Lecture 2D: Modular Arithmetic II

UC Berkeley EECS 70
Summer 2022
Tarang Srivastava

Announcements!

- Read the Weekly Post
- **HW 2** and **Vitamin 2** have been released, due **Today** (grace period Fri)
- No lecture, OH, or Discussions on July 4th

Repeated Squaring

How to find $x^y \pmod{m}$ for large exponents.
Example: $4^{42} \pmod 7$

(mod 7)

$4^0 \equiv 1$

$4^1 \equiv 4$

$4^2 \equiv 16 \equiv 2$

$4^4 \equiv (4^2)^2 \equiv (2)^2 \equiv 4$

$4^8 \equiv (4^4)^2 \equiv (4)^2 \equiv 16 \equiv 2$

$4^{16} \equiv (4^8)^2 \equiv 2^2 \equiv 4$

$4^{32} \equiv (4^{16})^2 \equiv (4)^2 \equiv 16 \equiv 2$

$4^{42} \equiv 4^{32} \cdot 4^8 \cdot 4^2 \equiv 4^{32+8+2}$

$\equiv 2 \cdot 2 \cdot 2 \equiv 8 \equiv 1 \pmod 7$

Recap

- Division Algorithm a, b $\quad a = b\underset{\text{quotient}}{q} + \underset{\text{remainder}}{r}$
- Greatest Common Divisor (GCD) Definition
- GCD Algorithm: Application and Proof $\gcd(x, y) = \gcd(y, x \bmod y)$
- Every number has a unique prime factorization ex: $52 = 13 \cdot 2 \cdot 2$
- Mod as a *Space*: Defined Addition, Subtraction, Multiplication and Division
- Definition of Coprime $\gcd(x, y) = 1$
- Definition of Inverse and division via multiplying inverse
- Extended Euclid's Algorithm to find inverse $ax + by = 1$
- Repeated Squaring

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

Bijections

$f: A \to B$

$f(x) = 2x$

$\mathbb{R} \to \mathbb{R}$

A *bijection* is a function for which every $b \in B$ has a unique *pre-image* $a \in A$ such that $f(a) = b$. Note that this consists of two conditions:

Contrapositive.

"surjective"

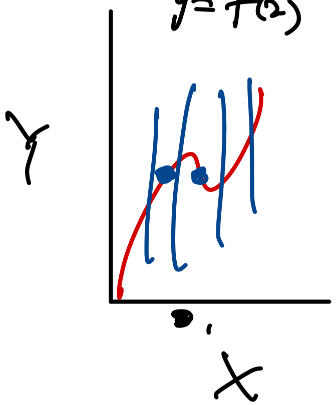
1. f is *onto*: every $b \in B$ has a pre-image $a \in A$.

if $a \neq a'$, then $f(a) \neq f(a')$

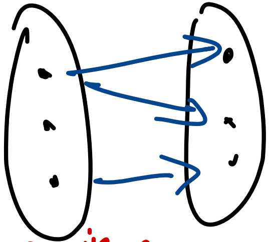
"injective"

2. f is *one-to-one*: for all $a, a' \in A$, if $f(a) = f(a')$ then $a = a'$.

$y = f(x)$



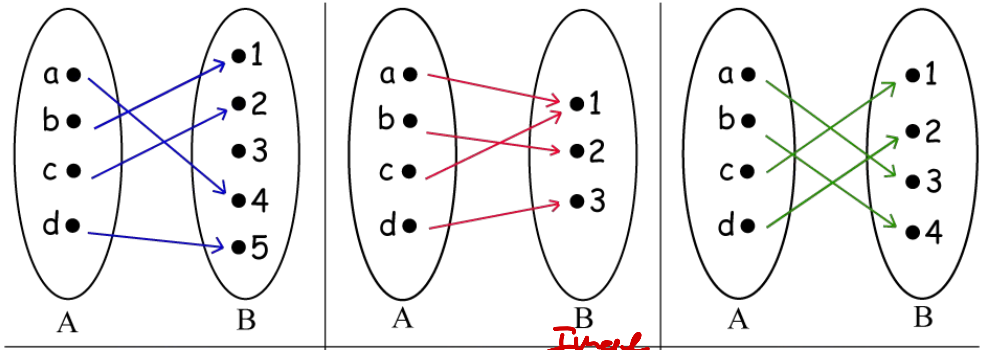
NOT A FUNCTION



pre-image

$f: X \quad Y$

$x \to \boxed{} \to y$



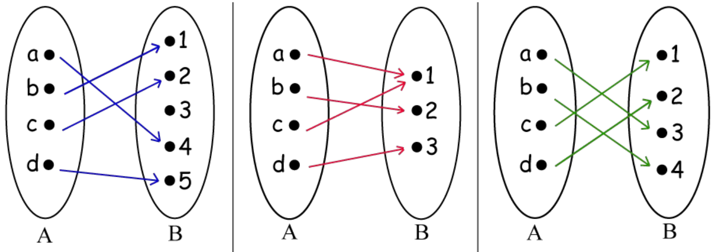
Injective (one-to-one) | **Surjective** (onto) | **Bijective** (one-to-one and onto)

Bijections Examples

g is an inverse of f if
$g(f(x)) = x \quad \forall x$

A *bijection* is a function for which every $b \in B$ has a unique *pre-image* $a \in A$ such that $f(a) = b$. Note that this consists of two conditions:

1. f is *onto*: every $b \in B$ has a pre-image $a \in A$.
2. f is *one-to-one*: for all $a, a' \in A$, if $f(a) = f(a')$ then $a = a'$.



Injective (one-to-one) | Surjective (onto) | Bijective (one-to-one and onto)

$f: A \to B$ and f is injective
$|A| \leq |B|$

. . . .

f is surjective
$|A| \geq |B|$

f is bijective
$|A| = |B|$

$f(x) = x^2$ $\quad f: \mathbb{R} \to \mathbb{R}$
neither

$f(x) = x^2$ $\quad f: \mathbb{R} \to \mathbb{R}^+ \cup \{0\}$
surjective

$f(x) = 2x$ $\quad f: \mathbb{N} \to \mathbb{N}$
injective

$f(x) = 2x$ $\quad f: \mathbb{R} \to \mathbb{R}$
inverse $\frac{1}{2}x$
bijective

$f(x) = x^3 - x$ $\quad f: \mathbb{R} \to \mathbb{R}$
$f(0) = 0$
$f(1) = 0$
surjective

A Useful Lemma

$f(x) = ax \pmod m$ a and m are coprime

$f : \{0, 1, \dots, m-1\} \to \{0, 1, \dots, m-1\}$

Claim: $f(x) = ax$ $(mod\ m)$ where a and m are coprime is a bijection.

Restated: The sequence $1a, 2a, 3a, \dots, (m-1)a$ is a reordering of the numbers $\{1, 2, \dots, m-1\}$.

Proof:

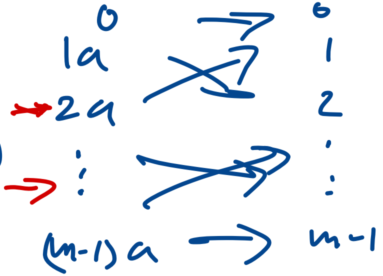
Assume for contradiction that f is not a bijection.

Then, $\exists x, y \in$ s.t. $ax \equiv ay \pmod m \Rightarrow ax - ay \equiv 0 \pmod m$

mod m $x \neq y$

$\Rightarrow \exists k \in \mathbb{Z}$ $ax - ay = km$. Since, a and m are coprime they share no factors and thus $m \mid (x-y)$

This is a contradiction since $x, y \in \{0, 1, \dots, m-1\}$ so $x - y < m$. Thus, f is a bijection.



$$\frac{a(x-y)}{m} = k$$

no common factor

integer

Existence of an Inverse

Goal:
$\exists x$ s.t. mod m
$ax \equiv 1 \mod m$

Thm: if a and m are coprime, then a has an inverse in $mod\ m$

Proof:

Consider the sequence from before $1a, 2a, \ldots, (m-1)a$

We know this sequence is a bijection to $\{1, 2, \ldots, m-1\}$

if a and m are coprime. $\exists$ some ya in the sequence that maps to 1

Thus, $ya \equiv 1 \pmod m$, y is then the inverse of $a \pmod m$.

A Necessary Lemma

the existence of an inverse

Lemma: ~~x~~ a and m being coprime is a <u>necessary</u> condition for ~~$f(x) = ax \pmod{m}$ to be a bijection.~~

Proof: if $\gcd(a, m) > 1$ then a doesn't have an inverse $\pmod{m}$

Prove directly. Let $d = \gcd(a, m)$ and a has an inverse $\pmod{m}$

$ay \equiv 1 \pmod{m} \Rightarrow ay = mk + 1 \quad k \in \mathbb{Z}$. Since, $d \mid a$ and $d \mid m$

inverse

we also know $d \mid ay$ and $d \mid mk \Rightarrow d \mid ay - mk$ Lec. 1B

$ay - mk = 1$, Thus $d \mid 1$. So, d must be equal to 1. Thus,

a and m are coprime.

Inverse is Unique (From Discussion 2C Q3E)

Suppose $x, x' \in \mathbb{Z}$ are both inverses of a modulo m. Is it possible that $x \not\equiv x' \pmod{m}$?

Suppose x and x' are inverses of a mod m

Then,

$$ax \equiv ax' \equiv 1 \pmod{m}$$

$$xax \equiv xax'$$

since $xa \equiv 1$

$$\cancel{xa}x \equiv \cancel{xa}x'$$

$$x \equiv x'$$

$\square$

What makes prime numbers so special?

$52 \to 2 \cdot 2 \cdot 13$

1. Building blocks of all numbers ← all numbers have a prime factorization
2. Given a prime p any number that's not a multiple of p is coprime to p

   i.e. $\gcd(x, p) = 1$ for all x that is not a multiple of p.

   Thus, the inverse always exists in modulo p

Working in mod p guarantees that division ~~almost~~ always

you can't divide by zero!

$0, p, 2p, 3p$

$0 \equiv p \equiv 2p \equiv \dots \pmod{p}$

Galois Field
"GF(p)"
mod p

Fermat's Little Theorem Examples

Thm: For any prime p and any a in $\{1, 2, \ldots, p-1\}$, we have $a^{p-1} \equiv 1$ $(mod\ p)$.

Examples: 4^6 (mod 7), 4^{42} (mod 7)

7 is prime

$4^{7-1} \equiv 4^6 \equiv 1 \pmod 7$

$\underbrace{4 \cdot 4}_{16} \cdot \underbrace{4 \cdot 4}_{\equiv} \cdot \underbrace{4 \cdot 4}_{\equiv}$

$\equiv 2 \cdot 2 \cdot 2 \equiv 8 \equiv 1 \pmod 7$

$4^{42} \equiv (4^6)^7 \pmod 7$

$\equiv 1^7$

$\equiv 1$

by FLT $4^6 \equiv 1$

Fermat's Little Theorem Proof

Thm: For any prime p and any a in $\{1, 2, \ldots, p-1\}$, we have $a^{p-1} \equiv 1 \ (mod\ p)$.

Proof:

$1a, 2a, 3a, \ldots, (p-1)a$ is a reordering of $1, 2, 3, \ldots, p-1$

$$1a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1)$$

$$1 \cdot 2 \cdot 3 \cdots (p-1) \cdot \underbrace{a \cdot a \cdots a}_{(p-1)} \equiv 1 \cdot 2 \cdot 3 \cdots (p-1)$$

$$\cancel{1 \cdot 2 \cdot 3 \cdots (p-1)} \cdot a^{p-1} \equiv \cancel{1 \cdot 2 \cdot 3 \cdots (p-1)}$$

$$a^{p-1} \equiv 1 \quad (mod\ p)$$

Chinese Remainder Theorem (CRT) Example

Find a x in mod 30 such that it satisfies the following equations

$x \equiv 1\ (mod\ 2), \quad x \equiv 2\ (mod\ 3), \quad x \equiv 3\ (mod\ 5)$

$x = 11$

idea! $x = a + b + c$

$a \equiv 1 \pmod 2$ ✓ $b \equiv 0 \pmod 2$ ✓ $c \equiv 0 \pmod 2$ ✓

$a \equiv 0 \pmod 3$ ✓ $b \equiv 2 \pmod 3$ ✓ $c \equiv 0 \pmod 3$ ✓

$a \equiv 0 \pmod 5$ ✓ $b \equiv 0 \pmod 5$ ✓ $c \equiv 3 \pmod 5$ ✓

Guess: $a = 3 \cdot 5 = 15$ ✓ $b = 2 \cdot 5 = 10$ $c = 2 \cdot 3 = 6$

$b = 2 \cdot 2 \cdot 5 = 20$ ✓ $c = 2 \cdot 3 \cdot 3 = 18$ ✓

$x = 15 + 20 + 18$ $53 \bmod 30 \Rightarrow \boxed{23 \pmod{30}} = x$

Chinese Remainder Theorem

Chinese Remainder Theorem: Let $n_1, n_2, \ldots, n_k$ be positive integers that are coprime to each other. Then, for any sequence of integers a_i there is a unique integer x between 0 and $N = \underbrace{\prod_{i=1}^{k} n_i}_{\text{product}}$ that satisfies the congruences:

$$\begin{cases} x & \equiv a_1 \pmod{n_1} \\ \vdots & \equiv \vdots \\ x & \equiv a_i \pmod{n_i} \\ \vdots & \equiv \vdots \\ x & \equiv a_k \pmod{n_k} \end{cases}$$

Given $n_1, n_2, \ldots, n_k$ that are coprime to each other. $N = n_1 \cdot n_2 \cdots n_k$

$\exists$ a unique solution $x \in \{0, 1, \ldots, N-1\}$ that satisfies all the equations.

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