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.

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.

3) Calcule todos los cuadrados módulo 25 y 125.

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

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

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.