18 Enero 2008 (SOLUCIONES)

1. **Sea K un cuerpo de número y denotemos por $\mathcal{O}_K$ el anillo de enteros de K. Sea $I \subset \mathcal{O}_K$ un ideal y $\mathfrak{p}, \mathfrak{q} \subset \mathcal{O}_K$ ideales primos distintos. Demostrar:**

   a. **Sea $s \in \mathbb{N}$ tal que $\mathfrak{p}^s \subset I$ entonces existe $r \in \{0, \dots, s\}$ tal que $I = \mathfrak{p}^r$. ¿Cómo es I si $r = 0$?**
   Solución: En el conjunto de ideales de $\mathcal{O}_K$ hay factorización única en ideales primos. Por lo tanto de $\mathfrak{p}^s \subset I$ se deduce que I aparece en la factorización en ideales primos de $\mathfrak{p}^s$, por lo tanto necesariamente se tiene que existe $r \in \{0, \dots, s\}$ tal que $I = \mathfrak{p}^r$.
   En el caso en el que $r = 0$, tendríamos que $\mathfrak{p}^0 \subset I$, es decir, $\mathcal{O}_K \subset I$. Concluyendo: $I = \mathcal{O}_K$.

   b. **$\mathcal{O}_K = \mathfrak{p} + \mathfrak{q}$.**
   Solución: Para todo $n \in \mathbb{N}$ se tiene $\mathfrak{p}^n \subset \mathfrak{p} \subset \mathfrak{p} + \mathfrak{q}$. Aplicando el apartado anterior al ideal $I = \mathfrak{p}+\mathfrak{q}$ tenemos que exite $r \in \{0, \dots, n\}$ tal que $\mathfrak{p}+\mathfrak{q} = \mathfrak{p}^r$. Análogamente aplicando lo anterior al ideal $\mathfrak{q}$, obtemos que existe $s \in \{0 \cdots n\}$ tal que $\mathfrak{p} + \mathfrak{q} = \mathfrak{q}^s$. Así que tendremos $\mathfrak{p}^r = \mathfrak{q}^s$, de lo que se deduce que por la factorización única en ideales primos la única posibilidad es que $r = s = 0$. Concluyendo: $\mathfrak{p} + \mathfrak{q} = \mathfrak{q}^0 = \mathcal{O}_K$.

2. **Sea $\mathcal{O}$ el anillo de enteros de $\mathbb{Q}(\sqrt{35})$. Determinar:**

   a. **Todos los ideales de $\mathcal{O}$ de norma 14.**
   Solución: Como $d \not\equiv 1 \pmod 4$, $\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\sqrt{35})} = \mathbb{Z}[\theta]$ con $\theta = \sqrt{35}$, $f_\theta(x) = x^2 - 35$ el polinomio mínimo de θ. Sabemos que para todo ideal I de $\mathcal{O}$ se tiene $N_{\mathbb{Q}(\sqrt{35})}(I) \in I$. Por lo tanto $\langle N_{\mathbb{Q}(\sqrt{35})}(I)\rangle \subset I$, es decir, I aparece en la factorización del ideal $\langle N_{\mathbb{Q}(\sqrt{35})}(I)\rangle$. En nuestro caso buscamos los ideales de norma 14, por lo tanto hemos de calcular la factorización en ideales primos del ideal $\langle 14\rangle\mathcal{O}$. Como $\langle 14\rangle = \langle 2 \cdot 7\rangle = \langle 2\rangle\langle 7\rangle$. Así tenemos que factorizar los ideales $\langle 2\rangle$ y $\langle 7\rangle$. Para ello vamos a utilizar un resultado que nos dice que si K es un cuerpo de números y $\mathcal{O}_K = \mathbb{Z}[\theta]$, entonces si $f_\theta(x) \in \mathbb{Z}[x]$ es el polinomio mínimo de θ, $p \in \mathbb{Z}$ es un primo y $\overline{f_\theta}(x) = \overline{f}_1^{r_1}(x) \cdots \overline{f}_s^{r_s}(x)$ la descomposición en polinomios irreducibles de $\overline{f_\theta}(x)$ en $\mathbb{F}_p[x]$. Obtenemos que la descomposición en ideales primos de $\mathcal{O}_K$ del ideal $\langle p\rangle\mathcal{O}_K$ es

   $$\langle p\rangle\mathcal{O}_K = \langle p, f_1(\theta)\rangle^{r_1} \cdots \langle p, f_s(\theta)\rangle^{r_s},$$

   donde $f_i(x) \in \mathbb{Z}[x]$ es un levantado de $\overline{f_i}$, $i = 1, \dots, s$.

   Apliquemos este resultado a nuestro caso. Tenemos $\theta = \sqrt{35}$, $f_\theta(x) = x^2 - 35$:

   - $p = 2$: Tenemos $f_\theta(x) \equiv (x-1)^2 \pmod 2$, por lo tanto

     $$\langle 2\rangle = \langle 2, 1 + \sqrt{35}\rangle^2 = \mathfrak{p}_2^2,$$

     con $\mathfrak{p}_2$ ideal primo de $\mathcal{O}$ de norma 2. Ya que

     $$4 = N_{\mathbb{Q}(\sqrt{35})}(2) = N_{\mathbb{Q}(\sqrt{35})}(\langle 2\rangle) = N_{\mathbb{Q}(\sqrt{35})}(\mathfrak{p}_2)^2.$$

- $p = 7$: Tenemos $f_\theta(x) \equiv x^2 \pmod 7$, por lo tanto

$$\langle 7\rangle = \langle 7, \sqrt{35}\rangle^2 = \mathfrak{p}_7^2,$$

con $\mathfrak{p}_7$ ideal primo de $\mathcal{O}$ de norma 7. Ya que

$$7^2 = N_{\mathbb{Q}(\sqrt{35})}(7) = N_{\mathbb{Q}(\sqrt{35})}(\langle 7\rangle) = N_{\mathbb{Q}(\sqrt{35})}(\mathfrak{p}_7)^2.$$

Por lo tanto:

$$\langle 14\rangle = \mathfrak{p}_2^2\mathfrak{p}_7^2\,.$$

Así deducimos que el único ideal de norma 14 es $I = \mathfrak{p}_2\mathfrak{p}_7$.

b. Todos los ideales de $\mathcal{O}$ que contienen a $\sqrt{14}$.
Solución: No hay ningún ideal de $\mathcal{O}$ que contenga a $\sqrt{14}$, ya que $\sqrt{14} \notin \mathbb{Q}(\sqrt{35})$.

c. Todos los ideales de $\mathcal{O}$ que contienen a $\sqrt{35}$.
Solución: En primer lugar obsérvese que $\sqrt{35} \in \mathcal{O}$. Por otro lado, $(\sqrt{35})^2 = 35$. Así que vamos a factorizar el ideal $\langle 35\rangle = \langle 5\rangle\langle 7\rangle$. Análogamente al apartado **a**, factorizamos el ideal $\langle 5\rangle$ y obtenemos

$$\langle 5\rangle = \langle 5, \sqrt{35}\rangle^2 = \mathfrak{p}_5^2,\,.$$

Así, $\langle 35\rangle = \mathfrak{p}_5^2\mathfrak{p}_7^2$, de lo que se deduce $\langle\sqrt{35}\rangle = \mathfrak{p}_5\mathfrak{p}_7$. Por lo tanto los ideales de $\mathcal{O}$ que contienen a $\sqrt{35}$ son:

$$\mathcal{O}, \mathfrak{p}_5, \mathfrak{p}_7, \mathfrak{p}_5\mathfrak{p}_7\,.$$

3. Determinar si el anillo de enteros de $\mathbb{Q}(\sqrt{-47})$ es una dominio de factorización única.
Solución 1: Veamos que $\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\sqrt{-47})} = \mathbb{Z}[\frac{1+\sqrt{-47}}{2}]$ no es un dominio de factorización única. Para ello basta con ver que las siguientes factorizaciones en irreducibles de 12 no son asociadas:

$$\left(\frac{1+\sqrt{-47}}{2}\right)\left(\frac{1-\sqrt{-47}}{2}\right) = 12 = 2^2\cdot 3.$$

Para ello basta con ver que los elementos 2,3,$\frac{1+\sqrt{-47}}{2}$,$\frac{1-\sqrt{-47}}{2}$ son irreducibles. No hace falta ver si son asociados ya que en la primera factorización aparecen dos factores y en la segunda tres. Sea $\alpha \in \mathcal{O}$ irreducible tal que $\alpha|2$ (resp. 3,$\frac{1+\sqrt{-47}}{2}$,$\frac{1-\sqrt{-47}}{2}$). Entonces $N_{\mathbb{Q}(\sqrt{-47})}(\alpha)|N_{\mathbb{Q}(\sqrt{-47})}(2) = 4$ (resp. 9,12,12). De aquí se deduce que todo se reduce a ver que no existe $\alpha \in \mathcal{O}$ de norma 2 ó 3. En el ejercicio 4 hemos visto dicha afirmación.
Solución 2: El Teorema de Heegner-Stark nos asegura que $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ para $d < 0$ entero libre de cuadrados es DFU si y sólo si $d \in \{-1,-2,-3,-7,-11,-19,-43,-67,-163\}$. Como -47 no esta en ese conjunto tenemos que $\mathcal{O}$ no es dominio de factorización única.
Solución 3: Se tiene que $\mathcal{O}$ es un dominio de ideales principales (DIP) si y sólo si es un dominio de factorización única (DFU). Para ello basta con ver que existe al menos un ideal que no es principal. En el ejercicio 4 hemos visto que el ideal $\mathfrak{p}_2$ no es principal. Por lo tanto $\mathcal{O}$ no es un DIP y por lo tanto no es un DFU.
Solución 4: En el ejercicio 4 hemos demostrado que $h_{\mathbb{Q}(\sqrt{-47})} = 5 \neq 1$ por lo tanto $\mathcal{O}$ no es DFU.

4. Calcular la estructura del grupo de clase del cuerpo cuadrático $\mathbb{Q}(\sqrt{-47})$
Solución: Sabemos que todo ideal de $\mathcal{O}_K$, para K cuerpo de números, es equivalente a uno de norma menor o igual a la cota de Minkowski:

$$M_K = \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta_K|},$$

donde

$$\begin{array}{rcl} 2\mathrm{t} & = & \text{número de inmersiones complejas de } K, \\ \mathrm{n} & = & [K:\mathbb{Q}], \\ \Delta_K & = & \text{discriminante de } K. \end{array}$$

En nuestro caso $K = \mathbb{Q}(\sqrt{-47})$ es un cuerpo cuadrático ($n = 2$) imaginario ($t = 1$) con $d = -47$ libre de cuadrados tal que $d \equiv 1 \pmod 4$. Por lo tanto $\mathcal{O}_{\mathbb{Q}(\sqrt{-47})} = \mathbb{Z}[\theta]$ con $\theta = \frac{1+\sqrt{-47}}{2}$, $f_\theta(x) = x^2 - x + 12$ el polinomio mínimo de θ y $\Delta_{\mathbb{Q}(\sqrt{-47})} = -47$. Así obtenemos $M_{\mathbb{Q}(\sqrt{-47})} = 4'3$. Así todo ideal de $\mathcal{O}_{\mathbb{Q}(\sqrt{-47})}$ es equivalente a uno de norma ≤ 4.

Sabemos que para todo ideal I de $\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\sqrt{-47})}$ se tiene $N_{\mathbb{Q}(\sqrt{-47})}(I) \in I$. Por lo tanto $\langle N_{\mathbb{Q}(\sqrt{-47})}(I)\rangle \subset I$, es decir, I aparece en la factorización del ideal $\langle N_{\mathbb{Q}(\sqrt{-47})}(I)\rangle$. Así que hemos de calcular la factorización de los ideales generados por $1, 2, 3, 4$. Para ello vamos a utilizar el resultado que nos dice que si K es un cuerpo de números y $\mathcal{O}_K = \mathbb{Z}[\theta]$, entonces si $f_\theta(x) \in \mathbb{Z}[x]$ es el polinomio mínimo de θ, $p \in \mathbb{Z}$ es un primo y $\overline{f_\theta}(x) = \overline{f}_1^{r_1}(x) \cdots \overline{f}_s^{r_s}(x)$ la descomposición en polinomios irreducibles de $\overline{f_\theta}(x)$ en $\mathbb{F}_p[x]$. Obtenemos que la descomposición en ideales primos de $\mathcal{O}_K$ del ideal $\langle p\rangle\mathcal{O}_K$ es

$$\langle p\rangle\mathcal{O}_K = \langle p, f_1(\theta)\rangle^{r_1} \cdots \langle p, f_s(\theta)\rangle^{r_s},$$

donde $f_i(x) \in \mathbb{Z}[x]$ es un levantado de $\overline{f_i}$, $i = 1, \ldots, s$.

Apliquemos este resultado a nuestro caso. Tenemos $\theta = \frac{1+\sqrt{-47}}{2}$, $f_\theta(x) = x^2 - x + 12$:

- $p = 2$: Tenemos $f_\theta(x) \equiv x(x+1) \pmod 2$, por lo tanto

  $$\langle 2\rangle = \left\langle 2, \frac{1+\sqrt{-47}}{2}\right\rangle \left\langle 2, \frac{1-\sqrt{-47}}{2}\right\rangle = \mathfrak{p}_2\overline{\mathfrak{p}}_2,$$

  con $\mathfrak{p}_2, \overline{\mathfrak{p}}_2$ ideales primos de $\mathcal{O}_{\mathbb{Q}(\sqrt{-47})}$ de norma 2. Ya que

  $$4 = N_{\mathbb{Q}(\sqrt{-47})}(2) = N_{\mathbb{Q}(\sqrt{-47})}(\langle 2\rangle) = N_{\mathbb{Q}(\sqrt{-47})}(\mathfrak{p}_2)N_{\mathbb{Q}(\sqrt{-47})}(\overline{\mathfrak{p}}_2).$$

- $p = 3$: Tenemos $f_\theta(x) \equiv x(x-1) \pmod 3$, por lo tanto

  $$\langle 3\rangle = \left\langle 3, \frac{1+\sqrt{-47}}{2}\right\rangle \left\langle 3, \frac{1-\sqrt{-47}}{2}\right\rangle = \mathfrak{p}_3\overline{\mathfrak{p}}_3,$$

  con $\mathfrak{p}_3$ y $\overline{\mathfrak{p}}_3$ ideales primos de $\mathcal{O}_{\mathbb{Q}(\sqrt{-47})}$ de norma 3. Ya que

  $$9 = N_{\mathbb{Q}(\sqrt{-47})}(3) = N_{\mathbb{Q}(\sqrt{-47})}(\langle 3\rangle) = N_{\mathbb{Q}(\sqrt{-47})}(\mathfrak{p}_3)N_{\mathbb{Q}(\sqrt{-47})}(\overline{\mathfrak{p}}_3).$$

Por lo tanto tenemos que si I es un ideal de $\mathcal{O}_{\mathbb{Q}(\sqrt{-47})}$ de norma $1, 2, 3$ ó 4 ha de ser:

- 1: $I = \mathcal{O}$.
- 2: $I = \mathfrak{p}_2$ ó $I = \overline{\mathfrak{p}}_2$.
- 3: $I = \mathfrak{p}_3$ ó $I = \overline{\mathfrak{p}}_3$..
- 4: $\langle 4\rangle = \mathfrak{p}_2^2\overline{\mathfrak{p}}_2^2$. Así $I \in \{\mathfrak{p}_2^2, \overline{\mathfrak{p}}_2^2, \mathfrak{p}_2\overline{\mathfrak{p}}_2 = \langle 2\rangle\}$. Como $\langle 2\rangle$ es principal, es equivalente a $\mathcal{O}_{\mathbb{Q}(\sqrt{-47})}$. Así tenemos que $I = \mathfrak{p}_2^2$ ó $I = \overline{\mathfrak{p}}_2^2$.

Concluimos que cualquier ideal de $\mathcal{O}$ es equivalente a uno de los siguientes ideales:

$$\mathcal{O}, \mathfrak{p}_2, \overline{\mathfrak{p}}_2, \mathfrak{p}_3, \overline{\mathfrak{p}}_3, \mathfrak{p}_2^2, \overline{\mathfrak{p}}_2^2$$

Por lo tanto el número de clase es menor o igual a 7, es decir:

$$1 \leq h_{\mathbb{Q}(\sqrt{-47})} \leq 7\,.$$

En primer lugar para acotar $h_{\mathbb{Q}(\sqrt{-47})}$ veamos si alguno de los ideales $\mathfrak{p}_2, \overline{\mathfrak{p}}_2, \mathfrak{p}_3, \overline{\mathfrak{p}}_3.\mathfrak{p}_2^2, \overline{\mathfrak{p}}_2^2$ es equivalente a $\mathcal{O}$. Para ello recordemos que si I es un ideal de $\mathcal{O}$ de norma n tal que $I \sim \mathcal{O}$, entonces es principal. Es decir, existirá $\alpha = \frac{a+b\sqrt{-47}}{2} \in \mathcal{O}$ tal que $I = \langle\alpha\rangle\mathcal{O}$ y por lo tanto $n = N_{\mathbb{Q}(\sqrt{-47})}(I) = |N_{\mathbb{Q}(\sqrt{-47})}(\alpha)| = \frac{a^2+47b^2}{4}$. Por lo tanto vamos a estudiar las soluciones enteras de $a^2 + 47b^2 = 4n$.

- $n = 2$: Entonces $b = 0$ ya que $a^2 = 8 - 47b^2 < 0$ para $b \neq 0$. Por lo tanto, $a^2 = 8$, pero entonces $a \notin \mathbb{Z}$. Así hemos visto que no existen elementos de norma 2. Es decir, $[\mathfrak{p}_2] \neq [\mathcal{O}]$ y $[\overline{\mathfrak{p}}_2] \neq [\mathcal{O}]$.
- $n = 3$: Equivalentemente al caso $n = 2$ obtenemos que no existen elementos de norma 3 y por lo tanto $[\mathfrak{p}_3] \neq [\mathcal{O}]$ y $[\overline{\mathfrak{p}}_3] \neq [\mathcal{O}]$.
- $n = 4$: Entonces $b = 0$ ya que $a^2 = 16 - 47b^2 < 0$ para $b \neq 0$. Por lo tanto, $a^2 = 16$, es decir, $a = \pm 4$. Así, los únicos elementos de norma 4 son $\alpha = \pm 2$. Sea $\mathfrak{p} = \mathfrak{p}_2$ ó $\mathfrak{p} = \overline{\mathfrak{p}}_2$ tal que $\mathfrak{p}^2 = \langle 2\rangle$. Entonces $\mathfrak{p}^2 = \langle 2\rangle\mathcal{O}$. Pero esto no puede ser, ya que entonces $\mathfrak{p}_2 = \overline{\mathfrak{p}}_2$ y se tendría que $1 = \frac{1+\sqrt{-47}}{2} + \frac{1-\sqrt{-47}}{2} \in \mathfrak{p}$. Así que hemos visto: $[\mathfrak{p}_2^2] \neq [\mathcal{O}]$ y $[\overline{\mathfrak{p}}_2^2] \neq [\mathcal{O}]$.

Por lo tanto:

$$2 \leq h_{\mathbb{Q}(\sqrt{-47})} \leq 7\,.$$

Seguimos acotando $h_{\mathbb{Q}(\sqrt{-47})}$. Para ello vamos a ver que relación de equivalencia hay entre los ideales $\mathfrak{p}_2, \overline{\mathfrak{p}}_2, \mathfrak{p}_3, \overline{\mathfrak{p}}_3, \mathfrak{p}_2^2, \overline{\mathfrak{p}}_2^2$.

- Supongamos $[\mathfrak{p}_2] = [\overline{\mathfrak{p}}_2]$. Entonces $[\mathfrak{p}_2][\mathfrak{p}_2] = [\overline{\mathfrak{p}}_2][\mathfrak{p}_2] = [\langle 2\rangle] = [\mathcal{O}]$. Por lo tanto $[\mathfrak{p}_2^2] = [\mathcal{O}]$. Es decir, existe $\alpha \in \mathcal{O}$ tal que $\mathfrak{p}_2^2 = \langle\alpha\rangle$, pero hemos visto anteriormente que esto es imposible. Por lo tanto, $[\mathfrak{p}_2] \neq [\overline{\mathfrak{p}}_2]$.
- Supongamos $[\mathfrak{p}_3] = [\overline{\mathfrak{p}}_3]$. Entonces $[\mathfrak{p}_3][\mathfrak{p}_3] = [\overline{\mathfrak{p}}_3][\mathfrak{p}_3] = [\langle 3\rangle] = [\mathcal{O}]$. Por lo tanto $[\mathfrak{p}_3^2] = [\mathcal{O}]$. Es decir, existe $\alpha = \frac{a+b\sqrt{-47}}{2} \in \mathcal{O}$ tal que $\mathfrak{p}_3^2 = \langle\alpha\rangle$ y por lo tanto $|N_{\mathbb{Q}(\sqrt{-47})}(\alpha)| = N_{\mathbb{Q}(\sqrt{-47})}(\mathfrak{p}_3)^2 = 3^2 = 9$. Por lo tanto se ha de cumplir $a^2 + 47b^2 = 36$. Entonces $b = 0$ ya que $a^2 = 36 - 47b^2 < 0$ para $b \neq 0$. Por lo tanto, $a^2 = 36$, es decir, $a \pm 6$. Así, los únicos elementos de norma 9 son $\alpha = \pm 3$. En este caso se tendría $\mathfrak{p}_3^2 = \langle 3\rangle$. Pero esto no puede ser, ya que entonces $\mathfrak{p}_3 = \overline{\mathfrak{p}}_3$ y se tendría que $1 = \frac{1+\sqrt{-47}}{2} + \frac{1-\sqrt{-47}}{2} \in \mathfrak{p}_3$. Por lo tanto, $[\mathfrak{p}_3] \neq [\overline{\mathfrak{p}}_3]$.
- Supongamos $[\mathfrak{p}_2] = [\mathfrak{p}_3]$. Entonces $[\mathfrak{p}_2][\overline{\mathfrak{p}}_3] = [\mathfrak{p}_3][\overline{\mathfrak{p}}_3] = [\langle 3\rangle] = [\mathcal{O}]$. Por lo tanto $[\mathfrak{p}_2\overline{\mathfrak{p}}_3] = [\mathcal{O}]$. Es decir, existe $\alpha = \frac{a+b\sqrt{-47}}{2} \in \mathcal{O}$ tal que $\mathfrak{p}_2\overline{\mathfrak{p}}_3 = \langle\alpha\rangle$ y por lo tanto $|N_{\mathbb{Q}(\sqrt{-47})}(\alpha)| = N_{\mathbb{Q}(\sqrt{-47})}(\mathfrak{p}_2\overline{\mathfrak{p}}_3) = N_{\mathbb{Q}(\sqrt{-47})}(\mathfrak{p}_2)N_{\mathbb{Q}(\sqrt{-47})}(\overline{\mathfrak{p}}_3) = 2\cdot 3 = 6$. Por lo tanto se ha de cumplir $a^2+47b^2 = 24$. De aquí se deduce que $b = 0$ y por lo tanto $a^2 = 24$, pero entonces $a \notin \mathbb{Z}$. Se concluye que no hay elemento de norma 6 y así $[\mathfrak{p}_2] \neq [\mathfrak{p}_3]$. De igual forma se ve $[\mathfrak{p}_2] \neq [\overline{\mathfrak{p}}_3]$, $[\mathfrak{p}_3] \neq [\overline{\mathfrak{p}}_2]$ y $[\overline{\mathfrak{p}}_2] \neq [\overline{\mathfrak{p}}_3]$.

De lo que se deduce:

$$5 \leq h_{\mathbb{Q}(\sqrt{-47})} \leq 7\,.$$

- Supongamos $[\mathfrak{p}_2^2] = [\overline{\mathfrak{p}}_3]$. Entonces $[\mathfrak{p}_2^2][\mathfrak{p}_3] = [\overline{\mathfrak{p}}_3][\mathfrak{p}_3] = [\langle 3\rangle] = [\mathcal{O}]$. Por lo tanto $[\mathfrak{p}_2^2\mathfrak{p}_3] = [\mathcal{O}]$. Es decir, existe $\alpha = \frac{a+b\sqrt{-47}}{2} \in \mathcal{O}$ tal que $\mathfrak{p}_2^2\mathfrak{p}_3 = \langle\alpha\rangle$ y por lo tanto $|N_{\mathbb{Q}(\sqrt{-47})}(\alpha)| = N_{\mathbb{Q}(\sqrt{-47})}(\mathfrak{p}_2^2\mathfrak{p}_3) = N_{\mathbb{Q}(\sqrt{-47})}(\mathfrak{p}_2)^2 N_{\mathbb{Q}(\sqrt{-47})}(\mathfrak{p}_3) = 2^2 \cdot 3 = 12$. Por lo tanto se ha de cumplir $a^2 + 47b^2 = 48$. Si $|b| > 1$ entonces $a^2 = 48 - 47b^2 < 0$, entonces $a \notin \mathbb{Z}$. Si $b = 0$ entonces $a^2 = 48$, pero entonces $a \notin \mathbb{Z}$. Si $|b| = 1$ entonces $a^2 = 1$, por lo tanto $a = \pm 1$. Asi que hemos visto que $\alpha = \frac{\pm 1 \pm \sqrt{-47}}{2}$ tienen norma 12 y por lo tanto son candidatos para que generen el ideal $\mathfrak{p}_2^2\mathfrak{p}_3$. Un cáculo explícito demuestra $\mathfrak{p}_2^2\mathfrak{p}_3 = \langle\frac{-1-\sqrt{-47}}{2}\rangle$. Equivalentemente obtenemos $[\overline{\mathfrak{p}}_2^2] = [\mathfrak{p}_3]$.

De lo que se deduce:

$$5 \leq h_{\mathbb{Q}(\sqrt{-47})} \leq 5\,.$$

Así hemos obtenido $h_{\mathbb{Q}(\sqrt{-47})} = 5$ y por lo tanto

$$\mathcal{H}_{\mathbb{Q}(\sqrt{-47})} = \mathbb{Z}/5\mathbb{Z}.$$

Por lo tanto las clases de cualquiera de los ideales $\mathfrak{p}_2, \overline{\mathfrak{p}}_2, \mathfrak{p}_3, \overline{\mathfrak{p}}_3$ generan el grupo de clase del cuerpo cuadrático $\mathbb{Q}(\sqrt{-47})$.

5. Determinar las soluciones enteras de la ecuación diofántica $C : x^3 = y^2 + 2$.
Solución: Factorizando C obtenemos $(y + \sqrt{-2})(y - \sqrt{-2}) = x^3$. Esto indica que hemos de trabajar sobre el cuerpo cuadrática $\mathbb{Q}(\sqrt{-2})$ cuyo anillo de enteros es $\mathcal{O} = \mathbb{Z}[\sqrt{-2}]$.

Vamos a trabajar con ideales. Sea $\mathfrak{p} \subset \mathbb{Z}[\sqrt{-2}]$ ideal primo tal que $\mathfrak{p}$ divide a $\langle y + \sqrt{-2}\rangle$ y a $\langle y - \sqrt{-2}\rangle$. Entonces dividirá a la resta: $\langle 2\sqrt{-2}\rangle = \mathfrak{p}_2^3$, donde $\mathfrak{p}_2 = \langle\sqrt{-2}\rangle$. De donde se deduce $\mathfrak{p} = \mathfrak{p}_2$. En ese caso, $\mathfrak{p} \,|\, \langle y + \sqrt{-2}\rangle\langle y - \sqrt{-2}\rangle = \langle x^3\rangle = \langle x\rangle^3$. Por lo tanto, tomando normas, $2|x$. Es decir, $x \equiv 0 \,(\mathrm{mod}\ 2)$ y mirando en la ecuación obtenemos $y \equiv 0 \,(\mathrm{mod}\ 2)$. Ahora mirando la ecuación módulo 4 se tendría $2 \equiv 0 \,(\mathrm{mod}\ 4)$. Así que los ideales $\langle y + \sqrt{-2}\rangle, \langle y - \sqrt{-2}\rangle$ son primos entre si. Por lo tanto, juntando lo anterior con el hecho de que $\langle x\rangle^3 = \langle y + \sqrt{-2}\rangle\langle y - \sqrt{-2}\rangle$ y de que en $\mathcal{O}$ hay factorización única en ideales obtenemos $\langle y + \sqrt{-2}\rangle = \mathfrak{s}^3$, para algún ideal $\mathfrak{s}$ de $\mathcal{O}$.

El Teorema de Heegner-Stark (o utilizando la cota de Minkowski en este caso, $M_{\mathbb{Q}(\sqrt{-2})} < 2$) nos dice que $\mathcal{O}$ es un D.I.P.. Aplicando este hecho a $\langle y + \sqrt{-2}\rangle = \mathfrak{s}^3$, se obtiene

$$y + \sqrt{-2} = u(a + b\sqrt{-2})^3 \qquad \text{donde } u \in \mathcal{U}(\mathcal{O}) = \{\pm 1\}.$$

Como las unidades son cubos podemos incluirla dentro y tenemos el sistema:

$$\left\{ \begin{array}{rcl} y & = & a^3 - 6ab^2 \\ 1 & = & b(3a^2 - 2b^2) \end{array} \right.$$

De la segunda ecuación obtenemos que o bien $b = 1$ y $3a^2 - 2b^2 = 1$, o bien $b = -1$ y $3a^2 - 2b^2 = -1$. Es decir, $a^2 = 1$ ó $3a^2 = 1$. Es decir, la única posibilidad es $(a, b) = (\pm 1, 1)$. Sustituyendo en la primera ecuación nos da $y = \pm 5$. Por lo tanto se ha de tener $x^3 = (\pm 5)^2 + 2 = 27 = 3^3$. Por lo que se obtienen las soluciones $(3, \pm 5)$.

Conclusión: Las únicas soluciones a la ecuación diofántica $C : x^3 = y^2 + 2$ son $(x, y) = (3, \pm 5)$. Es decir:

$$C(\mathbb{Z}) = \{(3, \pm 5)\}\,.$$