CS70 Modular Arithmetic

Kelvin Lee

kelvinlee@berkeley.edu

September 22, 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

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

Theorem (Existence of multiplicative inverse)

Theorems

Theorem (Modular operations)

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

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*

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

Euclid's Algorithm

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

Theorem (Euclid's Algorithm)

Let $x \geq y > 0$. Then

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

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*

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

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

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

Example

Compute gcd(16,10):

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

Extended Euclid's algorithm

Extended Euclid's algorithm

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:

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

Theorem (Bézout's Identity)

Extended Euclid's algorithm

How to compute the multiplicative inverse?

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

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

Theorem (Bézout's Identity)

For nonzero integers x and y, let d be the greatest common divisor such that $d = \gcd(x, y)$. Then, there exist integers a and b such that

$$ax + by = d.$$

Extended Euclid's algorithm

How to compute the multiplicative inverse?

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

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

Theorem (Bézout's Identity)

For nonzero integers x and y, let d be the greatest common divisor such that $d = \gcd(x, y)$. Then, there exist integers a and b such that

$$ax + by = d.$$

- 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:

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

Theorem (Bézout's Identity)

For nonzero integers x and y, let d be the greatest common divisor such that $d = \gcd(x, y)$. Then, there exist integers a and b such that

$$ax + by = d.$$

- When $\gcd(x, y) = 1$, we can deduce that b is an inverse of y mod x.
- This uses back substitutions repetitively so that the final expression is in terms of x and y.

Functions

Functions

Definition (Function)

Functions

Definition (Function)

Let A and B be nonempty sets. A **function** f from A to B is an assignment of exactly one element of B to each element of A. (vertical line test)

Functions

Definition (Function)

Let A and B be nonempty sets. A **function** f from A to B is an assignment of exactly one element of B to each element of A. (vertical line test)

- To denote such a function, we write $f : A \to B$ (f maps A to B).

Functions

Definition (Function)

Let A and B be nonempty sets. A **function** f from A to B is an assignment of exactly one element of B to each element of A. (vertical line test)

- To denote such a function, we write $f : A \to B$ (f maps A to B).

- A is the **domain** and B is the **co-domain**.

Functions

Definition (Function)

Let A and B be nonempty sets. A **function** f from A to B is an assignment of exactly one element of B to each element of A. (vertical line test)

- To denote such a function, we write $f : A \to B$ (f maps A to B).

- A is the **domain** and B is the **co-domain**.
- Pre-image is a **subset** of domain, and the image/range is the **subset** of co-domain.

Functions

Definition (Function)

Let A and B be nonempty sets. A **function** f from A to B is an assignment of exactly one element of B to each element of A. (vertical line test)

- To denote such a function, we write $f : A \to B$ (f maps A to B).

- A is the **domain** and B is the **co-domain**.
- Pre-image is a **subset** of domain, and the image/range is the **subset** of co-domain.
  - If $f(a) = b$, where $a \in A$ and $b \in B$, then we say that b is the image of a and a is the pre-image of b.

Bijection

Bijection

Definition (One-to-one)

Bijection

Definition (One-to-one)

A function f is said to be **one-to-one** if and only if $f(a) = f(a')$ implies that $a = a'$ for all $a, a' \in A$. A function is said to be **injective** if it is **one-to-one**.

Bijection

Definition (One-to-one)

A function f is said to be **one-to-one** if and only if $f(a) = f(a')$ implies that $a = a'$ for all $a, a' \in A$. A function is said to be **injective** if it is **one-to-one**.

- To show that a function is *one-to-one*, we show that $a \neq a' \implies f(a) \neq f(a')$. (Why?)

Bijection

Definition (One-to-one)

A function f is said to be **one-to-one** if and only if $f(a) = f(a')$ implies that $a = a'$ for all $a, a' \in A$. A function is said to be **injective** if it is **one-to-one**.

- To show that a function is *one-to-one*, we show that $a \neq a' \implies f(a) \neq f(a')$. (Why?)

Definition (Onto)

Bijection

Definition (One-to-one)

A function f is said to be **one-to-one** if and only if $f(a) = f(a')$ implies that $a = a'$ for all $a, a' \in A$. A function is said to be **injective** if it is **one-to-one**.

- To show that a function is *one-to-one*, we show that $a \neq a' \implies f(a) \neq f(a')$. (Why?)

Definition (Onto)

A function f is called **onto**, or a surjection, if and only if for every element $b \in B$ there is an element $a \in A$ such that $f(a) = b$. We also say that f is **surjective** if it's onto.

Bijection

Definition (One-to-one)

A function f is said to be **one-to-one** if and only if $f(a) = f(a')$ implies that $a = a'$ for all $a, a' \in A$. A function is said to be **injective** if it is **one-to-one**.

- To show that a function is *one-to-one*, we show that $a \neq a' \implies f(a) \neq f(a')$. (Why?)

Definition (Onto)

A function f is called **onto**, or a surjection, if and only if for every element $b \in B$ there is an element $a \in A$ such that $f(a) = b$. We also say that f is **surjective** if it's onto.

- To show that a function is *onto*, choose $a = f^{-1}(b)$ and so $f(f^{-1}(b)) = b$.

Bijection

Definition (Bijection)

Bijection

Definition (Bijection)

A function f is a **bijection** if and only if it is both *one-to-one* and *onto*. We also say that f is bijective.

Bijection

Definition (Bijection)

A function f is a **bijection** if and only if it is both *one-to-one* and *onto*. We also say that f is bijective.

- If $f : A \to B$ is a bijection, it will have an **inverse** function (a lemma from notes), and $|A| = |B|$.

Fermat's Little Theorem

Fermat's Little Theorem

Theorem (Fermat's Little Theorem)

Fermat's Little Theorem

Theorem (Fermat's Little Theorem)

For any prime p and any $a \in \{1, 2, ..., p1\}$, *we have*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Fermat's Little Theorem

Theorem (Fermat's Little Theorem)

For any prime p and any $a \in \{1, 2, ..., p1\}$, we have

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof:

Fermat's Little Theorem

Theorem (Fermat's Little Theorem)

For any prime p and any $a \in \{1, 2, ..., p1\}$, we have

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof:

- Consider $S = \{1, 2, \ldots, p-1\}$ and $S' = \{a \text{ mod } p, 2a \text{ mod } p, \ldots, (p-1)a \text{ mod } p\}$.

Fermat's Little Theorem

Theorem (Fermat's Little Theorem)

For any prime p and any $a \in \{1, 2, ..., p1\}$, we have

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof:

- Consider $S = \{1, 2, \ldots, p-1\}$ and $S' = \{a \bmod p, 2a \bmod p, \ldots, (p-1)a \bmod p\}$.
- They are the same set under mod p (different order).

Fermat's Little Theorem

Theorem (Fermat's Little Theorem)

For any prime p and any $a \in \{1, 2, ..., p1\}$, we have

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof:

- Consider $S = \{1, 2, \ldots, p-1\}$ and $S' = \{a \bmod p, 2a \bmod p, \ldots, (p-1)a \bmod p\}$.
- They are the same set under mod p (different order).

$$\prod_{k=1}^{p-1} k \equiv \prod_{k=1}^{p-1} ka \pmod{p}$$

Fermat's Little Theorem

Theorem (Fermat's Little Theorem)

For any prime p and any a $\in \{1, 2, ..., p1\}$, *we have*

$$a^{p-1} \equiv 1 \pmod p.$$

Proof:

- Consider $S = \{1, 2, \ldots, p-1\}$ and
  $S' = \{a \bmod p, 2a \bmod p, \ldots, (p-1)a \bmod p\}$.
- They are the same set under mod p (different order).

$$\prod_{k=1}^{p-1} k \equiv \prod_{k=1}^{p-1} ka \pmod p$$

$$(p-1)! \equiv a^{p-1}(p-1)! \pmod p$$

Fermat's Little Theorem

Theorem (Fermat's Little Theorem)

For any prime p and any $a \in \{1, 2, ..., p1\}$, we have

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof:

- Consider $S = \{1, 2, \ldots, p-1\}$ and $S' = \{a \bmod p, 2a \bmod p, \ldots, (p-1)a \bmod p\}$.
- They are the same set under mod p (different order).

$$\prod_{k=1}^{p-1} k \equiv \prod_{k=1}^{p-1} ka \pmod{p}$$

$$(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}$$

$$a^{p-1} \equiv 1 \pmod{p}$$

Problem Time!