CS70 Modular Arithmetic

Kelvin Lee

kelvinlee@berkeley.edu

September 21, 2020

Overview

Basic Definitions

Basic Definitions

Definition (Congruence)

Basic Definitions

Definition (Congruence)

x is **congruent** to y modulo m or $x \equiv y \pmod{m}$ if and only if any one of the following is true:

Basic Definitions

Definition (Congruence)

x is **congruent** to y modulo m or $x \equiv y \pmod{m}$ if and only if any one of the following is true:

- $(x - y)$ is divisible by m

Basic Definitions

Definition (Congruence)

x is **congruent** to y modulo m or $x \equiv y \pmod{m}$ if and only if any one of the following is true:

- $(x - y)$ is divisible by m
- x and y have the same remainder w.r.t. m

Basic Definitions

Definition (Congruence)

x is **congruent** to y modulo m or $x \equiv y \pmod{m}$ if and only if any one of the following is true:

- $(x - y)$ is divisible by m
- x and y have the same remainder w.r.t. m
- $x = y + km$ for some integer k

Basic Definitions

Definition (Congruence)

x is **congruent** to y modulo m or $x \equiv y \pmod{m}$ if and only if any one of the following is true:

- $(x - y)$ is divisible by m
- x and y have the same remainder w.r.t. m
- $x = y + km$ for some integer k

- In modulo m, only the numbers $\{0, 1, 2, \ldots, m - 1\}$ exist.

Basic Definitions

Definition (Congruence)

x is **congruent** to y modulo m or $x \equiv y \pmod{m}$ if and only if any one of the following is true:

- $(x - y)$ is divisible by m
- x and y have the same remainder w.r.t. m
- $x = y + km$ for some integer k

- In modulo m, only the numbers $\{0, 1, 2, \ldots, m - 1\}$ exist.
- Division is not well-defined.

Basic Definitions

Definition (Congruence)

x is **congruent** to y modulo m or $x \equiv y \pmod{m}$ if and only if any one of the following is true:

- $(x - y)$ is divisible by m
- x and y have the same remainder w.r.t. m
- $x = y + km$ for some integer k

- In modulo m, only the numbers $\{0, 1, 2, \ldots, m - 1\}$ exist.
- Division is not well-defined.

Definition (Multiplicative Inverse)

Basic Definitions

Definition (Congruence)

x is **congruent** to y modulo m or $x \equiv y \pmod{m}$ if and only if any one of the following is true:

- $(x - y)$ is divisible by m
- x and y have the same remainder w.r.t. m
- $x = y + km$ for some integer k

- In modulo m, only the numbers $\{0, 1, 2, \ldots, m - 1\}$ exist.
- Division is not well-defined.

Definition (Multiplicative Inverse)

Normally we say that the **multiplicative inverse** of x is y if $xy = 1$.

Basic Definitions

Definition (Congruence)

x is **congruent** to y modulo m or $x \equiv y \pmod{m}$ if and only if any one of the following is true:

- $(x - y)$ is divisible by m
- x and y have the same remainder w.r.t. m
- $x = y + km$ for some integer k

- In modulo m, only the numbers $\{0, 1, 2, \ldots, m - 1\}$ exist.
- Division is not well-defined.

Definition (Multiplicative Inverse)

Normally we say that the **multiplicative inverse** of x is y if $xy = 1$. In the modular space, the **multiplicative inverse** of x mod m is y if $xy \equiv 1 \pmod{m}$.

Theorems

Theorem (Modular operations)

Theorems

Theorem (Modular operations)

$a \equiv c \bmod m$ and $b \equiv d \bmod m \implies a + b \equiv c + d \pmod{m}$ and $a \cdot b \equiv c \cdot d \pmod{m}$.

Theorems

Theorem (Modular operations)

$a \equiv c \bmod m$ and $b \equiv d \bmod m \implies a + b \equiv c + d \ (\bmod\, m)$ and $a \cdot b \equiv c \cdot d \ (\bmod\, m)$.

Theorem (Existence of multiplicative inverse)

Theorems

Theorem (Modular operations)

$a \equiv c \bmod m$ and $b \equiv d \bmod m \implies a + b \equiv c + d \ (\bmod m)$ and $a \cdot b \equiv c \cdot d \ (\bmod m)$.

Theorem (Existence of multiplicative inverse)

$\gcd(x, m) = 1 \implies x$ has a multiplicative inverse modulo m and it is **unique**.

Euclid's Algorithm

Euclid's Algorithm

How do we compute gcd of two numbers x and y?

Euclid's Algorithm

How do we compute gcd of two numbers x and y?

Theorem (Euclid's Algorithm)

Euclid's Algorithm

How do we compute gcd of two numbers x and y?

Theorem (Euclid's Algorithm)

Let $x \geq y > 0$. Then

$$gcd(x, y) = gcd(y, x \bmod y)$$

Euclid's Algorithm

How do we compute gcd of two numbers x and y?

Theorem (Euclid's Algorithm)

Let $x \geq y > 0$. Then

$$gcd(x, y) = gcd(y, x \bmod y)$$

Example

Euclid's Algorithm

How do we compute gcd of two numbers x and y?

Theorem (Euclid's Algorithm)

Let $x \geq y > 0$. Then

$$gcd(x, y) = gcd(y, x \bmod y)$$

Example

Compute gcd(16,10):

Euclid's Algorithm

How do we compute gcd of two numbers x and y?

Theorem (Euclid's Algorithm)

Let $x \geq y > 0$. Then

$$gcd(x, y) = gcd(y, x \bmod y)$$

Example

Compute gcd(16,10):

$$
\begin{aligned}
\gcd(16, 10) &= \gcd(10, 6) \\
&= \gcd(6, 4) \\
&= \gcd(4, 2) \\
&= \gcd(2, 0) \\
&= 2.
\end{aligned}
$$

How to compute the multiplicative inverse?

Extended Euclid's algorithm

How to compute the multiplicative inverse?

- Need an algorithm that returns integers a and b such that:

$$\gcd(x, y) = ax + by.$$

Extended Euclid's algorithm

How to compute the multiplicative inverse?

- Need an algorithm that returns integers a and b such that:

$$\gcd(x, y) = ax + by.$$

- When $\gcd(x, y) = 1$, we can deduce that b is an inverse of y mod x.

Extended Euclid's algorithm

How to compute the multiplicative inverse?

- Need an algorithm that returns integers a and b such that:

$$\gcd(x, y) = ax + by.$$

- When $\gcd(x, y) = 1$, we can deduce that b is an inverse of y mod x.
- So basically repetitively substitute values so that the final expression is in terms of x and y.

Problem Time!