Ecuaciones lineales con congruencias

Teorema Dados $a, b, n \in \mathbb{Z}$ y sea $d = mcd(a, n)$. Entonces la ecuación $ax \equiv b \pmod{n}$ tiene solución $\leftrightarrow d \mid b$

Además existen exactamente d soluciones distintas mod n.

Definición Fijado n, decimos que $a \in \mathbb{Z}$ es **invertible módulo n** si $\exists c \in \mathbb{Z}: ac \equiv 1 \pmod{n}$

Siendo c el inverso de a módulo n

Corolario

a es invertible mod $n \leftrightarrow mcd(a, n) = 1$

Además si a es invertible el inverso de a módulo n es único módulo n

OBS: 2 es invertible módulo n $\leftrightarrow n$ es impar.