23 de Noviembre 2007 (SOLUCIONES)

1. Sean p_1, p_2, p_3 números primos tales que $p_1 < p_2 < p_3$:

(a) **Demostrar que no es posible que $p_1p_2p_3 = p_1^3 + p_2^3 + p_3^3$.**

Solución: Sea $n = p_1p_2p_3 = p_1^3 + p_2^3 + p_3^3$. De aquí obtenemos $p_3^3 = n - p_1^3 - p_2^3$ y tomando raíz cúbica a ambos lados de la igualdad tenemos $p_3 = \sqrt[3]{n - p_1^3 - p_2^3} < n^{1/3}$. Así que tenemos:

$$p_1 < p_2 < p_3 < n^{1/3}, \tag{1}$$

de lo que se deduce:

$$n^{1/3} > p_3 > p_2 = \frac{n}{p_1p_3} > \frac{n}{n^{1/3}p_1} = \frac{n^{2/3}}{p_1},$$

que implica

$$p_1 > \frac{n^{2/3}}{n^{1/3}} = n^{1/3},$$

que contradice (1).

(b) **¿Qué se puede decir de $p_1p_2p_3 = p_1^2 + p_2^2 + p_3^2$?**

Solución: Distinguiremos dos casos, dependiendo de si uno de los primos es 3 o no.
Supongamos en primer lugar que uno de los primos es 3 y llamemos a los otros dos primos p y q. Entonces tenemos que $n = 3pq$, es decir, $n \equiv 0 \pmod 3$. Por otro lado, $n = 3^2 + p^2 + q^2 \equiv 1 + 1 \equiv 2 \pmod 3$ que contradice lo anterior.
Ahora supongamos que ninguno de los primos es 3, por lo tanto $n \not\equiv 0 \pmod 3$ y por otro lado $n = p_1^2 + p_2^2 + p_3^2 \equiv 1 + 1 + 1 \equiv 0 \pmod 3$, que contradice lo anterior.
Por lo tanto concluimos que tampoco es posible este caso.

2. Encontrar el menor entero positivo n tal que $\sqrt[7]{n/7}$ y $\sqrt[11]{n/11}$ son ambos enteros.

Solución: Como n es divisible por 7 y 11, podemos escribirlo de la forma $n = 7^a11^b$. Ahora $n/7 = 7^{a-1}11^b$ ha de ser una potencia septima de un entero, por lo tanto $a \equiv 1 \pmod 7$ y $b \equiv 0 \pmod 7$. Por otro lado, $n/11 = 7^a11^{b-1}$ ha de ser una potencia onceava de un entero, por lo tanto $a \equiv 0 \pmod{11}$ y $b \equiv 1 \pmod{11}$. Así que tenemos los dos sistemas de congruencias siguientes

$$\begin{cases} a \equiv 1 \pmod 7 \\ a \equiv 0 \pmod{11} \end{cases} \quad \text{y} \quad \begin{cases} b \equiv 0 \pmod 7 \\ b \equiv 1 \pmod{11} \end{cases}$$

Resolviendo estos sistemas de ecuaciones utilizando el teorema chino del resto obtenemos $a \equiv 22 \pmod{77}$ y $b \equiv 56 \pmod{77}$. Por lo tanto, $n = 7^{22}11^{56}$. O lo que es lo mismo:

$$81310615612737839661014568033097645050397832978024738446229531364021868621489$$

3. En una carta a Christian Huygens en 1659, Fermat escribió que había encontrado todos los enteros de la forma $3k-1$ que a su vez son de la forma x^2+3y^2. ¿Cúales son estos enteros?

Solución: Buscamos las soluciones $x, y, k \in \mathbb{Z}$ de la ecuación diofántica

$$x^2 + 3y^2 = 3k - 1\,. \tag{2}$$

Reduciendo esta ecuación módulo 3 obtenemos $x^2 \equiv -1 \pmod 3$. Pero -1 no es residuo cuadrático módulo 3, ya que se puede comprobar que los cuadrados módulo 3 son $\{0, 1\}$.

Por lo tanto la ecuación (2) no tiene soluciones enteras x, y, k. Es decir no hay enteros que son a la vez de la forma $3k-1$ y x^2+3y^2.

4. Determinar para qué primos p es 6 un residuo cuadrático módulo p.

Solución: Si $p = 2$ ó 3, entonces $6 \equiv 0 \pmod p$ y por lo tanto es un residuo cuadrático módulo p. Supongamos $p > 3$, entonces 6 es residuo cuadrático si y sólo si el símbolo de Legendre $\left(\frac{6}{p}\right) = 1$. Ahora utilizando que el símbolo de Legendre es multiplicativo, la Ley de reciprocidad cuadrática y la segunda ley suplementaria, obtenemos

$$1 = \left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p^2-1}{8}}(-1)^{\frac{(3-1)(p-1)}{4}}\left(\frac{p}{3}\right) = (-1)^{\frac{p^2-1}{8}}(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right).$$

Por lo tanto:

$$\left(\frac{6}{p}\right) = 1 \iff \begin{cases} (-1)^{\frac{p^2-1}{8}} = 1 & \text{y} & (-1)^{\frac{p-1}{2}} = 1 & \text{y} & \left(\frac{p}{3}\right) = 1 \\ & & \text{ó} & & \\ (-1)^{\frac{p^2-1}{8}} = 1 & \text{y} & (-1)^{\frac{p-1}{2}} = -1 & \text{y} & \left(\frac{p}{3}\right) = -1 \\ & & \text{ó} & & \\ (-1)^{\frac{p^2-1}{8}} = -1 & \text{y} & (-1)^{\frac{p-1}{2}} = -1 & \text{y} & \left(\frac{p}{3}\right) = 1 \\ & & \text{ó} & & \\ (-1)^{\frac{p^2-1}{8}} = -1 & \text{y} & (-1)^{\frac{p-1}{2}} = 1 & \text{y} & \left(\frac{p}{3}\right) = -1 \end{cases}$$

O de forma equivalente:

$$\left(\frac{6}{p}\right) = 1 \iff \begin{cases} p \equiv 1, 7 \pmod 8 & \text{y} & p \equiv 1 \pmod 4 & \text{y} & p \equiv 1 \pmod 3 \\ & & \text{ó} & & \\ p \equiv 1, 7 \pmod 8 & \text{y} & p \equiv 3 \pmod 4 & \text{y} & p \equiv 2 \pmod 3 \\ & & \text{ó} & & \\ p \equiv 3, 5 \pmod 8 & \text{y} & p \equiv 3 \pmod 4 & \text{y} & p \equiv 1 \pmod 3 \\ & & \text{ó} & & \\ p \equiv 3, 5 \pmod 8 & \text{y} & p \equiv 1 \pmod 4 & \text{y} & p \equiv 2 \pmod 3 \end{cases}$$

Se sigue de las leyes suplementarias y de que los cuadrados mod 3 son 0 y 1.

Ahora vamos a trasladar estas condiciones a módulo $\text{mcm}(8, 4, 3) = 24$. De la primera condición tenemos que $p \equiv 1 \pmod 4$, así que $p \equiv 1, 5, 9, 13, 17, 21 \pmod{24}$. Como hemos de tener $p \equiv 1 \pmod 3$, obtenemos que la primera condición es equivalente a $p \equiv 1, 13 \pmod{24}$. Ahora como $p \equiv 1, 7 \pmod 8$, deducimos $p \equiv 1 \pmod{24}$. Análogamente el resto de los casos.

Juntándolo obtenemos:

$$\left(\frac{6}{p}\right) = 1 \iff \begin{cases} p \equiv 1 \,(\text{mod } 24) \\ \text{ó} \\ p \equiv 23 \,(\text{mod } 24) \\ \text{ó} \\ p \equiv 19 \,(\text{mod } 24) \\ \text{ó} \\ p \equiv 5 \,(\text{mod } 24) \end{cases}$$

Por lo tanto concluimos:

$$6 \text{ es residuo cuadrático módulo } p \iff p = 2 \text{ ó } 3 \text{ ó } p \equiv \pm 1, \pm 5 \,(\text{mod } 24).$$

5. Calcular las soluciones enteras de la ecuación diofántica $y^2 = x^3 + 7$.

Solución: En primer lugar reescribimos la ecuación de la forma siguiente:

$$y^2 + 1 = (x+2)((x-1)^2 + 3). \tag{3}$$

Ahora veamos que si $x, y \in \mathbb{Z}$ es una solución, entonces x es impar. Supongamos que $x = 2n$ para algún entero n. Entonces la ecuación anterior se transforma en

$$y^2 + 1 = 8n^3 + 8.$$

Pasándolo a mod 8 obtenemos que $y^2 \equiv -1 \,(\text{mod}\, 8)$. Pero se puede comprobar que los cuadrados módulo 8 son $\{0, 1, 4\}$.

Por lo tanto, x es impar. De aquí se deduce que $(x-1)^2 + 3 \equiv 3 \,(\text{mod}\, 4)$. Así que existe un primo p tal que $p|(x-1)^2 + 3$ y $p \equiv 3 \,(\text{mod}\, 4)$.

Reduciendo la ecuación (3) módulo p obtenemos:

$$y^2 + 1 \equiv 0 \,(\text{mod}\, p)\,.$$

Es decir, -1 es un residuo cuadrático mod p con $p \equiv 3 \,(\text{mod}\, 4)$. Pero esto es imposible por la primera ley suplementaria.

6. Calcular el número de soluciones de la congruencia $15n^2 + 12n - 6 \equiv 0$ (mod 2066715).

Solución: Para encontrar las raíces de $f(n) = 15n^2 + 12n - 6$ en $\mathbb{Z}/m\mathbb{Z}$ para $m = 2066715$ lo primero que hemos de hacer es factorizar m, obteniendo $m = 3^{10} \cdot 5 \cdot 7$. Así si denotamos por

$$C_N = \{n \in \mathbb{Z}/N\mathbb{Z} \,|\, f(n) \equiv 0 \,(\text{mod } N)\}\,,$$

se tendrá

$$C_{2066715} \simeq C_{3^{10}} \times C_5 \times C_7\,.$$

Obsérvese que $f(n)$ factoriza sobre $\mathbb{Z}[n]$ como $f(n) = 3(5n^2 + 4n - 2)$. Un simple cálculo demuestra

$$C_3 = \{0, 1, 2\} \qquad C_5 = \{3\} \quad \text{y} \quad C_7 = \{1\}\,.$$

Vamos usar el lema de Hensel para ver si podemos construir todas las soluciones módulo 3^{10} a partir de las de módulo 3. En nuestro caso se tiene $f'(n) = 3(10n + 4)$, así que $f'(0) \equiv f'(1) \equiv f'(2) \equiv 0 \,(\text{mod}\, 3)$. Por lo tanto hemos de utilizar la versión ampliada del Lema de Hensel. Tenemos

$$f(0) = -6 = -2 \cdot 3 \qquad f(1) = 21 = 3 \cdot 7 \quad \text{y} \quad f(2) = 78 = 2 \cdot 3 \cdot 13$$

Así que $f(i) \not\equiv 0 \,(\text{mod}\, 3^k)$ para $i = 0, 1, 2$ y $k > 1$. Por lo tanto se tiene que $C_{3^{10}} = \emptyset$. Así concluimos

$$\#C_{2066715} = 0.$$

7. Sean $a, b \in \mathbb{Z}$ y $m, n \in \mathbb{N}$. Demostrar que el sistema de congruencias

$$\begin{cases} x \equiv a \,(\textbf{mod } m)\,, \\ x \equiv b \,(\textbf{mod } n) \end{cases}$$

tiene solución si y sólo si $(m, n)|(a - b)$.

Solución: Como $x \equiv a \,(\text{mod } m)$, existe $k \in \mathbb{Z}$ tal que $x = a + km$ y por lo tanto $a + km \equiv b \,(\text{mod } n)$. Por lo tanto existe $j \in \mathbb{Z}$ tal que $a + km = b + jn$, es decir, $km - jn = -(a - b)$. Ahora, como (m, n) divide a m y n, se tiene $(m, n)|(a - b)$.

Demostremos el recíproco. Asumamos que $(m, n)|(a - b)$. Entonces existe $M \in \mathbb{Z}$ tal que $a - b = M(m, n)$ y por el teorema de Bezout sabemos que existen $k_1, k_2 \in \mathbb{Z}$ tales que $(m, n) = k_1 m + k_2 n$. Por lo tanto si tomamos $k = -k_1 M$ y $j = k_2 M$ tenemos $a - b = -km + jn$. Así obtenemos $a + km = b + jn$. Es decir que si tomamos $x = a + km$ tenemos que $x \equiv a \,(\text{mod } m)$ y como $x = a + km = b + jn$ se tiene $x \equiv b \,(\text{mod } n)$.