POLLARD-RHO

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

En la factorización de un entero n producto de dos factores desconocidos p y q, el algoritmo de Pollard-rho se basa en la búsqueda de dos valores a y b congruentes módulo uno de los factores de n.

Algoritmo 0.1 Algoritmo de Pollard-rho

Entrada: Un número entero positivo compuesto n
Salida: Un factor de n
Método
$A = B = random(2, n-1)$ // Habitualmente $A = B = 2$
Mientras True **hacer**
$A = A^2 + 1$ mód n
$B = B^2 + 1$ mód n
$B = B^2 + 1$ mód n
$p = mcd(A - B, n)$
Si $1 < p < n$ **entonces return** p
Si $p == n$ **entonces return** n
FinMientras
FinMétodo.

El algoritmo considera una función pseudoaleatoria que recorre el espacio de posibilidades con dos velocidades distintas. La justificación de este diseño puede abordarse de distintas formas. La que consideramos aquí tiene en cuenta que una secuencia de valores pseudoaleatorios módulo n, dado que el conjunto $\mathbb{Z}_n$ es finito y que cada número en la secuencia depende exclusivamente del anterior (y de la función pseudoaleatoria utilizada) llega un momento en que la secuencia se repite. Gráficamente, la Figura 1 muestra este comportamiento. La semejanza de la representación gráfica de este hecho con la letra griega ρ da nombre al algoritmo.

Dado $n = pq$, si consideramos $a_1, a_2, \ldots$ y $b_1, b_2, \ldots$ las dos secuencias pseudoaleatorias que, de acuerdo con el algoritmo, recorren $\mathbb{Z}_n$, hay que considerar que, en cierto modo, reducir módulo n reduce parcialmente módulo p y también módulo q, por lo que es factible encontrar valores a_i y b_i que sean congruentes módulo p o módulo q.

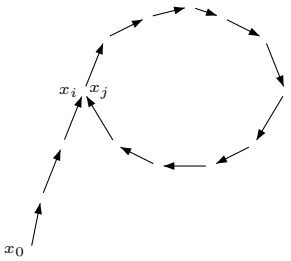

Figura 1: Una función pseudoaleatoria en $\mathbb{Z}_n$ que considera como único parámetro el valor anterior en la secuencia encuentra un punto a partir del cual la secuencia se repite.

Ejemplo 1. *Intentamos la factorización del número* 9077 *que resulta del producto de* $p = 29$ *y* $q = 313$*, mediante el algoritmo de Pollard-rho. La siguiente tabla muestra información relevante de los valores obtenidos en cada iteración:*

a	b	a mód p	b mód p	a mód q	b mód q
2	2				
5	26	5	26	5	26
26	4480	26	14	26	98
677	6475	10	8	51	215
4480	4284	14	21	98	215
1154	4284	23	21	215	215

Hay que recordar que las secuencias de a_i *y* b_i *lo son de valores en* $\mathbb{Z}_n$*, por lo que, en cierto modo, aunque estos valores no se limitan a los conjuntos* $\mathbb{Z}_p$ *y* $\mathbb{Z}_q$*, sí puede considerarse que existe cierta reducción teniendo en cuenta que* $n = p \cdot q$*.*

En la tabla anterior se muestra como eventualmente se puede alcanzar un par de valores $a = 1154$ *y* $b = 4284$ *tales que son congruentes módulo uno de los factores de* n*.*

Si se encuentran dos valores a y b congruentes con un factor p de n, entonces (por la definición de congruencia módulo p):

$$a - b = kp,\ k \in \mathbb{Z}$$

ya que $n = p \cdot q$, en la muchas ocasiones podremos obtener p calculando $mcd(a - b, n)$.

En ocasiones puede suceder que los valores de a y b sean congruentes módulo p y también módulo q, por lo que el $mcd(a - b, n)$ daría como resultado n, fallando el proceso de factorización. En este caso, una solución es considerar un polinómio del tipo $f(x) = x^2 + c$ mód n, con $c \notin \{0, -2\}$, en lugar del polinomio $f(x) = x^2 + 1$ mód n utilizado en el algoritmo inicial.

El algoritmo rho de Pollard es un heurístico por lo que no siempre proporciona un resultado a la factorización, sin embargo tiene muy buen comportamiento en caso que n posea factores pequeños. Asumiendo que la función pseudoaleatoria se comporta como tal, con probabilidad 0.5, bastan $\sqrt{p}$ iteraciones para encontrar dos números congruentes módulo p, esto es, el tiempo esperado para que el algoritmo de Pollard-rho encuentre un factor de n es $\mathcal{O}(\sqrt{p})$, o bien de aproximadamente $\mathcal{O}(n^{1/4})$.

Ejemplo 2. *Podemos resumir la factorización del número* 95939 *mediante el algoritmo de Pollard-rho con la siguiente tabla:*

n	A	B	$mcd(A\text{-}B,n)$
95939	2	2	
	5	26	1
	26	74574	1
	677	37619	1
	74574	66084	1
	81403	88248	1
	37619	13288	1
	88912	81944	1
	66084	46975	197

Por lo que uno de los factores de n es 197

Ejercicios

Ejercicio 1.

Utilice el algoritmo de Pollard-rho para obtener los factores primos de $n = 502991$.

Solución:

Considerando inicialmente $a = b = 2$*, después de cinco iteraciones se encuentra el factor* $p = 313$.

Ejercicio 2.

Utilice el algoritmo de Pollard-rho para obtener los factores primos de $n = 609053$.

Solución:

Considerando inicialmente $a = b = 2$, después de nueve iteraciones se encuentra un factor.

Ejercicio 3.

Utilice el algoritmo de Pollard-rho para obtener los factores primos de $n = 4394179$.

Solución:

Considerando inicialmente $a = b = 2$, después de diez iteraciones se encuentra un factor.
