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

Ayudantía 11

30 de Octubre

MAT2225 - Teoría de Números

1) Considere la función f definida como

$$f\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2x+y+z \\ x+2y+z \\ x+y+2z \end{pmatrix}$$

Encuentre las soluciones (x, y, z) en $[0, 1)^3$ tales que $f(x, y, z) \in \mathbb{Z}^3$.

Proof. Notar que la función se puede escribir como $f(\vec{v}) = A\vec{v}$, donde

$$A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$$

Luego, tenemos que la cantidad de soluciones está dada por el determinante de A, que es 4. Haciendo el reemplazo $x = y = z = k$, se tiene que $f(k, k, k) = (4k, 4k, 4k)$. Esto dice que $k = 1, 1/2, 1/4$ y 0 genera soluciones enteras. Como solo hay 4 soluciones, estas son las únicas. ∎

2) Sea $p \equiv_4 3$ primo tal que $q = 2p + 1$ también lo es. Muestre que $2^p - 1$ no puede ser primo.

Proof. Supongamos que $2^p - 1 = r$ es primo. Luego, $2^p \equiv_r 1$ y $2^{p+1} \equiv_r p$. Como $p + 1$ es par y $(2, r) = 1$, se tiene que p es residuo cuadrático módulo r. Por otro lado, $r \equiv_p 2^p - 1 \equiv_p 2 - 1 \equiv_p 1$, por lo que r es residuo cuadrático módulo p. Pero ambos son de la forma $4k + 3$, con lo que usando reciprocidad cuadrática genera a una contradicción.

Por lo tanto, $2^p - 1$ es compuesto. ∎

3) Encuentre todos los primos p tales que

a) 7

b) 15

sea un residuo cuadrático.

Solución.

a) 2 claramente funciona. Sea $p \neq 2, 7$ primo. Luego, buscamos que $\left(\frac{7}{p}\right)_L = 1$. Por reciprocidad cuadrática, se tiene

$$\left(\frac{7}{p}\right)_L \left(\frac{p}{7}\right)_L = (-1)^{(p-1)(7-1)/4} = (-1)^{(p-1)/2}.$$

Así, tenemos que $\left(\frac{7}{p}\right)_L = 1$ si $\left(\frac{p}{7}\right)_L = (-1)^{(p-1)/2}$. Tenemos dos casos:

- $p \equiv_4 1$. Luego, $(-1)^{(p-1)/2} = 1$, y buscamos además que $\left(\frac{p}{7}\right)_L = 1$. Como los residuos cuadráticos módulo 7 son $\{1, 2, 4\}$, usando CRT tenemos tres soluciones módulo 28 ($\{1, 9, 25\}$).
- $p \equiv_4 = 3$. Luego, $(-1)^{(p-1)/2} = -1$ y $\left(\frac{p}{7}\right)_L = -1$. Los no-residuos son $\{3, 5, 6\}$. De nuevo, por CRT tenemos 3 souciones ($\{3, 19, 27\}$).

Juntando todo se tiene lo pedido.

■