# 8 Septiembre 2008 (SOLUCIONES)

1. **Demostrar que hay infinitos primos congruentes con 4 módulo 5.**
*Solución:* Supongamos que hay un número finito. Sean dichos primos $p_1, \ldots, p_r$. Sea

$$N = 25(p_1 \cdots p_r)^2 - 5.$$

Entonces para cualquier divisor primo $p \neq 5$ de $N$ se tiene $\left(\frac{5}{p}\right) = 1$. Por lo tanto utilizando la ley de reciprocidad cuadrática obtenemos que $p \equiv 1, 4 \pmod 5$. Como $p \neq 5$, entonces $p | 5(p_1 \cdots p_r)^2 - 1$. Por lo tanto no todos los divisores primos de $N$ pueden ser congruentes con 1 módulo 5 ya que de lo contrario se tendría $-1 \equiv 1 \pmod 5$. Por lo tanto hay un primo $p \equiv 4 \pmod 5$ que divide a $5(p_1 \cdots p_r)^2 - 1$. Pero $p$ es distinto a $p_1, \ldots, p_r$ ya que si no, $p|1$. Esto contradice la suposición de que hay un número finito de primos congruentes con 4 módulo 5.

2. **Demostrar que si hay un número finito de primos de Fermat entonces hay un número finito de primos de la forma $2^n + 1$ con $n \in \mathbb{N}$.**
*Solución:* Es suficiente con ver que si $2^n + 1$ es primo, entonces es un primo de Fermat. Es decir, $n = 2^m$ para algún $m \in \mathbb{N}$. Supongamos que $n$ tiene un divisor impar $r$. Entonces $n = rs$ y $2^s + 1$ divide a $2^{rs} + 1$ ya que

$$2^{rs} + 1 = (2^s + 1) \sum_{k=0}^{r-1} (-2^s)^k.$$

3. **Sea $d < 0$ un entero libre de cuadrados y $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ el anillo de enteros del cuerpo cuadrático imaginario $\mathbb{Q}(\sqrt{d})$. Determinar $\mathcal{U}(\mathcal{O}_{\mathbb{Q}(\sqrt{d})})$, tanto sus elementos como su estructura como grupo, así como sus generadores.**
*Solución:* En primer lugar recuérdese que $u \in \mathcal{U}(\mathcal{O}_{\mathbb{Q}(\sqrt{d})})$ si y sólo si $\mathcal{N}_{\mathbb{Q}(\sqrt{d})}(u) = \pm 1$. Ahora, distinguiremos dos casos. Cuando $d \equiv 1 \pmod 4$ y cuando $d \not\equiv 1 \pmod 4$:
• $d \not\equiv 1\, (mod 4)$: En este caso, $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}]$. Sea $u = a + b\sqrt{d} \in \mathcal{U}(\mathcal{O}_{\mathbb{Q}(\sqrt{d})})$ entonces hemos de estudiar las soluciones a la ecuación

$$\mathcal{N}_{\mathbb{Q}(\sqrt{d})}(u) = \pm 1 \iff a^2 - db^2 = \pm 1 \overset{d<0}{\iff} a^2 - db^2 = 1 \quad a, b \in \mathbb{Z}$$

Veamos que ocurre dependiendo del valor de $d$:

- $d = -1$: $a^2 + b^2 = 1$ con $a, b \in \mathbb{Z}$. Las únicas posibilidades son $b = 0$ (por lo tanto $a = \pm 1$) ó $b = \pm 1$ (por lo tanto $a = 0$). Así la estructura de grupo es:

$$\mathcal{U}(\mathcal{O}_{\mathbb{Q}(\sqrt{-1})}) = \{\pm 1, \pm\sqrt{-1}\} \cong \langle \sqrt{-1} \rangle \cong \mathbb{Z}/4\mathbb{Z}\,.$$

- $d = -e$ con $e > 1$: $a^2 + eb^2 = 1$ con $a, b \in \mathbb{Z}$. La única posibilidad es $b = 0$ y por lo tanto $a = \pm 1$. Así la estructura de grupo es:

$$\mathcal{U}(\mathcal{O}_{\mathbb{Q}(\sqrt{d})}) = \{\pm 1\} \cong \langle -1 \rangle \cong \mathbb{Z}/2\mathbb{Z}\,.$$

• $d \equiv 1\,(mod 4)$*:* En este caso, $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Sea $u = \frac{a+b\sqrt{d}}{2} \in \mathcal{U}(\mathcal{O}_{\mathbb{Q}(\sqrt{d})})$ entonces hemos de estudiar las soluciones a la ecuación

$$\mathcal{N}_{\mathbb{Q}(\sqrt{d})}(u) = \pm 1 \Longleftrightarrow \frac{a^2 - db^2}{4} = \pm 1 \overset{d<0}{\Longleftrightarrow} a^2 - db^2 = 4 \quad a, b \in \mathbb{Z}$$

Veamos que ocurre dependiendo del valor de $d$:

- $d = -3$: $a^2 + 3b^2 = 4$ con $a, b \in \mathbb{Z}$. Las únicas posibilidades son $b = 0$ (por lo tanto $a = \pm 2$) ó $b = \pm 1$ (por lo tanto $a = \pm 1$). Así la estructura de grupo es:

$$\mathcal{U}(\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}) = \left\{ \pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2} \right\} \cong \langle \frac{1+\sqrt{-3}}{2} \rangle \cong \mathbb{Z}/6\mathbb{Z}\,.$$

- $d = -e$ con $e > 3$: $a^2 + eb^2 = 4$ con $a, b \in \mathbb{Z}$. La única posibilidad es $b = 0$ y por lo tanto $a = \pm 2$. Así la estructura de grupo es:

$$\mathcal{U}(\mathcal{O}_{\mathbb{Q}(\sqrt{d})}) = \{\pm 1\} \cong \langle -1 \rangle \cong \mathbb{Z}/2\mathbb{Z}\,.$$

*Conclusión:* Sea $d < 0$ un entero libre de cuadrados y $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ el anillo de enteros del cuerpo cuadrático imaginario $\mathbb{Q}(\sqrt{d})$. Entonces

$$\mathcal{U}(\mathcal{O}_{\mathbb{Q}(\sqrt{d})}) = \begin{cases} \{\pm 1, \pm\sqrt{-1}\} & \cong & \langle \sqrt{-1} \rangle & \cong & \mathbb{Z}/4\mathbb{Z} & \text{si } d = -1 \\ \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\} & \cong & \langle \frac{1+\sqrt{-3}}{2} \rangle & \cong & \mathbb{Z}/6\mathbb{Z} & \text{si } d = -3 \\ \{\pm 1\} & \cong & \langle -1 \rangle & \cong & \mathbb{Z}/2\mathbb{Z} & \text{si } d \neq -1, -3 \end{cases}$$

**4. Determinar si el anillo de enteros de $\mathbb{Q}(\sqrt{-13})$ es un dominio de ideales principales.**
*Solución:* Veamos que $\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\sqrt{-13})} = \mathbb{Z}[\sqrt{-13}]$ ya que $-13 \not\equiv 1\,(\text{mod } 4)$, no es un dominio de factorización única y por lo tanto no es un dominio de ideales principales. Para ello basta con ver que las siguientes factorizaciones en irreducibles de 14 no son asociadas:

$$14 = 2 \cdot 7 = (1 + \sqrt{-13})(1 - \sqrt{-13}).$$

Para ello hemos de ver que los elementos $2,7,1 + \sqrt{-13}$ y $1 - \sqrt{-13}$ son irreducibles y las dos factorizaciones son no asociados. Sea $\alpha \in \mathcal{O}$ irreducible tal que $\alpha | 2$ (resp. $7,1 + \sqrt{-13}, 1 - \sqrt{-13}$). Entonces $N_{\mathbb{Q}(\sqrt{-13})}(\alpha) | N_{\mathbb{Q}(\sqrt{-13})}(2) = 4$ (resp. $7^2$,14,14). De aquí se deduce que todo se reduce a ver que no existe $\alpha \in \mathcal{O}$ de norma $\pm 2$ ó $\pm 7$. Sea $\alpha = a + b\sqrt{-13}$ tal que $a^2 + 13b^2 = \pm 2, \pm 7$ entonces necesariamente $a^2 + 13b^2 = 2, 7$. De aquí se obtiene $b = 0$ y por lo tanto $a^2 = 2, 7$. Pero entonces $a \notin \mathbb{Z}$. Ahora se ve que las factorizaciones son no asociadas ya que las normas de los irreducibles de la izquierda es 14 y los de la derecha son 4 y 49.

**5. Determinar la estructura del grupo de clase de $\mathbb{Q}(\sqrt{15})$.**
*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

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

En nuestro caso $K = \mathbb{Q}(\sqrt{15})$ es un cuerpo cuadrático ($n = 2$) real ($t = 0$) con $d = 15$ libre de cuadrados tal que $d \not\equiv 1 \pmod 4$. Por lo tanto $\mathcal{O}_{\mathbb{Q}(\sqrt{15})} = \mathbb{Z}[\theta]$ con $\theta = \sqrt{15}$, $f_\theta(x) = x^2 - 15$ el polinomio mínimo de $\theta$ y $\Delta_{\mathbb{Q}(\sqrt{15})} = 4 \cdot 15$. Así obtenemos $M_{\mathbb{Q}(\sqrt{15})} = 3'87$. Así todo ideal de $\mathcal{O}_{\mathbb{Q}(\sqrt{15})}$ es equivalente a uno de norma $\leq 3$.

Sabemos que para todo ideal $I$ de $\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\sqrt{15})}$ se tiene $N_{\mathbb{Q}(\sqrt{15})}(I) \in I$. Por lo tanto $\langle N_{\mathbb{Q}(\sqrt{15})}(I)\rangle \subset I$, es decir, $I$ aparece en la factorización del ideal $\langle N_{\mathbb{Q}(\sqrt{15})}(I)\rangle$. 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 $\theta$, $p \in \mathbb{Z}$ 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 $\theta = \sqrt{15}$, $f_\theta(x) = x^2 - 15$:

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

  $$\langle 2\rangle\mathcal{O} = \left\langle 2, 1 + \sqrt{15}\right\rangle^2 = \mathfrak{p}_2^2,$$

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

  $$4 = N_{\mathbb{Q}(\sqrt{15})}(2) = N_{\mathbb{Q}(\sqrt{15})}(\langle 2\rangle\mathcal{O}) = N_{\mathbb{Q}(\sqrt{15})}(\mathfrak{p}_2)^2.$$

- $p = 3$: Tenemos $f_\theta(x) \equiv x^2 \pmod 3$, por lo tanto

  $$\langle 3\rangle\mathcal{O} = \left\langle 3, \sqrt{15}\right\rangle^2 = \mathfrak{p}_3^2,$$

  con $\mathfrak{p}_3$ ideal primo de $\mathcal{O}$ de norma 3. Ya que

  $$9 = N_{\mathbb{Q}(\sqrt{15})}(3) = N_{\mathbb{Q}(\sqrt{15})}(\langle 3\rangle\mathcal{O}) = N_{\mathbb{Q}(\sqrt{15})}(\mathfrak{p}_3)^2.$$

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: $I = \mathfrak{p}_2$.
- 3: $I = \mathfrak{p}_3$.

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

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

Por lo tanto el número de clase es menor o igual a 3, es decir:

$$1 \leq h_{\mathbb{Q}(\sqrt{15})} \leq 3\,.$$

Sea $\mathfrak{p}$ un ideal de $\mathcal{O}$ de norma $n$. Si $\mathfrak{p} \sim \mathcal{O}$, entonces es principal. Es decir, existirá $\alpha = a + b\sqrt{15} \in \mathcal{O}$ tal que $\mathfrak{p} = \langle\alpha\rangle\mathcal{O}$ y por lo tanto $n = N_{\mathbb{Q}(\sqrt{15})}(\mathfrak{p}) = |N_{\mathbb{Q}(\sqrt{15})}(\alpha)| = |a^2 - 15b^2|$. Veamos si existen elementos de norma $\pm 2$ y $\pm 3$:

- $n = \pm 2, \pm 3$: Si existen $a, b \in \mathbb{Z}$ tal que $a^2 - 15b^2 = \pm 2, \pm 3$, entonces módulo 5 se tendrá $a^2 = \pm 2 \pmod 5$. Pero los cuadrados módulo 5 son $\{0, \pm 1\}$. Por lo tanto no hay elementos de norma $\pm 2$ ni $\pm 3$. Concluyendo: $\mathfrak{p}_2 \not\sim \mathcal{O}$ y $\mathfrak{p}_3 \not\sim \mathcal{O}$.

Así hemos visto

$$2 \leq h_{\mathbb{Q}(\sqrt{15})} \leq 3\,.$$

Sólo nos queda ver si $\mathfrak{p}_2$ y $\mathfrak{p}_3$ están relacionados. Supongamos que lo están, entonces $\mathfrak{p}_2\mathfrak{p}_3 \sim \mathcal{O}$. Es decir, $\mathfrak{p}_2\mathfrak{p}_3 = \langle \alpha \rangle$ donde $\alpha = a + b\sqrt{15}$ satisface $|a^2 - 15b^2| = 6$. Se comprueba que el elemento $\alpha = 3 + \sqrt{15}$ tiene norma $-6$ y que $\mathfrak{p}_2\mathfrak{p}_3 = \langle 3 + \sqrt{15} \rangle$. Por lo tanto $\mathfrak{p}_2 \sim \mathfrak{p}_3$.

Concluimos con $h_{\mathbb{Q}(\sqrt{15})} = 2$. Por lo tanto

$$\mathcal{H}_{\mathbb{Q}(\sqrt{15})} = \{[\mathcal{O}], [\mathfrak{p}_2]\} \cong \mathbb{Z}/2\mathbb{Z}.$$

**6. Determinar las soluciones enteras de la ecuación diofántica $C : x^5 = y^2 + 19$.**

*Solución:* Factorizando la ecuación obtenemos $(y + \sqrt{-19})(y - \sqrt{-19}) = x^5$. Esto indica que hemos de trabajar sobre el cuerpo cuadrática $\mathbb{Q}(\sqrt{-19})$ cuyo anillo de enteros es $\mathcal{O} = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ ya que $-19 \equiv 1 \pmod 4$. Recordemos que por el Teorema de Heegner-Stark este anillo es un dominio de ideales principales y por lo tanto de factorización única.

En primer lugar veamos que $x$ es impar e $y$ par. Si $y$ es par entonces $y^2 + 19$ es impar y por lo tanto $x^5$ es impar y se deduce que $x$ es impar. Ahora si $y$ es impar se tiene que reduciendo módulo 8 tenemos $y^2 + 19 \equiv 4 \pmod 8$ ya que 1 es el único cuadrado impar módulo 8. Por lo tanto $x^5 \equiv 4 \pmod 8$ pero las potencias quintas módulo 8 son $0, 1, 3, 5, 7$. Es decir que $y$ es par.

Como sabemos que en $\mathcal{O}$ hay factorización única vamos a trabajar con elementos irreducibles y no con ideales. Sea $\alpha \in \mathcal{O}$ irreducible tal que divide a $y + \sqrt{-19}$ y a $y - \sqrt{-19}$. Entonces dividirá a la resta: $2\sqrt{-19}$. Así que tomando normas obtenemos que la norma de $\alpha$ divide a $2^2 19$. Por otro lado, $\alpha$ divide a $x^5$ ya que divide a $y + \sqrt{-19}$ y a $y - \sqrt{-19}$. Por lo tanto divide a $x$ y tomando normas obtenemos que la norma de $\alpha$ divide a la norma de $x$, por lo tanto divide a $x$. Ahora como $x$ es impar obtenemos que la norma de $\alpha$ es impar y sabiamos que divide a $2^2 19$. Así que la norma de $\alpha$ es $\pm 19$. De aquí se obtiene $19|x$ y como $19|x^5 = y^2 + 19$ obtenemos que $19|y$. Utilizando que $19|x, y$ reducimos la ecuación módulo $19^2$ y obtenemos $0 + 19 \equiv 0 \pmod{19^2}$. Por lo tanto, $y + \sqrt{-19}$ e $y - \sqrt{-19}$ no tienen factores irreducibles comunes.

Del anterior párrafo obtenemos

$$y + \sqrt{-19} = u\left(a + b\left(\frac{1+\sqrt{-19}}{2}\right)\right)^5 \qquad \text{donde } u \in \mathcal{U}(\mathcal{O}) = \{\pm 1\}.$$

Como las unidades son potencias quintas podemos incluirla dentro y tenemos la ecuacíon $y + \sqrt{-19} = \left(A + B\left(\frac{1+\sqrt{-19}}{2}\right)\right)^5$ donde $A, B \in \mathbb{Z}$. Hemos de resolver el siguiente sistema de ecuaciones:

$$\left\{\begin{array}{rcl} 2y & = & (2A+B)(A^4 + 2A^3B - 46A^2B^2 - 47AB^3 + 101B^4)\,, \\ 2 & = & B(5A^4 + 10A^3B - 40A^2B^2 - 45AB^3 + 11B^4). \end{array}\right.$$

De la segunda ecuación obtenemos que $B|2$ y reduciéndola módulo 5 obtenemos $B^5 \equiv 2 \pmod 5$. Juntando ambas condiciones obtenemos $B = 2$. Sustituimos este valor en esa misma ecuación:

$$5A^4 + 20A^3 - 160A^2 - 360A + 176 = 1.$$

Un cálculo sencillo muestra que las únicas soluciones enteras a la anterior ecuación son $A = 5, -7$. Por lo tanto sustituyendo las únicas posibilidades $(A, B) = (5, 2), (-7, 2)$ en la primera ecuación obtenemos $y = -22434$ e $y = 22434$ respectivamente. Por lo tanto $(\pm 22434)^2 + 19 = (55)^5$. Así concluimos::

$$C(\mathbb{Z}) = \{(55, \pm 22434)\},.$$