

Congruences

Congruence

Definition: Let n be a natural number and let a and b be integers. We say that a and b are **congruent** modulo n if $n|(a - b)$. We write this as $a \equiv b \pmod{n}$.

Examples:

Some basic properties of congruences

Proposition: Let n be a natural number and let a , b , and c be integers. Congruence has the following properties:

- ▶ $a \equiv a \pmod{n}$.
- ▶ If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.
- ▶ If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$.
(Chapter 5, Problem B19)

More properties

Arithmetic Progressions.

What is $\{x : x \equiv a \pmod{n}\}$?

Congruence arithmetic.

Proposition: Given integers a , b , c , and a natural number n , if $a \equiv b \pmod{n}$ then

► $a + c \equiv b + c \pmod{n}$

► $ac \equiv bc \pmod{n}$

► $a^r \equiv b^r \pmod{n}$ for any natural number r .

Casting out nines