Título: Nuevo algoritmo de prueba de primalidad Argentest.
Autor: Zeolla, Gabriel Martin
Comentarios: 23 paginas
gabrielzvirgo@hotmail.com

Palabras clave: Test de primalidad, número primo, pseudoprimo.

Resumen:

Este texto desarrolla un nuevo Algoritmo de Primalidad, este obtiene resultados opuestos al pequeño teorema de Fermat, ya que utiliza mecanismos similares pero aplicados al análisis de patrones.
En el Teorema de Fermat siempre hay Pseudoprimos escondidos entre los primos, lo cual no da certezas sobre la primalidad de un número impar analizado, más allá del cambio de bases como sucede con el número Pseudoprimo 561.
En el algoritmo Argentest sucede lo contrario los pseudoprimos no pasan el test, por lo cual podemos confirmar la primalidad de un número con absoluta certeza y determinación, pero hay un porcentaje de primos que tampoco pasan el test, por lo cual acudimos al cambio de base para volver a analizar los patrones y confirmar la primalidad luego.

Entonces este nuevo algoritmo de prueba de primalidad determinista utiliza dos mecanismos sencillos, el primero inspirado en el criterio de Euler, el segundo atreves del análisis de patrones formados por sus restos, con estos primeros dos procesos podemos determinar la primalidad del 70% del conjunto de los números primos con una exactitud del 100%
Para el 30% restante del conjunto de los números primos hay un tercer proceso que consiste en el cambio de base 2 a base 3 para luego volver analizar los patrones, este separa los pseudoprimos de los números primos restantes.
El 60 % de los primos que antes no pasaron, ahora confirman su primalidad. El 40% de los números primos restantes y una pequeña parte de los pseudoprimos de base 2 tampoco pasa el test. Por lo cual deberíamos volver a cambiar de base y repetir el proceso para seguir decantando estos números.
Con la combinación de la base 2 y la base 3 obtenemos la certificación de primalidad para el 90% del conjunto de los números primos. Para el 10% restante deberíamos repetir el proceso con otro cambio de base.

Introducción

Definición: Una prueba de Primalidad es un algoritmo que permite decidir si un número natural (n) es primo o compuesto.
El Argentest busca resolver la primalidad con cálculos eficientes, aunque se puede lograr mediante tablas gráficas. Las tablas graficas es como un documento de primalidad irrefutable. Un sello único para cada primo, como su propia huella digital. Estas tablas se construyen fácilmente, aunque para números primos muy grandes se hace demasiado largo. Por lo cual utilizar cálculos eficientes se aplica mejor para números grandes.

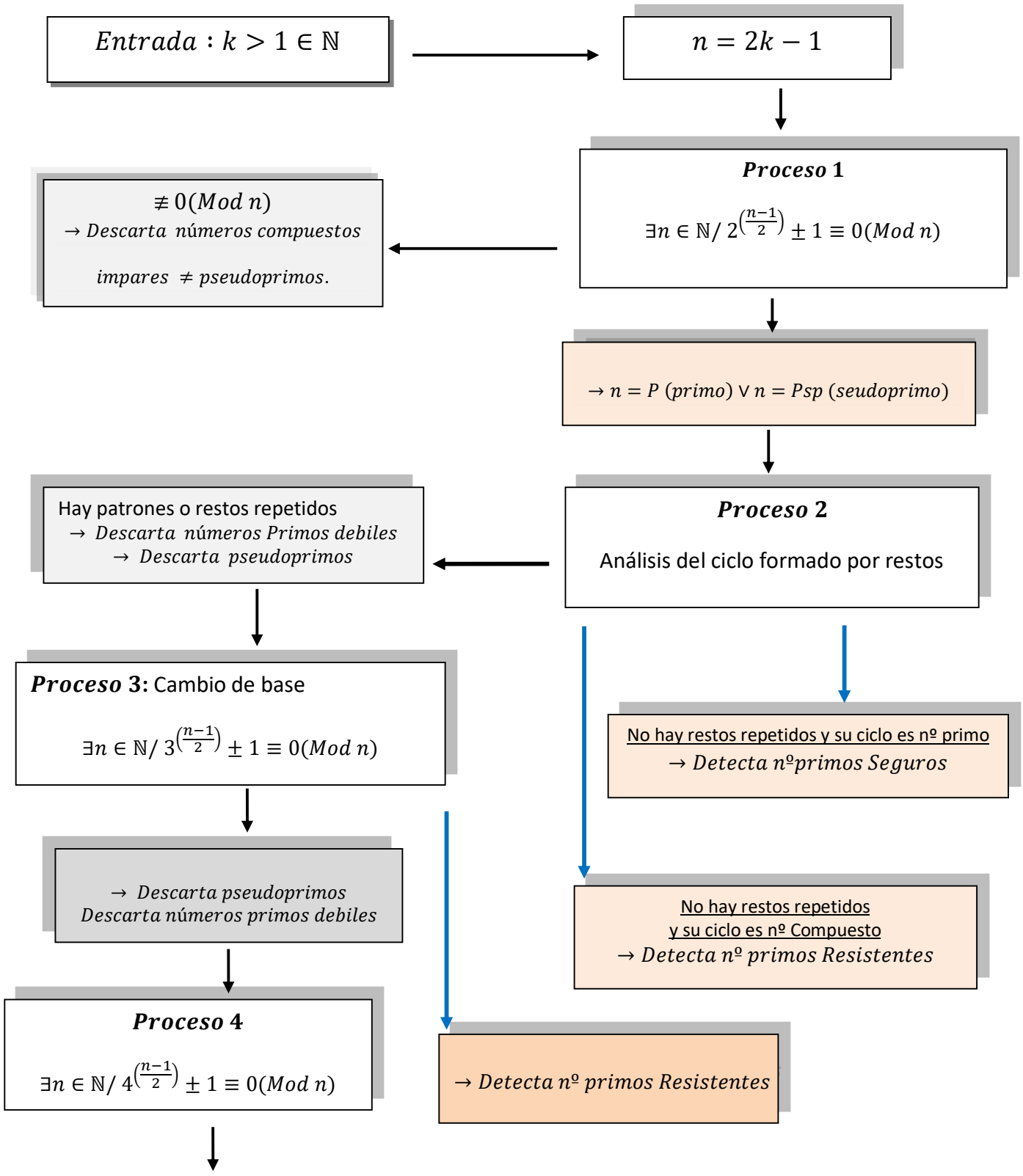
Profesor Zeolla Gabriel M.

Argentest

Índice

Profesor Zeolla Gabriel M.

Funcionamiento del algoritmo Argentest



Profesor Zeolla Gabriel M.

Capítulo I

Proceso 1: Prueba de Primalidad para números impares

Este proceso al igual que el pequeño teorema de Fermat tiene la capacidad de separar números y clasificarlos.
La fórmula utilizada por el Argentest está muy vinculada al mismo, este utiliza el criterio de Euler.

A) Cuando el algoritmo es negativo (No hay congruencia) entrega números compuestos que no son pseudoprimos.
B) Cuando el algoritmo es afirmativo (Hay congruencia) entrega números primos y Pseudoprimos.

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

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

$$\rightarrow n = P\ (primo) \vee\ n = Psp\ (pseudoprimo)$$

Desarrollando las dos variables

Formula A	Formula B
$\mathrm{k} > 1 \ \in \mathbb{N}$	$\mathrm{k} > 1 \ \in \mathbb{N}$
$n = 2k - 1 \Leftrightarrow\ \ k \equiv 1 \vee 2\ (Mod\ 4)$	$m = 2k - 1 \Leftrightarrow\ \ k \equiv 0 \vee 3\ (Mod\ 4)$
$Formula\ para\ testear\ n^{o}\ primos$ $\exists n \in \mathbb{N}$	$Formula\ para\ testear\ n^{o}\ primos$ $\exists m \in \mathbb{N}$
$2^{\left(\frac{n-1}{2}\right)} + 1 \Leftrightarrow n \mid 2^{\left(\frac{n-1}{2}\right)} + 1$	$2^{\left(\frac{m-1}{2}\right)} - 1 \Leftrightarrow m \mid 2^{\left(\frac{m-1}{2}\right)} - 1$
$\rightarrow n = P\ (primo) \vee\ n = Psp\ (pseudoprimo)$	$\rightarrow m = P\ (primo) \vee\ m = Psp\ (pseudoprimo)$
$\boldsymbol{2^{\left(\frac{n-1}{2}\right)} + 1 \equiv 0\ (mod\ n)}$	$\boldsymbol{2^{\left(\frac{m-1}{2}\right)} - 1 \equiv 0 (mod\ m)}$

Profesor Zeolla Gabriel M.

Capítulo II

Proceso 2: Prueba de Primalidad Argentest

Este es posible utilizarlo una vez finalizado el proceso 1.

Consiste en el análisis de números formado por sus **restos**, estos tienen características únicas y especiales que permiten afirmar su primalidad con una exactitud del 100%.

Este proceso puede ser **Afirmativo, Negativo o Neutro**.

A) Si es afirmativo certifica la primalidad del número analizado.
B) Si es neutro no niega su primalidad, lo postula para candidato a primo o con menos probabilidades a pseudoprimo.
C) Si es negativo certifica que es número compuesto. (Esto sucede porque su residuo es mayor a cero).
Estos números no pasan el proceso 1.

$$\boldsymbol{Residuo} = \mathbf{0} \wedge \boldsymbol{repeticion\ de\ resto} = \mathbf{0} \rightarrow \boldsymbol{n} = \boldsymbol{P}\ (\boldsymbol{n^{\underline{o}}\ primo})$$

$$Residuo = 0 \wedge repeticion\ de\ resto > 0 \rightarrow n = P \vee Psp\ (n^{\underline{o}}\ primo\ \ o\ pseudoprimo)$$

$$Residuo > 0 = C\ (n^{\underline{o}}\ compuesto)$$

Existen 4 tipos de números que podemos encontrar una vez finalizado el **Proceso 2**

A) Si el resultado es **afirmativo** obtenemos:	B) Si es el resultado es **neutro** obtenemos**:**
P_s: $N^{\underline{o}}\ Primo\ Seguro.$ P_r: $N^{\underline{o}}\ Primo\ Resistente.$	P_d: $N^{\underline{o}}\ Primo\ débil.$ Psp: $N^{\underline{o}}\ Pseudoprimo.$

Profesor Zeolla Gabriel M.

Características

$P_s = Nº\ Primo\ Seguro$

Su residuo es cero y no repite ningún resto, formando un ciclo de números sin repetición y su ciclo es **número primo**. Por lo cual son detectados fácilmente. Estos números primos pueden construirse simplemente buscando ciclos primos. Son de la forma 2p+1, ($p\ es\ primo$, $\in \mathbb{N}$)

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

A estos números se los conoce como primos Seguros, estos tienen ciclos formados por primos de ***Sophie Germain***

Referencia OEIS: A005385 Primos Seguros
Referencia OEIS: A005384 Sophie Germain.

$P_r = Nº\ primo\ Resistente$

Su residuo es cero. No repite ningún resto, formando un ciclo de números sin repetición, su ciclo es un **número compuesto**, el cual debemos factorizar para hallar sus divisores, los cuales nos darán información sobre la no repetición de restos.

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

$P_d = Nº\ Primo\ débil$

Su residuo es cero. Forma patrones numéricos ya que repite restos. Su ciclo es un número Compuesto.

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

Estos representan el 30% aproximadamente de los números primos.

Referencia OEIS: A082595

$Psp = Nº\ Pseudoprimo.$

Su residuo es cero. Forma patrones numéricos ya que repite restos. Su ciclo es un número compuesto.

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

Referencia OEIS A047713

Estos representan una muy pequeña porción de los números compuestos que pasan el proceso 2.

Profesor Zeolla Gabriel M.

Como analizar un patrón de restos

Existen 2 formas de hacerlo, la primera es aplicando un **Método artesanal** y la segunda mediante el **cálculo de divisores** de su ciclo.

Método Artesanal: Consiste armar toda la secuencia de restos, aplicando la fórmula del proceso 1. Y descendiendo exponente por exponente hasta su ¾ parte. Si ningún resto se repite hasta allí ya no se repetirán por lo cual podemos afirmar que ese número es Primo. Los restos se construyen fácilmente, cada vez que bajo un exponente si el resto es par lo divido por 2, si el resto es impar le sumo (n) y lo divido por 2.
Se puede utilizar como método determinante para confirmar la primalidad. Este método es explícito y didáctico. Muy sencillo de comprender para el alumno.
Con una simple hoja de Microsoft Excel podemos resolver cualquier número grande. Aunque para números de enormes cantidades de dígitos es recomendable el diseño de una aplicación o Software.

Ejemplo Test 37

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

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

Ciclo 18

Test **37**

Total	base	Resto	modulo
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)

Construcción de los restos

A) Si el resto anterior es **Par**, divido por 2 y le resto 1 al índice del exponente de 2.

B) Si el resto anterior es **impar**. Aplicamos $(r - n\ )/2$

Ejemplo en la tercer fila, $n = 37$

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

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

Lo puedo completar totalmente hasta el índice 0 de la potencia de 2, o lo puedo hacer como mínimo hasta la ¾ +1 del ciclo para chequear si se repite algún resto.

Este proceso es didáctico pero largo para números muy grandes.

El 37 es Primo ya que no repite restos y su residuo es cero.

Profesor Zeolla Gabriel M.

Calculo de divisores: Este permite evitar confeccionar la tabla completa y directamente resolver mediante un cálculo el cual a través de los divisores nos confirma si los restos se repiten o no. Ya que los restos se repiten respetando los divisores del ciclo.

El primer paso: Consiste en encontrar el ciclo de restos, este lo hallamos en el índice del exponente de 2 en la formula inicial.
En este caso utilizando el ejemplo anterior (test: 37)

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

Tomamos el $\mathbf{2^{17}}$ y al índice (17) le sumamos 1, ya que su ciclo se inicia en 0 y tiene 18 filas. Por lo tanto, su ciclo es de 18.
También se puede calcular el ciclo utilizando la fórmula:

$$ciclo\ de\ restos = \frac{n-1}{2}$$

$$Ciclo\ de\ restos = \frac{37-1}{2} = 18$$

Segundo paso Busco los divisores de 18

Los divisores de 18 son: {1,**2,3,6,9**,18}
Tomo los divisores $1 < d < 18$

Tercer paso Consiste en restar los divisores a la potencia de $\mathbf{2^{17-d}}$ y verificar si hay congruencia o no para determinar la primalidad.

Leer a continuación como detectar números primos Resistentes utilizando el cálculo de divisores.

Profesor Zeolla Gabriel M.

Fórmula para detectar números primos Resistentes

Método Cálculo de Divisores.

Los números primos resistentes tienen la característica de no repetir restos y tener residuo cero, pero para identificarlos necesitamos realizar el siguiente procedimiento.
Los números primos Resistentes están formados por ciclos que pertenecen a los números compuestos, por tal motivo se deberá factorizar a dicho número para obtener sus divisores. Una vez hallados nos permitirá definir con el 100% de exactitud si el número es primo o (primo débil o pseudoprimo).

Esta fórmula tiene dos variables

Formula A. Tiene ciclos Alternos. Significa que el primer patrón esta por la mitad, por lo que debemos multiplicar por dos a sus divisores.

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

$$Formula\ inicial$$
$$\exists n \in \mathbb{N}$$

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

$$\underline{Bajamos\ una\ potencia}$$

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

Entonces calculo el ciclo de restos.

$$\text{Ciclo de restos} = \frac{n-1}{2}$$

d = Divisores del Ciclo de restos.

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

Formula B: Ciclos Normales: Significa que sus patrones están completos.

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

$$Formula\ inicial$$
$$\exists m \in \mathbb{N}$$

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

$$\underline{Bajamos\ una\ potencia}$$

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

Entonces calculo el ciclo de restos.

$$\text{Ciclo de restos} = \frac{m-1}{2}$$

d = Divisores del Ciclo de restos

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

Ejemplo A: Test 67	**Ejemplo B**: Test 71
$$\mathbf{2^{\left(\frac{m-1}{2}\right)} + 1 \equiv 0\ (mod\ m)}$$	$$\mathbf{2^{\left(\frac{n-1}{2}\right)} - 1 \equiv 0\ (mod\ n)}$$
$$2^{\left(\frac{67-1}{2}\right)} + 1 \equiv 0\ (mod\ 67)$$ $$= 2^{33} + 1 \equiv 0\ (mod\ 67)$$	$$2^{\left(\frac{71-1}{2}\right)} - 1 \equiv 0\ (mod\ 71)$$ $$= 2^{35} - 1 \equiv 0\ (mod\ 71)$$
$$\underline{Bajamos\ una\ potencia}$$	$$\underline{Bajamos\ una\ potencia}$$
$$= \mathbf{2^{32} - 33 \equiv 0\ (mod\ 67)}$$	$$= \mathbf{2^{34} - 36 \equiv 0\ (mod\ 71)}$$
Ciclo de restos = $\frac{67-1}{2}$ =33	Ciclo de restos =$\frac{71-1}{2} = 35$
$$d_{(33)} = \{1,3,11,33\}$$	$$d_{(35)} = \{1,5,7,35\}$$
Entonces $= 2^{32-d} - 33 \not\equiv 0\ (mod\ 67)$ $\leftrightarrow se\ cumple\ \forall\ d/\ 1 < d < 33$ $\rightarrow n = P\ (nº\ primo)$	Entonces $= 2^{34-d} - 36 \not\equiv 0\ (mod\ 71)$ $\leftrightarrow se\ cumple\ \forall\ d/\ 1 < d < 35$ $\rightarrow n = P\ (nº\ primo)$
$$2^{32-2*11} - 33 \not\equiv 0\ (mod\ 67)$$ $$= 2^{10} - 33 \not\equiv 0\ (mod\ 67)$$	$$2^{34-7} - 36 \not\equiv 0\ (mod\ 71)$$ $$= 2^{27} - 36 \not\equiv 0\ (mod\ 71)$$
$$2^{32-2*3} - 33 \not\equiv 0\ (mod\ 67)$$ $$= 2^{26} - 33 \not\equiv 0\ (mod\ 67)$$	$$2^{34-5} - 36 \not\equiv 0\ (mod\ 71)$$ $$= 2^{29} - 36 \not\equiv 0\ (mod\ 71)$$
Como **No es congruente** en ambas expresiones entonces 67 es número primo Resistente. Esto significa que en el ciclo formado por restos no se repite ningún valor.	Como **No es congruente** en ambas expresiones entonces 71 es número primo Resistente. Esto significa que en el ciclo formado por restos no se repite ningún valor.

Profesor Zeolla Gabriel M.

Números Primos Seguros
Primos que construyen primos

Un primo (q) se dice que es seguro si, además de ser primo, es el resultado de multiplicar por dos un primo (p) menor y sumarle uno. Por ejemplo, el número 23 es primo seguro porque 23 = 2 x 11 + 1, siendo 11 y 23 primos.
Los números primos seguros están construidos por un número primo en su ciclo.

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

Los números primos Seguros son de la forma:

$$P_s = 2q + 1, cuando\ q\ es\ igual\ al\ ciclo\ y\ a\ su\ vez\ es\ numero\ primo.$$

Test de primalidad para números primos Seguros y números primos de Sophie Germain

Descarga el documento vinculado a este trabajo.
https://www.academia.edu/49807487/Argentest_primality_test_for_Sophie_Germains_prime_numbers_and_safe_prime_numbers.

Ejemplo: Test de un número primo Seguro n=47

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

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

Método: Calculo de divisores

$$Bajo\ una\ potencia$$

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

Ciclo de restos = $\frac{47-1}{2} = \mathbf{23}$

Profesor Zeolla Gabriel M.

Divisores de 23:

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

No hay (d) divisores entre 1 y 23, esto significa que el 23 es número primo de Sophie Germain por lo cual no se repetirá ningún resto en su ciclo.

∴ es un número primo seguro

Método Artesanal

Test 47 ciclo de 23

Total	Potencia	resto	Residuo y modulo
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)

Características de todos los números primos Seguro

- **No se repite ningún resto**
- **Sus residuos son 0**
- Su ciclo es **número primo**, en este caso el 23, ya que 22 es el índice de la potencia de dos, 22+1=**23** le sumamos 1 por que este se inicia en 0.
- El Patrón de restos finaliza en valores decrecientes hasta llegar a 1 en las últimas potencias.
- Los totales tienen valores que pertenecen a los números naturales y el cero.
- El 47 finalmente es número primo por todas las razones anteriores, pero sobre todo por las dos primeras.

Profesor Zeolla Gabriel M.

Números Pseudoprimos

Los pseudoprimos son números compuestos impares, que pasan el proceso 1 y logran mezclarse con los números primos. Estos números se los conoce como los números de Carmichael.
Por tal motivo cuando los llevamos al proceso 2 y analizamos los restos de sus ciclos estos números siempre tienen restos repetidos y forman patrones, ya que en su esencia son números compuestos, lo cual nos permite poder clasificarlos satisfactoriamente.

Los ciclos de los números pseudoprimos siempre son un número compuesto para la base 2.
He testeado los pseudoprimos hasta el número 285.000.000 y ninguno de ellos tiene ciclo primo hasta allí. Si bien no tengo una demostración, este resultado es para tener en cuenta sin lugar a dudas ya que si los ciclos primos no aparecieron hasta aquí difícilmente aparezcan con números más grandes. Pero es una posibilidad abierta.
Este detalle les da solidez a los números primos seguros.

$$Psp \neq 2p + 1, siendo\ p\ número\ primo$$

***Psp*: *Pseudoprimo*.**
Su residuo es cero. Forma patrones numéricos ya que repite restos. **Su ciclo es un número compuesto**.

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

Referencia OEIS A047713

Estos representan una muy pequeña porción de los números compuestos.

$$Ciclo\ de\ restos = \frac{n-1}{2}$$

Psp	Ciclo de restos	Característica del ciclo
561	280	Compuesto
1.105	552	Compuesto
1.729	864	Compuesto
1.905	952	Compuesto
2.047	1.023	Compuesto
2.465	1.232	Compuesto
3.277	1.638	Compuesto
4.033	2.016	Compuesto
4.681	2.340	Compuesto
6.601	3.300	Compuesto
8.321	4.160	Compuesto
8.481	4240	Compuesto
10.585	5.292	Compuesto
12.801	6.400	Compuesto

Profesor Zeolla Gabriel M.

Ejemplos donde los pseudoprimos no pasan el proceso 2

Ejemplo A: Test 3.277

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

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

Ciclo de restos= $\frac{3277-1}{2} = 1.638$

Divisores

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

$1 < d < 1.638$

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

Como es congruente en la última expresión entonces 3.277 es un pseudoprimo o número primo débil.

Esto significa que en el ciclo formado por restos se repiten valores y patrones.
En este caso habrá un patrón de 28 restos que se repiten simultáneamente.
En los ciclos alternos obtenemos ½ patrón sin completar.
Entonces tenemos 1638/28= 58,5
Esto significa que hay un patrón de 28 restos que se repiten 58 veces y 1 patrón queda por la mitad (14).

Por lo tanto, su ciclo alterno es de 28/14.
En el ciclo alterno el segundo número siempre es la mitad del primero y es el divisor que utilizamos para hallar el patrón.

$$28 * 56 + 14 = 1.638$$

Ejemplo B: Test 2.047

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

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

Ciclo de restos= $\frac{2.047-1}{2} = 1.023$

Divisores

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

$1 < d < 1.023$

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

Como es congruente en la segunda expresión entonces 2.047 es un pseudoprimo o número primo débil.
No hace falta seguir calculando más, basta con encontrar una congruencia para determinar el resultado.

Esto significa que en el ciclo formado por restos se repiten valores y patrones.
En este caso habrá un patrón de 11 restos que se repite 93 veces.

$$11 * 93 = 1.023$$

Profesor Zeolla Gabriel M.

Números Primos Débiles

Son aquellos números que no pasan el **proceso 2** satisfactoriamente y no podemos determinar si es un número primo o un pseudoprimo. Su ciclo es un número Compuesto.
Sus residuos son cero, pero la secuencia de restos tiene números repetidos que forman patrones, lo cual es condicionante y un impedimento para afirmar su primalidad.

Estos son algunos de los primos que no pasan el Argentest para la base 2.

P_d: Número Primo débil

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

Estos representan el 30% aproximadamente del conjunto de los números primos.

Referencia OEIS: A082595

Los pseudoprimos no pasan el Argentest para la base 2 ya que también sus restos forman patrones.

Psp: Pseudoprimo.

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

Referencia OEIS A047713

Estos representan una muy pequeña porción de los números compuestos.

Profesor Zeolla Gabriel M.

Los números primos de Mersenne son nº Primos Débiles

En el Argentest los Números primos de Mersenne mayores a 7 son primos débiles para la base 2.
Estos tienen restos que forman patrones formados por la secuencias de 2^n, esto No permite clasificarlos satisfactoriamente en esta base ya que existen números pseudoprimos del mismo estilo. **Ejemplo 2.047**

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

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

Podemos observar que prácticamente los patrones de restos están formados por la secuencias de $hasta\ 2^n < n$, También en ambos casos tienen residuo 0. La suma de cada patrón es igual n.
Y en todos los casos su resto comienza con $(n+1)/2$, luego sus restos van descendiendo en divisiones por 2 ininterrumpidas hasta llegar al 1.
Ejemplos

Número primo débil

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

Test 31 Patrón de 5

Total	Base	Resto	Residuo y Modulo
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 es el número de ciclo.
El cual tiene los divisores
d: {1,3, 5,15}
En este caso está formado por un patrón de 5 restos y 3 repeticiones.
El patrón de 5 restos tiene relación con los números de Mersenne, ya que $2^5 - 1 = 31$

Pseudoprimo (Recorte del ciclo completo)

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

Test 2.047 Patrón de 11

	Base	Resto	Residuo y modulo
	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 es el número de ciclo.
El cual tiene los divisores:
$d = \{1, 3, 11, 31, 33, 93, 341, 1023\}$
En este caso está formado por un patrón de 11 restos y 93 repeticiones.
El patrón de 11 restos tiene relación con los números de Mersenne, ya que $2^{11} - 1 = 2.047$

Profesor Zeolla Gabriel M.

Capítulo III

Proceso 3. Cambio de base

Fórmula para determinar primalidad con bases mayores a 2.
Es la misma que utilizamos en la base 2.

La fórmula principal funciona con el criterio de Euler, aunque tiene una pequeña modificación la cual nos facilita poder construir la secuencia de restos sin problemas en la base 3 de forma artesanal.

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

A los números primos débiles les aplicamos el proceso3.
El proceso 3 consiste en cambiar la base 2 por la base 3 y entonces formar la secuencia de restos y poder chequear si hay o no patrones para confirmar la primalidad.

Fórmula para determinar primalidad con base 3

La fórmula principal sale del criterio de Euler, aunque tiene una pequeña modificación la cual nos facilita poder construir la secuencia de restos sin problemas en la base 3 de forma artesanal.

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

Cuando $k \equiv 1 \vee 4\ (Mod\ 6)$
$n = 2k - 1\ \ (es\ numero\ compuesto\ múltiplo\ de\ 3)$.
Ejemplo: 561

Método artesanal.

Ejemplo Formula A: Test 31

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

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

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

Total	Base	resto	Residuo y modulo
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)

No repite ***Restos*** por lo cual se confirma su primalidad con el cambio de base.

Comenzamos analizando restos a partir de

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

<u>Construcción de restos tiene 3 opciones</u>

A) Si el resto anterior es múltiplo de 3, se divide por 3.

B) Si el resto anterior no es múltiplo de 3, entonces, aplicamos $(\boldsymbol{r-n})/\mathbf{3}$

$n = 31$

Ejemplo 3^{14}

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

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

C) Si realizando el primer paso y el segundo y no obtenemos un múltiplo de 3 entonces:

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

Ejemplo en 3^9

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

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

D) si realizando los pasos anteriores y no se consigue un múltiplo de 3. Significa que este número testeado es compuesto y múltiplo de 3.

Profesor Zeolla Gabriel M.

Método de cálculos de divisores

Es exactamente igual que en la base 2. Buscamos los divisores del ciclo para chequear si algún resto se repite.

Ejemplo A: Test 73. Ciclo normal

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

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

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

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

Busco los divisores del ciclo $\left(\frac{73-1}{2}\right)$ =36
$$d_{(36)} = \{1,2,3,4,6,9,12,18,36\}$$

$$entonces\ 1 < d < 36$$

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

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

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

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

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

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

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

Como es **congruente** en la ante última expresión, entonces 73 es número primo Débil de base 3.
Esto significa que en el ciclo formado por restos se repiten valores.
Por lo cual tendrá un patrón de 12 restos que se repite 3 veces (el 12 surge del divisor).
12*3=36 (número de ciclo)

Por lo cual debemos volver a analizarlo con la base 4 para volver examinar su ciclo.
Este número tiene la particularidad de confirmar su primalidad recién con la base 5.

Profesor Zeolla Gabriel M.

Ejemplo: Análisis del número 73 para la base 3.

Método: artesanal

Secuencia de restos abreviada.

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

Test 73

Total	base	resto	Residuo y modulo
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)

continua

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

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

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

Analizamos el ciclo a partir de la potencia anterior

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

Vemos que tiene un patrón de 12 restos el cual se vuelve a iniciar a partir de 3^{23}, luego en 3^{11}.

Profesor Zeolla Gabriel M.

Números Primos Débiles con la base 3

Los números primos débiles de base 2 que no pasaron el proceso 2, los pasamos por el proceso 3. El 60% de ellos podrá confirmar su primalidad, pero un 40% restante será primo débil nuevamente.
Por ejemplo, el 73. Este tiene patrones con la base 2 y también con la base 3. Por lo tanto, lo definimos como primo débil de base 3.

Para ser considerado número primo en la base 3 las condiciones siguen siendo las mismas que en la base 2, el (n) de entrada tiene que tener:

Residuo =0
Repeticiones de restos = 0

Estos números tienen residuo 0 pero tienen repeticiones de restos. Por lo cual no podemos confirmar su primalidad y los postulamos como número primo débil de base 3.
Ejemplos

$$P_{d3} = \{73,109,151,229,277,307,433,439,499,577,601, \dots .\}$$

A estos números deberíamos someterlos a otro cambio de base (proceso 4) para poder separarlos de los pseudoprimos de base 2. Realizar el mismo análisis y volver a depurar la secuencia.

Pseudoprimos con resultado neutro para la base 3

Son los pseudoprimos de base 2 que no pasan el proceso 3 y que siguen teniendo restos repetidos que forman patrones.
Estos pseudoprimos de base 2 tienen residuo 0 pero tienen repeticiones de restos por lo cual son candidatos a número primo débil de base 3.
Ejemplo

$$Psp_3 = \{\ 1.729, 10.585, 15.841, \dots . .\}$$

Pseudoprimos con resultado negativo para la Base 3

Son aquellos números que su residuo es mayor a 0 o son múltiplos de 3. Por lo cual certificamos que es número compuesto. **Po lo tanto el conjunto de los pseudoprimos se va reduciendo significativamente con el cambio de base.**

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

Ejemplos

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

Profesor Zeolla Gabriel M.

Capítulo VI

Proceso 4. Cambio de base

A los números primos débiles del proceso 3 les aplicamos el proceso 4.
El proceso 4 consiste en cambiar la base 3 por la base 4 y entonces formar la secuencia de restos y poder chequear si hay o no patrones para confirmar la primalidad.

El método es exactamente igual que en las bases anteriores.
Podemos cambiar de bases las veces que necesitemos y el mecanismo siempre será el mismo.

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

Construimos la secuencia de forma artesanal dividiendo por 4 cuando es múltiplo de 4, de lo contrario le restamos (n) hasta encontrar un múltiplo, para luego dividir por 4. La sucesión de restos finaliza en 1 cuando es primo o pseudoprimo.

Condiciones de primalidad
Residuo =0
Repeticiones de restos =0

Conclusión

Hace siglos los chinos utilizaban lo que hoy conocemos como el pequeño teorema de Fermat y creían que alcanzaba solo con el residuo igual a cero para certificar la primalidad de un número impar, hasta que mucho tiempo después se descubrieron los números pseudoprimos.
Argentest trae las condiciones faltantes para determinar la primalidad de un número impar, la cual es la no repetición de restos.
Argentest es una nueva y simple herramienta para poder certificar la primalidad de un número (n) impar, utiliza mecanismos sencillos y didácticos para los alumnos. Ya que mediante la construcción de tablas o cálculos eficientes logramos el objetivo en unos simples pasos.
El Argentest es una nueva posibilidad que aporta certidumbre ante la gran desazón que han provocado los números primos en grandes matemáticos del pasado.
Hoy existen muchos test de primalidad muy interesantes y con diferentes grados de aplicación, este nuevo algoritmo pretende ser una nueva posibilidad y otra forma de conocer e interpretar a los números primos.

Profesor Zeolla Gabriel Martín
Buenos Aires, Argentina.

Descarga la planilla de cálculo de Microsoft Excel: Para el cálculo del método artesanal.

Otros documentos del autor:
https://independent.academia.edu/GabrielZeolla

Referencias

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.

Profesor Zeolla Gabriel M.

Flannery, S. and Flannery, D. *In Code: A Mathematical Journey.* London: Profile Books, pp. 118-125, 2000.