TEORÍA DE NÚMEROS

GLENIER BELLO

5. Soluciones

Problema 1. Probar que existen infinitos números primos congruentes con 3 módulo 4.

Solución. Notar que el 3 es un número primo congruente con 3 módulo 4. Supongamos que hubiese sólo un número finito de primos congruentes con 3 módulo 4, digamos $p_1, p_2, \ldots, p_n$. Sea $P = 4p_1p_2\cdots p_n - 1$. Notar que P no es múltiplo de 2 ni tampoco múltiplo de ningún p_i. Luego todos los divisores primos de P son congruentes con 1 módulo 4. Pero entonces P sería congruente con 1 módulo 4, lo cual es una contradicción.

Problema 2. Sea m un entero positivo y sean a y b enteros, con mcd(a,m)=1. Sea S un conjunto completo de clases de residuos módulo m. Entonces el conjunto

$$T = aS + b = \{as + b : s \in S\}$$

también es un conjunto completo de clases de residuos módulo m.

Solución. Como S es un conjunto completo de clases de residuos módulo m, tendrá exactamente m elementos. Notar que T tiene los mismos elementos que S, es decir, m elementos. Además, dos cualesquiera de ellos no son congruentes módulo m. En efecto, si $as_1 + b \equiv as_2 + b \pmod{m}$, entonces $s_1 \equiv s_2 \pmod{m}$ (ya que mcd(a,m)=1). Pero como $s_1, s_2 \in S$, deducimos que $s_1 = s_2$. Por tanto, T es un conjunto completo de clases de residuos módulo m.

Problema 3. (Gauss). Probar que para todo entero positivo n se cumple

$$\sum_{d|n} \varphi(d) = n.$$

Solución. Consideremos los números racionales

$$\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}.$$

Claramente hay n números en la lista.

Obtenemos una nueva lista reduciendo cada término de la lista anterior a su fracción irreducible. Los denominadores que aparecen en la nueva lista son todos los divisores de n. Si $d|n$, hay exactamente $\varphi(d)$ números en la nueva

lista con denominador d. Por tanto, el número de elementos de la nueva lista es $\sum_{d|n} \varphi(d)$.

Como ambas listas tienen la misma cantidad de elementos, obtenemos el resultado deseado.

Problema 4. (OME 2014, Fase Local). Hallar las soluciones enteras de la ecuación

$$x^4 + y^4 = 3x^3y.$$

Solución. Observar que $n^4 \equiv 0$ ó $1 \pmod 3$. Tomando módulo 3 en la ecuación del enunciado, como el miembro de la derecha es 0, por la observación anterior deducimos que tanto x como y son múltiplos de 3, digamos $x = 3a$, $y = 3b$. Sustituyendo esto en la ecuación del enunciado y simplificando, obtenemos

$$a^4 + b^4 = 3a^3b.$$

Por tanto, de nuevo obtenemos que tanto a como b son múltiplos de 3. Repitiendo este proceso indefinidamente, obtenemos que la única solución posible es $x = y = 0$.

Problema 5. (OME 2014, Fase Local). Probar que

$$2014^3 - 1013^3 - 1001^3$$

divide a

$$2014^{2013} - 1013^{2013} - 1001^{2013}.$$

Solución. Usando el binomio de Newton tenemos

$$\begin{aligned} 2014^{2013} = (1013 + 1001)^{2013} &= \sum_{i=0}^{2013} \binom{2013}{i} \cdot 1013^{2013-i} \cdot 1001^i \\ &= 1013^{2013} + \binom{2013}{1} \cdot 1013^{2012} \cdot 1001 + \cdots + \binom{2013}{2012} \cdot 1013 \cdot 1001^{2012} + 1001^{2013} \end{aligned}$$

Luego

$$2014^{2013} - 1013^{2013} - 1001^{2013} = 1013 \cdot 1001 \cdot \left[\binom{2013}{1} \cdot 1013^{2011} + \cdots + \binom{2013}{2012} \cdot 1001^{2011} \right].$$

Análogamente obtenemos

$$2014^3 - 1013^3 - 1001^3 = 1013 \cdot 1001 \cdot \left[\binom{3}{1} \cdot 1013 + \binom{3}{2} \cdot 1001 \right] = 1013 \cdot 1001 \cdot 3 \cdot 2014.$$

Es decir, basta probar que $3 \cdot 2014$ divide a

$$\binom{2013}{1} \cdot 1013^{2011} + \cdots + \binom{2013}{2012} \cdot 1001^{2011}.$$

Pero como $3\cdot 2014$ es coprimo con $1013\cdot 1001$, es más sencillo probar que $3\cdot 2014$ divide a

$$2014^{2013} - 1013^{2013} - 1001^{2013},$$

lo cual es inmediato usando congruencias módulo 3 y módulo 2014.

Problema 6. (OME 2014, Fase Local). Hallar las tres últimas cifras de 7^{2014}.

Solución. Queremos hallar 7^{2014} módulo 1000. Como $\varphi(1000) = 400$ tenemos

$$7^{2014} = \left(7^{400}\right)^5 \cdot 7^{14} \equiv 7^{14} \equiv 849 \pmod{1000}.$$

Problema 7. Probar que para cada n entero positivo, $n^2 + n + 1$ no tiene ningún divisor congruente con 2 módulo 3.

Solución. Supongamos que $3k + 2$ divide a $n^2 + n + 1$, para algún k entero no negativo. Sea $p = 3j + 2$ un divisor primo de $3k + 2$. Luego p divide a $n^2 + n + 1$, que a su vez divide a $n^3 - 1$. Entonces p no divide a n, y usando el teorema pequeño de Fermat tenemos que $n^{3j+1} = n^{p-1} \equiv 1 \pmod{p}$. Como $n^3 \equiv 1 \pmod{p}$, de lo anterior deducimos que $n \equiv 1 \pmod{p}$. Entonces $0 \equiv n^2 + n + 1 \equiv 3 \pmod{p}$. Luego p divide a 3; es decir, $p = 3$. Pero esto contradice $p = 3j + 2$.

Problema 8. Sea n un entero positivo y sean $a_1, ..., a_k$ $(k \geq 2)$ enteros distintos del conjunto $1, ..., n$, tales que n divide a $a_i(a_{i+1} - 1)$, para $i = 1, ..., k - 1$. Demostrar que n no divide a $a_k(a_1 - 1)$.

Solución. Como n divide a $a_i(a_{i+1} - 1)$, para $i = 1, ..., k - 1$, tenemos que

$$\begin{aligned} a_1a_2 &\equiv a_1 \pmod{n} \\ a_2a_3 &\equiv a_2 \pmod{n} \\ &\vdots \\ a_{k-1}a_k &\equiv a_{k-1} \pmod{n} \end{aligned}$$

Supongamos que $a_ka_1 \equiv a_k \pmod{n}$. Multiplicando esta última congruencia por a_{k-1} y usando la última de las relaciones de congruencias antes citadas, obtenemos que

$$a_{k-1}a_ka_1 \equiv a_{k-1}a_k \pmod{n} \Rightarrow a_{k-1}a_1 \equiv a_{k-1} \pmod{n}$$

Multiplicando esta relación de congruencia por a_{k-2}, obtenemos

$$a_{k-2}a_1 \equiv a_{k-2} \pmod{n}.$$

Siguiendo este proceso, está claro que se llega a $a_2a_1 \equiv a_2 \pmod{n}$. Usando la primera de las relaciones de congruencias antes citadas, obtenemos que $a_1 \equiv a_2 \pmod{n}$. Pero como $a_1, ..., a_k$ $(k \geq 2)$ son enteros del conjunto $1, ..., n$,

deducimos que $a_1 = a_2$. Esto es una contradicción ya que $a_1, ..., a_k$ $(k \geq 2)$ son distintos.

Por tanto n no divide a $a_k(a_1 - 1)$.

Problema 9. Consideremos la sucesión $a_1, a_2, \ldots$ definida por

$$a_n = 2^n + 3^n + 6^n - 1,$$

para todos los enteros positivos n. Hallar todos los enteros positivos coprimos con todos los términos de la sucesión.

Solución. Veamos que la respuesta es 1.

Para ello, bastará probar que todo primo p divide a algún a_n. Notar que $p = 2$ y $p = 3$ dividen a $a_2 = 2^2 + 3^2 + 6^2 - 1 = 48$. Supongamos $p \geq 5$. Por el teorema pequeño de Fermat tenemos

$$2^{p-1} \equiv 3^{p-1} \equiv 6^{p-1} \equiv 1 \pmod{p}.$$

Luego

$$3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} \equiv 3 + 2 + 1 \equiv 6 \pmod{p},$$

y por tanto

$$6\left(2^{p-2} + 3^{p-2} + 6^{p-2} - 1\right) \equiv 0 \pmod{p}.$$

Como p no divide a 6, deducimos que p divide a $a_{p-2} = 2^{p-2} + 3^{p-2} + 6^{p-2} - 1$, como queríamos demostrar.