

# Ejercicio 10

Ana Buendía Ruiz-Azuaga

March 29, 2022

## 1 Ejercicio 10

### 1.1 Apartado 1

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

$$p = 77770081$$

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  $x^2 \equiv -11 \pmod{p}$ .

Tenemos que  $\left(\frac{-11}{p}\right) = 1$  luego aplicamos el algoritmo de Tonelli-Shanks para hallar las soluciones de  $x^2 \equiv -11 \pmod{p}$ .

Para ello, comenzamos factorizando  $p - 1 = 2^5 \cdot 3^2 \cdot 5 \cdot 53 \cdot 1019$

Para ello vamos a usar el método  $\rho$  de Polard. Comenzamos sacando los factores 2, y aplicamos el algoritmo a 2430315. Para factorizar este número han sido necesarias un total de 11 iteraciones.

Finalmente, aplicamos Lucas-Lehmer, obtenemos que 17 es elemento primitivo para  $p$ , ya que  $17^{p-1} \equiv 1 \pmod{p}$  y  $17^{\frac{p-1}{p}} \not\equiv 1 \pmod{p}$  para  $p \in \{2, 3, 5, 53, 1019\}$  pues::

$$\begin{aligned} 17^{(p-1)/2} &= 77770080 \pmod{p} \\ 17^{(p-1)/3} &= 58134188 \pmod{p} \\ 17^{(p-1)/5} &= 66432901 \pmod{p} \\ 17^{(p-1)/53} &= 68065795 \pmod{p} \\ 17^{(p-1)/1019} &= 65224721 \pmod{p} \end{aligned}$$

Luego  $p$  es primo

Como  $p \equiv 1 \pmod{8}$  tenemos que usar Tonelli-Shanks.

Hemos visto además que  $p - 1 = 2^5 \cdot 2430315$ , y como  $(-11)^{2430315} \equiv 158982 \pmod{p} \not\equiv 1 \pmod{p}$ . Y este tiene orden  $2^2 \pmod{p}$ .

Calculamos ahora un no residuo cuadrático módulo  $p$ , y el primero es  $n = 17$ .

Por tanto un generador del 2-subgrupo de Sylow  $G = \mathbb{Z}_{2^{17}}$ .

Aplicando el algoritmo obtenemos:

z: 55328379, t: 158982, i: 2, r: 29971170  
b: 12935680, t1: 1, i1: 0, r1: 796425  
Soluciones: 796425 76973656

Luego la soluciones son 796425 y 76973656, que se corresponden con  $r_1$  y  $p - r_1$ .

## 1.2 Apartado 2

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

Tomamos la solución impar  $n = 796425$  y como  $p$  es un impar primo que no divide a  $-11$  entonces  $(p) = (p, 796425 + \sqrt{-11})(796425 - \sqrt{-11})$

## 1.3 Apartado 3

Aplica el algoritmo de Cornachia-Smith modificado 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  $\mathbb{Q}(\sqrt{-11})$ .

Aplicamos el algoritmo de Cornachia-Smith:

Paso 1:  $155540162 = 195 \cdot 796425 + 237287$

Paso 2:  $796425 = 3 \cdot 237287 + 84564$

Paso 3:  $237287 = 2 \cdot 84564 + 68159$

Paso 4:  $84564 = 1 \cdot 68159 + 16405$

Tras 4 divisiones obtenemos el resto  $x = 16405$ . Por tanto, podemos hallar  $y$  despejando de la ecuación:

$$4p = x^2 + 11y^2 \Leftrightarrow y = \sqrt{\frac{4p - x^2}{11}} = 1953$$

Así, se cumple  $4p = 16405^2 + 11 \cdot 1953^2$

Luego tenemos que la factorización de  $p$  en a.e. de  $\mathbb{Q}[\sqrt{p}]$  es

$$p = \left( \frac{x + y\sqrt{-11}}{2} \right) \left( \frac{x - y\sqrt{-11}}{2} \right) = \left( \frac{16405 + 1953\sqrt{-11}}{2} \right) \left( \frac{16405 - 1953\sqrt{-11}}{2} \right)$$

## 1.4 Apartado 4

¿ Son principales tus ideales  $(p, n + \sqrt{-11})(p, n - \sqrt{-11})$

Son principales ya que  $\mathbb{Q}[\sqrt{-11}]$  es DIP.