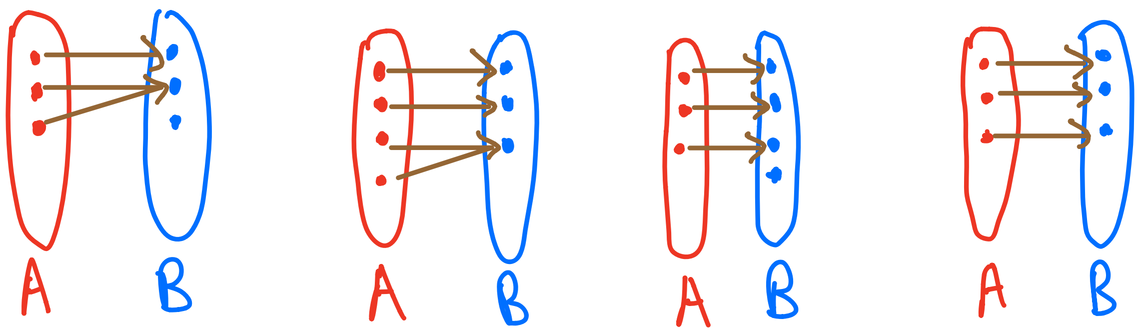
Bijections

Mapping $f: A \to B$

<u>onto</u> : Every element in B has some $a \in A$ mapping to it

<u>one-to-one</u>: No two elements in A map to the same element in B

Function | Onto Function | One-to-One Function | Bijection



f is both onto & one-to-one $\Leftrightarrow$ f is bijective $\Leftrightarrow$ f has an inverse function

Fermat's Little Theorem

For any prime p,

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

Or equivalently,

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{for } a \neq 0$$

2 Euler's Totient Function

Euler's totient function is defined as follows:

$$\phi(n) = |\{i : 1 \le i \le n, \texttt{gcd}(n,i) = 1\}|$$

In other words, $\phi(n)$ is the total number of positive integers less than or equal to n which are relatively prime to it. Here is a property of Euler's totient function that you can use without proof:

For m,n such that $\texttt{gcd}(m,n) = 1$, $\phi(mn) = \phi(m)\cdot\phi(n)$.

(a) Let p be a prime number. What is $\phi(p)$?

$1, 2, \ldots, p-1, p \rightarrow \boxed{p-1}$

1
p
p^2
$\vdots$
$p^k - p$

(b) Let p be a prime number and k be some positive integer. What is $\phi(p^k)$?

$$p^k - 1 - (p^{k-1} - 1)$$
$$= \boxed{p^k - p^{k-1} = p^{k-1}(p-1)}$$

(c) Let p be a prime number and a be a positive integer smaller than p. What is $a^{\phi(p)} \pmod{p}$? *(Hint: use Fermat's Little Theorem.)*

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

(d) Let b be a positive integer whose prime factors are $p_1, p_2, \ldots, p_k$. We can write $b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.

Show that for any a relatively prime to b, the following holds:

$$\forall i \in \{1,2,\ldots,k\},\ a^{\phi(b)} \equiv 1 \pmod{\underline{p_i}}$$

$$a^{\phi(b)} = a^{\phi(p_1^{\alpha_1})\,\phi(p_2^{\alpha_2})\cdots\phi(p_k^{\alpha_k})}$$
$$\left(a^{\phi(p_1^{\alpha_1})}\right)^{\phi(p_2^{\alpha_2})\phi(p_3^{\alpha_3})\cdots\phi(p_k^{\alpha_k})} \pmod{p_1}$$

$$a^{\left(p^{\alpha_1 - 1}\cdot(p-1)\right)}$$

$$\equiv \left(\left(a^{(p_1-1)}\right)^{p^{\alpha_1-1}}\right)^{\phi(p_2^{\alpha_2})\phi(p_3^{\alpha_3})\cdots\phi(p_k^{\alpha_k})}$$

$$\equiv \left(1^{p^{\alpha_1-1}}\right)^{\phi(p_2^{\alpha_2})\phi(p_3^{\alpha_3})\cdots\phi(p_k^{\alpha_k})} \equiv 1 \pmod{p_1}$$

Chinese Remainder Theorem

For coprime $n_1, n_2, n_3, \ldots, n_K$:

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$x \equiv a_3 \pmod{n_3}$$
$$\vdots$$
$$x \equiv a_K \pmod{n_K}$$

There exists a unique solution modulo $N = \prod_{i=1}^{K} n_i$

(i.e. in $\{0, 1, \ldots, N\}$)

How do we find this solution?

For $i = 1$ to K:

Let $N_i = \dfrac{N}{n_i}$ (i.e., multiply all $n_1 \cdots n_K$ except n_i)

Let I_i be $N_i^{-1} \pmod{n_i}$

Construct $v_i = N_i I_i$

$$x = a_1 v_1 + a_2 v_2 + \ldots + a_n v_n \pmod{N}$$

is our solution.

Satisfying Linear Algebraic Intuition

V_i's can be thought of as a k-dimensional "coordinate basis"

X represents the point $(a_1, a_2, \ldots, a_n)$ in this k-dimensional space

$$X = a_1 V_1 + a_2 V_2 + \ldots + a_n V_n$$

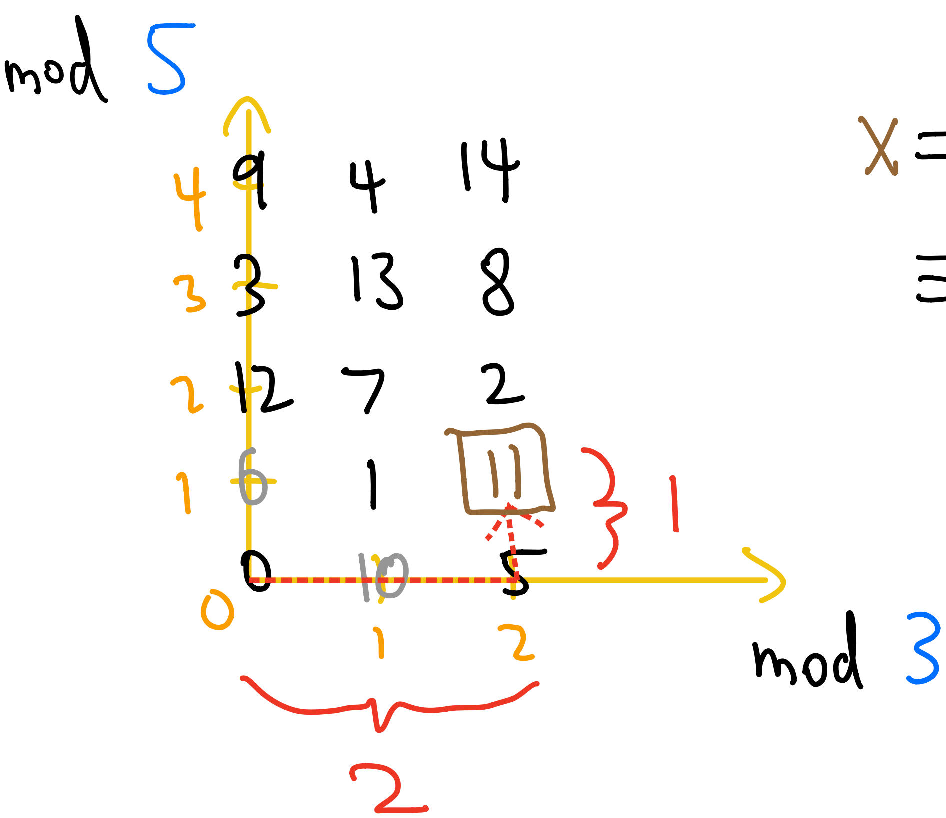
Example (in 2 dimensions)

$$X \equiv 2 \pmod 3$$
$$X \equiv 1 \pmod 5$$

$$N = 3 \cdot 5 = 15$$

$$V_1 = 10 \equiv \begin{bmatrix} 1 \pmod 3 \\ 0 \pmod 5 \end{bmatrix}$$

$$V_2 = 6 \equiv \begin{bmatrix} 0 \pmod 3 \\ 1 \pmod 5 \end{bmatrix}$$



$$X = 2 \cdot 10 + 1 \cdot 6$$
$$\equiv \boxed{11} \pmod{15}$$

3 Chinese Remainder Theorem Practice

In this question, you will solve for a natural number x such that,

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 4 \pmod 7 \end{aligned} \tag{1}$$

$N = 3 \cdot 5 \cdot 7 = 105$

(a) Suppose you find 3 natural numbers a, b, c that satisfy the following properties:

$$a \equiv 2 \pmod 3 \; ; \; a \equiv 0 \pmod 5 \; ; \; a \equiv 0 \pmod 7, \tag{2}$$

$$b \equiv 0 \pmod 3 \; ; \; b \equiv 3 \pmod 5 \; ; \; b \equiv 0 \pmod 7, \tag{3}$$

$$c \equiv 0 \pmod 3 \; ; \; c \equiv 0 \pmod 5 \; ; \; c \equiv 4 \pmod 7. \tag{4}$$

Show how you can use the knowledge of a, b and c to compute an x that satisfies (1).

$x = a + b + c$

In the following parts, you will compute natural numbers a, b and c that satisfy the above 3 conditions and use them to find an x that indeed satisfies (1).

(b) Find a natural number a that satisfies (2). In particular, an a such that $a \equiv 2 \pmod 3$ and is a multiple of 5 and 7. It may help to approach the following problem first:

(b.i) Find a^*, the multiplicative inverse of 5×7 modulo 3. What do you see when you compute $(5 \times 7) \times a^*$ modulo 3, 5 and 7? What can you then say about $(5 \times 7) \times (2 \times a^*)$?

$$a^* \equiv (5 \times 7)^{-1} \pmod 3$$

$$\equiv 2^{-1} \pmod 3$$

$$= 2$$

$$5 \times 7 \times 2 \equiv 1 \pmod 3$$

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

$a = \boxed{140}$

(c) Find a natural number b that satisfies (3). In other words: $b \equiv 3 \pmod 5$ and is a multiple of 3 and 7.

$$b^* \equiv (3 \times 7)^{-1} \pmod 5$$

$$\equiv 21^{-1} \pmod 5$$

$$\equiv 1^{-1} \pmod 5 = 1$$

$$3 \times 7 \times 1 \equiv 1 \pmod 5$$

$$3 \times 7 \times 1 \times 3 \equiv 3 \pmod 5 \qquad \boxed{63}$$

(d) Find a natural number c that satisfies (4). That is, c is a multiple of 3 and 5 and $\equiv 4 \pmod 7$.

$$c^* \equiv (3 \times 5)^{-1} \pmod 7$$

$$\equiv 15^{-1} \pmod 7$$

$$\equiv 1^{-1} \pmod 7 = 1$$

$$3 \times 5 \times 1 \equiv 1 \pmod 7 \Rightarrow 3 \times 5 \times 1 \times 4 = \boxed{60}$$

(e) Putting together your answers for Part (a), (b), (c) and (d), report an x that indeed satisfies (1).

$$x = a + b + c$$

$$= \boxed{263} \equiv \boxed{53} \pmod{105}$$

1 Baby Fermat

Assume that a does have a multiplicative inverse mod m. Let us prove that its multiplicative inverse can be written as $a^k \pmod{m}$ for some $k \geq 0$.

(a) Consider the sequence $a, a^2, a^3, \ldots \pmod{m}$. Prove that this sequence has repetitions. (**Hint:** Consider the Pigeonhole Principle.)

infinite numbers $\longleftrightarrow$ m residue classes

(b) Assuming that $a^i \equiv a^j \pmod{m}$, where $i > j$, what can you say about $a^{i-j} \pmod{m}$?

$$\underbrace{(a^{-1})\cdots(a^{-1})(a^{-1})}_{j}\, a^i \equiv \underbrace{(a^{-1})(a^{-1})\cdots(a^{-1})}_{j}\ \underbrace{a \cdot a \cdot a \cdots a}_{j} \pmod{m}$$

$$a^{i-j} \equiv 1 \pmod{m}$$

(c) Prove that the multiplicative inverse can be written as $a^k \pmod{m}$. What is k in terms of i and j?

$$a^{i-j} \equiv 1 \pmod{m}$$

$$\underbrace{\left(a^{i-j-1}\right)}_{\substack{\parallel \\ a^{-1}}} \cdot a \equiv 1 \pmod{m}$$