Ejercicio 10

David García Curbelo

Toma tu número $p = 45352609$ de la lista publicada para este ejercicio.

Apartado I. ***Calcula el símbolo de Jacobi*** $\left(\frac{-11}{p}\right)$***. Si sale 1, usa el algoritmo de Tonelli-Shanks para hallar soluciones a la congruencia*** $x^2 \equiv -11 \pmod{p}$***.***

Calculamos el símbolo de Jacobi:

$$\left(\frac{-11}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-11}{p}\right) = \left(\frac{p}{11}\right) = \left(\frac{5}{11}\right) = 1$$

Procedemos a calcular las soluciones de la ecuación $x^2 \equiv -1 \pmod{p}$ mediante el algoritmo de Tonelli-Shanks. Para ello primero necesitamos estudiar la primalidad del número $p = 45352609$, para el que trataremos de encontrar un elemento primitivo. Vemos primeramente que p pasa el test de Fermat para las bases $a = 2, 3, 5, 7, 11$, cumpliendo $a^{p-1} \equiv a \pmod{p}$, por lo que tenemos altas probabilidades de primalidad. Procedemos a buscar mediante el algoritmo de Lucas-Lehmer un elemento primitivo de p. Para ello primero factorizamos $p - 1 = 2^5 \cdot 3 \cdot 7 \cdot 67489$.

Veamos si $p_1 = 67489$ es primo. Dicho número pasa el test de Fermat para las bases $a = 2, 3, 5, 7, 11$, cumpliendo $a^{p_1-1} \equiv a \pmod{p_1}$, por lo que tenemos altas probabilidades de primalidad. Factorizamos por tanto $p_1 - 1$ para poder aplicar el algoritmo de Lucas-Lehmer para p_1, con lo que obtenemos que $p_1 - 1 = 2^5 \cdot 3 \cdot 703$. Vemos que 703 no se encuentra en la lista de primos, luego aplicando el algoritmo ρ de Polard obtenemos una factorización completa de $p_1 - 1 = 2^5 \cdot 3 \cdot 19 \cdot 37$. Por tanto estamos en condiciones de buscar un elemento primitivo para p_1:

- $23^{(p_1-1)} \equiv 1 \pmod{p_1}$
- $23^{(p_1-1)/2} \not\equiv 1 \pmod{p_1}$
- $23^{(p_1-1)/3} \not\equiv 1 \pmod{p_1}$
- $23^{(p_1-1)/19} \not\equiv 1 \pmod{p_1}$
- $23^{(p_1-1)/37} \not\equiv 1 \pmod{p_1}$

Con lo que hemos encontrado un elemento primitivo, y por tanto tenemos certificado de primalidad de $p_1 = 67489$. Tenemos factorizado por tanto nuestro número $p - 1 = 2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 67489$ en factores primos, y estamos en condiciones de buscar un elemento primitivo para p:

- $19^{(p-1)} \equiv 1 \pmod{p}$
- $19^{(p-1)/2} \not\equiv 1 \pmod{p}$
- $19^{(p-1)/3} \not\equiv 1 \pmod{p}$
- $19^{(p-1)/7} \not\equiv 1 \pmod{p}$
- $19^{(p-1)/67489} \not\equiv 1 \pmod{p}$

Con lo que hemos encontrado un elemento primitivo, y por tanto tenemos certificado de primalidad de $p = 45352609$, como andábamos buscando.

Además comprobamos que $p \equiv 1 \pmod 8$, por tanto necesitamos de un algoritmo especial, en nuestro caso del algoritmo de Tonelli-Shanks. Para ello, factorizamos $p = 2^5 \cdot 1417269$, luego tenemos que el algoritmo tendrá a lo sumo 5 pasos.

Tomamos un número que no sea residuo cuadrático, por lo que para $n = 20$ tenemos que $\left(\frac{20}{p}\right) = -1$, luego 20 no es residuo cuadrático. Entonces, un generador del 2-subgrupo de Sylow $G \cong \mathbb{Z}_{2^5} = \mathbb{Z}_{32}$, viene dado por:

- $$z = n^q \equiv 20^{1417269} \equiv 12390911 \pmod p$$

  Ahora, como $t = (-11)^1417269 \equiv 196563 \not\equiv -1 \pmod p$, aún no hemos acabado. Como no es así, tenemos que $O(t)$ es un divisor de $2^{e-1} = 16$, luego para $i = 3$ tenemos que $t^{i-1} \equiv -1 \pmod p$

Apartado II. ***Usa una de estas soluciones para factorizar el ideal principal,*** $(p) = (p, n + \sqrt{-11})(p, n + \sqrt{-11}) como producto de dos ideales.$

Apartado III. ***Aplica el algoritmo de Conachia-Smith modificando a*** $2p$ ***y*** n ***para encontrar una solución a la ecuación diofántica*** $4p = x^2 + 11y^2$ ***y la usas para encontrar una factorización de*** p ***en a.e. del cuerpo*** $\mathbb{Q}[\sqrt{p}]$***.***

Apartado IV. ***¿Son principales sus ideales*** $(p, n+\sqrt{-11})$ ***y*** $(p, n+\sqrt{-11})$ ***?***