Enrique R. Aznar García
eaznar@ugr.es

BUSCANDO UN ELEMENTO PRIMITIVO

El número $n = 27213647$ pasa el test Miller-Rabin y el de Solovay-Strassen para las bases $2, 3, 5, 7, 11$.
Queremos certificar su primalidad encontrándole un elemento primitivo.
Para eso necesitamos los factores primos de $n - 1 = 27213646 = 2 * 13606823$.

El cofactor impar $m = 13606823$ no pasa el test de primalidad de Fermat, ya que para la base $a = 2$, se tiene

$$2^{13606822} \equiv 3602703 \pmod{13606823}$$

Asi, la potencia $2^{m-1} \not\equiv 1 \pmod{m}$, m es un número compuesto y le podemos aplicar el método ρ de Pollard.

Usando la función $f(x) = x^2 + 1$ para iterar x, la variable y itera con la función $f(f(y)) = y^4 + 2y^2 + 2$. Calculando x, y módulo $m = 13606823$ y el mcd$(x - y, m)$, encontramos en 6 pasos el divisor 23

Paso	x	y	mcd
0	1	1	1
1	2	5	1
2	5	677	1
3	26	4255427	1
4	677	10477249	1
5	458330	9543242	1
6	4255427	3612623	23

Y obtenemos, la factorización $m = 13606823 = 23 * 591601$

ANÁLISIS DEL COFACTOR

Como el cofactor $m_1 = 591601$ pasa de nuevo los tests de Miller-Rabin y de Solovay-Strassen para distintas bases, sospechamos que es primo. Para poder certificar su primalidad encontrándole un elemento primitivo, necesitamos de nuevo los divisores primos de $m_1 - 1$, donde los primeros factores primos los hallamos a ojo:

$$m_1 - 1 = 591600 = 2^4 * 36975 = 2^4 * 5^2 * 1479 = 2^4 * 5^2 * 3 * 493$$

Como el último cofactor impar 493 no pasa el test de primalidad de Fermat, ya que para la base $a = 2$, se tiene

$$2^{492} \equiv 373 \pmod{493}$$

Asi, $m_2 = 493$ es un número compuesto y le podemos aplicar el método ρ de Pollard.

Usando la función $f(x) = x^2 + 1$ para iterar x, la variable y itera con la función $f(f(y)) = y^4 + 2y^2 + 2$. Calculando x, y módulo $m_2 = 493$ y el mcd$(x - y, m_2)$, encontramos en 6 pasos el divisor 17

Paso	x	y	mcd
0	1	1	1
1	2	5	1
2	5	184	1
3	26	458	1
4	184	413	1
5	333	65	1
6	458	152	17

Y obtenemos, la factorización, $493 = 17 * 29$ y por tanto $m_1 - 1 = 591600 = 2^4 * 5^2 * 3 * 17 * 29$.

OTRO ELEMENTO PRIMITIVO

Como ya conocemos todos los factores primos, $\{2,3,5,17,29\}$, de $m_1 - 1 = 591600$, iniciamos la búsqueda de un elemento primitivo para $m_1 = 591601$, sucesivamente probamos $2, 3, \ldots$ hasta encontrar que $a = 14$ es un elemento primitivo para m_1 porque $14^{591600} \equiv 1 \pmod{m_1}$,mientras que $14^{591600/p} \not\equiv 1 \pmod{m_1}$ para $p \in \{2,3,5,17,29\}$. O sea,

$$\begin{cases} 14^{m_1-1} \equiv 1 \pmod{m_1} \\ 14^{(m_1-1)/2} \equiv 591600 \pmod{m_1} \\ 14^{(m_1-1)/3} \equiv 231901 \pmod{m_1} \\ 14^{(m_1-1)/5} \equiv 134030 \pmod{m_1} \\ 14^{(m_1-1)/17} \equiv 391816 \pmod{m_1} \\ 14^{(m_1-1)/29} \equiv 555029 \pmod{m_1} \end{cases}$$

Lo anterior demuestra que 14 es un elemento primitivo para $m_1 = 591601$ y es un certificado de su primalidad.

UN ELEMENTO PRIMITIVO PARA 27213647

Como habíamos encontrado la factorización
$n-1=2*13606823=2*23*591601$

y hemos certificado que 591601 es primo, conocemos todos los factores primos, $\{2,23,591601\}$, de $n-1=27213646$. Ahora,podemos iniciar la búsqueda de un elemento primitivo para $n=27213647$ y el primer elemento encontrado es $a=5$ ya que se tienen las 4 congruencias

$$\begin{cases} 5^{n-1}\equiv 1 \pmod{n} \\ 5^{(n-1)/2}\equiv 27213646 \pmod{n} \\ 5^{(n-1)/23}\equiv 8258807 \pmod{n} \\ 5^{(n-1)/591601}\equiv 9374555 \pmod{n} \end{cases}$$

Lo anterior demuestra que 5 es un elemento primitivo para $n=27213647$ y es un certificado de su primalidad.

Enrique R. Aznar García
eaznar@ugr.es