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: $4^{42} \pmod{7}$

Recap

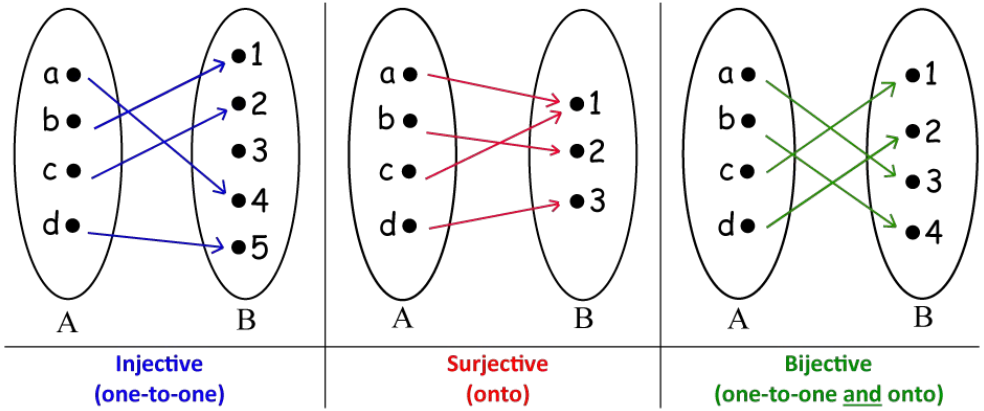
- Division Algorithm
- Greatest Common Divisor (GCD) Definition
- GCD Algorithm: Application and Proof
- Every number has a unique prime factorization
- Mod as a *Space*: Defined Addition, Subtraction, Multiplication and Division
- Definition of Coprime
- Definition of Inverse and division via multiplying inverse
- Extended Euclid's Algorithm to find inverse
- Repeated Squaring

Bijections

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 $a = a'$.

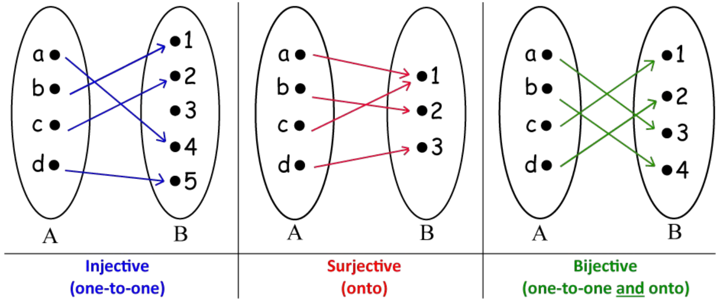


Bijections Examples

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 $a = a'$.



A Useful Lemma

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

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

Proof:

A Necessary Lemma

Lemma: x and m being coprime is a necessary condition for $f(x) = ax \ (mod\ m)$ to be a bijection.

Proof:

Existence of an Inverse

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

Inverse is Unique (From Discussion 2C Q3E)

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

What makes prime numbers so special?

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

Fermat's Little Theorem Examples

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

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

Fermat's Little Theorem Proof

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

Proof:

Chinese Remainder Theorem (CRT) Example

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

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

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 $N = \prod_{i=1}^{k} n_i$ that satisfies the congruences:

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

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