30 de Enero 2007 (SOLUCIONES)

(1) (a) Factorizar los enteros 127 **y** 173**.**

Soluciones: Sea $n \in \mathbb{N}$, entonces obsérvese que cualquier factor primo p de n ha de cumplir $p \leq \sqrt{n}$. Por lo tanto en nuestro caso hemos de buscar primos $p \leq \sqrt{127} = 11'2$ ó $p \leq \sqrt{173} = 13'1$. Se comprueba que para $p = 2, 3, 5, 7, 11, 13$, $p \nmid 127, 173$. Por lo tanto ambos números son primos.

(b) Calcular $\left(\frac{127}{173}\right)$**.**

Soluciones: Vamos a utilizar la *Ley de reciprocidad cuadrática* que nos dice que si p y q son primos, entonces

$$\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1))}{4}} \left(\frac{p}{q}\right).$$

Aplicada a nuestro caso, $q = 127$ y $p = 173$ obtenemos:

$$\left(\frac{127}{173}\right) = (-1)^{5418} \left(\frac{173}{127}\right) = \left(\frac{173}{127}\right) = \clubsuit,$$

utilizando que el símbolo de Legendre $\left(\frac{a}{p}\right)$ sólo depende de a módulo p y que es multiplicativo obtenemos

$$\clubsuit = \left(\frac{46}{127}\right) = \left(\frac{2}{127}\right)\left(\frac{23}{127}\right) = \clubsuit_2\,.$$

Ahora aplicando la segunda ley suplementaria que nos dice $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ y de nuevo la ley de reciprocidad cuadrática varias veces tenemos

$$\clubsuit_2 = (-1)^{2016} \cdot (-1)^{693} \left(\frac{127}{23}\right) = (-1)\left(\frac{12}{23}\right) = (-1)\left(\frac{4}{23}\right)\left(\frac{3}{23}\right) = (-1)(-1)^{11}\left(\frac{2}{3}\right) = -1.$$

Así concluimos:

$$\left(\frac{127}{173}\right) = -1\,.$$

(2) Calcular todas las soluciones enteras y racionales de las ecuaciones:

(a) $x^2 + y^2 = 2$**.**

Solución: Primero busquemos las soluciones enteras. Sea $y = 0$, entonces $x^2 = 2$, entonces $x \notin \mathbb{Z}$. Sea $y = \pm 1$, entonces $x = \pm 1$. Sea $|y| > 1$, entonces $x^2 = 2 - y^2 < 0$, por lo tanto $x \notin \mathbb{Z}$. Así que tenemos

$$C(\mathbb{Z}) = \{(1,1), (1,-1), (-1,1), (-1,-1)\}.$$

Ahora vamos a calcular las soluciones racionales. Para ello vamos a utilizar el método geométrico. Es decir, vamos a tomar el punto $(1,1) \in C(\mathbb{Q})$ y la recta que pasa por él con pendiente racional.

Así obtendremos una parametrización de los puntos de $C(\mathbb{Q})$. La recta que pasa por $(1,1)$ con pendiente t es $R : y - 1 = t(x-1)$. La intersección de esta recta con nuestra circunferencia es:

$$C \cap R : \begin{cases} x^2 + y^2 = 2 \\ y - 1 = t(x-1) \end{cases}$$

Sustituyendo la segunda ecuación en la primera obtenemos:

$$x = \frac{t(t-1) \pm (t+1)}{t^2+1} = \begin{cases} 1 \\ \dfrac{t^2 - 2t - 1}{t^2+1} \end{cases}$$

Así concluimos:

$$C(\mathbb{Q}) = \left\{ \left(\frac{t^2-2t-1}{t^2+1}, \frac{-t^2-2t+1}{t^2+1} \right) \,:\, t \in \mathbb{Q} \cup \{\infty\} \right\}.$$

(b) $x^2 + y^2 = 3$**.**
Solución: Sea $(x,y) \in C(\mathbb{Q})$, entonces podemos encontrar $X, Y, Z \in \mathbb{Z}$ primos entre si tales que $x = X/Z$ e $y = Y/Z$. Por lo tanto la ecuación C en las coordenadas enteras (X,Y,Z) es:

$$X^2 + Y^2 = 3Z^2 .$$

Pasandolo a módulo 3 tenemos

$$X^2 + Y^2 \equiv 0 \,(\text{mod } 3) .$$

Ahora, los cuadrado módulo 3 son $\{0,1\}$ así que la única posibilidad es que $X, Y \equiv 0 \,(\text{mod } 3)$. Es decir, $X = 3r, Y = 3s$. Sustituyendo en la ecuación obtenemos

$$9r^2 + 9s^2 = 3Z^2 .$$

Por lo tanto se tiene que $Z \equiv 0 \,(\text{mod } 3)$. Así que $3|(X,Y,Z)$. Pero esto contradice la hipótesis $(X,Y,Z) = 1$.
Conclusión:

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

(3) Calcular una solución entera de la ecuación diofántica $C : x^2 + 37y^2 = 1558$**.**
Solución 1: Factorizando ambos lados obtenemos $(x + y\sqrt{-37})(x - y\sqrt{-37}) = 1558 = 38 \cdot 41$. Busquemos $\alpha, \beta \in \mathbb{Z}[\sqrt{-37}]$ tales que $N_{\mathbb{Q}(\sqrt{-37})}(\alpha) = 38$ y $N_{\mathbb{Q}(\sqrt{-37})}(\beta) = 41$. Entonces

$$N_{\mathbb{Q}(\sqrt{-37})}(\alpha\beta) = N_{\mathbb{Q}(\sqrt{-37})}(\alpha) \cdot N_{\mathbb{Q}(\sqrt{-37})}(\beta) = 38 \cdot 41 = 1558.$$

Por lo tanto

$$C(\mathbb{Z}) = \{(x,y) \in \mathbb{Z} \,|\, x + y\sqrt{-37} = \alpha\beta \text{ tal que } N_{\mathbb{Q}(\sqrt{-37})}(\alpha) = 38,\, N_{\mathbb{Q}(\sqrt{-37})}(\beta) = 41\}.$$

Sea $\alpha = a + b\sqrt{-37}$, con $a, b \in \mathbb{Z}$ entonces $N_{\mathbb{Q}(\sqrt{-37})}(\alpha) = a^2 + 37b^2$. Así si buscamos α de norma 38 (resp. 41) hemos de resolver la ecuación diofántica

$$a^2 + 37b^2 = 38 \text{ (resp 41)}.$$

Sea $b = 0$, entonces $a^2 = 38$ (resp. $a^2 = 42$), entonces $a \notin \mathbb{Z}$. Sea $|b| = 1$ entonces $a^2 = 1$ (resp. $a^2 = 4$). Así obtenemos $a = \pm 1$ (resp. $a = \pm 2$). Si $|b| > 1$, entonces $a^2 = 38 - 37b^2 < 0$ (resp. $a^2 = 41 - 37b^2 < 0$), es decir, $a \notin \mathbb{Z}$. Por lo tanto las soluciones son:

$$\alpha = \pm 1 \pm \sqrt{-37} \quad \text{y} \quad \beta = \pm 2 \pm \sqrt{-37} .$$

Entonces

$$C(\mathbb{Z}) = \{(\pm 35, \pm 3), (\pm 39, \pm 1)\}.$$

Solución 2: En primer lugar obsérvese que $|y| \leq 6$ ya que de lo contrario $x^2 = 1558 - 37y^2 < 0$. Por otro lado si reducimos la ecuación módulo 37 obtenemos $x^2 \equiv 4 \pmod{37}$. Así que existirá un $k \in \mathbb{Z}$ tal que $x^2 = 4 + 37k$. Sustituyendo esto en nuestra ecuación tenemos $4 + 37k + 37y^2 = 1558$. O lo que es lo mismo $37(k + y^2) = 1554$. Ahora se tiene $1554 = 37 \cdot 42$. Así que nuestra ecuación diofántica se trasforma en para que valores de $y \in \mathbb{Z}$ con $|y| \leq 6$ se tiene que $4 + 37(42 - y^2)$ es un cuadrado en $\mathbb{Z}$. Se comprueba que los únicos valores son $|y| = 1, 3$ que nos dan $|x| = 39, 35$ respectivamente.

Por lo tanto:

$$C(\mathbb{Z}) = \{(\pm 35, \pm 3), (\pm 39, \pm 1)\}.$$

(4) (a) Calcular la estructura del grupo de clase del cuerpo cuadrático $\mathbb{Q}(\sqrt{19})$.

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 $K = \mathbb{Q}(\sqrt{19})$ es un cuerpo cuadrático ($n = 2$) real ($t = 0$) con $d = 19$ libre de cuadrados tal que $d \not\equiv 1 \pmod{4}$. Por lo tanto $\mathcal{O}_{\mathbb{Q}(\sqrt{19})} = \mathbb{Z}[\theta]$ con $\theta = \sqrt{19}$, $f_\theta(x) = x^2 + 19$ el polinomio mínimo de θ y $\Delta_{\mathbb{Q}(\sqrt{19})} = 4 \cdot 19$. Así obtenemos $M_{\mathbb{Q}(\sqrt{19})} = 4'35$. Así todo ideal de $\mathcal{O}_{\mathbb{Q}(\sqrt{19})}$ es equivalente a uno de norma ≤ 4.
Sabemos que para todo ideal I de $\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\sqrt{19})}$ se tiene $N_{\mathbb{Q}(\sqrt{19})}(I) \in I$. Por lo tanto $\langle N_{\mathbb{Q}(\sqrt{19})}(I)\rangle \subset I$, es decir, I aparece en la factorización del ideal $\langle N_{\mathbb{Q}(\sqrt{19})}(I)\rangle$. 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 $\theta = \sqrt{19}$, $f_\theta(x) = x^2 + 19$:

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

$$\langle 2\rangle\mathcal{O} = \left\langle 2, 1 + \sqrt{19}\right\rangle^2 = \mathfrak{p}_2^2,$$

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

$$4 = N_{\mathbb{Q}(\sqrt{19})}(2) = N_{\mathbb{Q}(\sqrt{19})}(\langle 2\rangle\mathcal{O}) = N_{\mathbb{Q}(\sqrt{19})}(\mathfrak{p}_2)^2.$$

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

$$\langle 3\rangle\mathcal{O} = \left\langle 3, 1 + \sqrt{19}\right\rangle \left\langle 3, 1 - \sqrt{19}\right\rangle = \mathfrak{p}_3\overline{\mathfrak{p}}_3,$$

  con $\mathfrak{p}_3$ y $\overline{\mathfrak{p}}_3$ ideales primos de $\mathcal{O}$ de norma 3. Ya que

$$9 = N_{\mathbb{Q}(\sqrt{19})}(3) = N_{\mathbb{Q}(\sqrt{19})}(\langle 3\rangle\mathcal{O}) = N_{\mathbb{Q}(\sqrt{19})}(\mathfrak{p}_3)N_{\mathbb{Q}(\sqrt{19})}(\overline{\mathfrak{p}}_3).$$

Por lo tanto tenemos que si I es un ideal de $\mathcal{O}$ de norma $1, 2, 3$ ó 4 ha de ser:

- 1: $I = \mathcal{O}$.
- 2: $I = \mathfrak{p}_2$.
- 3: $I = \mathfrak{p}_3$ ó $I = \overline{\mathfrak{p}}_3$..
- 4: $\langle 4 \rangle = \mathfrak{p}_2^4$. Así $I = \mathfrak{p}_2^2 = \langle 2 \rangle$. Como $\langle 2 \rangle$ es principal, es equivalente a $\mathcal{O}$. Así $I \sim \mathcal{O}$.

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

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

Por lo tanto el número de clase es menor o igual a 4, es decir:

$$h_{\mathbb{Q}(\sqrt{19})} \leq 4\,.$$

Sea $\mathfrak{p}$ un ideal de $\mathcal{O}$ de norma n. Si $\mathfrak{p} \sim \mathcal{O}$, entonces es principal. Es decir, existirá $\alpha = a + b\sqrt{19} \in \mathcal{O}$ tal que $\mathfrak{p} = \langle \alpha \rangle \mathcal{O}$ y por lo tanto $n = N_{\mathbb{Q}(\sqrt{19})}(\mathfrak{p}) = |N_{\mathbb{Q}(\sqrt{19})}(\alpha)| = |a^2 - 19b^2|$. Veamos si existen elementos de norma ± 2 y ± 3:

- $n = \pm 2$: $\alpha = \pm 13 \pm 3\sqrt{19}$ tiene $N_{\mathbb{Q}(\sqrt{19})}(\alpha) = -2$.
- $n = \pm 3$: $\beta = \pm 4 \pm \sqrt{19}$ tiene $N_{\mathbb{Q}(\sqrt{19})}(\beta) = -3$.

Se comprueba que $\mathfrak{p}_2 = \langle 13 + 3\sqrt{19} \rangle \mathcal{O}$ y $\mathfrak{p}_3 = \langle 4 + \sqrt{19} \rangle \mathcal{O}$.
Por lo tanto,

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

Concluimos con $h_{\mathbb{Q}(\sqrt{19})} = 1$. Por lo tanto $\mathcal{H}_{\mathbb{Q}(\sqrt{19})}$ es el grupo trivial, es decir

$$\mathcal{H}_{\mathbb{Q}(\sqrt{19})} \cong \{\mathcal{O}\}.$$

(b) Determinar si $\mathcal{O}_{\mathbb{Q}}(\sqrt{19})$ es un DFU.
Solución: Hemos demostrado en el apartado anterior que $\mathcal{O} = \mathbb{Z}[\sqrt{19}]$ es un DIP, ya que $h_{\mathbb{Q}(\sqrt{19})} = 1$. Por lo tanto $\mathcal{O} = \mathbb{Z}[\sqrt{19}]$ es un DFU.