Ejercicio 4

David García Curbelo

Dado tu número $n = 45352609$ de la lista del ejercicio 2:

Apartado I. ***Factoriza*** $n-1$ ***aplicando el método*** ρ ***de Polard. ¿Cuántas iteraciones necesitas?***

Tenemos que $n - 1 = 45352608 = 2^5 \cdot 3 \cdot 472423$. Ahora veamos si nuestro número 472423 es primo. Para ello aplicamos el test de composición de Fermat, con el que obtenemos que dicho número es compuesto, ya que $2^{472422} \equiv 64 \pmod{472423}$, luego tenemos certificado de composición. Tratamos ahora de factorizar 472423 mediante el método de Polard usando como función aleatoria $f(x) = x^2 + 1$:

Paso	x	y	mcd
0	1	1	-
1	2	5	1
2	5	677	7

Por lo que en dos iteraciones hemos encontrado que el número primo 7 es divisor de 472423, obteniendo así la factorización $n - 1 = 45352608 = 2^5 \cdot 3 \cdot 7 \cdot 67489$. Podemos ver que efectivamente el número 67489 pasa tanto el test de Miller-Rabin como el de Solovay-Strassen para los 5 primeros números primos, luego tenemos que la probabilidad de que efectivamente sea compuesto es de 4^{-5}.

Apartado II. ***Si es necesario aplica recursivamente Lucas-Lehmer para certificar factores primos de n-1 mayores de 4 cifras.***

Tenemos un factor mayor de cuatro cifras: el número 67489. Veamos si es primo. Para ello necesitamos calcular la factorización en primos de 67488, luego tenemos $67488 = 2^5 \cdot 3 \cdot 703$. Por la tabla de primos menores de 4 cifras, vemos que el número 703 no aparece en dicha tabla, luego es un número compuesto. Calculemos sus factores primos mediante el método ρ de Polard:

Paso	x	y	mcd
0	3	3	-
1	10	101	1
2	101	249	37

Por lo que en 2 iteraciones hemos encontrado la factorización completa de $67488 = 2^5 \cdot 3 \cdot 19 \cdot 37$. Como ya conocemos todos sus factores primos (2, 3, 19 y 37), iniciamos la búsqueda de un elemento primitivo para tratar de probar que efectivamente el número 67489 es primo. Para ello, aplicando el algoritmo de exponenciación rápida tenemos que, para $a = 23$ se cumple:

1. $23^{67488} \equiv 1 \pmod{67489}$
2. $23^{(67488)/2} \equiv -1 \pmod{67489}$
3. $23^{(67488)/3} \equiv 13861 \pmod{67489}$
4. $23^{(67488)/19} \equiv 52206 \pmod{67489}$
5. $23^{(67488)/37} \equiv 17698 \pmod{67489}$

Por lo que tenemos que 23 es un elemento primitivo de 67489 y por tanto tenemos un certificado de primalidad. Así hemos obtenido efectivamente la factorización en números primos de nuestro número original $n - 1 = 45352608 = 2^5 \cdot 3 \cdot 7 \cdot 67489$.

Apartado III. ***Aplica Lucas-Lehmer para encontrar un certificado de primalidad de*** n***.***

Para $n = 45352609$ tenemos $n - 1 = 45352608 = 2^5 \cdot 3 \cdot 7 \cdot 67489$, luego conocemos todos sus factores primos (2, 3, 7 y 67489). Iniciamos la búsqueda de un elemento primitivo para tratar de probar que efectivamente nuestro número n es primo. Para ello, aplicando el algoritmo de exponenciación rápida tenemos que, para $a = 19$ se cumple:

1. $19^{n-1} \equiv 1 \pmod{n}$
2. $19^{(n-1)/2} \equiv -1 \pmod{n}$
3. $19^{(n-1)/3} \equiv 3335204 \pmod{n}$
4. $19^{(n-1)/19} \equiv 43001658 \pmod{n}$
5. $19^{(n-1)/37} \equiv 14444632 \pmod{n}$

Por lo que podemos confirmar que 19 es un elemento primitivo de n. Así hemos obtenido efectivamente un certificado de primalidad y por tanto concluimos que 45352609 es un número primo.