19 de Enero 2007 (SOLUCIONES)

(1) Sea $\mathcal{O}$ el anillo de enteros de $\mathbb{Q}(\sqrt{-17})$.

(a) Calcular $\mathcal{O}$, una base entera de $\mathcal{O}$, $\mathcal{U}(\mathcal{O})$ y $\Delta_{\mathbb{Q}(\sqrt{-17})}$.
Solución: El cuerpo de números $\mathbb{Q}(\sqrt{-17})$ es un cuerpo cuadrático con $d = -17$ libre de cuadrados y tal que $d \not\equiv 1 \pmod 4$. Por lo tanto $\mathcal{O} = \mathbb{Z}[\sqrt{-17}]$. De aquí se deduce que una base entera es $\{1, \sqrt{-17}\}$, ya que $\mathbb{Z}[\sqrt{-17}] = 1 \cdot \mathbb{Z} \oplus \sqrt{-17} \cdot \mathbb{Z}$. El discriminante es $\Delta_{\mathbb{Q}(\sqrt{-17})} = 4(-17) = -68$. Como $d < 0$ y $d \neq -1, -3$ se tiene que las unidades de $\mathcal{O}$ son $\mathcal{U}(\mathcal{O}) = \{\pm 1\}$.

(b) Calcular la norma y la traza de los siguientes elementos de $\mathbb{Q}(\sqrt{-17})$: 3, $1 + \sqrt{-17}$ y $\frac{1}{2}(1 + 3\sqrt{-17})$
Solución: Las inmersiones de $\mathbb{Q}(\sqrt{-17})$ en $\overline{\mathbb{Q}}$ vienen determinadas por

$$\sigma_1(a + b\sqrt{-17}) = a + b\sqrt{-17} \quad \text{y} \quad \sigma_2(a + b\sqrt{-17}) = a - b\sqrt{-17}.$$

Por lo tanto si $\alpha = a + b\sqrt{-17} \in \mathbb{Q}(\sqrt{-17})$, se tiene

$$N_{\mathbb{Q}(\sqrt{-17})}(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) = a^2 + 17b^2 \qquad \text{y} \qquad Tr_{\mathbb{Q}(\sqrt{-17})}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) = 2a.$$

Aplicandolo a nuestros casos obtenemos

$$\begin{array}{lcllcl} N_{\mathbb{Q}(\sqrt{-17})}(3) & = & 9 & Tr_{\mathbb{Q}(\sqrt{-17})}(3) & = & 6 \\ N_{\mathbb{Q}(\sqrt{-17})}(1+\sqrt{-17}) & = & 18 & Tr_{\mathbb{Q}(\sqrt{-17})}(1+\sqrt{-17}) & = & 2 \\ N_{\mathbb{Q}(\sqrt{-17})}(\frac{1}{2}(1+3\sqrt{-17})) & = & \frac{77}{2} & Tr_{\mathbb{Q}(\sqrt{-17})}(\frac{1}{2}(1+\sqrt{-17})) & = & 1 \end{array}$$

(c) Encontrar todos los elementos de $\mathcal{O}$ de norma p donde $p = 2, 3, 5$.
Solución: Sea $\alpha = a + b\sqrt{-17} \in \mathcal{O}$, entonces $N_{\mathbb{Q}(\sqrt{-17})}(\alpha) = a^2 + 17b^2$. Si buscamos $\alpha \in \mathcal{O}$ tal que $N_{\mathbb{Q}(\sqrt{-17})}(\alpha) = p$ para $p = 2, 3, 5$. Hemos de buscar las soluciones enteras a las ecuaciones diofánticas

$$a^2 + 17b^2 = p, \qquad p = 2, 3, 5.$$

Si $b = 0$, entonces $p = a^2$, que es imposible ya que p es primo. Si $|b| > 0$, entonces $a^2 = p - 17b^2 < 0$ si $p = 2, 3, 5$. Así que en este caso tampoco hay solución. Por lo tanto no hay elementos en $\mathcal{O}$ de norma $2, 3$ ó 5.

(d) Demostrar que $\mathcal{O}$ no es un dominio de ideales principales.
Solución 1: Si $\mathcal{O}$ es un dominio de ideales principales entonces es un dominio de factorización única (DFU). Veamos que no es un DFU. Para ello basta con ver que las siguientes factorizaciones en irreducibles de 18 no son asociadas:

$$18 = 2 \cdot 3 \cdot 3 = (1 + \sqrt{-17})(1 - \sqrt{-17}).$$

Para ello basta con ver que los elementos 2,3,$1 + \sqrt{-17}$,$1 - \sqrt{-17}$ son irreducibles. No hace falta ver si son asociados ya que en la primera factorización aparecen tres factores y en la segunda sólo dos. Sea $\alpha \in \mathcal{O}$ irreducible tal que $\alpha | 2$ (resp. 3,$1 + \sqrt{-17}$,$1 - \sqrt{-17}$). Entonces $N_{\mathbb{Q}(\sqrt{-17})}(\alpha) | N_{\mathbb{Q}(\sqrt{-17})}(2) = 4$ (resp. 9,18,18). De aquí se deduce que $N_{\mathbb{Q}(\sqrt{-17})}(\alpha) = 2$ (resp. ± 3,

± 2 ó ± 3, ± 2 ó ± 3) ya que α no es una unidad y $N_{\mathbb{Q}(\sqrt{-17})}(\alpha) \geq 0$. Concluyendo que no puede existir $\alpha \in \mathcal{O}$ por el apartado **(c)**.
Solución 2: El Teorema de Heegner-Stark nos asegura que $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ para $d < 0$ es DFU si y sólo si $d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$. Como -17 no esta en ese conjunto tenemos que $\mathcal{O}$ no es DFU y por lo tanto no es DIP.
Solución 3: Veamos que existe al menos un ideal que no es principal. Utilizando el apartado **(e)** tenemos $\langle 2\rangle\mathcal{O} = \mathfrak{p}_2^2$. Por lo tanto

$$N_{\mathbb{Q}(\sqrt{-17})}(\mathfrak{p}_2^2) = N_{\mathbb{Q}(\sqrt{-17})}(\mathfrak{p}_2)^2 = N_{\mathbb{Q}(\sqrt{-17})}(\langle 2\rangle) = N_{\mathbb{Q}(\sqrt{-17})}(2) = 4.$$

Es decir, $N_{\mathbb{Q}(\sqrt{-17})}(\mathfrak{p}_2) = 2$. Si $\mathfrak{p}_2$ fuera principal existiría $\alpha \in \mathcal{O}$ tal que $\mathfrak{p}_2 = \langle\alpha\rangle$. Por lo tanto $|N_{\mathbb{Q}(\sqrt{-17})}(\alpha)| = N_{\mathbb{Q}(\sqrt{-17})}(\langle\alpha\rangle) = N_{\mathbb{Q}(\sqrt{-17})}(\mathfrak{p}_2) = 2$. Pero esto es una contradicción por lo demostrado en el apartado **(c)**.

(e) Factorizar los ideales $\langle p\rangle\mathcal{O}$ como producto de ideales primos de $\mathcal{O}$ para $p = 2, 3, 5$.
Solución: Sabemos 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 $K = \mathbb{Q}(\sqrt{-17})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-17}]$, $\theta = \sqrt{-17}$, $f_\theta(x) = x^2 + 17$.

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

  $$\langle 2\rangle\mathcal{O} = \langle 2, 1 + \sqrt{-17}\rangle^2 = \mathfrak{p}_2^2,$$

  con $\mathfrak{p}_2 = \langle 2, 1 + \sqrt{-17}\rangle$ ideal primo de $\mathcal{O}$.
- $p = 3$: Tenemos $f_\theta(x) \equiv (x+1)(x-1) \pmod 3$, por lo tanto

  $$\langle 3\rangle\mathcal{O} = \langle 3, 1 + \sqrt{-17}\rangle\langle 3, 1 - \sqrt{-17}\rangle = \mathfrak{p}_3\mathfrak{q}_3,$$

  con $\mathfrak{p}_3 = \langle 3, 1 + \sqrt{-17}\rangle$ y $\mathfrak{q}_3 = \langle 3, 1 - \sqrt{-17}\rangle$ ideales primos de $\mathcal{O}$.
- $p = 5$: Tenemos $f_\theta(x) \equiv x^2 + 2 \pmod 5$, que es irreducible en $\mathbb{F}_5[x]$ por lo tanto $\langle 5\rangle\mathcal{O} = \mathfrak{p}_5$ es un ideal primo de $\mathcal{O}$.

(f) Demostrar que todo ideal de $\mathcal{O}$ es equivalente, en el grupo de clases de $\mathcal{O}$, a uno de los ideales que aparecen en la factorización del apartado anterior.
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

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

En nuestro caso $K = \mathbb{Q}(\sqrt{-17})$ por lo tanto $n = 2$, $t = 1$ y $\Delta_{\mathbb{Q}(\sqrt{-17})} = -68$. Con lo que obtenemos $M_{\mathbb{Q}(\sqrt{-17})} = 5'2$. Así todo ideal de $\mathcal{O}$ es equivalente a uno de norma ≤ 5.
Sabemos que para todo ideal I de $\mathcal{O}$ se tiene $N_{\mathbb{Q}(\sqrt{-17})}(I) \in I$. Por lo tanto $\langle N_{\mathbb{Q}(\sqrt{-17})}(I)\rangle \subset I$, es decir, I aparece en la factorización del ideal $\langle N_{\mathbb{Q}(\sqrt{-17})}(I)\rangle$. Así que hemos de calcular la factorización de los ideales generados por $1, 2, 3, 4, 5$. Utilizando el apartado **(e)**:

- 1: $I = \mathcal{O}$.
- 2: $\langle 2\rangle\mathcal{O} = \mathfrak{p}_2^2$ con $N_{\mathbb{Q}(\sqrt{-17})}(\mathfrak{p}_2) = 2$ ya que $N_{\mathbb{Q}(\sqrt{-17})}(2) = 4$. Así $I = \mathfrak{p}_2$.
- 3: $\langle 3\rangle\mathcal{O} = \mathfrak{p}_3\mathfrak{q}_3$ con $N_{\mathbb{Q}(\sqrt{-17})}(\mathfrak{p}_3) = N_{\mathbb{Q}(\sqrt{-17})}(\mathfrak{q}_3) = 3$ ya que $N_{\mathbb{Q}(\sqrt{-17})}(3) = 9$. Así $I = \mathfrak{p}_3$ ó $I = \mathfrak{q}_3$..
- 4: $\langle 4\rangle\mathcal{O} = \mathfrak{p}_2^4$. Así $I = \langle 2\rangle\mathcal{O}$ que es principal y por lo tanto equivalente a $\mathcal{O}$.
- 5: $\langle 5\rangle\mathcal{O} = \mathfrak{p}_5$ por lo tanto $N_{\mathbb{Q}(\sqrt{-17})}(\mathfrak{p}_5) = N_{\mathbb{Q}(\sqrt{-17})}(5) = 25$. Por lo tanto no hay ideales de norma 5.

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

$$\mathcal{O}, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{q}_3.$$

(g) Encontrar todos los ideales de $\mathcal{O}$ de norma 30.
Solución: Hemos visto en el apartado anterior que si I es un ideal de norma 30 entonces I factoriza al ideal $\langle 30\rangle\mathcal{O}$, cuya factorización es:

$$\langle 30\rangle = \langle 2\rangle\langle 3\rangle\langle 5\rangle = \mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{q}_3\mathfrak{p}_5.$$

Pero ningún factor del ideal $\langle 30\rangle$ tiene norma 30.

Por lo tanto no hay ideales de $\mathcal{O}$ de norma 30.

(h) Encontrar todos los ideales de $\mathcal{O}$ que contienen al elemento 6. Y al 17.
Solución: Sea I un ideal de $\mathcal{O}$ tal que $6 \in I$, entonces $\langle 6\rangle\mathcal{O} \subset I$. Por lo tanto I es cualquier ideal que aparece en la factorización de $\langle 6\rangle\mathcal{O}$. Tenemos

$$\langle 6\rangle = \langle 2\rangle\langle 3\rangle = \mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{q}_3.$$

Por lo tanto $I \in \{\mathcal{O}, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{q}_3, \mathfrak{p}_2^2, \mathfrak{p}_2\mathfrak{p}_3, \mathfrak{p}_2\mathfrak{q}_3, \mathfrak{p}_3\mathfrak{q}_3, \mathfrak{p}_2^2\mathfrak{p}_3, \mathfrak{p}_2^2\mathfrak{q}_3, \mathfrak{p}_2\mathfrak{p}_3\mathfrak{q}_3, \mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{q}_3 = \langle 6\rangle\mathcal{O}\}$.
Para el caso de 17 hemos de descomponer el ideal $\langle 17\rangle\mathcal{O}$. Como $f_{\sqrt{-17}}(x) \equiv x^2 \pmod{17}$, por lo tanto

$$\langle 17\rangle\mathcal{O} = \langle 17, \sqrt{-17}\rangle^2 = \langle\sqrt{-17}\rangle^2 = \mathfrak{p}_{17}^2,$$

Si I es un ideal de $\mathcal{O}$ tal que $17 \in I$ entonces $I \in \{\mathcal{O}, \mathfrak{p}_{17}, \mathfrak{p}_{17}^2 = \langle 17\rangle\mathcal{O}\}$.

(i) Calcular el número de clase de $\mathbb{Q}(\sqrt{-17})$.
Solución: Hemos obtenido en el apartado **(f)** que cualquier ideal de $\mathcal{O}$ es equivalente a uno de los siguientes: $\mathcal{O}$, $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{q}_3$. Veamos en primer lugar que $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{q}_3$ no son equivalentes a $\mathcal{O}$. Para ello basta con ver que si $\mathfrak{p}$ es cualquiera de estos tres ideales, entonces no es principal. Sea $\alpha \in \mathcal{O}$ tal que $\langle\alpha\rangle\mathcal{O} = \mathfrak{p}$, entonces $|N_{\mathbb{Q}(\sqrt{-17})}(\alpha)| = N_{\mathbb{Q}(\sqrt{-17})}(\mathfrak{p}) = 2$ ó 3. Pero hemos visto en el apartado **(c)** que no hay elementos de norma 2 ni 3. Por lo tanto ninguno de estos ideales es equivalente a $\mathcal{O}$. Así obtenemos

$$2 \leq h_{\mathbb{Q}(\sqrt{-17})} \leq 4.$$

Veamos que $\mathfrak{p}_2$ no es equivalente a $\mathfrak{p}_3$. Si $\mathfrak{p}_2 \sim \mathfrak{p}_3$, entonces $\mathfrak{p}_2^2 = \langle 2\rangle\mathcal{O} \sim \mathfrak{p}_2\mathfrak{p}_3$. Así se tendría que $\mathfrak{p}_2\mathfrak{p}_3$ es principal. Sea $\alpha \in \mathcal{O}$ tal que $\langle\alpha\rangle\mathcal{O} = \mathfrak{p}_2\mathfrak{p}_3$, entonces $|N_{\mathbb{Q}(\sqrt{-17})}(\alpha)| = N_{\mathbb{Q}(\sqrt{-17})}(\mathfrak{p}_2\mathfrak{p}_3) = N_{\mathbb{Q}(\sqrt{-17})}(\mathfrak{p}_2)N_{\mathbb{Q}(\sqrt{-17})}((\mathfrak{p}_3) = 2 \cdot 3 = 6$. De forma análogo al apartado **(c)** se demuestra que no hay elementos de norma 6. Por lo tanto $\mathfrak{p}_2 \nsim \mathfrak{p}_3$, de forma análoga $\mathfrak{p}_2 \nsim \mathfrak{q}_3$. Así:

$$3 \leq h_{\mathbb{Q}(\sqrt{-17})} \leq 4.$$

Utilizando que $\langle 2\rangle\mathcal{O} = \mathfrak{p}_2^2$ se tiene que $[\mathfrak{p}_2]$ tiene orden 2 en $\mathcal{H}_{\mathbb{Q}(\sqrt{-17})}$. Así que $2|h_{\mathbb{Q}(\sqrt{-17})}$. Concluyendo

$$h_{\mathbb{Q}(\sqrt{-17})} = 4$$

De aquí se deduce que $\mathfrak{p}_3 \nsim \mathfrak{q}_3$

(j) Determinar la estructura del grupo de clase de $\mathbb{Q}(\sqrt{-17})$.
Solución: Hemos visto que el orden de $\mathcal{H}_{\mathbb{Q}(\sqrt{-17})}$ es 4. Por lo tanto

$$\mathcal{H}_{\mathbb{Q}(\sqrt{-17})} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \text{ó} \quad \mathbb{Z}/4\mathbb{Z}.$$

En el apartado **(f)** vimos que $\langle 3\rangle\mathcal{O} = \mathfrak{p}_3\mathfrak{q}_3$ y en el **(i)** hemos obtenido $\mathfrak{p}_3 \nsim \mathfrak{q}_3$ por lo tanto el orden de $[\mathfrak{p}_3]$ es mayor que 2 y es par ya que $h_{\mathbb{Q}(\sqrt{-17})} = 4$ por lo tanto ha de ser 4. Así que concluimos

$$\mathcal{H}_{\mathbb{Q}(\sqrt{-17})} \simeq \quad \mathbb{Z}/4\mathbb{Z}\,.$$

(2) Determinar las soluciones enteras de la ecuación diofántica $C : y^2 + 17 = x^3$.
Solución: Factorizando C obtenemos $(y+\sqrt{-17})(y-\sqrt{-17}) = x^3$. Esto indica que hemos de trabajar sobre el cuerpo cuadrática $\mathbb{Q}(\sqrt{-17})$ cuyo anillo de enteros es $\mathcal{O} = \mathbb{Z}[\sqrt{-17}]$.

Vamos a trabajar con ideales. Sea $\mathfrak{p} \subset \mathbb{Z}[\sqrt{-17}]$ ideal primo tal que $\mathfrak{p}$ divide a $\langle y + \sqrt{-17}\rangle$ y a $\langle y - \sqrt{-17}\rangle$. entonces dividirá a la resta: $\langle 2\sqrt{-17}\rangle = {\mathfrak{p}_2}^2\mathfrak{p}_{17}$. Así $\mathfrak{p} = \mathfrak{p}_2$ ó $\mathfrak{p} = \mathfrak{p}_{17}$.

Supongamos $\mathfrak{p} = \mathfrak{p}_2$, entonces $\mathfrak{p}^2 \,|\, \langle y + \sqrt{-17}\rangle\langle y - \sqrt{-17}\rangle = \langle x^3\rangle = \langle x\rangle^3$. Por lo tanto $2|x$. Es decir, $x \equiv 0 \,(\mathrm{mod}\ 2)$ y mirando en la ecuación obtenemos $y \equiv 1 \,(\mathrm{mod}\ 2)$. Ahora mirando la ecuación módulo 4 se tendría $2 \equiv 0 \,(\mathrm{mod}\ 4)$. Así que $\mathfrak{p} = \mathfrak{p}_{17}$.

Tenemos $\langle y+\sqrt{-17}\rangle = \mathfrak{p}_{17}^k\mathfrak{q}$ donde $\mathfrak{q} \subset \mathcal{O}$ ideal primo con $\mathfrak{p}_7$. Conjugando obtenemos $\langle y-\sqrt{-17}\rangle = \overline{\mathfrak{p}}_{17}^k\overline{\mathfrak{q}} = \mathfrak{p}_{17}^k\overline{\mathfrak{q}}$ ya que $\overline{\mathfrak{p}}_{17} = \mathfrak{p}_{17}$. Como el único ideal primo que puede dividir a $\langle y + \sqrt{-17}\rangle$ y a $\langle y - \sqrt{-17}\rangle$ es $\mathfrak{p}_{17}$, tenemos que $\mathfrak{q}$ y $\overline{\mathfrak{q}}$ son primos entre si. Así que tenemos

$$\langle x\rangle^3 = \langle y + \sqrt{-17}\rangle\langle y - \sqrt{-17}\rangle = \mathfrak{p}_{17}^{2k}\mathfrak{q}\overline{\mathfrak{q}}.$$

Utilizando que hay factorización única en ideales de $\mathcal{O}$ tenemos

$$\begin{cases} 2k \equiv 0 \,(\mathrm{mod}\ 3) \quad \text{es decir, } k \equiv 0 \,(\mathrm{mod}\ 3) \\ \mathfrak{q} = \mathfrak{r}^3, \quad \text{donde } \mathfrak{r} \subset \mathcal{O} \text{ ideal.} \end{cases}$$

Agrupando tenemos que existe un ideal $\mathfrak{s} \subset \mathcal{O}$ tal que $\langle y + \sqrt{-17}\rangle = \mathfrak{s}^3$. Por lo tanto el orden de $[\mathfrak{s}]$ en $\mathcal{H}_{\mathbb{Q}(\sqrt{-17})}$ divide a 3. Por otro lado dicho orden ha de dividir a $h_{\mathbb{Q}(\sqrt{-17})} = 4$. Así obtenemos que $\mathfrak{s}$ es principal, por lo tanto existe $\alpha = a + b\sqrt{-17} \in \mathcal{O}$ tal que $\langle y + \sqrt{-17}\rangle = \langle \alpha^3\rangle$. Con lo que tenemos

$$y + \sqrt{-17} = u(a + b\sqrt{-17})^3 \qquad \text{donde } u \in \mathcal{U}(\mathcal{O}) = \{\pm 1\}.$$

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

$$\begin{cases} y &= a^3 - 51ab^2 \\ 1 &= b(3a^2 - 17b^2) \end{cases}$$

De la segunda ecuación obtenemos que o bien $b = 1$ y $3a^2 - 17b^2 = 1$, o bien $b = -1$ y $3a^2 - 17b^2 = -1$. Es decir, $a^2 = 6$ ó $3a^2 = 16$. Pero entonces $a \notin \mathbb{Z}$. Por lo tanto este sistema no tiene solución. Asi que nuestra ecuación diofántica no tiene soluciones enteras. Es decir:

$$C(\mathbb{Z}) = \emptyset\,.$$