212 TEST DE PRIMALIDAD

Ghersi Liliana Beatriz
Facultad Ciencias Económicas Universidad de Buenos Aires
lbghersi@gmail.com

Especialidad: Matemática Aplicada

Palabras Clave: Primalidad, Pseudoprimos, Test probabilísticos, Test determinísticos, Firma digital

Resumen

La firma digital, es una herramienta tecnológica, que permite asegurar el origen de un documento digital o mensaje digital y verificar que su contenido no haya sido alterado; puede ser considerada como el resultado de una transformación de un documento digital empleando un criptograma asimétrico y un digesto seguro. Resulta ser recurso para desburocratizar, agilizar y transparentar los trámites, tanto en la administración pública como en el mundo de los negocios.
En la actualidad los algoritmos de firma digital que pueden citarse son: RSA (estándar internacional de facto), Gammal y DSA. Todos estos algoritmos, requieren el empleo de números primos muy grandes, siendo usual que la cantidad de bits de dichos números se ubique entre los 512 y 2048 y basan su seguridad en la imposibilidad práctica de factorizar números compuestos de gran tamaño.
Ahora bien, analizar la condición de primo o como se ha dado en llamar analizar la primalidad; como factorizar a números en el caso de que sea compuesto, son acciones que presentan un desafío operacional de alta complejidad cuando se trata de un número natural del tamaño de dígitos que requieren los citados sistemas criptográficos.
Es por ello, que es necesario de contar con técnicas apropiadas para la determinación sobre si un número puede ser considerado compuesto o primo. A tal efecto, existen pruebas de primalidad, comportando dos tipos; los test determinísticos de primalidad que son criterios que permite decidir si un número es o no primo y los test de pseudoprimalidad o probabilísticos de primalidad, que son criterios que permiten decidir con un alto grado de probabilidad si un número es o no primo. Estas pruebas, presentan un desafío operacional de alta complejidad puesto el/los números/s natural/es que requieren los citados sistemas criptográficos están determinados por una cantidad muy grande de bits.

1. Introducción:

La firma digital, como ya se dijo en el resumen de este trabajo; es una herramienta tecnológica, que permite asegurar el origen de un documento digital o mensaje digital y verificar que su contenido no haya sido alterado; puede ser considerada como el resultado de una transformación de un documento digital empleando un criptograma asimétrico y un digesto seguro. Resulta ser recurso para desburocratizar, agilizar y transparentar los trámites, tanto en la administración pública como en el mundo de los negocios. En la actualidad los algoritmos de firma digital que pueden citarse son: RSA (estándar internacional de facto), Gammal y DSA. Todos estos algoritmos, requieren el empleo de números primos muy grandes, siendo usual que la cantidad de bits de dichos números se ubique entre los 512 y 2048 y basan su seguridad en la imposibilidad práctica de factorizar números compuestos de gran tamaño; es por ello que analizar la condición de primo o como se ha dado en llamar analizar la primalidad y factorizar a números en el caso de que sea compuesto, son acciones que presentan un desafío operacional de alta complejidad cuando se trata de un número natural del tamaño de dígitos que requieren los citados sistemas criptográficos.

Los números primos, han llamado la atención desde la antigüedad, pues no existen pautas en cuanto a su aparición en la sucesión de los números naturales como tampoco tienen un comportamiento claro en lo que respecta a su ausencia o a la manera en que dejan de aparecer; y es esta peculiaridad lo que los hace tan interesantes para la aplicación en criptografía. Además, son la esencia de la aritmética ya que el vocablo primo, proviene del latín primus, que equivale a

decir primero y refiere al concepto de primitivo en el sentido de origen, puesto que todos los números pueden obtenerse a partir de ellos.

Considero oportuno subrayar las siguientes cuestiones:

1ª) Que el conjunto de los números primos es infinito, por lo tanto no es posible definirlo por extensión, lo que equivale a decir que es imposible listarlos completamente y que por ende la definición se basa en sus propiedades.

2ª) Que a partir de su definición, es posible describirlos y determinar las propiedades que los hacen identificables, pero usualmente la verificación práctica de las mismas resulta una actividad ardua en tiempo computacional.

3·ª) Que el número de veces que un número primo puede intervenir en la factorización de un compuesto no encuentra limitación

4ª) Que asimismo es inexistente la limitación en lo atinente al número de primos que pueden intervenir en la factorización de un compuesto.

Ahora bien, antes de abordar el tema relativo a los test de primalidad se presentarán algunas consideraciones, que pueden resultar conocidas, pero no por ello de peso en el desarrollo del presente trabajo. Definición: Si a y b son números naturales, el mayor de sus divisores positivos comunes será llamado el máximo común divisor de a y b, lo cual será denotado como: (a:b); si (a:b) = 1, o lo que es lo mismo decir que el único divisor positivo común de a y b es uno, siendo a y b números naturales; se dirá de a y b, que son coprimos.

Coprimalidad: Se emplea esta terminología para abordar el estudio del carácter de coprimos; que resulta ser una cuestión no menor en el contexto de este trabajo.

La probabilidad de que dos números enteros elegidos al azar sean coprimos es igual a $\frac{6}{\pi^2}$; un medio rápido para determinar si dos números enteros son primos entre sí es el algoritmo de Euclides.

Tabla 1: Ejemplo Algoritmo de Euclides

iteración	b	a	q	r
0	1326	129	10	36
1	129	36	3	21
2	36	21	1	15
3	21	15	1	6
4	15	6	2	3
5	6	3	1	3
6	3	3	1	0

$(1326:129) = (r_4 : r_5) = r_5 = 3;\ r_6 = 0$

Definición: Sea n un número natural y sean a y b números enteros. Se dice que a es congruente con b módulo n si y sólo si a-b es múltiplo de n y en tal caso se emplea la notación:

$$a \equiv b(\text{módulo } n)\ (1)$$

Pequeño Teorema de Fermat: El enunciado del teorema se puede presentar de dos maneras distintas;

A partir de la condición de primo/coprimos para los números intervinientes:

Si p es un número primo y a otro número cualquiera, de manera que a y p sean primos entre sí, entonces se cumple que la diferencia entre *a* potenciado a la *p* y *a*, es divisible por *p*.

Basándose en la aritmética modular: Si p es un número primo y a es un entero no divisible por p, entonces a potenciado a la (p-1) es congruente 1 módulo p.

La importancia de este teorema a la luz de la aritmética modular es que permite comprobar en determinadas condiciones y con cierta facilidad, si un número puede ser considerado primo.

Residuos Cuadráticos: Dados un primo p y un número a, se dice que a es un residuo cuadrático módulo p (RC módulo p) si y sólo si existe un número x tal que el cuadrado de dicho número es congruente *a* módulo *p*. Se puede interpretar como el residuo que corresponde a la división entre el cuadrado de un número y el número p. Todo cuadrado perfecto es un RC módulo p, pero la recíproca no es vale. Por ejemplo: 2 es RC módulo 7, ya que el cuadrado de 4 es 16 que resulta ser congruente con 2 módulo 7

Definición: Si a es un entero y p un primo impar, el símbolo de Legendre de a con respecto a p, denotado $\left(\frac{a}{p}\right)$, se define como: *cero* si *a* es divisible por *p,* uno si a es RC módulo p y el opuesto de uno si a no es RC módulo p

Criterio de Euler: afirma que si *a* es un entero no divisible por *p* (primo) y *p*>2, entonces, a es un RC módulo p si y solo si a potenciado a la mitad del anterior de p, es congruente 1 módulo p, que puede replantearse de la siguiente manera: el símbolo de Legendre de a con respecto a p, es congruente *a* potenciado a la mitad del anterior de p, módulo p

Tabla 2: Símbolo de Legendre módulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$a^9(19)$	1	18	18	1	1	1	1	18	1	18	1	18	18	18	18	1	1	18
Sìmbolo de Legendre	1	-1	-1	1	1	1	1	-1	1	-1	1	-1	-1	-1	-1	1	1	-1

El Símbolo de Jacobi: Es útil para evaluar si un número es pseudoprimo. Si a es un entero, se define el símbolo de Jacobi de *a* con respecto a *n* como el producto de los símbolos de Legendre de *a* con respecto a cada uno de los primos en que se factoriza *n*

Debe tenerse en cuenta que: Si n es primo el símbolo de Jacobi coincide con el símbolo de Legendre, por lo tanto es un buen elemento decisor sobre la condición de a respecto de si es RC módulo n.

Si n no es primo el símbolo de Jacobi no decide si a es RC módulo n; pero sí decide si a no es RC módulo n.

2. Pruebas de Primalidad.

En cuanto al tema de la determinación sobre si un número puede ser considerado compuesto o primo, existen pruebas de primalidad que no hacen necesaria la factorización del número y no brindan información n alguna referida a cuáles son los factores de ese número entero en el caso de que la prueba determine que el entero es compuesto. Existen dos tipos de pruebas de primalidad; los test determinísticos de primalidad que son criterios que permiten decidir si un número es o no primo y los test de pseudoprimalidad o probabilísticos de primalidad, que son criterios que permiten decidir con un alto grado de probabilidad si un número es o no primo. La condición de primalidad es fundamental, pues asegura la existencia de inversos para cualquier entero en la aritmética modular si el módulo es un primo, cuestión no menor en la criptografia asimétrica, que es la que sustenta la fortaleza de la firma digital.

2.1. Test Determinísticos de Primalidad:

2.1.1. Criba de Eratóstenes:

Uno de los primeros métodos de generación de números primos se conoce como la criba de Eratóstenes que se le atribuye a Eratóstenes de Cirene (276 – 194 a.C.) quien fuera director de la biblioteca de Alejandría; antes de abordarlo conviene tener presente el siguiente resultado: Todo número natural compuesto es divisible por algún primo menor ò igual que su raíz cuadrada.

Por lo tanto, si se desean obtener todos los números primos menores que una natural N se genera una matriz de $\sqrt{N} * \sqrt{N}$, se asigna a cada celda un natural de manera consecutiva hasta N, y a partir de ella sin el uno, se eliminan todos los números múltiplos de dos (1° ciclo), luego los de tres (2° ciclo), luego los de cinco (3° ciclo) y así sucesivamente por cada uno de los primos menores o iguales que $\sqrt{N}$; los números que no fueron eliminados de la tabla, son todos los números primos menores que N. Por ejemplo, si N=400, se requieren ocho ciclos, ya que hay ocho primos menores que $\sqrt{400} = 20$. Se descarta su uso en firma digital.

De la lista de los primos menores a mil, surge la siguiente distribución de frecuencias de números primos (visión probabilística):

Tabla 3: Distribución de frecuencias primos menores que 1000

Primos pertenecientes a:	(1-100]	(100-200]	(200-300]	(300-400]	(400-500]	(500-600]	(600-700]	(700-800]	(800-900]	(900-1000]
Frecuencia	25	21	16	16	17	14	16	14	15	14

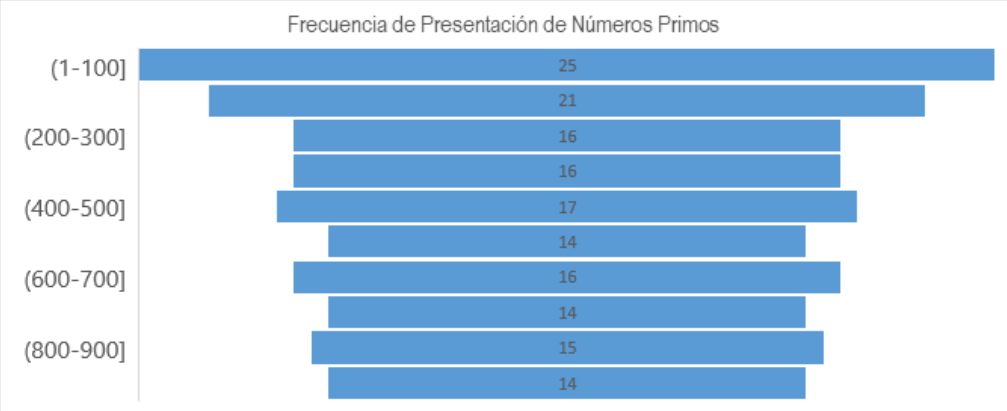

Gráfico 1: Distribución de Presentación de los Primos Menores que 1000

Teorema de Wilson: un número natural *n* es primo si y solo si, *n* es divisible por la suma entre factorial del anterior a n y uno

2.1.2. Prueba Resultante de Wilson:

Para determinar el carácter de primo de un número, a partir del Teorema de Wilson, no necesariamente se debe calcular el factorial en cuestión, pero si n es un valor grande la cantidad de reducciones módulo n necesarias lo hace impracticable, el enunciado del teorema a la luz de la aritmética modular es equivalente a la afirmación:

el factorial del anterior a *n*, es congruente a menos uno modulo *n*.

Tabla 4 – Ejemplos Numéricos del Teorema de Wilson

n	5	7	11	13
(n-1)!	24	720	3628800	479001600
A=(n-1)!+1	25	721	3628801	479001601
A/n	5,00	103,00	329891,00	36846277,00

Ambos procesos, la Criba de Eratóstenes y el que surge del Teorema de Wilson, son pruebas de primalidad determinísticas puesto que aseguran la condición de primo del número si el mismo supera el testeo, pero requieren de muchos ensayos y cálculos, con lo cual los mismos no resultan eficientes, para firma digital.

2.1.3. Prueba de Lucas-Lehmer:

La prueba de Lucas-Lehmer, desarrollada en 1878 por Edouard Lucas y perfeccionada por Derrick Henry Lehmer en la década de 1930, permite decidir de manera determinística si un número de Mersenne Mp es primo.

Los números primos de Mersenne M, son de la forma si $2^p - 1$ con p primo, pero debe tenerse en cuenta que p sea primo no implica que $2^p - 1$ sea primo, con lo cual tampoco resulta ser una fórmula de generación de primos.

La prueba para dichos números, consiste en definir una sucesión que viene dada de la siguiente manera: el primer elemento vale 4, y los siguientes se generan como el cuadra del anterior decrementado en dos. Entonces, Mp es primo si y sólo si el elemento p-2 de la sucesión es congruente 0 módulo Mp; para todo otro caso Mp es compuesto. El número s_{p-2} (módulo Mp) se llama residuo Lucas-Lehmer de p.

Tabla 5– Ejemplos Numéricos de la Prueba Lucas-Lehmer

p					Residuo Lucas-Lehmer de p
	s_0	4			
	s_1	14			
	s_2	194			
5	s_3	37634	31	0	0
	s_4	1416317954			
7	s_5	2,006E+18	127	0	0

2.2. Test de Pseudoprimalidad o Probabilísticos de Primalidad.

Estas pruebas someten a un número grande y candidato a primo, a varias rondas de chequeo; si bien las mismas no permiten afirmar que el número que supera las iteraciones sea primo, otorgan una razonable certeza que sí lo sea con una probabilidad alta y la que puede estimarse. Resultan ser muy ágiles en el caso que los números a validar como primos resulten ser compuesto.

Con estos tipos de pruebas, queda asegurada la condición de compuesto en tanto que la propiedad de primo es probabilística. Son las apropiadas para los algoritmos subyacentes en la firma digital.

2.2.1. Test de Fermat:

Sea n impar, el número natural que se pone a prueba su condición de primalidad. Sea a perteneciente al intervalo abierto (1; n-1) un número elegido aleatoriamente Vuelta Opcional recomendada: Por medio del algoritmo de Euclides

analizar si el máximo común divisor entre n y a es 1, o sea si son coprimos, de no serlos es evidencia de que n es compuesto, y habrá encontrado un factor propio de n. Se descartan a=1 o a=n-1 como bases, debido a que las mismas siempre pasarán el test.

Primera vuelta: se calcula x, el cual viene dado por el resto de dividir a la potencia de *a* a la n menos uno por n, de ser distinto de uno, el numero n es compuesto y en este caso el test finaliza con certeza; en caso contrario, la prueba falla; nada se puede asegurar sobre n, pero se puede comenzar a sospechar levemente su primalidad. Se dirá que n supera el test respecto a la base a o bien que n es un probable primo respecto a la base a.

Vueltas subsiguientes: Habiendo fallado la prueba con la base elegida, se analiza si la cantidad de pruebas coincide con el 50% de las bases coprimas con n, si es menor o igual se elige una nueva base y se repiten la vuelta opcional y la primera vuelta; si en las mismas el número pasa la prueba aumenta la certidumbre acerca de la primalidad de n. Cuando la cantidad de pruebas supera al 50% de las bases coprimas con n, finaliza el test, y nuevamente nada se puede asegurar sobre n, pero se puede comenzar a sospechar con mayor seguridad su primalidad. Se dirá que n supera el test respecto a todas las bases coprimas o bien que n es un probable primo. La cantidad de vueltas para llegar al convencimiento de que n es primo se basa en el siguiente lema: Suponiendo que n no pasa el test respecto a una cierta base b; entonces n es un probable primo respecto a lo sumo al 50% de las bases coprimas con n y siendo esta cota óptima.

El lema citado plantea que si n es compuesto y no pasa el test para todas las posibles bases entonces se tendrá por lo menos el 50% de chance de que no lo pase respecto a una base elegida al azar. Dicho de otra manera, si n pasa el test respecto a una cierta base, existe una probabilidad menor o igual que 0,5 de que no sea primo. Si lo hace con respecto a dos bases dicha probabilidad será menor o igual que 0,25=0,52 y, generalizando, la probabilidad de que n sea compuesto y pase el test de Fermat respecto a k bases es menor o igual a 0,5k. A partir de este dato cuantitativo se puede estimar el número de rondas que se ejecutará el test antes de declarar primo a n, dependiendo del grado de certidumbre que se desee obtener. Si se desea tener un grado de confianza superior al 0,99 respecto a la primalidad de n, se deberán ejecutar al menos 7 rondas de la prueba, ya que 0,57=0,0078125 que resulta ser menor a un centésimo.

Sea n un entero compuesto y se a un entero perteneciente al intervalo [1; n-1] y el resto de dividir la potencia n-1 de a por n, es uno, se dice que n es un pseudoprimo con respecto a la base a. Al entero a, se lo llama “embaucador de Fermat” para n.

Ejemplo: Sea n=645=3*5*43 es pseudoprimo en base 2, puesto que 2^{644} es congruente 1 modulo 645

Es curioso que los pseudoprimos en base 2 sean muy escasos. Por ejemplo, hay 882206716 primos inferiores a 2×1010 y solo hay 19685 pseudoprimos en base 2 inferiores a 2×1010. Esto nos dice que la base 2 parece ser muy poco “embaucadora” en el sentido de que si tomamos un número grande n de manera aleatoria y si se verifica que $2^{n-1} \equiv 1$(módulo n), entonces es muy probable que n sea primo. También los pseudoprimos en base 3 son muy escasos y es altamente improbable que si tomamos un número grande n de manera aleatoria, este sea compuesto y que a la vez sea simultáneamente pseudoprimo en base 2 y base 3. Es decir, si un número n pasa los dos test $2^{n-1} \equiv 1$(módulo) y $3^{n-1} \equiv 1$(módulo) es muy probable que sea primo.

Pseudoprimos: el test también falla cuando se trata de un pseudoprimo, que son números conocidos como de Carmichael (1912). Estos números (n) cumplen con la propiedad que potencia (n-1) en una base que es coprima con él

es congruente 1 módulo n. El número 561=3(11)17 no es primo, sin embargo Para toda base coprima con 560 es congruente 1 modulo 561.

$a^{560} = (a^2)^{280} \equiv 1(módulo\ 3)\ a^{560} = (a^{10})^{56} \equiv 1(módulo\ 11)\quad a^{560} = (a^{16})^{35} \equiv 1(módulo\ 17)$(2)

Estos números son realmente raros, por lo que su existencia no invalida la utilidad del test de Fermat y está demostrado desde 1992 que existen infinitos. es pertinente acotar que solo hay 2163 pseudoprimos menores que 25x109 o sea uno cada once millones y medio de números. El siguiente enunciado, permite caracterizar perfectamente a un pseudoprimo: Un número impar n es pseudoprimo si y solo si es producto de r primos distintos.

2.2.2. Test de Solovay-Strassen (SS):

También denominado test de Jacobi, se basa en la siguiente condición: sea n es un entero impar, y sea a, con 0<a<n, se calculan $a^{(n-1)/2}$ y el símbolo de Jaobi .Si estos dos valores no son congruentes módulo n entonces el criterio de Euler asegura con certeza que n es compuesto; si en cambio son congruentes se ha obtenido una cierta evidencia de que n es primo, y se dice que n es un pseudoprimo de Euler respecto a la base a.

Se elige al azar una base a (1<a<n-1): Si el máximo común divisor entre ello es distinto de uno, decae que n es compuesto y finaliza la prueba; de lo contrario se calculan a potenciado a la mitad de n-1 y el símbolo de Jacobi dependiendo de a y n; si estos dos valores no son congruentes módulo n entonces el criterio de Euler asegura con certeza que n es compuesto y finaliza la prueba y de ser congruentes se ha obtenido una cierta evidencia de que n es primo, y se dice que n es un pseudoprimo de Euler respecto a la base a.

Se vuelve a elegir otra base, y se repite el proceso de análisis descripto anteriormente. Se continúa ensayando hasta haber obtenido suficiente evidencia de la primalidad de n. Los valores de a que cumplen el criterio de Euler se denominan verificadores de Euler para la primalidad de n y los que no lo cumplen se denominan falsadores de Euler para la primalidad de n. Es conveniente observar, que una condición necesaria pero no suficiente para que n pase el test respecto a una base x cualquiera es que ésta verifique una de las relaciones : que $x^{(n-1)/2}$ sea congruente 1 o -1 módulo n, puestos que éstos son los únicos valores que toma el símbolo de Jacobi.

Comparando el test de Fermat con el SS se puede afirmar que si n supera el test de Jacobi respecto a una base a entonces supera el test de Fermat respecto a dicha base; asimismo el análisis de las probabilidades resulta semejante para ambas pruebas, pero para el test de Jacobi afortunadamente no se presenta la problemática que plantean los números Carmichael para el de Fermat, situaciones que están avaladas por la siguiente proposición: Si n es compuesto, entonces no pasa el test de Jacobi con respecto a alguna base b y en tal caso, pasará el test respecto a los sumo el 50% de las bases. Si se desea establecer la primalidad de n con una probabilidad de error menor ò igual a un cierto δ, se debe determinar k de manera que $2^{-k} \leq \delta$ y se somete a n a prueba k veces; si las supera, se confía en su primalidad de no ser así se puede asegurar que n es compuesto.

El test de Jacobi, se lo puede considerar determinístico de primalidad puesto que n es primo si supera el test respecto a más de la mitad de las bases coprimas con él; pero por ser necesario operar con números muy grandes esta alternativa se convierte en impracticable y queda entonces en el ámbito de lo probabilístico. Fue descubierto en 1978 y fue modificado en 1982 por Atkin y Larson, pero en la actualidad está descartada su aplicación.

2.2.3. Test de Rabin-Miller:

También conocido como test fuerte del pseudoprimo o test fuerte de primalidad (TFP), es el más utilizado en la actualidad, ya que aventaja al de Jacobi y profundiza el método del test de Fermat. Se supone que n es un número natural impar y se desea estudiar su primalidad, y todas las cantidades referenciadas son reducidas módulo n.

Teorema de Rabin: Si n es un entero compuesto, a lo sumo ¼ de todos los números a, 1≤a≤n−1, son embaucadores fuertes de n. Dada una base b coprima con n primo, $b^{(n-1)}$ es congruente 1 módulo n se satisface si y sólo si $b^{(n-1)/2}$ sea congruente 1 o -1 módulo n

Se presentan entonces tres alternativas a considerar:

1ª) Si $b^{(n-1)/2}$ no es congruente 1 o -1 módulo n; se tiene con certeza que n es compuesto. 2ª) Si $b^{(n-1)/2}$ es congruente -1 módulo n; daría indicio que n es primo y se podría poner a prueba otra base. 3ªa) Si $b^{(n-1)/2}$ es congruente 1 módulo n y si (n-1)/2 es impar se repite la situación 2ª). 3ªb) Si $b^{(n-1)/2}$ es congruente 1 módulo n y si (n-1)/2 es par se replican las situaciones 1ª), 2ª) y 3ªa) pero referidas a los posibles valores de $b^{\frac{n-1}{4}} = b^m$.

Y así repetitivamente pero dividiendo sucesivamente por dos al valor de m del paso anterior (en tanto sea factible).

En la práctica, el algoritmo se plasma en los siguientes pasos y con el ordenamiento que se indica:

P1) Se factoriza a n-1 con 2^s (s mayor o igual a 1) y d (d impar). Lo cual implica dividir a n-1 por 2 todas las veces que sea posible.

P2) Se calcula $x_0 = b^d$ (b comprimo con n)

P2.1) Si x_0 es congruente 1 o -1 módulo n finaliza con cierta presunción que n es primo

Se dice que n pasa el test respecto a la base b o que n es un pseudoprimo fuerte respecto a la base b.

P2.2) Si

$$x_0 \equiv r(n)\ r \neq 1, se\ calcula\ x_j = x_{j-1}^2, 1 \leq j \leq s-1, x_j = b^{2^k d} y\ x_{s-1} = b^{\frac{n-1}{2}} (3)$$

xj congruente -1 módulo n finaliza con cierta presunción que n es primo
xj congruente 1 módulo n finaliza con certeza que n es compuesto
xj congruente r módulo n, r distinto de 1 o -1 se calcula x_{j+1} y se repite el análisis anterior si es que j es a lo sumo s-1

Por lo tanto, si se llega a j=s-1 y no se verifica que

$$x_{s-1} \equiv -1(n)\ (4),$$

se da por finalizado el test con la seguridad que n es compuesto.

En resumidas cuentas: n pasa el test de Rabin-Miller respecto a la base b si y solo si se verifica alguna de las siguientes relaciones, las cuales son mutuamente excluyentes:

$$b^d \equiv \pm 1(n)\ o\ b^{2^j d} \equiv -1(n) 1 \leq j \leq s-1\ (5)$$

En cualquier otro caso n es compuesto con certeza.

Si n pasa el test respecto de b se sigue probando con otras bases, hasta estar suficientemente convencidos que n es primo, o absolutamente seguros que no lo es.

Ejemplo: Tomado de Aritmética

Si $n = 481 = 13 * 37 \rightarrow n - 1 = 480 = 2^5 * 15$

Trabajando con congruencias módulo 13 y 37 y a través del teorema chino del resto, 481 pasa el TFP respecto a la base 8, puesto que:

$x_0 \equiv 8^{15} \equiv 31(módulo\ 481)$ Y por lo tanto: $x_1 \equiv 31^2 = 961 \equiv -1(módulo\ 481)$

Pero 481 no pasa el TFP respecto a la base 10, puesto que:

$x_0 \equiv 10^{15} \equiv 38(módulo\ 481)$ Y: $x_1 = 10^{30} \equiv 38^2 = 1444 \equiv 1(módulo\ 481)$

Es conveniente destacar que 481 pasa el test de Jacobi respecto a la base 10, ya que la última relación asegura que: $10^{240} = 10^{30^8} \equiv 1(módulo\ 481)$ Y: $\left(\frac{10}{481}\right) = \left(\frac{10}{13}\right) * \left(\frac{10}{19}\right) = (-1) * (-1) = 1$

La siguiente proposición, que dará elementos para realizar el análisis probabilístico del test, confirmará que la supremacía del test de Jacobi sobre el TFP es aparente: Si n pasa el test de Rabin-Miller respecto a una cierta base, entonces también pasa el test de Jacobi respecto a dicha base. Además, si n es compuesto, sólo pasará el test de Rabin-Miller respecto a lo sumo el 25% se las bases.

Análisis de Probabilidad del test: si n pasa el TPF con respecto a una base, la probabilidad que n sea compuesto es a lo sumo 0,25 si n pasa el TPF con respecto a otra base (o sea dos bases), la probabilidad que n sea compuesto es a lo sumo el cuadrado de 0,25; si n pasa el TPF con respecto a k bases, la probabilidad que n sea compuesto es a lo sumo la potencia k-esima 0,25. Probabilidad que parece ser bastante conservadora; ya que está planteada la siguiente conjetura: si n es compuesto, entonces no pasa el TFP respecto a alguna base menor que $2ln^2n$; y que de ser así reduciría enormemente la cantidad de pruebas a efectuar.

3. Conclusiones y Trabajos Futuros:

Los tests probabilísticos están basados en la idea de relajar la corrección de la prueba para conseguir un comportamiento de respuesta polinomial o subpolinomial De los tres tests probabilísticos aquí presentados, el mejor desde el punto de vista técnico y práctico es el de Miller-Rabin. El test SS es computacionalmente peor y más difícil de implementar ya que hay que calcular el símbolo de Jacobi. Por otra parte ambos tienen la ventaja frente al de Fermat de que podemos aumentar la confianza de la primalidad con un valor de k (cantidad de rondas) arbitrariamente alto (Fermat tiene el límite definido por los números de Carmichael).

Se indagará a futuro sobre las pruebas que en este trabajo no se han abordado, debido a que el tema es de vigencia con fuerte volatilidad.

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

MENEZES, A.; VAN OORSCHOT, P.; VANSTONE, S. (1996); *Handbook of Applied Cryptography*; CRC Press

MORA, W. (2014); *Introducción a la Teoría de Números*; Revista digital Matemática, Educación e Internet; https://tecdigital.tec.ac.cr/revistamatematica [Consulta 15/04/2018].

SCOLNIK, H. (2014); *Qué es la Seguridad Informática*; Argentina, Paidós