Septiembre 2007 (SOLUCIONES)

(1) Sea $p \in \mathbb{Z}$ un primo impar. Demostrar que la ecuación diofántica $C : x^2 + y^2 = p$ tiene infinitas soluciones racionales si y sólo si $p \equiv 1 \pmod 4$.

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:

$$X^2 + Y^2 = pZ^2 .$$

Pasandolo a módulo p tenemos

$$X^2 + Y^2 \equiv 0 \pmod p .$$

Supongamos $X, Y \equiv 0 \pmod p$. Es decir $p|X, Y$. Por lo tanto $p^2|X^2, Y^2$. De lo que se obtiene $p^2|X^2 + Y^2 = p^2 Z$. Por lo tanto, $p|Z$. Así que $p|(X, Y, Z)$. Pero esto contradice la hipótesis $(X, Y, Z) = 1$.

Así que podemos suponer $Y \not\equiv 0 \pmod p$. Por lo tanto existe el inverso de Y módulo p. Así que la ecuación inicial módulo p es equivalente a:

$$\left(\frac{X}{Y}\right)^2 + 1 \equiv 0 \pmod p .$$

Por lo tanto -1 es un residuo cuadrático módulo p. Es decir:

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

Utilizando la primera ley suplementaria que nos dice:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}},$$

obtenemos $p \equiv 1 \pmod 4$.

(2) Encontrar los últimos dos digitos de 3^{1000}.

Solución: Hemos de calcular $3^{1000} \pmod{100}$. Es decir, hemos de encontrar $x \in \{0, \ldots, 99\}$ tal que $x \equiv 3^{1000} \pmod{100}$. Sea ϕ la función de Euler, entonces $\phi(100) = \phi(4)\phi(25) = 2 \cdot 20 = 40$. Como $(3, 100) = 1$ el Teorema de Euler-Fermat nos asegura $3^{\phi(100)} \equiv 1 \pmod{100}$. Por otro lado $1000 = 40 \cdot 25$, por lo tanto

$$3^{1000} = (3^{40})^{25} \equiv (1)^{25} \equiv 1 \pmod{100}.$$

Conclusión: Los últimos dos digitos son 01.

(3) Encontrar para que valores de $n \in \mathbb{Z}$, $n > 0$ se tiene que $2^{2n} + 5$ es primo.
Solución: En primer lugar obsérvese que $2 \equiv -1 \pmod 3$. Por lo tanto

$$2^{2n} + 5 \equiv (-1)^{2n} + 5 \equiv 0 \pmod 3$$

Así que 3 divide a $2^{2n} + 5$ para cualquier entero positivo n. Así que $2^{2n} + 5$ no es primo para ningún valor de n.

(4) Demostrar que la suma de tres cubos enteros consecutivos es divisible por 9.
Solución: Sea $n \in \mathbb{N}$ y $N = (n-1)^3+n^3+(n+1)^3$. Desarrollando obtenemos $N = 3n^3+6n = 3n(n^2+2)$. Ahora diferenciemos el caso en el que $3|n$ y $3 \nmid n$:

- $3|n$. Entonces $n = 3k$ para algún $k \in \mathbb{Z}$. Así $N = 9k(9k^2 + 2) \equiv 0 \pmod 9$. Es decir $9|N$.
- $3 \nmid n$. Entonces $n \equiv \pm 1 \pmod 3$. Por lo tanto $(n^2 + 2) \equiv 0 \pmod 3$. Y de forma análoga al caso anterior obtenemos que $9|N$.

(5) Calcular la estructura del grupo de clase del cuerpo cuadrático $\mathbb{Q}(\sqrt{-23})$.
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 $K = \mathbb{Q}(\sqrt{-23})$ es un cuerpo cuadrático ($n = 2$) imaginario ($t = 1$) con $d = -23$ libre de cuadrados tal que $d \equiv 1 \pmod 4$. Por lo tanto $\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\sqrt{-23})} = \mathbb{Z}[\theta]$ con $\theta = \frac{1+\sqrt{-23}}{2}$, $f_\theta(x) = x^2 - x + 6$ el polinomio mínimo de θ y $\Delta_{\mathbb{Q}(\sqrt{-23})} = -23$. Así obtenemos $M_{\mathbb{Q}(\sqrt{-23})} = 3'05$. Así todo ideal de $\mathcal{O}$ es equivalente a uno de norma ≤ 3.

Sabemos que para todo ideal I de $\mathcal{O}$ se tiene $N_{\mathbb{Q}(\sqrt{-23})}(I) \in I$. Por lo tanto $\langle N_{\mathbb{Q}(\sqrt{-23})}(I)\rangle \subset I$, es decir, I aparece en la factorización del ideal $\langle N_{\mathbb{Q}(\sqrt{-23})}(I)\rangle$. Así que hemos de calcular la factorización de los ideales generados por $1, 2, 3$. 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 $\theta = \frac{1+\sqrt{-23}}{2}$, $f_\theta(x) = x^2 - x + 6$:

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

$$\langle 2\rangle\mathcal{O} = \left\langle 2, \frac{1+\sqrt{-23}}{2}\right\rangle \left\langle 2, \frac{1-\sqrt{-23}}{2}\right\rangle = \mathfrak{p}_2\overline{\mathfrak{p}}_2,$$

  con $\mathfrak{p}_2, \overline{\mathfrak{p}}_2$ ideales primos de $\mathcal{O}$ de norma 2. Ya que

$$4 = N_{\mathbb{Q}(\sqrt{-23})}(2) = N_{\mathbb{Q}(\sqrt{-23})}(\langle 2\rangle\mathcal{O}) = N_{\mathbb{Q}(\sqrt{-23})}(\mathfrak{p}_2)N_{\mathbb{Q}(\sqrt{-23})}(\overline{\mathfrak{p}}_2).$$

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

$$\langle 3\rangle\mathcal{O} = \left\langle 3, \frac{1+\sqrt{-23}}{2}\right\rangle \left\langle 3, \frac{1-\sqrt{-23}}{2}\right\rangle = \mathfrak{p}_3\overline{\mathfrak{p}}_3,$$

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

$$9 = N_{\mathbb{Q}(\sqrt{-23})}(3) = N_{\mathbb{Q}(\sqrt{-23})}(\langle 3\rangle\mathcal{O}) = N_{\mathbb{Q}(\sqrt{-23})}(\mathfrak{p}_3)N_{\mathbb{Q}(\sqrt{-23})}(\overline{\mathfrak{p}}_3).$$

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

- 1: $I = \mathcal{O}$.
- 2: $I = \mathfrak{p}_2$ ó $I = \overline{\mathfrak{p}}_2$.
- 3: $I = \mathfrak{p}_3$ ó $I = \overline{\mathfrak{p}}_3$..

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

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

Por lo tanto el número de clase es menor o igual a 5, es decir:

$$h_{\mathbb{Q}(\sqrt{-23})} \leq 5\,.$$

Sea $\mathfrak{p}$ un ideal de $\mathcal{O}$ de norma n. Si $\mathfrak{p} \sim \mathcal{O}$, entonces es principal. Es decir, existirá $\alpha = \frac{a+b\sqrt{-23}}{2} \in \mathcal{O}$ tal que $\mathfrak{p} = \langle\alpha\rangle\mathcal{O}$ y por lo tanto $n = N_{\mathbb{Q}(\sqrt{-23})}(\mathfrak{p}) = N_{\mathbb{Q}(\sqrt{-23})}(\alpha) = \frac{a^2+23b^2}{4}$. Es decir $a^2 + 23b^2 = 4n$.
Veamos que no existen elementos en $\mathcal{O}$ de norma ± 2 (resp. ± 3). Como en este caso la norma es positiva basta con estudiar las soluciones enteras de $a^2 + 23b^2 = 8$ (resp. 12), entonces $b = 0$, ya que $a^2 = 8 - 23b^2 < 0$ (resp. $a^2 = 12 - 23b^2 < 0$) para $b \neq 0$. Pero si $a^2 = 8$ (resp. 12), $a \notin \mathbb{Z}$. Por lo tanto así hemos visto

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

Ahora veamos que relación en $\mathcal{H}_{\mathbb{Q}\sqrt{-23}}$ hay entre $\mathfrak{p}_2$ y $\overline{\mathfrak{p}}_2$. Si $\mathfrak{p}_2 \sim \overline{\mathfrak{p}}_2$ entonces como $\langle 2\rangle = \mathfrak{p}_2\overline{\mathfrak{p}}_2$ tendriamos $\mathfrak{p}_2^2 \sim \mathcal{O}$. Es decir que tenemos que encontrar $\alpha \in \mathcal{O}$ de norma 4. Análogamente a lo anterior se demuestra que los únicos elementos de norma 4 son $\alpha = \pm 2$. Pero entonces tendriamos que $\mathfrak{p}_2^2 = \langle 2\rangle$. Así tendriamos $\mathfrak{p}_2 = \overline{\mathfrak{p}}_2$ pero entonces $1 \in \mathfrak{p}_2$ ya que $1 = \frac{1+\sqrt{-23}}{2} + \frac{1-\sqrt{-23}}{2}$. De forma análoga para $\mathfrak{p}_3$ y $\overline{\mathfrak{p}}_3$. Así hemos visto

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

Así vemos que $h_{\mathbb{Q}(\sqrt{-23})} = 3$ ó 5.
Si vemos que $\mathfrak{p}_2 \sim \mathfrak{p}_3$ ó $\mathfrak{p}_2 \sim \overline{\mathfrak{p}}_3$ entonces se tendrá $h_{\mathbb{Q}(\sqrt{-23})} = 3$. En caso contrario $h_{\mathbb{Q}(\sqrt{-23})} = 5$.

Supongamos $\mathfrak{p}_2 \sim \overline{\mathfrak{p}}_3$, entonces $\mathfrak{p}_2\mathfrak{p}_3 \sim \mathcal{O}$, ya que $\mathfrak{p}_3\overline{\mathfrak{p}}_3 \sim \mathcal{O}$. Es decir que existe $\alpha = \frac{a+b\sqrt{-23}}{2} \in \mathcal{O}$ de norma 6 tal que $\mathfrak{p}_2\mathfrak{p}_3 = \langle\alpha\rangle\mathcal{O}$. Por lo tanto $a^2 + 23b^2 = 24$. Se tiene

$$\alpha = \frac{\pm 1 \pm \sqrt{-23}}{2}.$$

Por último se comprueba $\mathfrak{p}_2\mathfrak{p}_3 = \langle\frac{1+\sqrt{-23}}{2}\rangle\mathcal{O}$. Es decir $\mathfrak{p}_2 \sim \overline{\mathfrak{p}}_3$.

Conclusión: $h_{\mathbb{Q}(\sqrt{-23})} = 3$ y por lo tanto

$$\mathcal{H}_{\mathbb{Q}(\sqrt{-23})} \cong \mathbb{Z}/3\mathbb{Z}\,.$$

(6) Demostrar el primer caso del Último Teorema de Fermat para $p = 3$.

Solución: El primer caso del Último Teorema de Fermat para un primo impar p conjetura que la ecuación diofántica $x^p + y^p = z^p$ no tiene soluciones enteras tales que $xyz \neq 0$ y $p|xyz$. Vimos un resultado de Kummer que nos asegura que esta conjetura es cierta si p es un primo regular. Es decir, si $p \nmid h_{\mathbb{Q}(\zeta_p)}$.

En nuestro caso $p = 3$. Por lo tanto $\mathbb{Q}(\zeta_p) = \mathbb{Q}(\sqrt{-3})$. Así que hemos de calcular el número de clase de $\mathbb{Q}(\sqrt{-3})$. Por el Teorema de Heegner-Stark sabemos que $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ es un DIP (o bien utilizando la cota de Minkowski ya que $\mathbb{Q}(\sqrt{-3})$ es un cuerpo cuadrática ($n = 2$) imaginario ($t = 1$) con discriminante -3, ya que $-3 \equiv 1 \,(\mathrm{mod}\ 4)$ y por lo tanto $M_{\mathbb{Q}(\sqrt{-3})} = 1{,}1$). Por lo tanto $h_{\mathbb{Q}(\sqrt{-3})} = 1$. Es decir, $3 \nmid h_{\mathbb{Q}(\zeta_3)} = h_{\mathbb{Q}(\sqrt{-3})} = 1$. Utilizando el anterior resultado de Kummer se demuestra el primer caso del Último Teorema de Fermat para $p = 3$.