4 Febrero 2008 (SOLUCIONES)

1. **Demostrar que hay infinitos primos congruentes con 7 módulo 8.**
Solución: Supongamos que hay un número finito. Sean dichos primos $p_1, \ldots, p_r$. Sea

$$N = (4p_1 \cdots p_r)^2 - 2.$$

Entonces los únicos primos que dividen a N son 2 y aquellos que no son congruentes con 7 módulo 8. Ahora queremos ver que todos estos primos son congruentes con 1 módulo 8. Sea p un primo impar tal que $p|N$, entonces

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

ya que como $p|N$ se tiene $N \equiv 0 \,(\mathrm{mod}\, p)$, es decir, $(4p_1 \cdots p_r)^2 \equiv 2 \,(\mathrm{mod}\, p)$. La 2ª Ley Suplementaria nos dice que entonces $p \equiv 1$ ó $7 \,(\mathrm{mod}\, 8)$. Como sabemos que lo segundo no puede ser, obtenemos que todos los primos impares que dividen a N son congruentes con 1 módulo 8. Por lo tanto $N \equiv 2 \,(\mathrm{mod}\, 8)$. Por otro lado, como $N = (4p_1 \cdots p_r)^2 - 2$ tenemos $N \equiv -2 \,(\mathrm{mod}\, 8)$ que es un contradicción.

2. **Determinar para qué primos p es 11 un residuo cuadrático módulo p.**
Solución: Si $p = 11$, entonces $11 \equiv 0 \,(\mathrm{mod}\, p)$ y por lo tanto es un residuo cuadrático módulo p. Análogamente para $p = 2$, aunque en este caso se observa que todo número es residuo cuadrático módulo 2. A partir de ahora supongamos $p \neq 11$, entonces 11 es residuo cuadrático si y sólo si el símbolo de Legendre $\left(\frac{11}{p}\right) = 1$. Ahora utilizando la Ley de reciprocidad cuadrática obtenemos

$$1 = \left(\frac{11}{p}\right) = (-1)^{\frac{(11-1)(p-1)}{4}} \left(\frac{p}{11}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{11}\right).$$

Por lo tanto:

$$\left(\frac{11}{p}\right) = 1 \Longleftrightarrow \begin{cases} (-1)^{\frac{p-1}{2}} = 1 & \text{y} \quad \left(\frac{p}{11}\right) = 1 \\ & \text{ó} \\ (-1)^{\frac{p-1}{2}} = -1 & \text{y} \quad \left(\frac{p}{11}\right) = -1 \end{cases}$$

O de forma equivalente:

$$\left(\frac{11}{p}\right) = 1 \Longleftrightarrow \begin{cases} p \equiv 1 \,(\mathrm{mod}\ 4) & \text{y} \quad p \equiv 1, 3, 4, 5, 9 \,(\mathrm{mod}\ 11) \\ & \text{ó} \\ p \equiv 3 \,(\mathrm{mod}\ 4) & \text{y} \quad p \equiv 2, 6, 7, 8, 10 \,(\mathrm{mod}\ 11) \end{cases}$$

Se sigue de que los cuadrados mod 11 son $\{0, 1, 3, 4, 5, 9\}$.

Ahora utilizando el teorema chino de los resto vamos a trasladar estas condiciones a módulo 44, ya que $(4, 11) = 1$. De la primera condición tenemos que $p \equiv 1 \,(\mathrm{mod}\ 4)$, así que $p \equiv 1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41 \,(\mathrm{mod}\ 44)$. Como hemos de tener $p \equiv 1, 3, 4, 5, 9 \,(\mathrm{mod}\ 11)$, obtenemos que la primera condición es equivalente a $p \equiv 1, 5, 9, 25, 37 \,(\mathrm{mod}\ 44)$. Análogamente con segundo caso obtenemos $p \equiv 7, 19, 35, 39, 43 \,(\mathrm{mod}\ 44)$.

Juntándolo obtenemos:

$$\left(\frac{11}{p}\right) = 1 \Longleftrightarrow p \equiv \pm 1, \pm 5, \pm 9, \pm 25, \pm 37 \,(\text{mod } 44)$$

Por lo tanto concluimos:

$$11 \text{ es residuo cuadrático módulo } p \Longleftrightarrow p = 11 \text{ ó } p \equiv \pm 1, \pm 5, \pm 7, \pm 9, \pm 19 \,(\text{mod } 44).$$

3. Enunciar y demostrar el primer caso del Último Teorema de Fermat para $p = 5$.

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 $p = 5$. Por lo tanto hemos de calcular el número de clase de $\mathbb{Q}(\zeta_5)$. Para ello en primer lugar calculemos la cota de Minkowski de $\mathbb{Q}(\zeta_5)$. Recordemos la fórmula del discriminante de $\mathbb{Q}(\zeta_p)$: $\Delta_p = (-1)^{(p-1)/2} p^{p-2}$. En nuestro caso como $p = 5$ obtenemos $\Delta_5 = 5^3$. Además $\mathbb{Q}(\zeta_5)$ es un cuerpo cuartico ($n = 4$) totalmente imaginario ($t = 2$), por lo tanto

$$M_{\mathbb{Q}(\zeta_5)} = \left(\frac{4}{\pi}\right)^2 \frac{4!}{4^4} \sqrt{|5^3|} = 1'7.$$

Por lo tanto todo ideal es equivalente a un ideal de norma igual a 1, es decir, $h_{\mathbb{Q}(\zeta_5)} = 1$. Es decir, $5 \nmid h_{\mathbb{Q}(\zeta_5)} = 1$. Utilizando el anterior resultado de Kummer se demuestra el primer caso del Último Teorema de Fermat para $p = 5$.

4. Determinar la estructura del grupo de clase de $\mathbb{Q}(\sqrt{35})$.

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 $K = \mathbb{Q}(\sqrt{35})$ es un cuerpo cuadrático ($n = 2$) real ($t = 0$) con $d = 35$ libre de cuadrados tal que $d \not\equiv 1 \,(\text{mod } 4)$. Por lo tanto $\mathcal{O}_{\mathbb{Q}(\sqrt{35})} = \mathbb{Z}[\theta]$ con $\theta = \sqrt{35}$, $f_\theta(x) = x^2 - 35$ el polinomio mínimo de θ y $\Delta_{\mathbb{Q}(\sqrt{35})} = 4 \cdot 35$. Así obtenemos $M_{\mathbb{Q}(\sqrt{35})} = 5'91$. Así todo ideal de $\mathcal{O}_{\mathbb{Q}(\sqrt{35})}$ es equivalente a uno de norma ≤ 5.

Sabemos que para todo ideal I de $\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\sqrt{35})}$ 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 $\langle N_{\mathbb{Q}(\sqrt{35})}(I) \rangle$. Así que hemos de calcular la factorización de los ideales generados por $1, 2, 3, 4, 5$. 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 $\theta = \sqrt{35}$, $f_\theta(x) = x^2 - 35$:

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

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

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

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

- $p = 3$: Tenemos $f_\theta(x) \equiv x^2 + 1 \pmod 3$, por lo tanto $\langle 3\rangle\mathcal{O}$ es primo y su norma es 9, ya que $N_{\mathbb{Q}(\sqrt{35})}(3) = N_{\mathbb{Q}(\sqrt{35})}(\langle 3\rangle\mathcal{O}) = |N_{\mathbb{Q}(\sqrt{35})}(3)| = 3^2$.
- $p = 5$: Tenemos $f_\theta(x) \equiv x^2 \pmod 5$, por lo tanto

$$\langle 5\rangle\mathcal{O} = \left\langle 5, \sqrt{35}\right\rangle^2 = \mathfrak{p}_5^2,$$

  con $\mathfrak{p}_5$ ideal primo de $\mathcal{O}$ de norma 5. Ya que

$$25 = N_{\mathbb{Q}(\sqrt{35})}(5) = N_{\mathbb{Q}(\sqrt{35})}(\langle 5\rangle\mathcal{O}) = N_{\mathbb{Q}(\sqrt{35})}(\mathfrak{p}_5)^2.$$

Por lo tanto tenemos que si I es un ideal de $\mathcal{O}$ de norma $1, 2, 3, 4$ ó 5 ha de ser:

- 1: $I = \mathcal{O}$.
- 2: $I = \mathfrak{p}_2$.
- 3: No hay ideales de norma 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 $I \sim \mathcal{O}$.
- 5: $I = \mathfrak{p}_5$.

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

$$\mathcal{O}, \mathfrak{p}_2, \mathfrak{p}_5$$

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

$$1 \leq h_{\mathbb{Q}(\sqrt{35})} \leq 3\,.$$

Sea $\mathfrak{p}$ un ideal de $\mathcal{O}$ de norma n. Si $\mathfrak{p} \sim \mathcal{O}$, entonces es principal. Es decir, existirá $\alpha = a + b\sqrt{35} \in \mathcal{O}$ tal que $\mathfrak{p} = \langle\alpha\rangle\mathcal{O}$ y por lo tanto $n = N_{\mathbb{Q}(\sqrt{35})}(\mathfrak{p}) = |N_{\mathbb{Q}(\sqrt{35})}(\alpha)| = |a^2 - 35b^2|$. Veamos si existen elementos de norma ± 2 y ± 5:

- $n = \pm 2$: Si existen $a, b \in \mathbb{Z}$ tal que $a^2 - 35b^2 = \pm 2$, 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 2 ni -2. Concluyendo: $\mathfrak{p}_2 \not\sim \mathcal{O}$.
- $n = \pm 5$:
  - Si existen $a, b \in \mathbb{Z}$ tal que $a^2 - 35b^2 = 5$, entonces módulo 7 se tendrá $a^2 = 5 \pmod 7$. Pero los cuadrados módulo 7 son $\{0, 1, 2, 4\}$. Por lo tanto no hay elementos de norma 5.
  - Si existen $a, b \in \mathbb{Z}$ tal que $a^2 - 35b^2 = -5$, entonces módulo 4 se tendrá $a^2 + b^2 = 3 \pmod 4$. Pero los cuadrados módulo 4 son $\{0, 1\}$. Por lo tanto no hay elementos de norma -5.

  Concluyendo: $\mathfrak{p}_5 \not\sim \mathcal{O}$.

Así hemos visto

$$2 \leq h_{\mathbb{Q}(\sqrt{35})} \leq 3\,.$$

Sólo nos queda ver si $\mathfrak{p}_2$ y $\mathfrak{p}_5$ están relacionados. Supongamos que lo están, entonces $\mathfrak{p}_2\mathfrak{p}_5 \sim \mathcal{O}$. Es decir, $\mathfrak{p}_2\mathfrak{p}_5 = \langle\alpha\rangle$ donde $\alpha = a + b\sqrt{35}$ satisface $|a^2 - 35b^2| = 10$. Se comprueba que el elemento $\alpha = 5 + \sqrt{35}$ tiene norma -10. Se comprueba $\mathfrak{p}_2\mathfrak{p}_5 = \langle 5 + \sqrt{35}\rangle$. Por lo tanto $\mathfrak{p}_2 \sim \mathfrak{p}_5$.

Concluimos con $h_{\mathbb{Q}(\sqrt{35})} = 2$. Por lo tanto

$$\mathcal{H}_{\mathbb{Q}(\sqrt{35})} = \{[\mathcal{O}], [\mathfrak{p}_2]\} \cong \mathbb{Z}/2\mathbb{Z}.$$

5. Determinar si el anillo de enteros de $\mathbb{Q}(\sqrt{35})$ es una dominio de factorización única.
Solución 1: Veamos que $\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\sqrt{35})} = \mathbb{Z}[\sqrt{35}]$ no es un dominio de factorización única. Para ello basta con ver que las siguientes factorizaciones en irreducibles de 34 no son asociadas:

$$(1 + \sqrt{35})(1 - \sqrt{35}) = 34 = 2 \cdot 17.$$

Para ello hemos de ver que los elementos 2,17,$1 + \sqrt{35}$ y $1 - \sqrt{35}$ son irreducibles y las dos factorizaciones son no asociados. Sea $\alpha \in \mathcal{O}$ irreducible tal que $\alpha|2$ (resp. 17,$1 + \sqrt{35}$,$1 - \sqrt{35}$). Entonces $N_{\mathbb{Q}(\sqrt{35})}(\alpha)|N_{\mathbb{Q}(\sqrt{35})}(2) = 4$ (resp. 17^2,34,34). De aquí se deduce que todo se reduce a ver que no existe $\alpha \in \mathcal{O}$ de norma ± 2 ó ± 17. Sea $\alpha = a + b\sqrt{35}$ tal que $a^2 - 35b^2 = \pm 2, \pm 17$ entonces módulo 5 obtenemos $a^2 \equiv \pm 2 \pmod 5$. Pero los cuadrados módulo 5 son $\{0, \pm 1\}$. Ahora se ve que las factorizaciones son no asociadas ya que las normas de los irreducibles de la izquierda es 34 y los de la derecha son 4 y 17^2.
Solución 2: 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 3: En el ejercicio 4 hemos demostrado que $h_{\mathbb{Q}(\sqrt{35})} = 2 \neq 1$ por lo tanto $\mathcal{O}$ no es DFU.

6. Calcular las soluciones enteras de la ecuación diofántica $w^4 = t^4 + 35$.
Solución 1: En primer lugar obsérvese que podemos escribir la ecuación de la forma $w^4 - t^4 = 35$ y así factorizarla como $(w^2 - t^2)(w^2 + t^2) = 5 \cdot 7$. Ahora como $w, t \in \mathbb{Z}$ se tiene que $w^2 - t^2$, $w^2 + t^2$ son factores enteros de $5 \cdot 7$. Por lo tanto

$$(w^2 - t^2, w^2 + t^2) \in \{(1, 35), (35, 1), (-1, -35), (-35, -1), (5, 7), (-5, -7), (7, 5), (-7, -5)\}.$$

Es decir, que hay que resolver los siguientes sistemas de ecuaciones

$$\begin{cases} w^2 - t^2 &= 1, \quad 35, \quad -1, \quad -35, \quad 5, \quad -5, \quad 7, \quad -7. \\ w^2 + t^2 &= 35, \quad 1, \quad -35, \quad -1, \quad 7, \quad -7, \quad 5, \quad -5. \end{cases}$$

Sumando las ecuaciones de cada sistema obtenemos $2w^2 = 36$, 36, -36, -36, 12, -12, 12, -12 respectivamente. Claramente se observa que entonces $w \notin \mathbb{Z}$. Por lo tanto, la ecuación diofántica $w^4 = t^4 + 35$ no tiene soluciones enteras.

Solución 2 (Gabriel Mora): Sea $w, t \in \mathbb{Z}$ tal que $w^4 = t^4 + 35$. Entonces módulo 8 se tendrá $w^4 \equiv t^4 + 3 \pmod 8$. Pero esto es imposible ya que las potencia cuartas módulo 8 son 0 y 1. Por lo tanto, la ecuación diofántica $w^4 = t^4 + 35$ no tiene soluciones enteras.