Souvenirs from the Empire of Numbers

Florentin Smarandache, UNM-Gallup, USA

1. Forward.

Browsing through my fifth to twelfth grade years of preoccupation for creation I discovered a notebook of Number Theory.
I liked to play with numbers as Tudor Arghezi (1880-1967) – our second national Romanian poet {after the genial poet Mihai Eminescu (1850-1889)} – played with words.
I was so curious and amazed by the numbers' properties.
Interesting theorems, equations, and inequalities!
Such fascinating people who dedicated their research to numbers, just for the sake of science!
I collected many results and tried to write a handbook of mathematicians and their results.

As a child I stayed in bed, leaning my back against the wall, with some papers and a pen in my hands, thinking and scribbling with numbers!

As skilled for arithmetic I was remarked from the beginning by my first grade teacher Elena Bălaşa and especially my second to fourth grade teacher Elena Mişcoci, both at Primary School in Bălceşti (district of Vâlcea), who organized in class calculation competitions among students: "who computes the fastest this multiplication" [at that time there were no pocket calculators, we had to do everything by hand.]
Our elementary math teacher from fifth to eighth grade, Ion Bălaşa, an excellent and very passionate educator, asked us the students to subscribe to "Gazeta Matematică" [Mathematical Gazette] and submit solutions to its proposed problem of algebra, geometry, and trigonometry for our knowledgeable level.
We had a very serious, strong, rigid, and complex scientific education at that time.
In High Schools, at Craiova for the first three years, with the instructor Larisa Bistriceanu, and afterwards at Rm. Vâlcea for the next two years with instructor Nicolae Vlădescu, I participated every school year in students' Mathematical Olympiads winning various awards.

This Number Theory notebook is a compilation of known results about numbers, and it also includes a short list of some renowned mathematicians. Unfortunately, only a part of it was recovered when I came back to Romania from my volunteer exile in Turkey and USA. Most of this notebook was damaged by dust, mould, humidity, cobwebs, and mouse from my parents' house garret in Bălceşti, or simply lost. Other manuscripts, not only of science, but also of poetry, novels, diaries were confiscated by the secret police (Securitate) and never returned, although they are mentioned in the 4 folders' about 880 pages police secret report about me that I got copies from the CNSAS (Consiliul Naţional

de Studiere a Arhivelor Securităţii = National Council for Studying the Archives of the Secret Police).

2. Short List of Mathematicians.

***Waclaw Sierpinski** (1882-1970) – Polish - Set Theory (on Transfinite Numbers), Analytic Number Theory.
***Popoviciu Tiberiu** - Number Theory.
***Henri Poincarè** (1854-1912) – Integer Function Theory – Poincarè inequality.
***Giuseppe Peano** (1858-1932) – The founder of the Axiomatic Arithmetic (Peano Axioms).
***Blaise Pascal** (1623-1662) The Pascal's Arithmetic Triangle.
***Alexandru Myller** (1879-1965) – Romanian – Mathematics History.
***Andrei Andreevici Markov** (1856-1892) - Number Theory.
***Adrian Marie Legendre** (1752-1833) – Number Theory. He was the first who formulated the problem of the asymptotic distribution of the prime numbers.
***Gottfried Wilhelm Leibnitz** (1646-1716) – Binary Arithmetic.
***Joseph Louis Lagrange** (1736-1813) – Number Theory.
***Ion Ionescu** (1870-1946) – Mathematical Gazette B – Arithmetic problems, Mathematics History.
***Muhammed ibn Musa Horezmi** (c. 780 – c. 850) – Arab – Book about addition and subtraction – Indian system of numeration.
***David Hilbert** (1862-1943) – German – Algebraic Number Theory. In 1900 he proposed 23 problems at the International Congress in Paris.
***Jacques Hadamard** (1865-1963)- French – Number Theory.
***Sophie Germain** (1776-1831) – French - Number Theory.
***Friederich Karl Gauss** (1777-1831) – "*Disquitiones arithmeticae*"; The Quadratic Reciprocity Law, The Method of Least Squares.
***Pierre de Fermat** (1601-1665) – French – "*Varia opera Mathematica*", Number Theory. In 1637 – The great Fermat Theorem.
***Leonhard Euler** (1707-1783) – Swiss – Number Theory. He introduced:
- The notion of general and particular solution in Differential Equation Theory,
- The congruency notion and its notation "≡", in 1801.

***Pafnuti Lvovici Chebyshev** (1821-1894) – Russian – Number Theory. He gave the formula for numerical approximation of the prime numbers less or equal to a given number.
***Georg Cantor** (1845-1918) German – Number Theory:
- The analytic numeric theory,
- The geometric numeric theory.

***Herman Minkowschi** (1866-1909) – The geometry of numbers theory.
***Johann Peter Gustav Lejeune Dirichlet** (1805-1859) – The Analytical Number Theory.
***Dan Barbilian (Ion Barbu)** (1895-1961) – Number Theory.
***Gabriel Sudan** (1899-1977) – Computational Theory.
Grigore Moisil: when he was 28 he became doctor docent in mathematics having had published already 274 paper works.

3. <u>Mathematical Results</u>.

Observation: 0 is divisible by 0!

Property:

$\varphi(0) = 2$

$\varphi(\pm 1) = 1$,

where φ is Euler's function.

Observation: There exists $\sqrt[1]{s}$, and $\sqrt[1]{s} = s$.

Property: $(n+1)(n+2)\cdots(n+n) = 2^n \cdot 1 \cdot 3 \cdot 5 \cdots (2n-1)$.

Definition: $\sum a_1 ... a_m$ is the sum of all possible circular permutations of m numbers from N.

Giuseppe PEANO (1858-1932).

The Peano axioms: to create an axiomatic arithmetic (the natural number axiomatization).

1. There is the number 1 which does not follow after any other number.
2. Any natural number n has a successor n' and only one, therefore
   From $a = b$ results $a' = b'$.
3. From $a' = b'$ results $a = b$ (i.e. a natural number cannot be the successor of multiple numbers.
4. The induction axiom: If a sentence P is referring to any natural number n and if
   - 1 is proved for n=1,
   - 2 from the hypothesis of its validity for $n = m+1$, it results that P is true for any n.

(Some mathematicians and philosophers contest its validity, because he numbers the axioms 1, 2, 3, 4.)

Two journals: MATHESIS - 1898, and "Mathematical Review" – 1958.

Property (Brocard): The numbers whose square end in two equal digits are those numbers that end in 0, 12, 62, 38, 88.

Property (I. Ionescu): The numbers that multiplied by 9 that give as product the same numbers flipped are: $N = n_1 n_2 n_3 ... n_3 n_2 n_1$, where n_i are numbers (solutions) of the property's statement (explanation $n_i = 0...0$, or 1809,…).

Property: $(a+b)(b+c)(c+a) \geq 8abc$, $a, b, c \geq 0$.

(SF- generalization)

Property: $a^2 + b^2 + c^2 \geq ab + bc + ca$; it can be generalized.

Property (E. Cesaro): $a^p + (a+1)^p + ... + (a+9)^p$ ends as follows:

in 5, if $p \neq \mathcal{M}_4$,

in 3, if $p = \mathcal{M}_4$.

Property: If $a+b=$ constant , then $a\cdot b$ is maxim, when $a=b$ or $a=b-1$ (it depends if $a+b$ is divisible by 2).

Property: If $a_1+...+a_n=k>n$, where k constant, then $a_1...a_n$ is maximum for any a_ia_j or $a_i=a_j$ or $a_i=a_j-1$, ($a_j=a_i-1$).

Property: The sum of the squares of n natural numbers of a given sum is a minimum when any of the following numbers are equal or they differ by a unit:

Notations:

$N=\{0,1,2,...\},\ N^*=\{1,2,...\}$.

Integer Numbers:

- Rational: $a,\ a\in Z$;
- Complex: $a+ib,\ a,b\in Z$.

Property: The number of solutions in N of equation $x_1+x_2+...+x_{p+1}=n$ is

$$\frac{(n+1)(n+2)...(n+p)}{1\cdot 2\cdot ....\cdot p}$$

Definition: Magic squares are the squares filled with natural numbers with the property that the sum of the numbers on each line, each column, and each diagonal is the same.
Albrecht Dürer (1514) – painter and mathematician, introduced the magic square notion.
Bachet de Meziriac (1612) – wrote the "Mathematics for fun".

Property: There exist an infinity of prime numbers of the form $4k-1;\ \ 6k-1$.

Property: If three prime numbers are in arithmetic progression then the ratio is $\mathcal{M}_6$ (except for 3, 5, 7).

Observation: If $p, 8p-1=prime$, then $8p+1=$ is a composite number.

Property: If $(a,b)=1$, then $(a+b,a-b)=1\ or\ 2$.

Property: If $(a,b)=1$, then $(11a+2b,18a+5b)=1\ or\ 19$.

Property: If $2^n+1=$ *prime number* **,** then $n=2^\alpha$ **.**

Property: If $A^m+B^n=$ *prime number* , then $(m,n)=2^\alpha$.

Property: If $n=impar$, then a^n+1 are not prime numbers.

Property: There are n consecutive numbers non prime.

Proof: $\left((n+1)!+2,...,(n+1!+(n+1)\right)$

Definition: The Fermat's numbers $2^{2^n}+1$ prime.

Property (Gauss): A regular polygon with p sides can be designed with only the ruler and the compass only when $p=2^{2^n}+1$ and $p=2^{2^n}+1$ is a prime number.

Property: **The Euler's polynomial** x^2+x+41, for $x=\frac{1}{0,39}$ gives different prime numbers.

Property: $P(n)=n^2+n+17$ is a prime number for $n=0,1,2,3,...,15$.

Property: There does not exist a polynomial (excluding the identical polynomial) with coefficients in Z such that for any $x\in Z$, $P(x)$ is a prime number.

Property: The expression $\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+...$ gives the exponent of the prime number p when n is decomposed in prime factors!

Property: $\left[\frac{a_1+\cdots+a_n}{b}\right]\geq\left[\frac{a_1}{b}\right]+\cdots+\left[\frac{a_n}{b}\right]$.

Property: If $(a,b)=1$, then

$$\left[\frac{a}{b}\right]+\left[\frac{2a}{b}\right]+...+\left[\frac{(b-1)a}{b}\right]=\left[\frac{b}{a}\right]+\left[\frac{2b}{a}\right]+...+\left[\frac{(a-1)b}{a}\right]=\left[\frac{1}{2}\right](a-1)(b-1)$$

Property: $\tau_1+...+\tau_n=\left[\frac{n}{1}\right]+\left[\frac{n}{2}\right]+...+\left[\frac{n}{n}\right]$, where τ_i is the sum of the divisors of i.

Property (Iacobi): – An arithmetic progression, in which the ratio and the first term are co-prime (relative prime) numbers, contains an infinity of members that are prime with any given number.

Definition: Perfect Number is a number for which the sum of all positive divisors, strictly smaller than itself, is equal with the number itself. (Example: 6, 28, 496, 8128).

Property: Even perfect numbers have the general form: $N=2^t(2^{t+1}-1)$, where $t\in N$, $2^{t+1}-1$ is a prime number.

Theorem: If N is odd, perfect, then N has at least four different prime factors ($N>10^{20}$).

Property: $\sum_{k=1}^{n}\frac{1}{k(k+1)}=1-\frac{1}{n+1}$

Property: $1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+...+\frac{1}{2n-1}-\frac{1}{2n}=\frac{1}{n+1}+\frac{1}{n+2}+...+\frac{1}{2n}$

Property: $\sum_{k=1}^{\infty}\frac{(-1)^{k+1}}{k}=\ln 2=\lim_{n\to\infty}\sum_{k=1}^{n}\frac{1}{n+k}$

Property: For $n>1$, we have $\frac{1}{2}<\frac{1}{n+1}+...+\frac{1}{2n}<\frac{3}{4}$

Property (Hermite): $[x]+\left[x+\frac{1}{n}\right]+...+\left[x+\frac{n-1}{n}\right]=[nx]$

Theorem: Given an irreducible fraction $\frac{a}{b}$ we have:

1. If $2\nmid b$ and $5\nmid b$, then $\frac{a}{b}$ transforms in a simple periodical decimal fraction.
2. If $b=2^{\alpha}5^{\beta}p_1...p_n$, where $n\geq 1$ and $\alpha\neq 0$ or $\beta\neq 0$, then $\frac{a}{b}$ transforms in a mix periodical function with the non-periodical part being of $\max\{\alpha,\beta\}$ digits.

Definition: Continued fraction is an expression of the following form:

$$a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+...}},$$

$[a_1, a_2, a_3, ...]$, where $a_2, a_3, ... \in N$, $a_i \in Z$, a_i are called the elements of the continued fraction, or incomplete quotients.
The continued fractions can be:

1. Limited
2. Unlimited
    a. Periodically simple $[a_1, a_2, ..., a_n; a_1, a_2, ..., a_n; ...]$
    b. Periodically mixed $[b_1, ...b_k; a_1, ..., a_n; a_1, ..., a_n; ...]$

Definition: Fibonacci sequence.

A recursive sequence:

$$\begin{aligned} u_1 &= u_2 = 1 \\ u_n &= u_{n-1} + u_{n-12} \end{aligned};$$

It results:

$$u_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

Property: $\frac{n}{\frac{1}{a_1}+...+\frac{1}{a_n}} \le \sqrt[n]{a_1...a_n} \le \frac{a_1+...+a_n}{n}$

Harmonic mean ≤ Geometric mean ≤ Arithmetic mean.

Property: $\frac{a_1}{a_2}+\frac{a_2}{a_3}+...+\frac{a_{n-1}}{a_n}+\frac{a_n}{a_1} \ge n$

Property: If $x_1 + x_2 + ... + x_n = a$, where a is a constant, then $x_1^{P_1}...x_1^{P_n}$ for $p_i \ge 0$, is maxim when $\frac{x_1}{p_1} = ... = \frac{x_n}{p_n}$.

Property: $a_i \ge 0$, $\left(\frac{a_1+...+a_n}{n}\right)^k \le \frac{a_1^k+...+a_n^k}{n}$, $k \ge 0$.

The Cauchy-Buniakovski Inequality:

$$\left(a_1b_1 + ... + a_nb_n\right)^2 \le \left(a_1^2 + ... + a_n^2\right)\left(b_1^2 + ... + b_n^2\right)$$

We have equality when: $\frac{b_1}{a_1} = ... = \frac{b_n}{a_n}$

Property: $\left(h_1 + ... + h_n\right)^p \equiv h_1^p + ... + h_n^p \pmod p$

Property: $\varphi(a \cdot b) = \frac{\varphi(a) \cdot \varphi(b).(a,b)}{\varphi\left((a,b)\right)}$

Property: Let's consider N an odd number, then among the smaller numbers than N and prime with N there exist as many even numbers as odd numbers.

Property: Let's consider $S = 1^n + 2^n + ... + (p-1)^n$

1. If $n = \mathcal{M}_{(p-1)}$ then $S \equiv -1 \pmod p$
2. If $n \ne \mathcal{M}_{(p-1)}$ then $S \equiv 0 \pmod p$

Property (Gauss): The product of all primitive solutions is congruent to $1(\text{mod } p)$; $p \neq 3$

Property: $a^1 \cdot a^2 \cdots a^\delta \equiv (-1)^{\delta+1} (\text{mod } p)$, where $a^i \not\equiv a^j (\text{mod } p)$, for $\forall i \neq j$, and $a^1, \cdots, a^\delta$ constitute all the residues modulo p.

Property (Gauss): $a^1 + a^2 + ... + a^\delta \equiv 0(\text{mod } p)$, where $a^i \not\equiv a^j (\text{mod } p)$, for $\forall i \neq j$ and $a^1, \cdots, a^\delta$ constitute all the residues modulo p.

Property: $x^n - y^n = (x-y)\left(x^{n-1} + x^{n-2}y^1 + ... + x^1 y^{n-2} + y^{n-1}\right)$

Property: If n is odd, then

$$x^n + y^n = (x+y)\left(x^{n-1} - x^{n-2}y^1 + x^{n-3}y^2 - ... + y^{n-1}\right)$$

Definition: a is a square residue in rapport to the prime modulo p if the congruence $x^2 \equiv a(\text{mod } p)$ has solutions.

Theorem: The congruence $x^2 \equiv a(\text{mod } p)$ has:

1. Two solutions: x_0 and $p - x_0$ for a taking $\frac{p-1}{2}$ values
2. No solutions for a taking $\frac{p-1}{2}$ values

The Euler criterion:

1. If $a^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$, then a is a squared residue
2. If $a^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$, then a is a squared non-residue

Legendre's symbol:

$$\frac{a}{p} = \begin{cases} -1, \text{ if } a \text{ is squared non-residue in rapport with modulo } p \\ +1, \text{if } a \text{ is squared residue in rapport with modulo } p \end{cases}$$

Property: $\left(\frac{a_1 ... a_k}{p}\right) = \frac{a_1}{p} ... \frac{a_k}{p}$

Definition: The minimal absolute residue is the residue r for which $r \leq \frac{p-1}{2}$. If the residue $r > \frac{p-1}{2}$, will take $p - r$.

The reciprocity law: If p, q are prime, then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Theorem: Any natural number can be represented as a sum of at most four squares.

Dirichlet' s Theorem: If $(a,b) = 1$, then there exist an infinity of numbers of the form $a + b \cdot k$.

Observation: A pair of prime twin large numbers is:

10016957, 10016959.

Bertrand's Theorem: (proved by Chebyshev (1821-1894)): Between n and $2n$, $n > 1$, there exists at least one prime number.

Euclid's Theorem: There exist an infinity of prime numbers.

Observation: The prime numbers' density diminishes while advancing in the natural numbers' sequence.

Property (Euler): The series $\frac{1}{2^a}+\frac{1}{3^a}+\frac{1}{5^a}+...+\frac{1}{p^a}+...$ is divergent.

Property (Hogatt): Any natural number is the sum of some distinct terms of the Fibonacci' sequence.

4. Philosophy.

The mathematics cannot be axiomatically created; it cannot be reduced to a formal logic. Its notions are created in contact with the reality (although some mathematical domains can be made axiomatic).
The axiomatic is just a superior phase of abstract; it is a transcription in the logical mold of known processes and directly tested or examined.

Learn, teaching others. (Seneca)
The wisdom comes with ages. (Ovidius)
The experience is gained through diligence. (Shakespeare)
The forest cannot be seen because of the trees. (*Proverb*)
The art is the highest expression of an interior arithmetic. (Leibnitz)
Repeated things are pleasant. (Horatio)

5. Series.

$$\sum_{k=1}^{n} k\cdot k! = (n+1)!-1$$

$$\sum_{k=1}^{n} k(k+1)(k+2) = \frac{1}{4}n(n+1)(n+2)(n+3)$$

$$\sum_{k=1}^{n} k^2 = \frac{2n+1}{6}$$

$$\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$$

$$\sum_{k=1}^{n} k^4 = \frac{1}{30}n(n+1)(2n+1)(3n^2+3n-1)$$

$$\sum_{k=1}^{n} k^5 = \frac{1}{12}n^2(n+1)^2(2n^2+2n-1)$$

$$\sum_{k=0}^{n} (k+1)x^k = \frac{(n+1)x^{n+2}-(n+2)x^{n+1}+1}{(x-1)^2}$$ (it is proved using with derivatives)

$$\sum_{k=1}^{n} 2^k(tg2^k x) = 2ctg2x - 2^{n+1}ctg2^{n+1}x$$

6. Inequalities.

1. $2^n n! < (n+1)^n$, for $n > 1$.
2. $2!4!...(2n)! > \left[(n+1)!\right]^n$, for $n > 1$.
3. $n^n < \left(n!\right)^2 < 2^{n(n-1)}$, for $n > 2$.
4. $\sqrt[n]{n} < \dfrac{2+\sqrt{n}}{\sqrt{n}}$
5. If $a_i, b_i \geq 0$, $\dfrac{1}{p}+\dfrac{1}{q}=1$, then $a_1 b_1 + ... + a_n b_n \leq \left(a_1^p + ... + a_n^p\right)^{\frac{1}{p}} \left(b_1^q + ... + b_n^q\right)^{\frac{1}{q}}$
6. **The Stirling's Inequality**: $\sqrt{2\pi n}\left[\dfrac{e}{n}\right]^n < n! < \sqrt{2\pi n}\left[\dfrac{e}{n}\right]^n \cdot e^{\frac{1}{mn}}$
7. $\dfrac{1}{n^2+1}+\dfrac{1}{n^2+2}+...+\dfrac{1}{n^4} > 2\left(\dfrac{1}{2}+\dfrac{1}{3}+...+\dfrac{1}{n}\right)$
8. $\dfrac{1}{5n+1}+\dfrac{1}{5n+2}+...+\dfrac{1}{25n} > \dfrac{7}{6}$, where $n \in N$.
9. **The Jensen's Inequality**:
   Let's $f : I \to R$ and $epi(f) = \left\{\mathcal{M}(x,y) : x \in I, y \geq f(x)\right\}$ the epigraph (super graph) of f, then the $epi(f)$ is the a convex set $\Leftrightarrow$ $x_1, x_2 \in I$ and $t \in [0,1]$, we have $(1-t)x_1 + tx_2 \in I$ and $f\left((1-t)x_1 + tx_2\right) \leq (1-t) f(x_1) + tf(x_2)$.
10. **The Young-Fenchel Inequality**: Let's consider f convex, defined on an interval I, then:
    $\sup\left\{ax - f(x) : x \in I\right\} + f(x) \geq ax$, for $\forall x \in I$.

7. <u>More Properties</u>.

Property: $f(x) = ax^2 + bx + c$; $f(x) \in Z$, $\forall x \in Z$, if and only if $2a,\ a+b,\ c \in Z$.

Property (Erdös): $\forall k \in Z,\ k = \pm 1^2 \pm 2^2 \pm ... \pm m^2$, where m is dependent of k, and we can select the corresponding signs.

Property: $(n+1)(n+2)...(pn)$ is divisible by p^n.

Property: $(m_1 + ... + m_n)! = \mathcal{M}_{m_1! m_2! ... m_n!}$

Property (Cantor): If n prime numbers form an arithmetic progression, then the progression's ratio is divisible by every prim number $p < n$.

Observation: An arithmetic infinite progression of different natural numbers cannot have all its terms prime numbers.

Liouville's Theorem: The equation: $(p-1)!+1 = p^m$, for p prime and greater than 5, $m \in N$, does not have any solution.

Cucurezeanu's Theorem: If p prime and greater than 7, $k, m \in N$, and $1 \leq k \leq p$, then the equation: $(k-1)!(p-k)!+(-1)^{k+1} = p^m$ does not have any solution.

Property: There exist an infinity of prime numbers q with the property $q \mid (n-1)!+1$ for $n<2$.

Chebyshev's Theorem: Between n and $2n$, $n>1$, there exist at least a prime number (Bertrand's postulate).

Chebyshev's Theorem: Between n and $2n$, $n>3$, there exist at least a prime number.

Theorem: Between n and $2n$, $(n>5)$, there exist at least 2 prime numbers.

Cucurezeanu's Theorem: Between $2n$ and $3n$, $n>1$, there exist at least one prime number.

Property (Cucurezeanu): Between n and $\frac{3}{2}n$, there exist at least one prime number.

Property: If p_n is the nth prime number, then $p_n^2 < 2^n$ for $n \geq 10$.

Property: Between n and $3n$, $n>1$, there exist at least 2 prime numbers.

Property (Sierpinski): $\forall a,b \in N$, $a \neq 1$ or $b \neq 1$, there exist an infinity of n natural numbers with the property: $n \mid a^n + b^n$.

Property: The exponent of the prime number p, from the following canonic decomposition $1 \cdot 3 \cdot 5 \cdots (2m+1)$ is:

$$\left(\left[\frac{2m+1}{p} \right] + \left[\frac{2m+1}{p^2} \right] + \ldots \right) - \left(\left[\frac{m}{p} \right] + \left[\frac{m}{p^2} \right] - \ldots \right)$$

Property: The number of the multiples of n smaller than x, is $\left[\frac{x}{n} \right]$.

Property: $\tau(n) = \sum_{m \geq 1} \left(\left[\frac{n}{m} \right] - \left[\frac{n-1}{m} \right] \right)$

Property: $p^n \nmid \left[(p-1)n \right]!$, $n \in N$.

Canonic decomposition = decomposition in prime factors

Definition: Fermat numbers. $2^{2^n}+1 = F_n$,

$F_0 = 3$

$F_1 = 5$

$F_2 = 17$

$F_3 = 257$

$F_4 = 65537$

F_0, F_1, F_2, F_3, F_4 are prime numbers;

$F_5 = 4294967297 = 641 \cdot 6700417$

$F_6 = 18446744073709551617 = 274177 \cdot 67280421310721$

F_{1945} is divided by $5 \cdot 2^{1947}+1$ (which has 587 digits).

F_{12} is divisible with 114689.

F_{25} is divisible with 167772161.

F_{36} is divisible with 27487790694411 and it has 20 billion digits (Seelhof from Bremen).

F_{16} is divisible by $2^{18}\times 3150+1$.

F_{17} are 39457 digits, it is unknown if it is prime.

Property (Gauss): Using a ruler and a compass we can design polygons for which the number of sides is a number from the Fermat's sequence (which are prime numbers).

Property: $a^n > \frac{(a-1)^2}{4}\cdot n^2$, for $a>1$, $n\geq 2$.

Property: If $S_n=\sum_{k=1}^{n}\frac{x^k}{\left(1+x^{k+1}\right)\left(1+x^{k+1}\right)}$, $x\neq 1$, then

$$S_n=\frac{1}{x(1-x)}\left[\frac{1}{1+x^{n+2}}-\frac{1}{1+x^2}\right].$$

Observation: $2^{127}-1$ is prim number (the bigger known in 1934). It has 39 digits.

$180\left(2^{127}-1\right)^2-1$ is a prime number (1950).

$2^{2281}-1$ is a prime number (Prof. Lehmer, 1956).

$2^{4423}-1$ is a prime number with 1332 digits (Hurwitz in 1961, Selfridge, IBM, 7090 digits)

$2^{11273}-1$ the largest known prime number (computer generated).

$2^{257}-1$ is a composite number; $\underbrace{1\ldots1}_{23ori}$, is a prime number (M. Kraitchik).

Property (I. M. Vinogradov): There are values for a and p such that $a^p \equiv a(\text{mod } p^2)$.

Property: $e=2.7182818284...$ is an irrational number.

Property: The last digit non zero of

$$10^n!=\begin{cases}8, \ if \ n=1\\ 4, \ if \ n=2\\ 6, \ if \ n\geq 3\end{cases}$$

Property: If $p\geq 3$ is a prime number, $a,n\in N$, if $p^n=1+a^1+\ldots+a^p$, then $a=n=0$.

Theorem: Let's consider $x_i\geq 0$. If $x_1\cdots x_n=1$, then $x_1+\ldots+x_n\geq n$.

Property: If $a_i\geq 0$, $\alpha<0<\beta$, then

$$\left(\frac{a_1^\alpha+\ldots+a_n^\alpha}{n}\right)^{\frac{1}{\alpha}}\leq \sqrt[n]{a_1\cdots a_n}\leq\left(\frac{a_1^\beta+\ldots+a_n^\beta}{n}\right)^{\frac{1}{\beta}}$$

Property: $\sum_{n=1}^{\infty}\frac{n}{P_{p_n}}$ and $\prod_{n=4}^{\infty}\frac{1}{1-\frac{n}{P_{p_n}}}$ are divergent (p_n is the n th prime number).

Property (Waclaw Sierpinski): $\lim_{n\to\infty}\frac{p_n}{n\ln n}=1$, ($p_n$ is the n th prime number).

Property: $\sum_{n=1}^{\infty}\frac{1}{p_n}$ and $\prod_{n=2}^{\infty}\frac{1}{1-\frac{1}{p_n}}$ are divisible, (p_n is the n th prime number).

Property: $n\varphi(n!)\le n!\varphi(n)$, φ being Euler's function.

Property: The sum of the prime numbers with A and smaller than A is $s(A)=\frac{1}{2}A\varphi(A)$ where φ is Euler's function.

Property: $B^2 s(A)\le A^2 s(B)$, $A>B$, B contains only A factors, $s(A)$ is the sum of all prime numbers with A and smaller than A.

Property (Tiberiu Popoviciu): $\varphi(a,b)\le\sqrt{\varphi(a^2)\varphi(b^2)}$, $a,b\in N$, where φ is Euler's function.

Property: If $N=p_1^{\alpha_1}...p_n^{\alpha_n}$, $\alpha_i>1$, then $\varphi(N)$ determines uniquely N.

8. Criteria for Prime Numbers.

Wilson's Theorem: If $p>1$, then p is prime if and only if $(p-1)!\equiv -1(\text{mod } p)$.

Leibnitz's Theorem: If $p>2$, then p is prime if and only if $(p-2)!\equiv +1(\text{mod } p)$

Smarandache Criterion: If $p>3$, then p is prime if and only if

$(p-3)!\equiv\frac{p-1}{2}(\text{mod } p)$.

Smarandache Criterion: If $p=6h\pm1>4$, then p is prime if and only if

$(p-4)!\equiv\pm h(\text{mod } p)$.

Smarandache Criterion: If $p=24h+r>5$, $0\le r\le 24$, then p is prime if and only if

$$(p-5)!\equiv r\cdot h+\frac{r^2-1}{24}.$$

Smarandache Criterion: If $p=(k-1)!h\pm1$, then p is prime if and only if

$$(p-k)!\equiv\pm(-1)^k h(\text{mod } p).$$

Simionov's Criterion: If $1\le k\le p$, then p is prime if and only if

$$(k-1)!(p-k)!\equiv(-1)^k(\text{mod } p).$$

Criterion: p is prime if and only if $k\cdot\left[\frac{p}{k}\right]\ne p$, $k\ge 2$, $k\ne\mathcal{M}_p$.

Criterion: p is prime if and only if $k\cdot\left[\frac{p}{k}\right]\ne p$, $\forall k$, $2\le k\le\left[\sqrt{p}\right]$.

Fermat's Theorem: p is prime, $a\ne\mathcal{M}_p$, then $a^{p-1}\equiv 1(\text{mod } p)$.

Fermat's Theorem: p is prime, $a\ne\mathcal{M}_p$, then $a^p\equiv a(\text{mod } p)$.

Euler's Theorem: $(a,m)=1$, then $a^{\varphi(m)}\equiv 1(\text{mod } m)$, φ is the Euler function.

Moser's Theorem: p is prime, $a \in Z$, then $(p-1)!a^p + a = \mathcal{M}_p$.

Sierpinski's Theorem: p is prime, $a \in Z$, then $a^p + (p-1)!a = \mathcal{M}_p$.

Clement's Theorem:

$$\left.\begin{array}{l} p = prime \\ p+2 = prime \end{array}\right\} \Leftrightarrow 4\left[(p-1)!+1\right] + p \equiv 0 \left(\mathrm{mod}\ p(p+2)\right).$$

Cucuruzeanu's Theorem: (a generalization of Clement's theorem):

$$\left.\begin{array}{l} (p,i) = 1; \quad p = prime \\ i = \overline{2, n-1}; \ p+2 = prime \end{array}\right\} \Leftrightarrow n \cdot n!\left[(p-1)!+1\right] + \left[n! - (-1)^n\right] p \equiv 0 \left(\mathrm{mod}\ p(p+n)\right)$$

Property: If p is prime and $1 \le k \le p-1$, then:

1. $C_{p+k}^k \equiv 1 (\mathrm{mod}\ p)$.
2. $C_{p-1}^k \equiv (-1)^k (\mathrm{mod}\ p)$.

Property: If $a \equiv b (\mathrm{mod}\, m^n)$, then $a^m \equiv b^m \left(\mathrm{mod}\, m^{n+1}\right)$ (Proof with the Newton's binomial).

Property: If p is prime and $a^p \equiv b^p \left(\mathrm{mod}\ p\right)$, then $a^p \equiv b^p \left(\mathrm{mod}\ p^2\right)$.

Property: If p is prime, $p > 3$, then $a^p \equiv a \left(\mathrm{mod}\, 6p\right)$.

Property: If p and q are prime, $p \ne q$, $a^p \equiv b^p \left(\mathrm{mod}\ p\right)$, $a^q \equiv b^q \left(\mathrm{mod}\, q\right)$, then

$$a \equiv b \left(\mathrm{mod}\ pq\right).$$

Observation: If $a \equiv b \left(\mathrm{mod}\, m_1\right)$, $a \equiv b \left(\mathrm{mod}\, m_2\right)$, and $\left(m_1, m_2\right) = 1$, then

$$a \equiv b \left(\mathrm{mod}\, m_1 m_2\right).$$

Property: If p is prime, $(a, p) = 1$, and $a^{p-1} + b^{p-1} \equiv 0 (\mathrm{mod}\ p)$, then

$a^{p-1} + b^{p-1} \equiv 0 (\mathrm{mod}\ p^{p-1})$, (proof for $p = 2$).

Property: If p is prime, $p > 5$, then any number formed of $p-1$ equal digits, will be divisible by p.

Property: If p is prime, $p \ne 2$ and $a^p + b^p \equiv 0 (\mathrm{mod}\ p)$, then $a^p + b^p \equiv 0 (\mathrm{mod}\ p^2)$.

Property: If $m = p_1 \cdots p_s$, $p_i \ne p_j$, p_i and p_j prime numbers, and $a^m \equiv b^m \left(\mathrm{mod}\, m\right)$,

then $a^m \equiv b^m \left(\mathrm{mod}\, m^2\right)$.

Property: The last 3 digits of $N = n^{100}$ are:

$$\begin{cases} 000, \ if \ \ n = 10k \\ 001, \ if \ \ n = 10k \pm 1, \ n = 10k \pm 3 \\ 376, \ if \ \ n = 10k \pm 2, \ n = 10k \pm 4 \\ 625, \ if \ \ n = 10k + 5 \end{cases}$$

Property: If $\left(a, m\right) = 1$, then the congruence $ax \equiv b (\mathrm{mod}\, m)$ solution is

$x \equiv b a^{\varphi(m)-1} (\mathrm{mod}\, m)$, φ is Euler's function.

Property: If $\left(a, b\right) = 1$, then $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 (\mathrm{mod}\, ab)$.

Property: If $p \neq q$, p, q are prime, then $p^{q-1} + q^{p-1} \equiv 1 (\text{mod } pq)$; (consequence of the previous property).

Property: If $(m,10) = 1$, then there exist a multiple of m of the form $\overline{\underbrace{a \cdots a}}$, with $a \in \overline{1,9}$

Property (W. Sierpinski): Let $s \in N$, then there exist $n \in N$ such that $s \mid n$ and the sum of the digits of n is equal to s.

Proof: $s = 2^{\alpha} 5^{\beta} t$, $(10,t) = 1$, then $n = 10^{\alpha+\beta}\left[10^{\varphi(t)} + 10^{2\varphi(t)} + ... + 10^{s\varphi(t)}\right]$.

Property: If $(a,n) = 1$, then $n \mid a^{(n-1)!} - 1$.

Property: If n is an even number, then $(n^2 - 1) \mid 2^{n!} - 1$.

Property: There does not exist $n > 1$ such that $n \mid (a+1)^n - a^n$, for $\forall a \in Z$.

Theorem (I. Moser): If p is prime, $\forall a$, then $(p-1)!a^p + a = \mathcal{M}_p$ (Fermat and Wilson theorem put together).

Theorem: If p is prime, $\forall a$, then $a^p + (p-1)!a = \mathcal{M}_p$.

Property: There is an infinity of composite numbers of the form: $(n!)^2 + 1$.

Property: If $n < p$, then p is prime if and only if $\dfrac{(n+1)...(n+p)}{p} + 1 = \mathcal{M}_p$ (Gh. Zapan).

Property: If p is prime; $A = a_0 x^n + ... + a_n$, $a_n \neq db_p$, $a_i \in Z$, if there exist $x_0 \in Z$ such that $p \mid A$, then there exist an infinity of $y \in Z$ such that $p \mid B = a_n y^n + ... + a_0$.

Proof: y has the property $x_0 y \equiv 1 (\text{mod } p)$.

Property: If n is odd, then $n \mid 1^n + 2^n + ... + (n-1)^n$.

Theorem: For $n > 2$, between n and $n!$ there exist at least a prime number.

Theorem: Any natural number greater or equal to 2 has at least a prime divisor.

Theorem: There exist at least 3 prime numbers each containing s digits ($\forall s \in N^*$).

The Eratosthenes Sieve.

Observation: There are**:**

4 prime numbers of 1 digit;
21 prime numbers of 2 digits;
163 prime numbers of 3 digits.

Statistics: 6,000,000 prime numbers. $P_{6,000,000} = 104,395,301$.

American scientists have a computer that will store in its memory the first 500,000,000 consecutive prime numbers.

There are 152,892 pairs of twin prime numbers until 30,000,000.

Property (Cucurezeanu): If $\forall x \in R$, $\prod_{\substack{p \leq x \\ p \text{ prime}}} p < 3,3^x$;

if $\forall x > 29$, $\prod_{p \leq x} p \geq 2^x$.

Property: $\frac{3}{4}\cdot\frac{x}{\ln x}<\prod(x)<\frac{3}{2}\frac{x}{\ln x}$, where $\prod(x)$ is the number of the prime numbers $\le x$.

Property (A. Schinzel): If $\min\{x,y\}\le 146$, then

$$\prod(x+y)\le\prod(x)+\prod(y).$$

Property: The exponent of the prime number p from $\frac{a!}{b!c!}$ is

$$\left(\left[\frac{a}{p}\right]-\left[\frac{b}{p}\right]-\left[\frac{c}{p}\right]\right)+\left(\left[\frac{a}{p^2}\right]-\left[\frac{b}{p^2}\right]-\left[\frac{c}{p^2}\right]\right)+\ldots.$$

Property (Vinogradov): $\forall n>3^{3^{16}}$, n odd, ca be written as the sum of 3 different odd prime numbers. (Until the number $3^{3^{16}}$ the property was unknown).

Observation: The $\underbrace{1\ldots1}_{37times}$ is a composite number; the number $\underbrace{1\ldots1}_{641times}$ is divisible by 1283.

Observation: ***There exist prime numbers that remain prime after any permutation of their digits.

Examples: 13 and 31; 17 and 71; 37 and 73; 79 and 97;
113 and 131, 311; 199, 919, 991; 337, 373, 733.

Property (H. E. Richert): For $3<n<6\cdot10^{175}$ there does not exist prime numbers with the property (*), except of those that are formed with only digit 1.

F. Smarandache: A prime number of the form (*) is formed only with digits: 1, 3, 7, 9.

Proof: If the number would have also the digits: 0, 2, 4, 5, 6, 8 by permutations these digits will take the last position and, therefore, they'll be divisible by 2 or 5.

Theorem (W. Sierpinski): Let's consider $a_1,\ldots,a_m$ and $b_1,\ldots,b_n$ with $b_1,\ldots,b_n\in\{1,3,7,9\}$, then there exist an infinity of prime numbers of the form: $p=\overline{a_1\cdots a_m r_1\cdots r_s b_1\cdots b_n}$ (that start with $a_1\cdots a_m$ and end with $b_1\cdots b_n$).

Observation: It is not known if there exist an infinity of prime numbers formed only with the digit 1.

Statistics: L. Moser found all the prime numbers smaller than 100,000 if the digits from which are formed are written in an inverse order. (There are 102 prime numbers of this kind which are less than 100,000.)

Examples: The numbers of this gen less than 1,000 are:
101, 131, 151, 181, 313, 353, 373, 383, 727, 757, 787, 797, 919, 929.

Observation: It is not known if there exist an infinity of this type of numbers.

Property (Sierpinski): $\forall a,b\in N^*$, there exist p,q prime numbers such that $a<\frac{p}{q}<b$.

Property: $\lim_{n\to\infty}\frac{p_{\Pi(nx)}}{n}=x$, $\forall x\in N$, p_h is the h-th prime number

Property: There exist an infinite set of prime numbers such that $p_n>\frac{p_{n-1}+p_{n+1}}{2}$.

Property: There exist an infinite set of prime numbers such that $p_n < \frac{p_{n-1} + p_{n+1}}{2}$.

Hypotheses: There exist an infinite set of prime numbers such that $p_n = \frac{p_{n-1} + p_{n+1}}{2}$.

Example: for $n = 16, 37, 40, 47, 55, 56, 240, 273$.

Theorem (Erdös, P. Turan): There is an infinity of prime numbers such that $p_n^2 > p_{n-1} p_{n+1}$.

There is an infinity of prime numbers such that $p_n^2 < p_{n-1} p_{n+1}$.

Observation: (quadruple) $p,\ p+2,\ p+6,\ p+8$ are prime.

Example: $p = 5, 101, 191, 821, 1481, 3251$.

Statistics: Among the first 10,000,000 numbers there are 899 quadruples (Golubev).

Among the first 15,000,000 numbers there are 1209 quadruples.

The largest known quadruple is $p = 2{,}863{,}308{,}731$ (A. Ferrier).

Property (B. M. Bredihin): There is an infinity of prime numbers of the form $x^2 + y^2 + 1$.

Property: There is an infinity of prime numbers of the form $x^2 + y^2$.

Hypothesis: there exists the polynomial: $P(n)$ such that for $n \in N$ will give an infinite of prime numbers? (not all values to be prime).

Example: for first degree there is $P(x) = 2x + 1$.

Hypothesis: Does $P(x) = x^2 + 1$ give an infinite of prime numbers?

Property (Van der Corput): There is an infinity of arithmetic progressions that are formed from 3 different prime numbers.

Example: 3, 7, 11; 3, 11, 19; 3, 43, 83; … .

The Chinese wrong theorem: If $n \mid 2^n - 2$, then n is a prime number. (This is true for $1 < n \le 300$).

Property (N. G. W. H. Beeger, 1951): There exist an infinity of even numbers n such that $n \mid 2^n - 2$.

Property: There exist an infinity of pairs of different prime numbers p, q such that $pq \mid 2^{pq} - 2$.

Theorem (A Schinzel): For $\forall a \in Z,\ \forall m \in N$, there exist p, q different such that $pq \mid a^{pq} - a$.

Definition: n is a pseudo prime number if n is a composite number such that $n \mid 2^n - 2$.

Definition: n is an absolute pseudo prime number if n is a composite number such that $\forall a \in Z$, $n \mid a^n - a$. The smallest is $561 = 3 \cdot 11 \cdot 17$.

Other examples are: $7 \cdot 17 \cdot 31, ..., 5 \cdot 17 \cdot 29 \cdot 113 \cdot 337 \cdot 673 \cdot 2689$.

Hypothesis: There exist an infinity of such numbers (not proved).

Property: If p is a prime number, then $1^{p-1} + 2^{p-1} + ... + (p-1)^{p-1} + 1$ is divisible by p.

Hypothesis (G. Giuca - 1950): If $1^{p-1} + 2^{p-1} + ... + (p-1)^{p-1} + 1$ is divisible by p, then p is a prime number (not proved). It has been verified for $n \le 10^{1000}$.

Property (Littlewood): Let's consider $\Pi_1(x)=$ the number of prime numbers of the form: $4k+1$, which are $\leq x$, then exists an infinity of natural numbers x such that $\Pi_1(x)>\Pi_3(x)$.

Let's consider $\Pi_3(x)=$ the number of prime numbers of the form: $4k+3$, which are $\leq x$, then exists an infinity of natural numbers x such that $\Pi_1(x)<\Pi_3(x)$.

Example: $\Pi_1(26862)=1473>1472=\Pi_3(x)$.

Property: Any natural number of the form $4k+3,\ 6k+5$ contains at least a prim divisor of the same form ($4k+3$, respectively $6k+5$).

F. Smarandache: Analogously for $3k+2$.

F. Smarandache: for $n=4k+1$ or $n=6k+5$ it is not true.

Property (Ingham): Between m $(m+1)^3$, there exists an arbitrary large number of prime numbers.

Theorem: If $(a,m)=1$, a is the primitive root modulo m iff a does not satisfy none of the congruencies: $a^{\frac{\varphi(m)}{p_1}}\equiv 1(\mathrm{mod}\, m),...,a^{\frac{\varphi(m)}{p_r}}\equiv 1(\mathrm{mod}\, m)$, where p_i are all prime positive divisors of $\varphi(m)$.

Theorem: a is the primitive root p, $t\in Z$ such that $(a+pt)^{p-1}=1+pu$, $p\nmid u$, then $a+pt$ is a primitive root modulo $\pm p^{\beta}$.

Theorem: If a is a primitive root modulo p^{β}, then the odd number between a and $a+p^{\beta}$ is the primitive root modulo $\pm 2p^{\beta}$.

Definition: $(a,m)=1$, $g=$ primitive root modulo m is called the index of a modulo m in rapport to the base g**.** The number γ with the property $a\equiv g^{\gamma}(\mathrm{mod}\, m)$; is noted $\gamma=ind_g a$ or $\gamma=inda$.

Observation: $ind_g a$ has a similar property with the algorithm.

Property: The number of primitive roots modulo m is $\varphi(\varphi(m))$.

The number of the residue classes modulo m, prime with m, of order δ is $\varphi(\delta)$.

Definition: $\frac{\sqrt{5}+1}{2}$ is called "*the golden number*"**.**

The principle of inclusion and exclusion:

$$Card\left(\bigcup_{i=1}^{q}A_i\right)=\sum_{i=1}^{9}CardA_i-\sum_{1\leq i<j\leq 9}Card\left(A_i\cap A_j\right)+...+(-1)^{9+1}Card\left(\bigcap_{i=1}^{9}A_i\right)$$

The formula of a multinomial:

$$(a_1+a_2+...+a_p)^n=\sum_{\substack{n_1+...+n_p=n\\ n_1,...,n_p\geq 0}}\binom{n}{n_1,n_2,...,n_p}a_1^{n_1}a_2^{n_2}...a_p^{n_p}\text{, where}$$

$$\binom{n}{n_1,n_2,...,n_p}=\frac{n!}{n_1!n_2!...n_p!}$$

Van der Waerden's theorem: For $\forall k,t$ positive integer numbers, there exists a natural number denoted $w(k,t)$ which is the smallest integer number with the following property: If the set $\{1,2,...,w(k,t)\}$ is partitioned in k classes, there exists a class of the partition which contains an arithmetic progression with $t+1$ terms. $w(k,t)$ is called the Van der Waerden number.

9. Diophantine Equations.

1. $x^2+2xy+y^2-x-3y-2z+2=0$, $x,y,z\in N$ (Ilie Iliescu).
   Solutions: $(x_1,y_1,z_1)=(1,1,1)$

$$(x_{n+1},y_{n+1},z_{n+1})=\begin{cases}(x_{n+1},y_{n+1},z_{n+1}), & if\ y_n\neq 1\\ (1,x_{n+1},z_{n+1}), & if\ y_n=1\end{cases}$$

   The function $f:N\times N\to N$, $f(x,y)=\dfrac{(x+y-1)(x+y-2)}{2}+x$ is bijective.
2. $x^2+x+y^2=0$ does not have solutions in N.
3. If $x,y,z\in N: x^2+y^2+1=xyz$, then $z=3$ (Ilie Iliescu).
4. $x^2+x-2y^2=0$; Solutions: $(x_1,y_1)=(1,1)$; $(3x_n+4y_n+1,2x_n+3y_n+1)$, $n\in N$ (Ilie Iliescu).
   Proof: $g:E\setminus\{(1,1)\}\to E$, $g(x,y)=(3x-4y+1,3y-2x-1)$ is bijective;
   $E=\{(x,y)\in N\times N / x^2+x-2y^2=0\}$.
5. $x^2+1-7y^2=0$ does not have a solution in Z. (Ilie Iliescu)
6. $x^2-2y^n=1$ has an infinity of solutions in Z. (Ilie Iliescu)
   Proof: $G=\{z\in R/z=x+y\sqrt{2},\ x,y\in Z,\ x^2-2y^n=1\}$, G multinomial,
   $M=\left\{\begin{pmatrix}a & b\\ 2b & a\end{pmatrix} | a,b\in Z\ \ a^2-2b^2=1\right\}$, M is multiplicative group.
   $G\approx M$.
   It results that if $z_1=x_1+y_1\sqrt{2}$ is a solution (x_1,y_1) of the equation, then $z_1^n=x_n+y_n\sqrt{2}$ it is also a solution (x_n,y_n).
7. (Gelfond) The equation $x^2+2y^n=z^2$ has the solutions:

$$\begin{cases}x=\pm(a^2-2b^2)\\ y=2ab\\ z=a^2+2b^2\end{cases},$$

where $a,b\in Z_+$, $(a,b)=1$, b odd.

10. Euclid's Algorithm extended.

$Z : a, b \in N^*$

$E : d, h, k \in Z$ such that $d(a,b)$; $d = ah + bk$

M :

1. $(u, v, x) \leftarrow (1, 0, a)$
   $(s, t, y) \leftarrow (0, 1, b)$
2. z is the residue of the division of x by y
3. If $z = 0$, then 6)
4. $q \leftarrow \left[\frac{x}{y}\right]$
   $(\xi, \eta, z) \leftarrow (u, v, x) - (s, t, y)q$
5. $(u, v, x) \leftarrow (s, t, y)$ and $(s, t, y) \leftarrow (\xi, \eta, z)$, goes to 3)
6. $(h, k, d) = (s, t, y)$

11. Binary Algorithm.

The calculation of the LCD (Least Common Denominator):

$I : a, b \in N^*$

$E : d = (a, b)$

M :

1. $x \leftarrow a, y \leftarrow b, k \leftarrow 0$
2. If $2 \nmid x$ and $2 \nmid y$ then 4)
3. $x \leftarrow \frac{x}{2}$, $y \leftarrow \frac{y}{2}$, $k \leftarrow k + 1$
4. If $2 \nmid x$, then 6)
5. $x \leftarrow \frac{x}{2}$, then 4)
6. If $2 \nmid y$, then 10)
7. $y \leftarrow \frac{y}{2}$, then 6)
8. If $x \leq y$, then 10)
9. $x \leftarrow x - y$, then 5)
10. If $x \geq y$, then 12)
11. If $y \leftarrow y - x$, then 7)
12. $d = 2^k x$

12. **Conclusion**.

My intention was to thinking at writing a handbook of elliptic function theory applied in number theory, but also a volume of amusing/amazing (!) (recreational) problems, that require fantasy thinking, deviation from the rational, and scientific tricks.