**Title**: New Argentest primality test algorithm.
**Author**: Zeolla, Gabriel Martin
**Comments**: 23 pages
gabrielzvirgo@hotmail.com

**Keywords:** Primality test, prime number, pseudoprime.

## Abstract:

This text develops a new Primality Algorithm, this one obtains opposite results to Fermat's little theorem, since it uses similar mechanisms but applied to the analysis of patterns.
In Fermat's Theorem there are always Pseudoprimes hidden among the primes, which does not give certainty about the primality of an odd number analyzed, beyond the change of bases as happens with the Pseudoprime number 561.
In the Argentest algorithm, the opposite happens, the pseudoprimes do not pass the test, so we can confirm the primality of a number with absolute certainty and determination, but there is a percentage of primes that do not pass the test either, so we go to the change of base to re-analyze the patterns and confirm primality later.

Then this new deterministic primality test algorithm uses two simple mechanisms, the first inspired by the Euler criterion, the second through the analysis of patterns formed by their remains, with these first two processes we can determine the primality of 70% of the set of prime numbers with 100% accuracy
For the remaining 30% of the set of primes there is a third process that consists of changing from base 2 to base 3 and then re-analyzing the patterns, this separates the pseudoprimes from the remaining prime numbers.
60% of the primes who did not pass before, now confirm their primality. 40% of the remaining primes and a small part of the base-2 pseudoprimes also fail the test. Therefore, we should change the base again and repeat the process to continue decanting these numbers.
With the combination of base 2 and base 3 we obtain the certification of primality for 90% of the set of prime numbers. For the remaining 10% we should repeat the process with another base change.

## Introduction

**Definition:** A Primality test is an algorithm that allows deciding whether a natural number (n) is prime or composite.
The Argentest seeks to solve primality with efficient calculations, although it can be achieved through graphical tables. The graphic tables is like a document of irrefutable primality. A unique stamp for each prime, like their own fingerprint. These tables are easily constructed, although for very large primes it is too long. So using efficient calculations is best applied for large numbers.

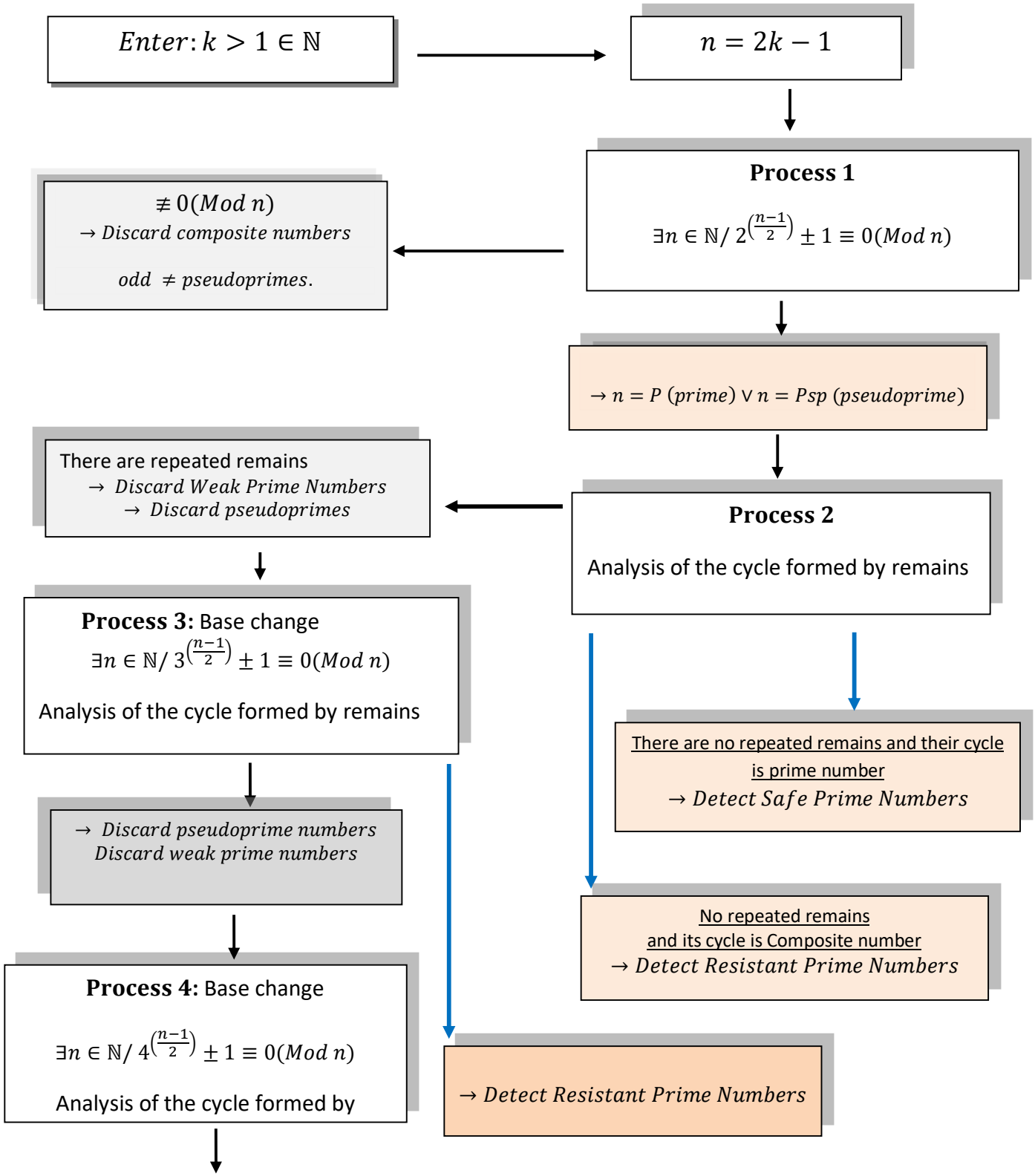
Professor Zeolla Gabriel M.

# Argentest

## Index

Professor Zeolla Gabriel M.

# How the Argentest algorithm works



Professor Zeolla Gabriel M.

## Chapter I

### Process 1: Primality Test for Odd Numbers

This process, like Fermat's little theorem, has the ability to separate numbers and classify them.
The formula used by the Argentest is closely linked to it, it uses the Euler criterion.

A) When the algorithm is negative (There is no congruence) it returns composite numbers that are not pseudo-prime.
B) When the algorithm is affirmative (There is congruence) it returns primes and Pseudoprimes.

$$(\mathrm{k} > 1) \in \mathbb{N} \quad \wedge\ n = 2k - 1$$

$$\exists n \in \mathbb{N} / \ 2^{\left(\frac{n-1}{2}\right)} \pm 1 \equiv 0 (Mod\ n)$$

$$\rightarrow n = P\ (prime) \vee\ n = Psp\ (pseudoprime)$$

### Developing the two variables

| Formula A | Formula B |
|---|---|
| $\mathrm{k} > 1\ \in \mathbb{N}$ | $\mathrm{k} > 1\ \in \mathbb{N}$ |
| $n = 2k - 1 \Leftrightarrow\ \ k \equiv 1 \vee 2\ (Mod\ 4)$ | $m = 2k - 1 \Leftrightarrow\ \ k \equiv 0 \vee 3\ (Mod\ 4)$ |
| $Formula\ to\ test\ prime\ numbers$ <br> $\exists n \in \mathbb{N}$ | $Formula\ to\ test\ prime\ numbers$ <br> $\exists m \in \mathbb{N}$ |
| $2^{\left(\frac{n-1}{2}\right)} + 1 \Leftrightarrow n \mid 2^{\left(\frac{n-1}{2}\right)} + 1$ | $2^{\left(\frac{m-1}{2}\right)} - 1 \Leftrightarrow m \mid 2^{\left(\frac{m-1}{2}\right)} - 1$ |
| $\rightarrow n = P\ (prime) \vee\ n = Psp\ (pseudoprime)$ | $\rightarrow m = P\ (prime) \vee\ m = Psp\ (pseudoprime)$ |
| $\boldsymbol{2^{\left(\frac{n-1}{2}\right)} + 1 \equiv 0\ (mod\ n)}$ | $\boldsymbol{2^{\left(\frac{m-1}{2}\right)} - 1 \equiv 0 (mod\ m)}$ |

Professor Zeolla Gabriel M.

## Chapter II

### Process 2: Argentest Primality Test

This can be used after process 1 is finished.
It consists of the analysis of numbers formed by their remains, these have unique and special characteristics that allow us to affirm their primality with 100% accuracy.

This process can be **Affirmative, Negative or Neutral**.

A) If it is affirmative, it certifies the primality of the analyzed number.
B) If it is neutral, it does not deny its primality, it postulates it as a candidate for a prime number or with less probability for a pseudo-prime.
C) If it is negative, it certifies that it is a composite number. (This happens because its residual is greater than zero).
These numbers do not pass process 1.

$$\boldsymbol{Residue} = \mathbf{0} \wedge \boldsymbol{Repetition\ of\ rest} = \mathbf{0} \rightarrow \boldsymbol{n} = \boldsymbol{P}\ (\boldsymbol{Prime})$$

$$Residue = 0 \wedge Repetition\ of\ rest > 0 \rightarrow n = P \vee Psp\ (Prime\ \ or\ Pseudoprime)$$

$$Residue > 0 = C\ (Composite\ number)$$

There are 4 types of numbers that we can find once Process 2 is finished

| A) If the result is affirmative, we obtain: | B) If the result is neutral we obtain**:** |
|---|---|
| $P_s: Safe\ prime\ number.$<br>$P_r: Resistant\ prime\ number.$ | $P_w: Weak\ prime\ number$<br>$Psp:\ Pseudoprime\ number.$ |

Professor Zeolla Gabriel M.

## Characteristics

### $P_s = Safe\ prime\ number$

Its remainder is zero and it does not repeat any remainder, forming a cycle of numbers without repetition and its cycle is a prime number. Therefore, they are easily detected. These prime numbers can be constructed simply by looking for prime cycles. They are of the form $2p + 1$, ( $p\ es\ prime$ , $\in \mathbb{N}$)

$P_s = \{5, 7, 11, 23, 47, 59, 83,107,167, 179,227,263,347,359,383,467,479,503,563,587,$
$719,839,863,887,983, \ldots\ldots\}$

*These numbers are known as Safe primes, they have cycles formed by primes of Sophie Germain*
Reference OEIS: A005385 Safe prime number
Reference OEIS: A005384 Sophie Germain.

### $P_r = Resistant\ prime\ number$

Its residual is zero. It does not repeat any remainder, forming a cycle of numbers without repetition, its cycle is a composite number, which we must factor to find its divisors, which will give us information about the non-repetition of remainders.

$P_r = \{3,13,17,19,29,37,41,53,61,67,71,79,97,101,103,131,137,139,149,163,173, \ldots\ldots\}$

### $P_w = Weak\ Prime\ Number$

Its residual is zero. It forms number patterns as it repeats remains. Its cycle is a composite number.

$P_w = \{31,43,73, 89,109,113,127,151,157,223,229,233,241,251,257,277,281,283,307,331,337,.\}$

These represent approximately 30% of the prime numbers.

Reference OEIS: A082595

### $\underline{Psp = Pseudoprime\ Number.}$

Its residual is zero. It forms number patterns as it repeats remains. Its cycle is a composite number.

$Psp = \{561, 1.105, 1.729, 1.905, 2.047, 2.465, 3.277, 4.033, 4.681, 6.601, 8.321, 8.481, 10.585,$
$12.801, 15.841, 16.705, 18.705, 25.761, 29.341, 30.121, 33.153, 34.945, 41041, 42.799, \ldots\ldots\}$

Reference OEIS A047713

These represent a very small portion of the composite numbers that pass process 2.

Professor Zeolla Gabriel M.

## How to analyze a pattern of remnants

There are 2 ways to do it, the first is by applying an artisan method and the second by calculating the divisors of its cycle.

Artisan Method: Consists of assembling the entire sequence of remains, applying the formula of process 1. And descending exponent by exponent until its ¾ part. If no remainder is repeated up to there, they will no longer be repeated, so we can affirm that it is a Prime number. The remainders are easily constructed, each time I under an exponent if the remainder is even I divide it by 2, if the remainder is odd I add (n) it and divide it by 2.
It can be used as a determining method to confirm primality. This method is explicit and didactic. Very easy for the student to understand.
With a simple Microsoft Excel sheet we can solve any large number. Although for numbers with enormous amounts of digits, the design of an application or software is recommended.

Example Test 37

$$2^{\left(\frac{n-1}{2}\right)} + 1 \equiv 0\ (mod\ n)$$

$$2^{18} + 1 \equiv 0\ (mod\ 37)$$

Cycle 18

**Test** **37**

| Total | base | Rest | module |
|---|---|---|---|
| 131054 | $2^{17}$ | -18 | $\equiv 0$ (Mod 37) |
| 65527 | $2^{16}$ | -9 | $\equiv 0$ (Mod 37) |
| 32745 | $2^{15}$ | -23 | $\equiv 0$ (Mod 37) |
| 16354 | $2^{14}$ | -30 | $\equiv 0$ (Mod 37) |
| 8177 | $2^{13}$ | -15 | $\equiv 0$ (Mod 37) |
| 4070 | $2^{12}$ | -26 | $\equiv 0$ (Mod 37) |
| 2035 | $2^{11}$ | -13 | $\equiv 0$ (Mod 37) |
| 999 | $2^{10}$ | -25 | $\equiv 0$ (Mod 37) |
| 481 | $2^{9}$ | -31 | $\equiv 0$ (Mod 37) |
| 222 | $2^{8}$ | -34 | $\equiv 0$ (Mod 37) |
| 111 | $2^{7}$ | -17 | $\equiv 0$ (Mod 37) |
| 37 | $2^{6}$ | -27 | $\equiv 0$ (Mod 37) |
| 0 | $2^{5}$ | -32 | $\equiv 0$ (Mod 37) |
| 0 | $2^{4}$ | -16 | $\equiv 0$ (Mod 37) |
| 0 | $2^{3}$ | -8 | $\equiv 0$ (Mod 37) |
| 0 | $2^{2}$ | -4 | $\equiv 0$ (Mod 37) |
| 0 | $2^{1}$ | -2 | $\equiv 0$ (Mod 37) |
| 0 | $2^{0}$ | -1 | $\equiv 0$ (Mod 37) |

### Construction of the remains

A) If the remainder above is Even, divide by 2 and subtract 1 from the index of the exponent of 2.

B) If the above remainder is odd. We apply $(r - n\ )/2$

Example in the third row, $n = 37$

$$\frac{-9 - 37}{2} = \mathbf{-23}$$

$$\mathbf{2^{15} - 23 \equiv 0}\ \textbf{(Mod 37)}$$

I can complete it completely up to index 0 of the power of 2, or I can do it at least until ¾ +1 of the cycle to check if any remainder is repeated.

This process is didactic but long for very large numbers.

**37 is Prime number since it does not repeat remainders and its remainder is zero.**

**Calculation of divisors:** This allows avoiding making the complete table and directly solving by means of a calculation which, through the dividers, confirms whether the remains are repeated or not. Since the remains are repeated respecting the dividers of the cycle.

The first step: It consists of finding the cycle of remainders, this is found in the index of the exponent of 2 in the initial formula.
In this case using the previous example (test: 37)

$$\mathbf{2^{17} - 18 \equiv 0\ (Mod\ 37)}$$

We take the $\mathbf{2^{17}}$ and to the index (17) we add 1, since its cycle starts at 0 and has 18 rows. Therefore, his cycle is 18.
You can also calculate the cycle using the formula:

$$Cycle\ of\ remains = \frac{n-1}{2}$$

$$Cycle\ of\ remains = \frac{37-1}{2} = 18$$

**Second step I look for the divisors of 18**

The divisors of 18 are: {1,**2,3,6,9**,18}
I take the dividers $1 < d < 18$

**Third step:** It consists of subtracting the divisors from the power of $\mathbf{2^{17-d}}$ and checking if there is congruence or not to determine the primality.

*Read below how to detect resistant prime numbers using the calculation of divisors.*

Professor Zeolla Gabriel M.

# Formula to detect resistant prime numbers
# Divisor Calculation Method.

Resistant prime numbers have the characteristic of not repeating remainders and have zero residue, but to identify them we need to perform the following procedure.

The Resistant prime numbers are formed by cycles that belong to the composite numbers, for this reason this number must be factored to obtain its divisors. Once found, it will allow us to define with 100% accuracy if the number is prime or (weak prime or pseudo prime).

## This formula has two variables

**Formula A.** It has Alternate cycles. It means that the first pattern is in half, so we must multiply its divisors by two.

$$\mathrm{k} > 1 \in \mathbb{N}$$
$$n = 2k - 1 \Leftrightarrow \ k \equiv 1 \vee 2\ (Mod\ 4)$$

$$Initial\ formula$$
$$\exists n \in \mathbb{N}$$

$$2^{\left(\frac{n-1}{2}\right)} + 1 \equiv 0\ (mod\ n)$$

$$\underline{We\ lower\ a\ power}$$

$$2^{\left(\frac{n-1}{2}\right)-1} - \left(\frac{n+1}{2}\right) \equiv 0\ (mod\ n)$$

So I calculate the cycle of remains.

$$Cycle\ of\ remains = \frac{n-1}{2}$$

$d$ = Remains Cycle Dividers.

$$\boldsymbol{2^{\left(\frac{n-1}{2}\right)-1-2d} - \left(\frac{n+1}{2}\right) \not\equiv 0\ (mod\ n)}$$
$$\boldsymbol{\leftrightarrow\ \forall\ d/\ 1 < d < \frac{n-1}{2}}$$
$$\boldsymbol{\rightarrow n = P\ (Prime)}$$

**Formula B:** Normal Cycles: It means that your patterns are complete.

$$\mathrm{k} > 1 \in \mathbb{N}$$
$$m = 2k - 1 \Leftrightarrow \ k \equiv 0 \vee 3\ (Mod\ 4)$$

$$Initial\ formula$$
$$\exists m \in \mathbb{N}$$

$$2^{\left(\frac{m-1}{2}\right)} - 1 \equiv 0(mod\ m)$$

$$\underline{We\ lower\ a\ power}$$

$$2^{\left(\frac{m-1}{2}\right)-1} - \left(\frac{m-1}{2}\right) \equiv 0\ (mod\ n)$$

So I calculate the cycle of remains.

$$Cycle\ of\ remains = \frac{m-1}{2}$$

$d$ = Remains Cycle Dividers

$$\boldsymbol{2^{\left(\frac{m-1}{2}\right)-1-d} - \left(\frac{m-1}{2}\right) \not\equiv 0\ (mod\ n)}$$
$$\boldsymbol{\leftrightarrow\ \forall\ d/\ 1 < d < \frac{m-1}{2}}$$
$$\boldsymbol{\rightarrow n = P\ (Prime)}$$

| **Example A**: Test 67 | **Example B**: Test 71 |
|---|---|
| $$\mathbf{2^{\left(\frac{m-1}{2}\right)} + 1 \equiv 0\ (mod\ m)}$$ | $$\mathbf{2^{\left(\frac{n-1}{2}\right)} - 1 \equiv 0\ (mod\ n)}$$ |
| $$2^{\left(\frac{67-1}{2}\right)} + 1 \equiv 0\ (mod\ 67)$$ $$= 2^{33} + 1 \equiv 0\ (mod\ 67)$$ | $$2^{\left(\frac{71-1}{2}\right)} - 1 \equiv 0\ (mod\ 71)$$ $$= 2^{35} - 1 \equiv 0\ (mod\ 71)$$ |
| $$\underline{We\ lower\ a\ power}$$ | $$\underline{We\ lower\ a\ power}$$ |
| $$\mathbf{= 2^{32} - 33 \equiv 0\ (mod\ 67)}$$ | $$\mathbf{= 2^{34} - 36 \equiv 0\ (mod\ 71)}$$ |
| $$Cycle\ of\ remains\ = \frac{67-1}{2} = 33$$ | $$Cycle\ of\ remains = \frac{71-1}{2} = 35$$ |
| $$d_{(33)} = \{1,3,11,33\}$$ | $$d_{(35)} = \{1,5,7,35\}$$ |
| Then $$= 2^{32-d} - 33 \not\equiv 0\ (mod\ 67)$$ $$\leftrightarrow\ \forall\, d/\ 1 < d < 33$$ $$\rightarrow n = P\ (Prime)$$ | Then $$= 2^{34-d} - 36 \not\equiv 0\ (mod\ 71)$$ $$\leftrightarrow\ \forall\, d/\ 1 < d < 35$$ $$\rightarrow n = P\ (Prime)$$ |
| $$2^{32-2*11} - 33 \not\equiv 0\ (mod\ 67)$$ $$= 2^{10} - 33 \not\equiv 0\ (mod\ 67)$$ | $$2^{34-7} - 36 \not\equiv 0\ (mod\ 71)$$ $$= 2^{27} - 36 \not\equiv 0\ (mod\ 71)$$ |
| $$2^{32-2*3} - 33 \not\equiv 0\ (mod\ 67)$$ $$= 2^{26} - 33 \not\equiv 0\ (mod\ 67)$$ | $$2^{34-5} - 36 \not\equiv 0\ (mod\ 71)$$ $$= 2^{29} - 36 \not\equiv 0\ (mod\ 71)$$ |
| Since it is not congruent in both expressions then 67 is a resistant prime number. This means that no value is repeated in the cycle formed by remainders. | Since it is not congruent in both expressions then 71 is a resistant prime number. This means that no value is repeated in the cycle formed by remainders. |

Professor Zeolla Gabriel M.

# Safe Prime Numbers

## Prime numbers who build Prime numbers

A prime (q) is said to be safe if, in addition to being a prime, it is the result of multiplying a smaller prime (p) by two and adding one to it. For example, the number 23 is a safe prime because 23 = 2 x 11 + 1, with 11 and 23 being primes.
Safe prime numbers are constructed by a prime number in its cycle.

$$P_s = \{5, 7, 11, 23, 47, 59, 83, 107, 167, 179, 227, 263, 347, 359, 383, 467, 479, 503, 563, 587, 719, 839, 863, 887, 983, \ldots\ldots\}$$

## Safe prime numbers are of the form:

$$P_s = 2q + 1, when\ q\ is\ equal\ to\ the\ cycle\ and\ also\ a\ prime\ number.$$

## Primality Test for Safe Prime Numbers and Sophie Germain's Prime Numbers

Download the document linked to this work.
https://www.academia.edu/49807487/Argentest_primality_test_for_Sophie_Germains_prime_numbers_and_safe_prime_numbers.

**Example**: Test of a safe prime number: $n = 47$

$$2^{\left(\frac{n-1}{2}\right)} - 1 \equiv 0(mod\ n)$$

$$2^{\left(\frac{47-1}{2}\right)} - 1 \equiv 0(mod\ 47)$$

$$2^{23} - 1 \equiv 0(mod\ 47)$$

Method: Calculation of divisors

$$We\ lower\ a\ power$$

$$\mathbf{2^{22} - 24 \equiv 0\ (mod\ 47)}$$

$$Cycle\ of\ remains\ = \frac{47-1}{2} = \mathbf{23}$$

Dividers of 23:

$$d_{(23)} = \{1, 23\}$$

$$1 < d < 23$$

There are no (d) divisors between 1 and 23, this means that 23 is Sophie Germain's prime number, so no remainder will be repeated in its cycle.

**∴ is a safe prime number**

Professor Zeolla Gabriel M.

## Artisan Method

Test 47 cycle de 23

| Total | Powe | rest | Residue and modulus |
|---|---|---|---|
| 4194280 | $2^{22}$ | -24 | $\equiv 0$ (Mod 47) |
| 2097140 | $2^{21}$ | -12 | $\equiv 0$ (Mod 47) |
| 1048570 | $2^{20}$ | -6 | $\equiv 0$ (Mod 47) |
| 524285 | $2^{19}$ | -3 | $\equiv 0$ (Mod 47) |
| 262119 | $2^{18}$ | -25 | $\equiv 0$ (Mod 47) |
| 131036 | $2^{17}$ | -36 | $\equiv 0$ (Mod 47) |
| 65518 | $2^{16}$ | -18 | $\equiv 0$ (Mod 47) |
| 32759 | $2^{15}$ | -9 | $\equiv 0$ (Mod 47) |
| 16356 | $2^{14}$ | -28 | $\equiv 0$ (Mod 47) |
| 8178 | $2^{13}$ | -14 | $\equiv 0$ (Mod 47) |
| 4089 | $2^{12}$ | -7 | $\equiv 0$ (Mod 47) |
| 2021 | $2^{11}$ | -27 | $\equiv 0$ (Mod 47) |
| 987 | $2^{10}$ | -37 | $\equiv 0$ (Mod 47) |
| 470 | $2^{9}$ | -42 | $\equiv 0$ (Mod 47) |
| 235 | $2^{8}$ | -21 | $\equiv 0$ (Mod 47) |
| 94 | $2^{7}$ | -34 | $\equiv 0$ (Mod 47) |
| 47 | $2^{6}$ | -17 | $\equiv 0$ (Mod 47) |
| 0 | $2^{5}$ | -32 | $\equiv 0$ (Mod 47) |
| 0 | $2^{4}$ | -16 | $\equiv 0$ (Mod 47) |
| 0 | $2^{3}$ | -8 | $\equiv 0$ (Mod 47) |
| 0 | $2^{2}$ | -4 | $\equiv 0$ (Mod 47) |
| 0 | $2^{1}$ | -2 | $\equiv 0$ (Mod 47) |
| 0 | $2^{0}$ | -1 | $\equiv 0$ (Mod 47) |

Characteristics of all prime numbers Safe

**No rest is repeated.**

**Residues= 0**

Its cycle is a prime number, in this case 23, since 22 is the index of the power of two, 22 + 1 = 23 we add 1 because it starts at 0.

The Remnant Pattern ends in decreasing values until it reaches 1 in the last powers.

Totals have values that belong to the natural numbers and zero.

47 is finally a prime number for all the above reasons, but especially for the first two.

Professor Zeolla Gabriel M.

# Pseudoprime numbers

Pseudoprimes are odd composite numbers, which pass process 1 and manage to mix with the prime numbers. These numbers are known as the Carmichael numbers.
For this reason, when we take them to process 2 and analyze the remains of their cycles, these numbers always have repeated remains and form patterns, since in their essence they are composite numbers, which allows us to be able to classify them satisfactorily.

The cycles of pseudo prime numbers are always a composite number for the base 2.
I have tested the pseudoprimes up to the number 285,000,000 and none of them have a prime cycle up to there. Although I do not have a proof, this result is to take into account without a doubt since if the prime cycles did not appear up to here they hardly appear with larger numbers. But it is an open possibility.
This detail gives solidity to the safe prime numbers.

$$Psp \neq 2p + 1, where\ p\ is\ a\ prime\ number$$

***Psp*: *Pseudoprime*.**
Its residual is zero. Forms numerical patterns, has repeating remains. Your cycle is a composite number.

$$Psp = \{561, 1.105, 1.729, 1.905, 2.047, 2.465, 3.277, 4.033, 4.681, 6.601, 8.321, 8.481, 10.585, 12.801, 15.841, 16.705, 18.705, 25.761, 29.341, 30.121, 33.153, 34.945, 41041, 42.799, \ldots\ldots\}$$

Reference OEIS A047713

These represent a very small portion of the composite numbers.

$$Cycle\ of\ remains\ = \frac{n-1}{2}$$

| $Psp$ | Cycle of remains | Cycle characteristic |
|---|---|---|
| 561 | 280 | Composite |
| 1.105 | 552 | Composite |
| 1.729 | 864 | Composite |
| 1.905 | 952 | Composite |
| 2.047 | 1.023 | Composite |
| 2.465 | 1.232 | Composite |
| 3.277 | 1.638 | Composite |
| 4.033 | 2.016 | Composite |
| 4.681 | 2.340 | Composite |
| 6.601 | 3.300 | Composite |
| 8.321 | 4.160 | Composite |
| 8.481 | 4240 | Composite |

| | | |
|---|---|---|
| 10.585 | 5.292 | Composite |
| 12.801 | 6.400 | Composite |

## Examples where pseudoprime fail the process 2

**Example A**: Test 3.277

$$2^{\left(\frac{3.277-1}{2}\right)-1} - \left(\frac{3.277-1}{2}\right) \equiv 0\ (mod\ 3.277)$$

$$2^{1637} - 1638 \equiv 0\ (mod\ 3.277)$$

$$Cycle\ of\ remains\ = \frac{3277-1}{2} = 1.638$$

Dividers

$$d_{(1638)} = \{1, 2, 3, 6, 7, 9, 13, 14, 18, 21, 26, 39, 42, 63, 78, 91, 117, 126, 182, 234, 273, 546, 819, 1.638\}$$

$$1 < d < 1.638$$

$$2^{1.637-2*2} - 1.638 \not\equiv 0\ (mod\ 3.277)$$
$$2^{1.637-2*3} - 1.638 \not\equiv 0\ (mod\ 3.277)$$
$$2^{1.637-2*6} - 1.638 \not\equiv 0\ (mod\ 3.277)$$
$$2^{1.637-2*7} - 1.638 \not\equiv 0\ (mod\ 3.277)$$
$$2^{1.637-2*9} - 1.638 \not\equiv 0\ (mod\ 3.277)$$
$$2^{1.637-2*13} - 1.638 \not\equiv 0\ (mod\ 3.277)$$
$$\mathbf{2^{1.637-2*14} - 1.638 \equiv 0\ (mod\ 3.277)}$$

Since it is congruent in the last expression then 3.277 is a pseudo prime or weak prime number.

This means that values and patterns are repeated in the cycle formed by remains.
In this case there will be a pattern of 28 residues that repeat simultaneously.
In the alternating cycles we obtain ½ pattern without completing.
So we have 1638/28 = 58.5
This means that there is a pattern of 28 residues that are repeated 58 times and 1 pattern is left in the middle (14).

Therefore, your alternating cycle is 28/14.
In the alternating cycle the second number is always half of the first and it is the divisor that we use to find the pattern.

$$28 * 56 + 14 = 1.638$$

**Example B**: Test 2.047

$$2^{\left(\frac{2.047-1}{2}\right)-1} - \left(\frac{2.047+1}{2}\right) \equiv 0\ (mod\ 2.047)$$

$$2^{1022} - 1.024 \equiv 0\ (mod\ 2.047)$$

$$Cycle\ of\ remains\ = \frac{2.047-1}{2} = 1.023$$

Dividers

$$d_{(1023)} = \{1,3,11,31,33,93,341,1023\}$$

$$1 < d < 1.023$$

$$2^{1022-3} - 1.024 \not\equiv 0\ (mod\ 2047)$$
$$\mathbf{2^{1022-11} - 1.024 \equiv 0\ (mod\ 2047)}$$

Since it is congruent in the second expression then 2.047 is a pseudo prime or weak prime number.
No need to keep calculating any more, just find a congruence to determine the result.

This means that values and patterns are repeated in the cycle formed by remains.
In this case there will be a pattern of 11 remains that is repeated 93 times.

$$11 * 93 = 1.023$$

Professor Zeolla Gabriel M.

## Weak Prime Numbers

They are those numbers that do not pass process 2 successfully and we cannot determine if it is a prime number or a pseudo prime. Its cycle is a Composite number.
Its residues are zero, but the sequence of residues has repeating numbers that form patterns, which is conditioning and an impediment to affirming its primality.

These are some of the prime numbers that do not pass the Argentest for base 2.

### $P_w$: *Weak prime number*

$P_w = \{31,43,73,89,109,113,127,151,157,223,229,233,241,251,257,277,281,283,307,331,337,353,..\}$

These represent approximately 30% of the set of prime numbers.

Reference OEIS: A082595

Pseudoprimes do not pass the Argentest for base 2 since their remains also form patterns.

### *Psp*: *Pseudoprime*.

$Psp = \{561, 1.105, 1.729, 1.905, 2.047, 2.465, 3.277, 4.033, 4.681, 6.601, 8.321, 8.481, 10.585, 12.801, 15.841, 16.705, 18.705, 25.761, 29.341, 30.121, 33.153, 34.945, 41041, 42.799, \ldots..\}$

Reference OEIS A047713

These represent a very small portion of the composite numbers.

Professor Zeolla Gabriel M.

# Mersenne Prime Numbers are Weak Prime numbers

In the Argentest the Mersenne primes greater than 7 are weak primes for the base 2.
These have remnants that form patterns formed by the sequences of $2^n$, this does not allow to classify them satisfactorily in this base since there are pseudo prime numbers of the same style. Example 2.047

$$\frac{Mp-1}{2} \equiv 3\ (Mod\ 4)$$

$$Mp = \{31, 127, 8.191, 131.071, 524.287, 2.147.483.647, \ldots.\}$$

We can observe that practically the patterns of remains are formed by the sequences of up to $2^n < n$, Also in both cases they have a remainder of 0. The sum of each pattern is equal to $n$.
And in all cases its rest begins with $(n+1)/2$ , then his remains are descending in divisions by 2 uninterrupted until reaching 1.
Examples

Weak prime number

$$2^{15} - 1 \equiv 0(mod\ 31)$$

Test 31 Pattern of 5

| Total | Base | Resto | Residue and Modulus |
|---|---|---|---|
| 16368 | $2^{14}$ | -16 | $\equiv 0$(Mod 31) |
| 8184 | $2^{13}$ | -8 | $\equiv 0$(Mod 31) |
| 4092 | $2^{12}$ | -4 | $\equiv 0$(Mod 31) |
| 2046 | $2^{11}$ | -2 | $\equiv 0$(Mod 31) |
| 1023 | $2^{10}$ | -1 | $\equiv 0$(Mod 31) |
| 496 | $2^9$ | -16 | $\equiv 0$(Mod 31) |
| 248 | $2^8$ | -8 | $\equiv 0$(Mod 31) |
| 124 | $2^7$ | -4 | $\equiv 0$(Mod 31) |
| 62 | $2^6$ | -2 | $\equiv 0$(Mod 31) |
| 31 | $2^5$ | -1 | $\equiv 0$(Mod 31) |
| 0 | $2^4$ | -16 | $\equiv 0$(Mod 31) |
| 0 | $2^3$ | -8 | $\equiv 0$(Mod 31) |
| 0 | $2^2$ | -4 | $\equiv 0$(Mod 31) |
| 0 | $2^1$ | -2 | $\equiv 0$(Mod 31) |
| 0 | $2^0$ | -1 | $\equiv 0$(Mod 31) |

15 is the cycle number.
Which has the divisors $d$: {1,3, 5,15}
In this case, it is made up of a pattern of 5 residues and 3 repetitions.
The 5 remainder pattern is related to the Mersenne numbers, $2^5 - 1 = 31$

Pseudoprime (Trim the full cycle)

$$2^{1023} - 1 \equiv 0(mod\ 2.047)$$

Test 2.047 Pattern of 11

| | Base | Rest | Residue and modulus |
|---|---|---|---|
| | $2^{1022}$ | -1024 | $\equiv 0$(Mod 2.047) |
| | $2^{1021}$ | -512 | $\equiv 0$(Mod 2.047) |
| | $2^{1020}$ | -256 | $\equiv 0$(Mod 2.047) |
| | $2^{1019}$ | -128 | $\equiv 0$(Mod 2.047) |
| | $2^{1018}$ | -64 | $\equiv 0$(Mod 2.047) |
| | $2^{1017}$ | -32 | $\equiv 0$(Mod 2.047) |
| | $2^{1016}$ | -16 | $\equiv 0$(Mod 2.047) |
| | $2^{1015}$ | -8 | $\equiv 0$(Mod 2.047) |
| | $2^{1014}$ | -4 | $\equiv 0$(Mod 2.047) |
| | $2^{1013}$ | -2 | $\equiv 0$(Mod 2.047) |
| | $2^{1012}$ | -1 | $\equiv 0$(Mod 2.047) |
| | $2^{1011}$ | -1024 | $\equiv 0$(Mod 2.047) |
| | $2^{1010}$ | -512 | $\equiv 0$(Mod 2.047) |
| | $2^{1009}$ | -256 | $\equiv 0$(Mod 2.047) |
| | $2^{1008}$ | -128 | $\equiv 0$(Mod 2.047) |
| | $2^{1007}$ | -64 | $\equiv 0$(Mod 2.047) |

1.023 is the cycle number.
Which has the divisors:
$d = \{1, 3, 11, 31, 33, 93, 341, 1023\}$
In this case, it is made up of a pattern of 11 residues and 93 repetitions.
The pattern of 11 remains is related to the Mersenne numbers, In this case, it is made up of a pattern of 11 residues and 93 repetitions.
The pattern of 11 remains is related to the Mersenne numbers$2^{11} - 1 = 2.047$

Professor Zeolla Gabriel M.

## Chapter III

### Process 3. Change of base

Formula to determine primality with bases greater than 2.
It is the same that we use in base 2.
The main formula works with the Euler criteria, although it has a small modification which makes it easier for us to build the sequence of remains without problems in base 3 in an artisanal way.

| Formula A | Formula B |
|---|---|
| $\boldsymbol{a^{\left(\frac{n-1}{2}\right)} + 1 \equiv 0 (mod\ n)}$ | $\boldsymbol{a^{\left(\frac{m-1}{2}\right)} - 1 \equiv 0 (mod\ m)}$ |

We apply the process 3 to the weak prime numbers.
Process 3 consists of changing base 2 to base 3 and then forming the sequence of residues and being able to check whether or not there are patterns to confirm primality.

### Fórmula para determinar primalidad con base 3

| Formula A | Formula B |
|---|---|
| $k > 1 \in \mathbb{N}$<br>$n = 2k - 1 \Leftrightarrow\ k \equiv 2 \vee 3\ (Mod\ 6)$<br><br>$\exists n \in \mathbb{N}$<br>$3^{\left(\frac{n-1}{2}\right)} + 1 \Leftrightarrow n \mid 3^{\left(\frac{n-1}{2}\right)} + 1$<br>$\rightarrow n = P\ (prime) \vee\ n = Psp\ (pseudoprime)$<br><br>$\boldsymbol{3^{\left(\frac{n-1}{2}\right)} + 1 \equiv 0\ (mod\ n)}$ | $k > 1 \in \mathbb{N}$<br>$m = 2k - 1 \Leftrightarrow\ k \equiv 0 \vee 5\ (Mod\ 6)$<br><br>$\exists n \in \mathbb{N}$<br>$3^{\left(\frac{m-1}{2}\right)} - 1 \Leftrightarrow m \mid 3^{\left(\frac{m-1}{2}\right)} - 1$<br>$\rightarrow m = P\ (prime) \vee\ m = Psp\ (pseudoprime)$<br><br>$\boldsymbol{3^{\left(\frac{m-1}{2}\right)} - 1 \equiv 0 (mod\ m)}$ |

When $k \equiv 1 \vee 4\ (Mod\ 6)$
$n = 2k - 1\ \ (is\ a\ composite\ number\ multiple\ of\ 3)$.
Example: 561

## Artisan method.

Example Formula A: Test 31

$$\mathbf{3}^{\left(\frac{\boldsymbol{n-1}}{\mathbf{2}}\right)} + \mathbf{1} \equiv \mathbf{0}\ (\boldsymbol{mod\ n})$$

$$3^{\left(\frac{31-1}{2}\right)} + 1 \equiv 0\ (mod\ 31)$$

$$3^{15} + 1 \equiv 0(\text{Mod } 31)$$

| Total | Base | rest | Residue and modulus |
|---|---|---|---|
| 4782959 | $3^{14}$ | -10 | $\equiv 0$(Mod 31) |
| 1594299 | $3^{13}$ | -24 | $\equiv 0$(Mod 31) |
| 531433 | $3^{12}$ | -8 | $\equiv 0$(Mod 31) |
| 177134 | $3^{11}$ | -13 | $\equiv 0$(Mod 31) |
| 59024 | $3^{10}$ | -25 | $\equiv 0$(Mod 31) |
| 19654 | $3^{9}$ | -29 | $\equiv 0$(Mod 31) |
| 6541 | $3^{8}$ | -20 | $\equiv 0$(Mod 31) |
| 2170 | $3^{7}$ | -17 | $\equiv 0$(Mod 31) |
| 713 | $3^{6}$ | -16 | $\equiv 0$(Mod 31) |
| 217 | $3^{5}$ | -26 | $\equiv 0$(Mod 31) |
| 62 | $3^{4}$ | -19 | $\equiv 0$(Mod 31) |
| 0 | $3^{3}$ | -27 | $\equiv 0$(Mod 31) |
| 0 | $3^{2}$ | -9 | $\equiv 0$(Mod 31) |
| 0 | $3^{1}$ | -3 | $\equiv 0$(Mod 31) |
| 0 | $3^{0}$ | -1 | $\equiv 0$(Mod 31) |

It does not repeat Remains, which is why its primality is confirmed with the change of base.

We begin by analyzing remains from

$$3^{\left(\frac{n-1}{2}\right)-1} = 3^{14}$$

**Building remains has 3 options**

A) If the remainder above is a multiple of 3, divide by 3.

B) If the above remainder is not a multiple of 3, then we apply $(\boldsymbol{r-n})/\mathbf{3}$

$n = 31$

**Example** $3^{14}$

$$(1-31)/3 = -10$$

$$3^{14} - 10 \equiv 0(\text{Mod } 31)$$

C) If performing the first step and the second and we do not obtain a multiple of 3 then:

$(\boldsymbol{r-2n})/\mathbf{3}$

**Example** $3^{9}$

$$(-25 - 2 * 31)/3 = -29$$

$$3^{9} - 29 \equiv 0(\text{Mod } 31)$$

D) *if performing the previous steps and a multiple of 3 is not achieved. It means that this tested number is compound and multiple of* 3.

Professor Zeolla Gabriel M.

# Divisor Calculation Method

It is exactly the same as in base 2. We look for the divisors of the cycle to check if any remainder is repeated.

**Example A**: Test 73. Normal cycle

$$3^{\left(\frac{m-1}{2}\right)} - 1 \equiv 0 \ (mod\ m)$$

$$3^{\left(\frac{73-1}{2}\right)} - 1 \equiv 0 \ (mod\ 73)$$
$$= 3^{36} - 1 \equiv 0 \ (mod\ 73)$$

$$We\ lower\ a\ power$$
$$= \mathbf{3^{35} - 49 \equiv 0 \ (mod\ 73)}$$

Then
$$3^{35-d} - 49 \not\equiv 0 \ (mod\ 73)$$
$$\leftrightarrow \forall\ d/\ 1 < d < \frac{m-1}{2}$$
$$\rightarrow n = P\ (nº\ primo)$$

I look for the dividers of the cycle $\left(\frac{73-1}{2}\right)$ =36

$$d_{(36)} = \{1,2,3,4,6,9,12,18,36\}$$

$$then\ 1 < d < 36$$

$$3^{35-2} - 49 \not\equiv 0 \ (mod\ 73)$$
$$= 3^{33} - 49 \not\equiv 0 \ (mod\ 73)$$

$$3^{35-3} - 49 \not\equiv 0 \ (mod\ 73)$$
$$= 3^{32} - 49 \not\equiv 0 \ (mod\ 73)$$

$$3^{35-4} - 49 \not\equiv 0 \ (mod\ 73)$$
$$= 3^{31} - 49 \not\equiv 0 \ (mod\ 73)$$

$$3^{35-6} - 49 \not\equiv 0 \ (mod\ 73)$$
$$= 3^{29} - 49 \not\equiv 0 \ (mod\ 73)$$

$$3^{35-9} - 49 \not\equiv 0 \ (mod\ 73)$$
$$= 3^{26} - 49 \not\equiv 0 \ (mod\ 73)$$

$$\mathbf{3^{35-12} - 49 \equiv 0 \ (mod\ 73)}$$
$$\mathbf{= 3^{23} - 49 \equiv 0 \ (mod\ 73)}$$

$$3^{35-18} - 49 \not\equiv 0 \ (mod\ 73)$$
$$= 3^{17} - 49 \not\equiv 0 \ (mod\ 73)$$

Since it is congruent, then 73 is a Base 3 Weak prime number.
This means that values are repeated in the cycle formed by remains.
Therefore, it will have a pattern of 12 remains that is repeated 3 times (12 arises from the divisor).
12 * 3 = 36 (cycle number)

Therefore, we must re-analyze it with base 4 to examine its cycle again.
This number has the peculiarity of confirming its primality only with the base 5.

Professor Zeolla Gabriel M.

Example: Analysis of the number 73 for base 3.

## Method: artisan

Abbreviated sequence.

$$3^{36} - 1 \equiv 0\ (mod\ 73)$$

Test 73

| Total | base | rest | Residue and modulus |
|---|---|---|---|
| 5,0032E+16 | $3^{35}$ | -49 | $\equiv 0$(Mod 73) |
| 1,6677E+16 | $3^{34}$ | -65 | $\equiv 0$(Mod 73) |
| 5,5591E+15 | $3^{33}$ | -46 | $\equiv 0$(Mod 73) |
| 1,853E+15 | $3^{32}$ | -64 | $\equiv 0$(Mod 73) |
| 6,1767E+14 | $3^{31}$ | -70 | $\equiv 0$(Mod 73) |
| 2,0589E+14 | $3^{30}$ | -72 | $\equiv 0$(Mod 73) |
| 6,863E+13 | $3^{29}$ | -24 | $\equiv 0$(Mod 73) |
| 2,2877E+13 | $3^{28}$ | -8 | $\equiv 0$(Mod 73) |
| 7,6256E+12 | $3^{27}$ | -27 | $\equiv 0$(Mod 73) |
| 2,5419E+12 | $3^{26}$ | -9 | $\equiv 0$(Mod 73) |
| 8,4729E+11 | $3^{25}$ | -3 | $\equiv 0$(Mod 73) |
| 2,8243E+11 | $3^{24}$ | -1 | $\equiv 0$(Mod 73) |
| 9,4143E+10 | $3^{23}$ | -49 | $\equiv 0$(Mod 73) |
| 3,1381E+10 | $3^{22}$ | -65 | $\equiv 0$(Mod 73) |
| 1,046E+10 | $3^{21}$ | -46 | $\equiv 0$(Mod 73) |
| 3486784337 | $3^{20}$ | -64 | $\equiv 0$(Mod 73) |

continue

$$\mathbf{3^{\left(\frac{m-1}{2}\right)} - 1 \equiv 0\ (mod\ m)}$$

$$3^{\left(\frac{73-1}{2}\right)} - 1 \equiv 0\ (mod\ 73)$$

$$3^{36} - 1 \equiv 0\ (mod\ 73)$$

We analyze the cycle from the previous power

$$\mathbf{3^{35} - 49 \equiv 0\ (mod\ 73)}$$

We see that it has a pattern of 12 remains which starts again from $3^{23}$, then $3^{11}$

Professor Zeolla Gabriel M.

## Weak Prime Numbers with base 3

The base 2 weak primes that did not pass process 2, we pass them through process 3. 60% of them will be able to confirm their primality, but the remaining 40% will be weak prime again.
For example, 73. This has patterns with base 2 and also with base 3. Therefore, we define it as a weak prime of base 3.
To be considered a prime number in base 3 the conditions remain the same as in base 2, the input (n) must have:

Residue =0
Repetitions of remains = 0

These numbers have residue 0 but have residue repeats. Therefore, we cannot confirm their primality and we postulate them as a weak prime number with base 3.
Examples

$$P_{w3} = \{73,109,151,229,277,307,433,439,499,577,601, \ldots.\}$$

These numbers should be subjected to another base change (process 4) in order to separate them from the base 2 pseudo-primes. Perform the same analysis and re-debug the sequence.

## Pseudoprimes with neutral result for base 3

They are the base-2 pseudoprimes that do not pass process 3 and that continue to have repeating residues that form patterns.
These base 2 pseudoprimes have residue 0 but have residue repeats and are therefore candidates for a weak base-3 prime number.

Example

$$Psp_3 = \{\ 1.729, 10.585, 15.841, 29.341, 41.041, \ldots..\}$$

## Pseudoprimes with negative result for Base 3

They are those numbers whose remainder is greater than 0 or are multiples of 3. Therefore, we certify that it is a composite number. Therefore, the set of pseudoprimes decreases significantly with the change of base.

$$Psp = C = \{561, 1.105, 1.905, 2.047, 2.465, 3.277, 4.033, 4.681, 6.601, 8.321, 8.481, \ldots.\}$$

Examples

$$3^{280} - 1 \not\equiv 0 (\text{Mod } 561)$$
$$3^{552} - 1 \not\equiv 0 (\text{Mod } 1.105)$$

Professor Zeolla Gabriel M.

## Chapter VI

### Process 4. Base change

We apply process 4 to the weak prime numbers of process 3.
Process 4 consists of changing base 3 to base 4 and then forming the sequence of residues and being able to check whether or not there are patterns to confirm primality.
The method is exactly the same as in the previous bases.
We can change bases as many times as we need and the mechanism will always be the same.

$$\exists n \in \mathbb{N} / \ 4^{\left(\frac{n-1}{2}\right)} \pm 1 \equiv 0 (Mod\ n)$$

We build the sequence in an artisanal way dividing by 4 when it is a multiple of 4, otherwise we subtract (n) until we find a multiple, and then divide by 4. The sequence of remainders ends in 1 when it is prime or pseudo-prime.

Primality conditions

Residual = 0
Repetitions of remains = 0

## Conclusion

Centuries ago the Chinese used what we now know as Fermat's little theorem and believed that it reached only the remainder equal to zero to certify the primality of an odd number, until a long time later pseudo prime numbers were discovered.
Argentest brings up the missing conditions to determine the primality of an odd number, which is the non-repetition of remainders.
Argentest is a new and simple tool to be able to certify the primality of an odd number (n), it uses simple and didactic mechanisms for students. Since through the construction of tables or efficient calculations we achieve the objective in a few simple steps.
The Argentest is a new possibility that provides certainty in the face of the great distress that prime numbers have caused in great mathematicians of the past.
Today there are many very interesting primality tests and with different degrees of application, this new algorithm aims to be a new possibility and another way of knowing and interpreting prime numbers.

Professor Zeolla Gabriel Martín
Buenos Aires, Argentina.

*Download the Microsoft Excel spreadsheet: For the calculation of the artisan method.*

Other documents of the author:
https://independent.academia.edu/GabrielZeolla

## References

BECKER, M. E.; PIETROCOLA, N. Y SÁNCHEZ, C. (2001); Aritmética, Red Olímpica, Argentina.
GRACIÁN, E. (2011); Los Números Primos, un Largo Camino al Infinito, Navarra: EDITEC.
GÓMEZ, J. (2011); Matemáticos, Espías y Piratas Informáticos, Codificación y Criptografía, Navarra: EDITEC
Papadimitriou, Christos H.: Computational Complexity. Sección 10.2: "Primality", pp.222–227. Addison-Wesley, 1era edición, 1993. (ISBN201-53082-1.)
Caldwell, Chris,Finding primes & proving primality [1]
Caldwell, Chris: The Prime Pages. Universidad de Tennessee. (Ver enlaces externos.)
Agrawal, Manindra; Kayal, Neeraj; Saxena, Nitin: "PRIMES is in P". Annals of Mathematics 160 (2004), no. 2, pp. 781–793.
H. W. Lenstra jr. and Carl Pomerance: "Primality testing with Gaussian periods".
Ball, W. W. R. and Coxeter, H. S. M. *Mathematical Recreations and Essays, 13th ed.* New York: Dover, p. 61, 1987.
Beiler, A. H. *Recreations in the Theory of Numbers: The Queen of Mathematics Entertains.* New York: Dover, 1966.
Conway, J. H. and Guy, R. K. *The Book of Numbers.* New York: Springer-Verlag, pp. 141-142, 1996.
Courant, R. and Robbins, H. "Fermat's Theorem." §2.2 in Supplement to Ch. 1 in *What Is Mathematics?: An Elementary Approach to Ideas and Methods, 2nd ed.* Oxford, England: Oxford University Press, pp. 37-38, 1996.
Flannery, S. and Flannery, D. *In Code: A Mathematical Journey.* London: Profile Books, pp. 118-125, 2000.