1. Descomposición de primos en c.c.

Dados $p, m \in \mathbb{Z}$, donde m libre de cuadrados y p primo. Sabemos por teoría que si $p \nmid m$, entonces el ideal principal (p) descompone como el producto de dos ideales primos en $O_{\mathbb{Q}(\sqrt{m})}$ si y sólo si el símbolo de Jacobi es $\left(\frac{m}{p}\right) = 1$ y si n es una solución a $x^2 \equiv m \pmod{p}$, entonces la factorización es

$$(p) = \left(p, n + \sqrt{m}\right)\left(p, n - \sqrt{m}\right)$$

Además, los dos ideales primos $\left(p, n + \sqrt{m}\right)$ y $\left(p, n - \sqrt{m}\right)$ en el anillo de enteros del c.c. $K = \mathbb{Q}(\sqrt{m})$ son principales cuando el nº de clases $h(K) = 1$.

Se puede llevar a cabo el proceso anterior, usando el algoritmo de Tonelli-Shanks para hallar una solución a la congruencia $x^2 \equiv m \pmod{p}$. Y si $h(K) = 1$, usar el algoritmo de Cornachia- Smith modificado para hallar generadores de los dos ideales primos en que descompone (p).

Ejemplo 1. *Vamos a descomponer* $p = 27213937$ *en* $O_{\mathbb{Q}(\sqrt{-11})}$. *Sabemos que* 27213937 *es primo porque 10 es un elemento primitivo en* $\mathbb{Z}_{27213937}$. *Además, si calculamos el símbolo de Jacobi sale* $\left(\frac{-11}{p}\right) = 1$.
Por tanto, $x^2 \equiv -11 \pmod{27213937}$ *tiene soluciones, que se pueden calcular con el algoritmo de Tonelli-Shanks. Iniciamos el método:*

Factorizamos $p - 1 = 2^4 * 1700871 = 2^e q$.
Como $(-11)^q \mod p = 4653122 = t$ *no sale 1 y tiene orden* $2^2 = 2^i$ *mod p.*
Hay que iterar para encontrar una raíz cuadrada de $-11 \mod p$.

Calculamos un no residuo cuadrático módulo p. El primero es $n = 5$.
Definimos $z = n^q \mod p = 24658840$. *Este z tiene orden* $2^4 = 2^e$ *módulo p.*

$$\left.\begin{array}{l} r = (-11)^{(q+1)/2} \mod p = 3595104 \\ b = z^{2^{e-i-1}} = z^2 \mod p = 6048857 \\ t_1 = t * b^2 = 4653122 * 6048857^2 \mod p = 1 \end{array}\right\} \Longrightarrow r * b \mod p = 21148483$$

Como $t_1 = 1$, *hemos terminado y las soluciones son* 21148483 *y* 6065454.
Tomamos la impar $n = 21148483$ *y como* $p = 27213937$ *es un primo impar y no divide a* $m = -11$, *tenemos la descomposición*

$$(p) = \left(p, 21148483 + \sqrt{-11}\right)\left(p, 21148483 - \sqrt{-11}\right)$$

Ahora, según el algoritmo de Cornachia- Smith modificado, si aplicamos el AE a $2p$ *y n, después de 9 divisiones obtenemos el primer resto* $a = 10297$

$$\left.\begin{array}{l} 54427874 = 2 * 21148483 + 12130908 \\ 21148483 = 1 * 12130908 + 9017575 \\ 12130908 = 1 * 9017575 + 3113333 \\ 9017575 = 2 * 3113333 + 2790909 \\ 3113333 = 1 * 2790909 + 322424 \\ 2790909 = 8 * 322424 + 211517 \\ 322424 = 1 * 211517 + 110907 \\ 211517 = 1 * 110907 + 100610 \\ 110907 = 1 * 100610 + 10297 \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} a = 10297 \\ b = \sqrt{4 * p - a^2)/11} = 507 \\ p = a^2 + 11 * b^2 \end{array}\right.$$

que es menor que $2\sqrt{p} \approx 10433.4$. *Este nos da la factorización*

$$4p = 10297^2 + 11 * 507^2 \Rightarrow p = \left(\frac{10297 + 507\sqrt{-11}}{2}\right)\left(\frac{10297 - 507\sqrt{-11}}{2}\right)$$

O sea, hemos encontrado los generadores de los ideales $\left(p, n \pm \sqrt{m}\right)$.