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:

$8 \equiv 4 \mod 2$ $\quad 2|(8-4)$

$7 \equiv 2 \mod 5$ $\quad 5|(7-2)$

$101 \equiv 64 \mod 37$ $\quad 37|101-64$

which x are $\equiv 1 \mod 3$?

$\ldots -5, -2, 1, 4, 7, 10, 13, \ldots$

$3|(x-1)$

$x-1 = 3k \quad k \in \mathbb{Z}$

$x = 3k+1 \quad k \in \mathbb{Z}$

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:

- $a \equiv a \pmod{n}$. $n \mid (a-a)$ ⊗ $n \mid 0$ because $0 = n \cdot 0$
- If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$. $n \mid (a-b) \Rightarrow a - b = kn$, $b - a = (-k)n$
- If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$. (Chapter 5, Problem B19)

If $n \mid (b-a)$ and $n \mid (c-b)$ then $n \mid (c-a)$

$\begin{cases} b - a = kn \\ c - b = k'n \end{cases}$ want → $c - a = k''n$

$c - b + b - a = (k + k')n = c - a$

$k'' = k + k'$

More properties

Arithmetic Progressions.

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

$$\{x : x \equiv 1 \bmod 3\}$$

$$= \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$$

$$\{x : x \equiv 5 \bmod 11\}$$

$$\ldots, -28, -17, -6, 5, 16, 27, 38, \ldots$$

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