$a \equiv a \mod n$ reflexive

$a \equiv b \mod n \Leftrightarrow b \equiv a \mod n$ symmetric

$(a \equiv b \mod n \wedge b \equiv c \mod n) \Rightarrow (a \equiv c \mod n)$ transitive

$$\left[\begin{array}{l} a \equiv b \mod n \\ a \% n = b \% n \\ a = b + kn \\ n \mid a-b \end{array}\right]$$

all equivalent definitions

If: $a_1 \equiv b_1 \mod n \wedge a_2 \equiv b_2 \mod n$

Then:

$$\left.\begin{array}{l} a_1 + a_2 \equiv b_1 + b_2 \mod n \\ a_1 a_2 \equiv b_1 b_2 \mod n \\ a_1 - a_2 \equiv b_1 - b_2 \mod n \end{array}\right] \begin{array}{l} + \\ \times \\ - \end{array}$$

no division

multiplicative inverse of a for mod n

$a u \equiv 1 \mod n$

$(u \text{ exists}) \Leftrightarrow (n \perp a)$

There can be many or no multiplicative inverses

$$\left.\begin{array}{l} a x \equiv b \mod n \\ x \equiv u b \mod n \end{array}\right]$$

use this instead of division to solve certain congruences

Fermat's Little Thm.

p is positive prime $\quad a^p \equiv a \mod p$

Corollary

p is positive prime $\wedge\ p \nmid a \quad a^{p-1} \equiv 1 \mod p$

notice relationship

Euler's Thm.

$a \perp n \quad a^{\varphi(n)} \equiv 1 \mod n$

Totient of n: number of integers from $[n]$ which are coprime to n

$$\varphi(n) = \left| \{ k \in [n] \mid k \perp n \} \right|$$

$$\varphi(p) = p - 1$$

$$\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

Wilson's Thm

$(n \text{ is prime}) \Leftrightarrow (n-1)! \equiv -1 \mod n$

Chinese Remainder Thm.

$m \perp n$

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases} \Rightarrow x \equiv y \mod mn$$