Pontificia Universidad Católica de Chile
Facultad de Matemáticas
2° semestre 2020

Ayudantía 04

04 de Septiembre

MAT2225 - Teoría de Números

1) Muestre el criterio de divisibilidad por 9: “un entero n es divisible por 9 si y solo si la suma de sus dígitos también lo es”.

Demostración. Sea $n = \overline{a_k a_{k-1} \cdots a_1 a_0}$. Así,

$$\sum_{i=0}^{k} 10^i a_i.$$

Como $10 \equiv_9 1$, $10^i \equiv_9 1$ para todo $i \in \mathbb{N}$. Luego,

$$n \equiv_9 \sum_{i=0}^{k} 10^i a_i \equiv_9 \sum_{i=0}^{k} a_i$$

Por transitividad se tiene lo pedido. ■

2) ¿Existen dos potencias de 2 distintas tales que al reordenar los dígitos de una se llegue a la otra? (sin tener ceros a la izquierda).

Demostración. Supongamos que existen. Sean $n < m$ las potencias. Como tienen la misma cantidad de dígitos, $10^k \leq n < m < 10^{k+1}$ para algún $k \in \mathbb{P}$, por lo que $m \leq 8n$. Además, como tienen los mismos dígitos, $n \equiv_9 m$. Luego, $9 \mid m - n$. Pero $m - n = (2^a - 1)2^b$, donde $2 \leq 2^a \leq 8$. Pero $(9, 2^b) = 1$ y $1 \leq 2^a - 1 \leq 7$, $\rightarrow\leftarrow$.

Por lo tanto, no existen potencias que cumplen lo pedido. ■

3) Encuentre 5^{2020} (mód 36).

Demostración. Notar que

$$\varphi(36) = 36 \prod_{p|36} \frac{p-1}{p} = 36 \cdot \frac{1}{2} \cdot \frac{2}{3} = 12.$$

Luego, por Euler tenemos que $5^{12} \equiv_{36} 1$. Como $2020 = 12 \cdot 168 + 4$, entonces

$$5^{2020} = (5^{12})^{168} \cdot 5^4 \equiv_{36} 5^4.$$

Por lo tanto, $5^{2020} \equiv 5^4 \equiv 625 \equiv 13$ módulo 36. ∎

4) Sea p primo impar y a un natural tal que $(a, p) = 1$. Encuentre el inverso de a.

Demostración. Por pequeño teorema de Fermat, tenemos que $a^{p-1} \equiv 1 \pmod{p}$. Luego, $a \cdot a^{p-2} \equiv_p 1$ y a^{p-2} es el inverso de a. ∎

5) Sea p un primo y n, m enteros tales que $a^n \equiv_p 1$ y $a^m \equiv_p 1$. Muestre que $a^{(n,m)} \equiv_p 1$.

Demostración. Por Bézout se tiene que existen enteros α, β tales que $\alpha n + \beta m = (n, m)$. Como $a^n \equiv_p 1$, se tiene $a^{\alpha n} \equiv (a^n)^\alpha \equiv 1^\alpha \equiv 1 \pmod{p}$. Análogamente, $a^{\beta m} \equiv_p 1$. Multiplicando ambas, tenemos que $1 = a^{\alpha n + \beta m} = a^{(n,m)}$, que es lo que buscábamos. ∎

6) Sea p un primo impar. Muestre que el conjunto $\{[1^2]_p, [2^2]_p, \ldots, [(p-1)^2]_p\}$ tiene exactamente $(p-1)/2$ elementos distintos.

Demostración. Notar que

$$a^2 \equiv_p a^2 - 2ap + p^2 \equiv_p (p-a)^2$$

Luego, $\{[1^2]_p, [2^2]_p, \ldots, [((p-1)/2)^2]_p\}$ tiene la misma cantidad de elementos distintos que el conjunto original. Supongamos que hay dos elementos iguales dentro de este conjunto. Luego, existen $1 \leq a < b \leq (p-1)/2$ tales que $a^2 \equiv_p b^2$. Luego, $p \mid b^2 - a^2 = (b-a)(b+a)$. Como p es primo, entonces $p \mid b - a$ o $p \mid b + a$. Pero $2 \leq a + b \leq p - 2$, por lo que $(p, a + b) = 1$. Así, $p \mid b - a$ y $a = b$, $\rightarrow\leftarrow$.

Por lo tanto, hay exactamente $(p-1)/2$ elementos distintos. ∎

Bonus: *(Iberoamericana 2016)* Encuentre todos los primos p, q, r, k tales que

$$pq + pr + qr = 12k + 1.$$

Demostración. Sin perder generalidad, $p \leq q \leq r$. Viendo la igualdad inicial módulo 4, tenemos que

$$pq + pr + qr \equiv_4 1.$$

Si ninguno de los primos es 2, entonces son de la forma $4k \pm 1$. Por inspección, vemos que ninguna de las opciones genera la igualdad de arriba. Luego, alguno de los 3 primos es 2, y por la desigualdad inicial $p = 2$. Reemplazando, se tiene

$$2q + 2r + qr = 12k + 1.$$

Viendo esta igualdad módulo 3, se tiene

$$2q + 2r + qr \equiv_3 1.$$

Si ninguno de los primos es 3, entonces son de la forma $3k \pm 1$. Igual que antes, ninguna de las configuraciones da la igualdad buscada, por lo que alguno de los 2 primos restantes es 3, y por la desigualdad inicial $q = 3$. Volviendo a reemplazar:

$$5 + 5r = 12k.$$

Desde acá, $5 \mid 12k$, por lo que $5 \mid k$. Como k es primo, $k = 5$. Reemplazando, se tiene $r = 11$.

Por lo tanto, las soluciones son $\{p, q, r\} = \{2, 3, 11\}$ (en algún orden) y $k = 5$. ∎