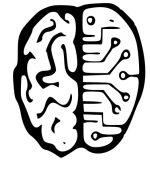
Preliminares matemáticos

Primalidad
Factorización

Universidad del País Vasco
Euskal Herriko Unibertsitatea

KISA



Primalidad

En Criptografía de clave pública se utilizan números primos grandes.

Asegurar de manera determinista que uno de tales números es primo supone comprobar que no es divisible por ninguno de los primos $2, 3, 5, 7, \ldots$ hasta el mayor entero primo menor o igual que $[\sqrt{n}]$ ($[x]$ es la parte entera de x), lo cual es computacionalmente imposible.

Se impone la necesidad de obtener números primos de manera probabilística. Consiste en determinar que un número entero es primo con una cierta probabilidad, que puede ser tan grande como queramos.

Para ello se desarrollan los llamados *Tests de primalidad*.

Los siguientes resultados indican que tenemos "abundancia" de números primos y nos dan una idea de cómo están distribuidos.

Teorema (Euclides)

Dado un número p primo, siempre existe otro mayor.

Proposición

1. *Dado un entero n, el número de primos menores que n es aproximadamente* $\frac{n}{\ln n}$.
2. *Hay aproximadamente* 10^{151} *primos de* 512 *bits.*

Test de primalidad de Miller-Rabin

Se basa en el siguiente

Teorema

Sea n un número entero impar y sea $n-1 = 2^s t$ con t impar.

1. *Si n es primo, entonces para cualquier entero a tal que $\mathrm{mcd}(a, n) = 1$ se cumple que*

$$\left.\begin{array}{l} a^t \equiv 1 \mod n \\ o \\ a^{2^j t} \equiv n-1 \mod n \text{ para algún } j,\ 0 \leq j < s. \end{array}\right\} \quad (1)$$

2. *Si n es compuesto, entonces la condición (1) se satisface como máximo para $\frac{1}{4}$ de los enteros a tales que $0 < a < n$.*

Observación: $a^{2t} = (a^t)^2, \quad a^{2^2 t} = (a^{2t})^2, \quad a^{2^3 t} = (a^{2^2 t})^2, \quad \ldots.$

Ejemplo

- $n = 49, \quad n - 1 = 2^4 \cdot 3.$

$$2^3 \equiv 8 \not\equiv \pm 1 \mod 49, \quad 8^2 \equiv 15 \not\equiv -1 \mod 49,$$
$$15^2 \equiv 29 \not\equiv -1 \mod 49, \quad 29^2 \equiv 8 \not\equiv -1 \mod 49.$$

Podemos asegurar que 49 es compuesto.

- $n = 41, \quad n - 1 = 2^3 \cdot 5.$

$$3^5 \equiv 38 \not\equiv \pm 1 \mod 41, \quad 38^2 \equiv 9 \not\equiv -1 \mod 41,$$
$$9^2 \equiv 40 \equiv -1 \mod 41.$$

$p(n \text{ es compuesto }) < \frac{1}{4}$.

Test:

$$\left.\begin{array}{l} a^t \not\equiv 1 \mod n \\ \text{y} \\ a^{2^j t} \not\equiv n-1 \mod n \text{ para todo } j,\ 0 \le j < s \end{array}\right\} \Rightarrow n \text{ es compuesto.}$$

$$\left.\begin{array}{l} a^t \equiv 1 \mod n \\ \text{o} \\ \exists j,\ 0 \le j < s,\ \text{t. q. } a^{2^j t} \equiv n-1 \mod n \end{array}\right\} \Rightarrow p(n \text{ es compuesto }) < \frac{1}{4}.$$

Pasando el test una vez, $p(n \text{ es compuesto }) < 1/4$.

Si pasamos el test dos veces, $p(n \text{ es compuesto }) < 1/4^2$.

Si pasamos el test k veces, $p(n \text{ es compuesto }) < 1/4^k$.

Consecuencia: Si n pasa el test k veces, entonces

$$p(n \text{ es primo}) > 1 - 4^{-k}.$$

Procedimiento de generación de números primos

1. Generar un número aleatorio p de n bits.
2. Poner a uno el bit más significativo (garantizamos que el número es de n bits) y el menos significativo (garantizamos que el número sea impar).
3. Comprobar que no es divisible por primos pequeños: 3,5,7,11, ... (hasta 256).
4. Efectuar un test de primalidad varias veces.

Observación: El paso 3 es opcional, pero
el no ser divisible por $3, 5, 7$ elimina $54\,\%$ de los números impares,
el no ser divisible por los enteros menores que 100, elimina $76\,\%$,
el no ser divisible por los enteros menores que 256, elimina $80\,\%$.

Factorización

El problema de la factorización de enteros:

Dado un entero positivo n, hallar su descomposición en factores primos

$$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$$

en donde $p_1, p_2, \dots, p_r$ *son primos distintos y* $e_i \geq 1, i = 1, \dots, r$.

Observaciones:

- Es uno de los problemas de matemáticas que se considera *intratable* computacionalmente. *No se conoce ningún algoritmo que permita factorizar un entero en tiempo polinomial.*
- En realidad, su complejidad computacional se desconoce.

- Un sencillo algoritmo de factorización consiste en probar si el número dado n es divisible por alguno de los primos menores o iguales que $[\sqrt{n}]$. Para enteros grandes, este cálculo no se puede llevar a cabo.
- El hecho de que se considere un problema intratable permite desarrollar en base a él un criptosistema de clave pública: el RSA.
- El RSA se basa en un caso particular del problema de factorización.

El problema RSA

Dado un entero positivo n del que se sabe que es producto de dos números primos p y q, hallar sus factores.

- Existen numerosos algoritmos que tratan de encontrar los factores de un número entero compuesto para ciertos tipos de enteros.
- Vamos a ver dos de ellos que tratan de resolver el problema RSA.
    1. El método método rho de Pollard.
    2. El método de factorización de Fermat.

Método rho de Pollard

Permite encontrar un factor pequeño de un entero compuesto.

El método consiste en lo siguiente:

- Se elige un polinomio $p(x)$ con coeficientes en $\mathbb{Z}_n$.
- Se elige un entero x_0 (por ejemplo $x_0 = 1$ ó $x_0 = 2$).
- Se calcula la sucesión $x_0, x_1, \ldots,$ con

$$x_i = p(x_{i-1}) \mod n, \quad i = 1, \ldots.$$

- Se hacen comparaciones entre los valores calculados hasta encontrar $x_j,\ x_k$ tales que para algún divisor propio d de n,

$$x_k \equiv x_j \mod d \quad \text{y} \quad x_k \not\equiv x_j \mod n.$$

Es decir, tales que

$$d \mid n, \quad d \mid x_k - x_j, \quad n \not| x_k - x_j,$$

- Una vez obtenidos los números $x_j,\ x_k$ cumpliendo la anterior condición, se tiene que $\mathrm{mcd}(x_k - x_j, n)$ es un divisor propio de n.

Observación: Los polinomios más comunes utilizados son de la forma $p(x) = x^2 + c$, con $c \neq 0, -2$.

Ejemplo

Para factorizar $n = 91$, elegimos $p(x) = x^2 + 1$ y $x_0 = 1$.

Construimos la sucesión: $x_1 = 2,\ x_2 = 5,\ x_3 = 26,\ x_4 = 40, \ldots$.

Calculamos $\mathrm{mcd}(x_k - x_j, n)$, $k, j = 0, 1, 2, \ldots$:

$$\mathrm{mcd}(x_1 - x_0, n) = \mathrm{mcd}(1, 91) = 1, \quad \mathrm{mcd}(x_2 - x_0, n) = \mathrm{mcd}(4, 91) = 1,$$

$$\mathrm{mcd}(x_2 - x_1, n) = \mathrm{mcd}(3, 91) = 1, \quad \ldots,$$

$$\mathrm{mcd}(x_3 - x_2, n) = \mathrm{mcd}(21, 91) = 7.$$

Así,

$$91 = 7 \cdot 13.$$

Método de factorización de Fermat

El método se basa en el siguiente

Teorema

Sea n entero positivo impar. Entonces existe una correspondencia uno a uno entre una factorización $n = ab$, donde $a \geq b > 0$ y una representación de n de la forma $n = t^2 - s^2$ donde s y t son enteros no negativos.

La correspondencia es:

- Dados a, b, entonces

$$t = \frac{a+b}{2}, \quad s = \frac{a-b}{2}.$$

- Dados t, s, entonces

$$a = t + s, \quad b = t - s.$$

Si $n = ab$, con a, b próximos, entonces $s = \frac{a-b}{2}$ es pequeño y $t = \frac{a+b}{2}$ es poco mayor que $\sqrt{n}$.

En ese caso, podemos obtener a y b probando con todos los valores de t empezando con $t = [\sqrt{n}] + 1$, hasta que encontremos uno para el que $t^2 - n = s^2$ sea un cuadrado perfecto.

Ejemplo

Si queremos factorizar $n = 200819$.

Se tiene $\sqrt{200819} = 448.1283\ldots$. Empezamos con $t = 449$.

$$t = 449, \quad 449^2 - n = 782, \text{ no cuadrado perfecto.}$$

$$t = 450, \quad 450^2 - n = 1681, \ 1681 = 41^2, \text{ cuadrado perfecto.}$$

Entonces

$$200819 = 450^2 - 41^2 = (450 + 41)(450 - 41) = 491{\cdot}409.$$

Fin de la sección