[Introduction to Info Security].

Camlin Page
Date / /

Cryptography –

Number theory :- ~~Divisibility~~

Relation b/w types of numbers –

$$\boxed{\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}}$$

1) → Divisibility – Let $a, b \in \mathbb{Z}$

If a is divisible by b (or) b divides a ($b \mid a$) then there exist $\exists\ c$ ($c \in \mathbb{Z}$) such that

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

*(Terms :- Divisor, Divident, proper divisor)

Theorems – $a, b, c \in \mathbb{Z}$

1) $\forall : 1 \mid a$, $a \mid a$ and $a \mid 0$
2) $0 \nmid a$ (except $a = 0$) ($0 \mid 0$ case acceptable)
3) $a \mid b$ & $b \mid a \Rightarrow a = \pm b$
4) $a \mid b \Rightarrow a \mid -b$
5) $a \mid b$ & $b \mid c \Rightarrow a \mid c$
6) $a \mid b$ & $a \mid c \Rightarrow a \mid (b \pm c)$

*(Try to proove above theorems)

Proof of 6.

$a \mid b$, $\exists\ x$ such that $b = ax$ — ①

$a \mid c$, $\exists\ y$ such that $c = ay$ — ②

from ① & ②

$b + c = ax + ay$

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

$a \mid b + c$

$b - c = ax - ay$

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

$a \mid b - c$

Division Algorithm – let $a, b \in \mathbb{Z}$, $a \neq b$ $\exists\, q, r \in \mathbb{Z}$

Then $b = aq + r$

$$\boxed{0 \leq r < a}$$

$n \in \mathbb{Z}$, $1 \mid n$ & $n \mid n$

here (1 & n are trivial divisors of n)*

P → prime numbers → Only have trivial divisors

$1 \mid P$ & $P \mid P$ only

Composite numbers : $n = ab$

$1 \leq a, b < n$

(or) opposite of prime numbers.

GCD

gcd(a,b) → let $a, b \in \mathbb{N}$

↳ $d \Rightarrow d \mid a$ & $d \mid b$ where d is highest possible value.

$a < b$

$$\boxed{1 < d \leq a}$$

So let

if $\exists\, f \in \mathbb{N}$ such that $f \mid a$ & $f \mid b \Rightarrow f \mid d$ — gcd(a,b)

$$\boxed{1 \leq f \leq d}$$

Theorem → $\gcd(a,b) = d$

then

$\exists\, x, y \in \mathbb{Z}$ such that

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

Camlin Page
Date / /

$\boxed{gcd(a,b) = 1}$ → means a, b are co-prime / relatively prime

or a, b doesn't have common divisors other than 1.

Theorem: For $a, b, c \in \mathbb{Z}$ such that $c \mid ab$ & $gcd(a,b) = 1$ then $c \mid b$.

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

$\exists x, y \in \mathbb{Z} \Rightarrow \boxed{ax + cy = 1}$

$b(ax + cy) = b$

$abx + bcy = b$

$gcd(ab, bc) = b \Rightarrow b \mid ab$ & $b \mid bc$

given

$c \mid ab$ & $c \mid cb \Rightarrow (c \mid b)$

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

$p \mid ab \Rightarrow p \mid a$ or $p \mid b$

proof: $p \nmid a$, $\boxed{gcd(p,a) = 1}$ → p, a → relatively prime

$p \mid ab$ → using above theorem $(p \mid b)$

else

$p \mid a \Rightarrow a = p \cdot c \quad \exists c \in \mathbb{Z}$

Camlin Page
Date / /

★ **Theorem: There are infinite no. of prime numbers**

→ **Fundamental Theorem of Arithmetic (FTA)**

$$\pm n = (\pm 1) \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_n^{\alpha_n}$$

(every number can be represented as ~~power~~ product of primes)

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

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n}$$

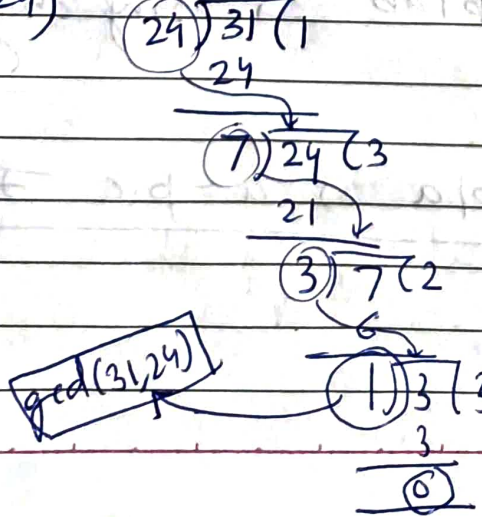
$$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_n^{\beta_n}$$

$$\gcd(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)} \cdots p_n^{\min(\alpha_n,\beta_n)}$$

$$\text{lcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} \cdot p_2^{\max(\alpha_2,\beta_2)} \cdots p_n^{\max(\alpha_n,\beta_n)}$$

Euclidean Algorithm

let gcd(31, 24)



Euclidean Algorithm
Extended Euclidean Algorithm] → study Online

Camlin | Page
Date / /

Theorem: — Assume $a<b$
$\gcd(a,b)=d \Rightarrow ?$

---

5 Modular Arithmetic ⇒ Congruence

$\mathbb{Z}$ → infinite

$\mathbb{Z}_5 = \{0,1,2,3,4\}$ → complete class residue modulo/modulo.

Residue class →
$[0] = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$
$[1] = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$
$[2]$
$[3]$
$[4]$

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

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

Congruence (≡)

① $a \equiv b \bmod n \Rightarrow n \mid (a-b)$

Equivalence Relations

Reflexive ① $a \equiv a \bmod n \Rightarrow n \mid (a-a) = n \mid 0.$

Symmetry ② if $a \equiv b \bmod n \Rightarrow b \equiv a \bmod n.$

Transitive ③ if $a \equiv b \bmod n$ & $b \equiv c \bmod n \Rightarrow a \equiv c \bmod n$

Standard Notations

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

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

$\text{Lcm}(a,b) = c$
$[a,b] = c$

$(a+b) \bmod n = a \bmod n + b \bmod n$

$(a-b) \bmod n = a \bmod n - b \bmod n$

$(a*b) \bmod n = a \bmod n * b \bmod n$

* Identities in congruences

1. Additive (e=0)
2. Additive Inverse
3. Multiplicative (e=1)
4. Multiplicative Inverse

consider $\mathbb{Z}_m$ not $\mathbb{Z}$ *

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

Proof:- Assume $\gcd(a,m) = 1$, $\exists\ x, y \in \mathbb{Z}$ such that

~~$ax + by = 1$~~

$ax + my = 1$

$ax = 1 - my$

$ax = 1 + m(-y)$

$m \mid ax - 1$

$ax = 1 \bmod m$

Notation –

$\mathbb{Z}_5^*$ → Elements having multiplicative inverse

$|\mathbb{Z}_5^*|$ → No. of elements having multiplicative inverse.

Camlin | Page
Date / /

Theorem :-

1. $a \equiv b(m)$ and $b \equiv a(m)$, then $(a-b) = 0(m)$

2. If $a \equiv b(m)$ and $c \equiv d(m)$ then ① $(a+c) \equiv (b+d)(m)$
   ② $ac = bd(m)$

3. If $a \equiv b(m)$ then $ac = bc \bmod mc$ for $c > 0$

Euler's totient (ϕ) →

→ $\boxed{\phi(p^\alpha) = p^\alpha - p^{\alpha-1}}$ *

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

$= p^{\alpha-1}(p-1)$

→ $\phi(n) = \phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_n^{\alpha_n})$ — ①
(∵ FTA)

$\boxed{\phi(ab) = \phi(a) \cdot \phi(b) \text{ iff } (a,b) = 1}$ *

as in ① $p_1, p_2, \ldots p_n$ are primes

$\boxed{\phi(n) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdots \phi(p_n^{\alpha_n})}$ *

→ $\boxed{\phi(n) \rightarrow \text{returns } |\mathbb{Z}_n^*|.}$ *

Let $p \rightarrow$ prime

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

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

Linear Congruence →

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

① $ax \equiv b \bmod m$

if a^{-1} exists

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

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

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

Proof: → $\phi(n) = \phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n})$ {∵ FTA}

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

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

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

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

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

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

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

$\phi(1) = 1$

Camlin | Page
Date / /

#(2) $\sum_{d|n} \phi(d) = n$. $\quad 1 \le d \le n$

ex $n = 8$

$1 \le d \le 8$

$d = 1, 2, 4, 8$

$\sum_{d|8} \phi(d) = 8$

$\phi(1) + \phi(2) + \phi(4) + \phi(8) =$

$1 + 1 + 2 + 4 = 8$ ✓

Fermat's little theorem –

$\mathbb{Z}_p \in \{0, 1, \cdots, p-1\} \Rightarrow |\mathbb{Z}_p| = p$ ∴ order / cardinality

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

$$a^{p-1} \equiv 1 \bmod p \quad \star$$

proof :–

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

a, p are co-prime

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

Parts

① Uniqueness $\quad a_i, a_j \quad i \neq j$, $a_i, a_j \in \mathbb{Z}_p$

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

Assume $a \cdot a_i = a \cdot a_j$

$\cdot\ a \cdot a_i \equiv a \cdot a_j \pmod p$

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

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

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

$p \mid a$ or $p \mid (a_i - a_j)$ → contradiction (as both divisions are not possible)

$p \mid ab \Rightarrow p \mid a$ or $p \mid b$

So, $a \cdot a_i \neq a \cdot a_j$

↳ even after multiplying, elements are distinct.

$Z_p = a \cdot Z_p$

$a \cdot Z_p \equiv Z_p \pmod{p}$

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

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

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

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

Not possible

possible

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

multiply 'a' on both sides

$a^p \equiv a \bmod p$

Camlin | Page
Date / /

~~Let~~ If $p \mid a$ $\quad p=5, a=5$

$5 \mid 5 \Rightarrow 5^5 \equiv 5 (5)$

$5^5 (5) = 0$

$0 = 0$

Hence, $p \nmid a$.

Extension of proof

Corollary $\Rightarrow$ $\boxed{p \nmid a, \; n \equiv m (p-1)}$

$\Rightarrow \boxed{a^n = a^m (p)}$

Let $p=5, a=3 \Rightarrow 5 \nmid 3$

consider n, m w.r.t 4

$5 \equiv 1 \bmod (5-1)$

$5 \equiv 1 \bmod 4$

$4 \mid 5-1$ ✓

$3^5 \equiv 3^1 (5)$

$5 \mid 3^5 - 3^1$

$5 \mid 3(3^4 - 1) \Rightarrow 5 \mid 240$ ✓

if $n \equiv m (p-1) \Rightarrow (p-1) \mid n-m$, $\exists \; x \in \mathbb{Z}$ such that $n \equiv m + x(p-1) \Rightarrow a^n \equiv a^{m+x(p-1)} (p)$

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

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

$a^n = a^m \; (1)^x \bmod p$

$\boxed{a^n = a^m \bmod p}$

Camlin | Page
Date / /

Eg – $2^{1000000} \bmod 7$

$a^m \bmod p \Rightarrow a=2,\ m=1000000,\ p=7$

$n \equiv m(p-1)$

$n \equiv {}^{\circ}1000000\ (6)$

$n=4$ ↓

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

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

Chinese – Remainder theorem (CRT)

'r' no. of congruence relations.

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

$n_1, n_2, n_3, \ldots n_r \rightarrow$ moduli's

↳ they should satisfy $\underline{\gcd(n_1, n_2, \ldots, n_r) = 1}$

1. consistent → if solution exists.
2. Inconsistent → if solution doesn't exist.

$N = n_1 \cdot n_2 \cdot n_3 \cdot \ldots n_r =$ [illegible]

$\boxed{N_1 = \frac{N}{n_1}}$ → shows that $\boxed{\gcd(N_1, n_1) = 1}$

Camlin | Page
Date / /

$\gcd(N_i, n_i) = 1 \Rightarrow \boxed{N_i m_i = 1 \bmod n_i}$

$\boxed{m_i = N_i^{-1}}$ ★

(or this can be calculated using Extended Euclidean Method.)

So,

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

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

Ex:- $x \equiv 2(3)$, $x \equiv 3(5)$, $x \equiv 2(7)$

$a_1 = 2, a_2 = 3, a_3 = 2$

$n_1 = 3, n_2 = 5, n_3 = 7$

$N = n_1 \cdot n_2 \cdot n_3 \Rightarrow 3 \cdot 5 \cdot 7 \Rightarrow 105$

$\boxed{N = 105}$

$N_1 = \frac{105}{3} = 35 \Rightarrow (35, 3) = 1$

$\Rightarrow 35 \cdot 2 \equiv 1(3)$ $\quad m_1 = 2$

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

$\Rightarrow 21 \cdot 1 \equiv 1(5)$ $\quad m_2 = 1$

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

$\Rightarrow 15 \cdot 1 = 1(7)$ $\quad m_3 = 1$

$$x = \left(\sum_{i=1}^{3} a_i N_i m_i\right) \bmod N \Rightarrow (a_1 N_1 m_1 + a_2 N_2 m_2 + a_3 N_3 m_3) \bmod N$$

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

$= 233 \bmod 105$

$x \Rightarrow 23 \bmod 105$

for multiple values of x,

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

Method-2 for previous Example (~~Euler's theorem~~)

$x \equiv 2(3)$ — ① $\Rightarrow 3 \mid (x-2)$ $\exists\ k \in \mathbb{Z}$

$x \equiv 3(5)$ — ②

$x \equiv 2(7)$ — ③

$\boxed{x = 2+3k}$ — ④

④ in ② $\quad x \equiv 3(5)$

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

$5 \mid (3k-1)$

$\Rightarrow 3k \equiv 1(5)$

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

NOTE: if they are not co-prime, then No solution exist, equations inconsistent

$(3,5)=1$

When these 2 values are co-prime we have a solution for this equation

multiply $(3)^{-1}$ w.r.t mod 5 on both sides

$\boxed{3^{-1} \text{ w.r.t mod } 5 = 2}$

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

$k \equiv 2(5)$

$\boxed{k = 2+5u,\ u \in \mathbb{Z}}$ — ⑤

Substitute ⑤ in ④

$x = 2+3k, \quad k = 2+5u$

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

$x = 2+6+15u$

$\boxed{x = 8+15u}$ — ⑥

Substitute ⑥ in ③

$x \equiv 2(7)$

$8+15u \equiv 2(7), \quad w \in \mathbb{Z}$

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

$\Rightarrow 7 \mid 6+15u$

$15u = -6(7)$

$15(7) \cdot u = (-6+7)(7)$

$u = 1(7)$

$\boxed{u = 1+7w}$ $w \in \mathbb{Z}$ — (7)

Substitute (7) in (6)

$x = 8+15u$

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

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

$\underline{x = 23 \bmod 105}$

Primality Test

$n \rightarrow$ check it is prime or not.

Euler's Theorem (ϕ) → (8)

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

obtained through Formatts little theorem,

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

if $n = p$, $a^{\phi(p)} \equiv 1(p)$ $\quad \phi(p) = p-1$

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

* (Euler's theorem → for composite numbers
Fermat's little theorem → for prime numbers)

Camlin Page
Date / /

Ex- $n = 15$ ∴ a composite number

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

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

$= 2 \cdot 4 = 8$

$\boxed{\phi(15) = 8}$

let $a = 2$,

so, $(2, 15) = 1$

$a^{\phi(n)} \equiv 1 (n)$

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

$\Rightarrow 2^4 (15) \cdot 2^4 (15) \equiv 1 (n)$

$1 \cdot 1 \equiv 1 (15)$

$\boxed{1 \equiv 1 (15)}$

Primality Test

* For primality test, we choose only odd numbers because '2' is only even prime number

$n \rightarrow$ prime or not ?

(deterministic algorithm) = (n) is prime with 100% confidence
(n) is not prime with 100% confidence

but all algorithms available are probabilistic.

prime (not 100% sure) ← → not prime (100% sure)

(1) Fermat's little theorem test:

Why primality test :- In any cryptography algorithm, when we need to choose a prime number, we select a number and check if that number is prime or not.

Camlin Page
Date / /

① Prime Root

To check if n is prime or not

Use Trial division method :-

$(2 \to \sqrt{n})$ range of numbers to check if they divide 'n' or not.

② Miller-Rabin Test :-

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

$\mathbb{Z}_n^* = \{0 < a < n : (a, n) = 1\}$ or { No. having multiplicative inverse w.r.t n

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

Charmichael number

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

[Smallest charmichael number = 561]

1. If 'n' is divisible by a perfect square >1, then 'n' is not a charmichael number.
2. If 'n' is square free, then 'n' is a charmichael number iff $p-1 \mid n-1$ for every prime $p \mid n$.

---

1. Choose n. ($\because$ n is odd)
2. $n-1 = 2^k \cdot m$
3. choose a, $(a, n) = 1$ $(1 < a < n-1)$
4. ~~$b_0 = a^m \bmod n$~~

Camlin Page
Date / /

4. $b_0 = a^m \pmod n$ → ± 1 → probable prime
$b_1 = b_0^2 \pmod n$ → -1 → probable prime
otherwise → composite

process continues

$b_{k-1} = b_{k-2}^2 \pmod n$ → -1 → probable prime
otherwise → composite.

generally, $b_i = (b_{i-1})^2 \bmod n \quad 0 \le i \le k-1$

Wilson's Method Theorem —

If p is prime, and it holds
$(p-1)! \equiv -1 \pmod p \Rightarrow p \mid (p-1)! + 1$

proof :-
∵ If p is prime,
$k^2 \equiv 1 \bmod p$ iff $k=1$ or $k=p-1$ ★
because $k \cdot k \Rightarrow$ inverse of k is k
only true when

$(p-1)! \pmod p = (1 \cdot 2 \cdot 3 \cdots (p-2)(p-1)) \bmod p$
$= (1 \cdot (\cdot)(\cdot) \cdots (\cdot)(p-1)) \bmod p$

$(2, 3, \cdots, (p-1))$ → have their inverse between $(2, (p-2))$

These are inverse of $(2, (p-2))$ but these are also $(2, (p-2))$

(proof of wilson theorem → study online)

Camlin | Page
Date / /

as $(a \cdot a^{-1}) \bmod p = 1$

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

$\Rightarrow -1 \bmod p.$

Try – CH10 → Ex-1,2,3,4 → important

Primitive Roots → $a \in Z_m$, $Z_m = \{0, 1, \cdots, m-1\}$

order of an element: $a^h \equiv e \pmod m$, +ve integer

↳ (identity w.r.t multiplication)

↳ by default 1.

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

1. If $a^h \equiv 1 \pmod m$ and $a^k \equiv 1 \pmod m$ such that $\boxed{k > h}$

so, then $h \mid k$

Ex: $m = 5$ $\quad Z_5^* = \{1, 2, 3, 4\}$

$1^1 = 1 \pmod 5$	$2^1 = 2 \pmod 5$	$3^1 = 3 \pmod 5$	$4^1 = 4 \pmod 5$
	$2^2 = 4 \pmod 5$	$3^2 = 4 \pmod 5$	$4^2 = 1 \pmod 5$
$\text{order}_5(1) = 1$	$2^3 = 3 \pmod 5$	$3^3 = 2 \pmod 5$	$\text{order}_5(4) = 2$
	$2^4 = 1 \pmod 5$	$3^4 = 1 \pmod 5$	
	$\text{ordre}_5(2) = 4$	$\text{order}_5(3) = 4$	

→ here {2,3} are primitive roots of 5.

So, we have $a^{\phi(m)} \equiv 1 \pmod m$, $(a, m) = 1$

If → this holds $\boxed{\text{order}_m(a) = h = \phi(m)}$ then it primitive root of element / generator of element.

So, No. of primitive roots of element 'm' is,

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

Ex → Z_{13}^{*} =