ALGORITMOS PARA PRUEBAS DE PRIMALIDAD

RAÚL MARTINES ZOCON[1], LOLO ORTIZ CESPEDES, JORGE HORNA MERCEDES Y AZUCENA ZAVALETA QUIPUSCOA.

Resumen. En este artículo se discuten algoritmos determinísticos y probabilísticos para la determinación de la primalidad de un número lo que es de suma utilidad en procedimientos criptográficos.

Key words. Criptografía, números primos, algoritmos de primalidad, teoría de números computacional.

1. **Introducción.** En la actualidad tanto en el sector público como en el sector privado se intercambia una cantidad enorme de datos a través de un canal, por ejemplo, la red Internet. Algunos de estos deben ser protegidos contra lectores ilegales, es por ello la necesidad de desarrollar procedimientos criptográficos para proteger la información.

   De este problema se ocupa la criptografía, la cual a pesar de ser antigua, es recién en el año 1949,en que se logra una formulación clara, sistemática y concreta de los conceptos involucrados con el artículo de C.E. Shannon titulado "Communication theory of secrecy systems" [7].

   Para números enteros grandes, en general, no es posible calcular en un tiempo justificable su descomposición en factores primos [3]. La factorización de un número $n = pq$, donde p y q son números primos y n tiene una longitud de 2048 bits, no es realizable en un tiempo aceptable. Entonces, la multiplicación de números primos grandes se puede ver como una función de una via.

   Este hecho es el fundamento del procedimiento criptográfico RSA.

[1]Departamento de Matemáticas, Universidad Nacional de Trujillo (rnmz@yahoo.com)

En el año 1978, Rivest, Shamir y Adleman presentaron lo que hoy se conoce como procedimiento criptográfico RSA[6], cuya seguridad reside en la dificultad para factorizar.

El procedimiento criptográfico RSA necesita el conocimiento de números primos grandes, siendo este el problema que es el objeto de estudio del presente artículo.

2. Algoritmos para pruebas de primalidad.

Existen muchos procedimientos para probar si un número natural dado n es primo o no.

Empezamos con la caracterización de números primos dada por el teorema de Wilson.

Teorema (Wilson)

Un número natural n es un número primo si y sólo si $(n-1)! \equiv -1 \mod n$

Demostración.

Supongamos que n es un número primo. La expresión $(n-1)!$ es el producto de todos los elementos del grupo $\mathbb{Z}_n^*$. En este producto, con cada $a \in \mathbb{Z}_n^*$, aparece $a^{-1} \in \mathbb{Z}_n^*$ y podemos juntar las parejas $aa^{-1} = 1$, con excepción de los $a \in \mathbb{Z}_n^*$ para los cuales se verifica que $a^2 = 1$. Por otro lado, la ecuación $x^2 = 1$ tiene en $\mathbb{Z}_n^*$ solamente las soluciones ± 1 y se tiene así la conclusión.

Recíprocamente, supongamos que n no es un número primo y que que admite un divisor $1 < q < n$. Entonces $(n-1)!$ también es divisible por q, por lo tanto, no es primo relativo con n. Pero -1 es primo relativo con n, lo que es una contradicción.

Esta caracterización requiere el cálculo de $(n-1)! \mod n$ que para números grandes no se puede realizar. Los algoritmos tienen un tiempo de ejecución exponencial, de modo que el cálculo es muy grande.

En el año 2002 Agrawal, Kayal y Saxena [2] han presentado un algoritmo con tiempo de ejecución polinomial, el cual determina si un número natural n es primo o no. Este algoritmo en la actualidad es denominado algoritmo AKS.

Diferentes investigadores han logrado mejoramientos del tiempo de ejecución [4], obteniendo tiempos de orden $O((\ln n)^{6+\varepsilon})$ con $\varepsilon > 0$ arbitrario, no obstante todos son hasta el momento impracticables para n suficientemente grande.

El AKS es el único algoritmo con tiempo de ejecución polinomial que puede determinar si un número natural n dado es un número primo o no.

Tanto la prueba de primalidad usando el teorema de Wilson como la del algoritmo AKS son determinísticas, es decir, uno puede decidir de manera efectiva, si n es un número primo.

Ninguno de los procedimientos determinísticos conocidos, son practicables para n grande. En lugar de estas se recurre a pruebas probabilísticas de primalidad, las cuales son rápidas, pero sólo nos dicen que "n" con alguna probabilidad ε es un número primo.

Test de Fermat

Dado $n \in \mathbb{N}$, verifique para $2 \leq a < n$, con $mcd(a, n) = 1$ si $a^{n-1} \equiv 1 \mod n$.

Observaciones sobre el Test de Fermat

Sea $n \in \mathbb{N}$:

1. Si $a^{n-1} \not\equiv 1 \mod n$, entonces con certeza n no es un número primo.
2. Puede suceder que $a^{n-1} \equiv 1 \mod n$, para todo a con $mcd(a, n) = 1$ y sin embargo, n no es un número primo. Tales números son llamados números de Carmichael [1].
3. En 1994 Alford, Granville y Pommerence [1] demostraron que existe un nú-

mero infinito de números de Carmichael. En consecuencia, tenemos que para infinitos números naturales $n \in \mathbb{N}$ el test de Fermat no puede determinar si n es un número primo o no.

Definición

Sea n un número impar y $n-1 = 2^s t$ con $2 \not| \, t$. Llamaremos a $a \in \{2, \ldots, n-1\}$ un testigo para la composición de n si $a^t \not\equiv 1 \mod n$ y $a^{2^r t} \not\equiv -1 \mod n$ para $0 \leq r < s$.

Test de Miller- Rabin

Supóngase que se desea determinar si un número $n \in \mathbb{N}$ impar grande dado es un número primo o compuesto.

1. Elija de manera arbitraria e independiente k números a tal que $2 \leq a \leq n-1$.
2. Determine con el algoritmo de Euclides $mcd(a, n)$. Si $mcd(a, n) \neq 1$ entonces n es compuesto.
3. Pruebe si bajo el a elegido se encuentra un testigo para la composición. Con el primer encuentro finaliza el algoritmo y n no es un número primo.

   Si no es posible encontrar tal número a entonces el algoritmo termina con fallido.

Observaciones sobre el Test de Miller - Rabin

Si el test de Miller - Rabin finaliza con fallido entonces n tiene la apariencia de un número primo, pero no necesariamente lo es. La probabilidad de que para un número compuesto "n" el test de Miller - Rabin termine con fallido es menor que $(\frac{1}{4})^k$.

Si se escoge k muy grande, entonces la probabilidad de que n sea un número primo es alta, sobre la base que el test de Miller - Rabin termine con fallido.

Un test de primalidad probabilístico menos efectivo que el de Miller - Rabin es el de Solovay - Strassen, el cual se fundamenta en el teorema de Euler.

Teorema (Euler)

Sea p un número primo impar. Entonces para todo $a \in \mathbb{Z}$

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \quad \text{mód } p$$

Definición.

Sea $n \in \mathbb{N}$ un número impar dado. Llamaremos $a \in \{2, \ldots, n-1\}$ un testigo para la composición de n si se verifica que

$$a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{p}\right) \quad \text{mód } n$$

donde $(\frac{a}{n})$ denota el símbolo de Jacobi.

Ejemplo.

Sea p un número primo impar

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & , \quad p \equiv \pm 1 \quad \text{mód } 8 \\ -1 & , \quad p \equiv \pm 3 \quad \text{mód } 8 \end{cases}$$

Solución.

Consideremos las siguientes $\frac{p-1}{2}$ congruencias

$$p-1 \equiv 1(-1)^1 \quad \text{mód } p$$

$$p-2 \equiv 2(-1)^2 \quad \text{mód } p$$

$$p-3 \equiv 3(-1)^3 \quad \text{mód } p$$

$$\vdots$$

$$p - \frac{p-1}{2} \equiv \frac{p-1}{2}(-1)^{\frac{p-1}{2}} \quad \text{mód } p$$

$$\frac{p-1}{2} \equiv \frac{p-1}{2}(-1)^{\frac{p-1}{2}} \quad \text{mód } p$$

multiplicando miembro a miembro estas congruencias, se obtiene

$$2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!(-1)^{\frac{p^2-1}{8}} \quad \text{mód } p$$

Dado que $(\frac{p-1}{2})! \not\equiv 0 \mod p$, a partir de estas congruencias obtenemos que

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \quad \text{mód } p$$

Utilizando el teorema de Euler se tiene que $2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \mod p$ y como cada uno de estos miembros es 1 ó -1 se verifica la igualdad de dichos miembros dado que $p > 2$.

Test de Solovay - Strassen

Sea $n \in \mathbb{N}$ impar dado y $k \in \mathbb{N}$.

Escojase de manera arbitraria e independiente k números $a \in \{2, \ldots, n-1\}$ con $mcd(a, n) = 1$ hasta que se encuentre (si es posible) un testigo para la composición de n.

Si tal número existe entonces n es compuesto. De otra manera, finaliza el algoritmo con output fallido.

Observaciones sobre el Test de Solovay - Strassen

Como en el Test de Miller - Rabin, uno puede demostrar otra vez que un testigo para la composición existe si n es compuesto.

La probabilidad de que para un número compuesto n el Test de Solovay - Strassen termine con fallido es menor que $(\frac{1}{2})^k$.

Por lo tanto, si k es grande entonces la probabilidad de que n sea un número primo es alta, si el Test de Solovay - Strassen termina con fallido.

CONCLUSIONES

1. El problema de la primalidad consiste en averiguar si un número es primo o compuesto. Existen métodos muy antiguos para determinar la primalidad de un nú-

mero tales como la Criba de Eratóstenes (2000 AC), pero el cual es ineficaz para el análisis de un número n grande.

2. Fermat, en el año 1636 presento su celebre " Pequeño Teorema de Fermat " en el cual determina una característica que cumplen todos los números primos.

3. El teorema afirma que cuando n es un número primo y a un número coprimo de n se cumple $a^n \equiv a \mod n$.

4. En el año 1770,John Wilson encontró una caracterización de números primos que es de utilidad en el desarrollo teórico,pero que en la práctica no es utilizada frecuentemente como prueba de primalidad ya que para calcular $(n-1)! \mod n$ para un número n grande se tiene un costo computacional elevado.

5. Las pruebas de primalidad de Wilson y el algoritmo AKS son determinísticas,es decir, uno puede decidir de manera efectiva si un número es primo.

6. Ninguno de los procesos deterministicos conocidos son prácticos para n grande, por ello es que se usan pruebas probabilísticas de primalidad las cuales tiene la ventaja de ser rápidas, pero sólo nos dicen que n con alguna probabilidad ε es un número primo.

7. El test de Fermat es un algoritmo probabilístico que tiene la fortaleza de que tras un número pequeño de repeticiones la probabilidad de que un número compuesto pase como número primo es muy pequeña,pero adolece de un conocido problema:Los números de Carmichael. Los números de Carmichael pasan la condición de Fermat para todos los posibles valores de a, esto significa que si nuestro candidato a número primo es un número de Carmichael, no importa cuantas veces pasemos el test de Fermat, el resultado siempre será negativo y en consecuencia el resultado del Test

seria un falso primo positivo.

8. El test de Miller Rabin es un algoritmo probabilístico para determinar si un número dado es primo. Se tiene las siguientes posibilidades para un entero impar n sometido al test de Miller- Rabin. Si n es primo entonces n pasara los k test y será declarado primo. Si n es compuesto, la probabilidad de que el algoritmo termine con n declarado primo es menor o igual que $\frac{1}{4^k}$.

9. Finalizamos el presente artículo con el Test de Solovay - Strassen el cual también es un algoritmo probabilístico de utilidad en la determinación de la primalidad de un número.

REFERENCIAS

[1] **ALFORD** *There are infinitely many Carmichael numbers*, Annals of Mathematics 140, 703-722, Princeton ,1994.

[2] **AGRAWAL M.** *Primes is in P*, Annals of Mathematics 160, 781-793, Princeton , 2002.

[3] **DIFFIE W.** *New Directions in Cryptography*, IEEE Trans. Inform Theory 22, 644-654, New York , 1976.

[4] **KOBLITZ N.** *A course in Number Theory and Cryptography*, Springer-Verlag , Berlin , 1998.

[5] **LENSTRA, A.** *Computational Methods in public key Cryptography*, http://www.win.tue.nl/klenstra.

[6] **RIVEST, R.** *A Method for obtaining digital signatures and public key Cryptosystems*, Communications of the ACM, Vol 21 pp. 120-126 , New York , 1978.

[7] **SHANNON, C** *Communication theory of secrecy systems*, Bell Syst. Tech. J. 28, 656-715, New Jersey ,1949.