FERMAT

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, muchos de los algoritmos de factorización propuestos consideran la búsqueda de valores a y b cuyos cuadrados son congruentes módulo n. En caso de encontrar estos valores se tiene que:

$$\begin{aligned} a^2 &\equiv b^2 \pmod{n} \\ a^2 - b^2 &= kn,\ k \in \mathbb{Z} \\ (a+b)(a-b) &= kn \end{aligned}$$

por lo que, si $n = pq$ entonces uno de los factores puede obtenerse como resultado del $mcd(a-b, n)$. El algoritmo de Fermat es uno de los que se basan en este resultado. Este algoritmo es muy eficiente en el caso particular de que ambos factores son muy cercanos.

Algoritmo 1 Algoritmo de factorización de Fermat

Entrada: Un número entero positivo compuesto n
Salida: p y q tales que $n = p \cdot q$
  Método
  $A = \lceil \sqrt{n} \rceil$
  $B = A^2 - n$
  Mientras B no sea un cuadrado perfecto **hacer**
    $A++$
    $B = A^2 - n$
  FinMientras
  Devolver $\langle A - \sqrt{B}, A + \sqrt{B} \rangle$
  FinMétodo.

Si los factores son próximos entre si, la raíz de n es una aproximación de ellos. Por esto iniciar la búsqueda de los factores a partir de la raíz de n es un buen punto de partida.

El algoritmo inicializa A al valor por exceso de la raíz de n. El cuadrado A será un valor mayor que n, pero restando n obtenemos un valor equivalente y cercano a 0. La pregunta es si el valor obtenido tiene una raíz exacta. En caso de encontrarse el algoritmo dispone

de valores cuyos cuadrados son congruentes módulo n:

$$B = A^2 - n, \qquad \text{por lo que}$$
$$A^2 \equiv B \pmod{n}.$$

Obviamente, es fácil obtener la raíz de A^2. Si B es un cuadrado perfecto, entonces el algoritmo dispone de toda la información para factorizar n.

Ejemplo 1. *Podemos resumir la factorización del número* 40723 *mediante el algoritmo de Fermat con la siguiente tabla:*

n	A	B	$\sqrt{B}\sim$
40723			
	202	81	9

Una vez encontrados dos valores con cuadrados son congruentes módulo n, se obtienen los factores $202 + 9 = 211$ *y* $202 - 9 = 193$

Ejemplo 2. *Podemos resumir la factorización del número* 666917 *mediante el algoritmo de Fermat con la siguiente tabla:*

n	A	B	$\sqrt{B}\sim$
666917			
	817	572	23,91
	818	2207	46,97
	819	3844	62

Con lo que los factores de n son $p = 881$ y $q = 757$.

Ejemplo 3. *Podemos resumir la factorización del número* 377746339 *mediante el algoritmo de Fermat con la siguiente tabla:*

n	A	B	$\sqrt{B} \sim$
377746339			
	19436	11757	108,43
	19437	50630	225,011
	19438	89505	299,174
	19439	128382	358,304
	19440	167261	408,976
	19441	206142	454,029
	19442	245025	495

Una vez encontrados dos valores $a = 19442$ *y* $b = 495$ *cuyos cuadrados son congruentes módulo* n*, los valores* $(a+b) = 19937$ *y* $(a-b) = 18947$ *son los factores que buscábamos.*

Ejercicios

Ejercicio 1.

Utilice el algoritmo de Fermat para obtener los factores primos de $n = 2379967$*.*

Ejercicio 2.

Utilice el algoritmo de Fermat para obtener los factores primos de $n = 4377361$*.*

Ejercicio 3.

Utilice el algoritmo de Fermat para obtener los factores primos de $n = 4746943$*.*

Solución:

Después de diez iteraciones, el algoritmo devuelve el par de factores 1987 *y* 2389*.*
