13 de mayo de 2024

Teoría de números

Osmar Dominique Santana Reyes

1. Sea $m = 1, 2, 4, p^\alpha, 2p^\alpha$, con p primo impar y $\alpha \in \mathbb{N}$, y $a \in \mathbb{Z}$. $x^n \equiv a(\mod m)$ tiene $(n, \phi(m))$ soluciones si y solo si $a^{\frac{\phi(m)}{(n,\phi(m))}} \equiv 1 (\mod m)$.

   Demostración.

   Sea g raíz primitiva módulo m e $i \in \{1, 2, \ldots, \phi(m)$ tal que $g^i \equiv a (\mod m)$.

   Primero, si se supone que $x^n \equiv a (\mod m)$ tiene $(n, \phi(m))$ soluciones, entonces sea x_0 una de estas soluciones y u tal que $x_0 \equiv g^u (\mod m)$, se tiene que

   $$g^i \equiv a \equiv x_0^n \equiv g^{un} (\mod m)$$

2.