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

Ayudantía 06

02 de Octubre

MAT2225 - Teoría de Números

1) Pruebe que si a es invertible en $\mathbb{Z}/p\mathbb{Z}$, entonces a es invertible en $\mathbb{Z}/p^k\mathbb{Z}$ para todo k natural.

Solución. Como a es invertible, existe un b en $\mathbb{Z}/p\mathbb{Z}$ tal que $ab \equiv_p 1$. Consideremos el polinomio $f(x) = bx - 1$. Notar que $f(a) = ab - 1 \equiv_p 1 - 1 \equiv_p 0$. $f'(x) = b \not\equiv_p 0$ (ya que b es invertible). Luego, por lema de Hensel existe un x tal que $x \equiv_{p^k} a$ y $f(x) \equiv_{p^k} 0$, por lo que tenemos lo pedido. ∎

2) Pruebe que si a, k son coprimos con p, entonces a es una potencia $k-$ésima módulo p si y solo si es una potencia $k-$ésima módulo p^n para todo n natural.

Solución.
$\Leftarrow$: Como es potencia $k-$ésima, existe un x tal que $x^k \equiv a \pmod{p^n}$. Esto dice que $x^k = p^n \cdot c + a$, por lo que $x^k \equiv_p a$.

$\Rightarrow$: Tomemos el polinomio $f(x) = x^k - a$. Como a es potencia $k-$ésima módulo p, existe un b tal que $f(b) \equiv_p 0$. $f'(x) = kx^{k-1}$. La única solución a $f'(x) \equiv_p 0$ es $x \equiv_p 0$, pero si $f(0) \equiv_p 0$ entonces a no sería coprimo con p, $\rightarrow\leftarrow$. Usando lema de Hensel se tiene lo pedido. ∎

3) Calcule todos los cuadrados módulo 25 y 125.

Solución. Recordemos que los cuadrados módulo 5 son $0, 1$ y 4. Los elementos módulo 25 son de la forma $25k+a$, con $0 \leq a < 25$. Si $(5, 25k+a) = 1$, por la pregunta anterior $25k+a$ es cuadrado módulo 25 ssi es cuadrado módulo 5. Luego, a tiene que ser cuadrado módulo 5. Luego, $a = 5j + 1$

o $5j+4$. Esto nos da $1, 4, 6, 9, 11, 14, 16, 19, 21$ y 24.

Si $25k+a$ no es coprimo con 5, entonces $a = 5a'$. Luego, $25k + 5a' = 5(5k + a')$. Como es un cuadrado, $5k + a'$ es un múltiplo de 5 y $a' = 5a''$. Luego, $a = 25a''$ y $0 \leq a < 25$, por lo que $a = 0$.

Por lo tanto, los residuos módulo 25 son $0, 1, 4, 6, 9, 11, 14, 16, 19, 21$ y 24.

Para módulo 125, podemos escribir $n = 125k + a$, donde $0 \leq a < 125$. Si $(a, 5) = 1$, haciendo lo mismo de antes tenemos que todos los $a \equiv_5 1, 4$ son cuadrados.

Si $(a, 5) \neq 1$, entonces $(a, 5) = 5$ y $a = 5a'$. Luego, $n = 125k + 5a' = 5(25k + a')$. Como $5(25k + a')$ es un cuadrado, $\nu_5(5(25k + a'))$ es par y $a' = 5a''$. Luego, $n = 25(5k + a'')$. Como $5k + a''$ es un cuadrado, entonces $a'' \equiv_5 0, 1$ o 4. Pero $a = 25a''$ y $0 \leq a < 125$, por lo que $0 \leq a'' < 5$. Revisando los 3 casos, se tiene que $0, 25$ y 100 son cuadrados. ∎

4) Sean a, n coprimos y l, m enteros positivos tales que $a^m \equiv_n a^l$. Pruebe que $m \equiv l \pmod{\text{ord}_n(a)}$.

Solución. Multiplicando por a^{-l} a ambos lados, tenemos que $a^{m-l} \equiv_n 1$. Luego, $\text{ord}_n(a) \mid m - l$ y $m \equiv l \pmod{\text{ord}_n(a)}$ por definición. ∎

5) Muestre que existen infinitos n tales que todos los divisores mayores a 1 de $2^n - 1$ son mayores que n.

Solución. Probaremos que los $n > 2$ primos funcionan. Sea $q \neq 1$ el divisor más pequeño de $2^n - 1$. Notar que q es impar y primo. Consideremos $\text{ord}_q(2)$. Sabemos que $\text{ord}_q(2) \mid n$. Como n es primo, $\text{ord}_q(2) = 1$ o $\text{ord}_q(2) = n$. Si $\text{ord}_q(2) = 1$, entonces $2 \equiv_q 1$, $\rightarrow\leftarrow$. Luego, $\text{ord}_q(2) = n$. Por Euler, $2^{q-1} \equiv_q 1$ y $n \mid q - 1$, por lo que $n \leq q - 1$ y $n < q$. ∎

Bonus: Sea $p > 2$ primo. Muestre que si a es raíz primitiva módulo p y p^2, entonces a es raíz primitiva módulo p^k para todo k natural.