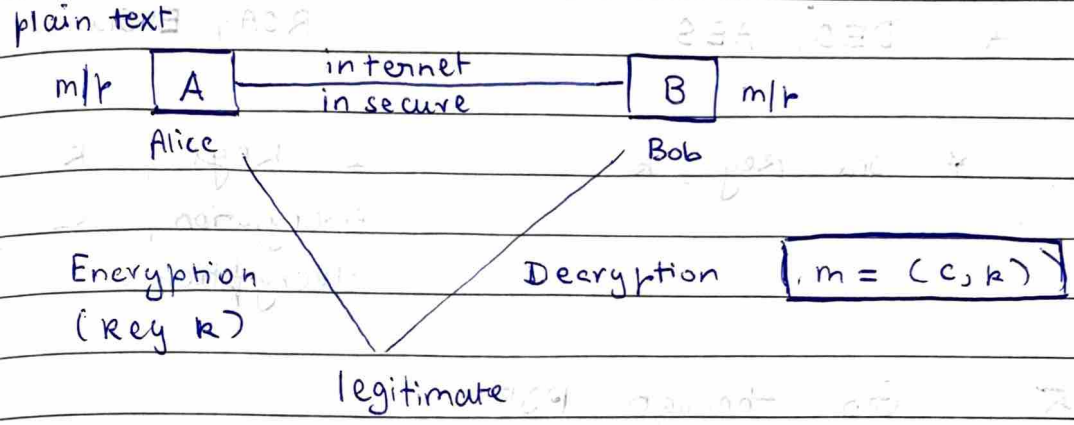
## Cryptography :

E Eve (Intruder / Evesdropper)




## CIA triads :

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

## Attacks :

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

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

31/12/21

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

① Divisibility : Let $a, b \in \mathbb{Z}$

if $a$ is divisible by $b$,
$b$ divides $a$ ($b \mid a$) then
$\exists\ c \in \mathbb{Z}$ such that $a = bc$
otherwise $b \nmid a$ ($b$ doesn't divide $a$)

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

$4 \mid 4$

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

$b$ : divisor, $a$ : dividend

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

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

1. $1 \mid a$, $a \mid a$ and $a \mid 0$
2. $0 \nmid a$ (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 $a \mid c \Rightarrow a \mid (b \pm c)$

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

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

- from equation ① and ②

$b + c = ax + ay$

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

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

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

$\therefore \quad a \mid (b - c) \Rightarrow a \mid (b \pm c)$

② Division Algorithm:

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

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

↓

a is proper divisor of b

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

prime no. has # only trivial # divisors

$p$ – prime number : $1 \mid p$ and $p \mid p$ only

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

gcd $(a, b, \ldots)$ Greatest common Divisor

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

if

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

assuming $a < b$, $d$ ranges from $\boxed{1 < d < a}$

eg. GCD(25, 125) = 25

i.e.

25 | 25 and 25 | 125

Rule: * if $\exists\ f \in \mathbb{N}$, $f \mid a$ and $f \mid b$

$\Rightarrow f \mid d$

$(1 \leq f \leq d)$

in this case $f = 5$

i.e. $5 \mid 25$ and $5 \mid 125 \Rightarrow 5 \mid 25$

Theorem: * $\gcd(a, b) = d$ then $\exists\ x, y \in \mathbb{Z}$ such that

$\Rightarrow \boxed{ax + by = d}$

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

$c \mid a.b$ and

$\boxed{\gcd(a, c) = 1}$ (Coprime / relatively prime)

then

$\boxed{c \mid b}$

Proof: $\gcd(a, c) = 1$ 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 :

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

$\Rightarrow b \mid ab$ and $b \mid bc$

given $c \mid ab$

and we can say $c \mid a \cdot bc$

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

**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

$p \nmid a$ 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(a,b) ≠ 1~~

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

$$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_r^{\beta_r}$$

so,

$$\gcd(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)} \cdots p_r^{\min(\alpha_r,\beta_r)}$$

and

$$\text{lcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} \cdots p_r^{\max(\alpha_r,\beta_r)}$$

eg. $a = 36 = 2^2 \cdot 3^2$

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

so

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

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

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

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

$$= 72$$

7/1/22

# Euclidean Algorithm:

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

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

$i = 1$ to $a$ :

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

gcd (-31, 24) =

| 24 | 31 | 1 |
|---|---|---|
| 24 | | |

$\longrightarrow$ gcd (24, 31) $\Rightarrow$

| 7 | 24 | 3 |
|---|---|---|
| 21 | | |

$\longrightarrow$ gcd (7, 24) $\Rightarrow$

| 3 | 7 | 2 |
|---|---|---|
| 6 | | |

$\longrightarrow$ gcd (3, 7)

| 1 | 3 | 3 |
|---|---|---|
| 3 | | |

$\longrightarrow$ gcd (1, 3)

gcd $\quad$ 0 $\quad = 1$

Therefore

1|3, 1|7,

1|24, 1|31

- hence gcd(24, 31) = 1

on generalizing : assume $a < b$ :

gcd (a, b) = d = ?

$(0 \leq r < a)$

| a | b | q |
|---|---|---|
| | -aq | |
| r | a | $q_1$ |
| | $-rq_1$ | |
| $r_1$ | | |

$\longrightarrow b = aq + r$

$(0 \leq r_1 < r)$ $\longrightarrow a = rq_1 + r_1$

$(0 \leq r_2 \leq r_1)$

$(0 \leq r_3 < r_2)$

$r_{j-2} = r_{j-1} \cdot q$

$31 = 24 \cdot 1 + 7$

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

We

then

to

eu

$(0 \le r_2 \le r_1)$ $\quad r_1 \mid r \mid q_2 \longrightarrow r = r_1 q_2 + r_2$

$-r_1 q_2$

$(0 \le r_3 < r_2)$ $\quad r_2 \mid r_1 \mid q_3 \rightarrow r_1 = r_2 q_3 + r_3$

$r_2 q_3$

$r_3$

$r_{j-2} = r_{j-1} \cdot q_j + r_j \quad | \quad r_{j-1} \mid r_{j-2} \mid q_j \quad (0 \le r_j < r_{j-1})$

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

$r_j \mid r_{j-1} \mid q_{j+1}$

$r_j \cdot q_{j+1}$

0

$31 = 24 \cdot 1 + 7$

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

gcd

$r_{j-1} = r_j \cdot q_{j+1} + 0$

Since

$r_j \mid r_{j-1}, \; r_j \mid r_{j-2}, \ldots$

$r_j \mid r_3, \; r_j \mid a, \; r_j \mid b$

$\therefore \quad \gcd(a, b) = r_j$

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

to calculate $x$ and $y$, we extended euclidean algorithm.

## * Extended Euclidean Algorithm:

gcd(21, 33) =

$33 = 21 \cdot 1 + 12$

$21 = 12 \cdot 1 + 9$

$12 = 9 \cdot 1 + 3$

$9 = 3 \cdot 3$

21 | 33 | 1
21
12 | 21 | 1
12
9 | 12 | 1
9
3 | 9 | 3
3
0

So;
3|9, 3|12,
3|21, 3|33
hence,
gcd(21, 33)
= 3

traversing bottom to top.

from ③ : $3 = 12 + 9 \cdot (-1)$

from ② : $9 = 21 + 12(-1)$

so;

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

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

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

From ① : $12 = 33 + 21 \cdot (-1)$

so;

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

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

$3 = 33(2) + 21(-3)$ ----- ... →

hence

$gcd(a, b) = d = by + ax$

## * Modular Arithmetic:

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

to make it finite:

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

$\mathbb{Z}/5\mathbb{Z}$ ← zero class

$\mathbb{Z}_5$

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

$15 \bmod 5$

$17 \bmod 5$

18

19

20

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

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

⋮

hence

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

therefore, $\mathbb{Z}_n = \{0, 1, \}$

Inverse: inverse of 33 = 2 |

inverse of 21 = -3 |

# Modular Arithmetic :

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

to make it finite :

$\mathbb{Z} \bmod 5 = \{ [0], [1], [2], [3], [4] \}$ complete class residue modulo / moduli 5.

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

$\mathbb{Z}_5$

$15 \bmod 5 = 0$

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

$17 \quad " \quad " = 2$

$18 = 3$

$19 = 4$

$20 = 0$

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

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

$\vdots$

Hence

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

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

---

Inverse : inverse of $33 = 2$

inverse of $21 = -3$

→

## * Congruence : ( $\equiv$ )

① $a \equiv b \mod n \Rightarrow n \mid a-b$

② $a \not\equiv b \mod n \Rightarrow n \nmid a-b$

eg. $6 \equiv 1 (5) \Rightarrow 5 \mid (6-1)$ ✓

$6 \equiv 2 (5) \Rightarrow 5 \mid (6-2)$ ✗

## Equivalence Relations :

① Reflexive : $a \equiv a \mod n$

$n \mid a-a = n \mid 0$

hence satisfied.

② Symmetric :

if $a \equiv b \mod n \Rightarrow b \equiv a \mod n$

eg. $6 \equiv 1 (5)$

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

$5 \mid (-5)$ ✓

③ Transitive :

if $a \equiv b \mod n$ and

$b \equiv c \mod n$

$\Rightarrow a \equiv c \mod n$

# Standard notations :

① $a \equiv b \bmod n$

$\Updownarrow$

$\boxed{a \equiv b\ (n)}$

② $\gcd(a, b) = d$

$\boxed{(a, b) = d}$

③ $\text{lcm}(a, b) = c$

$\boxed{[a, b] = c}$

Rule

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

eg.

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

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

$\vdots$

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

then $11 \equiv 1\ (5) \Rightarrow 5 \mid (11-1)$ ✓

but if

$a = 11$ and $b = 5$

$\in [1]$ $\in [0]$

then $11 = 5\ (5) \Rightarrow 5 \mid (11-5)$ ✗

assume a is known:
and b, n is known

$$a \equiv b \ (n)$$

eg.

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

We can see

$$11 \bmod 5 = 1$$

$$11 \ (\bmod 5) = 1$$

So

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

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

↑

* exclude this.

hence

$$11 \equiv 1 \ (5) \Rightarrow 5 \mid (11-1)$$

* Modulus operations:

1. $(a+b) \bmod n = a \ (\bmod n) + b \ (\bmod n)$
2. $(a-b) \bmod n = a \ (\bmod n) - b \ (\bmod n)$
3. $(a * b) \bmod n = a \ (\bmod n) \cdot b \ (\bmod n)$

11/1/22

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

# $+$ (ADD), $*$ (MUL) operations :-

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

↑ additive identity denoted as (e)

Additive Inverse

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

eg.

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

but $-2 \bmod 5 = 3$

and

$2 + 3 = 5$ and $5 \bmod 5 = 0$.

So;

$0 + 0 = 0$

$1 + 4 = 0$

$2 + 3 = 0$

$3 + 2 = 0$

$4 + 1 = 0$

③ For $a \in \mathbb{Z} \Rightarrow a * \boxed{1} = a$ Multiplicative Identity

here $e = 1$ always.

④ Multiplicative Inverse $a * \boxed{\quad} = e$

↑

$a * \left(\frac{1}{a}\right) = 1$

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

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

$0 * \square = 0$ (special case)

$1 * 1 = 1$

$2 * 3 = 1$ i.e. $(2 * 3) \bmod 5 = 1$

$3 * 2 = 1$

$4 * 4 = 1$

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

- $2 * \square = 1$ : no multiplicative inverse
- $5 * \boxed{5} = 1$ ✓ $25 \pmod 6 = 1$

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 $\gcd(a, m) = 1$.

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

$ax + my = 1$.

→: $ax = 1 + m(-y)$

and we know $a \equiv b \pmod n \Rightarrow n \mid (a-b)$ or

$\exists\ k \in \mathbb{Z}$ s.t. $a - b = kn$

$\Rightarrow a = b + kn$

Similar proof

Therefore $ax = 1 + m(-y)$

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

$\Rightarrow ax \equiv 1 \ (m) \Rightarrow ax \ (m) = 1$

↓

$x$ can be found using extended euclidean algo.

In sets :

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\} \Rightarrow$ 4 elements $\{1, 2, 3, 4\}$ have multiplicative inverse.

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\} \Rightarrow$ 2 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 $a \equiv b \ (m)$ and $b \equiv a \ (m)$ then $a - b \equiv 0 \ (m)$

Similar proof

② If $a \equiv b \ (m)$ and $c \equiv d \ (m)$ then $a + c \equiv b + d \ (m)$ and

③ " " $ac \equiv bd \ (m)$

④ If $a \equiv b \ (m)$ then $ac \equiv bc \ (\text{mod } mc)$ for $c > 0$

↓

$\alpha > 0$

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

prime

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$$
$$= p^\alpha\left(1 - \frac{1}{p}\right)$$
$$= p^{\alpha-1}(p-1).$$

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 $(a,b) = 1$

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

eg.

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

i.e.

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

$$\phi(6) = \phi(2 \cdot 3) = \phi(2^1) \cdot \phi(3^1)$$
$$= (2^1 - 2^0) \cdot (3^1 - 3^0)$$
$$= 1 \cdot (2)$$
$$= 2$$

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

So, $\boxed{\phi(p) = p - 1}$

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

↓ product of $(1 - 1/p)$ → where $p$ are prime factors of $n$

eg.

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

$$= 4.$$

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

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

* Linear Congruence : $ax \equiv b \bmod m \Rightarrow m \mid ax - b$

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

$ax \equiv b \bmod m$

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

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

So we can substitute

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

i.e.

$b \equiv b \bmod m \Rightarrow m \mid b - b$ ✓

↓

② if a and m are not coprime
i.e. $(a, m) = d > 1$ solution exists
iff $d \mid b$.

examples :

1. $3x \equiv 4 \mod 5$

we know $(3,5) = 1$

So

$3 \cdot 2 \equiv 1 \mod 5$

↑ multiplicative inverse

On multiplying 2 on both sides

We know
$ax(m)$
$a(m) \cdot x(m)$

$2 \cdot 3x \equiv 2 \cdot 4 \ (5)$

$6x \ (5) \equiv 8 \ (5)$

$6(5)\ x(5) \equiv 8 \ (5)$

$x \ (5) \equiv 8 \ (5)$

$\boxed{x \equiv 3 \ (5)}$

So $x = 3$

putting in equation

$3 \cdot 3 \equiv 4 \mod 5$

$9 \equiv 4 \mod 5$

$5 \mid (9-4) \Rightarrow 5 \mid 5$ ✓

↓

$a \quad x \quad b \quad m$

2. $6x \equiv 4 \bmod 10$

$d$

$(6,10) = 2 > 1$ but $2 \mid 4$

hence solution exists.

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

hence

$3x \equiv 2 \bmod 5$

now

$(3,5) = 1$

$3 \cdot 2 \equiv 1 \bmod 5$

$\uparrow$

$a^{-1}$.

$2 \cdot 3x \equiv 2 \cdot 2 \bmod 5$

$x \equiv 4 \bmod 5$

$x = 4$

so

$6 \cdot 4 \equiv 4 \bmod 10 \Rightarrow 10 \mid 6 \cdot 4 - 4$

$10 \mid 20$ ✓

3. $8x \equiv 5 \ (16)$ since $(8,16) = 4 > 1$

but $4 \nmid 5$

hence solution does not exist.

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

using fundamental theorem of arithmetic:

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

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

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

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

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

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

$$\downarrow$$

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

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

(2) Theo

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

$$\downarrow$$

Date
Page

eg. $n = 8$ 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

$1 \nmid 1$ and $1 \mid 0$.

hence 1 and 0 are relatively prime.

Also note: $\gcd(2,0) = 2$

⋮

---

Hence $\phi(1) = 1$

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

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

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

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

Hence

$1 + 1 + 2 + 4 = 8$

Verified.

## * Fermat's little theorem:

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

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

then

$$\boxed{a^{p-1} \equiv 1 \bmod p}$$

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

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

$\blacksquare$ $3^{5-1} \equiv 1 (5)$ verified.

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

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 $a \cdot a_i \equiv a \cdot a_j (p)$

eg. $4 = 4$

$4 \equiv 4 (p) \Rightarrow p \mid (4-4)$

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

$p \mid a(a_i - a_j)$

from the previous rule :

if $p \mid a \cdot b$

then $p \mid a$ or $p \mid b$

then

$p \mid a$ or $p \mid (a_i - a_j)$

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

and for

$p \mid (a_i - a_j)$

$a_i, a_j \in Z_p$ and $a_i - a_j < p$

hence

$p \nmid (a_i - a_j)$

contradiction.

Hence $\boxed{a \cdot a_i \neq a \cdot a_j}$.

(2) $\boxed{Z_p = a \cdot Z_p}$

eg. $Z_5 = \{0, 1, 2, 3, 4\}$, let $a = 3$

$3 \cdot Z_5 = \{0, 3, 1, 4, 2\}$

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 $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ except 0.

$$a^{p-1}(p-1)! \equiv (p-1)! \bmod p$$

$$p \mid (p-1)!\,(a^{p-1} - 1)$$

so

$$p \mid (p-1)! \quad \text{or} \quad p \mid (a^{p-1} - 1)$$

but

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

hence

$$\boxed{p \mid (a^{p-1} - 1)}$$

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

multiply $a$ on both sides

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

$$\boxed{a^p \equiv a \ (p)}$$

* if $p \mid a$ eg. $5 \mid 5 \Rightarrow 5^5 \equiv 5 \ (15)$

$$5(5) = 0$$

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

So $\boxed{0 = 0}$ hence, due to this exception, $(a, p) = 1$ i.e. $p \nmid a$.

# Corollary (Extension of proof):

if $p \nmid a$ and $n \equiv m \ (p-1)$

then $\boxed{a^n \equiv a^m \ (p)}$

eg. $p \quad a \qquad\qquad n \quad m \quad p$

$5 \nmid 3$ and $5 \equiv 1 \ (5-1) \Rightarrow 5 \equiv 1 \ (4)$

$\Rightarrow 4 \mid (5-1)$ ✓

So, $3^5 \equiv 3^1 \ (5) \Rightarrow 5 \mid (3^5 - 3^1)$

$\downarrow$

$(3^2 . 3^2 . 3) \ (5)$

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

$= (4 . 4 . 3) \ (5)$

$= 16(5) . 3(5)$

$= 3(5)$

so,

$\boxed{3(5) = 3(5)}$ verified.

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

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

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

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

$[a^{p-1} \equiv 1 \ (p)]$ $\quad a^n \equiv a^m . 1^x \ (p)$

$\boxed{a^n \equiv a^m \ (p)}$ proved

** Example :

$2^{1000000} \bmod 7 =$

$a^n \bmod p$ i.e. $a = 2, n = 1000000, p = 7.$

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

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

↓ ↓ ↓

n m p

$1000000 \ (6) = 4$

so

$1000000 \equiv 4 \ (6) \Rightarrow 6 \mid 1000000 - 4$ ✓

↓

m

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

$2^4 \ (7) = 2$

so

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

13/1/22

## Chinese Remainder Theorem : (requires minimum 2 equations)

r no. of congruence equations :

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

$n_1, n_2, \ldots n_r$ → moduli's

if all these moduli's should be coprime

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

then solution exists.

i.e.

consistent → if solution exists

and inconsistent → if solution doesn't exist.

Let

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

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

so,

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

i.e. $(N_1, n_1) = 1$

then

$$\boxed{N_1 m_1 = 1 \ (n_1)}$$

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

$$N_r = \frac{N}{n_r}, \quad (N_r, n_r) = 1$$

So,

$$N_r m_r = 1 \ (n_r)$$

$$m_r = N_r^{-1}.$$

Therefore the solution can be calculated;

$$\boxed{x = \left(\sum_{i=1}^{r} a_i N_i m_i\right) \bmod N}$$

Multiple solutions can be found

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

* **eg. 1**

| | | |
|---|---|---|
| $x \equiv 2 \ (3)$ | $a_1 = 2$ | $n_1 = 3$ |
| $x \equiv 3 \ (5)$ | $a_2 = 3$ | $n_2 = 5$ |
| $x \equiv 2 \ (7)$ | $a_3 = 2$ | $n_3 = 7$ |

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

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

$$35 \cdot (2) = 1 \ (3)$$

$N_1$ $m_1$ $n_1$

↳ found using extended euclidean algo.

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

So, $21 \cdot (1) \equiv 1 \pmod 5$

$N_2 \quad m_2 \quad n_2$

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

$N_3 \quad m_3 \quad n_3$

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

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

$$= 233 \bmod 105$$

$$x = 23$$

$$x_0 = 23 + k \cdot 105 \qquad k \geq 0.$$

We can check

$23 \equiv 2 \pmod 3 \Rightarrow 3 \mid 23 - 2$ ✓

$23 \equiv 3 \pmod 5 \Rightarrow 5 \mid 23 - 3$ ✓

$23 \equiv 2 \pmod 7 \Rightarrow 7 \mid 23 - 2$ ✓

Verified.

* Eg. 2

$x \equiv 29 \ (52)$

$x \equiv 19 \ (72)$

So

$52 = a \cdot b$

$= 4 \cdot 13$ and $(4, 13) = 1$.

So

$x \equiv 29 (52) \Rightarrow 52 \mid x - 29$,

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

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

So,

$x \equiv 29 (4)$ and similarly

$x \equiv 29 (13)$

Similarly,

$72 = a \cdot b = 8 \cdot 9$ and $(8, 9) = 1$

So,

$x \equiv 19 (8)$

$x \equiv 19 (9)$

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

unnecessary step I guess

$\Rightarrow x \equiv 19 (4)$

$\downarrow$

$x \equiv 3 (4)$

$x \equiv 1 (4)$

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: $x \equiv 3 (10)$ → remainders
$x \equiv 8 (15)$
$x \equiv 5 (84)$
↳ moduli

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

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

but $(1260, 10) \neq 1$
$= 10$

so we cannot find $m_1$ (inverse).

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

So,

$x \equiv 3 (10)$ ⇓
$x \equiv 3 (2)$
$x \equiv 3 (5)$

$x \equiv 8 (15)$ ⇓
$x \equiv 8 (3)$
$x \equiv 8 (5)$

$x \equiv 5 (84)$ ⇓
$x \equiv 5 (4)$
$x \equiv 5 (21)$

classmate
Date
Page

$x \equiv 1 (2)$
$x \equiv 3 (5)$

$x \equiv 2 (3)$
$x \equiv 3 (5)$

$x \equiv 5 (4)$

$\Downarrow$

$x \equiv 5 (2)$ and $x \equiv 5 (2)$

and

$x \equiv 5 (21)$

$\Downarrow$

$x \equiv 5 (7)$ and $x \equiv 5 (3)$

$\Downarrow$

$x \equiv 1 (2)$
$x \equiv 3 (5)$

$\Downarrow$

$x \equiv 2 (3)$
$x \equiv 3 (5)$

$\Downarrow$

$x \equiv 1 (2)$
$x \equiv 5 (7)$
$x \equiv 2 (3)$

So;

$x \equiv 1 (2)$
$x \equiv 2 (3)$
$x \equiv 3 (5)$
$x \equiv 5 (7)$

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

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

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

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

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

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

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

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

$\downarrow$

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

$$= 173$$

14/1/22 Taking the same example:

$x \equiv 2 (3)$ — ① $\Rightarrow$ $x \equiv 2 (3) \Rightarrow 3 \mid x-2$

$x \equiv 3 (5)$ — ② then $\exists\, k \in \mathbb{Z}$

$x \equiv 2 (7)$ — ③ $x = 2 + 3k$ — ④

Substitute ④ in ②

$x \equiv 3 (5)$

$2 + 3k \equiv 3 (5) \Rightarrow 5 \mid 2 + 3k - 3$

$3k \equiv 1 (5) \Leftarrow 5 \mid 3k - 1$

and

$(3, 5) = 1$

$3 \cdot 2 \equiv 1 (5)$

$2 = a^{-1}$.

note: if they were not prime, system of eqn's would be inconsistent — so multiply inverse of 3 on both sides

$2 \cdot 3k \equiv 2 \cdot 1 (5)$

$k \equiv 2 (5) \Rightarrow k = 2 + 5u, \; u \in \mathbb{Z}$ — ⑤

Substitute ⑤ in ④:

$x = 2 + 3k$

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

$x = 8 + 15u$ — ⑥

Substitute ⑥ in ③ :

$$x \equiv 2 (7)$$

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

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

$$7 \mid 6 + 15u$$

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

$$u \equiv 1 (7)$$

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

Substitute ⑦ in ⑥ :

$$x = 8 + 15u$$

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

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

$$\Downarrow$$

$$x \equiv 23 (105) \quad \rightarrow \text{Solution}$$

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

# Euler's theorem ($\phi$) :

if $(n, a) = 1$ then $\boxed{a^{\phi(n)} \equiv 1 \,(n)}$

↳ composite numbers.

# Fermat's little theorem :

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

if $n = p$,

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

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

so euler theorem is for composite numbers and fermatt's theorem is for prime n.

↳ eg. $n = 15$, $a = 2$

$\phi(15) = \phi(3 \cdot 5) = \phi(3) \cdot \phi(5)$

$= 2 \cdot 4 = 8$.

and $(15, 2) = 1$

so

$2^8 \equiv 1 \,(15)$

↓

$2^8 \,(15) = (2^4 \,(15) \cdot 2^4 \,(15))\,(15)$

$= 1 \cdot 1 \,(15)$

$= 1 \,(15)$ verified.

Continuing Primality test ...

① deterministic primality test : ⇒ n is prime with 100% confidence
⇒ n is not prime " n "

② probabilistic primality test : ⇒ n is prime, without 100% confidence
⇒ 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 = [ _ _ _ _ _ _ ]

↓

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 $n \nmid a$ and $a^{n-1} \equiv 1 \pmod{n}$
then n is prime

but fermat's thm is probabilistic !

Proving 91 is probable 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.

eg. $n = 91$ , $a = 2$

we see

$(n, a) = 1$ but

$2^{90} \equiv 64 \,(91)$ ,

hence 91 is composite.

Hence for different bases 91 is prime/comp.

* Prime/not prime : ① $n = 5$ $O(n)$

base tests

1 2 ... 5 = 2 (1 and 5)

check divisible or not

② $n = 5$ $O(n)$ 1 | 2 ..... 4 | 5

check

③ $n = 5$ $O(\sqrt{n})$ 2 ... $\sqrt{5}$

check

trail division method

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

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

$\mathbb{Z}_n^* = \{0 < a < n : (a, n) = 1\}$

The smallest number that satisfies this is 561.

## * Shortcut properties :

1. IF n is divisible by a perfect square >1 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. $n-1 = 2^k \cdot m$
   ↳ odd
3. choose a, s.t. $(a,n) = 1$ , $1 < a < n-1$.

4. $b_0 = a^m \pmod n$ — $\pm 1$ Probable prime
   $b_1 = b_0^2 \pmod n$ — $-1$ Probable prime
   ⋮ — Composite
   $b_{k-1} = b_{k-2}^2 \pmod n$ — $-1$ Probable prime
   — Composite.

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

↓

eg. ① $n = 23$

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

Choose $a=2$, $\because (2,23)=1$

$b_0 = 2^{11} \pmod{23}$

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

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

$= 1$

Hence 23 is probable prime.

Since $k=1$ stop at $b_0$.

eg. ② : $n = 55$

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

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

$b_0 = 2^{27}(55)$

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

$= ((2^6(55))^4 2^3)(55)$

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

$= 18(55) \neq \pm 1$

hence it is composite number.

H.W.

eg. ③ $n = 53$

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

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

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

$= (2^6(53))(2^6(53))(2))(53)$

$= (11 \cdot 11 \cdot 2)(53)$

$= (242)(53) = 30(53)$.

$b_1 = (30)^2 \bmod 53$

$= 900(53)$

$= 52 \cdot (53) = -1 \cdot (53)$

$b_1 = -1$ , hence probable prime

P.T.O.

## * WILSON'S METHOD :

$$(P-1)! \equiv -1 \bmod P \Rightarrow P \mid (P-1)! - (-1)$$

All primes satisfies this method.

P = 2, 3, 5, 7 ..

$(2-1)! \equiv -1 \bmod 2 \Rightarrow 2 \mid 2$ ✓

$(3-1)! \equiv -1 \bmod 3 \Rightarrow 3 \mid 3$ ✓

$(5-1)! \equiv -1 \bmod 5 \Rightarrow 5 \mid 25$ ✓

Drawback :

1. Factorial operation is very tedious.
   O(n) complexity.

19/01/22 * $k^2 \equiv 1 \bmod p$ iff $k = 1$ or $k = p-1$

i.e.

$k \cdot k \equiv 1 \bmod p$

↓

i.e. k inverse is k.

eg. $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ ($5-1$)

$1 \cdot 1 \equiv 1 \,(5) \Rightarrow 5 \mid 1-1$ ✓

$4 \cdot 4 \equiv 1 \,(5) \Rightarrow 5 \mid 16-1$ ✓

↓

rest of the numbers will have inverse from within the set.

↓

## * Proof of Wilson's Theorem:

LHS ← $(p-1)! \bmod p = (1 \cdot 2 \cdot 3 \cdots (p-2)(p-1)) \bmod p$.

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

1 1 1

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

$= (p-1) \bmod p$

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

$= -1 \bmod p \rightarrow$ RHS

Hence proved.

eg. 0

$p = 11 \Rightarrow (p-1)! \equiv -1 \ (p)$

$(11-1)! \equiv -1 \ (11)$

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

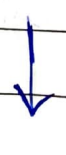
$= (1 \cdot (2 \cdot 6)(3 \cdot 4)(5 \cdot 9)(7 \cdot 8) \cdot 10)(11)$

$= (1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 10)(11)$

$= 10 \bmod 11 = -1 \bmod 11$. ✓

Verified

eg. 1 $x = \frac{130!}{87} \pmod{131}$.



$\Rightarrow \quad x = (87)^{-1} 130! \pmod{131}$.

$P = 131$

$(131-1)! \equiv -1 \mod 131$.

so

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

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

We know $87(-3) \mod 131 = 1$

So,

$x = -(-3) \mod 131$

$x = 3 \ (131)$

eg 2 : $x = (146)! \ (149)$

$\Rightarrow \quad (147 \cdot 148)\, x = (148)! \ (149)$

$(-2 \cdot -1)\, x = -1 (149)$.

$2x = -1 (149)$

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

and

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

So

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

$x \equiv 74 (149)$ ✓

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

$a = 47$, $p = 113$.

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

$x = 47^{110} \cdot \underbrace{47^{112} \pmod{113}}_{1 \pmod{113}}$

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

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

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

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

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

So

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

31 is multiplicative inverse of 62.

Hence

| 113 | 62 | 0 |
|---|---|---|
| 0 | | |

| 62 | 113 | 1 |
|---|---|---|
| 62 | | |

| 51 | 62 | 1 |
|---|---|---|
| 51 | | |

| 11 | 51 | 4 |
|---|---|---|
| 44 | | |

| 7 | 11 | 1 |
|---|---|---|
| 7 | | |

| 4 | 7 | 1 |
|---|---|---|
| 4 | | |
| 3 | | |

| 3 | 4 | 1 |
|---|---|---|
| | 3 | |

| 1 | 3 | 3 |
|---|---|---|
| | 3 | |
| | 0 | |

$113 = 62 \cdot 1 + 51$

$62 = 51 \cdot 1 + 11$

$51 = 11 \cdot 4 + 7$

$11 = 7 \cdot 1 + 4$

$7 = 4 \cdot 1 + 3$

$4 = 3 \cdot 1 + 1$

~~$113 = 62 \cdot 1 + 62 = (1$~~

$1 = 4 - 3 \cdot 1$

$1 = 4 - (7 - 4 \cdot 1) \Rightarrow 1 = 4 \cdot 2 + 7(-1)$

$1 = (11 - 7) \cdot 2 + 7(-1) \Rightarrow 1 = 11 \cdot 2 + 7 \cdot (-3)$

$1 = 11 \cdot 2 + (51 - 11 \cdot 4)(-3)$

$\Rightarrow 1 = 11 \cdot 14 + 51 \cdot (-3)$

$1 = (62 - 51) \cdot 14 + 51(-3)$

$\Rightarrow 1 = 62 \cdot 14 + 51 \cdot (-17)$

$1 = 62 \cdot 14 + (113 - 62)(-17)$

$1 = 62 \cdot (31) + 113(-17)$

↓

31 is inverse of 62.

Hence

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

$x \equiv 31 \pmod{113}$

↓

too much difference!

* **Eg. 4:** $x = 701 \pmod{5183}$ — (1)

$5183 = 71 \times 73$ and $5183 \mid x - 701$

So we can write

$x \equiv 701 \pmod{71} = -1 \bmod 71.$ — (2)

$x \equiv 701 \pmod{73}$

Using wilson's theorem

$701 \pmod{71} = -1 \bmod 71.$

$71.72\, x \equiv (72)! \bmod 73$

$(-2 \cdot -1)\, x \equiv (-1) \bmod 73$

$-2x \equiv +1 \bmod 73.$

We know

$((+2 \cdot 37) \equiv 1 \bmod 73)$

$-37.2x \equiv 37 \bmod 73$

$x \equiv -37 \bmod 73.$

$x \equiv 36 \bmod 73$ — (3)

i.e.

| | | |
|---|---|---|
| $x \equiv -1 \ (71)$ | $n_1 = 71$ | $a_1 = -1$ |
| $x \equiv 36 \ (73)$ | $n_2 = 73$ | $a_2 = 36$ |

Using CRT

| $N_1$ | $n_1$ | $N_2$ | $n_2$ |
|---|---|---|---|
| $73\ m_1 = 1\ (71)$ | | $71\ m_2 = 1\ (73)$ | |
| $2\ m_1 = 1\ (71)$ | | $-2\ m_2 = 1\ (73)$ | |
| $2 \cdot 36 \equiv 1\ (71)$ | | $-2 \cdot 36 \equiv 1\ (73)$ | |
| $m_1 = 36\ (71)$ | | $m_2 = 36\ (73)$. | |

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

## * PRIMITIVE ROOTS

Order of element : $a \in \mathbb{Z}_m$, $\mathbb{Z}_m = \{0, 1, \ldots m-1\}$

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

- $a^h$: least positive integer
- $e$: multiplicative identity (1)
- $m$: set size

in such conditions

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

if

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

then $h \mid k$.

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

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

$1^1 = 1 \Rightarrow$

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

$2^1 = 2 (5)$

$2^2 = 4 (5)$

$2^3 = 3 (5)$

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

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

$3^1 = 3$

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

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

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

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

$4^1 = 4$

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

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

** According to Euler's theorem:

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

Whenever,

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

* that $\boxed{a}$

We say is primitive root / generator

of that set.

↓

eg. $m = 5$, then $\phi(5) = 5 - 1 = 4$.
then as seen above

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

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

* To find no. of primitive roots:

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

eg.

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

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

eg. calculate primitive roots of $\mathbb{Z}_{13}$.

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

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

$$\mathbb{Z}_{13}^* = \{1, 2, \ldots, 12\}$$

So $\phi(13) = 12$

primitive roots $= \{2, 6, 7, 11\}$

Shortcut to calculate Primitive roots :

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

$a \in \mathbb{Z}^*_m \qquad a^{12} \equiv 1 \ (13)$

if ~~is a primitive root~~ $a^h \equiv 1 \ (m)$

and if $a^k \equiv 1 \ (m)$ then $h \mid k$.

$h \leq k$.

So

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 $a = 2$

$2^{12} \equiv 1 \ (13)$

$2^1 = 2 \ (13)$

$2^2 = 4 \ (13)$

$2^3 = 8 \ (13)$

$2^4 = 16 \ (13) = 3$

$2^6 = 2^4 \cdot 2^2 \ (13) = 12 \ (13) = -1$

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

Hence 2 is a primitive root

**** Now when

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

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

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

$k = 1$ , $2^1 (13) = 2$

$k = 5$ , $2^5 (13) = 6$

$k = 7$ , $2^7 (13) = 11$

$k = 11$ $2^{11} (13) = 7$

} Primitive roots

* Playfair Key Matrix :

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

eg.

BA LL OO N

repeated

no pair

insert filler character X.

BA LX LO ON