CS/MATH 111, Discrete Structures - Winter 2019. Discussion 3 - Modular Arithmetic

Andres, Sara, Elena

University of California, Riverside

January 22, 2019

Outline

Definition

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

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

$$A \bmod B = R$$

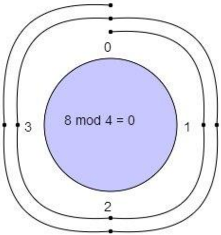
Definition

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

$$13 \bmod 5 = 3$$

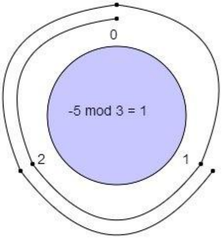
Definition

$$8 \bmod 4 = ?$$



Definition

$$-5 \bmod 3 = ?$$



Definition

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

For example:

$$3 \bmod 10 = 3$$

$$13 \bmod 10 = 3$$

$$23 \bmod 10 = 3$$

$$33 \bmod 10 = 3$$

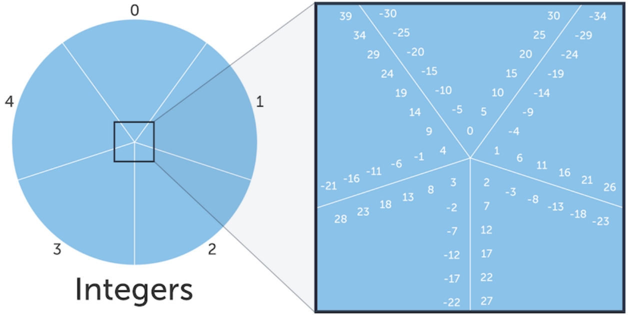
Congruence modulo

Congruence modulo:

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

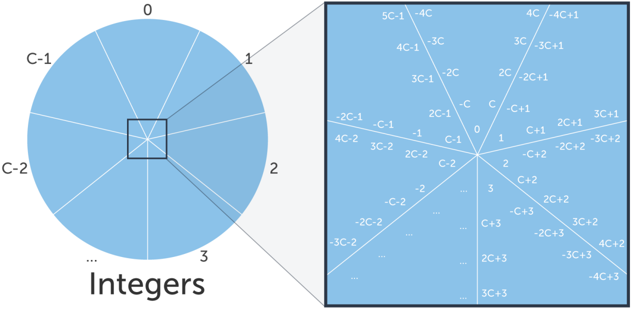
Congruence modulo

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



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

$$A \bmod B = R$$

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:

$$2^{50} \bmod 13 = 1125899906842624 \bmod 13 = 4$$

$$2^{40} \bmod 13 = 1099511627776 \bmod 13 = 3$$

Modular exponentiation

Example:

$$2^{90} \bmod 13 = 2^{50} * 2^{40} \bmod 13$$

$$2^{90} \bmod 13 = (2^{50} \bmod 13 * 2^{40} \bmod 13) \bmod 13$$

$$2^{90} \bmod 13 = (2^{50} \bmod 13 * 2^{40} \bmod 13) \bmod 13$$

$$2^{90} \bmod 13 = (4 * 3) \bmod 13$$

$$2^{90} \bmod 13 = 12 \bmod 13$$

$$2^{90} \bmod 13 = 12$$

Modular exponentiation by squaring

$$A^2 \bmod C = (A * A) \bmod C = ((A \bmod C) * (A \bmod C)) \bmod C$$

Solve:

$$7^{256} \bmod 13$$

Modular exponentiation by squaring

$$7^1 \bmod 13 = 7$$

$$7^2 \bmod 13 = (7^1 * 7^1) \bmod 13 = (7^1 \bmod 13 * 7^1 \bmod 13) \bmod 13$$

Modular exponentiation by squaring

$$7^1 \bmod 13 = 7$$

$$7^2 \bmod 13 = (7^1 * 7^1) \bmod 13 = (7^1 \bmod 13 * 7^1 \bmod 13) \bmod 13$$

$$7^2 \bmod 13 = (7 * 7) \bmod 13 = 49 \bmod 13 = 10$$

$$7^2 \bmod 13 = 10$$

$$7^4 \bmod 13 = (7^2 * 7^2) \bmod 13 = (7^2 \bmod 13 * 7^2 \bmod 13) \bmod 13$$

Modular exponentiation by squaring

$$7^1 \bmod 13 = 7$$
$$7^2 \bmod 13 = (7^1 * 7^1) \bmod 13 = (7^1 \bmod 13 * 7^1 \bmod 13) \bmod 13$$

$$7^2 \bmod 13 = (7 * 7) \bmod 13 = 49 \bmod 13 = 10$$
$$7^2 \bmod 13 = 10$$
$$7^4 \bmod 13 = (7^2 * 7^2) \bmod 13 = (7^2 \bmod 13 * 7^2 \bmod 13) \bmod 13$$

$$7^4 \bmod 13 = (10 * 10) \bmod 13 = 100 \bmod 13 = 9$$
$$7^4 \bmod 13 = 9$$
$$7^8 \bmod 13 = (7^4 * 7^4) \bmod 13 = (7^4 \bmod 13 * 7^4 \bmod 13) \bmod 13$$

$$\vdots$$

Modular exponentiation by squaring

$$\vdots$$

$$7^{256} \bmod 13 = (7^{128} * 7^{128}) \bmod 13 = (7^{128} \bmod 13 * 7^{128} \bmod 13) \bmod 13$$

$$7^{256} \bmod 13 = (3 * 3) \bmod 13 = 9 \bmod 13 = 9$$

$$7^{256} \bmod 13 = 9$$

Modular exponentiation by squaring

Solve:

$$5^{117} \bmod 19$$

Check the solution at `https://tinyurl.com/gvq9vxz`...

Outline

Inverse modulo

What is a modular inverse?

- The modular inverse of $A \pmod{C}$ is A^{-1}.
- $(A * A^{-1}) \equiv 1 \pmod{C}$ or equivalently $(A * A^{-1}) \bmod C = 1$.
- Only the numbers coprime (or relatively prime) to C (numbers that share no prime factors with C) have a modular inverse $\pmod{C}$.

Inverse modulo

Find the inverse for:

- $3 \pmod{7}$.
- $2 \pmod{6}$.

Solution at `https://tinyurl.com/hgxskmk`...

Linear congruence modulo

Solve:

- $17x \equiv 1 \pmod{43}$.

Linear congruence modulo

$17x \equiv 1 \pmod{43}$.
$17^{-1} \cdot 17x \equiv 17^{-1} \pmod{43}$.
$x \equiv 17^{-1} \pmod{43}$.

Now we find $17^{-1} \pmod{43}$

$$a \cdot b \equiv 1 \pmod{m}$$

$$a \cdot 17 \equiv 1 \pmod{43}$$

$$a \cdot 17 = 43 \cdot b + 1$$

Linear congruence modulo[3]

Now we find $17^{-1} \pmod{43}$

$$a \cdot 17 \equiv 1 \pmod{43}$$

$$a \cdot 17 = 43 \cdot b + 1$$

$$a = 38, b = 15$$

So we have

$$38 \cdot 17 = 43 \cdot 15 + 1$$

$$38 \cdot 17 \equiv 1 \pmod{43}$$

and

$$17^{-1} = 38 \pmod{43}$$

[3] Have a look at `https://tinyurl.com/y7jtxze4` for an alternative method...

Linear congruence modulo

$17x \equiv 1 \pmod{43}$.
$17^{-1} \cdot 17x \equiv 17^{-1} \pmod{43}$.
$x \equiv 17^{-1} \pmod{43}$.

We know that: $17^{-1} = 38 \pmod{43}$, so:

$$x \equiv 38 \pmod{43}$$

Outline

Fermat's Little Theorem

Let's have a loot at `https://tinyurl.com/l4ta3ym`

Fermat's Little Theorem

If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Example: $a = 5, p = 23$.
So, $5^{22} \equiv 1 \pmod{23}$.

Fermat's Little Theorem

$5^{22} \equiv 1 \pmod{23}$.

We compute this large power of 5 by succesive squaring...

$$5^2 \equiv 25 \equiv 2 \pmod{23}$$

$$5^4 \equiv 2^2 \equiv 4 \pmod{23}$$

$$5^8 \equiv 4^2 \equiv 16 \pmod{23}$$

$$5^16 \equiv 16^2 \equiv 256 \equiv 26 \equiv 3 \pmod{23}$$

Hence we have...

$$5^{22} \equiv 5^{16+4+2} \equiv 5^{16} \cdot 5^4 \cdot 5^2 \equiv 3 \cdot 4 \cdot 2 \equiv 24 \equiv 1 \pmod{23}$$

Webography

1. Khan Academy - Journey into Cryptography
   Modular arithmetic
   `https://tinyurl.com/jvqfq8t`
2. Khan Academy - Journey into Cryptography
   Randomized algorithms
   `https://tinyurl.com/l4ta3ym`