Session 54: Congruence

- Congruences
- Properties of congruences

Congruence Relation

Definition: If a and b are integers and m is a positive integer, then ***a* is congruent to *b* modulo *m*** if m divides $a - b$.

Notations

- The notation $a \equiv b$ (**mod** m) says that a is congruent to b modulo m.
- We say that $a \equiv b$ (**mod** m) is a **congruence** and that m is its **modulus**.
- If a is not congruent to b modulo m, we write $a \not\equiv b$ (**mod** m)

Theorem: $a \equiv b \pmod{m}$ is an equivalence relation.

Example

Determine whether 17 is congruent to 5 modulo 6

$17 - 5 = 12$, $6 \mid 12$ therefore $17 \equiv 5 \pmod 6$

Determine whether 24 and 14 are congruent modulo 6.

$24 - 14 = 10$, $6 \nmid 10$ therefore $24 \not\equiv 14 \pmod 6$

(mod m) and mod m Notations

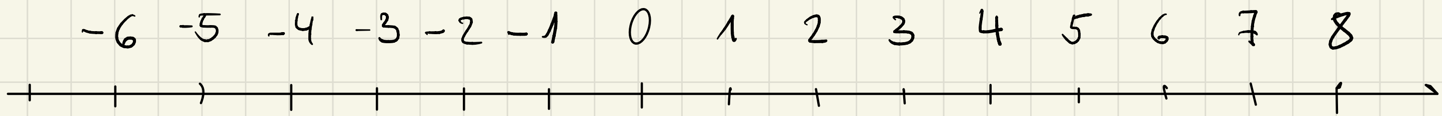
The notations $a \equiv b$ (**mod** m) and a **mod** $m = b$ are different.

- $a \equiv b$ (**mod** m) is a ***relation*** on the set of integers.
- In a **mod** $m = b$, the notation **mod** denotes a ***function***.

Theorem 3: Let a and b be integers, and let m be a positive integer. Then $a \equiv b$ (**mod** m) if and only if a **mod** $m = b$ **mod** m.

Corollary: Two integers are congruent **mod** m if and only if they have the same remainder when divided by m.

Illustration : $m = 4$



$-5 \bmod 4 = 3$ $\quad -1 \bmod 4 = 3$ $\quad 3 \bmod 4 = 3$ $\quad 7 \bmod 4 = 3$

$-5 \equiv -1 \pmod 4$ $\quad -1 \equiv 3 \pmod 4$ $\quad 3 \equiv 7 \pmod 4$

also : $-5 \equiv 7 \pmod 4$

note : $\equiv$ is transitive

Theorem on Congruences

Theorem 4: Let m be a positive integer. The integers *a* and *b* are congruent modulo *m* if and only if there is an integer *k* such that $a = b + km$.

Proof: • assume $a \equiv b \pmod{m}$, by definition $m \mid a-b$, by definition there exists k such that $km = a-b$ and therefore $a = b + km$

• assume $a = b + km$, therefore $km = a - b$, and $m \mid a - b$, and thus $a \equiv b \pmod{m}$

Congruences of Sums and Products

Theorem 5: Let m be a positive integer.
If $a \equiv b$ (**mod** m) and $c \equiv d$ (**mod** m),
then $a + c \equiv b + d$ (**mod** m) and $ac \equiv bd$ (**mod** m).

Proof: there exist k_1, k_2 s.t. $a = b + k_1 m$ and $c = d + k_2 m$

Therefore $a + c = b + d + (k_1 + k_2)m$ and thus $a + c \equiv b + d \pmod{m}$

and $a \cdot c = b \cdot d + b \cdot k_2 m + d \cdot k_1 m + k_1 \cdot k_2 m =$

$= b \cdot d + (b \cdot k_2 + d k_1 + k_1 \cdot k_2) m$

Example

Because $7 \equiv 2$ (**mod** 5) and $11 \equiv 1$ (**mod** 5)

$18 \equiv 3 \pmod 5$ and $77 \equiv 2 \pmod 5$

Algebraic Manipulation of Congruences

Multiplying both sides of a valid congruence by an integer preserves validity.

If $a \equiv b \pmod{m}$ then $c \cdot a \equiv c \cdot b \pmod{m}$, where c is any integer.

Proof: by Theorem 5 with $d = c$.

Adding an integer to both sides of a valid congruence preserves validity.

If $a \equiv b \pmod{m}$ then $c + a \equiv c + b \pmod{m}$, where c is any integer

Proof: by Theorem 5 with $d = c$.

Example

Since $14 \equiv 8$ (**mod** 6) also

multiply by 2 : $28 \equiv 16 \pmod{6}$

add 7 $21 \equiv 15 \pmod{6}$

Dividing both sides by 2 does not produce a valid congruence:

$7 \not\equiv 4 \pmod{6}$

Dividing a congruence by an integer does not always produce a valid congruence!

Summary

- Definition of congruences
- **mod** m relation vs. **mod** function
- Congruences of arithmetic operations

Theorem: If $n = 4k+3$ for some positive integer $k > 0$, then n is not the sum of two squares

Proof: we show that if m is an integer, then $m^2 \equiv 0$ or $1 \pmod 4$

Case 1: m is even, then m^2 is even, therefore, $m^2 \equiv 0 \pmod 4$

Case 2: m is odd, then m^2 is odd, therefore, $m^2 \equiv 1 \pmod 4$

Let n be the sum of two squares n_1, n_2, $n = n_1 + n_2$

n_1, n_2 are $\equiv 0$ or $1 \pmod 4$

therefore using theorem 5, $n_1 + n_2$ is $\equiv 0, 1, 2 \pmod 4$

Thus, n cannot be of the form $4k+3$, since $4k+3 \equiv 3 \pmod 4$