Divisibility & the Division Algorithm

'b divides a' if $a = mb$ [$b|a$]

Eg:- 13 divides 182 , $13|182$
-5 divides 30 , $-5|30$
17 divides 0 , $17|0$

Properties

↳ If $a|1$, then $a = \pm 1$
↳ If $a|b$ and $b|a$, then $a = \pm b$
↳ Any $b \neq 0$ divides 0
↳ If $a|b$ and $b|c$, then $a|c$
↳ If $b|g$ and $b|h$, then $b|(mg+nh)$ for arbitrary integers m & n.

Proof
If $b|g$, then $g = b * g_1$ for some integer g_1
If $b|h$, then $h = b * h_1$ " " " h_1

$$mg + nh = mbg_1 + nbh_1$$
$$= b * (mg_1 + nh_1)$$

$\therefore$ b divides $mg + nh$

Eg:- $b = 7$, $g = 14$, $h = 63$
$7|14$ and $7|63$
$\therefore 7 | 14m + 63n$ where $m = 3$, $n = 2$

$$14m + 63n$$
$$= 14 * 3 + 63 * 2$$
$$= 2*3[7 + 21]$$
$$= 7[6 + 18]$$

Division algorithm

If we divide positive int. 'a' by positive int. 'n'

quotient $= q$

remainder $= r$ ('residue')

$n \overline{)\, a \,(} q$
$\overline{\quad r \quad}$

$$\boxed{a = qn + r}$$

$$0 \leq r \leq n$$

$$q = \lfloor a/n \rfloor$$

$$qn \leq a$$

$$(q+1)n > a$$

The distⁿ from qn to a is r

Eg:- $a = 11$, $n = 7$
$q = 1$, $r = 4$

$11 = 7 * 1 + 4$

Eg:- $a = -11$, $n = 7$
$q = -2$, $r = 3$

$-11 = 7 * -2 + 3$

Euclidean Algorithm

↳ to determine (gcd) greatest common divisor
or (hcf) highest common factor

GCD: The largest ~~com~~ integer that divides both 'a' and 'b'
of 'a' & 'b'

$$\gcd(a, b) = \max[k, \text{ such that } k|a \text{ and } k|b]$$

GCD should be positive

$$\gcd(a,b) = \gcd(a,-b) = \gcd(-a,b) = \gcd(-a,-b)$$
$$= \gcd(|a|, |b|)$$

→ Because all non-zero integers divide 0,
∴ $\gcd(a,0) = |a|$

→ 'a' and 'b' are relatively prime if $\gcd(a,b)=1$

How to find GCD (a,b)?

Divide a by b

$b\overline{)a}(q_1$

$a = q_1 b + r_1 \quad 0<r_1<b$

$b = q_2 r_1 + r_2 \quad 0<r_2<r_1$

$r_1 = q_3 r_2 + r_3 \quad 0<r_3<r_2$

⋮

$r_1\overline{)b}(q_2$

$r_2\overline{)r_1}(q_3$

r_3

Euclidean algorithm

$r_{n-1} = q_{n+1} r_n + 0 \quad 0<r_n<r_{n-1}$

$GCD(a,b) = r_n$

Eg:- Find GCD of 326 and 16

$$
\begin{array}{l}
16\overline{)326}(20 \\
\quad 320 \\
\quad \overline{\quad 6\overline{)16}(2} \\
\qquad\quad 12 \\
\qquad\quad \overline{4\overline{)6}(1} \\
\qquad\qquad 4 \\
\qquad\qquad \overline{2\overline{)4}(2} \\
\qquad\qquad\quad 4 \\
\qquad\qquad\quad \overline{0}
\end{array}
$$

Ans :- 2

Modular Arithmetic

Two integers 'a' and 'b' are said to be congruent modulo n,

if $\boxed{(a \bmod n) = (b \bmod n)}$

This is written as

$a \equiv b \pmod{n}$

Eg :- $73 \equiv 4 \pmod{23}$

$21 \equiv -9 \pmod{10}$

Properties

↳ $a \equiv b \bmod n$

if $n \mid (a-b)$

↳ $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$

↳ $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$ implies $a \equiv c \pmod{n}$

Modular Arithmetic operations properties.

↳ $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$

↳ $[(a \bmod n) - (b \bmod n)] \bmod n = (a-b) \bmod n$

↳ $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Eg :- Find $11^7 \bmod 13$

$11^2 \bmod 13 = 121 \bmod 13 = 4$

$11^4 \bmod 13 = (11^2)^2 \bmod 13 = 4^2 \bmod 13 = 16 \bmod 13 = 3$

$11^7 = 11 \times 11^2 \times 11^4$

$11^7 \bmod 13 = (11 * 4 * 3) \bmod 13$

$= 132 \bmod 13$

$= 2$

$Z_n = \{0, 1, 2, \ldots, n-1\}$

Arithmetic Modulo 8.

Addition modulo 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Multiplication modulo 8

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Additive & Multiplicative inverse modulo 8.

w	$-w$	w^{-1}
0	0	–
1	7	1
2	6	–
3	5	3
4	4	–
5	3	5
6	2	–
7	1	7

Set of residues / residue classes (mod n)

$Z_n = \{0, 1, 2, \ldots (n-1)\}$

Residue classes (mod n) are $[0], [1], [2], \ldots, [n-1]$

where $[x] = \{a : a$ is an integer, $a \equiv x \pmod n\}$

Eg:- The residue classes (mod 4) are

$[0] = \{, \ldots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\}$

$[1] = \{, \ldots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\}$

$[2] = \{ \ldots, -14, -10, -6, -2, 2, 6, 10, 14, 18, \ldots\}$

$[3] = \{ \ldots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \ldots\}$

The smallest non-negative integer is used to represent the residue class.

Z_n is a commutative ring with a multiplicative identity element.

$$\boxed{\text{If } (a+b) \equiv (a+c) \bmod n \quad \text{then } b \equiv c \pmod n}$$

Eg:- $(5+23) \equiv (5+7) \bmod 8$

then $23 \equiv 7 \bmod 8$

Properties for modular arithmetic for integers in Z_n

- Commutative laws. $(w+x) \bmod n = (x+w) \bmod n$
  $(w*x) \bmod n = (x*w) \bmod n$
- Associative laws
- Distributive laws
- Identities $(0+w) \bmod n = w \bmod n$
  $(1*w) \bmod n = w \bmod n$
- Additive inverse For each $w \in Z_n$, there exists a z such that $w+z \equiv 0 \bmod n$

$$\boxed{\text{If } (a \times b) \equiv (a \times c) \bmod n \quad \text{then } b \equiv c \pmod n \quad \text{if } a \text{ is relatively prime to } n}$$

Two integers are relatively prime if their only common positive integer factor is 1

$$ab \equiv ac \bmod n$$

$$(a^{-1})ab \equiv (a^{-1})ac \bmod n$$

$$b \equiv c \bmod n$$

Eg:- 6 and 8 are not relatively prime $[\gcd(6,8) \neq 1]$

$6 \times 3 = 18 \equiv 2 \bmod 8$

$6 \times 7 = 42 \equiv 2 \bmod 8$

Yet $3 \not\equiv 7 \pmod 8$

With $a = 6$ and $n = 8$,

Z_8	0	1	2	3	4	5	6	7
Multiply by 6	0	6	12	18	24	30	36	42
Residues	0	6	4	2	0	6	4	2

∴ There is not a unique inverse to the multiply operation

With $a = 5$ and $n = 8$ $\gcd(5, 8) = 1$

Z_8	0	1	2	3	4	5	6	7
Multiply by 5	0	5	10	15	20	25	30	35
Residues	0	5	2	7	4	1	6	3

→ Integers 1, 3, 5 and 7 have a multiplicative inverse in Z_8, but 2, 4 and 6 do not.

Euclidean Algorithm Revisited

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

Eg:- $\gcd(55, 22) = \gcd(22, 55 \bmod 22)$
$= \gcd(22, 11) = 11$

~~Proof~~ :- ~~gcd(a,b)~~. ~~gcd(b, a mod b)~~

~~a = kb + r~~ ~~b = k'(a mod b) + r'~~

~~b = k br + r'~~

Extended Euclidean Algorithm (useful in RSA)

↳ not only it calculates the gcd 'd', but also 2 additional integers 'x' and 'y' that satisfy the following equation :-

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

Eg:- $\gcd(42, 30) = 6 = 42x + 30y$
$= 6(7x + 5y)$

$y \backslash x$	3	2	-1	0	1	2	3
3	-216	-174	-132	-90	-48	-6	36
2	186	-144	-102	-60	-18	24	66
-1	-156	-114	-72	-30	12	54	96
0	-126	-84	-42	0	42	84	126
1	-96	-54	-12	30	72	114	156
2	-66	-24	18	60	102	144	186
3	-36	6	48	90	132	174	216

$42x + 30y = 6(7x+5y)$ is a multiple of 6.

Note $\gcd(42,30) = 6$.

Eg:- Use $a = 1759$ and $b = 550$ and solve for $1759x + 550y = \gcd(1759, 550)$

i	r_i	q_i	x_i	y_i
-1	1759		1	0
0	550		0	1
1	109	3	1	-3
2	5	5	-5	16
3	4	21	106	-339
4	1	$\boxed{1}$	$\boxed{-111}$	$\boxed{355}$
5	$\boxed{0}$	4		

gcd   x   y

21
16
126
21
336
$-3-16\times21$
$-3-336$
339
16
355

$\gcd(1759,550) = 1 = 1759(-111) + 550(355)$

$550 \overline{)1759}(3$
1650
$109 \overline{)550}(5$
545
$5 \overline{)109}(21$
105
$4 \overline{)5}(1$
4
$1 \overline{)4}(4$
4
x

$$\begin{cases} x_n = x_{n-2} - q_n x_{n-1} \\ y_n = y_{n-2} - q_n y_{n-1} \end{cases}$$

Prime Numbers

An integer $p > 1$ is a prime no. if and only if its only divisors are ± 1 and $\pm p$.

Any integer 'a' can be factored in a unique way as :-

$$a = p_1^{a_1} \times p_2^{a_2} \times p_3^{a_3} \ldots \times p_t^{a_t}$$

where $p_1 < p_2 < p_3 \ldots < p_t$ are prime numbers and each a_i is a positive integer

---

Given, $a = \prod_{p \in P} p^{a_p}$ and $b = \prod_{p \in P} p^{b_p}$

If a/b then $a_p \leq b_p \ \forall p$

If $k = \gcd(a;b)$, then $k_p = \min(a_p, b_p) \ \forall p$

Eg :- $300 = 2^2 \times 3^1 \times 5^2$

$18 = 2^1 \times 3^2$

$\gcd(18, 300) = 2^1 \times 3^1 \times 5^0 = 6$

FERMAT'S THEOREM. (Imp. in public key cryptography)

p is prime.
a is positive integer not divisible by p

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

Eg :- $a = 7$, $p = 19$

$a^{p-1} = 7^{18}$

$7^2 \bmod 19 = 11$
$7^4 \bmod 19 = 121 \bmod 19 = 7$
$7^8 \bmod 19 = 49 \bmod 19 = 11$
$7^{16} \bmod 19 = 121 \bmod 19 = 7$
$\therefore 7^{18} \bmod 19 = (7 \times 11) \bmod 19 = 1$

$7^{18} \bmod 19 = 1$

$\therefore 7^{18} \equiv 1 \bmod 19$

$\therefore a^{p-1} = 1 \bmod p.$

Proof :-

$p : \{1, 2, \ldots\ldots p-1\}$

multiply each element by a and modulo p

$X = \{a \bmod p,\ 2a \bmod p, \ldots\ldots (p-1)a \bmod p\}$

None of the elements is 0 ~~beach~~ as p does not divide a

No two integers in X are equal.

$[\because\ ja \equiv ka \pmod p)$ where $1 \leq j < k \leq p-1$

gcd $(a, p) = 1$

So $j \equiv k \pmod p)$

This is impossible because j & k are both positive int. less than p. $j \neq k$

$[a \times 2a \times 3a \ldots\ldots \times (p-1)a]\ \cancel{\equiv} \bmod p$

$\Rightarrow [1 \times 2 \times 3 \times \ldots\ldots (p-1)] \bmod p$

$[a^{p-1} \cancel{(p-1)!}]\ \bmod p \Rightarrow [\cancel{(p-1)!}] \bmod p$

$(p-1)!$ is relatively prime to p.

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

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

Alternate form of Fermat's theorem

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

Eg:- $a = 3,\ p = 5$

$$\underbrace{\underbrace{\underbrace{\underbrace{3^2}_{4} * \underbrace{3^2}_{4}}_{16}}_{1} * \underbrace{3}_{3}}_{3} = 3^5 \equiv 3 \bmod 5$$

Euler's Totient function : $\phi(n)$

$\phi(n) \Rightarrow$ defined as the no. of positive integers less than n & relatively prime to n.

$\phi(37) = 36$ (All no.s 1 to 36 are relatively prime to 37, because 37 is prime no.)

$\phi(35) = 24$.

$\{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34\}$

For prime number (p),

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

Let 2 prime no.s p & q, $p \neq q$

$n = p \times q$

$$\phi(n) = \phi(p * q) = \phi(p) * \phi(q) = (p-1)(q-1)$$

Eg:- $\phi(21) = \phi(3) * \phi(7)$

$= 2 * 6$

$= 12$

Euler's Theorem

For every 'a' and 'n' that are relatively prime:

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

If n is prime,

$\phi(n) = (n-1)$ then $a^{\phi(n)} = a^{n-1} \equiv 1 \bmod (n)$

[$\because$ Fermats' theorem]

Let set of integers : $R = \{x_1, x_2, \ldots x_{\phi(n)}\}$

Each element x_i of R is a unique positive int less than n with $\gcd(x_i, n) = 1$

$S = \{(ax_1 \bmod n), (ax_2 \bmod n), \ldots (ax_{\phi(n)} \bmod n)\}$

S is a permutation of R because

→ Because ~~x~~ a is relatively prime to n
& x_i " " " n

∴ ax_i must also be relatively prime to n

Thus all members of S are ~~read~~ less than n, and that are relatively prime to n

→ There are no duplicates in S

$$\prod_{i=1}^{\phi(n)} (a x_i \bmod n) = \prod_{i=1}^{\phi(n)} x_i$$

$$\prod_{i=1}^{\phi(n)} a x_i \equiv \prod_{i=1}^{\phi(n)} x_i \pmod n$$

$$a^{\phi(n)} \left[\cancel{\prod_{i=1}^{\phi(n)} x_i} \right] \equiv \cancel{\prod_{i=1}^{\phi(n)} x_i} \pmod n$$

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

Euler's Theorem

Eg:- $a = 3, \quad n = 10$

$\phi(10) = 4 \qquad \{1, 3, 7, 9\}$

$a^{\phi(n)} = 3^4 = 81$

$81 \equiv 1 \bmod 10$

Alternate form of Euler's Theorem

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

Testing for primality

For many cryptographic algorithms, it is necessary to select one or more very large prime no.s at random. Thus, the task is :- determining whether a given large no. is prime.

Properties of Prime Numbers.

(1) p: prime

a is a +ve integer less than p,

then $a^2 \bmod p = 1$ iff $a \bmod p = 1$

or $a \bmod p = -1 \bmod p = p-1$

Proof:- $(a \bmod p)(a \bmod p) = a^2 \bmod p.$

for $a^2 \bmod p = 1$, either $a \bmod p = 1$

or $a \bmod p = -1$

Conversely, If $a^2 \bmod p = 1$, then $(a \bmod p)^2 = 1$

which is true only for

$a \bmod p = \pm 1$.

(2) p: prime no. > 2

$k > 0$, q: odd

then $p-1 = 2^k q$.

Let a: int, $1 < a < p-1$

Then one of the two conditions is true.

(a) $a^q \equiv 1 \bmod p$

(b) One of the numbers $a^q, a^{2q}, a^{4q}, \ldots a^{2^{k-1}q}$ is congruent to $-1 \bmod p$

There is some int j, $1 \leq j \leq k$ such that $a^{2^{j-1}q} \bmod p = -1 \bmod p = p-1$

or $a^{2^{j-1}q} \equiv -1 \bmod p$

Miller - Rabin test / Rabin - Miller test

If n is prime, then either the first element in the list of residues or remainders

$$(a^q, a^{2q}, a^{3q} \ldots a^{2^{k-1}q}, a^{2^k q}) \bmod n$$

equals 1

Or, some element in the list equals $(n-1)$

Otherwise, n is composite (not prime)

Eg:- $n = 2047 = 23 * 89$

then $n-1 = 2046$

$= 2 * 1023$

$2^{1023} \bmod 2047 = 1$

2047 meets the condition, but is not prime

TEST (n)

(1) Find int. k, q with $k > 0$, q: odd, so that

$n-1 = 2^k q$

(2) Select a random int a, $1 < a < n-1$

(3) if $a^q \bmod n = 1$, then return ("inconclusive")

(4) For $j = 0$ to $k-1$, do

(5) If $a^{2^j q} \bmod n = n-1$, then return ("inconclusive")

(6) return ("composite")

Eg:- test for $n = 29$ (prime)

$n-1 = 28 = 2^2 * 7 = 2^k \cdot q$ $\quad k = 2$, $q = 7$

let $a = 10$ (random)

$a^q \bmod n = 10^7 \bmod 29 = 17$

which is neither 1 nor $n-1$ 28

Next calculate $(10^7)^2 \bmod 29 = 28$.

Return "inconclusive"

$10 \bmod 29 = 10$
$10^2 \bmod 29 = 13$
$10^3 \bmod 29 = 14$
$10^4 \bmod 29 = 24$
$10^5 \bmod 29 = 8$
$10^6 \bmod 29 = 5$
$10^7 \bmod 29 = 11$

let $a = 2$. (random)

$2^q \bmod n$ $\qquad$ $2^{2q} \bmod n$

$2^7 \bmod 29 = 12$ $\qquad$ $2^{14} \bmod 29 = 28$

~~Redacon~~ Test for all $a \in [1, 28]$ we get same "inconclusive" result

Eg:- Test for $n = 221$ (composite)

$221 = 13 * 17$

$n - 1 = 220$. $= 2 * 110$
$= 2 * 2 * 55$
$= 2^2 . (55)$
$= 2^k . q$ $\qquad$ $k = 2$, $q = 55$

let $a = 5$.

$a^q \bmod n = 5^{55} \bmod 221 = 112$
$\neq 1$.
$\neq n-1\ (220)$

$5^{55.2} \bmod 221 = 168$

After checking all values of j, test returns composite.

Only for $a = 21, 47, 174, 200$.
test returns ("inconclusive")

For all other $a \in [1, 220]$, test returns "composite"

Miller's test

Repeatedly invoke $\overline{\text{TEST}(n)}$ using randomly chosen values for 'a'. If at any point, TEST returns composite, then 'n' is determined to be non-prime.

If TEST continues to return inconclusive for t tests, then for sufficiently large values of 't', assume that 'n' is prime.

Chinese Remainder Theorem (example)

used to solve a set of different congruent equations with one variable but different moduli which are relatively prime.

$$\left.\begin{array}{l} X \equiv a_1 \bmod m_1 \\ X \equiv a_2 \bmod m_2 \\ \vdots \\ X \equiv a_n \bmod m_n \end{array}\right\}$$

CRT states that the above eq^n has a unique solution ~~of the moduli~~ if $m_1, m_2 \ldots m_n$ are relatively prime.

$$\boxed{X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \ldots + a_n M_n M_n^{-1}) \bmod M}$$

Eg: 1 Solve the following equations using CRT

$X \equiv 2 \pmod 3$ $\quad a_1 = 2 \quad m_1 = 3$

$X \equiv 3 \pmod 5$ $\quad a_2 = 3 \quad m_2 = 5$

$X \equiv 2 \pmod 7$ $\quad a_3 = 2 \quad m_3 = 7$

Solution:

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$

unique soln exists because $(3, 5, 7)$ are relatively prime.
$\quad m_1, m_2, m_3$

$$M = m_1 \times m_2 \times m_3 = 3 \times 5 \times 7 = 105$$

$$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$$

$$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$$

$$M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$$

$M_1 * M_1^{-1} = 1 \bmod m_1$

$35 * M_1^{-1} = 1 \bmod 3$

$M_1^{-1} = 2$

$M_2 * M_2^{-1} = 1 \bmod m_2$

$21 * M_2^{-1} = 1 \bmod 5$

$M_2^{-1} = 1$

$M_3 * M_3^{-1} = 1 \bmod m_3$

$15 * M_3^{-1} = 1 \bmod 7$

$M_3^{-1} = 1$

$$X = \left(a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}\right) \bmod M$$

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

$$= (140 + 63 + 30) \bmod 105$$

$$= 233 \bmod 105$$

$$= 23$$

$23 \equiv 2 \bmod 3$

$23 \equiv 3 \bmod 5$

$23 \equiv 2 \bmod 7$