Congruencia

Ecuaciones de congruencias

- $a \equiv b \pmod{m}$
- $k.a \equiv k.a \pmod{b} \Leftrightarrow k \perp b$
- $ka \equiv kb \pmod{km} \Leftrightarrow a \equiv b \pmod{m}$
- $a^n \equiv 0 \pmod{p} \Leftrightarrow a \equiv 0 \pmod{p}$
- $n \equiv x_0 \pmod{m} \Leftrightarrow \begin{cases} n \equiv x_1 \pmod{p_0} \\ n \equiv x_2 \pmod{p_1} \\ \dots \\ n \equiv x_m \pmod{p_n} \end{cases}$
- $ax \equiv b \pmod{m} \Rightarrow ax + my = b \overset{\text{tiene solucion}}{\Leftrightarrow} (a:m)|b$

Ecuaciones Diofanticas

Sea $ax + by = c \overset{\text{tiene solucion}}{\Leftrightarrow} (a:b)|c$

$\Rightarrow ax + bx = c \overset{\text{coprimizar}}{\Leftrightarrow} \frac{a}{(a:b)}x + \frac{b}{(a:b)}x = \frac{c}{(a:b)} \Leftrightarrow a'x + b'x = c'$

busco solucion particular:

$a'x + b'x = c' \Rightarrow a'(s) + b'(t) = c'$

$\Rightarrow s_0 = (x_0, y_0) = (s, t)$

busco solucion general:

$(a, b) = k(b', -a') + (x_0, y_0) = (b'k + x_0, -a'k + y_0)$

TCR

sean $a \perp b \perp c$

$$\begin{cases} n \equiv x_1 \pmod{a} \\ n \equiv x_2 \pmod{b} \\ n \equiv x_3 \pmod{c} \end{cases}$$

por TCR $\exists!$ $solucion\ x_0 : n \equiv x_0 \pmod{a.b.c}$

PTF

Sea p primo $\wedge\ p \nmid a$:

- $a^p \equiv a \pmod{p}$
- $a^{p-1} \equiv 1 \pmod{p}$
- $a^n \equiv a^{r_{p-1}n} \pmod{p}$