Prueba de Evaluación (Diciembre de 2018)

Problema

a) Probar que $mcd(x^2+y^2,4)=2$ si x e y son impares. (2 puntos)

b) Si a es un número no es divisible por un número p primo, y $n \equiv m \mod(p-1)$. Demostrar que $a^n \equiv a^m \mod(p)$ (4 puntos)

c) Encontrar el residuo de la división del número $(12371^{12}+34)^{28}$ por 11. (4 puntos)

Solución

a) Sean $x=2n+1$ e $y=2m+1$, entonces $x^2+y^2=4(n^2+m^2+m+n)+2$, por lo tanto $mcd(x^2+y^2,4)=2$.

b) Supongamos que $n>m$. Como $p-1 \mid n-m$, tenemos que $n-m=c(p-1)$ para algún entero positivo c. Como a no es no es divisible por p, por el Pequeño Teorema de Fermat, $a^{p-1} \equiv 1 mod(p)$ y $a^{(p-1)c} \equiv 1\ mod(p)$, así $a^{n-m} \equiv 1 mod(p)$, como $a^m \equiv a^m mod(p)$, tenemos que $a^{n-m}a^m \equiv a^m\ mod(p)$, por lo tanto $a^n \equiv a^m \mod(p)$.

c) Como $12371 \equiv 7 \mod(11)$ y $34 \equiv 1 \mod(11)$, se tiene que

$12371^2 \equiv 5 \mod(11)$,

$12371^6 \equiv 4 \mod(11)$, y $12371^{12} \equiv 5 \mod(11)$.

Por lo tanto

$12371^{12}+34 \equiv 6 \mod(11) \Rightarrow$

$(12371^{12}+34)^2 \equiv 3 \mod(11) \Rightarrow$

$(12371^{12}+34)^{14} \equiv 9 \mod(11) \Rightarrow$

$(12371^{12}+34)^{28} \equiv 4 \mod(11)$.