Q : When I was a TA, I once tried to put students in my discussion into groups.

If I group students into 3, there'll be 2 students left;

If I group students into 5, there'll be 3 students left;

If I group students into 7, there'll be 2 students left;

Guess : how many students attended my discussion?

1. Exponentiation

Notation: For $a, n \in \mathbb{N}$, we use a^n to denote $\underbrace{a \cdot \ldots \cdot a}_{n\# \text{ of } a\text{'s}}$.

Question: How to efficiently compute $a^n \% m$?

$a^n \bmod m$

Idea: If $n = 2k$, then $a^n = a^{2k} = a^k \cdot a^k$

If $n = 2k+1$, then $a^n = a^{2k+1} = a^k \cdot a^k \cdot a$

After computing $a^k \% m$, the rest is easy!

Algorithm.

```
mod-exp (a, n, m):
  # the repeated squares algorithm to compute modular exponentiation
  # input: natural numbers a, n, m and m > 0
  # output: a^n % m
  if n = 0: return 1
  if n is even:
    z = mod-exp(a, n/2, m)
    return (z * z) % m
  if n is odd:
    z = mod-exp(a, (n-1)/2, m)
    return (z * z * a) % m
```

(1) $z = a^k \% m$

$a^k \equiv z \pmod m$

$a^n = (a^k)(a^k) \equiv z \cdot z \pmod m$

$\Rightarrow a^n \% m = (z \cdot z) \% m$

k

(2) $a^n = a^k \cdot a^k \cdot a \equiv z \cdot z \cdot a \pmod m$

$\Rightarrow a^n \% m = (z \cdot z \cdot a) \% m$

E.g. Compute $10^{20} \% 7$.

$10 \equiv 3 \pmod 7$

$\Rightarrow 10^{20} \equiv 3^{20} \pmod 7$

$\Rightarrow 10^{20} \% 7 = 3^{20} \% 7$ $\qquad 3^{20} \equiv$ __ $\pmod 7$.

$3^1 \equiv 3 \pmod 7$

$3^2 \equiv 3^2 \equiv 2 \pmod 7$

$\rightarrow 3^4 \equiv 4 \pmod 7$

$3^8 \equiv 16 \equiv 2 \pmod 7$

$\rightarrow 3^{16} \equiv 4 \pmod 7$

$20 = 16+4. \Rightarrow 3^{20} = 3^{16} \cdot 3^4 \equiv 4 \cdot 4 \equiv 2 \pmod 7$

Hence $10^{20} \equiv 3^{20} \equiv 2 \pmod 7$

$\Rightarrow 10^{20} \% 7 = 2 \% 7 = 2.$

2. Linear Congruences

Goal: want to solve linear congruences $ax \equiv b \pmod m$

where $m \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$, x is a variable.

Recall
- If $ax \equiv 1 \pmod m$ then x is an inverse of a modulo m denoted a^{-1} modulo m.
- An inverse of a modulo m exists $\Longleftrightarrow$ $\boxed{\gcd(a,m) = 1.}$

$x_1, x_2 \in \mathbb{Z}$ are both a^{-1} mod m, $\Rightarrow x_1 \equiv x_2 \pmod m$

This inverse is unique modulo m, and can be found using extended Euclidean algorithm, because

I can find $s, t \in \mathbb{Z}$, s.t. $1 = as + mt$.

$\Rightarrow 1 \equiv as \pmod m$

$\Rightarrow s$ is an inverse of a modulo m.

- If $a \equiv b \pmod{m}$ and $c \in \mathbb{Z}$, then $ac \equiv bc \pmod{m}$.
- Can't divide both sides by an integer.

  e.g. $4 \equiv 2 \pmod{2}$ $\quad 2 \not\equiv 1 \pmod{2}$

$\boxed{\text{Thm}}$ Let $a, b, c \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

Pf: Since $\gcd(c, m) = 1$, there exists c^{-1} modulo m.

$$ac \equiv bc \pmod{m}$$

$$\Rightarrow acc^{-1} \equiv bcc^{-1} \pmod{m}$$

$$\Rightarrow a \equiv b \pmod{m}.$$

$\boxed{\text{Goal}}$ $x \equiv ? \pmod{7}$

all sol. $x = ? + 7n$

E.g. Find all solutions of $3x \equiv 4 \pmod{7}$.

Step 1: Check $\gcd(3,7) = 1$ using Euclidean algorithm.

$$7 = 2 \times 3 + 1$$

$$3 = 3 \times 1 + 0 \qquad \Rightarrow \gcd(3,7) = 1.$$

Step 2: Find a 3^{-1} modulo 7 using extended Euclidean algo.

$$1 = 7 - 2 \times 3 \leftarrow$$

$$\Rightarrow \boxed{1 \equiv -2 \times 3 \pmod{7}}$$

$$\Rightarrow -2 \text{ is a } 3^{-1} \text{ modulo } 7.$$

Step 3: $3x \equiv 4 \pmod{7}$

$$3^{-1} 3x \equiv \boxed{3^{-1}} 4 \pmod{7}$$

$$\Rightarrow x \equiv -2 \cdot 4 = -8 \pmod{7}$$

Conclude: solutions are $-8 + 7n$ for $n \in \mathbb{Z}$

2. The Chinese Remainder Theorem

Goal: want to solve system of linear congruences.

E.g.
$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

e.g. 23 is a solution.
a solution means a integer that satisfies all three congruences.

Rem. For a general system of linear congruences, the existence of solution is not guaranteed. For example, the system

$$\begin{cases} x \equiv 1 \pmod 2 & \Rightarrow x \text{ is odd} \\ x \equiv 0 \pmod 4 & \Rightarrow x \text{ is even.} \end{cases}$$

has no solution.

$\boxed{\text{Def}}$ The integers a, b are **relatively prime** if $\gcd(a,b) = 1$.

$\boxed{\text{Thm}}$ (The Chinese Remainder Theorem)

Let $1 < m_1, m_2, \ldots, m_n \in \mathbb{Z}^+$ be pairwise relatively prime.
Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Then the system

$\rightarrow x \equiv a_1 \pmod{m_1}$

$\rightarrow x \equiv a_i \pmod{m_i}$

$\rightarrow x \equiv a_n \pmod{m_n}$

has a solution.

① $x \equiv a_1 \pmod{m_1}$
② $x \equiv a_2 \pmod{m_2}$
③ $x \equiv a_3 \pmod{m_3}$

$a_1 (m_2 m_3)^{-1} \bmod m_1$

$$x = \underbrace{(?_1)\, m_2 m_3}_{\equiv a_1 \pmod{m_1}} + \underbrace{(?_2)\, m_1 m_3}_{\equiv a_2 \pmod{m_2}} + \underbrace{(?_3)\, m_1 m_2}_{\equiv a_3 \pmod{m_3}}$$

Pf: Let $M_i = \prod_{j \neq i} m_j$. ~~$m_i$~~

m_i's are pairwise relatively prime,

$\Rightarrow \gcd(M_i, m_i) = 1$.

$\Rightarrow M_i^{-1}$ modulo m_i exists.

$\exists\, y_i \in \mathbb{Z}$, $M_i y_i \equiv 1 \pmod{m_i}$.

Now, $x = \underbrace{a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n}_{m_i}$ is a solution to the system.

[Check: $\forall i$, $x \equiv a_i M_i y_i \pmod{m_i} \Rightarrow x \equiv a_i \pmod{m_i}$] $\square$

Rem. In today's discussion, you will see that the solution in the theorem above is unique modulo $m = m_1 \cdot m_2 \cdots m_n$.

E.g. Find the smallest positive integer solution to the system

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

Step 1: $m = 3 \times 5 \times 7 = 105$

$M_1 = \frac{m}{3} = 35$

$M_2 = \frac{m}{5} = 21$

$M_3 = \frac{m}{7} = 15$

Step 2: compute y_i, an inverse of M_i modulo m_i.

$M_1 = 35 \equiv 2 \pmod 3$

$2 \times 2 \equiv 1 \pmod 3 \Rightarrow$ let $y_1 = 2$.

$M_2 = 21 \equiv 1 \pmod 5 \Rightarrow$ let $y_2 = 1$.

$M_3 = 15 \equiv 1 \pmod 7 \Rightarrow$ let $y_3 = 1$.

Step 3: Find a solution

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$$
$$= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$$

Conclude: Any solution is congruent to 232 modulo 105

$\Rightarrow$ the smallest positive integer solution is 23.

$233 - 105 - 105 = 23$

Ex. (prep for tmr). Given prime p, integer a s.t. $a \not\equiv 0 \pmod p$.

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

$x \mapsto ax \bmod p$

is a bijection.

Pf: First, notice that f is well-defined.

Goal: Prove injection.

Now, suppose $f(x_1) = f(x_2)$ for $0 \le x_1, x_2 \le p-1$. integers.

$\Rightarrow ax_1 \bmod p = ax_2 \bmod p$

$\Rightarrow ax_1 \equiv ax_2 \pmod p$

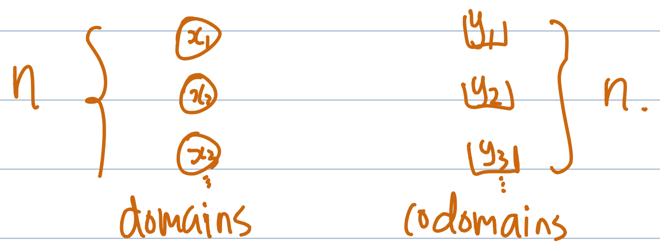
$\Rightarrow p \mid a(x_1 - x_2)$

Since p is prime, and $p \nmid a$, so $p \mid x_1 - x_2$.

Since $0 \le x_1, x_2 \le p-1$, so $x_1 = x_2$.

Thus f is an injection.

Notice domain and codomain are of the same finite cardinality.
By Pigeonhole, f is a bijection.



Ex: Find $f: X \to Y$, s.t. f is an injection, and
$|X| = |Y| = |\mathbb{N}|$, but f is not a surjection.