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

Ayudantía 07

09 de Octubre

MAT2225 - Teoría de Números

1) Sea $p \geq 3$ primo. Muestre que 4 no es raíz primitiva módulo p.

Demostración. Como $p \geq 3$, p es impar y $(p, 2) = 1$. Luego, por Euler, $2^{p-1} \equiv_p 1$. Luego, se tiene que

$$4^{\frac{p-1}{2}} \equiv_p (2^2)^{\frac{p-1}{2}} \equiv_p 2^{p-1} \equiv 1$$

Luego, 4 no puede ser una raíz primitiva. ∎

2) Encuentre una raíz primitiva módulo 343.

Solución. Por inspección se tiene que 3 es raíz primitiva módulo 7. Por teorema visto en clases, 3 o 10 es raíz primitiva módulo 49. Revisando 3 primero, basta ver que 3^{42} es congruente a 1, y que 3^k falla, con $k \mid 42$ menor a 42. Para esto, notemos que $3^2 \equiv_{49} 9$, $3^3 \equiv_{49} 27$, $3^6 \equiv_{49} (3^3)^2 \equiv_{49} 27^2 \equiv_{49} -6$, $3^7 \equiv_{49} 3^6 \cdot 3 \equiv_{49} -6 \cdot 3 \equiv_{49} -18$, $3^{14} \equiv_{49} (3^7)^2 \equiv_{49} (-18)^2 \equiv_{49} 30$, y $3^{21} \equiv_{49} 3^7 \cdot 3^{14} \equiv_{49} (-18) \cdot 30 \equiv_{49} -1$. Luego, ninguna de las opciones menores funciona. Para verificar que es raíz primitiva, basta ver que $3^{42} \equiv_{49} (3^{21})^2 \equiv_{49} (-1)^2 \equiv_{49} 1$. Como 3 es raíz primitiva módulo 7^2, es raíz primitiva módulo 7^k para todo $k \geq 2$, en particular para $7^3 = 343$. ∎

3) Muestre que si $p \geq 3$ es primo y g, g' son raíces primitivas módulo p, entonces gg' no es una raíz primitiva módulo p.

Demostración. Como p es impar, $p - 1$ es par. Además, como p es primo y g, g' son raíces primitivas, entonces $g^{(p-1)/2} \equiv_p g'^{(p-1)/2} \equiv_p -1$. Luego,

$$(gg')^{(p-1)/2} \equiv_p (g)^{(p-1)/2}(g')^{(p-1)/2} \equiv_p (-1)^2 \equiv 1.$$

Por lo tanto, gg' no puede ser raíz primitiva. ∎

4) Suponga que existe una raíz primitiva módulo n. Pruebe que existen exactamente $\varphi(\varphi(n))$ raíces primitivas módulo n.

Demostración. Sea g la raíz primitiva. Tenemos que $g, g^2, \ldots, g^{\varphi(n)}$ es el grupo completo de unidades, por lo que todas las raíces primitivas son de la forma g^k, con $1 \leq k \leq \varphi(n)$. Mostraremos que solo los k coprimos con $\varphi(n)$ funcionan.

Si $(k, \varphi(n) = a \neq 1$, basta ver que

$$(g^k)^{\frac{\varphi(n)}{a}} \equiv_n (g^{\varphi(n)})^{\frac{k}{a}} \equiv_n 1^{\frac{k}{a}} \equiv_n 1,$$

donde todas las fracciones son naturales por definición de gcd. Luego, los únicos candidatos a raíz primitiva son los exponentes coprimos con $\phi(n)$.

Para mostrar que todos los exponentes coprimos con $\phi(n)$ funcionan, supongamos que existe un k coprimo con $\varphi(n)$ tal que $\mathrm{ord}_n(g^k) = m < \varphi(n)$. Luego, $m \mid \varphi(n)$ (ya que $(g^k)^{\varphi(n)} \equiv_p (g^{\varphi(n)})^k \equiv_n 1$. Del mismo modo, $1 \equiv_n (g^k)^m \equiv_n g^{km}$. Pero el orden de g es $\varphi(n)$, por lo que $\varphi(n) \mid km$. Como $(\varphi(n), k) = 1$, lo anterior implica $\varphi(n) \mid m$. Como $\varphi(n) \mid m$ y $m \mid \varphi(n)$, se tiene la igualdad.

Por lo tanto, los únicos elementos que son raíz primitiva son g^k, donde $1 \leq k \leq \varphi(n)$ y $(k, \varphi(n)) = 1$. Así, se tienen exactamente $\varphi(\varphi(n))$ raíces primitivas, que es lo que buscábamos. ∎

5) Determine cuantas soluciones tienen las siguientes ecuaciones:

a) $x^{12} \equiv_{17} 16$.

Solución. Sea g una raíz primitiva de $\mathbb{Z}/17\mathbb{Z}$. Como 17 es primo, se tiene que $g, g^2, \ldots, g^{16}$ forma todas las unidades. Además, como $16 \equiv_{17} -1$, se tiene que $16 \equiv_{17} g^8$. Luego, podemos reescribir la ecuación como

$$(g^k)^{12} \equiv_{17} g^8.$$

Esto es equivalente a

$$g^{12k-8} \equiv_{17} 1,$$

donde k está entre 1 y 16. Como $\mathrm{ord}_{17}(g) = 16$, lo anterior es equivalente a buscar los valores de k que cumplen $16 \mid 12k - 8$, por lo que hay 4 soluciones (los exponentes $\{2, 6, 10, 14\}$ funcionan). ■

b) $x^{20} \equiv_{17} 13$. Notar que 0 no es solución. Luego, $x^{16} \equiv_{17} 1$ y la ecuación se reduce a

$$x^4 \equiv_{17} 13.$$

También, notar que $13^2 \equiv_{17} 169 \equiv_{17} -1$. Luego, $13^2 \equiv_{17} g^8$, por lo que $13 \equiv_{17} g^4$ o $13 \equiv_{17} g^{12}$. Sin perder generalidad, supongamos que es congruente a g^4 (en otro caso, basta elegir g^{-1} en vez de g como raíz primitiva). Así, nuestra ecuación se reduce a

$$g^4 k \equiv_{17} g^4,$$

que es equivalente a

$$g^{4k-4} \equiv_{17} 1.$$

De nuevo, buscamos soluciones entre 1 y 16 a $16 \mid 4k - 4$, por lo que hay 4 soluciones (los exponentes $\{1, 5, 9, 13\}$ funcionan).

Bonus: TBD