Enrique R. Aznar García
eaznar@ugr.es

BUSCANDO UN LUCAS-CERTIFICADO

El número $n = 740580514804901$ pasa el test Miller-Rabin y el de Solovay-Strassen para las bases $2, 3, 5, 7, 11$.
Queremos certificar su primalidad encontrándole una s.L.
Para eso necesitamos los factores primos de
$n + 1 = 740580514804902 = 2 * 370290257402451 = 2 * 3 * 123430085800817$.

El cofactor $m = 123430085800817$ no pasa el test de primalidad de Fermat, ya que para la base $a = 2$, se tiene

$$2^{m-1} \equiv 78526559169539 \pmod{m}$$

Como 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 y el mcd$(x - y, m)$, encontramos en 6 pasos el divisor 17

Paso	x	y	mcd
0	1	1	1
1	2	5	1
2	5	677	1
3	26	210066388901	1
4	677	115039510878259	1
5	458330	66454599203495	1
6	210066388901	91841093998594	17

Y obtenemos, la factorización $m = 123430085800817 = 17 * 7260593282401$

ANÁLISIS DEL COFACTOR

El cofactor $m_1 = 7260593282401$ no pasa el test de Fermat, ya que para la base $a = 2$, se tiene

$$2^{m_1 - 1} \equiv 1956858885248 \pmod{m_1}$$

Como la potencia 2^{m_1-1} no da 1, m_1 es compuesto y le podemos aplicar el método ρ de Pollard.
Aquí ρ de Pollard es eficiente mientras que el método de factorización de Fermat no lo es (tarda demasiado).
Esta vez en 115 iteraciones del ρ de Pollard, se encuentra la factorización

$$m_1 = 7260593282401 = 4759 * 1525655239$$

y por tanto

$$n + 1 = 740580514804902 = 2 * 3 * 17 * 4759 * 1525655239$$

Como se comprueba que 4759 es primo (p. ej., mirando en una tabla), nos queda analizar el cofactor

$$m_2 = 1525655239$$

ANÁLISIS DEL SEGUNDO COFACTOR

$m_2 = 1525655239$ pasa el test Miller-Rabin y el de Solovay-Strassen para las bases $2, 3, 5, 7, 11$. Vamos a certificar su primalidad encontrándole una s.L.

Para eso, necesitamos factorizar $m_2 + 1 = 1525655240 = 2^3 * 5 * 38141381$ Pero el nuevo cofactor 38141381 no pasa el test de Fermat y lo factorizamos con el método ρ de Pollard. En 28 iteraciones, conseguimos

$$38141381 = 967 * 39443$$

donde ambos factores son primos, 967 se mira en una tabla, y 39443 se certifica que es primo porque 2 es un elemento primitivo. Por tanto,

$$m_2 + 1 = 1525655240 = 2^3 * 5 * 967 * 39443$$

Ahora, buscando entre las s.L. para $Q = 2, 3, 4, \ldots$, encontramos que la s.L. definida por P=1 y Q=6 el número m_2 tiene rango $m_2 + 1$ ya que calculando los términos

$$\begin{cases} U_{m_2+1} \equiv 0 \pmod{m_2} \\ U_{(m_2+1)/2} \equiv 959080291 \pmod{m_2} \\ U_{(m_2+1)/5} \equiv 1335495812 \pmod{m_2} \\ U_{(m_2+1)/967} \equiv 817967711 \pmod{m_2} \\ U_{(m_2+1)/39443} \equiv 448183651 \pmod{m_2} \end{cases}$$

Por tanto, se certifica que $m_2 = 1525655239$ es primo.

LUCAS CERTIFICADO

Como $m_2 = 1525655239$ es primo, tenemos la factorización en primos de

$$n + 1 = 740580514804902 = 2 * 3 * 17 * 4759 * 1525655239$$

podemos por tanto empezar a buscar una s.L. para certificar que $n = 740580514804901$ es primo. Entre las s.L. para $Q = 2, 3, 4, \ldots$, encontramos que la s.L. definida por P=1 y Q=31 el número n tiene rango $w(n) = n + 1$ ya que calculando los términos

$$\begin{cases} U_{n+1} \equiv 0 \pmod{n} \\ U_{(n+1)/2} \equiv 541879725150419 \pmod{n} \\ U_{(n+1)/3} \equiv 107159771256277 \pmod{n} \\ U_{(n+1)/17} \equiv 713517050696461 \pmod{n} \\ U_{(n+1)/4759} \equiv 251516807968421 \pmod{n} \\ U_{(n+1)/1525655239} \equiv 464091933503725 \pmod{n} \end{cases}$$

Y finalmente, se certifica que $n = 740580514804901$ es primo.

Enrique R. Aznar García
eaznar@ugr.es