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

Ayudantía 10

30 de Octubre

MAT2225 - Teoría de Números

1) Sean $m, n \geq 2$ enteros positivos tales que $2^m - 1 \mid 3^n - 1$. Pruebe que n es par.

Proof. Supongamos que n es impar. Sea p algún primo que divide a $2^m - 1$. Luego, $p \mid 3^n - 1$. Esto implica que $3^n \equiv_p 1$, por lo que $3^{n+1} \equiv_p 3$ y 3 es residuo cuadrático. Usando reciprocidad cuadrática, se tiene

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

Claramente p no puede ser 3. Si p es residuo mod 3, entonces $p \equiv_3 1$. Por otro lado, como el lado derecho debe ser 1, entonces $p \equiv_4 1$, y por lo tanto $p = 12k + 1$ para algún k natural. Si p no es residuo, entonces es de la forma $3a - 1$, y es de la forma $4b - 1$ (ya que el lado derecho también debe ser -1), por lo que es de la forma $12k - 1$. Como esto aplica para cualquier $p \mid 2^m - 1$ primo, todos los factores primos de $2^m - 1$ son de la forma $12k \pm 1$, y por lo tanto $2^m - 1$ también lo es. Pero por inspección tenemos que $2^m - 1 \equiv_{12} 3, 7$ con $m \geq 2$, $\rightarrow\leftarrow$.

Por lo tanto, n debe ser par. ∎

2) Sea $f(n) = n^2 + 8n + 11$ y p un primo que divide a $f(n)$ para algún n natural. ¿De qué forma es p?

Solución. $2, 5$ funcionan con $n = 1$. Ahora, sea p un primo impar distinto de 5 que divide a $n^2 + 8n + 11$ para algún n. Luego, tenemos que $p \mid n^2 + 8n + 11 = (n+4)^2 - 5$. Así, $(n+4)^2 \equiv_p 5$ y 5 es residuo cuadrático. Usando reciprocidad cuadrática tenemos que

$$\left(\frac{5}{p}\right)_L \cdot \left(\frac{p}{5}\right)_L = (-1)^{\frac{(5-1)(p-1)}{4}} = 1.$$

Luego, $\left(\frac{p}{5}\right) = 1$ y p es de la forma $5k \pm 1$. ∎

3) Sea p un número primo. Muestre que existe un x tal que $p \mid x^2 - x + 3$ ssi existe un y tal que $p \mid y^2 - y + 25$.

Solución. Para $p = 2$ se tiene $x = y = 1$. Para $p = 3$ se tiene $x = 3, y = 2$. Para $p = 11$ se tiene $x = y = 11$. Sea p distinto de los anteriores primo. Si existe un x que cumple lo pedido, entonces $p \mid 4(x^2-x+3) = (2x-2)^2+11$, por lo que -11 es residuo cuadrático mod p. Del mismo modo, si existe un y que cumple lo pedido, entonces $p \mid 4(y^2 - y + 25) = (2y - 2)^2 + 99$, por lo que -99 es residuo cuadrático. Como $p \neq 3, 11$ nos piden probar entonces que -99 es residuo ssi -11 es residuo. Como $-99 = -11 \cdot 9$, 9 es claramente residuo y la función $\left(\frac{a}{p}\right)_L$ es multiplicativa, se tiene lo pedido. ∎

4) Reduzca la siguiente matriz en $Z[n]$:

$$\begin{pmatrix} 8 & 3 & 4 \\ 1 & 5 & 9 \\ 6 & 7 & 2 \end{pmatrix}$$

Solución. Cambiando la primera y segunda fila, y restando la nueva primera fila suficientes veces a las otras dos, se llega a

$$\begin{pmatrix} 1 & 5 & 9 \\ 0 & -37 & -68 \\ 0 & -23 & -52 \end{pmatrix}.$$

Multiplicando por -1 en la segunda y tercera fila, lo anterior es equivalente a

$$\begin{pmatrix} 1 & 5 & 9 \\ 0 & 37 & 68 \\ 0 & 23 & 52 \end{pmatrix}.$$

Como $(37, 23) = 1$, aplicando el algoritmo de la división en estas dos filas la matriz anterior se puede llevar a

$$\begin{pmatrix} 1 & 5 & 9 \\ 0 & 1 & -76 \\ 0 & 4 & 56 \end{pmatrix}.$$

Restando 4 veces la segunda fila a la tercera, se llega a

$$\begin{pmatrix} 1 & 5 & 9 \\ 0 & 1 & -76 \\ 0 & 0 & 360 \end{pmatrix}.$$

Trabajando un poco en la primera fila, lo anterior se puede dejar como

$$\begin{pmatrix} 1 & 0 & 29 \\ 0 & 1 & -76 \\ 0 & 0 & 360 \end{pmatrix}.$$

$\blacksquare$