Pollard (p-1)

Este documento no pretende ser un curso exhaustivo, en el mejor de los casos, únicamente puede considerarse como un conjunto de notas complementarias en alguna asignatura. Por supuesto, todo documento es susceptible de mejora, cualquier sugerencia o comunicación de error u omisión será bienvenida.

Algoritmo

El algoritmo de Pollard $p-1$ considera el caso especial en que uno de los factores p es tal que los factores de $p-1$ son *pequeños*. El algoritmo considera que es posible encontrar un valor L tal que sea un múltiplo de $p-1$ (obviamente sin conocer p). Disponiendo de este valor obtenemos, que para todo a en $\mathbb{Z}_n$:

$$a^L = a^{k(p-1)},\ k \in \mathbb{Z}$$

porque $p-1|L$ (esto es, L es un múltipilo de $p-1$). A partir de este punto, aplicando el Teorema de Fermat:

$$a^{(p-1)^k} \equiv 1^k \pmod{p}$$

y por lo tanto, como a^L y 1 son congruentes módulo p, aplicando la definición de congruencia módulo obtenemos que $a^L - 1 = kp$ para algún k entero y por lo tanto que $p|a^L - 1$, por lo que el $mcd(a^L - 1, n)$ puede devolver un factor de n o bien n en el caso particular que L sea múltiplo de ambos factores de n.

Existen distintas formas de abordar la construcción de L. Una forma es calcular el factorial de valores sucesivos. La función factorial posee múltiples divisores y puede ser calculada eficientemente de forma incremental. Es importante tener en cuenta que en este contexto es suficiente considerar el módulo respecto n, evitando los problemas de rápido crecimiento de la función factorial.

Los siguientes ejemplos muestran el comportamiento del algoritmo de Pollard $p-1$.

Ejemplo 1. *Intentamos la factorización del número* 999919 *mediante el algoritmo de Pollard* $p-1$. *Consideramos un valor inicial de* $A = 3$.

Algoritmo 1 Algoritmo de Pollard $p-1$

Entrada: Un número entero positivo compuesto n
Salida: Un factor de n (o bien n)
Método
Escoger A aleatorio tal que $2 \leq A \leq n-1$
Si $1 < mcd(A,n) < n$ **entonces return** $mcd(A,n)$
$k = 2$
Mientras True **hacer**
$A = A^k$ mód n
$d = mcd(A-1,n)$
Si $1 < d < n$ **entonces return** d
Si $d == n$ **entonces return** $False$
$k++$
FinMientras
FinMétodo.

k	$A^{k!}$ mód n	$mcd(A^{k!}-1,n)$
2	9	1
3	729	1
4	415093	1
5	455994	1
6	227884	1
7	724463	1009

Por lo que un factor de n es 1009. *Puede comprobarse que el número de iteraciones viene determinado por la descomposición de* $1008 = 2^4 \cdot 3^2 \cdot 7$.

Ejemplo 2. *La siguiente tabla muestra la ejecución del algoritmo de Pollard $p-1$ en el proceso de factorización de* 328747. *Consideramos que A se inicializa con el valor* 3.

k	$A^{k!}$ mód n	$mcd(A^{k!}-1,n)$
2	9	1
3	729	1
4	30058	1
5	319445	1
6	254537	1
7	261467	547

Por lo que un factor de n es 547 *siendo el otro factor* 601. *Puede comprobarse que el*

número de iteraciones está acotado por la descomposición de uno de los factores de n. En efecto, $600 = 2^3 \cdot 3 \cdot 5^2$.

Ejercicios

Ejercicio 1.

Utilice el algoritmo de Pollard $p-1$ para obtener los factores primos de $n = 677489$.

Ejercicio 2.

Utilice el algoritmo de Pollard $p-1$ para obtener los factores primos de $n = 443713$.

Ejercicio 3.

Utilice el algoritmo de Pollard $p-1$ para obtener los factores primos de $n = 484391$. *Analice el resultado obtenido.*

Ejercicio 4.

Utilice el algoritmo de Pollard $p-1$ para obtener los factores primos de $n = 543577$. *Analice el resultado obtenido.*
