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:

$n = 7$

$a = 11 \quad b = 3$

is $11 \equiv 3 \bmod 7$?

does 7 divide $11 - 3 = 8$

is $8 = 7x$ where x is an integer

$n = 7$

$a = 11 \quad b = 4$

$a - b = 11 - 4 = 7$

that is a multiple of 7

$11 \equiv 4 \bmod 7$.

$n = 7$

$13 = 1 \cdot 7 + 6$

$13 - 6 = 1 \cdot 7$

$13 \equiv 6 \bmod 7$

$20 = 2 \cdot 7 + 6$

$27 = 3 \cdot 7 + 6$

$34 = 4 \cdot 7 + 6$

!

$20 \equiv 6 \bmod 7$

$20 - 6 = 14 = 2 \cdot 7$

$34 \equiv 20 \ (7)$

$34 - 20 = 14 = 2 \cdot 7$

6, 13, 20, 27, 34, ...

0 1 2 3 4 5 6 7 8 9 10 11 12

$n = 2$

$a \equiv 0 \ (2)$ a even

$a \equiv 1 \ (2)$

$a = 2k + 1$

$a - 1 = 2k$

$a \equiv 1 \bmod 2$

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:

- $a \equiv a \pmod{n}$. Proof: $n \mid (a-a)$ or $n \mid 0$ because $0 = n \cdot 0$.
- If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$. Pf: if $a \equiv b \bmod n$ then $n \mid (a-b)$ so $a-b = kn$, $b-a = (-k)n$, $n \mid (b-a)$
- If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$. (Chapter 5, Problem B19)

$n = 5$

$7 \equiv 2 \bmod 5$ $(7-2 = 5 \cdot 1)$

$137 \equiv 2 \bmod 5$ $137-2 = 135$ a multiple of 5

$7 \equiv 2 \ (5)$ and $2 \equiv 137 \bmod 5$ and so $7 \equiv 137 \bmod 5$

More properties

Arithmetic Progressions.

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

Fix $n \in \mathbb{N}$ and $a \in \mathbb{Z}$.

$\{x : x \equiv a \pmod{n},\ x \in \mathbb{Z}\}$.

$x \equiv a \bmod n$ means $x - a = k \cdot n$ for some integer k.

$x = a + kn \quad k \in \mathbb{Z}$,

$n = 5 \quad a = 3$

$\{x : x \equiv 3 \bmod 5\} = \{3 + 5k : k \in \mathbb{Z}\}$

$\{\ldots, -12, -7, -2, 3, 8, 13, 18, 23, \ldots\}$ arithmetic progression

This is all integers with remainder 3 when divided by 5

$N = 5k + r$ $\quad N - r = 5k$ $\quad N \equiv r \bmod 5$

$r = 0, 1, 2, 3, 4$