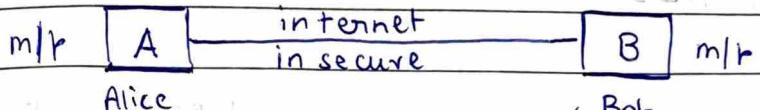


Cryptography :

Eve (Intruder/Eavesdropper)

plain text



Encryption
(key k)

Decryption

$$m = (c, k)$$

legitimate

triads

CIA ~~Security~~ :

1. Confidentiality
2. Integrity
3. Authentication \Rightarrow Authorization } Access control
4. non-repudiation : the assurance that someone cannot deny the validity of something
5. Availability



Attacks :

1. Phishing
 2. Side channel
 3. Dictionary
- } Identity Theft

1. DoS | DDOS
- } Disruption of Service

1. Malware
- } Information Warfare

a. Trojan Horse (looks like utility program)

b. virus (from one file to another)

c. worms (" " " computer " ")

#

Symmetric

Cryptography Algo's

Asymmetric

Cryptography Algo's

*

DES, AES

RSA, ElGamal, ECC

* one key, k 2 keys, k_1 for
encryption, k_2 for
decryption.

★

Go through PDF

Number Theory : $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

3/12/21
① Divisibility : Let $a, b \in \mathbb{Z}$

If a is divisible by b ,

b divides a ($b \mid a$) \Leftrightarrow then

$\exists c \in \mathbb{Z}$ such that $a = bc$

otherwise $b \nmid a$ (b doesn't divide a)

Eg. $2 \mid 4$, $2 \nmid 5$

\downarrow

~~if $b \neq 0$ then $a = b \cdot c$~~

i.e. $b \mid a \quad b \leq a$

\downarrow divisor \downarrow dividend

divisor dividend

~~if $b \neq 0$ then $a = b \cdot c$~~

If $b < a$, b is called proper divisor

Theorems: $a, b, c \in \mathbb{Z}$

1. $|a|$, $a \neq 0$ and $a \neq 0$

2. $0 \mid a$ (except $a = 0$)

3. $a \mid b$ and $b \mid a \Rightarrow a = \pm b$

4. $a \mid b \Rightarrow a \mid -b$

5. $a \mid b$ and $b \mid c \Rightarrow a \mid c$

6. $a \mid b$ and $a \mid c \Rightarrow a \mid (b \pm c)$

\downarrow

proof: If $a \mid b$, $\exists x$ s.t. $b = ax$ - ①

$a \mid c$, $\exists y$ s.t. $c = ay$ - ②

$\therefore b \pm c$ s.t. $b \pm c = ax \pm ay$

from equation ① and ② \Rightarrow

$$\begin{aligned} b+c &= a(x+y) \\ b+c &= a(x+y) \end{aligned}$$

$$\begin{array}{l} pq+q \neq \neq \\ b+c = \end{array}$$

$$\therefore a \mid (b+c)$$

$$b-c = a(x-y)$$

$$\therefore a \mid (b-c) \Rightarrow a \mid (b+c)$$

② Division Algorithm:

Let $a, b \in \mathbb{Z}$, $a \nmid b \exists q, r \in \mathbb{Z}$

$$b = aq + r \quad 0 \leq r \leq a$$

if $a \mid b$ then $r = 0$

a is perfect divisor of b

$n \in \mathbb{Z}$, $1 \mid n$ and $n \mid n \leftarrow$ trivial divisors

prime no.

has # prime number : $\exists p$ such that $p \mid n$ and $p \nmid k$ only

only

trivial # composite numbers : $n = ab$: $1 \leq a, b < n$

divisors

$\text{gcd}(a, b, \dots)$ → Greatest common Divisor

for $\text{GCD}(a, b)$, let $a, b \in \mathbb{N}$

if $a = b = 0 \rightarrow \text{GCD}(a, b) = 0$

$$\text{GCD}(a, b) = d \Rightarrow d \mid a \text{ and } d \mid b$$

assuming $a < b$, d ranges from

$$1 < d < a$$

e.g. $\text{GCD}(25, 125) = 25$
i.e.

$\exists f \in \mathbb{N}$ such that $f \mid 25$ and $f \mid 125$

Rule: If $\exists f \in \mathbb{N}$, such that $f \mid a$ and $f \mid b$

$\Rightarrow f \mid d$ where $d = \text{l.c.m. of } a, b$

$\exists f \in (\ 1 \leq f \leq d)$

in this case $f = 5$

$\exists f \in \text{i.e. } 5 \mid 25 \text{ and } 5 \mid 125 \Rightarrow 5 \mid 125$

Theorem: If $a, b \in \mathbb{Z}$ then $\text{d} \mid a$ and $\text{d} \mid b$

$\text{gcd}(a, b) = d$; $\exists x, y \in \mathbb{Z}$ such that

$$= (d \cdot x) + (b \cdot y) \Rightarrow \boxed{ax + by = d}$$

Theorem: For $a, b, c \in \mathbb{Z}$ s.t. $c \neq 0$

$c \mid a \cdot b$ and

$$\boxed{\text{gcd}(a, c) = 1} \quad (\text{Coprime})$$

then $c \mid b$ (relatively prime)

Proof: $\text{gcd}(a, c) = 1$ then $\exists x, y \in \mathbb{Z}$ such that

$$ax + cy = 1$$

$$b(ax + cy) = b$$

$$abx + bcy = b$$

from previous theorem we can rewrite as:

$$\gcd(ab, bc) = b$$

$$\Rightarrow b \mid ab \text{ and } b \mid bc$$

given $c \mid ab$

and we can say $c \mid abc$

 $\Rightarrow c \mid b$
(From the previous rule)

Theorem : Let p be prime and let $a, b \in \mathbb{Z}$

$$p \mid ab \Rightarrow p \mid a \text{ or } p \mid b$$

Proof : Let

$$p \nmid a + \text{then } \gcd(a, p) = 1$$

and given $p \mid ab$

then from previous theorem

$$p \mid b$$

Homework, check book for soln.

Theorem : There are infinite no. of primes

Fundamental Theorem of Arithmetic (FTA)

$$\pm n = (\pm 1) \cdot P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdots P_r^{\alpha_r}$$

eg.

$$36 = 4 \cdot 9 = 2^2 \cdot 3^2$$

$$23 = 23^1$$

Factorization of a number cannot be done in polynomial time that is why RSA algo. is secure.

gcd(12, 18)

$$a = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdots P_r^{\alpha_r}$$

$$b = P_1^{\beta_1} \cdot P_2^{\beta_2} \cdots P_r^{\beta_r}$$

so,

$$\text{gcd}(a, b) = P_1^{\min(\alpha_1, \beta_1)} \cdot P_2^{\min(\alpha_2, \beta_2)} \cdots P_r^{\min(\alpha_r, \beta_r)}$$

And

$$\text{lcm}(a, b) = P_1^{\max(\alpha_1, \beta_1)} \cdot P_2^{\max(\alpha_2, \beta_2)} \cdots P_r^{\max(\alpha_r, \beta_r)}$$

$$\text{eg. } a = 36 = 2^2 \cdot 3^2$$

$$b = 24 = 2^3 \cdot 3^1$$

so

$$\text{gcd}(24, 36) = 2^{\min(2, 3)} \cdot 3^{\min(2, 1)}$$

$$= 2^2 \cdot 3^1 = 12$$

$$\text{lcm}(24, 36) = 2^{\max(2, 3)} \cdot 3^{\max(2, 1)}$$

$$= 2^3 \cdot 3^2$$

$$= 72$$

7/1/22

Euclidean Algorithm:

Time complexity: $\log^3(n)$

$$(a, b) = d \Rightarrow \text{if } a < b:$$

$i = 1$ to a :

$$\frac{a}{i} \text{ & } \frac{b}{i}$$

$$\gcd(-31, 24) = ?$$

$$\begin{array}{r} 24 \\ | \\ 31 \end{array} \longrightarrow \gcd(24, 31) \Rightarrow$$

$$24 \quad 31$$

$$\begin{array}{r} 7 \\ | \\ 24 \end{array} \longrightarrow \gcd(7, 24)$$

$$24 \quad 21$$

$$\begin{array}{r} 3 \\ | \\ 7 \end{array} \longrightarrow \gcd(3, 7)$$

$$3 \quad 7$$

$$\begin{array}{r} 1 \\ | \\ 3 \end{array} \longrightarrow \gcd(1, 3)$$

$$1 \quad 3$$

$$\begin{array}{r} 0 \\ | \\ 0 \end{array} \quad = \quad 1$$

Therefore

$$1|3, 1|7,$$

$$\boxed{1|24, 1|31}$$

hence

$$\gcd(24, 31) = 1$$

on generalizing: assume $a < b$:

$$\gcd(a, b) = d = ? = ?$$

$$(0 \leq r_2 < a) \quad \begin{array}{r} a \\ | \\ b \\ -ar_2 \\ \hline r_2 \end{array} \longrightarrow b = ar_2 + r_2$$

$$(0 \leq r_1 < r_2) \quad \begin{array}{r} r_2 \\ | \\ a \\ -r_2r_1 \\ \hline r_1 \end{array} \longrightarrow a = r_2r_1 + r_1$$

We

then

to
eu

$$(0 \leq r_2 \leq r_1)$$

$$(0 \leq r_3 < r_2)$$

$$r_{j-2} = r_{j-1} - r_j$$

$$31 = 24 \cdot 1 + 7$$

↓

$$7 = 24 \cdot (-1) + 31$$

⋮

⋮

$$(0 \leq g_2 \leq g_1) \quad \underline{g_{11}} \quad \boxed{g_1} \quad \boxed{g_2} \quad \rightarrow g = g_1 g_2 + g_2$$

$-g_1 g_2$

$$(0 \leq g_3 < g_2) \quad \underline{g_2} \quad \boxed{g_1} \quad \boxed{g_3} \rightarrow g_1 = g_2 g_3 + g_3$$

$\frac{g_2 g_3}{g_3}$

$$g_{j-2} = g_{j-1} \cdot q_j + r_j \quad \underline{g_{j-1}} \quad \boxed{g_{j-2}} \quad \boxed{r_j} \quad (0 \leq r_j < g_j)$$

$-g_{j-1} \cdot q_j$

$$\dots$$

$\frac{g_j}{\text{gcd}}$

$\frac{g_j \cdot q_{j+1}}{0}$

$$g_{j-1} = g_j \cdot q_{j+1} + 0$$

Since $(-).P + (-)I = P$: \oplus mark

$g_j | g_{j-1}$, $g_j | g_{j-2}$, ...

$(-).(-g_j | g_3) + g_j \cdot a_1 | g_j \cdot b$

$$(-).a_1 + (-).b + b = b$$

$$\therefore \text{gcd}(a, b) = -g_j$$

$$(-).1 + 80 = 27 \quad \text{is gcd}$$

We know if $\text{gcd}(a, b) = d$, $\exists x, y \in \mathbb{Z}$
then $a \cdot x + b \cdot y = d$.

$$(-).(-) + 80 + (-) = 27$$

$$(-).a + (-).b + (-) = 27$$

$$(-).a + (-).b + (-) = 27$$

To calculate x and y , we extended
Euclidean algorithm.

* Extended Euclidean Algorithm:

$$\gcd(21, 33) =$$

$$\begin{aligned} 33 &= 21 \cdot 1 + 12 \\ 21 &= 12 \cdot 1 + 9 \\ 12 &= 9 \cdot 1 + 3 \\ 9 &= 3 \cdot 3 \end{aligned}$$

$$\begin{array}{r} 21 \mid 33 \quad | \\ 21 \\ \hline 12 \mid 21 \quad | \\ 12 \\ \hline 9 \mid 12 \quad | \\ 9 \\ \hline 3 \mid 9 \quad | \\ 3 \\ \hline 0 \end{array}$$

so;
 $3 \mid 9, 3 \mid 12, 3 \mid 21, 3 \mid 33$
hence,
 $\gcd(21, 33) = 3$

traversing bottom to top.

$$\text{from } ③: 3 = 12 + 9 \cdot (-1)$$

$$\text{from } ②: 9 = 21 + 12 \cdot (-1)$$

~~$$\text{from } ①: 50;$$~~

$$3 = 12 + (21 + 12 \cdot (-1)) \cdot (-1)$$

$$3 = 12 + 21 \cdot (-1) + 12 \cdot (1)$$

$$3 = 21 \cdot (-1) + 12 \cdot (2)$$

$$\text{from } ①: 12 = 33 + 21 \cdot (-1)$$

~~$$\text{so,}$$~~

$$3 = 21 \cdot (-1) + (33 + 21 \cdot (-1)) \cdot (2)$$

$$= 21 \cdot (-1) + 33 \cdot (2) + 21 \cdot (-2)$$

$$3 = 33 \cdot (2) + 21 \cdot (-3)$$

hence
 $\{ \gcd(a, b) = d = by + ax \}$

* Modular Arithmetic:

$$\mathbb{Z} = \{ \dots -3, -2, -1, 0, 1, 2, 3, \dots \}$$

to make it finite:

$$\mathbb{Z} \bmod 5 = \{ [0], [1], [2], [3], [4] \}$$

$$\begin{array}{c} \mathbb{Z}/5\mathbb{Z} \\ \text{zero} \\ \text{class} \\ 11 \end{array}$$

$$\mathbb{Z}/5$$

$$16 \in \mathbb{Z} \bmod 5 = 16 \bmod 5$$

18

19

20

$$[0] = \{ \dots -10, -5, 0, 5, 10 \}$$

$$[1] = \{ \dots -9, -4, 1, 6, 11 \}$$

$$\vdots$$

$$\vdots$$

hence $[2] = [3]$

$$\mathbb{Z} = [0] \cup [1] \cup [2]$$

therefore,

$$\mathbb{Z}_n = \{ 0, 1, \dots, n-1 \}$$

Inverse: inverse of 33 = 21
inverse of 21 = -3

Modular Arithmetic:

$\mathbb{Z} = \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \}$ infinite

to make it finite consider $\mathbb{Z}/5\mathbb{Z}$

$\mathbb{Z} \text{ mod } 5 = \{ [0], [1], [2], [3], [4] \}$ complete

$x \equiv a \pmod{5} \iff x \in [a]$

$\mathbb{Z}/5\mathbb{Z}$ zero residue class

modulo / moduli

\mathbb{Z}_5

$0 \leq a < 5 \quad 15 \pmod{5} = 0$

$16 \in \mathbb{Z} \text{ mod } 5 = 16 \pmod{5} = 1$

$0, 1, 2, 3, 4 \quad 17 \pmod{5} = 2$

$18 \pmod{5} = 3$

$19 \pmod{5} = 4$

$20 \pmod{5} = 0$

$[0] = \{ \dots, -10, -5, 0, 5, 10, \dots \}$

$[1] = \{ \dots, -9, -4, 1, 6, 11, \dots \}$

$(x-1) \pmod{5} = (x \pmod{5}) - 1$

Hence $\mathbb{Z} \text{ mod } 5$

$\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3] \cup [4]$

therefore,

$$\boxed{\mathbb{Z}_n = \{ 0, 1, 2, \dots, n-1 \}}$$

Inverse: inverse of 33 $\equiv 21$

inverse of 21 $\equiv -3$

* Congruence : (\equiv)

Ex. ① $a \equiv b \pmod{n} \Leftrightarrow n \mid a - b$

② $a \not\equiv b \pmod{n} \Rightarrow \exists n \nmid a - b$

eg. $[+]$ $6 \equiv -1(5) \Rightarrow 5 \mid (6-1) \quad \checkmark$

$6 \equiv 2(5) \Rightarrow 5 \mid (6-2) \quad \times$

Equivalence Relations:

① Reflexive: $a \equiv a \pmod{n}$

$a = a \pmod{n} \Rightarrow n \mid a - a = n \mid 0$

hence satisfied.

② Symmetric:

eg. $6 \equiv 1(5)$

$1 \equiv 6(5) \Rightarrow 5 \mid (1-6)$

$5 \mid (-5) \quad \checkmark$

③ Transitive:

if $a \equiv b \pmod{n}$ and

$b \equiv c \pmod{n}$

$\Rightarrow a \equiv c \pmod{n}$

Standard notations:

$$\textcircled{1} \quad a \equiv b \pmod{n} \quad \textcircled{2} \quad \gcd(a, b) = d$$

\Updownarrow

$a \equiv b \pmod{n}$

$(a, b) = d$

$$\textcircled{3} \quad \operatorname{lcm}(a, b) = c$$

$[a, b] = c$

Rule

Theorem: IF both a and b are from same class then they are congruent else not congruent.

e.g.

$$[0] = \{ \dots, -10, -5, 0, 5, 10, \dots \}$$

$$[1] = \{ \dots, -9, -4, 11, 6, 11, \dots \}$$

⋮

$$\text{let } a = 11, b = 1 \in [1]$$

$$\text{then } 11 \equiv 1 \pmod{5} \Rightarrow 5 \mid (11-1) \quad \checkmark$$

but if $a = 11$ and $b = 5$

$$a \in [1] \quad b \in [0]$$

$$\text{then } 11 = 5(5) \Rightarrow 5 \mid (11-5) \quad \times$$



assume a is known in standard form
and b, n is unknown

$$b = c \cdot a \quad a \equiv b(n) \text{ or } a \equiv 0$$

e.g. $(d, 0)$

$$11 \equiv 1(5)$$

we can see

$$11 \bmod 5 = 1 \quad \text{and} \quad 11 \equiv 1(5)$$

$$11(5) = 1$$

so

$$B = [1, 0]$$

$11 \equiv 1(5)$ can also be written as

$$11(5) \equiv 1(5)$$

↑ 10 thousand

* exclude this

$$\text{hence } 1, 0, 2, \dots, 9 \equiv 1 \pmod{5}$$

$$\text{hence } 11 \equiv 1(5) \Rightarrow 5 \mid (11-1)$$

* Modulus operations:

$$\textcircled{1} \quad (a+b) \bmod n = a \bmod n + b \bmod n$$

$$\textcircled{2} \quad (a-b) \bmod n = a \bmod n - b \bmod n$$

$$\textcircled{3} \quad (a \cdot b) \bmod n = a \bmod n \cdot b \bmod n$$

11/1/22

$$\mathbb{Z}/5\mathbb{Z} = \mathbb{Z}_5 = \mathbb{Z} \text{ mod } 5 \cdot = \{0, 1, 2, 3, 4\}$$

\oplus (ADD), \otimes (MUL). Operations :-

$$\textcircled{1} \quad \text{let } a \in \mathbb{Z}_5, \quad a + \boxed{0} = a$$

↑
additive identity

denoted as e

Additive $\textcircled{2} \quad a + \boxed{-a} = 0 \equiv e \}$ here $a \in \mathbb{Z}$ and

Inverse eg. $-1 \in \mathbb{Z}$ s.t. $1 + (-1) = 0 \in \mathbb{Z}$

$$2 + \boxed{-2} = 0 \quad \text{but } -2 \notin \mathbb{Z}_5$$

$$\text{but } -2 \text{ mod } 5 = 3$$

and also $2 + 3 = 5 \in \mathbb{Z}$ and $5 \text{ mod } 5 = 0$.

so;

$$0 + 0 = 0$$

$$1 + 4 = 0$$

$$2 + 3 = 0$$

$$3 + 2 = 0$$

$$4 + 1 = 0$$

$\textcircled{3}$ For $a \in \mathbb{Z} \Rightarrow a * \boxed{1} = a$ Multiplicative Identity
 \Rightarrow here $e = 1$ always.

$\textcircled{4}$ Multiplicative Inverse $\Rightarrow a * \boxed{\frac{1}{a}} = e$

$$a * \frac{1}{a} = 1$$

$$a * b = 1 \Rightarrow \boxed{b = a^{-1}} = \frac{1}{a}$$

eg. $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

$$0 * \square = 0 \quad (\text{special case})$$

$$1 * 1 = 1$$

$$2 * 3 = 1 \quad \text{i.e. } (2 * 3) \bmod 5 = 1$$

$$3 * 2 = 1$$

$$4 * 4 = 1$$

∴ $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

~~2 * 5 = -2 * \square = 1~~ no multiplicative inverse

~~5 * 5 = -5 * \square = 1~~ ✓ $25(6) = 1$

∴ Therefore;

Multiplicative Inverse exists when

group size (n) is relatively prime with
element of the set.

eg.

⇒ 6 and 2 are not relatively prime

⇒ 6 and 5 are relatively prime.

Theorem: IF $a \in \mathbb{Z}_m$ has multiplicative inverse
iff $\gcd(a, m) = 1$.

Similar
proof

Proof: Assume $\gcd(a, m) = 1$, $\exists x, y \in \mathbb{Z}$, s.t.

$$ax + my = 1.$$

$$\Rightarrow ax = 1 + m(-y)$$

and we know $a \equiv b \pmod{n} \Rightarrow n|(a-b)$ or
 $\exists k \in \mathbb{Z}$ s.t. $a-b = kn$

$$\Rightarrow a = b + kn$$

Therefore $a \equiv 1 + m(-y)$

$$\Rightarrow m | (ax - 1)$$

$$\Rightarrow ax \equiv 1 \pmod{m} \Rightarrow ax(m) = 1$$

x can be found using extended euclidean algo.

In sets :

$$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\} \Rightarrow 4 \text{ elements } \{1, 2, 3, 4\}$$

have multiplicative inverse.

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\} \Rightarrow 2 \text{ elements } \{1, 5\}$$

It can be denoted as :

$$\mathbb{Z}_5^* = \{1, 2, 3, 4\} \quad |\mathbb{Z}_5^*| = 4$$

$$\mathbb{Z}_6^* = \{1, 5\} \quad |\mathbb{Z}_6^*| = 2$$

* Theorems :

① If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$

Similar { ② If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then

$a+c \equiv b+d \pmod{m}$ and

③ ... $a \cdot c \equiv b \cdot d \pmod{m}$

④ If $a \equiv b \pmod{m}$ then $a \cdot c \equiv b \cdot c \pmod{mc}$ for $c > 0$

Date _____
Page _____

* Euler's Totient (ϕ) = $\phi(p^\alpha)$

\downarrow
prime

$$\begin{aligned}\phi(p^\alpha) &= p^\alpha - p^{\alpha-1} \\ &= p^\alpha \left(1 - \frac{1}{p}\right) \\ &= p^{\alpha-1}(p-1)\end{aligned}$$

For composite numbers :-

From fundamental theorem of arithmetic (FTA)

$$\Rightarrow n = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdot P_3^{\alpha_3} \cdots P_r^{\alpha_r}$$

$$\phi(n) = \phi(P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdots P_r^{\alpha_r})$$

Theorem: $\phi(ab) = \phi(a) \cdot \phi(b)$, iff $(a, b) = 1$

$$\rightarrow \phi(n) = \phi(P_1^{\alpha_1}) \cdot \phi(P_2^{\alpha_2}) \cdots \phi(P_r^{\alpha_r})$$

e.g. Find the value of $\phi(5)$

$$\phi(5) = 5^1 - 5^0 = 4$$

i.e. \mathbb{Z}_5^* has 4 elements

$$|\mathbb{Z}_5^*| = 4$$

$$\phi(6) = \phi(2 \cdot 3) = \phi(2^1) \cdot \phi(3^1)$$

$$= (2^1 - 2^0) \cdot (3^1 - 3^0)$$

$$= 2$$

$$|\mathbb{Z}_6^*| = 2$$

So,

$$\phi(p) = p - 1$$

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

↓ → where p are prime factors

of product of $(1 - 1/p)$ of n

eg.

$$\phi(5) = 5 \times \left(1 - \frac{1}{5}\right) \quad \left[\text{because 5 is only prime value} \right]$$

$$= 4 \times \frac{4}{5} = 4 \times 0.8$$

$$\phi(6) = 6 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right)$$

$$= 6 \times \frac{1}{2} \times \frac{2}{3} = 2$$

* Linear Congruence: $\exists ax \equiv b \pmod{m} \Rightarrow m | ax - b$

① IF a^{-1} exists: (i.e. $(a, m) = 1$)

$$ax \equiv b \pmod{m}$$

$$(a^{-1}a)x \equiv a^{-1}b \pmod{m}$$

$$x \equiv a^{-1}b \pmod{m}$$

so we can substitute

$$a(a^{-1}b) \equiv b \pmod{m}$$

i.e.

$$\exists b \equiv b \pmod{m} \Rightarrow m | b - b \quad \checkmark$$



② If a and m are not coprime

i.e. $(a, m) = d > 1$ solution exists

iff $d \mid b$.

examples :

$$1. 3x \equiv 4 \pmod{5}$$

We know $(3, 5) = 1$

so

$$3 \cdot 2 \equiv \frac{1}{\cancel{5}} \pmod{5}$$

multiplicative inverse

On multiplying 2 on both sides

$$\text{We know } \left\{ \begin{array}{l} 2 \cdot 3x \equiv 2 \cdot 4 \pmod{5} \\ 6x \equiv 8 \pmod{5} \end{array} \right.$$

$$\left. \begin{array}{l} 6x \equiv 8 \pmod{5} \\ x \equiv 8 \pmod{5} \end{array} \right\} \leftarrow -6(5) \cdot x(5) \equiv 8(5)$$

$$x \equiv 8 \pmod{5}$$

$$x \equiv 3 \pmod{5}$$

so $x = 3$ is a solution

putting in equation

$$3 \cdot 3 \equiv 4 \pmod{5}$$

$$9 \equiv 4 \pmod{5}$$

$$5 \mid (9-4) \Rightarrow 5 \mid 5 \quad \checkmark$$

$$a x \equiv b \pmod{m}$$

$$2. \quad 6x \equiv 4 \pmod{10}$$

$(6, 10) = 2 > 1$ but $2 \nmid 4$
hence solution exists.

From previous theorem we can take
out the common factor i.e. 2
hence

$$3x \equiv 2 \pmod{5}$$

now

$$(3, 5) = 1$$

$$3 \cdot 2 \equiv 1 \pmod{5}$$

↑

a^{-1} .

$$2 \cdot 3x \equiv 2 \cdot 2 \pmod{5}$$

$$x \equiv 4 \pmod{5}$$

$$x = 4$$

so

$$6 \cdot 4 \equiv 4 \pmod{10} \Rightarrow 10 \mid 6 \cdot 4 - 4$$

$$10 \mid 20 \quad \checkmark$$

$$3. \quad 8x \equiv 5 \pmod{16} \quad \text{since } (8, 16) = 4 > 1$$

but $4 \nmid 5$

hence solution does not exist.

Proof:

$$\phi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

using fundamental theorem of arithmetic:

$$\phi(n) = \phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r})$$

$$= \phi\left(\prod_{i=1}^r p_i^{\alpha_i}\right)$$

$$= \prod_{i=1}^r \phi(p_i^{\alpha_i})$$

$$= \prod_{i=1}^r (p_i^{\alpha_i} - p_i^{\alpha_i-1})$$

$$= \prod_{i=1}^r p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right)$$

$$= \prod_{i=1}^r p_i^{\alpha_i} \cdot \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$$



$$(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r})$$

$$\boxed{\phi(n) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)}$$

QED

②

$$\boxed{\sum_{d|n} \phi(d) = n \quad (1 \leq d \leq n)}$$



e.g. $n = 8$ then
 $d = 1, 2, 4, 8$

$$\sum_{d|8} \phi(d) = 8 \Rightarrow \phi(1) + \phi(2) + \phi(4) + \phi(8) = 8$$

$\mathbb{Z}_1 = \{0\}$ and $\gcd(1, 0) = 1$ because
 $1|1$ and $1|0$.

$2|4$, $2|8$ hence, ~~1~~ 1 and 0 are relatively prime.

Also note: $\gcd(2, 0) = 2 = (-)^{1-0}$

$$(2)^{0-0} =$$

$$(2)((-2)^{1-0} - (-2)^{0-0}) =$$

Hence $\phi(1) = 1 - 2^{0-0} =$

for $\phi(2) = 2^1 - 2^0 = 1$

$\mathbb{Z}_2 = \{0, 1\}$ and $\mathbb{Z}_2^* = \{1\}$

$$\phi(4) = 2^2 - 2^1 = 2^1 - 2^0 + 1 - 2^{0-0} = 2^1 - 2^0 = 1$$

$$\phi(8) = 2^3 - 2^2 = 4.$$

hence

$$1 + 1 + 2 + 4 = 8$$

Verified.

$$\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

$$0+0=0, 1+1=2, 2+2=4, 3+3=6, 4+4=8$$

$$(0, 1, 2, 3, 4, 5, 6, 7) \rightarrow (0, 1, 2, 3, 4, 5, 6, 7)$$

$$0+1=1$$

$$1+2=3$$

$$2+3=5$$

* Fermat's little theorem:

$$\mathbb{Z}_p = \{0, 1, \dots, p-1\} \quad |\mathbb{Z}_p| = p \quad (\text{order}/\text{cardinality})$$

given $a \in \mathbb{Z}_p$, $(a, p) = 1$ and $a \neq 0$:
then

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

e.g. $\mathbb{Z}_5 = \{0, 1, \dots, 4\} \quad a = 3, \quad p = 5$

$$\begin{aligned} 3^{5-1}(5) &= 3^4(5) \\ &= 3^2 \cdot 3^2(5) \\ &= (3^2(5)) \cdot 3^2(5)(5) \\ &= (4 \cdot 4)(5) \\ &= 16(5) = 1 \end{aligned}$$

■ $3^{5-1} \equiv 1(5)$ verified.

Proof : $\mathbb{Z}_p = \{0, 1, \dots, p-1\} = a \in \mathbb{Z}_p, \quad (a, p) = 1$

so

$$a \cdot \mathbb{Z}_p = \{0 \cdot a, 1 \cdot a, \dots, (p-1) \cdot a\}$$

① uniqueness a_i, a_j s.t. $i \neq j$ and

$$a_i, a_j \in \mathbb{Z}_p$$

$$a \cdot a_i, a \cdot a_j \in a \cdot \mathbb{Z}_p$$

assume $a \cdot a_i = a \cdot a_j$

then $a \cdot a_i \equiv a \cdot a_j \pmod{p}$

e.g. $4 = 4$

$$4 \equiv 4 \pmod{p} \Rightarrow p \mid (4-4)$$

hence $P \mid (a \cdot a_i - a \cdot a_j)$

$$\therefore P \mid a(a_i - a_j)$$

from the previous rule:

$$\text{if } P \mid ab$$

then $P \mid a$ or $P \mid b$

then

$$P \mid a \text{ or } P \mid (a_i - a_j)$$

and since $(P, a) = 1 \Rightarrow P \nmid a$

so, and for

$$P \mid (a_i - a_j)$$

$a_i, a_j \in \mathbb{Z}_P$ and $a_i - a_j < P$

hence

$$P \nmid (a_i - a_j)$$

contradiction

Hence

$$a \cdot a_i \neq a \cdot a_j$$

②

$$|\mathbb{Z}_P = a \cdot \mathbb{Z}_P|$$

e.g. $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, let $a = 3$

$$3 \cdot \mathbb{Z}_5 = \{0, 3, 1, 4, 2\}$$

hence the set values are same, only different
in order.

Proof for Fermat's little theorem:

We can write

$$a \cdot \mathbb{Z}_p \equiv \mathbb{Z}_p \pmod{P}$$

on multiplying with every element

of $\mathbb{Z}_p = \{0, 1, \dots, P-1\}$ except 0.

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

$$(P-1)(P-2) \dots (a^{P-1} - 1)$$

so

$$P \nmid (P-1)! \text{ or } P \mid (a^{P-1} - 1)$$

but

$$P \nmid (P-1)! \quad \text{eg. } 5 \nmid 4!$$

hence

$$\boxed{P \nmid (a^{P-1} - 1)}$$

$$\checkmark \boxed{a^{P-1} \equiv 1 \pmod{P}}$$

Multiply a on both sides

$$a \cdot a^{P-1} \equiv a \pmod{P}$$

$$\boxed{a^P \equiv a \pmod{P}}$$

* If $P \mid a$ - eg. $5 \mid 5 \Rightarrow 5^5 \equiv 5 \pmod{5}$

$$5(5) = 0$$

$$5^5(5) = (5(5))^5 = 0^5 = 0.$$

So $|0=0|$ hence, due to this exception, $(a,p) = 1$ hence $p \nmid a$.

Corollary (Extension of proof) :

If $p \nmid a$ and $n \equiv m \pmod{p-1}$

then

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

e.g. $p = 5$ and $n \equiv m \pmod{4}$
 $5 \nmid 3$ and $5 \equiv 1 \pmod{4} \Rightarrow 5 \equiv 1(4)$
 $\Rightarrow 4 \mid (5-1) \checkmark$

so,

$$5 = (2) \text{ mod } 5$$

$$5^5 \equiv 3^1 \pmod{5} \Rightarrow 5 \mid (3^5 - 3^1)$$

$$(3^2 \cdot 3^2 \cdot 3) \pmod{5}$$

$$= (3^2 \pmod{5}) \cdot (3^2 \pmod{5}) \cdot 3 \pmod{5}$$

$$= (4 \cdot 4 \cdot 3) \pmod{5}$$

$$= 16 \pmod{5} \cdot 3 \pmod{5}$$

$$= 3 \pmod{5}$$

so,

$$3^5 \equiv 3^1 \pmod{5}$$

verified.

If $n \equiv m \pmod{p-1} \Rightarrow (p-1) \mid n-m$, $\exists x \in \mathbb{Z}$

$$\text{s.t. } n \equiv m + x(p-1)$$

$$\Rightarrow a^n \equiv a^{m+x(p-1)} \pmod{p}$$

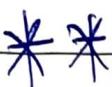
$$a^n \equiv a^m \cdot (a^{(p-1)x}) \pmod{p}$$

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

$$a^n \equiv a^m \cdot 1^x \pmod{p}$$

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

proved



Example:

$$2^{1000000}$$

$$\text{mod } 7 = ?$$

$$a^n \text{ mod } p \text{ for e.g. } a = 2, n = 1000000, p = 7.$$

$$n \equiv m(p-1)$$

$$1000000 \equiv - (7-1)$$

$$\downarrow \quad \downarrow \quad \downarrow$$

$$1000000 \equiv 4 \quad (6) \quad (m \quad p-1)$$

$$1000000(6) = 4$$

$$(2^6)^{1000000} \equiv (-1)^{1000000} = 1$$

$$1000000 \equiv 4(6) \Rightarrow 6 \mid 1000000 - 4 \quad \checkmark$$

$$\downarrow (2^3)(2^3)(2^3)$$

$$2^{1000000} \equiv 2^4(7) =$$

$$2^4(7) = 2$$

Ansatz: so

$$2^{1000000}$$

$$(7) = 2$$

$$2^{1000000} + 1 \equiv 2^{1000000} + 1$$

$$2^{1000000} + 1 \equiv 2^4(7) + 1$$

$$2^{1000000} + 1 \equiv 16 + 1$$

$$16 + 1 \equiv 0$$

13/1/22

Chinese Remainder Theorem : (requires minimum 2 equations)

if no. of congruence equations :

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_r \pmod{n_r} \end{cases}$$

↓
moduli's

if all these moduli's should be coprime

$$\gcd(n_1, n_2, \dots, n_r) = 1.$$

then solution exists.

i.e.

consistent \rightarrow if solution exists

and inconsistent \rightarrow if solution doesn't exist.

Let

$$N = n_1 \cdot n_2 \cdots n_r$$

$$\therefore N_1 = \frac{N}{n_1} = \frac{n_1 \cdot n_2 \cdots n_r}{n_1} = n_2 \cdot n_3 \cdots n_r$$

so,

$$\therefore (n_2 \cdot n_3 \cdots n_r, n_1) = 1$$

$$\text{i.e. } (N_1, n_1) = 1$$

then

$$N_1 m_1 = 1 (n_1)$$

$$\text{i.e. } m_1 = N_1^{-1}$$

$$N_{gr} = \frac{N}{n_{gr}}, \quad (N_{gr}, n_{gr}) = 1$$

so,

$$N_{gr} m_{gr} = 1 (n_{gr})$$

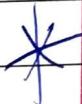
$$m_{gr} = N_{gr}^{-1}.$$

Therefore the solution can be calculated;

$$x = \left(\sum_{i=1}^{gr} a_i n_i m_i \right) \text{ mod } N$$

Multiple solutions can be found

$$x_0 = x + kN, \quad k \geq 0.$$



e.g. 1

$$x \equiv 2 \pmod{3}$$

$$a_1 = 2 \quad n_1 = 3$$

$$x \equiv 3 \pmod{5}$$

$$a_2 = 3 \quad n_2 = 5$$

$$x \equiv 2 \pmod{7}$$

$$a_3 = 2 \quad n_3 = 7$$

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

$$N_1 = \frac{N}{n_1} = 35, \quad (35, 3) = 1,$$

$$35 \cdot \underline{\circ} = 1(3)$$

↑ ↑ ↑

$N_1 \quad m_1 \quad n_1$

↳ found using extended euclidean algo.

$$N_2 = \frac{105}{5} = 21, \quad (21, 5) = 1 \Rightarrow N_2 = 21$$

$$\text{So, } 21 \cdot 1 \equiv 1(5) \quad \text{mod } 5$$

$$\downarrow \quad \downarrow \quad \downarrow$$

$$N_2 \quad m_2 \quad n_2 \quad \text{mod } 5 = 1$$

$$N_3 = \frac{105}{7} = 15, \quad (15, 7) = 1 \Rightarrow 15 \cdot 1 \equiv 1(7) \quad \text{mod } 7$$

$$\downarrow \quad \downarrow \quad \downarrow$$

$$N_3 \quad m_3 \quad n_3$$

$$x = \left(\sum_{i=1}^3 a_i N_i m_i \right) \text{ mod } N$$

$$= (2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1)(105)$$

$$= 233 \text{ mod } 105$$

$$x = 23$$

$$x_0 = 23 + k \cdot 105 \quad k \geq 0$$

We can check

$$23 \equiv 2(3) \Rightarrow 3 | 23 - 2 \quad \checkmark$$

$$23 \equiv 3(5) \Rightarrow 5 | 23 - 3 \quad \checkmark$$

$$23 \equiv 2(7) \Rightarrow 7 | 23 - 2 \quad \checkmark$$

Verified.



* eq. 2 $x \equiv 29(52)$
 $x \equiv 19(72)$

so

$$52 = a \cdot b \\ = 4 \cdot 13 \quad \text{and} \quad (4, 13) = 1.$$

$$\therefore x \equiv 29(52) \Rightarrow 52 | x - 29,$$

by transitive property $a|b, b|c \Rightarrow a|c$.

$$4 | 52, 52 | x - 29 \Rightarrow 4 | x - 29.$$

so,

$\boxed{x \equiv 29(4)}$ and similarly
 ~~$x \equiv 29(13)$~~

Similarly,

$$72 = a \cdot b = 8 \cdot 9 \quad \text{and} \quad (8, 9) = 1$$

so,

$\boxed{x \equiv 19(8)}$

$\boxed{x \equiv 19(9)}$

$$\Rightarrow 4 | 8, 8 | x - 19 \Rightarrow 4 | x - 19$$

$$\Rightarrow x \equiv 19(4)$$

unpossible
step II goes



\times	$x \equiv 3(4)$
	$x \equiv 1(4)$

both have
same moduli but
different remainder for
same value of x .

This is impossible in reality, i.e. not unique

When they are not unique, the system of equations are inconsistent.

Note: # inconsistency can be found using whether a moduli are coprime or not
i.e. $(52, 72) \neq 1$

but that is not true always, hence use above approach.

* Example : $x \equiv 3 \pmod{10}$
 $x \equiv 8 \pmod{15}$
 $x \equiv 5 \pmod{84}$
 L \rightarrow moduli

$$\Rightarrow (10, 15, 84) \neq 1$$

on calculating $N_1 = \frac{10 \cdot 15 \cdot 84}{10} = 1260$

$$\text{but } (1260, 10) \neq 1$$

so we cannot find m_1 (inverse).

but if example 2 approach is followed
we see system of equations are consistent.

So,

$$x \equiv 3 \pmod{10} \quad x \equiv 8 \pmod{15} \quad x \equiv 5 \pmod{84}$$

$$\Downarrow \quad \Downarrow \quad \Downarrow$$

$$x \equiv 3 \pmod{2} \quad x \equiv 8 \pmod{3} \quad x \equiv 5 \pmod{4}$$

$$x \equiv 3 \pmod{5} \quad x \equiv 8 \pmod{5} \quad x \equiv 5 \pmod{21}$$

$$x \equiv 1(2)$$

$$x \equiv 3(5)$$

$$x \equiv 2(3)$$

$$x \equiv 3(5)$$

$$x \equiv 5(4)$$

$$x \equiv 5(2) \text{ and } x \equiv 5(2)$$

and

$$x \equiv 5(21)$$

$$x \equiv 5(7) \text{ and } x \equiv 5(3)$$



$$x \equiv 1(2)$$

$$x \equiv 3(5)$$



$$x \equiv 2(3)$$

$$x \equiv 3(5)$$



$$x \equiv 1(2)$$

$$x \equiv 5(7)$$

$$x \equiv 2(3)$$

So;

$$x \equiv 1(2)$$

$$x \equiv 2(3)$$

$$x \equiv 3(5)$$

$$x \equiv 5(7)$$

$$N_1 = 105, (105, 2) = 1$$

$$105 \cdot \frac{1}{m_1} \equiv 1(2)$$

$$m_1$$

$$N_2 = 70, (70, 3) = 1$$

$$70 \cdot \frac{1}{m_2} \equiv 1(3)$$

$$m_2$$

$$N_3 = 42, (42, 5) = 1$$

$$42 \cdot \frac{3}{m_3} \equiv 1(5)$$

$$m_3$$

$$N_4 = 30, (30, 7) = 1$$

$$30 \cdot \frac{4}{m_4} \equiv 1(7)$$

$$m_4$$

$$n = (1 \cdot 105 \cdot 1 + 2 \cdot 70 \cdot 1 + 3 \cdot 42 \cdot 3 + 5 \cdot 30 \cdot 4) \mod 210$$

$$= 173$$

14/1/22 Taking the same example:

$$x \equiv 2 \pmod{3} \quad \text{--- (1)} \Rightarrow x \equiv 2 \pmod{3} \Rightarrow 3 \mid x - 2$$

$$x \equiv 3 \pmod{5} \quad \text{--- (2)} \quad (\text{F}) + \text{then } \exists k \in \mathbb{Z}$$

$$x \equiv 2 \pmod{7} \quad \text{--- (3)} \quad x = 2 + 3k \quad \text{--- (4)}$$

Substitute (4) in (2)

$$x \equiv 3 \pmod{5} \quad \text{--- (5)}$$

$$2 + 3k \equiv 3 \pmod{5} \Rightarrow 5 \mid 2 + 3k - 3$$

$$3k \equiv 1 \pmod{5} \quad \Leftarrow 5 \mid 3k - 1$$

and $(3, 5) = 1$

Note: If they were not prime, system of eqns. would be inconsistent.

$3 \cdot 2 \equiv 1 \pmod{5}$

so multiply inverse of 3 on both sides

$$2 \cdot 3k \equiv 2 \cdot 1 \pmod{5}$$

$$k \equiv 2 \pmod{5} \Rightarrow k = 2 + 5u, u \in \mathbb{Z}$$

L(5)

Substitute (5) in (4):

$$x = 2 + 3k$$

$$x = 2 + 3(2 + 5u)$$

$$x = 8 + 15u \quad \text{--- (6)}$$



+ substitute + ⑥ in ③

$$x \equiv 2(7)$$

$$8 + 15u \equiv 2(7)$$

$$\Rightarrow 7 \mid 8 + 15u - 2$$

$$7 \mid 6 + 15u$$

$$15u \equiv -6(7)$$

$$5u \equiv -1(7)$$

$$u = 1 + 7w, w \in \mathbb{Z}$$

Substitute ⑦ in ③

$$x = 8 + 15u$$

$$x = 8 + 15(1 + 7w)$$

$$x = 23 + 105w, w \in \mathbb{Z}$$

$$x \equiv 23(105) \rightarrow \underline{\text{solution}}$$

* PRIMALITY TEST : To check whether n is prime or not.

Euler's theorem (ϕ) : If $(n, a) = 1$ then $a^{\phi(n)} \equiv 1 \pmod{n}$
 Ls composite numbers.

Fermat's little theorem:

$(a, p) = 1$ i.e. $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$

If $n = p$, then $a^{p-1} \equiv 1 \pmod{p}$

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

So Euler theorem is for composite numbers

and Fermat's theorem in prime n .

eg. $n = 15$, $a = 2$

$$\begin{aligned}\phi(15) &= \phi(3 \cdot 5) = \phi(3) \cdot \phi(5) \\ &= 2 \cdot 4 = 8.\end{aligned}$$

and $(15, 2) = 1$

so

$$2^8 \equiv 1 \pmod{15}$$

↓

$$2^8 \pmod{15} = (2^4 \pmod{15} \cdot 2^4 \pmod{15}) \pmod{15}$$

$$= 1 \cdot 1 \pmod{15}$$

$$= 1 \pmod{15}$$

verified.

Continuing Primality test

- ① deterministic : $\Rightarrow n$ is prime with 100% confidence
 primality test $\Rightarrow n$ is not prime " "
- ② probabilistic : $\Rightarrow n$ is prime, without 100% confidence
 primality test $\Rightarrow n$ is not prime, with "

*

Fermat's little thm is a probabilistic algo

where

n is chosen at random which
 is of random length

$$n = \underline{\quad \quad \quad \quad \quad}$$



if last digit is odd

it is chosen as input to the primality
 algorithm i.e. odd number is "likely"
 to be prime.

18/1/22

So, if $a \neq 1$ and $a^{n-1} \equiv 1 \pmod{n}$
 then n is prime

but Fermat's thm is probabilistic!

Proving
 91 is
 probably
 prime
 with
 base 3

eg. $n = 91$, $a = 3$
 we see
 $n \nmid a$ and $(n, a) = 1$.

and
 $3^{90} \equiv 1 \pmod{91}$ ✓
 probable

hence 91 is prime. But it is not prime.

$91 = 13 \times 7$, hence composite.

e.g. $n = 91$, $a = 2$

we see $a^{n-1} \equiv 1 \pmod{n}$

$$(n, a) = 1 \text{ but}$$

$$2^{90} \equiv 64(91), \text{ hence } 91 \text{ is composite.}$$

Hence for different bases $n = 91$ is prime/composite.

* Prime / not prime: ① $f_n = 5^{\frac{n-1}{2}} - 1 \in O(n)$

base tests: $\sqrt[2]{1} = 1, \sqrt[3]{1} = 1, \dots, \sqrt[n]{1} = 1$

$$\underbrace{1 \ 2 \ 0 \ 0 \ 0}_{\text{check divisible or not}}, \underbrace{5}_{\text{check divisible or not}} = 2(1 \text{ and } 5)$$

check divisible or not

$$\textcircled{2} \quad n = 5$$

$$\begin{array}{c} \text{division} \\ \text{method} \\ \hline \textcircled{1} \quad n = 5 \\ \textcircled{0}(n) \quad 1 \quad | \quad 2 \dots 4 \quad \boxed{5} \\ \text{check } (n, a) \end{array}$$

$$\textcircled{3} \quad n = 5 \quad \text{trial}$$

$$\begin{array}{c} \text{division} \\ \text{method} \\ \hline \textcircled{2} \quad n = 5 \\ \textcircled{0}(n) \quad 1 \quad | \quad 2 \dots 4 \quad \boxed{5} \\ \text{check } (n, a) \end{array}$$

** Charmichael numbers: A number is a composite integer such that $a^{n-1} \equiv 1 \pmod{n}$ holds for every $a \in \mathbb{Z}_n^*$.

$$\text{note: } \mathbb{Z}_n^* = \{0, 1, \dots, n-1\}$$

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : (a, n) = 1\}$$

The smallest number that satisfies this is 561.

* Shortcut properties:

1. IF n is divisible by a perfect square \Rightarrow
then n is not a charmichael number.
2. IF n is square free i.e. it is not
a perfect square then n is a
charmichael number iff
 $p-1 \mid n-1$ For every prime $p \mid n$
i.e.

$$561 = 3 \cdot 11 \cdot 17$$

$$3-1 \mid 561-1, 11-1 \mid 561-1, 17-1 \mid 561-1.$$

verified.

* MILLER-RABIN PRIMALITY TEST :

- take only odd numbers
1. choose n (that needs to be tested)
 2. $n-1 = 2^k \cdot m$ \rightarrow odd
 3. choose a , s.t. $(a, n) = 1, 1 < a < n-1$.

$$b_0 = a^m \pmod{n} \xrightarrow{\pm 1} \text{Probable prime}$$

$$b_1 = b_0^2 \pmod{n} \xrightarrow{-1} \text{Probable prime}$$

\vdots and (all) $\equiv 1 \pmod{n}$ \rightarrow composite

$$b_{k-1} = b_{k-2}^2 \pmod{n} \xrightarrow{-1} \text{Probable prime}$$

\vdots and (all) $\not\equiv 1 \pmod{n}$ \rightarrow composite.

$$b_i = b_{i-1}^2 \pmod{n} \quad 1 \leq i \leq k-1$$



eg. ①

$$n = 23$$

$$n-1 = 22 = 2^1 \times 11 \quad \text{i.e. } k=1, m=11$$

choose $a=2$, $\therefore (2, 23) = 1$

$$b_0 = 2^1 \pmod{23} \quad \cancel{= 1}$$

$$= (2^5(23) \cdot 2^5(23) \cdot 2(23))(23)$$

$$= (9 \cdot 9 \cdot 2)(23) = 162(23) = 1(23)$$

$$= 1$$

Hence 23 is probably prime.

Since $k=1$ stop at b_0 .

eg. ② : $n = 55$

$$n-1 = 54 = 2^1 \cdot 17, \quad k=1, m=27$$

$$a=2, \quad (2, 55) = 1.$$

$$b_0 = 2^{27} \pmod{55}$$

$$= (2^6)^4 \cdot 2^3 \pmod{55}$$

$$\cancel{= (2^4 \cdot 2^3 \cdot 2^3) \pmod{55}}$$

$$= ((2^6(55))^4 \cdot 2^3) \pmod{55}$$

$$= (9^4 \cdot 2^3) \pmod{55}$$

$$= 18 \pmod{55} \neq \pm 1$$

Hence it is composite number.

H.W.eg. ③ $n = 53$

$$n-1 = 52 = 2^2 \cdot 13, \quad k=2, m=13$$

$$a=2, \quad (2, 53) = 1$$

$$b_0 = 2^{13} \pmod{53}$$

$$\cancel{= (2^6(53))^2(2^6(53)) \pmod{53}}$$

$$= (11 \cdot 11 \cdot 2) \pmod{53}$$

$$= (242) \pmod{53} = 30 \pmod{53}.$$

$$b_1 = (30)^2 \pmod{53}$$

$$= 900 \pmod{53}$$

$$= 52 \pmod{53} = -1 \cdot (53)$$

$b_1 = -1$, hence probably prime

$$\text{Let } n = 21 \Rightarrow x^2 \equiv 52 \pmod{n}$$

$$x = \sqrt{52} \pmod{n}, \quad x = 2 \pmod{n}$$

$$\text{So } (\sqrt{52})^2 \equiv 52$$

$$(x+1)^2 \equiv (x-1)^2 + 4x \equiv 52 \pmod{n}$$

$$(x+1) = (x-1) \pm 4 \Rightarrow (x+1)(x-1) =$$

$$\text{writing } 52 = 25 + 27 \Rightarrow 25 \pmod{n}$$

$$\text{and } 25 = 1 \pmod{n} \quad \text{then } 27 \pmod{n}$$

$$\text{So } 27 \pmod{n} \quad \text{Q.E.D.} \quad \text{(B) P9}$$

$$\text{Example } 2 \pmod{n} \quad \text{Frob.} \quad \text{P9}$$

$$n = 21 \Rightarrow x^2 \equiv 1 \pmod{n}$$

$$(\sqrt{1})^2 \pmod{n} = 1$$

$$\text{P.T.O. } \text{E7}(2) =$$

$$\text{Comparing LHS & RHS}$$

$$(1)(\sqrt{1})^2 \pmod{n} =$$

$$(1)^2 \pmod{n} =$$

$$1 \pmod{n} \quad \text{Q.E.D.} \quad \text{P9}$$

$$27 \pmod{n} \quad \text{Q.E.D.} \quad \text{P9}$$

$$x = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21$$

$$x^2 = 0, 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, 256, 289, 324, 361, 400, 441, 484, 529, 576, 625, 676, 729, 784, 841, 900, 961, 1024, 1089, 1156, 1225, 1296, 1369, 1444, 1521, 1600, 1681, 1764, 1849, 1936, 2025, 2116, 2209, 2304, 2401, 2500, 2609, 2704, 2809, 2904, 3001, 3100, 3209, 3304, 3409, 3500, 3609, 3704, 3809, 3900, 4009, 4104, 4209, 4300, 4409, 4504, 4609, 4700, 4809, 4904, 5009, 5100, 5209, 5304, 5409, 5500, 5609, 5704, 5809, 5900, 6009, 6104, 6209, 6300, 6409, 6504, 6609, 6700, 6809, 6904, 7009, 7100, 7209, 7304, 7409, 7500, 7609, 7704, 7809, 7900, 8009, 8104, 8209, 8300, 8409, 8504, 8609, 8700, 8809, 8904, 9009, 9100, 9209, 9304, 9409, 9500, 9609, 9704, 9809, 9900, 10009, 10104, 10209, 10300, 10409, 10504, 10609, 10700, 10809, 10904, 11009, 11100, 11209, 11304, 11409, 11500, 11609, 11704, 11809, 11900, 12009, 12104, 12209, 12300, 12409, 12504, 12609, 12700, 12809, 12904, 13009, 13100, 13209, 13304, 13409, 13500, 13609, 13704, 13809, 13900, 14009, 14104, 14209, 14300, 14409, 14504, 14609, 14700, 14809, 14904, 15009, 15100, 15209, 15304, 15409, 15500, 15609, 15704, 15809, 15900, 16009, 16104, 16209, 16300, 16409, 16504, 16609, 16700, 16809, 16904, 17009, 17100, 17209, 17304, 17409, 17500, 17609, 17704, 17809, 17900, 18009, 18104, 18209, 18300, 18409, 18504, 18609, 18700, 18809, 18904, 19009, 19100, 19209, 19304, 19409, 19500, 19609, 19704, 19809, 19900, 20009, 20104, 20209, 20300, 20409, 20504, 20609, 20700, 20809, 20904, 21009, 21100, 21209, 21304, 21409, 21500, 21609, 21704, 21809, 21900, 22009, 22104, 22209, 22300, 22409, 22504, 22609, 22700, 22809, 22904, 23009, 23100, 23209, 23304, 23409, 23500, 23609, 23704, 23809, 23900, 24009, 24104, 24209, 24300, 24409, 24504, 24609, 24700, 24809, 24904, 25009, 25100, 25209, 25304, 25409, 25500, 25609, 25704, 25809, 25900, 26009, 26104, 26209, 26300, 26409, 26504, 26609, 26700, 26809, 26904, 27009, 27100, 27209, 27304, 27409, 27500, 27609, 27704, 27809, 27900, 28009, 28104, 28209, 28300, 28409, 28504, 28609, 28700, 28809, 28904, 29009, 29100, 29209, 29304, 29409, 29500, 29609, 29704, 29809, 29900, 30009, 30104, 30209, 30300, 30409, 30504, 30609, 30700, 30809, 30904, 31009, 31100, 31209, 31304, 31409, 31500, 31609, 31704, 31809, 31900, 32009, 32104, 32209, 32300, 32409, 32504, 32609, 32700, 32809, 32904, 33009, 33100, 33209, 33304, 33409, 33500, 33609, 33704, 33809, 33900, 34009, 34104, 34209, 34300, 34409, 34504, 34609, 34700, 34809, 34904, 35009, 35100, 35209, 35304, 35409, 35500, 35609, 35704, 35809, 35900, 36009, 36104, 36209, 36300, 36409, 36504, 36609, 36700, 36809, 36904, 37009, 37100, 37209, 37304, 37409, 37500, 37609, 37704, 37809, 37900, 38009, 38104, 38209, 38300, 38409, 38504, 38609, 38700, 38809, 38904, 39009, 39100, 39209, 39304, 39409, 39500, 39609, 39704, 39809, 39900, 40009, 40104, 40209, 40300, 40409, 40504, 40609, 40700, 40809, 40904, 41009, 41100, 41209, 41304, 41409, 41500, 41609, 41704, 41809, 41900, 42009, 42104, 42209, 42300, 42409, 42504, 42609, 42700, 42809, 42904, 43009, 43100, 43209, 43304, 43409, 43500, 43609, 43704, 43809, 43900, 44009, 44104, 44209, 44300, 44409, 44504, 44609, 44700, 44809, 44904, 45009, 45100, 45209, 45304, 45409, 45500, 45609, 45704, 45809, 45900, 46009, 46104, 46209, 46300, 46409, 46504, 46609, 46700, 46809, 46904, 47009, 47100, 47209, 47304, 47409, 47500, 47609, 47704, 47809, 47900, 48009, 48104, 48209, 48300, 48409, 48504, 48609, 48700, 48809, 48904, 49009, 49100, 49209, 49304, 49409, 49500, 49609, 49704, 49809, 49900, 50009, 50104, 50209, 50300, 50409, 50504, 50609, 50700, 50809, 50904, 51009, 51100, 51209, 51304, 51409, 51500, 51609, 51704, 51809, 51900, 52009, 52104, 52209, 52300, 52409, 52504, 52609, 52700, 52809, 52904, 53009, 53100, 53209, 53304, 53409, 53500, 53609, 53704, 53809, 53900, 54009, 54104, 54209, 54300, 54409, 54504, 54609, 54700, 54809, 54904, 55009, 55100, 55209, 55304, 55409, 55500, 55609, 55704, 55809, 55900, 56009, 56104, 56209, 56300, 56409, 56504, 56609, 56700, 56809, 56904, 57009, 57100, 57209, 57304, 57409, 57500, 57609, 57704, 57809, 57900, 58009, 58104, 58209, 58300, 58409, 58504, 58609, 58700, 58809, 58904, 59009, 59100, 59209, 59304, 59409, 59500, 59609, 59704, 59809, 59900, 60009, 60104, 60209, 60300, 60409, 60504, 60609, 60700, 60809, 60904, 61009, 61100, 61209, 61304, 61409, 61500, 61609, 61704, 61809, 61900, 62009, 62104, 62209, 62300, 62409, 62504, 62609, 62700, 62809, 62904, 63009, 63100, 63209, 63304, 63409, 63500, 63609, 63704, 63809, 63900, 64009, 64104, 64209, 64300, 64409, 64504, 64609, 64700, 64809, 64904, 65009, 65100, 65209, 65304, 65409, 65500, 65609, 65704, 65809, 65900, 66009, 66104, 66209, 66300, 66409, 66504, 66609, 66700, 66809, 66904, 67009, 67100, 67209, 67304, 67409, 67500, 67609, 67704, 67809, 67900, 68009, 68104, 68209, 68300, 68409, 68504, 68609, 68700, 68809, 68904, 69009, 69100, 69209, 69304, 69409, 69500, 69609, 69704, 69809, 69900, 70009, 70104, 70209, 70300, 70409, 70504, 70609, 70700, 70809, 70904, 71009, 71100, 71209, 71304, 71409, 71500, 71609, 71704, 71809, 71900, 72009, 72104, 72209, 72300, 72409, 72504, 72609, 72700, 72809, 72904, 73009, 73100, 73209, 73304, 73409, 73500, 73609, 73704, 73809, 73900, 74009, 74104, 74209, 74300, 74409, 74504, 74609, 74700, 74809, 74904, 75009, 75100, 75209, 75304, 75409, 75500, 75609, 75704, 75809, 75900, 76009, 76104, 76209, 76300, 76409, 76504, 76609, 76700, 76809, 76904, 77009, 77100, 77209, 77304, 77409, 77500, 77609, 77704, 77809, 77900, 78009, 78104, 78209, 78300, 78409, 78504, 78609, 78700, 78809, 78904, 79009, 79100, 79209, 79304, 79409, 79500, 79609, 79704, 79809, 79900, 80009, 80104, 80209, 80300, 80409, 80504, 80609, 80700, 80809, 80904, 81009, 81100, 81209, 81304, 81409, 81500, 81609, 81704, 81809, 81900, 82009, 82104, 82209, 82300, 82409, 82504, 82609, 82700, 82809, 82904, 83009, 83100, 83209, 83304, 83409, 83500, 83609, 83704, 83809, 83900, 84009, 84104, 84209, 84300, 84409, 84504, 84609, 84700, 84809, 84904, 85009, 85100, 85209, 85304, 85409, 85500, 85609, 85704, 85809, 85900, 86009, 86104, 86209, 86300, 86409, 86504, 86609, 86700, 86809, 86904, 87009, 87100, 87209, 87304, 87409, 87500, 87609, 87704, 87809, 87900, 88009, 88104, 88209, 88300, 88409, 88504, 88609, 88700, 88809, 88904, 89009, 89100, 89209, 89304, 89409, 89500, 89609, 89704, 89809, 89900, 90009, 90104, 90209, 90300, 90409, 90504, 90609, 90700, 90809, 90904, 91009, 91100, 91209, 91304, 91409, 91500, 91609, 91704, 91809, 91900, 92009, 92104, 92209, 92300, 92409, 92504, 92609, 92700, 92809, 92904, 93009, 93100, 93209, 93304, 93409, 93500, 93609, 93704, 93809, 93900, 94009, 94104, 94209, 94300, 94409, 94504, 94609, 94700, 94809, 94904, 95009, 95100, 95209, 95304, 95409, 95500, 95609, 95704, 95809, 95900, 96009, 96104, 96209, 96300, 96409, 96504, 96609, 96700, 96809, 96904, 97009, 97100, 97209, 97304, 97409, 97500, 97609, 97704, 97809, 97900, 98009, 98104, 98209, 98300, 98409, 98504, 98609, 98700, 98809, 98904, 99009, 99100, 99209, 99304, 99409, 99500, 99609, 99704, 99809, 99900, 100009, 100104, 100209, 100300, 100409, 100504, 100609, 100700, 100809, 100904, 101009, 101100, 101209, 101304, 101409, 101500, 101609, 101704, 101809, 101900, 102009, 102104, 102209, 102300, 102409, 102504, 102609, 102700, 102809, 102904, 103009, 103100, 103209, 103304, 103409, 103500, 103609, 103704, 103809, 103900, 104009, 104104, 104209, 104300, 104409, 104504, 104609, 104700, 104809, 104904, 105009, 105100, 105209, 105304, 105409, 105500, 105609, 105704, 105809, 105900, 106009, 106104, 106209, 106300, 106409, 106504, 106609, 106700, 106809, 106904, 107009, 107100, 107209, 107304, 107409, 107500, 107609, 107704, 107809, 107900, 108009, 108104, 108209, 108300, 108409, 108504, 108609, 108700, 108809, 108904, 109009, 109100, 109209, 109304, 109409, 109500, 109609, 109704, 109809, 109900, 110009, 110104, 110209, 110300, 110409, 110504, 110609, 110700, 110809, 110904, 111009, 111100, 111209, 111304, 111409, 111500, 111609, 111704, 111809, 111900, 112009, 112104, 112209, 112300, 112409, 112504, 112609, 112700, 112809, 112904, 113009, 113100, 113209, 113304, 113409, 113500, 113609, 113704, 113809, 113900, 114009, 114104, 114209, 114300, 114409, 114504, 114609, 114700, 114809, 114904, 115009, 115100, 115209, 115304, 115409, 115500, 115609, 115704, 115809, 115900, 116009, 116104, 116209, 116300, 116409, 116504, 116609, 116700, 116809, 116904, 117009, 117100, 117209, 117304, 117409, 117500, 117609, 117704, 117809, 117900, 118009, 118104, 118209, 118300, 118409, 118504, 118609, 118700, 118809, 118904, 119009, 119100, 119209, 119304, 119409, 119500, 119609, 119704, 119809, 119900, 120009, 120104, 120209, 120300, 120409, 120504, 120609, 120700, 120809, 120904, 121009, 121100, 121209, 121304, 121409, 121500, 121609, 121704, 121809, 121900, 122009, 122104, 122209, 122300, 122409, 122504, 122609, 122700, 122809, 122904, 123009, 123100, 123209, 123304, 123409, 123500, 123609, 123704, 123809, 123900, 124009, 124104, 124209, 124300, 124409, 124504, 124609, 124700, 124809, 124904, 125009, 125100, 125209, 125304, 125409, 125500, 125609, 125704, 125809, 125900, 126009, 126104, 126209, 126300, 126409, 126504, 126609, 126700, 126809, 126904, 127009, 127100, 127209, 127304, 127409, 127500, 127609, 127704, 127809, 127900, 128009, 128104, 128209, 128300, 128409, 128504, 128609, 128700, 128809, 128904, 129009, 129100, 129209, 129304, 129409, 129500, 129609, 129704, 129809, 129900, 130009, 130104, 130209, 130300, 130409, 130504, 130609, 130700, 130809, 130904, 131009, 131100, 131209, 131304, 131409, 131500, 131609, 131704, 131809, 131900, 132009, 132104, 132209, 132300, 132409, 132504, 132609, 132700, 132809, 132904, 133009, 133100, 133209, 133304, 133409, 133500, 133609, 133704, 133809, 133900, 134009, 134104, 134209, 134300, 134409, 134504, 134609, 134700, 134809, 134904, 135009, 135100, 135209, 135304, 135409, 135500, 135609, 135704, 135809, 135900, 136009, 136104, 136209, 136300, 136409, 136504, 136609, 136700, 136809, 136904, 137009, 137100, 137209, 137304, 137409, 137500, 137609, 137704, 137809, 137900, 138009, 138104, 138209, 138300, 138409, 138504, 138609, 138700, 138809, 138904, 139009, 139100, 139209, 139304, 139409, 139500, 139609, 139704, 139809, 139900, 140009, 140104, 140209, 140300, 140409, 140504, 140609, 140700, 140809, 140904, 141009, 141100, 141209, 141304, 141409, 141500, 141609, 141704, 141809, 141900, 142009, 142104, 142209, 142300, 142409, 142504, 142609, 142700, 142809, 142904, 14300$$

WILSON'S METHOD

$$\boxed{(P-1)! \equiv -1 \pmod{P}} \Rightarrow (P) | (P-1)! + (-1)$$

All primes satisfies this method.

$$P = 2, 3, 5, 7, \dots$$

$$(2-1)! \equiv -1 \pmod{2} \Rightarrow 2 | 2 \quad \checkmark$$

$$(3-1)! \equiv -1 \pmod{3} \Rightarrow 3 | 3 \quad \checkmark$$

$$(5-1)! \equiv -1 \pmod{5} \Rightarrow 5 | 25 \quad \checkmark$$

Drawback:

1. Factorial operation is very tedious.

$O(n)$ complexity.

19/01/22

*

$$\boxed{k^2 \equiv 1 \pmod{P} \text{ iFF } k=1 \text{ or } k=P-1}$$

i.e.

$$k \cdot k \equiv 1 \pmod{P}$$



i.e. k 's inverse is k .

$$\text{eg. } \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$$

$$1 \cdot 1 \equiv 1 \pmod{5} \Rightarrow 5 | 1-1 \quad \checkmark$$

$$4 \cdot 4 \equiv 1 \pmod{5} \Rightarrow 5 | 16-1 \quad \checkmark$$

rest of the numbers will have

inverse from within the set.



* Proof of Wilson's Theorem

$$\text{LHS} \leftarrow (P-1)! \bmod P = (1 \cdot 2 \cdot 3 \cdots (P-2) \cdot (P-1)) \bmod P$$

$$= (1 \cdot (-1) \cdot (-1) \cdots (-1) \cdot (P-1)) \bmod P$$

$$= (1 \cdot 1 \cdot 1 \cdots 1 \cdot (P-1)) \bmod P$$

$$= (P-1) \bmod P$$

$$= P \bmod P + (-1 \bmod P)$$

$$= -1 \bmod P \rightarrow \text{RHS}$$

Hence proved.

Eg. 0

$$P=11 \Rightarrow (P-1)! \equiv -1 \pmod{P}$$

$$(11-1)! \equiv -1 \pmod{11}$$

$$10! = (1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10) \pmod{11}$$

$$= (1 \cdot (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \cdot 10) \pmod{11}$$

$$= (1 \cdot 12 \cdot 12 \cdot 12 \cdot 12) \pmod{11}$$

$$= 10 \pmod{11} = -1 \pmod{11}$$

$$10! \in \{1, 2, 4, 5, 7, 9\}$$

$$10! \not\in \{1, 2, 4, 5, 7, 9\}$$

Verified

Eg. 1 $x = 130! \pmod{131}$



$$\Rightarrow x = (87)^{-1} \cdot 1301 \pmod{131}$$

$$P = 131$$

$$(87)(131 - 1) \equiv -1 \pmod{131}$$

so

$$x = (87)^{-1}(-1) \pmod{131}$$

$$= -(87)^{-1} \pmod{131}$$

$$\text{we know } 87(-3) \pmod{131} = 1$$

so,

$$x = -(-3) \pmod{131}$$

$$x = 3(131) \pmod{131} = 3$$

$$\text{eg 2: } x = (146)^{-1}(149)$$

$$\Rightarrow (147 \cdot 148)x = (148)(149)$$

$$(-2 \cdot -17)x = -1(149)$$

$$2x = -1(149)$$

$$-2x \equiv 1(149)$$

and

$$-2 \cdot 74 \equiv 1(149) \quad \text{so } 74 \text{ is inverse of } -2.$$

so

$$\boxed{1 \boxed{74} \boxed{149}}$$

$$-2 \cdot 74x \equiv 1(149)$$

$$\cancel{-2} \cancel{74} \equiv 1(149) \quad \checkmark$$

∴

$$\boxed{1 \boxed{74} \boxed{149}}$$

F

$$\cancel{F} \cancel{F} \cancel{P}$$



Eg. 3 Fermat's theorem: $a^{p-1} \equiv 1 \pmod{p}$

$$a = 47, p = 113$$

calculate $x = 47^{222} \pmod{113}$.

$$x = 47^{110} \cdot 47^{112} \pmod{113}$$

$\underbrace{\quad}_{1(113)}$

$$x = 47^{110} \pmod{113}$$

$$47^2 x = 47^{112} \pmod{113}$$

$$2209 x = 1 \pmod{113}$$

$$2209 \pmod{113} x = 1 \pmod{113}$$

$$62 x \equiv 1 \pmod{113}$$

so $62^{-1} \pmod{113}$ is multiplicative inverse of 62.

Hence

$$\begin{array}{r} 113 \\ \overline{)62 \quad 0} \\ \quad 0 \end{array}$$

$$\begin{array}{r} 62 \\ \overline{)113 \quad 1} \\ \quad 62 \end{array}$$

$$\begin{array}{r} 51 \\ \overline{)62 \quad 1} \end{array}$$

$$\begin{array}{r} 51 \\ \overline{)11 \quad 4} \end{array}$$

$$\begin{array}{r} 44 \\ \overline{)3 \quad 11 \quad 1} \\ \quad 3 \end{array}$$

$$\begin{array}{r} 4 \\ \overline{)4 \quad 7 \quad 1} \\ \quad 4 \end{array}$$

$$\begin{array}{r}
 113 = 62 \cdot 1 + 51 \\
 62 = 51 \cdot 1 + 11 \\
 51 = 11 \cdot 4 + 7 \\
 11 = 7 \cdot 1 + 4 \\
 7 = 4 \cdot 1 + 3 \\
 4 = 3 \cdot 1 + 1 \\
 3 = 1 \cdot 3 + 0
 \end{array}$$

$\therefore 113 = 62 \cdot 1 + 51$

$$113 = 62 \cdot 1 + 51$$

$$\begin{aligned}
 1 &= 4 - 3 \cdot 1 \\
 1 &= 4 - 1 - (7 - (4 \cdot 1)) \Rightarrow 1 = 4 \cdot 2 + 7(-1) \\
 1 &= (11 - 7) \cdot 2 + 7(-1) \Rightarrow 1 = 11 \cdot 2 + 7 \cdot (-3) \\
 1 &= 11 \cdot 2 + (51 - 11 \cdot 4)(-3) \\
 \Rightarrow 1 &= 11 \cdot 14 + 51 \cdot (-3) \\
 1 &= (62 - 51) \cdot 14 + 51 \cdot (-3) \\
 \Rightarrow 1 &= 62 \cdot 14 + 51 \cdot (-17) \\
 1 &= 62 \cdot 14 + (113 - 62) \cdot (-17) \\
 1 &= 62 \cdot (31) + 113 \cdot (-17)
 \end{aligned}$$

\downarrow If $31 \cdot 62 \equiv 1 \pmod{113}$

31 is inverse of 62 .

Hence $31 \cdot 62 \equiv 1 \pmod{113}$

$$31 \cdot 62x \equiv 31 \pmod{113}$$

$$31 \cdot 62x \equiv 31 \pmod{113}$$

$$62x \equiv 1 \pmod{113}$$

$$x \equiv 31^{-1} \pmod{113}$$



too much difference!

* Eg. 4: $x \equiv 70! \pmod{5183} \quad \text{--- (1)}$

$$5183 = 71 \times 73 \text{ and } 5183 \mid x - 70!$$

So we can write

$$x \equiv 70! \pmod{71} = -1 \pmod{71} \quad \text{L (2)}$$

$$x \equiv 70! \pmod{73} \quad \text{L (3)}$$

using Wilson's theorem

$$(71-1)(72-1) \dots (73-1) \equiv (-1)^{71-1} \pmod{71}$$

$$71 \cdot 72 \dots \equiv (-1) \pmod{71}$$

$$(-2 \cdot -1) \dots \equiv (-1) \pmod{73} \quad \text{L (4)}$$

$$-2 \cdot -1 \dots \equiv +1 \pmod{73} \quad \text{L (5)}$$

We know

$$((+2 \cdot 3 \dots) \pmod{73}) \equiv 1 \pmod{73} \quad \text{L (6)}$$

$$(+2 \cdot 3 \dots + (-1)) \pmod{73} \equiv 1 \pmod{73}$$

$$-37 \cdot 2 \equiv 37 \pmod{73}$$

$$x \equiv -37 \pmod{73}.$$

$$x \equiv 36 \pmod{73} \quad \text{--- (3)}$$

i.e.

$$\boxed{x \equiv 70! \pmod{5183}}$$

$$x \equiv -1 \pmod{71}$$

$$x \equiv 36 \pmod{73}$$

$$\boxed{n_1 \neq 5183}$$

$$n_2 = 71$$

$$n_2 = 73$$

$$\boxed{a_1 \neq 70!}$$

$$a_2 = -1$$

$$a_2 = 36$$

Using CRT

DNT

$\begin{array}{l} N_1 \\ \uparrow \\ 73 m_1 = 1 \pmod{71} \\ 2 m_1 = 1 \pmod{71} \\ 2 \cdot 36 \equiv 1 \pmod{71} \\ m_1 = 36 \pmod{71} \end{array}$	$\begin{array}{l} n_1 \\ \uparrow \\ 71 m_2 = 1 \pmod{73} \\ -2 m_2 = 1 \pmod{73} \\ -2 \cdot 36 \not\equiv 1 \pmod{73} \\ m_2 = 36 \pmod{73} \end{array}$
--	--

$$\begin{aligned} x &= (-1 \cdot 73 \cdot 36 + 36 \cdot 71 \cdot 36) \pmod{5183} \\ &= 36(-71 \cdot 36 - 73) \pmod{5183} \\ &= 1277 \pmod{5183}. \end{aligned}$$

* PRIMITIVE ROOTS

\exists (Order of element) : $a \in \mathbb{Z}_m^*, \mathbb{Z}_m^* = \{0, 1, \dots, m-1\}$

$$a^h \equiv e \pmod{m}$$

\downarrow \downarrow

least positive

integer $\neq 0$ satisfying multiplicative identity (1)

in such conditions

$$\boxed{\text{order}_m(a) = h}$$

if

$$a^k \equiv 1 \pmod{m} \quad \text{where } k > h$$

then $h | k$



Eg. $m = 5$, $a \in \mathbb{Z}_5$, $(a, 5) = 1$

$$\mathbb{Z}_5 = \{1, 2, 3, 4\}$$

$$1^1 = 1 \Rightarrow$$

$$\text{order}_5(1) = 1$$

$$2^1 = 2(5)$$

$$2^2 = 4(5)$$

$$2^3 = 3(5)$$

$$2^4 = 16(5) = 1$$

$$\text{order}_5(2) = 4$$

$$3^1 = 3$$

$$3^2 = 9(5) = 4$$

$$3^3 = 3^2 \cdot 3(5) = 4 \cdot 3(5) = 2$$

$$3^4 = 3^3 \cdot 3(5) = 2 \cdot 3(5) = 1$$

$$\text{order}_5(3) = 4$$

$$4^1 = 4$$

$$4^2 = 16(5) = 1$$

$$\text{order}_5(4) = 2.$$

* According to Euler's theorem:

$$a^{\phi(m)} = 1 \pmod{m}, \quad (a, m) = 1$$

Whenever,

$$\text{order}_m(a) = h = \phi(m)$$

then \boxed{a}

We say \boxed{a} is primitive root / generator

of that ~~element~~ set.

e.g. if $m = 5$, then $\phi(5) = 5-1 = 4$.

then all seen above = 1 mod

$$(1+1 \equiv 2) \quad 2 \neq 0$$

$$\text{order}_5(2) = \text{order}_5(3) = 4 = \phi(5)$$

and $1 \equiv 1$ and $2 \equiv 2$ and $3 \equiv 3$

Hence primitive roots of set 5 are $\{2, 3\}$

* To find no. of primitive roots:

$$\boxed{\phi(\phi(m))}$$

e.g. $\phi(\phi(5)) = \phi(4) = 2$

$$\phi(4) = 2^2 - 2^1 = 2 \text{ primitive roots.}$$

$$\phi(4) = 2^2 - 2^1 = 2$$

e.g. calculate primitive roots of \mathbb{Z}_{13} .

$$\phi(\phi(13)) = \phi(12) = \phi(3) \cdot \phi(4)$$

$$= (3-1)(2^2 - 2^1) = 2 \cdot 2 = 4.$$

$$\mathbb{Z}_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

$\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

$$\text{so } \phi(13) = 12$$

primitive roots = $\{2, 3, 4, 5\}$

So $2^0 \equiv 1$ and $2^1 \equiv 2$ and $2^2 \equiv 4$ and $2^3 \equiv 8$
 From division

Shortcut to calculate Primitive roots!

$$\phi(m) = \phi(13) = 12$$

$$a \in \mathbb{Z}_m^* \quad a^{12} \equiv 1 \pmod{13}$$

$a^{12} \equiv 1 \pmod{13} \Rightarrow a^{12} \equiv 1 \pmod{m}$

If a is a primitive root $a^h \equiv 1 \pmod{m}$

and if $a^k \equiv 1 \pmod{m}$ then $h|k$.
 $h \leq k$.

So we need to find factors of 12

$$12 \Rightarrow 1, 2, 3, 4, 6, 12$$

so we'll have to check for its factors to know if there exists an $h \leq 12$

so

for $a=2$

$$2^{12} \equiv 1 \pmod{13}$$

$$2^1 \equiv 2 \pmod{13}$$

$$2^2 \equiv 4 \pmod{13}$$

$$2^3 \equiv 8 \pmod{13}$$

$$2^4 \equiv 16 \pmod{13} = 3 \pmod{13}$$

$$2^6 \equiv 24 \cdot 2^2 \pmod{13} = 12 \pmod{13} = -1$$

$$2^{12} = 2^6 \cdot 2^6 \pmod{13} = -1 \cdot -1 \pmod{13} = 1 \pmod{13}$$

Hence 2 is a primitive root

Now when

$\forall k, \gcd(k, \phi(m)) = 1$ then $2^k \pmod{m}$ is a primitive root



$$(k, \phi(13)) = (k, 12) = 1$$

$$\Rightarrow k \in \{1, 5, 7, 11\}$$

$$\left. \begin{array}{l} k=1, \quad 2^1(13)=2 \\ k=5, \quad 2^5(13)=6 \\ k=7, \quad 2^7(13)=11 \\ k=11, \quad 2^{11}(13)=7 \end{array} \right\} \begin{array}{l} \text{Primitive} \\ \text{Roots} \end{array}$$

* Playfair Key Matrix:

if the pair is a repeated letter
or only single character is available

e.g.

B A L L O O N

2/001

repeated

insert filler character X.

B A L X L O O N

✓