CS/MATH 111, Discrete Structures - Fall 2018. Discussion 3 - Modular Arithmetic

Andres, Sara, Elena

University of California, Riverside

October 11, 2018

Outline

Definition

$$\frac{A}{B} = Q \ remainder \ R$$

- A is the dividend
- B is the divisor
- Q is the quotient
- R is the remainder

$$A \bmod B = R$$

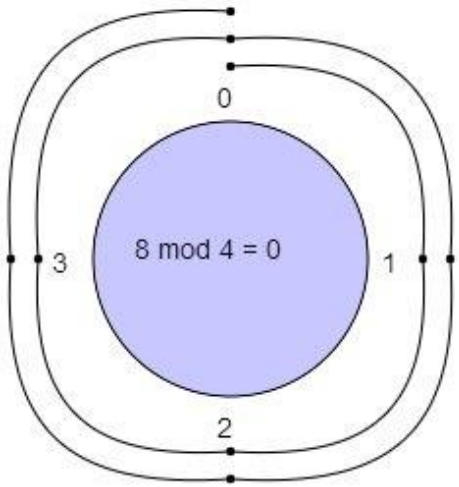
Definition

$$\frac{13}{5} = 2 \textit{ remainder } 3$$

$$13 \bmod 5 = 3$$

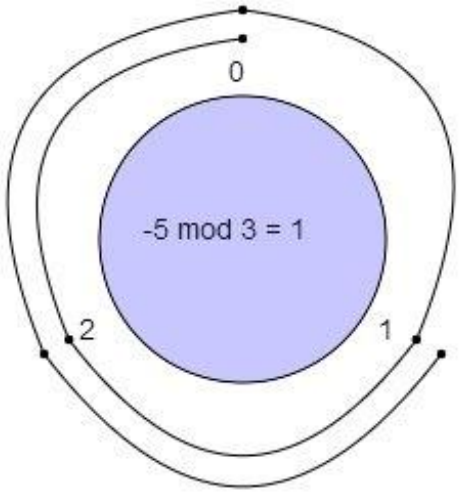
Definition

$$8 \bmod 4 = ?$$



Definition

$$-5 \bmod 3 = ?$$



Definition

$$A \bmod B = (A + K \cdot B) \bmod B$$

For example:

$$3 \bmod 10 = 3$$

$$13 \bmod 10 = 3$$

$$23 \bmod 10 = 3$$

$$33 \bmod 10 = 3$$

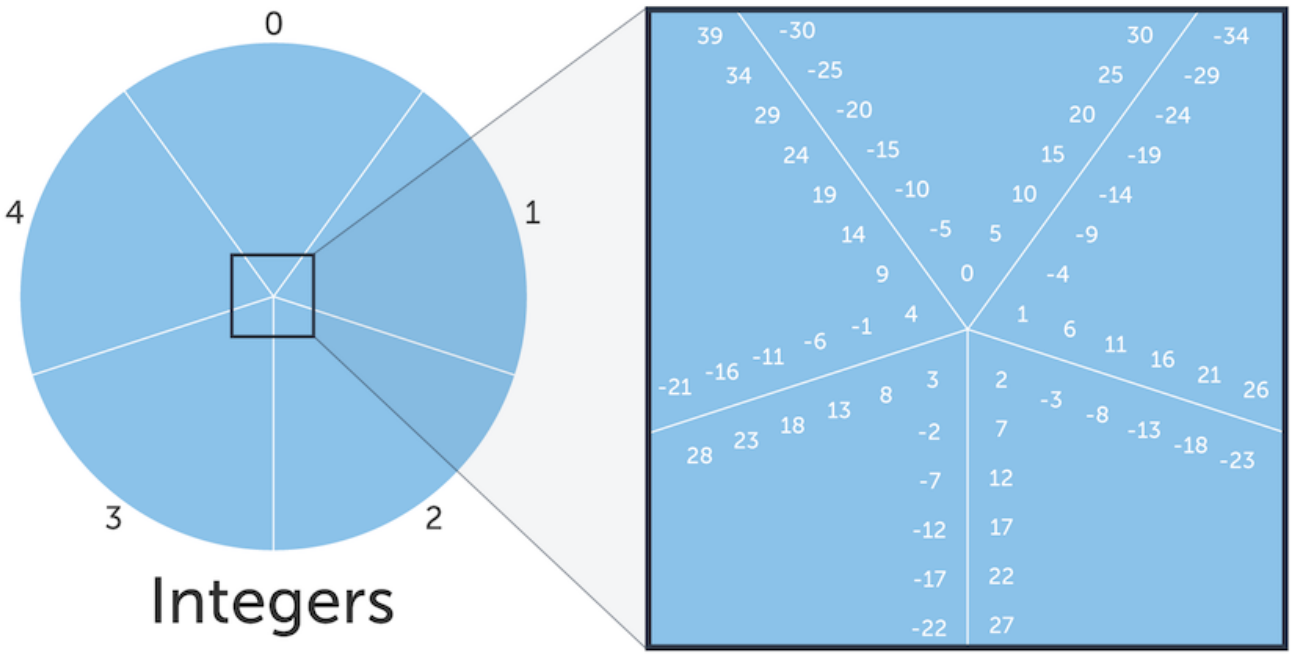
Congruence modulo

Congruence modulo:

$$A \equiv B \pmod{C}$$

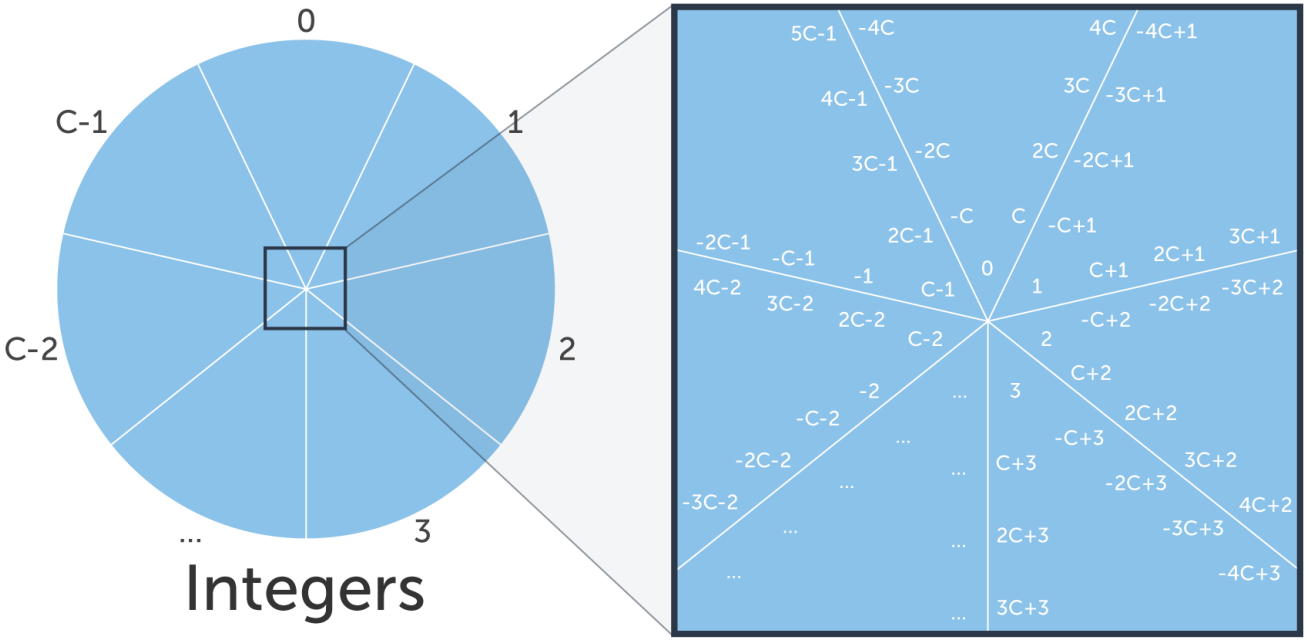
Congruence modulo

$$26 \equiv 11 \pmod 5$$



Congruence modulo

$$A \equiv B \pmod{C}$$



Equivalent Statements

Equivalent Statements:

- $A \equiv B \pmod{C}$
- $A \bmod C = B \bmod C$
- $C \mid (A - B)$
- $A = B + K \cdot C$

Equivalent Statements

For example:

- $13 \equiv 23 \pmod 5$
- $13 \bmod 5 = 23 \bmod 5$
- $5 \mid (13 - 23)$ by $5 \times -2 = -10$
- $13 = 23 + K \cdot 5$ by $K = -2$

Equivalence relation

Equivalence relation:

- $A \equiv A \pmod{C}$ **[reflexive]**
- $A \equiv B \pmod{C}$ then $B \equiv A \pmod{C}$ **[symmetric]**
- $A \equiv B \pmod{C}$ and $B \equiv D \pmod{C}$ then $A \equiv D \pmod{C}$ **[transitive]**

Equivalence relation

For example:

- $3 \equiv 3 \pmod 5$
- $3 \equiv 8 \pmod 5$ then $8 \equiv 3 \pmod 5$
- $3 \equiv 8 \pmod 5$ and if $8 \equiv 18 \pmod 5$ then $3 \equiv 18 \pmod 5$

Outline

The quotient remainder theorem

Given any integer A, and a **positive** integer B, there exist unique integers Q and R such that:

$$A = B * Q + R \text{ where } 0 \leq R < B$$

If we can write a number in this form then

$$A \bmod B = R$$

Webography

1. Khan Academy - Journey into Cryptography
   `https://tinyurl.com/jvqfq8t`
2. `https://tinyurl.com/y7jbfqfe`