

## Ejercicio 8

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  $x^2 \equiv -1 \pmod{p}$ .*

**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  $(p, n + \sqrt{-11})$  ?*