an integer then its modular multiplicative inverse modulo k is an integer m^* defined by the following modular relation:

$$mm^* \overset{k}{=} 1 \tag{52}$$

The modular multiplicative inverse can be computed by solving the equation $mm^* + kn = 1$ (which is equivalent to Eq. 52) for m^* and n $(\in \mathbb{Z})$ using the extended Euclidean algorithm (see § 2.3.4 and § 2.4 as well as § 4.1.1).

Some of the facts, rules and properties of modular multiplicative inverse are listed in the following points (noting that $m, n, k, s, t \in \mathbb{Z}$ and $k > 1$):

1. The modular multiplicative inverse of m (modulo k) exists *iff* m and k are coprime (see Eq. 52 and refer to § 4.1.1).
2. The modular multiplicative inverse (when exists) is unique (i.e. in modular arithmetic sense).
3. If $m \stackrel{k}{=} n$ then $m^* \stackrel{k}{=} n^*$ (assuming the existence of modular multiplicative inverse).
4. If $mx \stackrel{k}{=} n$ then $x \stackrel{k}{=} m^*n$ ($x \in \mathbb{Z}$ and m^* exists).
5. Modular multiplicative inversion is a symmetric relation, i.e. if m is the modular multiplicative inverse of n (modulo k) then n is the modular multiplicative inverse of m (modulo k). We may express this mathematically as $(m^*)^* \stackrel{k}{=} m$, i.e.

$$n \stackrel{k}{=} m^* \qquad \rightarrow \qquad m \stackrel{k}{=} n^* \stackrel{k}{=} (m^*)^*$$

Problems

1. Find the modular multiplicative inverse of the following:
   (**a**) 23 modulo 6. (**b**) 71 modulo 13. (**c**) 125 modulo 57.
   Solution: From Eq. 52 we have $mm^* + kn = 1$.
   (**a**) $m = 23$ and $k = 6$. On using the extended Euclidean algorithm we get:

$$mm^* + kn = 23(-1) + 6(4) = 1$$

   Hence, $m^* = -1 \stackrel{6}{=} 5$.
   (**b**) $m = 71$ and $k = 13$. On using the extended Euclidean algorithm we get:

$$mm^* + kn = 71(-2) + 13(11) = 1$$

   Hence, $m^* = -2 \stackrel{13}{=} 11$.
   (**c**) $m = 125$ and $k = 57$. On using the extended Euclidean algorithm we get:

$$mm^* + kn = 125(26) + 57(-57) = 1$$

   Hence, $m^* = 26$.
2. Prove (or justify) the following:
   (**a**) The modular multiplicative inverse exists *iff* m and k are coprime (see Eq. 52).
   (**b**) The modular multiplicative inverse is unique (if it exists).
   (**c**) If $mx \stackrel{k}{=} n$ and m^* (mod k) exists then $x \stackrel{k}{=} m^*n$.
   (**d**) If $m \stackrel{k}{=} n$ and m^* (mod k) exists then $m^* \stackrel{k}{=} n^*$.
   (**e**) A positive integer m is its own inverse (mod p where $p \in \mathbb{P}$) *iff* p is a divisor of $(m-1)$ or p is a divisor of $(m+1)$.
   (**f**) A positive integer m is its own inverse (mod p where $p \in \mathbb{P}$) *iff* $m \stackrel{p}{=} 1$ or $m \stackrel{p}{=} (p-1)$.
   (**g**) If $m, n, k \in \mathbb{N}$ with m and k being coprime then $(m^*)^n \stackrel{k}{=} (m^n)^*$.
   (**h**) If $p \in \mathbb{P}$ then each member of the set $S = \{1, 2, \ldots, (p-1)\}$ must have a modular inverse in S (modulo p).
   Solution:
   (**a**) For the "**if part**" we argue that if m and k are coprime then $\gcd(m, k) = 1$. Now, the extended Euclidean algorithm (or rather the Bezout theorem; see § 2.3.4) guarantees the existence of s, t such that $\gcd(m, k) = sm + tk = 1$ and this is equivalent to $sm \stackrel{k}{=} 1$, i.e. $s = m^*$ (also see § 4.1.1).
   For the "**only if part**" we argue that if the modular multiplicative inverse exists then we have $mm^* \stackrel{k}{=} 1$ which is equivalent to $mm^* + tk = 1$ ($t \in \mathbb{Z}$). Now, if $g = \gcd(m, k)$ then $m = g\mu$ and $k = g\kappa$ ($\mu, \kappa \in \mathbb{Z}$) and hence:

$$mm^* + tk = g\mu m^* + tg\kappa = g(\mu m^* + t\kappa) = 1$$

   This means $g|1$ (noting that $\mu m^* + t\kappa$ is an integer; see rule 1 of § 1.8) and hence $g = 1$, i.e. m and k are coprime (see part a of Problem 1 of 2.2).

(**b**) Let assume that there are two modular multiplicative inverses of m (mod k). Thus, $mm_1^* \stackrel{k}{=} 1$ and $mm_2^* \stackrel{k}{=} 1$ (where m_1^*, m_2^* are the two modular inverses) and hence $mm_1^* \stackrel{k}{=} mm_2^*$. Now by rule 7 of § 2.7 (noting that m and k are coprime according to part a) we get $m_1^* \stackrel{k}{=} m_2^*$ which means the inverse is unique (i.e. in modular arithmetic modulo k).
(**c**) On multiplying both sides of $mx \stackrel{k}{=} n$ by m^* (see rule 6 of § 2.7) we get $m^*mx \stackrel{k}{=} m^*n$. Now, by Eq. 52 we have $mm^* \stackrel{k}{=} 1$ and hence $x \stackrel{k}{=} m^*n$.
(**d**)

$$\begin{aligned} m &\stackrel{k}{=} n && \\ m^*m &\stackrel{k}{=} m^*n && \text{(rule 6 of § 2.7)} \\ 1 &\stackrel{k}{=} m^*n && \text{(Eq. 52)} \\ n^* &\stackrel{k}{=} m^*nn^* && \text{(rule 6 of § 2.7)} \\ n^* &\stackrel{k}{=} m^* && \text{(Eq. 52)} \\ m^* &\stackrel{k}{=} n^* && \text{(rule 1 of § 2.7)} \end{aligned}$$

(**e**) For the "**if part**" we argue that if p is a divisor of $(m-1)$ or p is a divisor of $(m+1)$ then $m \stackrel{p}{=} +1$ or $m \stackrel{p}{=} -1$ (respectively). Hence, by rule 11 of § 2.7 (with $t = 2$) we get (in each case) $m^2 = mm \stackrel{p}{=} 1$ which means (according to Eq. 52) that m is its own inverse (mod p).
For the "**only if part**" we argue that if m is its own inverse (mod p) then $mm = m^2 \stackrel{p}{=} 1$ which means that $(m^2 - 1) = (m-1)(m+1)$ is divisible by p. Therefore, p is a divisor of $(m-1)$ or p is a divisor of $(m+1)$ (see rule 22 of § 1.9).
(**f**) This is a corollary of part (e) because "p is a divisor of $(m-1)$" (in the statement of part e) means $(m-1) \stackrel{p}{=} 0$ (i.e. $m \stackrel{p}{=} 1$), while "p is a divisor of $(m+1)$" (in the statement of part e) means $(m+1) \stackrel{p}{=} 0$, i.e. $m \stackrel{p}{=} -1 \stackrel{p}{=} (p-1)$.
(**g**) Because m and k are coprime then m^* exists (see part a). Hence:

$$\begin{aligned} mm^* &\stackrel{k}{=} 1 && \text{(Eq. 52)} \\ (mm^*)^n &\stackrel{k}{=} 1^n && \text{(rule 11 of § 2.7)} \\ m^n(m^*)^n &\stackrel{k}{=} 1 && \text{(rules of indices)} \\ (m^*)^n &\stackrel{k}{=} (m^n)^* && \text{(part c)} \end{aligned}$$

It is worth noting (with reference to the last line) that m^n and k are coprime (see part l of Problem 12 of § 2.2) and hence $(m^n)^*$ exists (according to part a of the present Problem).
(**h**) We note first that all the members in the set $S = \{1, 2, \ldots, (p-1)\}$ are coprime to p because p is prime (and hence its only divisors are 1 and p). So, each member of S must have a multiplicative inverse modulo p (see point 1 in the preamble as well as part a of the present Problem). Now, the members of S represent all the possible residue classes that have inverse (modulo p).[92] Hence, any member of S must have a modular multiplicative inverse in S (whether this inverse is itself or different; see parts e and f). In brief, each member in S must have a modular inverse in S (modulo p), as required.

2.7.2 Residue Systems

A **complete residue system** modulo k is defined as a set of integers such that every integer is congruent modulo k to exactly one member of the set, i.e. the set contains exactly one element of every residue class

[92] We note that 0 (which is the only residue class modulo p that is not present in S) cannot have a multiplicative inverse (see Eq. 52 and note as well that 0 and p are not coprime; see part l of Problem 1 of § 2.2).

modulo k. For example, the set $S_c = \{0, 1, 2, 3, 4, 5, 6\}$ is a complete residue system modulo 7 because any integer must be congruent (mod 7) to exactly one member of S_c. Accordingly, a set of non-congruent integers (mod k) is a complete residue system (mod k) *iff* the size of the set is k. This should be obvious because the remainder r of dividing any integer by k must belong to the set $\{0, 1, \ldots, k-1\}$ which is of size k. Each one of the elements of the set $\{0, 1, \ldots, k-1\}$ represents a class for the complete residue system (mod k) where all the integers in a given class differ from each other by multiples of k (e.g. class 0 contains $\ldots, -2k, -k, 0, k, 2k, \ldots$ and class 1 contains $\ldots, 1-2k, 1-k, 1, 1+k, 1+2k, \ldots$). Any set of k non-congruent integers modulo k forms a complete residue system modulo k. Accordingly, there are infinitely many complete residue systems for any given modulo k. The simplest complete residue system modulo k is the set $\{0, 1, \ldots, k-1\}$.

A **reduced residue system** modulo k is defined as a set of integers of size $\phi(k)$ elements such that all the elements are coprime to k and no two elements are congruent modulo k. For example, the set $S_r = \{1, 2, 3, 4\}$ is a reduced residue system modulo 5 because $\phi(5) = 4$ (which is the size of S_r), moreover all the elements of S_r are coprime to 5 and no two elements of S_r are congruent modulo 5. Each one of the elements of the reduced residue system $\{r_i : i = 1, 2, \ldots, \phi(k)\}$ with $0 < r_i < k$ represents a class for the reduced residue system (mod k) where all the integers in a given class differ from each other by multiples of k (as demonstrated earlier for the complete residue system). It is obvious that a reduced residue system (S_r) modulo k is obtained from a complete residue system (S_c) modulo k by eliminating the elements of S_c which are not coprime to k.

Problems

1. Give two examples of complete residue systems modulo 11.
   Solution: For example:

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \qquad \{22, 12, 35, -8, -40, 16, 61, -59, 96, 9, -12\}$$

2. Of which modulo (if any) the following can be complete residue systems CRS (justify your answer):
   (**a**) $\{-68, -53, -36, -10, 2, 23, 39, 62, 79\}$. (**b**) $\{1, 5, 36, -40, 22, -21\}$.
   (**c**) $\{-102, -67, -65, -17, -12, 7, 21, 44, 69, 101, 116, 120, 201\}$.
   Solution:
   (**a**) This set contains 9 elements and hence if it is a CRS then it must be a CRS modulo 9. Now, the only condition required for this set to be a CRS modulo 9 is that the set contains exactly one element of every residue class modulo 9 which is not the case (noting that these elements represent respectively the residue classes $4, 1, 0, 8, 2, 5, 3, 8, 7$ modulo 9 and hence we have two representatives of class 8 and no representative of class 6).
   (**b**) This set contains 6 elements and hence if it is a CRS then it must be a CRS modulo 6. Now, the only condition required for this set to be a CRS modulo 6 is that the set contains exactly one element of every residue class modulo 6 which is the case (noting that these elements represent respectively the residue classes $1, 5, 0, 2, 4, 3$ modulo 6).
   (**c**) This set contains 13 elements and hence if it is a CRS then it must be a CRS modulo 13. Now, the only condition required for this set to be a CRS modulo 13 is that the set contains exactly one element of every residue class modulo 13 which is the case (noting that these elements represent respectively the residue classes $2, 11, 0, 9, 1, 7, 8, 5, 4, 10, 12, 3, 6$ modulo 13).
3. Give a reduced residue system for each of the following moduli: $k = 7$, $k = 10$, and $k = 16$.
   Solution:

$$S_r(7) = \{1, 2, 3, 4, 5, 6\} \qquad S_r(10) = \{1, 3, 7, 9\} \qquad S_r(16) = \{1, 3, 5, 7, 9, 11, 13, 15\}$$

4. Which of the following is a reduced residue system RRS (where we use S_r here tentatively):
   (**a**) $S_r(9) = \{1, 2, 4, 5, 7, 8\}$. (**b**) $S_r(11) = \{1, 2, 3, 4, 5, 7, 8, 9, 10\}$.
   (**c**) $S_r(16) = \{1, -13, -11, 7, -7, 11, -3, 15\}$. (**d**) $S_r(20) = \{-19, -17, -13, -11, 11, 13, 17, 19\}$.
   Solution:

(**a**) This is RRS because it has $\phi(9) = 6$ elements and all elements are coprime to 9 with no two elements being congruent modulo 9.
(**b**) This is not RRS because it contains only 9 elements while $\phi(11) = 10$ (the 6 class is not included).
(**c**) This is RRS because it has $\phi(16) = 8$ elements and all elements are coprime to 16 with no two elements being congruent modulo 16.
(**d**) This is RRS because it has $\phi(20) = 8$ elements and all elements are coprime to 20 with no two elements being congruent modulo 20.

5. Give five examples of reduced residue system modulo 5.
Solution: For example:

$$\{1,2,3,4\} \qquad \{6,7,8,9\} \qquad \{-4,-3,-2,-1\} \qquad \{11,42,83,104\} \qquad \{-6,22,-17,51\}$$

6. Prove (or justify) the following statements about complete and reduced residue systems.
(**a**) If $S_c = \{r_1, r_2, \ldots, r_k\}$ is a complete residue system modulo k, and $m \in \mathbb{N}$ and $n \in \mathbb{Z}$ with k and m being coprime then

$$S_{mn} = \{mr_1 + n, mr_2 + n, \ldots, mr_k + n\}$$

is also a complete residue system modulo k.
(**b**) For k odd, the sum of the elements of any complete residue system modulo k is divisible by k.
(**c**) If r_i represents a class of a reduced residue system (mod k) then $k - r_i$ represents another class of that reduced residue system.
(**d**) The sum of elements of a reduced residue system modulo k ($k > 2$) is divisible by k.
(**e**) If $S_r = \{r_1, r_2, ..., r_{\phi(k)}\}$ is a reduced residue system modulo k, then $S_{re} = \{mr_1, mr_2, ..., mr_{\phi(k)}\}$ is also a reduced residue system modulo k (where $m \in \mathbb{N}$, and k and m are coprime).
Solution:
(**a**) In brief, this is because S_{mn} has k elements and no two elements of S_{mn} are congruent modulo k (since by rules 3 and 7 of § 2.7 if $mr_i + n \overset{k}{=} mr_j + n$ then $r_i \overset{k}{=} r_j$ noting that k and m are coprime). So, S_{mn} meets all the conditions of complete residue system (mod k) and hence it is a complete residue system (mod k).
In more details, it is obvious that S_{mn} is of size k, so all we need to do is to show that no two elements of S_{mn} are congruent (mod k). Now, if $mr_i + n$ and $mr_j + n$ are two congruent elements of S_{mn} (where $r_i, r_j \in S_c$) then we have:

$$\begin{aligned} mr_i + n &\overset{k}{=} mr_j + n \\ mr_i &\overset{k}{=} mr_j && \text{(rule 3 of § 2.7)} \\ r_i &\overset{k}{=} r_j && \text{(rule 7 of § 2.7 noting that } k \text{ and } m \text{ are coprime)} \end{aligned}$$

Thus, $r_i = r_j$ (because S_c is a complete residue system modulo k and hence if $r_i \neq r_j$ then $r_i \overset{k}{\neq} r_j$) which means that r_i and r_j are the same element of S_c, i.e. $i = j$. Accordingly, $mr_i + n$ and $mr_j + n$ must represent the same element of S_{mn}, i.e. no two elements of S_{mn} are congruent (mod k). Therefore, S_{mn} is a set of k non-congruent (mod k) elements and hence it is a complete residue system (mod k).
(**b**) Let consider the simplest complete residue system modulo k, that is $\{0, 1, \ldots, k-1\}$. Accordingly, the sum of the elements of this system is (see Eq. 15):

$$\sum_{i=0}^{k-1} i = 0 + \sum_{i=1}^{k-1} i = 0 + \frac{(k-1)([k-1]+1)}{2} = \frac{(k-1)k}{2} = mk$$

where $m \in \mathbb{N}$ because k is odd and hence $(k-1)$ is even. As we see, the sum of the elements of the simplest complete residue system modulo k is divisible by k.
Now, the elements of any other complete residue system modulo k differ from the corresponding elements of the simplest complete residue system (i.e. those in their class) by multiples of k (see the preamble of

the present subsection), so their sum just adds multiples of k to the sum of the elements of the simplest complete residue system, and hence the total sum must be divisible by k (see rule 14 of § 1.9).
(**c**) Let consider the simplest reduced residue system modulo k, that is $\{r_i : i = 1, 2, \ldots, \phi(k)\}$ with $0 < r_i < k$. Now, since r_i represents a reduced residue class (mod k) then it must be coprime to k and hence $k - r_i$ must also be coprime to k (see part b of Problem 19 of § 2.2).[93] Thus, $k - r_i$ which is less than k (since $0 < r_i < k$) and is not equal to r_i (since r_i is coprime to k and hence it cannot be half k) must represent another class in that reduced residue system.
Now, the elements of any other reduced residue system modulo k differ from the corresponding elements of the simplest reduced residue system (i.e. those in their class) by multiples of k (see the preamble of the present subsection). Since the difference by multiples of k does not change the residue class to which an integer belongs then the statement is valid for all reduced residue systems (modulo k). In other words, we can convert any other reduced residue system to the simplest form (by canceling the multiples of k) and apply the above argument which is based on the consideration of the simplest reduced residue system.
(**d**) This is because (for $k > 2$) $\phi(k)$ is even (see point 5 of § 2.6.4). Moreover, according to part (c) if r_i is a reduced residue class (mod k) then $k - r_i$ must be another reduced residue class (mod k). So, the elements of the reduced residue system will be matched in pairs where r_i is canceled in each pair leaving a sum of multiples of k which is divisible by k.
(**e**) This is because:
• S_{re} has $\phi(k)$ elements $\big[$since S_r has $\phi(k)$ elements$\big]$,
• the elements of S_{re} are coprime to k $\big[$since the elements of S_r are coprime to k and m is coprime to k; see part (e) of Problem 1 of § 2.2$\big]$, and
• no two elements of S_{re} are congruent modulo k $\big[$since by rule 7 of § 2.7 if $mr_i \overset{k}{=} mr_j$ then $r_i \overset{k}{=} r_j$ noting that k and m are coprime, and hence $r_i = r_j$ (because no two elements of S_r are congruent modulo k and thus if $r_i \neq r_j$ then $r_i \overset{k}{\neq} r_j$) which means that mr_i and mr_j represent the same element of $S_{re}\big]$.
So, S_{re} meets all the conditions of reduced residue system (mod k) and hence it is a reduced residue system (mod k).

2.7.3 The Chinese Remainder Method

The Chinese remainder method (for solving a system of simultaneous linear congruence equations) is based on the **Chinese remainder theorem** which states: if $m_1, m_2, \ldots, m_k$ are moduli that are pairwise coprime[94] and $n_1, n_2, \ldots, n_k$ are integers then the following system of simultaneous linear congruence equations in the unknown $x \in \mathbb{Z}$:

$$x \overset{m_1}{=} n_1 \qquad x \overset{m_2}{=} n_2 \qquad \cdots \qquad x \overset{m_k}{=} n_k \tag{53}$$

has a unique solution modulo $M = m_1 \times m_2 \times \ldots \times m_k$, i.e. there is a single solution $0 \leq x_m < M$ and all other solutions are congruent modulo M to x_m.

According to the Chinese remainder method, to solve such a system of congruences we do the following (where $i = 1, 2, \ldots, k$):
• Calculate $y_i = M/m_i$.
• Calculate y_i^* (which is the modular multiplicative inverse of y_i modulo m_i; see § 2.7.1).
• Calculate $s = \sum_{i=1}^{k} n_i y_i y_i^*$.
The required solution is $x_m \overset{M}{=} s$ (noting that all $x = x_m + Mq$ where $q \in \mathbb{Z}$ satisfy the given congruence equations).

---

[93] In fact, we are using the "only if part" of part b of Problem 19 of § 2.2 where k, r_i and $k - r_i$ here correspond (respectively) to m, n and $(m - n)$ there.
[94] Although the Chinese remainder theorem can be applied to systems with moduli that are not coprime there is no guarantee that a solution does exist in this case.

Problems

1. Solve the following system of congruence equations using the Chinese remainder method:

$$x \overset{3}{=} 1 \qquad x \overset{5}{=} 4 \qquad x \overset{7}{=} 6$$

Solution: This system meets all the stated conditions in the Chinese remainder theorem (noting that $M = 3 \times 5 \times 7 = 105$).

• Calculate $y_i = M/m_i$:

$$y_1 = 5 \times 7 = 35 \qquad y_2 = 3 \times 7 = 21 \qquad y_3 = 3 \times 5 = 15$$

• Calculate y_i^*:[95]

$$y_1^* = 35^* = 2 \pmod 3 \qquad y_2^* = 21^* = 1 \pmod 5 \qquad y_3^* = 15^* = 1 \pmod 7$$

• Calculate $s = \sum_{i=1}^{k} n_i y_i y_i^*$:

$$n_1 y_1 y_1^* + n_2 y_2 y_2^* + n_3 y_3 y_3^* = (1 \times 35 \times 2) + (4 \times 21 \times 1) + (6 \times 15 \times 1) = 244$$

So, the required solution is $x_m \overset{105}{=} 244$, i.e. $x_m = 34$. As we see, 34 satisfies all the given congruence equations. In fact, all $x = 34 + 105q$ ($q \in \mathbb{Z}$) satisfy these congruence equations.

2. Solve the following system of congruence equations using the Chinese remainder method:

$$x \overset{4}{=} 3 \qquad x \overset{7}{=} 5 \qquad x \overset{9}{=} 8$$

Solution: This system meets all the stated conditions in the Chinese remainder theorem (noting that $M = 4 \times 7 \times 9 = 252$):

• Calculate $y_i = M/m_i$:

$$y_1 = 7 \times 9 = 63 \qquad y_2 = 4 \times 9 = 36 \qquad y_3 = 4 \times 7 = 28$$

• Calculate y_i^*:

$$y_1^* = 63^* = 3 \pmod 4 \qquad y_2^* = 36^* = 1 \pmod 7 \qquad y_3^* = 28^* = 1 \pmod 9$$

• Calculate $s = \sum_{i=1}^{k} n_i y_i y_i^*$:

$$n_1 y_1 y_1^* + n_2 y_2 y_2^* + n_3 y_3 y_3^* = (3 \times 63 \times 3) + (5 \times 36 \times 1) + (8 \times 28 \times 1) = 971$$

So, the required solution is $x_m \overset{252}{=} 971$, i.e. $x_m = 215$. As we see, 215 satisfies all the given congruence equations. In fact, all $x = 215 + 252q$ ($q \in \mathbb{Z}$) satisfy these congruence equations.

3. Find the smallest $n \in \mathbb{N}$ such that $5|(n+1)$, $7|(n+2)$ and $11|(n+6)$.

Solution: These three divisibility relations are equivalent (respectively) to:

$$n \overset{5}{=} -1 \overset{5}{=} 4 \qquad n \overset{7}{=} -2 \overset{7}{=} 5 \qquad n \overset{11}{=} -6 \overset{11}{=} 5$$

So, we are required to solve the following system of congruence equations:

$$n \overset{5}{=} 4 \qquad n \overset{7}{=} 5 \qquad n \overset{11}{=} 5$$

On using the Chinese remainder method (noting that this system meets the conditions of this method and following the procedure demonstrated in the previous Problems) we get $n = 159$ (which is the smallest $n \in \mathbb{N}$ that satisfy the given divisibility relations). We note that all $x = 159 + 385q$ ($q \in \mathbb{Z}$) satisfy the given divisibility relations.

4. Compare the Chinese remainder theorem to rule 14 of § 2.7.

Solution: Referring to Eq. 53, we note that rule 14 of § 2.7 is a special case of the Chinese remainder theorem from the perspective of the values of n's (i.e. in rule 14 of § 2.7 we have $n_1 = n_2 = \ldots = n_k = n$). However, rule 14 of § 2.7 is more general than the Chinese remainder theorem (as stated above) from the perspective of pairwise coprimality of the moduli.

[95] For the calculation of modular multiplicative inverse (i.e. y_i^*) see § 2.7.1.

2.7.4 The Equivalent Equation Method

This is a method for solving a system of simultaneous linear congruence equations and hence it can be used as an alternative to the Chinese remainder method which we investigated in the last subsection. We outline this method in the following Problems.

Problems

1. Solve the system of Problem 1 of § 2.7.3 using the equivalent equation method:
   Solution: We do the following:
   - From the third congruence (which is the one with the largest modulo) we get: $x = 7i + 6$.
   - We substitute this in the second congruence: $7i + 6 \stackrel{5}{=} 4$ and hence $i \stackrel{5}{=} 4$, i.e. $i = 5j + 4$.
   - On substituting this into $x = 7i + 6$ we get: $x = 7(5j + 4) + 6 = 35j + 34$.
   - On substituting this into the first congruence we get: $35j + 34 \stackrel{3}{=} 1$ and hence $j \stackrel{3}{=} 0$, i.e. $j = 3q$.
   - On substituting this into $x = 35j + 34$ we get $x = 35(3q) + 34 = 105q + 34$.

   So, we finally get $x_m \stackrel{105}{=} 105q + 34$, i.e. $x_m = 34$ (as before).
2. Solve the system of Problem 2 of § 2.7.3 using the equivalent equation method:
   Solution: We do the following:
   - From the third congruence (which is the one with the largest modulo) we get: $x = 9i + 8$.
   - We substitute this in the second congruence: $9i + 8 \stackrel{7}{=} 5$ and hence $i \stackrel{7}{=} 2$, i.e. $i = 7j + 2$.
   - On substituting this into $x = 9i + 8$ we get: $x = 9(7j + 2) + 8 = 63j + 26$.
   - On substituting this into the first congruence we get: $63j + 26 \stackrel{4}{=} 3$ and hence $j \stackrel{4}{=} 3$, i.e. $j = 4q + 3$.
   - On substituting this into $x = 63j + 26$ we get $x = 63(4q + 3) + 26 = 252q + 215$.

   So, we finally get $x_m \stackrel{252}{=} 252q + 215$, i.e. $x_m = 215$ (as before).

2.7.5 Multivariate Congruence Equations

In this subsection we briefly investigate (through solved Problems) some simple types of multivariate congruence equations and how they are solved. Also see § 4.2.[96]

Problems

1. Solve the following multivariate congruence equations (where $x, y, z \in \mathbb{Z}$):

   (**a**) $5x + 3y \stackrel{7}{=} 1$. (**b**) $13x + 6y \stackrel{11}{=} 8$. (**c**) $5x + 7y + 9z \stackrel{17}{=} 21$.

   (**d**) $x^2 - 19y \stackrel{3}{=} 14$. (**e**) $2x^2 + 23y^2 \stackrel{7}{=} 6$. (**f**) $x^3 + 13y^2 - z^2 \stackrel{2}{=} 1$.

   Solution:

   (**a**) If $y = k$ ($k \in \mathbb{Z}$) then $5x \stackrel{7}{=} 1 - 3k$. On multiplying the two sides by the modular multiplicative inverse (mod 7) of 5 (which is 3) we get: $x \stackrel{7}{=} 3 - 9k \stackrel{7}{=} 3 + 5k$. So, the solution is $(x, y) = (3 + 5k,\ k)$ where $k \in \mathbb{Z}$.

   We may solve this congruence differently by considering all the combinations of $x \stackrel{7}{=} 0, 1, 2, 3, 4, 5, 6$ and $y \stackrel{7}{=} 0, 1, 2, 3, 4, 5, 6$ where we will find that $5x + 3y \stackrel{7}{=} 1$ is satisfied by the following combinations:

   $$(x, y) \stackrel{7}{=} (0, 5),\ (1, 1),\ (2, 4),\ (3, 0),\ (4, 3),\ (5, 6),\ (6, 2)$$

   and hence the solutions are (where $s, t \in \mathbb{Z}$):

   $(x, y) = (7s,\ 5 + 7t)$ $(x, y) = (1 + 7s,\ 1 + 7t)$ $(x, y) = (2 + 7s,\ 4 + 7t)$ $(x, y) = (3 + 7s,\ 7t)$

   $(x, y) = (4 + 7s,\ 3 + 7t)$ $(x, y) = (5 + 7s,\ 6 + 7t)$ $(x, y) = (6 + 7s,\ 2 + 7t)$

   It is straightforward to show that the solutions of these two methods are equivalent (see Problem 2).

   (**b**) If $y = k$ ($k \in \mathbb{Z}$) then $13x \stackrel{11}{=} 8 - 6k$. On multiplying the two sides by the modular multiplicative inverse (mod 11) of 13 (which is 6) we get: $x \stackrel{11}{=} 48 - 36k \stackrel{11}{=} 4 + 8k$. So, the solution is $(x, y) = (4 + 8k,\ k)$

[96] We note that some of the Problems of § 2.7 are about multivariate congruence equations.

where $k \in \mathbb{Z}$.
We may solve this congruence differently (as we did in part a) and obtain the following solutions (x, y) where $s, t \in \mathbb{Z}$:

$(11s,\ 5 + 11t)$ $(1 + 11s,\ 1 + 11t)$ $(2 + 11s,\ 8 + 11t)$ $(3 + 11s,\ 4 + 11t)$
$(4 + 11s,\ 11t)$ $(5 + 11s,\ 7 + 11t)$ $(6 + 11s,\ 3 + 11t)$ $(7 + 11s,\ 10 + 11t)$
$(8 + 11s,\ 6 + 11t)$ $(9 + 11s,\ 2 + 11t)$ $(10 + 11s,\ 9 + 11t)$

(**c**) If $y = k$ and $z = s$ $(k, s \in \mathbb{Z})$ then $5x \overset{17}{=} 21 - 7k - 9s$. On multiplying the two sides by the modular multiplicative inverse (mod 17) of 5 (which is 7) we get: $x \overset{17}{=} 147 - 49k - 63s \overset{17}{=} 11 + 2k + 5s$. So, the solution is $(x, y, z) = (11 + 2k + 5s,\ k,\ s)$ where $k, s \in \mathbb{Z}$.
(**d**) We have $x^2 \overset{3}{=} 14 + 19y \overset{3}{=} 2 + y$. Now, we have three cases to consider (where $s \in \mathbb{Z}$):
• $x \overset{3}{=} 0$ and hence $x^2 \overset{3}{=} 0$. Accordingly, $2 + y = 3s$ and hence $y = -2 + 3s \overset{3}{=} 1 + 3s$.
• $x \overset{3}{=} 1$ and hence $x^2 \overset{3}{=} 1$. Accordingly, $2 + y = 1 + 3s$ and hence $y = -1 + 3s \overset{3}{=} 2 + 3s$.
• $x \overset{3}{=} 2$ and hence $x^2 \overset{3}{=} 4 \overset{3}{=} 1$. Accordingly, $2 + y = 1 + 3s$ and hence $y = -1 + 3s \overset{3}{=} 2 + 3s$.
So overall, the solutions are all pairs of the following three forms (where $k, s \in \mathbb{Z}$):

$(x, y) = (3k,\ 1 + 3s)$ $(x, y) = (1 + 3k,\ 2 + 3s)$ $(x, y) = (2 + 3k,\ 2 + 3s)$

(**e**) We have $2x^2 \overset{7}{=} 6 - 23y^2$. On multiplying the two sides by the modular multiplicative inverse (mod 7) of 2 (which is 4) we get: $x^2 \overset{7}{=} 24 - 92y^2 \overset{7}{=} 3 - y^2$. Now, we have seven cases to consider (where $s \in \mathbb{Z}$):
• $x \overset{7}{=} 0$ and hence $x^2 \overset{7}{=} 0$. Accordingly, $3 - y^2 \overset{7}{=} 0$ and hence $y^2 \overset{7}{=} 3$ which has no solution.
• $x \overset{7}{=} 1$ and hence $x^2 \overset{7}{=} 1$. Accordingly, $3 - y^2 \overset{7}{=} 1$ and hence $y^2 \overset{7}{=} 2$ which has two solutions: $y = 3 + 7s$ and $y = 4 + 7s$.
• $x \overset{7}{=} 2$ and hence $x^2 \overset{7}{=} 4$. Accordingly, $3 - y^2 \overset{7}{=} 4$ and hence $y^2 \overset{7}{=} 6$ which has no solution.
• $x \overset{7}{=} 3$ and hence $x^2 \overset{7}{=} 9 \overset{7}{=} 2$. Accordingly, $3 - y^2 \overset{7}{=} 2$ and hence $y^2 \overset{7}{=} 1$ which has two solutions: $y = 1 + 7s$ and $y = 6 + 7s$.
• $x \overset{7}{=} 4$ and hence $x^2 \overset{7}{=} 16 \overset{7}{=} 2$. Accordingly, $3 - y^2 \overset{7}{=} 2$ and hence $y^2 \overset{7}{=} 1$ which has two solutions: $y = 1 + 7s$ and $y = 6 + 7s$.
• $x \overset{7}{=} 5$ and hence $x^2 \overset{7}{=} 25 \overset{7}{=} 4$. Accordingly, $3 - y^2 \overset{7}{=} 4$ and hence $y^2 \overset{7}{=} 6$ which has no solution.
• $x \overset{7}{=} 6$ and hence $x^2 \overset{7}{=} 36 \overset{7}{=} 1$. Accordingly, $3 - y^2 \overset{7}{=} 1$ and hence $y^2 \overset{7}{=} 2$ which has two solutions: $y = 3 + 7s$ and $y = 4 + 7s$.
So overall, the solutions are all pairs of the following eight forms (where $k, s \in \mathbb{Z}$):

$(x, y) = (1 + 7k,\ 3 + 7s)$ $(x, y) = (1 + 7k,\ 4 + 7s)$ $(x, y) = (3 + 7k,\ 1 + 7s)$
$(x, y) = (3 + 7k,\ 6 + 7s)$ $(x, y) = (4 + 7k,\ 1 + 7s)$ $(x, y) = (4 + 7k,\ 6 + 7s)$
$(x, y) = (6 + 7k,\ 3 + 7s)$ $(x, y) = (6 + 7k,\ 4 + 7s)$

(**f**) We have $x^3 + 13y^2 - z^2 \overset{2}{=} 1$. Now, we have four cases to consider (where we refer the reader to the rules of parity in § 1.8):
• x is even and y is even and hence z is odd.
• x is even and y is odd and hence z is even.
• x is odd and y is even and hence z is even.
• x is odd and y is odd and hence z is odd.
So overall, the solutions are all triples of the following four forms (where e stands for even and o stands for odd):

$(x, y, z) = (e, e, o)$ $(x, y, z) = (e, o, e)$ $(x, y, z) = (o, e, e)$ $(x, y, z) = (o, o, o)$

2. Show that the solutions obtained in part (a) of Problem 1 by the two methods are equivalent.
Solution: The solutions obtained by the first method are given by: $(x, y) = (3 + 5k,\ k)$ where $k \in \mathbb{Z}$, while the solutions obtained by the second method are given by the list in the end of that part. Now,

if we substitute the y entries from the second method for k in the first method (since $y = k$ according to the first method) then we get the following solutions:

The first method	**The second method**
$(x, y) = (7[4 + 5t],\ 5 + 7t)$	$(x, y) = (7s,\ 5 + 7t)$
$(x, y) = (1 + 7[1 + 5t],\ 1 + 7t)$	$(x, y) = (1 + 7s,\ 1 + 7t)$
$(x, y) = (2 + 7[3 + 5t],\ 4 + 7t)$	$(x, y) = (2 + 7s,\ 4 + 7t)$
$(x, y) = (3 + 7[5t],\ 7t)$	$(x, y) = (3 + 7s,\ 7t)$
$(x, y) = (4 + 7[2 + 5t],\ 3 + 7t)$	$(x, y) = (4 + 7s,\ 3 + 7t)$
$(x, y) = (5 + 7[4 + 5t],\ 6 + 7t)$	$(x, y) = (5 + 7s,\ 6 + 7t)$
$(x, y) = (6 + 7[1 + 5t],\ 2 + 7t)$	$(x, y) = (6 + 7s,\ 2 + 7t)$

As we see, the two solutions are equivalent where s in the second method corresponds to the expression inside the square brackets in the first method (e.g. $s = 4 + 5t$ for the first row).

2.7.6 Relationship between Ordinary and Congruence Equations

In this subsection we briefly investigate some rules and properties related to the relationship between an ordinary equation and the corresponding congruence equation.[97] For example, what is the relationship between the ordinary equation $x = y$ and its corresponding congruence equation $x \overset{m}{=} y$ (where $x, y, m \in \mathbb{Z}$ and $m > 1$). In this regard we note the following points:[98]

1. The ordinary equation can be seen as a special case of the corresponding congruence equation.[99] This is because the congruence equation $x \overset{m}{=} y$ means $x = y + km$ ($k \in \mathbb{Z}$) and hence the ordinary equation $x = y$ is a special case of the congruence equation $x \overset{m}{=} y$ corresponding to $k = 0$.
2. We can convert an ordinary equation to a congruence equation for any modulo. For example, if $x = y$ then $x \overset{m}{=} y$ (for any $\mathbb{N} \ni m > 1$). This is justified by the reflexivity of the congruence relation (i.e. $x = y \overset{m}{=} y$; see point 1 of § 2.7). This may also be justified (in a rather different way) by point 1 because $x = y$ is equivalent to $x = y + km$ with $k = 0$ and hence it is true that $x \overset{m}{=} y$ for this value of k.
3. We cannot convert a congruence equation to an ordinary equation in general. For example, if $x \overset{m}{=} y$ then it is not necessarily true that $x = y$ (e.g. $17 \overset{3}{=} 5$ but $17 \neq 5$). This is justified by the fact that the congruence relation is more general than the equality relation (see point 1) and hence the validity of the congruence equation does not imply the validity of the ordinary equation. Yes, if the congruence equation is true unconditionally then its corresponding ordinary equation is true, because in this case the congruence equation implies the ordinary equation (as will be clarified further later on).
4. Based on the previous points we can conclude that if $x = y$ then $x \overset{m}{=} y$ (for any $\mathbb{N} \ni m > 1$), but if $x \overset{m}{=} y$ (for some $\mathbb{N} \ni m > 1$) then it is not necessarily that $x = y$. Yes, if $x \overset{m}{=} y$ for every $\mathbb{N} \ni m > 1$ then it is necessarily that $x = y$ (see point 8).
5. To prove that $x \neq y$ it is enough to prove that $x \overset{m}{\neq} y$ (for some $\mathbb{N} \ni m > 1$). This is because (according to point 4) if $x = y$ then $x \overset{m}{=} y$ and hence by contraposition (see § 1.5.4) if $x \overset{m}{\neq} y$ then $x \neq y$. So, proving that $x \overset{m}{\neq} y$ is enough for proving that $x \neq y$.
6. To find the solution(s) of $x = y$ (assuming it has a solution; see point 5) we may start by investigating the solution(s) of $x \overset{m}{=} y$ (for any specific $\mathbb{N} \ni m > 1$), and then use these solutions to extract or infer

[97] We may also say: the relationship between equality and congruence.

[98] We note that there is some overlap and repetition in these points. This is justified by our desire to be very clear as well as the use of these points in different positions and contexts (where the use of some forms is more appropriate than the use of others).

[99] We may also say: the ordinary equation is more specific than the corresponding congruence equation. We can also say: the truth of the congruence equation is more general than the truth of the corresponding ordinary equation (i.e. the congruence equation can be true whether the corresponding ordinary equation is true or not).

the solutions of $x = y$. This is because managing a congruence equation by the versatile congruence rules and properties can be easier as it usually leads to many simplifications (such as reducing the size of numbers or powers) and hence we find ourselves dealing with much simpler arithmetic and algebra.

7. To investigate if $x = y$ has a solution or not, we may start by investigating if $x \overset{m}{=} y$ has a solution or not (noting that the latter investigation is usually easier than the former; see point 6). Accordingly, if we find out that $x \overset{m}{=} y$ has no solution then we can conclude that $x = y$ has no solution (see point 5) and this could save considerable time and effort in searching for the elusive solution of $x = y$. However, if we find out that $x \overset{m}{=} y$ has a solution then this does not mean that $x = y$ has a solution (within the given conditions) although this could lead us to the solution (see point 6) if it does exist (as well as it could clarify the situation and indicate if and how and why there is no solution in the opposite case).
8. Based on the previous points, we should be aware of (and distinguish between) the following cases (where $\mathbb{N} \ni m > 1$):
   (**a**) If $x = y$ then $x \overset{m}{=} y$ for *any* m.
   (**b**) If $x \overset{m}{\neq} y$ for a *specific* m then $x \neq y$. This is the contrapositive of (a).
   (**c**) If $x \overset{m}{=} y$ for *any* m (i.e. for all $\mathbb{N} \ni m > 1$) then $x = y$. This is because if $x \neq y$ then $x - y \neq 0$ and hence the prime factorization of $(x - y)$ cannot be divisible by some primes (say p_1). This means that $x \overset{p_1}{\neq} y$ which contradicts the assumption that $x \overset{m}{=} y$ for *any* m (i.e. including $m = p_1$). So, the only possibility is $x = y$ (i.e. $x - y = 0$) since 0 is divisible by any other number.
   (**d**) From (a) and (c) we conclude that $x = y$ *iff* $x \overset{m}{=} y$ for *all* m.
9. We should finally note that in modular arithmetic[100] (unlike ordinary arithmetic), terms like "root" and "solution" of an equation should mean a class and not a single number. For instance, $x - 1 = 0$ (in ordinary arithmetic) has a single root or solution which is $x = 1$, while $x - 1 \overset{3}{=} 0$ (in modular arithmetic) has a "single modular" root or solution which is $x \overset{3}{=} 1$ (i.e. $x = 1 + 3k$ where $k \in \mathbb{Z}$). So, the reader should be aware of this difference in terminology.

Problems

1. Show that the following equations have no solution in $\mathbb{Z}$:
   (**a**) $x^{10} + 12x^5 - 5 = 0$.
   (**b**) $6x^{19} - 6x^{11} - 5x^3 - 7 = 0$.
   (**c**) $8x^6 - 11y^3 - 13 = 0$.
   (**d**) $8x^4 + 16y^4 - 5z^6 - 1 = 0$.

   Solution:
   (**a**) It is difficult to investigate the solutions of a tenth degree polynomial equation. So, instead we will investigate the solutions of its corresponding congruence equation. Now, if we consider modulo 3 then when $x \overset{3}{=} 0, 1, 2$ we get (by substitution) respectively: $x^{10} + 12x^5 - 5 \overset{3}{=} 1, 2, 2$. So, $x^{10} + 12x^5 - 5 \overset{3}{=} 0$ has no solution and hence $x^{10} + 12x^5 - 5 = 0$ has no solution (see point 5 in the preamble).
   (**b**) Repeating our argument in part (a), if we consider modulo 5 then when $x \overset{5}{=} 0, 1, 2, 3, 4$ we get (by substitution): $6x^{19} - 6x^{11} - 5x^3 - 7 \overset{5}{=} 3, 3, 3, 3, 3$. So, $6x^{19} - 6x^{11} - 5x^3 - 7 \overset{5}{=} 0$ has no solution and hence $6x^{19} - 6x^{11} - 5x^3 - 7 = 0$ has no solution (see point 5).
   (**c**) If we consider modulo 7 then we can easily find that none of the 49 combinations of $x \overset{7}{=} 0, 1, 2, 3, 4, 5, 6$ and $y \overset{7}{=} 0, 1, 2, 3, 4, 5, 6$ satisfy the congruence equation $8x^6 - 11y^3 - 13 \overset{7}{=} 0$.[101] So, from point 5 we conclude that $8x^6 - 11y^3 - 13 = 0$ has no solution.
   (**d**) If we consider modulo 4 then we can easily find that none of the 64 combinations of $x \overset{4}{=} 0, 1, 2, 3$, $y \overset{4}{=} 0, 1, 2, 3$ and $z \overset{4}{=} 0, 1, 2, 3$ satisfy the congruence equation $8x^4 + 16y^4 - 5z^6 - 1 \overset{4}{=} 0$. So, from point 5 we conclude that $8x^4 + 16y^4 - 5z^6 - 1 = 0$ has no solution.

[100] We mean by "modular arithmetic" in this context the mathematics of congruence equations and by "ordinary arithmetic" the mathematics of ordinary equations.
[101] These 49 combinations can be easily and quickly checked using (for instance) a spreadsheet or a simple computer code.

2.8 Perfect Numbers

A perfect number is a positive integer that is equal to the sum of its proper divisors. The first few perfect numbers are 6, 28, 496, 8128, 33550336. We list in the following points some common facts about perfect numbers:

1. All known perfect numbers are even, so it is unknown if there is any odd perfect number or not.
2. A natural number n is perfect *iff* $\sigma(n) = 2n$. This is based on the definition of perfect number.
3. A natural number n is perfect *iff* $s(n) = n$. This is based on the definition of perfect number.
4. A number $m \in \mathbb{N}$ is an even perfect *iff* $m = 2^{n-1}(2^n - 1)$ where $(2^n - 1)$ is prime (see Problem 2).[102]
5. Referring to the previous point, even perfect numbers and Mersenne primes are connected by the formula $P_e = 2^{p-1}M_p$ where P_e is an even perfect number and M_p is the corresponding Mersenne prime (see § 2.2.2).
6. All even perfect numbers end in 6 or 8.
7. All even perfect numbers (excluding 6) end in 16, 28, 36, 56, 76, or 96.
8. Any even perfect number (except 6) is the sum of consecutive odd cubes.
9. There are 51 known perfect numbers.
10. It is unknown if there are infinitely many perfect numbers or not.

Problems

1. Propose an algorithm for finding (or generating) even perfect numbers.
   Solution: The following algorithm is based on point 4 (see the preamble of this section):[103]
   • Take a prime number p.
   • Calculate $(2^p - 1)$.
   • If $(2^p - 1)$ is prime then $2^{p-1}(2^p - 1)$ is an even perfect number.
2. Show that $m \in \mathbb{N}$ is even perfect *iff* $m = 2^{n-1}(2^n - 1)$ where $(2^n - 1) \in \mathbb{P}$.
   Solution: We have two parts to prove:
   The if part is shown in the following points:
   • $\sigma(m) = \sigma(2^{n-1})\,\sigma(2^n - 1)$ because σ is multiplicative noting that 2^{n-1} is a power of 2 and $(2^n - 1)$ is odd (which cannot contain a factor of 2) and hence they are coprime (see rule 8 of § 1.8).
   • The divisors of 2^{n-1} are $1, 2^1, 2^2, \ldots, 2^{n-1}$ and hence we have (using the identity of Eq. 12):

$$\sigma(2^{n-1}) = 1 + 2^1 + 2^2 + \cdots + 2^{n-1} = 2^n - 1 \tag{54}$$

   • Because $(2^n - 1)$ is prime, $\sigma(2^n - 1) = 1 + (2^n - 1) = 2^n$ (see rule 2 of § 2.6.1).
   • Therefore:

$$\sigma(m) = \sigma(2^{n-1})\,\sigma(2^n - 1) = (2^n - 1)\,2^n = 2\Big[2^{n-1}(2^n - 1)\Big] = 2m$$

   i.e. m is even perfect as required (see point 2 in the preamble noting as well that $n > 1$ since $n \in \mathbb{P}$).
   The only if part is shown in the following points:
   ★ Because m is even, it can be written as:

$$m = 2^{n-1}q \tag{55}$$

   where $\mathbb{N} \ni n > 1$ and $q \in \mathbb{O}$ (see rule 8 of § 1.8).
   ★ Because m is perfect, we have (using point 2 with Eq. 55):

$$\sigma(m) = 2m = 2^n q \tag{56}$$

   ★ Noting that 2^{n-1} is a natural power of 2 and q is odd (which cannot contain a factor of 2) and hence they are coprime, we have:

$$\sigma(m) = \sigma(2^{n-1})\,\sigma(q) \qquad (\sigma \text{ is multiplicative, Eq. 55})$$

[102] We note that the primality of $(2^n - 1)$ should incur the primality of n (see part c of Problem 12 of § 2.2 as well as Problem 13 of § 2.2) and hence we can write $m = 2^{p-1}(2^p - 1)$.

[103] Noting the link between even perfect numbers and Mersenne primes, this is also an algorithm for finding Mersenne primes.

$$\begin{aligned}
\sigma(m) &= (2^n-1)\,\sigma(q) && \text{(Eq. 54)}\\
\sigma(m) &= (2^n-1)\,(s+q) && (s \text{ is the sum of proper divisors of } q)\\
2^n q &= (2^n-1)\,(s+q) && \text{(Eq. 56)}\\
2^n q &= \big[(2^n-1)s\big] + \big[(2^n-1)q\big] && \text{(distributivity)}\\
2^n q - q + q &= \big[(2^n-1)s\big] + \big[(2^n-1)q\big] && (\pm q)\\
(2^n-1)\,q + q &= \big[(2^n-1)s\big] + \big[(2^n-1)q\big]\\
q &= (2^n-1)s
\end{aligned}$$

★ From the last equation we see that s divides q and $s < q$ (noting that $n > 1$) and hence s is a proper divisor of q. So, from Problem 2 of § 2.6.2 we can conclude that q is prime.
★ Also, from the last equation (noting that $s = 1$; see point 2 of § 2.6.2) we have $(2^n - 1) = q$ which means that $(2^n - 1)$ is also prime.
★ So, from Eq. 55 we get $m = 2^{n-1}q = 2^{n-1}(2^n - 1)$ where $(2^n - 1) \in \mathbb{P}$, as required.
Note: from the "only if" part of this Problem plus part (c) of Problem 12 of § 2.2 we conclude that any even perfect number has the form $2^{p-1}(2^p - 1)$ where $p \in \mathbb{P}$.

3. Show the following:
(**a**) If $(2^n - 1)$ is a Mersenne prime then $2^{n-1}(2^n - 1)$ is an even perfect number.
(**b**) If m is an even perfect number then there is a Mersenne prime $(2^n - 1)$ such that $m = 2^{n-1}(2^n - 1)$.
(**c**) There is a one-to-one correspondence between Mersenne primes and even perfect numbers, i.e. for each Mersenne prime there is exactly one even perfect number and for each even perfect number there is exactly one Mersenne prime.
(**d**) If M_p is a Mersenne prime then $M_p(M_p + 1)/2$ is an even perfect number.
(**e**) If M_p is a Mersenne prime then $\sum_{k=1}^{M_p} k$ is an even perfect number.
Solution:
(**a**) This is just a re-statement of the "if part" of the proposition of Problem 2 considering the definition of Mersenne prime.
(**b**) This is just a re-statement of the "only if part" of the proposition of Problem 2 considering the definition of Mersenne prime.
(**c**) This is just a combination of the results of part (a) and part (b).
(**d**) From the definition of Mersenne prime we have $M_p = 2^p - 1$, and hence:

$$\frac{1}{2}M_p(M_p+1) = \frac{1}{2}(2^p-1)(2^p-1+1) = 2^{p-1}(2^p-1)$$

which is an even perfect number (see Problem 2).
(**e**) From the identity of Eq. 15 we have:

$$\sum_{k=1}^{M_p} k = \frac{1}{2}M_p(M_p+1)$$

which is an even perfect number according to part (d).

4. Show that any even perfect number (except 6) is the sum of consecutive odd cubes.
Solution: Any even perfect number has the form $2^{p-1}(2^p - 1)$ (see the note of Problem 2). Now, p is prime and hence it is odd (noting the exception of 6), and thus $(p - 1)$ is even. So, let $p = 2k + 1$ and hence $p - 1 = 2k$ (for some $k \in \mathbb{N}$). Accordingly:

$$2^{p-1}(2^p-1) = 2^{2k}(2^{2k+1}-1) = (2^k)^2\Big[2\times(2^k)^2-1\Big] = n^2(2n^2-1) = 1^3+3^3+\cdots+(2n-1)^3$$

where $n = 2^k$ and we used the identity of Eq. 20 in the last equality.
Note: for example:

$$28 = 1^3+3^3 \qquad 8128 = 1^3+3^3+\cdots+15^3 \qquad 33550336 = 1^3+3^3+\cdots+127^3$$

5. Show that all even perfect numbers end in 6 or 8.
   Solution: Any even perfect number has the form $2^{p-1}(2^p-1)$ (see the note of Problem 2). Now, the even perfect numbers corresponding to $p=2$ and $p=3$ are 6 and 28 and hence they end in 6 and 8. For $p>3$ we note that all $p>3$ are odd and hence $(p-1)$ is even. So, 2^{p-1} ends either in 6 or 4 (see Problem 6 of § 1.8) and correspondingly (2^p-1) ends either in 1 or 7.[104] Therefore, their product must end in 6 (since $6\times 1=6$) or 8 (since $4\times 7=28$).
6. Show that if n is a perfect number then $\sum_{d|n}\frac{d}{n}=\sum_{d|n}\frac{1}{d}=2$ where d represents the positive divisors of n (including 1 and n).
   Solution: We have:

$$\begin{aligned}
&\sigma(n)=2n && \text{(see point 2 in the preamble)}\\
&\sum_{d|n} d=2n && \text{(Eq. 33)}\\
&\sum_{d|n}\frac{d}{n}=2 && (\div n)\\
&\sum_{d|n}\frac{1}{d}=2 && \text{(see part c of Problem 19 of § 1.9)}
\end{aligned}$$

7. Show that no perfect number is a perfect square.
   Solution: Let $n\in\mathbb{N}$ be a perfect square. Now, we have two cases:
   • n is odd: if n is a perfect square then the number of its positive divisors is odd (see Problem 18 of § 1.9 and Problem 3 of § 2.6.3) and hence the number of its proper divisors is even. Therefore, $s(n)$ is even (see rule 4 of § 1.8 noting that all the proper divisors of n must be odd since no odd number is divisible by an even number according to rule 7 of § 1.8) and hence it cannot be equal to n which is odd (see point 3 in the preamble).
   • n is even: if n is a perfect number then we must have $n=2^{p-1}(2^p-1)$ where (2^p-1) is prime (see Problem 2). Now, if n is also a perfect square then $\sqrt{n}=\sqrt{2^{p-1}}\sqrt{(2^p-1)}$ must be an integer which is impossible because (2^p-1) is prime and hence $\sqrt{(2^p-1)}$ is irrational (see Problem 9 of § 2.2) noting that for $p>2$ the square root $\sqrt{2^{p-1}}$ is an integer because $\sqrt{2^{p-1}}=\sqrt{2^{2k}}=2^k$ $(k\in\mathbb{N})$ while for $p=2$ we have $\sqrt{n}=\sqrt{6}$ which is obviously not an integer.

2.9 Interesting Theorems in Number Theory

We discuss in this section some interesting and commonly used theorems in number theory.

2.9.1 Wilson's Theorem

According to this theorem, an integer $p>1$ is prime *iff* $(p-1)!+1\overset{p}{=}0$.

Problems

1. Prove Wilson's Theorem.
   Solution: For $p=2$ and $p=3$ the statement is obviously true, i.e. 2 and 3 are primes and we have $(2-1)!+1=2\overset{2}{=}0$ and $(3-1)!+1=3\overset{3}{=}0$ and hence the two parts of the *iff* statement are true. So, in the following we consider only $p>3$ (noting that all primes are odd except 2; see point 3 of § 2.2).
   The if part: if $(m-1)!+1\overset{m}{=}0$ where m is composite then $m=cd$ (where c,d are integers such that $1<c,d<m$) and hence c must divide both $(m-1)!$ and $(m-1)!+1$.[105] Therefore, c must divide their difference which is 1 (see rule 14 of § 1.9). Thus, c must be 1 which is a contradiction. Therefore,

[104] We note that $2^p=2\times 2^{p-1}$ and hence 2^p ends in 2 when 2^{p-1} ends in 6 while 2^p ends in 8 when 2^{p-1} ends in 4 (see rule 21 of § 1.8). Accordingly, (2^p-1) ends in 1 and 7 respectively.

[105] c must divide $(m-1)!$ because $1<c<m$ (see rule 46 of § 1.9), and c must divide $(m-1)!+1$ because $(m-1)!+1\overset{m}{=}0$ which means $(m-1)!+1=km=kcd=c(kd)$ for some $k\in\mathbb{N}$.

m cannot be composite, i.e. it must be prime.
The only if part: we note first that all the numbers in the set $S = \{1, 2, \ldots, (p-1)\}$ are coprime to p because p is prime (and hence its only divisors are 1 and p). So, each number in S must have a modular inverse modulo p in S (see part h of Problem 2 of § 2.7.1). Now, from part (f) of Problem 2 of § 2.7.1 we know that 1 and $(p-1)$ are the only members of S which are their own inverse, so if we exclude them then we have the set $S' = \{2, \ldots, (p-2)\}$ where each number m in S' must have a modular inverse m^* (in S') which is different from m. Noting that S' contains an even number of elements (because p is odd) and the modular inverse exists and is unique (according to parts a and b of Problem 2 of § 2.7.1),[106] we can couple each element m_i in S' to its existing and unique inverse m_i^* and hence we form the following modular relations (see Eq. 52):

$$m_i m_i^* \overset{p}{=} 1 \qquad \left(i = 1, \ldots, \frac{p-3}{2}\right)$$

On multiplying these modular relations side by side (rule 10 of § 2.7) we get:

$$\prod_{i=1}^{(p-3)/2} m_i m_i^* = 2 \times \cdots \times (p-2) \overset{p}{=} 1$$

On multiplying the two sides of the last equation by $1 \times (p-1)$ (see rule 6 of § 2.7) we get:

$$\begin{aligned} 1 \times 2 \times \cdots \times (p-2) \times (p-1) &\overset{p}{=} 1 \times (p-1) \\ (p-1)! &\overset{p}{=} p-1 \\ (p-1)! &\overset{p}{=} -1 && (p-1 \overset{p}{=} -1) \\ (p-1)! + 1 &\overset{p}{=} 0 && \text{(rule 3 of § 2.7)} \end{aligned}$$

as required.

2. Find the remainder $r \in \mathbb{N}^0$ for the following divisions:
(**a**) $49! \div 53$. (**b**) $59! \div 61$. (**c**) $73! \div 67$.
Solution: The remainder $r \in \mathbb{N}^0$ of the division $a \div b$ $(a, b \in \mathbb{N})$ is the same as the residue r in the congruence equation $a \overset{b}{=} r$ where $0 \leq r < b$.
(**a**) According to Wilson's theorem $52! \overset{53}{=} -1$ and hence $(52)(51)(50)\,49! \overset{53}{=} -1$. Now, $52 \overset{53}{=} -1$, $51 \overset{53}{=} -2$ and $50 \overset{53}{=} -3$ and hence from the congruence equation $(52)(51)(50)\,49! \overset{53}{=} -1$ we get:

$$(-1)(-2)(-3)\,49! \overset{53}{=} -1 \quad \rightarrow \quad (-6)\,49! \overset{53}{=} -1 \quad \rightarrow \quad (6)\,49! \overset{53}{=} 1 \quad \rightarrow \quad 49! \overset{53}{=} 6^*$$

where we used rule 6 of § 2.7 in step 3 and rule 4 of § 2.7.1 in step 4. Now, the modular multiplicative inverse of 6 (mod 53) is $6^* = 9$ and hence $49! \overset{53}{=} 9$, i.e. $r = 9$.
(**b**) According to Wilson's theorem $60! \overset{61}{=} -1$ and hence $(60)\,59! \overset{61}{=} -1$. Now, $60 \overset{61}{=} -1$ and hence from the congruence equation $(60)\,59! \overset{61}{=} -1$ we get:

$$(-1)\,59! \overset{61}{=} -1 \quad \rightarrow \quad (1)\,59! \overset{61}{=} 1 \quad \rightarrow \quad 59! \overset{61}{=} 1$$

i.e. $r = 1$.
(**c**) $73! = (73)(72)(71)(70)(69)(68)(67)\,66!$ and hence it is divisible by 67, i.e. $r = 0$. This can also be obtained directly from rule 46 of § 1.9.

[106] In fact, we are also considering in this argument (implicitly) the symmetry of the inversion relation (see point 5 of § 2.7.1) which makes the uniqueness a bijective relation.

3. Prove the following:
(**a**) $(q!)^2 + (-1)^q$ is divisible by $p \in \mathbb{P}$ where $p = 2q + 1$.
(**b**) There is $n \in \mathbb{Z}$ such that $n^2 + 1$ is divisible by $p \in \mathbb{P}$ where $p = 4q + 1$.
Solution:
(**a**) We have:

$$\begin{aligned}
(2q)! + 1 &\overset{p}{=} 0 && \text{(Wilson's theorem)}\\
\Big[(2q)(2q-1)\cdots(q+1)\Big]\,(q!) + 1 &\overset{p}{=} 0 && \text{(definition of factorial)}\\
\Big[(-1)(-2)\cdots(-q)\Big]\,(q!) + 1 &\overset{p}{=} 0 && (2q \overset{p}{=} -1, 2q-1 \overset{p}{=} -2, \ldots, q+1 \overset{p}{=} -q)\\
\Big[(-1)^q(q!)\Big]\,(q!) + 1 &\overset{p}{=} 0\\
(-1)^q\,(q!)^2 + 1 &\overset{p}{=} 0\\
\left[(-1)^q\right]^2\,(q!)^2 + (-1)^q &\overset{p}{=} 0 && [\times(-1)^q]\\
(q!)^2 + (-1)^q &\overset{p}{=} 0
\end{aligned}$$

(**b**) We have:

$$\begin{aligned}
(4q)! + 1 &\overset{p}{=} 0 && \text{(Wilson's theorem)}\\
\Big[(4q)(4q-1)\cdots(2q+1)\Big]\,(2q)! + 1 &\overset{p}{=} 0 && \text{(definition of factorial)}\\
\Big[(-1)(-2)\cdots(-2q)\Big]\,(2q)! + 1 &\overset{p}{=} 0 && (4q \overset{p}{=} -1, 4q-1 \overset{p}{=} -2, \ldots, 2q+1 \overset{p}{=} -2q)\\
\Big[(-1)^{2q}(2q)!\Big]\,(2q)! + 1 &\overset{p}{=} 0\\
\Big[(1)(2q)!\Big]\,(2q)! + 1 &\overset{p}{=} 0 && (2q \text{ is even})\\
\Big[(2q)!\Big]^2 + 1 &\overset{p}{=} 0\\
n^2 + 1 &\overset{p}{=} 0 && \big[\mathbb{Z} \ni n = (2q)!\big]
\end{aligned}$$

2.9.2 Euler's Theorem

According to this theorem, if $m \in \mathbb{N}$ and $\mathbb{N} \ni k > 1$ are coprime then $m^{\phi(k)} \overset{k}{=} 1$.[107]

Problems

1. Prove Euler's Theorem.
Solution: If the set of integers $S = \{n_1, n_2, \ldots, n_{\phi(k)}\}$ is a reduced residue system modulo k (see § 2.7.2) then the set $S_s = \{mn_1, mn_2, \ldots, mn_{\phi(k)}\}$ is another reduced residue system modulo k (see part e of Problem 6 of § 2.7.2 noting that m and k are coprime). Accordingly, we can form $\phi(k)$ congruence equations in each of which one element of S_s is equated (modular k) to one element of S uniquely. Now, if we multiply these $\phi(k)$ congruent relations side by side (according to rule 10 of § 2.7) we get:

$$\begin{aligned}
mn_1 \times mn_2 \times \ldots \times mn_{\phi(k)} &\overset{k}{=} n_1 \times n_2 \times \ldots \times n_{\phi(k)}\\
m^{\phi(k)} n_1 n_2 \ldots n_{\phi(k)} &\overset{k}{=} n_1 n_2 \ldots n_{\phi(k)} \qquad (57)
\end{aligned}$$

Now, S is a reduced residue system (mod k) and hence by definition all its elements are coprime to k (see § 2.7.2). Therefore, $(n_1 n_2 \ldots n_{\phi(k)})$ and k are coprime (see part e of Problem 1 of § 2.2). Thus, by rule 7 of § 2.7 we can cancel $(n_1 n_2 \ldots n_{\phi(k)})$ from the two sides of Eq. 57 and hence we get $m^{\phi(k)} \overset{k}{=} 1$ (as required).

[107] We note that $\phi(n)$ is even for all integers greater than 2 (see point 5 of § 2.6.4) and hence this theorem should be valid for all $\mathbb{Z} \ni m \neq 0$ [noting that $m^{\phi(2)} \overset{2}{=} 1$ since m is odd when m and 2 are coprime].

2. What is the remainder R when:
   (**a**) $\Sigma_{i=0}^{368} 2^i$ is divided by 61. (**b**) $2\sum_{i=0}^{123} 3^i$ is divided by 29.
   Solution:
   (**a**) We have:

$$\begin{aligned}
2^{\phi(61)} &\overset{61}{\equiv} 1 && \text{(Euler's theorem)}\\
2^{60} &\overset{61}{\equiv} 1 && \left[\phi(61) = 60\right]\\
2^{360} &\overset{61}{\equiv} 1^6 && \text{(rule 11 of § 2.7)}\\
2^{369} &\overset{61}{\equiv} 2^9 && (\times 2^9;\ \text{rule 6 of § 2.7})\\
2^{369} - 1 &\overset{61}{\equiv} 2^9 - 1 && \text{(rule 3 of § 2.7)}\\
\sum_{i=0}^{368} 2^i &\overset{61}{\equiv} 2^9 - 1 && \text{(Eq. 22 with } a = 1,\ r = 2, \text{ and } n = 368)\\
\sum_{i=0}^{368} 2^i &\overset{61}{\equiv} 23 && (2^9 - 1 \overset{61}{\equiv} 23)
\end{aligned}$$

   Hence, $R = 23$.
   (**b**) We have:

$$\begin{aligned}
3^{\phi(29)} &\overset{29}{\equiv} 1 && \text{(Euler's theorem)}\\
3^{28} &\overset{29}{\equiv} 1 && \left[\phi(29) = 28\right]\\
3^{112} &\overset{29}{\equiv} 1^4 && \text{(rule 11 of § 2.7)}\\
3^{124} &\overset{29}{\equiv} 3^{12} && (\times 3^{12};\ \text{rule 6 of § 2.7})\\
3^{124} - 1 &\overset{29}{\equiv} 3^{12} - 1 && \text{(rule 3 of § 2.7)}\\
2\sum_{i=0}^{123} 3^i &\overset{29}{\equiv} 3^{12} - 1 && \text{(Eq. 22 with } a = 2,\ r = 3, \text{ and } n = 123)\\
2\sum_{i=0}^{123} 3^i &\overset{29}{\equiv} 15 && (3^{12} - 1 \overset{29}{\equiv} 15)
\end{aligned}$$

   Hence, $R = 15$.
3. Show that if $m \overset{\phi(k)}{\equiv} n$, then $s^m \overset{k}{\equiv} s^n$ (where $\mathbb{N} \ni k > 1$ and $s \in \mathbb{N}$ are coprime).
   Solution: We have (assuming $t \in \mathbb{Z}$ and $m \geq n$ which does not affect the generality):

$$\begin{aligned}
m &\overset{\phi(k)}{\equiv} n && \text{(given)}\\
m - n &= t\,\phi(k) && \text{(definition of congruence, see Eq. 49)}\\
s^{m-n} &= s^{t\phi(k)} && \text{(rules of ordinary exponentiation)}\\
s^{m-n} &= \left[s^{\phi(k)}\right]^t && \text{(rules of ordinary exponentiation)}\\
s^{m-n} &\overset{k}{\equiv} \left[1\right]^t && \text{(Euler's theorem noting the coprimality of } k \text{ and } s)\\
s^{m-n} &\overset{k}{\equiv} 1 && \text{(rules of ordinary exponentiation)}\\
s^m &\overset{k}{\equiv} s^n && \text{(multiplying both sides by } s^n, \text{ rule 6 of § 2.7)}
\end{aligned}$$

4. Prove the following: $2^{(n-1)!} \overset{n}{\equiv} 1$ (where $n > 1$ is odd).
   Solution: The proof is outlined in the following points:

- From point 7 of § 2.6.4 we have: $\phi(n) \leq (n-1)$.
- By rule 46 of § 1.9 we have $(n-1)! = k\,\phi(n)$ where $k \in \mathbb{N}$.
- Accordingly:

$$\begin{aligned}
2^{\phi(n)} &\overset{n}{=} 1 && \text{(Euler's theorem noting that 2 and odd } n \text{ are coprime)}\\
\left[2^{\phi(n)}\right]^k &\overset{n}{=} 1^k && \text{(rule 11 of § 2.7)}\\
2^{k\phi(n)} &\overset{n}{=} 1 && \text{(rules of indices)}\\
2^{(n-1)!} &\overset{n}{=} 1 && \left[(n-1)! = k\,\phi(n)\right]
\end{aligned}$$

5. Show that $a^{(p^n - p^{n-1})} \overset{p^n}{=} 1$ (where $p \in \mathbb{P}$, $a \in \mathbb{N}$, $n \in \mathbb{N}$, and $p \nmid a$).
Solution: From Euler's theorem we have (noting that a and p^n are coprime because $p \nmid a$):

$$a^{\phi(p^n)} \overset{p^n}{=} 1 \qquad \rightarrow \qquad a^{(p^n - p^{n-1})} \overset{p^n}{=} 1$$

where we used Eq. 42 in the last step.

2.9.3 Fermat's Little Theorem

Fermat's little theorem states: if p is a prime and a is an integer then $a^p \overset{p}{=} a$. Equivalently, if $p \nmid a$ then $a^{p-1} \overset{p}{=} 1$ (see the note of Problem 1). It is worth noting that the converse of Fermat's little theorem is not true in general. This means that there are composite numbers that satisfy the congruence relation of Fermat's little theorem and these composite numbers ($\mathbb{N} \ni m > 2$ and $m \notin \mathbb{P}$) are called **Carmichael numbers** (i.e. $a^m \overset{m}{=} a$ for all $a \in \mathbb{Z}$, and $a^{m-1} \overset{m}{=} 1$ for all $a \in \mathbb{Z}$ where a and m are coprime).

Problems

1. Prove Fermat's little theorem.
Solution: $a^p \overset{p}{=} a$ means $(a^p - a)$ is divisible by p and this is what we will prove using mathematical induction.[108] For $a = 1$ we have $(1^p - 1) = 0$ which is divisible by p. Now, let assume that $(a^p - a)$ is divisible by p for some $a = n$ and hence we need to show that it is also divisible by p for $a = n + 1$, that is:

$$\begin{aligned}
(n+1)^p - (n+1) &= \left[\sum_{k=0}^{p} C_k^p n^k\right] - (n+1) && \text{(Eq. 13)}\\
&= \left[\sum_{k=1}^{p} C_k^p n^k\right] + 1 - (n+1) && (C_0^p n^0 = 1)\\
&= \left[\sum_{k=1}^{p} C_k^p n^k\right] - n\\
&= \left[\sum_{k=1}^{p-1} C_k^p n^k\right] + (n^p - n) && (C_p^p n^p = n^p)
\end{aligned}$$

Now, all the terms in the sum (inside the square brackets in the last line) are divisible by p because all the binomial coefficients C_k^p contain a factor of p (see Eq. 5 noting that $1 \leq k < p$).[109] Moreover, $(n^p - n)$ is also divisible by p according to our assumption. Hence, their sum (as seen in the last line) must also be divisible by p (see rule 14 of § 1.9). So, by the principle of mathematical induction $(a^p - a)$ is divisible by p for all integers a, i.e. $a^p \overset{p}{=} a$ (as required).

[108] Mathematical induction may suggest the restriction $a \in \mathbb{N}$. However, this is not the case.

[109] We should remember that $C_k^p = \frac{p \times (p-1) \times \cdots \times (p-k+1)}{k!}$ is an integer (see rule 26 of § 1.8) and $k!$ (for $1 \leq k < p$) cannot contain a factor of p that cancels the factor of p in the numerator. So in brief, $C_k^p = tp$ ($1 \leq k < p$ and $t \in \mathbb{N}$).

Note: according to Euler's theorem (see § 2.9.2) we have $m^{\phi(k)} \overset{k}{=} 1$ (where m and k are coprime). We also have $\phi(p) = (p-1)$ where $p \in \mathbb{P}$ (see point 2 of § 2.6.4). So, if k is prime and we replace $\phi(k)$ in Euler's theorem by $(p-1)$ and k by p (noting that m and k are coprime) we get $m^{p-1} \overset{p}{=} 1$ $(p \not| m)$ which is Fermat's little theorem (with $a \equiv m \in \mathbb{N}$). This means that Fermat's little theorem is a special case of Euler's theorem (corresponding to $k \equiv p \in \mathbb{P}$, $a \equiv m \in \mathbb{N}$ and $p \not| m$).[110]

2. Find 7^{3333} mod 13.
Solution: From Fermat's little theorem we have $7^{12} \overset{13}{=} 1$ and hence $\left(7^{12}\right)^m \overset{13}{=} 1$ for all $m \in \mathbb{N}$ (see rule 11 of § 2.7). Therefore:

$$7^{3333} = 7^{(12\times 277)+9} = 7^{(12\times 277)} \times 7^9 = \left(7^{12}\right)^{277} \times 7^9 \overset{13}{=} 1 \times 7^9 = 40353607 \overset{13}{=} 8$$

3. Show the following:
(**a**) $a^p \overset{p}{=} a$ and $a^{p-1} \overset{p}{=} 1$ $(p \not| a)$ are equivalent.
(**b**) If $p \in \mathbb{P}$, $a \in \mathbb{Z}$ and $p \not| a$ then a^{p-2} is the modular multiplicative inverse of a (mod p).
Solution:
(**a**) If $a^p \overset{p}{=} a$ and $p \not| a$ then by rule 7 of § 2.7 we can divide both sides of $a^p \overset{p}{=} a$ by a and hence we get $a^{p-1} \overset{p}{=} 1$. On the other hand if $a^{p-1} \overset{p}{=} 1$ then we can multiply both sides by a (using rule 6 of § 2.7) and hence we get $a^p \overset{p}{=} a$.[111]
(**b**) From Fermat's little theorem we have $a^{p-1} \overset{p}{=} 1$ (where $p \not| a$). This can be written as $aa^{p-2} \overset{p}{=} 1$ which shows that a^{p-2} is the modular multiplicative inverse of a (mod p). See § 2.7.1 and Eq. 52 in particular.

4. Find the remainder $r \in \mathbb{N}^0$ for the following divisions:
(**a**) $34^{100} \div 97$. (**b**) $21^{355} \div 173$. (**c**) $52^{119} \div 31$.
Solution: We use Fermat's little theorem noting that the remainder $r \in \mathbb{N}^0$ of the division $a \div b$ $(a, b \in \mathbb{N})$ is the same as the residue r in the congruence equation $a \overset{b}{=} r$ where $0 \leq r < b$.
(**a**) $r = 64$ because:

$$\begin{aligned} 34^{100} &\overset{97}{=} r \\ 34^{97-1} \times 34^4 &\overset{97}{=} r && \text{(rules of indices)} \\ 1 \times 34^4 &\overset{97}{=} r && (a^{p-1} \overset{p}{=} 1, 97 \not| 34) \\ 64 &\overset{97}{=} r && (34^4 \overset{97}{=} 64) \end{aligned}$$

(**b**) $r = 41$ because:

$$\begin{aligned} 21^{355} &\overset{173}{=} r \\ \left(21^{173-1}\right)^2 \times 21^{11} &\overset{173}{=} r && \text{(rules of indices)} \\ 1^2 \times 21^{11} &\overset{173}{=} r && (a^{p-1} \overset{p}{=} 1, 173 \not| 21) \\ 41 &\overset{173}{=} r && (21^{11} \overset{173}{=} 41) \end{aligned}$$

(**c**) $r = 3$ because:

$$52^{119} \overset{31}{=} r$$

[110] In fact, it is a special case but with the restriction $p \not| a$. Moreover, if we consider the condition $m \in \mathbb{N}$ in Euler's theorem and the condition $a \in \mathbb{Z}$ in Fermat's little theorem then Fermat's little theorem should be more general from this perspective.

[111] We note that the condition $p \not| a$ belongs to $a^{p-1} \overset{p}{=} 1$ and hence they are not exactly equivalent. In fact, $a^{p-1} \overset{p}{=} 1$ is a consequence of $a^p \overset{p}{=} a$ when $p \not| a$ (and hence $a^{p-1} \overset{p}{=} 1$ can be seen as a special case or an instance of $a^p \overset{p}{=} a$). So, they are exactly equivalent if we impose the condition $p \not| a$ on both. To be more clear, we argue that obtaining $a^{p-1} \overset{p}{=} 1$ from $a^p \overset{p}{=} a$ by dividing the two sides of $a^p \overset{p}{=} a$ by a (using rule 7 of § 2.7) is justified only when p and a are coprime (which means $p \not| a$; see part k of Problem 1 of § 2.2).

$$\begin{aligned} 52^{119} \times 52 &\overset{31}{=} r52 && \text{(rule 6 of § 2.7)} \\ 52^{120} &\overset{31}{=} r52 && \text{(rules of indices)} \\ \left(52^{31-1}\right)^4 &\overset{31}{=} r52 && \text{(rules of indices)} \\ 1^4 &\overset{31}{=} r52 && (a^{p-1} \overset{p}{=} 1, 31 \not| 52) \\ r52 &\overset{31}{=} 1 \end{aligned}$$

So, r is the modular multiplicative inverse of 52 (mod 31) which is 3, i.e. $r = 3$.

5. Justify the following (where $x \in \mathbb{Z}$ and $p \in \mathbb{P}$):
(**a**) $x^p - x \overset{p}{=} 0$ has p modular solutions (i.e. $x \overset{p}{=} 0, 1, \ldots, p-1$).
(**b**) $x^p - x + 1 \overset{p}{=} 0$ has no modular solution.
(**c**) $x^p \overset{p}{=} 0$ has no modular solution other than 0 (i.e. $x \overset{p}{=} 0$).
Solution:
(**a**) This is a direct result of Fermat's little theorem (i.e. $x^p \overset{p}{=} x$) since this congruence relation is satisfied by all the possible values of x (mod p) which are: $x \overset{p}{=} 0, 1, , p-1$. More formally:

$$\begin{aligned} x^p &\overset{p}{=} x && \text{(Fermat's little theorem, } x \in \mathbb{Z}) \\ x^p - x &\overset{p}{=} 0 && \text{(rule 3 of § 2.7)} \end{aligned}$$

Now, if we note that $x \in \mathbb{Z}$ then we conclude that the congruence equation $x^p - x \overset{p}{=} 0$ is valid for all integers which means that it has p modular solutions (i.e. $x \overset{p}{=} 0, 1, \ldots, p-1$) since these modular classes represent all integers.
(**b**) This can be inferred from part (a) because if $x^p - x \overset{p}{=} 0$ (according to part a) for all possible values of x (mod p) then for any possible value of x we should have (from the congruence of part b considering the congruence of part a) $0 + 1 \overset{p}{=} 0$ which is impossible and hence $x^p - x + 1 \overset{p}{=} 0$ must have no modular solution. More formally:

$$\begin{aligned} x^p - x + 1 &\overset{p}{=} 0 && \text{(given)} \\ 0 + 1 &\overset{p}{=} 0 && \text{(part a)} \\ 1 &\overset{p}{=} 0 \end{aligned}$$

which is nonsensical and hence this congruence equation has no solution.
(**c**) This can be inferred from part (a) since dropping x (i.e. from the congruence of part a) does not affect the congruence only if $x \overset{p}{=} 0$. In a more formal way:

$$\begin{aligned} x^p &\overset{p}{=} 0 && \text{(given)} \\ x^p - (x^p - x) &\overset{p}{=} 0 - 0 && \text{(from part a; also see rule 5 of § 2.7)} \\ x &\overset{p}{=} 0 \end{aligned}$$

6. Show that $(p_1 p_2) | (p_1^{p_2-1} + p_2^{p_1-1} - 1)$ where $p_1, p_2 \in \mathbb{P}$ and $p_1 \neq p_2$.
Solution: p_1 and p_2 are coprime (see part j of Problem 1 of § 2.2) and hence by Fermat's little theorem we have $p_2^{p_1-1} \overset{p_1}{=} 1$. Moreover, it is obvious that $p_1^{p_2-1} \overset{p_1}{=} 0$ (since $p_1^{p_2-1}$ is a multiple of p_1 noting that $p_2 > 1$). On adding these two congruences side by side (see rule 4 of § 2.7) we get:

$$p_1^{p_2-1} + p_2^{p_1-1} \overset{p_1}{=} 1 \qquad \rightarrow \qquad p_1 | (p_1^{p_2-1} + p_2^{p_1-1} - 1)$$

Similarly, p_1 and p_2 are coprime and hence by Fermat's little theorem we have $p_1^{p_2-1} \overset{p_2}{=} 1$. Moreover, it is obvious that $p_2^{p_1-1} \overset{p_2}{=} 0$ (since $p_2^{p_1-1}$ is a multiple of p_2 noting that $p_1 > 1$). On adding these two congruences side by side we get:

$$p_1^{p_2-1} + p_2^{p_1-1} \overset{p_2}{=} 1 \qquad \rightarrow \qquad p_2 | (p_1^{p_2-1} + p_2^{p_1-1} - 1)$$

As we see, $(p_1^{p_2-1}+p_2^{p_1-1}-1)$ is divisible by both p_1 and p_2 and hence it is divisible by their product (see rule 20 of § 1.9), i.e. $(p_1p_2)|(p_1^{p_2-1}+p_2^{p_1-1}-1)$.

7. Show that no Fermat prime F_k (see § 2.2.3) can be expressed as $F_k = s^p - t^p$ where $s,t \in \mathbb{N}$ $(s > t)$ and p is an odd prime.
   Solution: We prove this by contradiction. So, let assume that $F_k = s^p - t^p$ and hence $F_k = (s-t)n$ where $\mathbb{N} \ni n > 1$ (see the identity of Eq. 10). Now, since F_k is prime then $(s-t) = 1$. Also, from Fermat's little theorem we have $s^p \overset{p}{=} s$ and $t^p \overset{p}{=} t$ and hence (see rule 5 of § 2.7):

   $$F_k = s^p - t^p \overset{p}{=} s - t = 1 \qquad \rightarrow \qquad 2^{2^k}+1 \overset{p}{=} 1 \qquad \rightarrow \qquad 2^{2^k} \overset{p}{=} 0$$

   i.e. $p|2^{2^k}$ which is impossible because 2^{2^k} is a natural power of 2 while p is odd and hence they have no common prime factor.
8. State some general known facts about Carmichael numbers.
   Solution: For example:
   - There are infinitely many Carmichael numbers.
   - Carmichael number is square free (see § 2.1).
   - Carmichael number is odd.
   - Carmichael number has at least three prime factors.
   - Every prime factor of Carmichael number n is less than $\sqrt{n}$.
   - The largest known Carmichael number is much bigger than the largest known prime number.
9. Show that all Carmichael numbers are odd.
   Solution: If m is a Carmichael number then we must have $a^m \overset{m}{=} a$ for all $a \in \mathbb{Z}$. So, let $a = (m-1)$ and hence we have:

   $$\begin{aligned} (m-1)^m &\overset{m}{=} m-1 && \text{(given)} \\ (-1)^m &\overset{m}{=} -1 && (m-1 \overset{m}{=} -1) \end{aligned}$$

   This congruence relation is true only if m is odd (noting that $m > 2$)[112] and hence m must be odd.
   Note: noting that all the primes greater than 2 are odd we can see that the relation $a^m \overset{m}{=} a$ (for all $a \in \mathbb{Z}$) applies only for odd $m > 2$ (i.e. whether m is prime or not).[113] In fact, there is no reference in the above proof to the composity of m.

2.9.4 Lagrange's Polynomial Roots Theorem

According to this theorem, if $f(x)$ is a polynomial of degree $n \in \mathbb{N}$ with integer coefficients then $f(x) \overset{p}{=} 0$ has at most n distinct roots (where $x \in \mathbb{Z}$ and $p \in \mathbb{P}$).[114] It is noteworthy that this theorem is stated and conditioned in the literature in many different ways. For example, some impose the condition that the coefficients are not divisible by p (or being coprime to p). However, this condition does not affect the statement of the theorem although it may affect the form of the polynomial or its degree (noting that the terms with coefficients divisible by p can be canceled without affecting the congruence equation). Yes, we may need to impose the condition that not all the coefficients are divisible by p because otherwise the congruence equation will be satisfied by any integer since it can be written as $p\big[f'(x)\big] \overset{p}{=} 0$ which is satisfied by any $x \in \mathbb{Z}$.[115] Also, some impose the condition that $n \leq p$ which is an issue that we will discuss briefly later on (see the note of Problem 2).

Problems

1. Prove Lagrange's polynomial roots theorem.
   Solution: We use induction. So, let $f(x) = ax + b$ be a linear polynomial in its simple form (i.e. all

[112] If m is odd then we have $-1 \overset{m}{=} -1$ which is true identically, while If m is even then we have $1 \overset{m}{=} -1$ which is true only if $m = 2$ since $m \nmid (1-[-1]) = 2$ if $m > 2$.

[113] This does not mean it applies to every odd $m > 2$, but it means when it applies then m is odd > 2.

[114] We refer the reader to point 9 of § 2.7.6.

[115] This means that this congruence equation has p modular solutions, i.e. it is an identity valid for all $x \in \mathbb{Z}$. We should also note that $p\big[f'(x)\big] = f(x)$, i.e. the prime does not mean derivative.

the terms congruent to p are canceled and hence a and p are coprime). Now, let assume that $f(x)$ has two solutions x_1 and x_2 (mod p) and hence we have:

$$\begin{aligned} ax_1 + b \overset{p}{=} ax_2 + b \overset{p}{=} 0 \quad & \text{(given)} \\ ax_1 \overset{p}{=} ax_2 \quad & \text{(rule 3 of § 2.7)} \\ x_1 \overset{p}{=} x_2 \quad & \text{(rule 7 of § 2.7 noting that } a \text{ and } p \text{ are coprime)} \end{aligned}$$

This means that the two solutions are identical (mod p) and hence we actually have only one (modular) solution. So, the statement of the theorem is true for $n = 1$ (i.e. a polynomial with $n = 1$ has at most one solution mod p).

Now, let assume that the statement of this theorem is true for some $n \in \mathbb{N}$ and hence we need to show (based on this assumption) that the statement is also true for $n + 1$. So, let assume that $f(x)$ is a polynomial of degree $n+1$. Now, if $f(x)$ has no root at all then that is it, while if it has any root then (from algebra) the polynomial can be factored as $(x - x_1)Q(x)$ where $Q(x)$ is a polynomial of degree n and x_1 is a root of $f(x)$. So, we have $(x-x_1)Q(x) \overset{p}{=} 0$ which is equivalent to $p|(x-x_1)Q(x)$, and hence by rule 22 of § 1.9 we must have $p|(x-x_1)$ or $p|Q(x)$.[116] Now, $p|(x-x_1)$ is equivalent to $(x-x_1) \overset{p}{=} 0$ (which we already proved that it has at most one root), and $p|Q(x)$ is equivalent to $Q(x) \overset{p}{=} 0$ (which by the induction assumption has at most n roots), and hence we must have at most $n+1$ roots, i.e. the roots of $Q(x) \overset{p}{=} 0$ plus the root of $(x - x_1) \overset{p}{=} 0$.

So, we proved that the statement is true for $n = 1$, and if it is true for n then it is true for $n + 1$. Hence, by the principle of mathematical induction (see § 1.5.4) the statement is true for all $n \in \mathbb{N}$ (as required).

2. Determine the number of roots of the following polynomial congruence equations and comment:

(**a**) $x^3 - x \overset{3}{=} 0$. (**b**) $6x^4 - 2x^2 + 22 \overset{5}{=} 0$. (**c**) $x^5 - 3x^3 + 7x - 4 \overset{7}{=} 0$.

(**d**) $4x^2 + 8x \overset{12}{=} 0$. (**e**) $10x^7 + 13x^6 - x^3 - 15 \overset{11}{=} 0$. (**f**) $x^{15} - x^3 \overset{3}{=} 0$.

Solution:

(**a**) This has 3 roots (i.e. $x \overset{3}{=} 0$,1,2). This is consistent with Lagrange's polynomial roots theorem.

(**b**) This has 2 roots (i.e. $x \overset{5}{=} 2, 3$). This is consistent with Lagrange's theorem.

(**c**) This has no root. This is consistent with Lagrange's theorem.

(**d**) This has 8 roots (i.e. $x \overset{12}{=} 0, 1, 3, 4, 6, 7, 9, 10$). This seems inconsistent with Lagrange's theorem but we should note that 12 is composite.

(**e**) This has 1 root only (i.e. $x \overset{11}{=} 10$). This is consistent with Lagrange's theorem.

(**f**) This has 3 roots (i.e. $x \overset{3}{=} 0, 1, 2$). This is consistent with Lagrange's theorem.

Note: the observant reader should have noticed that part (f) is different from the other parts by having $p < n$ which is an interesting case. It should be obvious that if $p < n$ then the maximum number of possible distinct solutions (mod p) cannot exceed p, i.e. the number of solutions is $\leq p$. Accordingly, we can restate Lagrange's theorem as follows: if $f(x)$ is a polynomial of degree $n \in \mathbb{N}$ with integer coefficients then $f(x) \overset{p}{=} 0$ has at most m distinct roots where m is the lowest of n and p. This condition may also be imposed by other ways.

3. Use Lagrange's polynomial roots theorem to "prove" Wilson's theorem (for $p > 2$; see § 2.9.1).

Solution: We start by noting that according to Fermat's little theorem (see § 2.9.3) we have $x^{p-1} \overset{p}{=} 1$ (where $p \not| x$) which we write as $x^{p-1} - 1 \overset{p}{=} 0$ (see rule 3 of § 2.7). Now, $p \not| x$ for $x \overset{p}{=} 1, 2, \ldots, p-1$ and hence the congruence equation $x^{p-1} - 1 \overset{p}{=} 0$ has $(p-1)$ solutions since it is satisfied by all these $(p-1)$ values of x. Also, according to Lagrange's polynomial roots theorem the equation $x^{p-1} - 1 \overset{p}{=} 0$ has at most $(p-1)$ solutions. So, by combining these facts we conclude that $x^{p-1} - 1 \overset{p}{=} 0$ has exactly $(p-1)$

[116] In modular arithmetic, being divisible by p and being congruent to 0 (modulo p) are equivalent (see Eq. 49).

solutions which are $x \stackrel{p}{=} 1, 2, \ldots, p-1$. Accordingly, we get the following congruence *identity*:

$$x^{p-1} - 1 \stackrel{p}{=} (x-1)(x-2)\cdots(x-p+1) = (-1)^{p-1}(1-x)(2-x)\cdots(p-1-x)$$

Now, if we put $x \stackrel{p}{=} 0$ in this congruence *identity* [noting that $(-1)^{p-1} = 1$ since $p > 2$ is odd and considering that this congruence *identity* is valid for all $x \in \mathbb{Z}$ including $x \stackrel{p}{=} 0$][117] we get $(p-1)! \stackrel{p}{=} -1$ which is Wilson's theorem.

Note 1: as indicated, this is not a proof of the entire content of Wilson's theorem since Wilson's theorem (as stated in § 2.9.1) has more content (noting for instance that Wilson's theorem is an *iff* statement and hence it has two parts). However, the proof may be elaborated further to include at least some of the remaining content of Wilson's theorem.

Note 2: an important result that we obtained already (as a byproduct of this Problem) is that the congruence equation $x^{p-1} - 1 \stackrel{p}{=} 0$ has exactly $(p-1)$ solutions which are $x \stackrel{p}{=} 1, 2, \ldots, p-1$.

2.9.5 Other Interesting Theorems

There are other interesting theorems which are used less in this book than the previous theorems (and some may not even be used at least in this volume) and hence we list them here for casual reference and general knowledge:

1. **Fermat's last theorem**: no natural numbers a, b, c satisfy the equation $a^n + b^n = c^n$ for any $n \in \mathbb{N}$ greater than 2.
2. **Dirichlet's theorem**: for any two coprime numbers $m, n \in \mathbb{N}$ there are infinitely many primes of the form $mk + n$ (where $k \in \mathbb{N}$).[118]
3. **Diophantus identity theorem**: if $m, n \in \mathbb{N}$ are each the sum of two squares then $m \times n$ is the sum of two squares.
4. **Two square theorem 1 (Fermat)**: a prime $p > 2$ can be expressed as a sum of two squares *iff* $p = 4k + 1$ for some $k \in \mathbb{N}$.
5. **Two square theorem 2 (Jacobi)**: $N_n = 4(N_{d1} - N_{d3})$ where N_n is the number of representations of $n \in \mathbb{N}$ as the sum of two squares, and N_{d1} (N_{d3}) is the number of divisors of n congruent to 1 (3) modulo 4.
6. **Two square theorem 3**: a natural number n is the sum of 2 squares *iff* every prime of the form $4k + 3$ occurs an even number of times in the prime factorization of n.
7. **Three square theorem (Legendre)**: a number $n \in \mathbb{N}$ can be expressed as a sum of three squares *iff* $n \neq 4^m(8k + 7)$ where $m, k \in \mathbb{N}^0$.
8. **Four square theorem** (**Lagrange**): any natural number can be expressed as a sum of four (non-negative integer) squares. This theorem may also be stated as: any natural number is the sum of at most four squares of positive integers. Each one of these versions has some implications which are missing from the other version and hence it is stronger (or is more specific or has more content) from certain aspects. There are other versions in the literature which differ slightly from these versions.
9. **Four square theorem (Jacobi)**: the number of ways of representing a number $n \in \mathbb{N}$ as the sum of four squares equals eight times the sum of the divisors of n which are not divisible by 4.

Problems

1. Outline the proof of Diophantus identity theorem.
   Solution: If we express m and n as sums of two squares (e.g. $m = a^2 + b^2$ and $n = c^2 + d^2$) and multiply them then their product $m \times n$ can be expressed (with some basic algebraic manipulation) as a sum of two squares.

[117] We note that the solutions of $x^{p-1} - 1 \stackrel{p}{=} 0$ and the validity domain of this congruence *identity* are different issues.

[118] It is important to note that this theorem is about the existence of infinitely many primes of a certain form and hence it does not mean that a number is prime if it is of that form. For example, there are infinitely many primes of the form $4k + 3$ (like 7, 11 and 19 corresponding to $k = 1$, $k = 2$ and $k = 4$) but this does not mean that every number of this form is prime, e.g. 15 and 27 are of this form (corresponding to $k = 3$ and $k = 6$) but they are not prime. A similar note should apply to similar theorems.

2. Based on the proposition of Diophantus identity theorem, express the products of the following pairs of natural numbers as sums of two squares.
   (**a**) $m = 5$ and $n = 8$. (**b**) $m = 8$ and $n = 10$. (**c**) $m = 13$ and $n = 17$.
   Solution:
   (**a**) $5 \times 8 = (1^2 + 2^2) \times (2^2 + 2^2) = 40 = 2^2 + 6^2$
   (**b**) $8 \times 10 = (2^2 + 2^2) \times (1^2 + 3^2) = 80 = 4^2 + 8^2$
   (**c**) $13 \times 17 = (2^2 + 3^2) \times (1^2 + 4^2) = 221 = 5^2 + 14^2 = 10^2 + 11^2$

3. Show that there are infinitely many prime numbers of the following forms (where $n, s, t \in \mathbb{N}$):
   (**a**) $5n + 11$. (**b**) $33n + 2^s$. (**c**) $13^s n + 42$. (**d**) $25^s n + 63^t$.
   Solution: All these are justified by the Dirichlet theorem (see point 2 in the preamble).

Chapter 3
Univariate Equations and Systems

In this chapter we investigate univariate equations in number theory (and how they are solved) whether these are single univariate equations or systems of such equations. In fact, our investigation is largely on congruence equations although we will also discuss (rather briefly) ordinary equations.

3.1 Ordinary Equations

Ordinary equations (as opposite to congruence equations) in number theory are supposed to have domain and range in the set of integers or some of its subsets such as natural numbers. In fact, these equations are mostly polynomial equations with integer coefficients and integer solutions (which we may label as ordinary integer polynomial equations). In the following subsections we investigate several types of univariate ordinary equations related to number theory and present a number of methods and techniques that we use in their solution.

3.1.1 Polynomial Equations

In this subsection we demonstrate how to solve univariate ordinary polynomial equations by giving some simple examples.

Problems

1. Outline the method of solving an ordinary integer polynomial equation by the use of representation of integers.
   Solution: In this method we treat the variable as an unknown base that to be found by using the technique of conversion from one base system to another base system which we outlined in § 1.6. The method is illustrated in the next Problem. However, we should note that this method is very limited in application. For example, it is limited to small non-negative coefficients (< 10) and to non-negative roots.
2. Solve the following equations for $n \in \mathbb{N}$:
   (**a**) $3n^4 + 9n^3 + 6n = 55968$. (**b**) $2n^9 + n^7 + 5n^4 + 2 = 81542764$.
   Solution:
   (**a**) We need to find n such that $(39060)_n = (55968)_{10}$. From the notation of 39060 (i.e. it is smaller than 55968 in decimal) it is obvious that $n > 10$. On trying the few integers just above 10 (using for instance a spreadsheet or a base converter) we get:
   $$(3 \times 11^4) + (9 \times 11^3) + (0 \times 11^2) + (6 \times 11^1) + (0 \times 11^0) = (55968)_{10}$$
   Hence, $n = 11$.
   (**b**) We need to find n such that $(2010050002)_n = (81542764)_{10}$. From the notation of 2010050002 (i.e. it is larger than 81542764 in decimal) it is obvious that $n < 10$. On trying the few integers just below 10 (using for instance a spreadsheet or a base converter) we get:
   $$(2 \times 7^9) + (1 \times 7^7) + (5 \times 7^4) + (2 \times 7^0) = (81542764)_{10}$$
   Hence, $n = 7$.
3. Solve the following ordinary polynomial equations for $n \in \mathbb{Z}$:
   (**a**) $n^5 + 12n^4 - 7n^3 - 12n + 17 = 0$. (**b**) $2n^7 - 3n^5 + 8n^3 - n^2 + 3n + 234 = 0$.
   (**c**) $2n^5 - 15n^4 - 135n^3 - 125n^2 + 273n = 0$. (**d**) $n^8 - 256 = 0$.

Solution:
(**a**) According to the rules of parity (see § 1.8), this polynomial is always odd and hence it cannot be equal to 0 (which is even). Hence, this equation has no integer solution.
(**b**) The leading term $2n^7$ becomes much bigger in magnitude than the sum of the other terms when we move just a few integer values to the left or right of 0. This means (noting that n^7 is an odd power) that the polynomial will be negative for all integer values to the left of 0 (except possibly for a few values in the neighborhood of 0) and will be positive for all integer values to the right of 0 (except possibly for a few values in the neighborhood of 0). Accordingly, if this polynomial is equal to 0 for any $n \in \mathbb{Z}$ then this can happen only in the neighborhood of 0. So, all we need to do is to test the few integer values in the neighborhood of 0 to see if any one of these values satisfies this polynomial equation (noting that we stop our search when the polynomial becomes increasingly negative to the left and increasingly positive to the right). On doing this with (say) $n = 0, -1, 1, -2, 2, -3, 3, -4, 4$ we find that only $n = -2$ satisfies this equation. So, the only integer solution to this polynomial equation is $n = -2$.
It is worth noting that to be absolutely certain that there is no other solution, we can divide $(2n^7 - 3n^5 + 8n^3 - n^2 + 3n + 234)$ by $(n + 2)$ to obtain $(2n^6 - 4n^5 + 5n^4 - 10n^3 + 28n^2 - 57n + 117)$ which is always odd (see the rules of parity in § 1.8) and hence it cannot be equal to zero. This confirms that $n = -2$ is the only possible solution.
(**c**) $n = 0$ is an obvious solution. So, all we need is to find the solutions (if any) of $2n^4 - 15n^3 - 135n^2 - 125n + 273 = 0$. As a quartic polynomial with a positive leading term, it should have a parabola-like shape that concaves upwards and hence it should be always positive except possibly in the neighborhood of 0. So, if it vanishes at all then this can happen only in the neighborhood of 0. On testing the few integer values in the neighborhood of 0 we find that $n = -3$ and $n = 1$ are solutions. On dividing $(2n^4 - 15n^3 - 135n^2 - 125n + 273)$ by $(n + 3)(n - 1)$ we get $(2n^2 - 19n - 91)$ which (as a quadratic and hence can be easily solved by the quadratic formula) has two solutions: $n = 13$ and $n = -7/2$ (which is not acceptable). So, we found 5 solutions to the given equation (only 4 of which are acceptable) and hence we do not expect other solutions to this quintic polynomial equation. So in brief, we have only four integer solutions to the given equation which are $n = -3, 0, 1, 13$.
(**d**) We have:

$$n^8 - 256 = (n^4 - 16)(n^4 + 16) = (n^2 - 4)(n^2 + 4)(n^4 + 16) = (n - 2)(n + 2)(n^2 + 4)(n^4 + 16) = 0$$

So, this equation has only two integer solutions which are $n = -2, 2$ (noting that $n^2 + 4 \neq 0$ and $n^4 + 16 \neq 0$ for any $n \in \mathbb{Z}$).

3.1.2 Exponential Equations

In this subsection we demonstrate how to solve univariate ordinary exponential equations by giving some simple examples. We note that we may not keep ourselves strictly within the borders of number theory in the entirety of some of the following Problems.

Problems

1. Solve the following ordinary exponential equations for $n \in \mathbb{Z}$:

(**a**) $(70)3^n - 7^n = 203$.
(**b**) $7^n + 8^n - 860 = 0$.
(**c**) $3^n - (162)3^{-n} - 79 = 0$.
(**d**) $17^n + 23^{-n} = \frac{152882}{289}$.
(**e**) $(33)9^{2n} - (13)5^{3n} = 0$.
(**f**) $a^n + b^n = 0$ $(a, b \in \mathbb{Z})$.
(**g**) $a^n - b^n = 0$ $(a, b \in \mathbb{Z})$.
(**h**) $9^{2n+1} - 9^n = 720$.

Solution:
(**a**) If we write this equation as $(70)3^n = 203 + 7^n$ we can see that no $n \leq 0$ can satisfy this equation because $(70)3^n$ is too small to equal $203 + 7^n$. So, if there is any solution then n must be > 0. Moreover, it is obvious that 7^n increases much faster than 3^n with increasing n (> 0) which means that any possible solution must be in the neighborhood of 0 because after a certain value of n (> 0) the growth of $203 + 7^n$ (due to the growth of 7^n) exceeds the growth of $(70)3^n$ (due to the growth of 3^n which is

enhanced by the constant factor of 70). So in brief, any potential solution $n \in \mathbb{Z}$ must be a positive small integer. On trying different values of positive small n (e.g. by using a spreadsheet) we get two solutions: $n = 1$ and $n = 5$. These are the only possible solutions because after $n = 5$ the expression $203+7^n$ becomes bigger then $(70)3^n$ and it increases much faster than $(70)3^n$ which makes it impossible for $(70)3^n$ to catch up.
(**b**) If this equation has any solution then n must be greater than 0 (because otherwise $7^n + 8^n$ will be too small to equal 860). Now, according to the rules of parity (see § 1.8), the expression $(7^n + 8^n - 860)$ is odd for any $n > 0$ and hence it cannot be equal to 0 which is even. So, this equation has no solution.
(**c**) If we multiply the two sides by 3^n we get $3^{2n} - (79)3^n - 162 = 0$ which is a quadratic equation in 3^n. On solving this quadratic equation (using the quadratic formula) we get:

$$3^n = \frac{79 \pm \sqrt{(-79)^2 - 4(-162)}}{2} \qquad \rightarrow \qquad 3^n = 81 \quad \text{or} \quad 3^n = -2$$

The only acceptable solution is $3^n = 81$ (since $3^n > 0$) and hence $n = 4$.
(**d**) If we multiply both sides by 289 (which is equal to 17^2) we get: $17^{n+2} + (17^2)23^{-n} = 152882$. Now, we have two cases:
• $n > 0$ which is impossible because in this case 17^{n+2} is an integer while $(17^2)23^{-n}$ is a fraction (noting that 17 and 23 are coprime) and hence their sum cannot be equal to to an integer (i.e. 152882).
• $n \leq 0$ which is also impossible if $n < -2$ for the same reason, i.e. 17^{n+2} is a fraction while $(17^2)23^{-n}$ is an integer and hence their sum cannot be equal to the integer 152882.
This means that we have only 3 possible integer values to test (i.e. $n = -2, -1, 0$) since these values make both 17^{n+2} and $(17^2)23^{-n}$ integers. On testing these 3 values we find that only $n = -2$ satisfies this equation. So, we have only one solution to this equation.
(**e**) We have three cases to consider:
• $n = 0$: this is impossible because $33 - 13 \neq 0$.
• $n > 0$: if we write this equation as $(33)9^{2n} = (13)5^{3n}$ then we can see that this equation cannot have a solution because the prime factors of the left hand side are 3 and 11 while the prime factors of the right hand side are 5 and 13 and hence the two sides cannot be equal (noting that if two numbers are equal then they must have the same prime factors due to the uniqueness of prime factorization; see § 2.1).
• $n < 0$: let $m = -n$ and hence:
$(33)9^{2n} - (13)5^{3n} = 0 \quad \rightarrow \quad (33)9^{2n} = (13)5^{3n} \quad \rightarrow \quad \frac{33}{9^{2m}} = \frac{13}{5^{3m}} \quad \rightarrow \quad (33)5^{3m} = (13)9^{2m}$
Again, the prime factors on the left and right hand sides are different (i.e. $3, 5, 11$ on the left and $3, 13$ on the right) and hence the two sides cannot be equal.
So, we have no solution in any one of these three cases and hence the equation has no solution.
(**f**) We have $a^n + b^n = 0$ and hence $a^n = -b^n$. Now, we have five cases to consider:
• $a = b = 0$: the solution is all $n \in \mathbb{N}$ (or $n \in \mathbb{N}^0$).
• $a = 0$ and $b \neq 0$ (or $b = 0$ and $a \neq 0$): there is no solution.
• $ab \neq 0$ and $|a| \neq |b|$: there is no solution.
• $ab \neq 0$ and $a = b$: there is no solution.
• $ab \neq 0$ and $a = -b$: the solution is all odd n.
(**g**) We have $a^n - b^n = 0$ and hence $a^n = b^n$. Now, we have five cases to consider:
• $a = b = 0$: the solution is all $n \in \mathbb{N}$ (or $n \in \mathbb{N}^0$).
• $a = 0$ and $b \neq 0$ (or $b = 0$ and $a \neq 0$): there is no solution.
• $ab \neq 0$ and $|a| \neq |b|$: the only solution is $n = 0$.
• $ab \neq 0$ and $a = b$: the solution is all $n \in \mathbb{Z}$.
• $ab \neq 0$ and $a = -b$: the solution is all even n.
(**h**) If we multiply the two sides by 9^{-2n} we get $(720)9^{-2n} + 9^{-n} - 9 = 0$ which is a quadratic equation in 9^{-n}. On solving this quadratic equation (using the quadratic formula) we get:

$$9^{-n} = \frac{-1 \pm \sqrt{1^2 - 4(720)(-9)}}{2(720)} \qquad \rightarrow \qquad 9^{-n} = 9^{-1} \quad \text{or} \quad 9^{-n} = -\frac{9}{80}$$

The only acceptable solution is $9^{-n} = 9^{-1}$ (since $9^{-n} > 0$) and hence $n = 1$.

3.1.3 Mixed Polynomial-Exponential Equations

In this subsection we demonstrate how to solve univariate ordinary mixed polynomial-exponential equations by giving some simple examples.

Problems

1. Solve the following mixed polynomial-exponential equations (where $n \in \mathbb{N}$):

(**a**) $8n - 5^n + 48828037 = 0$. (**b**) $3^n n + 17n = 2195383060$. (**c**) $2401^n - n^{98} = 0$.

(**d**) $14n^n - 11n^6 - 3n^2 = 4523811$. (**e**) $(2)11^n - 66n^5 - 5n = 51868249152$.

Solution: We note first that some simple Problems like these can be solved (easily and more efficiently) by just trying the first few values of n (using for instance a spreadsheet). However, for the sake of diversity and to demonstrate the application of the rules and principles of number theory we generally use in the following standard methods of number theory (noting that these standard methods are generally needed in tackling more complicated problems of this kind).

(**a**) If we reduce the equation modulo 5 we get: $3n+2 \stackrel{5}{=} 0$ whose solution is $n \stackrel{5}{=} 1$ (see § 2.7). On testing the first few values of $n \stackrel{5}{=} 1$ (i.e. $n = 1, 6, 11, \ldots$) we find that $n = 11$ satisfies the given equation. There is no hope to find another solution because beyond $n = 11$ the term -5^n will dominate making the expression $(8n - 5^n + 48828037)$ increasingly negative.

(**b**) If we reduce the equation modulo 3 we get: $2n \stackrel{3}{=} 1$ whose solution is $n \stackrel{3}{=} 2$ (see § 2.7.1). On testing the first few values of $n \stackrel{3}{=} 2$ (i.e. $n = 2, 5, 8, \ldots$) we find that $n = 17$ satisfies the given equation. There is no hope to find another solution because beyond $n = 17$ the term $3^n n$ will dominate making the expression $(3^n n + 17n)$ increasingly bigger than 2195383060.
We may also follow a different approach by noting that $3^n n + 17n = (3^n + 17)n$ and hence n is a divisor of 2195383060 (and must be a small divisor noting the eventual magnitude of $3^n + 17$ which is another divisor). So, on trying the few small divisors of 2195383060 we get the same answer.

(**c**) We have $2401 = 7^4$ and hence $2401^n - n^{98} = 7^{4n} - n^{98} = 0$, i.e. $7^{4n} = n^{98}$. Considering the prime factorization of n it must be a natural power of 7. This is because the base on the left hand side of the last equation is 7 and so the base on the right hand side must be a natural power of 7. Now, if we take the square root of both sides of $7^{4n} = n^{98}$ we get $7^{2n} = n^{49}$, i.e. $49^n = n^{49}$ which shows that $n = 49$. So, this value is the solution of the given equation (with no other possible value).

(**d**) The left hand side is even (see the rules of parity in § 1.8) while the right hand side is odd and hence this equation has no solution.

(**e**) If we reduce the equation modulo 11 we get: $6n \stackrel{11}{=} 5$ whose solution is $n \stackrel{11}{=} 10$. On testing the first value of $n \stackrel{11}{=} 10$ (i.e. $n = 10$) we find this value satisfies the given equation. There is no other solution because beyond $n = 10$ the term $(2)11^n$ will dominate making the expression $(2)11^n - 66n^5 - 5n$ increasingly bigger than 51868249152.

3.1.4 Equations Involving Fractions

In this subsection we demonstrate how to solve univariate ordinary equations involving fractions by giving some simple examples.

Problems

1. Find all $n \in \mathbb{Z}$ that satisfy the following equations (which involve fractions):

(**a**) $\frac{5n^2-5}{n^2+1} = 4$. (**b**) $\frac{n+13}{n^3-2n^2+5} = 11$. (**c**) $n + 4 = \frac{22}{9-n}$.

(**d**) $n^2 + 5n - 7 = \frac{13}{2n^2-8n-25}$. (**e**) $\frac{30}{n^2} - \frac{73}{n} = 5$. (**f**) $\frac{2}{n-1} + \frac{3}{n+1} = a \quad (a \in \mathbb{Z})$.

Solution:

(**a**) We have $5n^2 - 5 = 4n^2 + 4$, i.e. $n^2 = 9$ and hence $n = \pm 3$.

(**b**) We have $n+13 = 11n^3 - 22n^2 + 55$, i.e. $11n^3 - 22n^2 - n + 42 = 0$. This cubic equation has no integer solution and hence the given equation has no solution in $\mathbb{Z}$.
(**c**) We have $(n+4)(9-n) = 22$, i.e. $n^2 - 5n - 14 = 0$. This quadratic equation has two solutions: $n = -2$ and $n = 7$.
(**d**) The left hand side is an integer and so must be the right hand side. Hence, $(2n^2 - 8n - 25)$ must be a divisor of 13, i.e. ± 1 or ± 13. On equating $(2n^2 - 8n - 25)$ to each one of these 4 divisors and solving for $n \in \mathbb{Z}$, we find that only $(2n^2 - 8n - 25) = -1$ has solutions in $n \in \mathbb{Z}$ which are $n = -2$ and $n = 6$. However, only $n = -2$ is acceptable because it is the only value satisfying the given equation (i.e. it makes the left and right hand sides equal).
(**e**) On multiplying the given equation by n^2 and simplifying we get: $5n^2 + 73n - 30 = 0$ which has only one integer solution, i.e. $n = -15$.
(**f**) We have:

$$\frac{2}{n-1} + \frac{3}{n+1} = \frac{2n+2+3n-3}{(n-1)(n+1)} = \frac{5n-1}{n^2-1} = a$$

Now, since $a \in \mathbb{Z}$ then we must have $|n^2 - 1| \leq |5n - 1|$. On comparing the two sides of this semi-inequality, it is obvious that $|n|$ cannot be greater than 5 (because in this case $n^2 = nn > 5|n|$ with the difference being more than 1 in magnitude).[119] So, $|n^2 - 1| \leq |5n - 1|$ can only be within the range $-5 \leq n \leq 5$. On testing these few values (excluding $n = \pm 1$ because of singularities), we find that only $n = -3, 0, 2, 5$ makes $\frac{5n-1}{n^2-1}$ (and hence $\frac{2}{n-1} + \frac{3}{n+1}$) an integer (corresponding to $a = -2, 1, 3, 1$). So, these are all the $n \in \mathbb{Z}$ that satisfy the given equation.

3.1.5 Equations Involving Series

In this subsection we demonstrate how to solve univariate ordinary equations involving series by giving some simple examples.

Problems

1. Find all $n \in \mathbb{Z}$ $(n \neq 0)$ that make the following series equal to an integer: $\sum_{k=1}^{m} \frac{1}{n^k}$ where $m \in \mathbb{N}$. Also find the value of the series corresponding to these values of n.

   Solution: If we write this series as $\sum_{k=1}^{m} \left(\frac{1}{n}\right)^k$ then we can see that it is a geometric series which adds up to less than 1 (in magnitude) for $|n| \geq 2$. So, if this series is to be equal to an integer then we must have $n = -1$ or $n = +1$ (noting that $n \neq 0$). Now, we have 4 cases:
   • $n = -1$ and m is even and hence the series is alternating (i.e. $-1+1-\cdots$) where each two consecutive terms add up to 0. Accordingly, the series is equal to 0.
   • $n = -1$ and m is odd and hence the series is alternating where each two consecutive terms (except the last) add up to 0. Accordingly, the series is equal to -1 (because the last term is -1 noting that m is odd).
   • $n = +1$ and m is even and hence the series is a sum of m 1's. Accordingly, the series is equal to m.
   • $n = +1$ and m is odd and hence the series is a sum of m 1's. Accordingly, the series is equal to m.
   To sum up, with even m we have $n = -1$ (making the series equal to 0) and $n = +1$ (making the series equal to m), while with odd m we have $n = -1$ (making the series equal to -1) and $n = +1$ (making the series equal to m). So, these are all $n \in \mathbb{Z}$ that make the given series equal to an integer (with the corresponding values of the series).
2. Find all $n \in \mathbb{N}$ that satisfy the following series equations:

   (**a**) $\sum_{k=1}^{n} \big[\cos(k\pi) + 1\big] = n$. (**b**) $\sum_{k=1}^{n} \big[\cos(k\pi) + 1\big] = (n-1)$. (**c**) $\sum_{k=1}^{n} \sin\left(\frac{(2k-1)\pi}{4}\right) = 0$.

   Solution:
   (**a**) The terms of this series are $0, 2, 0, 2, \ldots$ and hence to make the sum of n terms equal to n we need to use the first n terms where n is even. Therefore, $\sum_{k=1}^{n} \big[\cos(k\pi) + 1\big] = n$ for all positive even n (i.e. $n = 2, 4, 6, \ldots$).

[119] We intentionally use this simple (and rather non-rigorous) method of analysis to avoid unnecessary complications noting that more rigorous approach will not affect the result of this analysis.

(**b**) From the analysis of part (a) we can easily conclude that $\sum_{k=1}^{n}\big[\cos(k\pi)+1\big]=(n-1)$ for all positive odd n (i.e. $n=1,3,5,\ldots$). This is because the odd terms are 0 and hence the sum of the first n terms when n is odd is equal to the sum of the first $(n-1)$ terms which is equal to $(n-1)$ since $(n-1)$ is even.[120]

(**c**) The terms of this series are:

$$\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}},-\frac{1}{\sqrt{2}},-\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}},-\frac{1}{\sqrt{2}},-\frac{1}{\sqrt{2}},\ldots$$

As we see, every 4 consecutive terms add up to 0 which means that the sum of the first n terms is equal to 0 when $n=4m$ where $m\in\mathbb{N}$. So, the given series equation is satisfied by all $n=4m$ $(m\in\mathbb{N})$.

3.1.6 Equations Involving Roots

In this subsection we demonstrate how to solve univariate ordinary equations involving roots by giving some simple examples.

Problems

1. Find all $n\in\mathbb{Z}$ that satisfy the following equations (which involve roots):

(**a**) $\sqrt[8]{n}+\sqrt[4]{n}+\sqrt[2]{n}=6651$. (**b**) $\sqrt[3]{n}+n+130=0$. (**c**) $\sqrt[5]{n}-n^3=0$.

(**d**) $n^3-224n^{3/2}+1728=0$. (**e**) $\sqrt[7]{n}+n^3+11n^2+n=199^{31}$. (**f**) $\sqrt[5]{\sqrt[3]{n^2}}=\sqrt[5]{n^4}$.

Solution:

(**a**) Let $m=\sqrt[8]{n}$ $(m\in\mathbb{R})$ and hence the given equation can be written as $m+m^2+m^4=6651$. The solutions of this quartic polynomial equation are $m=9$ and $m\simeq-9.0061$ (with two other complex roots). However, $m\simeq-9.0061$ cannot be a solution because $\sqrt[8]{n}>0$. So, we must have $m=\sqrt[8]{n}=9$ and hence $n=9^8=43046721$ (which is the only possible solution because n must be positive and the sum is equal to a fixed number).

(**b**) We have: $n+130=-\sqrt[3]{n}$ and hence by raising the two sides to power 3 and simplifying we get: $n^3+390n^2+50701n+2197000=0$. The solution of this cubic polynomial equation is $n=-125$ (with two other complex roots). This is the only possible solution because $\sqrt[3]{n}+n$ must be negative and hence n must be negative.

(**c**) We have: $\sqrt[5]{n}=n^3$ and hence by raising the two sides to power 5 and simplifying we get: $n=n^{15}$, i.e. $n^{15}-n=n(n^{14}-1)=0$. The solutions of the last equation are: $n=0,\pm1$. There is no solution other than these 3 solutions.

(**d**) This is a quadratic equation in $n^{3/2}$. So, by the quadratic formula we have:

$$n^{3/2}=\frac{224\pm\sqrt{(-224)^2-4(1728)}}{2}=\frac{224\pm208}{2}$$

i.e. $n^{3/2}=8$ and hence $n=4$, or $n^{3/2}=216$ and hence $n=36$.

(**e**) 199^{31} and (n^3+11n^2+n) are integers (noting that $n\in\mathbb{Z}$), and hence if $(\sqrt[7]{n}+n^3+11n^2+n)$ should be an integer then $\sqrt[7]{n}$ must be an integer. So, let assume that $\sqrt[7]{n}$ is an integer. Now, if $\sqrt[7]{n}$ is odd then n is odd (see rule 10 of § 1.8) and hence n^3+11n^2+n is odd which means that $\sqrt[7]{n}+n^3+11n^2+n$ is even (see the rules of parity in § 1.8), while if $\sqrt[7]{n}$ is even then n is even and hence n^3+11n^2+n is even which means that $\sqrt[7]{n}+n^3+11n^2+n$ is even. So, in both cases the left hand side of the given equation is even and hence it cannot be equal to 199^{31} which is odd. So, there is no solution to this equation.

(**f**) $\sqrt[5]{\sqrt[3]{n^2}}=\sqrt[15]{n^2}=n^{2/15}$ and $\sqrt[5]{n^4}=n^{4/5}$. So, we have $n^{2/15}=n^{4/5}$. Now, if we raise both sides to power $15/2$ we get $n=n^6$ which obviously has 2 solutions: $n=0,1$. However, if we inspect the given equation we can easily see that $n=-1$ is another solution (which we lost when we raised to power $15/2$). In fact, if we have to keep all the solutions of the given equation then we should have raised to

[120] We note that for $n=1$ we consider the sum of 0 terms which is 0.

power 15 instead of 15/2 to get $n^2 = n^{12}$ which preserves all the 3 solutions of the given equation, i.e. $n = 0, \pm 1$. This should highlight an important issue which is the necessity to be careful when we raise to power or take a root which could lead to losing some solutions or introducing new (false) solutions which do not satisfy the original equation.

2. Find all $n \in \mathbb{Z}$ that satisfy the equation $\sqrt[9]{n} + 3n^4 - n^2 + 2n = a$ where $a \in \mathbb{Z}$.
Solution: Since n is an integer then $(3n^4 - n^2 + 2n)$ is an integer (see rule 1 and other general rules in § 1.8). So, if a should be an integer then $\sqrt[9]{n}$ must be an integer. Therefore, the solutions of the given equation are: all integers n which make $\sqrt[9]{n}$ an integer (i.e. all integers n whose ninth roots are integers). In other words, the solutions of the given equation are all $n \in \mathbb{Z}$ of the form $n = b^9$ (where $b \in \mathbb{Z}$).

3.2 Congruence Equations

Solving congruence equations (whether in one variable or in multiple variables) is a big and rather complicated subject and can be more difficult than the subject of solving the corresponding ordinary equations. Therefore, our approaches are mostly practical where we try (through presenting illustrating solved Problems) to enable the reader to guess and capture the theory or method behind the solution of the given Problem. In fact, we will use in our solutions different treatments and approaches depending not only on the type of the problem but also on the availability, applicability and convenience of these treatments and approaches (as well as the level of the book). In the following subsections we investigate solving a number of types of univariate congruence equations.

3.2.1 Polynomial Congruence Equations

There are several methods for solving polynomial congruence equations (assuming they are solvable). In the following Problems and subsections we investigate a number of these methods applied to a number of polynomials of various orders. However, before that we list a number of useful remarks about solving polynomial congruence equations:

• The solutions of linear polynomial congruence equation are determined (in their existence, number and form) by the following theorem (which we label as the **LCE theorem**): if $d = \gcd(a, m)$ then the congruence equation $ax \overset{m}{=} b$ (in the unknown x) has a solution *iff* $d|b$ (where $a, b, m, x \in \mathbb{Z}$ and $m > 1$). Moreover, there are exactly d *modular solutions* (in mod m):

$$x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, \ldots, x_0 + \frac{(d-1)m}{d} \tag{58}$$

and hence all *ordinary solutions* are given by $x_0 + k\frac{m}{d}$ (i.e. $x \overset{m/d}{=} x_0$) where x_0 is a given solution and $k \in \mathbb{Z}$.[121]

• The number of solutions of polynomial congruence equations is subject to Lagrange's polynomial roots theorem which was investigated in § 2.9.4. Hence, it is useful (and important) to keep this theorem in mind when dealing with polynomial congruence equations. However, we should remember that this theorem has several limitations such as the limitation about the modulo (i.e. $p \in \mathbb{P}$) and the limitation about the size of p relative to n (see the note of Problem 2 of § 2.9.4). We should also remember that this theorem is about "at most" and hence it does not guarantee the existence of solution or determine the number of solutions.

Problems

1. Solve the following linear congruence equations (where $n \in \mathbb{Z}$):

(**a**) $33n \overset{5}{=} 6$. (**b**) $69n \overset{17}{=} 23$. (**c**) $59n \overset{30}{=} -88$. (**d**) $55n + 7 \overset{23}{=} 8$.

[121] "Modular solutions" mean distinct solutions in modular arithmetic, while "ordinary solutions" mean solutions in ordinary (non-congruence) arithmetic.

Solution: We use rule 4 of § 2.7.1.
(**a**) The modular multiplicative inverse of 33 (mod 5) is $33^* = 2$. Hence:

$$33n \overset{5}{=} 6 \quad \rightarrow \quad n \overset{5}{=} 6(33^*) \quad \rightarrow \quad n \overset{5}{=} 6(2) \quad \rightarrow \quad n \overset{5}{=} 12 \overset{5}{=} 2 \quad \rightarrow \quad n = 2 + 5k \quad (k \in \mathbb{Z})$$

(**b**) The modular multiplicative inverse of 69 (mod 17) is $69^* = 1$. Hence:

$$69n \overset{17}{=} 23 \quad \rightarrow \quad n \overset{17}{=} 23(69^*) \quad \rightarrow \quad n \overset{17}{=} 23(1) \quad \rightarrow \quad n \overset{17}{=} 23 \overset{17}{=} 6 \quad \rightarrow \quad n = 6+17k \quad (k \in \mathbb{Z})$$

(**c**) The modular multiplicative inverse of 59 (mod 30) is $59^* = 29$. Hence:

$$59n \overset{30}{=} -88 \quad \rightarrow \quad n \overset{30}{=} -88(59^*) \quad \rightarrow \quad n \overset{30}{=} -88(29) \quad \rightarrow \quad n \overset{30}{=} -2552 \overset{30}{=} 28 \quad \rightarrow \quad n = 28+30k \quad (k \in \mathbb{Z})$$

(**d**) On adding -7 to both sides (rule 3 of § 2.7) we get $55n \overset{23}{=} 1$. The modular multiplicative inverse of 55 (mod 23) is $55^* = 18$. Hence:

$$55n \overset{23}{=} 1 \quad \rightarrow \quad n \overset{23}{=} 1(55^*) \quad \rightarrow \quad n \overset{23}{=} 1(18) \quad \rightarrow \quad n \overset{23}{=} 18 \quad \rightarrow \quad n = 18 + 23k \quad (k \in \mathbb{Z})$$

Note: all the solutions in this Problem follow the criteria set by the LCE theorem (noting that we have $d = 1$ in all cases and hence we have a single modular solution in each case, i.e. $n \overset{m}{=} 2, 6, 28, 18$ for parts a, b, c, d corresponding to $m = 5, 17, 30, 23$ respectively).

2. Solve the following linear congruence equations (where $n \in \mathbb{Z}$):

(**a**) $3n + 5 \overset{3}{=} 17$. (**b**) $9n - 4 \overset{9}{=} 33$. (**c**) $16n - 44 \overset{11}{=} 39$. (**d**) $13n + 6 \overset{32}{=} -14$. (**e**) $161n \overset{98}{=} 343$.

Solution:
(**a**) If we write $3n + 5 \overset{3}{=} 17$ as $3(n + 1) + 2 \overset{3}{=} (3 \times 5) + 2$ we can see that this congruence equation is identically correct for all $n \in \mathbb{Z}$ because $2 \overset{3}{=} 2$. Alternatively, $3n + 5 \overset{3}{=} 17$ is equivalent to $5 \overset{3}{=} 17$ which is equivalent to $2 \overset{3}{=} 2$ which is identically correct.
Regarding the LCE theorem, we have $d|b$ (where $d = 3$ and $b = 12$) and hence we have 3 modular solutions, i.e. $n \overset{3}{=} 0, 1, 2$ which represent all $n \in \mathbb{Z}$.
(**b**) If we write $9n - 4 \overset{9}{=} 33$ as $9(n - 1) + 5 \overset{9}{=} (9 \times 3) + 6$ then we can see that this congruence equation has no solution because $5 \overset{9}{\neq} 6$. More simply, $9n - 4 \overset{9}{=} 33$ is equivalent to $-4 \overset{9}{=} 33$, i.e. $5 \overset{9}{=} 6$ which is obviously invalid regardless of any $n \in \mathbb{Z}$.
Regarding the LCE theorem, $d \not| b$ (noting that $d = 9$ and $b = 37$) and hence we must have no solution.
(**c**) We have:

$$16n - 44 \overset{11}{=} 39 \quad \rightarrow \quad 16n \overset{11}{=} 83 \quad \rightarrow \quad n \overset{11}{=} 83(16^*) = 83(9) \overset{11}{=} 10 \quad \rightarrow \quad n = 10 + 11k \quad (k \in \mathbb{Z})$$

Regarding the LCE theorem, $d = 1$ and hence we must have a single modular solution, i.e. $n \overset{11}{=} 10$.
(**d**) We have:

$$13n + 6 \overset{32}{=} -14 \quad \rightarrow \quad 13n \overset{32}{=} -20 \quad \rightarrow \quad n \overset{32}{=} -20(13^*) = -20(5) \overset{32}{=} 28 \quad \rightarrow \quad n = 28 + 32k \quad (k \in \mathbb{Z})$$

Regarding the LCE theorem, $d = 1$ and hence we must have a single modular solution, i.e. $n \overset{32}{=} 28$.
(**e**) 161 has no modular multiplicative inverse (mod 98) because 161 and 98 are not coprime (see point 1 of § 2.7.1). Hence, we cannot use the method used in the previous parts. So, let us use the LCE theorem. Accordingly, we have $d = \gcd(98, 161) = 7$. Also, $d|b$ (where $b = 343$). So, by the LCE theorem we must have 7 modular solutions. By inspection we find that $n = 7$ is a solution and hence (from Eq. 58 with $x_0 = 7$ and $m/d = 98/7 = 14$) the 7 modular solutions are: $n \overset{98}{=} 7, 21, 35, 49, 63, 77, 91$.
Moreover, all the ordinary solutions are given by $n = 7 + 14k$ where $k \in \mathbb{Z}$ (i.e. $n \overset{98/7}{=} 7$).
In fact, we could have reached this result more easily by using rule 9 of § 2.7, that is:

$$(161/7)n \overset{98/7}{=} (343/7) \quad \rightarrow \quad 23n \overset{14}{=} 49 \quad \rightarrow \quad n \overset{14}{=} 49(23^*) = 49(11) \overset{14}{=} 7 \quad \rightarrow \quad n = 7 + 14k \quad (k \in \mathbb{Z})$$

3. Solve the following quadratic congruence equations (where $n \in \mathbb{Z}$):

   (**a**) $4n^2 - n + 6 \overset{5}{=} 0$. (**b**) $11n^2 + 18n + 23 \overset{7}{=} 0$. (**c**) $n^2 + 33n - 16 \overset{22}{=} 0$.

   (**d**) $51n^2 + 1 \overset{13}{=} 0$. (**e**) $44n^2 - 3n \overset{17}{=} 0$.

   Solution: In this sort of simple polynomial congruence equations we can use a trial method by trying $n = 0, 1, 2, \ldots, m-1$ (where m is the modulo).[122]

   (**a**) This congruence is equivalent to $4n^2 - n + 1 \overset{5}{=} 0$. On trying $n = 0, 1, 2, 3, 4$ we find $n = 2$ satisfies this equation and hence the solution is $n = 2 + 5k$ (where $k \in \mathbb{Z}$).

   (**b**) This congruence is equivalent to $4n^2 + 4n + 2 \overset{7}{=} 0$. On trying $n = 0, 1, 2, 3, 4, 5, 6$ we find no solution, so this congruence equation has no solution.

   (**c**) This congruence is equivalent to $n^2 + 11n - 16 \overset{22}{=} 0$. On trying $n = 0, 1, 2, \ldots, 21$ we find $n = 4, 7, 15, 18$ satisfy this equation and hence the solution is $n = m + 22k$ (where $m = 4, 7, 15, 18$ and $k \in \mathbb{Z}$). We note that Lagrange's polynomial roots theorem (see § 2.9.4) does not apply to this quadratic equation because the modulo is composite.

   (**d**) This congruence is equivalent to $-n^2 + 1 \overset{13}{=} 0$. On trying $n = 0, 1, 2, \ldots, 12$ we find $n = 1, 12$ satisfy this equation and hence the solution is $n = m + 13k$ (where $m = 1, 12$ and $k \in \mathbb{Z}$).

   (**e**) This congruence is equivalent to $10n^2 - 3n \overset{17}{=} 0$. On trying $n = 0, 1, 2, \ldots, 16$ we find $n = 0, 2$ satisfy this equation and hence the solution is $n = m + 17k$ (where $m = 0, 2$ and $k \in \mathbb{Z}$).

4. Describe and justify the method of factorization for solving congruence equations.

   Solution: Let $f(n) \overset{m}{=} 0$ be a congruence equation where $f(n)$ is an integer function of $n \in \mathbb{Z}$ (noting that f is usually a polynomial with integer coefficients and this is what it is supposed to be in this subsection) and where we assume (for simplicity) that m is a square free integer.[123] To get the solutions of this congruence equation we do the following:

   • We factorize $f(n)$ to its simplest form: $f(n) = f_1(n) f_2(n) \ldots f_q(n)$.[124]

   • We prime-factorize m to $m = p_1 p_2 \ldots p_k$.

   • We find the solutions (if exist) of all the congruence equations $f_i(n) \overset{p_j}{=} 0$ where $i = 1, 2, \ldots, q$ and $j = 1, 2, \ldots, k$.

   • The solutions of $f(n) \overset{m}{=} 0$ then are the union of the solutions of all the following systems of congruence equations:

   $$n \overset{p_1}{=} \alpha \qquad n \overset{p_2}{=} \beta \qquad \cdots \qquad n \overset{p_k}{=} \gamma \tag{59}$$

   where $\alpha, \beta, \ldots, \gamma$ represent a possible combination of the solutions obtained in the previous point.

   The justification of this method is that the congruence equation $f(n) \overset{m}{=} 0$ is equivalent to the following congruence equation:

   $$f_1 f_2 \ldots f_q \overset{p_1 p_2 \ldots p_k}{=} 0$$

   The last congruence equation means that $(f_1 f_2 \ldots f_q)$ is divisible by $(p_1 p_2 \ldots p_k)$. Now, by rule 20 of § 1.9 if $(f_1 f_2 \ldots f_q)$ is divisible by $(p_1 p_2 \ldots p_k)$ then $(f_1 f_2 \ldots f_q)$ must be divisible by each one of the factors $p_1, p_2, \ldots, p_k$ (noting that these factors are pairwise coprime), while by rule 22 of § 1.9 if $(f_1 f_2 \ldots f_q)$ is divisible by each one of the factors $p_1, p_2, \ldots, p_k$ then each one of the factors $p_1, p_2, \ldots, p_k$ must divide at least one of the factors $f_1, f_2, \ldots, f_q$. Accordingly, any possible solution must make each one of the factors $p_1, p_2, \ldots, p_k$ a divisor of at least one of the factors $f_1, f_2, \ldots, f_q$. This means that any possible solution should be a solution of a system of the form given by Eq. 59, and hence the solutions of the congruence equation $f(n) \overset{m}{=} 0$ should be the union of all these solutions. This also means that if for a given p_j the congruence equation $f_i(n) \overset{p_j}{=} 0$ has no solution for all $f_i(n)$ then the congruence

[122] A simple spreadsheet or a few lines of code can do this.

[123] The assumption of square free (see § 2.1) is to avoid some confusing details in the following description and justification. However, we should return to this issue by providing more details in the future (see for instance Problem 7). It is worth noting that all the examples treated in Problems 5 and 6 (which are about the method of factorization) use square free m.

[124] When $f(n)$ is a polynomial, "simplest form" means that the factors $f_1, f_2, \ldots, f_q$ are linear or non-factorizable quadratic.

equation $f(n) \overset{m}{=} 0$ has no solution. The best way to understand and appreciate this method is to put it to practice and this is what we will do in the next Problems.

5. Solve the following quadratic congruence equations (where $n \in \mathbb{Z}$):

(**a**) $15n^2 - n - 2 \overset{70}{=} 0$. (**b**) $28n^2 - 123n + 110 \overset{165}{=} 0$. (**c**) $4n^2 + 18n - 70 \overset{210}{=} 0$.

(**d**) $9n^2 - 39n + 40 \overset{105}{=} 0$. (**e**) $n^2 + 2n + 5 \overset{2210}{=} 0$.

Solution:[125] We use in this Problem the method of factorization (which we described and justified in Problem 4) with the use of the Chinese remainder method (see § 2.7.3) or the equivalent equation method (see § 2.7.4) for solving the systems of Eq. 59 (as will be demonstrated and clarified in the following solutions).

(**a**) We prime-factorize the modulo: $70 = 2 \times 5 \times 7$.

We factorize the polynomial: $15n^2 - n - 2 = (3n + 1)(5n - 2) \overset{70}{=} 0$.

If $(3n+1)(5n-2)$ is divisible by 70 (as implied by $15n^2 - n - 2 \overset{70}{=} 0$) then it must be divisible by $2, 5, 7$ (as justified in Problem 4). So, let consider the divisibility of $(3n + 1)(5n - 2)$ by $2, 5, 7$.

Regarding 2 we must have either $(3n + 1)$ is divisible by 2 (and hence $3n + 1 \overset{2}{=} 0$ whose solution is $n \overset{2}{=} 1$) or $(5n - 2)$ is divisible by 2 (and hence $5n - 2 \overset{2}{=} 0$ whose solution is $n \overset{2}{=} 0$).

Regarding 5 we must have either $(3n + 1)$ is divisible by 5 (and hence $3n + 1 \overset{5}{=} 0$ whose solution is $n \overset{5}{=} 3$) or $(5n - 2)$ is divisible by 5 (and hence $5n - 2 \overset{5}{=} 0$ which has no solution).

Regarding 7 we must have either $(3n + 1)$ is divisible by 7 (and hence $3n + 1 \overset{7}{=} 0$ whose solution is $n \overset{7}{=} 2$) or $(5n - 2)$ is divisible by 7 (and hence $5n - 2 \overset{7}{=} 0$ whose solution is $n \overset{7}{=} 6$).

So in brief, we have five linear congruence equations (which represent the solutions of $f_i(n) \overset{p_j}{=} 0$ that we already obtained): $n \overset{2}{=} 0$, $n \overset{2}{=} 1$, $n \overset{5}{=} 3$, $n \overset{7}{=} 2$ and $n \overset{7}{=} 6$.

We now consider all the (triple) combinations that can be formed from these five linear congruence equations by taking in each (triple) combination one and only one congruence equation of each of the three moduli 2, 5, 7 (and hence we have $2 \times 1 \times 2 = 4$ triple combinations). These combinations are represented by the columns (i.e. the second to the fifth) of the following table (ignoring for the time being the last row):

mod 2	0	0	1	1
mod 5	3	3	3	3
mod 7	2	6	2	6
mod 70	58	48	23	13

So, the Problem is reduced to solving four systems of three simultaneous linear congruence equations (e.g. the second column represents the system $n \overset{2}{=} 0$, $n \overset{5}{=} 3$ and $n \overset{7}{=} 2$) which can be easily done using the Chinese remainder method (see § 2.7.3) or the equivalent equation method (see § 2.7.4). These solutions (i.e. the smallest positive solutions) are given in the last row of the table. So, the general solutions of the given quadratic congruence equation are: $n = m + 70k$ (where $m = 13, 23, 48, 58$ and $k \in \mathbb{Z}$).

(**b**) We prime-factorize the modulo: $165 = 3 \times 5 \times 11$.

We factorize the polynomial: $28n^2 - 123n + 110 = (4n - 5)(7n - 22) \overset{165}{=} 0$.

If $(4n-5)(7n-22)$ is divisible by 165 (as implied by $28n^2 - 123n + 110 \overset{165}{=} 0$) then it must be divisible by $3, 5, 11$. So, let consider the divisibility of $(4n - 5)(7n - 22)$ by $3, 5, 11$.

Regarding 3 we must have either $(4n - 5)$ is divisible by 3 (and hence $4n - 5 \overset{3}{=} 0$ whose solution is $n \overset{3}{=} 2$) or $(7n - 22)$ is divisible by 3 (and hence $7n - 22 \overset{3}{=} 0$ whose solution is $n \overset{3}{=} 1$).

Regarding 5 we must have either $(4n - 5)$ is divisible by 5 (and hence $4n - 5 \overset{5}{=} 0$ whose solution is $n \overset{5}{=} 0$) or $(7n - 22)$ is divisible by 5 (and hence $7n - 22 \overset{5}{=} 0$ whose solution is $n \overset{5}{=} 1$).

[125] We remind the reader that Lagrange's polynomial roots theorem (see § 2.9.4) does not apply to these quadratic equations (because the moduli are composite) and hence the number of solutions can exceed 2.

Regarding 11 we must have either $(4n-5)$ is divisible by 11 (and hence $4n-5 \overset{11}{=} 0$ whose solution is $n \overset{11}{=} 4$) or $(7n-22)$ is divisible by 11 (and hence $7n-22 \overset{11}{=} 0$ whose solution is $n \overset{11}{=} 0$).
So in brief, we have six linear congruence equations: $n \overset{3}{=} 2$, $n \overset{3}{=} 1$, $n \overset{5}{=} 0$, $n \overset{5}{=} 1$, $n \overset{11}{=} 4$ and $n \overset{11}{=} 0$.
We now consider all the (triple) combinations as we did in part (a) and hence we have $2 \times 2 \times 2 = 8$ triple combinations. These combinations are given in the following table (ignoring for the time being the last row):

mod 3	2	2	2	2	1	1	1	1
mod 5	0	0	1	1	0	0	1	1
mod 11	4	0	4	0	4	0	4	0
mod 165	125	110	26	11	70	55	136	121

So, the Problem is reduced to solving eight systems of three simultaneous linear congruence equations (e.g. the second column represents the system $n \overset{3}{=} 2$, $n \overset{5}{=} 0$ and $n \overset{11}{=} 4$) which can be easily done using the Chinese remainder method (see § 2.7.3) or the equivalent equation method (see § 2.7.4). These solutions (i.e. the smallest positive solutions) are given in the last row of the table. So, the general solutions are: $n = m + 165k$ (where $m = 11, 26, 55, 70, 110, 121, 125, 136$ and $k \in \mathbb{Z}$).
(**c**) We prime-factorize the modulo: $210 = 2 \times 3 \times 5 \times 7$.
We factorize the polynomial: $4n^2 + 18n - 70 = (n+7)(4n-10) \overset{210}{=} 0$.
If $(n+7)(4n-10)$ is divisible by 210 (as implied by $4n^2 + 18n - 70 \overset{210}{=} 0$) then it must be divisible by $2, 3, 5, 7$. So, let consider the divisibility of $(n+7)(4n-10)$ by $2, 3, 5, 7$.
Regarding 2 we must have either $(n+7)$ is divisible by 2 (and hence $n+7 \overset{2}{=} 0$ whose solution is $n \overset{2}{=} 1$) or $(4n-10)$ is divisible by 2 (and hence $4n-10 \overset{2}{=} 0$ whose solution is $n \overset{2}{=} 0$).
Regarding 3 we must have either $(n+7)$ is divisible by 3 (and hence $n+7 \overset{3}{=} 0$ whose solution is $n \overset{3}{=} 2$) or $(4n-10)$ is divisible by 3 (and hence $4n-10 \overset{3}{=} 0$ whose solution is $n \overset{3}{=} 1$).
Regarding 5 we must have either $(n+7)$ is divisible by 5 (and hence $n+7 \overset{5}{=} 0$ whose solution is $n \overset{5}{=} 3$) or $(4n-10)$ is divisible by 5 (and hence $4n-10 \overset{5}{=} 0$ whose solution is $n \overset{5}{=} 0$).
Regarding 7 we must have either $(n+7)$ is divisible by 7 (and hence $n+7 \overset{7}{=} 0$ whose solution is $n \overset{7}{=} 0$) or $(4n-10)$ is divisible by 7 (and hence $4n-10 \overset{7}{=} 0$ whose solution is $n \overset{7}{=} 6$).
So in brief, we have eight linear congruence equations: $n \overset{2}{=} 1$, $n \overset{2}{=} 0$, $n \overset{3}{=} 2$, $n \overset{3}{=} 1$, $n \overset{5}{=} 3$, $n \overset{5}{=} 0$, $n \overset{7}{=} 0$ and $n \overset{7}{=} 6$.
We now consider all the (quadruple) combinations as we did in the previous parts, and hence we have $2 \times 2 \times 2 \times 2 = 16$ quadruple combinations. These combinations are given in the following table (ignoring for the time being the last row):

mod 2	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
mod 3	2	2	2	2	1	1	1	1	2	2	2	2	1	1	1	1
mod 5	3	3	0	0	3	3	0	0	3	3	0	0	3	3	0	0
mod 7	0	6	0	6	0	6	0	6	0	6	0	6	0	6	0	6
mod 210	203	83	35	125	133	13	175	55	98	188	140	20	28	118	70	160

So, the Problem is reduced to solving sixteen systems of four simultaneous linear congruence equations (e.g. the second column represents the system $n \overset{2}{=} 1$, $n \overset{3}{=} 2$, $n \overset{5}{=} 3$ and $n \overset{7}{=} 0$) which can be easily done using the Chinese remainder method (see § 2.7.3) or the equivalent equation method (see § 2.7.4). These solutions (i.e. the smallest positive solutions) are given in the last row of the table. So, the general solutions are: $n = m + 210k$ (where $m = 13, 20, 28, 35, 55, 70, 83, 98, 118, 125, 133, 140, 160, 175, 188, 203$ and $k \in \mathbb{Z}$).
(**d**) We prime-factorize the modulo: $105 = 3 \times 5 \times 7$.
We factorize the polynomial: $9n^2 - 39n + 40 = (3n-5)(3n-8) \overset{105}{=} 0$.
If $(3n-5)(3n-8)$ is divisible by 105 (as implied by $9n^2 - 39n + 40 \overset{105}{=} 0$) then it must be divisible by

$3, 5, 7$. So, let consider the divisibility of $(3n-5)(3n-8)$ by $3, 5, 7$.
Regarding 3 we must have either $(3n-5)$ is divisible by 3 (and hence $3n-5 \overset{3}{=} 0$ which has no solution) or $(3n-8)$ is divisible by 3 (and hence $3n-8 \overset{3}{=} 0$ which has no solution).
Regarding 5 we must have either $(3n-5)$ is divisible by 5 (and hence $3n-5 \overset{5}{=} 0$ whose solution is $n \overset{5}{=} 0$) or $(3n-8)$ is divisible by 5 (and hence $3n-8 \overset{5}{=} 0$ whose solution is $n \overset{5}{=} 1$).
Regarding 7 we must have either $(3n-5)$ is divisible by 7 (and hence $3n-5 \overset{7}{=} 0$ whose solution is $n \overset{7}{=} 4$) or $(3n-8)$ is divisible by 7 (and hence $3n-8 \overset{7}{=} 0$ whose solution is $n \overset{7}{=} 5$).
As we see, $9n^2-39n+40$ is not divisible by 3 and hence this congruence equation has no solution (even though the polynomial is divisible by 5 and 7 and hence it is divisible by 35 because what is required is the divisibility by 105 and the divisibility by 35 is not enough).
(**e**) We prime-factorize the modulo: $2210 = 2 \times 5 \times 13 \times 17$.
We rewrite the polynomial as:

$$n^2+2n+5 = n^2+2n+1+4 = (n+1)^2+4 = m^2+4 \overset{2210}{=} 0 \qquad (m = n+1)$$

Now, if m^2+4 is divisible by 2210 (as implied by $m^2+4 \overset{2210}{=} 0$) then it must be divisible by $2, 5, 13, 17$. So, let consider the divisibility of m^2+4 by $2, 5, 13, 17$:

$$\begin{array}{lcll} m^2+4 & \overset{2}{=} & 0 & \rightarrow \quad m \overset{2}{=} 0 \\ m^2+4 & \overset{5}{=} & 0 & \rightarrow \quad m \overset{5}{=} 1 \quad \text{or} \quad m \overset{5}{=} 4 \\ m^2+4 & \overset{13}{=} & 0 & \rightarrow \quad m \overset{13}{=} 3 \quad \text{or} \quad m \overset{13}{=} 10 \\ m^2+4 & \overset{17}{=} & 0 & \rightarrow \quad m \overset{17}{=} 8 \quad \text{or} \quad m \overset{17}{=} 9 \end{array}$$

Now, since $m = n+1$ then we must have:

$$\begin{array}{lcll} n+1 & \overset{2}{=} & 0 & \rightarrow \quad n \overset{2}{=} 1 \\ n+1 & \overset{5}{=} & 1 & \rightarrow \quad n \overset{5}{=} 0 \\ n+1 & \overset{5}{=} & 4 & \rightarrow \quad n \overset{5}{=} 3 \\ n+1 & \overset{13}{=} & 3 & \rightarrow \quad n \overset{13}{=} 2 \\ n+1 & \overset{13}{=} & 10 & \rightarrow \quad n \overset{13}{=} 9 \\ n+1 & \overset{17}{=} & 8 & \rightarrow \quad n \overset{17}{=} 7 \\ n+1 & \overset{17}{=} & 9 & \rightarrow \quad n \overset{17}{=} 8 \end{array}$$

On considering all the eight (quadruple) combinations (i.e. $1 \times 2 \times 2 \times 2$) and solving the resulting eight systems of four simultaneous linear congruence equations (as we did in the previous parts) we get:

mod 2	1	1	1	1	1	1	1	1
mod 5	0	0	0	0	3	3	3	3
mod 13	2	2	9	9	2	2	9	9
mod 17	7	8	7	8	7	8	7	8
mod 2210	925	535	2115	1725	483	93	1673	1283

So, the general solutions are: $n = s + 2210k$ (where $s = 93, 483, 535, 925, 1283, 1673, 1725, 2115$ and $k \in \mathbb{Z}$).

6. Solve the following cubic polynomial congruence equations (where $n \in \mathbb{Z}$):

(**a**) $n^3-12n^2+5n+150 \overset{399}{=} 0$. (**b**) $n^3-5n^2-13n-7 \overset{11362}{=} 0$. (**c**) $2n^3+7n^2+3n-5 \overset{12710}{=} 0$.

Solution: We follow a similar method to the method we used in Problem 5 to solve the quadratic congruence equations, and hence we present our solution in a brief form.
(**a**) We prime-factorize the modulo: $399 = 3 \times 7 \times 19$.

We factorize the polynomial: $n^3 - 12n^2 + 5n + 150 = (n+3)(n-5)(n-10) \overset{399}{=} 0$.

$$\begin{aligned}
n+3 &\overset{3}{=} 0 \quad \rightarrow \quad n \overset{3}{=} 0\\
n-5 &\overset{3}{=} 0 \quad \rightarrow \quad n \overset{3}{=} 2\\
n-10 &\overset{3}{=} 0 \quad \rightarrow \quad n \overset{3}{=} 1\\
n+3 &\overset{7}{=} 0 \quad \rightarrow \quad n \overset{7}{=} 4\\
n-5 &\overset{7}{=} 0 \quad \rightarrow \quad n \overset{7}{=} 5\\
n-10 &\overset{7}{=} 0 \quad \rightarrow \quad n \overset{7}{=} 3\\
n+3 &\overset{19}{=} 0 \quad \rightarrow \quad n \overset{19}{=} 16\\
n-5 &\overset{19}{=} 0 \quad \rightarrow \quad n \overset{19}{=} 5\\
n-10 &\overset{19}{=} 0 \quad \rightarrow \quad n \overset{19}{=} 10
\end{aligned}$$

Hence:

mod 3	0	0	0	0	0	0	0	0	0
mod 7	4	4	4	5	5	5	3	3	3
mod 19	16	5	10	16	5	10	16	5	10
mod 399	396	81	333	54	138	390	339	24	276

mod 3	2	2	2	2	2	2	2	2	2
mod 7	4	4	4	5	5	5	3	3	3
mod 19	16	5	10	16	5	10	16	5	10
mod 399	263	347	200	320	5	257	206	290	143

mod 3	1	1	1	1	1	1	1	1	1
mod 7	4	4	4	5	5	5	3	3	3
mod 19	16	5	10	16	5	10	16	5	10
mod 399	130	214	67	187	271	124	73	157	10

(**b**)We prime-factorize the modulo: $11362 = 2 \times 13 \times 19 \times 23$.
We factorize the polynomial: $n^3 - 5n^2 - 13n - 7 = (n+1)^2(n-7) \overset{11362}{=} 0$.

$$\begin{aligned}
n+1 &\overset{2}{=} 0 \quad \rightarrow \quad n \overset{2}{=} 1\\
n-7 &\overset{2}{=} 0 \quad \rightarrow \quad n \overset{2}{=} 1\\
n+1 &\overset{13}{=} 0 \quad \rightarrow \quad n \overset{13}{=} 12\\
n-7 &\overset{13}{=} 0 \quad \rightarrow \quad n \overset{13}{=} 7\\
n+1 &\overset{19}{=} 0 \quad \rightarrow \quad n \overset{19}{=} 18\\
n-7 &\overset{19}{=} 0 \quad \rightarrow \quad n \overset{19}{=} 7\\
n+1 &\overset{23}{=} 0 \quad \rightarrow \quad n \overset{23}{=} 22\\
n-7 &\overset{23}{=} 0 \quad \rightarrow \quad n \overset{23}{=} 7
\end{aligned}$$

Hence:

mod 2	1	1	1	1	1	1	1	1
mod 13	12	12	12	12	7	7	7	7
mod 19	18	18	7	7	18	18	7	7
mod 23	22	7	22	7	22	7	22	7
mod 11362	11361	3457	1793	5251	6117	9575	7911	7

(**c**) We prime-factorize the modulo: $12710 = 2 \times 5 \times 31 \times 41$.
We factorize the polynomial: $2n^3 + 7n^2 + 3n - 5 = (2n+5)(n^2+n-1) \overset{12710}{=} 0$.

On testing the divisibility of $(2n+5)(n^2+n-1)$ by $2, 5, 31, 41$ we find that $(2n+5)(n^2+n-1)$ is not divisible by 2 for any $n \in \mathbb{Z}$ (because it is always odd; see the parity rules in § 1.8) and hence this congruence equation has no solution. In fact, if we were sharp-eyed then we could have identified this from the beginning by noting that $2n^3+7n^2+3n-5$ is always odd and hence it cannot be divisible by 12710 which is even.

7. Solve the following quadratic congruence equation (where $n \in \mathbb{Z}$): $2n^2-11n-51 \overset{180}{=} 0$.
Solution: This congruence equation looks very much like the quadratic congruence equations of Problem 5. However, its modulo (i.e. $m = 180$; see Problem 4) is not square free (unlike the moduli in Problem 5). So, for the p_j's which are not square free we consider the divisibility of $(2n^2-11n-51)$ as a whole (rather than as factorized) by these p_j's (i.e. $p_j^{a_j}$ where $a_j > 1$). This is because the divisibility of $f(n)$ by these $p_j^{a_j}$'s could be realized by the divisibility of the factors of $f(n)$ by the factors of these $p_j^{a_j}$'s (rather than by the divisibility of individual factors of f by the entire $p_j^{a_j}$). Accordingly:
We prime-factorize the modulo: $180 = 2^2 \times 3^2 \times 5 = 4 \times 9 \times 5$.
We factorize the polynomial: $2n^2-11n-51 = (n+3)(2n-17) \overset{180}{=} 0$.
If $(n+3)(2n-17)$ is divisible by 180 (as implied by $2n^2-11n-51 \overset{180}{=} 0$) then it must be divisible by $4, 9, 5$. So, let consider the divisibility of $(n+3)(2n-17)$ by $4, 9, 5$.
Regarding 4 we consider the divisibility of $(2n^2-11n-51)$ as a whole by 4, i.e. $2n^2-11n-51 \overset{4}{=} 0$ whose solution (using for instance the trial method of Problem 3) is $n \overset{4}{=} 1$.
Regarding 9 we consider the divisibility of $(2n^2-11n-51)$ as a whole by 9, i.e. $2n^2-11n-51 \overset{9}{=} 0$ whose solutions are $n \overset{9}{=} 4$ and $n \overset{9}{=} 6$.
Regarding 5 we must have either $(n+3)$ is divisible by 5 (and hence $n+3 \overset{5}{=} 0$ whose solution is $n \overset{5}{=} 2$) or $(2n-17)$ is divisible by 5 (and hence $2n-17 \overset{5}{=} 0$ whose solution is $n \overset{5}{=} 1$).[126]
So in brief, we have five linear congruence equations: $n \overset{4}{=} 1$, $n \overset{9}{=} 4$, $n \overset{9}{=} 6$, $n \overset{5}{=} 2$ and $n \overset{5}{=} 1$.
We now consider all the four (triple) combinations in the following table:

mod 4	1	1	1	1
mod 9	4	4	6	6
mod 5	2	1	2	1
mod 180	157	121	177	141

On solving the four systems of three simultaneous linear congruence equations (as we did in the previous Problems) we get the (smallest positive) solutions in the last row of the table. So, the general solutions are: $n = m + 180k$ (where $m = 121, 141, 157, 177$ and $k \in \mathbb{Z}$).
Note: we may adjust the method of factorization (which was described and justified in Problem 4) by the observations we made in the present Problem (i.e. we consider the divisibility of f as a whole by the non-"square free" prime factors).

8. What is the maximum number of distinct (modular) solutions of the following polynomials:
(**a**) Cubic (mod 13). (**b**) Quartic (mod 77). (**c**) Quintic (mod 130169).
Solution: We use Lagrange's polynomial roots theorem (see § 2.9.4).
(**a**) 13 is prime and hence we must have a maximum of 3 solutions.
(**b**) $77 = 7 \times 11$ and hence we must have a maximum of $4 \times 4 = 16$ solutions (because for each prime factor we have a maximum of 4 solutions).
(**c**) $130169 = 13 \times 17 \times 19 \times 31$ and hence we must have a maximum of $5 \times 5 \times 5 \times 5 = 625$ solutions (because for each prime factor we have a maximum of 5 solutions).

9. Find all $n \in \mathbb{Z}$ that satisfy the following congruence equations:
(**a**) $n-2 \overset{n+7}{=} 0$. (**b**) $77n+2 \overset{3n+11}{=} 0$. (**c**) $6n-5 \overset{15n+1}{=} 0$. (**d**) $13n-17 \overset{2n+14}{=} 0$.
Solution:

[126] It should be obvious that we can consider the divisibility of $(2n^2-11n-51)$ as a whole by 5 (as we did with 4 and 9).

(**a**) This congruence equation means that $(n+7)$ is a divisor of $(n-2)$. Now:

$$\frac{n-2}{n+7} = 1 - \frac{9}{n+7}$$

So, if $(n+7)$ divides $(n-2)$ then $9/(n+7)$ must be an integer. The $(\pm)$ divisors of 9 are $\pm 1, \pm 3, \pm 9$ which means that $(n+7) = \pm 1, \pm 3, \pm 9$ and hence $n = -8, -10, -16, -6, -4, 2$. All these values are acceptable from a divisibility perspective. However, since the modulo must be greater than 1 then we should accept only $n = -4, 2$.
(**b**) This congruence equation means that $(3n+11)$ is a divisor of $(77n+2)$. Now:

$$\frac{77n+2}{3n+11} = \frac{1}{3}\left(77 - \frac{841}{3n+11}\right)$$

So, if $(3n+11)$ divides $(77n+2)$ then the expression inside the brackets in the last equation must be an integer divisible by 3. For the expression inside the brackets to be an integer, $841/(3n+11)$ must be an integer. The $(\pm)$ divisors of 841 are $\pm 1, \pm 29, \pm 841$. So, we must have $(3n+11) = \pm 1, \pm 29, \pm 841$ and hence (considering $n \in \mathbb{Z}$) $n = -4, -284, 6$. All these values are acceptable from a divisibility perspective (noting that they make the expression inside the brackets an integer divisible by 3). However, since the modulo must be greater than 1 then we should accept only $n = 6$.
(**c**) This congruence equation means that $(15n+1)$ is a divisor of $(6n-5)$. Now:

$$\frac{6n-5}{15n+1} = \frac{1}{5}\left(2 - \frac{27}{15n+1}\right)$$

So, if $(15n+1)$ divides $(6n-5)$ then the expression inside the brackets in the last equation must be an integer divisible by 5. For the expression inside the brackets to be an integer, $27/(15n+1)$ must be an integer. The $(\pm)$ divisors of 27 are $\pm 1, \pm 3, \pm 9, \pm 27$. So, we must have $(15n+1) = \pm 1, \pm 3, \pm 9, \pm 27$ and hence (considering $n \in \mathbb{Z}$) $n = 0$. So, we have no solution other than this trivial solution (which should be rejected since the modulo must be greater than 1).
(**d**) This congruence equation means that $(2n+14)$ is a divisor of $(13n-17)$. Now:

$$\frac{13n-17}{2n+14} = \frac{1}{2}\left(13 - \frac{108}{n+7}\right)$$

So, if $(2n+14)$ divides $(13n-17)$ then the expression inside the brackets in the last equation must be an even integer which means that $108/(n+7)$ must be an odd integer. The $(\pm)$ divisors of 108 are: ± 1, ± 2, ± 3, ± 4, ± 6, ± 9, ± 12, ± 18, ± 27, ± 36, ± 54, ± 108. So, for $108/(n+7)$ to be an integer we must have $(n+7) = \pm 1$, ± 2, ± 3, ± 4, ± 6, ± 9, ± 12, ± 18, ± 27, ± 36, ± 54, ± 108 and hence: $n = -8$, -9, -10, -11, -13, -16, -19, -25, -34, -43, -61, -115, -6, -5, -4, -3, -1, 2, 5, 11, 20, 29, 47, 101. Noting that $108/(n+7)$ must be an odd integer, only $n = -11$, -19, -43, -115, -3, 5, 29, 101 are acceptable solutions (i.e. from a divisibility perspective). However, since the modulo must be greater than 1 then we should accept only $n = -3$, 5, 29, 101.

10. Find all $n \in \mathbb{Z}$ that satisfy the following congruence equations:

(**a**) $n^2 + 3n - 9 \overset{n-1}{=} 0$. (**b**) $5n^3 - 4n^2 + n - 6 \overset{3n+11}{=} 0$. (**c**) $n^4 + 3n^3 - 8n^2 + 15 \overset{n^2+5}{=} 0$.

Solution:
(**a**) This congruence equation means that $(n-1)$ is a divisor of (n^2+3n-9). Now:

$$\frac{n^2+3n-9}{n-1} = n + 4 - \frac{5}{n-1}$$

So, if $(n-1)$ divides (n^2+3n-9) then $(n-1)$ must divide 5, i.e. $(n-1) = \pm 1, \pm 5$ and hence $n = 0, -4, 2, 6$. All these values are acceptable solutions from a divisibility perspective. However, since

the modulo must be greater than 1 then we should accept only $n = 6$.
(**b**) This congruence equation means that $(3n + 11)$ is a divisor of $(5n^3 - 4n^2 + n - 6)$. Now:

$$\frac{5n^3 - 4n^2 + n - 6}{3n + 11} = \frac{1}{27}\left(45n^2 - 201n + 746 - \frac{8368}{3n + 11}\right)$$

So, if $(3n + 11)$ divides $(5n^3 - 4n^2 + n - 6)$ then the expression inside the brackets in the last equation must be an integer divisible by 27. For the expression inside the brackets to be an integer, $8368/(3n+11)$ must be an integer. The $(\pm)$ divisors of 8368 are ±1, ±2, ±4, ±8, ±16, ±523, ±1046, ±2092, ±4184, ±8368. So, $(3n + 11)$ must be equal to (some of) these values and hence (noting that $n \in \mathbb{Z}$): $n = -4$, -5, -9, -178, -701, -2793, -3, -1, 345, 1391. All these values are acceptable solutions from a divisibility perspective. However, since the modulo must be greater than 1 then we should accept only $n = -3$, -1, 345, 1391.
(**c**) This congruence equation means that $(n^2 + 5)$ is a divisor of $(n^4 + 3n^3 - 8n^2 + 15)$. Now:

$$\frac{n^4 + 3n^3 - 8n^2 + 15}{n^2 + 5} = n^2 + 3n - 13 + \left(\frac{80 - 15n}{n^2 + 5}\right)$$

So, if $(n^2 + 5)$ divides $(n^4 + 3n^3 - 8n^2 + 15)$ then the expression inside the brackets in the last equation must be an integer which implies $|80 - 15n| \geq (n^2 + 5)$. The solution of this inequality (within the integers) is $-18 \leq n \leq 3$. On trying these values we find only $n = 0$ can be a solution. So, the solution is $n = 0$.

11. Solve the following polynomial congruence equations (where $n \in \mathbb{Z}$):

(**a**) $n^{105} + n^{67} - 17 \stackrel{5}{=} 0$. (**b**) $n^{1640} - n^{122} + 89 \stackrel{41}{=} 0$. (**c**) $n^{120} + 2n^{50} + 33 \stackrel{36}{=} 0$.

Solution: In this type of high degree polynomial congruence equations we may be able to reduce the degree of the polynomial repeatedly using, for instance, Euler's theorem (see § 2.9.2) or Fermat's little theorem (see § 2.9.3) as outlined in the following.
(**a**) We have (using Fermat's little theorem):

$$\begin{aligned} n^{105} + n^{67} - 17 &= \left(n^5\right)^{21} + \left(n^5\right)^{13} n^2 - 17 \stackrel{5}{=} n^{21} + n^{15} - 17 = \left(n^5\right)^4 n + \left(n^5\right)^3 - 17 \\ &\stackrel{5}{=} n^5 + n^3 - 17 \stackrel{5}{=} n + n^3 - 17 \stackrel{5}{=} n^3 + n - 2 \end{aligned}$$

So, the given congruence equation is equivalent to the congruence equation $n^3 + n - 2 \stackrel{5}{=} 0$ (thanks to Fermat's little theorem) which has a general solution $n = 1 + 5k$ $(k \in \mathbb{Z})$.
(**b**) We have (using Fermat's little theorem):

$$\begin{aligned} n^{1640} - n^{122} + 89 &= \left(n^{41}\right)^{40} - \left(n^{41}\right)^3 n^{-1} + 89 \stackrel{41}{=} n^{40} - n^3 n^{-1} + 89 \\ &= n^{41} n^{-1} - n^2 + 89 \stackrel{41}{=} nn^{-1} - n^2 + 89 = 1 - n^2 + 89 = 90 - n^2 \stackrel{41}{=} 8 - n^2 \end{aligned}$$

So, the given congruence equation is equivalent to the congruence equation $8 - n^2 \stackrel{41}{=} 0$ (thanks to Fermat's little theorem) which has general solutions $n = m + 41k$ (where $m = 7, 34$ and $k \in \mathbb{Z}$).
(**c**) We have (using Euler's theorem):

$$n^{120} + 2n^{50} + 33 = \left(n^{12}\right)^{10} + 2\left(n^{12}\right)^4 n^2 + 33 \stackrel{36}{=} 1^{10} + 2 \times 1^4 \; n^2 + 33 = 2n^2 + 34$$

So, the given congruence equation is equivalent to the congruence equation $2n^2 + 34 \stackrel{36}{=} 0$ (thanks to Euler's theorem) which has general solutions $n = m + 36k$ (where $m = 1, 17, 19, 35$ and $k \in \mathbb{Z}$).

Note: we refer the reader to the previous Problems about how to solve $n^3 + n - 2 \stackrel{5}{=} 0$ (for part a), $8 - n^2 \stackrel{41}{=} 0$ (for part b) and $2n^2 + 34 \stackrel{36}{=} 0$ (for part c).

3.2.2 Hensel's Lemma

This lemma (or rather theorem which, by the way, has several variants and flavors with various levels of abstraction and generality) provides a practical method for solving polynomial congruence equations of modular powers of primes, and hence it is important for solving univariate polynomial congruence equations in general. According to Hensel's lemma, if:

- $P(m)$ is a polynomial with integer coefficients and P' is its derivative,
- p is a prime number,
- $P(m) \overset{p^d}{=} 0$ and $P'(m) \overset{p}{\neq} 0$,

then there is a unique "lift" $c \pmod p$ such that $P(m + cp^d) \overset{p^{d+1}}{=} 0$ where c is given by:

$$c = -\big[P'(m)\big]^* \frac{P(m)}{p^d} \tag{60}$$

with $\big[P'(m)\big]^*$ being the multiplicative inverse of $P'(m)$ modulo p.

As a result of this lemma we can propose the following recursive formula for obtaining successive lifts and progressing toward obtaining the final solution:

$$m_{d+1} \overset{p^{d+1}}{=} m_d + c_d\, p^d \overset{p^{d+1}}{=} m_d - \big[P'(m_d)\big]^* \frac{P(m_d)}{p^d} p^d \overset{p^{d+1}}{=} m_d - \big[P'(m_d)\big]^* P(m_d) \tag{61}$$

The best way to understand and appreciate Hensel's lemma and learn how to make use of it in solving polynomial congruence equations of modular prime powers is to put it to practice and that is what we will do in the following Problems.

Problems

1. Solve the following polynomial congruence equations for $n \in \mathbb{Z}$:

   (**a**) $2n^3 - n^2 + 5n + 14 \overset{27}{=} 0$. (**b**) $n^4 + 33n^2 - 1 \overset{343}{=} 0$. (**c**) $n^9 - 9n^4 + 4n^2 + 1 \overset{125}{=} 0$.

   Solution:

   (**a**) $27 = 3^3$ and the polynomial has integer coefficients. Hence, this polynomial congruence equation is potentially subject to Hensel's lemma.

   We start by finding a solution to $2n^3 - n^2 + 5n + 14 \overset{3}{=} 0$ which by simple trial gives $n = 2$. So, $m_1 = 2$.

   We also note that $P'(m_1) = P'(2) = 6(2^2) - 2(2) + 5 = 25 \overset{3}{\neq} 0$, so the condition for lifting is satisfied. Now, if we note that $\big[P'(m_1)\big]^* = \big[P'(2)\big]^* = 25^* \pmod 3$ equals 1 and $P(m_1) = P(2) = 36$ then from Eq. 61 we get:

   $$m_2 \overset{3^2}{=} m_1 - \big[P'(m_1)\big]^* P(m_1) = 2 - (1 \times 36) = -34 \overset{3^2}{=} 2$$

   If we note again that $\big[P'(m_2)\big]^* = \big[P'(2)\big]^* = 25^* \pmod 3$ equals 1 and $P(m_2) = P(2) = 36$ then from Eq. 61 we get:

   $$m_3 \overset{3^3}{=} m_2 - \big[P'(m_2)\big]^* P(m_2) = 2 - (1 \times 36) = -34 \overset{3^3}{=} 20$$

   So, the general solution to this congruence equation is $n = 20 + 27k$ $(k \in \mathbb{Z})$.

   (**b**) $343 = 7^3$ and the polynomial has integer coefficients. Hence, this polynomial congruence equation is potentially subject to Hensel's lemma.

   We start by finding a solution to $n^4 + 33n^2 - 1 \overset{7}{=} 0$ which by simple trial gives $n = 2$ or $n = 5$. So, $m_1 = 2$ or $m_1 = 5$.

   We also note that $P'(m_1 = 2) = 4(2^3) + 66(2) = 164 \overset{7}{\neq} 0$, so the condition for lifting is satisfied for $m_1 = 2$. Similarly, $P'(m_1 = 5) = 4(5^3) + 66(5) = 830 \overset{7}{\neq} 0$, so the condition for lifting is also satisfied for $m_1 = 5$. Accordingly, we need to consider both cases by applying the recursive lifting formula (Eq. 61) as we did in part (a).

   Regarding $m_1 = 2$:

   $$m_2 \overset{7^2}{=} m_1 - \big[P'(m_1)\big]^* P(m_1) \quad = \quad 2 - (5 \times 147) = -733 \overset{7^2}{=} 2$$

$$m_3 \overset{7^3}{=} m_2 - \left[P'(m_2)\right]^* P(m_2) \quad = \quad 2 - (5 \times 147) = -733 \overset{7^3}{=} 296$$

Regarding $m_1 = 5$:

$$m_2 \overset{7^2}{=} m_1 - \left[P'(m_1)\right]^* P(m_1) \quad = \quad 5 - (2 \times 1449) = -2893 \overset{7^2}{=} 47$$
$$m_3 \overset{7^3}{=} m_2 - \left[P'(m_2)\right]^* P(m_2) \quad = \quad 47 - (2 \times 4952577) = -9905107 \overset{7^3}{=} 47$$

So, the general solutions to this congruence equation are $n = 47 + 343k$ and $n = 296 + 343k$ ($k \in \mathbb{Z}$).
(**c**) $125 = 5^3$ and the polynomial has integer coefficients. Hence, this polynomial congruence equation is potentially subject to Hensel's lemma.
We start by finding a solution to $n^9 - 9n^4 + 4n^2 + 1 \overset{5}{=} 0$ which by simple trial gives $n = 2$ or $n = 4$. So, $m_1 = 2$ or $m_1 = 4$.

We also note that $P'(m_1 = 2) = 9(2^8) - 36(2^3) + 8(2) = 2032 \overset{5}{\neq} 0$, so the condition for lifting is satisfied for $m_1 = 2$. Similarly, $P'(m_1 = 4) = 9(4^8) - 36(4^3) + 8(4) = 587552 \overset{5}{\neq} 0$, so the condition for lifting is also satisfied for $m_1 = 4$. Accordingly, we need to consider both cases by applying the recursive lifting formula (Eq. 61) as we did in parts (a) and (b).
Regarding $m_1 = 2$:

$$m_2 \overset{5^2}{=} m_1 - \left[P'(m_1)\right]^* P(m_1) \quad = \quad 2 - (3 \times 385) = -1153 \overset{5^2}{=} 22$$
$$m_3 \overset{5^3}{=} m_2 - \left[P'(m_2)\right]^* P(m_2) \quad = \quad 22 - (3 \times 1207267111425) = -3621801334253 \overset{5^3}{=} 122$$

Regarding $m_1 = 4$:

$$m_2 \overset{5^2}{=} m_1 - \left[P'(m_1)\right]^* P(m_1) \quad = \quad 4 - (3 \times 259905) = -779711 \overset{5^2}{=} 14$$
$$m_3 \overset{5^3}{=} m_2 - \left[P'(m_2)\right]^* P(m_2) \quad = \quad 14 - (3 \times 20660701825) = -61982105461 \overset{5^3}{=} 39$$

So, the general solutions to this congruence equation are $n = 39 + 125k$ and $n = 122 + 125k$ ($k \in \mathbb{Z}$).

3.2.3 Euler's Criterion

There are many details about Euler's criterion. However, here we only introduce this criterion as a test for solvability of congruence equations. According to this criterion, the quadratic congruence equation $x^2 \overset{p}{=} m$ has a solution *iff* $m^{(p-1)/2} \overset{p}{=} 1$ (where $m \in \mathbb{Z}$, p is an odd prime and $p \nmid m$). It is important to note the following about Euler's criterion:
• Despite its restriction (as stated above) to a simple quadratic form (i.e. $x^2 \overset{p}{=} m$), this criterion can be applied to quadratic polynomial congruence equations in general by transforming other quadratic forms to this form by some congruence and algebraic manipulations (using the techniques of modular multiplicative inverse and completing the square). This will be demonstrated in the following Problems.
• Despite its restriction (as stated above) to quadratic polynomials, its usefulness extends (as a test for solvability) to higher degree polynomials by factorizing these polynomials to quadratic factors (as well as a linear factor if the degree is odd) noting that any polynomial (with integer coefficients) can be factorized as a product of linear or/and quadratic factors.
• We should note the limitation of Euler's criterion from two main sides: its restriction to prime moduli and the restriction of $p \nmid m$.
• Despite its usefulness in general (as stated above and within the given conditions and restrictions), the usefulness of Euler's criterion as a test for solvability is mainly related to non-factorizable quadratic polynomials (or higher-order polynomials which have non-factorizable quadratic factors). This is because if the quadratic is factorizable (i.e. to linear factors) then it is generally easier to test its divisibility by testing the divisibility of its linear factors.

Problems

1. Verify the validity of Euler's criterion test by applying it to the following quadratic congruence equations:

$$11n^2+18n+23 \overset{7}{=} 0 \qquad\qquad 44n^2-3n \overset{17}{=} 0$$

Solution: We note first that these congruences can be simplified (e.g. the first congruence is equivalent to $4n^2+4n+2 \overset{7}{=} 0$) before applying the procedure of verifying Euler's criterion (where this simplification results in arithmetic simplification in the subsequent calculations), but we prefer to deal with the given congruences as they are.

Regarding $11n^2+18n+23 \overset{7}{=} 0$, if we multiply this congruence by the multiplicative inverse (mod 7) of 11 (which is 2) and complete the square then we get:

$$(2)11n^2+(2)18n+(2)23 \overset{7}{=} 0 \quad \rightarrow \quad n^2+36n+46 \overset{7}{=} 0 \quad \rightarrow \quad n^2+36n+18^2-18^2+46 \overset{7}{=} 0 \quad \rightarrow$$

$$(n+18)^2 \overset{7}{=} 278 \quad \rightarrow \quad N^2 \overset{7}{=} 278$$

where $N=n+18$. Now, $278^{(7-1)/2}=278^3 \overset{7}{=} -1 \neq 1$ and hence according to Euler's criterion (noting that $7 \not| 278$) the congruence $11n^2+18n+23 \overset{7}{=} 0$ is unsolvable (in agreement with the result of part b of Problem 3 of § 3.2.1).

Regarding $44n^2-3n \overset{17}{=} 0$, if we multiply this congruence by the multiplicative inverse (mod 17) of 44 (which is 12) and complete the square then we get:

$$(12)44n^2-(12)3n \overset{17}{=} 0 \quad \rightarrow \quad n^2-36n \overset{17}{=} 0 \quad \rightarrow \quad n^2-36n+18^2-18^2 \overset{17}{=} 0 \quad \rightarrow$$

$$(n-18)^2 \overset{17}{=} 324 \quad \rightarrow \quad N^2 \overset{17}{=} 324$$

where $N=n-18$. Now, $324^{(17-1)/2}=324^8 \overset{17}{=} 1$ and hence according to Euler's criterion (noting that $17 \not| 324$) the congruence $44n^2-3n \overset{17}{=} 0$ is solvable (in agreement with the result of part e of Problem 3 of § 3.2.1).

2. Determine if the following polynomial congruence equations are solvable or not by using Euler's criterion:

(**a**) $28n^2+27n+3 \overset{13}{=} 0$. (**b**) $3n^2-96n+702 \overset{31}{=} 0$.

(**c**) $10n^3+43n^2-44n+7 \overset{5}{=} 0$. (**d**) $40n^4-63n^3+107n^2-87n+39 \overset{7}{=} 0$.

Solution: We employ the method which we used in Problem 1. As indicated earlier, these congruences can be simplified (e.g. the congruence of part a is equivalent to $2n^2+n+3 \overset{13}{=} 0$) before applying this method, but we prefer to deal with the given congruences as they are.

(**a**) We have:

$$(7)28n^2+(7)27n+(7)3 \overset{13}{=} 0 \quad \rightarrow \quad n^2+189n+21 \overset{13}{=} 0 \quad \rightarrow \quad n^2+202n+21 \overset{13}{=} 0 \quad \rightarrow$$

$$(n+101)^2-101^2+21 \overset{13}{=} 0 \quad \rightarrow \quad (n+101)^2 \overset{13}{=} 10180 \quad N^2 \overset{13}{=} 10180$$

Now, $10180^{(13-1)/2}=10180^6 \overset{13}{=} 1$ and hence according to Euler's criterion (noting that $13 \not| 10180$) the congruence $28n^2+27n+3 \overset{13}{=} 0$ is solvable.[127]

(**b**) We have:

$$(21)3n^2-(21)96n+(21)702 \overset{31}{=} 0 \quad \rightarrow \quad n^2-2016n+14742 \overset{31}{=} 0 \quad \rightarrow$$

$$(n-1008)^2-1008^2+14742 \overset{31}{=} 0 \quad \rightarrow \quad (n-1008)^2 \overset{31}{=} 1001322 \quad \rightarrow \quad N^2 \overset{31}{=} 1001322$$

Now, $1001322^{(31-1)/2}=1001322^{15} \overset{31}{=} -1$ and hence according to Euler's criterion (noting that $31 \not|$

[127] We note that we replaced 189 by 202 (by adding 13 which does not affect its modularity) because 189 is odd and hence halving it (which is needed for completing the square) is not possible (due to the restriction to integers). This approach is valid in general (noting that we will use it again in part c where we replace 27 with 32). We also note that we could have done substantial simplifications in arithmetic during our calculations by exploiting the rules and properties of congruence but we avoided this for plainness and to avoid unnecessary distraction (as well as to demonstrate certain features and details in the method of solution with regard to some of these congruences).

1001322) the congruence $3n^2 - 96n + 702 \overset{31}{=} 0$ is not solvable.

(**c**) We have $10n^3+43n^2-44n+7 = (5n-1)(2n^2+9n-7)$. So, if the congruence $10n^3+43n^2-44n+7 \overset{5}{=} 0$ is solvable then we must have $5n-1 \overset{5}{=} 0$ or/and $2n^2+9n-7 \overset{5}{=} 0$ (see rule 22 of § 1.9). Now, $5n-1 \overset{5}{=} 0$ is not solvable (noting that $-1 \overset{5}{\neq} 0$). Regarding $2n^2 + 9n - 7 \overset{5}{=} 0$ we use Euler's criterion as we did in the previous parts, that is:

$(3)2n^2 + (3)9n - (3)7 \overset{5}{=} 0 \quad \rightarrow \quad n^2 + 27n - 21 \overset{5}{=} 0 \quad \rightarrow \quad n^2 + 32n - 21 \overset{5}{=} 0 \quad \rightarrow$

$(n + 16)^2 - 16^2 - 21 \overset{5}{=} 0 \quad \rightarrow \quad (n + 16)^2 \overset{5}{=} 277 \quad \rightarrow \quad N^2 \overset{5}{=} 277$

Now, $277^{(5-1)/2} = 277^2 \overset{5}{=} -1$ and hence according to Euler's criterion (noting that $5 \not| 277$) the congruence $2n^2 + 9n - 7 \overset{5}{=} 0$ is not solvable.

So, neither $5n-1 \overset{5}{=} 0$ nor $2n^2+9n-7 \overset{5}{=} 0$ is solvable and hence the congruence $10n^3+43n^2-44n+7 \overset{5}{=} 0$ is not solvable.

(**d**) We have $40n^4 - 63n^3 + 107n^2 - 87n + 39 = (5n^2 - 6n + 3)(8n^2 - 3n + 13)$. So, if the congruence $40n^4 - 63n^3 + 107n^2 - 87n + 39 \overset{7}{=} 0$ is solvable then we must have $5n^2 - 6n + 3 \overset{7}{=} 0$ or/and $8n^2 - 3n + 13 \overset{7}{=} 0$ (see rule 22 of § 1.9). Regarding $5n^2 - 6n + 3 \overset{7}{=} 0$ we use Euler's criterion as we did before, that is:

$(3)5n^2 - (3)6n + (3)3 \overset{7}{=} 0 \quad \rightarrow \quad n^2 - 18n + 9 \overset{7}{=} 0 \quad \rightarrow \quad (n - 9)^2 - 9^2 + 9 \overset{7}{=} 0 \quad \rightarrow$

$(n - 9)^2 \overset{7}{=} 72 \quad \rightarrow \quad N^2 \overset{7}{=} 72$

Now, $72^{(7-1)/2} = 72^3 \overset{7}{=} 1$ and hence according to Euler's criterion (noting that $7 \not| 72$) the congruence $5n^2 - 6n + 3 \overset{7}{=} 0$ is solvable. So, the congruence $40n^4 - 63n^3 + 107n^2 - 87n + 39 \overset{7}{=} 0$ is solvable.[128]

3.2.4 Exponential Congruence Equations

We present in the Problems of this subsection a small sample of exponential congruence equations in one variable and illustrate how they are solved.

Problems

1. Solve the following exponential congruence equations (where $n \in \mathbb{N}$):

(**a**) $6^n \overset{5}{=} 1$. (**b**) $5^n \overset{7}{=} 6$. (**c**) $8^n \overset{10}{=} 4$. (**d**) $13^n \overset{10}{=} 1$. (**e**) $17^n \overset{60}{=} 17$.

Solution:

(**a**) All natural powers of 6 end in 6 (rule 16 of § 1.8). Now, if a number ends in 6 then it is equal to 1 modulo 5 (because the number can be written as $5m + 1$ for some $m \in \mathbb{N}$). Therefore, any positive integer is a solution of this exponential congruence (i.e. $n = 1, 2, 3, \ldots$). In fact, even $n = 0$ is a valid solution to this congruence.

(**b**) We have $5^3 \overset{7}{=} 6$. We also have $5^6 \overset{7}{=} 1$ and hence $\left(5^6\right)^m \overset{7}{=} 1$ (see rule 11 of § 2.7). On multiplying these two congruences side by side (using rule 10 of § 2.7) we get:

$$5^3 \times \left(5^6\right)^m \overset{7}{=} 6 \times 1 \quad \rightarrow \quad 5^{3+6m} \overset{7}{=} 6$$

Hence, $n = 3 + 6m$ ($m \in \mathbb{N}^0$ to include $n = 3$).

(**c**) We have $8^2 \overset{10}{=} 4$. We also have $8^4 \overset{10}{=} 6$ and hence $\left(8^4\right)^m \overset{10}{=} 6$ (rule 11 of § 2.7 as well as rule 16 of § 1.8). On multiplying these two congruences side by side (using rule 10 of § 2.7) we get:

$$8^2 \times \left(8^4\right)^m \overset{10}{=} 4 \times 6 \quad \rightarrow \quad 8^{2+4m} \overset{10}{=} 24 \quad \rightarrow \quad 8^{2+4m} \overset{10}{=} 4$$

[128] We do not need to test the solvability of $8n^2-3n+13 \overset{7}{=} 0$ because (by rule 22 of § 1.9) the solvability of $5n^2-6n+3 \overset{7}{=} 0$ is enough (noting that $8n^2 - 3n + 13 \overset{7}{=} 0$ is not solvable).

Hence, $n = 2 + 4m$ ($m \in \mathbb{N}^0$ to include $n = 2$).

(**d**) We have $13^4 \overset{10}{=} 1$ and hence $\left(13^4\right)^m \overset{10}{=} 1$ (rule 11 of § 2.7). Hence, $n = 4m$ ($m \in \mathbb{N}$). In fact, even $n = 0$ is a valid solution to this congruence (and hence $m \in \mathbb{N}^0$).

(**e**) We have $17^1 \overset{60}{=} 17$. We also have $17^4 \overset{60}{=} 1$ and hence $\left(17^4\right)^m \overset{60}{=} 1$ (rule 11 of § 2.7). On multiplying these two congruences side by side (using rule 10 of § 2.7) we get:

$$17^1 \times \left(17^4\right)^m \overset{60}{=} 17 \times 1 \qquad \rightarrow \qquad 17^{1+4m} \overset{60}{=} 17$$

Hence, $n = 1 + 4m$ ($m \in \mathbb{N}^0$ to include $n = 1$).

2. Solve the following exponential congruence equations (where $n \in \mathbb{N}$):

(**a**) $121^n - 11^n - 20 \overset{9}{=} 0$. (**b**) $6^{3n} - (2)6^{2n} + 6^n \overset{17}{=} 0$. (**c**) $5^{2n} + (6)5^n - 8 \overset{13}{=} 0$.

Solution:

(**a**) We have:

$$121^n - 11^n - 20 = 11^{2n} - 11^n - 20 = (11^n + 4)(11^n - 5) \overset{9}{=} 0$$

This means that $(11^n + 4)(11^n - 5)$ must be divisible by 9 and hence we have three cases to consider:

• $(11^n + 4)$ is divisible by 9, i.e. $(11^n + 4) \overset{9}{=} 0$ and hence $11^n \overset{9}{=} -4 \overset{9}{=} 5$. On solving this congruence equation (using for instance the method we used in the previous Problem) we get: $n = 5+6m$ ($m \in \mathbb{N}^0$).

• $(11^n - 5)$ is divisible by 9, i.e. $(11^n - 5) \overset{9}{=} 0$ and hence $11^n \overset{9}{=} 5$ (i.e. the same as the previous case).[129]

• $(11^n + 4)$ is divisible by 3 and $(11^n - 5)$ is divisible by 3, i.e. $11^n \overset{3}{=} -4 \overset{3}{=} 2$ and $11^n \overset{3}{=} 5 \overset{3}{=} 2$. On solving this congruence equation (i.e. $11^n \overset{3}{=} 2$) we get: $n = 1 + 2m$ ($m \in \mathbb{N}^0$), i.e. n is odd positive.

Noting that the general solution of the first two cases is included in the general solution of the third case, we conclude that the general solution of the given congruence equation is $\mathbb{O} \ni n > 0$.

Note: as indicated in the previous footnote, all these details are unnecessary if we noticed that $(11^n + 4)(11^n - 5) \overset{9}{=} 0$ is equivalent to $(11^n + 4)^2 \overset{9}{=} 0$ and hence we must have $(11^n + 4) \overset{3}{=} 0$ [see rule 23 and Problem 20 of § 1.9 noting that $(11^n + 4)^2 \overset{9}{=} 0$ is equivalent to $3^2 | (11^n + 4)^2$ and $3 | (11^n + 4)$ is equivalent to $(11^n + 4) \overset{3}{=} 0$]. However, we wanted to show the standard method of solution.

(**b**) We have:

$$6^{3n} - (2)6^{2n} + 6^n = 6^n \left[6^{2n} - (2)6^n + 1\right] = 6^n (6^n - 1)^2 \overset{17}{=} 0$$

This means that $6^n(6^n - 1)^2$ must be divisible by 17 and hence we have two cases to consider (see rule 22 of § 1.9):

• 6^n is divisible by 17, i.e. $6^n \overset{17}{=} 0$ which has no solution (noting that 6^n cannot have a factor of 17 to be divisible by 17).

• $(6^n - 1)$ is divisible by 17, i.e. $6^n - 1 \overset{17}{=} 0$ and hence $6^n \overset{17}{=} 1$. On solving this congruence equation (using for instance the method we used in the previous Problem) we get: $n = 16m$ ($m \in \mathbb{N}$).

So, the general solution of the given congruence equation is: $n = 16m$ ($m \in \mathbb{N}$).

(**c**) We have:

$$5^{2n} + (6)5^n - 8 = 5^{2n} + (6)5^n + 9 - 9 - 8 = (5^n + 3)^2 - 17 \overset{13}{=} 0 \qquad \rightarrow \qquad N^2 \overset{13}{=} 4$$

where $N = 5^n + 3$. Now, the solution of $N^2 \overset{13}{=} 4$ is $N \overset{13}{=} 2$ and $N \overset{13}{=} 11$ (see § 3.2.1). Accordingly, we have two cases:

• $5^n + 3 \overset{13}{=} 2$, i.e. $5^n \overset{13}{=} -1 \overset{13}{=} 12$ which has the general solution (see the previous Problem) $n = 2 + 4m$ ($m \in \mathbb{N}^0$).

• $5^n + 3 \overset{13}{=} 11$, i.e. $5^n \overset{13}{=} 8$ which has the general solution $n = 3 + 4m$ ($m \in \mathbb{N}^0$).

So, the general solutions of the given congruence equation are: $n = 2 + 4m$ and $n = 3 + 4m$ ($m \in \mathbb{N}^0$).

[129] In fact, we should have noticed this earlier because $(11^n - 5) \overset{9}{=} 0$ is equivalent to $11^n \overset{9}{=} 5 \overset{9}{=} -4$, i.e. $(11^n + 4) \overset{9}{=} 0$. Hence, $(11^n + 4)(11^n - 5) \overset{9}{=} 0$ is equivalent to $(11^n + 4)^2 \overset{9}{=} 0$.

3. Solve the following exponential congruence equations (where $n \in \mathbb{N}$):

(**a**) $21^{n+5} \overset{9^n}{=} 0$. (**b**) $77^{3n-1} \overset{8^n+1}{=} 0$. (**c**) $3^n + 5 \overset{5^{n-1}+2}{=} 0$.

Solution:

(**a**) This congruence equation means 9^n divides 21^{n+5}, that is:

$$\frac{21^{n+5}}{9^n} = \frac{3^{n+5} \times 7^{n+5}}{3^{2n}} = 3^{n+5-2n} \times 7^{n+5} = 3^{5-n} \times 7^{n+5}$$

Now, $(3^{5-n} \times 7^{n+5})$ is an integer if $(5-n) \geq 0$. So, considering that $n \in \mathbb{N}$, only $n = 1, 2, 3, 4, 5$ meet this condition, and hence the solutions of $21^{n+1} \overset{9^n}{=} 0$ are $n = 1, 2, 3, 4, 5$.

(**b**) This congruence equation means $(8^n + 1)$ divides 77^{3n-1}. However, if $(8^n + 1)$ divides 77^{3n-1} then $(8^n + 1)$ must contain a factor of 7 (noting that $77 = 7 \times 11$) which means that $(8^n + 1)$ must be divisible by 7. But we will show (by induction) that $(8^n + 1)$ is not divisible by 7. For $n = 1$ we have $(8^1 + 1) = 9$ which is not divisible by 7. Now, let assume that $(8^n + 1)$ is not divisible by 7 for a given $k \in \mathbb{N}$ $\left[\text{i.e. } (8^k + 1) \overset{7}{\neq} 0\right]$ and we will show that if this is the case then $(8^{k+1} + 1)$ is not divisible by 7, that is:

$$8^{k+1} + 1 = (8^k \times 8) + 1 = (8^k \times 7) + (8^k + 1) \overset{7}{=} (8^k + 1) \overset{7}{\neq} 0$$

So, $(8^n + 1)$ is not divisible by 7 for any $n \in \mathbb{N}$ and hence it does not contain a factor of 7. Therefore, $(8^n + 1)$ cannot divide 77^{3n-1} and thus the given congruence equation has no solution.

(**c**) This congruence equation means $(5^{n-1} + 2)$ divides $(3^n + 5)$. However, if $(5^{n-1} + 2)$ should divide $(3^n + 5)$ then $(5^{n-1} + 2)$ must not exceed $(3^n + 5)$ in magnitude. But it is obvious that $(5^{n-1} + 2)$ grows faster in magnitude than $(3^n + 5)$ as n increases which means that we expect $(5^{n-1} + 2)$ to exceed $(3^n + 5)$ in magnitude very soon (as n grows). Hence, the given congruence equation can be satisfied only for low values of $n \in \mathbb{N}$. On testing the first few values of $n \in \mathbb{N}$ we find that only $n = 2$ satisfies the given congruence equation. So, $n = 2$ is the only solution to the given congruence equation.

3.2.5 Mixed Polynomial-Exponential Congruence Equations

We present in the Problems of this subsection a few simple examples of mixed polynomial-exponential congruence equations in one variable and demonstrate how they are solved.

Problems

1. Solve the following mixed polynomial-exponential congruence equation: $2n^3 - 4n^2 + 5^n \overset{11}{=} a$ (where $n \in \mathbb{N}$ and $a = 0, 1, \ldots, 10$).

Solution: For $n \overset{11}{=} 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$ we have $2n^3 - 4n^2 \overset{11}{=} 9, 0, 7, 9, 7, 2, 6, 9, 1, 5, 0$. For $n = 1, 2, 3, 4, 5$ we have $5^n \overset{11}{=} 5, 3, 4, 9, 1$ and this cycle of 5 repeats itself every 5 consecutive integers. Accordingly, we have a cycle of 55 (i.e. 11×5). This cycle of 55 is given in the following table where the columns represent the ones digits of n and the rows represent the tens digits of n. For example, the cell corresponding to row "**2**" and column "**7**" represents $2n^3 - 4n^2 + 5^n \overset{11}{=} 10$ for $n = 27$.

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0		3	3	0	7	8	7	9	2	10
1	6	5	1	4	5	10	1	5	10	7
2	2	10	3	2	9	8	3	10	6	4
3	10	6	8	4	7	1	1	1	0	0
4	7	3	4	9	9	10	5	10	2	5
5	3	0	1	5	3	1				

Accordingly:

- $2n^3 - 4n^2 + 5^n \overset{11}{=} 0$ for $n = m + 55k$ (where $m = 3, 38, 39, 51$ and $k \in \mathbb{N}^0$).
- $2n^3 - 4n^2 + 5^n \overset{11}{=} 1$ for $n = m + 55k$ (where $m = 12, 16, 35, 36, 37, 52, 55$ and $k \in \mathbb{N}^0$).

- $2n^3 - 4n^2 + 5^n \overset{11}{=} 2$ for $n = m + 55k$ (where $m = 8, 20, 23, 48$ and $k \in \mathbb{N}^0$).
- $2n^3 - 4n^2 + 5^n \overset{11}{=} 3$ for $n = m + 55k$ (where $m = 1, 2, 22, 26, 41, 50, 54$ and $k \in \mathbb{N}^0$).
- $2n^3 - 4n^2 + 5^n \overset{11}{=} 4$ for $n = m + 55k$ (where $m = 13, 29, 33, 42$ and $k \in \mathbb{N}^0$).
- $2n^3 - 4n^2 + 5^n \overset{11}{=} 5$ for $n = m + 55k$ (where $m = 11, 14, 17, 46, 49, 53$ and $k \in \mathbb{N}^0$).
- $2n^3 - 4n^2 + 5^n \overset{11}{=} 6$ for $n = m + 55k$ (where $m = 10, 28, 31$ and $k \in \mathbb{N}^0$).
- $2n^3 - 4n^2 + 5^n \overset{11}{=} 7$ for $n = m + 55k$ (where $m = 4, 6, 19, 34, 40$ and $k \in \mathbb{N}^0$).
- $2n^3 - 4n^2 + 5^n \overset{11}{=} 8$ for $n = m + 55k$ (where $m = 5, 25, 32$ and $k \in \mathbb{N}^0$).
- $2n^3 - 4n^2 + 5^n \overset{11}{=} 9$ for $n = m + 55k$ (where $m = 7, 24, 43, 44$ and $k \in \mathbb{N}^0$).
- $2n^3 - 4n^2 + 5^n \overset{11}{=} 10$ for $n = m + 55k$ (where $m = 9, 15, 18, 21, 27, 30, 45, 47$ and $k \in \mathbb{N}^0$).

2. Solve the following mixed polynomial-exponential congruence equations (where $n \in \mathbb{N}$):

(**a**) $3^n - 3n^2 \overset{5}{=} 0$. (**b**) $7n^3 - 4n^2 + 5^n \overset{3}{=} 0$.

(**c**) $n^4 - 3n^3 - 3 + 4326^n \overset{10}{=} 0$. (**d**) $(4)3^n + 3n^4 - 3n^2 \overset{12}{=} 0$.

Solution:

(**a**) We have $3(3^{n-1} - n^2) \overset{5}{=} 0$ and hence by dividing both sides by 3 (see rule 7 of § 2.7) we get $3^{n-1} - n^2 \overset{5}{=} 0$.

Now, for $n = 1, 2, 3, 4$ we have $3^{n-1} \overset{5}{=} 1, 3, 4, 2$ and this cycle of 4 repeats itself every 4 consecutive integers. Also, for $n = 1, 2, 3, 4, 5$ we have $n^2 \overset{5}{=} 1, 4, 4, 1, 0$ and this cycle of 5 repeats itself every 5 consecutive integers. Accordingly, $3^{n-1} - n^2 \overset{5}{=} 0$ has a cycle of 20 (i.e. 4×5). On inspecting the first 20 natural numbers, we find that $n = 1, 3, 7, 9$ satisfy the congruence $3^{n-1} - n^2 \overset{5}{=} 0$ (i.e. $3^{n-1} \overset{5}{=} n^2$ for these values of n). Therefore, the solutions of the given congruence equation are $n = m + 20k$ (where $m = 1, 3, 7, 9$ and $k \in \mathbb{N}^0$).

(**b**) For $n \overset{3}{=} 1, 2, 3$ we have $7n^3 - 4n^2 \overset{3}{=} 0, 1, 0$ while for 5^n we have a cycle of 2 (i.e. $5^n \overset{3}{=} 2$ for odd n and $5^n \overset{3}{=} 1$ for even n). Accordingly, we have a cycle of 6. On inspecting the first 6 natural numbers, we find that only $n = 5$ satisfies the congruence $7n^3 - 4n^2 + 5^n \overset{3}{=} 0$. Therefore, the solutions of the given congruence equation are $n = 5 + 6k$ (where $k \in \mathbb{N}^0$).

(**c**) $4326^n \overset{10}{=} 6$ for all $n \in \mathbb{N}$ (see rule 17 of § 1.8) while for $n = 1, 2, 3, 4, 5$ we have $n^4 - 3n^3 - 3 \overset{10}{=} 5, 9, 7, 1, 7$ and this cycle of 5 repeats itself every 5 consecutive integers. Therefore, there is no $n \in \mathbb{N}$ such that $n^4 - 3n^3 - 3 + 4326^n \overset{10}{=} 0$. In fact, if we were vigilant then we could have reached this conclusion with no effort by noting that $n^4 - 3n^3 - 3 + 4326^n$ is always odd and hence it cannot be divisible by 10 which is even.

(**d**) From rule 9 of § 2.7 we have $(4)3^{n-1} + n^4 - n^2 \overset{4}{=} 0$. Now, $(4)3^{n-1}$ is obviously divisible by 4. Also, $(n^4 - n^2)$ is divisible by 4 because $n^4 - n^2 = (n^2 - n)(n^2 + n)$ and both $(n^2 - n)$ and $(n^2 + n)$ are even (see the rules of parity in § 1.8). Therefore, by rule 14 of § 1.9, $(4)3^{n-1} + n^4 - n^2$ is divisible by 4, i.e. $(4)3^n + 3n^4 - 3n^2 \overset{12}{=} 0$ for all $n \in \mathbb{N}$.

3.2.6 Congruence Equations Involving Roots

We present in the Problems of this subsection a few simple examples of univariate congruence equations involving roots and demonstrate how they are solved.

Problems

1. Solve the following congruence equations (where $n \in \mathbb{Z}$):

(**a**) $\sqrt[3]{n} - 5\sqrt[2]{n} \overset{8}{=} 0$. (**b**) $\sqrt[3]{n} + \sqrt[5]{n} \overset{3}{=} 0$. (**c**) $n - \sqrt{n} \overset{4}{=} 0$.

(**d**) $n + 2\sqrt{n} \overset{7}{=} 0$. (**e**) $3n + 5\sqrt[3]{n} - 1 \overset{2}{=} 0$. (**f**) $n + 7\sqrt[5]{n} + 6 \overset{2}{=} 0$.

Solution:

(**a**) We outline the solution in the following points:

• $\sqrt[2]{n}$ requires n to be non-negative, i.e. $n \in \mathbb{N}^0$.
• $\sqrt[3]{n}$ must be an integer and hence n must be a cube of an integer, i.e. $n = a^3$ $(a \in \mathbb{N}^0)$.
• $\sqrt[2]{n}$ must be an integer and hence n must be a square of an integer, i.e. $n = b^2$ $(b \in \mathbb{Z})$. Hence, $a^3 = b^2$, i.e. $b = (\sqrt[2]{a})^3$.
• If $n = 0$ then $\sqrt[6]{n}$ is an integer. If $n \neq 0$ then $\sqrt[6]{n}$ must also be an integer as will be shown in the next point.
• $\sqrt[6]{n} = \sqrt[2]{\sqrt[3]{n}} = \sqrt[2]{a}$ is an integer because if $\sqrt[2]{a}$ is not an integer then it must be irrational (see rule 28 of § 1.8) and hence $b = (\sqrt[2]{a})^3 = a\sqrt[2]{a}$ must be irrational because it is a product of an integer (i.e. a) times an irrational number (i.e. $\sqrt[2]{a}$) which is a contradiction because b is an integer.
• So in brief, $\sqrt[6]{n}$ is an integer which means that n is a sixth power of an integer, i.e. $n = c^6$ $(c \in \mathbb{Z})$.
• Accordingly, the given congruence equation becomes: $c^2 - 5c^3 \stackrel{8}{=} 0$ $(c \in \mathbb{Z})$. Now, we have two main cases: $c \leq 0$ and $c > 0$.
• If $c \leq 0$ then $c^2 - 5c^3 = c^2 + 5|c|^3 \stackrel{8}{=} 0$ has the solutions: $c = m + 8k$ where $m = 3, 4, 8$ and $\mathbb{Z} \ni k < 0$.
• If $c > 0$ then $c^2 - 5c^3 = c^2 - 5|c|^3 \stackrel{8}{=} 0$ has the solutions: $c = m + 8k$ where $m = 4, 5, 8$ and $\mathbb{Z} \ni k \geq 0$.
• So in brief, the solution of $\sqrt[3]{n} - 5\sqrt[2]{n} \stackrel{8}{=} 0$ is $n = c^6 = (m + 8k)^6$ (where $m = 3, 4, 8$ for $k < 0$, and $m = 4, 5, 8$ for $k \geq 0$).
(**b**) $\sqrt[3]{n}$ and $\sqrt[5]{n}$ must be integers and hence n must be a 15^{th} power of an integer, i.e. $n = a^{15}$ where $a \in \mathbb{Z}$. Now, we have 3 cases:
• $a \stackrel{3}{=} 0$ and hence $a = 3k$ $(k \in \mathbb{Z})$. Accordingly:

$$\sqrt[3]{n} + \sqrt[5]{n} = \sqrt[3]{3^{15}k^{15}} + \sqrt[5]{3^{15}k^{15}} = 3^5k^5 + 3^3k^3 \stackrel{3}{=} 0$$

• $a \stackrel{3}{=} 1$ and hence $a = 3k + 1$ $(k \in \mathbb{Z})$. Accordingly (see Eq. 13):

$$\sqrt[3]{n} + \sqrt[5]{n} = \sqrt[3]{(3k+1)^{15}} + \sqrt[5]{(3k+1)^{15}} = (3k+1)^5 + (3k+1)^3 \stackrel{3}{=} 1^5 + 1^3 = 2 \stackrel{3}{\neq} 0$$

• $a \stackrel{3}{=} 2$ and hence $a = 3k + 2$ $(k \in \mathbb{Z})$. Accordingly (see Eq. 13):

$$\sqrt[3]{n} + \sqrt[5]{n} = \sqrt[3]{(3k+2)^{15}} + \sqrt[5]{(3k+2)^{15}} = (3k+2)^5 + (3k+2)^3 \stackrel{3}{=} 2^5 + 2^3 = 40 \stackrel{3}{=} 1 \stackrel{3}{\neq} 0$$

Therefore, the solution of the given congruence equation is: $n = a^{15}$ where $a = 3k$ $(k \in \mathbb{Z})$.
(**c**) We must have $n \in \mathbb{N}^0$ because of $\sqrt{n}$. Also, $\sqrt{n}$ must be an integer and hence if $m = \sqrt{n}$ $(m \in \mathbb{N}^0)$ then the given congruence equation becomes $m^2 - m \stackrel{4}{=} 0$. The solutions of this equation (see § 3.2.1) are $m = 4k$ and $m = 1 + 4k$ $(k \in \mathbb{N}^0)$, i.e. $\sqrt{n} = 4k$ and $\sqrt{n} = 1 + 4k$ and hence $n = 16k^2$ and $n = (1 + 4k)^2$.
So in brief, the solutions are: $n = 16k^2$ and $n = (1 + 4k)^2$ where $k \in \mathbb{N}^0$.
(**d**) We must have $n \in \mathbb{N}^0$ because of $\sqrt{n}$. Also, $\sqrt{n}$ must be an integer and hence if $m = \sqrt{n}$ $(m \in \mathbb{N}^0)$ then the given congruence equation becomes $m^2 + 2m \stackrel{7}{=} 0$. The solutions of this equation (see § 3.2.1) are $m = 7k$ and $m = 5 + 7k$ $(k \in \mathbb{N}^0)$, i.e. $\sqrt{n} = 7k$ and $\sqrt{n} = 5 + 7k$ and hence $n = 49k^2$ and $n = (5 + 7k)^2$.
So in brief, the solutions are: $n = 49k^2$ and $n = (5 + 7k)^2$ where $k \in \mathbb{N}^0$.
(**e**) $\sqrt[3]{n}$ must be an integer and hence n and $\sqrt[3]{n}$ must have the same parity which means that $3n + 5\sqrt[3]{n} - 1$ is always odd (see the rules of parity in § 1.8). Therefore, the given congruence equation has no solution in $n \in \mathbb{Z}$.
(**f**) $\sqrt[5]{n}$ must be an integer and hence n and $\sqrt[5]{n}$ must have the same parity which means that $n + 7\sqrt[5]{n} + 6$ is always even (see the rules of parity in § 1.8). Therefore, the given congruence equation has a solution for all $\sqrt[5]{n} \in \mathbb{Z}$, i.e. for all $n = k^5$ where $k \in \mathbb{Z}$.

3.2.7 Congruence Equations Involving Fractions

We present in the Problems of this subsection a few simple examples of univariate congruence equations involving fractions and demonstrate how they are solved.

Problems

1. Solve the following congruence equations (where $n \in \mathbb{Z}$):

(**a**) $\frac{435}{n} + 3n \overset{5}{=} a \quad (a = 0, 1, 2, 3, 4)$. (**b**) $\frac{60}{n} + \frac{1200}{n^2} \overset{13}{=} a \quad (a = 0, 1, 2, \ldots, 12)$.

(**c**) $7n^3 - \frac{900}{n^2} + 143 \overset{17}{=} a \quad (a = 0, 1, 2, \ldots, 16)$.

Solution:

(**a**) $\frac{435}{n}$ must be an integer and hence n must be a divisor of 435.

The divisors of 435 are 1, 3, 5, 15, 29, 87, 145, 435 and their negatives. On trying these divisors we find the following:

- $\frac{435}{n} + 3n \overset{5}{=} 0$ has no solution.
- $\frac{435}{n} + 3n \overset{5}{=} 1$ has the solutions: $n = -15, -3, 87, 435$.
- $\frac{435}{n} + 3n \overset{5}{=} 2$ has the solutions: $n = -145, -1, 5, 29$.
- $\frac{435}{n} + 3n \overset{5}{=} 3$ has the solutions: $n = -29, -5, 1, 145$.
- $\frac{435}{n} + 3n \overset{5}{=} 4$ has the solutions: $n = -435, -87, 3, 15$.

(**b**) $\frac{60}{n} + \frac{1200}{n^2} = \frac{60n+1200}{n^2}$ must be an integer. Now, if $\frac{60n+1200}{n^2}$ should be an integer then we must have either:

$$\frac{60n+1200}{n^2} = 0 \text{ (i.e. } n = -20) \qquad \text{or} \qquad |60n + 1200| \geq n^2 \text{ (whose solution is: } -15 \leq n \leq 75)$$

On trying these values of n we find the following:

- $\frac{60}{n} + \frac{1200}{n^2} \overset{13}{=} a$ has no solution for $a = 1, 2, 3, 4, 7, 11$.
- $\frac{60}{n} + \frac{1200}{n^2} \overset{13}{=} 0$ has the solution: $n = -20$.
- $\frac{60}{n} + \frac{1200}{n^2} \overset{13}{=} 5$ has the solutions: $n = 2, 10$.
- $\frac{60}{n} + \frac{1200}{n^2} \overset{13}{=} 6$ has the solutions: $n = -10, 20$.
- $\frac{60}{n} + \frac{1200}{n^2} \overset{13}{=} 8$ has the solutions: $n = -4, 5$.
- $\frac{60}{n} + \frac{1200}{n^2} \overset{13}{=} 9$ has the solution: $n = -1$.
- $\frac{60}{n} + \frac{1200}{n^2} \overset{13}{=} 10$ has the solutions: $n = -5, -2$.
- $\frac{60}{n} + \frac{1200}{n^2} \overset{13}{=} 12$ has the solutions: $n = 1, 4$.

(**c**) $\frac{900}{n^2}$ must be an integer and hence n^2 must be a divisor of 900. The divisors of 900 are 1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 25, 30, 36, 45, 50, 60, 75, 90, 100, 150, 180, 225, 300, 450, 900 and their negatives. However, because $n^2 > 0$ we consider only the positive divisors. Moreover, because n is an integer, n^2 must be a perfect square. So in brief, the only eligible values of n are: $n = 1, 2, 3, 5, 6, 10, 15, 30$ and their negatives. On trying these values of n we find the following:

- $7n^3 - \frac{900}{n^2} + 143 \overset{17}{=} a$ has no solution for $a = 3, 4, 5, 6, 9, 10, 16$.
- $7n^3 - \frac{900}{n^2} + 143 \overset{17}{=} 0$ has the solutions: $n = -6, 30$.
- $7n^3 - \frac{900}{n^2} + 143 \overset{17}{=} 1$ has the solution: $n = -1$.
- $7n^3 - \frac{900}{n^2} + 143 \overset{17}{=} 2$ has the solution: $n = -10$.
- $7n^3 - \frac{900}{n^2} + 143 \overset{17}{=} 7$ has the solution: $n = -3$.
- $7n^3 - \frac{900}{n^2} + 143 \overset{17}{=} 8$ has the solutions: $n = -15, 2$.
- $7n^3 - \frac{900}{n^2} + 143 \overset{17}{=} 11$ has the solutions: $n = 3, 10$.
- $7n^3 - \frac{900}{n^2} + 143 \overset{17}{=} 12$ has the solution: $n = -30$.
- $7n^3 - \frac{900}{n^2} + 143 \overset{17}{=} 13$ has the solution: $n = 5$.
- $7n^3 - \frac{900}{n^2} + 143 \overset{17}{=} 14$ has the solution: $n = -5$.
- $7n^3 - \frac{900}{n^2} + 143 \overset{17}{=} 15$ has the solutions: $n = -2, 1, 6, 15$.

3.3 Systems of Ordinary Equations

There are two main methods for solving systems of ordinary univariate equations in number theory. The first is based on using the traditional methods of solving systems of multivariate equations (as investigated in algebra and linear algebra for instance) such as by substitution and comparison, and the second is by solving the individual equations separately (either by the general methods of algebra or by the special methods and techniques of number theory) and selecting the solutions that satisfy the system as a whole (i.e. by accepting only the solutions which are common to all the equations). In the following Problems we highlight the use of these methods in a few examples. Also see § 4.3.

It is useful to note that the set of solutions of a system of equations is the intersection of the sets of solutions of its individual equations. As a result, a system of equations is solvable only if its individual equations are solvable, although the converse is not true in general. Accordingly, a system of equations has no solution if some of its equations have no solution, but a system may not have a solution even though all its individual equations have solutions (i.e. when the intersection of these solutions is empty).

Problems

1. Solve the following systems of univariate ordinary equations (where $n \in \mathbb{Z}$):

(**a**) $n^3 - 49n + 120 = 0$	$n^2 + 3n - 18 = 0.$	
(**b**) $4n^2 + 8n + 13 = 0$	$2n^4 - 3n + 1 = 0.$	
(**c**) $n^4 - n^3 - 22n^2 + 16n + 96 = 0$	$n^3 + 8n^2 - 15n - 54 = 0$	$n^2 - n - 6 = 0.$
(**d**) $n^2 - 6n - 55 = 0$	$n^2 - 17n + 66 = 0$	$n^2 - n - 30 = 0.$
(**e**) $2n^5 - 15n^4 - 135n^3 - 125n^2 + 273n = 0$	$(70)3^n - 7^n = 203$	$9^{2n+1} - 9^n = 720.$

Solution:

(**a**) If we solve these equations individually (e.g. by the methods demonstrated in § 3.1.1), we find that the first equation has the solutions $n = -8, 3, 5$ while the second equation has the solutions $n = -6, 3$. Hence, the solution of this system is $n = 3$.

Similarly, if we compare these equations (i.e. $n^3 - 49n + 120 = n^2 + 3n - 18$) then we get $n^3 - n^2 - 52n + 138 = 0$ which has only one integer solution, i.e. $n = 3$.

(**b**) This system has no solution because the first equation has no solution (noting that its left hand side is odd and hence it cannot be equal to 0 which is even).

(**c**) If we solve these equations individually we find that the first equation has the solutions $n = -2, 3, \pm 4$ and the second equation has the solutions $n = -9, -2, 3$ while the third equation has the solutions $n = -2, 3$. Hence, the solutions of this system are $n = -2, 3$.

(**d**) The solutions of the first equation are $n = -5, 11$ and the solutions of the second equation are $n = 6, 11$ while the solutions of the third equation are $n = -5, 6$. Hence, this system has no solution because the intersection of the solutions of the three equations is empty (even though the intersection of the solutions of each two equations is not empty).

(**e**) The solutions of the first equation (according to part c of Problem 3 of § 3.1.1) are $n = -3, 0, 1, 13$. The solutions of the second equation (according to part a of Problem 1 of § 3.1.2) are $n = 1, 5$. The solution of the third equation (according to part h of Problem 1 of § 3.1.2) is $n = 1$. Hence, the solution of this system is $n = 1$.

3.4 Systems of Congruence Equations

If the system is made of (solvable) linear congruence equations then we can use the Chinese remainder method (see § 2.7.3) or the equivalent equation method (see § 2.7.4) where solution is guaranteed to exist only if the moduli are pairwise coprime. If the system is made of non-linear congruences (or mixed of linear and non-linear) then we need to consider some rather elaborate methods (some of which will be illustrated in the following Problems).

Problems

1. Solve the following systems of (linear) congruence equations:

   (**a**) $6n + 3 \overset{2}{=} 0$ $4n + 8 \overset{3}{=} 0$ $19n - 7 \overset{11}{=} 0$.

   (**b**) $3n - 23 \overset{10}{=} 0$ $14n + 9 \overset{17}{=} 0$ $n + 8 \overset{27}{=} 0$ $60n + 9 \overset{29}{=} 0$.

   (**c**) $4n - 20 \overset{3}{=} 0$ $n + 4 \overset{8}{=} 0$ $n + 10 \overset{15}{=} 0$ $3n - 63 \overset{23}{=} 0$.

   (**d**) $2n + 14 \overset{5}{=} 0$ $n - 13 \overset{12}{=} 0$ $3n + 78 \overset{17}{=} 0$ $5n - 195 \overset{24}{=} 0$.

   Solution:
   (**a**) The congruence equation $6n + 3 \overset{2}{=} 0$ is not solvable (because the left hand side is odd while the right hand side is even). Hence, the system has no solution.
   (**b**) These congruences are solvable individually. By moving the constant terms to the right hand side followed by multiplying by the modular inverse of the coefficients of n we get the following (simpler) system:

   $$n \overset{10}{=} 1 \qquad n \overset{17}{=} 3 \qquad n \overset{27}{=} 19 \qquad n \overset{29}{=} 10$$

   The moduli are pairwise coprime and hence a unique solution is guaranteed to exist. On solving this system (by the Chinese remainder method or by the equivalent equation method) we get: $n = 65521$. As we see, 65521 satisfies all these congruences.
   So, the general solution to the given congruence system is: $n = 65521 + 133110k$ ($k \in \mathbb{Z}$).
   (**c**) These congruences are solvable individually and can be simplified (as we did in part b), that is:

   $$n \overset{3}{=} 2 \qquad n \overset{8}{=} 4 \qquad n \overset{15}{=} 5 \qquad n \overset{23}{=} 21$$

   The moduli are not pairwise coprime and hence there is no guarantee that a solution exists. However, let's try! On solving this system (as we did in part b) we get: $n = 1700$. As we see, 1700 satisfies all these congruences.
   So, the general solution to the given congruence system is: $n = 1700 + 2760k$ ($k \in \mathbb{Z}$).
   (**d**) These congruences are solvable individually and can be simplified (as we did in part b), that is:

   $$n \overset{5}{=} 3 \qquad n \overset{12}{=} 1 \qquad n \overset{17}{=} 8 \qquad n \overset{24}{=} 15$$

   This system has no solution (noting that the moduli are not pairwise coprime and hence there is no guarantee that a solution exists).

2. Solve the following systems of (non-linear) congruence equations:

   (**a**) $15n - 8 \overset{31}{=} 0$ $6n^2 - 22n + 49 \overset{11}{=} 0$.

   (**b**) $n^2 - 165 \overset{7}{=} 0$ $2n^2 - 84 \overset{17}{=} 0$.

   (**c**) $n^2 + 4n - 10 \overset{5}{=} 0$ $3n^3 - n^2 + 4n - 22 \overset{29}{=} 0$.

   (**d**) $n^5 - 6n^4 + 212n - 12 \overset{7}{=} 0$ $n^3 + 3n^2 + 5n - 12 \overset{9}{=} 0$ $n^5 - 8n^3 - 35n + 2 \overset{25}{=} 0$.

   Solution:
   (**a**) We note first that in this part the system is not linear even though one of the congruences is linear. If we solve these congruences individually (using the methods investigated earlier; see for instance the Problems of § 3.2.1) then we get: $n \overset{31}{=} 15$, $n \overset{11}{=} 1$, $n \overset{11}{=} 10$. On considering these combinations (as we did in § 3.2.1) we get:

mod 31	15	15
mod 11	1	10
mod 341	232	263

   On solving the two pairs of linear congruences (using for instance the Chinese remainder theorem; see § 2.7.3) we get the (smallest positive) solutions in the last row of this table. So, the general solutions are: $n = m + 341k$ (where $m = 232, 263$ and $k \in \mathbb{Z}$).

(**b**) If we solve these congruences individually (using the methods investigated earlier; see for instance the Problems of § 3.2.1) then we get: $n \overset{7}{=} 2$, $n \overset{7}{=} 5$, $n \overset{17}{=} 5$, $n \overset{17}{=} 12$. On considering all these combinations (as we did in § 3.2.1) we get:

mod 7	2	2	5	5
mod 17	5	12	5	12
mod 119	107	114	5	12

On solving the four pairs of linear congruences (using for instance the Chinese remainder theorem; see § 2.7.3) we get the (smallest positive) solutions in the last row of this table. So, the general solutions are: $n = m + 119k$ (where $m = 5, 12, 107, 114$ and $k \in \mathbb{Z}$).

(**c**) If we solve these congruences individually (as we did before) then we get: $n \overset{5}{=} 0$, $n \overset{5}{=} 1$, $n \overset{29}{=} 5$, $n \overset{29}{=} 7$, $n \overset{29}{=} 27$. On considering all these combinations (as we did in § 3.2.1) we get:

mod 5	0	0	0	1	1	1
mod 29	5	7	27	5	7	27
mod 145	5	65	85	121	36	56

On solving the six pairs of linear congruences (e.g. by the Chinese remainder theorem) we get the (smallest positive) solutions in the last row of this table. So, the general solutions are: $n = m + 145k$ (where $m = 5, 36, 56, 65, 85, 121$ and $k \in \mathbb{Z}$).

(**d**) If we solve these congruences individually (as we did before) then we get: $n \overset{7}{=} 6$, $n \overset{9}{=} 2$, $n \overset{9}{=} 6$, $n \overset{9}{=} 7$, $n \overset{25}{=} 2$, $n \overset{25}{=} 16$. On considering all these combinations (as we did in § 3.2.1) we get:

mod 7	6	6	6	6	6	6
mod 9	2	2	6	6	7	7
mod 25	2	16	2	16	2	16
mod 1575	902	1091	1077	1266	727	916

On solving the six triples of linear congruences we get the (smallest positive) solutions in the last row of this table. So, the general solutions are: $n = m + 1575k$ (where $m = 727, 902, 916, 1077, 1091, 1266$ and $k \in \mathbb{Z}$).

3. Find $n \in \mathbb{Z}$ that satisfies the following systems of congruence equations:

(**a**) $n - 15 \overset{2n+3}{=} 0$ $\quad n + 9 \overset{n-8}{=} 0$.

(**b**) $8n + 24 \overset{2n-36}{=} 0$ $\quad 5n - 3 \overset{3n-14}{=} 0$.

(**c**) $44n - 4 \overset{2n+8}{=} 0$ $\quad 6n^2 - 18n + 4 \overset{3n-7}{=} 0$.

(**d**) $n^2 + 8n - 6 \overset{n+27}{=} 0$ $\quad 3n^3 - 9n - 13 \overset{5n+1}{=} 0$.

(**e**) $4n^2 + 6n - 4 \overset{3n-23}{=} 0$ $\quad 5n^3 - 3n + 5 \overset{4n+19}{=} 0$ $\quad 12n^2 - 28 \overset{n+12}{=} 0$.

Solution:

(**a**) If we solve these congruence equations individually from a divisibility perspective (following the methods we used in Problems 9 and 10 of § 3.2.1) we find:

• For $n - 15 \overset{2n+3}{=} 0$ we have $n = -18, -7, -3, -2, -1, 0, 4, 15$ (of which we accept only $n = 0, 4, 15$ since the modulo must be greater than 1).

• For $n + 9 \overset{n-8}{=} 0$ we have $n = -9, 7, 9, 25$ (of which we accept only $n = 25$).

As we see, there is no n that solves these congruence equations simultaneously. So, this system has no solution.

(**b**) If we solve these congruence equations individually from a divisibility perspective we find:

• For $8n + 24 \overset{2n-36}{=} 0$ we have $n = -66$, -24, -10, -3, 4, 6, 11, 12, 14, 15, 16, 17, 19, 20, 21, 22, 24, 25, 30, 32, 39, 46, 60, 102 (of which we accept only $n = 19, 20, 21, 22, 24, 25, 30, 32, 39, 46, 60, 102$).

• For $5n - 3 \overset{3n-14}{=} 0$ we have $n = 5, 25$ (of which we accept only $n = 25$).

As we see, only $n = 25$ solves these congruence equations simultaneously, and this is acceptable from

the congruence perspective (i.e. considering the modulo to be greater than 1) as well as from the divisibility perspective.

(**c**) If we solve these congruence equations individually from a divisibility perspective we find:

• For $44n - 4 \overset{2n+8}{=} 0$ we have $n = -94, -49, -34, -22, -19, -14, -13, -10, -9, -7, -6, -5, -3, -2, -1, 1, 2, 5, 6, 11, 14, 26, 41, 86$.

• For $6n^2 - 18n + 4 \overset{3n-7}{=} 0$ we have: $n = -3, 1, 2, 3, 5$.

From the divisibility perspective, $n = -3, 1, 2, 5$ solve these congruence equations simultaneously. However, from the congruence perspective (i.e. considering the modulo to be greater than 1) we accept only $n = 5$.

(**d**) If we solve these congruence equations individually from a divisibility perspective we find:

• For $n^2 + 8n - 6 \overset{n+27}{=} 0$ we have $n = -534, -196, -66, -40, -30, -28, -26, -24, -14, 12, 142, 480$.

• For $3n^3 - 9n - 13 \overset{5n+1}{=} 0$ we have $n = 0, 12$.

As we see, only $n = 12$ solves these congruence equations simultaneously, and this is acceptable from the congruence perspective (i.e. considering the modulo to be greater than 1) as well as from the divisibility perspective.

(**e**) If we solve these congruence equations individually from a divisibility perspective we find:

• For $4n^2 + 6n - 4 \overset{3n-23}{=} 0$ we have $n = -408, -21, -2, 7, 8, 22, 27, 839$.

• For $5n^3 - 3n + 5 \overset{4n+19}{=} 0$ we have $n = -2760, -85, -82, -5, -4, 21, 22, 8261$.

• For $12n^2 - 28 \overset{n+12}{=} 0$ we have $n = -1712, -862, -437, -352, -182, -112, -97, -80, -62, -46, -37, -32, -29, -22, -17, -16, -14, -13, -11, -10, -8, -7, -2, 5, 8, 13, 22, 38, 56, 73, 88, 158, 328, 413, 838, 1688$.

As we see, only $n = 22$ solves these congruence equations simultaneously, and this is acceptable from the congruence perspective (i.e. considering the modulo to be greater than 1) as well as from the divisibility perspective.

4. Solve the following systems of congruence equations (where $n \in \mathbb{N}$):

(**a**) $3^n - 1 \overset{7}{=} 0$ $\quad$ $4^n - 1 \overset{7}{=} 0$ $\quad$ $5^n - 1 \overset{7}{=} 0$.

(**b**) $3^n - 3 \overset{5}{=} 0$ $\quad$ $5^n - 5 \overset{8}{=} 0$ $\quad$ $n^5 - 3n^3 \overset{11}{=} 0$.

(**c**) $n^5 - 3n^2 \overset{4}{=} 0$ $\quad$ $n^4 \overset{9}{=} 0$ $\quad$ $7^{n-1} + 3 \overset{13}{=} 0$.

Solution:

(**a**) We note first that in this part we use a single modulo in all the congruence equations. If we solve these congruences individually (see § 3.2.4) we find that:

• The solution of $3^n - 1 \overset{7}{=} 0$ is $n = 6k$ (where $k \in \mathbb{N}$).

• The solution of $4^n - 1 \overset{7}{=} 0$ is $n = 3k$ (where $k \in \mathbb{N}$).

• The solution of $5^n - 1 \overset{7}{=} 0$ is $n = 6k$ (where $k \in \mathbb{N}$).

Hence, the solution of this system is $n = 6k$ (where $k \in \mathbb{N}$).

(**b**) If we solve these congruences individually (see § 3.2.1 and § 3.2.4) we find that:

• The solution of $3^n - 3 \overset{5}{=} 0$ is $n = 1 + 4k$ (where $k \in \mathbb{N}^0$), i.e. $n \overset{4}{=} 1$.

• The solution of $5^n - 5 \overset{8}{=} 0$ is $n = 1 + 2k$ (where $k \in \mathbb{N}^0$), i.e. $n \overset{2}{=} 1$.

• The solutions of $n^5 - 3n^3 \overset{11}{=} 0$ are $n \overset{11}{=} 0, 5, 6$.

Now, the solution of the 2-congruence system $n \overset{2}{=} 1$ and $n \overset{4}{=} 1$ is $n \overset{4}{=} 1$ because $n \overset{4}{=} 1$ is what is common between $n \overset{2}{=} 1$ and $n \overset{4}{=} 1$. So, what we need is to solve the 2-congruence systems $n \overset{4}{=} 1$ and $n \overset{11}{=} 0, 5, 6$. On considering these combinations (as we did earlier) we get:

mod 4	1	1	1
mod 11	0	5	6
mod 44	33	5	17

On solving these three pairs of linear congruences (using for instance the Chinese remainder theorem;

see § 2.7.3) we get the (smallest positive) solutions in the last row of this table. So, the solutions of the given system of congruence equations are: $n = m + 44k$ (where $m = 5, 17, 33$ and $k \in \mathbb{N}^0$).

(**c**) If we solve these congruences individually (see § 3.2.1 and § 3.2.4) we find that:

- The solutions of $n^5 - 3n^2 \overset{4}{=} 0$ are $n \overset{4}{=} 0, 2, 3$.
- The solution of $n^4 \overset{9}{=} 0$ is $n \overset{3}{=} 0$.
- The solution of $7^{n-1} + 3 \overset{13}{=} 0$ is $n \overset{12}{=} 3$.

Now, the solution of the 2-congruence system $n \overset{3}{=} 0$ and $n \overset{12}{=} 3$ is $n \overset{12}{=} 3$ because $n \overset{12}{=} 3$ is what is common between $n \overset{3}{=} 0$ and $n \overset{12}{=} 3$. Also, the solution of the 2-congruence systems $n \overset{4}{=} 0, 2, 3$ and $n \overset{12}{=} 3$ is $n \overset{12}{=} 3$ because $n \overset{12}{=} 3$ is what is common between $n \overset{4}{=} 0, 2, 3$ and $n \overset{12}{=} 3$.

So in brief, the solution of the given system of congruence equations is $n \overset{12}{=} 3$.

3.5 Congruence Equations with Multiple Moduli

In § 3.2 we investigated the methods of solution of univariate congruence equations with a single modulo (like $15n^2 - n - 2 \overset{7}{=} 0$), while in § 3.4 we investigated the methods of solution of systems of univariate congruence equations with multiple moduli (like $4n + 8 \overset{3}{=} 0$ and $19n - 7 \overset{11}{=} 0$).[130] So, in § 3.2 we deal with a *single* univariate congruence equation with a *single* modulo, while in § 3.4 we deal with *multiple* univariate congruence equations with *multiple* moduli.

In this section, we will investigate how to deal with something in between these cases, that is the case of a *single* univariate congruence equation with *multiple* moduli such as $n^2 - n + 3 \overset{6}{=} 0$ and $n^2 - n + 3 \overset{11}{=} 0$. So, this case is like the case of § 3.2 from the perspective of having a single equation, and it is like the case of § 3.4 from the perspective of having *multiple* moduli (and hence *multiple* "equations" as if we are dealing with a system of equations).

Problems

1. Solve the following "systems" of congruence equations (where $n \in \mathbb{Z}$):

(**a**) $6n + 43 \overset{11}{=} 0$ $\quad$ $6n + 43 \overset{25}{=} 0$.

(**b**) $5n^2 - 16n - 33 \overset{5}{=} 0$ $\quad$ $5n^2 - 16n - 33 \overset{61}{=} 0$.

(**c**) $3n^3 - 16n^2 + n - 1 \overset{3}{=} 0$ $\quad$ $3n^3 - 16n^2 + n - 1 \overset{31}{=} 0$ $\quad$ $3n^3 - 16n^2 + n - 1 \overset{83}{=} 0$.

Solution:

(**a**) The solution of the congruence equation $6n + 43 \overset{11}{=} 0$ is $n \overset{11}{=} 2$, while the solution of the congruence equation $6n + 43 \overset{25}{=} 0$ is $n \overset{25}{=} 22$.[131]

Now, if we solve the system of congruence equations $n \overset{11}{=} 2$ and $n \overset{25}{=} 22$ simultaneously (using for instance the Chinese remainder method; see § 2.7.3) then we get $n \overset{275}{=} 222$, that is:

$$n = 222 + (11 \times 25)k = 222 + 275k \qquad (k \in \mathbb{Z})$$

So, the solution of the given system is $n = 222 + 275k$ where $k \in \mathbb{Z}$.

(**b**) The solution of the congruence equation $5n^2 - 16n - 33 \overset{5}{=} 0$ is $n \overset{5}{=} 2$, while the solutions of the congruence equation $5n^2 - 16n - 33 \overset{61}{=} 0$ are $n \overset{61}{=} 20$ and $n \overset{61}{=} 32$.

Now, if we solve the system of congruence equations $n \overset{5}{=} 2$ and $n \overset{61}{=} 20$ simultaneously then we get $n \overset{305}{=} 142$, that is:

$$n = 142 + (5 \times 61)k = 142 + 305k \qquad (k \in \mathbb{Z})$$

[130] We should mention the exception of part (a) of Problem 4 of § 3.4 where we used a single modulo in all the congruence equations.

[131] The reader is referred to § 3.2.1 for the methods of solving such congruence equations.

Similarly, if we solve the system of congruence equations $n \overset{5}{=} 2$ and $n \overset{61}{=} 32$ simultaneously then we get $n \overset{305}{=} 32$, that is:

$$n = 32 + (5 \times 61)k = 32 + 305k \qquad (k \in \mathbb{Z})$$

So, the solutions of the given system are $n = 142 + 305k$ and $n = 32 + 305k$ where $k \in \mathbb{Z}$.

(**c**) The solution of the congruence equation $3n^3 - 16n^2 + n - 1 \overset{3}{=} 0$ is $n \overset{3}{=} 2$.

The solution of the congruence equation $3n^3 - 16n^2 + n - 1 \overset{31}{=} 0$ is $n \overset{31}{=} 9$.

The solution of the congruence equation $3n^3 - 16n^2 + n - 1 \overset{83}{=} 0$ is $n \overset{83}{=} 59$.

Now, if we solve the system of congruence equations $n \overset{3}{=} 2$, $n \overset{31}{=} 9$ and $n \overset{83}{=} 59$ simultaneously then we get $n \overset{7719}{=} 3047$, that is:

$$n = 3047 + (3 \times 31 \times 83)k = 3047 + 7719k \qquad (k \in \mathbb{Z})$$

So, the solution of the given system is $n = 3047 + 7719k$ where $k \in \mathbb{Z}$.

2. Solve the following "systems" of congruence equations (where $n \in \mathbb{N}$):

(**a**) $3^n - 1 \overset{4}{=} 0$ $\qquad$ $3^n - 1 \overset{5}{=} 0$ $\qquad$ $3^n - 1 \overset{11}{=} 0$.

(**b**) $5^n - 4 \overset{3}{=} 0$ $\qquad$ $5^n - 4 \overset{7}{=} 0$ $\qquad$ $5^n - 4 \overset{19}{=} 0$.

Solution:

(**a**) The solution of $3^n - 1 \overset{4}{=} 0$ is $n = 2k$ $(k \in \mathbb{N})$, i.e. $n \overset{2}{=} 0$. The solution of $3^n - 1 \overset{5}{=} 0$ is $n = 4k$ $(k \in \mathbb{N})$, i.e. $n \overset{4}{=} 0$. The solution of $3^n - 1 \overset{11}{=} 0$ is $n = 5k$ $(k \in \mathbb{N})$, i.e. $n \overset{5}{=} 0$.

Now, the solution of the system $n \overset{2}{=} 0$, $n \overset{4}{=} 0$ and $n \overset{5}{=} 0$ is $n = 20k$ $(k \in \mathbb{N})$. So, the solution of the given system is $n = 20k$ where $k \in \mathbb{N}$. In fact, even $n = 0$ is a solution to this system.

(**b**) The solution of $5^n - 4 \overset{3}{=} 0$ is $n = 2k$ $(k \in \mathbb{N})$, i.e. $n \overset{2}{=} 0$. The solution of $5^n - 4 \overset{7}{=} 0$ is $n = 2 + 6k$ $(k \in \mathbb{N}^0)$, i.e. $n \overset{6}{=} 2$. The solution of $5^n - 4 \overset{19}{=} 0$ is $n = 8 + 9k$ $(k \in \mathbb{N}^0)$, i.e. $n \overset{9}{=} 8$.

Now, the solution of the system $n \overset{2}{=} 0$, $n \overset{6}{=} 2$ and $n \overset{9}{=} 8$ is $n = 8 + 18k$ $(k \in \mathbb{N}^0)$. So, the solution of the given system is $n = 8 + 18k$ where $k \in \mathbb{N}^0$.

Chapter 4
Multivariate Equations and Systems

In this chapter we investigate some common types of multivariate equations (ordinary and modular) and systems of such equations and discuss and demonstrate how they are solved.

4.1 Diophantine Equations

Diophantine equation is an algebraic equation in two or more unknowns that involves only sums, products, and powers where all the constants (i.e. coefficients and powers) and allowed solutions are integers. Before we go through the details of the Diophantine equations it is important to take notice of the following points:

1. A Diophantine equation may have no solution, or a single solution, or multiple solutions (whether finitely many or infinitely many).
2. Before trying to solve a given Diophantine equation it is important to asses the sensibility of the equation quickly (by inspecting its general characteristics) to see if it is possible to have a solution or not. For example, by using the parity rules (see § 1.8) we can easily conclude that $16n - 22m = 219$ has no solution because the left hand side is even while the right hand side is odd. Similarly, $m^2 + n^4 = -256$ has no solution because the left hand side is non-negative while the right hand side is negative. So, in general an initial and systematic inspection using general rules (such as the rules of parity, sign, primality, divisibility, etc.) can save a lot of time trying to solve an equation that has no solution or has an obvious solution and hence it does not require any effort to solve. See Problem 1.
3. The previous point applies not only to single Diophantine equations but also to systems of Diophantine equations, i.e. if a system contains a non-solvable equation then the system is not solvable. So, it is worthwhile to inspect the individual equations of the system (to check if they are solvable or not) before trying to solve the system. It is also worthwhile to inspect the characteristics of the system as a whole to see if it is sensible to have a solution or not. See Problem 2.
4. It seems that there are some ambiguities and differences between authors about the "algebraic equation" term (which is used in the above definition of Diophantine equation) and this could affect the definition of Diophantine equation and its instances (e.g. whether equations involving negative or fractional powers are Diophantine equations or not). This is also related to the use and meaning of "polynomial" in the definition of Diophantine equation or algebraic equation which may occur in the writing of some authors. Anyway, these differences are generally trivial and are essentially about convention and terminology. So, it is useful to be aware of these differences and possible contradictions when reading the literature although the reader should focus on the content and essence (which should be clear in general and can be identified from explicit or implicit signs and indications).
5. Diophantine problems (such as solving Diophantine equations and systems of such equations) are generally more difficult to tackle and solve than their corresponding ordinary versions. This is because the demand for the solutions (and answers in general) to be integers imposes extra requirements and conditions and hence it usually complicates the process and methods of solution.

Problems

1. Determine (with justification) if the following Diophantine equations have solutions or not ($m, n \in \mathbb{Z}$):
   (**a**) $2m + 8n = 19$. (**b**) $21m^2 + 23n^2 = 291$. (**c**) $3m^3 - 27n = 677$. (**d**) $9m^6 + 13n^8 + 88 = 0$.
   Solution:
   (**a**) This equation has no solution because the left hand side is even while the right hand side is odd.
   (**b**) This equation has solution. For example, $m = 2$ and $n = 3$ is a solution.
   (**c**) This equation has no solution because $3m^3 - 27n = 3(m^3 - 9n)$ and 677 is prime and hence they cannot be equal (considering their prime factorization; see point 4 of § 2.1).

(**d**) This equation has no solution because $9m^6 + 13n^8$ is non-negative and hence the left hand side cannot be zero.

2. Why the following systems of Diophantine equations have no solution ($m, n, k \in \mathbb{Z}$):

   (**a**) $m^2 + n^8 + k^6 = 0$ $\quad$ $m^4 + n^2 - 17 = 0$.

   (**b**) $m^2 + n^3 - k^4 = 3$ $\quad$ $2m + n - n^2 = 75$.

   (**c**) $m + n - 9 = 0$ $\quad$ $(m + n)^2 = 49$.

   (**d**) $m^4 + n^5 + k - 43 = 0$ $\quad$ $m^2 + k^2 + 2mk - 101 = 0$.

   (**e**) $m^6 + n^2 - k^3 = 0$ $\quad$ $m^2 + n^4 + k + 1 = 0$ $\quad$ $m + n + k + 1 = 0$.

   Solution:
   (**a**) A quick initial inspection should reveal that the first equation has only the trivial solution (i.e. $n = m = k = 0$), while the second equation can have only non-trivial solutions (i.e. it cannot accept the trivial solution). This means that the two equations cannot have a common solution and hence the system has no solution.
   (**b**) A quick initial inspection should reveal that the second equation has no solution (due to parity violation) and hence the system has no solution.
   (**c**) According to the first equation, $(m + n) = 9$ and this is obviously inconsistent with the second equation which implies $(m + n) = \pm 7$.
   (**d**) If we write the second equation as $(m + k)^2 = 101$ then it is obvious that this equation has no solution because a perfect square cannot by prime (since 101 is prime). Therefore, this system has no solution.
   (**e**) If the first equation has a solution then k must be non-negative, while if the second equation has a solution then k must be negative. So, the two equations cannot have a common solution and hence this system has no solution.

3. A sum of two squares equation is a Diophantine equation of the form $m^2 + n^2 = k$ where $m, n \in \mathbb{Z}$ and $k \in \mathbb{N}^0$. Give some properties and theorems about this type of equations.
   Solution: Refer for instance to § 2.9.5 for some of the two squares theorems which reflect some of their properties.

4.1.1 Linear Diophantine Equations in Two Variables

A linear Diophantine equation in two variables is a Diophantine equation of the form:

$$ax + by = c \tag{62}$$

where x and y are variables and a, b, c are constants. We present in the following Problems a number of types of linear Diophantine equations in two variables and demonstrate how they are solved. However, before that we outline the main types of these equations and the methods that we use for their solution. In fact, we have three main cases:

1. $c = \gcd(a, b)$. In this case we use the extended Euclidean algorithm (see § 2.3.4) to express $\gcd(a, b)$ as a linear combination of a and b and hence we obtain the solution.
2. c is a multiple of $\gcd(a, b)$. In this case we use the extended Euclidean algorithm to express $\gcd(a, b)$ as a linear combination of a and b and obtain the solution by scaling the equation.
3. c is not equal to $\gcd(a, b)$ or a multiple of it. In this case there is no (integer) solution.

We finally note that when we get a solution in case 1 and case 2 by the extended Euclidean algorithm, what we actually get is a particular solution. So, to get the general (or complete) solution we use the fact that adding zero to the particular solution will not affect the solution. Hence, all we need to do is to express this zero in a special (and clever) way that generates all the possible solutions. This issue will be clarified in the Problems. We will also investigate in the Problems other methods and procedures that can be used to find the general solution of such Diophantine equations (including developing closed-form formulae).

Problems

1. Show the following:
   (**a**) The Diophantine equation $ax + by = c$ has a solution *iff* $g|c$ where $g = \gcd(a, b)$.
   (**b**) If the Diophantine equation $ax + by = c$ has a solution then it has infinitely many solutions (i.e. in $\mathbb{Z}$ although it may have no solution or only finitely many solutions in a subset of $\mathbb{Z}$).
   (**c**) If $\gcd(a, b) = 1$ then the Diophantine equation $ax + by = c$ has a solution (and hence infinitely many solutions).
   Solution:
   (**a**) **The if part**: if $g|c$ then $c = gc'$ (for some $c' \in \mathbb{Z}$). Now, by rule 8 of § 2.4 we have:

$$\begin{aligned} g &= ax' + by' && \text{(for some } x', y' \in \mathbb{Z}) \\ gc' &= ax'c' + by'c' && (\times c') \\ c &= ax + by && (gc' = c,\ x'c' = x,\ y'c' = y) \end{aligned}$$

   where $x, y \in \mathbb{Z}$ (since $c', x', y' \in \mathbb{Z}$), i.e. $ax + by = c$ has a solution which is $x = x'c'$ and $y = y'c'$.
   The only if part: if $ax + by = c$ has a solution (i.e. there are $x, y \in \mathbb{Z}$ such that $ax + by = c$) then g is a divisor of $(ax + by)$ and hence it is a divisor of c since $c = ax + by$, that is (where $ga' = a$, $gb' = b$ and $m \in \mathbb{Z}$):

$$ax + by = g(a'x + b'y) = gm = c$$

   i.e. $g|c$ noting that $m \in \mathbb{Z}$.
   (**b**) We note first that the homogeneous equation $ax_0 + by_0 = 0$ has infinitely many solutions (e.g. $x_0 = -bt$ and $y_0 = at$ where $t \in \mathbb{Z}$). Hence, if (X, Y) is a solution to the Diophantine equation $ax + by = c$ and we add to this Diophantine equation the homogeneous equation $ax_0 + by_0 = 0$ (which should not affect the solutions of the Diophantine equation since it is identically zero) then we obtain infinitely many solutions $(X + x_0, Y + y_0)$, that is:

$$c = aX + bY = aX + bY + 0 = aX + bY + (ax_0 + by_0) = a(X + x_0) + b(Y + y_0)$$

   In fact, it can be shown that all the solutions are given by $(X + x_0, Y + y_0)$.
   (**c**) If $\gcd(a, b) = 1$ then according to part (a) the equation must have a solution (since $1|c$). Hence, according to part (b) the equation must have infinitely many solutions.
   Note: as indicated and demonstrated in part (b), the Diophantine homogeneous equation $ax + by = 0$ always has a solution (and actually infinitely many solutions).
2. Find the general solution of the following linear Diophantine equations in two variables $(x, y \in \mathbb{Z})$:
   (**a**) $124x - 56y = 4$. (**b**) $39x + 169y = 65$. (**c**) $22x + 4y = 7$.
   Solution: In the following we use the extended Euclidean algorithm (see § 2.3.4) for expressing $\gcd(a, b)$ as a linear combination of a and b.
   (**a**) This is an example of case 1 (see the preamble of this subsection) because:

$$c = 4 = \gcd(124, -56) = 124(5) - 56(11)$$

   Hence, a particular solution is $x = 5$ and $y = 11$. We obtain the general solution as follows:

$$124(5) - 56(11) + \Big[0\Big] = 124(5) - 56(11) + \Big[124(14k) - 56(31k)\Big] = 124(5 + 14k) - 56(11 + 31k)$$

   Hence, the general solution is $x = 5 + 14k$ and $y = 11 + 31k$ $(k \in \mathbb{Z})$.[132]
   (**b**) This is an example of case 2 (see the preamble) because:

$$c = 65 = 5 \times 13 = 5 \times \gcd(39, 169) = 5 \times \Big[39(-4) + 169(1)\Big] = 39(-20) + 169(5)$$

[132] We note that it is easier in this case to simplify the equation first by dividing its two sides by $\gcd(a, b)$ when the gcd is > 1 to simplify the subsequent calculations (and hence our equation in this example becomes $31x - 14y = 1$). However, we preferred to work with the original equation without this simplification. In fact, this simplification should make the solvability of the equation obvious because the gcd after simplification is 1 (see part c of Problem 1).

Hence, a particular solution is $x = -20$ and $y = 5$. We obtain the general solution as follows:

$$39(-20) + 169(5) + \Big[0\Big] = 39(-20) + 169(5) + \Big[39(13k) + 169(-3k)\Big] = 39(-20 + 13k) + 169(5 - 3k)$$

Hence, the general solution is $x = -20 + 13k$ and $y = 5 - 3k$ ($k \in \mathbb{Z}$).[133]
(**c**) This is an example of case 3 (see the preamble) because $c = 7$ is not equal to or a multiple of $\gcd(22, 4) = 2$. Hence, there is no solution to this (as a Diophantine equation). This can also be easily seen from the fact that the left hand side is even while the right hand side is odd.

3. Show that if $ax + by = 0$ is a Diophantine equation and $g = \gcd(a, b)$ then all the solutions of this equation are given by $x = k(b/g)$ and $y = -k(a/g)$ where $k \in \mathbb{Z}$.
Solution: This equation has a solution since it is homogeneous (and in fact it has infinitely many solutions; see Problem 1). Moreover, it is obvious that $x = k(b/g)$ and $y = -k(a/g)$ represent valid solutions (which can be easily verified by substitution noting that b/g and a/g are integers). So, all we need to do is to show that all the solutions can be expressed in this form. To show this we use the LCE theorem (see § 3.2.1) as follows.
We can assume first that $ab \neq 0$ (where the other cases can be treated as special cases). We can also assume (with no loss of generality) that $b > 0$ (otherwise we multiply the equation by -1 to make $b > 0$ noting that this does not change the solutions). We can also assume that $b > 1$ (otherwise we multiply the equation by an integer > 1 to make $b > 1$ noting that this does not change the solutions). So in brief, we can assume that b is already > 1.
Now, if reduce the equation modulo b then we get $ax \stackrel{b}{=} 0$. So, from the LCE theorem (see Eq. 58 and related text), all the solutions of this congruence equation (noting that $x_0 = 0$, $m \equiv b$ and $d \equiv g$) are given by: $x = k(b/g)$ (where $k \in \mathbb{Z}$). Now, if we substitute this into the equation $ax + by = 0$ (to get the corresponding y's) then we get: $y = -k(a/g)$. So, all the solutions of the equation $ax + by = 0$ are given by $x = k(b/g)$ and $y = -k(a/g)$ where $k \in \mathbb{Z}$.

4. Find the general solutions of the following homogeneous linear Diophantine equations in two variables:
(**a**) $3x - 27y = 0$. (**b**) $5x + 48y = 0$. (**c**) $2x + 26y = 0$.
Solution: We use in this Problem the result of Problem 3.
(**a**) $\gcd(3, -27) = 3$ and hence the general solution is: $x = k(-27/3) = -9k$ and $y = -k(3/3) = -k$ ($k \in \mathbb{Z}$), i.e. $x = 9y$ and $y \in \mathbb{Z}$.
(**b**) $\gcd(5, 48) = 1$ and hence the general solution is: $x = k(48/1) = 48k$ and $y = -k(5/1) = -5k$ ($k \in \mathbb{Z}$).
(**c**) $\gcd(2, 26) = 2$ and hence the general solution is: $x = k(26/2) = 13k$ and $y = -k(2/2) = -k$ ($k \in \mathbb{Z}$), i.e. $x = -13y$ and $y \in \mathbb{Z}$.

5. Outline a practical procedure[134] to obtain the general solution of the Diophantine equation $ax+by = c$ (assuming it has a solution, i.e. $g|c$).
Solution: We do the following:
• Find a particular solution (x_0, y_0) to the equation $ax + by = g$ (where g is the gcd of a and b).[135]
• Let $x = (c/g)x_0$ and $y = (c/g)y_0$.
• Define $U = x - (c/g)x_0$ and $V = y - (c/g)y_0$.
• Obtain the solution of $aU + bV = 0$ (by using the result of Problem 3), i.e. $U = k(b/g)$ and $V = -k(a/g)$ where $k \in \mathbb{Z}$.
• Substitute for U and V and hence obtain the solution (i.e. x, y):

$$\begin{array}{lllll} U = k(b/g) & \rightarrow & x - (c/g)x_0 = k(b/g) & \rightarrow & x = (c/g)x_0 + k(b/g) \\ V = -k(a/g) & \rightarrow & y - (c/g)y_0 = -k(a/g) & \rightarrow & y = (c/g)y_0 - k(a/g) \end{array}$$

[133] We repeat the previous footnote noting that the equation after simplification in this example becomes $3x + 13y = 5$. We should also note that this simplification should unify case 1 and case 2 from the perspective of having a gcd equal to 1 after simplification.
[134] We mean a procedure that does not refer to or based on the extended Euclidean algorithm.
[135] Because we are not supposed to use the extended Euclidean algorithm, we can find a particular solution by inspection which is generally straightforward.

6. Find the general solution of parts (a) and (b) of Problem 2 using the procedure of Problem 5.
Solution:
(**a**) We have $g = \gcd(124, -56) = 4$.
• A particular solution to the equation $ax + by = g$ (i.e. $124x - 56y = 4$) is $x_0 = 5$ and $y_0 = 11$.
• Let $x = (c/g)x_0 = (4/4)5 = 5$ and $y = (c/g)y_0 = (4/4)11 = 11$.
• Define $U = x - (c/g)x_0 = x - 5$ and $V = y - (c/g)y_0 = y - 11$.
• Obtain the solution of $aU + bV = 124U - 56V = 0$, i.e. $U = k(b/g) = k(-56/4) = -14k$ and $V = -k(a/g) = -31k$.
• On substitution we obtain the general solution: $x = (c/g)x_0 + k(b/g) = 5 - 14k$ and $y = (c/g)y_0 - k(a/g) = 11 - 31k$.
Note: this solution is the same as the solution we obtained in part (a) of Problem 2 noting that $k \in \mathbb{Z}$ takes all the positive and negative values (i.e. k in one solution corresponds to $-k$ in the other solution).
(**b**) We have $g = \gcd(39, 169) = 13$.
• A particular solution to the equation $ax + by = g$ (i.e. $39x + 169y = 13$) is $x_0 = 9$ and $y_0 = -2$.
• Let $x = (c/g)x_0 = (65/13)9 = 45$ and $y = (c/g)y_0 = (65/13)(-2) = -10$.
• Define $U = x - (c/g)x_0 = x - 45$ and $V = y - (c/g)y_0 = y + 10$.
• Obtain the solution of $aU + bV = 39U + 169V = 0$, i.e. $U = k(b/g) = k(169/13) = 13k$ and $V = -k(a/g) = -k(39/13) = -3k$.
• On substitution we obtain the general solution: $x = (c/g)x_0 + k(b/g) = 45 + 13k$ and $y = (c/g)y_0 - k(a/g) = -10 - 3k$.
Note: this solution is the same as the solution we obtained in part (b) of Problem 2 because if $k' = k+5$ and we substitute this k' in the general solution of Problem 2 then we get:

$$x = -20 + 13k' = -20 + 13(k + 5) = 45 + 13k \qquad \text{and} \qquad y = 5 - 3k' = 5 - 3(k + 5) = -10 - 3k$$

which is the general solution obtained in the present Problem. So, the solutions are the same but k in one solution is shifted by 5 units from its value in the other solution and hence both generate all the possible solutions noting that $k \in \mathbb{Z}$.

7. Find the general solution of parts (a) and (b) of Problem 2 using modular arithmetic.
Solution:
(**a**) We have (see part a of point 8 of § 2.7.6):

$$124x - 56y = 4 \quad \rightarrow \quad 124x - 56y \overset{56}{=} 4 \quad \rightarrow \quad 124x \overset{56}{=} 4 \quad \rightarrow \quad 31x \overset{14}{=} 1 \quad \rightarrow \quad x = 5 + 14k_1$$

$$124x - 56y = 4 \quad \rightarrow \quad 124x - 56y \overset{124}{=} 4 \quad \rightarrow \quad -56y \overset{124}{=} 4 \quad \rightarrow \quad -14y \overset{31}{=} 1 \quad \rightarrow \quad y = 11 + 31k_2$$

where we used rule 9 of § 2.7 in the fourth steps. On substituting these forms of x and y in the equation $124x - 56y = 4$ we get:

$$124(5 + 14k_1) - 56(11 + 31k_2) = 4 \qquad \rightarrow \qquad 1736k_1 - 1736k_2 = 0 \qquad \rightarrow \qquad k_2 = k_1$$

So, the general solution is $x = 5 + 14k$ and $y = 11 + 31k$ ($k \in \mathbb{Z}$). This solution is the same as the solution of Problem 2.
(**b**) We have:

$$39x + 169y = 65 \quad \rightarrow \quad 39x + 169y \overset{169}{=} 65 \quad \rightarrow \quad 39x \overset{169}{=} 65 \quad \rightarrow \quad 3x \overset{13}{=} 5 \quad \rightarrow \quad x = 6 + 13k_1$$

$$39x + 169y = 65 \quad \rightarrow \quad 39x + 169y \overset{39}{=} 65 \quad \rightarrow \quad 169y \overset{39}{=} 65 \quad \rightarrow \quad 13y \overset{3}{=} 5 \quad \rightarrow \quad y = 2 + 3k_2$$

On substituting these forms of x and y in the equation $39x + 169y = 65$ we get:

$$39(6 + 13k_1) + 169(2 + 3k_2) = 65 \qquad \rightarrow \qquad 507k_1 + 507k_2 + 507 = 0 \qquad \rightarrow \qquad k_2 = -k_1 - 1$$

i.e. $y = 2 + 3(-k_1 - 1) = -1 - 3k_1$. So, the general solution is $x = 6 + 13k$ and $y = -1 - 3k$ ($k \in \mathbb{Z}$). This solution is the same as the solution of Problem 2 with an offset of 2 in the values of k due to the difference in the particular solutions.

8. Give a simple formula for the general solution of the Diophantine equation $ax + by = c$ (assuming it is solvable).
Solution: The general solution is $x = x_0 + (b/g)k$ and $y = y_0 - (a/g)k$ where $g = \gcd(a, b)$, (x_0, y_0) is a particular solution to the equation $ax + by = c$, and $k \in \mathbb{Z}$. This is a result of the fact that the general solution of the non-homogeneous equation $ax + by = c$ is the solution of the homogeneous equation $ax + by = 0$ (which we obtained in Problem 3) plus a particular solution of $ax + by = c$ (see Problem 2).
Note: all the results that we already obtained in the previous Problems can be easily obtained from this formula. However, we did not use this formula because we want to get more insight by demonstrating the different methods and techniques used in solving Diophantine equations. In fact, we will use this formula in the future for convenience.
9. We have 572 cars which we want to transport by trailers. There are two types of trailer: small (S) of capacity 7 cars, and large (L) of capacity 12 cars. The cost of transport on an S trailer is \$3750 and the cost of transport on an L trailer is \$5350. Do the following:
(**a**) Find the number of S and L trailers required to transport these cars such that all the trailers are fully loaded.
(**b**) Find the minimum cost required to transport these cars (i.e. with the condition that "all the trailers are fully loaded").
(**c**) Find the minimum cost required if we ignore the condition that "all the trailers are fully loaded".
Solution: This problem can be modeled (in its parts a and b) by the following Diophantine equation: $7x + 12y = 572$ where x is the required number of S trailers and y is the required number of L trailers (noting that $x, y \in \mathbb{N}^0$).
(**a**) From the formula of Problem 8 we get (using the particular solution $x_0 = 8$ and $y_0 = 43$):

$$x = x_0 + \frac{b}{g}k = 8 + \frac{12}{1}k = 8 + 12k \qquad \text{and} \qquad y = y_0 - \frac{a}{g}k = 43 - \frac{7}{1}k = 43 - 7k \qquad (k \in \mathbb{N}^0)$$

Now, by trying $k = 0, 1, \ldots$ while observing the condition $x, y \in \mathbb{N}^0$ we get all the acceptable solutions of x and y, that is:

$\boldsymbol{k}$	0	1	2	3	4	5	6
$\boldsymbol{x}$	8	20	32	44	56	68	80
$\boldsymbol{y}$	43	36	29	22	15	8	1

So, we have only 7 acceptable solutions.
(**b**) The total cost C is: $C = 3750x + 5350y$. On calculating the cost of these 7 acceptable solutions we find that the minimum cost is $C_{\min} = 3750(8) + 5350(43) = \$260050$ (which corresponds to $k = 0$).
(**c**) The transport cost per car for the S and L trailers are (respectively) $3750/7 \simeq \$535.71$ and $5350/12 \simeq \$445.83$. So, it is obvious that it is cheaper to transport the cars by L trailers. Now we need 47 fully-loaded L trailers to transport 564 cars and we need an extra L trailer to transport the remaining 8 cars. So, in total we need 48 L trailers to transport all the cars, and hence the minimum cost (without the condition of "fully loaded") is $48 \times 5350 = \$256800$.

4.1.2 Linear Diophantine Equations in Three Variables

In this subsection we investigate how to solve linear Diophantine equations in three variables (mostly by giving simple examples in which we demonstrate and illustrate the methods of solution). However, before that we note that the results that we obtained in Problem 1 of § 4.1.1 for Diophantine equations in two variables can be extended to Diophantine equations in three variables (and indeed to Diophantine equations in n variables), that is:
1. The Diophantine equation $ax + by + cz = d$ has a solution *iff* $g|d$ where $g = \gcd(a, b, c)$.
2. If the Diophantine equation $ax + by + cz = d$ has a solution then it has infinitely many solutions (i.e. in $\mathbb{Z}$ although it may have no solution or only finitely many solutions in a subset of $\mathbb{Z}$).

3. If $\gcd(a,b,c)=1$ then the Diophantine equation $ax+by+cz=d$ has a solution (and hence infinitely many solutions).

It is useful to take notice of the following remarks:

• The general solution of a Diophantine equation in n variables contains $(n-1)$ *free* parameters (and hence the general solution of a Diophantine equation in 3 variables contains 2 free parameters).[136]

• The homogeneous Diophantine equation (in any number of variables) is always solvable because it has (at least) the trivial solution (i.e. all its variables are zero). This is consistent with the fact that $g|0$ (also see Problem 1 of § 4.1.1).

• There are several (and possibly many) methods for solving linear Diophantine equations in three variables (some of which are unnecessarily messy).[137] Our choice (and preference) in the following Problems (and in general) is to use (when applicable) a simple method based on the fact that the general solution of a non-homogeneous equation is the solution of the corresponding homogeneous equation plus a particular solution.

• We will also investigate a closed form formula (or rather formulae considering the number of variables) that can be used to solve these equations. This formula can be more convenient to use in certain cases and circumstances (like in coding) and hence we will investigate its derivation and demonstrate its application.

Problems

1. Find the general solutions (if exist) of the following linear Diophantine equations in three variables $(x,y,z\in\mathbb{Z})$:

   (**a**) $2x+14y-22z=3$. (**b**) $6x+10y-19z=0$.

   (**c**) $21x+35y-12z=41$. (**d**) $48x-6y-14z=32$.

   Solution:

   (**a**) We have $g=\gcd(2,14,-22)=2$ and $d=3$. Since, $g\not|d$ then this equation has no solution. In fact, this can be easily inferred from the fact that the left hand side of this equation is even while its right hand side is odd.

   (**b**) This homogeneous equation is obviously solvable (because it has at least the trivial solution noting as well that 0 is divisible by any gcd). Now, if we write this equation as $6x-19z=-10y$ then it is obvious that this equation is solvable for any $y\in\mathbb{Z}$ because $g=\gcd(6,-19)=1$ (see part c of Problem 1 of § 4.1.1). So, let $y=s$ $(s\in\mathbb{Z})$. Now, a particular solution for $6x-19z=-10s$ is $x_0=11s$ and $z_0=4s$. So, from the formula of Problem 8 of § 4.1.1 we get (noting that b in that formula corresponds to c here):

   $$x=x_0+\frac{b}{g}k=11s+\frac{-19}{1}k=11s-19k \qquad \text{and} \qquad z=z_0-\frac{a}{g}k=4s-\frac{6}{1}k=4s-6k$$

   So, the general solution is:

   $$x=11s-19k \qquad y=s \qquad z=4s-6k \qquad (s,k\in\mathbb{Z})$$

   (**c**) This equation is solvable because $\gcd(21,35,-12)=1$ (see point 3 in the preamble). So, let first get the general solution of the homogeneous equation $21x+35y-12z=0$ (which is obviously solvable). If we write this homogeneous equation as $21x-12z=-35y$ then it is obvious that this equation is solvable for any $y=3s$ $(s\in\mathbb{Z})$ because $g=\gcd(21,-12)=3$ and $3|(-35\times 3s)=-105s$ (see part a of Problem 1 of § 4.1.1). So, let $y=3s$ $(s\in\mathbb{Z})$. Now, a particular solution for $21x-12z=-105s$ is $x_0=-5s$ and $z_0=0$. So, from the formula of Problem 8 of § 4.1.1 we get:

   $$x=x_0+\frac{b}{g}k=-5s+\frac{-12}{3}k=-5s-4k \qquad \text{and} \qquad z=z_0-\frac{a}{g}k=0-\frac{21}{3}k=-7k$$

[136] If there was more than $(n-1)$ parameters (see for instance Problem 2) then they are not free.

[137] It is worth noting that the methods of solving Diophantine equations in general (whether linear or not) largely depend in their applicability and validity on the specifications and types of the equations noting that some types may require case-specific methods and techniques. So in brief, there is no general method or technique of solution to Diophantine equations that can be applied in every case.

So, the general solution of the homogeneous equation $21x + 35y - 12z = 0$ is: $x = -5s - 4k$, $y = 3s$ and $z = -7k$ $(s, k \in \mathbb{Z})$.
A particular solution of the equation $21x + 35y - 12z = 41$ is: $(x_0, y_0, z_0) = (2, 1, 3)$.
So, the general solution of the equation $21x + 35y - 12z = 41$ is:

$$x = 2 - 5s - 4k \qquad y = 1 + 3s \qquad z = 3 - 7k \qquad (s, k \in \mathbb{Z})$$

(**d**) This equation is solvable because $\gcd(48, -6, -14) = 2$ which divides 32 (see point 1 in the preamble). First, we solve the homogeneous equation $48x - 6y - 14z = 0$. Writing this equation as $48x - 14z = 6y$ we can see it is solvable for any $y = s \in \mathbb{Z}$ because $g = \gcd(48, -14) = 2$ and $2|(6s)$ for any $s \in \mathbb{Z}$ (see part a of Problem 1 of § 4.1.1). So, let $y = s$ $(s \in \mathbb{Z})$. Now, a particular solution for $48x - 14z = 6s$ is $x_0 = s$ and $z_0 = 3s$. So, from the formula of Problem 8 of § 4.1.1 we get:

$$x = x_0 + \frac{b}{g}k = s + \frac{-14}{2}k = s - 7k \qquad \text{and} \qquad z = z_0 - \frac{a}{g}k = 3s - \frac{48}{2}k = 3s - 24k$$

So, the general solution of the homogeneous equation $48x - 6y - 14z = 0$ is: $x = s - 7k$, $y = s$ and $z = 3s - 24k$ $(s, k \in \mathbb{Z})$.
A particular solution of the equation $48x - 6y - 14z = 32$ is: $(x_0, y_0, z_0) = (3, 0, 8)$.
So, the general solution of the equation $48x - 6y - 14z = 32$ is:

$$x = 3 + s - 7k \qquad y = s \qquad z = 8 + 3s - 24k \qquad (s, k \in \mathbb{Z})$$

2. Find a formula for the general solution of the Diophantine equation $ax + by + cz = d$ (assuming it is solvable).
Solution: We are looking for a formula similar to the formula of Problem 8 of § 4.1.1. We first find a general solution to the homogeneous equation $ax + by + cz = 0$ and then add a particular solution $(x_0, y_{0,0} z)$ to it.
If we write $ax + by + cz = 0$ as $ax + cz = -by$ and follow the method of part (b) of Problem 1 then we get:

$$x = x_0 + \frac{c}{g_{ac}}m \qquad \text{and} \qquad z = z_0 - \frac{a}{g_{ac}}m$$

where $g_{ac} = \gcd(a, c)$ and $m \in \mathbb{Z}$.
Similarly, if we write $ax + by + cz = 0$ once as $ax + by = -cz$ and once as $by + cz = -ax$ then we get (respectively):

$$x = x_0 + \frac{b}{g_{ab}}n \qquad \text{and} \qquad z = z_0 - \frac{b}{g_{bc}}k$$

where $g_{ab} = \gcd(a, b)$, $g_{bc} = \gcd(b, c)$ and $n, k \in \mathbb{Z}$.
Now, if these equations are consistent then $x = x$ and $z = z$ and hence:

$$\begin{aligned} x - x &= \left(x_0 + \frac{c}{g_{ac}}m\right) - \left(x_0 + \frac{b}{g_{ab}}n\right) = \frac{c}{g_{ac}}m - \frac{b}{g_{ab}}n = 0 \\ z - z &= \left(z_0 - \frac{a}{g_{ac}}m\right) - \left(z_0 - \frac{b}{g_{bc}}k\right) = \frac{b}{g_{bc}}k - \frac{a}{g_{ac}}m = 0 \end{aligned}$$

If we substitute these expressions into the homogeneous equation $ax + by + cz = 0$ we get:

$$\begin{aligned} a\big[0\big] + by + c\big[0\big] &= 0 \\ a\left[\frac{c}{g_{ac}}m - \frac{b}{g_{ab}}n\right] + by + c\left[\frac{b}{g_{bc}}k - \frac{a}{g_{ac}}m\right] &= 0 \\ by + \left[\frac{bc}{g_{bc}}k - \frac{ab}{g_{ab}}n\right] &= 0 \\ y &= \frac{a}{g_{ab}}n - \frac{c}{g_{bc}}k \end{aligned}$$

This means that if $y = \frac{a}{g_{ab}}n - \frac{c}{g_{bc}}k$ then the homogeneous equation $ax + by + cz = 0$ is an identity. In other words, $x = \frac{c}{g_{ac}}m - \frac{b}{g_{ab}}n$, $y = \frac{a}{g_{ab}}n - \frac{c}{g_{bc}}k$ and $z = \frac{b}{g_{bc}}k - \frac{a}{g_{ac}}m$ satisfy the homogeneous equation identically for all values of m, n, k (where these three parameters are coupled by the y condition to reduce them effectively to just two parameters). If we now add the particular solution $(x_0, y_{0,0}\, z)$ to the general solution of the homogeneous equation $ax + by + cz = 0$ we get the general solution of the non-homogeneous equation $ax + by + cz = d$, that is:

$$x = x_0 + \frac{c}{g_{ac}}m - \frac{b}{g_{ab}}n \qquad y = y_0 + \frac{a}{g_{ab}}n - \frac{c}{g_{bc}}k \qquad z = z_0 + \frac{b}{g_{bc}}k - \frac{a}{g_{ac}}m$$

We finally note that if we use the identity $st = \gcd(s,t) \times \text{lcm}(s,t)$ [see part a of Problem 6 of § 2.5] then the formulae in the last equation can be simplified to the following forms:

$$\begin{aligned} x &= x_0 + \frac{m\,\text{lcm}(a,c) - n\,\text{lcm}(a,b)}{a} \\ y &= y_0 + \frac{n\,\text{lcm}(a,b) - k\,\text{lcm}(b,c)}{b} \\ z &= z_0 + \frac{k\,\text{lcm}(b,c) - m\,\text{lcm}(a,c)}{c} \end{aligned}$$

3. Show that the general solutions found in Problem 1 (parts b, c, d) are equivalent to the general solutions obtained from the formulae of Problem 2 (i.e. all the solutions of Problem 1 can be obtained from the formulae of Problem 2 and vice versa).
Solution:
(**b**) From part (b) of Problem 1 we have (where we replace k with t due to the use of k in the formulae of Problem 2):

$$x = 11s - 19t \qquad y = s \qquad z = 4s - 6t \qquad (s, t \in \mathbb{Z}) \tag{63}$$

while from the formulae of Problem 2 we get:

$$x = \frac{114m - 30n}{6} = 19m - 5n \qquad y = \frac{30n - 190k}{10} = 3n - 19k \qquad z = \frac{190k - 114m}{-19} = 6m - 10k \tag{64}$$

On equating x, y, z from Eq. 63 to x, y, z from Eq. 64 and simplifying we get:

$$19m - 5n = 11s - 19t \qquad 3n - 19k = s \qquad 6m - 10k = 4s - 6t$$

On solving these three equations in the variables s, t (treating m, n, k as parameters) we get:

$$s = 3n - 19k \qquad t = -m + 2n - 11k$$

This means that we always have $s, t \in \mathbb{Z}$ corresponding to $m, n, k \in \mathbb{Z}$ that produce $x, y, z \in \mathbb{Z}$ that satisfy the given equation.
Similarly, on solving these three equations in the variables m, n, k (treating s, t as parameters) we get:

$$m = \frac{2s + 5r}{3} - t \qquad n = \frac{s + 19r}{3} \qquad k = r \qquad (\text{for some } r \in \mathbb{Z})$$

Now, since $m, n, k \in \mathbb{Z}$ then we take $r = -s$ (noting that any $r \overset{3}{=} -s$ should suffice) and hence we can write these equations as:

$$m = -s - t \qquad n = -6s \qquad k = -s$$

This means that we always have $m, n, k \in \mathbb{Z}$ corresponding to $s, t \in \mathbb{Z}$ that produce $x, y, z \in \mathbb{Z}$ that satisfy the given equation (in fact we have infinitely many such $m, n, k \in \mathbb{Z}$ noting that the condition

$r = -s$ is a special case of the condition $r \stackrel{3}{=} -s$).
So, the two solutions are equivalent, (i.e. all the solutions found in part b of Problem 1 can be obtained from the formulae of Problem 2 and vice versa).
(**c**) From part (c) of Problem 1 we have (where we replace k with t due to the use of k in the formulae of Problem 2):

$$x = 2 - 5s - 4t \qquad y = 1 + 3s \qquad z = 3 - 7t \qquad (s, t \in \mathbb{Z}) \tag{65}$$

while from the formulae of Problem 2 we get:

$$x = 2 + \frac{84m - 105n}{21} = 2 + 4m - 5n \tag{66}$$

$$y = 1 + \frac{105n - 420k}{35} = 1 + 3n - 12k \tag{67}$$

$$z = 3 + \frac{420k - 84m}{-12} = 3 + 7m - 35k \tag{68}$$

On equating x, y, z from Eq. 65 to x, y, z from Eqs. 66-68 and simplifying we get:

$$4m - 5n = -5s - 4t \qquad 3n - 12k = 3s \qquad 7m - 35k = -7t$$

On solving these three equations in the variables s, t (treating m, n, k as parameters) we get:

$$s = n - 4k \qquad t = 5k - m$$

This means that we always have $s, t \in \mathbb{Z}$ corresponding to $m, n, k \in \mathbb{Z}$ that produce $x, y, z \in \mathbb{Z}$ that satisfy the given equation.
Similarly, on solving these three equations in the variables m, n, k (treating s, t as parameters) we get:

$$m = 5r - t \qquad n = 4r + s \qquad k = r \qquad (r \in \mathbb{Z})$$

This means that we always have $m, n, k \in \mathbb{Z}$ corresponding to $s, t \in \mathbb{Z}$ that produce $x, y, z \in \mathbb{Z}$ that satisfy the given equation (in fact we have infinitely many such $m, n, k \in \mathbb{Z}$ noting that we have infinitely many $r \in \mathbb{Z}$).
So, the two solutions are equivalent, (i.e. all the solutions found in part c of Problem 1 can be obtained from the formulae of Problem 2 and vice versa).
(**d**) From part (d) of Problem 1 we have (where we replace k with t due to the use of k in the formulae of Problem 2):

$$x = 3 + s - 7t \qquad y = s \qquad z = 8 + 3s - 24t \qquad (s, t \in \mathbb{Z}) \tag{69}$$

while from the formulae of Problem 2 we get:

$$x = 3 + \frac{336m - 48n}{48} = 3 + 7m - n \tag{70}$$

$$y = 0 + \frac{48n - 42k}{-6} = 7k - 8n \tag{71}$$

$$z = 8 + \frac{42k - 336m}{-14} = 8 + 24m - 3k \tag{72}$$

On equating x, y, z from Eq. 69 to x, y, z from Eqs. 70-72 and simplifying we get:

$$7m - n = s - 7t \qquad 7k - 8n = s \qquad 24m - 3k = 3s - 24t$$

On solving these three equations in the variables s, t (treating m, n, k as parameters) we get:

$$s = -8n + 7k \qquad t = -m - n + k$$

This means that we always have $s, t \in \mathbb{Z}$ corresponding to $m, n, k \in \mathbb{Z}$ that produce $x, y, z \in \mathbb{Z}$ that satisfy the given equation.
Similarly, on solving these three equations in the variables m, n, k (treating s, t as parameters) we get:

$$m = \frac{s - 8t + r}{8} \qquad n = \frac{7r - s}{8} \qquad k = r \qquad \text{(for some } r \in \mathbb{Z})$$

Now, since $m, n, k \in \mathbb{Z}$ then we take $r = -s$ (noting that any $r \stackrel{8}{=} -s$ should suffice) and hence we can write these equations as:

$$m = -t \qquad n = -s \qquad k = -s$$

This means that we always have $m, n, k \in \mathbb{Z}$ corresponding to $s, t \in \mathbb{Z}$ that produce $x, y, z \in \mathbb{Z}$ that satisfy the given equation (in fact we have infinitely many such $m, n, k \in \mathbb{Z}$ noting that the condition $r = -s$ is a special case of the condition $r \stackrel{8}{=} -s$).
So, the two solutions are equivalent, (i.e. all the solutions found in part d of Problem 1 can be obtained from the formulae of Problem 2 and vice versa).

4. Using a different method to the one used in Problem 2, find another formula for the general solution of the Diophantine equation $ax + by + cz = d$ (assuming it is solvable).
Solution: We use in this Problem a method (based on analytic geometry) whose essence is to convert the equation $ax+by+cz = d$ (which represents the Cartesian form of a plane surface in a 3D Euclidean space) to its equivalent parametric form in two integer parameters. In brief, the equation $ax+by+cz = d$ represents a plane in a 3D flat space and hence the Diophantine equation $ax + by + cz = d$ represents the triplets of integers (x, y, z) which are on this surface. So, we first obtain (through the equation $ax+by+cz = d$) three non-collinear points (i.e. three non-collinear triplets of integers) on this surface, say $\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3$. We then use the well known formula for obtaining the parametric form of a plane passing through a given point (say $\mathbf{r}_1$) and parallel to two vectors (say $\mathbf{r}_2 - \mathbf{r}_1$ and $\mathbf{r}_3 - \mathbf{r}_1$), that is:

$$\begin{aligned} \mathbf{r} &= \mathbf{r}_1 + (\mathbf{r}_2 - \mathbf{r}_1)u + (\mathbf{r}_3 - \mathbf{r}_1)v \\ (x, y, z) &= (x_1, y_1, z_1) + (x_2 - x_1, y_2 - y_1, z_2 - z_1)u + (x_3 - x_1, y_3 - y_1, z_3 - z_1)v \end{aligned}$$

where $u, v \in \mathbb{Z}$. Hence, the general solution of the Diophantine equation $ax + by + cz = d$ is:

$$x = x_1+(x_2-x_1)u+(x_3-x_1)v \qquad y = y_1+(y_2-y_1)u+(y_3-y_1)v \qquad z = z_1+(z_2-z_1)u+(z_3-z_1)v \tag{73}$$

where $u, v \in \mathbb{Z}$.
Note: we can derive a similar formula (or formulae) for the Diophantine equation in 2 variables following a similar method to the one used in this Problem by converting the equation $ax + by = c$ (which represents the Cartesian form of a straight line in a 2D plane) to its equivalent parametric form in one integer parameter.

5. Show that the general solutions found in Problem 1 (parts b, c, d) are equivalent to the general solutions obtained from the formulae of Problem 4 (i.e. all the solutions of Problem 1 can be obtained from the formulae of Problem 4 and vice versa).
Solution:
(**b**) Let $\mathbf{r}_1 = (0, 0, 0)$, $\mathbf{r}_2 = (-2, 81, 42)$ and $\mathbf{r}_3 = (4, 161, 86)$. So, from Eq. 73 we get:

$$x = -2u + 4v \qquad y = 81u + 161v \qquad z = 42u + 86v \tag{74}$$

On equating x, y, z from this equation to x, y, z obtained in part (b) of Problem 1 (replacing k with t) we get:

$$11s - 19t = -2u + 4v \qquad s = 81u + 161v \qquad 4s - 6t = 42u + 86v$$

On solving these three equations in the variables s, t (treating u, v as parameters) we get:

$$s = 81u + 161v \qquad t = 47u + 93v \qquad (u, v \in \mathbb{Z})$$

This means that we always have $s, t \in \mathbb{Z}$ corresponding to $u, v \in \mathbb{Z}$ that produce $x, y, z \in \mathbb{Z}$ that satisfy the given equation.
Similarly, on solving these three equations in the variables u, v (treating s, t as parameters) we get:

$$u = \frac{-93s + 161t}{34} \qquad v = \frac{47s - 81t}{34} \qquad (s, t \in \mathbb{Z})$$

Now, since $u, v \in \mathbb{Z}$ then we simply multiply these expressions by 34 and hence we take u and v as:

$$u = -93s + 161t \qquad v = 47s - 81t \qquad (s, t \in \mathbb{Z})$$

Accordingly, u, v in Eq. 74 must be scaled down by a factor of 34, that is:

$$x = \frac{-2u + 4v}{34} \qquad y = \frac{81u + 161v}{34} \qquad z = \frac{42u + 86v}{34}$$

This means that we always have $u, v \in \mathbb{Z}$ corresponding to $s, t \in \mathbb{Z}$ that produce $x, y, z \in \mathbb{Z}$ that satisfy the given equation.
So, the two solutions are equivalent, (i.e. all the solutions found in part b of Problem 1 can be obtained from the formulae of Problem 4 and vice versa).
(**c**) Let $\mathbf{r}_1 = (2, 1, 3)$, $\mathbf{r}_2 = (-7, 4, -4)$ and $\mathbf{r}_3 = (-2, 1, -4)$. So, from Eq. 73 we get:

$$x = 2 - 9u - 4v \qquad y = 1 + 3u \qquad z = 3 - 7u - 7v$$

On equating x, y, z from this equation to x, y, z obtained in part (c) of Problem 1 (replacing k with t) we get:

$$-5s - 4t = -9u - 4v \qquad 3s = 3u \qquad -7t = -7u - 7v$$

On solving these three equations in the variables s, t (treating u, v as parameters) we get:

$$s = u \qquad t = u + v$$

This means that we always have $s, t \in \mathbb{Z}$ corresponding to $u, v \in \mathbb{Z}$ that produce $x, y, z \in \mathbb{Z}$ that satisfy the given equation.
Similarly, on solving these three equations in the variables u, v (treating s, t as parameters) we get:

$$u = s \qquad v = t - s$$

This means that we always have $u, v \in \mathbb{Z}$ corresponding to $s, t \in \mathbb{Z}$ that produce $x, y, z \in \mathbb{Z}$ that satisfy the given equation.
So, the two solutions are equivalent, (i.e. all the solutions found in part c of Problem 1 can be obtained from the formulae of Problem 4 and vice versa).
(**d**) Let $\mathbf{r}_1 = (3, 0, 8)$, $\mathbf{r}_2 = (-4, 0, -16)$ and $\mathbf{r}_3 = (4, 1, 11)$. So, from Eq. 73 we get:

$$x = 3 - 7u + v \qquad y = v \qquad z = 8 - 24u + 3v$$

On equating x, y, z from this equation to x, y, z obtained in part (d) of Problem 1 (replacing k with t) we get:

$$s - 7t = -7u + v \qquad s = v \qquad 3s - 24t = -24u + 3v$$

On solving these three equations in the variables s, t (treating u, v as parameters) we get:

$$s = v \qquad t = u$$

This means that we always have $s, t \in \mathbb{Z}$ corresponding to $u, v \in \mathbb{Z}$ that produce $x, y, z \in \mathbb{Z}$ that satisfy the given equation.
Similarly, on solving these three equations in the variables u, v (treating s, t as parameters) we get:

$$u = t \qquad v = s$$

This means that we always have $u, v \in \mathbb{Z}$ corresponding to $s, t \in \mathbb{Z}$ that produce $x, y, z \in \mathbb{Z}$ that satisfy the given equation.
So, the two solutions are equivalent, (i.e. all the solutions found in part d of Problem 1 can be obtained from the formulae of Problem 4 and vice versa).

6. We have 572 trolleys which we want to transport by ship containers. There are three types of container: small (S) of capacity 30 trolleys, medium (M) of capacity 35 trolleys, and large (L) of capacity 39 trolleys. The cost of transport by an S container is £250, the cost of transport by an M container is £258 and the cost of transport by an L container is £263. Do the following:
(**a**) Find the number of S, M and L containers required to transport these trolleys such that all the containers are fully loaded.
(**b**) Find the minimum cost required to transport these trolleys (i.e. with the condition that "all the containers are fully loaded").
(**c**) Find the minimum cost required if we ignore the condition that "all the containers are fully loaded".
Solution: This problem can be modeled (in its parts a and b) by the following Diophantine equation: $30x + 35y + 39z = 572$ where x is the required number of S containers, y is the required number of M containers, and z is the required number of L containers (noting that $x, y, z \in \mathbb{N}^0$).
(**a**) Let first get the general solution of the homogeneous equation $30x+35y+39z = 0$ (which is obviously solvable). If we write this homogeneous equation as $30x + 39z = -35y$ then it is obvious that this equation is solvable for any $y = 3s$ ($s \in \mathbb{Z}$) because $g = \gcd(30, 39) = 3$ and $3|(-35 \times 3s) = -105s$ (see part a of Problem 1 of § 4.1.1). So, let $y = 3s$ ($s \in \mathbb{Z}$). Now, a particular solution for $30x+39z = -105s$ is $x_0 = 3s$ and $z_0 = -5s$. So, from the formula of Problem 8 of § 4.1.1 we get:

$$x = x_0 + \frac{b}{g}k = 3s + \frac{39}{3}k = 3s + 13k \qquad \text{and} \qquad z = z_0 - \frac{a}{g}k = -5s - \frac{30}{3}k = -5s - 10k$$

So, the general solution of the homogeneous equation $30x + 35y + 39z = 0$ is: $x = 3s + 13k$, $y = 3s$ and $z = -5s - 10k$ ($s, k \in \mathbb{Z}$).
A particular solution of the equation $30x + 35y + 39z = 572$ is: $(x_0, y_0, z_0) = (0, 13, 3)$.
So, the general solution of the equation $30x + 35y + 39z = 572$ is:

$$x = 3s + 13k \qquad y = 13 + 3s \qquad z = 3 - 5s - 10k \qquad (s, k \in \mathbb{Z})$$

Now, the capacity of container M is 35 and hence $572/35 \simeq 16$ and hence $0 \leq y \leq 16$. So, we need only to consider the values of $y = 1, 4, 7, 10, 13, 16$ which correspond to the values of $s = -4, -3, -2, -1, 0, 1$, that is (where we consider only the values of k that produce acceptable solutions, i.e. $x, y, z \geq 0$ and $30x + 35y + 39z = 572$):

$s = -4$	$k = 1$	$\rightarrow$	$x = 1$	$y = 1$	$z = 13$
$s = -4$	$k = 2$	$\rightarrow$	$x = 14$	$y = 1$	$z = 3$
$s = -3$	$k = 1$	$\rightarrow$	$x = 4$	$y = 4$	$z = 8$
$s = -2$	$k = 1$	$\rightarrow$	$x = 7$	$y = 7$	$z = 3$
$s = -1$		$\rightarrow$	No acceptable solution		
$s = 0$	$k = 0$	$\rightarrow$	$x = 0$	$y = 13$	$z = 3$
$s = 1$		$\rightarrow$	No acceptable solution		

So, we have only 5 acceptable solutions, i.e.
$(x, y, z) = (1, 1, 13), (14, 1, 3), (4, 4, 8), (7, 7, 3), (0, 13, 3)$.
(**b**) The total cost C is: $C = 250x+258y+263z$. On calculating the cost of these 5 acceptable solutions we find that the minimum cost is $C_{\min} = 250(1) + 258(1) + 263(13) =$ £3927 (which corresponds to $s = -4$ and $k = 1$).
(**c**) The transport cost per trolley for the S, M and L trailers are (respectively) $250/30 \simeq$ £8.33, $258/35 \simeq$ £7.37 and $263/39 \simeq$ £6.74. So, it is obvious that it is cheaper to transport the bulk of trolleys

by L containers. In fact, the solution in part (b) should indicate this. However, let see if we can find an even cheaper solution than the solution of part (b). The only potentially cheaper solution is to use 14 L containers to transport $14 \times 39 = 546$ trolleys and use 1 S container to transport the remaining $572 - 546 = 26$ trolleys. The cost of this option is $(14 \times 263) + (1 \times 250) =$ £3932. As we see, this solution is not cheaper than the solution of part (b). So, the minimum cost (with and without the condition of "fully loaded") is £3927 (i.e. by using 1 S, 1 M and 13 L containers).

4.1.3 Linear Diophantine Equations in Multiple Variables

In the last two subsections we investigated two cases of linear Diophantine equations in multiple variables (i.e. in two variables in § 4.1.1 and in three variables in § 4.1.2). In this subsection we generalize the principles and procedures of these subsections. So, a Diophantine equation in n variables given by:

$$\sum_{k=1}^{n} a_k x_k = b \qquad (a_k, x_k, b \in \mathbb{Z} \text{ and } a_k \neq 0) \tag{75}$$

has a solution $(X_1, X_2, \ldots, X_n)$ in $\mathbb{Z}$ *iff* $g|b$ where $g = \gcd(a_1, a_2, \ldots, a_n)$.

As before, if this equation has a solution then it has infinitely many solutions (i.e. in $\mathbb{Z}$ although it may have no solution or only finitely many solutions in a subset of $\mathbb{Z}$). Moreover, if $g = 1$ or $b = 0$ then this equation has always a solution (and hence infinitely many solutions in $\mathbb{Z}$).

Problems

1. Which of the following linear Diophantine equations has a solution:
   (**a**) $\sum_{k=1}^{20} kx_k = 23$. (**b**) $\sum_{k=1}^{6} (2k)^2 x_k = 14$. (**c**) $14x_1 + 35x_2 - 21x_3 + 119x_4 = 91$.
   Solution:
   (**a**) This equation has a solution because $\gcd(1, 2, \ldots, 20) = 1$ which divides 23.
   (**b**) This equation has no solution because $\gcd(4, 16, 36, 64, 100, 144) = 4$ which does not divide 14.
   (**c**) This equation has a solution because $\gcd(14, 35, -21, 119) = 7$ which divides 91.
2. Solve the following linear Diophantine equations in 4 variables:
   (**a**) $14x_1 + 35x_2 - 21x_3 + 119x_4 = 91$. (**b**) $36x_1 - 15x_2 + 26x_3 + 22x_4 = 3$.
   Solution:
   (**a**) This equation has a solution (see part c of Problem 1). To simplify the calculations and manipulations we divide both sides by 7 and hence we obtain: $2x_1 + 5x_2 - 3x_3 + 17x_4 = 13$.
   Let $X = 2x_1 + 5x_2$ and $Y = -3x_3 + 17x_4$. Hence, we have $X + Y = 13$ whose solution (according to the formula of Problem 8 of § 4.1.1) is: $X = 6 + k$ and $Y = 7 - k$ $(k \in \mathbb{Z})$, that is:

$$2x_1 + 5x_2 = 6 + k \qquad\qquad -3x_3 + 17x_4 = 7 - k$$

   Now, if we solve each one of these equations (using the formula of Problem 8 of § 4.1.1) then we get:

$$x_1 = (-2 - 7k) + 5s \qquad x_2 = (2 + 3k) - 2s \qquad x_3 = (-8 + 6k) + 17t \qquad x_4 = (-1 + k) + 3t$$

   where $k, s, t \in \mathbb{Z}$.
   (**b**) This equation has a solution because $\gcd(36, -15, 26, 22) = 1$.
   Let $X = 12x_1 - 5x_2$ and $Y = 13x_3 + 11x_4$. Hence, we have $3X + 2Y = 3$ whose solution (according to the formula of Problem 8 of § 4.1.1) is: $X = 1 + 2k$ and $Y = -3k$ $(k \in \mathbb{Z})$, that is:

$$12x_1 - 5x_2 = 1 + 2k \qquad\qquad 13x_3 + 11x_4 = -3k$$

   Now, if we solve each one of these equations (using the formula of Problem 8 of § 4.1.1) then we get:

$$x_1 = (3 + k) - 5s \qquad x_2 = (7 + 2k) - 12s \qquad x_3 = (-7k) + 11t \qquad x_4 = (8k) - 13t$$

   where $k, s, t \in \mathbb{Z}$.

4.1.4 Pythagorean Triples

A Pythagorean triple is a collection of three natural numbers (a, b, c) such that:

$$a^2 + b^2 = c^2 \tag{76}$$

For example, $(3, 4, 5)$, $(14, 48, 50)$ and $(20, 99, 101)$ are Pythagorean triples. The "Pythagorean" label is because such triples satisfy the Pythagorean theorem about right-angled triangles.

If the numbers a, b, c of the Pythagorean triple (a, b, c) have no common divisor $d > 1$ then the Pythagorean triple is described as **primitive**.[138] For example, $(3, 4, 5)$, $(20, 21, 29)$ and $(9, 40, 41)$ are primitive Pythagorean triples, but $(6, 8, 10)$, $(14, 48, 50)$ and $(18, 80, 82)$ are non-primitive Pythagorean triples. There are infinitely many Pythagorean triples. There are also infinitely many primitive Pythagorean triples.

Problems

1. Show that if $m, n \in \mathbb{N}$ and $m > n$ then $(2mn, m^2 - n^2, m^2 + n^2)$ is a Pythagorean triple.
   Solution: We have:

$$(2mn)^2 + (m^2 - n^2)^2 = 4m^2n^2 + m^4 - 2m^2n^2 + n^4 = m^4 + 2m^2n^2 + n^4 = (m^2 + n^2)^2$$

   Hence, $(2mn, m^2 - n^2, m^2 + n^2)$ is a Pythagorean triple.
   Note: the result of this Problem provides a method for generating Pythagorean triples. However, it should be noted that this method does not generate all the Pythagorean triples, i.e. all triples of the form $(2mn, m^2 - n^2, m^2 + n^2)$ are Pythagorean but not all the Pythagorean triples are of the form $(2mn, m^2 - n^2, m^2 + n^2)$. For example, the Pythagorean triple $(12, 5, 13)$ is of this form (corresponding to $m = 3$ and $n = 2$), but the Pythagorean triple $(9, 12, 15)$ is not of this form. We note that the formula $(a, b, c) = (2mn, m^2 - n^2, m^2 + n^2)$ for this type of Pythagorean triple is called **Euclid's formula**.
2. Show the following [where (a, b, c) is a Pythagorean triple]:
   (**a**) (a, b, c) is primitive *iff* $\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1$ (i.e. a, b, c are pairwise coprime).
   (**b**) If (a, b, c) is primitive then a and b have opposite parity (and hence c is odd).
   Solution:
   (**a**) **The if part**: if $\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1$ then $\gcd(a, b, c) = 1$ (see point 7 of § 2.2) and hence (a, b, c) is primitive.
   The only if part: if (a, b, c) is primitive then $\gcd(a, b, c) = 1$. Now, if $\gcd(a, b) \neq 1$ then it must be > 1 and hence $\gcd(a, b)$ must have a prime divisor p. This means that $p|a$ and $p|b$ and hence $p|a^2$ and $p|b^2$ (see rule 6 of § 1.9). Therefore, by rule 14 of § 1.9 $p|\left(a^2 + b^2\right)$, i.e. $p|c^2$. So, by rule 22 of § 1.9 $p|c$. This means that p divides all three numbers and hence $\gcd(a, b, c) \neq 1$ which is a contradiction. Similar arguments apply if $\gcd(a, c) \neq 1$ or $\gcd(b, c) \neq 1$. So, we conclude that if (a, b, c) is primitive then $\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1$.[139]
   (**b**) Referring to the rules of parity (see rules 4-10 of § 1.8):
   • a and b cannot be both even because $\gcd(a, b) = 1$ (see part a) whereas if they are both even then they must have a common factor of 2 and hence $\gcd(a, b) \neq 1$.
   • a and b cannot be both odd because in this case c^2 as a sum of two odd squares (i.e. $c^2 = a^2 + b^2$) must have remainder 2 on division by 4 (see Problem 4 of 1.8). However, c^2 as a square of c must either have remainder 1 (if c is odd) or remainder 0 (if c is even) on division by 4 (see Problem 4 of § 1.8).
   So, a and b cannot be both even and cannot be both odd and hence they must have opposite parity. Accordingly, by the rules of parity a^2 and b^2 must also have opposite parity, and hence their sum (i.e. $c^2 = a^2 + b^2$) must be odd which means that c is odd. So in brief, a and b have opposite parity and c is odd (as required).

[138] This means that the Pythagorean triple (a, b, c) is primitive *iff* $\gcd(a, b, c) = 1$.

[139] It should be noted that the phrasing of this part (i.e. part a of this Problem) is rather misleading because the "if part" should be: if $\gcd(a, b) = 1$ or $\gcd(a, c) = 1$ or $\gcd(b, c) = 1$ then (a, b, c) is primitive, while the "only if part" should be: if (a, b, c) is primitive then $\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1$. So, it is not exactly an *iff* statement although the *iff* statement is correct (but it is conceptually weaker in its "if part" because we unnecessarily impose pairwise coprimality while what is needed is only the coprimality of any two of a, b, c although these are equivalent in reality).

3. Show that if (a,b,c) is a primitive Pythagorean triple, then there are coprimes $m,n \in \mathbb{N}$ of opposite parity with $m>n$ such that (a,b,c) is given by Euclid's formula, i.e. $(a,b,c)=(2mn,m^2-n^2,m^2+n^2)$.
Solution: According to part (b) of Problem 2, a and b have opposite parity and c is odd. So, we can assume (with no loss of generality) that a is even and b is odd (and hence b and c are both odd). Therefore, $c+b$ and $c-b$ are both even (see rule 4 of § 1.8), that is:

$$q=\frac{c+b}{2} \qquad\qquad r=\frac{c-b}{2} \qquad\qquad (q,r\in\mathbb{Z})$$

Now, q and r are coprime. This is because if $g=\gcd(q,r)$ then $g|(q-r)=b$ and $g|(q+r)=c$. But according to part (a) of Problem 2, b and c are coprime (because their gcd is 1). This means that g (which divides both b and c) must be 1, i.e. $g=\gcd(q,r)=1$ which means that q and r are coprime. Also, q and r are squares because:

$$qr=\left(\frac{c+b}{2}\right)\left(\frac{c-b}{2}\right)=\frac{c^2-b^2}{4}=\frac{a^2}{4}=\left(\frac{a}{2}\right)^2$$

and hence according to Problem 20 of § 2.2 q and r are squares (noting that a is even and hence $a/2$ is an integer).
Now, since each one of q and r is a square (of an integer) then $\sqrt{q}$ and $\sqrt{r}$ are integers. So, let $m=\sqrt{q}$ and $n=\sqrt{r}$ (noting that the condition $m>n$ is satisfied). Accordingly:

$$\begin{aligned} 2mn &= 2\sqrt{q}\sqrt{r}=2\sqrt{\frac{c+b}{2}}\sqrt{\frac{c-b}{2}}=\sqrt{c^2-b^2}=\sqrt{a^2}=a \\ m^2-n^2 &= q-r=\frac{c+b}{2}-\frac{c-b}{2}=b \\ m^2+n^2 &= q+r=\frac{c+b}{2}+\frac{c-b}{2}=c \end{aligned}$$

i.e. we can always find coprimes m,n of opposite parity with $m>n$ such that (a,b,c) is given by Euclid's formula.
Note 1: m and n are coprime because q and r are coprime and hence their square roots (which are m and n) must also be coprime (noting that coprimes have no common prime factor; see part n of Problem 1 of § 2.2).
Note 2: m and n are of opposite parity because b and c are odd noting that $b=m^2-n^2$ and $c=m^2+n^2$ and hence by the rules of parity (see rules 4-10 of § 1.8) m and n must be of opposite parity.
Note 3: this Problem shows that Euclid's formula produces all the primitive Pythagorean triples.

4. Show that the Pythagorean triple $(2mn,m^2-n^2,m^2+n^2)$ is primitive *iff* m and n are coprimes of opposite parity (where $m,n\in\mathbb{N}$ and $m>n$).
Solution: We note first that according to Problem 1, $(a,b,c)=(2mn,m^2-n^2,m^2+n^2)$ is a Pythagorean triple (where $m,n\in\mathbb{N}$ and $m>n$).
The if part: what we need for proving this part is to show that if m and n are coprimes of opposite parity then $\gcd(a,b,c)=1$ (and hence by definition the triple is primitive). So, let $g\equiv\gcd(a,b,c)$. Accordingly, $g|b$ and $g|c$, and hence $g|(c+b)=2m^2$ and $g|(c-b)=2n^2$. However, because m and n are of opposite parity, m^2-n^2 and m^2+n^2 (which are equal to b and c) must be odd and hence g must be odd (see the rules of parity in § 1.8). This means that $g|m^2$ and $g|n^2$. But since m and n are coprime, m^2 and n^2 must also be coprime (noting that coprimes have no common prime factor; see part n of Problem 1 of § 2.2) and hence $g=1$, i.e. $\gcd(a,b,c)=1$ and hence the triple is primitive.
The only if part: if m and n are not coprime then they have a common factor $d>1$ and hence the triple $(2mn,m^2-n^2,m^2+n^2)$ will have a common factor of $d^2>1$ in contradiction to the given fact that the triple $(2mn,m^2-n^2,m^2+n^2)$ is primitive. So, m and n must be coprime. Also, if m and n have the same parity then m^2-n^2 and m^2+n^2 are even and hence the triple will be even (i.e. $2mn$, m^2-n^2 and m^2+n^2 will have a common factor of 2) in contradiction to the given fact that the triple $(2mn,m^2-n^2,m^2+n^2)$ is primitive (since their gcd will then be ≥ 2). Thus, m and n must have opposite parity. So in brief, m and n are coprimes of opposite parity (as required).

4.1.5 Non-Linear Diophantine Polynomial Equations in Two Variables

We investigate here (through solved Problems) a few examples of non-linear Diophantine polynomial equations in two variables outlining some methods of solution of such equations.

Problems

1. Find all the solutions (if exist) of the following non-linear Diophantine polynomial equations in two variables ($x, y \in \mathbb{Z}$):

   (**a**) $x^2 - 21y = 10$. (**b**) $x^2 + 9x - 3 - 7y = 0$. (**c**) $5x^2 + 8y^2 = 28$.

   (**d**) $x^2 + y^2 + 18xy - x^2y^2 - 81 = 0$. (**e**) $x^3y - 125x + 125 = 0$. (**f**) $x^6y + xy^6 - 256 = 0$.

   (**g**) $(x-1)^2 = (y+2)^3$. (**h**) $5x + xy - 2y = 0$. (**i**) $x^2 - xy + y^2 + 2x - y = 2$.

   (**j**) $15x + 13xy - 20y = 0$.

   Solutions:

   (**a**) If we reduce the equation modulo 7 we get: $x^2 \stackrel{7}{=} 3$. Now, for $x \stackrel{7}{=} 0, 1, 2, 3, 4, 5, 6$ we have (respectively) $x^2 \stackrel{7}{=} 0, 1, 4, 2, 2, 4, 1$. As we see, $x^2 \stackrel{7}{\neq} 3$ and hence this equation has no solution (see part b of point 8 of § 2.7.6).

   (**b**) If we reduce the equation modulo 7 we get: $x^2 + 2x - 3 \stackrel{7}{=} 0$. Now, for $x \stackrel{7}{=} 0, 1, 2, 3, 4, 5, 6$ we have (respectively) $x^2 + 2x - 3 \stackrel{7}{=} 4, 0, 5, 5, 0, 4, 3$. So, the solutions of $x^2 + 2x - 3 \stackrel{7}{=} 0$ are $x = 1 + 7k$ and $x = 4 + 7k$ ($k \in \mathbb{Z}$). On substituting these solutions into the original equation we get:

   $$(1+7k)^2 + 9(1+7k) - 3 - 7y = 0 \qquad \text{and} \qquad (4+7k)^2 + 9(4+7k) - 3 - 7y = 0$$

   On simplifying these equations and solving for y we get: $y = 7k^2 + 11k + 1$ and $y = 7k^2 + 17k + 7$. So, the solutions are (where $k \in \mathbb{Z}$):

   $$(x, y) = (1 + 7k,\ 7k^2 + 11k + 1) \qquad (x, y) = (4 + 7k,\ 7k^2 + 17k + 7)$$

   (**c**) If we reduce the equation modulo 2 we get: $x^2 \stackrel{2}{=} 0$ and hence $x \stackrel{2}{=} 0$, i.e. $x = 2k$ where $k \in \mathbb{Z}$. On substituting this into the given equation we get: $5(2k)^2 + 8y^2 = 28$, i.e. $8y^2 = 28 - 20k^2$. Now, $8y^2 \geq 0$ and hence $k^2 \leq 1$. So, we have only 3 possible values for k, i.e. $k = 0, \pm 1$. However, $k = 0$ does not lead to an integer y and therefore we only have $k = \pm 1$ which lead to the following solutions:

   $(x, y) = (-2, -1)$ $(x, y) = (-2, 1)$ $(x, y) = (2, -1)$ $(x, y) = (2, 1)$

   A simpler approach to solve this type of problems is to note that $0 \leq 5x^2 \leq 28$ (i.e. $|x| \leq \sqrt{28/5} \simeq 2.4$) and $0 \leq 8y^2 \leq 28$ (i.e. $|y| \leq \sqrt{28/8} \simeq 1.9$). So, all we need to do is to test the 15 combinations of $x = -2, -1, 0, 1, 2$ and $y = -1, 0, 1$ and this test should lead to the same result, i.e. only $x = \pm 2$ with $y = \pm 1$ (considering all the 4 possible sign combinations) satisfy the equation $5x^2 + 8y^2 = 28$.

   (**d**) We have:

   $$\begin{aligned} x^2 + y^2 + 18xy - x^2y^2 - 81 &= 0 \\ (x^2 + 2xy + y^2) + (16xy - x^2y^2 - 64) - 17 &= 0 \\ (x^2 + 2xy + y^2) - (x^2y^2 - 16xy + 64) &= 17 \\ (x+y)^2 - (xy-8)^2 &= 17 \\ \Big[(x+y) - (xy-8)\Big]\Big[(x+y) + (xy-8)\Big] &= 17 \end{aligned}$$

   Now, either $17 = 1 \times 17$ or $17 = (-1) \times (-17)$, i.e.

   $$\Big[(x+y)-(xy-8)\Big]\Big[(x+y)+(xy-8)\Big] = 1\times 17 \quad \textbf{OR} \quad \Big[(x+y)-(xy-8)\Big]\Big[(x+y)+(xy-8)\Big] = (-1)\times(-17)$$

   Thus, we have 4 cases to consider:

   Case 1: $(x+y) - (xy-8) = 1$ and $(x+y) + (xy-8) = 17$. These equations simplify (by addition and subtraction) to: $x + y = 9$ and $xy = 16$. These equations have no integer solution.

Case 2: $(x+y)-(xy-8)=17$ and $(x+y)+(xy-8)=1$. These equations simplify to: $x+y=9$ and $xy=0$. These equations have two solutions: $(x,y)=(0,9)$ and $(x,y)=(9,0)$.
Case 3: $(x+y)-(xy-8)=-1$ and $(x+y)+(xy-8)=-17$. These equations simplify to: $x+y=-9$ and $xy=0$. These equations have two solutions: $(x,y)=(0,-9)$ and $(x,y)=(-9,0)$.
Case 4: $(x+y)-(xy-8)=-17$ and $(x+y)+(xy-8)=-1$. These equations simplify to: $x+y=-9$ and $xy=16$. These equations have no integer solution.
So, in total we have 4 possible solutions:
$(x,y)=(0,9)$ $(x,y)=(9,0)$ $(x,y)=(0,-9)$ $(x,y)=(-9,0)$
(**e**) We have:

$$x^3y-125x+125=0 \quad \rightarrow \quad x^3y=125x-125 \quad \rightarrow \quad y=\frac{125(x-1)}{x^3}$$

Now, x and $(x-1)$ are coprime (see part h of Problem 1 of § 2.2) and hence x^3 must divide 125 $(=5^3)$, i.e. $x=\pm1,\pm5$. So, from the equation $y=\frac{125(x-1)}{x^3}$ we get:
$y=\frac{125(-5-1)}{(-5)^3}=6$ $y=\frac{125(-1-1)}{(-1)^3}=250$ $y=\frac{125(1-1)}{(1)^3}=0$ $y=\frac{125(5-1)}{(5)^3}=4$
Hence, the solutions are $(x,y)=(-5,6)$, $(-1,250)$, $(1,0)$, $(5,4)$.
(**f**) $x(x^5y+y^6)=256$ and hence x is a divisor of 256 (noting that 256 has 18 positive and negative divisors). Similarly, $y(x^6+xy^5)=256$ and hence y is a divisor of 256. So, by testing all the possibilities of x being equal to one of these 18 divisors and y being equal to one of these 18 divisors (noting that we have $18\times18=324$ possibilities) we find that only $x=y=2$ satisfies the given equation. So, the solution is $x=y=2$.
(**g**) Let $X=(x-1)$ and $Y=(y+2)$, and hence we have $X^2=Y^3$, i.e. $X=\pm Y^{3/2}$. The solution of the latter equation is $X=\pm k^3$ and $Y=k^2$ (where $k\in\mathbb{Z}$), i.e. $(x-1)=\pm k^3$ and $(y+2)=k^2$. So, the solutions are: $(x,y)=(\pm k^3+1,\ k^2-2)$ where $k\in\mathbb{Z}$.
(**h**) From the given equation we have:

$$\begin{aligned} 5x+xy-2y-10 &= -10 \\ (x-2)(y+5) &= (-1)\times10=1\times(-10)=(-2)\times5=2\times(-5) \end{aligned}$$

So, we have 8 cases to consider (and hence we have 8 solutions):
• $(x-2)=-1$ and $(y+5)=10$, i.e. $(x,y)=(1,5)$.
• $(x-2)=10$ and $(y+5)=-1$, i.e. $(x,y)=(12,-6)$.
• $(x-2)=1$ and $(y+5)=-10$, i.e. $(x,y)=(3,-15)$.
• $(x-2)=-10$ and $(y+5)=1$, i.e. $(x,y)=(-8,-4)$.
• $(x-2)=-2$ and $(y+5)=5$, i.e. $(x,y)=(0,0)$.
• $(x-2)=5$ and $(y+5)=-2$, i.e. $(x,y)=(7,-7)$.
• $(x-2)=2$ and $(y+5)=-5$, i.e. $(x,y)=(4,-10)$.
• $(x-2)=-5$ and $(y+5)=2$, i.e. $(x,y)=(-3,-3)$.
(**i**) We algebraically manipulate the given equation as follows:

$$\begin{aligned} 2x^2-2xy+2y^2+4x-2y &= 4 && (\times2)\\ 2x^2-2xy+2y^2+4x-2y+5 &= 9 && (+5)\\ (x^2+4x)+(y^2-2y)+(x^2-2xy+y^2)+5 &= 9 && (\text{manipulation})\\ (x^2+4x+4)+(y^2-2y+1)+(x^2-2xy+y^2) &= 9 && (\text{manipulation})\\ (x+2)^2+(y-1)^2+(x-y)^2 &= 9 \end{aligned}$$

From the last equation it is obvious that $-3\le(x+2)\le3$ and hence we have 7 cases:
• $(x+2)=-3$, i.e. $x=-5$ and hence $(y-1)^2+(-5-y)^2=0$ which has no solution.
• $(x+2)=-2$, i.e. $x=-4$ and hence $(y-1)^2+(-4-y)^2=5$ which has no solution.
• $(x+2)=-1$, i.e. $x=-3$ and hence $(y-1)^2+(-3-y)^2=8$ which has one solution: $y=-1$.

• $(x+2)=0$, i.e. $x=-2$ and hence $(y-1)^2+(-2-y)^2=9$ which has two solutions: $y=-2$ and $y=1$.
• $(x+2)=1$, i.e. $x=-1$ and hence $(y-1)^2+(-1-y)^2=8$ which has no solution.
• $(x+2)=2$, i.e. $x=0$ and hence $(y-1)^2+y^2=5$ which has two solutions: $y=-1$ and $y=2$.
• $(x+2)=3$, i.e. $x=1$ and hence $(y-1)^2+(1-y)^2=0$ which has one solution: $y=1$.
So in brief, we have 6 solutions: $(x,y)=(-3,-1)$, $(-2,-2)$, $(-2,1)$, $(0,-1)$, $(0,2)$, $(1,1)$.
(**j**) We have $15x+13xy-20y=0$ and hence:

$$15x=20y-13xy \quad \rightarrow \quad 15x=(20-13x)y \quad \rightarrow \quad y=\frac{15x}{20-13x}$$

Now, $(20-13x)$ divides any of its multiples, and hence $(20-13x)$ divides $15(20-13x)=300-195x$. Also, if $(20-13x)$ should divide $15x$ (since y is an integer) then $(20-13x)$ must divide any multiple of $15x$, and hence $(20-13x)$ should divide $13\times 15x=195x$. So, $(20-13x)$ divides both $(300-195x)$ and $195x$ and hence it must divide their sum which is 300 (rule 14 of § 1.9). Noting that the divisors of 300 are 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 25, 30, 50, 60, 75, 100, 150, 300 and their negatives, we conclude that $(20-13x)$ must be equal to (some of) these divisors. Considering all these 36 possibilities (i.e. $20-13x=\pm 1,\pm 2,\ldots,\pm 300$) and accepting only those possibilities that produce integer x we get:
• $20-13x=-6$ and hence $x=2$ and $y=-5$.
• $20-13x=20$ and hence $x=0$ and $y=0$.
• $20-13x=150$ and hence $x=-10$ and $y=-1$.
So, the solutions of the given equation are: $(x,y)=(2,-5)$, $(0,0)$, $(-10,-1)$.

4.1.6 Non-Linear Diophantine Polynomial Equations in Three Variables

In this subsection we present a number of solved Problems related to non-linear Diophantine polynomial equations in three variables. Some special types of non-linear Diophantine polynomial equations in three variables are investigated in other parts of the book (see for instance § 4.1.4).

Problems

1. Which of the following non-linear Diophantine polynomial equations in three variables have solutions (where $x,y,z\in\mathbb{N}$):
   (**a**) $x^2+y^2=z^2$. (**b**) $x^2-y^2=z^2$. (**c**) $x^3+y^3=z^3$.
   (**d**) $x^3-y^3=z^3$. (**e**) $x^4+y^4=z^4$. (**f**) $x^4-y^4=z^4$.
   Solution:
   (**a**) This has infinitely many solutions (i.e. Pythagorean triples; see § 4.1.4).
   (**b**) This has infinitely many solutions (since we can write it as $y^2+z^2=x^2$ and hence it is like part a).
   (**c**) This has no solution (by Fermat's last theorem; see § 2.9.5).
   (**d**) This has no solution (because we can write it as $y^3+z^3=x^3$ and hence it is like part c).
   (**e**) This has no solution (by Fermat's last theorem; see § 2.9.5).
   (**f**) This has no solution (because we can write it as $y^4+z^4=x^4$ and hence it is like part e).
2. Show that $x^4+y^4=z^2$ has no solution in $\mathbb{N}$ (i.e. there are no $x,y,z\in\mathbb{N}$ that satisfy this equation).
   Solution: We use here the method of infinite descent (see Problem 3 of § 1.5.4) where we show that if a solution $x,y,z\in\mathbb{N}$ exists, then we must have a minimal such solution in $\mathbb{N}$ (i.e. z in this minimal solution is smaller than any z in any other solution of this equation). We then construct in the proof a solution smaller than the presumed minimal solution, and this contradicts the presumption of minimality that we started with. Thus, we conclude by contradiction (see point 4 of § 1.5.4) that no solution can exist. This proof is outlined in the following points:
   • Assume that the equation $x^4+y^4=z^2$ has a solution.
   • Assume that (x,y,z) is the minimal solution to this equation.[140]
   • If we write $x^4+y^4=z^2$ as $\left(x^2\right)^2+\left(y^2\right)^2=z^2$, then we can see that (x^2,y^2,z) is a Pythagorean triple.

[140] In fact, this is an abuse of notation since x,y,z are already used as variables. However, this will avoid some unwanted complications in this messy proof. Anyway, this abuse of notation should cause no confusion.

• The triple (x^2, y^2, z) must be primitive because otherwise x^2 and y^2 must have a common factor p^2 ($p \in \mathbb{P}$), and hence p^2 should divide z (noting that $z^2 = x^4 + y^4$) which contradicts the assumption that z is minimal.
• According to Problem 3 of § 4.1.4, there are coprimes $m, n \in \mathbb{N}$ of opposite parity with $m > n$ such that (x^2, y^2, z) is given by Euclid's formula, i.e.

$$x^2 = 2mn \qquad y^2 = m^2 - n^2 \qquad z = m^2 + n^2$$

• If we write $y^2 = m^2 - n^2$ as $n^2 + y^2 = m^2$ then (n, y, m) is a Pythagorean triple. Moreover, since m and n are coprime then $\gcd(n, y, m) = 1$ (see point 7 of § 2.2 as well as part a of Problem 2 of § 4.1.4) and hence (n, y, m) is primitive.
• According to Problem 3 of § 4.1.4, there are coprimes $\mu, \nu \in \mathbb{N}$ of opposite parity with $\mu > \nu$ such that (n, y, m) is given by Euclid's formula, i.e.

$$n = 2\mu\nu \qquad y = \mu^2 - \nu^2 \qquad m = \mu^2 + \nu^2$$

• As we see, m is odd (noting that μ and ν are of opposite parity) and n is even (noting that $n = 2\mu\nu$). Now, since m and n are coprime then m and $2n$ are coprime (noting that 2 is not a factor of m since m is odd).
• If we write $x^2 = (m)(2n)$ and note that m and $2n$ are coprime, then from Problem 20 of § 2.2 we conclude that each one of m and $2n$ is a square (of an integer). So, let $m = s^2$ and $2n = t^2$ ($s, t \in \mathbb{N}$).
• $2n = t^2$ means t^2 is even and hence t is even (see the rules of parity in § 1.8). So, let $t = 2\sigma$ and hence $2n = 4\sigma^2$, and thus $n = 2\sigma^2$ ($\sigma \in \mathbb{N}$).
• If we substitute from $n = 2\sigma^2$ into $n = 2\mu\nu$ we get $\sigma^2 = \mu\nu$. Now, since μ and ν are coprime then each one of them is a square (see Problem 20 of § 2.2), i.e. $\mu = b^2$ and $\nu = c^2$ ($b, c \in \mathbb{N}$).
• Now, if we substitute from $m = s^2$, $\mu = b^2$ and $\nu = c^2$ into $m = \mu^2 + \nu^2$ we get:

$$b^4 + c^4 = s^2$$

So, we got another solution, i.e. (b, c, s), to the equation $x^4 + y^4 = z^2$.
• Now, $z = m^2 + n^2$ and $m = s^2$ and hence $z = s^4 + n^2$. So, $z > s$ which means that (x, y, z) is not the minimal solution to the equation $x^4 + y^4 = z^2$, and this contradicts our assumption that (x, y, z) is the minimal solution.
• Thus, from this contradiction we conclude that no solution can exist, i.e. $x^4 + y^4 = z^2$ has no solution in $\mathbb{N}$ because the presumption of solution leads to infinite descent (see point 4 of § 1.5.4 as well as Problem 3 of § 1.5.4).

3. Prove Fermat's last theorem (see § 2.9.5) for the special case $n = 4$, i.e. $x^4 + y^4 = z^4$ has no solution (x, y, z) in $\mathbb{N}$.
Solution: If we write $x^4 + y^4 = z^4$ as $x^4 + y^4 = Z^2$ where $Z = z^2$ then from the result of Problem 2 we conclude that there is no solution to $x^4 + y^4 = Z^2$ and hence no solution to $x^4 + y^4 = z^4$. In other words, if there is a solution (x, y, z) to $x^4 + y^4 = z^4$ then there should be a solution (x, y, Z) to $x^4 + y^4 = Z^2$ (noting that if $z \in \mathbb{N}$ exists in the first solution then $Z \in \mathbb{N}$ exists in the second solution since $Z = z^2$), and this contradicts the result of Problem 2.
4. Show that the following non-linear Diophantine equations in three variables have no solutions in $\mathbb{N}$ (i.e. there are no $x, y, z \in \mathbb{N}$ that satisfy these equations).
(**a**) $x^4 - y^4 = z^2$. (**b**) $x^4 - y^4 = z^4$. (**c**) $x^4 + y^2 = z^4$. (**d**) $x^4 - y^2 = z^4$.
Solution:
(**a**) Let assume that this equation has a solution in $\mathbb{N}$ and hence we have a (minimal) solution (x, y, z) that minimizes $x^2 + y^2$. If we write $x^4 - y^4 = z^2$ as $z^2 + y^4 = x^4$ then we can see that (z, y^2, x^2) is a Pythagorean triple. This triple must be primitive because otherwise z, y^2, x^2 must have a common prime factor p, and hence p should divide $x^2 + y^2$ which contradicts the assumption that $x^2 + y^2$ is minimal. Now, according to Problem 3 of § 4.1.4 there are coprimes $m, n \in \mathbb{N}$ of opposite parity with $m > n$ such that (z, y^2, x^2) is given by Euclid's formula, i.e. either

$$z = 2mn \qquad y^2 = m^2 - n^2 \qquad x^2 = m^2 + n^2$$

or

$$y^2 = 2mn \qquad z = m^2 - n^2 \qquad x^2 = m^2 + n^2$$

As we see, we have two possibilities to consider:
• $y^2 = m^2 - n^2$ and hence:

$$x^2y^2 = (m^2 + n^2)(m^2 - n^2) = m^4 - n^4 \qquad \rightarrow \qquad m^4 - n^4 = t^2 \qquad (t^2 \equiv x^2y^2)$$

So, (m, n, t) is another solution. However, according to this solution: $m^2 + n^2 = x^2 < (x^2 + y^2)$, i.e. the presumed solution is not minimal since $(m^2 + n^2) < (x^2 + y^2)$.
• $y^2 = 2mn$. Now, $x^2 = m^2 + n^2$ means that (m, n, x) is a Pythagorean triple and it is primitive (since m and n are coprime; see point 7 of § 2.2 as well as part a of Problem 2 of § 4.1.4). So, according to Problem 3 of § 4.1.4, there are coprimes $\mu, \nu \in \mathbb{N}$ of opposite parity with $\mu > \nu$ such that (m, n, x) is given by Euclid's formula, i.e.

$$m = 2\mu\nu \qquad n = \mu^2 - \nu^2 \qquad x = \mu^2 + \nu^2$$

Hence:

$$\mu\nu(\mu^2 - \nu^2) = \frac{m}{2}n = \frac{1}{2}mn = \frac{1}{2}\left(\frac{y^2}{2}\right) = \frac{y^2}{4} = \left(\frac{y}{2}\right)^2 \tag{77}$$

Now, μ and ν are coprime and hence each of μ and ν is coprime to $\mu^2 - \nu^2$ (see part b of Problem 19 of § 2.2). Thus, $\mu\nu$ and $(\mu^2 - \nu^2)$ are coprime (see part e of Problem 1 of § 2.2) and hence from Eq. 77 we conclude that $\mu\nu$ and $(\mu^2 - \nu^2)$ are squares (see Problem 20 of § 2.2). Thus, let $\mu\nu = A^2$ and $(\mu^2 - \nu^2) = c^2$ $(A, c \in \mathbb{N})$.
If we repeat this argument on $\mu\nu = A^2$ (noting that μ and ν are coprime and using Problem 20 of § 2.2) we conclude that μ and ν are squares. Thus, let $\mu = a^2$ and $\nu = b^2$ $(a, b \in \mathbb{N})$. So in brief we have:

$$\mu = a^2 \qquad \nu = b^2 \qquad \mu^2 - \nu^2 = c^2 \qquad (a, b, c \in \mathbb{N})$$

On substituting from the first two equations into the last equation we get $a^4 - b^4 = c^2$. So, (a, b, c) is another solution. However (see Eq. 77):

$$a^2 + b^2 = (\mu + \nu) < (\mu + \nu)(\mu - \nu)(\mu\nu) = \mu\nu(\mu^2 - \nu^2) = \frac{y^2}{4} < y^2 < (x^2 + y^2)$$

This means that the presumed solution is not minimal since $(a^2 + b^2) < (x^2 + y^2)$.
So, in both possibilities the presumption of solution leads to infinite descent (see point 4 of § 1.5.4 as well as Problem 3 of § 1.5.4) and hence we conclude that the equation $x^4 - y^4 = z^2$ has no solution in $\mathbb{N}$.
(**b**) If we write $x^4 - y^4 = z^4$ as $x^4 - y^4 = Z^2$ where $Z = z^2$ then from the result of part (a) we conclude that there is no solution to $x^4 - y^4 = Z^2$ and hence no solution to $x^4 - y^4 = z^4$. We may also use the result of Problem 3 directly because $x^4 - y^4 = z^4$ is equivalent to $z^4 + y^4 = x^4$ which has no solution.
(**c**) This is a corollary of the result of part (a) noting that $x^4 + y^2 = z^4$ is equivalent to $z^4 - x^4 = y^2$.
(**d**) This is a corollary of the result of part (a) noting that $x^4 - y^2 = z^4$ is equivalent to $x^4 - z^4 = y^2$.

5. Find the solutions of the following non-linear Diophantine polynomial equations in the three variables x, y, z (where $x, y, z \in \mathbb{Z}$):
(**a**) $x^2 - 3y - 2z = 0$. (**b**) $3x^2 - 8y^2 + 7z = 11$. (**c**) $x^2 - y^2 - 2x - 8y - 15 - 11z = 0$.
(**d**) $x^3 - 4y^2 + 5z = 0$. (**e**) $x^4 + y^4 + z^4 = 3042$.

Solution:
(**a**) If we reduce the equation modulo 2 we get: $x^2 - y \stackrel{2}{=} 0$, i.e. $x^2 \stackrel{2}{=} y$. This equation means that x and y must have the same parity. So, we have two cases to consider:
• x and y are even, i.e. $x = 2k$ and $y = 2s$ $(k, s \in \mathbb{Z})$. On substituting these into the equation and solving for z we get:

$$(2k)^2 - 3(2s) - 2z = 0 \qquad \rightarrow \qquad z = \frac{4k^2 - 6s}{2} = 2k^2 - 3s$$

• x and y are odd, i.e. $x = 2k+1$ and $y = 2s+1$ ($k, s \in \mathbb{Z}$). On substituting these into the equation and solving for z we get:

$$(2k+1)^2 - 3(2s+1) - 2z = 0 \qquad \rightarrow \qquad z = \frac{4k^2+4k-6s-2}{2} = 2k^2+2k-3s-1$$

So, the solutions are all triples of the following two forms (where $k, s \in \mathbb{Z}$):

$$(x, y, z) = (2k, 2s, 2k^2-3s) \qquad\qquad (x, y, z) = (2k+1, 2s+1, 2k^2+2k-3s-1)$$

(**b**) If we reduce the equation modulo 7 we get: $3x^2 - y^2 \stackrel{7}{=} 4$, i.e. $3x^2 \stackrel{7}{=} y^2 + 4$. If we multiply both sides by the multiplicative inverse (mod 7) of 3 (which is 5) we get: $x^2 \stackrel{7}{=} 5y^2 + 20$, i.e. $x^2 \stackrel{7}{=} 5y^2 + 6$. Now, for $x \stackrel{7}{=} 0, 1, 2, 3, 4, 5, 6$ we have (respectively) $x^2 \stackrel{7}{=} 0, 1, 4, 2, 2, 4, 1$. So, we need to consider these seven cases:
• $x \stackrel{7}{=} 0$ and hence $5y^2 + 6 \stackrel{7}{=} 0$ which has no solution.
• $x \stackrel{7}{=} 1$ and hence $5y^2 + 6 \stackrel{7}{=} 1$ which has no solution.
• $x \stackrel{7}{=} 2$ and hence $5y^2 + 6 \stackrel{7}{=} 4$ which has two solutions: $y \stackrel{7}{=} 1$ and $y \stackrel{7}{=} 6$. So, if $x \stackrel{7}{=} 2$ and $y \stackrel{7}{=} 1$ then we have (where $k, s \in \mathbb{Z}$):

$$3(2+7k)^2 - 8(1+7s)^2 + 7z = 11 \qquad \rightarrow \qquad z = -21k^2 - 12k + 56s^2 + 16s + 1$$

Similarly, if $x \stackrel{7}{=} 2$ and $y \stackrel{7}{=} 6$ then we have:

$$3(2+7k)^2 - 8(6+7s)^2 + 7z = 11 \qquad \rightarrow \qquad z = -21k^2 - 12k + 56s^2 + 96s + 41$$

• $x \stackrel{7}{=} 3$ and hence $5y^2 + 6 \stackrel{7}{=} 2$ which has two solutions: $y \stackrel{7}{=} 3$ and $y \stackrel{7}{=} 4$. So, if $x \stackrel{7}{=} 3$ and $y \stackrel{7}{=} 3$ then we have:

$$3(3+7k)^2 - 8(3+7s)^2 + 7z = 11 \qquad \rightarrow \qquad z = -21k^2 - 18k + 56s^2 + 48s + 8$$

Similarly, if $x \stackrel{7}{=} 3$ and $y \stackrel{7}{=} 4$ then we have:

$$3(3+7k)^2 - 8(4+7s)^2 + 7z = 11 \qquad \rightarrow \qquad z = -21k^2 - 18k + 56s^2 + 64s + 16$$

• $x \stackrel{7}{=} 4$ and hence $5y^2 + 6 \stackrel{7}{=} 2$ which has two solutions: $y \stackrel{7}{=} 3$ and $y \stackrel{7}{=} 4$. So, if $x \stackrel{7}{=} 4$ and $y \stackrel{7}{=} 3$ then we have:

$$3(4+7k)^2 - 8(3+7s)^2 + 7z = 11 \qquad \rightarrow \qquad z = -21k^2 - 24k + 56s^2 + 48s + 5$$

Similarly, if $x \stackrel{7}{=} 4$ and $y \stackrel{7}{=} 4$ then we have:

$$3(4+7k)^2 - 8(4+7s)^2 + 7z = 11 \qquad \rightarrow \qquad z = -21k^2 - 24k + 56s^2 + 64s + 13$$

• $x \stackrel{7}{=} 5$ and hence $5y^2 + 6 \stackrel{7}{=} 4$ which has two solutions: $y \stackrel{7}{=} 1$ and $y \stackrel{7}{=} 6$. So, if $x \stackrel{7}{=} 5$ and $y \stackrel{7}{=} 1$ then we have:

$$3(5+7k)^2 - 8(1+7s)^2 + 7z = 11 \qquad \rightarrow \qquad z = -21k^2 - 30k + 56s^2 + 16s - 8$$

Similarly, if $x \stackrel{7}{=} 5$ and $y \stackrel{7}{=} 6$ then we have:

$$3(5+7k)^2 - 8(6+7s)^2 + 7z = 11 \qquad \rightarrow \qquad z = -21k^2 - 30k + 56s^2 + 96s + 32$$

• $x \stackrel{7}{=} 6$ and hence $5y^2 + 6 \stackrel{7}{=} 1$ which has no solution.
So, the solutions are all triples (i.e. x, y, z) of the following eight forms (where $k, s \in \mathbb{Z}$):

$(2+7k,\ 1+7s,\ -21k^2 - 12k + 56s^2 + 16s + 1)$ $\qquad$ $(2+7k,\ 6+7s,\ -21k^2 - 12k + 56s^2 + 96s + 41)$

$(3+7k,\ 3+7s,\ -21k^2 - 18k + 56s^2 + 48s + 8)$ $\qquad$ $(3+7k,\ 4+7s,\ -21k^2 - 18k + 56s^2 + 64s + 16)$

$(4+7k,\ 3+7s,\ -21k^2 - 24k + 56s^2 + 48s + 5)$ $\qquad$ $(4+7k,\ 4+7s,\ -21k^2 - 24k + 56s^2 + 64s + 13)$

$(5+7k,\ 1+7s,\ -21k^2 - 30k + 56s^2 + 16s - 8)$ $\qquad$ $(5+7k,\ 6+7s,\ -21k^2 - 30k + 56s^2 + 96s + 32)$

(**c**) If we reduce the equation modulo 11 we get: $x^2 - y^2 - 2x - 8y - 15 \stackrel{11}{=} 0$. Considering all the 11 possibilities of $x \stackrel{11}{=} 0, 1, \ldots, 10$ with all the 11 possibilities of $y \stackrel{11}{=} 0, 1, \ldots, 10$ we find that only the following 21 combinations satisfy the equation $x^2 - y^2 - 2x - 8y - 15 \stackrel{11}{=} 0$:

$(x,y) \stackrel{11}{=} (0,6),\ (0,8),\ (1,7),\ (2,6),\ (2,8),\ (3,5),\ (3,9),\ (4,4),\ (4,10),\ (5,0),\ (5,3),\ (6,1),\ (6,2),\ (7,1),\ (7,2),\ (8,0),\ (8,3),\ (9,4),\ (9,10),\ (10,5),\ (10,9)$.
So, if $k, s \in \mathbb{Z}$ then the third combination (for instance) represents: $x = 1 + 11k$ and $y = 7 + 11s$.
Now, if we solve the given equation for z we get: $z = \frac{x^2 - y^2 - 2x - 8y - 15}{11}$. So, if we consider all these 21 combinations in this equation (to get z as we did in part b) then we get the following 21 general solutions to the given equation (where the triples represent x, y, z and $k, s \in \mathbb{Z}$):

$(11k, 6 + 11s, 11k^2 - 11s^2 - 2k - 20s - 9)$
$(11k, 8 + 11s, 11k^2 - 11s^2 - 2k - 24s - 13)$
$(1 + 11k, 7 + 11s, 11k^2 - 11s^2 - 22s - 11)$
$(2 + 11k, 6 + 11s, 11k^2 - 11s^2 + 2k - 20s - 9)$
$(2 + 11k, 8 + 11s, 11k^2 - 11s^2 + 2k - 24s - 13)$
$(3 + 11k, 5 + 11s, 11k^2 - 11s^2 + 4k - 18s - 7)$
$(3 + 11k, 9 + 11s, 11k^2 - 11s^2 + 4k - 26s - 15)$
$(4 + 11k, 4 + 11s, 11k^2 - 11s^2 + 6k - 16s - 5)$
$(4 + 11k, 10 + 11s, 11k^2 - 11s^2 + 6k - 28s - 17)$
$(5 + 11k, 11s, 11k^2 - 11s^2 + 8k - 8s)$
$(5 + 11k, 3 + 11s, 11k^2 - 11s^2 + 8k - 14s - 3)$
$(6 + 11k, 1 + 11s, 11k^2 - 11s^2 + 10k - 10s)$
$(6 + 11k, 2 + 11s, 11k^2 - 11s^2 + 10k - 12s - 1)$
$(7 + 11k, 1 + 11s, 11k^2 - 11s^2 + 12k - 10s + 1)$
$(7 + 11k, 2 + 11s, 11k^2 - 11s^2 + 12k - 12s)$
$(8 + 11k, 11s, 11k^2 - 11s^2 + 14k - 8s + 3)$
$(8 + 11k, 3 + 11s, 11k^2 - 11s^2 + 14k - 14s)$
$(9 + 11k, 4 + 11s, 11k^2 - 11s^2 + 16k - 16s)$
$(9 + 11k, 10 + 11s, 11k^2 - 11s^2 + 16k - 28s - 12)$
$(10 + 11k, 5 + 11s, 11k^2 - 11s^2 + 18k - 18s)$
$(10 + 11k, 9 + 11s, 11k^2 - 11s^2 + 18k - 26s - 8)$

(**d**) If we reduce the equation modulo 5 we get: $x^3 - 4y^2 \stackrel{5}{=} 0$, i.e. $4y^2 \stackrel{5}{=} x^3$. So, we have five cases to consider:
• $x \stackrel{5}{=} 0$ and hence $4y^2 \stackrel{5}{=} 0$ whose solution is $y \stackrel{5}{=} 0$, i.e. $y = 5s$ ($s \in \mathbb{Z}$). On substituting $x = 5k$ ($k \in \mathbb{Z}$) and $y = 5s$ in the original equation we get:

$$(5k)^3 - 4(5s)^2 + 5z = 0 \qquad \rightarrow \qquad z = 20s^2 - 25k^3$$

• $x \stackrel{5}{=} 1$ and hence $4y^2 \stackrel{5}{=} 1$ whose solutions are $y \stackrel{5}{=} 2$ and $y \stackrel{5}{=} 3$, i.e. $y = 2 + 5s$ and $y = 3 + 5s$. On substituting $x = 1 + 5k$ and $y = 2 + 5s$ in the original equation we get:

$$(1 + 5k)^3 - 4(2 + 5s)^2 + 5z = 0 \qquad \rightarrow \qquad z = -25k^3 - 15k^2 + 20s^2 - 3k + 16s + 3$$

Similarly, on substituting $x = 1 + 5k$ and $y = 3 + 5s$ in the original equation we get:

$$(1 + 5k)^3 - 4(3 + 5s)^2 + 5z = 0 \qquad \rightarrow \qquad z = -25k^3 - 15k^2 + 20s^2 - 3k + 24s + 7$$

• $x \stackrel{5}{=} 2$ and hence $4y^2 \stackrel{5}{=} 8$ which has no solution.
• $x \stackrel{5}{=} 3$ and hence $4y^2 \stackrel{5}{=} 27$ which has no solution.
• $x \stackrel{5}{=} 4$ and hence $4y^2 \stackrel{5}{=} 64$ whose solutions are $y \stackrel{5}{=} 1$ and $y \stackrel{5}{=} 4$, i.e. $y = 1 + 5s$ and $y = 4 + 5s$. On substituting $x = 4 + 5k$ and $y = 1 + 5s$ in the original equation we get:

$$(4 + 5k)^3 - 4(1 + 5s)^2 + 5z = 0 \qquad \rightarrow \qquad z = -25k^3 - 60k^2 + 20s^2 - 48k + 8s - 12$$

Similarly, on substituting $x = 4 + 5k$ and $y = 4 + 5s$ in the original equation we get:

$$(4 + 5k)^3 - 4(4 + 5s)^2 + 5z = 0 \qquad \rightarrow \qquad z = -25k^3 - 60k^2 + 20s^2 - 48k + 32s$$

So, the solutions are all triples of the following five forms (where $k, s \in \mathbb{Z}$):
$(x, y, z) = (5k,\ 5s,\ 20s^2 - 25k^3)$
$(x, y, z) = (1 + 5k,\ 2 + 5s,\ -25k^3 - 15k^2 + 20s^2 - 3k + 16s + 3)$
$(x, y, z) = (1 + 5k,\ 3 + 5s,\ -25k^3 - 15k^2 + 20s^2 - 3k + 24s + 7)$

$(x, y, z) = (4 + 5k,\ 1 + 5s,\ -25k^3 - 60k^2 + 20s^2 - 48k + 8s - 12)$
$(x, y, z) = (4 + 5k,\ 4 + 5s,\ -25k^3 - 60k^2 + 20s^2 - 48k + 32s)$
(**e**) On inspecting the given equation we note that $xyz \neq 0$ (since the equation has no solution in integers if at least one of the variables is zero; see the upcoming note). So, we are looking for solutions in non-zero integers. However, for simplicity we start by searching for solutions in natural numbers (i.e. $x, y, z \in \mathbb{N}$) and then generalize the obtained solution(s) to integers (i.e. $x, y, z \in \mathbb{Z}$). So, let assume that $x, y, z \in \mathbb{N}$ and $x \leq y \leq z$.
Now, z cannot be greater than 7 because otherwise:

$$8^4 = 4096 \leq z^4 \leq x^4 + y^4 + z^4 = 3042$$

which is a contradiction. Similarly, z cannot be less than 6 because otherwise (noting that $x \leq y \leq z$):

$$3042 = x^4 + y^4 + z^4 \leq 3z^4 \leq 3(5)^4 = 1875$$

which is a contradiction. So, we must have $z = 6$ or $z = 7$.
• If $z = 6$ then we have $x^4 + y^4 = 1746$, i.e. $x^4 = 1746 - y^4$. Now, y cannot be greater than 6 because x^4 becomes negative (which is impossible; also note the condition $x \leq y \leq z$). So, we have $x^4 = 1746 - y^4$ where $1 \leq y \leq 6$. On testing these values of y we find that $x^4 = 1746 - y^4$ (i.e. $x^4 + y^4 = 1746$) has no solution. This means that $x^4 + y^4 + z^4 = 3042$ has no solution when $z = 6$.
• If $z = 7$ then we have $x^4 + y^4 = 641$, i.e. $x^4 = 641 - y^4$. Now, y cannot be greater than 5 because x^4 becomes negative (which is impossible). So, we have $x^4 = 641 - y^4$ where $1 \leq y \leq 5$. On testing these values of y we find that $x^4 = 641 - y^4$ has only one solution, i.e. $y = 5$ and hence $x = 2$.[141] So, we found only one solution $\big[$i.e. $(x, y, z) = (2, 5, 7)\big]$ under the two conditions: $x, y, z \in \mathbb{N}$ and $x \leq y \leq z$. Now, to find all solutions we need to lift these conditions.
We lift the condition $x \leq y \leq z$ (noting the symmetry in x, y, z) by permuting x, y, z (and hence permuting the values in the above solution). Accordingly, the given equation has 6 solutions (where $x, y, z \in \mathbb{N}$): $(x, y, z) = (2, 5, 7)$, $(2, 7, 5)$, $(5, 2, 7)$, $(5, 7, 2)$, $(7, 2, 5)$, $(7, 5, 2)$.
We lift the condition $x, y, z \in \mathbb{N}$ by noting that all the variables are raised to power 4 and hence each one of these variables can be positive and negative (independently of the signs of the other two variables). So, we have 8 sign combinations for each one of the aforementioned 6 solutions, e.g. from the solution $(x, y, z) = (2, 5, 7)$ we get 8 solutions which are:
$(2, 5, 7)$ $(2, 5, -7)$ $(2, -5, 7)$ $(2, -5, -7)$ $(-2, 5, 7)$ $(-2, 5, -7)$ $(-2, -5, 7)$ $(-2, -5, -7)$
So in brief, the given equation has 48 solutions in $\mathbb{Z}$ (i.e. the 6 permuted solutions in $\mathbb{N}$ times the 8 sign combinations).
Note: it is obvious that $x = y = z = 0$ is not a solution. Similarly, when two of the variables are 0 (say $y = z = 0$) then the equation is not satisfied by any integer x (noting that 3042 is not a fourth power of an integer). Now, if only one variable is zero (say $z = 0$) then we have $x^4 + y^4 = 3042$. Noting that $x^4 \leq 3042$ it is obvious that $-7 \leq x \leq 7$ (and this similarly applies to y). On testing these few possibilities[142] we can easily verify that no integer x, y satisfy the equation $x^4 + y^4 = 3042$.

6. A right-angled triangle has sides a, b and hypotenuse c (where $a, b, c \in \mathbb{N}$). Show that the area of this triangle cannot be a perfect square.
Solution: From Pythagoras theorem we have $a^2 + b^2 = c^2$ and hence (a, b, c) is a Pythagorean triple. If a, b, c are not mutually coprimes we can cancel their gcd and hence reduce them mutually coprimes. So, we can assume that a, b, c are already reduced and hence (a, b, c) is primitive. Now, according to Problem 3 of § 4.1.4, there are coprimes $m, n \in \mathbb{N}$ of opposite parity with $m > n$ such that (a, b, c) is given by Euclid's formula, i.e.

$$a = 2mn \qquad b = m^2 - n^2 \qquad c = m^2 + n^2$$

[141] In fact, there is another solution (i.e. $x = 5$ and $y = 2$) but we are currently assuming $x \leq y$.
[142] In fact, we need to test only the non-negative (or non-positive) values because the fourth power of positive and negative integers is the same)

Now, if the area of the triangle is a perfect square (say S^2 where $S \in \mathbb{N}$) then from the formula of the area of right-angled triangle we have:

$$S^2 = \frac{1}{2}ab = \frac{1}{2} \times 2mn \times (m^2 - n^2) = mn(m^2 - n^2) \tag{78}$$

Now, m and n are coprime and hence each of m and n is coprime to $m^2 - n^2$ (see part b of Problem 19 of § 2.2). Thus, mn and $(m^2 - n^2)$ are coprime (see part e of Problem 1 of § 2.2) and hence from Eq. 78 we conclude that mn and $(m^2 - n^2)$ are squares (see Problem 20 of § 2.2). Thus, let $mn = A^2$ and $(m^2 - n^2) = B^2$ $(A, B \in \mathbb{N})$.
If we repeat this argument on $mn = A^2$ (noting that m and n are coprime and using Problem 20 of § 2.2) we conclude that m and n are squares. Thus, let $m = D^2$ and $n = E^2$ $(D, E \in \mathbb{N})$. So in brief we have:

$$m = D^2 \qquad n = E^2 \qquad m^2 - n^2 = B^2 \qquad (B, D, E \in \mathbb{N})$$

On substituting from the first two equations into the last equation we get $D^4 - E^4 = B^2$. However, $D^4 - E^4 = B^2$ has no solution in $\mathbb{N}$ (see part a of Problem 4). So, we conclude that the area of this triangle cannot be a perfect square (because the assumption of being a perfect square leads to no solution).

4.1.7 Diophantine Exponential Equations

In this subsection we give a few examples of Diophantine exponential equations in two and three variables and illustrate how they are solved.

Problems

1. Find the solutions of the following exponential Diophantine equations (where $x, y \in \mathbb{N}^0$):
   (**a**) $2^x + 3^y = 1$. (**b**) $4^x + 9^y = 2$. (**c**) $5^x + 7^y = 40369232$. (**d**) $11^x - 9^y = 34219$.
   Solution:
   (**a**) Noting that $2^x \geq 1$ and $3^y \geq 1$ (since $x, y \in \mathbb{N}^0$) there is no solution to this equation.
   (**b**) It should be obvious that the only solution is $x = y = 0$ because if $x > 0$ or $y > 0$ then the sum will be greater than 2.
   (**c**) If we test all the few combinations of low-value x and y that could possibly produce 40369232 (using for instance a spreadsheet) we can find that only $x = 6$ and $y = 9$ can satisfy this equation.
   (**d**) $11^x - 9^y$ is even and 34219 is odd (see the rules of parity in § 1.8). So, we can conclude immediately that this equation has no solution.
2. Find the solutions of the following exponential Diophantine equations (where $x, y \in \mathbb{N}^0$):
   (**a**) $4^x - 12^y = 0$. (**b**) $4^x - 12^y = 1$. (**c**) $4^x - 12^y = 2$. (**d**) $4^x - 12^y = 3$.
   (**e**) $4^x - 12^y = 4$. (**f**) $4^x - 12^y = 5$. (**g**) $4^x - 12^y = 6$. (**h**) $4^x - 12^y = 7$.
   (**i**) $4^x - 12^y = 8$. (**j**) $4^x - 12^y = 9$. (**k**) $4^x - 12^y = 10$. (**l**) $4^x - 12^y = 11$.
   (**m**) $4^x - 12^y = 12$. (**n**) $4^x - 12^y = 19$.
   Solution: Let us first investigate the modular behavior of $4^x - 12^y$ for a given modulo (say 13). If we test the powers of 4 and the powers of 12 (i.e. 4^x and 12^y for $x, y = 0, 1, 2, 3, \ldots$) modulo 13 then we find that the powers of 4 have a cycle of 6 (i.e. $4^x \overset{13}{=} 1, 4, 3, 12, 9, 10, 1, 4, 3, 12, 9, 10, \ldots$ for $x = 0, 1, 2, 3, \ldots, 11, \ldots$) while the powers of 12 have a cycle of 2 (i.e. $12^y \overset{13}{=} 1, 12, 1, 12, \ldots$ for $y = 0, 1, 2, 3, \ldots$). The modular value of $4^x - 12^y$ (mod 13) for all these 12 combinations (i.e. 6×2) are presented in the following table (where $k, s \in \mathbb{N}^0$):

	$\mathbf{4^{6k} \overset{13}{=} 1}$	$\mathbf{4^{6k+1} \overset{13}{=} 4}$	$\mathbf{4^{6k+2} \overset{13}{=} 3}$	$\mathbf{4^{6k+3} \overset{13}{=} 12}$	$\mathbf{4^{6k+4} \overset{13}{=} 9}$	$\mathbf{4^{6k+5} \overset{13}{=} 10}$
$\mathbf{12^{2s} \overset{13}{=} 1}$	0	3	2	11	8	9
$\mathbf{12^{2s+1} \overset{13}{=} 12}$	2	5	4	0	10	11

(**a**) From the modular table we can see that 0 is a modular value of $(4^x - 12^y)$ and hence there is a possibility that the equation $4^x - 12^y = 0$ has a solution (see points 6-8 of § 2.7.6). However, if we consider the prime factorization of 4^x and 12^y then we have $4^x = 2^{2x}$ and $12^y = 2^{2y} \times 3^y$. So, considering their prime factors, $4^x \neq 12^y$ (see § 2.1), and hence $4^x - 12^y = 0$ has no solution.
(**b**) From the modular table we can see that 1 is not a modular value of $(4^x - 12^y)$ and hence the equation $4^x - 12^y = 1$ has no solution (see point 7 of § 2.7.6 as well as part b of point 8 of § 2.7.6). We may also argue (more simply) that $4^x - 12^y$ is even unless $x = 0$ and $y \neq 0$ OR $x \neq 0$ and $y = 0$ (see the rules of parity in § 1.8), and hence $4^x - 12^y$ cannot be equal to 1 (which is odd) except (possibly) in one of these cases. However, if $x = 0$ and $y \neq 0$ then $(4^x - 12^y) \leq -11$, while if $x \neq 0$ and $y = 0$ then $(4^x - 12^y) \geq 3$ and hence in both cases $(4^x - 12^y) \neq 1$. Hence, $4^x - 12^y = 1$ has no solution.
(**c**) 2 is a modular value of $(4^x - 12^y)$ and hence $4^x - 12^y = 2$ may have a solution (see points 6-8 of § 2.7.6). Now, if $x = 0$ and $y \neq 0$ OR $x \neq 0$ and $y = 0$ then $4^x - 12^y$ is odd and hence it cannot be equal to 2 (which is even), while if $x = y = 0$ then $4^x - 12^y = 0 \neq 2$. So, the only possibility for $4^x - 12^y$ to be equal to 2 is if $x \neq 0$ and $y \neq 0$. However, in this case we have $4^x - 12^y = 4^x - 3^y\, 4^y = 4(4^{x-1} - 3^y\, 4^{y-1}) \neq 2$ (since 2 cannot be an integer multiple of 4). Hence, $4^x - 12^y = 2$ has no solution.
(**d**) 3 is a modular value of $(4^x - 12^y)$ and hence $4^x - 12^y = 3$ may have a solution (see points 6-8 of § 2.7.6). As we see, $4^x - 12^y \overset{13}{=} 3$ only for the combination $x = 6k + 1$ and $y = 2s$ $(k, s \in \mathbb{N}^0)$. On inspection we note that $4^x - 12^y = 3$ for $k = s = 0$ (i.e. $x = 1$ and $y = 0$). So, we have one solution to $4^x - 12^y = 3$. However, this solution should be the only possible solution because if $k \neq 0$ and $s = 0$ then $(4^x - 12^y) > 3$, while in the other two cases (i.e. $k = 0$ and $s \neq 0$ OR $k \neq 0$ and $s \neq 0$) $4^x - 12^y$ is even (see the rules of parity in § 1.8) and hence it cannot be equal to an odd number (i.e. 3). Hence, $4^x - 12^y = 3$ has only one solution, i.e. $x = 1$ and $y = 0$.
(**e**) 4 is a modular value of $(4^x - 12^y)$ and hence $4^x - 12^y = 4$ may have a solution. As we see, $4^x - 12^y \overset{13}{=} 4$ only for the combination $x = 6k + 2$ and $y = 2s + 1$ $(k, s \in \mathbb{N}^0)$. It is obvious that we have one solution to $4^x - 12^y = 4$, i.e. $x = 2$ and $y = 1$ corresponding to $k = s = 0$. However, this is the only possible solution because if $s = 0$ then $4^x - 12^y = 4^{6k+2} - 12$ which can be equal to 4 only if $k = 0$ (as we found already), while if $s \neq 0$ then we have:

$$4^x - 12^y = 4^{6k+2} - 12^{2s+1} = 4^{6k+2} - 3^{2s+1}4^{2s+1} = 4^2(4^{6k} - 3^{2s+1}4^{2s-1})$$

Now, $(4^{6k} - 3^{2s+1}4^{2s-1})$ is an integer (noting that $s > 0$) and hence $4^2(4^{6k} - 3^{2s+1}4^{2s-1})$ is a multiple of 4^2 and hence it cannot be equal to 4, i.e. $(4^x - 12^y)$ cannot be equal to 4 in this case. Hence, $4^x - 12^y = 4$ has no solution other than $x = 2$ and $y = 1$.
(**f**) 5 is a modular value of $(4^x - 12^y)$ and hence $4^x - 12^y = 5$ may have a solution. As we see, $4^x - 12^y \overset{13}{=} 5$ only for the combination $x = 6k + 1$ and $y = 2s + 1$ $(k, s \in \mathbb{N}^0)$. This means that we cannot have any solution to $4^x - 12^y = 5$ because for any value of k and s (including $k = s = 0$) the expression $(4^x - 12^y)$ is even and hence it cannot be equal to an odd number (i.e. 5). So, $4^x - 12^y = 5$ has no solution.
(**g**) 6 is not a modular value of $(4^x - 12^y)$ and hence the equation $4^x - 12^y = 6$ has no solution.
(**h**) 7 is not a modular value of $(4^x - 12^y)$ and hence the equation $4^x - 12^y = 7$ has no solution.
(**i**) 8 is a modular value of $(4^x - 12^y)$ and hence $4^x - 12^y = 8$ may have a solution. As we see, $4^x - 12^y \overset{13}{=} 8$ only for the combination $x = 6k + 4$ and $y = 2s$ $(k, s \in \mathbb{N}^0)$. Now, if we factorize $(4^{6k+4} - 12^{2s})$ and 8 we get:

$$4^{6k+4} - 12^{2s} = (4^{3k+2} - 12^s)(4^{3k+2} + 12^s) \overset{?}{=} 8 = 1 \times 8 = (-1) \times (-8) = 2 \times 4 = (-2) \times (-4)$$

It is obvious that $(4^{3k+2} + 12^s)$ (which is > 16) is not equal to ± 1 or ± 8 or ± 2 or ± 4. Hence, $(4^{6k+4} - 12^{2s}) \neq 8$, i.e. the equation $(4^x - 12^y) = 8$ has no solution.
(**j**) 9 is a modular value of $(4^x - 12^y)$ and hence $4^x - 12^y = 9$ may have a solution. As we see, $4^x - 12^y \overset{13}{=} 9$ only for the combination $x = 6k + 5$ and $y = 2s$ $(k, s \in \mathbb{N}^0)$. Now, $4^{6k+5} - 12^{2s}$ is even unless $s = 0$ and hence it cannot be equal to 9 (which is odd) except (possibly) when $s = 0$. However, if $s = 0$ then $(4^{6k+5} - 12^{2s}) \geq 1023$. Hence, $4^x - 12^y = 9$ has no solution.
(**k**) 10 is a modular value of $(4^x - 12^y)$ and hence $4^x - 12^y = 10$ may have a solution. As we see,

$4^x - 12^y \overset{13}{=} 10$ only for the combination $x = 6k + 4$ and $y = 2s + 1$ ($k, s \in \mathbb{N}^0$). Hence:

$$4^x - 12^y = 4^{6k+4} - 12^{2s+1} = 4^{6k+4} - 3^{2s+1}4^{2s+1} = 4(4^{6k+3} - 3^{2s+1}4^{2s})$$

As we see, $(4^x - 12^y)$ is a multiple of 4 in this case and hence it cannot be equal to 10 (which is not a multiple of 4). Hence, $4^x - 12^y = 10$ has no solution.

(**l**) 11 is a modular value of $(4^x - 12^y)$ and hence $4^x - 12^y = 11$ may have a solution. As we see, $4^x - 12^y \overset{13}{=} 11$ only for the combination $x = 6k + 3$ and $y = 2s$ and the combination $x = 6k + 5$ and $y = 2s+1$ ($k, s \in \mathbb{N}^0$). In all cases for both combinations, $(4^x - 12^y)$ is even and hence it cannot be equal to 11 which is odd. The only exception is in the case of $s = 0$ for the first combination (since $4^{6k+3} - 12^0$ is odd). However, even in this case $(4^x - 12^y)$ cannot be equal to 11 because $(4^{6k+3} - 12^0) \geq 63$. Hence, $4^x - 12^y = 11$ has no solution.

(**m**) 12 is not a modular value of $(4^x - 12^y)$ and hence the equation $4^x - 12^y = 12$ has no solution.

(**n**) We have $19 \overset{13}{=} 6$ and hence $4^x - 12^y = 19 \overset{13}{=} 6$. So, from part (g) we conclude that $4^x - 12^y = 19$ has no solution. We may also argue that $(4^x - 12^y)$ is even unless $x = 0$ and $y \neq 0$ OR $x \neq 0$ and $y = 0$ (see the rules of parity in § 1.8), and hence $(4^x - 12^y)$ cannot be equal to 19 (which is odd) except (possibly) in these two cases. However, if $x = 0$ and $y \neq 0$ then $(4^x - 12^y) \leq -11$, while if $x \neq 0$ and $y = 0$ then $(4^x - 12^y) = 3, 15, 63, \ldots$ and hence in both cases $(4^x - 12^y) \neq 19$. Hence, $4^x - 12^y = 19$ has no solution.

3. Find the solutions of the following exponential Diophantine equations (where $x, y \in \mathbb{N}^0$):

(**a**) $4^x - 3^y = 1$. (**b**) $4^x - 3^y = 3$.

Solution:

(**a**) For $x = 0$ we have $1 - 3^y = 1$ (i.e. $3^y = 0$) which has no solution.

For $x = 1$ we have $4 - 3^y = 1$ (i.e. $3^y = 3$) which has only one solution, i.e. $y = 1$.

For $x > 1$ we have no solution because:

$$4^x - 3^y = 2^{2x} - 3^y = (2^3 \times 2^{2x-3}) - 3^y = (8 \times 2^{2x-3}) - 3^y \overset{8}{=} -3^y \overset{8}{\neq} 1$$

where the last step is justified by the fact that $-3^y \overset{8}{=} -1 \overset{8}{=} 7$ for even y and $-3^y \overset{8}{=} -3 \overset{8}{=} 5$ for odd y.[143] This means that $4^x - 3^y \overset{8}{\neq} 1$ ($x > 1$) and hence $4^x - 3^y \neq 1$ (see part b of point 8 of § 2.7.6). So, the only possible solution is $(x, y) = (1, 1)$.

(**b**) For $x = 0$ we have $1 - 3^y = 3$ (i.e. $3^y = -2$) which has no solution.

For $x = 1$ we have $4 - 3^y = 3$ (i.e. $3^y = 1$) which has only one solution, i.e. $y = 0$.

For $x > 1$ we have no solution for the same reason as in part (a).

So, the only possible solution is $(x, y) = (1, 0)$.

4. Find the solutions of the following exponential Diophantine equations (where $x, y, z \in \mathbb{N}^0$):

(**a**) $3^x + 5^y - 7^z = 0$. (**b**) $4^x + 5^y - 6^z = 0$.

Solution:

(**a**) The expression $(3^x + 5^y - 7^z)$ is odd for all values of $x, y, z \in \mathbb{N}^0$,[144] and hence it cannot be equal to 0 (which is even). Therefore, $3^x + 5^y - 7^z = 0$ has no solution.

(**b**) The expression $(4^x + 5^y - 6^z)$ is odd for all values of $x, y, z \in \mathbb{N}^0$ except in two cases: $x = 0$ and $z \neq 0$ OR $x \neq 0$ and $z = 0$.[145] Hence, the equation $4^x + 5^y - 6^z = 0$ has no solution (since 0 is not

---

[143] This is because if $y = 2k$ ($k \in \mathbb{N}^0$) then $3^y = 3^{2k} = 9^k \overset{8}{=} 1^k = 1$, while if $y = 2k + 1$ ($k \in \mathbb{N}^0$) then $3^y = 3^{2k+1} = 3^{2k}\,3 = 9^k\,3 \overset{8}{=} 1^k\,3 = 3$.

[144] This includes the case when some or all of x, y, z are zero because the parity of an odd number (i.e. $3, 5, 7$ in our case) does not change when it is raised to power 0 (since any non-zero integer raised to power 0 is 1 which is odd). See rule 10 of § 1.8.

[145] What distinguishes these two cases from all other cases is that in these two cases exactly one term changes its parity (i.e. 4^0 and 6^0) from even to odd and hence the parity of the sum $(4^x + 5^y - 6^z)$ becomes even noting that the parity of an even number (i.e. $4, 6$ in our case) does change when it is raised to power 0 (since any non-zero integer raised to power 0 is 1 which is odd). See rule 10 of § 1.8.

odd) except (possibly) in these two cases. So, all we need to do is to investigate these two cases:
• Case 1: $x = 0$ and $z \neq 0$:
If $y = 0$ then we have $4^0 + 5^0 - 6^z = (2 - 6^z) < 0$ and hence $4^x + 5^y - 6^z = 0$ has no solution.
If $y \neq 0$ then we have $4^0 + 5^y - 6^z = 0$, i.e. $6^z = 1 + 5^y$ which has an obvious solution $y = z = 1$. However, $6^z = 1 + 5^y$ has no other solution because for $y > 1$ the numbers 5^y end in 25 (see rule 14 of § 1.8), while for $z > 1$ the numbers 6^z end in $36, 16, 96, 76, 56$ (see Problem 14 of § 2.7) and hence $6^z \neq 1 + 5^y$ when $y > 1$ and $z > 1$. If $y = 1$ and $z > 1$ then $6^z > (1 + 5^1)$, while if $y > 1$ and $z = 1$ then $6^1 < (1 + 5^y)$.
So, in Case 1 we have only one solution, i.e. $x = 0$ and $y = z = 1$.
• Case 2: $x \neq 0$ and $z = 0$:
If $y = 0$ then we have $4^x + 5^0 - 6^0 = 4^x > 0$ and hence $4^x + 5^y - 6^z = 0$ has no solution.
If $y \neq 0$ then we have $4^x + 5^y - 6^0 = (4^x + 5^y - 1) \geq 8$ and hence $4^x + 5^y - 6^z = 0$ has no solution.
So, in Case 2 we have no solution.
Therefore, $4^x + 5^y - 6^z = 0$ has only one solution, i.e. $x = 0$ and $y = z = 1$.

4.1.8 Mixed Diophantine Polynomial-Exponential Equations

In this subsection we give a few examples of mixed Diophantine polynomial-exponential equations in two and three variables and demonstrate how they are solved.

Problems

1. Find the solutions of the following mixed Diophantine polynomial-exponential equations:
   (**a**) $5x + 4^y - 11 = 0$ $(x \in \mathbb{Z}, y \in \mathbb{N}^0)$.
   (**b**) $5^x - 6y + 21 = 0$ $(x \in \mathbb{N}^0, y \in \mathbb{Z})$.
   (**c**) $5^x - 11x + 3y + 1 = 0$ $(x \in \mathbb{N}^0, y \in \mathbb{Z})$.
   (**d**) $3^x + 5^y - 4z - 2 = 0$ $(x, y \in \mathbb{N}^0, z \in \mathbb{Z})$.

   Solution:
   (**a**) If we reduce this equation modulo 5 we get: $4^y - 11 \overset{5}{=} 0$, i.e. $(-1)^y - 1 \overset{5}{=} 0$. The solution of this congruence equation is all even $y \geq 0$, i.e. $y = 2k$ $(k \in \mathbb{N}^0)$. On solving the given equation for x we get:

$$x = \frac{11 - 4^y}{5} = \frac{11 - 4^{2k}}{5}$$

   So, the solutions of the given equation are all pairs of the following form: $(x, y) = \left(\frac{11-4^{2k}}{5}, 2k\right)$ where $k \in \mathbb{N}^0$. It is worth noting that $(11 - 4^{2k})/5$ is always integer because for $k = 0$ it is equal to 2, while for $k > 0$ the numerator $(11 - 4^{2k})$ ends in 5 (because 4^{2k} ends in 6; see rule 13 of § 1.8) and hence it is divisible by 5 (see rule 27 of § 1.9).
   (**b**) If we reduce this equation modulo 6 we get: $5^x + 21 \overset{6}{=} 0$, i.e. $(-1)^x + 3 \overset{6}{=} 0$. As we see, this congruence equation has no solution (because the left hand side is either 2 or 4) and hence the given equation has no solution (see part b of point 8 of § 2.7.6).
   (**c**) If we reduce this equation modulo 3 we get: $5^x + x + 1 \overset{3}{=} 0$. The solutions of this congruence equation are $x = 3 + 6k$ and $x = 4 + 6k$ where $k \in \mathbb{N}^0$ (see the upcoming notes 1 and 2). On substituting these expressions of x in the original equation and solving for y we get:

$$y = \frac{-5^{3+6k} + 32 + 66k}{3} \qquad \text{and} \qquad y = \frac{-5^{4+6k} + 43 + 66k}{3}$$

   So, the solutions of the given equation are all pairs of the following two forms:

$$(x, y) = \left(3 + 6k, \frac{-5^{3+6k} + 32 + 66k}{3}\right) \qquad \text{and} \qquad (x, y) = \left(4 + 6k, \frac{-5^{4+6k} + 43 + 66k}{3}\right)$$

   It is worth noting that $(-5^{3+6k} + 32 + 66k)/3$ and $(-5^{4+6k} + 43 + 66k)/3$ are always integers (see the upcoming note 3).
   Note 1: if we test the first few values of $x \in \mathbb{N}^0$ we find $x = 3, 9$ and $x = 4, 10$ satisfy the congruence

equation $5^x + x + 1 \overset{3}{=} 0$. This suggests that this may be true for all $x = 3 + 6k$ and $x = 4 + 6k$ ($k \in \mathbb{N}^0$) and that is what we will try to establish using proof by induction (see § 1.5.4). In fact, we will give in the following the proof for $x = 3 + 6k$ only (noting that the proof for $x = 4 + 6k$ is similar).

For $k = 0$ we have $5^3 + 3 + 1 \overset{3}{=} 0$ which is true. Now, let assume that $5^{3+6k} + (3 + 6k) + 1 \overset{3}{=} 0$ is true for a given $k \in \mathbb{N}$ and hence we have:

$$\begin{aligned} 5^{3+6k} + (3 + 6k) + 1 &\overset{3}{=} 0 && \text{(given)} \\ 5^{3+6k} \times 5^6 + (3 + 6k + 6) + 1 &\overset{3}{=} 0 && (5^6 \overset{3}{=} 1 \text{ and } 6 \overset{3}{=} 0) \\ 5^{3+6k+6} + (3 + 6k + 6) + 1 &\overset{3}{=} 0 && \text{(rules of indices)} \\ 5^{3+6(k+1)} + \big[3 + 6(k + 1)\big] + 1 &\overset{3}{=} 0 \end{aligned}$$

So, it is true for $k + 1$ (assuming it is true for k) and hence it is true for all $k \in \mathbb{N}^0$.

Note 2: we could have reduced the given equation modulo 3 as: $(-1)^x + x + 1 \overset{3}{=} 0$ and hence we prove that the solutions of this congruence are $x = 3 + 6k$ and $x = 4 + 6k$ as follows:

The congruence equation $(-1)^x + x + 1 \overset{3}{=} 0$ is satisfied in the following two (comprehensive and mutually exclusive) cases:

• $(-1)^x \overset{3}{=} -1$ (i.e. x is odd) and $x \overset{3}{=} 0$ (i.e. $x = 3s$ for some $s \in \mathbb{N}$). So, for these conditions to be satisfied simultaneously we need s to be odd (say $s = 2k + 1$ for some $k \in \mathbb{N}^0$) and hence $x = 3(1 + 2k) = 3 + 6k$.

• $(-1)^x \overset{3}{=} 1$ (i.e. x is even) and $x \overset{3}{=} 1$ (i.e. $x = 1 + 3s$ for some $s \in \mathbb{N}$). So, for these conditions to be satisfied simultaneously we need s to be odd (say $s = 1 + 2k$ for some $k \in \mathbb{N}^0$) and hence $x = 1 + 3(1 + 2k) = 4 + 6k$.

Note 3: we have:

$$-5^{3+6k} + 32 + 66k \overset{3}{=} -(-1)^{3+6k} + 2 = 1 + 2 = 3 \overset{3}{=} 0$$

where step 2 is because $(3 + 6k)$ is odd. So, $(-5^{3+6k} + 32 + 66k)/3$ is always integer.

Similarly:

$$-5^{4+6k} + 43 + 66k \overset{3}{=} -(-1)^{4+6k} + 1 = -1 + 1 = 0$$

where step 2 is because $(4 + 6k)$ is even. So, $(-5^{4+6k} + 43 + 66k)/3$ is always integer.

(**d**) If we reduce this equation modulo 4 we get: $3^x + 5^y - 2 \overset{4}{=} 0$, i.e. $(-1)^x + (1)^y - 2 \overset{4}{=} 0$. The solution of this equation is $x = 2k$ and $y = s$ ($k, s \in \mathbb{N}^0$). On solving the given equation for z we get:

$$z = \frac{3^x + 5^y - 2}{4} = \frac{3^{2k} + 5^s - 2}{4}$$

So, the solutions of the given equation are all triples of the following form: $(x, y, z) = \left(2k,\ s,\ \frac{3^{2k}+5^s-2}{4}\right)$ where $k, s \in \mathbb{N}^0$. It is worth noting that $(3^{2k} + 5^s - 2)/4$ is always integer because:

$$3^{2k} + 5^s - 2 \overset{4}{=} (-1)^{2k} + (1)^s - 2 = 1 + 1 - 2 = 0$$

4.1.9 Diophantine Equations Involving Roots

In this subsection we give a few examples of Diophantine equations involving roots in two and three variables and illustrate how they are solved. In fact, labeling this type of equations as "Diophantine equations" is rather loose and could be controversial although this is of no concern to us (see § 4.1).

Problems

1. Find the solutions of the following Diophantine equations involving roots (where $x, y, z \in \mathbb{Z}$):

(**a**) $\sqrt{x} + \sqrt{y} = 9$. (**b**) $3\sqrt[3]{x^2} + 5\sqrt[3]{y} = 47$. (**c**) $\sqrt{x} - y = 379$.

(**d**) $6x + 10\sqrt{y} - 19z = 0$. (**e**) $21x + 35\sqrt{y} - 12\sqrt{z} = 41$. (**f**) $\sqrt{x} + \sqrt{y} = \sqrt{363}$.

(**g**) $\sqrt{(x+1)} - \sqrt{(y+5)} = 1$.

Solution:

(**a**) We have only 10 pairs of $\sqrt{x}$ and $\sqrt{y}$ that can add up to 9, i.e. $(\sqrt{x}, \sqrt{y}) = (0,9), (1,8) \ldots (9,0)$. So, if we square the numbers in each pair then we get all the possible solutions. In fact, because of the symmetry of x and y we need only to obtain the first 5 pairs and then get the remaining 5 pairs by reversing x and y. So, the 10 solutions are:

$(x,y) = (0,81)$ $(x,y) = (1,64)$ $(x,y) = (4,49)$ $(x,y) = (9,36)$ $(x,y) = (16,25)$

$(x,y) = (25,16)$ $(x,y) = (36,9)$ $(x,y) = (49,4)$ $(x,y) = (64,1)$ $(x,y) = (81,0)$

(**b**) If $X = \sqrt[3]{x^2}$ and $Y = \sqrt[3]{y}$ then we have: $3X + 5Y = 47$ ($X \in \mathbb{N}^0$ and $Y \in \mathbb{Z}$). The solution of this equation is (see § 4.1.1): $X = 9 + 5k$ and $Y = 4 - 3k$ ($k \in \mathbb{Z}$, $k \geq -1$ noting that $X \in \mathbb{N}^0$). Accordingly:

$\sqrt[3]{x^2} = 9 + 5k \quad \rightarrow \quad x^2 = 125k^3 + 675k^2 + 1215k + 729 \quad \rightarrow \quad x = \pm\sqrt{125k^3 + 675k^2 + 1215k + 729}$

$\sqrt[3]{y} = 4 - 3k \quad \rightarrow \quad y = -27k^3 + 108k^2 - 144k + 64$

However, since $x \in \mathbb{Z}$ the square root $\sqrt{125k^3 + 675k^2 + 1215k + 729}$ must be an integer. This can be achieved by imposing the following condition on k:

$$k = \frac{10m^2 - 10m - 6m(-1)^m + 3(-1)^m - 11}{8} \qquad (m \in \mathbb{Z}) \qquad (79)$$

So, the solutions are: $(x,y) = \left(\pm\sqrt{125k^3 + 675k^2 + 1215k + 729},\ -27k^3 + 108k^2 - 144k + 64\right)$ where k is given by Eq. 79.

(**c**) x must be a perfect square (i.e. $x = s^2$ where $s \in \mathbb{Z}$) and hence $y = \sqrt{x} - 379 = |s| - 379$ (where $|s|$ is the absolute value of s). So, the solutions are $(x,y) = (s^2, |s| - 379)$ where $s \in \mathbb{Z}$.

(**d**) Let $Y = \sqrt{y}$ and hence $6x + 10Y - 19z = 0$ whose solution is (see part b of Problem 1 of § 4.1.2):

$$x = 11s - 19k \qquad Y = s \qquad z = 4s - 6k \qquad (s, k \in \mathbb{Z})$$

Now, for $\sqrt{y}$ to be an integer we must have $y = t^2$ ($t \in \mathbb{Z}$). Hence, $Y = \sqrt{y} = \sqrt{t^2} = |t| = s$ (where $|t|$ is the absolute value of t). Therefore, the solution of $6x + 10\sqrt{y} - 19z = 0$ is:

$$x = 11|t| - 19k \qquad y = t^2 \qquad z = 4|t| - 6k \qquad (t, k \in \mathbb{Z})$$

(**e**) Let $Y = \sqrt{y}$ and $Z = \sqrt{z}$ and hence $21x + 35Y - 12Z = 41$ whose solution is (see part c of Problem 1 of § 4.1.2):

$$x = 2 - 5s - 4k \qquad Y = 1 + 3s \qquad Z = 3 - 7k \qquad (s, k \in \mathbb{Z})$$

Now, $Y = \sqrt{y} \geq 0$ and hence s must be ≥ 0 (i.e. $s \in \mathbb{N}^0$). Also, $Z = \sqrt{z} \geq 0$ and hence k must be ≤ 0 (i.e. $\mathbb{Z} \ni k \leq 0$). Therefore, the solution of $21x + 35\sqrt{y} - 12\sqrt{z} = 41$ is:

$$x = 2 - 5s - 4k \qquad y = (1 + 3s)^2 \qquad z = (3 - 7k)^2 \qquad (s \in \mathbb{N}^0,\ \mathbb{Z} \ni k \leq 0)$$

(**f**) We have $\sqrt{y} = \sqrt{363} - \sqrt{x}$ and hence by squaring both sides we get $y = 363 - 2\sqrt{363x} + x = 363 - 22\sqrt{3x} + x$. Since x and y are integers then $22\sqrt{3x}$ must be an integer and hence $\sqrt{3x}$ must be a rational number, i.e. $\sqrt{3x} = s/t$ where s and t are coprime ($s, t \in \mathbb{Z}$). By squaring and arranging we get: $3xt^2 = s^2$. Now, since s and t are coprime then all the prime factors of s^2 should belong to $3x$, i.e. $3x = s^2$ (or $t^2 = 1$). Accordingly, $3|s$ and hence $s = 3m$ ($m \in \mathbb{Z}$). Thus $x = s^2/3 = 9m^2/3 = 3m^2$.
By a similar argument we should also have $y = 3n^2$ ($n \in \mathbb{Z}$).

So, we have:

$\sqrt{x}+\sqrt{y}=\sqrt{363} \quad \rightarrow \quad \sqrt{3m^2}+\sqrt{3n^2}=\sqrt{363} \quad \rightarrow \quad |m|\sqrt{3}+|n|\sqrt{3}=11\sqrt{3} \quad \rightarrow \quad |m|+|n|=11$

i.e. $|n|=11-|m|$. Hence, $x=3m^2$ and $y=3(11-|m|)^2$. Now, $|n|=11-|m|$ and hence we have only 12 possible values of m, i.e. $m=0,1,\ldots,11$ (noting that the negative values of m produce the same solutions). So, we have only 12 possible solutions to the equation $\sqrt{x}+\sqrt{y}=\sqrt{363}$, i.e. $(x,y)=(0,363)$, $(3,300)$, $(12,243)$, $(27,192)$, $(48,147)$, $(75,108)$, $(108,75)$, $(147,48)$, $(192,27)$, $(243,12)$, $(300,3)$, $(363,0)$.

Note: we may solve this Problem more simply by a method similar to the method of part (a). In brief, $\sqrt{363}=11\sqrt{3}$ and hence we have only 12 pairs of $\sqrt{x}$ and $\sqrt{y}$ that can add up to $\sqrt{363}$, i.e. $(\sqrt{x},\sqrt{y})=(0\sqrt{3},11\sqrt{3}),(1\sqrt{3},10\sqrt{3}),\ldots,(11\sqrt{3},0\sqrt{3})$. So, if we square the numbers in each pair then we get all the possible solutions. In fact, because of the symmetry of x and y we need only to obtain the first 6 pairs and then get the remaining 6 pairs by reversing x and y. So, by this method we obtain the same 12 solutions that we obtained above.

(**g**) Let $X=(x+1)$ and $Y=(y+5)$ and hence we have $\sqrt{X}-\sqrt{Y}=1$. Now, if $X=k^2$ $(k\in\mathbb{Z})$ then $\sqrt{Y}=\sqrt{X}-1=|k|-1$, i.e. $Y=(|k|-1)^2$ where $|k|$ is the absolute value of k. However, since $\sqrt{X}-\sqrt{Y}=1$ then we must have:

$(\sqrt{X}-\sqrt{Y})>0 \quad \rightarrow \quad \sqrt{X}>\sqrt{Y} \quad \rightarrow \quad X>Y \quad \rightarrow \quad k^2>(k^2-2\,|k|+1) \quad \rightarrow \quad |k|>(1/2)$

i.e. $k\in\mathbb{Z}$ and $k\neq 0$. Hence, $X=(x+1)=k^2$ and $Y=(y+5)=(|k|-1)^2$ where $k\in\mathbb{Z}$ and $k\neq 0$. So, the solutions of the given equation are all pairs of the following form: $(x,y)=\big(k^2-1,\,\{|k|-1\}^2-5\big)$ where $k\in\mathbb{Z}$ and $k\neq 0$.

2. Find the solutions of the following Diophantine equation: $5^x-7^y-2\sqrt{z}=0$ (where $x,y,z\in\mathbb{N}^0$).

Solution: If we reduce this equation modulo 2 we get: $1^x-1^y\overset{2}{=}0$. The solutions of this congruence are $x=k$ and $y=s$ $(k,s\in\mathbb{N}^0)$. On solving the given equation for z we get:

$$\sqrt{z}=\frac{5^x-7^y}{2}=\frac{5^k-7^s}{2} \qquad \rightarrow \qquad z=\left(\frac{5^k-7^s}{2}\right)^2 \qquad \big[(5^x-7^y)\geq 0\big]$$

where we imposed the condition $(5^x-7^y)\geq 0$ because $\sqrt{z}$ is non-negative. So, the solutions of the given equation are all triples of the following form: $(x,y,z)=\left(k,\,s,\,\left[\frac{5^k-7^s}{2}\right]^2\right)$ where $k,s\in\mathbb{N}^0$ and $(5^x-7^y)\geq 0$. It is worth noting that z is always integer because (5^k-7^s) is always even for $k,s\in\mathbb{N}^0$.

4.1.10 Diophantine Equations Involving Fractions

In this subsection we give a few examples of Diophantine equations involving fractions in two and three variables and demonstrate how they are solved. Again, labeling this type of equations as "Diophantine equations" is rather loose and could be controversial although this is of no concern to us.

Problems

1. Find all $n,k\in\mathbb{Z}$ that satisfy the following equations:

(**a**) $\frac{5-3n}{5n-6}=k$. (**b**) $\frac{n^2-9n+13}{n+4}=k$.

Solution:

(**a**) $(5n-6)$ divides any of its multiples, and hence $(5n-6)$ divides $3(5n-6)=15n-18$. Also, if $(5n-6)$ should divide $(5-3n)$ then $(5n-6)$ must divide any multiple of $(5-3n)$, and hence $(5n-6)$ should divide $5(5-3n)=25-15n$. So, $(5n-6)$ divides both $(15n-18)$ and $(25-15n)$ and hence it must divide their sum which is 7 (rule 14 of § 1.9). Noting that the divisors of 7 are ±1 and ±7, we conclude that $(5n-6)$ must be ±1 or ±7 (which are the four possible divisors of 7). Considering all these four possibilities we have:

- $(5n-6)=-1$, i.e. $n=1$ and hence $k=-2$.
- $(5n-6)=+1$, i.e. $n=7/5$ (which is not acceptable).
- $(5n-6)=-7$, i.e. $n=-1/5$ (which is not acceptable).

• $(5n-6)=+7$, i.e. $n=13/5$ (which is not acceptable).
So, we have only one acceptable solution, i.e. $n=1$ and $k=-2$.
(**b**) We have:

$$\frac{n^2-9n+13}{n+4}=n-13+\frac{65}{n+4}$$

Hence, $(n+4)$ is a divisor of 65 (since $k\in\mathbb{Z}$). Noting that the divisors of 65 are $\pm1,\pm5,\pm13,\pm65$, we conclude that $(n+4)$ must be equal to these divisors. Considering all these eight possibilities we have:
• $(n+4)=-65$, i.e. $n=-69$ and hence $k=-83$.
• $(n+4)=-13$, i.e. $n=-17$ and hence $k=-35$.
• $(n+4)=-5$, i.e. $n=-9$ and hence $k=-35$.
• $(n+4)=-1$, i.e. $n=-5$ and hence $k=-83$.
• $(n+4)=1$, i.e. $n=-3$ and hence $k=49$.
• $(n+4)=5$, i.e. $n=1$ and hence $k=1$.
• $(n+4)=13$, i.e. $n=9$ and hence $k=1$.
• $(n+4)=65$, i.e. $n=61$ and hence $k=49$.

2. Find all $x,y\in\mathbb{Z}$ that satisfy the following equations:
(**a**) $\frac{14}{x}+\frac{y}{19}=25$. (**b**) $\frac{20}{x}+\frac{33}{y}=2$. (**c**) $\frac{x}{y}+\frac{y}{x}=1$. (**d**) $\frac{x}{y}+\frac{y}{x}=2$.
Solution:
(**a**) From the given equation we get: $y=475-\frac{266}{x}$. Now, y is an integer and hence x must divide 266. Noting that the divisors of 266 are $1,2,7,14,19,38,133,266$ and their negatives, we conclude that x must be equal to these divisors (i.e. the 16 possible divisors of 266). Considering all these 16 possibilities (i.e. $x=\pm1,\pm2,\ldots,\pm266$) we obtain y from the formula $y=475-\frac{266}{x}$. On doing this we obtained the following 16 solutions: $(x,y)=(-266,476)$, $(-133,477)$, $(-38,482)$, $(-19,489)$, $(-14,494)$, $(-7,513)$, $(-2,608)$, $(-1,741)$, $(1,209)$, $(2,342)$, $(7,437)$, $(14,456)$, $(19,461)$, $(38,468)$, $(133,473)$, $(266,474)$.
(**b**) From the given equation we get: $x=\frac{20y}{2y-33}$. Now, $(2y-33)$ divides any of its multiples, and hence $(2y-33)$ divides $10(2y-33)=20y-330$. Also, since x is an integer then $(2y-33)$ should divide $20y$. So, $(2y-33)$ divides both $(20y-330)$ and $20y$ and hence it must divide their difference which is 330 (rule 14 of § 1.9). Noting that the divisors of 330 are 1, 2, 3, 5, 6, 10, 11, 15, 22, 30, 33, 55, 66, 110, 165, 330 and their negatives, we conclude that $(2y-33)$ must be equal to some of these divisors (i.e. the 32 possible divisors of 330). Considering all these 32 possibilities (i.e. $2y-33=\pm1,\pm2,\ldots,\pm330$) we obtain y (accepting only $\mathbb{Z}\ni y\neq0$). We then obtain (from the obtained integer y's) the corresponding x's using the formula $x=\frac{20y}{2y-33}$. On doing this we obtained the following 15 solutions: $(x,y)=(-320,16)$, $(-100,15)$, $(-56,14)$, $(-20,11)$, $(-12,9)$, $(4,-11)$, $(8,-66)$, $(12,99)$, $(16,44)$, $(20,33)$, $(32,24)$, $(40,22)$, $(76,19)$, $(120,18)$, $(340,17)$.
Note: we may also solve for y (i.e. $y=\frac{33x}{2x-20}$) and follow a similar argument which will lead to the same solutions.
(**c**) We note that $xy\neq0$. We also note that if this equation has a solution then x and y must have the same sign because otherwise the sum will be negative. Now:
• If we multiply the given equation by xy and solve for x^2 we get $x^2=xy-y^2$. Since $x^2>0$ then $xy>y^2$.
• If we multiply the given equation by xy and solve for y^2 we get $y^2=xy-x^2$. Since $y^2>0$ then $xy>x^2$.
So, we have $xy>y^2$ and $xy>x^2$. Now:
• If $x>0$ and $y>0$ then we have (on dividing by y and x respectively) $x>y$ and $y>x$ which is a contradiction.
• If $x<0$ and $y<0$ then we have (on dividing by y and x respectively) $x<y$ and $y<x$ which is a contradiction.
So, this equation has no solution.
(**d**) We note that $xy\neq0$. On multiplying the given equation by xy and rearranging we get $x^2+y^2-2xy=0$, i.e. $(x-y)^2=0$ and hence $x=y\neq0$. So, the general solution of this equation is $(x,y)=(k,k)$ where $k\in\mathbb{Z}$ and $k\neq0$.

3. Repeat Problem 2 but replacing the plus sign by minus sign.
Solution:
(**a**) If we write the equation as $\frac{14}{x} + \frac{Y}{19} = 25$ where $Y = -y$ then we get the same solutions for (x, Y) as those found in part (a) of Problem 2 for (x, y). Hence, the solutions of the given equation are the same as the solutions found in part (a) of Problem 2 but with y replaced by $-y$.
(**b**) If we repeat the argument of part (a) then we conclude that the solutions are the same as those of part (b) of Problem 2 but with y replaced by $-y$.
(**c**) On multiplying the given equation by xy ($\neq 0$) we get $x^2 - y^2 = xy$, i.e. $x^2 - yx - y^2 = 0$. On solving this quadratic equation in x we get:

$$x = \frac{y \pm \sqrt{(-y)^2 - 4(-y^2)}}{2} = \frac{y \pm \sqrt{y^2 + 4y^2}}{2} = \frac{y \pm \sqrt{5y^2}}{2} = \frac{y \pm |y|\sqrt{5}}{2}$$

which is impossible because x is an integer while the right hand side is irrational (since $\sqrt{5}$ is irrational). So, the given equation has no solution.
(**d**) On multiplying the given equation by xy ($\neq 0$) we get $x^2 - y^2 = 2xy$, i.e. $x^2 = (2xy + y^2)$. Hence:

$$2x^2 = x^2 + x^2 = x^2 + (2xy + y^2) = x^2 + 2xy + y^2 = (x + y)^2$$

Now, if we take the square root of both sides we get: $x\sqrt{2} = \pm(x + y)$ which is impossible because $x\sqrt{2}$ is irrational (since $\sqrt{2}$ is irrational) while $(x + y)$ is an integer. So, the given equation has no solution.
4. Prove the following: if $x, y, k \in \mathbb{Z}$ ($xy \neq 0$) then $\frac{x}{y} + \frac{y}{x} = k$ has no solution except for $k = \pm 2$.
Solution: On multiplying the given equation by xy and rearranging we get: $y^2 - kxy + x^2 = 0$. Now, if we solve this equation for y (using the quadratic formula) we get:

$$y = \frac{kx \pm \sqrt{k^2x^2 - 4x^2}}{2} = \frac{kx \pm |x|\sqrt{k^2 - 4}}{2}$$

Now, since y is an integer then $\sqrt{k^2 - 4}$ must be an integer (because otherwise $\sqrt{k^2 - 4}$ is irrational; see rule 28 of § 1.8) and hence $(k^2 - 4)$ must be a perfect square,[146] i.e. $k^2 - 4 = s^2$ (where $s \in \mathbb{Z}$). Accordingly, we have:

$$k^2 - s^2 = (k - s)(k + s) = 4 = (-1) \times (-4) = 1 \times 4 = (-2) \times (-2) = 2 \times 2$$

So, we have 6 cases:
- $(k - s) = -1$ and $(k + s) = -4$, i.e. $k = -5/2$ and $s = -3/2$ which is not acceptable.
- $(k - s) = -4$ and $(k + s) = -1$, i.e. $k = -5/2$ and $s = 3/2$ which is not acceptable.
- $(k - s) = 1$ and $(k + s) = 4$, i.e. $k = 5/2$ and $s = 3/2$ which is not acceptable.
- $(k - s) = 4$ and $(k + s) = 1$, i.e. $k = 5/2$ and $s = -3/2$ which is not acceptable.
- $(k - s) = -2$ and $(k + s) = -2$, i.e. $k = -2$ and $s = 0$ which is acceptable.
- $(k - s) = 2$ and $(k + s) = 2$, i.e. $k = 2$ and $s = 0$ which is acceptable.

So in brief, we have only two acceptable values of k, i.e. $k = \pm 2$. The general solution of $\frac{x}{y} + \frac{y}{x} = -2$ is $y = -x$ while the general solution of $\frac{x}{y} + \frac{y}{x} = 2$ is $y = x$ (where $x, y \in \mathbb{Z}$ and $xy \neq 0$).
5. Prove the following: if $x, y, k \in \mathbb{Z}$ ($xy \neq 0$) then $\frac{x}{y} - \frac{y}{x} = k$ has no solution except for $k = 0$.
Solution: If we repeat the analysis of Problem 4 then we should get:

$$y = \frac{-kx \pm |x|\sqrt{k^2 + 4}}{2}$$

and hence $s^2 - k^2 = 4$. So, on considering the 6 cases for $(s - k)$ and $(s + k)$ we get only one acceptable value for k (i.e. $k = 0$ from the last two cases). The general solutions of $\frac{x}{y} - \frac{y}{x} = 0$ are $y = x$ and $y = -x$ (where $x, y \in \mathbb{Z}$ and $xy \neq 0$).

[146] In fact, this is a necessary but not sufficient condition, but we will do a test later.

6. Find all $x, y, z \in \mathbb{Z}$ that satisfy the following equations:
(**a**) $\frac{x}{8} + \frac{y}{5} - \frac{3}{z} = 7$. (**b**) $\frac{1}{x} + \frac{1}{y} = z$. (**c**) $\frac{x}{y} + \frac{y}{z} = 1$.
Solution:
(**a**) From the given equation we get: $z = \frac{120}{5x+8y-280}$. Now, z is an integer and hence $(5x + 8y - 280)$ must divide 120. Noting that the divisors of 120 are $1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120$ and their negatives, we conclude that $(5x + 8y - 280)$ must be equal to these divisors (i.e. the 32 possible divisors of 120). Considering all these 32 possibilities (i.e. $5x + 8y - 280 = \pm 1, \pm 2, \ldots, \pm 120$) we can obtain x and y (parameterized by $k \in \mathbb{Z}$; see § 4.1.1) and the corresponding z (by dividing 120 on the corresponding divisor). On doing this we obtained the following 32 parameterized solutions (i.e. x, y, z):

$(8k, 20 - 5k, -1)$	$(4 + 8k, 25 - 5k, -2)$	$(8k, 30 - 5k, -3)$	$(2 + 8k, 30 - 5k, -4)$
$(8k, 32 - 5k, -5)$	$(4 + 8k, 30 - 5k, -6)$	$(5 + 8k, 30 - 5k, -8)$	$(4 + 8k, 31 - 5k, -10)$
$(6 + 8k, 30 - 5k, -12)$	$(8k, 34 - 5k, -15)$	$(2 + 8k, 33 - 5k, -20)$	$(7 + 8k, 30 - 5k, -24)$
$(4 + 8k, 32 - 5k, -30)$	$(1 + 8k, 34 - 5k, -40)$	$(6 + 8k, 31 - 5k, -60)$	$(3 + 8k, 33 - 5k, -120)$
$(5 + 8k, 32 - 5k, 120)$	$(2 + 8k, 34 - 5k, 60)$	$(7 + 8k, 31 - 5k, 40)$	$(4 + 8k, 33 - 5k, 30)$
$(1 + 8k, 35 - 5k, 24)$	$(6 + 8k, 32 - 5k, 20)$	$(8k, 36 - 5k, 15)$	$(2 + 8k, 35 - 5k, 12)$
$(4 + 8k, 34 - 5k, 10)$	$(3 + 8k, 35 - 5k, 8)$	$(4 + 8k, 35 - 5k, 6)$	$(8k, 38 - 5k, 5)$
$(6 + 8k, 35 - 5k, 4)$	$(8k, 40 - 5k, 3)$	$(4 + 8k, 40 - 5k, 2)$	$(8k, 50 - 5k, 1)$

(**b**) It is obvious that $xy \neq 0$. If we multiply the given equation by x we get $1 + \frac{x}{y} = xz$, i.e. $y|x$ (noting that $xz \in \mathbb{Z}$). If we multiply the given equation by y we get $\frac{y}{x} + 1 = yz$, i.e. $x|y$ (noting that $yz \in \mathbb{Z}$). Hence, $y = \pm x$ (see rule 9 of § 1.9). Now, we have two cases:
• $y = -x$ and hence $\frac{1}{x} - \frac{1}{x} = z$, i.e. $(x, y, z) = (k, -k, 0)$ where $k \in \mathbb{Z}$ and $k \neq 0$.
• $y = x$ and hence $\frac{1}{x} + \frac{1}{x} = z$, i.e. $xz = 2 = (-1) \times (-2) = 1 \times 2$. So, we have the following 4 solutions: $(x, y, z) = (-1, -1, -2)$, $(-2, -2, -1)$, $(1, 1, 2)$, $(2, 2, 1)$.
So in brief, we have an infinite number of solutions, i.e. $(x, y, z) = (k, -k, 0)$ plus the 4 other solutions.
(**c**) It is obvious that $yz \neq 0$. Now, if we write the equation as $x = y - \frac{y^2}{z}$ we can see (noting that $x, y \in \mathbb{Z}$) that $z|y^2$. So, the general solution is $(x, y, z) = \left(k - \frac{k^2}{s},\ k,\ s\right)$ where $k, s \in \mathbb{Z}$, $k \neq 0$ and $s|k^2$. This means (in practice) that to build a specific solution (related to a specific k) we choose an integer $k \neq 0$ and then we find all the positive and negative divisors (represented by s) of k^2 and thus we build the solutions corresponding to that k. For example, if $k = 5$ then $s = \pm 1, \pm 5, \pm 25$ and hence we have 6 solutions (x, y, z) corresponding to $k = 5$, i.e.

$(5 - \frac{25}{-1}, 5, -1) = (30, 5, -1)$	$(5 - \frac{25}{-5}, 5, -5) = (10, 5, -5)$	$(5 - \frac{25}{-25}, 5, -25) = (6, 5, -25)$
$(5 - \frac{25}{1}, 5, 1) = (-20, 5, 1)$	$(5 - \frac{25}{5}, 5, 5) = (0, 5, 5)$	$(5 - \frac{25}{25}, 5, 25) = (4, 5, 25)$

7. Find all $x, y, z \in \mathbb{N}$ that satisfy the following equations:
(**a**) $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 4$. (**b**) $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 3$. (**c**) $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 2$. (**d**) $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1$.
Solution:
(**a**) This equation has no solution because $\frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ cannot be greater than 3 (i.e. when $x = y = z = 1$).
(**b**) This equation has only one solution, i.e. $x = y = z = 1$ because if any one of x, y, z is greater than 1 then $\frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ will be less than 3.
(**c**) Let assume that $x \leq y \leq z$ (noting that the given equation is symmetric in the variables x, y, z). Now, x cannot be greater than 1 because in this case $\frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ will be less than 2 for any values of $y, z \in \mathbb{N}$ noting that $x \leq y \leq z$. So, the only possibility is $x = 1$, i.e. $\frac{1}{y} + \frac{1}{z} = 1$.
Now, y cannot be 1 because no (finite) value of z satisfies $\frac{1}{1} + \frac{1}{z} = 1$, i.e. $\frac{1}{z} = 0$. Similarly, y cannot be greater than 2 because in this case $\frac{1}{y} + \frac{1}{z}$ will be less than 1 for any value of $z \in \mathbb{N}$ noting that $y \leq z$. So, the only possibility is $y = 2$.
So, the only possibility is $x = 1$ and $y = 2$ and hence (from the given equation) we get $z = 2$. So, the

only solution (assuming $x \le y \le z$) is $(x, y, z) = (1, 2, 2)$.
However, to get all the possible solutions we must lift the condition $x \le y \le z$ (noting the symmetry in x, y, z) by permuting x, y, z (and hence permuting the values in the above solution). Accordingly, the given equation has 3 solutions: $(x, y, z) = (1, 2, 2)$, $(2, 1, 2)$, $(2, 2, 1)$.
(**d**) Let assume that $x \le y \le z$ (noting that the given equation is symmetric in the variables x, y, z). Now, x cannot be 1 because in this case $\frac{1}{y} + \frac{1}{z} = 0$ which has no solution in $y, z \in \mathbb{N}$. Similarly, x cannot be greater than 3 because in this case $\frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ will be less than 1 for any values of $x, y, z \in \mathbb{N}$ noting that $x \le y \le z$. So, we have only 2 possibilities for x, i.e. $x = 2$ and $x = 3$ (assuming $x \le y \le z$).
• If $x = 2$ then we have $\frac{1}{y} + \frac{1}{z} = \frac{1}{2}$. Now, y cannot be 2 because no (finite) value of z satisfies $\frac{1}{2} + \frac{1}{z} = \frac{1}{2}$, i.e. $\frac{1}{z} = 0$. Similarly, y cannot be greater than 4 because in this case $\frac{1}{y} + \frac{1}{z}$ will be less than $\frac{1}{2}$ for any values of $y, z \in \mathbb{N}$ noting that $y \le z$. So, we have only 2 possibilities for y, i.e. $y = 3$ (and hence $z = 6$) and $y = 4$ (and hence $z = 4$).
• If $x = 3$ then we have $\frac{1}{y} + \frac{1}{z} = \frac{2}{3}$. Now, y cannot be greater than 3 because in this case $\frac{1}{y} + \frac{1}{z}$ will be less than $\frac{2}{3}$ for any values of $y, z \in \mathbb{N}$ noting that $y \le z$. So, we have only 1 possibility for y, i.e. $y = 3$ (and hence $z = 3$).
Accordingly, we found 3 solutions: $(x, y, z) = (2, 3, 6)$, $(2, 4, 4)$, $(3, 3, 3)$. However, to get all the possible solutions we must lift the condition $x \le y \le z$ (noting the symmetry in x, y, z) by permuting x, y, z (and hence permuting the values in the above solutions). Accordingly, the given equation has 10 solutions: $(x, y, z) = (2, 3, 6)$, $(2, 6, 3)$, $(3, 2, 6)$, $(3, 6, 2)$, $(6, 2, 3)$, $(6, 3, 2)$, $(2, 4, 4)$, $(4, 2, 4)$, $(4, 4, 2)$, $(3, 3, 3)$.

4.2 Congruence Diophantine Equations

In § 4.1 we investigated ordinary Diophantine equations, and in this section we will briefly investigate congruence Diophantine equations.[147] In fact, this subject was introduced in § 2.7.5, and hence our investigation here is a continuation of that investigation.

4.2.1 Polynomial Congruence Equations

We present in the Problems of this subsection a small sample of polynomial congruence equations in two and three variables and illustrate how they are solved.

Problems

1. Solve the following multivariate congruence equations (where $x, y, z \in \mathbb{Z}$):

(**a**) $3x - 7y \overset{8}{=} 4$. (**b**) $27x + 18y \overset{19}{=} 3$. (**c**) $3x + 16y - 9z \overset{5}{=} 28$.

(**d**) $4x^2 - 5y \overset{7}{=} 31$. (**e**) $7x^2 - 33y^2 \overset{13}{=} 10$. (**f**) $x^3 - 2y^2 + 35z^2 \overset{3}{=} 1$.

Solution:
(**a**) We have:

$3x(x \overset{8}{=} 0, 1, 2, 3, 4, 5, 6, 7) \overset{8}{=} 0, 3, 6, 1, 4, 7, 2, 5$ and $7y(y \overset{8}{=} 0, 1, 2, 3, 4, 5, 6, 7) \overset{8}{=} 0, 7, 6, 5, 4, 3, 2, 1$

On considering all these 64 combinations (i.e. 8×8) we find that $3x - 7y \overset{8}{=} 4$ for the following eight cases:

$x \overset{8}{=} 0$ and $y \overset{8}{=} 4$ $x \overset{8}{=} 1$ and $y \overset{8}{=} 1$ $x \overset{8}{=} 2$ and $y \overset{8}{=} 6$ $x \overset{8}{=} 3$ and $y \overset{8}{=} 3$

$x \overset{8}{=} 4$ and $y \overset{8}{=} 0$ $x \overset{8}{=} 5$ and $y \overset{8}{=} 5$ $x \overset{8}{=} 6$ and $y \overset{8}{=} 2$ $x \overset{8}{=} 7$ and $y \overset{8}{=} 7$

Hence, the general solutions are (where $k, s \in \mathbb{Z}$):

$(x, y) = (8k, 4 + 8s)$ $(x, y) = (1 + 8k, 1 + 8s)$ $(x, y) = (2 + 8k, 6 + 8s)$ $(x, y) = (3 + 8k, 3 + 8s)$

$(x, y) = (4 + 8k, 8s)$ $(x, y) = (5 + 8k, 5 + 8s)$ $(x, y) = (6 + 8k, 2 + 8s)$ $(x, y) = (7 + 8k, 7 + 8s)$

(**b**) We have:

$27x(x \overset{19}{=} 0, 1, 2 \ldots, 18) \overset{19}{=} 0, 8, 16, 5, 13, 2, 10, 18, 7, 15, 4, 12, 1, 9, 17, 6, 14, 3, 11$ and

[147] "Congruence Diophantine" may sound nonsensical but we use it for clarity and comparison.

$18y(y \overset{19}{=} 0, 1, 2 \ldots, 18) \overset{19}{=} 0, 18, 17, 16, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1$
On considering all these 361 combinations (i.e. 19×19) as we did in part (a) we get the following 19 general solutions (x, y) where $k, s \in \mathbb{Z}$:

$(19k, 16 + 19s)$	$(1 + 19k, 5 + 19s)$	$(2 + 19k, 13 + 19s)$	$(3 + 19k, 2 + 19s)$
$(4 + 19k, 10 + 19s)$	$(5 + 19k, 18 + 19s)$	$(6 + 19k, 7 + 19s)$	$(7 + 19k, 15 + 19s)$
$(8 + 19k, 4 + 19s)$	$(9 + 19k, 12 + 19s)$	$(10 + 19k, 1 + 19s)$	$(11 + 19k, 9 + 19s)$
$(12 + 19k, 17 + 19s)$	$(13 + 19k, 6 + 19s)$	$(14 + 19k, 14 + 19s)$	$(15 + 19k, 3 + 19s)$
$(16 + 19k, 11 + 19s)$	$(17 + 19k, 19s)$	$(18 + 19k, 8 + 19s)$	

(**c**) The given congruence is equivalent to $3x + y + z \overset{5}{=} 3$. Now, we have:

$3x(x \overset{5}{=} 0, 1, 2, 3, 4) \overset{5}{=} 0, 3, 1, 4, 2 \qquad y \overset{5}{=} 0, 1, 2, 3, 4 \qquad z \overset{5}{=} 0, 1, 2, 3, 4$

On considering all these 125 combinations (i.e. $5 \times 5 \times 5$) as we did in parts (a) and (b) we get the following 25 general solutions (x, y, z) noting that for brevity we deleted $(+5k, +5s, +5t)$ from the (x, y, z) components (where $k, s, t \in \mathbb{Z}$):

(0,0,3)	(0,1,2)	(0,2,1)	(0,3,0)	(0,4,4)	(1,0,0)	(1,1,4)	(1,2,3)	(1,3,2)
(1,4,1)	(2,0,2)	(2,1,1)	(2,2,0)	(2,3,4)	(2,4,3)	(3,0,4)	(3,1,3)	(3,2,2)
(3,3,1)	(3,4,0)	(4,0,1)	(4,1,0)	(4,2,4)	(4,3,3)	(4,4,2)		

(**d**) We have $4x^2 - 5y \overset{7}{=} 31 \overset{7}{=} 3$. Now, we have seven cases to consider (where $s \in \mathbb{Z}$):
• $x \overset{7}{=} 0$ and hence $x^2 \overset{7}{=} 0$. Accordingly, $0 - 5y \overset{7}{=} 3$ and hence $y \overset{7}{=} 5$, i.e. $y = 5 + 7s$ where $s \in \mathbb{Z}$.
• $x \overset{7}{=} 1$ and hence $x^2 \overset{7}{=} 1$. Accordingly, $4 - 5y \overset{7}{=} 3$ and hence $y \overset{7}{=} 3$, i.e. $y = 3 + 7s$.
• $x \overset{7}{=} 2$ and hence $x^2 \overset{7}{=} 4$. Accordingly, $16 - 5y \overset{7}{=} 3$ and hence $y \overset{7}{=} 4$, i.e. $y = 4 + 7s$.
• $x \overset{7}{=} 3$ and hence $x^2 \overset{7}{=} 2$. Accordingly, $8 - 5y \overset{7}{=} 3$ and hence $y \overset{7}{=} 1$, i.e. $y = 1 + 7s$.
• $x \overset{7}{=} 4$ and hence $x^2 \overset{7}{=} 2$. Accordingly, $8 - 5y \overset{7}{=} 3$ and hence $y \overset{7}{=} 1$, i.e. $y = 1 + 7s$.
• $x \overset{7}{=} 5$ and hence $x^2 \overset{7}{=} 4$. Accordingly, $16 - 5y \overset{7}{=} 3$ and hence $y \overset{7}{=} 4$, i.e. $y = 4 + 7s$.
• $x \overset{7}{=} 6$ and hence $x^2 \overset{7}{=} 1$. Accordingly, $4 - 5y \overset{7}{=} 3$ and hence $y \overset{7}{=} 3$, i.e. $y = 3 + 7s$.
So overall, the solutions are all pairs (x, y) of the following seven forms (where $k, s \in \mathbb{Z}$):

$(7k,\ 5 + 7s)$	$(1 + 7k,\ 3 + 7s)$	$(2 + 7k,\ 4 + 7s)$	$(3 + 7k,\ 1 + 7s)$
$(4 + 7k,\ 1 + 7s)$	$(5 + 7k,\ 4 + 7s)$	$(6 + 7k,\ 3 + 7s)$	

(**e**) We have $7x^2 \overset{13}{=} 10 + 33y^2$. On multiplying the two sides by the modular multiplicative inverse (mod 13) of 7 (which is 2) we get: $x^2 \overset{13}{=} 20 + 66y^2 \overset{13}{=} 7 + y^2$. Now, we have 13 cases to consider (where $s \in \mathbb{Z}$):
• $x \overset{13}{=} 0$ and hence $x^2 \overset{13}{=} 0$. Accordingly, $7 + y^2 \overset{13}{=} 0$ and hence $y^2 \overset{13}{=} -7 \overset{13}{=} 6$ which has no solution.
• $x \overset{13}{=} 1$ and hence $x^2 \overset{13}{=} 1$. Accordingly, $7 + y^2 \overset{13}{=} 1$ and hence $y^2 \overset{13}{=} -6 \overset{13}{=} 7$ which has no solution.
• $x \overset{13}{=} 2$ and hence $x^2 \overset{13}{=} 4$. Accordingly, $7 + y^2 \overset{13}{=} 4$ and hence $y^2 \overset{13}{=} -3 \overset{13}{=} 10$ which has two solutions: $y = 6 + 13s$ and $y = 7 + 13s$.
If we continue doing this with $x \overset{13}{=} 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$ then we get the following 12 general solutions (where the pairs represent x, y and $k, s \in \mathbb{Z}$):

$(2 + 13k,\ 6 + 13s)$	$(2 + 13k,\ 7 + 13s)$	$(4 + 13k,\ 3 + 13s)$	$(4 + 13k,\ 10 + 13s)$
$(6 + 13k,\ 4 + 13s)$	$(6 + 13k,\ 9 + 13s)$	$(7 + 13k,\ 4 + 13s)$	$(7 + 13k,\ 9 + 13s)$
$(9 + 13k,\ 3 + 13s)$	$(9 + 13k,\ 10 + 13s)$	$(11 + 13k,\ 6 + 13s)$	$(11 + 13k,\ 7 + 13s)$

(**f**) We have $x^3 - 2y^2 + 35z^2 \overset{3}{=} 1$ which is equivalent to $x^3 - 2y^2 + 2z^2 \overset{3}{=} 1$. Now, we have nine cases to consider:
• $x \overset{3}{=} 0$ and $y \overset{3}{=} 0$ and hence $(0)^3 - 2(0)^2 + 2z^2 \overset{3}{=} 1$, i.e. $2z^2 \overset{3}{=} 1$ which has no solution.

• $x \stackrel{3}{=} 0$ and $y \stackrel{3}{=} 1$ and hence $(0)^3 - 2(1)^2 + 2z^2 \stackrel{3}{=} 1$, i.e. $2z^2 \stackrel{3}{=} 3 \stackrel{3}{=} 0$ which has one solution: $z \stackrel{3}{=} 0$.
• $x \stackrel{3}{=} 0$ and $y \stackrel{3}{=} 2$ and hence $(0)^3 - 2(2)^2 + 2z^2 \stackrel{3}{=} 1$, i.e. $2z^2 \stackrel{3}{=} 9 \stackrel{3}{=} 0$ which has one solution: $z \stackrel{3}{=} 0$.
• $x \stackrel{3}{=} 1$ and $y \stackrel{3}{=} 0$ and hence $(1)^3 - 2(0)^2 + 2z^2 \stackrel{3}{=} 1$, i.e. $2z^2 \stackrel{3}{=} 0$ which has one solution: $z \stackrel{3}{=} 0$.
• $x \stackrel{3}{=} 1$ and $y \stackrel{3}{=} 1$ and hence $(1)^3 - 2(1)^2 + 2z^2 \stackrel{3}{=} 1$, i.e. $2z^2 \stackrel{3}{=} 2$ which has two solutions: $z \stackrel{3}{=} 1$ and $z \stackrel{3}{=} 2$.
• $x \stackrel{3}{=} 1$ and $y \stackrel{3}{=} 2$ and hence $(1)^3 - 2(2)^2 + 2z^2 \stackrel{3}{=} 1$, i.e. $2z^2 \stackrel{3}{=} 8 \stackrel{3}{=} 2$ which has two solutions: $z \stackrel{3}{=} 1$ and $z \stackrel{3}{=} 2$.
• $x \stackrel{3}{=} 2$ and $y \stackrel{3}{=} 0$ and hence $(2)^3 - 2(0)^2 + 2z^2 \stackrel{3}{=} 1$, i.e. $2z^2 \stackrel{3}{=} -7 \stackrel{3}{=} 2$ which has two solutions: $z \stackrel{3}{=} 1$ and $z \stackrel{3}{=} 2$.
• $x \stackrel{3}{=} 2$ and $y \stackrel{3}{=} 1$ and hence $(2)^3 - 2(1)^2 + 2z^2 \stackrel{3}{=} 1$, i.e. $2z^2 \stackrel{3}{=} -5 \stackrel{3}{=} 1$ which has no solution.
• $x \stackrel{3}{=} 2$ and $y \stackrel{3}{=} 2$ and hence $(2)^3 - 2(2)^2 + 2z^2 \stackrel{3}{=} 1$, i.e. $2z^2 \stackrel{3}{=} 1$ which has no solution.
So, the solutions are all triples (x, y, z) of the following 9 forms (where $k, s, t \in \mathbb{Z}$):

$(3k, 1+3s, 3t)$	$(3k, 2+3s, 3t)$	$(1+3k, 3s, 3t)$
$(1+3k, 1+3s, 1+3t)$	$(1+3k, 1+3s, 2+3t)$	$(1+3k, 2+3s, 1+3t)$
$(1+3k, 2+3s, 2+3t)$	$(2+3k, 3s, 1+3t)$	$(2+3k, 3s, 2+3t)$

2. Re-solve parts (a, b, c) of the previous Problem using a different approach.
Solution:
(**a**) If $y = k$ $(k \in \mathbb{Z})$ then $3x \stackrel{8}{=} 4 + 7k$. On multiplying the two sides by the modular multiplicative inverse (mod 8) of 3 (which is 3) we get: $x \stackrel{8}{=} 12 + 21k \stackrel{8}{=} 4 + 5k$. So, the solution is $(x, y) = (4 + 5k,\ k)$ where $k \in \mathbb{Z}$.
(**b**) If $y = k$ $(k \in \mathbb{Z})$ then $27x \stackrel{19}{=} 3 - 18k$. On multiplying the two sides by the modular multiplicative inverse (mod 19) of 27 (which is 12) we get: $x \stackrel{19}{=} 36 - 216k \stackrel{19}{=} 17 - 7k$. So, the solution is $(x, y) = (17 - 7k,\ k)$ where $k \in \mathbb{Z}$.
(**c**) If $y = k$ and $z = s$ $(k, s \in \mathbb{Z})$ then $3x \stackrel{5}{=} 28 - 16k + 9s$. On multiplying the two sides by the modular multiplicative inverse (mod 5) of 3 (which is 2) we get: $x \stackrel{5}{=} 56 - 32k + 18s \stackrel{5}{=} 1 - 2k + 3s$. So, the solution is $(x, y, z) = (1 - 2k + 3s,\ k,\ s)$ where $k, s \in \mathbb{Z}$.

4.2.2 Exponential Congruence Equations

We present in the Problems of this subsection a small sample of exponential congruence equations in two and three variables and illustrate how they are solved.

Problems

1. Solve the following congruence equations (where $x, y, z \in \mathbb{N}^0$):

(**a**) $2^x + 3^y \stackrel{5}{=} 1$.	(**b**) $4^x + 5^y \stackrel{8}{=} 2$.	(**c**) $4^x + 7^y \stackrel{6}{=} 5$.
(**d**) $2^x + 3^y + 5^z \stackrel{7}{=} 2$.	(**e**) $4^x + 7^y - 9^z \stackrel{11}{=} 10$.	(**f**) $4^x + 7^y + 9^z \stackrel{5}{=} 0$.

Solution:
(**a**) We have: $2^{x \stackrel{4}{=} 0,1,2,3} \stackrel{5}{=} 1, 2, 4, 3$ and $3^{y \stackrel{4}{=} 0,1,2,3} \stackrel{5}{=} 1, 3, 4, 2$. On considering all these 16 combinations (i.e. 4×4) we find that $2^x + 3^y \stackrel{5}{=} 1$ for the following three cases:

$x \stackrel{4}{=} 1$ and $y \stackrel{4}{=} 2$	$x \stackrel{4}{=} 2$ and $y \stackrel{4}{=} 3$	$x \stackrel{4}{=} 3$ and $y \stackrel{4}{=} 1$

Hence, the general solutions are: $(x, y) = (1+4k, 2+4s),\ (2+4k, 3+4s),\ (3+4k, 1+4s)$ where $k, s \in \mathbb{N}^0$.
(**b**) $4^x + 5^y \stackrel{8}{=} 2$ means $(4^x + 5^y - 2)$ is divisible by 8. However, $(4^x + 5^y - 2)$ is always odd (and hence it cannot be divisible by 8 which is even) except when $x = 0$. Hence, the solutions of the given congruence equation are the same as the solutions of the congruence equation $1 + 5^y \stackrel{8}{=} 2$, i.e. $5^y \stackrel{8}{=} 1$. The solution of the latter congruence is $y \in \mathbb{E}$ (see § 3.2.4). Hence, the general solution is: $(x, y) = (0, 2k)$ where $k \in \mathbb{N}^0$.

(**c**) $4^x + 7^y \overset{6}{=} 5$ is equivalent to $4^x + 1^y \overset{6}{=} 5$, i.e. $4^x \overset{6}{=} 4$. This is obviously untrue for $x = 0$. However, it is true for all $x > 0$ because $4^x \overset{6}{=} 4$ is equivalent to $4^x - 4 \overset{6}{=} 0$ which is always true for $x > 0$.[148] So, $4^x + 7^y \overset{6}{=} 5$ for all $x \in \mathbb{N}$ and $y \in \mathbb{N}^0$.

(**d**) We have:

$2^{x \overset{3}{=} 0,1,2} \overset{7}{=} 1, 2, 4$ $\qquad$ $3^{y \overset{6}{=} 0,1,2,3,4,5} \overset{7}{=} 1, 3, 2, 6, 4, 5$ $\qquad$ $5^{z \overset{6}{=} 0,1,2,3,4,5} \overset{7}{=} 1, 5, 4, 6, 2, 3$

On considering all these 108 combinations (i.e. $3 \times 6 \times 6$) we find that $2^x + 3^y + 5^z \overset{7}{=} 2$ for 16 cases (similar to what we did in part a). Hence, the general solutions (x, y, z) are (where $k, s, t \in \mathbb{N}^0$):

$(3k, 1 + 6s, 1 + 6t)$ $\quad$ $(3k, 2 + 6s, 3 + 6t)$ $\quad$ $(3k, 3 + 6s, 4 + 6t)$ $\quad$ $(3k, 4 + 6s, 2 + 6t)$

$(3k, 5 + 6s, 5 + 6t)$ $\quad$ $(1 + 3k, 6s, 3 + 6t)$ $\quad$ $(1 + 3k, 1 + 6s, 2 + 6t)$ $\quad$ $(1 + 3k, 2 + 6s, 1 + 6t)$

$(1 + 3k, 3 + 6s, 6t)$ $\quad$ $(1 + 3k, 4 + 6s, 5 + 6t)$ $\quad$ $(1 + 3k, 5 + 6s, 4 + 6t)$ $\quad$ $(2 + 3k, 6s, 2 + 6t)$

$(2 + 3k, 1 + 6s, 4 + 6t)$ $\quad$ $(2 + 3k, 2 + 6s, 5 + 6t)$ $\quad$ $(2 + 3k, 3 + 6s, 3 + 6t)$ $\quad$ $(2 + 3k, 4 + 6s, 6t)$

(**e**) We have:

$4^{x \overset{5}{=} 0,1,2,3,4} \overset{11}{=} 1, 4, 5, 9, 3$ $\qquad$ $7^{y \overset{10}{=} 0,1,2,3,4,5,6,7,8,9} \overset{11}{=} 1, 7, 5, 2, 3, 10, 4, 6, 9, 8$ $\qquad$ $9^{z \overset{5}{=} 0,1,2,3,4} \overset{11}{=} 1, 9, 4, 3, 5$

On considering all these 250 combinations (i.e. $5 \times 10 \times 5$) we find that $4^x + 7^y - 9^z \overset{11}{=} 10$ for 23 cases (similar to what we did in the previous parts). Hence, the general solutions (x, y, z) are (where $k, s, t \in \mathbb{N}^0$):

$(5k, 10s, 3 + 5t)$ $\quad$ $(5k, 1 + 10s, 1 + 5t)$ $\quad$ $(5k, 3 + 10s, 2 + 5t)$ $\quad$ $(5k, 4 + 10s, 4 + 5t)$

$(5k, 5 + 10s, 5t)$ $\quad$ $(1 + 5k, 1 + 10s, 5t)$ $\quad$ $(1 + 5k, 5 + 10s, 2 + 5t)$ $\quad$ $(1 + 5k, 6 + 10s, 1 + 5t)$

$(1 + 5k, 8 + 10s, 3 + 5t)$ $\quad$ $(2 + 5k, 4 + 10s, 1 + 5t)$ $\quad$ $(2 + 5k, 5 + 10s, 4 + 5t)$ $\quad$ $(2 + 5k, 7 + 10s, 5t)$

$(2 + 5k, 8 + 10s, 2 + 5t)$ $\quad$ $(2 + 5k, 9 + 10s, 3 + 5t)$ $\quad$ $(3 + 5k, 2 + 10s, 2 + 5t)$ $\quad$ $(3 + 5k, 3 + 10s, 5t)$

$(3 + 5k, 5 + 10s, 1 + 5t)$ $\quad$ $(3 + 5k, 6 + 10s, 3 + 5t)$ $\quad$ $(3 + 5k, 7 + 10s, 4 + 5t)$ $\quad$ $(4 + 5k, 10s, 4 + 5t)$

$(4 + 5k, 2 + 10s, 1 + 5t)$ $\quad$ $(4 + 5k, 5 + 10s, 3 + 5t)$ $\quad$ $(4 + 5k, 9 + 10s, 5t)$

(**f**) $4^x + 7^y + 9^z \overset{5}{=} 0$ is equivalent to $(-1)^x + 2^y + (-1)^z \overset{5}{=} 0$. Now, if we note that $2^{y \overset{4}{=} 0,1,2,3} \overset{5}{=} 1, 2, 4, 3$ then we can easily see that $4^x + 7^y + 9^z \overset{5}{=} 0$ is true only in two cases: x and z are even and $y \overset{4}{=} 3$, and x and z are odd and $y \overset{4}{=} 1$. Hence, the general solutions are: $(x, y, z) = (2k, 3+4s, 2t)$, $(1+2k, 1+4s, 1+2t)$ (where $k, s, t \in \mathbb{N}^0$).

4.2.3 Mixed Polynomial-Exponential Congruence Equations

We present in the Problems of this subsection a small sample of mixed polynomial-exponential congruence equations in two and three variables and illustrate how they are solved.

Problems

1. Solve the following congruence equations (where $x, y, z \in \mathbb{Z}$ and the exponents are ≥ 0):

(**a**) $2^x - 3y^7 \overset{5}{=} 4$. $\qquad$ (**b**) $4^x + 5^y + 2y - 3y^2 \overset{7}{=} 0$. $\qquad$ (**c**) $3^x - 5x^2 + 7y^2 + 6y^3 \overset{8}{=} 2$.

(**d**) $3^x + 9y^4 - 5^z \overset{11}{=} 3$. $\qquad$ (**e**) $6^x + 7^y + 4z \overset{10}{=} 1$. $\qquad$ (**f**) $2x^3 + x^2 - y^5 + 5^z \overset{3}{=} 1$.

Solution:

(**a**) We have: $2^{x \overset{4}{=} 0,1,2,3} \overset{5}{=} 1, 2, 4, 3$ and $3y^7 (y \overset{5}{=} 0, 1, 2, 3, 4) \overset{5}{=} 0, 3, 4, 1, 2$. On considering all these 20 combinations (i.e. 4×5) we find that $2^x - 3y^7 \overset{5}{=} 4$ for the following four cases:

$x \overset{4}{=} 0$ and $y \overset{5}{=} 4$ $\qquad$ $x \overset{4}{=} 1$ and $y \overset{5}{=} 1$ $\qquad$ $x \overset{4}{=} 2$ and $y \overset{5}{=} 0$ $\qquad$ $x \overset{4}{=} 3$ and $y \overset{5}{=} 2$

[148] We prove this by induction as follows: $4^1 - 4 \overset{6}{=} 0$ which is true. Moreover, if we assume $4^k - 4 \overset{6}{=} 0$ for a given $k \in \mathbb{N}$ then $4^{k+1} - 4 = (3)4^k + (4^k - 4) \overset{6}{=} 0$ which is true because $(3)4^k$ is divisible by 6 (since it is divisible by 2 and 3) and $(4^k - 4)$ is divisible by 6 (according to the assumption) and hence their sum is divisible by 6.

Hence, the general solutions are: $(x, y) = (4k, 4 + 5s)$, $(1 + 4k, 1 + 5s)$, $(2 + 4k, 5s)$, $(3 + 4k, 2 + 5s)$ where $k \in \mathbb{N}^0$ and $s \in \mathbb{Z}$.
(**b**) We have:

$4^x \overset{3}{=} 0,1,2 \overset{7}{=} 1, 4, 2$ $\qquad$ $5^y \overset{6}{=} 0,1,2,3,4,5 \overset{7}{=} 1, 5, 4, 6, 2, 3$ $\qquad$ $2y - 3y^2 (y \overset{7}{=} 0, 1, 2, 3, 4, 5, 6) \overset{7}{=} 0, 6, 6, 0, 2, 5, 2$

On considering all these 126 combinations (i.e. $3 \times 6 \times 7$) we find that $4^x + 5^y + 2y - 3y^2 \overset{7}{=} 0$ for the following 18 cases (where $k, s \in \mathbb{N}^0$ and where we solve the 2-congruence system in y by the Chinese remainder theorem):

- $x \overset{3}{=} 0$, $y \overset{6}{=} 0$, $y \overset{7}{=} 5$, i.e. $(x, y) = (3k,\ 12 + 42s)$.
- $x \overset{3}{=} 0$, $y \overset{6}{=} 2$, $y \overset{7}{=} 4$, i.e. $(x, y) = (3k,\ 32 + 42s)$.
- $x \overset{3}{=} 0$, $y \overset{6}{=} 2$, $y \overset{7}{=} 6$, i.e. $(x, y) = (3k,\ 20 + 42s)$.
- $x \overset{3}{=} 0$, $y \overset{6}{=} 3$, $y \overset{7}{=} 0$, i.e. $(x, y) = (3k,\ 21 + 42s)$.
- $x \overset{3}{=} 0$, $y \overset{6}{=} 3$, $y \overset{7}{=} 3$, i.e. $(x, y) = (3k,\ 3 + 42s)$.
- $x \overset{3}{=} 1$, $y \overset{6}{=} 0$, $y \overset{7}{=} 4$, i.e. $(x, y) = (1 + 3k,\ 18 + 42s)$.
- $x \overset{3}{=} 1$, $y \overset{6}{=} 0$, $y \overset{7}{=} 6$, i.e. $(x, y) = (1 + 3k,\ 6 + 42s)$.
- $x \overset{3}{=} 1$, $y \overset{6}{=} 1$, $y \overset{7}{=} 5$, i.e. $(x, y) = (1 + 3k,\ 19 + 42s)$.
- $x \overset{3}{=} 1$, $y \overset{6}{=} 2$, $y \overset{7}{=} 1$, i.e. $(x, y) = (1 + 3k,\ 8 + 42s)$.
- $x \overset{3}{=} 1$, $y \overset{6}{=} 2$, $y \overset{7}{=} 2$, i.e. $(x, y) = (1 + 3k,\ 2 + 42s)$.
- $x \overset{3}{=} 1$, $y \overset{6}{=} 5$, $y \overset{7}{=} 0$, i.e. $(x, y) = (1 + 3k,\ 35 + 42s)$.
- $x \overset{3}{=} 1$, $y \overset{6}{=} 5$, $y \overset{7}{=} 3$, i.e. $(x, y) = (1 + 3k,\ 17 + 42s)$.
- $x \overset{3}{=} 2$, $y \overset{6}{=} 1$, $y \overset{7}{=} 0$, i.e. $(x, y) = (2 + 3k,\ 7 + 42s)$.
- $x \overset{3}{=} 2$, $y \overset{6}{=} 1$, $y \overset{7}{=} 3$, i.e. $(x, y) = (2 + 3k,\ 31 + 42s)$.
- $x \overset{3}{=} 2$, $y \overset{6}{=} 3$, $y \overset{7}{=} 1$, i.e. $(x, y) = (2 + 3k,\ 15 + 42s)$.
- $x \overset{3}{=} 2$, $y \overset{6}{=} 3$, $y \overset{7}{=} 2$, i.e. $(x, y) = (2 + 3k,\ 9 + 42s)$.
- $x \overset{3}{=} 2$, $y \overset{6}{=} 5$, $y \overset{7}{=} 4$, i.e. $(x, y) = (2 + 3k,\ 11 + 42s)$.
- $x \overset{3}{=} 2$, $y \overset{6}{=} 5$, $y \overset{7}{=} 6$, i.e. $(x, y) = (2 + 3k,\ 41 + 42s)$.

(**c**) We have:

$3^x \overset{2}{=} 0,1 \overset{8}{=} 1, 3$ $\qquad$ $5x^2 (x \overset{4}{=} 0, 1, 2, 3) \overset{8}{=} 0, 5, 4, 5$ $\qquad$ $7y^2 + 6y^3 (y \overset{4}{=} 0, 1, 2, 3) \overset{8}{=} 0, 5, 4, 1$

On considering all these 32 combinations (i.e. $2 \times 4 \times 4$) we find that $3^x - 5x^2 + 7y^2 + 6y^3 \overset{8}{=} 2$ for the following 8 cases (where $k \in \mathbb{N}^0$ and $s \in \mathbb{Z}$ and where we solve the 2-congruence system in x by the Chinese remainder theorem):

- $x \overset{2}{=} 0$, $x \overset{4}{=} 0$, $y \overset{4}{=} 1$, i.e. $(x, y) = (4k,\ 1 + 4s)$.
- $x \overset{2}{=} 0$, $x \overset{4}{=} 0$, $y \overset{4}{=} 3$, i.e. $(x, y) = (4k,\ 3 + 4s)$.
- $x \overset{2}{=} 0$, $x \overset{4}{=} 2$, $y \overset{4}{=} 1$, i.e. $(x, y) = (2 + 4k,\ 1 + 4s)$.
- $x \overset{2}{=} 0$, $x \overset{4}{=} 2$, $y \overset{4}{=} 3$, i.e. $(x, y) = (2 + 4k,\ 3 + 4s)$.
- $x \overset{2}{=} 1$, $x \overset{4}{=} 1$, $y \overset{4}{=} 0$, i.e. $(x, y) = (1 + 4k,\ 4s)$.
- $x \overset{2}{=} 1$, $x \overset{4}{=} 1$, $y \overset{4}{=} 2$, i.e. $(x, y) = (1 + 4k,\ 2 + 4s)$.
- $x \overset{2}{=} 1$, $x \overset{4}{=} 3$, $y \overset{4}{=} 0$, i.e. $(x, y) = (3 + 4k,\ 4s)$.
- $x \overset{2}{=} 1$, $x \overset{4}{=} 3$, $y \overset{4}{=} 2$, i.e. $(x, y) = (3 + 4k,\ 2 + 4s)$.

In fact, the first 4 cases mean: "x even and y odd" while the last 4 cases mean: "x odd and y even". So, all these cases can be summarized by: $(x, y) = (2k, 1+2s)$ and $(x, y) = (1+2k, 2s)$ where $k \in \mathbb{N}^0$ and $s \in \mathbb{Z}$. This can be explained in part by the fact that this congruence means 8 divides $(3^x - 5x^2 + 7y^2 + 6y^3 - 2)$ and this cannot happen if $(3^x - 5x^2 + 7y^2 + 6y^3 - 2)$ is odd (since no even can divide an odd). Now, if x and y are of the same parity then $(3^x - 5x^2 + 7y^2 + 6y^3 - 2)$ is odd and hence the given congruence equation cannot be true.

(**d**) We have:

$3^{x \overset{5}{=} 0,1,2,3,4} \overset{11}{=} 1,3,9,5,4$ $\qquad$ $9y^4(y \overset{11}{=} 0,1,2,3,4,5,6,7,8,9,10) \overset{11}{=} 0,9,1,3,5,4,4,5,3,1,9$

$5^{z \overset{5}{=} 0,1,2,3,4} \overset{11}{=} 1,5,3,4,9$

On considering all these 275 combinations (i.e. $5 \times 11 \times 5$) we find that $3^x + 9y^4 - 5^z \overset{11}{=} 3$ for the following 28 cases (where $k, t \in \mathbb{N}^0$ and $s \in \mathbb{Z}$):

- $x \overset{5}{=} 0$, $y \overset{11}{=} 0$, $z \overset{5}{=} 4$, i.e. $(x, y, z) = (5k,\ 11s,\ 4 + 5t)$.
- $x \overset{5}{=} 0$, $y \overset{11}{=} 3$, $z \overset{5}{=} 0$, i.e. $(x, y, z) = (5k,\ 3 + 11s,\ 5t)$.
- $x \overset{5}{=} 0$, $y \overset{11}{=} 4$, $z \overset{5}{=} 2$, i.e. $(x, y, z) = (5k,\ 4 + 11s,\ 2 + 5t)$.
- $x \overset{5}{=} 0$, $y \overset{11}{=} 7$, $z \overset{5}{=} 2$, i.e. $(x, y, z) = (5k,\ 7 + 11s,\ 2 + 5t)$.
- $x \overset{5}{=} 0$, $y \overset{11}{=} 8$, $z \overset{5}{=} 0$, i.e. $(x, y, z) = (5k,\ 8 + 11s,\ 5t)$.
- $x \overset{5}{=} 1$, $y \overset{11}{=} 1$, $z \overset{5}{=} 4$, i.e. $(x, y, z) = (1 + 5k,\ 1 + 11s,\ 4 + 5t)$.
- $x \overset{5}{=} 1$, $y \overset{11}{=} 2$, $z \overset{5}{=} 0$, i.e. $(x, y, z) = (1 + 5k,\ 2 + 11s,\ 5t)$.
- $x \overset{5}{=} 1$, $y \overset{11}{=} 3$, $z \overset{5}{=} 2$, i.e. $(x, y, z) = (1 + 5k,\ 3 + 11s,\ 2 + 5t)$.
- $x \overset{5}{=} 1$, $y \overset{11}{=} 4$, $z \overset{5}{=} 1$, i.e. $(x, y, z) = (1 + 5k,\ 4 + 11s,\ 1 + 5t)$.
- $x \overset{5}{=} 1$, $y \overset{11}{=} 5$, $z \overset{5}{=} 3$, i.e. $(x, y, z) = (1 + 5k,\ 5 + 11s,\ 3 + 5t)$.
- $x \overset{5}{=} 1$, $y \overset{11}{=} 6$, $z \overset{5}{=} 3$, i.e. $(x, y, z) = (1 + 5k,\ 6 + 11s,\ 3 + 5t)$.
- $x \overset{5}{=} 1$, $y \overset{11}{=} 7$, $z \overset{5}{=} 1$, i.e. $(x, y, z) = (1 + 5k,\ 7 + 11s,\ 1 + 5t)$.
- $x \overset{5}{=} 1$, $y \overset{11}{=} 8$, $z \overset{5}{=} 2$, i.e. $(x, y, z) = (1 + 5k,\ 8 + 11s,\ 2 + 5t)$.
- $x \overset{5}{=} 1$, $y \overset{11}{=} 9$, $z \overset{5}{=} 0$, i.e. $(x, y, z) = (1 + 5k,\ 9 + 11s,\ 5t)$.
- $x \overset{5}{=} 1$, $y \overset{11}{=} 10$, $z \overset{5}{=} 4$, i.e. $(x, y, z) = (1 + 5k,\ 10 + 11s,\ 4 + 5t)$.
- $x \overset{5}{=} 2$, $y \overset{11}{=} 1$, $z \overset{5}{=} 3$, i.e. $(x, y, z) = (2 + 5k,\ 1 + 11s,\ 3 + 5t)$.
- $x \overset{5}{=} 2$, $y \overset{11}{=} 3$, $z \overset{5}{=} 4$, i.e. $(x, y, z) = (2 + 5k,\ 3 + 11s,\ 4 + 5t)$.
- $x \overset{5}{=} 2$, $y \overset{11}{=} 8$, $z \overset{5}{=} 4$, i.e. $(x, y, z) = (2 + 5k,\ 8 + 11s,\ 4 + 5t)$.
- $x \overset{5}{=} 2$, $y \overset{11}{=} 10$, $z \overset{5}{=} 3$, i.e. $(x, y, z) = (2 + 5k,\ 10 + 11s,\ 3 + 5t)$.
- $x \overset{5}{=} 3$, $y \overset{11}{=} 2$, $z \overset{5}{=} 2$, i.e. $(x, y, z) = (3 + 5k,\ 2 + 11s,\ 2 + 5t)$.
- $x \overset{5}{=} 3$, $y \overset{11}{=} 3$, $z \overset{5}{=} 1$, i.e. $(x, y, z) = (3 + 5k,\ 3 + 11s,\ 1 + 5t)$.
- $x \overset{5}{=} 3$, $y \overset{11}{=} 8$, $z \overset{5}{=} 1$, i.e. $(x, y, z) = (3 + 5k,\ 8 + 11s,\ 1 + 5t)$.
- $x \overset{5}{=} 3$, $y \overset{11}{=} 9$, $z \overset{5}{=} 2$, i.e. $(x, y, z) = (3 + 5k,\ 9 + 11s,\ 2 + 5t)$.
- $x \overset{5}{=} 4$, $y \overset{11}{=} 0$, $z \overset{5}{=} 0$, i.e. $(x, y, z) = (4 + 5k,\ 11s,\ 5t)$.
- $x \overset{5}{=} 4$, $y \overset{11}{=} 3$, $z \overset{5}{=} 3$, i.e. $(x, y, z) = (4 + 5k,\ 3 + 11s,\ 3 + 5t)$.
- $x \overset{5}{=} 4$, $y \overset{11}{=} 5$, $z \overset{5}{=} 1$, i.e. $(x, y, z) = (4 + 5k,\ 5 + 11s,\ 1 + 5t)$.
- $x \overset{5}{=} 4$, $y \overset{11}{=} 6$, $z \overset{5}{=} 1$, i.e. $(x, y, z) = (4 + 5k,\ 6 + 11s,\ 1 + 5t)$.
- $x \overset{5}{=} 4$, $y \overset{11}{=} 8$, $z \overset{5}{=} 3$, i.e. $(x, y, z) = (4 + 5k,\ 8 + 11s,\ 3 + 5t)$.

(**e**) We have two main cases:

- $x = 0$ and hence $6^0 + 7^y + 4z \overset{10}{=} 1$, i.e. $7^y + 4z \overset{10}{=} 0$. As we see, $(7^y + 4z)$ is odd (for all $y \in \mathbb{N}^0$ and $z \in \mathbb{Z}$) and hence it cannot be divisible by 10 which is even (see the rules of parity in § 1.8). Therefore, there is no solution to the given congruence for $x = 0$.
- $x > 0$ and hence $6^x \overset{10}{=} 6$ (see rule 16 of § 1.8). Accordingly, we have $6 + 7^y + 4z \overset{10}{=} 1$, i.e. $7^y + 4z \overset{10}{=} 5$. Now, we have: $7^{y \overset{4}{=} 0,1,2,3} \overset{10}{=} 1,7,9,3$ and $4z(z \overset{5}{=} 0,1,2,3,4) \overset{10}{=} 0,4,8,2,6$. On considering all these 20 combinations (i.e. 4×5) we find that $7^y + 4z \overset{10}{=} 5$ for the following four cases:

$y \overset{4}{=} 0$ and $z \overset{5}{=} 1$ $\qquad$ $y \overset{4}{=} 1$ and $z \overset{5}{=} 2$ $\qquad$ $y \overset{4}{=} 2$ and $z \overset{5}{=} 4$ $\qquad$ $y \overset{4}{=} 3$ and $z \overset{5}{=} 3$

Hence, the general solutions of $6^x + 7^y + 4z \overset{10}{=} 1$ are: $(x, y, z) = (k, 4s, 1 + 5t)$, $(k, 1 + 4s, 2 + 5t)$,

$(k, 2+4s, 4+5t)$, $(k, 3+4s, 3+5t)$ where $k \in \mathbb{N}$, $s \in \mathbb{N}^0$ and $t \in \mathbb{Z}$.

(**f**) The given congruence equation is equivalent to $2x^3+x^2-y^5+(-1)^z \stackrel{3}{=} 1$. Now, we have two main cases:

• z is even and hence the congruence becomes $2x^3+x^2-y^5+1 \stackrel{3}{=} 1$, i.e. $2x^3+x^2-y^5 \stackrel{3}{=} 0$. The solutions of this congruence (see § 4.2.1) are: $(x,y) = (3k, 3s)$, $(1+3k, 3s)$, $(2+3k, 2+3s)$ where $k, s \in \mathbb{Z}$.

• z is odd and hence the congruence becomes $2x^3+x^2-y^5-1 \stackrel{3}{=} 1$, i.e. $2x^3+x^2-y^5 \stackrel{3}{=} 2$. The solutions of this congruence (see § 4.2.1) are: $(x,y) = (3k, 1+3s)$, $(1+3k, 1+3s)$, $(2+3k, 3s)$ where $k, s \in \mathbb{Z}$.

So, the general solutions of $2x^3+x^2-y^5+5^z \stackrel{3}{=} 1$ are (where $k, s \in \mathbb{Z}$ and $t \in \mathbb{N}^0$):

$(x,y,z) = (3k, 3s, 2t)$ $(x,y,z) = (1+3k, 3s, 2t)$ $(x,y,z) = (2+3k, 2+3s, 2t)$

$(x,y,z) = (3k, 1+3s, 1+2t)$ $(x,y,z) = (1+3k, 1+3s, 1+2t)$ $(x,y,z) = (2+3k, 3s, 1+2t)$

4.2.4 Congruence Equations Involving Roots

We present in the following Problems a few examples of multivariate congruence equations involving roots and illustrate how they are solved.

Problems

1. Solve the following congruence equations (where $x, y \in \mathbb{Z}$):

(**a**) $4\sqrt[3]{x} + 3\sqrt{y} \stackrel{5}{=} 0$. (**b**) $4\sqrt[3]{x} - 3\sqrt{y} \stackrel{5}{=} 0$. (**c**) $\sqrt[3]{x} + \sqrt[5]{y} \stackrel{3}{=} 1$.

(**d**) $3x - 2\sqrt{y} \stackrel{4}{=} 2$. (**e**) $5\sqrt[3]{x} - 6y^2 + 3\sqrt[7]{z} \stackrel{7}{=} 4$.

Solution:

(**a**) $\sqrt[3]{x}$ and $\sqrt{y}$ must be integers and hence $X = \sqrt[3]{x}$ and $Y = \sqrt{y}$ where $X \in \mathbb{Z}$ and $Y \in \mathbb{N}^0$. So, the given congruence is reduced to $4X + 3Y \stackrel{5}{=} 0$ whose solutions (X, Y) are (see § 4.2.1):

$(5k, 5s)$ $(1+5k, 2+5s)$ $(2+5k, 4+5s)$ $(3+5k, 1+5s)$ $(4+5k, 3+5s)$

where $k \in \mathbb{Z}$ and $s \in \mathbb{N}^0$. The solutions of the given congruence equation (i.e. $4\sqrt[3]{x} + 3\sqrt{y} \stackrel{5}{=} 0$) are then given by: $(x,y) = (X^3, Y^2)$ where (X, Y) are given by the above five forms.

(**b**) We repeat our answer to part (a) but with the exception that the solutions (X, Y) of $4X - 3Y \stackrel{5}{=} 0$ are now:

$(5k, 5s)$ $(1+5k, 3+5s)$ $(2+5k, 1+5s)$ $(3+5k, 4+5s)$ $(4+5k, 2+5s)$

(**c**) We have $X + Y \stackrel{3}{=} 1$ (where $X = \sqrt[3]{x}$ and $Y = \sqrt[5]{y}$ with $X, Y \in \mathbb{Z}$) whose solutions are (see § 4.2.1):

$(X,Y) = (3k, 1+3s)$ $(X,Y) = (1+3k, 3s)$ $(X,Y) = (2+3k, 2+3s)$

where $k, s \in \mathbb{Z}$. Hence, the solutions of the given congruence equation are: $(x,y) = (X^3, Y^5)$ where (X, Y) are given by the above three forms.

(**d**) We have $3x - 2Y \stackrel{4}{=} 2$ (where $Y = \sqrt{y}$ with $x \in \mathbb{Z}$ and $y, Y \in \mathbb{N}^0$) whose solutions are (see § 4.2.1):

$(x,Y) = (4k, 1+4s)$ $(x,Y) = (4k, 3+4s)$ $(x,Y) = (2+4k, 4s)$ $(x,Y) = (2+4k, 2+4s)$

where $k \in \mathbb{Z}$ and $s \in \mathbb{N}^0$. Hence, the solutions of the given congruence equation are: $(x,y) = (x, Y^2)$ where (x, Y) are given by the above four forms.

(**e**) We have $5X - 6y^2 + 3Z \stackrel{7}{=} 4$ (where $X = \sqrt[3]{x}$ and $Z = \sqrt[7]{z}$ with $X, y, Z \in \mathbb{Z}$) whose solutions (X, y, Z) are (noting that for brevity we deleted $+7k, +7s, +7t$ from the X, y, Z components where $k, s, t \in \mathbb{Z}$):

(0,0,6) (0,1,1) (0,2,0) (0,3,3) (0,4,3) (0,5,0) (0,6,1) (1,0,2) (1,1,4) (1,2,3)

(1,3,6) (1,4,6) (1,5,3) (1,6,4) (2,0,5) (2,1,0) (2,2,6) (2,3,2) (2,4,2) (2,5,6)

(2,6,0) (3,0,1) (3,1,3) (3,2,2) (3,3,5) (3,4,5) (3,5,2) (3,6,3) (4,0,4) (4,1,6)

(4,2,5) (4,3,1) (4,4,1) (4,5,5) (4,6,6) (5,0,0) (5,1,2) (5,2,1) (5,3,4) (5,4,4)

(5,5,1) (5,6,2) (6,0,3) (6,1,5) (6,2,4) (6,3,0) (6,4,0) (6,5,4) (6,6,5)

Hence, the solutions of the given congruence equation are: $(x, y, z) = (X^3, y, Z^7)$ where (X, y, Z) are given by the above 49 forms.

4.2.5 Congruence Equations Involving Fractions

We present in the Problems of this subsection a few examples of multivariate congruence equations involving fractions and illustrate how they are solved.

Problems

1. Solve the following congruence equations (where $x, y, z \in \mathbb{Z}$):

(**a**) $\frac{14}{x} + \frac{19}{y} \stackrel{5}{=} 0 \quad (xy \neq 0)$. (**b**) $\frac{x}{y} + y \stackrel{2}{=} 0 \quad (y \neq 0)$. (**c**) $\frac{x}{y} + y \stackrel{2}{=} 1 \quad (y \neq 0)$.

(**d**) $\frac{x}{y} + 5z^2 \stackrel{7}{=} 3 \quad (y \neq 0)$. (**e**) $\frac{x}{3} + \frac{y}{4} \stackrel{5}{=} 0$.

Solution:

(**a**) This congruence means 5 divides $\frac{14}{x} + \frac{19}{y}$. Now, the magnitude of $\frac{14}{x} + \frac{19}{y}$ cannot exceed 33 and hence we have only 13 values to consider, i.e. $A \equiv \frac{14}{x} + \frac{19}{y} = 0, \pm 5, \pm 10, \pm 15, \pm 20, \pm 25, \pm 30$.

- $A = -30$, i.e. $19x + 14y + 30xy = 0$ which has no solution.[149]
- $A = -25$, i.e. $19x + 14y + 25xy = 0$ which has no solution.
- $A = -20$, i.e. $19x + 14y + 20xy = 0$ whose solution is: $(x, y) = (-14, -1)$.
- $A = -15$, i.e. $19x + 14y + 15xy = 0$ whose solution is: $(x, y) = (-1, -19)$.
- $A = -10$, i.e. $19x + 14y + 10xy = 0$ whose solution is: $(x, y) = (-28, -2)$.
- $A = -5$, i.e. $19x + 14y + 5xy = 0$ whose solutions are: $(x, y) = (-3, -57), (-56, -4), (1, -1)$.
- $A = 0$, i.e. $19x + 14y = 0$ whose solutions are: $(x, y) = (14k, -19k)$ where $\mathbb{Z} \ni k \neq 0$.
- $A = 5$, i.e. $19x + 14y - 5xy = 0$ whose solutions are: $(x, y) = (3, 57), (56, 4), (-1, 1)$.
- $A = 10$, i.e. $19x + 14y - 10xy = 0$ whose solution is: $(x, y) = (28, 2)$.
- $A = 15$, i.e. $19x + 14y - 15xy = 0$ whose solution is: $(x, y) = (1, 19)$.
- $A = 20$, i.e. $19x + 14y - 20xy = 0$ whose solution is: $(x, y) = (14, 1)$.
- $A = 25$, i.e. $19x + 14y - 25xy = 0$ which has no solution.
- $A = 30$, i.e. $19x + 14y - 30xy = 0$ which has no solution.

(**b**) For this congruence to be true we need two conditions: x/y is an integer and the parity of x/y and y is the same. Now, for x/y to be an integer we should have $x = ky$ ($k \in \mathbb{Z}$). Regarding the parity condition, we have two cases:

- y is odd: for x/y to be odd we need k to be odd (since $x/y = k$). Hence, the solution in this case is: $(x, y) = (ks, s)$ where k and s are odd.
- y is even: for x/y to be even we need k to be even (since $x/y = k$). Hence, the solution in this case is: $(x, y) = (ks, s)$ where k and s are even ($s \neq 0$).

(**c**) If we repeat the analysis of part (b) then we can conclude that the solutions are: $(x, y) = (ks, s)$ where k and s are of opposite parity.

(**d**) x/y must be an integer and hence $x = qy$ ($q \in \mathbb{Z}$). Now, we have 7 cases:

- $z \stackrel{7}{=} 0$ and hence $5z^2 \stackrel{7}{=} 0$. Therefore, we must have: $x/y = q \stackrel{7}{=} 3$, i.e. $q = 3 + 7k$ and hence $x = qy = (3 + 7k)s = 3s + 7ks$ and $y = s$ ($k, s \in \mathbb{Z}$).
- $z \stackrel{7}{=} 1$ and hence $5z^2 \stackrel{7}{=} 5$. Therefore, we must have: $x/y = q \stackrel{7}{=} 5$, i.e. $q = 5 + 7k$ and hence $x = qy = (5 + 7k)s = 5s + 7ks$ and $y = s$.
- $z \stackrel{7}{=} 2$ and hence $5z^2 \stackrel{7}{=} 6$. Therefore, we must have: $x/y = q \stackrel{7}{=} 4$, i.e. $q = 4 + 7k$ and hence $x = qy = (4 + 7k)s = 4s + 7ks$ and $y = s$.
- $z \stackrel{7}{=} 3$ and hence $5z^2 \stackrel{7}{=} 3$. Therefore, we must have: $x/y = q \stackrel{7}{=} 0$, i.e. $q = 7k$ and hence $x = qy = (7k)s = 7ks$ and $y = s$.
- $z \stackrel{7}{=} 4$ and hence $5z^2 \stackrel{7}{=} 3$. Therefore, we must have: $x/y = q \stackrel{7}{=} 0$, i.e. $q = 7k$ and hence $x = qy = (7k)s = 7ks$ and $y = s$.

[149] For investigating the solution of this Diophantine equation and its alike we refer the reader to § 4.1.

• $z \overset{7}{=} 5$ and hence $5z^2 \overset{7}{=} 6$. Therefore, we must have: $x/y = q \overset{7}{=} 4$, i.e. $q = 4 + 7k$ and hence $x = qy = (4 + 7k)s = 4s + 7ks$ and $y = s$.
• $z \overset{7}{=} 6$ and hence $5z^2 \overset{7}{=} 5$. Therefore, we must have: $x/y = q \overset{7}{=} 5$, i.e. $q = 5 + 7k$ and hence $x = qy = (5 + 7k)s = 5s + 7ks$ and $y = s$.
So, the solutions (x, y, z) are (where $k, s, t \in \mathbb{Z}$ and $s \neq 0$):

$(3s + 7ks, s, 7t)$ $(5s + 7ks, s, 1 + 7t)$ $(4s + 7ks, s, 2 + 7t)$ $(7ks, s, 3 + 7t)$

$(7ks, s, 4 + 7t)$ $(4s + 7ks, s, 5 + 7t)$ $(5s + 7ks, s, 6 + 7t)$

(**e**) We have: $\frac{x}{3} + \frac{y}{4} = \frac{4x+3y}{12} \overset{5}{=} 0$. This means that $4x+3y$ is divisible by 12 and 5 and hence $4x+3y \overset{60}{=} 0$ (where this can be obtained from the Chinese remainder theorem or from rule 20 of § 1.9). Now, if $x = 3k$ ($k \in \mathbb{Z}$) then this congruence can be simplified to $4k + y \overset{20}{=} 0$ (see rule 9 of § 2.7) and hence $y \overset{20}{=} -4k$, i.e. $y = 20s - 4k$ ($s \in \mathbb{Z}$). So, the solution of the given congruence equation is: $(x, y) = (3k,\ 20s - 4k)$ where $(k, s \in \mathbb{Z})$.

4.3 Systems of Ordinary Diophantine Equations

Systems of ordinary (as opposite to congruence) Diophantine equations can be solved by the well-known methods of solving systems of equations in $\mathbb{R}$ with the rejection of non-integer solutions (since we are in number theory and dealing with Diophantine equations). So, we refer the reader to the literature (e.g. of linear algebra) about these methods (with a few demonstrating examples investigated in the Problems). These systems may also be solved by using the techniques of number theory (some of which have been investigated earlier and will be demonstrated in the Problems).[150]

Problems

1. Solve the following systems of Diophantine linear equations in the unknowns $m, n, k \in \mathbb{Z}$:

(**a**) $6m + 3n - 12k = 23$ $26m + 9n - 36k = 78$.

(**b**) $12m - 4n - 13k = 73$ $3m + 11n + 8k = 46$ $2m + 5n + k = 36$.

(**c**) $51m + 3n + 33k = -3$ $5m - 2n - 91k = 23$ $16m + n + 10k = 4$.

(**d**) $11m - 12n - 8k = 25$ $8m + 3n + 12k = 44$ $13m - 17n - 10k = 14$.

(**e**) $15m + 10n + 30k = 41$ $22m - 21n + 8k = 5$ $m + 19n - 39k = 73$.

Solution:
(**a**) We have:

$$(26m + 9n - 36k) - 3(6m + 3n - 12k) = 78 - 3(23) \qquad \rightarrow \qquad 8m = 9$$

Hence, there is no (integer) solution.
We may also obtain this result (more easily and directly) by noting that the left hand side of the first equation is 0 (mod 3) while its right hand side is 2 (mod 3) and hence this equation (as well as the system) has no solution (see part b of point 8 of § 2.7.6 as well as the preamble of § 3.3).
(**b**) From the third equation we get $k = 36 - 2m - 5n$. On substituting this into the first and second equations and simplifying we get (respectively):

$$38m + 61n = 541 \qquad \& \qquad 13m + 29n = 242$$

Hence:

$$13(38m + 61n) - 38(13m + 29n) = 13(541) - 38(242) \qquad \rightarrow \qquad n = 7$$

[150] The reader is referred to the preamble of § 3.3 where we explained the two main methods for solving systems of ordinary equations in number theory (as well as other relevant issues).

Thus:

$$\begin{aligned} 38m + 61(7) &= 541 \quad \rightarrow \quad m = 3 \\ k &= 36 - 2(3) - 5(7) = -5 \end{aligned}$$

So, the solution of this system is: $(m, n, k) = (3, 7, -5)$.
(**c**) Solving this system by the familiar methods (as demonstrated in parts a and b), we get: $(m, n, k) = (-3, 72, -2)$.
(**d**) Solving this system by the familiar methods (as demonstrated in parts a and b), we get: $(m, n, k) = (7, 6, -5/2)$. So, there is no solution to this system in $\mathbb{Z}$.
(**e**) Solving this system by the familiar methods, we get no integer solution and hence there is no solution to this system in $\mathbb{Z}$. This result can also be reached (more simply and directly) by noting that the left hand side of the first equation is 0 (mod 5) while its right hand side is 1 (mod 5) and hence this equation (as well as the system) has no solution (see part b of point 8 of § 2.7.6 as well as the preamble of § 3.3).

2. Solve the following systems of Diophantine non-linear equations in the unknowns $m, n \in \mathbb{Z}$:
   (**a**) $16m + 5n^2 = 93 \qquad 7m^2 - 4n = 8.$
   (**b**) $7m^2 + 8n^2 = 351 \qquad 2m^2 - 45n^2 = 53.$

   Solution:
   (**a**) From the second equation we get $n = \frac{7m^2-8}{4}$. On substituting this into the first equation we get:
   $16m + 5\left(\frac{7m^2-8}{4}\right)^2 = 93 \quad \rightarrow \quad 245m^4 - 560m^2 + 256m - 1168 = 0 \quad \rightarrow \quad m = -2, 1.7871$
   So, only $m = -2$ is acceptable and hence $n = \frac{7(-2)^2-8}{4} = 5$. Thus, the solution of this systems is: $(m, n) = (-2, 5)$.
   (**b**) From the second equation we get $m^2 = \frac{45n^2+53}{2}$. On substituting this into the first equation we get:
   $7\left(\frac{45n^2+53}{2}\right) + 8n^2 = 351 \quad \rightarrow \quad n^2 = 1 \quad \rightarrow \quad n = \pm 1$
   Thus, $m^2 = \frac{45(1)+53}{2} = 49$ and hence $m = \pm 7$. So, we have four solutions:
   $(m, n) = (-7, -1) \qquad (m, n) = (-7, 1) \qquad (m, n) = (7, -1) \qquad (m, n) = (7, 1)$

3. Solve the following systems of Diophantine non-linear equations in the unknowns $x, y, z \in \mathbb{Z}$:
   (**a**) $2x - y + 3z = 11 \qquad 4x + xz - y - z = 1.$
   (**b**) $x + 3y - 7z = 22 \qquad 2x - 3xy + z = -31.$
   (**c**) $3x + 17y - 4z^2 = 23 \qquad 14x^2 - 84yx + 231z^3 = 131 \qquad 15x^2 - 3y + z = 33.$
   (**d**) $x + 12y - 9z = -221 \qquad 17x - 29y^2 + z^2 = -384 \qquad 89x + y^2 + z^2 = 438.$
   (**e**) $3x^2 + 72y - 51z = 21 \qquad 5x + 33y + 15z^3 = 48 \qquad 4^x + 5^y - 6^z = 0.$

   Solution:
   (**a**) If we subtract the first equation from the second we get $2x+xz-4z = -10$, that is $(4-x)(z+2) = 18$ and hence:

   $$(4 - x)(z + 2) = 18 = (1)(18) = (-1)(-18) = (2)(9) = (-2)(-9) = (3)(6) = (-3)(-6)$$

   Therefore, we have 12 possibilities:
   - $(4 - x) = 1$ and $(z + 2) = 18$, i.e. $x = 3$ and $z = 16$ and hence (from the given equations) $y = 43$.
   - $(4 - x) = 18$ and $(z + 2) = 1$, i.e. $x = -14$ and $z = -1$ and hence $y = -42$.
   - $(4 - x) = -1$ and $(z + 2) = -18$, i.e. $x = 5$ and $z = -20$ and hence $y = -61$.
   - $(4 - x) = -18$ and $(z + 2) = -1$, i.e. $x = 22$ and $z = -3$ and hence $y = 24$.
   - $(4 - x) = 2$ and $(z + 2) = 9$, i.e. $x = 2$ and $z = 7$ and hence $y = 14$.
   - $(4 - x) = 9$ and $(z + 2) = 2$, i.e. $x = -5$ and $z = 0$ and hence $y = -21$.
   - $(4 - x) = -2$ and $(z + 2) = -9$, i.e. $x = 6$ and $z = -11$ and hence $y = -32$.

• $(4-x)=-9$ and $(z+2)=-2$, i.e. $x=13$ and $z=-4$ and hence $y=3$.
• $(4-x)=3$ and $(z+2)=6$, i.e. $x=1$ and $z=4$ and hence $y=3$.
• $(4-x)=6$ and $(z+2)=3$, i.e. $x=-2$ and $z=1$ and hence $y=-12$.
• $(4-x)=-3$ and $(z+2)=-6$, i.e. $x=7$ and $z=-8$ and hence $y=-21$.
• $(4-x)=-6$ and $(z+2)=-3$, i.e. $x=10$ and $z=-5$ and hence $y=-6$.
So in brief, the given system has these 12 solutions.
(**b**) If we multiply the second equation by 7 and add the two equations side by side we get:
$(x+3y-7z)+7(2x-3xy+z)=22+7(-31) \quad \rightarrow \quad 15x+3y-21xy+195=0 \quad \rightarrow \quad y=\frac{5x+65}{7x-1}$
If we multiply the first equation by x and add the two equations side by side we get:
$x(x+3y-7z)+(2x-3xy+z)=22x-31 \quad \rightarrow \quad x^2-7xz-20x+z+31=0 \quad \rightarrow \quad z=\frac{x^2-20x+31}{7x-1}$
Now:

$$y=\frac{5x+65}{7x-1}=\frac{1}{7}\left(5+\frac{460}{7x-1}\right) \qquad \text{and} \qquad z=\frac{x^2-20x+31}{7x-1}=\frac{1}{49}\left(7x-139+\frac{1380}{7x-1}\right)$$

So, if y and z are to be integers then $(7x-1)$ should be (as a necessary but not sufficient condition) a divisor of 460 (noting that 460|1380). The divisors of 460 are $1,2,4,5,10,20,23,46,92,115,230,460$ and their negatives, and hence $(7x-1)$ should be equal to (some of) these divisors. On equating $(7x-1)$ to these divisors and solving for x we get the following integer values: $x=-13,0,3,33$ which correspond to (using $y=\frac{5x+65}{7x-1}$ and $z=\frac{x^2-20x+31}{7x-1}$): $y=0,-65,4,1$ and $z=-5,-31,-1,2$. So, the solutions of the given system of equations are:
$(x,y,z)=(-13,0,-5) \qquad (x,y,z)=(0,-65,-31) \qquad (x,y,z)=(3,4,-1) \qquad (x,y,z)=(33,1,2)$
(**c**) The left hand side of the second equation is 0 (mod 7) while its right hand side is 5 (mod 7) and hence this equation (as well as the system) has no solution (see part b of point 8 of § 2.7.6 as well as the preamble of § 3.3).
(**d**) From the second and third equations we get:

$$(89x+y^2+z^2)-(17x-29y^2+z^2)=438-(-384) \quad \rightarrow \quad 72x+30y^2=822 \quad \rightarrow \quad 12x+5y^2=137$$

Now:

$$12x+5y^2 \overset{3}{=} 137 \quad \rightarrow \quad 2y^2 \overset{3}{=} 2 \quad \rightarrow \quad y=1+3k \quad \text{and} \quad y=2+3k \quad (k\in\mathbb{Z})$$

$$12x+5y^2 \overset{4}{=} 137 \quad \rightarrow \quad y^2 \overset{4}{=} 1 \quad \rightarrow \quad y=1+4k \quad \text{and} \quad y=3+4k \quad (k\in\mathbb{Z})$$

Now, since $y=y$ then we must have:
• $1+3k=1+4k$ and hence $k=0$ and $y=1$. So, from $12x+5y^2=137$ we get $x=11$ and from the first equation we get $z\simeq 27.11$ which is not acceptable.
• $1+3k=3+4k$ and hence $k=-2$ and $y=-5$. So, from $12x+5y^2=137$ we get $x=1$ and from the first equation we get $z=18$ which is acceptable.
• $2+3k=1+4k$ and hence $k=1$ and $y=5$. So, from $12x+5y^2=137$ we get $x=1$ and from the first equation we get $z\simeq 31.33$ which is not acceptable.
• $2+3k=3+4k$ and hence $k=-1$ and $y=-1$. So, from $12x+5y^2=137$ we get $x=11$ and from the first equation we get $z\simeq 24.44$ which is not acceptable.
So in brief, we have only one solution, i.e. $(x,y,z)=(1,-5,18)$.
(**e**) The equation $4^x+5^y-6^z=0$ has only one solution, i.e. $x=0$ and $y=z=1$ (see part b of Problem 4 of § 4.1.7). So, all we need to do is to check if this solutions satisfies the other two equations. As we see, this solution satisfies the other two equations and hence the solution of this system is $(x,y,z)=(0,1,1)$.

4.4 Systems of Congruence Diophantine Equations

Systems of congruence Diophantine equations are similar to systems of ordinary Diophantine equations (which we investigated in § 4.3) except that congruence, rather than ordinary, equations are used. In fact,

the similarities between the two types of systems is not restricted to their general structure but extend to include other things like their classifications and methods of solution. So, more familiarity with the systems of ordinary Diophantine equations will make the work with congruence Diophantine equations easier and more rewarding (and the reverse is also true).

4.4.1 Systems of Linear Congruence Equations with Single Modulo

Systems of multivariate linear congruence equations with a single modulo can be solved by the ordinary techniques of linear algebra (with some minor adaptations) such as by substitution or matrix inversion. This, in fact, applies literally when the modulo is prime and that is what we will focus on in the following Problems. It is useful to take note of the following remarks:

• As indicated, some caution is needed when dealing with systems of congruence equations since they do not behave exactly like systems of ordinary equations. Some of these issues will be outlined in the following Problems.

• Systems of congruence equations may be solved by solving the equations individually with taking the intersection of their solutions.

Problems

1. Solve the following system of linear congruence equations in the unknowns $m, n \in \mathbb{Z}$:

$$31m + 59n \overset{11}{\equiv} 9 \qquad \text{and} \qquad 7m - 2n \overset{11}{\equiv} 10$$

(**a**) Using the method of substitution.
(**b**) Using the method of matrix inversion.
(**c**) Using the method of solving the individual equations and taking the intersection of their solutions.
(**d**) Using the method of comparison.

Solution:

(**a**) From the first equation we get:

$$31m \overset{11}{\equiv} 9 - 59n \qquad \rightarrow \qquad m \overset{11}{\equiv} 31^{*}(9 - 59n) = 5(9 - 59n) = 45 - 295n \overset{11}{\equiv} 2n + 1 \tag{80}$$

On substituting this in the second equation we get:

$$7(2n + 1) - 2n \overset{11}{\equiv} 10 \qquad \rightarrow \qquad 12n + 7 \overset{11}{\equiv} 10 \qquad \rightarrow \qquad n \overset{11}{\equiv} 3$$

On substituting this into Eq. 80 we get:

$$m \overset{11}{\equiv} 2(3) + 1 = 7$$

Hence, $(m, n) \overset{11}{\equiv} (7, 3)$, i.e. $m = 7 + 11q$ and $n = 3 + 11r$ $(q, r \in \mathbb{Z})$.

(**b**) We have:

$$\begin{bmatrix} 31 & 59 \\ 7 & -2 \end{bmatrix} \begin{bmatrix} m \\ n \end{bmatrix} \overset{11}{\equiv} \begin{bmatrix} 9 \\ 10 \end{bmatrix}$$

that is:

$$\begin{bmatrix} m \\ n \end{bmatrix} \overset{11}{\equiv} \begin{bmatrix} 31 & 59 \\ 7 & -2 \end{bmatrix}^{-1} \begin{bmatrix} 9 \\ 10 \end{bmatrix} = 475^{-1} \begin{bmatrix} 2 & 59 \\ 7 & -31 \end{bmatrix} \begin{bmatrix} 9 \\ 10 \end{bmatrix} \overset{11}{\equiv} 475^{*} \begin{bmatrix} 2 & 59 \\ 7 & -31 \end{bmatrix} \begin{bmatrix} 9 \\ 10 \end{bmatrix}$$

Now, $475^{*} = 6 \pmod{11}$ and hence:

$$\begin{bmatrix} m \\ n \end{bmatrix} \overset{11}{\equiv} 6 \begin{bmatrix} 2 & 59 \\ 7 & -31 \end{bmatrix} \begin{bmatrix} 9 \\ 10 \end{bmatrix} = \begin{bmatrix} 12 & 354 \\ 42 & -186 \end{bmatrix} \begin{bmatrix} 9 \\ 10 \end{bmatrix} = \begin{bmatrix} 3648 \\ -1482 \end{bmatrix} \overset{11}{\equiv} \begin{bmatrix} 7 \\ 3 \end{bmatrix}$$

Hence, $(m, n) \overset{11}{\equiv} (7, 3)$ which is identical to the solution obtained in part (a).

(**c**) The solutions (m, n) of $31m + 59n \overset{11}{\equiv} 9$ are (see § 4.2.1 noting that we delete $+11q, +11r$ for brevity):

(0,5) (1,0) (2,6) (3,1) (4,7) (5,2) (6,8) (7,3) (8,9) (9,4) (10,10)

while the solutions of $7m - 2n \overset{11}{=} 10$ are:

(0,6) (1,4) (2,2) (3,0) (4,9) (5,7) (6,5) (7,3) (8,1) (9,10) (10,8)

As we see, the intersection of their solutions is $(m, n) \overset{11}{=} (7, 3)$ as before.

(**d**) We have $31m + 59n - 9 \overset{11}{=} 0$ and $7m - 2n - 10 \overset{11}{=} 0$ and hence:

$$31m + 59n - 9 \overset{11}{=} 7m - 2n - 10 \quad \rightarrow \quad 24m + 61n + 1 \overset{11}{=} 0 \quad \rightarrow \quad 2m + 6n + 1 \overset{11}{=} 0$$

The solutions (m, n) of the last congruence are (see § 4.2.1 noting that we delete $+11q, +11r$ for brevity):

(0,9) (1,5) (2,1) (3,8) (4,4) (5,0) (6,7) (7,3) (8,10) (9,6) (10,2)

As we see, the solution $(m, n) \overset{11}{=} (7, 3)$ of the system is there but it cannot be identified among other solutions (i.e. of the congruence which is the result of comparison). Yes, it can be identified by substituting these solutions in the given congruence equations where we find that only $(7, 3)$ satisfies these equations.

2. Repeat parts (a) and (b) of Problem 1 for the following system (in the unknowns $m, n, k \in \mathbb{Z}$):

$$5m - 2n - k \overset{5}{=} 1 \quad \text{and} \quad 11m + 4n + 5k \overset{5}{=} 3 \quad \text{and} \quad 2m + 4n - 8k \overset{5}{=} 0$$

Solution:

(**a**) The first two equations can be simplified and solved for k and m as follows:

$$\begin{aligned} -2n - k &\overset{5}{=} 1 \quad \text{and} \quad m + 4n \overset{5}{=} 3 \\ k &\overset{5}{=} -2n - 1 \quad \text{and} \quad m \overset{5}{=} 3 - 4n \end{aligned} \tag{81}$$

Now, if we substitute from these congruences in the third congruence we get:

$$2(3 - 4n) + 4n - 8(-2n - 1) \overset{5}{=} 0 \quad \rightarrow \quad 12n + 14 \overset{5}{=} 0 \quad \rightarrow \quad n \overset{5}{=} 3$$

On substituting this value of n into the congruences of Eq. 81 we get:

$$k \overset{5}{=} -2(3) - 1 = -7 \overset{5}{=} 3 \quad \text{and} \quad m \overset{5}{=} 3 - 4(3) = -9 \overset{5}{=} 1$$

Hence, $(m, n, k) \overset{5}{=} (1, 3, 3)$, i.e. $m = 1 + 5q$, $n = 3 + 5r$ and $k = 3 + 5s$ $(q, r, s \in \mathbb{Z})$.

(**b**) We have:

$$\begin{bmatrix} 5 & -2 & -1 \\ 11 & 4 & 5 \\ 2 & 4 & -8 \end{bmatrix} \begin{bmatrix} m \\ n \\ k \end{bmatrix} \overset{5}{=} \begin{bmatrix} 1 \\ 3 \\ 0 \end{bmatrix}$$

that is:

$$\begin{bmatrix} m \\ n \\ k \end{bmatrix} \overset{5}{=} \begin{bmatrix} 5 & -2 & -1 \\ 11 & 4 & 5 \\ 2 & 4 & -8 \end{bmatrix}^{-1} \begin{bmatrix} 1 \\ 3 \\ 0 \end{bmatrix} = 246^{-1} \begin{bmatrix} 26 & 10 & 3 \\ -49 & 19 & 18 \\ -18 & 12 & -21 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \\ 0 \end{bmatrix}$$

$$\overset{5}{=} 246^{*} \begin{bmatrix} 26 & 10 & 3 \\ -49 & 19 & 18 \\ -18 & 12 & -21 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \\ 0 \end{bmatrix}$$

Now, $246^{*} = 1 \pmod 5$ and hence:

$$\begin{bmatrix} m \\ n \\ k \end{bmatrix} \overset{5}{=} \begin{bmatrix} 26 & 10 & 3 \\ -49 & 19 & 18 \\ -18 & 12 & -21 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \\ 0 \end{bmatrix} = \begin{bmatrix} 56 \\ 8 \\ 18 \end{bmatrix} \overset{5}{=} \begin{bmatrix} 1 \\ 3 \\ 3 \end{bmatrix}$$

Hence, $(m, n, k) \overset{5}{=} (1, 3, 3)$ which is identical to the solution obtained in part (a).

4.4.2 Systems of Non-Linear Congruence Equations

There is no general approach for solving systems of non-linear congruence equations as such. Yes, in principle it should always be possible to solve the individual equations of such systems with taking the intersection of their solutions (noting that such systems have solutions only when all the individual equations have solutions and the intersection of their solutions is not empty).

Chapter 5
Last Digits

In this chapter we investigate the issue of obtaining the last digits of an integer which is usually very long[151] and hence it is impossible or impractical or inconvenient to obtain the number for this purpose. It is important to note that although this issue may be seen to belong to fun and entertainment, it is not so in general. In fact, we do not do this for the sheer fun (although it may be so) but this issue has many theoretical and practical applications. For example, when we have a number consisting of hundreds or thousands (or even millions) of digits, it may be necessary to know its last digits to determine for instance its divisibility or parity or composity.

However, before we start our investigation it is important to take notice of the following points:

• The **power tower** (or **tower of exponents**) of a natural number m of order n (symbolized as $m \uparrow n$) means repeated exponentiation of m n times. For example, $5 \uparrow 3$ means 5^{5^5}. This operation is called **tetration**. It should be obvious that the evaluation of power tower is up-down not down-up, e.g. $5^{5^5} = 5^{(5^5)} = 5^{3125}$ and $5^{5^5} \not\equiv \left(5^5\right)^5 = 3125^5$.

• The **sequence of exponents** of a natural number m of order n [which is usually symbolized as $(((m)^m)^m \ldots)^m$ where we have a single m in the middle (i.e. base) and n exponents m] should not be mistaken as a power tower. In fact, from the rules of indices the sequence of exponents of m of order n is $(((m)^m)^m \ldots)^m = m^{m^n}$. The base of the sequence of exponents may also be different from the exponents, e.g. the sequence of exponents of k to power m of order n is $(((k)^m)^m \ldots)^m = k^{m^n}$.

• We define the **factorial power** of n as:

$$\widehat{n} \equiv n^{(n-1)^{\cdot^{\cdot^{\cdot^{2^1}}}}}$$

For example, $\widehat{4} = 4^{3^{2^1}} = 4^9$. It should be obvious that the evaluation of factorial power is up-down not down-up, e.g. $\widehat{4} = 4^{\left(3^2\right)} = 4^9$ and $\widehat{4} \not\equiv \left(4^3\right)^2 = 64^2$.

• Although this chapter is about obtaining the last digits of large numbers, we will also discuss (but briefly) obtaining the first digits of large numbers (see § 5.2) and obtaining the middle digits of large numbers (see § 5.3).

5.1 Methods for Finding Last Digits

We investigate in the subsections of this section some common methods for dealing with the problems and issues of last digits. As we will see, most of these methods are similar as they are based on similar principles and rationales. So, this division and classification is generally for the purpose of identifying and demonstrating the principles and rationales used in such problems rather than identifying different methods to choose from. As we will see, most of these methods are based explicitly or implicitly on modular arithmetic and the rules of congruence.

5.1.1 Use of Basic General Rules

In this subsection we investigate the use of some basic general rules (which we investigated mostly in § 1.8) to find the last digits of some types of integers where these rules are applicable and can be exploited to find the last digits.

[151] "Very long" is just an example (which possibly is the most common and familiar one) noting that the integer could be represented (for instance) by a symbol or an expression. This also applies to expressions like "large numbers". In brief, last-digit problems (and their alike) are not restricted in their applicability and usability to long integers.

Problems

1. Find the last digit of the following powers:

   (**a**) $5^{6^{100}}$. (**b**) $4^{7^{999}}$. (**c**) 2467231^{7820}. (**d**) $9^{88^{9999}}$. (**e**) 6^{349012}.

   Solution:

   (**a**) By rule 14 of § 1.8 the last digit is 5.

   (**b**) By rule 13 of § 1.8 the last digit is 4 (noting that 7^{999} is odd; see the rules of parity in § 1.8).

   (**c**) By rule 12 of § 1.8 the last digit is 1.

   (**d**) By rule 18 of § 1.8 the last digit is 1 (noting that 88^{9999} is even; see the rules of parity in § 1.8).

   (**e**) By rule 16 of § 1.8 the last digit is 6.

2. What is the last digit of the following:

   (**a**) $5^{534} - 34279^2$. (**b**) $6^{791} - 2341^{42}$. (**c**) $(6^{2711} - 5^{2341})^{934}$. (**d**) $(5372^2 + 7638^2)^4$.

   (**e**) $3^{31} - 2^{284}$. (**f**) $3949^{231} + 6234^{52}$. (**g**) $3949^{231} \times 6234^{52}$.

   Solution:

   (**a**) 5^{534} ends in 5 (rule 14 of § 1.8), and 34279^2 ends in 1 (rule 11 of § 1.8), and hence their difference ends in 4 (noting that $5^{534} > 34279^2$; see rule 20 of § 1.8).

   (**b**) 6^{791} ends in 6 (rule 16 of § 1.8), and 2341^{42} ends in 1 (rule 12 of § 1.8), and hence their difference ends in 5 (see rule 20 of § 1.8).

   (**c**) 6^{2711} ends in 6 (rule 16 of § 1.8), and 5^{2341} ends in 5 (rule 14 of § 1.8), and hence $(6^{2711} - 5^{2341})$ ends in 1 (noting that $6^{2711} > 5^{2341}$; see rule 20 of § 1.8). Thus, $(6^{2711} - 5^{2341})^{934}$ ends in 1 (rule 12 of § 1.8).

   (**d**) 5372^2 ends in 4 (rule 11 of § 1.8), and 7638^2 ends in 4 (rule 11 of § 1.8), and hence (5372^2+7638^2) ends in 8 (rule 19 of § 1.8). Thus, $(5372^2 + 7638^2)^2$ ends in 4 (rule 11 of § 1.8) and hence $(5372^2 + 7638^2)^4 = \left[(5372^2 + 7638^2)^2\right]^2$ ends in 6 (rule 11 of § 1.8).

   (**e**) $3^{31} = 3^{28} \times 3^3 = 9^{14} \times 27$. Now, 9^{14} ends in 1 (rule 18 of § 1.8) and hence $9^{14} \times 27$ ends in 7 (rule 21 of § 1.8), i.e. 3^{31} ends in 7.

   $2^{284} = (2^4)^{71} = 16^{71}$ and hence it ends in 6 (rule 17 of § 1.8).

   Therefore, $(3^{31} - 2^{284})$ ends in 9 (noting that $3^{31} < 2^{284}$; see rule 20 of § 1.8).

   (**f**) $3949^{231} = (3949^2)^{115} \times 3949$. Now, 3949^2 ends in 1 (rule 11 of § 1.8) and hence $(3949^2)^{115}$ ends in 1 (rule 12 of § 1.8). Thus, $(3949^2)^{115} \times 3949$ ends in 9 (rule 21 of § 1.8), i.e. 3949^{231} ends in 9.

   $6234^{52} = (6234^2)^{26}$. Now, 6234^2 ends in 6 (rule 11 of § 1.8) and hence $(6234^2)^{26}$ ends in 6 (rule 17 of § 1.8), i.e. 6234^{52} ends in 6.

   Therefore, $(3949^{231} + 6234^{52})$ ends in 5 (rule 19 of § 1.8).

   (**g**) 3949^{231} ends in 9 and 6234^{52} ends in 6 (see part f). Therefore, $(3949^{231} \times 6234^{52})$ ends in 4 (rule 21 of § 1.8).

3. Find the last digit(s) of the following factorial powers:

   (**a**) Last digit of $\widehat{621}$. (**b**) Last digit of $\widehat{3416}$. (**c**) Last digit of $\widehat{9}$. (**d**) Last 2 digits of $\widehat{235}$.

   Solution:

   (**a**) We have $\widehat{621} = 621^m$ for some $m \in \mathbb{N}$. Hence, by rule 12 of § 1.8 the last digit of $\widehat{621}$ is 1.

   (**b**) We have $\widehat{3416} = 3416^m$ for some $m \in \mathbb{N}$. Hence, by rule 17 of § 1.8 the last digit of $\widehat{3416}$ is 6.

   (**c**) We have $\widehat{9} = 9^{8^m}$ for some $m \in \mathbb{N}$. Now, the power of 9 is 8^m which is even because 8 is even (see rule 6 of § 1.8). Hence, by rule 18 of § 1.8 the last digit of $\widehat{9}$ is 1.

   (**d**) We have $\widehat{235} = 235^{234^m}$ for some $m \in \mathbb{N}$. Now, the power of 235 is 234^m which is even because 234 is even (see rule 6 of § 1.8). Hence, by rule 15 of § 1.8 the last 2 digits of $\widehat{235}$ is 25.

4. Find the following:

   (**a**) The last two digits of 5^n ($\mathbb{N} \ni n > 1$). (**b**) The last three digits of 5^n ($\mathbb{N} \ni n > 2$).

   Solution:

   (**a**) For $n = 2$ and $n = 3$ we have: $5^2 = 25$ and $5^3 = 125$. For $n > 3$ we have:

$$5^n = 5^n - 5^2 + 5^2 = \left[5^2(5^{n-2} - 1)\right] + 5^2 = \left[25(5-1)m\right] + 25 = 100m + 25 \qquad (m \in \mathbb{N})$$

where we used Eq. 12 in step 3. Accordingly, the last two digits of 5^n $(\mathbb{N} \ni n > 1)$ is 25.
(**b**) For $n = 3$ and $n = 4$ we have: $5^3 = 125$ and $5^4 = 625$. For $n > 4$ we have:

$$5^n = 5^n - 5^3 + 5^3 = \big[5^3(5^{n-3} - 1)\big] + 5^3 = \big[125(5-1)m\big] + 125 = 500m + 125 \qquad (m \in \mathbb{N})$$

where we used Eq. 12 in step 3. Now, from Eq. 12 we can see that:
• If n is odd then $(n-3)$ is even and hence m is even (because it is the sum of an even number of odd terms). Accordingly, $500m = 1000\mu$ (where $m = 2\mu$ with $\mu \in \mathbb{N}$) and hence $5^n = 1000\mu + 125$ which means that 5^n ends in 125.
• If n is even then $(n-3)$ is odd and hence m is odd (because it is the sum of an odd number of odd terms). Accordingly, $500m$ ends in 500 which means that $5^n = 500m + 125$ ends in 625.
So in brief, the last three digits of 5^n $(\mathbb{N} \ni n > 2)$ is 125 if n is odd and is 625 if n is even.

5.1.2 Use of Congruence Rules

In this subsection we investigate the use of some rules of congruence (which we investigated in § 2.7) to find the last digits of some types of integers where these rules are applicable and can be exploited to find the last digits. As indicated earlier most of the last digit methods are based on the rules of congruence so the investigation of this subsection is actually about those cases in which only the rules of congruence are used.

Problems

1. Find the following:
(**a**) Last digit of 7^{2961}. (**b**) Last two digits of 11^{3618}. (**c**) Last three digits of 19^{1157}.
Solution: The last n digits of an integer m can be obtained as the residue of $m \div 10^n$ and hence it can be obtained from the congruence of m modulo 10^n.
(**a**) We have $7^4 = 2401 \overset{10}{=} 1$ and hence by rule 11 of § 2.7 we get $\big(7^4\big)^{740} \overset{10}{=} 1$. We also have $7 \overset{10}{=} 7$. On multiplying these two congruences side by side (using rule 10 of § 2.7) we get:

$$\begin{aligned} \big(7^4\big)^{740} \times 7 &\overset{10}{=} 1 \times 7 \\ 7^{2961} &\overset{10}{=} 7 \end{aligned}$$

Hence, the last digit of 7^{2961} is 7.[152]
(**b**) If we follow a similar argument to the argument of part (a) then we have (concisely):

$$11^{10} = 25937424601 \overset{100}{=} 01 = 1 \qquad\qquad 11^{3618} = \big(11^{10}\big)^{361} \times 11^8 \overset{100}{=} 1 \times 11^8 = 214358881$$

Hence, the last two digits of 11^{3618} is 81.
(**c**) We have:

$$\begin{aligned} 19^3 &\overset{1000}{=} 6859 && (19^3 = 6859) \\ 19^3 &\overset{1000}{=} 859 && \\ \big(19^3\big)^5 &\overset{1000}{=} 859^5 && (\text{rule 11 of § 2.7}) \\ \big(19^3\big)^5 &\overset{1000}{=} 299 && (859^5 = 467698329968299) \\ \Big[\big(19^3\big)^5\Big]^7 &\overset{1000}{=} 299^7 && (\text{rule 11 of § 2.7}) \\ \Big[\big(19^3\big)^5\Big]^7 &\overset{1000}{=} 99 && (299^7 = 213647747443112099) \end{aligned}$$

[152] We may also use the basic general rules (as we did in § 5.1.1) by writing: $7^{2961} = \big[(7^2)^2\big]^{740} \times 7$ (where we use rules 11, 12 and 21 of § 1.8).

$$\left\{\left[\left(19^3\right)^5\right]^7\right\}^{11} \overset{1000}{=} 99^{11} \qquad \text{(rule 11 of § 2.7)}$$

$$\left\{\left[\left(19^3\right)^5\right]^7\right\}^{11} \overset{1000}{=} 99 \qquad (99^{11} = 895338254258716445109 9)$$

$$\left\{\left[\left(19^3\right)^5\right]^7\right\}^{11} \times 19^2 \overset{1000}{=} 99 \times 19^2 \qquad \text{(rule 6 of § 2.7)}$$

$$19^{1155} \times 19^2 \overset{1000}{=} 35739 \qquad (99 \times 19^2 = 35739)$$

$$19^{1157} \overset{1000}{=} 739$$

Hence, the last three digits of 19^{1157} is 739.

2. Find the last 10 digits of the series $\sum_{k=1}^{257} 10^k k^{10}$.
Solution: The last n digits of an integer m can be obtained as the residue of $m \div 10^n$ and hence it can be obtained from the congruence of m modulo 10^n. So, we have:

$$\sum_{k=1}^{257} 10^k k^{10} = \sum_{k=1}^{9} 10^k k^{10} + \sum_{k=10}^{257} 10^k k^{10} = \sum_{k=1}^{9} 10^k k^{10} + 10^{10} \sum_{k=10}^{257} 10^{k-10} k^{10} \overset{10^{10}}{=} \sum_{k=1}^{9} 10^k k^{10}$$

Now, $\sum_{k=1}^{9} 10^k k^{10} = 3597044789173411410$ and hence the last 10 digits of the series is: 9173411410.

3. Find the last two digits of $2(6^n - 1)$ where $n \in \mathbb{N}$.
Solution: We have $6^5 \overset{25}{=} 1$ and hence $6^{5k} \overset{25}{=} 1$ where $k \in \mathbb{N}^0$ (noting that the congruence is valid for $k = 0$ and we use rule 11 of § 2.7 for $k > 0$). Now, we have 5 cases to consider:
• $n = 5k+1$ and hence (see rules 6, 9 and 3 of § 2.7):
$6^{5k}3 \overset{25}{=} 3 \quad \rightarrow \quad 6^{5k}12 \overset{100}{=} 12 \quad \rightarrow \quad 6^{5k+1}2 \overset{100}{=} 12 \quad \rightarrow \quad 6^{5k+1}2 - 2 \overset{100}{=} 10 \quad \rightarrow \quad 2(6^{5k+1} - 1) \overset{100}{=} 10$
• $n = 5k+2$ and hence:
$6^{5k}9 \overset{25}{=} 9 \quad \rightarrow \quad 6^{5k}36 \overset{100}{=} 36 \quad \rightarrow \quad 6^{5k+2} \overset{100}{=} 36 \quad \rightarrow \quad 6^{5k+2}2 - 2 \overset{100}{=} 70 \quad \rightarrow \quad 2(6^{5k+2} - 1) \overset{100}{=} 70$
• $n = 5k+3$ and hence:
$6^{5k}54 \overset{25}{=} 54 \quad \rightarrow \quad 6^{5k}216 \overset{100}{=} 216 \quad \rightarrow \quad 6^{5k+3} \overset{100}{=} 16 \quad \rightarrow \quad 6^{5k+3}2 - 2 \overset{100}{=} 30 \quad \rightarrow \quad 2(6^{5k+3} - 1) \overset{100}{=} 30$
• $n = 5k+4$ and hence:
$6^{5k}324 \overset{25}{=} 324 \quad \rightarrow \quad 6^{5k}1296 \overset{100}{=} 1296 \quad \rightarrow \quad 6^{5k+4} \overset{100}{=} 96 \quad \rightarrow \quad 6^{5k+4}2 \overset{100}{=} 92 \quad \rightarrow$
$6^{5k+4}2 - 2 \overset{100}{=} 90 \quad \rightarrow \quad 2(6^{5k+4} - 1) \overset{100}{=} 90$
• $n = 5k+5$ and hence:
$6^{5k}1944 \overset{25}{=} 1944 \quad \rightarrow \quad 6^{5k}7776 \overset{100}{=} 7776 \quad \rightarrow \quad 6^{5k+5} \overset{100}{=} 76 \quad \rightarrow \quad 6^{5k+5}2 \overset{100}{=} 52 \quad \rightarrow$
$6^{5k+5}2 - 2 \overset{100}{=} 50 \quad \rightarrow \quad 2(6^{5k+5} - 1) \overset{100}{=} 50$

So in brief, the last two digits of $2(6^n - 1)$ is 10, 70, 30, 90, 50 corresponding to $n = 5k + 1$, $5k + 2$, $5k + 3$, $5k + 4$, $5k + 5$ (where $k \in \mathbb{N}^0$).

5.1.3 Use of Euler's Theorem

In this subsection we investigate the use of Euler's theorem (see § 2.9.2) to find the last digits of some types of integers where this theorem is applicable. We note that the difference between this subsection and subsection § 5.1.2 is that in § 5.1.2 we use only the rules of congruence while here we use Euler's theorem in association with the rules of congruence (noting that in some examples of § 5.1.2 we could also have used Euler's theorem). So, the two subsections are not very different.

Problems

1. Find the following:
(**a**) Last digit of 23^{341}. (**b**) Last two digits of 77^{358}. (**c**) Last three digits of 127^{805}.

Solution:
(**a**) The last digit d of an integer should be congruent (mod 10) to the integer. We use Euler's theorem (i.e. $m^{\phi(k)} \overset{k}{=} 1$) with $m = 23$ and $k = 10$ (noting that 23 and 10 are coprime), that is:

$$\begin{aligned}
23^{\phi(10)} &\overset{10}{=} 1 && \text{(Euler's theorem)}\\
23^{4} &\overset{10}{=} 1 && \left[\phi(10) = 4\right]\\
\left(23^{4}\right)^{85} &\overset{10}{=} 1^{85} && \text{(rule 11 of § 2.7)}\\
\left(23^{4}\right)^{85} \times 23 &\overset{10}{=} 1 \times 23 && \text{(rule 6 of § 2.7)}\\
23^{341} &\overset{10}{=} 23 && \text{(rules of indices)}\\
23^{341} &\overset{10}{=} 3 && (23 \overset{10}{=} 3)
\end{aligned}$$

Hence, $d = 3$.
(**b**) The last 2 digits dd of an integer should be congruent (mod 100) to the integer. We use Euler's theorem (i.e. $m^{\phi(k)} \overset{k}{=} 1$) with $m = 77$ and $k = 100$ (noting that 77 and 100 are coprime), that is:

$$\begin{aligned}
77^{\phi(100)} &\overset{100}{=} 1 && \text{(Euler's theorem)}\\
77^{40} &\overset{100}{=} 1 && \left[\phi(100) = 40\right]\\
\left(77^{40}\right)^{9} &\overset{100}{=} 1^{9} && \text{(rule 11 of § 2.7)}\\
77^{360} &\overset{100}{=} 1 && \text{(rules of indices)}\\
77^{2} \times 77^{358} &\overset{100}{=} 1 && \text{(rules of indices)}\\
77^{358} &\overset{100}{=} (77^{2})^{*} \times 1 && \text{(multiplicative inverse)}\\
77^{358} &\overset{100}{=} 69 && \left[(77^{2})^{*} = 69 \text{ (mod 100)}\right]
\end{aligned}$$

Hence, $dd = 69$.
(**c**) The last 3 digits ddd of an integer should be congruent (mod 1000) to the integer. We use Euler's theorem (i.e. $m^{\phi(k)} \overset{k}{=} 1$) with $m = 127$ and $k = 1000$ (noting that 127 and 1000 are coprime), that is:

$$\begin{aligned}
127^{\phi(1000)} &\overset{1000}{=} 1 && \text{(Euler's theorem)}\\
127^{400} &\overset{1000}{=} 1 && \left[\phi(1000) = 400\right]\\
\left(127^{400}\right)^{2} &\overset{1000}{=} 1^{2} && \text{(rule 11 of § 2.7)}\\
\left(127^{400}\right)^{2} \times 127^{5} &\overset{1000}{=} 1 \times 127^{5} && \text{(rule 6 of § 2.7)}\\
127^{805} &\overset{1000}{=} 127^{5} && \text{(rules of indices)}\\
127^{805} &\overset{1000}{=} 407 && (127^{5} = 33038369407 \overset{1000}{=} 407)
\end{aligned}$$

Hence, $ddd = 407$.

5.1.4 Use of Power Tower Rules

In this subsection we investigate the use of the rules of power towers when we deal with a last-digit problem of a power tower. We note that the use of the rules of power towers to find last digits is based in part on the congruence rules (which underlie most last-digit methods).

Problems

1. Calculate the following:

(**a**) Last two digits of $3 \uparrow 99$. (**b**) Last two digits of $7 \uparrow 238$. (**c**) Last three digits of $11 \uparrow 59$.

Solution: We draw the attention to the following points which are used in (or related to) the solution:
• The last two (three) digits of a natural number are the residue of the number modulo 100 (1000).
• If $m \overset{\phi(k)}{=} n$ then $s^m \overset{k}{=} s^n$ where k and s are coprime (see rule 12 of § 2.7 and Problem 3 of § 2.9.2).
• $m \uparrow n = m^{m\uparrow(n-1)}$.
• $\phi(1000) = 400$, $\phi(400) = 160$, $\phi(160) = 64$, $\phi(100) = 40$, $\phi(64) = 32$, $\phi(40) = 16$, $\phi(32) = 16$, $\phi(16) = 8$, $\phi(8) = 4$, $\phi(4) = 2$.
• For calculating the residues of very large numbers (e.g. 11^{51}) which we need to do in this solution, we refer the reader to the methods and theorems that facilitate these calculations.[153]

(**a**) We have:

$$\begin{aligned}
3 \uparrow 98 &\overset{\phi(100)}{=} c_1 \quad \rightarrow \quad 3^{3\uparrow 98} \overset{100}{=} 3^{c_1} \\
3 \uparrow 97 &\overset{\phi(40)}{=} c_2 \quad \rightarrow \quad 3^{3\uparrow 97} \overset{40}{=} 3^{c_2} \\
3 \uparrow 96 &\overset{\phi(16)}{=} c_3 \quad \rightarrow \quad 3^{3\uparrow 96} \overset{16}{=} 3^{c_3} \\
3 \uparrow 95 &\overset{\phi(8)}{=} c_4 \quad \rightarrow \quad 3^{3\uparrow 95} \overset{8}{=} 3^{c_4} \\
3 \uparrow 94 &\overset{\phi(4)}{=} c_5 \quad \rightarrow \quad 3^{3\uparrow 94} \overset{4}{=} 3^{c_5} \\
3 \uparrow 93 &\overset{\phi(2)}{=} c_6 \quad \rightarrow \quad 3^{3\uparrow 93} \overset{2}{=} 1 \qquad (3^{3\uparrow 93} \text{ is odd})
\end{aligned}$$

Now, if we work backwards starting from the last equation then we have:

$$\begin{aligned}
3^{3\uparrow 93} &\overset{\phi(4)}{=} 1 \quad \rightarrow \quad 3^{3\uparrow 94} \overset{4}{=} 3^1 \overset{4}{=} 3 \\
3^{3\uparrow 94} &\overset{\phi(8)}{=} 3 \quad \rightarrow \quad 3^{3\uparrow 95} \overset{8}{=} 3^3 \overset{8}{=} 3 \\
3^{3\uparrow 95} &\overset{\phi(16)}{=} 3 \quad \rightarrow \quad 3^{3\uparrow 96} \overset{16}{=} 3^3 \overset{16}{=} 11 \\
3^{3\uparrow 96} &\overset{\phi(40)}{=} 11 \quad \rightarrow \quad 3^{3\uparrow 97} \overset{40}{=} 3^{11} \overset{40}{=} 27 \\
3^{3\uparrow 97} &\overset{\phi(100)}{=} 27 \quad \rightarrow \quad 3^{3\uparrow 98} \overset{100}{=} 3^{27} \overset{100}{=} 87
\end{aligned}$$

So, the last two digits of $3 \uparrow 99 \equiv 3^{3\uparrow 98}$ is 87.

(**b**) We have:

$$\begin{aligned}
7 \uparrow 237 &\overset{\phi(100)}{=} c_1 \quad \rightarrow \quad 7^{7\uparrow 237} \overset{100}{=} 7^{c_1} \\
7 \uparrow 236 &\overset{\phi(40)}{=} c_2 \quad \rightarrow \quad 7^{7\uparrow 236} \overset{40}{=} 7^{c_2} \\
7 \uparrow 235 &\overset{\phi(16)}{=} c_3 \quad \rightarrow \quad 7^{7\uparrow 235} \overset{16}{=} 7^{c_3} \\
7 \uparrow 234 &\overset{\phi(8)}{=} c_4 \quad \rightarrow \quad 7^{7\uparrow 234} \overset{8}{=} 7^{c_4} \\
7 \uparrow 233 &\overset{\phi(4)}{=} c_5 \quad \rightarrow \quad 7^{7\uparrow 233} \overset{4}{=} 7^{c_5} \\
7 \uparrow 232 &\overset{\phi(2)}{=} c_6 \quad \rightarrow \quad 7^{7\uparrow 232} \overset{2}{=} 1 \qquad (7^{7\uparrow 232} \text{ is odd})
\end{aligned}$$

Now, if we work backwards starting from the last equation then we have:

$$\begin{aligned}
7^{7\uparrow 232} &\overset{\phi(4)}{=} 1 \quad \rightarrow \quad 7^{7\uparrow 233} \overset{4}{=} 7^1 \overset{4}{=} 3 \\
7^{7\uparrow 233} &\overset{\phi(8)}{=} 3 \quad \rightarrow \quad 7^{7\uparrow 234} \overset{8}{=} 7^3 \overset{8}{=} 7
\end{aligned}$$

[153] Some of these methods and theorems have been investigated earlier (see for instance § 2.9.2 and § 2.9.3). They are also demonstrated in the Problems of the previous subsections.

$$
\begin{array}{llll}
7^{7\uparrow 234} \overset{\phi(16)}{=} 7 & \rightarrow & 7^{7\uparrow 235} \overset{16}{=} 7^7 \overset{16}{=} 7 \\
7^{7\uparrow 235} \overset{\phi(40)}{=} 7 & \rightarrow & 7^{7\uparrow 236} \overset{40}{=} 7^7 \overset{40}{=} 23 \\
7^{7\uparrow 236} \overset{\phi(100)}{=} 23 & \rightarrow & 7^{7\uparrow 237} \overset{100}{=} 7^{23} \overset{100}{=} 43
\end{array}
$$

So, the last two digits of $7 \uparrow 238 \equiv 7^{7\uparrow 237}$ is 43.
(**c**) We have:

$$
\begin{array}{llll}
11 \uparrow 58 \overset{\phi(1000)}{=} c_1 & \rightarrow & 11^{11\uparrow 58} \overset{1000}{=} 11^{c_1} & \\
11 \uparrow 57 \overset{\phi(400)}{=} c_2 & \rightarrow & 11^{11\uparrow 57} \overset{400}{=} 11^{c_2} & \\
11 \uparrow 56 \overset{\phi(160)}{=} c_3 & \rightarrow & 11^{11\uparrow 56} \overset{160}{=} 11^{c_3} & \\
11 \uparrow 55 \overset{\phi(64)}{=} c_4 & \rightarrow & 11^{11\uparrow 55} \overset{64}{=} 11^{c_4} & \\
11 \uparrow 54 \overset{\phi(32)}{=} c_5 & \rightarrow & 11^{11\uparrow 54} \overset{32}{=} 11^{c_5} & \\
11 \uparrow 53 \overset{\phi(16)}{=} c_6 & \rightarrow & 11^{11\uparrow 53} \overset{16}{=} 11^{c_6} & \\
11 \uparrow 52 \overset{\phi(8)}{=} c_7 & \rightarrow & 11^{11\uparrow 52} \overset{8}{=} 11^{c_7} & \\
11 \uparrow 51 \overset{\phi(4)}{=} c_8 & \rightarrow & 11^{11\uparrow 51} \overset{4}{=} 11^{c_8} & \\
11 \uparrow 50 \overset{\phi(2)}{=} c_9 & \rightarrow & 11^{11\uparrow 50} \overset{2}{=} 1 & (11^{11\uparrow 51} \text{ is odd})
\end{array}
$$

Now, if we work backwards starting from the last equation then we have:

$$
\begin{array}{llll}
11^{11\uparrow 50} \overset{\phi(4)}{=} 1 & \rightarrow & 11^{11\uparrow 51} \overset{4}{=} 11^1 \overset{4}{=} 3 \\
11^{11\uparrow 51} \overset{\phi(8)}{=} 3 & \rightarrow & 11^{11\uparrow 52} \overset{8}{=} 11^3 \overset{8}{=} 3 \\
11^{11\uparrow 52} \overset{\phi(16)}{=} 3 & \rightarrow & 11^{11\uparrow 53} \overset{16}{=} 11^3 \overset{16}{=} 3 \\
11^{11\uparrow 53} \overset{\phi(32)}{=} 3 & \rightarrow & 11^{11\uparrow 54} \overset{32}{=} 11^3 \overset{32}{=} 19 \\
11^{11\uparrow 54} \overset{\phi(64)}{=} 19 & \rightarrow & 11^{11\uparrow 55} \overset{64}{=} 11^{19} \overset{64}{=} 51 \\
11^{11\uparrow 55} \overset{\phi(160)}{=} 51 & \rightarrow & 11^{11\uparrow 56} \overset{160}{=} 11^{51} \overset{160}{=} 51 \\
11^{11\uparrow 56} \overset{\phi(400)}{=} 51 & \rightarrow & 11^{11\uparrow 57} \overset{400}{=} 11^{51} \overset{400}{=} 211 \\
11^{11\uparrow 57} \overset{\phi(1000)}{=} 211 & \rightarrow & 11^{11\uparrow 58} \overset{1000}{=} 11^{211} \overset{1000}{=} 611
\end{array}
$$

So, the last three digits of $11 \uparrow 59 \equiv 11^{11\uparrow 58}$ is 611.
Note: in the above solutions we used unnecessarily lengthy method for the sake of clarity and to demonstrate the rationale behind the method of solution. Otherwise, we can use in parts (a, b) the fact that going down from $\phi(100)$ to $\phi(2)$ includes six steps on the ϕ ladder and hence we can start immediately from $3^{3\uparrow 93} \overset{\phi(4)}{=} 1$ in part (a), and from $7^{7\uparrow 232} \overset{\phi(4)}{=} 1$ in part (b).[154] Similarly, going down from $\phi(1000)$ to $\phi(2)$ includes nine steps on the ϕ ladder and hence we can start immediately from $11^{11\uparrow 50} \overset{\phi(4)}{=} 1$ in part (c).

5.1.5 Use of Chinese Remainder Theorem

The last n digits of a natural number m is equal to (m mod 10^n). Now, $10^n = 2^n \times 5^n$ and hence if we obtain (m mod 2^n) and (m mod 5^n) and combine the results by using the Chinese remainder theorem (see § 2.7.3) then we obtain the last n digits. This method will be illustrated in the following Problems.

Problems

[154] We draw the attention of the reader who may feel confused about these numbers that: $\phi(4) = 2$, $93 = 99 - 6$, and $232 = 238 - 6$.

1. Find the following:
(**a**) Last two digits of 63^{352}. (**b**) Last three digits of 48^{289}. (**c**) Last four digits of 92^{186}.
Solution: We have $n = 2$ and hence $2^n = 2^2 = 4$ and $5^n = 5^2 = 25$. Now:

$$63 \overset{4}{=} 3 \qquad \rightarrow \qquad 63^{352} \overset{4}{=} 3^{352} = \left(3^4\right)^{88} = (81)^{88} \overset{4}{=} 1^{88} = 1$$

Also:

$$63 \overset{25}{=} 13 \qquad \rightarrow \qquad 63^{352} \overset{25}{=} 13^{352} = \left(13^4\right)^{88} \overset{25}{=} (11)^{88} = \left(11^5\right)^{17} (11)^3 \overset{25}{=} (1)^{17} (11)^3 = 11^3 \overset{25}{=} 6$$

This means that we have the following simultaneous congruences:[155]

$$m \overset{4}{=} 1 \qquad \text{and} \qquad m \overset{25}{=} 6$$

which can be solved by the Chinese remainder theorem (see § 2.7.3) to give $m \overset{100}{=} 81$. So, the last two digits of 63^{352} is 81.
(**b**) We have $n = 3$ and hence $2^n = 2^3 = 8$ and $5^n = 5^3 = 125$. Now:

$$48 \overset{8}{=} 0 \qquad \rightarrow \qquad 48^{289} \overset{8}{=} 0$$

Also, $48 \overset{125}{=} 48$ and hence:

$$48^{289} = \left(48^{10}\right)^{28} (48)^9 \overset{125}{=} (24)^{28} (48)^9 = \left(24^7\right)^4 (48)^9 \overset{125}{=} (49)^4 (48)^9 \overset{125}{=} (51)(63) = 3213 \overset{125}{=} 88$$

This means that we have the following simultaneous congruences:

$$m \overset{8}{=} 0 \qquad \text{and} \qquad m \overset{125}{=} 88$$

which can be solved by the Chinese remainder theorem (see § 2.7.3) to give $m \overset{1000}{=} 088$. So, the last three digits of 48^{289} is 088.
(**c**) We have $n = 4$ and hence $2^n = 2^4 = 16$ and $5^n = 5^4 = 625$. Now:

$$92 \overset{16}{=} 12 \qquad \rightarrow \qquad 92^{186} \overset{16}{=} 12^{186} = \left(12^2\right)^{93} \overset{16}{=} (0)^{93} = 0$$

Also, $92 \overset{625}{=} 92$ and hence:

$$92^{186} = \left(92^{10}\right)^{18} (92)^6 \overset{625}{=} (74)^{18} (92)^6 = \left(74^9\right)^2 (92)^6 \overset{625}{=} (49)^2 (92)^6 \overset{625}{=} (526)(94) = 49444 \overset{625}{=} 69$$

This means that we have the following simultaneous congruences:

$$m \overset{16}{=} 0 \qquad \text{and} \qquad m \overset{625}{=} 69$$

which can be solved by the Chinese remainder theorem (see § 2.7.3) to give $m \overset{10000}{=} 6944$. So, the last four digits of 92^{186} is 6944.

5.2 First Digits

Obtaining the first digits of large numbers is generally easier than obtaining their last digits. For example, if we want to obtain the first 10 digits of the number 234^{185} then we simply take the logarithm of 234^{185} to the base 10, that is:

$$\log_{10}(234^{185}) = 185 \log_{10}(234) \simeq 438.304933620876$$

[155] We note that m (which is already mentioned in the preamble) is the natural number represented by 63^{352} (e.g. 4 is the natural number represented by 2^2).

and hence:

$$\begin{aligned} 234^{185} &= 10^{\log_{10}(234^{185})} \simeq 10^{438.304933620876} = 10^{0.304933620876} \times 10^{438} \simeq 2.018057892 \times 10^{438} \\ &= 2018057892 \times 10^{429} \end{aligned}$$

So, the first 10 digits of 234^{185} is 2018057892. However, the calculations should be carried out to high precision (taking sufficient significant figures) to ensure that the rounding errors do not affect the accuracy of the required first digits.

5.3 Middle Digits

There is no general and simple method or procedure for obtaining middle digits (i.e. digits not on the left edge or the right edge of the number) independently, i.e. without obtaining them within an edge block or through obtaining the entire number. For example, if we want to obtain the tenth digit from the right (i.e. the last tenth digit representing the 10^9 place) of the number 234^{185} then the general method for doing this is either by obtaining the last 10 digits of the number or by obtaining the entire number. Both these methods are generally difficult (and could be impossible within the available means and resources), moreover they require unneeded extra work since the edge block and the entire number contain more (unwanted) information than what we need. However, sometimes the task can be eased by the existence of certain conditions or specific information about the number (e.g. about the pattern of the digits in the number) and hence obtaining middle digits independently becomes viable and potentially easy. Some of these special cases will be demonstrated by some examples later on (see the Problems of § 6.15).

Chapter 6
Divisibility

In this chapter we investigate the divisibility of integers which is an essential topic in number theory. In the following sections we study (mainly through solved Problems) a number of categories of divisibility problems and issues focusing mostly on the main and most common ones (and usually at the basic level commensurate with the level of the present volume of this book).

6.1 Divisibility of Numbers by Numbers

The divisibility of numbers by numbers (i.e. integers by integers) is the most basic and elementary divisibility problem in number theory since it *mostly* involves explicit (i.e. not symbolized) numbers and hence it essentially belongs to arithmetic.[156] However, when the numbers are too big their divisibility usually becomes complicated and hence it may require certain techniques to tackle and solve. Nevertheless, in some cases the divisibility can be inferred from simple rules and principles (most of which have been investigated in the previous chapters). So, when we are faced with a divisibility problem of numbers by numbers (and indeed even other categories and types of divisibility problems which will be investigated in the next sections) the first thing we should try (i.e. before setting off for a systematic and general approach to solve the problem) is to inspect the problem for special features to see if it can be solved with essentially no work by just using some general rule or principle or guesswork or something like this. So, in this context it is useful and important to keep in mind the simple divisibility rules (as well as other rules and principles) that we listed and investigated earlier (e.g. in § 1.9 as well as in § 1.8). In the following Problems we will give some examples of these "simple" (or elementary or specific) methods as well as other more general (and usually more complicated) methods.

Problems

1. Show the following:

(**a**) $5|(6^{5633}-3218561^{3289})^{271}$. (**b**) $10|(3567437^{12}-3218569^{8})$. (**c**) $10^{34}|(3561^{623}-45629^{2})^{34}$.

(**d**) $5|(8234506^{8}-6523119^{4})$. (**e**) $10|(456676^{4}+298018^{2})$. (**f**) $5|(6^{397}+4^{325})$.

Solution:

(**a**) 6^{5633} ends in 6 (rule 16 of § 1.8), and 3218561^{3289} ends in 1 (rule 12 of § 1.8), and hence their difference $(6^{5633}-3218561^{3289})$ ends in 5 (rule 20 of § 1.8). So, $(6^{5633}-3218561^{3289})^{271}$ ends in 5 (rule 15 of § 1.8) and hence it is divisible by 5 (rule 27 of § 1.9).

(**b**) $3567437^{12}=\left[(3567437^{2})^{2}\right]^{3}$ ends in 1 (rules 11 and 12 of § 1.8), and $3218569^{8}=(3218569^{2})^{4}$ also ends in 1 (rules 11 and 12 of § 1.8) and hence their difference ends in 0 (rule 20 of § 1.8), i.e. it is divisible by 10 (rule 32 of § 1.9).

(**c**) 3561^{623} ends in 1 (rule 12 of § 1.8), and 45629^{2} ends in 1 (rule 11 of § 1.8), and hence their difference ends in 0 (rule 20 of § 1.8). So, $(3561^{623}-45629^{2})$ is divisible by 10 and hence its 34^{th} power must be divisible by 10^{34} (rule 7 of § 1.6 and rule 48 of § 1.9).

(**d**) 8234506^{8} ends in 6 (rule 17 of § 1.8), and $6523119^{4}=(6523119^{2})^{2}$ ends in 1 (rule 11 of § 1.8) and hence their difference ends in 5 (rule 20 of § 1.8), i.e. it is divisible by 5.

(**e**) 456676^{4} ends in 6 (rule 17 of § 1.8), and 298018^{2} ends in 4 (rule 11 of § 1.8) and hence their sum ends in 0 (rule 19 of § 1.8), i.e. it is divisible by 10.

(**f**) 6^{397} ends in 6 (rule 16 of § 1.8), and 4^{325} ends in 4 (rule 13 of § 1.8) and hence their sum ends in 0 (rule 19 of § 1.8), i.e. it is divisible by 5 (and by 10 as well).

[156] In fact, we include in the Problems of this section some cases of "symbolic numbers" representing certain types of numbers which seem more suitable to be assigned to this section.

2. Is 36389052 divisible by 7?
   Solution: Using rules 29 and 39 of § 1.9 we have:
   $3638905 - (2 \cdot 2) = 3638901$ $363890 - (2 \cdot 1) = 363888$ $36388 - (2 \cdot 8) = 36372$
   $3637 - (2 \cdot 2) = 3633$ $363 - (2 \cdot 3) = 357$ $35 - (2 \cdot 7) = 21$
   Since 21 is divisible by 7 then 36389052 is divisible by 7.
3. Is $(36389051^{32} - 825678921^{65})$ divisible by 10? What about $(45178301^{73} - 74109229^{2})$ and $(478203359^{2} - 5662340129^{2})$?
   Solution: All these numbers are divisible by 10 because by rules 11 and 12 of § 1.8 all the terms in these differences end in 1 and hence their differences must end in 0 (rule 20 of § 1.8), i.e. they are divisible by 10 (by rule 32 of § 1.9).
4. Is 5327094421 divisible by 11?
   Solution: Using rule 33 of § 1.9 we have:
   $$+5 - 3 + 2 - 7 + 0 - 9 + 4 - 4 + 2 - 1 = -11$$
   and hence 5327094421 is divisible by 11 because -11 is divisible by 11.
5. Is 62348179 divisible by 13?
   Solution: Using rules 35 and 39 of § 1.9 we have:
   $6234817 + (4 \cdot 9) = 6234853$ $623485 + (4 \cdot 3) = 623497$ $62349 + (4 \cdot 7) = 62377$
   $6237 + (4 \cdot 7) = 6265$ $626 + (4 \cdot 5) = 646$ $64 + (4 \cdot 6) = 88$
   Since 88 is not divisible by 13 then 62348179 is not divisible by 13.
6. Classify the following as true or false:
   (**a**) $420|116950451520$. (**b**) $12^5|563478924537$. (**c**) $5^8|56231980562502$.
   (**d**) $3|(7231^2 - 6907^2)$. (**e**) $50|(1 + 2 + \cdots + 100)$. (**f**) $11|(643225^7 + 972631^{13})$.
   Solution:
   (**a**) $420 = 3 \times 4 \times 5 \times 7$. So, if 420 divides this number then this number must be divisible by each one of $3, 4, 5, 7$ (see rule 20 of § 1.9). On using the tests of divisibility by $3, 4, 5, 7$ which we stated in § 1.9 we find that this number is divisible by each one of $3, 4, 5, 7$ and hence $420|116950451520$ is true.
   (**b**) This is false because no odd number is divisible by an even number (rule 7 of § 1.8) noting that 12^5 is even (rule 6 of § 1.8).
   (**c**) This is false because for this number to be divisible by 5^8 it must be divisible by 5 (see rule 7 of § 1.9) and this requires this number to end in 0 or 5 (rule 27 of § 1.9).
   (**d**) This is true because $7231^2 - 6907^2 = (7231 - 6907)(7231 + 6907) = 324(7231 + 6907)$ and hence it is divisible by 3 because 324 is divisible by 3 (rules 22 and 25 of § 1.9).
   (**e**) This is true because according to the arithmetic series formula (see Eq. 15) we have:
   $$1 + 2 + \cdots + 100 = \frac{100(1 + 100)}{2} = \mathbf{50} \times 101$$
   (**f**) This is true because both 643225 and 972631 are divisible by 11 (rule 33 of § 1.9) and hence their natural powers are divisible by 11 (rule 6 of § 1.9), and consequently the sum of their natural powers should also be divisible by 11 (rule 14 of § 1.9).
7. Which of the following is correct/incorrect:
   (**a**) $9856056^{15}|646537561488^{34}$. (**b**) $5722751^{49}|253904179^{23}$. (**c**) $184546477125^{11}|3837320375130^{52}$.
   Solution: In this type of problems we use prime factorization to see if the prime factors in the divisor can be canceled by the prime factors in the dividend (to get an integer) or not.
   (**a**) This is correct because:
   $$\frac{646537561488^{34}}{9856056^{15}} = \frac{\left(2^4 \cdot 3^2 \cdot 7^2 \cdot 13^1 \cdot 17^2 \cdot 29^3\right)^{34}}{\left(2^3 \cdot 3^1 \cdot 7^2 \cdot 17^2 \cdot 29^1\right)^{15}} = 2^{91} \cdot 3^{53} \cdot 7^{38} \cdot 13^{34} \cdot 17^{38} \cdot 29^{87}$$

As we see, the quotient is an integer because it is a product of natural powers of integers (or primes; see § 2.1).
(**b**) This is obviously incorrect because the divisor is bigger than the dividend.
(**c**) This is incorrect because:

$$\begin{aligned}\frac{3837320375130^{52}}{18454647712 5^{11}} &= \frac{\left(2^1\cdot 3^2\cdot 5^1\cdot 11^2\cdot 19^2\cdot 23^1\cdot 31^1\cdot 37^2\right)^{52}}{\left(3^2\cdot 5^3\cdot 17^2\cdot 23^2\cdot 29^1\cdot 37^1\right)^{11}}\\ &= \frac{2^{52}\cdot 3^{82}\cdot 5^{19}\cdot 11^{104}\cdot 19^{104}\cdot 23^{30}\cdot 31^{52}\cdot 37^{93}}{17^{22}\cdot 29^{11}}\end{aligned}$$

As we see, the quotient is not an integer because it is not a product of natural powers of integers (or primes) due to the existence of $17^{22}\cdot 29^{11}$ in the denominator which cannot be canceled by corresponding factors in the numerator (see § 2.1).

8. Prove the following:
(**a**) $27|(16^{18}-1)$. (**b**) $55|(82^{40}-1)$. (**c**) $102|(49^{32}-1)$.
Solution: All these are instances of Euler's theorem (see § 2.9.2) noting that:
• $m^{\phi(k)} \overset{k}{=} 1$ is equivalent to $k|(m^{\phi(k)}-1)$.
• $\phi(27)=18$, $\phi(55)=40$, and $\phi(102)=32$.
• The pairs: $(27,16)$, $(55,82)$, and $(102,49)$ are coprime.
9. Prove the following:
(**a**) $11|(15^{10}-1)$. (**b**) $23|(68^{22}-1)$. (**c**) $181|(152^{180}-1)$.
Solution: All these are instances of Fermat's little theorem (see § 2.9.3) noting that:
• $a^{p-1} \overset{p}{=} 1$ is equivalent to $p|(a^{p-1}-1)$.
• $11\not|15$, $23\not|68$, and $181\not|152$.
10. Give an example of 10 natural numbers $m_1, m_2, \ldots, m_{10}$ that form a cycle (i.e. $m_1, m_2, \ldots, m_{10}, m_1$) such that each 3 consecutive numbers in this cycle satisfy the relation $11|(m_{k-1}m_{k+1}-m_k^2)$.
Solution: Any $m_k = n^k$ where $n\in\mathbb{N}$ and $k=1,2,\ldots,10$ should be acceptable because for $1<k<10$ we have:

$$m_{k-1}m_{k+1}-m_k^2 = n^{k-1}\,n^{k+1}-(n^k)^2 = n^{2k}-n^{2k}=0$$

and hence $11|(m_{k-1}m_{k+1}-m_k^2)$ because $11|0$.
Also:

$$m_9m_1-m_{10}^2 = n^9\,n^1-(n^{10})^2 = n^{10}-n^{20}=n^{10}(1-n^{10})$$

and hence $11|(m_9m_1-m_{10}^2)$ because if $11|n$ then $11|n^{10}$ and hence $11|(m_9m_1-m_{10}^2)$ while if $11\not|n$ then $11|(1-n^{10})$ according to Fermat's little theorem (see § 2.9.3) and hence $11|(m_9m_1-m_{10}^2)$.
11. Prove the following:
(**a**) $15|(31^{21}+29^{69})$. (**b**) $12|(25^{53}+47^{81})$. (**c**) $131|(86^{34}+51^{28}-102^{43})$. (**d**) $73|(67^{82}-91^{43})$.
Solution:
(**a**) $15|(31^{21}+29^{69})$ is equivalent to $(31^{21}+29^{69}) \overset{15}{=} 0$. Now, $31^{21} \overset{15}{=} 1$ and $29^{69} \overset{15}{=} -1$ and hence:[157]

$$31^{21}+29^{69} \overset{15}{=} 1-1=0$$

(**b**) $12|(25^{53}+47^{81})$ is equivalent to $(25^{53}+47^{81}) \overset{12}{=} 0$. Now, $25^{53} \overset{12}{=} 1^{53}=1$ and $47^{81} \overset{12}{=} (-1)^{81}=-1$ and hence:

$$(25^{53}+47^{81}) \overset{12}{=} 1-1=0$$

(**c**) $131|(86^{34}+51^{28}-102^{43})$ is equivalent to $(86^{34}+51^{28}-102^{43}) \overset{131}{=} 0$. Now, $86^{34} \overset{131}{=} 39$, $51^{28} \overset{131}{=} 112$ and $102^{43} \overset{131}{=} 20$ and hence:

$$86^{34}+51^{28}-102^{43} \overset{131}{=} 39+112-20=131 \overset{131}{=} 0$$

[157] The methods for getting these congruences were investigated previously. For example, $31 \overset{15}{=} 1$ and hence $31^{21} \overset{15}{=} 1^{21}=1$. Similarly, $29 \overset{15}{=} -1$ and hence $29^{69} \overset{15}{=} (-1)^{69}=-1$.

(**d**) $73|(67^{82}-91^{43})$ is equivalent to $(67^{82}-91^{43}) \overset{73}{=} 0$. Now, $67^{82} \overset{73}{=} 57$ and $91^{43} \overset{73}{=} 57$ and hence:

$$67^{82}-91^{43} \overset{73}{=} 57-57=0$$

12. Show that if $m^2 \overset{p}{=} n^2$ (where p is prime) then p divides $(m-n)$ or $(m+n)$.
Solution: We have $m^2 \overset{p}{=} n^2$ and hence $m^2-n^2 \overset{p}{=} 0$ which means that p divides (m^2-n^2). Now, $m^2-n^2=(m-n)(m+n)$ and hence p must divide $(m-n)$ or $(m+n)$ (see rule 22 of § 1.9).
13. Show that $(n+1)^n-1$ is divisible by n^2 (where $n \in \mathbb{N}$).
Solution: For $n=1$ we have $(1+1)^1-1=1$ which is divisible by $1^2=1$. For $n>1$ we have:

$$\begin{aligned}(n+1)^n-1 &= \left(\sum_{k=0}^{n} C_k^n n^k\right)-1 && \text{(Eq. 13)}\\ &= \sum_{k=1}^{n} C_k^n n^k && (C_0^n n^0=1)\end{aligned}$$

Now, for $k=1$ we have $C_1^n n^1=n^2$, while for $2 \le k \le n$ the expression $C_k^n n^k$ must contain a factor of n^2 (noting that C_k^n is an integer; see rule 26 of § 1.8). Therefore, each term of the sum in the last equation contains a factor of n^2. Thus, $(n+1)^n-1$ (which is equal to this sum) should be divisible by n^2 (rule 14 of § 1.9).
14. Show that if $\gcd(m,259)=\gcd(n,259)$ then $259|(m^{36}-n^{36})$.
Solution: We note first that $259=7\times 37$.
Since $\gcd(m,259)=\gcd(n,259)$ then $\gcd(m,7)=\gcd(n,7)$ (see Problem 18 of § 2.4). Now, if $\gcd(m,7)=\gcd(n,7)=1$ then by Fermat's little theorem (see § 2.9.3) we have $m^6 \overset{7}{=} 1 \overset{7}{=} n^6$ and hence by raising to power 6 (see rule 11 of § 2.7) we get $m^{36} \overset{7}{=} 1 \overset{7}{=} n^{36}$, i.e. $m^{36}-n^{36} \overset{7}{=} 0$ which means $7|(m^{36}-n^{36})$. On the other hand, if $\gcd(m,7)=\gcd(n,7)=7$ then 7 divides both m and n and hence it should divide both m^{36} and n^{36} (see rule 6 of § 1.9) and thus it should divide their difference (see rule 14 of § 1.9), i.e. $7|(m^{36}-n^{36})$.
Also, since $\gcd(m,259)=\gcd(n,259)$ then $\gcd(m,37)=\gcd(n,37)$. Now, if $\gcd(m,37)=\gcd(n,37)=1$ then by Fermat's little theorem we have $m^{36} \overset{37}{=} 1 \overset{37}{=} n^{36}$, i.e. $37|(m^{36}-n^{36})$. On the other hand, if $\gcd(m,37)=\gcd(n,37)=37$ then 37 divides both m and n and hence it should divide both m^{36} and n^{36} and thus it should divide their difference, i.e. $37|(m^{36}-n^{36})$.
This means that in all possible cases we have $7|(m^{36}-n^{36})$ and $37|(m^{36}-n^{36})$ and hence $(m^{36}-n^{36})$ should be divisible by their product 259 (see rule 20 of § 1.9), i.e. $259|(m^{36}-n^{36})$.
15. Show that if p is prime then p divides both $\left[(p-1)^{p-1}-1\right]$ and $\left[(p+1)^{p-1}-1\right]$.
Solution: It is obvious that $p \nmid (p-1)$ and $p \nmid (p+1)$ (see part h of Problem 1 of § 2.2). Hence, by Fermat's little theorem (see § 2.9.3) we have:

$$(p-1)^{p-1} \overset{p}{=} 1 \quad \rightarrow \quad (p-1)^{p-1}-1 \overset{p}{=} 0 \qquad \text{and} \qquad (p+1)^{p-1} \overset{p}{=} 1 \quad \rightarrow \quad (p+1)^{p-1}-1 \overset{p}{=} 0$$

i.e. p divides $\left[(p-1)^{p-1}-1\right]$ and p divides $\left[(p+1)^{p-1}-1\right]$.
16. Show that if p is prime then p divides both $\left[(p-1)^{mp-m}-1\right]$ and $\left[(p+1)^{mp-m}-1\right]$ where $m \in \mathbb{N}$.
Solution: From Problem 15 we have $(p-1)^{p-1} \overset{p}{=} 1$ and $(p+1)^{p-1} \overset{p}{=} 1$. Now, if we raise both sides of these congruence equations to m (see rule 11 of § 2.7) then we get $(p-1)^{mp-m} \overset{p}{=} 1$ and $(p+1)^{mp-m} \overset{p}{=} 1$, i.e. p divides $\left[(p-1)^{mp-m}-1\right]$ and p divides $\left[(p+1)^{mp-m}-1\right]$.

6.2 Divisibility of Polynomials by Numbers

In this type of problems we mostly exploit the rules of divisibility of integers and the rules of parity as well as other general divisibility-related rules (see § 1.8 and § 1.9). We may also need to employ certain methods of proof and general arguments (like mathematical induction) to establish certain divisibility rules for specific types of polynomial. These issues will be clarified and illustrated in the following Problems.

Problems

1. Use rule 44 of § 1.9 to form polynomial expressions in $n \in \mathbb{Z}$ which are always divisible by $2, 3, 4, 5$.
   Solution: For example:
   • $(n-1)n = n^2 - n$ is always divisible by 2.
   • $n(n+1) = n^2 + n$ is always divisible by 2.
   • $(n-1)n(n+1) = n^3 - n$ is always divisible by 3.
   • $n(n+1)(n+2) = n^3 + 3n^2 + 2n$ is always divisible by 3.
   • $(n-1)n(n+1)(n+2) = n^4 + 2n^3 - n^2 - 2n$ is always divisible by 4.
   • $n(n+1)(n+2)(n+3) = n^4 + 6n^3 + 11n^2 + 6n$ is always divisible by 4.
   • $(n-2)(n-1)n(n+1)(n+2) = n^5 - 5n^3 + 4n$ is always divisible by 5.
2. Which of the following polynomial expressions are divisible by 2 (where $n \in \mathbb{Z}$):
   (**a**) $n^3 - n$. (**b**) $n^4 + n$. (**c**) $n^5 - n^3 + 1$. (**d**) $n^2 + n + 2$.
   (**e**) $3n^3 + 2n^2 - 7$. (**f**) $n^6 + 5n^3 + n$. (**g**) $5n^{11} + n - 7^7$. (**h**) $n^2 - 19^2$.
   Solution: We use rules 4 and 6 of § 1.8 to determine if they are even (i.e. divisible by 2) or odd (i.e. not divisible by 2).
   (**a**) It is even for both n odd and n even. So, it is divisible by 2 unconditionally.
   (**b**) It is even for both n odd and n even. So, it is divisible by 2 unconditionally.
   (**c**) It is odd for both n odd and n even. So, it is non-divisible by 2 unconditionally.
   (**d**) It is even for both n odd and n even. So, it is divisible by 2 unconditionally.
   (**e**) It is even only for n odd. So, it is divisible by 2 only for n odd.
   (**f**) It is even only for n even. So, it is divisible by 2 only for n even.
   (**g**) It is odd for both n odd and n even. So, it is non-divisible by 2 unconditionally.
   (**h**) It is even only for n odd. So, it is divisible by 2 only for n odd.
3. Prove that the following polynomial expressions are divisible by 3 (where $n \in \mathbb{Z}$):
   (**a**) $n^3 - n$. (**b**) $n^3 + 2n$. (**c**) $n^3 + 3n^2 + 5n + 3$. (**d**) $n^4 - n^2$.
   Solution:
   (**a**) This was established in Problem 1.
   (**b**) We have:
   $$n^3 + 2n = (n^3 - n) + 3n$$
   Now, $(n^3 - n)$ is divisible by 3 (according to part a) and $3n$ is obviously divisible by 3 and hence (by rule 14 of § 1.9) $n^3 + 2n$ is divisible by 3.
   (**c**) We have:
   $$n^3 + 3n^2 + 5n + 3 = (n^3 + 3n^2 + 3n + 1) + (2n + 2) = (n+1)^3 + 2(n+1)$$
   which is divisible by 3 according to part (b).
   (**d**) $n^4 - n^2 = n(n^3 - n)$. Now, since $(n^3 - n)$ is divisible by 3 (according to part a), $(n^4 - n^2)$ must be divisible by 3 (see rule 18 of § 1.9).
4. Prove that the following polynomial expressions are divisible by 4 (where $n \in \mathbb{Z}$):
   (**a**) $n^4 - n^2$. (**b**) $n^4 + 3n^2$. (**c**) $n^4 + 2n^3 - n^2 - 2n$. (**d**) $2n^2 \pm 2n$.
   Solution:
   (**a**) We have $n^4 - n^2 = (n^2 - n)(n^2 + n)$. Now, both $(n^2 - n)$ and $(n^2 + n)$ are even (see rules 4 and 6 of § 1.8 or see Problem 1) and hence their product must be divisible by 4 (since each should contain a factor of 2).
   (**b**) We have $n^4 + 3n^2 = (n^4 - n^2) + 4n^2$. Now, $(n^4 - n^2)$ is divisible by 4 (from part a) as well as $4n^2$ and hence $(n^4 + 3n^2)$ is divisible by 4 (see rule 14 of § 1.9).
   (**c**) We have $n^4 + 2n^3 - n^2 - 2n = (n^4 - n^2) + 2(n^3 - n)$. Now, $(n^4 - n^2)$ is divisible by 4 (from part a) as well as $2(n^3 - n)$ $\big[$because $(n^3 - n)$ is even$\big]$ and hence $(n^4 + 2n^3 - n^2 - 2n)$ is divisible by 4 (see rule 14 of § 1.9).

(**d**) We have $2n^2 \pm 2n = 2(n^2 \pm n)$. Now, $(n^2 \pm n)$ is even (see rules 4 and 6 of § 1.8) and hence $(2n^2 \pm 2n)$ is divisible by 4 (since it contains explicit and implicit factors of 2).

5. Prove that the following polynomial expressions are divisible by 5 (where $n \in \mathbb{Z}$):

(**a**) $n^5 - n$. (**b**) $n^5 + 10n^4 + 35n^3 + 50n^2 + 24n$. (**c**) $n^9 - n$.

Solution:

(**a**) The divisibility of $(n^5 - n)$ by 5 is equivalent to the congruence equation $n^5 - n \stackrel{5}{=} 0$. Considering this with $n = 0, 1, 2, 3, 4$ (which are the residues of modulo 5) we have:

$0^5 - 0 \stackrel{5}{=} 0$ $1^5 - 1 \stackrel{5}{=} 0$ $2^5 - 2 \stackrel{5}{=} 0$ $3^5 - 3 \stackrel{5}{=} 0$ $4^5 - 4 \stackrel{5}{=} 0$

As we see, $(n^5 - n)$ is congruent to 0 (mod 5) in all cases and hence it is divisible by 5.
We may also use one of the results of Problem 1, that is:

$$n^5 - n = (n^5 - 5n^3 + 4n) + (5n^3 - 5n) = (n^5 - 5n^3 + 4n) + 5(n^3 - n)$$

As we see, both terms in the last equality are divisible by 5 and so is their sum (see rule 14 of § 1.9).
(**b**) We have:

$$n^5 + 10n^4 + 35n^3 + 50n^2 + 24n = (n^5 - n) + 5(2n^4 + 7n^3 + 10n^2 + 5n)$$

As we see, both terms in the last equality are divisible by 5 (see part a) and so is their sum.

(**c**) The divisibility of $(n^9 - n)$ by 5 is equivalent to the congruence equation $n^9 - n \stackrel{5}{=} 0$. Considering this with $n = 0, 1, 2, 3, 4$ (which are the residues of modulo 5) we have:

$0^9 - 0 \stackrel{5}{=} 0$ $1^9 - 1 \stackrel{5}{=} 0$ $2^9 - 2 \stackrel{5}{=} 0$ $3^9 - 3 \stackrel{5}{=} 0$ $4^9 - 4 \stackrel{5}{=} 0$

As we see, $(n^9 - n)$ is congruent to 0 (mod 5) in all cases and hence it is divisible by 5.

6. Prove that the following polynomial expressions are divisible by 6 (where $n \in \mathbb{Z}$):

(**a**) $n^3 - n$. (**b**) $n^4 - n^2$. (**c**) $3n^2 + 3n - 60$. (**d**) $n^5 - n$.

Solution:

(**a**) $(n^3 - n)$ is even (see rules 4 and 6 of § 1.8) and hence it is divisible by 2. Also, $(n^3 - n)$ is divisible by 3 (see part a of Problem 3). Hence, $(n^3 - n)$ is divisible by $2 \times 3 = 6$ (see rule 28 of § 1.9).
(**b**) $(n^4 - n^2)$ is even (see rules 4 and 6 of § 1.8) and divisible by 3 (see part d of Problem 3) and hence it is divisible by 6. Alternatively, $n^4 - n^2 = n(n^3 - n)$ and hence it is divisible by 6 (see part a).
(**c**) $3n^2 + 3n - 60 = 3(n^2 + n - 20)$ is even and divisible by 3 and hence it is divisible by 6.

(**d**) The divisibility of $(n^5 - n)$ by 6 is equivalent to the congruence equation $n^5 - n \stackrel{6}{=} 0$. Considering this with $n = 0, 1, 2, 3, 4, 5$ (which are the residues of modulo 6) we have:

$0^5 - 0 \stackrel{6}{=} 0$ $1^5 - 1 \stackrel{6}{=} 0$ $2^5 - 2 \stackrel{6}{=} 0$ $3^5 - 3 \stackrel{6}{=} 0$ $4^5 - 4 \stackrel{6}{=} 0$ $5^5 - 5 \stackrel{6}{=} 0$

As we see, $(n^5 - n)$ is congruent to 0 (mod 6) in all cases and hence it is divisible by 6.

7. Prove the following polynomial divisibility statements (where $n \in \mathbb{Z}$):

(**a**) $10|(n^5 - n)$. (**b**) $10|(n^9 - n)$. (**c**) $12|(n^4 - n^2)$.

Solution:

(**a**) $(n^5 - n)$ is even (see rules 4 and 6 of § 1.8) and hence it is divisible by 2. Also, $(n^5 - n)$ is divisible by 5 (see part a of Problem 5). Hence, $(n^5 - n)$ is divisible by $2 \times 5 = 10$ (see rules 20 and 32 of § 1.9).
(**b**) $(n^9 - n)$ is even (see rules 4 and 6 of § 1.8) and hence it is divisible by 2. Also, $(n^9 - n)$ is divisible by 5 (see part c of Problem 5). Hence, $(n^9 - n)$ is divisible by $2 \times 5 = 10$ (see rules 20 and 32 of § 1.9).
(**c**) $(n^4 - n^2)$ is divisible by 3 and 4 (see Problems 3 and 4) and hence it must be divisible by 12 (see rules 20 and 34 of § 1.9).

8. Prove the following polynomial divisibility statements (where $n \in \mathbb{Z}$):

(**a**) $4 \not| (n^2 + 2)$. (**b**) $4 \not| (n^2 - 2)$. (**c**) $4 \not| \big[(n+1)^2 - n^2\big]$.

(**d**) $5 \not| \big[(n+1)^3 - n^3\big]$. (**e**) $5 \not| \big[(n+1)^5 - n^5\big]$. (**f**) $7 \not| \big[(n+1)^7 - n^7\big]$.

Solution:

(**a**) If n is odd then n^2 is odd and hence (n^2+2) is odd, therefore (n^2+2) is not divisible by 4 which is even (see the rules of parity in § 1.8). If n is even then n^2 is divisible by 4 (because n^2 contains a factor of 2^2) and hence (n^2+2) is not divisible by 4 (because the difference between any consecutive multiples of 4 must be 4 or because of rule 17 of § 1.9).
(**b**) The argument is the same as the argument of part (a).
(**c**) If n is odd then $(n+1)^2$ is even and n^2 is odd and hence $(n+1)^2-n^2$ is odd (see the parity rules in § 1.8), therefore it cannot be divisible by 4 which is even. If n is even then $(n+1)^2$ is odd and n^2 is even and hence $(n+1)^2-n^2$ is odd, therefore it cannot be divisible by 4.
(**d**) The divisibility of $(n+1)^3-n^3$ by 5 is equivalent to the congruence equation $(n+1)^3-n^3 \stackrel{5}{=} 0$. Considering this with $n=0,1,2,3,4$ (which are the residues of modulo 5) we have:

$$(0+1)^3-0^3 \stackrel{5}{=} 1 \qquad (1+1)^3-1^3 \stackrel{5}{=} 2 \qquad (2+1)^3-2^3 \stackrel{5}{=} 4 \qquad (3+1)^3-3^3 \stackrel{5}{=} 2 \qquad (4+1)^3-4^3 \stackrel{5}{=} 1$$

As we see, $(n+1)^3-n^3$ can be congruent (mod 5) only to $1,2,4$ and hence $(n+1)^3-n^3$ cannot be divisible by 5.
(**e**) We have:

$$(n+1)^5-n^5 = 5n^4+10n^3+10n^2+5n+1 = 5(n^4+2n^3+2n^2+n)+1$$

Therefore, $(n+1)^5-n^5 \stackrel{5}{=} 1$ and hence it cannot be divisible by 5 (also see rule 17 of § 1.9).
(**f**) We have:

$$(n+1)^7-n^7 = 7n^6+21n^5+35n^4+35n^3+21n^2+7n+1 = 7(n^6+3n^5+5n^4+5n^3+3n^2+n)+1$$

Therefore, $(n+1)^7-n^7 \stackrel{7}{=} 1$ and hence it cannot be divisible by 7 (also see rule 17 of § 1.9).

9. Find all pairs of integers (m,n) that satisfy the following "polynomial" divisibility statements:
(**a**) $5|(21m+35n-9)$. (**b**) $13|(152m+278n+22)$. (**c**) $15|(81m+33n+6)$.
Solution:
(**a**) $5|(21m+35n-9)$ is equivalent to $21m+35n-9 \stackrel{5}{=} 0$, i.e. $m \stackrel{5}{=} 4$. So, all pairs of integers $(m,n)=(4+5k,s)$ where $k,s \in \mathbb{Z}$ should satisfy this divisibility statement.
(**b**) $13|(152m+278n+22)$ is equivalent to $152m+278n+22 \stackrel{13}{=} 0$, i.e. $9m+5n+9 \stackrel{13}{=} 0$. The solutions (m,n) of this congruence (see § 4.2.1) are (noting that for brevity we delete $+13k, +13s$ from the m,n components where $k,s \in \mathbb{Z}$):

(0,6)	(1,12)	(2,5)	(3,11)	(4,4)	(5,10)	(6,3)
(7,9)	(8,2)	(9,8)	(10,1)	(11,7)	(12,0)	

So, all pairs of integers (m,n) of these 13 forms satisfy this divisibility statement.
(**c**) $15|(81m+33n+6)$ is equivalent to $81m+33n+6 \stackrel{15}{=} 0$, i.e. $6m+3n+6 \stackrel{15}{=} 0$. The solutions (m,n) of this congruence are (noting that for brevity we delete $+15k, +15s$ from the m,n components where $k,s \in \mathbb{Z}$):

(0,3)	(0,8)	(0,13)	(5,3)	(5,8)	(5,13)	(10,3)	(10,8)	(10,13)
(1,1)	(1,6)	(1,11)	(6,1)	(6,6)	(6,11)	(11,1)	(11,6)	(11,11)
(2,4)	(2,9)	(2,14)	(7,4)	(7,9)	(7,14)	(12,4)	(12,9)	(12,14)
(3,2)	(3,7)	(3,12)	(8,2)	(8,7)	(8,12)	(13,2)	(13,7)	(13,12)
(4,0)	(4,5)	(4,10)	(9,0)	(9,5)	(9,10)	(14,0)	(14,5)	(14,10)

So, all pairs of integers (m,n) of these 45 forms satisfy this divisibility statement.

10. Find all $n \in \mathbb{Z}$ such that:
(**a**) $(n^2-12n+6)$ is divisible by 3 and 5. (**b**) $(4n^3+2n-1)$ is divisible by 7 and 19.
(**c**) $(2n^4+11n^3+22)$ is divisible by 5, 14 and 31.
Solution: We use in the solution of this type of problems an approach that we used in § 3.5.

(**a**) If $(n^2-12n+6)$ is divisible by 3 then $n^2-12n+6 \overset{3}{=} 0$ whose solution is $n \overset{3}{=} 0$.[158]
If $(n^2-12n+6)$ is divisible by 5 then $n^2-12n+6 \overset{5}{=} 0$ whose solution is $n \overset{5}{=} 1$.
Now, if we solve the system of congruence equations $n \overset{3}{=} 0$ and $n \overset{5}{=} 1$ simultaneously (using for instance the Chinese remainder theorem; see § 2.7.3) then we get: $n = 6+15k$ $(k \in \mathbb{Z})$. So, $(n^2-12n+6)$ is divisible by 3 and 5 for all $n = 6+15k$ where $k \in \mathbb{Z}$.
We may also solve this Problem in one go (using rule 20 of § 1.9 noting that 3 and 5 are coprime) by considering the divisibility of $(n^2-12n+6)$ by 15, i.e. by obtaining the solution of $(n^2-12n+6) \overset{15}{=} 0$.
(**b**) If $(4n^3+2n-1)$ is divisible by 7 then $4n^3+2n-1 \overset{7}{=} 0$ whose solutions are $n \overset{7}{=} 2$ and $n \overset{7}{=} 6$.
If $(4n^3+2n-1)$ is divisible by 19 then $4n^3+2n-1 \overset{19}{=} 0$ whose solution is $n \overset{19}{=} 12$.
Now, if we solve the system of congruence equations $n \overset{7}{=} 2$ and $n \overset{19}{=} 12$ simultaneously then we get: $n = 107+133k$ $(k \in \mathbb{Z})$. Similarly, if we solve the system of congruence equations $n \overset{7}{=} 6$ and $n \overset{19}{=} 12$ simultaneously then we get: $n = 69+133k$ $(k \in \mathbb{Z})$. So, $(4n^3+2n-1)$ is divisible by 7 and 19 for all $n = 107+133k$ and $n = 69+133k$ where $k \in \mathbb{Z}$.
We may also solve this Problem in one go (as explained in part a).
(**c**) If $(2n^4+11n^3+22)$ is divisible by 5 then $2n^4+11n^3+22 \overset{5}{=} 0$ whose solution is $n \overset{5}{=} 1$.
If $(2n^4+11n^3+22)$ is divisible by 14 then $2n^4+11n^3+22 \overset{14}{=} 0$ whose solution is $n \overset{14}{=} 8$.
If $(2n^4+11n^3+22)$ is divisible by 31 then $2n^4+11n^3+22 \overset{31}{=} 0$ whose solution is $n \overset{31}{=} 20$.
Now, if we solve the system of congruence equations $n \overset{5}{=} 1$, $n \overset{14}{=} 8$ and $n \overset{31}{=} 20$ simultaneously then we get: $n = 2066+2170k$ $(k \in \mathbb{Z})$. So, $(2n^4+11n^3+22)$ is divisible by 5, 14 and 31 for all $n = 2066+2170k$ where $k \in \mathbb{Z}$.
We may also solve this Problem in one go (as explained in part a).

11. Find all $n \in \mathbb{Z}$ such that:
(**a**) $7|(n^{12}+6)$. (**b**) $25|(n^{33}-8)$. (**c**) $39|(n^{52}+17)$.
Solution:
(**a**) $7|(n^{12}+6)$ means $n^{12}+6 \overset{7}{=} 0$ which is equivalent to $n^{12}-1 \overset{7}{=} 0$, i.e. $n^{12} \overset{7}{=} 1$. Now, by Fermat's little theorem (see § 2.9.3) we have $n^6 \overset{7}{=} 1$ (where $7 \not| n$) and hence by squaring we get: $n^{12} \overset{7}{=} 1$ for all $7 \not| n$. In other words, $7|(n^{12}+6)$ for all $n \in \mathbb{Z}$ where $7 \not| n$.
(**b**) If $25|(n^{33}-8)$ then (by rule 7 of § 1.9) we must have $5|(n^{33}-8)$ which is equivalent to $n^{33}-8 \overset{5}{=} 0$, i.e. $n^{33} \overset{5}{=} 3$. Now, we have (by applying Fermat's little theorem repeatedly; see § 2.9.3):

$$n^{33} = (n^5)^6 \times n^3 \overset{5}{=} n^6 \times n^3 = n^5 \times n^4 \overset{5}{=} n \times n^4 = n^5 \overset{5}{=} n$$

i.e. $n \overset{5}{=} 3$. Accordingly, $n \overset{25}{=} 3$ or $n \overset{25}{=} 8$ or $n \overset{25}{=} 13$ or $n \overset{25}{=} 18$ or $n \overset{25}{=} 23$. Now:

$3^3 \overset{25}{=} 2 \quad \rightarrow \quad 3^{33} \overset{25}{=} 2^{11} \overset{25}{=} 23 \quad \rightarrow \quad 3^{33}-8 \overset{25}{=} 23-8 = 15 \overset{25}{\neq} 0$

$8^7 \overset{25}{=} 2 \quad \rightarrow \quad 8^{33} = 8^{28}\,8^5 \overset{25}{=} 2^4\,8^5 \overset{25}{=} 13 \quad \rightarrow \quad 8^{33}-8 \overset{25}{=} 13-8 = 5 \overset{25}{\neq} 0$

$13^6 \overset{25}{=} 9 \quad \rightarrow \quad 13^{33} = 13^{30}\,13^3 \overset{25}{=} 9^5\,13^3 \overset{25}{=} 3 \quad \rightarrow \quad 13^{33}-8 \overset{25}{=} 3-8 = -5 \overset{25}{\neq} 0$

$18^4 \overset{25}{=} 1 \quad \rightarrow \quad 18^{33} = 18^{32}\,18^1 \overset{25}{=} 1^8\,18^1 \overset{25}{=} 18 \quad \rightarrow \quad 18^{33}-8 \overset{25}{=} 18-8 = 10 \overset{25}{\neq} 0$

$23^2 \overset{25}{=} 4 \quad \rightarrow \quad 23^{33} = 23^{32}\,23^1 \overset{25}{=} 4^{16}\,23^1 \overset{25}{=} 8 \quad \rightarrow \quad 23^{33}-8 \overset{25}{=} 8-8 \overset{25}{=} 0$

So, $25|(n^{33}-8)$ only for $n \overset{25}{=} 23$, i.e. $25|(n^{33}-8)$ for all $n = 23+25k$ where $k \in \mathbb{Z}$.
(**c**) $39 = 3 \times 13$ and hence if $39|(n^{52}+17)$ then (according to rule 20 of § 1.9) we must have $3|(n^{52}+17)$ and $13|(n^{52}+17)$, i.e. $n^{52} \overset{3}{=} -17 \overset{3}{=} 1$ and $n^{52} \overset{13}{=} -17 \overset{13}{=} 9$. Now, we have (by applying Fermat's little theorem repeatedly; see § 2.9.3):

[158] The reader is referred to § 3.2.1 for the methods of solving such a congruence equation.

$n^{52} \overset{3}{=} 1 \quad \rightarrow \quad (n^3)^{17} \times n \overset{3}{=} 1 \quad \rightarrow \quad n^{17} \times n \overset{3}{=} 1 \quad \rightarrow \quad n^{18} \overset{3}{=} 1 \quad \rightarrow$

$(n^3)^6 \overset{3}{=} 1 \quad \rightarrow \quad n^6 \overset{3}{=} 1 \quad \rightarrow \quad (n^3)^2 \overset{3}{=} 1 \quad \rightarrow \quad n^2 \overset{3}{=} 1$

$n^{52} \overset{13}{=} 9 \quad \rightarrow \quad (n^{13})^4 \overset{13}{=} 9 \quad \rightarrow \quad n^4 \overset{13}{=} 9$

Now, the congruence $n^2 \overset{3}{=} 1$ has 2 solutions which are $n \overset{3}{=} 1$ and $n \overset{3}{=} 2$, while the congruence $n^4 \overset{13}{=} 9$ has 4 solutions which are $n \overset{13}{=} 4$, $n \overset{13}{=} 6$, $n \overset{13}{=} 7$ and $n \overset{13}{=} 9$. On considering the combination of all these possibilities (i.e. $8 = 2 \times 4$) we get the following table:

mod 3	1	1	1	1	2	2	2	2
mod 13	4	6	7	9	4	6	7	9
mod 39	4	19	7	22	17	32	20	35

where the last row represents the solutions of the 8 pairs of congruences (obtained by using, for instance, the Chinese remainder theorem; see § 2.7.3).

So, $39|(n^{52}+17)$ for $n \overset{39}{=} 4, 7, 17, 19, 20, 22, 32, 35$. In other words, $39|(n^{52}+17)$ for all $n = m + 39k$ where $m = 4, 7, 17, 19, 20, 22, 32, 35$ and $k \in \mathbb{Z}$.

12. Show that:
(**a**) $8|(n^2-1)$ where n is odd. (**b**) $22 \not| (n^{77} - n^3 + n - 13)$ where $n \in \mathbb{Z}$.

Solution:
(**a**) Since n is odd then $n = 2k+1$ ($k \in \mathbb{Z}$) and hence:

$$n^2 - 1 = (2k+1)^2 - 1 = 4k^2 + 4k = 4(k^2 + k)$$

Now, (k^2+k) is even (see the parity rules in § 1.8) and hence $(n^2-1) = 8m$ ($m \in \mathbb{Z}$), i.e. $8|(n^2-1)$.
(**b**) $22 = 2 \times 11$ and hence if $22|(n^{77} - n^3 + n - 13)$ then we must have $2|(n^{77} - n^3 + n - 13)$ and $11|(n^{77} - n^3 + n - 13)$ (see rule 20 of § 1.9). Now, $11|(n^{77} - n^3 + n - 13)$ is equivalent to $n^{77} - n^3 + n \overset{11}{=} 13$ and hence from Fermat's little theorem (see § 2.9.3) we have:

$n^{77} - n^3 + n \overset{11}{=} 13 \quad \rightarrow \quad (n^{11})^7 - n^3 + n \overset{11}{=} 13 \quad \rightarrow \quad n^7 - n^3 + n \overset{11}{=} 2$

On testing $n = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ (which are the residues of n mod 11) we find $n^7 - n^3 + n \overset{11}{=} 0, 1, 1, 7, 0, 4, 7, 0, 4, 10, 10$. So, there is no solution to $n^7 - n^3 + n \overset{11}{=} 2$ which means that $11 \not| (n^{77} - n^3 + n - 13)$ and hence $22 \not| (n^{77} - n^3 + n - 13)$.

6.3 Divisibility of Numbers by Polynomials

In this type of Problems we usually want to find integers or natural numbers that make a given polynomial $P(n)$ divide a given number m. In this case we consider all the divisors of m to see if there is any (integer or natural) value n that makes $P(n)$ equal to any one of these divisors. This can be easily done by solving polynomial equations by the usual methods of algebra. This procedure is demonstrated in the following Problems.

Problems

1. Find all the values (if any) of $n \in \mathbb{Z}$ that satisfy the following divisibility statements:
(**a**) $(n^2+3n-10)|1544$. (**b**) $(2n^3 - 19n^2 - 85n - 78)|1414$. (**c**) $(n^4 + 8n^3 - 159n^2 + 378n)|400$.

Solution:
(**a**) The divisors of 1544 are $1, 2, 4, 8, 193, 386, 772, 1544$ (as well as their negatives). If $(n^2+3n-10)$ divides 1544 then it must be equal to some of these divisors for certain values of $n \in \mathbb{Z}$. So, what we need to do is to equate the polynomial to each one of these divisors (and their negatives) and solve the resulting equation to see if there is an integer solution to this equation (e.g. $n^2+3n-10 = 1$ has no integer solution, while $n^2+3n-10 = 8$ has some integer solutions and hence we take these solutions). In brief, on inspecting each one of these divisors (and their negatives) we find that only $n = -6$ and $n = 3$ (corresponding to the divisor 8) satisfy this divisibility statement.

(**b**) The divisors of 1414 are $1, 2, 7, 14, 101, 202, 707, 1414$ (as well as their negatives). On repeating the argument and procedure of part (a) we find that only $n = -1$ (corresponding to the divisor -14) satisfies this divisibility statement.
(**c**) The divisors of 400 are $1, 2, 4, 5, 8, 10, 16, 20, 25, 40, 50, 80, 100, 200, 400$ (as well as their negatives). On repeating the argument and procedure of part (a) we find that only $n = 2$ (corresponding to the divisor 200) satisfies this divisibility statement.

6.4 Divisibility of Polynomials by Polynomials

In this kind of divisibility problems we usually look for certain values of $n \in \mathbb{N}$ or $n \in \mathbb{Z}$ that make a given polynomial $P_1(n)$ divisible by another polynomial $P_2(n)$. There are several approaches for solving this kind of problems. Some of these approaches are outlined and demonstrated in the following Problems.

Problems

1. Find all $n \in \mathbb{Z}$ such that:
(**a**) $(2n+1)|(5n-13)$. (**b**) $(6n+9)|(8n-16)$. (**c**) $(2n-3)|(4n+12)$. (**d**) $(5n+32)|(23-5n)$.
Solution: Our approach in this Problem is to try to convert the problem from being a problem of divisibility of polynomials by polynomials to a problem of divisibility of numbers by polynomials. We note that none of the divisors in this Problem vanishes for any $n \in \mathbb{Z}$.
(**a**) It is obvious that $(2n+1)$ divides any of its multiples, and hence $(2n+1)$ divides $5(2n+1) = 10n+5$. Also, if $(2n+1)$ should divide $(5n-13)$ then $(2n+1)$ must divide any multiple of $(5n-13)$, and hence $(2n+1)$ divides $2(5n-13) = 10n-26$. So, $(2n+1)$ divides both $(10n+5)$ and $(10n-26)$ and hence it must divide their difference which is 31 (rule 14 of § 1.9). Noting that the divisors of 31 are ± 1 and ± 31, we conclude that if $(2n+1)|(5n-13)$ then $(2n+1)$ must be equal to ± 1 or ± 31. Considering all these four possibilities we have:

$2n+1 = -1$	$\rightarrow$	$n = -1$	that is:	$-1\|-18$
$2n+1 = +1$	$\rightarrow$	$n = 0$	that is:	$+1\|-13$
$2n+1 = -31$	$\rightarrow$	$n = -16$	that is:	$-31\|-93$
$2n+1 = +31$	$\rightarrow$	$n = +15$	that is:	$+31\|+62$

(**b**) As in part (a), $(6n+9)$ divides any of its multiples, and hence $(6n+9)$ divides $4(6n+9) = 24n+36$. Also, $(6n+9)$ presumably divides $(8n-16)$ and hence it divides $3(8n-16) = 24n-48$. So, $(6n+9)$ divides their difference which is 84. Noting that the divisors of 84 are $1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84$ (and their negatives) we conclude that if $(6n+9)|(8n-16)$ then $(6n+9)$ must be equal to (some of) these divisors. Considering all these 24 possibilities we find that only $(6n+9) = +3$ and $(6n+9) = +21$ satisfy this divisibility statement (i.e. for $n \in \mathbb{Z}$), that is:

$6n+9 = +3$	$\rightarrow$	$n = -1$	that is:	$+3\|-24$
$6n+9 = +21$	$\rightarrow$	$n = +2$	that is:	$+21\|0$

(**c**) $(2n-3)$ divides any of its multiples, and hence $(2n-3)$ divides $2(2n-3) = 4n-6$. Also, $(2n-3)$ presumably divides $(4n+12)$. Hence, $(2n-3)$ divides their difference which is 18. Noting that the divisors of 18 are $1, 2, 3, 6, 9, 18$ (and their negatives) we conclude that $(2n-3)$ must be equal to (some of) these divisors. Considering all these 12 possibilities we find that only $(2n-3) = \pm 1$, $(2n-3) = \pm 3$ and $(2n-3) = \pm 9$ satisfy this divisibility statement (i.e. for $n \in \mathbb{Z}$), that is:

$2n-3=-1$	$\rightarrow$	$n=+1$	that is:	$-1\vert+16$
$2n-3=+1$	$\rightarrow$	$n=+2$	that is:	$+1\vert+20$
$2n-3=-3$	$\rightarrow$	$n=0$	that is:	$-3\vert+12$
$2n-3=+3$	$\rightarrow$	$n=+3$	that is:	$+3\vert+24$
$2n-3=-9$	$\rightarrow$	$n=-3$	that is:	$-9\vert 0$
$2n-3=+9$	$\rightarrow$	$n=+6$	that is:	$+9\vert+36$

(**d**) $(5n+32)$ divides itself, and $(5n+32)$ presumably divides $(23-5n)$. Hence, $(5n+32)$ divides their sum which is 55 (rule 14 of § 1.9). Noting that the divisors of 55 are $1, 5, 11, 55$ (and their negatives) we conclude that if $(5n+32)|(23-5n)$ then $(5n+32)$ must be equal to (some of) these divisors. Considering all these 8 possibilities we find that no value of $n \in \mathbb{Z}$ makes $(5n+32)$ equal to one of these divisors, and hence no value of $n \in \mathbb{Z}$ satisfies this divisibility statement.

2. Re-solve Problem 1 using a different approach.

Solution: We will use in this Problem the direct division approach.

(**a**) We have:

$$\frac{5n-13}{2n+1} = \frac{1}{2}\left(5 - \frac{31}{2n+1}\right)$$

This quotient must be an integer which can only be achieved (with integer n) if $2n+1 = \pm 1$ or $2n+1 = \pm 31$ (as before).

(**b**) We have:

$$\frac{8n-16}{6n+9} = \frac{1}{3}\left(4 - \frac{28}{2n+3}\right)$$

This quotient must be an integer which can only be achieved (with integer n) if $2n+3 = 1$ or $2n+3 = 7$, i.e. $6n+9 = 3$ or $6n+9 = 21$ (as before).

(**c**) We have:

$$\frac{4n+12}{2n-3} = 2 + \frac{18}{2n-3}$$

This quotient must be an integer which can only be achieved (with integer n) if $2n-3 = \pm 1$ or $2n-3 = \pm 3$ or $2n-3 = \pm 9$ (as before).

(**d**) We have:

$$\frac{23-5n}{5n+32} = -1 + \frac{55}{5n+32}$$

As we see, $5n+32 \neq \pm 1, \pm 5, \pm 11, \pm 55$ for any $n \in \mathbb{Z}$ and hence this quotient cannot be an integer.

3. Find all $n \in \mathbb{Z}$ such that:

(**a**) $(n-3)|(n^2-7n+5)$. (**b**) $(2n+5)|(n^2+6n-9)$.

Solution: Our approach in this Problem is to form a polynomial (in n) that represents the essence of the divisibility statement (by combining the expressions of the divisor and dividend in a proportionality statement) where this polynomial contains a parameter k and hence the polynomial represents a Diophantine equation in two variables $(n, k \in \mathbb{Z})$ whose solutions represent the solutions of the given divisibility statement (as will be demonstrated in the following).

(**a**) If $(n-3)$ divides (n^2-7n+5) then we must have (where $k \in \mathbb{Z}$):

$$n^2-7n+5 = k(n-3) \qquad \rightarrow \qquad n^2-7n-kn+3k+5=0$$

On solving this Diophantine equation (using the methods we learned in § 4.1.5) we find the following solutions: $n = -4, 4, 2, 10$ (corresponding to $k = -7, -7, 5, 5$). All these values satisfy the given divisibility statement. This is verified as follows:

$n=-4 \rightarrow -7|49$ $n=4 \rightarrow 1|-7$ $n=2 \rightarrow -1|-5$ $n=10 \rightarrow 7|35$

(**b**) If $(2n+5)$ divides (n^2+6n-9) then we must have (where $k \in \mathbb{Z}$):

$$n^2+6n-9 = k(2n+5) \qquad \rightarrow \qquad n^2+6n-2kn-5k-9=0$$

On solving this Diophantine equation (see § 4.1.5) we find the following solutions: $n=-38,-2,-3,33$ (corresponding to $k=-17,-17,18,18$). All these values are acceptable.

4. Re-solve Problem 3 using a different approach.
Solution: We will use in this Problem the direct division approach.
(**a**) We have:

$$\frac{n^2-7n+5}{n-3} = n-4-\frac{7}{n-3}$$

This quotient must be an integer which can only be achieved (with integer n) if $n-3=\pm 1$ or $n-3=\pm 7$, i.e. $n=4$ or $n=2$ or $n=10$ or $n=-4$ (as before).
(**b**) We have:

$$\frac{n^2+6n-9}{2n+5} = \frac{1}{4}\left(2n+7-\frac{71}{2n+5}\right)$$

This quotient must be an integer which can only be achieved (with integer n) if $2n+5=\pm 1$ or $2n+5=\pm 71$, i.e. $n=-2$ or $n=-3$ or $n=33$ or $n=-38$ (as before).

5. Find all $n \in \mathbb{Z}$ such that:
(**a**) $(n^2+10n-15)|(7n-5)$. (**b**) $(n^3-n^2+4n+8)|(n^2+11n-24)$.
Solution: In this type of problems where the divisor is of higher degree than the dividend, we can have an integer quotient in two obvious cases: $n=0$ with the constant of the divisor being a divisor of the constant of the dividend,[159] or the divisor and the dividend are equal in magnitude (i.e. the quotient is equal to ± 1). However, these two cases may not produce all the solutions and hence we need to consider a third case where we inspect the values of n for which the absolute value of the divisor is less than the absolute value of the dividend to see if some of these values can produce integer quotient.[160] These three cases will be considered and demonstrated in the following.
(**a**) Considering the aforementioned three cases we have:
• If $n=0$ then we have (-15)|(−5) which is untrue.
• If $n^2+10n-15=\pm(7n-5)$ then:

$$n^2+17n-20=0 \qquad \text{or} \qquad n^2+3n-10=0$$

The first quadratic equation has no integer solution, while the second quadratic equation has two integer solutions: $n=-5$ and $n=2$.
• If $|n^2+10n-15| < |7n-5|$ then $-18 \le n \le -6$ where $n=-13$ and $n=-10$ produce integer quotient.
So, the given divisibility statement is true for the following values of n: $-13,-10,-5,2$.
(**b**) Considering the aforementioned three cases we have:
• If $n=0$ then we have $(8)|(-24)$ which is true.
• If $n^3-n^2+4n+8=\pm(n^2+11n-24)$ then:

$$n^3+15n-16=0 \qquad \text{or} \qquad n^3-2n^2-7n+32=0$$

The first cubic equation has only one integer solution which is $n=1$, while the second cubic equation has no integer solution.
• If $|n^3-n^2+4n+8| < |n^2+11n-24|$ then $-3 \le n \le 0$ where $n=-1$ and $n=0$ produce integer quotient (noting that $n=0$ is considered already).
So, the given divisibility statement is true for the following values of n: $-1,0,1$.

[159] We should pay attention to two particular cases: when the constant of the divisor is zero (and hence it should be excluded), and when the constant of the dividend is zero with the constant of the divisor is not zero (and hence it should be included).

[160] Because the degree of the divisor is higher than the degree of the dividend these values are usually few and can be easily identified.

6. Find all $n \in \mathbb{Z}$ such that:
(**a**) $(n-7)|(n^3-12n^2+38n-17)$. (**b**) $(n^2-4n+5)|(n^7+5n^5+9n-19)$.
Solution: We use in this Problem the direct division approach.
(**a**) We have:
$$\frac{n^3-12n^2+38n-17}{n-7} = n^2-5n+3+\frac{4}{n-7}$$
Now, the divisors of 4 are $\pm1, \pm2, \pm4$ and hence $(n-7) = \pm1, \pm2, \pm4$, i.e. $n = 8, 6, 9, 5, 11, 3$.
(**b**) We have:
$$\frac{n^7+5n^5+9n-19}{n^2-4n+5} = n^5+4n^4+16n^3+44n^2+96n+164+\frac{185n-839}{n^2-4n+5}$$
So, now we are dealing with the following divisibility problem: $(n^2-4n+5)|(185n-839)$ which can be solved by the method of Problem 5. In brief, $n = 0$ and $(n^2-4n+5) = \pm(185n-839)$ have no solution, while considering $|n^2-4n+5| < |185n-839|$ leads to the following solutions: $n = 1, 2, 3, 61$.
7. Determine if the following divisibility statements are correct for all $n \in \mathbb{Z}$ (excluding the zeros of the divisors) or not where in the latter case determine $n \in \mathbb{Z}$ to which the statement is correct:
(**a**) $(n-2)|(n^6+5n^3-7n^2-76)$. (**b**) $(n-3)|(n^2-7n+5)$.
(**c**) $(n-5)|(n^3-5n^2+n-1)$. (**d**) $(n+1)|(n^9+19n^5+13n^2+22)$.
Solution: In this Problem we use rule 51 of § 1.9 where $P_1(n)$ represents the dividend polynomial.
(**a**) $P_1(2) = 0$ and hence the given statement is correct for all $n \in \mathbb{Z}$ (excluding 2) because the remainder of the division is 0 regardless of the value of $n \in \mathbb{Z}$ (excluding 2). This can also be seen by direct division:
$$\frac{n^6+5n^3-7n^2-76}{n-2} = n^5+2n^4+4n^3+13n^2+19n+38$$
(**b**) $P_1(3) = -7$ and hence the given statement is not correct for all $n \in \mathbb{Z}$ because the remainder is not 0. To determine $n \in \mathbb{Z}$ to which the statement is correct we note that since the remainder of the division is -7 then the result of dividing (n^2-7n+5) by $(n-3)$ is some integer expression plus $-7/(n-3)$. So, if the result of the division is to be an integer then $-7/(n-3)$ must be an integer. Noting that the divisors of -7 are ±1 and ±7 we equate $(n-3)$ to these divisors and hence we obtain $n = \pm4, 2, 10$ which are the same values that we obtained in part (a) of Problems 3 and 4. So, these are the values of $n \in \mathbb{Z}$ to which the statement is correct.
(**c**) $P_1(5) = 4$ and hence the given statement is not correct for all $n \in \mathbb{Z}$ because the remainder is not 0. To determine $n \in \mathbb{Z}$ to which the statement is correct we note that since the remainder of the division is 4 then the result of dividing (n^3-5n^2+n-1) by $(n-5)$ is some integer expression plus $4/(n-5)$. So, if the result of the division is to be an integer then $4/(n-5)$ must be an integer. Noting that the divisors of 4 are $\pm1, \pm2, \pm4$ we equate $(n-5)$ to these divisors and hence we obtain $n = 6, 4, 7, 3, 9, 1$. So, these are the values of $n \in \mathbb{Z}$ to which the statement is correct.
(**d**) $P_1(-1) = 15$ and hence the given statement is not correct for all $n \in \mathbb{Z}$ because the remainder is not 0. To determine $n \in \mathbb{Z}$ to which the statement is correct we note that since the remainder of the division is 15 then the result of dividing $(n^9+19n^5+13n^2+22)$ by $(n+1)$ is some integer expression plus $15/(n+1)$. So, if the result of the division is to be an integer then $15/(n+1)$ must be an integer. Noting that the divisors of 15 are $\pm1, \pm3, \pm5, \pm15$ we equate $(n+1)$ to these divisors and hence we obtain $n = 0, \pm2, \pm4, -6, 14, -16$. So, these are the values of $n \in \mathbb{Z}$ to which the statement is correct.
8. Find all $n \in \mathbb{Z}$ such that:
(**a**) $(n^2+2n-15)|(n^4-6n^3-24n^2+134n-105)$.
(**b**) $(n^2-13n+36)|(n^4+5n^3-8n^2-16n+9)$.
(**c**) $(n^2-n-2)|(n^4+3n^3-41n^2-13n-10)$.
(**d**) $(n^3+4n^2-553n+3332)|(2n^5-17n^4+11n^3-74n^2+n+30)$.
Solution: In this Problem we mainly employ rules 19, 20 and 51 of § 1.9 where we use $P_1(n)$ to refer to the dividend polynomial.

(**a**) $(n^2+2n-15)=(n-3)(n+5)$ and hence if this divides $P_1(n)$ then $P_1(n)$ must be divisible by $(n-3)$ and by $(n+5)$ simultaneously (rule 19 of § 1.9).
Now, $P_1(3)=0$ which means that $(n-3)$ divides $P_1(n)$ for all $n\in\mathbb{Z}$ (excluding 3) because the remainder of the division is 0 (rule 51 of § 1.9) regardless of the value of $n\in\mathbb{Z}$ (excluding 3).
Also, $P_1(-5)=0$ which means that $(n+5)$ divides $P_1(n)$ for all $n\in\mathbb{Z}$ (excluding -5) because the remainder of the division is 0 regardless of the value of $n\in\mathbb{Z}$ (excluding -5).
So, $(n-3)$ and $(n+5)$ divide $P_1(n)$ simultaneously for all $n\in\mathbb{Z}$ excluding $n=3$ and $n=-5$, and hence this divisibility statement is valid for all values of $n\in\mathbb{Z}$ except $n=3$ and $n=-5$.
This can also be seen easily by direct division:

$$\frac{n^4-6n^3-24n^2+134n-105}{n^2+2n-15}=n^2-8n+7 \qquad\qquad (n\neq 3,-5)$$

(**b**) $(n^2-13n+36)=(n-4)(n-9)$ and hence if this divides $P_1(n)$ then $P_1(n)$ must be divisible by $(n-4)$ and by $(n-9)$ simultaneously.
Now, $P_1(4)=393$ whose divisors are $\pm1,\pm3,\pm131,\pm393$. On equating $(n-4)$ to these divisors we get $n=5,3,7,1,135,-127,397,-389$.
Also, $P_1(9)=9423$ whose divisors are $\pm1,\pm3,\pm9,\pm27,\pm349,\pm1047,\pm3141,\pm9423$. On equating $(n-9)$ to these divisors we get $n=10$, 8, 12, 6, 18, 0, 36, -18, 358, -340, 1056, -1038, 3150, -3132, 9432, -9414.
As we see, there is no common value of n that makes $P_1(n)$ divisible by $(n-4)$ and by $(n-9)$ simultaneously and hence there is no value of n that satisfies this divisibility statement.
This can also be seen easily by noting that $(n^4+5n^3-8n^2-16n+9)$ is odd while $(n^2-13n+36)$ is even and hence there is no value of n that satisfies this divisibility statement (see the rules of parity in § 1.8).
(**c**) $(n^2-n-2)=(n-2)(n+1)$ and hence if this divides $P_1(n)$ then $P_1(n)$ must be divisible by $(n-2)$ and by $(n+1)$ simultaneously.
Now, $P_1(2)=-160$ whose divisors are $1,2,4,5,8,10,16,20,32,40,80,160$ and their negatives. On equating $(n-2)$ to these divisors we get $n=-158$, -78, -38, -30, -18, -14, -8, -6, -3, -2, 0, 1, 3, 4, 6, 7, 10, 12, 18, 22, 34, 42, 82, 162.
Also, $P_1(-1)=-40$ whose divisors are $1,2,4,5,8,10,20,40$ and their negatives. On equating $(n+1)$ to these divisors we get $n=-41$, -21, -11, -9, -6, -5, -3, -2, 0, 1, 3, 4, 7, 9, 19, 39.
As we see, $n=-6,-3,-2,0,1,3,4,7$ are common to both cases which means that these values of n make $P_1(n)$ divisible by $(n-2)$ and by $(n+1)$ simultaneously, and hence these values of n make $P_1(n)$ divisible by their product which is (n^2-n-2).[161] So, this divisibility statement is satisfied for $n=-6,-3,-2,0,1,3,4,7$.
(**d**) $(n^3+4n^2-553n+3332)=(n-17)(n-7)(n+28)$ and hence if this divides $P_1(n)$ then $P_1(n)$ must be divisible by $(n-17)$ and by $(n-7)$ and by $(n+28)$ simultaneously.
Now, $P_1(17)=1452561$ whose divisors are $1,3,11,33,44017,132051,484187,1452561$ and their negatives. On equating $(n-17)$ to these divisors we get $n=-1452544$, -484170, -132034, -44000, -16, 6, 14, 16, 18, 20, 28, 50, 44034, 132068, 484204, 1452578.
Also, $P_1(7)=-7019$ whose divisors are $1,7019$ and their negatives. On equating $(n-7)$ to these divisors we get $n=-7012,6,8,7026$.
Also, $P_1(-28)=-45169374$ whose divisors are 1, 2, 3, 6, 17, 34, 51, 102, 442837, 885674, 1328511, 2657022, 7528229, 15056458, 22584687, 45169374 and their negatives. On equating $(n+28)$ to these divisors we get $n=-45169402$, -22584715, -15056486, -7528257, -2657050, -1328539, -885702, -442865, -130, -79, -62, -45, -34, -31, -30, -29, -27, -26, -25, -22, -11, 6, 23, 74, 442809, 885646, 1328483, 2656994, 7528201, 15056430, 22584659, 45169346.
As we see, only $n=6$ is common to all these 3 cases which means that $n=6$ makes $P_1(n)$ divisible by $(n-17)$ and by $(n-7)$ and by $(n+28)$ simultaneously, and hence $n=6$ makes $P_1(n)$ divisible by their product which is $(n^3+4n^2-553n+3332)$. So, this divisibility statement is satisfied only for $n=6$.

[161] In this argument we are using rule 20 of § 1.9 noting that $(n-2)$ and $(n+1)$ are coprime for these values of n. In fact, we can use an argument based on rule 19 of § 1.9 but this should be enough.

6.5 Divisibility of Exponentials by Numbers

We investigate in this section the divisibility of expressions involving numeric bases raised to variable exponents by numbers such as the divisibility of $(5^n - 1)$ by 4. In this kind of problems it is useful to keep in mind the theorems that deal with this type of expressions such as Euler's theorem and Fermat's little theorem (see § 2.9.2 and § 2.9.3) as well as general mathematical rules (like the rules of § 1.8 and § 1.9) and mathematical methods (like induction and modular arithmetic).

Problems

1. Prove the following (where $n \in \mathbb{N}$):

(**a**) $3|(7^n - 4^n)$. (**b**) $3|(5^n - 2^n)$. (**c**) $4|(7^n - 3^n)$. (**d**) $4|(5^n - 1)$.

(**e**) $5|(6^n + 4)$. (**f**) $5|(6^n - 1)$. (**g**) $5|(2^{4n-1} - 3)$. (**h**) $7|(11^n - 4^n)$.

(**i**) $7|(10^n - 3^n)$. (**j**) $10|(5^n - 5)$. (**k**) $10|(6^n - 6)$.

Solution: We note first that these divisibility statements (excluding parts g, j, k) are also valid for $n = 0$ and hence these statements (excluding parts g, j, k) are actually valid for all $n \in \mathbb{N}^0$.
(**a**) We use induction. For $n = 1$ we have $3|(7^1 - 4^1) = 3$. Assuming $3|(7^k - 4^k)$ for some $k \in \mathbb{N}$, we have:

$$7^{k+1} - 4^{k+1} = (7 \times 7^k) - (4 \times 4^k) = (3 \times 7^k) + (4 \times 7^k) - (4 \times 4^k) = (3 \times 7^k) + 4(7^k - 4^k)$$

Now, since $3|(3 \times 7^k)$ and we assumed $3|(7^k - 4^k)$ then the sum in the last equality must be divisible by 3 (see rule 14 of § 1.9). So, by induction $3|(7^n - 4^n)$ for all $n \in \mathbb{N}$.
(**b**) We use induction. For $n = 1$ we have $3|(5^1 - 2^1) = 3$. Assuming $3|(5^k - 2^k)$ for some $k \in \mathbb{N}$, we have:

$$5^{k+1} - 2^{k+1} = (5 \times 5^k) - (2 \times 2^k) = (3 \times 5^k) + (2 \times 5^k) - (2 \times 2^k) = (3 \times 5^k) + 2(5^k - 2^k)$$

Now, since $3|(3 \times 5^k)$ and we assumed $3|(5^k - 2^k)$ then the sum in the last equality must be divisible by 3 (see rule 14 of § 1.9). So, by induction $3|(5^n - 2^n)$ for all $n \in \mathbb{N}$.
(**c**) We use induction. For $n = 1$ we have $4|(7^1 - 3^1) = 4$. Assuming $4|(7^k - 3^k)$ for some $k \in \mathbb{N}$, we have:

$$7^{k+1} - 3^{k+1} = (7 \times 7^k) - (3 \times 3^k) = (4 \times 7^k) + (3 \times 7^k) - (3 \times 3^k) = (4 \times 7^k) + 3(7^k - 3^k)$$

Now, since $4|(4 \times 7^k)$ and we assumed $4|(7^k - 3^k)$ then the sum in the last equality must be divisible by 4 (see rule 14 of § 1.9). So, by induction $4|(7^n - 3^n)$ for all $n \in \mathbb{N}$.
(**d**) For $n = 1$ we have $4|(5^1 - 1) = 4$. For $n > 1$, 5^n ends in 25 (see rule 14 of § 1.8). Hence, $(5^n - 1)$ ends in 24 which is divisible by 4 (see rule 26 of § 1.9).
We may also use induction. For $n = 1$ we have $4|(5^1 - 1) = 4$. Assuming $4|(5^k - 1)$ for some $k \in \mathbb{N}$, we have:

$$5^{k+1} - 1 = (5 \times 5^k) - 1 = (4 \times 5^k) + (5^k - 1)$$

Now, since $4|(4 \times 5^k)$ and we assumed $4|(5^k - 1)$ then their sum must be divisible by 4 (see rule 14 of § 1.9). So, by induction $4|(5^n - 1)$ for all $n \in \mathbb{N}$.
(**e**) 6^n ends in 6 (rule 16 of § 1.8) and hence $(6^n + 4)$ ends in 0. Thus, $5|(6^n + 4)$ (rule 32 of § 1.9).
We may also use induction. For $n = 1$ we have $5|(6^1 + 4) = 10$. Assuming $5|(6^k + 4)$ for some $k \in \mathbb{N}$, we have:

$$6^{k+1} + 4 = (6 \times 6^k) + 4 = (5 \times 6^k) + (6^k + 4)$$

Now, since $5|(5 \times 6^k)$ and we assumed $5|(6^k + 4)$ then their sum must be divisible by 5 (see rule 14 of § 1.9). So, by induction $5|(6^n + 4)$ for all $n \in \mathbb{N}$.
(**f**) 6^n ends in 6 (rule 16 of § 1.8) and hence $(6^n - 1)$ ends in 5. Thus, $5|(6^n - 1)$ (rule 27 of § 1.9).
We may also use induction. For $n = 1$ we have $5|(6^1 - 1) = 5$. Assuming $5|(6^k - 1)$ for some $k \in \mathbb{N}$, we have:

$$6^{k+1} - 1 = (6 \times 6^k) - 1 = (5 \times 6^k) + (6^k - 1)$$

Now, since $5|(5 \times 6^k)$ and we assumed $5|(6^k - 1)$ then their sum must be divisible by 5 (see rule 14 of § 1.9). So, by induction $5|(6^n - 1)$ for all $n \in \mathbb{N}$.[162]

(**g**) We use induction. For $n = 1$ we have $5|(2^{4-1} - 3) = 5$. Assuming $5|(2^{4k-1} - 3)$ for some $k \in \mathbb{N}$, we have:

$$\begin{aligned} 2^{4(k+1)-1} - 3 &= 2^{4k+3} - 3 = (2^3)2^{4k} - 3 = (2^4)2^{4k-1} - 3 = (16)2^{4k-1} - 3 \\ &= (15+1)2^{4k-1} - 3 = (15)2^{4k-1} + (2^{4k-1} - 3) \end{aligned}$$

Now, 5|15 and we assumed $5|(2^{4k-1} - 3)$ and hence 5 divides $(15)2^{4k-1} + (2^{4k-1} - 3)$ (see rule 14 of § 1.9). So, by induction $5|(2^{4n-1} - 3)$ for all $n \in \mathbb{N}$.

(**h**) We use induction. For $n = 1$ we have $7|(11^1 - 4^1) = 7$. Assuming $7|(11^k - 4^k)$ for some $k \in \mathbb{N}$, we have:

$$11^{k+1} - 4^{k+1} = (7 \times 11^k) + (4 \times 11^k) - (4 \times 4^k) = (7 \times 11^k) + 4(11^k - 4^k)$$

Now, since $7|(7 \times 11^k)$ and we assumed $7|(11^k - 4^k)$ then the sum in the last equality must be divisible by 7 (see rule 14 of § 1.9). So, by induction $7|(11^n - 4^n)$ for all $n \in \mathbb{N}$.

(**i**) We use induction. For $n = 1$ we have $7|(10^1 - 3^1) = 7$. Assuming $7|(10^k - 3^k)$ for some $k \in \mathbb{N}$, we have:

$$10^{k+1} - 3^{k+1} = (10 \times 10^k) - (3 \times 3^k) = (7 \times 10^k) + (3 \times 10^k) - (3 \times 3^k) = (7 \times 10^k) + 3(10^k - 3^k)$$

Now, since $7|(7 \times 10^k)$ and we assumed $7|(10^k - 3^k)$ then the sum in the last equality must be divisible by 7 (see rule 14 of § 1.9). So, by induction $7|(10^n - 3^n)$ for all $n \in \mathbb{N}$.

(**j**) For $n = 1$ we have $10|(5^1 - 5) = 0$. For $n > 1$ we have:

$$5^n - 5 = 5(5^{n-1} - 1)$$

Now, 5^{n-1} is odd (see rule 6 of § 1.8) and hence $(5^{n-1} - 1)$ is even, i.e. $(5^{n-1} - 1) = 2k$ for some $k \in \mathbb{N}$. Therefore, $5^n - 5 = 5(5^{n-1} - 1) = 5 \times 2k = 10k$ and hence it is divisible by 10.

We may also argue (more simply) that 5^n ends in 5 (see rule 14 of § 1.8) and hence $(5^n - 5)$ ends in 0, therefore it is divisible by 10 (see rule 32 of § 1.9).

(**k**) For $n = 1$ we have $10|(6^1 - 6) = 0$. For $n > 1$ we have:

$$6^n - 6 = 6(6^{n-1} - 1)$$

Now, $5|(6^{n-1} - 1)$ according to part (f) (noting that $n > 1$) and hence $(6^{n-1} - 1) = 5k$ for some $k \in \mathbb{N}$. Therefore, $6^n - 6 = 6(6^{n-1} - 1) = 6 \times 5k = 10 \times 3k$ and hence it is divisible by 10.

We may also argue (more simply) that 6^n ends in 6 (see rule 16 of § 1.8) and hence $(6^n - 6)$ ends in 0, therefore it is divisible by 10 (see rule 32 of § 1.9).

2. Prove the following (where $n \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$):

(**a**) $133|(12^{n+2} - 12^{n+1} + 12^n)$.

(**b**) $17|(51^n - 136^n - 187^n)$.

(**c**) $25|(a5^{n+1} - b50^n - c175^n)$.

(**d**) $19|(41^{n+5} + 98^{n+3} - 60^{n+1} - 136^n)$.

Solution:

(**a**) $12^{n+2} - 12^{n+1} + 12^n = 12^n(12^2 - 12^1 + 1) = 12^n \times 133$.

(**b**) $51^n - 136^n - 187^n = (3^n \times 17^n) - (8^n \times 17^n) - (11^n \times 17^n) = 17^n(3^n - 8^n - 11^n)$.

(**c**) We have:

$$a5^{n+1} - b50^n - c175^n = 25a5^{n-1} - b(2^n \times 25^n) - c(7^n \times 25^n) = 25(a5^{n-1} - 2^n b25^{n-1} - 7^n c25^{n-1})$$

(**d**) We have: $41 \overset{19}{=} 3$, $98 \overset{19}{=} 3$, $60 \overset{19}{=} 3$, and $136 \overset{19}{=} 3$. Hence:

$$41^{n+5} + 98^{n+3} - 60^{n+1} - 136^n \overset{19}{=} 3^{n+5} + 3^{n+3} - 3^{n+1} - 3^n = 3^n(3^5 + 3^3 - 3^1 - 1) = 3^n(266) = 3^n(14 \times 19)$$

[162] It is worth noting that from a congruence perspective $5|(6^n - 1)$ is equivalent to $5|(6^n + 4)$ and hence the proof of part (e) should be enough. We may also state the proof in a concise form as: $6^n - 1 = (6^n + 4) - 5$ and hence $5|(6^n - 1)$ since $5|(6^n + 4)$ according to part (e) and 5|5 (see rule 14 of § 1.9).

3. Show that for all $m, n, k \in \mathbb{N}^0$ the following divisibility statements are true:
(**a**) $13|(7^{12m+2} + 9^{12n+4} + 11^{12k+5})$. (**b**) $25|(4^{20m+3} + 17^{20n+4} + 21^{20k+7} + 24)$.
Solution:
(**a**) This statement is equivalent to $7^{12m+2} + 9^{12n+4} + 11^{12k+5} \overset{13}{=} 0$. Now, by Fermat's little theorem (see § 2.9.3) and rule 11 of § 2.7 we have:

$$7^{12m} = (7^{12})^m \overset{13}{=} 1^m = 1 \qquad 9^{12n} = (9^{12})^n \overset{13}{=} 1^n = 1 \qquad 11^{12k} = (11^{12})^k \overset{13}{=} 1^k = 1$$

Hence, by the rules of indices and congruences we have:

$$7^{12m+2} + 9^{12n+4} + 11^{12k+5} = 7^{12m}7^2 + 9^{12n}9^4 + 11^{12k}11^5 \overset{13}{=} (1)7^2 + (1)9^4 + (1)11^5 = 167661 \overset{13}{=} 0$$

(**b**) This statement is equivalent to $4^{20m+3} + 17^{20n+4} + 21^{20k+7} + 24 \overset{25}{=} 0$. Now, by Euler's theorem (see § 2.9.2) and rule 11 of § 2.7 we have:

$$4^{20m} = (4^{20})^m \overset{25}{=} 1^m = 1 \qquad 17^{20n} = (17^{20})^n \overset{25}{=} 1^n = 1 \qquad 21^{20k} = (21^{20})^k \overset{25}{=} 1^k = 1$$

Hence, by the rules of indices and congruences we have:

$$\begin{aligned} 4^{20m+3} + 17^{20n+4} + 21^{20k+7} + 24 &= 4^{20m}4^3 + 17^{20n}17^4 + 21^{20k}21^7 + 24 \\ &\overset{25}{=} (1)4^3 + (1)17^4 + (1)21^7 + 24 = 1801172150 \overset{25}{=} 0 \end{aligned}$$

4. Find all $n \in \mathbb{N}^0$ such that:
(**a**) $33|(7^n - 1)$. (**b**) $47|(5^n + 8)$. (**c**) $19|(3^{2n+3} + 6)$. (**d**) $3|(5^n + 5)$.
(**e**) $3|(5^n - 5)$. (**f**) $5|(7^n - 3)$. (**g**) $7|(5^{2n+2} - 1)$.
Solution:
(**a**) $33|(7^n - 1)$ means $(7^n - 1) \overset{33}{=} 0$ and hence $7^n \overset{33}{=} 1$ (see rule 3 of § 2.7). Now, $7^0 \overset{33}{=} 1$ which means that $n = 0$ is a valid solution. On testing the few values of positive n we find that the lowest $n \in \mathbb{N}$ such that $7^n \overset{33}{=} 1$ is $n = 10$.[163] Hence:

$$7^{10} \overset{33}{=} 1 \qquad \rightarrow \qquad \left(7^{10}\right)^k \overset{33}{=} 1^k \qquad \rightarrow \qquad 7^{10k} \overset{33}{=} 1 \qquad (k \in \mathbb{N})$$

where we used rule 11 of § 2.7 in the second step. So, $33|(7^n - 1)$ for all $n = 10k$ (where $k \in \mathbb{N}^0$ to include $n = 0$).
(**b**) $47|(5^n + 8)$ means $(5^n + 8) \overset{47}{=} 0$ and hence $5^n \overset{47}{=} -8$, i.e. $5^n \overset{47}{=} 39$. On testing the first values of positive n we find that the lowest $n \in \mathbb{N}$ such that $5^n \overset{47}{=} 39$ is $n = 31$. Moreover, according to Euler's theorem (see § 2.9.2) we have: $5^{\phi(47)} \overset{47}{=} 1$, i.e. $5^{46} \overset{47}{=} 1$. Also, from rule 11 of § 2.7 we get $5^{46k} \overset{47}{=} 1$ $(k \in \mathbb{N})$. Hence:

$$\begin{aligned} 5^{31} &\overset{47}{=} 39 \\ 5^{31} \times 5^{46k} &\overset{47}{=} 39 \times 1 && \text{(rule 10 of § 2.7)} \\ 5^{31+46k} &\overset{47}{=} 39 && \text{(rules of indices)} \end{aligned}$$

So, $47|(5^n + 8)$ for all $n = 31 + 46k$ (where $k \in \mathbb{N}^0$ to include $n = 31$).
(**c**) $19|(3^{2n+3} + 6)$ means $(3^{2n+3} + 6) \overset{19}{=} 0$ and hence $3^{2n+3} \overset{19}{=} -6$, i.e. $3^{2n+3} \overset{19}{=} 13$. Now, by the rules of indices we have: $3^{2n+3} = 3^{2n} \times 3^3 = 3^{2n} \times 27$. Hence:

$$3^{2n+3} \overset{19}{=} 13 \quad \rightarrow \quad 3^{2n} \times 27 \overset{19}{=} 13 \quad \rightarrow \quad 3^{2n} \overset{19}{=} 13 \times 27^* \quad \rightarrow \quad 3^{2n} \overset{19}{=} 156 \quad \rightarrow \quad 3^{2n} \overset{19}{=} 4$$

[163] Such simple calculations can be done easily by using, for instance, a spreadsheet or a small piece of code (but be careful about the precision and accuracy of the used tool; see § 1.3.1).

On testing the first values of positive n we find that the lowest $n \in \mathbb{N}$ such that $3^{2n} \overset{19}{=} 4$ is $n = 7$, i.e. $3^{14} \overset{19}{=} 4$. Moreover, according to Euler's theorem we have: $3^{\phi(19)} \overset{19}{=} 1$, i.e. $3^{18} \overset{19}{=} 1$. Also, from rule 11 of § 2.7 we get $3^{18k} \overset{19}{=} 1$ ($k \in \mathbb{N}$). Hence:

$$\begin{aligned} 3^{14} &\overset{19}{=} 4 \\ 3^{14} \times 3^{18k} &\overset{19}{=} 4 \times 1 && \text{(rule 10 of § 2.7)} \\ 3^{14+18k} &\overset{19}{=} 4 && \text{(rules of indices)} \end{aligned}$$

So, $19|(3^{2n+3} + 6)$ for all $2n = 14 + 18k$, i.e. $n = 7 + 9k$ (where $k \in \mathbb{N}^0$).
(**d**) $3|(5^n + 5)$ for all even $n \in \mathbb{N}^0$. This can be proved by induction as follows.
For $n = 0$ we have $(5^0 + 5) = 6$ which is divisible by 3.
Let assume that $(5^k + 5)$ is divisible by 3 for a given even $k \in \mathbb{N}^0$. Hence:

$$5^{k+2} + 5 = (25 \times 5^k) + 5 = (24 \times 5^k) + (5^k + 5) = 3(8 \times 5^k) + (5^k + 5)$$

As we see, both terms in the last equality are divisible by 3 (the first because it has a factor of 3 and the second because of our assumption). So, we conclude (by induction) that $3|(5^n + 5)$ for all even $k \in \mathbb{N}^0$. We finally note that $3 \not| (5^n + 5)$ for any odd $n \in \mathbb{N}^0$ because:

$$5^n + 5 = 5^{2k+1} + 5 = (5 \times 5^{2k}) + 5 = (4 \times 5^{2k}) + (5^{2k} + 5)$$

Now, $3|(5^{2k} + 5)$ (as we already proved by induction) while $3 \not| (4 \times 5^{2k})$ (because there is no factor of 3 in 4×5^{2k}) and hence $3 \not| (5^n + 5)$ for any odd $n \in \mathbb{N}^0$ (see rule 17 of § 1.9).
(**e**) $3|(5^n - 5)$ for all odd $n \in \mathbb{N}^0$. This can be proved by induction as we did in part (d), that is:
For $n = 1$ we have $(5^1 - 5) = 0$ which is divisible by 3. Now, if we assume that $(5^k - 5)$ is divisible by 3 for a given odd $k \in \mathbb{N}^0$ then:

$$5^{k+2} - 5 = (25 \times 5^k) - 5 = (24 \times 5^k) + (5^k - 5) = 3(8 \times 5^k) + (5^k - 5)$$

As we see, both terms in the last equality are divisible by 3 (the first because it has a factor of 3 and the second because of our assumption). So, we conclude (by induction) that $3|(5^n - 5)$ for all odd $k \in \mathbb{N}^0$. We finally note that $3 \not| (5^n - 5)$ for any even $n \in \mathbb{N}^0$ because:

$$5^n - 5 = (5^n + 5) - 10$$

Now, according to part (d) $3|(5^n + 5)$ for all even $n \in \mathbb{N}^0$ and hence the divisibility of $(5^n - 5)$ by 3 is determined by the divisibility of 10 by 3. However, $3 \not| 10$ and hence $3 \not| (5^n - 5)$ for any even $n \in \mathbb{N}^0$.
(**f**) $5|(7^n - 3)$ means $7^n \overset{5}{=} 3$. Now, we have $7^4 \overset{5}{=} 1$ and hence $7^{4k} \overset{5}{=} 1$ ($k \in \mathbb{N}^0$; see rule 11 of § 2.7 noting that the congruence is valid even for $k = 0$). Also, the first $n \in \mathbb{N}^0$ to which $7^n \overset{5}{=} 3$ is $n = 3$, i.e. $7^3 \overset{5}{=} 3$. On multiplying these two congruences (i.e. $7^{4k} \overset{5}{=} 1$ and $7^3 \overset{5}{=} 3$) side by side (see rule 10 of § 2.7) we get: $7^{3+4k} \overset{5}{=} 3$, i.e. $5|(7^n - 3)$ for all $n = 3 + 4k$ ($k \in \mathbb{N}^0$).
(**g**) $7|(5^{2n+2} - 1)$ means $5^{2n+2} \overset{7}{=} 1$. Now, we have $5^6 \overset{7}{=} 1$ and hence $5^{6k} \overset{7}{=} 1$ ($k \in \mathbb{N}^0$; see rule 11 of § 2.7 noting that the congruence is valid even for $k = 0$). Also, the first $n \in \mathbb{N}$ to which $5^{2n+2} \overset{7}{=} 1$ is $n = 2$, i.e. $5^6 \overset{7}{=} 1$. On multiplying these two congruences (i.e. $5^{6k} \overset{7}{=} 1$ and $5^6 \overset{7}{=} 1$) side by side (see rule 10 of § 2.7) we get: $5^{6k+6} \overset{7}{=} 1$, i.e. $5^{2(3k+2)+2} \overset{7}{=} 1$. This means that $5^{2n+2} - 1 \overset{7}{=} 0$ for all $n = 2 + 3k$ ($k \in \mathbb{N}^0$ to include $n = 2$).

5. Show that the following are composite for all $m, n \in \mathbb{N}$:
(**a**) $31(41^n) - 175$. (**b**) $5^{2n} + 2$. (**c**) $19(105^m) - 46(308^n)$.
(**d**) $2^{2^{3n+1}} - 1$. (**e**) $3^{3^{2n-1}} + 38$.
Solution:

(**a**) By the rules of parity (see § 1.8) this is even (> 2) and hence it is composite for all $n \in \mathbb{N}$ (see point 3 in the preamble of § 2.2).
(**b**) We prove this by showing that $3|(5^{2n}+2)$ for all $n \in \mathbb{N}$ where we use induction.
For $n = 1$ we have $5^{2\times 1}+2 = 27$ which is divisible by 3. Now, we show that if $3|(5^{2n}+2)$ for a given $n \in \mathbb{N}$ then $3|(5^{2(n+1)}+2)$, that is:

$$5^{2(n+1)}+2 = 5^{2n+2}+2 = (25\times 5^{2n})+2 = (24\times 5^{2n})+(5^{2n}+2) = 3(8\times 5^{2n})+(5^{2n}+2)$$

As we see, 3 obviously divides $3(8\times 5^{2n})$, and 3 divides $(5^{2n}+2)$ by assumption. Therefore, by rule 14 of § 1.9, 3 divides their sum which is $(5^{2(n+1)}+2)$. So, by mathematical induction $3|(5^{2n}+2)$ for all $n \in \mathbb{N}$, i.e. $(5^{2n}+2)$ is composite for all $n \in \mathbb{N}$.
(**c**) We have:

$$19(105^m)-46(308^n) = 7\Big[19(105^{m-1}\times 15)-46(308^{n-1}\times 44)\Big]$$

i.e. it is divisible by 7 and hence it is composite for all $m, n \in \mathbb{N}$.
(**d**) We note that $2^{3n+1} \overset{16}{\equiv} 0$, i.e. $2^{3n+1} = 16k$ ($k \in \mathbb{N}$).[164] Accordingly:

$$\begin{aligned}
2^{16} &\overset{17}{\equiv} 1 && \text{(Fermat's little theorem; see § 2.9.3)}\\
2^{16k} &\overset{17}{\equiv} 1 && \text{(rule 11 of § 2.7)}\\
2^{2^{3n+1}} &\overset{17}{\equiv} 1 && (2^{3n+1} = 16k)\\
2^{2^{3n+1}}-1 &\overset{17}{\equiv} 0 && \text{(rule 3 of § 2.7)}
\end{aligned}$$

So, $(2^{2^{3n+1}}-1)$ is divisible by 17 and hence it is composite for all $n \in \mathbb{N}$.
(**e**) We note that $3^{2n-1} \overset{12}{\equiv} 3$, i.e. $3^{2n-1} = 12k+3$ ($k \in \mathbb{N}^0$).[165] Accordingly:

$$\begin{aligned}
3^{12} &\overset{13}{\equiv} 1 && \text{(Fermat's little theorem; see § 2.9.3)}\\
3^{12k} &\overset{13}{\equiv} 1 && \text{(rule 11 of § 2.7)}\\
3^{12k+3} &\overset{13}{\equiv} 3^3 && (\times 3^3)\\
3^{3^{2n-1}} &\overset{13}{\equiv} 27 && (3^{2n-1} = 12k+3)\\
3^{3^{2n-1}} &\overset{13}{\equiv} -38 && (27 \overset{13}{\equiv} -38)\\
3^{3^{2n-1}}+38 &\overset{13}{\equiv} 0 && \text{(rule 3 of § 2.7)}
\end{aligned}$$

So, $(3^{3^{2n-1}}+38)$ is divisible by 13 and hence it is composite for all $n \in \mathbb{N}$.

6.6 Divisibility of Numbers by Exponentials

This kind of problems are generally solved by equating the exponential to each one of the divisors of the number to see if there is a (non-negative integer) value of the exponent that satisfies the equation (as will be demonstrated in the following Problems).

Problems

---

[164] We have $2^{3n+1} = 2^4\times 2^{3n+1-4} = 2^4\times 2^{3n-3} = 16\times 2^{3n-3} \overset{16}{\equiv} 0$.

[165] $3^{2n-1} \overset{12}{\equiv} 3$ can be proved by induction as follows (noting that it is valid for $n = 1$ and assuming it is valid for some $n \in \mathbb{N}$):

$$3^{2(n+1)-1} = 3^{2n+1} = 9\times 3^{2n-1} \overset{12}{\equiv} 9\times 3 = 27 \overset{12}{\equiv} 3$$

where we used the induction assumption in step 3.

1. Find all $n \in \mathbb{N}^0$ such that:
   (**a**) $3^n|289$. (**b**) $5^n|250$. (**c**) $23^n|1058$. (**d**) $7^n|84035$.
   Solution:
   (**a**) The (positive) divisors of 289 are $1, 17, 289$.[166] If we equate each one of these divisors to 3^n we find that only $n = 0$ (corresponding to the divisor 1) satisfies this divisibility statement.
   (**b**) The (positive) divisors of 250 are $1, 2, 5, 10, 25, 50, 125, 250$. If we equate each one of these divisors to 5^n we find that only $n = 0, 1, 2, 3$ (corresponding to the divisors $1, 5, 25, 125$) satisfy this divisibility statement.
   (**c**) The (positive) divisors of 1058 are $1, 2, 23, 46, 529, 1058$. If we equate each one of these divisors to 23^n we find that only $n = 0, 1, 2$ (corresponding to the divisors $1, 23, 529$) satisfy this divisibility statement.
   (**d**) The (positive) divisors of 84035 are $1, 5, 7, 35, 49, 245, 343, 1715, 2401, 12005, 16807, 84035$. If we equate each one of these divisors to 7^n we find that only $n = 0, 1, 2, 3, 4, 5$ (corresponding to the divisors 1, 7, 49, 343, 2401, 16807) satisfy this divisibility statement.

6.7 Divisibility of Exponentials by Exponentials

This type of problems can be tackled (depending on the type of problem) by using prime factorization (to see if the dividend contains enough prime factors to cancel the divisor), or by using the rules of exponents (associated with the familiar rules of divisibility), or by other similar approaches. Some of these methods will be demonstrated in the following Problems (using very simple examples).

Problems

1. Which of the following statements is true (where $m, n \in \mathbb{N}$):
   (**a**) $161^n|907235^n$. (**b**) $9^n|726^n$. (**c**) $5^n|24565^m$.
   Solution:
   (**a**) This is true because:

$$\frac{907235^n}{161^n} = \left(\frac{5 \times 7^3 \times 23^2}{7 \times 23}\right)^n = \left(5 \times 7^2 \times 23\right)^n = 5635^n \quad \text{which is an integer.}$$

   (**b**) This is untrue because:

$$\frac{726^n}{9^n} = \left(\frac{726}{9}\right)^n = \left(\frac{2 \times 3 \times 11^2}{3^2}\right)^n = \left(\frac{2 \times 11^2}{3}\right)^n \quad \text{which is not an integer.}$$

   (**c**) This is true for $m \geq n$ and untrue for $m < n$ because:

$$\frac{24565^m}{5^n} = \frac{(5 \times 17^3)^m}{5^n} = \frac{5^m \times 17^{3m}}{5^n} = 5^{m-n} \times 17^{3m} \quad \text{which is an integer only if } m \geq n.$$

2. Prove the following (where $n \in \mathbb{N}$):
   (**a**) $14^n|(154^n - 126^n)$. (**b**) $(3^n + 1)|(24^n + 8^n)$. (**c**) $(7^n + 5^n - 2^n)|(63^n + 45^n - 18^n)$.
   Solution:
   (**a**) $154^n - 126^n = (11^n \times 14^n) - (9^n \times 14^n) = 14^n(11^n - 9^n)$.
   (**b**) $24^n + 8^n = (3 \times 8)^n + 8^n = (3^n \times 8^n) + 8^n = 8^n(3^n + 1)$.
   (**c**) $63^n + 45^n - 18^n = (7^n \times 9^n) + (5^n \times 9^n) - (2^n \times 9^n) = 9^n(7^n + 5^n - 2^n)$.
3. Find all $m, n \in \mathbb{N}^0$ such that:
   (**a**) $8^n|10^{3n}$. (**b**) $6^m|(13^n - 8)$.
   Solution:

[166] We consider only positive divisors because 3^n is positive. This similarly applies to the other parts of this Problem.

(**a**) $8^n|10^{3n}$ means $10^{3n} = k8^n$ ($k \in \mathbb{N}$), that is:

$$10^{3n} = k8^n \qquad \rightarrow \qquad \frac{10^{3n}}{8^n} = k \qquad \rightarrow \qquad \left(\frac{10^3}{8}\right)^n = k \qquad \rightarrow \qquad 125^n = k$$

As we see, $125^n = k$ ($k \in \mathbb{N}$) for all $n \in \mathbb{N}^0$. So, $8^n|10^{3n}$ for all $n \in \mathbb{N}^0$.
(**b**) We have two cases to consider:
• $m = 0$, i.e. $1|(13^n - 8)$ which is true.
• $m > 0$, i.e. $6^m|(13^n - 8)$ which is untrue because 6^m is even while $(13^n - 8)$ is odd, and no odd number is divisible by an even number (see the parity rules in § 1.8).
So, $6^m|(13^n - 8)$ for all $(m, n) = (0, k)$ where $k \in \mathbb{N}^0$.

4. Show that $2^{k+2}|(3^{2^k} - 1)$ but $2^{k+3} \not| (3^{2^k} - 1)$ where $k \in \mathbb{N}$.
Solution: We prove this by induction. For $k = 1$ we have $2^{1+2}|(3^{2^1} - 1)$ but $2^{1+3} \not| (3^{2^1} - 1)$. Now, let assume that $2^{k+2}|(3^{2^k} - 1)$ but $2^{k+3} \not| (3^{2^k} - 1)$ for a given $k \in \mathbb{N}$ and hence $(3^{2^k} - 1) = 2^{k+2}q$ where q is odd.[167] Accordingly:

$$3^{2^{k+1}} - 1 = 3^{2^k \times 2} - 1 = \left(3^{2^k}\right)^2 - 1 = (3^{2^k} - 1)(3^{2^k} + 1) = 2^{k+2}q\,(3^{2^k} + 1) \tag{82}$$

Now:

$$3^{2^k} + 1 = (3^{2^k} - 1) + 2 = \left(2^{k+2}q\right) + 2 = 2(2^{k+1}q + 1) = 2r$$

Now, since $(2^{k+1}q + 1)$ is odd (see parity rules in § 1.8) then r is odd and hence from Eq. 82 we get:

$$3^{2^{k+1}} - 1 = 2^{k+2}q\,(3^{2^k} + 1) = 2^{k+2}q \times 2r = 2^{k+3}qr = 2^{(k+1)+2}qr$$

Now, qr is odd (because q and r are odd) and hence $2^{(k+1)+2}|(3^{2^{k+1}} - 1)$ but $2^{(k+1)+3} \not| (3^{2^{k+1}} - 1)$. So, by mathematical induction $2^{k+2}|(3^{2^k} - 1)$ but $2^{k+3} \not| (3^{2^k} - 1)$ for all $k \in \mathbb{N}$.

5. Find all $m, n \in \mathbb{N}^0$ such that: $2^m|(3^n - 1)$.
Solution: We consider the following three cases:
(**a**) If $n = 0$ then $2^m|(3^n - 1)$ for all $m \in \mathbb{N}^0$. This is because $2^m|(3^0 - 1) = 0$ for all $m \in \mathbb{N}^0$ (see rule 1 of § 1.9).
(**b**) If n is odd then $2^m|(3^n - 1)$ for $m = 0, 1$ only. This is because (see Eq 12):

$$3^n - 1 = (3 - 1)(3^{n-1} + 3^{n-2} + \cdots + 3 + 1) = 2(3^{n-1} + 3^{n-2} + \cdots + 3 + 1)$$

Now, since n is odd then $(3^{n-1} + 3^{n-2} + \cdots + 3 + 1)$ is odd (because it is a sum of n odd terms) and hence $(3^n - 1)$ contains a single factor of 2 which makes it divisible only by 2^0 and 2^1.
(**c**) If n ($\neq 0$) is even then we have $n = 2^k q$ ($k \in \mathbb{N}$ and $q \in \mathbb{O}$, i.e. $q = 1, 3, \ldots$) and hence (see Eq. 12):

$$3^n - 1 = 3^{2^k q} - 1 = \left(3^{2^k}\right)^q - 1 = \left(3^{2^k} - 1\right)\left[\left(3^{2^k}\right)^{q-1} + \left(3^{2^k}\right)^{q-2} + \cdots + 3^{2^k} + 1\right]$$

Now, the expression in the square brackets is odd (because it is a sum of q odd terms noting that q is odd). Moreover, from Problem 4 we have: $2^{k+2}|(3^{2^k} - 1)$ but $2^{k+3} \not| (3^{2^k} - 1)$. So, in this case we have: $2^m|(3^n - 1)$ for $m = 0, 1, \ldots, (k + 2)$ only.

6. Show that $(k^m - 1)|(k^n - 1)$ *iff* $m|n$ (where $m, n, k \in \mathbb{N}$ and $k > 1$).
Solution: Regrading **the if part**, if $m|n$ then $n = qm$ ($q \in \mathbb{N}$) and hence:

$$k^n - 1 = k^{qm} - 1 = (k^m)^q - 1 = (k^m - 1)\left[(k^m)^{q-1} + (k^m)^{q-2} + \cdots + k^m + 1\right]$$

where we used Eq. 12 in the last equality. So, $(k^m - 1)|(k^n - 1)$ as required.
Regrading **the only if part**, let $n = qm + r$ ($q \in \mathbb{N}$, $r \in \mathbb{N}^0$, $r < m$)[168] and hence:

$$k^n - 1 = (k^n - k^r) + (k^r - 1) \qquad (\mp k^r)$$

[167] q is odd because otherwise $2^{k+3}|(3^{2^k} - 1)$ which contradicts our assumption.
[168] We are assuming $m \leq n$ because $(k^m - 1)|(k^n - 1)$.

$$k^n - 1 = k^r(k^{n-r} - 1) + (k^r - 1)$$
$$k^n - 1 = k^r(k^{qm} - 1) + (k^r - 1) \qquad (n = qm + r)$$
$$(k^n - 1) - k^r(k^{qm} - 1) = (k^r - 1)$$

Now, by assumption we have $(k^m - 1)|(k^n - 1)$. Also, form the "if part" we have $(k^m - 1)|(k^{qm} - 1)$ because $m|(qm)$. Hence, by rule 14 of § 1.9 we must have $(k^m - 1)|(k^r - 1)$. However, since $r < m$ we must have $(k^r - 1) = 0$ and hence $r = 0$, i.e. $n = qm$ which means $m|n$ as required.

6.8 Divisibility of Exponentials by Polynomials

There is no general approach for tackling this type of problems and hence the method of solution depends on the specifications of the problem. However, it is useful to keep in mind the general rules of number theory such as the rules of parity (as well as the general rules of divisibility) when tackling this type of problems. In the following Problems we present a tiny sample of very simple examples of this type of problems.

Problems

1. Find all $n \in \mathbb{N}^0$ such that:
   (**a**) $(n^3 + 4n^2 - n + 2)|11^{2n+3}$. (**b**) $(n-1)|3^n$. (**c**) $(3n-5)|5^{2n-4}$. (**d**) $n^2|\,[(n+1)^n - 1]$.

   Solution:
   (**a**) $(n^3 + 4n^2 - n + 2)$ is even while 11^{2n+3} is odd for all $n \in \mathbb{N}^0$ and hence there is no $n \in \mathbb{N}^0$ that satisfies the given divisibility statement (see the rules of parity in § 1.8).
   (**b**) For $(n-1)$ to divide 3^n it must be a power of 3, that is:

$$n - 1 = 3^k \qquad \rightarrow \qquad n = 3^k + 1 \qquad (k \in \mathbb{N}^0)$$

   We also note that $(n-1)|3^n$ for $n = 0$.
   So, $(n-1)|3^n$ for all $n = 3^k + 1$ $(k \in \mathbb{N}^0)$ as well as for $n = 0$.
   (**c**) For $(3n-5)$ to divide 5^{2n-4} it must be a power of 5, that is:

$$3n - 5 = 5^k \qquad \rightarrow \qquad n = \frac{5^k + 5}{3} \qquad (k \in \mathbb{N}^0, k \in \mathbb{E})$$

   where the condition $k \in \mathbb{E}$ is justified by the result of part (d) of Problem 4 of § 6.5. So, $(3n-5)|5^{2n-4}$ for all $n = (5^k + 5)/3$ $(k \in \mathbb{N}^0, k \in \mathbb{E})$.
   (**d**) This divisibility relation is valid for $n = 0$ if we accept $0|0$.
   This divisibility relation is obviously valid for $n = 1$.
   This divisibility relation is also valid for all $n > 1$ because:

$$(n+1)^n = C_0^n + C_1^n n + C_2^n n^2 + \cdots + C_n^n n^n \qquad \text{(Eq. 13)}$$
$$(n+1)^n = 1 + n^2 + C_2^n n^2 + \cdots + C_n^n n^n \qquad (C_0^n = 1, C_1^n = n)$$
$$(n+1)^n - 1 = n^2 + C_2^n n^2 + \cdots + C_n^n n^n$$
$$(n+1)^n - 1 = n^2\left[1 + C_2^n + \cdots + C_n^n n^{n-2}\right]$$

   So, $n^2|\,[(n+1)^n - 1]$ for all $n \in \mathbb{N}^0$ (if we accept $0|0$) or for all $n \in \mathbb{N}$ (if we do not accept $0|0$).
2. Find all $m \in \mathbb{Z}$ and $n \in \mathbb{N}^0$ such that:
   (**a**) $(m^3 + 4m^2 - m + 2)|11^{2n+3}$. (**b**) $(m-1)|3^n$. (**c**) $(3m-5)|5^{2n-4}$.

   Solution: We note that these are the same as parts (a, b, c) of Problem 1 but with n in the polynomial (i.e. the divisor) being replaced by m.
   (**a**) $(m^3 + 4m^2 - m + 2)$ is even for all $m \in \mathbb{Z}$ and 11^{2n+3} is odd for all $n \in \mathbb{N}^0$ and hence there is no $m \in \mathbb{Z}$ and $n \in \mathbb{N}^0$ that satisfy the given divisibility statement (see the rules of parity in § 1.8).
   (**b**) For $(m-1)$ to divide 3^n it must be a divisor of 3^n. Now, the divisors of 3^n are $\pm 3^k$ $(0 \le k \le n)$.

So, $(m-1)|3^n$ for all $(m-1)=\pm 3^k$, i.e. $m=1\pm 3^k$ where $0\le k\le n$ and $n\in\mathbb{N}^0$.
(**c**) We must have $n\ge 2$ because 5^{2n-4} must be an integer. For $(3m-5)$ to divide 5^{2n-4} it must be a divisor of 5^{2n-4}. Now, the divisors of 5^{2n-4} are $\pm 5^k$ where $0\le k\le(2n-4)$. So, $(3m-5)|5^{2n-4}$ for $(3m-5)=\pm 5^k$, i.e. $m=(5\pm 5^k)/3$ where $0\le k\le(2n-4)$ and $n\ge 2$. However, since m must be an integer we must impose a condition to ensure this. This condition is: $m=(5+5^k)/3$ for even k and $m=(5-5^k)/3$ for odd k (see parts d and e of Problem 4 of § 6.5). So, $(3m-5)|5^{2n-4}$ for all $m=(5+5^k)/3$ (k is even) and for all $m=(5-5^k)/3$ (k is odd) where $0\le k\le(2n-4)$ and $n\ge 2$.

6.9 Divisibility of Polynomials by Exponentials

In this type of problems the magnitude of the exponential usually exceeds the magnitude of the polynomial very quickly as the variable increases and hence we normally have very few values (which are near zero) of the variable that satisfy the divisibility relation. However, we should also consider the roots of the polynomial (which could be of any magnitude) because 0 is divisible by any other integer. In the following Problems we present a few simple examples of this type of problems.

Problems

1. Find all $n\in\mathbb{N}^0$ such that:
   (**a**) $5^n|(n-2)^7$. (**b**) $3^n|(n^3-49n^2+704n-2420)$. (**c**) $(7^n-1)|(n^2-6876n+10191668)$.
   Solution:
   (**a**) For $(n-2)^7$ to be divisible by 5^n, $(n-2)^7$ must be a power of multiple of 5 such that $5^n\le(n-2)^7$, that is:
   $$n-2=5k \quad\rightarrow\quad n=5k+2 \qquad (\text{for some } k\in\mathbb{N}^0)$$
   On considering $n=2,7,\ldots$ we see that only $n=2$ and $n=7$ (corresponding to $k=0$ and $k=1$) are acceptable because for n corresponding to $k\ge 2$ (i.e. $n=12,17,\ldots$) we have $5^n>(n-2)^7$ and hence 5^n cannot divide $(n-2)^7$. We also note that $5^n|(n-2)^7$ for $n=0$.
   So, $5^n|(n-2)^7$ only for $n=0,2,7$.
   (**b**) We note that for $n>4$ the magnitude of 3^n is greater than the magnitude of $(n^3-49n^2+704n-2420)$ and hence 3^n cannot divide $(n^3-49n^2+704n-2420)$. So, all we need to do is to test the values $n=0,1,2,3,4$. On testing these values we find that only $n=0,1,4$ are acceptable.
   However, we should also note that $n=5$ and $n=22$ [which are the roots of the polynomial since $(n^3-49n^2+704n-2420)=(n-5)(n-22)^2$] also satisfy the given divisibility relation because $3^n|0$.
   So, $3^n|(n^3-49n^2+704n-2420)$ only for $n=0,1,4,5,22$.
   (**c**) We note the following:
   • $n=0$ is not acceptable because the divisor cannot be 0.
   • For $n>8$ the magnitude of (7^n-1) is greater than the magnitude of $(n^2-6876n+10191668)$ and hence we need to test only the values $n=1,2,\ldots,8$. On testing these values we find that only $n=2$ is acceptable.
   • $n^2-6876n+10191668=(n-2162)(n-4714)$ and hence $n=2162$ and $n=4714$ also satisfy this divisibility relation because $(7^n-1)|0$.
   So, $(7^n-1)|(n^2-6876n+10191668)$ only for $n=2,2162,4714$.
2. Find all $m\in\mathbb{N}^0$ and $n\in\mathbb{Z}$ such that $5^m|(n-2)^7$.
   Solution: We consider the following three cases:
   • For $m=0$ the statement is valid for all $n\in\mathbb{Z}$ because 1 divides any integer.
   • For $n=2$ the statement is valid for all $m\in\mathbb{N}^0$ because 0 is divisible by any other integer.
   • For $m>0$ and $n\ne 2$, $5^m|(n-2)^7$ when the prime factorization of $|n-2|$ contains 5, i.e. $(n-2)=5^s t$ where $s\in\mathbb{N}$, $t\in\mathbb{Z}$ and t is not a multiple of 5. Accordingly, $(n-2)^7=5^{7s}T$ $(T=t^7)$ and hence $5^m|(n-2)^7$ for all $1\le m\le 7s$. So in brief, $5^m|(n-2)^7$ for all $1\le m\le 7s$ where $n=2+5^s t$.[169]

[169] For example, when $n=77=2+75=2+(5^2\times 3)$ then $s=2$ and hence $5^m|(n-2)^7$ for all $1\le m\le 14$. On the other hand, if $n=76=2+74=2+(5^0\times 74)$ then $s=0$ and hence $5^m\not|(n-2)^7$ for any $m>0$.

6.10 Divisibility of Mixed Polynomials-Exponentials by Numbers

We mean by "mixed polynomials-exponentials" expressions like $(5n-3^n)$ which contain polynomial terms and exponential terms.[170] The solution of this type of problems is usually more difficult than the solution of problems involving polynomials only or exponentials only (noting that a typical method of solution for this type of problems is induction). In the following Problems we present a few simple examples of this type of divisibility problems in which the polynomials are linear.

Problems

1. Show that $4|(5^n-3^n+2n)$ for all $n\in\mathbb{N}^0$.
   Solution: We use induction. For $n=0$ we have $4|(5^0-3^0+0)=0$. Assuming $4|(5^k-3^k+2k)$ for some $k\in\mathbb{N}$, we have:

$$\begin{aligned} 5^{k+1}-3^{k+1}+2(k+1) &= (5\times 5^k)-(3\times 3^k)+2(k+1)\\ &= (4\times 5^k)+5^k-(2\times 3^k)-3^k+2k+2\\ &= (4\times 5^k)-2(3^k-1)+(5^k-3^k+2k)\end{aligned}$$

   Now, (4×5^k) is obviously divisible by 4 and $2(3^k-1)$ is also divisible by 4 $\big[$because 3^k is odd and hence (3^k-1) is even and thus $2(3^k-1)$ is divisible by $4\big]$. Moreover, we assumed (5^k-3^k+2k) is divisible by 4. Therefore, their algebraic sum must be divisible by 4 (see rule 14 of § 1.9). So, by induction $4|(5^n-3^n+2n)$ for all $n\in\mathbb{N}^0$.
2. Find all $n\in\mathbb{N}^0$ such that:
   (**a**) $18|(3^{n+4}+36n-9)$. (**b**) $35|(70n-7^n+28)$. (**c**) $49|(5^{2n+2}-14n-15)$.
   Solution:
   (**a**) If $(3^{n+4}+36n-9)$ is divisible by 18 then it must be divisible by 2 and 9 (see rule 20 of § 1.9). Now, $(3^{n+4}+36n-9)$ is even (see parity rules in § 1.8) and hence it is divisible by 2 for any $n\in\mathbb{N}^0$. Also, all the terms of $(3^{n+4}+36n-9)$ are divisible by 9 and hence $(3^{n+4}+36n-9)$ is divisible by 9 for any $n\in\mathbb{N}^0$. So, $(3^{n+4}+36n-9)$ is divisible by their product (i.e. $18=2\times 9$) for any $n\in\mathbb{N}^0$, i.e. $18|(3^{n+4}+36n-9)$ for all $n\in\mathbb{N}^0$.
   (**b**) If $(70n-7^n+28)$ is divisible by 35 then it must be divisible by 5 and 7 (see rule 20 of § 1.9). Now, all the terms of $(70n-7^n+28)$ are divisible by 7 and hence $(70n-7^n+28)$ is divisible by 7 for any $n\in\mathbb{N}$. Also, $70n$ is divisible by 5 for any $n\in\mathbb{N}^0$ and hence if $(70n-7^n+28)$ should be divisible by 5 then (-7^n+28) must be divisible by 5 (see rule 16 of § 1.9), that is: $-7^n+28\overset{5}{=}0$, i.e. $7^n\overset{5}{=}3$. Now, $7^n\overset{5}{=}3$ for all $n=3+4k$ where $k\in\mathbb{N}^0$ (see part f of Problem 4 of § 6.5). Hence, $(70n-7^n+28)$ is divisible by 5 for all $n=3+4k$. Accordingly, $(70n-7^n+28)$ is divisible by 35 $(=5\times 7)$ for all $n=3+4k$ $(k\in\mathbb{N}^0)$.
   (**c**) $49|(5^{2n+2}-14n-15)$ is equivalent to $5^{2n+2}-14n-15\overset{49}{=}0$. Now, if we test the first few values of $n\in\mathbb{N}^0$ we find $n=2$ and $n=5$ satisfy this congruence relation. This may suggest that this is true for all $n=2+3k$ $(k\in\mathbb{N}^0)$ and that is what we will try to establish (by induction). So, let assume that $49|(5^{2n+2}-14n-15)$ for a given $n=2+3k$ (such as 2 and 5) and we will show that if this is the case then this divisibility statement is valid for $2+3(k+1)=n+3$, that is (noting that the given assumption is equivalent to $5^{2n+2}\overset{49}{=}14n+15$):

$$\begin{aligned} 5^{2n+2} &\overset{7}{=} 1 && \text{(part g of Problem 4 of § 6.5)}\\ 5^{2n+2}(2232) &\overset{7}{=} 2232 && (\times 2232;\ \text{rule 6 of § 2.7})\\ 5^{2n+2}(2232) &\overset{7}{=} 6 && (2232\overset{7}{=}6)\\ 5^{2n+2}(15624) &\overset{49}{=} 42 && (\times 7;\ \text{rule 9 of § 2.7})\\ 5^{2n+2}(15624)-42 &\overset{49}{=} 0 && \text{(rule 3 of § 2.7)}\end{aligned}$$

[170] In fact, we deal in some of the following Problems with expressions not exactly like this.

$$\begin{aligned} 5^{2n+2}(5^6-1)-42 &\overset{49}{=} 0 && (15624 = 5^6-1)\\ 5^{2(n+3)+2}-\left[5^{2n+2}\right]-42 &\overset{49}{=} 0 &&\\ 5^{2(n+3)+2}-\left[14n+15\right]-42 &\overset{49}{=} 0 && (\text{the given assumption})\\ 5^{2(n+3)+2}-14(n+3)-15 &\overset{49}{=} 0 && \end{aligned}$$

As we see, the given divisibility statement is valid for $n+3 = 2+3(k+1)$ when it is valid for $n = 2+3k$ and hence by induction it is valid for all $n = 2+3k$ ($k \in \mathbb{N}^0$).
We finally note that this divisibility statement is not valid for $n = 3k$ because for $k = 0$ we have $5^{0+2}-14(0)-15 = 10$ which is not divisible by 49 while for $k > 0$ we have:

$$\begin{aligned} 5^{2n+2}-14n-15 &= 5^{2(3k)+2}-14(3k)-15 = 5^{2(3k-3+2)+2}\,5^2-14(3k-3+2)-14-15\\ &= 5^{2(3[k-1]+2)+2}\,5^2-14(3[k-1]+2)-14-15\\ &= \left[5^{2(3[k-1]+2)+2}-14(3[k-1]+2)-15\right]+\left[(5^2-1)5^{2(3[k-1]+2)+2}-14\right]\\ &= \left[5^{2n'+2}-14n'-15\right]+\left[(24)5^{2n'+2}-14\right] \equiv A+B \end{aligned}$$

Now, A is divisible by 49 (because n' is of the form $3k'+2$) and hence the divisibility of $(5^{2n+2}-14n-15)$ by 49 is determined by the divisibility of B by 49. However, for B to be divisible by 49 it must be divisible by 7, but B is not divisible by 7 because 14 is divisible by 7 but $(24)5^{2n'+2}$ is not since it does not contain a factor of 7. Therefore, $A+B$ is not divisible by 49, i.e. $49 \not| (5^{2n+2}-14n-15)$ when $n = 3k$.
Similarly, this divisibility statement is not valid for $n = 1+3k$ because for $k = 0$ we have $5^{2+2}-14(1)-15 = 596$ which is not divisible by 49 while for $k > 0$ we have:

$$\begin{aligned} 5^{2n+2}-14n-15 &= 5^{2(1+3k)+2}-14(1+3k)-15 = 5^{2(3k-3+2)+2}\,5^4-14(3k-3+2)-28-15\\ &= 5^{2(3[k-1]+2)+2}\,5^4-14(3[k-1]+2)-28-15\\ &= \left[5^{2(3[k-1]+2)+2}-14(3[k-1]+2)-15\right]+\left[(5^4-1)5^{2(3[k-1]+2)+2}-28\right]\\ &= \left[5^{2n'+2}-14n'-15\right]+\left[(624)5^{2n'+2}-28\right] \equiv A+B \end{aligned}$$

Now, A is divisible by 49 (because n' is of the form $3k'+2$) and hence the divisibility of $(5^{2n+2}-14n-15)$ by 49 is determined by the divisibility of B by 49. However, for B to be divisible by 49 it must be divisible by 7, but B is not divisible by 7 because 28 is divisible by 7 but $(624)5^{2n'+2}$ is not since it does not contain a factor of 7. Therefore, $A+B$ is not divisible by 49, i.e. $49 \not| (5^{2n+2}-14n-15)$ when $n = 1+3k$.
So in brief, $49|(5^{2n+2}-14n-15)$ for all $n = 2+3k$ ($k \in \mathbb{N}^0$) but not for any n of different forms (i.e. $n = 3k$ and $n = 1+3k$).

3. Show that the following is composite for all $m, n \in \mathbb{N}$: $(2m)^{2n+1}+1$.
Solution: $(2m)^{2n+1}+1 = (2m)^{2n+1}+1^{2n+1}$ and hence by Eq. 11 (noting that $2n+1 = 3, 5, \ldots$) we have:
$$(2m)^{2n+1}+1 = (2m+1)\left[(2m)^{2n}-(2m)^{2n-1}+\cdots-(2m)+1\right]$$
i.e. it is a product of two factors (both of which are integers greater than 1) and hence it is composite for all $m, n \in \mathbb{N}$.
4. Show that $p|(m^{n(p-1)+1}-m)$ (where $m \in \mathbb{Z}$, $n \in \mathbb{N}^0$, and $p \in \mathbb{P}$).
Solution: If $p \not| m$ then from Fermat's little theorem (see § 2.9.3) we have:
$$m^{p-1} \overset{p}{=} 1 \qquad \rightarrow \qquad m^{n(p-1)} \overset{p}{=} 1 \qquad \rightarrow \qquad m^{n(p-1)+1} \overset{p}{=} m$$
where in step 2 we raised both sides to power n (see rule 11 of § 2.7), and in step 3 we multiplied both sides by m (see rule 6 of § 2.7).

If $p|m$ then we have:

$$m \stackrel{p}{=} 0 \qquad \rightarrow \qquad m^{n(p-1)+1} \stackrel{p}{=} 0 \qquad \rightarrow \qquad m^{n(p-1)+1} \stackrel{p}{=} m$$

where in step 2 we raised both sides to power $n(p-1)+1$ (see rule 11 of § 2.7), and in step 3 we compared the two previous congruences.
So, in both cases we have $m^{n(p-1)+1} \stackrel{p}{=} m$ which is equivalent to $p|(m^{n(p-1)+1} - m)$.

6.11 Divisibility of Factorials

In this type of problems we usually use some general and basic divisibility rules (and guidelines) related to factorials. The following are some of these rules (where $m, n \in \mathbb{N}$ and $p \in \mathbb{P}$):[171]
1. $0 < m \leq n \ \rightarrow \ m|n!$. This is because m is a factor of $n!$.
2. $0 \leq m \leq n \ \rightarrow \ m!|n!$. This is because $m!$ is a factor of $n!$.
3. $m|n!$ and $k > n \ \rightarrow \ m|k!$. This is because $n!$ is a factor of $k!$.
4. $p > n \ \rightarrow \ p \not| n!$. This is because p cannot be a factor of $n!$.
5. $m|n \ \rightarrow \ m|n!$. This is because n is a factor of $n!$.
6. It is useful to keep Wilson's theorem (see § 2.9.1) in mind when dealing with factorial divisibility problems.

It is noteworthy that this section is about divisibility problems involving factorials and hence it includes different types of divisibility problems, e.g. divisibility of factorials by numbers or by factorials. It may also include some problems which are not explicitly about divisibility. So in brief, the following Problems deal (possibly implicitly) with divisibility of mathematical expressions involving factorials but not necessarily about the divisibility of factorials directly and explicitly.

Problems

1. Show that the highest power s of a prime p that divides $n!$ is given by the formula:

$$s = \sum_i \text{floor}\left(\frac{n}{p^i}\right) \qquad (i = 1, 2, \ldots) \tag{83}$$

where floor is the floor function.
Solution: Let us consider the following cases:
• $n < p$: in this case no factor of $n!$ (i.e. $1, 2, \ldots, n$) contains a factor of p and hence the formula of Eq. 83 should produce $s = 0 + 0 + \cdots = 0$ as it should be.
• $p^1 \leq n < p^2$: in this case if any factor of $n!$ contains p (i.e. in its prime factorization) then it should contain only p^1 (because $n < p^2$). This means that $n!$ contains only factors which are multiples of p^1 but not factors which are multiples of higher powers of p. Now, the number of factors of $n!$ which are multiples of p^1 should be $\text{floor}(n/p^1)$ and hence the formula of Eq. 83 should produce:

$$s = \text{floor}\left(\frac{n}{p^1}\right) + 0 + \cdots = \text{floor}\left(\frac{n}{p^1}\right)$$

This is exactly the number of factors of p in $n!$ since the product of all factors of $n!$ should contain only this number of p^1 factors (i.e. p^s).[172] So, the formula of Eq. 83 is correct.
• $p^2 \leq n < p^3$: in this case if any factor of $n!$ contains p (i.e. in its prime factorization) then it should contain only p^1 or p^2 (because $n < p^3$). This means that $n!$ contains only factors which are multiples of p^1 and factors which are multiples of p^2 but not factors which are multiples of higher powers of p. Now,

[171] We note that most of these rules are trivial and hence they are stated here as reminder and reference (especially for novice readers).

[172] If $p^1 \leq n < p^2$ then by the division algorithm (see § 2.3.2) we have $n = sp + r$ and hence:

$$n! = 1 \times 2 \times \ldots \times (1p) \times \ldots \times (2p) \times \ldots \times (3p) \times \ldots \times (sp) \times \ldots \times (n-1) \times n$$

So, in this product we have s factors of p.

the number of factors of $n!$ which are multiples of p^1 should be $\text{floor}(n/p^1)$ (as shown in the previous point), while the number of factors of $n!$ which are multiples of p^2 should be $\text{floor}(n/p^2)$ (by a similar argument to the argument of the previous point). Hence, the formula of Eq. 83 should produce:

$$s = \text{floor}\left(\frac{n}{p^1}\right) + \text{floor}\left(\frac{n}{p^2}\right) + 0 + \cdots = \text{floor}\left(\frac{n}{p^1}\right) + \text{floor}\left(\frac{n}{p^2}\right)$$

This is exactly the number of factors of p in $n!$ since the product of all factors of $n!$ should contain only this number of p^1 and p^2 factors (i.e. p^s). So, the formula of Eq. 83 is correct.
It is important to note that the factors of $n!$ which are multiples of p^2 contain two factors of p each and hence it may be thought that in this case we should have:

$$s = \text{floor}\left(\frac{n}{p^1}\right) + 2\,\text{floor}\left(\frac{n}{p^2}\right)$$

However, this is not the case because although the factors of $n!$ which are multiples of p^2 contain two factors of p each, one of their factors is already accounted for by $\text{floor}(n/p^1)$ because a factor that is a multiple of p^2 is also a multiples of p^1 and hence it is already counted by $\text{floor}(n/p^1)$. So, each factor that is a multiple of p^2 contributes only one extra p, i.e. it contributes an extra factor of p^1 and not an extra factor of p^2. This also applies (by the same logic) to the following cases (or stages) where each new factor that is a multiple of p^i contributes an extra factor of p^1 and not an extra factor of p^i because p^{i-1} of its factors have already been counted in the previous stages.
Now, let us consider the next case in more general terms, that is:
• $p^i \leq n < p^{i+1}$: in this case we just repeat the argument in the previous point (where i here corresponds to 2 there, and $i+1$ here corresponds to 3 there), and hence we get:

$$s = \text{floor}\left(\frac{n}{p^1}\right) + \text{floor}\left(\frac{n}{p^2}\right) + \cdots + \text{floor}\left(\frac{n}{p^i}\right) + 0 + \cdots = \text{floor}\left(\frac{n}{p^1}\right) + \text{floor}\left(\frac{n}{p^2}\right) + \cdots + \text{floor}\left(\frac{n}{p^i}\right)$$

which is exactly the number of factors of p in $n!$ (in accord with the formula of Eq. 83).
So, we conclude that the formula of Eq. 83 is correct in all cases (which establishes its general validity, as required; see point 7 of § 1.5.4).

2. Show that the number of trailing zeros in $n!$ is given by the formula:

$$m = \sum_i \text{floor}\left(\frac{n}{5^i}\right) \qquad (i = 1, 2, \ldots) \tag{84}$$

where m is the number of trailing zeros in $n!$ and floor is the floor function.
Solution: Every trailing zero in $n!$ represents a factor of 10 (i.e. 2×5) in the prime factorization of $n!$. Now, if we note that every factor of 5 in $n!$ must be preceded by a factor of 2 (or rather more than one factor of 2) in $n!$ then we can conclude that the number of factors of 10 (i.e. 2×5) in $n!$ is the same as the number of factors of 5 in $n!$.[173] Now, if we use the formula of Eq. 83 to find the number of factors of 5 in $n!$ then this same formula should give us the number of factors of 10 in $n!$. This means that Eq. 84 is no more than an application (or "misuse") of Eq. 83 to find the number of factors of 10 in $n!$ through finding the number of factors of 5 in $n!$ where we exploit the fact that (at least) one factor of 2 must associate each factor of 5 in $n!$.

3. Find the highest power s such that:
(**a**) $7^s|44!$. (**b**) $11^s|561!$. (**c**) $37^s|258!$. (**d**) $59^s|72!$. (**e**) $101^s|429!$.
Solution: Using Eq. 83 we get:
(**a**) 6. (**b**) 55. (**c**) 6. (**d**) 1. (**e**) 4.

[173] We note here that the number of factors of 10 (which is the same as the number of trailing zeros) in a given integer k is the minimum of the exponents of 2 and 5 in the prime factorization of k.

4. Find the lowest n such that:
   (**a**) $3^8|n!$. (**b**) $17^5|n!$. (**c**) $53^{12}|n!$. (**d**) $89^6|n!$. (**e**) $131^{21}|n!$.
   Solution: On trying $n = 2, 3, \ldots$ (using Eq. 83) we get:[174]
   (**a**) $n = 18$. (**b**) $n = 85$. (**c**) $n = 636$. (**d**) $n = 534$. (**e**) $n = 2751$.
5. Find the number of trailing zeros of the following factorials: 23!, 145!, 238!, 776!.
   Solution: Using Eq. 84 we get 4, 35, 57, 193 (respectively).
6. Find the minimum n for which $n!$ is divisible by (**a**) 10^4 (**b**) 10^{12}.
   Solution: To be divisible by 10^m the number must have at least m trailing zeros (see rule 48 of § 1.9). So, we use Eq. 84.[175]
   (**a**) For 10^4, m must be at least 4. It is obvious that in this case only the first term $\big[$i.e. floor$(n/5)\big]$ is needed to reach 4 and the minimum n that achieves this is 20. Hence, the minimum n for which $n!$ is divisible by 10^4 is 20.
   (**b**) For 10^{12}, m must be at least 12. It is obvious that in this case the first term is not enough and hence we need the second term as well $\big[$i.e. floor$(n/25)\big]$ to reach 12 and the minimum n that achieves this is 50. Hence, the minimum n for which $n!$ is divisible by 10^{12} is 50.
7. Show the following:
   (**a**) p divides $(p-2)!-1$ (p is prime). (**b**) p divides $2(p-3)!+1$ (p is odd prime).
   (**c**) p divides $4(p-3)!+2$ (p is odd prime). (**d**) $n!(n+1)!$ divides $(2n)!$.
   (**e**) $(n-1)!n!$ divides $(2n-2)!$. (**f**) 2^n divides $(2n)!$.
   (**g**) n divides $(n-1)!$ ($n \geq 6$ is composite). (**h**) $m|(n! \pm m)$ where $1 \leq m \leq n$.
   Solution:
   (**a**) From Wilson's theorem (see § 2.9.1) we have $(p-1)!+1 \stackrel{p}{=} 0$ that is:

$$\begin{aligned} (p-1)(p-2)!+1 &\stackrel{p}{=} 0 \\ (-1)(p-2)!+1 &\stackrel{p}{=} 0 && \Big[(p-1) \stackrel{p}{=} -1\Big] \\ (p-2)!-1 &\stackrel{p}{=} 0 && \Big[\times(-1)\Big] \end{aligned}$$

   i.e. p divides $(p-2)!-1$.
   (**b**) From Wilson's theorem (see § 2.9.1) we have $(p-1)!+1 \stackrel{p}{=} 0$ that is:

$$\begin{aligned} (p-1)(p-2)(p-3)!+1 &\stackrel{p}{=} 0 \\ (-1)(-2)(p-3)!+1 &\stackrel{p}{=} 0 && \Big[(p-1) \stackrel{p}{=} -1 \text{ and } (p-2) \stackrel{p}{=} -2\Big] \\ 2(p-3)!+1 &\stackrel{p}{=} 0 \end{aligned}$$

   i.e. p divides $2(p-3)!+1$.
   (**c**) We have $4(p-3)!+2 = 2\big[2(p-3)!+1\big]$. Now, according to part (b) p divides $2(p-3)!+1$. Hence, p divides $4(p-3)!+2$ (see rule 18 of § 1.9).
   (**d**) We have:

$$\frac{(2n)!}{n!(n+1)!} = \frac{1}{(n+1)}\left[\frac{(2n)!}{n!n!}\right] = \frac{1}{(n+1)}C_n^{2n}$$

   where we used Eq. 5 in the last step. So, to prove that $n!(n+1)!$ divides $(2n)!$ we need to prove that

[174] This sort of problems can be easily solved by using a spreadsheet or a simple computer code where the various values of n are tried consecutively and automatically. We may also use the result of Problem 8 (which generally requires less work).
[175] We may also use the result of Problem 8.

$C_n^{2n}/(n+1)$ is an integer, that is:[176]

$$\begin{aligned}
C_{n+1}^{2n} &= \frac{(2n)!}{(n+1)!(n-1)!} && \text{(Eq. 5)}\\
C_{n+1}^{2n} &= n\frac{(2n)!}{(n+1)!n!} && (\times n/n)\\
C_{n+1}^{2n} &= \frac{n}{(n+1)}\,\frac{(2n)!}{n!n!}\\
C_{n+1}^{2n} &= \frac{n}{(n+1)}\,C_n^{2n} && \text{(Eq. 5)}\\
C_{n+1}^{2n} &= \frac{n+1-1}{(n+1)}\,C_n^{2n} && (\pm 1)\\
C_{n+1}^{2n} &= \left[1-\frac{1}{(n+1)}\right]C_n^{2n}\\
C_{n+1}^{2n} &= C_n^{2n}-\frac{1}{(n+1)}C_n^{2n}\\
\frac{1}{(n+1)}C_n^{2n} &= C_n^{2n}-C_{n+1}^{2n}
\end{aligned}$$

Now, both C_n^{2n} and C_{n+1}^{2n} are integers (rule 26 of § 1.8) and so is their difference. Hence, $C_n^{2n}/(n+1)$ is an integer and thus $n!(n+1)!$ divides $(2n)!$.
(**e**) This is the same as part (d) with $(n-1)$ replacing n.
(**f**) We have:

$$\begin{aligned}
(2n)! &= 1\times 2\times 3\times 4\times\cdots\times(2n-1)\times(2n)\\
&= \Big[1\times 3\times\cdots\times(2n-1)\Big]\times\Big[2\times 4\times\cdots\times(2n)\Big]\\
&= \Big[1\times 3\times\cdots\times(2n-1)\Big]\times 2^n\Big[1\times 2\times\cdots\times n\Big]\\
&= 2^n n!\Big[1\times 3\times\cdots\times(2n-1)\Big]
\end{aligned}$$

As we see, 2^n is a factor of $(2n)!$ and hence 2^n divides $(2n)!$.
(**g**) Since n is composite then $n=mk$ ($m,k\in\mathbb{N}$ and $1<m,k<n$). Now, we have two (comprehensive and mutually exclusive) cases:
• $m\neq k$: in this case m and k should appear as two factors in $(n-1)!$ (because $1<m,k<n$) and hence their product (which is equal to n) should divide $(n-1)!$ (as required).
• $m=k$: in this case $n=m^2$ and hence m must be a factor in $(n-1)!$ (because $1<m<n$). Now, since $n\geq 6$ then $m>2$ and hence $m^2>2m$ which implies that $2m$ must be a factor in $(n-1)!$. So, both m and $2m$ are factors in $(n-1)!$ (i.e. separately) and hence their product (which is equal to $2n$) should divide $(n-1)!$, i.e. n divides $(n-1)!$ (as required).
(**h**) By rule 1 (see the preamble of this section) we have $m|n!$. Also we have $m|m$. Hence, by rule 14 of § 1.9 we have $m|(n!\pm m)$.

8. Given a number $m\in\mathbb{N}$, what is the smallest number $n\in\mathbb{N}$ whose factorial $n!$ is divisible by m?
Solution: If $p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ is the prime factorization of m and $ap=\max(a_1p_1,a_2p_2,\cdots,a_kp_k)$ then the factorial of ap is certainly divisible by m. This is because $(ap)!$ contains all the factors $p_1^{a_1},p_2^{a_2},\cdots,p_k^{a_k}$ in the prime factorization of m and hence it is divisible by m. So, we found an "upper limit" to n. However, the factorials of some lower multiples of p [e.g. $(a-1)p$] may also work. Hence, $n=bp$ where $b\in\{a,a-1,\ldots,1\}$. So, we should try these numbers excluding the numbers whose factorials are less than m.

[176] It is noteworthy that $C_n^{2n}/(n+1)$ is called the n^{th} Catalan number (which may be symbolized as C_n) and hence this is a demonstration that Catalan numbers are integers.

Note: if m is prime then $n = m$ (see point 4 in the preamble). This is a special case of the above procedure.

9. Find the smallest $n \in \mathbb{N}$ such that:
   (**a**) $25|n!$. (**b**) $43|n!$. (**c**) $175|n!$. (**d**) $480|n!$. (**e**) $813|n!$.
   Solution: Referring to Problem 8 we have:
   (**a**) $25 = 5^2$ and hence $n = 2 \times 5 = 10$.
   (**b**) $43 = 43^1$ and hence $n = 1 \times 43 = 43$.
   (**c**) $175 = 5^2 \times 7^1$ and hence $n = 2 \times 5 = 10$.
   (**d**) $480 = 2^5 \times 3^1 \times 5^1$ and hence $n = 8$.
   (**e**) $813 = 3^1 \times 271^1$ and hence $n = 271$.
10. How many values of n we have such that:
    (**a**) $5^{10}|n!$ but $5^{20} \not| n!$. (**b**) $5^{10}|n!$ but $7^{10} \not| n!$.
    Solution: From Problem 8 we have:
    (**a**) The smallest $n \in \mathbb{N}$ such that $5^{10}|n!$ is $n = 45$. The smallest $n \in \mathbb{N}$ such that $5^{20}|n!$ is $n = 85$. So, we have $84 - 44 = 40$ (or $85 - 45 = 40$) values.
    (**b**) The smallest $n \in \mathbb{N}$ such that $5^{10}|n!$ is $n = 45$. The smallest $n \in \mathbb{N}$ such that $7^{10}|n!$ is $n = 63$. So, we have $62 - 44 = 18$ (or $63 - 45 = 18$) values.
11. Find the condition for $n \in \mathbb{N}$ whose factorial is divisible by $\sum_{i=1}^{n} i$.
    Solution: The trivial case $n = 1$ is obvious and hence in the following we deal only with $n > 1$.
    We have $\sum_{i=1}^{n} i = n(n+1)/2$ (Eq. 15). Now, let consider the ratio of $n!$ to $n(n+1)/2$, that is:

$$\frac{n!}{n(n+1)/2} = \frac{(n-1)!}{(n+1)/2} = \frac{2(n-1)!}{(n+1)}$$

    Here, we have three main cases (which are comprehensive and mutually exclusive):
    • If n is odd then $(n+1)$ is even and hence $(n+1)/2$ (refer to the middle equation) is a positive integer $\leq (n-1)$ which means that $(n-1)!$ is divisible by $(n+1)/2$, i.e. $n!$ is divisible by $\sum_{i=1}^{n} i$.
    • If n is even and $n+1$ (which is odd) is composite then $(n+1)$ must be made of prime factors less than $(n-1)$ (refer to the last equation) and hence $2(n-1)!$ is divisible by $(n+1)$, i.e. $n!$ is divisible by $\sum_{i=1}^{n} i$.
    • If n is even and $n+1$ (which is odd) is prime then $(n+1)$ cannot be a factor of $2(n-1)!$ (refer to the last equation) because all the prime factors in $2(n-1)!$ are less than $(n+1)$ and hence $2(n-1)!$ is not divisible by $(n+1)$,[177] i.e. $n!$ is not divisible by $\sum_{i=1}^{n} i$.
    So in brief, the condition that makes $n!$ divisible by $\sum_{i=1}^{n} i$ is either n is odd or n is even with $n+1$ being composite.
12. Show that $n!$ is divisible by $(n_1!n_2!\cdots n_k!)$ where $n_1 + n_2 + \cdots + n_k = n$ $(n, n_1, n_2, \cdots, n_k \in \mathbb{N}^0)$.
    Solution: The number $n!/(n_1!n_2!\cdots n_k!)$ is the multinomial coefficient which is an integer (see rule 27 and Problem 2 of § 1.8), i.e. $n!$ is divisible by $(n_1!n_2!\cdots n_k!)$.
    Note: the binomial coefficient is a special case of the multinomial coefficient (corresponding to $k = 2$) and hence it is an integer (see rule 26 and Problem 2 of § 1.8), i.e. $n!$ is divisible by $\big[n_1!(n-n_1)!\big]$.
13. Show that $(p-1)! + 1$ has more than one prime divisor *iff* $p \geq 7$ $(p \in \mathbb{P})$.
    Solution: **The only if part** [which is "if $(p-1)!+1$ has more than one prime divisor then $p \geq 7$"] is equivalent in truth to its contrapositive [which (in essence) is "if $p < 7$ (i.e. $p = 2, 3, 5$) then $(p-1)!+1$ has only one prime divisor"]. This is easy to prove because:

$$(2-1)! + 1 = 2 \qquad (3-1)! + 1 = 3 \qquad (5-1)! + 1 = 25 = 5^2$$

    As we see, $(p-1)! + 1$ has only one prime divisor in these three cases.
    Regarding **the if part** [which is "if $p \geq 7$ then $(p-1)! + 1$ has more than one prime divisor"], from Wilson's theorem (see § 2.9.1) we have $(p-1)! + 1 \overset{p}{=} 0$ which means that $(p-1)! + 1 = kp$ $(k \in \mathbb{N})$.

[177] Also see point 4 in the preamble.

Now, $k \neq 1$ because $(p-1)!+1$ is obviously greater than p (noting that $p \geq 7$). So, to finish this proof we need to show that k is not a power of p, i.e. $(p-1)!+1 \neq p^n$ $(n \in \mathbb{N})$. Now, if we assume that $(p-1)!+1 = p^n$ then we have:

$$\begin{aligned}
(p-1)! &= p^n - 1 \\
(p-1)! &= (p-1)(p^{n-1} + p^{n-2} + \cdots + p + 1) && \text{(Eq. 12)} \\
(p-2)! &= p^{n-1} + p^{n-2} + \cdots + p + 1 && \text{(canceling } p-1\text{)} \\
(p-2)! &= (p^{n-1}-1) + (p^{n-2}-1) + \cdots + (p-1) + (1-1) + n && (\pm n) \\
n &= (p-2)! - (p^{n-1}-1) - (p^{n-2}-1) - \cdots - (p-1)
\end{aligned}$$

Now, $(p-1)$ is a composite number ≥ 6 (because p is odd ≥ 7) and hence $(p-1)$ divides $(p-2)!$ (see part g of Problem 7). So, from the last line we conclude that n is divisible by $(p-1)$ because every term on the right hand side is divisible by $(p-1)$ (see Eq. 12 as well as rule 14 of § 1.9). Accordingly, we must have $n \geq (p-1)$. But this contradicts our previous assumption $\big[$i.e. $(p-1)!+1 = p^n\big]$ because if $n \geq (p-1)$ then we must have $(p-1)!+1 < p^n$. Therefore, our assumption must be untrue because it leads to a contradiction (see point 4 of § 1.5.4). This means that $(p-1)!+1 \neq p^n$ and hence $(p-1)!+1$ must have more than one prime divisor (as required).

14. Show the following (where $n, i, j \in \mathbb{N}$):
(**a**) $n!+1$ and $(n+1)!+1$ are coprime.
(**b**) The numbers $n!i+1$ and $n!j+1$ $(1 \leq i < j \leq n)$ are pairwise coprime.
Solution:
(**a**) From rule 12 of § 2.4 we have:

$$\begin{aligned}
\gcd\big[n!+1,\,(n+1)!+1\big] &= \gcd\big[n!+1,\,\{(n+1)!+1\} - \{n!+1\}\big] = \gcd\big[n!+1,\,(n+1)!-n!\big] \\
&= \gcd\big[n!+1,\,n!\{(n+1)-1\}\big] = \gcd\big[n!+1,\,n!n\big]
\end{aligned}$$

Now, if this gcd is > 1 then $n!+1$ and $n!n$ must have a common prime factor p which means that $p|n!$. This is because if $p|n$ then $p|n!$ (by rule 5) while if $p \not| n$ then $p|n!$ (by rule 22 of § 1.9).
Now, since p divides both $n!+1$ and $n!$ then p must divide their difference (see rule 14 of § 1.9) which is 1 and this is impossible. So, this gcd must be 1, i.e. $n!+1$ and $(n+1)!+1$ are coprime (as required).
(**b**) From rule 12 of § 2.4 we have:

$$\gcd\big[n!i+1, n!j+1\big] = \gcd\big[n!i+1, \{n!j+1\} - \{n!i+1\}\big] = \gcd\big[n!i+1, n!(j-i)\big]$$

Now, if this gcd is > 1 then $n!i+1$ and $n!(j-i)$ must have a common prime factor p which means that $p|n!$. This is because if $p|(j-i)$ then $p|n!$ $\big[$since $(j-i) < n$ and hence it is a factor of $n!$; see rule 1 in the preamble of this section$\big]$ while if $p \not| (j-i)$ then $p|n!$ (by rule 22 of § 1.9).
Now, since $p|n!$ then $p|n!i$ (see rule 18 of § 1.9). However, since p divides both $n!i+1$ and $n!i$ then p must divide their difference (see rule 14 of § 1.9) which is 1 and this is impossible. So, this gcd must be 1, i.e. $n!i+1$ and $n!j+1$ are coprime for any pair of $1 \leq i < j \leq n$ (as required).

6.12 Divisibility of Permutations, Binomial and Multinomial Coefficients

In this section we present a few Problems about the divisibility of permutations, binomial and multinomial coefficients.

Problems

1. Show the following (where P_k^n represents the number of permutations of k in n noting that $n \geq 1$ and $1 \leq k \leq n$):
(**a**) $P_{k-1}^{n-1} | P_k^n$. (**b**) $P_{k-1}^n | P_k^n$. (**c**) $P_{k-1}^n \big| \big(P_k^{n+1} - P_k^n\big)$.
Solution: We note first that all permutation symbols (like P_k^n) represent integers (see point 25 of §

1.8).
(**a**) We have (see Eq. 4):

$$P_k^n = \frac{n!}{(n-k)!} = n\left[\frac{(n-1)!}{(n-k)!}\right] = n\left[\frac{(n-1)!}{(n-1-k+1)!}\right] = n\left[\frac{(n-1)!}{(\{n-1\}-\{k-1\})!}\right] = nP_{k-1}^{n-1}$$

Now, since n is an integer then $P_{k-1}^{n-1}|P_k^n$.
(**b**) We have (see Eq. 4):

$$\frac{P_k^n}{P_{k-1}^n} = \frac{\frac{n!}{(n-k)!}}{\frac{n!}{(n-k+1)!}} = \frac{(n-k+1)!}{(n-k)!} = n-k+1$$

Now, since $(n-k+1)$ is an integer then $P_{k-1}^n|P_k^n$.
(**c**) We have:

$$\begin{aligned}
n+1 &= n+1 \\
(n+1-k)+k &= n+1 && (\pm k) \\
\frac{1}{(n-k)!} + k\frac{1}{(n+1-k)!} &= \frac{n+1}{(n+1-k)!} && \left[\div (n+1-k)!\right] \\
\frac{n!}{(n-k)!} + k\frac{n!}{(n+1-k)!} &= \frac{(n+1)!}{(n+1-k)!} && (\times n!) \\
\frac{n!}{(n-k)!} + k\frac{n!}{(n-\{k-1\})!} &= \frac{(n+1)!}{(n+1-k)!} \\
P_k^n + kP_{k-1}^n &= P_k^{n+1} && (\text{Eq. 4}) \\
kP_{k-1}^n &= P_k^{n+1} - P_k^n
\end{aligned}$$

Now, since k is an integer then $P_{k-1}^n|\left(P_k^{n+1} - P_k^n\right)$.

2. Show the following (where C_m^n and $C_{n_1,n_2,\ldots,n_k}^n$ represent the binomial and multinomial coefficients):
(**a**) $(n+1)|C_n^{2n}$ $(n \in \mathbb{N}^0)$. (**b**) $p|C_m^p$ $(p \in \mathbb{P},\, 0 < m < p)$.
(**c**) $n|C_{n_1,n_2,\ldots,n_k}^n$ $(n \in \mathbb{P},\, n > n_1, n_2, \ldots, n_k)$.
Solution:
(**a**) This was shown in part (d) of Problem 7 of § 6.11.
(**b**) From Eq. 5 we have:

$$m!\, C_m^p = p \times (p-1) \times \cdots \times (p-m+1)$$

Now, $m!\, C_m^p$ is an integer (since it is a product of integers) and it is divisible by p $\left[\text{since } (p-1)\times\cdots\times(p-m+1) \text{ is an integer}\right]$. Therefore, $p|m!$ or $p|C_m^p$ (see rule 22 of § 1.9). However, $p \not| m!$ because $p > m$ (see rule 4 of § 6.11). Therefore, $p|C_m^p$ (as required).
(**c**) From Eq. 6 we have:

$$n_1!\, n_2! \ldots n_k!\, C_{n_1,n_2,\ldots,n_k}^n = n! = n\ (n-1)!$$

Now, $n_1!\, n_2! \ldots n_k!\, C_{n_1,n_2,\ldots,n_k}^n$ is an integer (since it is a product of integers) and it is divisible by n $\left[\text{since } (n-1)! \text{ is an integer}\right]$. Therefore, $n|n_1!$ or $n|n_2!\cdots$ or $n|n_k!$ or $n|C_{n_1,n_2,\ldots,n_k}^n$ (see rule 22 of § 1.9 noting that n is prime). However, $n \not| n_1!$, $n \not| n_2!\cdots$ and $n \not| n_k!$ because $n > n_1, n_2, \ldots, n_k$ (see rule 4 of § 6.11 noting that n is prime). Therefore, $n|C_{n_1,n_2,\ldots,n_k}^n$ (as required).[178]

3. Show that if (2^k+1) is prime then $2^k + 1 \neq m^p - n^p$ where $m, n, k \in \mathbb{N}$, $m > n$, and p is an odd prime.
Solution: Let $2^k + 1 = m^p - n^p$. Now, from Eq. 10 we have $m^p - n^p = (m-n)(\cdots)$ and hence if $(m-n) > 1$ then $m^p - n^p$ (and hence 2^k+1) will be composite noting that $(\cdots) > 1$. So, if (2^k+1)

[178] We note that part (b) is a special case of part (c) because the binomial coefficient is a special case of the multinomial coefficient (corresponding to $k = 2$).

is to be prime then we must have $(m-n)=1$, i.e. $m=n+1$. Accordingly, if (2^k+1) is to be prime (where $2^k+1=m^p-n^p$) then:

$$\begin{aligned}
2^k &= m^p - n^p - 1 && (2^k+1=m^p-n^p)\\
&= (n+1)^p - n^p - 1 && (m=n+1)\\
&= \left[\sum_{i=0}^{p} C_i^p n^i\right] - n^p - 1 && (\text{Eq. } 13)\\
&= \left[1 + \left(\sum_{i=1}^{p-1} C_i^p n^i\right) + n^p\right] - n^p - 1 && (C_0^p n^0 = 1,\ C_p^p n^p = n^p)\\
&= \sum_{i=1}^{p-1} C_i^p n^i
\end{aligned}$$

Now, according to part (b) of Problem 2 we have $p|C_i^p$ $(p\in\mathbb{P},\ 0<i<p)$ which means that the terms of the sum in the last line have a common factor of p. However, 2^k does not have such a factor since it is a power of 2 (noting that p is an odd prime). So, this contradiction leads to the conclusion that $2^k+1\neq m^p-n^p$ if (2^k+1) is prime.

6.13 Divisibility of Series

In this section we present a small number of Problems about the divisibility of series.

Problems

1. Determine the divisibility of $\sum_{k=1}^{100} k10^k$ by $2,3,4,\ldots,16$.[179]

Solution: We have:

$$\sum_{k=1}^{100} k10^k = 10\sum_{k=1}^{100} k10^{k-1}$$

and hence it is obviously divisible by 2, 5 and 10.

Regarding the divisibility by 3 we have [see rule 13 of § 2.7 noting that $\sum_{k=1}^{100} k10^k$ is a polynomial $P(m)$ with $m=10$]:

$$10 \overset{3}{=} 1 \qquad \rightarrow \qquad P(10) \overset{3}{=} P(1) = \sum_{k=1}^{100} k\,1^k = \sum_{k=1}^{100} k = 50(101) = 5050 \overset{3}{=} 1$$

and hence it is not divisible by 3.

Regarding the divisibility by 4, 8 and 16 we have:

$$\sum_{k=1}^{100} k10^k = 10 + 200 + 3000 + \sum_{k=4}^{100} k10^k = \left(10^4 \sum_{k=4}^{100} k10^{k-4}\right) + 3210$$

and hence (by rule 41 of § 1.9) it is not divisible by any of these numbers.

Regarding the divisibility by 6, it is not divisible by 3 and hence it cannot be divisible by 6 (see rule 28 of § 1.9).

Regarding the divisibility by 7, it is not divisible by 7. This can be easily established by noting that $10^k \overset{6}{=} {}^{1,2,3,4,5,6} \overset{7}{=} 3,2,6,4,5,1$ and hence:

$$\sum_{k=1}^{100} k10^k \ \overset{7}{=}\ \sum_{k=1}^{100} (k \bmod 7)(10^k \bmod 7) = 1037 \overset{7}{=} 1$$

[179] This Problem may also be classified as part of § 6.2.

This may also be established by using rule 29 of § 1.9 (if we have such calculation capability).[180]
Regarding the divisibility by 9, it is not divisible by 3 and hence it cannot be divisible by 9 (noting that $9 = 3^2$).
Regarding the divisibility by 11 we have $\big[$see rule 13 of § 2.7 noting that $\sum_{k=1}^{100} k10^k$ is a polynomial $P(m)$ with $m = 10\big]$:

$$10 \overset{11}{=} -1 \qquad \rightarrow \qquad P(10) \overset{11}{=} P(-1) = \sum_{k=1}^{100} k\,(-1)^k = -1 + 2 - 3 + 4 - \cdots - 99 + 100 = 50 \overset{11}{=} 6$$

and hence it is not divisible by 11.
Regarding the divisibility by 12, it is not divisible by 3 (or 4) and hence it cannot be divisible by 12 (see rule 34 of § 1.9).
Regarding the divisibility by 13, it is not divisible by 13. This can be easily established by noting that $10^k \overset{6}{=} {}_{1,2,3,4,5,6} \overset{13}{=} 10, 9, 12, 3, 4, 1$ and hence:

$$\sum_{k=1}^{100} k10^k \overset{13}{=} \sum_{k=1}^{100} (k \bmod 13)(10^k \bmod 13) = 3789 \overset{13}{=} 6$$

This may also be established by using rule 35 of § 1.9 (see footnote [180]).
Regarding the divisibility by 14, it is not divisible by 7 and hence it cannot be divisible by 14 (see rule 36 of § 1.9).
Regarding the divisibility by 15, it is not divisible by 3 and hence it cannot be divisible by 15 (see rule 37 of § 1.9).
So in brief, $\sum_{k=1}^{100} k10^k$ is divisible only by 2, 5 and 10 (i.e. within 2-16 inclusive).

2. Determine the divisibility of $\sum_{k=1}^{4526786285} k^2$ by $2, 3, 4, \ldots, 60$.
Solution: From Eq. 16 we have:

$$\begin{aligned}
\sum_{k=1}^{4526786285} k^2 &= \frac{(4526786285)(4526786286)(9053572571)}{6} \\
&= \frac{(5 \times 7 \times 23 \times 163 \times 34499)(2 \times 3^2 \times 11 \times 53 \times 431369)(127 \times 131 \times 544183)}{2 \times 3} \\
&= 3 \times 5 \times 7 \times 11 \times 23 \times 53 \times 127 \times 131 \times 163 \times 34499 \times 431369 \times 544183
\end{aligned}$$

where we used prime factorization in the second line. So, it is divisible only by 3, 5, 7, 11, 15, 21, 23, 33, 35, 53, 55 (i.e. within 2-60 inclusive).

3. Determine the divisibility of $\sum_{k=1}^{7428906264} k^3$ by $2, 3, 4, \ldots, 60$.
Solution: From Eq. 17 we have:

$$\begin{aligned}
\sum_{k=1}^{7428906264} k^3 &= \frac{(7428906264)^2(7428906265)^2}{4} \\
&= \frac{(2^3 \times 3 \times 13 \times 23810597)^2(5 \times 11 \times 409 \times 330247)^2}{2 \times 2} \\
&= 2^4 \times 3^2 \times 5^2 \times 11^2 \times 13^2 \times 409^2 \times 330247^2 \times 23810597^2
\end{aligned}$$

[180] We note that

$$\sum_{k=1}^{100} k10^k = 1109876543209876543209876543209876543209876543209876543209876543209876543209876543209876543210$$

In fact, if we note that $10 \overset{7}{=} 3$ then we can (by rule 13 of § 2.7) use $P(10) \overset{7}{=} P(3) = \sum_{k=1}^{100} k\,3^k = 769200949692526911571918236175189749507895476586 50 \overset{7}{=} 1$ (where result can be obtained for instance by division).

where we used prime factorization in the second line. So, it is divisible only by 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 15, 16, 18, 20, 22, 24, 25, 26, 30, 33, 36, 39, 40, 44, 45, 48, 50, 52, 55, 60 (i.e. within 2-60 inclusive).

4. Show that the series $\sum_{k=0}^{2n+1} 10^k m$ is divisible by 11 (where $n \in \mathbb{N}^0$ and $m = 0, 1, \ldots, 9$).
Solution: We have $\sum_{k=0}^{2n+1} (-1)^k m = 0$ and hence by rule 33 of § 1.9 the series $\sum_{k=0}^{2n+1} 10^k m$ is divisible by 11.
5. Show that the series $\sum_{k=0}^{n} \phi(p^k)$ is divisible by all the divisors of p^n (where $n \in \mathbb{N}$ and $p \in \mathbb{P}$).
Solution: We have:

$$\sum_{k=0}^{n} \phi(p^k) = 1 + \sum_{k=1}^{n} \phi(p^k) = 1 + \sum_{k=1}^{n} (p^k - p^{k-1}) = 1 + (p^n - 1) = p^n$$

where we used $\phi(p^0) = \phi(1) = 1$ in step 1, used Eq. 42 in step 2, and justified step 3 in the upcoming note 1. So, the series is equal to p^n and hence it is divisible by all the divisors of p^n (which are $p^0, p^1, \ldots, p^n$).
Note 1: we have:

$$\begin{aligned} \sum_{k=1}^{n} (p^k - p^{k-1}) &= \left[\sum_{k=1}^{n} p^k\right] - \left[\sum_{k=1}^{n} p^{k-1}\right] \\ &= \left[p^1 + p^2 + \cdots + p^{n-1} + p^n\right] - \left[1 + p^1 + \cdots + p^{n-2} + p^{n-1}\right] = p^n - 1 \end{aligned}$$

Note 2: from Eq. 45 we get $\sum_{k=0}^{n} \phi(p^k) = p^n$ (noting that the divisors of p^n are $p^0, p^1, \ldots, p^n$) and hence we can prove this result more easily.
6. Show the following (where $n \in \mathbb{N}$ and $i = 0, 1, \ldots, n$):
(**a**) 2^i divides $\sum_{k=0}^{n} C_k^n$. (**b**) 3^i divides $\sum_{k=0}^{n} C_k^n\, 2^k$. (**c**) 5^i divides $\sum_{k=0}^{n} C_k^n\, 2^{2k}$.
(**d**) 9^i divides $\sum_{k=0}^{n} C_k^n\, 2^{3k}$. (**e**) $(2^m + 1)^i$ divides $\sum_{k=0}^{n} C_k^n\, 2^{mk}$. (**f**) C_m^n divides $\sum_{k=m}^{n} C_k^n C_m^k$.
Solution:
(**a**) We have:

$$\sum_{k=0}^{n} C_k^n = \sum_{k=0}^{n} C_k^n\ 1^k\ 1^{n-k} = (1+1)^n = 2^n$$

where we used Eq. 13 in the second step. So, 2^i divides $\sum_{k=0}^{n} C_k^n$.
(**b**) We have:

$$\sum_{k=0}^{n} C_k^n\, 2^k = \sum_{k=0}^{n} C_k^n\ 2^k\ 1^{n-k} = (2+1)^n = 3^n$$

where we used Eq. 13 in the second step. So, 3^i divides $\sum_{k=0}^{n} C_k^n\, 2^k$.
(**c**) We have:

$$\sum_{k=0}^{n} C_k^n\, 2^{2k} = \sum_{k=0}^{n} C_k^n\, 4^k = \sum_{k=0}^{n} C_k^n\ 4^k\ 1^{n-k} = (4+1)^n = 5^n$$

where we used Eq. 13 in the third step. So, 5^i divides $\sum_{k=0}^{n} C_k^n\, 2^{2k}$.
(**d**) We have:

$$\sum_{k=0}^{n} C_k^n\, 2^{3k} = \sum_{k=0}^{n} C_k^n\, 8^k = \sum_{k=0}^{n} C_k^n\ 8^k\ 1^{n-k} = (8+1)^n = 9^n$$

where we used Eq. 13 in the third step. So, 9^i divides $\sum_{k=0}^{n} C_k^n\, 2^{3k}$.
(**e**) We have (noting that $m \in \mathbb{N}^0$):

$$\sum_{k=0}^{n} C_k^n\, 2^{mk} = \sum_{k=0}^{n} C_k^n\, (2^m)^k = \sum_{k=0}^{n} C_k^n\ (2^m)^k\ 1^{n-k} = (2^m + 1)^n$$

where we used Eq. 13 in the third step. So, $(2^m+1)^i$ divides $\sum_{k=0}^{n} C_k^n\, 2^{mk}$. We note that parts (a,b,c,d) are instances of part (e).

(**f**) We have (noting that $0 \leq m \leq n$):

$$\begin{aligned}
\sum_{k=m}^{n} C_k^n C_m^k &= \sum_{k=m}^{n} \frac{n!}{k!(n-k)!}\frac{k!}{m!(k-m)!} = \sum_{k=m}^{n} \frac{n!}{(n-k)!}\frac{1}{m!(k-m)!} = \frac{n!}{m!}\sum_{k=m}^{n}\frac{1}{(n-k)!(k-m)!} \\
&= \frac{n!}{m!(n-m)!}\sum_{k=m}^{n}\frac{(n-m)!}{(n-k)!(k-m)!} = C_m^n \sum_{k=m}^{n}\frac{(n-m)!}{(n-k)!(k-m)!} \\
&= C_m^n \sum_{k=0}^{n-m}\frac{(n-m)!}{(n-\{k+m\})!(\{k+m\}-m)!} = C_m^n \sum_{k=0}^{n-m}\frac{(n-m)!}{k!(n-m-k)!} = C_m^n \sum_{k=0}^{n-m} C_k^{n-m} \\
&= C_m^n\, 2^{n-m}
\end{aligned}$$

where we shifted the index in step 6 and used Eq. 21 in the last step. So, C_m^n divides $\sum_{k=m}^{n} C_k^n C_m^k$ (noting that 2^{n-m} is an integer).

7. Show that if 2 divides the series $\sum_{k=1}^{n} m_k^s$ then 3 divides the product $\prod_{k=1}^{n} m_k$ (where $m_k \in \mathbb{Z}$, $s \in \mathbb{N}$ and n is odd).

   Solution: We prove this by contraposition (see § 1.5.4) by showing that if 3 does not divide $\prod_{k=1}^{n} m_k$ then 2 does not divide $\sum_{k=1}^{n} m_k^s$.

   According to rule 22 of § 1.9, 3 divides the product $\prod_{k=1}^{n} m_k$ *iff* at least one of m_k is divisible by 3. So, if 3 does not divide $\prod_{k=1}^{n} m_k$ then none of m_k is divisible by 3, i.e. $m_k \overset{3}{\neq} 0$ $(k = 1, 2, \ldots, n)$. This means that either $m_k \overset{3}{=} 1$ or $m_k \overset{3}{=} -1$ (noting that $2 \overset{3}{=} -1$), and hence either $m_k^s \overset{3}{=} 1$ or $m_k^s \overset{3}{=} -1$ (see rule 11 of § 2.7). Now, if for each m_k we have either $m_k^s \overset{3}{=} 1$ or $m_k^s \overset{3}{=} -1$ then the series $\sum_{k=1}^{n} m_k^s$ should be odd (noting that n is odd) and hence the series cannot be divisible by 2 (see rule 7 of § 1.8). So, the divisibility of the series by 2 should imply the divisibility of the product by 3.

8. Show the following:

   (**a**) $\sum_{k=1}^{n} k$ divides $\sum_{k=1}^{n} 3k^2$. (**b**) $\sum_{k=1}^{n} k$ divides $\sum_{k=1}^{n} 2k^3$. (**c**) $\sum_{k=1}^{n} k$ divides $\sum_{k=1}^{n} 15k^4$.

   (**d**) $\sum_{k=1}^{n} k$ divides $\sum_{k=1}^{n} 6k^5$. (**e**) $\sum_{k=1}^{n} k^2$ divides $\sum_{k=1}^{n} 5k^4$. (**f**) $\sum_{k=1}^{n} k^3$ divides $\sum_{k=1}^{n} 3k^5$.

   Solution: We use the identities of Eqs. 15-19 where a direct division leads to an integer expression, that is:

   (**a**) $\dfrac{\sum_{k=1}^{n} 3k^2}{\sum_{k=1}^{n} k} = \dfrac{3\sum_{k=1}^{n} k^2}{\sum_{k=1}^{n} k} = \dfrac{3\left[n(n+1)(2n+1)/6\right]}{n(1+n)/2} = 2n+1$

   (**b**) $\dfrac{\sum_{k=1}^{n} 2k^3}{\sum_{k=1}^{n} k} = \dfrac{2\sum_{k=1}^{n} k^3}{\sum_{k=1}^{n} k} = \dfrac{2\left[n^2(n+1)^2/4\right]}{n(1+n)/2} = n(n+1)$

   (**c**) $\dfrac{\sum_{k=1}^{n} 15k^4}{\sum_{k=1}^{n} k} = \dfrac{15\sum_{k=1}^{n} k^4}{\sum_{k=1}^{n} k} = \dfrac{15\left[n(n+1)(2n+1)(3n^2+3n-1)/30\right]}{n(1+n)/2} = (2n+1)(3n^2+3n-1)$

   (**d**) $\dfrac{\sum_{k=1}^{n} 6k^5}{\sum_{k=1}^{n} k} = \dfrac{6\sum_{k=1}^{n} k^5}{\sum_{k=1}^{n} k} = \dfrac{6\left[n^2(n+1)^2(2n^2+2n-1)/12\right]}{n(1+n)/2} = n(n+1)(2n^2+2n-1)$

   (**e**) $\dfrac{\sum_{k=1}^{n} 5k^4}{\sum_{k=1}^{n} k^2} = \dfrac{5\sum_{k=1}^{n} k^4}{\sum_{k=1}^{n} k^2} = \dfrac{5\left[n(n+1)(2n+1)(3n^2+3n-1)/30\right]}{n(n+1)(2n+1)/6} = 3n^2+3n-1$

   (**f**) $\dfrac{\sum_{k=1}^{n} 3k^5}{\sum_{k=1}^{n} k^3} = \dfrac{3\sum_{k=1}^{n} k^5}{\sum_{k=1}^{n} k^3} = \dfrac{3\left[n^2(n+1)^2(2n^2+2n-1)/12\right]}{n^2(n+1)^2/4} = 2n^2+2n-1$

9. Determine all $n \in \mathbb{N}$ and all $x \in \mathbb{Z}$ for which $\sum_{k=0}^{n} x^k$ divides $\sum_{k=0}^{n} x^{2k}$.

Solution: From Eq. 12 we have:

$$\sum_{k=0}^{n} x^k = 1 + x + x^2 + \cdots + x^{n-1} + x^n = \frac{x^{n+1}-1}{x-1} \qquad (x \neq 1)$$
$$\sum_{k=0}^{n} x^{2k} = 1 + x^2 + x^4 + \cdots + +x^{2n-2} + x^{2n} = \frac{x^{2(n+1)}-1}{x^2-1} \qquad (x \neq \pm 1)$$

Hence:

$$\frac{\sum_{k=0}^{n} x^{2k}}{\sum_{k=0}^{n} x^k} = \frac{\left(x^{2(n+1)}-1\right)/\left(x^2-1\right)}{\left(x^{n+1}-1\right)/(x-1)} = \frac{\left(x^{n+1}-1\right)\left(x^{n+1}+1\right)(x-1)}{\left(x^{n+1}-1\right)(x-1)(x+1)} = \frac{x^{n+1}+1}{x+1} \qquad (x \neq \pm 1)$$

Now, we have two cases to consider:
• n is even (i.e. $n = 2, 4, \ldots$ and hence $n+1 = 3, 5, \ldots$): from the identity of Eq. 11, $(x+1)$ divides $(x^{n+1}+1)$ for all x (excluding at the moment $x = 0, \pm 1$). In fact, this can also be concluded from rule 51 of § 1.9 since the remainder of dividing $(x^{n+1}+1)$ by $(x+1)$ is equal to $\left[(-1)^{n+1}+1\right]$ which is equal to 0 for even n.
Regarding, $x = 0, \pm 1$ we consider the original series. For $x = 0$ the original series vanish and hence if we do not allow the division of 0 by 0 then we should exclude $x = 0$. For $x = \pm 1$ they should be included as valid values since they do not cause any of the series to vanish when n is even. So in brief, $\sum_{k=0}^{n} x^k$ divides $\sum_{k=0}^{n} x^{2k}$ for all (non-zero) $x \in \mathbb{Z}$ if $n \in \mathbb{N}$ is even (i.e. $n = 2, 4, 6, \ldots$).
• n is odd (i.e. $n = 1, 3, \ldots$ and hence $n+1 = 2, 4, \ldots$): by rule 51 of § 1.9 the remainder of dividing $(x^{n+1}+1)$ by $(x+1)$ is equal to $\left[(-1)^{n+1}+1\right]$ which is equal to 2 for odd n. This means that the result of dividing $\sum_{k=0}^{n} x^{2k}$ by $\sum_{k=0}^{n} x^k$ is an integer plus $2/(x+1)$. So, if this result is to be an integer then $2/(x+1)$ must be an integer. However, for $2/(x+1)$ to be an integer $(x+1)$ should be a divisor of 2, i.e. $(x+1) = \pm 1, \pm 2$ and hence $x = 0, -2, 1, -3$ (where $x = 0$ may not be accepted because it causes vanishing of both series leading to 0/0 which may not be defined). So in brief, $\sum_{k=0}^{n} x^k$ divides $\sum_{k=0}^{n} x^{2k}$ for $x = -3, -2, 1$ if $n \in \mathbb{N}$ is odd (i.e. $n = 1, 3, 5, \ldots$).

10. Give an example of a condition that makes the series $\sum_{k=1}^{n} x_k$ necessarily composite (where $x_k \in \mathbb{N}$ and $n > 1$).
Solution: For example, if $g \equiv \gcd(x_1, x_2, \ldots, x_n) > 1$ then this series is necessarily composite because:

$$\sum_{k=1}^{n} x_k = g\left(\sum_{k=1}^{n} \xi_k\right) \qquad (x_k = g\xi_k)$$

which is obviously composite since it is a product of two integers both of which are greater than 1 (noting that $g > 1$ and ξ_k in the sum are natural numbers since $x_k \in \mathbb{N}$).

11. Find all $n \in \mathbb{N}$ such that the series $\sum_{k=1}^{n} k$ is divisible by:
(**a**) 4. (**b**) 6. (**c**) 12. (**d**) 19.

Solution: From Eq. 15 we have $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$. Accordingly:
(**a**) For this series to be divisible by 4, $n(n+1)$ must be divisible by 8. Now, only one of n and $(n+1)$ can be divisible by 8 because the other is odd.[181] This means that we must have either $8|n$ (and hence $n = 8m$ where $m \in \mathbb{N}$) or $8|(n+1)$ (and hence $n = 8m-1$). So in brief, $\sum_{k=1}^{n} k$ is divisible by 4 for all $n = 8m-1$ and $n = 8m$ where $m \in \mathbb{N}$ (i.e. $n = 7, 8, 15, 16, 23, 24, \ldots$).
(**b**) For this series to be divisible by 6, $n(n+1)$ must be divisible by 12, i.e. $n(n+1) \overset{12}{=} 0$. On testing $n \overset{12}{=} 1, 2, 3, \ldots, 12$ we find that $n(n+1) \overset{12}{=} 0$ only for $n \overset{12}{=} 3, 8, 11, 12$. So in brief, $\sum_{k=1}^{n} k$ is divisible by 6 for all n of the following four forms (where $m \in \mathbb{N}^0$):

[181] We note that $8 = 2^3$ and hence 8 in its entirety must divide either n or $(n+1)$, i.e. 2^n cannot split between them since one of them is odd and hence it cannot be divisible by a natural power of 2. In other words, 8 is coprime to one of them and hence if it should divide $n(n+1)$ then it must divide exactly one of them (see rule 21 of § 1.9).

$n = 3 + 12m$ $n = 8 + 12m$ $n = 11 + 12m$ $n = 12(1 + m)$

(**c**) If we repeat our treatment in part (b) then we can conclude that the series $\sum_{k=1}^{n} k$ is divisible by 12 for all n of the following four forms (where $m \in \mathbb{N}^0$):

$n = 8 + 24m$ $n = 15 + 24m$ $n = 23 + 24m$ $n = 24(1 + m)$

(**d**) For this series to be divisible by 19, $n(n + 1)$ must be divisible by 19. Now, only one of n and $(n + 1)$ can be divisible by 19 because if 19 divides both then it divides their difference (i.e. 1) which is impossible (see rule 14 of § 1.9). This means that we must have either $19|n$ (and hence $n = 19m$ where $m \in \mathbb{N}$) or $19|(n + 1)$ (and hence $n = 19m - 1$). So in brief, $\sum_{k=1}^{n} k$ is divisible by 19 for all $n = 19m - 1$ and $n = 19m$ where $m \in \mathbb{N}$ (i.e. $n = 18, 19, 37, 38, 56, 57, \ldots$).

12. Find all $n \in \mathbb{N}$ such that:
(**a**) $\sum_{k=1}^{n} k^2$ is divisible by 36. (**b**) $\sum_{k=1}^{n} k^4$ is divisible by 2. (**c**) $\sum_{k=1}^{n} k^4$ is divisible by 2^t ($t \in \mathbb{N}$).
Solution:
(**a**) From Eq. 16 we have:

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6} = \frac{2n^3 + 3n^2 + n}{6}$$

So, for the given series to be divisible by 36, $(2n^3 + 3n^2 + n)$ must be divisible by $6 \times 36 = 216$, i.e. $2n^3 + 3n^2 + n \overset{216}{=} 0$. The solutions of this congruence equation in $\mathbb{N}$ are (see for instance § 3.2.1): $n \overset{216}{=} 40, 80, 135, 175, 215, 216$. So, $\sum_{k=1}^{n} k^2$ is divisible by 36 for all $n = r + 216m$ where $r = 40, 80, 135, 175, 215, 216$ and $m \in \mathbb{N}^0$.
(**b**) From Eq. 18 we have:

$$\sum_{k=1}^{n} k^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$$

So, for the given series to be divisible by 2, $n(n+1)(2n+1)(3n^2+3n-1)$ must be divisible by 4 (noting that 30 contains a single factor of 2, i.e. $30 = 2 \times 3 \times 5$). Now, $(2n + 1)$ and $(3n^2 + 3n - 1)$ are always odd and hence we must have either $4|n$ (and hence $n = 4m$ where $m \in \mathbb{N}$) or $4|(n + 1)$ (and hence $n = 4m - 1$). So in brief, $\sum_{k=1}^{n} k^4$ is divisible by 2 for all $n = 4m - 1$ and $n = 4m$ where $m \in \mathbb{N}$ (i.e. $n = 3, 4, 7, 8, 11, 12, \ldots$). It is worth noting that we do not need to worry about the divisibility by 15 (i.e. 3×5) because the given series is an integer and hence $n(n+1)(2n+1)(3n^2+3n-1)$ is guaranteed to be divisible by 30 (and hence divisible by 15 as well as by 2), so the required extra condition that we need to impose to guarantee the divisibility of the given series by 4 is its divisibility by an extra factor of 2 which means that $n(n + 1)(2n + 1)(3n^2 + 3n - 1)$ is divisible by 4.
(**c**) If we follow the analysis of part (b) then we can easily conclude that $\sum_{k=1}^{n} k^4$ is divisible by 2^t ($t \in \mathbb{N}$) for all $n = 2^{t+1}m - 1$ and $n = 2^{t+1}m$ where $m \in \mathbb{N}$.

13. Give some examples of integer series $\sum_{k=1}^{n} a_k$ (or $\sum_{k=0}^{n} a_k$) which are not divisible by m for any $n \in \mathbb{N}$ where:
(**a**) $m \neq 0$ is a given integer. (**b**) $m \neq \pm 1$ is an odd integer. (**c**) $m \neq 0$ is an even integer.
Solution: There are many ways for finding and constructing such series. In the following we give some simple examples.
(**a**) Any alternating series of the following form:

$$\sum_{k=1}^{n} a_k = -q + \sum_{k=2}^{n} (-1)^k 2q \qquad (m \not| q)$$

should do.[182] This is because this series alternates between $-q$ (for odd n) and $+q$ (for even n) and hence it cannot be divisible by m (because of the imposed condition $m \not| q$).

[182] We note that "alternating series" here means the sum is alternating (so the term may not be used in its exact conventional meaning in calculus). We should also note that for $n = 1$ the sum on the right hand side is 0 (because the upper limit is smaller than the lower limit).

(**b**) The series $\sum_{k=0}^{n} C_k^n$ should do (where $n \in \mathbb{N}$). This is because (according to Eq. 21) we have $\sum_{k=0}^{n} C_k^n = 2^n$ and hence it cannot be divisible by any odd integer (excluding ± 1) because it is a natural power of 2 and hence it does not contain any odd factor (excluding ± 1).
(**c**) Any series which is odd for all $n \in \mathbb{N}$ should do. This is because no odd number is divisible by an even number. An example of such series is the alternating series of part (a) when q is odd. Another example is the series:

$$\sum_{k=1}^{n} a_k = 1 + 2 \sum_{k=2}^{n} k$$

14. Give some examples of integer series $\sum_{k=1}^{n} a_k$ which are divisible by m for all $n \in \mathbb{N}$ where:
(**a**) $m = \pm 2$. (**b**) $m = \pm 5$. (**c**) $m = \pm 13$.

Solution: Again, there are many ways for finding and constructing such series, so we give some simple examples.
(**a**) Any series which is even for all $n \in \mathbb{N}$ should do. This is because any even number is divisible by ± 2. An example of such series is $\sum_{k=1}^{n} a_k = \sum_{k=1}^{n} 2^k$.
(**b**) For example, the series $\sum_{k=1}^{n} a_k = 5 + \sum_{k=2}^{n} \left(5^k - 5^{k-1}\right)$ should do because it ends in 5 for all $n \in \mathbb{N}$ and hence it is divisible by ± 5 for all $n \in \mathbb{N}$.
(**c**) For example, the series $\sum_{k=1}^{n} a_k = \sum_{k=1}^{n} 13$ should do because it represents the natural multiples of 13 and hence it is divisible by ± 13 for all $n \in \mathbb{N}$.

6.14 Divisibility and Permutations of Digits

There are some problems about the divisibility of numbers formed by permutations of digits. A small sample of this type of problems is given in the following Problems. It is worth noting that "numbers" in the following Problems means natural numbers (noting that if we consider the negative integers as well then the results will be doubled).

Problems

1. How many 10-digit even numbers can be formed from the 10 digits $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ assuming no repetition of digits is allowed?
Solution: The first digit (from left) cannot be zero (since we want 10-digit numbers) and hence we have only 9 possibilities for the first digit. The last digit must be even (since we want even numbers) and hence in principle we have 5 possibilities for the last digit (i.e. $0, 2, 4, 6, 8$). For the remaining 8 middle digits we have 8! possibilities (i.e. all the 8-digit permutations of the remaining 8 digits).
Now, if the first digit is odd (i.e. $1, 3, 5, 7, 9$) then we have 5 possibilities for the last digit (i.e. $0, 2, 4, 6, 8$), while if the first digit is even (i.e. $2, 4, 6, 8$) then we have 4 possibilities for the last digit (i.e. the remaining 4 even digits since repetition is not allowed). Therefore, the number of 10-digit even numbers (with no repetition) is:

$$\Big[5 \times (8!) \times 5\Big] + \Big[4 \times (8!) \times 4\Big] = 1653120$$

2. How many 6-digit numbers divisible by 5 can be formed from the digits $\{0, 1, 2, 3, 4, 5, 6\}$ if:
(**a**) The digits cannot be repetitive. (**b**) The digits can be repetitive.

Solution: To be divisible by 5 the last digit must be 0 or 5 (rule 27 of § 1.9). Now, the sets of 6 digits of theses 7 digits that include 0 or/and 5 are:

$\{1, 2, 3, 4, 5, 6\}$ $\{0, 2, 3, 4, 5, 6\}$ $\{0, 1, 3, 4, 5, 6\}$ $\{0, 1, 2, 4, 5, 6\}$

$\{0, 1, 2, 3, 5, 6\}$ $\{0, 1, 2, 3, 4, 6\}$ $\{0, 1, 2, 3, 4, 5\}$

So, let us consider these sets for the cases (a) and (b):
(**a**) We have two sets that contain only one of the two digits 0 and 5 (i.e. sets $\{1, 2, 3, 4, 5, 6\}$ and $\{0, 1, 2, 3, 4, 6\}$). So, we have only one possibility for the last digit (i.e. 5 or 0) and $P_5^5 = 120$ possibilities for the other digits (see Eq. 4), i.e. we have a total of $120 \times 1 = 120$ numbers for each one of these two sets.

Regarding the other five sets, each one of these sets contains both 0 and 5. Now, we have two possibilities for each one of these five sets: the last digit is 0 and the last digit is 5. If the last digit is 0 then we have $P_5^5 = 120$ possibilities for the other digits. If the last digit is 5 then we have $4 \times P_4^4 = 96$ possibilities for the other digits (noting that a 6-digit number cannot start with 0). Accordingly, for each one of these five sets we have:

$$(P_5^5 \times 1) + (4 \times P_4^4 \times 1) = 120 + 96 = 216$$

So, in total we have $(2 \times 120) + (5 \times 216) = 1320$ numbers.

(**b**) For set $\{1, 2, 3, 4, 5, 6\}$ the last digit must be 5 while each one of the remaining 5 digits has 6 possibilities. Hence, we have $6^5 \times 1 = 7776$ possibilities.

For set $\{0, 1, 2, 3, 4, 6\}$ the last digit must be 0 and the first digit cannot be 0 (since a 6-digit number cannot start with 0) while each one of the remaining 4 digits has 6 possibilities. Hence, we have $5 \times 6^4 \times 1 = 6480$ possibilities.

Regarding the other five sets, each one of these sets contains both 0 and 5. Now, the first digit cannot be 0 (and hence we have 5 possibilities for the first digit), and the last digit must be either 0 or 5 (and hence we have 2 possibilities for the last digit), while we have 6 possibilities for each one of the 4 middle digits. Accordingly, for each one of these five sets we have:

$$5 \times 6^4 \times 2 = 12960$$

So, in total we have $7776 + 6480 + (5 \times 12960) = 79056$ numbers.

3. How many 6-digit numbers divisible by 3 can be formed from the digits $\{0, 1, 2, 3, 4, 5, 6\}$ assuming that the digits cannot be repetitive.

   Solution: To be divisible by 3 the sum of the digits must be divisible by 3 (rule 25 of § 1.9). Now, the sets of 6 digits of theses 7 digits that can form numbers the sum of whose digits is divisible by 3 are: $\{1, 2, 3, 4, 5, 6\}$, $\{0, 1, 2, 4, 5, 6\}$ and $\{0, 1, 2, 3, 4, 5\}$.[183] So, let us consider these sets:

   • The set $\{1, 2, 3, 4, 5, 6\}$ produces $P_6^6 = 6! = 720$ numbers (see Eq. 4).

   • Noting that a 6-digit number cannot start with 0, the set $\{0, 1, 2, 4, 5, 6\}$ produces $5 \times P_5^5 = 5 \times 5! = 600$ numbers. This also applies to the set $\{0, 1, 2, 3, 4, 5\}$.

   So, in total we have $720 + 600 + 600 = 1920$ numbers.

4. How many 10-digit numbers divisible by 8 can be formed from the 10 digits $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ assuming repetition of digits is allowed?

   Solution: The first digit cannot be zero (since we want 10-digit numbers) and hence we have only 9 possibilities for the first digit. Also, according to rule 30 of § 1.9 the last three digits must be divisible by 8 (since we want numbers divisible by 8) and hence we have only 125 possibilities for the last three digits (i.e. $000, 008, 016, \ldots, 984, 992$). For the remaining 6 middle digits we have 10^6 possibilities (since we have 10 possibilities for each one of the 6 digits noting that repetition is allowed). Therefore, the number of 10-digit numbers divisible by 8 (with repetition) is:

   $$9 \times (10^6) \times 125 = 1125000000$$

   We may also argue more simply that we have 9000000000 10-digit numbers (i.e. $9999999999 - 999999999$ or $10^{10} - 10^9$) and these 9000000000 numbers must contain among them $9000000000/8 = 1125000000$ numbers divisible by 8.

5. Find the 4-permutations of the digits $5, 6, 8, 9$ (e.g. 5689 and 5869) which are divisible by 11.

   Solution: We have 24 permutations which are:

   5689 **5698** 5869 **5896** 5968 5986 **6589** 6598 6859 6895 6958 **6985**

   8569 8596 8659 8695 8956 **8965** 9568 9586 **9658** 9685 **9856** 9865

   The permutations which are divisible by 11 (i.e. those whose alternating digit sum is divisible by 11; see rule 33 of § 1.9) are emboldened (i.e. the $2^{nd}, 4^{th}, 7^{th}, 12^{th}, 13^{th}, 18^{th}, 21^{st}, 23^{rd}$).

[183] We note that we have seven possibilities for the 6-digit sets where in each one of these seven possibilities one digit is removed (these sets are shown in Problem 2). Only the above three sets satisfy the divisibility by 3 condition.

6. Find the 4-permutations of the digits $3, 4, 7, 9$ (e.g. 3479 and 4973) which are divisible by 11.
   Solution: The alternating sum of none of the 4-permutations of these digits is divisible by 11 and hence by rule 33 of § 1.9 none of these 4-permutations is divisible by 11.
7. How many 4-digit numbers divisible by 16 can be formed from the 10 digits $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ assuming repetition of digits is allowed?
   Solution: The 4-digit numbers divisible by 16 start with 1008 and end with 9984 and hence their number is:
$$\frac{9984 - 1008}{16} + 1 = 562$$

6.15 Miscellaneous Divisibility Problems

There are many other types of divisibility problems that do not belong to the previous categories (which we investigated in the previous sections). For example, there are divisibility problems involving certain types of mathematical functions or based on special requirements and conditions. In this section we provide a sample of these problems.[184]

Problems

1. Find the digits a and b of every number $m = 2a3b$ which is divisible by 5 and 13.
   Solution: Since m is divisible by 5 then b must be either 0 or 5.
   • If b is 0 then $m = 2a30 = 2030 + a00$ (see point 6 in the preamble of § 1.6) and hence:
$$\begin{aligned} 2030 + a00 &\overset{13}{\equiv} 0 \\ a00 &\overset{13}{\equiv} -2030 \\ a00 &\overset{13}{\equiv} 11 \\ a \times 100 &\overset{13}{\equiv} 11 \\ a &\overset{13}{\equiv} 11 \times 100^* \\ a &\overset{13}{\equiv} 11 \times 3 \\ a &\overset{13}{\equiv} 33 \\ a &\overset{13}{\equiv} 7 \end{aligned}$$
   Hence, $m = 2730$. Alternatively, we may try $a = 0, 1, \ldots, 9$ to find that only $a = 7$ makes $2a30$ divisible by 13.
   • If b is 5 then $m = 2a35 = 2035 + a00$ and hence:
$$\begin{aligned} 2035 + a00 &\overset{13}{\equiv} 0 \\ a00 &\overset{13}{\equiv} -2035 \\ a00 &\overset{13}{\equiv} 6 \\ a &\overset{13}{\equiv} 6 \times 100^* \\ a &\overset{13}{\equiv} 6 \times 3 \\ a &\overset{13}{\equiv} 5 \end{aligned}$$
   Hence, $m = 2535$. Alternatively, we may try $a = 0, 1, \ldots, 9$ to find that only $a = 5$ makes $2a35$ divisible by 13.
2. Find the digits a and b of every number $m = 1a007b12$ which is divisible by 11.
   Solution: By rule 33 of § 1.9 we must have (where k is an integer):
$$1 - a + 0 - 0 + 7 - b + 1 - 2 = 11k \qquad \rightarrow \qquad 7 - a - b = 11k$$

[184] In fact, some of these Problems are assigned to this section because they depend on results obtained later than the sections they naturally belong to. Anyway, this is a trivial issue.

Now, if we note that $a, b \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ we can see that $-11 \leq (7 - a - b) \leq 7$ (where -11 corresponds to $a = b = 9$ and 7 corresponds to $a = b = 0$) and hence k can only be -1 or 0. Now:
• If $k = -1$ then $7 - a - b = -11$ (i.e. $a + b = 18$) and hence we have only one possibility for a and b, i.e. $a = b = 9$ and hence $m = 19007912$.
• If $k = 0$ then $7 - a - b = 0$ (i.e. $a + b = 7$) and hence we have 8 possibilities:

$$a = 0, 1, 2, 3, 4, 5, 6, 7 \qquad \text{corresponding respectively to:} \qquad b = 7, 6, 5, 4, 3, 2, 1, 0$$

and hence m represents the following numbers:

$$10007712 \quad 11007612 \quad 12007512 \quad 13007412 \quad 14007312 \quad 15007212 \quad 16007112 \quad 17007012$$

Note: a simpler approach for solving this Problem (and indeed this type of problems) is to try all the possible combinations of $a = 0, 1, \ldots, 9$ and $b = 0, 1, \ldots, 9$ (i.e. $10 \times 10 = 100$ combinations) to find out which of these combinations satisfy the given divisibility requirement.

3. Find the digits a and b of every number of the form $6a85842b$ which is divisible by 7.
Solution: We have $6a85842b = 60858420 + a00000b$ (see point 6 in the preamble of § 1.6) and hence (noting that $6a85842b$ is supposedly divisible by 7):

$$\begin{aligned} 6a85842b &\overset{7}{=} 0 \\ 60858420 + a00000b &\overset{7}{=} 0 \\ a00000b &\overset{7}{=} 0 \qquad (60858420 \text{ is a multiple of } 7) \end{aligned}$$

So, $a00000b$ is divisible by 7 and hence (see rule 29 of § 1.9) we have:

$$\begin{aligned} a00000 - 2b &\overset{7}{=} 0 \\ a00000 &\overset{7}{=} 2b \\ a &\overset{7}{=} 2b \times 100000^* \\ a &\overset{7}{=} 2b \times 3 \\ a &\overset{7}{=} 6b \end{aligned}$$

By inserting $b = 0, 1, \ldots, 9$ in the last congruence equation and obtaining the corresponding values of a (i.e. from the digits $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$) we get:

$a = 0, 7, 6, 5, 4, 3, 2, 9, 1, 8, 0, 7, 6, 5$ corresponding respectively to: $b = 0, 0, 1, 2, 3, 4, 5, 5, 6, 6, 7, 7, 8, 9$

4. How many numbers of the form $4a27831b4$ (where a and b are digits, i.e. $a, b \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$) we have if they have to be divisible by 12?
Solution: For a number to be divisible by 12 it must be divisible by 3 and 4 (see rule 34 of § 1.9). To be divisible by 4 the last two digits must be divisible by 4 (see rule 26 of § 1.9). This means that b must be 0 or 2 or 4 or 6 or 8. To be divisible by 3 the sum of the digits must be divisible by 3 (see rule 25 of § 1.9). This means that:
• If b is 0 then a is 1 or 4 or 7.
• If b is 2 then a is 2 or 5 or 8.
• If b is 4 then a is 0 or 3 or 6 or 9.
• If b is 6 then a is 1 or 4 or 7.
• If b is 8 then a is 2 or 5 or 8.
So, in total we have 16 numbers of this form which are divisible by 12.

5. Find all $n \in \mathbb{N}$ such that:
(**a**) $8|(3^n n^3)$. (**b**) $3|(5^n n^7 - 1)$. (**c**) $5|(2^n n^3 - 3^n n^2)$.
Solution:
(**a**) It is obvious that all even $n \in \mathbb{N}$ satisfy this divisibility statement because $3^n n^3 = 2^3 m^3 3^n = 8m^3 3^n$ (where $n = 2m$ and $m \in \mathbb{N}$). It is also obvious that no odd $n \in \mathbb{N}$ satisfies this divisibility statement

because $3^n n^3$ is odd in this case and no even number can divide an odd number (see the divisibility rules in § 1.8). So, $8|(3^n n^3)$ for all even $n \in \mathbb{N}$.

(**b**) $3|(5^n n^7 - 1)$ is equivalent to $5^n n^7 \overset{3}{=} 1$. Now, for even n we have $5^n \overset{3}{=} 1$ and for odd n we have $5^n \overset{3}{=} 2$ $\big[$because $5^n \overset{3}{=} (-1)^n$ noting that $-1 \overset{3}{=} 2\big]$. Also, $n^7 \overset{3}{=} n$ (because $0^7 \overset{3}{=} 0$, $1^7 \overset{3}{=} 1$ and $2^7 \overset{3}{=} 2$). Hence, by rule 10 of § 2.7 we have $n^7 5^n \overset{3}{=} 1$ only if n is even and $n \overset{3}{=} 1$ (i.e. $n = 4 + 6k$ where $k \in \mathbb{N}^0$), or n is odd and $n \overset{3}{=} 2$ (i.e. $n = 5 + 6k$ where $k \in \mathbb{N}^0$).[185] So, $3|(5^n n^7 - 1)$ for all $n = m + 6k$ where $m = 4, 5$ and $k \in \mathbb{N}^0$ (i.e. $n = 4, 5, 10, 11, 16, 17, \ldots$).

(**c**) $5|(2^n n^3 - 3^n n^2)$ is equivalent to $2^n n^3 - 3^n n^2 \overset{5}{=} 0$. Now, $2^n \pmod 5$ and $3^n \pmod 5$ have a cycle of 4, while $n^3 \pmod 5$ and $n^2 \pmod 5$ have a cycle of 5. These cycles are presented in the following table:

$k \in \mathbb{N}^0$	$n = k+1$	$n = k+2$	$n = k+3$	$n = k+4$	$n = k+5$
$2^n \pmod 5$	2	4	3	1	
$n^3 \pmod 5$	1	3	2	4	0
$3^n \pmod 5$	3	4	2	1	
$n^2 \pmod 5$	1	4	4	1	0

Now, if we combine all these possibilities we get a cycle of 20 for $(2^n n^3 - 3^n n^2)$ which is presented in the following table:

m	$2^n \pmod 5$	$n^3 \pmod 5$	$3^n \pmod 5$	$n^2 \pmod 5$	$2^n n^3 - 3^n n^2 \pmod 5$
1	2	1	3	1	4
2	4	3	4	4	1
3	3	2	2	4	3
4	1	4	1	1	3
5	2	0	3	0	0
6	4	1	4	1	0
7	3	3	2	4	1
8	1	2	1	4	3
9	2	4	3	1	0
10	4	0	4	0	0
11	3	1	2	1	1
12	1	3	1	4	4
13	2	2	3	4	2
14	4	4	4	1	2
15	3	0	2	0	0
16	1	1	1	1	0
17	2	3	3	4	4
18	4	2	4	4	2
19	3	4	2	1	0
20	1	0	1	0	0

As we see, only $m = 5, 6, 9, 10, 15, 16, 19, 20$ satisfy this congruence equation, and hence $5|(2^n n^3 - 3^n n^2)$ for all $n = m + 20k$ where $m = 5, 6, 9, 10, 15, 16, 19, 20$ ($k \in \mathbb{N}^0$).

6. Find all $n \in \mathbb{N}$ such that n, $8n^2 + 1$ and $8n^2 + 2n + 1$ are all primes.

Solution: Since $8n^2 + 1$ is prime then it is not divisible by 3 (noting that $8n^2 + 1 > 3$), and hence either $8n^2 + 1 \overset{3}{=} 1$ or $8n^2 + 1 \overset{3}{=} 2$. However, $8n^2 + 1 \overset{3}{=} 2$ is not acceptable because it leads to $8n^2 \overset{3}{=} 1$ which has no solution.

So, we must have $8n^2 + 1 \overset{3}{=} 1$ and hence $8n^2 \overset{3}{=} 0$ whose only solution is $n = 3$. This is because n is prime and 8 has no factor of 3 (i.e. 3 and 8 are coprime) and hence if $8n^2$ is divisible by 3 (as implied

[185] These conclusions should be intuitive. However, they can be obtained formally (and easily) by using the Chinese remainder theorem, i.e. by solving the the system $n \overset{2}{=} 0$ and $n \overset{3}{=} 1$ in the first case, and the system $n \overset{2}{=} 1$ and $n \overset{3}{=} 2$ in the second case.

by $8n^2 \stackrel{3}{=} 0$) then n must be 3 since 3 is the only prime divisible by 3 (see rule 21 of § 1.9).
Now, if $n = 3$ then $8n^2 + 1 = 73$ and $8n^2 + 2n + 1 = 79$ which are both primes and hence we have three primes that satisfy the given forms.
So in brief n, $8n^2 + 1$ and $8n^2 + 2n + 1$ are all primes only if $n = 3$.

7. Let $\{m_1, m_2, \ldots, m_n\}$ be a set of n pairwise coprime numbers ($n > 1$) where the sum of any k numbers in this set is a composite number ($2 \leq k \leq n$). Give an example of such a set.
Solution: The set $\{n!i + 1 : 1 \leq i \leq n\}$ is an example of such a set. This is because the numbers in this set are pairwise coprime (see part b of Problem 14 of § 6.11). Moreover, the sum of any k numbers of this set is composite because this sum is divisible by k. This is because the sum of k numbers consists of terms containing $n!$ plus k (where this k comes from the sum of 1's). Now, $k|n!$ (since $k \leq n$; see rule 1 of § 6.11) and $k|k$ and hence the sum must be divisible by k since each term in this sum is divisible by k (see rule 14 of § 1.9).
8. Show the following:
(**a**) If $m, n \in \mathbb{N}$ and $p \in \mathbb{P}$ then p divides $(m+n)^p - (m^p + n^p)$.
(**b**) If $x_1, \ldots, x_k \in \mathbb{N}$ and $p \in \mathbb{P}$ then p divides $(x_1 + \cdots + x_k)^p - (x_1^p + \cdots + x_k^p)$.
(**c**) $(2^k - 1)^2 | \left[2^{k(2^k-1)} - 1\right]$ where $k \in \mathbb{N}$.
(**d**) For any $n \in \mathbb{N}$ there are n consecutive composite numbers.
Solution:
(**a**) From Eq. 13 we have:

$$\begin{aligned}
(m+n)^p &= \sum_{k=0}^{p} C_k^p m^k n^{p-k} \\
(m+n)^p &= m^p + n^p + \sum_{k=1}^{p-1} C_k^p m^k n^{p-k} \\
(m+n)^p - (m^p + n^p) &= \sum_{k=1}^{p-1} C_k^p m^k n^{p-k}
\end{aligned}$$

Now, by the result of part (b) of Problem 2 of § 6.12 all the binomial coefficients in the terms of the sum in the last equality are divisible by p and hence this sum is divisible by p. So, $(m+n)^p - (m^p + n^p)$ is divisible by p.
(**b**) From Eq. 14 we have:

$$\begin{aligned}
(x_1 + \cdots + x_k)^p &= \sum_{\forall\ n_1 + \cdots + n_k = p} C_{n_1,\ldots,n_k}^p\, x_1^{n_1} \ldots x_k^{n_k} \\
(x_1 + \cdots + x_k)^p &= x_1^p + \cdots + x_k^p + \\
&\qquad \sum_{n_1 + \cdots + n_k = p,\ p > n_1,\ldots,n_k} C_{n_1,\ldots,n_k}^p\, x_1^{n_1} \ldots x_k^{n_k} \\
(x_1 + \cdots + x_k)^p - (x_1^p + \cdots + x_k^p) &= \sum_{n_1 + \cdots + n_k = p,\ p > n_1,\ldots,n_k} C_{n_1,\ldots,n_k}^p\, x_1^{n_1} \ldots x_k^{n_k}
\end{aligned}$$

Now, by the result of part (c) of Problem 2 of § 6.12 all the multinomial coefficients in the terms of the sum in the last equality are divisible by p and hence this sum is divisible by p. Therefore, $(x_1 + \cdots + x_k)^p - (x_1^p + \cdots + x_k^p)$ is divisible by p.[186]
(**c**) From part (d) of Problem 1 of § 6.8 we have $n^2 | [(n+1)^n - 1]$. Now, if $n = 2^k - 1$ we get:

$$n^2 | [(n+1)^n - 1] \quad \rightarrow \quad (2^k - 1)^2 | \left[(2^k - 1 + 1)^{(2^k-1)} - 1\right] \quad \rightarrow \quad (2^k - 1)^2 | \left[2^{k(2^k-1)} - 1\right]$$

[186] We note that part (a) is a special case of part (b) corresponding to $k = 2$ (see footnote [178] on page 218) and hence the proof of part (b) is sufficient for proving part (a).

(**d**) For example, the following n consecutive natural numbers are composite:

$$(n+1)!+m \qquad\qquad (m=2,3,\ldots,n+1)$$

This is because (according to part h of Problem 7 of § 6.11) each one of these numbers is divisible by m which means that $\big[(n+1)!+m\big]$ is composite noting that $1<m<\big[(n+1)!+m\big]$.

9. Show that $n|(2^n+1)$ for all $n=3^m$ where $m\in\mathbb{N}$.
Solution: We use induction (see § 1.5.4). This divisibility statement is true for $m=1$ because $3^1|(2^{3^1}+1)$. Now, let assume that this statement is true for some $k\in\mathbb{N}$ which means that $2^{3^k}+1=a3^k$ ($a\in\mathbb{N}$), i.e. $2^{3^k}=a3^k-1$. Accordingly:

$$\begin{aligned} 2^{3^{k+1}} &= 2^{3^k\times 3}=\left(2^{3^k}\right)^3=\left(a3^k-1\right)^3=\left(a3^k\right)^3-3\left(a3^k\right)^2+3\left(a3^k\right)-1 \qquad \text{(see Eq. 13)}\\ 2^{3^{k+1}}+1 &= a^3 3^{3k}-a^2 3^{2k+1}+a3^{k+1}\\ 2^{3^{k+1}}+1 &= \left(a^3 3^{2k-1}-a^2 3^k+a\right)3^{k+1} \end{aligned}$$

The last line shows that $3^{k+1}|(2^{3^{k+1}}+1)$ since $(a^3 3^{2k-1}-a^2 3^k+a)$ is an integer.
So, the given statement is true for $m=1$, and it is shown that if it is true for $m=k$ then it is true for $m=k+1$. Hence, by mathematical induction it is true for all $m\in\mathbb{N}$, i.e. it is true for all $n=3^m$ where $m\in\mathbb{N}$ (as required).

10. Show that there are infinitely many composite numbers of the following forms (where $n\in\mathbb{N}$):
(**a**) 3^n+25. (**b**) 2^n-3. (**c**) $2^{2^n}+3$.
Solution:
(**a**) 3^n+25 is the sum of two odd numbers and hence it is even (see the parity rules in § 1.8). Therefore, it is composite for all $n\in\mathbb{N}$ (and even $n\in\mathbb{N}^0$; see point 3 in the preamble of § 2.2). So, we have infinitely many composite numbers of this form.[187]
(**b**) If $n=4k-1$ ($k\in\mathbb{N}$) then (by the result of part g of Problem 1 of § 6.5) 2^n-3 is divisible by 5 and hence it is composite (noting that there are infinitely many $n=4k-1$ where $k\in\mathbb{N}$).
(**c**) In part (i) of Problem 5 of § 2.7 we proved that $2^{2^n}+3\overset{7}{=}0$ for odd $n\in\mathbb{N}^0$, i.e. $2^{2^n}+3$ is divisible by 7 for all odd $n\in\mathbb{N}^0$ and hence it is composite for infinitely many $n\in\mathbb{N}$.

11. Show that $6765|(m^{41}-m)$ where $m\in\mathbb{Z}$.
Solution: We note first that $6765=3\times5\times11\times41$. Now, $6765|(m^{41}-m)$ is equivalent to $m^{41}\overset{6765}{=}m$. From the result of Problem 4 of § 6.10 we have $m^{n(p-1)+1}\overset{p}{=}m$, that is:

$$m^{41}\overset{3}{=}m\ \ (n=20) \qquad m^{41}\overset{5}{=}m\ \ (n=10) \qquad m^{41}\overset{11}{=}m\ \ (n=4) \qquad m^{41}\overset{41}{=}m\ \ (n=1)$$

So, from rule 14 of § 2.7 we have $m^{41}\overset{6765}{=}m$.

12. Find all $m,n\in\mathbb{Z}$ such that:
(**a**) $7|(m^3-n^5)$. (**b**) $5|(3m^3+m^2-11n^4+8n-2)$. (**c**) $4|(7^m-n^5)$.
Solution:
(**a**) We note that $7|(m^3-n^5)$ is equivalent to $m^3\overset{7}{=}n^5$. Now, we have:

$0^3\overset{7}{=}0$ $1^3\overset{7}{=}1$ $2^3\overset{7}{=}1$ $3^3\overset{7}{=}6$ $4^3\overset{7}{=}1$ $5^3\overset{7}{=}6$ $6^3\overset{7}{=}6$

$0^5\overset{7}{=}0$ $1^5\overset{7}{=}1$ $2^5\overset{7}{=}4$ $3^5\overset{7}{=}5$ $4^5\overset{7}{=}2$ $5^5\overset{7}{=}3$ $6^5\overset{7}{=}6$

Accordingly, $m^3\overset{7}{=}n^5$ in the following seven cases:

$m\overset{7}{=}0$ & $n\overset{7}{=}0$ $m\overset{7}{=}1$ & $n\overset{7}{=}1$ $m\overset{7}{=}2$ & $n\overset{7}{=}1$ $m\overset{7}{=}3$ & $n\overset{7}{=}6$

$m\overset{7}{=}4$ & $n\overset{7}{=}1$ $m\overset{7}{=}5$ & $n\overset{7}{=}6$ $m\overset{7}{=}6$ & $n\overset{7}{=}6$

[187] The purpose of such trivial questions is to test the vigilance of the reader.

Therefore, $7|(m^3 - n^5)$ for all pairs of integers (m, n) of the following seven forms (where $k, s \in \mathbb{Z}$):

$(7k, 7s)$ $(1 + 7k, 1 + 7s)$ $(2 + 7k, 1 + 7s)$ $(3 + 7k, 6 + 7s)$

$(4 + 7k, 1 + 7s)$ $(5 + 7k, 6 + 7s)$ $(6 + 7k, 6 + 7s)$

(**b**) We note that $5|(3m^3+m^2-11n^4+8n-2)$ is equivalent to $3m^3+m^2 \stackrel{5}{=} 11n^4-8n+2$. Now, we have:

$3(0^3) + 0^2 \stackrel{5}{=} 0$ $3(1^3) + 1^2 \stackrel{5}{=} 4$ $3(2^3) + 2^2 \stackrel{5}{=} 3$ $3(3^3) + 3^2 \stackrel{5}{=} 0$ $3(4^3) + 4^2 \stackrel{5}{=} 3$

$11(0^4) - 8(0) + 2 \stackrel{5}{=} 2$ $11(1^4) - 8(1) + 2 \stackrel{5}{=} 0$ $11(2^4) - 8(2) + 2 \stackrel{5}{=} 2$

$11(3^4) - 8(3) + 2 \stackrel{5}{=} 4$ $11(4^4) - 8(4) + 2 \stackrel{5}{=} 1$

Accordingly, $3m^3 + m^2 \stackrel{5}{=} 11n^4 - 8n + 2$ in the following three cases:

$m \stackrel{5}{=} 0$ & $n \stackrel{5}{=} 1$ $m \stackrel{5}{=} 1$ & $n \stackrel{5}{=} 3$ $m \stackrel{5}{=} 3$ & $n \stackrel{5}{=} 1$

Therefore, $5|(3m^3 + m^2 - 11n^4 + 8n - 2)$ for all pairs of integers (m, n) of the following three forms (where $k, s \in \mathbb{Z}$):

$(5k, 1 + 5s)$ $(1 + 5k, 3 + 5s)$ $(3 + 5k, 1 + 5s)$

(**c**) We note first that m must be non-negative. As before, $4|(7^m - n^5)$ is equivalent to $7^m \stackrel{4}{=} n^5$. Now, we have $7^m \stackrel{4}{=} 1$ when m is even and $7^m \stackrel{4}{=} 3$ when m is odd (see Problem 13 of § 2.7). We also have:

$0^5 \stackrel{4}{=} 0$ $1^5 \stackrel{4}{=} 1$ $2^5 \stackrel{4}{=} 0$ $3^5 \stackrel{4}{=} 3$

Accordingly, $7^m \stackrel{4}{=} n^5$ when m is even and $n \stackrel{4}{=} 1$ and when m is odd and $n \stackrel{4}{=} 3$.
Therefore, $4|(7^m - n^5)$ for all pairs of integers (m, n) of the following two forms: $(2k, 1 + 4s)$ and $(1 + 2k, 3 + 4s)$ where $k \in \mathbb{N}^0$ and $s \in \mathbb{Z}$.

Index