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

$$A \bmod B = R$$

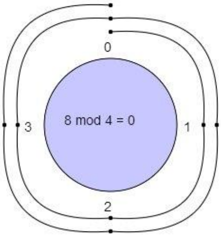
Definition

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

$$13 \bmod 5 = 3$$

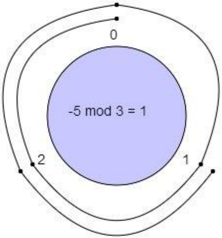
Definition

$$8 \bmod 4 = ?$$



Definition

$$-5 \bmod 3 = ?$$



Definition

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

For example:

$$3 \bmod 10 = 3$$

$$13 \bmod 10 = 3$$

$$23 \bmod 10 = 3$$

$$33 \bmod 10 = 3$$

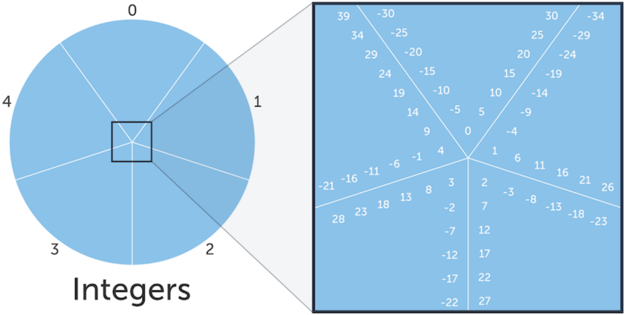
Congruence modulo

Congruence modulo:

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

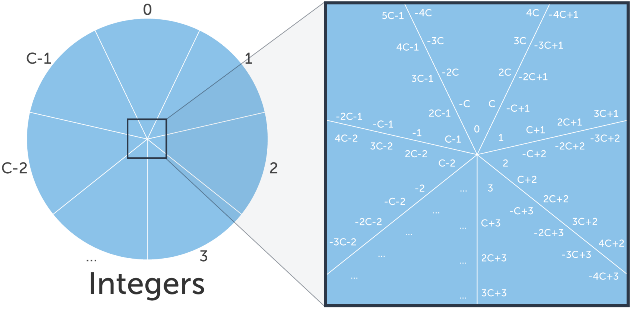
Congruence modulo

$$26 \equiv 11 \pmod{5}$$



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:

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

If we can write a number in this form then

$$A \bmod B = R$$

Modular Addition and Subtraction[1]

$$(A + B) \bmod C = (A \bmod C + B \bmod C) \bmod C$$

Example:

$$A = 14, B = 17, C = 5$$

[1] For prove have a look at https://tinyurl.com/yaltbzgz

Modular Addition and Subtraction

Solve for Y:

$$(699 + 997) \bmod 3 = Y$$

Modular Addition and Subtraction

Solve for Y:

$$(699 + 997) \bmod 3 = Y$$

$Y = 1$

Modular Addition and Subtraction

Give:
$A \bmod 8 = 3$
$(A + 19) \bmod 8 = Y$
Solve for Y.

Modular Addition and Subtraction

Give:
$A \bmod 8 = 3$
$(A + 19) \bmod 8 = Y$
Solve for Y.
$Y = 6$

Outline

Modular multiplication[2]

$$(A * B) \bmod C = (A \bmod C * B \bmod C) \bmod C$$

Example:

$$A = 4, B = 7, C = 6$$

[2] For prove have a look at https://tinyurl.com/ksf5muz

Modular exponentiation

$$A^B \bmod C = ((A \bmod C)^B) \bmod C$$

Example:
Let's solve:

$$2^{90} \bmod 13$$

but we have a calculator that can't hold any numbers larger than 2^50...

Modular exponentiation

Example:
$2^{90} \bmod 13 = 2^{50} * 2^{40} \bmod 13$
$2^{90} \bmod 13 = (2^{50} \bmod 13 * 2^{40} \bmod 13) \bmod 13$
$2^{90} \bmod 13 = (2^{50} \bmod 13 * 2^{40} \bmod 13) \bmod 13$
Using our calculator we know:
$2^{50} \bmod 13 = 1125899906842624 \bmod 13 = 4$
$2^{40} \bmod 13 = 1099511627776 \bmod 13 = 3$
So,
$2^{90} \bmod 13 = (4 * 3) \bmod 13$ $2^{90} \bmod 13 = 12 \bmod 13$ $2^{90} \bmod 13 = 12$

Webography

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