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 $n = 19$ tenemos que $\left(\frac{19}{p}\right) = -1$, luego 19 no es residuo cuadrático. Entonces, un generador del 2-subgrupo de Sylow $G \cong \mathbb{Z}_{2^5}$, viene dado por:

- $z = n^q \equiv 19^{1417269} \equiv 26515681 \pmod p$
  $r = (-11)^{(q+1)/2} \equiv 11370107 \pmod p$
  Notemos ahora que $t = (-11)^q \equiv 196563 \not\equiv -1 \pmod p$, luego tenemos que r no es raíz de la ecuación buscada. Calculamos ahora $O(t)$, que es un divisor de $2^{e-1} = 16$. Luego tenemos que $t^{2^2} \equiv -1 \pmod p$, y por tanto obtenemos que $O(t) = 2^3$.

- Lamamos ahora $b = z^{2^{e-i-1}} \equiv 23477766 \pmod p \not\equiv 1$
  Definimos $t_1 = t \cdot b^2 \equiv 41942710 \pmod p$
  $r_1 = r \cdot b \equiv 25961315 \pmod p$

- Definimos $t_2 = t_1 \cdot b^2 \equiv 6231274 \pmod p \not\equiv 1$
  $r_2 = r_1 \cdot b \equiv 11123330 \pmod p$

- Definimos $t_3 = t_2 \cdot b^2 \equiv -1 \pmod p \not\equiv 1$
  $r_3 = r_2 \cdot b \equiv 3748274 \pmod p$

- Definimos $t_4 = t_3 \cdot b^2 \equiv 45156046 \pmod p \not\equiv 1$
  $r_4 = r_3 \cdot b \equiv 31187509 \pmod p$

- Definimos $t_5 = t_4 \cdot b^2 \equiv 3409899 \pmod p \not\equiv 1$
  $r_5 = r_4 \cdot b \equiv 18849057 \pmod p$

- Definimos $t_6 = t_5 \cdot b^2 \equiv 39121335 \pmod p \not\equiv 1$
  $r_6 = r_5 \cdot b \equiv 43525646 \pmod p$

- Definimos $t_7 = t_6 \cdot b^2 \equiv 1 \pmod p$
  $r_7 = r_6 \cdot b \equiv 36504054 \pmod p$

Hemos encontrado por fin las soluciones de la congruencia $x^2 \equiv -11 \pmod p$, las cuales vienen dadas por:

- $x_1 = r_7 = 36504054$
- $x_2 = p - r_7 = 8848555$

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.***
Tomando la solución impar $x_2 = 8848555$, y teniendo en cuenta que -11 no divide a nuestro primo p, tenemos que los ideales $\left(p, 8848555 + \sqrt{-11}\right)$ y $\left(p, 8848555 - \sqrt{-11}\right)$ son primos entre sí:

$$(p) = \left(p, 8848555 + \sqrt{-11}\right)\left(p, 8848555 - \sqrt{-11}\right)$$

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*** $\mathbb{Q}[\sqrt{p}]$**.**
Para ello usaremos la solución impar del apartado 1, $x_2 = 8848555$, y aplicaremos el algoritmo de Conachia-Smith.

- $90705218 = 8848555 \cdot 10 + 2219668$
- $8848555 = 2219668 \cdot 3 + 2189551$
- $2219668 = 2189551 \cdot 1 + 30117$
- $2189551 = 30117 \cdot 72 + 21127$
- $30117 = 21127 \cdot 1 + 8990$

Por tanto, después de 10 divisores tenemos $x = 8990$ y $x^2 + 11 \cdot y^2 = 181410436$, con lo que despejando obtenemos la solución $y = 3024$. Encontremos ahora una factorización de p en a.e. del cuerpo $\mathbb{Q}[\sqrt{p}]$:

$$p = \frac{x^2 + 11 \cdot y^2}{4} = \frac{8990^2 + 11 \cdot 3024^2}{4} \quad \Rightarrow \quad p = \left(\frac{8990 + 3024\sqrt{-11}}{2}\right)\left(\frac{8990 - 3024\sqrt{-11}}{2}\right)$$

Apartado IV. ***¿Son principales sus ideales*** $(p, n+\sqrt{-11})$ ***y*** $(p, n+\sqrt{-11})$ ***?***
Por resultados vistos en teoría (ver Teorema 17), $\mathbb{Q}(\sqrt{-11})$ es un dominio de ideales principales, además de que $\left(p, 8848555+\sqrt{-11}\right)$ y $\left(p, 8848555-\sqrt{-11}\right)$ son ideales suyos. Por tanto podemos concluir que estos son ideales principales.