# CS70 Modular Arithmetic

Kelvin Lee

*kelvinlee@berkeley.edu*

September 28, 2020

# Overview

1. Basic Definitions
2. Multiplicative Inverse
3. Euclid's Algorithm
4. Extended Euclid's algorithm
5. Functions
6. Bijection
7. Fermat's Little Theorem
8. Chinese Remainder Theorem

# 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):

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

# 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* $a \in \{1, 2, ..., p-1\}$, *we have*

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

# Fermat's Little Theorem

**Theorem (Fermat's Little Theorem)**

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

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

***Proof:***

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

# Fermat's Little Theorem

## Theorem (Fermat's Little Theorem)

*For any prime $p$ and any $a \in \{1, 2, ..., p-1\}$, 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 $a \in \{1, 2, ..., p-1\}$, 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).

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

**Theorem (Fermat's Little Theorem)**

*For any prime $p$ and any $a \in \{1, 2, ..., p-1\}$, 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 $a \in \{1, 2, ..., p-1\}$, 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).

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

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

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

# Chinese Remainder Theorem

**Theorem (Chinese Remainder Theorem)**

# Chinese Remainder Theorem

## Theorem (Chinese Remainder Theorem)

*Let $n_1, n_2, \ldots, n_k$ be positive integers that are coprime to each other. Then, for any integers $a_i$, the system of simultaneous congruences*

# Chinese Remainder Theorem

## Theorem (Chinese Remainder Theorem)

*Let $n_1, n_2, \ldots, n_k$ be positive integers that are coprime to each other. Then, for any integers $a_i$, the system of simultaneous congruences*

$$x \equiv a_1 \pmod{n_1}, x \equiv a_2 \pmod{n_2}, \ \ldots \ , x \equiv a_k \pmod{n_k}$$

# Chinese Remainder Theorem

## Theorem (Chinese Remainder Theorem)

*Let* $n_1, n_2, \ldots, n_k$ *be positive integers that are coprime to each other. Then, for any integers* $a_i$*, the system of simultaneous congruences*

$$x \equiv a_1 \pmod{n_1}, x \equiv a_2 \pmod{n_2}, \ \ldots \ , x \equiv a_k \pmod{n_k}$$

*has a unique solution*

$$x = \left( \sum_{i=1}^{k} a_i b_i \right) \bmod N$$

# Chinese Remainder Theorem

**Theorem (Chinese Remainder Theorem)**

*Let $n_1, n_2, \ldots, n_k$ be positive integers that are coprime to each other. Then, for any integers $a_i$, the system of simultaneous congruences*

$$x \equiv a_1 \pmod{n_1}, x \equiv a_2 \pmod{n_2}, \ \ldots \ , x \equiv a_k \pmod{n_k}$$

*has a unique solution*

$$x = \left(\sum_{i=1}^{k} a_i b_i\right) \bmod N$$

*where $N = \prod_{i=1}^{k} n_i$ and $b_i = \frac{N}{n_i}\left(\frac{N}{n_i}\right)_{n_i}^{-1}$ where $\left(\frac{N}{n_i}\right)_{n_i}^{-1}$ denotes the multiplicative inverse $(\bmod\, n_i)$ of the integer $\frac{N}{n_i}$.*

# Chinese Remainder Theorem

# Chinese Remainder Theorem

***Proof:***

To see why $x$ is a solution, notice that for each $i = 1, 2, \dots, k$, we have

$$x \equiv a_1 y_1 z_1 + a_2 y_2 z_2 + \cdots + a_k y_k z_k \pmod{n_i}$$

# Chinese Remainder Theorem

***Proof:***

To see why $x$ is a solution, notice that for each $i = 1, 2, \ldots, k$, we have

$$\begin{aligned} x &\equiv a_1y_1z_1 + a_2y_2z_2 + \cdots + a_ky_kz_k \pmod{n_i} \\ &\equiv a_iy_iz_i \pmod{n_i} \end{aligned}$$

***Proof:***

To see why $x$ is a solution, notice that for each $i = 1, 2, \ldots, k$, we have

$$\begin{aligned} x &\equiv a_1 y_1 z_1 + a_2 y_2 z_2 + \cdots + a_k y_k z_k \pmod{n_i} \\ &\equiv a_i y_i z_i \pmod{n_i} \\ &\equiv a_i \pmod{n_i}. \end{aligned}$$

# Chinese Remainder Theorem

***Proof:***

To see why $x$ is a solution, notice that for each $i = 1, 2, \ldots, k$, we have

$$\begin{aligned} x &\equiv a_1y_1z_1 + a_2y_2z_2 + \cdots + a_ky_kz_k \pmod{n_i} \\ &\equiv a_iy_iz_i \pmod{n_i} \\ &\equiv a_i \pmod{n_i}. \end{aligned}$$

- The second line follows since $y_j \equiv 0 \bmod n_i$ for each $j \neq i$.

# Chinese Remainder Theorem

***Proof:***

To see why $x$ is a solution, notice that for each $i = 1, 2, \ldots, k$, we have

$$\begin{aligned} x &\equiv a_1 y_1 z_1 + a_2 y_2 z_2 + \cdots + a_k y_k z_k \pmod{n_i} \\ &\equiv a_i y_i z_i \pmod{n_i} \\ &\equiv a_i \pmod{n_i}. \end{aligned}$$

- The second line follows since $y_j \equiv 0 \bmod n_i$ for each $j \neq i$.
- The third line follows since $y_i z_i \equiv 1 \bmod n_i$.

# Chinese Remainder Theorem

***Proof:***

To see why $x$ is a solution, notice that for each $i = 1, 2, \ldots, k$, we have

$$\begin{aligned} x &\equiv a_1 y_1 z_1 + a_2 y_2 z_2 + \cdots + a_k y_k z_k \pmod{n_i} \\ &\equiv a_i y_i z_i \pmod{n_i} \\ &\equiv a_i \pmod{n_i}. \end{aligned}$$

- The second line follows since $y_j \equiv 0 \bmod n_i$ for each $j \neq i$.
- The third line follows since $y_i z_i \equiv 1 \bmod n_i$.

Now, to prove uniqueness, suppose there are two solutions $x$ and $y$.

# Chinese Remainder Theorem

***Proof:***

To see why $x$ is a solution, notice that for each $i = 1, 2, \ldots, k$, we have

$$\begin{aligned} x &\equiv a_1y_1z_1 + a_2y_2z_2 + \cdots + a_ky_kz_k \pmod{n_i} \\ &\equiv a_iy_iz_i \pmod{n_i} \\ &\equiv a_i \pmod{n_i}. \end{aligned}$$

- The second line follows since $y_j \equiv 0 \bmod n_i$ for each $j \neq i$.
- The third line follows since $y_iz_i \equiv 1 \bmod n_i$.

Now, to prove uniqueness, suppose there are two solutions $x$ and $y$.

- Then $n_1 \,|(x - y), n_2|\,(x - y), \ldots, n_k \mid (x - y)$.

# Chinese Remainder Theorem

***Proof:***

To see why $x$ is a solution, notice that for each $i = 1, 2, \ldots, k$, we have

$$\begin{aligned} x &\equiv a_1 y_1 z_1 + a_2 y_2 z_2 + \cdots + a_k y_k z_k \pmod{n_i} \\ &\equiv a_i y_i z_i \pmod{n_i} \\ &\equiv a_i \pmod{n_i}. \end{aligned}$$

- The second line follows since $y_j \equiv 0 \bmod n_i$ for each $j \neq i$.
- The third line follows since $y_i z_i \equiv 1 \bmod n_i$.

Now, to prove uniqueness, suppose there are two solutions $x$ and $y$.

- Then $n_1 \mid (x - y), n_2 \mid (x - y), \ldots, n_k \mid (x - y)$.
- Since $n_1, n_2, \ldots, n_k$ are relatively prime, we have that $n_1 n_2 \cdots n_k$ divides $x - y$, or

# Chinese Remainder Theorem

***Proof:***

To see why $x$ is a solution, notice that for each $i = 1, 2, \ldots, k$, we have

$$\begin{aligned} x &\equiv a_1 y_1 z_1 + a_2 y_2 z_2 + \cdots + a_k y_k z_k \pmod{n_i} \\ &\equiv a_i y_i z_i \pmod{n_i} \\ &\equiv a_i \pmod{n_i}. \end{aligned}$$

- The second line follows since $y_j \equiv 0 \bmod n_i$ for each $j \neq i$.
- The third line follows since $y_i z_i \equiv 1 \bmod n_i$.

Now, to prove uniqueness, suppose there are two solutions $x$ and $y$.

- Then $n_1 \mid (x - y), n_2 \mid (x - y), \ldots, n_k \mid (x - y)$.
- Since $n_1, n_2, \ldots, n_k$ are relatively prime, we have that $n_1 n_2 \cdots n_k$ divides $x - y$, or

$$x \equiv y \pmod{N}.$$

# Chinese Remainder Theorem

***Proof:***

To see why $x$ is a solution, notice that for each $i = 1, 2, \ldots, k$, we have

$$\begin{aligned} x &\equiv a_1 y_1 z_1 + a_2 y_2 z_2 + \cdots + a_k y_k z_k \pmod{n_i} \\ &\equiv a_i y_i z_i \pmod{n_i} \\ &\equiv a_i \pmod{n_i}. \end{aligned}$$

- The second line follows since $y_j \equiv 0 \bmod n_i$ for each $j \neq i$.
- The third line follows since $y_i z_i \equiv 1 \bmod n_i$.

Now, to prove uniqueness, suppose there are two solutions $x$ and $y$.

- Then $n_1 \,|(x-y), n_2|\,(x-y), \ldots, n_k \mid (x-y)$.
- Since $n_1, n_2, \ldots, n_k$ are relatively prime, we have that $n_1 n_2 \cdots n_k$ divides $x - y$, or

$$x \equiv y \pmod{N}.$$

Thus, the solution is unique modulo $N$. □

# Chinese Remainder Theorem

**General construction:**

# Chinese Remainder Theorem

**General construction:**

1. Compute $N = n_1 \times n_2 \times \cdots \times n_k$.

# Chinese Remainder Theorem

**General construction:**

1. Compute $N = n_1 \times n_2 \times \cdots \times n_k$.
2. For each $i = 1, 2, \ldots, k$, compute

$$y_i = \frac{N}{n_i} = n_1 n_2 \cdots n_{i-1} n_{i+1} \cdots n_k.$$

**General construction:**

1. Compute $N = n_1 \times n_2 \times \cdots \times n_k$.
2. For each $i = 1, 2, \ldots, k$, compute

$$y_i = \frac{N}{n_i} = n_1 n_2 \cdots n_{i-1} n_{i+1} \cdots n_k.$$

3. For each $i = 1, 2, \ldots, k$, compute $z_i \equiv y_i^{-1} \bmod n_i$ ($z_i$ exists since $n_1, n_2, \ldots, n_k$ are pairwise coprime).

# Chinese Remainder Theorem

**General construction:**

1. Compute $N = n_1 \times n_2 \times \cdots \times n_k$.
2. For each $i = 1, 2, \ldots, k$, compute
$$y_i = \frac{N}{n_i} = n_1 n_2 \cdots n_{i-1} n_{i+1} \cdots n_k.$$
3. For each $i = 1, 2, \ldots, k$, compute $z_i \equiv y_i^{-1} \bmod n_i$ ($z_i$ exists since $n_1, n_2, \ldots, n_k$ are pairwise coprime).
4. Compute
$$x = \sum_{i=1}^{k} a_i y_i z_i$$
and $x \bmod N$ is the unique solution modulo $N$.

**Intuitive way to solve for CRT:**

# Chinese Remainder Theorem

**Intuitive way to solve for CRT:**

1. Begin with the congruence with the largest modulus, $x \equiv a_k \pmod{n_k}$.

# Chinese Remainder Theorem

**Intuitive way to solve for CRT:**

1. Begin with the congruence with the largest modulus, $x \equiv a_k \pmod{n_k}$.
2. Re-write this modulus as an equation, $x = j_k n_k + a_k$, for some positive integer $j_k$.

**Intuitive way to solve for CRT:**

1. Begin with the congruence with the largest modulus, $x \equiv a_k \pmod{n_k}$.
2. Re-write this modulus as an equation, $x = j_k n_k + a_k$, for some positive integer $j_k$.
3. Substitute the expression for $x$ into the congruence with the next largest modulus, $x \equiv a_k \pmod{n_k} \implies j_k n_k + a_k \equiv a_{k-1} \pmod{n_{k-1}}$.

# Chinese Remainder Theorem

**Intuitive way to solve for CRT:**

1. Begin with the congruence with the largest modulus, $x \equiv a_k \pmod{n_k}$.
2. Re-write this modulus as an equation, $x = j_k n_k + a_k$, for some positive integer $j_k$.
3. Substitute the expression for $x$ into the congruence with the next largest modulus, $x \equiv a_k \pmod{n_k} \implies j_k n_k + a_k \equiv a_{k-1} \pmod{n_{k-1}}$.
4. Solve this congruence for $j_k$.

# Chinese Remainder Theorem

**Intuitive way to solve for CRT:**

1. Begin with the congruence with the largest modulus, $x \equiv a_k \pmod{n_k}$.
2. Re-write this modulus as an equation, $x = j_k n_k + a_k$, for some positive integer $j_k$.
3. Substitute the expression for $x$ into the congruence with the next largest modulus, $x \equiv a_k \pmod{n_k} \implies j_k n_k + a_k \equiv a_{k-1} \pmod{n_{k-1}}$.
4. Solve this congruence for $j_k$.
5. Write the solved congruence as an equation, and then substitute this expression for $j_k$ into the equation for $x$.

# Chinese Remainder Theorem

**Intuitive way to solve for CRT:**

1. Begin with the congruence with the largest modulus, $x \equiv a_k \pmod{n_k}$.
2. Re-write this modulus as an equation, $x = j_k n_k + a_k$, for some positive integer $j_k$.
3. Substitute the expression for $x$ into the congruence with the next largest modulus, $x \equiv a_k \pmod{n_k} \implies j_k n_k + a_k \equiv a_{k-1} \pmod{n_{k-1}}$.
4. Solve this congruence for $j_k$.
5. Write the solved congruence as an equation, and then substitute this expression for $j_k$ into the equation for $x$.
6. Continue substituting and solving congruences until the equation for $x$ implies the solution to the system of congruences.

# Chinese Remainder Theorem

**Example:**

# Chinese Remainder Theorem

**Example:**

$$\begin{cases} x \equiv 1 & \pmod{3} \\ x \equiv 4 & \pmod{5} \\ x \equiv 6 & \pmod{7} \end{cases}$$

# Chinese Remainder Theorem

**Example:**

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 4 \pmod{5} \\ x \equiv 6 \pmod{7} \end{cases}$$

**Solution:**

**Example:**

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 4 \pmod{5} \\ x \equiv 6 \pmod{7} \end{cases}$$

**Solution:**

- Start with mod 7. Write $x = 7k + 6$.

**Example:**

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 4 \pmod{5} \\ x \equiv 6 \pmod{7} \end{cases}$$

**Solution:**

- Start with mod 7. Write $x = 7k + 6$.
- Then we have $7k + 6 \equiv 4 \pmod{5} \implies k \equiv 4 \pmod{5}$.

# Chinese Remainder Theorem

**Example:**

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 4 \pmod 5 \\ x \equiv 6 \pmod 7 \end{cases}$$

**Solution:**

- Start with mod 7. Write $x = 7k + 6$.
- Then we have $7k + 6 \equiv 4 \pmod 5 \implies k \equiv 4 \pmod 5$.
- Then solving for $k$ gives $5j + 4$.

# Chinese Remainder Theorem

**Example:**

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 4 \pmod{5} \\ x \equiv 6 \pmod{7} \end{cases}$$

**Solution:**

- Start with mod 7. Write $x = 7k + 6$.
- Then we have $7k + 6 \equiv 4 \pmod{5} \implies k \equiv 4 \pmod{5}$.
- Then solving for $k$ gives $5j + 4$.
- Now we have $x = 7k + 6 = 7(5j + 4) + 6 = 35j + 34$.

# Chinese Remainder Theorem

**Example:**

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 4 \pmod 5 \\ x \equiv 6 \pmod 7 \end{cases}$$

**Solution:**

- Start with mod 7. Write $x = 7k + 6$.
- Then we have $7k + 6 \equiv 4 \pmod 5 \implies k \equiv 4 \pmod 5$.
- Then solving for $k$ gives $5j + 4$.
- Now we have $x = 7k + 6 = 7(5j + 4) + 6 = 35j + 34$.
- Then $35j + 34 \equiv 1 \pmod 3 \implies j \equiv 0 \pmod 3 \implies j = 3t$.

**Example:**

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 4 \pmod{5} \\ x \equiv 6 \pmod{7} \end{cases}$$

**Solution:**

- Start with mod 7. Write $x = 7k + 6$.
- Then we have $7k + 6 \equiv 4 \pmod{5} \implies k \equiv 4 \pmod{5}$.
- Then solving for $k$ gives $5j + 4$.
- Now we have $x = 7k + 6 = 7(5j + 4) + 6 = 35j + 34$.
- Then $35j + 34 \equiv 1 \pmod{3} \implies j \equiv 0 \pmod{3} \implies j = 3t$.
- Finally, we have $x = 35(3t) + 34 = 105t + 34 \implies x \equiv \boxed{34} \pmod{105}$.

# Problem Time!