Enrique R. Aznar García
eaznar@ugr.es

EL MÉTODO ρ DE POLARD

Dado un número entero n que queremos factorizar, y dada una función $f : \mathbb{Z}_n \to \mathbb{Z}_n$, que suponemos se comporta como una variable aleatoria distribuida uniformemente, definimos recursivamente
$x_i = f(x_{i-1}),\ \forall i \in \mathbb{N}$

Si $1 \neq p \in \mathbb{N}$ es un divisor de n, como $\mathbb{Z}_p$ es finito, los sucesivos x_i no pueden ser distintos módulo p y la primera vez que se repiten, nos da dos naturales $k, 0 \neq l$ tal que

$$x_k \equiv x_{k+l} \pmod{n} \Rightarrow p \mid \gcd(x_k - x_{k+l}, n)$$

Observamos que $x_k = x_{k+jl} \in \mathbb{Z}_p$ para todo $j \in \mathbb{N}$.
O sea, que los x_i se repiten cíclicamente con periodo l a partir del índice k (recuerda la forma de la letra griega ρ).

El método de Pollard (1971) consiste en encontrar la primera colisión, el correspondiente mcd y el posible factor de n. El inconveniente es guardar los sucesivos x_i que lo harían ineficaz. Pollard propuso guardar sucesivamente sólo dos de ellos a una determinada distancia y computar los mcd sucesivos hasta encontrar un factor.

A continuación veremos otra estrategia debida a Lloyd.

EL MÉTODO DE DETECCIÓN DE FLOYD

Para encontrar una repetición y calcular el mcd correspondiente y el posible factor, no es necesario guardar todos los valores de los sucesivos x_i.

Sea $y_0 = x_0 \in \mathbb{Z}_n$ elegido como queramos. Definimos sucesivamente, $y_i = f(f(x_i))$, entonces por inducción

$$y_i = x_{2i} \Rightarrow y_{i+1} = f(f(y_i)) = f(f(x_{2i})) = f(x_{2i+1}) = x_{2i+2} = x_{2(i+1)}$$

Entonces, tenemos que
$$x_i = y_i \in \mathbb{Z}_p \Leftrightarrow k \leq i \text{ y } l \text{ divide a } 2i - i = i$$

Como el periodo es l y se repite a partir de k. El primer i que cumple esto será un elemento de $\{k, \ldots, k + l\}$ y necesitaremos como mucho $k + l$ pasos para llegar a esta situación (si existe un divisor p).
Observamos, que si p es pequeño, también k y l lo son y la colisión se produce pronto.

Esto conduce al siguiente algoritmo tipo Las Vegas:

Elegimos x_0 y el número, $t \in \mathbb{N}$, de pasos a dar.

$y = x_0$; $i = 0$;

While $i < t$,

$$i = i + 1;\ x = f(x);\ y = f(f(y));\ g = \gcd(x - y, n);\ \text{if}(1 < g < n) \text{ Return } g$$

Return "No hay divisores con t iteraciones"

EJEMPLO

Para $n = 7429$ y usando como función aleatoria $f(x) = x^2 + 1$, encontramos en 4 pasos el divisor 19

Paso	x	y	mcd
0	1	1	-
1	2	5	1
2	5	677	1
3	26	2957	1
4	677	6890	19

Como $7429 = 19 * 391$, podemos volver a correr el ρ-Pollard para el cofactor encontrado

Paso	x	y	mcd
0	1	1	-
1	2	5	1
2	26	220	1
3	286	243	1
4	78	82	1
5	220	220	391
6	308	243	1
7	243	82	23

Finalmente, obtenemos las descomposiciones

$$391 = 23 * 17 \Rightarrow 7429 = 19 * 391 = 23 * 17 * 19$$

Enrique R. Aznar García
eaznar@ugr.es