NUMBER THEORY

To study the properties of integers, more particularly the +ve integers or natural numbers.

The principle of well-ordering: Every non-empty set of S of non-negative integers contains a least element i.e an integer 'a' in S, such that $a \leq b$ $\forall$ b belonging to S

Ex: $S = \{1, 2, 3, 4 \ldots N\} = \mathbb{N}$

Ans. least element = 1.

$S = \mathbb{Z}$ does not have a least element.

bcz. range $= [-\infty, \infty]$

Archimedean Property: If a and b are any +ve integers, then $\exists$ a +ve integer n such that

$na \geq b$

Ex. If $a = 2$, $b = 7$

then $na \geq b$ will only be satisfied if $n = 4$

Proof:- Assume that the statement is false.

For some a and b,

$na < b$ for every +ve integer n.

Let $S = \{b - na \mid n \text{ is a +ve integer}\}$

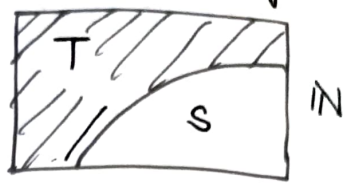
By well-ordering principle, S has a least element say $b - ma$

So $b - (m+1)a = b - ma - a < b - ma$. is not possible since we ~~co~~ stated that $b - ma$ is the least element and we found that another element

$b - ma - a$.

$\therefore$ The above assumption is false.

Principle of Finite induction: Let S be a Set of +ve integers with the following properties



a) Integer $1 \in S$

b) Whenever integer 'k' is in S, the next integer $k+1$ must also be in S

Then set S is the set of natural numbers.

Proof: Assume T is a set of +ve integers which is not in S.

Let's assume T is non-empty.

By well-ordering principle, T has a least element say 'a'

$\therefore 1 \in S \Rightarrow a > 1$ and so $0 < a-1 < a$

$\Rightarrow a - 1 \notin T$

$a - 1 \in S$

$\therefore (a-1) + 1 \in S = a \in S$. → This is a contradiction

$\therefore$ T is empty

$\therefore S = \mathbb{N}$

Ex: $B = \{n \in \mathbb{N} \mid n = -11 + 7m$ for some $m \in Z\}$

Find the least element of B.

Ans.

$B = \{-11, -4, -18, 3, -25, 10, -32, \ldots\}$

So the least element is 3.

Ex: $C = \{n \mid \mathbb{N} \mid n = x^2 - 8x + 12 \text{ for some } x \in \mathbb{Z}\}$

Find the least element of C

Ans. $n \in \mathbb{N}$

$\Rightarrow x^2 - 8x + 12 > 0$.

$\Rightarrow (x-6)(x-2) > 0$

$x \in (-\infty, 2) \cup (6, \infty)$

So $x = 1$, $n = 5$

$x = 7$, $n = 5$.

$\therefore$ 5 is the least element.

Definition: A set T of real numbers is said to be well-ordered if every non-empty subset of T has a least number.

$[0, 1]$ is not well-ordered because

$\mathbb{N}$ ✓ $\quad \mathbb{Z}$ ✗ $\quad \mathbb{Q}$ ✗ $\left[\begin{matrix} x \in \mathbb{Q} \\ x-1 \in \mathbb{Q} \end{matrix}\right]$

Ex: Assume

$\phi = T_1 \subsetneq T_2 \subsetneq R$.

Show that if T_2 is well ordered, then T_1 is also well ordered.

Ans: S is a non-empty subset of T_1

$S \subseteq T_1 \subsetneq T_2$

$\Rightarrow S \subseteq T_2$

$\therefore$ S has a least element

Division Algorithm:

Given two integers a & b with $a > 0$, then integers q & r such that

$$b = aq + r \qquad 0 \le r < a.$$

Given two integers a & b with $a \neq 0$, there exists integer q and r such that:

$$b = aq + r \qquad 0 \le r < |a|$$

Ex: Show by division algorithm, square of an odd integer is of the form $8k+1$ for some $k \in \mathbb{Z}$

Ans. n is any integer.

By division algorithm,

$$n = 4q + r \qquad 0 \le r < 4$$

Possible values = $4q, 4q+1, 4q+2, 4q+3$.

If n is odd = $4q+1, 4q+3$

If $n = 4q+1$

$$n^2 = (4q+1)^2 = 16q^2 + 8q + 1$$
$$= 8(2q^2 + q) + 1$$
$$= 8k + 1.$$

$$n = 4q + 3$$

$$n^2 = (4q+3)^2 = 16q^2 + 24q + 9$$
$$= 16q^2 + 24q + 1 + 8$$
$$= 8(2q^2 + 3q + 1) + 1$$
$$= 8k + 1.$$

Ex: Show that the expression $\frac{a(a^2+2)}{3}$ is an integer for all $a \geq 1$

Ans: By division algorithm,

$a = 3q + r \qquad 0 \leq r < 3$

So, $a = 3q+1, 3q+2, 3q$.

If $a = 3q \Rightarrow \frac{a(a^2+2)}{3} = \frac{3q(9q^2+2)}{3} = q(9q^2+2) \in \mathbb{Z}$

$a = 3q+1 \Rightarrow \frac{(3q+1)((3q+1)^2+2)}{3}$

$= \frac{(3q+1)[9q^2+1+6q+2]}{3}$

$= (3q+1) \cdot \cancel{3} \cdot \frac{(3q^2+2q+1)}{\cancel{3}} = (3q+1)(3q^2+2q+1) \in \mathbb{Z}$

$a = 3q+2$

$\Rightarrow \frac{(3q+2)[(3q+2)^2+2]}{3}$

$= \frac{(3q+2)}{3}[9q^2+6+12q]$

$= (3q+2)(3q^2+4q+2) \in \mathbb{Z}$.

Hence, proved.

Definition: a, b are two integers, $a \neq 0$

$\exists\ q$ & r such that

$b = aq + r \qquad 0 \leq r < |a|$

q is quotient, r is remainder

Define two binary operation 'div' and 'mod'

→ b div $a = q$

b mod $a = r$

Ex: Let n be an integer such that

n div $6 = q$ and n mod $6 = 4$

Determine the values of $(2n+5)$ div 6

& $(2n+5)$ mod 6.

Ans: $n = 6q + 4$

$\Rightarrow 2n = 12q + 8$

$(2n + 5) = (12q + 13)$.

$\Rightarrow 12q + 12 + 1 = 6(2q+2) + 1$

$\therefore (2n+5)$ div $6 = 2q + 2$

$(2n+5)$ mod $6 = 1$.

Ex: Today is Friday. which day of the week is a year from now.

Ans: No. of days - 365 days.

If Sun = 0

Mon = 1

⋮

Sat = 6.

So $365 + 5 = 7(q) + r$.

$\therefore q = 52$

$r = 6$.

$r = 6 \therefore$ Ans = Saturday.

Ex: Prove that among any three consecutive integers, one of them is a multiple of 3.

Ans: Let 3 consecutives integers are $n, n+1, n+2$.

$n = 3q + r \qquad 0 \le r < 3$

$\Rightarrow n = 3q, 3q+1, 3q+2$

① $n = 3q \rightarrow$ multiple of 3.

~~② $n+1 = 3q+1 \Rightarrow n \le 3q \rightarrow$ multiple of 3.~~

③ $n+2 \le 3$.

$n+1 = 3q+2$.

$n+1 = 3q+2 = 3(q+1) \rightarrow$ multiple of 3.

② $n = 3q+1$

$n+1 = 3q+2$

$n+2 = 3q+3 = 3(q+1) \rightarrow$ multiple of 3.

---

* a, b are two integers.

If $\exists\ q$ such that $b = aq$

then we say that a divides b

a is a divisor of b

or b is a multiple of a

or b is divisible by a.

$a \mid b \iff \exists q$ such that $b = aq$.

$a \nmid b$ (a does not divide b).

$= 3(0.1)\,[0.47000 + 3(1.$

Definition:

An integer $p > 1$ is prime if its +ve divisors are 1 and p itself.

Any integer greater than 1 but not prime is called composite i.e a +ve integer is composite if it has a divisor d that satisfies $1 < d < n$.

Greatest common Divisor (GCD)

Definition: Let a and b be given integers with atleast one of them different from zero. The GCD is the +ve integer d satisfying the following conditions.

a) $d \mid a$ & $d \mid b$

b) If $c \mid a$ & $c \mid b$ then $c \leq d$.

* $GCD(0, n) = |n|$.

Theorem: If a and b are integers such that $1 \leq a \leq b$.

If $b = aq + r$, where $0 \leq r < a$,

then $GCD(a, b) = GCD(a, r)$

Proof: Suppose $d = GCD(a, b)$ -①

$e = GCD(a, r)$ -②

From ①

$\Rightarrow d \mid a$, $d \mid b$

$\Rightarrow a = dx$ and $b = dy$ for some integer x and y.

$r = b - aq$

$= dy - dxq = d(y - xq)$ $\therefore$ d divides r.

$\Rightarrow$ d is a common divisor of a and r.

$\Rightarrow$ $d \leq e$ - (3)

Similarly,

$e = GCD(a, r) \Rightarrow a = eu$, $b = ev$ where u, v are some integers.

$b = aq + r$

$= euq + ev = e(uq + v)$

$\Rightarrow$ e is a common divisor $e \mid b$ and $e \mid a$.

e is the common divisor of b and a

$\Rightarrow$ $e \leq d$ - (4).

From (3) and (4),

$e = d$. Hence, proved.

Ex: gcd (997, 996)

Ans: gcd (997, 996)

= gcd (996, 997)

Now, $997 = 996 \times 1 + 1 \Rightarrow r = 1$

= gcd (996, 1) = 1.

Euclidean's Algorithm:

Let a and b are two +ve integers such that,

$1 \leq a \leq b$

Let $b = r_0$, $a = r_1$

According to Division algorithm :

$b = aq + r$

$\Rightarrow r_0 = r_1 q_1 + r_2 \quad ; \quad 0 \le r_2 < r_1 : \gcd(r_0, r_1) = \gcd(r_1, r_2)$

Similarly ;

$r_1 = r_2 q_2 + r_3 \quad ; \quad 0 \le r_3 < r_2 : \gcd(r_1, r_2) = \gcd(r_2, r_3)$

$r_2 = r_3 q_3 + r_4 \quad ; \quad 0 \le r_4 < r_3 : \gcd(r_2, r_3) = \gcd(r_3, r_4)$

$\vdots$

$r_{n-1} = r_n q_n + r_{n+1} \quad ; \quad 0 \le r_{n+1} < r_n : \gcd(r_{n-1}, r_n) = \gcd(r_n, r_{n+1})$

$r_n = r_{n+1} q_{n+1} + 0 : \gcd(r_n, r_{n+1}) = \gcd(r_{n+1}, 0)$

$= r_{n+1}$

Ans = Last non zero remainder is the G.C.D.

Ex. GCD (426, 246) = ?

Ans. $r_0 = 426, \quad r_1 = 246.$

→ $426 = 246 \times 1 + 180 \Rightarrow \gcd(246, 180)$

→ $246 = 180 \times 1 + 66 \Rightarrow \gcd(180, 66)$

→ $180 = 66 \times 2 + 48 \Rightarrow \gcd(66, 48)$

→ $66 = 48 \times 1 + 18 \Rightarrow \gcd(48, 18)$

→ $48 = 18 \times 2 + 12 \Rightarrow \gcd(18, 12)$

→ $18 = 12 \times 1 + 6 \Rightarrow \gcd(12, 6)$

→ $12 = 6 \times 2 + 0. \Rightarrow \gcd(6, 0)$

$\therefore$ G.C.D = 6.

Ex: GCD (530, 124) = ?

Ans. $530 = 124 \times 4 + 34 \Rightarrow \gcd(124, 34)$

$\rightarrow 124 = 34 \times 3 + 22 \Rightarrow \gcd(34, 22)$

$\rightarrow 34 = 22 \times 1 + 12 \Rightarrow \gcd(22, 12)$

$\rightarrow 22 = 12 \times 1 + 10 \Rightarrow \gcd(12, 10)$

$\rightarrow 12 = 10 \times 1 + 2 \Rightarrow \gcd(10, 2)$

$\rightarrow 10 = 2 \times 5 + 0 \Rightarrow \gcd(2, 0)$

$\therefore$ Ans. 2.

Theorem: For any non-zero integers a and b, there exists 's' and 't' such that

$\gcd(a, b) = as + bt.$

Corollary: Every linear combination of a and b is a multiple of gcd (a, b). Also every multiple of gcd (a, b) is a linear combination of a and b.

Proof:

Suppose $T = ax + by$ is a linear combination of a and b.

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

$\Rightarrow d \mid a$ and $d \mid b$.

$a = dn_1, \quad b = dn_2 \quad (n_1, n_2 \in \mathbb{Z})$

Substitute a and b in T,

$$T = dn_1 x + dn_2 y = d\underbrace{[n_1 x + n_2 y]}_{\text{Integer}}$$

$\Rightarrow d \mid T$

$\therefore T = d \cdot n$ Hence, proved.

Converse, proof:

$\exists$ s, t such that,

$\gcd(a, b) = as + bt$

$n \cdot \gcd(a, b) = n \cdot (as + bt)$

$= a(ns) + b(nt)$

$= ax_0 + by_0$ (where $x_0, y_0 \in \mathbb{Z}$)

Corollary: The GCD of 2 non-zero integers a and b is the smallest +ve integer among all their linear combinations.

Proof: $ax + by = n \cdot \gcd(a, b) = n \cdot d$.

If $n = 0, \pm 1, \pm 2, \ldots$

Set of all linear combinations of a & b =

$\{\ldots, -3d, -2d, -d, 0, d, 2d, 3d, \ldots\}$

Among these, $+d$ is the smallest +ve integers.

$\therefore$ d is the G.C.D.

Ex: G.C.D $(n, n+1) = 1$

Prove.

Ans: Using Euclidean Algorithm,

$n + 1 = 1 \cdot n + 1 \Rightarrow$ G.C.D $(1, n) = \underline{1}$

Using $ax + by$ proof:

$\Rightarrow a = n, \quad b = n+1$

$1(n+1) - 1(n) = 1$

$\Rightarrow d = \gcd(n, n+1)$

$\therefore d \mid 1 \quad \therefore d = 1.$

Definition: Two integers a and b such that $a, b \neq 0$ are said to be relatively prime if $G.C.D(a, b) = 1$.

Equivalent definition of G.C.D:

Let a, b are two integers such that $a, b \neq 0$. For a +ve integer d, $\gcd(a, b)$ iff

a) $d \mid a$ and $d \mid b$

b) If $\exists c$ such that $c \mid a$ and $c \mid b$ then $c \mid d$.

Proof: Lets assume $d = \gcd(a, b)$

$\Rightarrow d \mid a$ and $d \mid b$.

$\exists x, y$ such that $d = ax + by$

$\exists c$, such that $c \mid a$ and $c \mid b$

$\Rightarrow c \mid ax + by.$

$c \mid d$. Hence, proved.

Converse, proof:

$c \mid d \Rightarrow c \leq d.$

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

Ex. Prove that for $k > 0$, $GCD(ka, kb) = k \cdot GCD(a, b)$

Ans. Let $d = gcd(a, b)$

$d = ax + by.$

Let $f = gcd(u, v)$ where $(u = ka, v = kb)$

$f = kax_1 + kby$

$= k(ax + by) = k \cdot G \cdot C \cdot D(a, b)$

Hence, proved.

2.) $kb = kq_1 a + kr_1 \quad ; \quad 0 \le kr_1 \le a$

$ka = kq_2 r_1 + kr_2 \quad ; \quad 0 \le kr_2 < kr_1$

$\vdots$

$kr_{n-1} = kq_n r_n + kr_{n+1} \qquad 0 \le kr_{n+1} < kr_n$

$kr_n = kq_{n+1} r_{n+1} + 0.$

$\Rightarrow G \cdot C \cdot D(a, b) = r_{n+1}$

$G \cdot C \cdot D(ka, kb) = kr_{n+1} = k \cdot G \cdot C \cdot D(a, b).$

* For any $k \neq 0$, $G \cdot C \cdot D(ka, kb) = |k| \, G \cdot C \cdot D(a, b)$

Proof:

If $k > 0 \Rightarrow G \cdot C \cdot D(ka, kb) = |k| \, G \cdot C \cdot D(a, b)$

If $k < 0 \Rightarrow (-k) > 0$

$\Rightarrow G \cdot C \cdot D(-ka, -kb) = -k \, G \cdot C \cdot D(a, b)$

$= |k| \, G \cdot C \cdot D(a, b)$

Ex: Prove that,
if $\gcd(a, b) = 1$ then $\gcd(a+b, a-b)$ is either 1 or 2.

Ans: $(a+b) + (a-b) = 2a$

$(a+b) - (a-b) = 2b$

let's assume $G.C.D(a+b, a-b) = d$.

$\Rightarrow d \mid 2a$ and $d \mid 2b$.

$\Rightarrow d \mid \gcd(2a, 2b) \Rightarrow d \mid \gcd(a, b) \cdot 2 = d \mid 2$.

$\therefore d = 1, 2$.

Ex: Prove that,
if $\gcd(a, b) = 1$, then $\gcd(2a+b, a+2b) = 1$ or 3

Ans: $2(2a+b) - (a+2b) = 3a$.

$2(a+2b) - (2a+b) = 3b$.

$\Rightarrow d = \gcd(2a+b, a+2b)$

$\Rightarrow d \mid 3a$, $d \mid 3b$

$\Rightarrow d \mid 3$ $\therefore d = 1$ or 3.

Ex: For the pair (24, 84), find the linear combination that equals to their gcd.

Ans: Let $d = \gcd(24, 84) = 12$.

$84 = 24 \times 3 + 12$ $\quad \gcd(24, 12)$

$24 = 2 \times 12 + 0$ $\quad \gcd(12, 0) \therefore d = 12$.

From ①.

$12 = (84 - 3 \cdot 24)$

~~Another approach~~

Ex: Same question only 1380 and 3020.

Ans. Using Euclidean algo:

$3020 = 2 \cdot 1380 + 260 \quad -①$

$1380 = 5 \cdot 260 + 80 \quad -②$

$260 = 3 \cdot 80 + 20 \quad -③$

$80 = 4 \cdot 20 + 0. \quad -④$

③ $20 = 260 - 3 \cdot 80$

$= 260 - 3[1380 - 5 \cdot 260]$

$= 260 - 3[1380 - 5(3020 - 2 \cdot 1380)]$

$= 16 \cdot 260 - 3 \cdot 1380$

$= 16(3020 - 2 \cdot 1380) - 3 \cdot 1380$

$= 16 \cdot 3020 - 35 \cdot 1380.$

Theorem: If a and b are integers, not both zero. Then a & b are relatively prime iff ∃ integers x and y such that

$ax + by = 1.$

Ex: If G.C.D $(a, b) = d$ then, prove G.C.D $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

Ans. I. G.C.D $(a, b) = d$

$\Rightarrow \frac{1}{d}$ G.C.D $(a, b) = 1$

$\Rightarrow$ G.C.D $\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$ Hence, proved.

II. G.C.D $(a, b) = d$

$ax + by = d$

$\Rightarrow \left(\frac{a}{d}\right)x + \left(\frac{b}{d}\right)y = 1$

$\Rightarrow$ G.C.D $\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$

Ex: If $a|c$ and $b|c$ with gcd $(a, b) = 1$, then $ab|c$. Prove.

Ans. gcd $(a, b) = 1$. $a|c$ and $b|c$.

$\Rightarrow ax + by = 1 \quad -①$ $\quad c \neq cu$, $\quad b \neq cv$.

$\Rightarrow cux + cvy = 1 \Rightarrow a|1$, $b|1$

$c(ux + vy) = 1$

$ux + vy = \frac{1}{c}$

$\therefore$ G.C.D $(u, v) = \frac{1}{c}$.

Multiply by

$c = cax + cby$

$a|c \Rightarrow c = a \cdot a_1$

$b|c \Rightarrow c = b \cdot b_1$.

$\Rightarrow c = b \cdot b_1 x \cdot a + b \cdot a \cdot a_1 y$

$c = a \cdot b [b_1 x + a_1 y]$

$\Rightarrow ab|c$.

Euclid's Lemma:

If $ab|c$ with $\gcd(a, b) = 1$ then $a|c$.

Proof:

$\gcd(a, b) = 1$

$ax + by = 1$

$ab|c \Rightarrow c = ab(xy)$. $bc = au$

$\Rightarrow c = cax + cby$.

$c = cax + auy$

$c = a(cx + uy)$

$a|ac$ and $a|bc$ (given)

$a|acx + bcy = c$

$\therefore a|c$.

$\Rightarrow c|a$. Hence, proved.

L.C.M (Least Common Multiple)

The L.C.M of two non-zero integers a & b denoted by $LCM(a, b)$ is the +ve integer satisfying the following conditions.

i) $a|m$ and $b|m$

ii) If $a|c$ and $b|c$ with $c > 0 \therefore m \leq c$.

Theorem: For +ve integers a & b,

$G.C.D(a, b) \cdot LCM(a, b) = ab$.

Proof: Let's assume $\gcd(a, b) = d$.

$\exists\ x, y$ such that

$dx = a$
$dy = b$.
} where x and y are co-prime.

Assume $m = \frac{ab}{d}$

Aim: To prove m is the $lcm(a, b)$.

So,

$m = \frac{ab}{d} = a \cdot y \qquad \left(y = \frac{b}{d}\right)$

$m = b \cdot \frac{a}{d} = b \cdot x \qquad \left(y = \frac{a}{d}\right)$

$\therefore m$ is a common multiple of a and b.

Let's assume that there exist a c such that

$c = ax_0$
$c = by_0$

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

$\exists\ x_1, y_1$ such that,

$d = ax_1 + by_1$

So $\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax_1 + by_1)}{ab} = \frac{cx_1}{b} + \frac{cy_1}{a}$

$= x_0 y_1 + y_0 x_1 \in \mathbb{Z}$

$\frac{c}{m}$ = integer.

$\Rightarrow$ $a|c$ or $b|c$. or $m \leq c$.

$\therefore m = \text{lcm}(a,b)$

$\therefore m \cdot d = ab = \text{lcm}(a,b) \cdot \gcd(a,b) = ab$.

$\gcd(a,b) = 1$ iff $\text{lcm}(a,b) = ab$.

Prove that:

$\gcd(a,b) = \text{lcm}(a,b)$ if $a = \pm b$.

Proof: $\gcd(a,b) = \text{lcm}(a,b) = d$

$\Rightarrow d^2 = ab$. - ⓒ

$\because$ d is the gcd (a, b):

$a = dx$ - ①

$b = dy$. - ②

} Not required

d is the lcm (a, b):

$d = ax_1$ - ③

$d = by_1$ - ④

Substitute ② and ③ in ⓒ,

$a^2x_1^2y \neq ab$.

$ax_1^2 \neq b$

$d^2 = ab$	$d^2 = ab$
$a^2x_1^2 = ab$	$b^2y_1^2 = ab$
$x_1^2 = \frac{b}{a}$	$y_1^2 = \frac{a}{b}$.

$\Rightarrow x_1^2 y_1^2 = 1$

$\therefore x_1, y_1 = \pm 1$. $(1,1), (1,-1), (-1,1), (-1,-1)$

If $x_1, y_1 = (1,1)$

$d = a$, $d = b$ $\Rightarrow$ $a = b$.

If $x_1, y_1 = (1,-1)$

$d = a$, $d = -b$ $\therefore a = -b$.

If $x_1, y_1 = (-1,1)$

$d = -a$, $d = b$ $\therefore a = -b$

If $x_1, y_1 = (-1,-1)$

$d = -a$, $d = -b$ $\therefore -a = -b$ $\therefore a = b$.

Hence, proved.

Converse:

If $a = \pm b$

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

$\text{lcm}(a,b) = |a|$

Hence, proved.

Ex: If $a, b \in \mathbb{Z}$ and p is a prime such that $p|ab$ then either $p|a$ ~~and~~ or $p|b$.

Ans: If $p|a$ then nothing is to be proved.

Suppose $p \nmid a$ - ①

So $\gcd(p,q) = 1$ or p.

In case ① $\gcd(p,a) = 1$.

and $p|ab \Rightarrow p|b$ (By Euclid's lemma)

If

$p|a_1, a_2, a_3, \ldots a_n$ p: prime

$\Rightarrow p|a_1$ or $p|a_2$ or .... or $p|a_n$.

Ex: Prove that $\sqrt{2}$ is irrational.

Ans: Lets assume $\sqrt{2}$ is rational

$\Rightarrow \sqrt{2} = \frac{p}{q}$ (where $p, q \in \mathbb{Z}$ and $q \neq 0$.)
relatively prime

$\Rightarrow 2 = \frac{p^2}{q^2}$

$\Rightarrow q^2 = \frac{p^2}{2}. \Rightarrow p^2 = 2q^2$ - ①

$\Rightarrow 2 | p^2 \Rightarrow 2 | p$ - ③

$p = 2m.$ - ②

Substitute ② in ①

$(2m)^2 = 2q^2$

$\Rightarrow q^2 = 2m^2$

$\Rightarrow 2 | q^2$

$\Rightarrow 2 | q.$ - ④

From ③, ④,

It proves that 2 is a common divisor of p & q but it contradicts the fact that p and q are relatively prime

∴ Our assumption is wrong ∴ $\sqrt{2}$ is irrational

Diophantine Equation:

An equation with one or more variables that is to be solved in the integers.

E.g $ax + by = c$

↳ Linear diophantine equations with two unknowns

$ax + by = c$ admits a solution iff $d | c$ where $d = gcd(a, b)$

Proof: Let assume $\exists\ x_0, y_0$ s.t

$ax_0 + by_0 = c$

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

$a = dx, \quad b = dy.$ - ①

Substitute ① in $ax_0 + by_0 = c$

$\Rightarrow dxx_0 + byy_0 = c$

$d(xx_0 + yy_0) = c$

$\Rightarrow d | c.$

Let assume that $d | c$

$c = dt$

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

$\exists\ x, y$ s.t

$d = ax_1 + by_1$

$dt = ax_1t + by_1t$

$\Rightarrow c = a(x_1t) + b(y_1t)$

∴ This has a solution x_1t and y_1t.

Theorem: If x_0, y_0 is any particular solution of eq. ① then all other solutions are given by:

$$x = x_0 + \left(\frac{b}{d}\right)t \qquad y_0 = y_0 - \left(\frac{a}{d}\right)t.$$

where 't' is any arbitary integer.

$d = \gcd(a, b)$

Ex: Find the solutions if exist.

$$172x + 20y = 1000$$

Ans. GCD:

$$172 = 20 \times 8 + 12$$

$$20 = 12 \times 1 + 8$$

$$12 = 8 \times 1 + 4$$

$$8 = (4) \times 2 + 0$$

$G.C.D(172, 20) = 4$

$\because$ $G.C.D(172, 20) \mid 1000 \Rightarrow$ Solution exists i.e (4)

$$12 = 8 \times 1 + 4.$$

$$\Rightarrow 4 = 12 - 8 \times 1$$

$$= 12 - (20 - 12 \cdot 1)$$

$$= 2 \cdot 12 - 20$$

$$= 2(172 - 20 \cdot 8) - 20$$

$$4 = 2 \cdot 172 - 17 \cdot 20. \quad - ③$$

$250 \times ③$

$$= 1000 = \boxed{500} \cdot 172 - \boxed{4250} \cdot 20.$$

$\therefore x_0 = 500, \quad y_0 = -4250.$

$$x = x_0 + \left(\frac{b}{d}\right)t \qquad y = y_0 - \left(\frac{a}{d}\right)t$$

$$= 500 + \left(\frac{172}{4}\frac{20}{}\right)t \qquad = -4250 - \left(\frac{172}{4}\right)t$$

$$= 500 + 4t \qquad = -4250 - 43t.$$

Ex: check the solvability & solve (if solution exists)

$$18x + 5y = 48.$$

Ans. GCD (18, 5)

$$18 = 5 \times 3 + 3$$

$$5 = 3 \times 1 + 2$$

$$3 = 2 \times 1 + 1$$

$$2 = 1 \times 2 + 0$$

$GCD(18, 5) = 1 \mid 48 \quad \therefore$ Solution exists.

$$\Rightarrow 1 = 3 - 2 \times 1$$

$$= 3 - (5 - 3)$$

$$= 2 \cdot 3 - 5$$

$$= (18 - 5 \cdot 3)2 - 5$$

$$1 = 2 \cdot 18 - 7 \cdot 5$$

$\therefore x_0 = 2, \quad y_0 = -7$

$$\Rightarrow 48 = 96 \times 18 - 336 \times 5.$$

$x_0 = 96, \quad y_0 = -336.$

$\therefore x = 96 + 5t \qquad y = -336 - 18t.$

Theorem:

Fundamental Theorem of Arithmetic

Given any integer $n \geq 2$, there exists primes $p_1 \leq p_2 \leq \cdots \leq p_s$ such that $n = p_1 p_2 p_3 \cdots p_s$.

Furthermore this factorization is unique in the sense that if $n = q_1 q_2 \cdots q_t$ for some primes $q_1 \leq q_2 \leq \cdots \leq q_t$, then $t = s$ & $q_i = p_i$ for $i = 1, 2, \cdots, t$.

There are infinitely many prime numbers. Prove it.

Ans. Assume that there are finite number of primes:

say $p_1, p_2, p_3, \cdots, p_n$.

Assume:

$x = (p_1 p_2 \cdots p_n) + 1$

$\therefore x \neq p_i$ for all $i = 1, 2, \cdots, n$.

$\therefore x$ = Composite number

$\therefore$ There exists a prime p_k divides x (by Fundamental Theorem of Arithmetic)

$\Rightarrow x = p_k q$

$1 = x - p_1 p_2 \cdots p_n$

$= p_k q - p_1 p_2 \cdots p_n$

$= p_k [q - p_1 p_2 \cdots p_{k-1} p_{k+1} \cdots p_n]$

$\Rightarrow p_k \mid 1$ This is a contradiction $\because p_k \geq 1 \Rightarrow$ It cannot divide 1.

$\therefore$ Assumption is wrong.

All integers $n \geq 2$ can be uniquely expressed in the form $n = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ for some distinct primes p_i and +ve integers e_i.

If $a = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ and

$b = p_1^{f_1} p_2^{f_2} \cdots p_t^{f_t}$ for some distinct primes p_i & $e_i, f_i \geq 0$.

$\Rightarrow \gcd(a, b) = p_1^{\min(e_1, f_1)} \cdot p_2^{\min(e_2, f_2)} \cdots p_t^{\min(e_t, f_t)}$

$\text{lcm}^{(a,b)} = p_1^{\max(e_1, f_1)} \cdot p_2^{\max(e_2, f_2)} \cdots p_t^{\max(e_t, f_t)}$

Ex: Find GCD and LCM of 12300 and 34128 using prime factorization.

Ans.

2	12300
2	6150
5	3075
5	615
3	123
41	41
	1

$= 2^2 \cdot 5^2 \cdot 3 \cdot 41$

2	34128
2	17064
2	8532
2	4266
3	2133
3	711
3	237
	79

$= 2^4 \cdot 3^3 \cdot 79.$

$\therefore$ H.C.F $= 2^2 \cdot 3^1 \cdot 5^0 \cdot 41^0 \cdot 79^0 = 12.$

L.C.M $= 2^4 \cdot 3^3 \cdot 41 \cdot 5^2 \cdot 79 =$

Ex: Prove, any prime of the form $(3n+1)$ is also the form $(6m+1)$

Ans. Let $(3n+1)$ is a prime number where $n \in \mathbb{Z}$

Now $n = 2m$ or $2m+1$

If $n = 2m$, $p = 3m + 1 = (6m + 1)$ ✓

$n = 2m+1$, $p = 6m + 3 + 1 = (6m + 4) = 2(3m+2)$ ✗

$n = 2m$ is valid.

Ex: Each integer of the form $(3n+2)$ has a prime factor of this form.

Ans: **Proof:**

Let's assume the prime factors of an integer is not in the form $(3n+2)$.

So, the prime factors are of $3n$, or $(3n+1)$

only prime of form $3n = 3$.

Integer : $p_1 p_2 \cdots p_n$

where $p_i = 3$ or $(3n+1)$

If $p_i = 3$ for any i

Integer = $3K$.

If $p_i = (3n+1)$ for all i

$$\text{Integer} = (3n_1+1)(3n_2+1)\cdots(3n_k+1)$$

$$= [9n_1n_2 + 3n_1 + 3n_2 + 1](3n_3+1)\cdots(3n_k+1)$$

$$= [3[3n_1n_2 + n_1 + n_2] + 1](3n_3+1)\cdots(3n_k+1)$$

$$= (3K+1)$$

$\Rightarrow$ If prime factor is of $(3n+2)$ form then the integer will be of $(3n+2)$ form. Hence, proved.

Ex: Prove the only prime of the form (n^3-1) is 7

Ans: $(n^3-1) = (n-1)(n^2+n+1)$

Since n^3-1 is prime

$\Rightarrow n-1 = \pm 1$ or $(n^2+n+1) = \pm 1$

If $n-1 = 1$ $\quad$ $n-1 = -1$

$n = 2$ $\quad$ $n = 0$.

If $n^2+n+1 = 1$ $\quad$ $n^2+n+1 = -1$

$n^2+n = 0$ $\quad$ $n^2+n+2 = 0$ ✗

$n = 0, n = -1$

$\therefore$ Possible values = $0, -1, 2$.

If $n = 0$, $n^3-1 = -1$ ✗

$n = 2$, $n^3-1 = 7$ ✓.

$n = -1$, $-1-1 = -2$ ✗

Ex: The only prime p for which $(3p+1)$ is a perfect square is 5.

Ans: $(3p+1) = n^2$

$$3p = n^2 - 1$$

$$p = \frac{n^2-1}{3}$$

p is prime, so, it is divisible by 1 and p itself.

$$\frac{n^2-1}{3} = 1 \Rightarrow \frac{(n+1)(n-1)}{3}$$

$\Rightarrow n^2 - 4 \neq 0$

$(n+2)(n-2) = 0$

$\Rightarrow$ Either $\frac{n+1}{3} = 1$ or $\frac{n+1}{3} = -1$

$n = 2$ $\quad$ $n = -4$.

$\frac{n-1}{3} = 1$ $\quad$ $\frac{n-1}{2} = -1$

$n = 4$ $\quad$ $n = -2$.

$n = 2, 4, -2, -4$

$p = \frac{n^2-1}{3}$

For $n = 2$, $p = \frac{4-1}{3} = \frac{3}{3}$

$n = 4$, $p = \frac{16-1}{3} = \frac{15}{3}$

$n = -2$, $p = \frac{4-1}{3} = -3$

$n = -4$, $p = -\frac{16-1}{3} = -6$

For $p = \frac{n^2-1}{3}$

$n = 2$, $p = \frac{4-1}{3} = 1$

$n = 4$, $p = \frac{16-1}{3} = 5$. ✓

$n = -4$, $p = \frac{16-1}{3} = 5$ ✓

$n = -2$, $p = \frac{4-1}{3} = 1$

Ex: The only prime of the form $n^2 - 4$ is 5.

Ans: $n^2 - 4 = (n+2)(n-2)$

Either $n + 2 = 1$ | $n + 2 = -1$

$n = -1$ | $n = -3$

$n - 2 = 1$ | $n - 2 = -1$

$n = 3$ | $n = 1$

$n = \pm 1, \pm 3$.

For $n = \pm 1$, Ans $= -3$

$n = \pm 3$, Ans $= 5$.

Ex: Every integer of the form $n^4 + 4$ with $n > 1$ is composite.

Ans: Let the integer of the form $n^4 + 4$ is prime

$n^4 + 4 = n^4 + 4 + 16 - 6$

$= (n^4 + 16) + 20$

$= (n^2 + 2)^2 - 2 \times n^2 \times 2$

$n^4 + 4 = (n^2 + 2)^2 - 4n^2$

$= (n^2 + 2 + 2n)(n^2 + 2 - 2n)$

Either $n^2 + 2n + 2 = 1$ | $n^2 + 2n + 2 = -1$

$n^2 + 2n + 1 = 0$ | $n^2 + 2n + 3 = 0$.

$(n+1)^2 = 0$ | X.

$n = -1$

$n^2 + 2n + 2 = 1$ | $n^2 + 2n + 2 = -1$

$n^2 + 2n + 1 = 0$

$(n+3)(n-1) = 0$

$n = 1, -3$.

$(n+1)^2 = 0$

$n = -1$

If $n^2 - 2n + 2 = 1$ | $n^2 - 2n + 2 = -1$

$n^2 - 2n + 1 = 0$ | $n^2 - 2n + 3 = 0$

$n = 1$ | X No integer

$\therefore n = 1, -1,$

But $n > 1$ so, these values are not possible

$\therefore$ Our assumption is false.

$\therefore n^4 + 4$ is composite.

Congruence:

Definition: Let $n \geq 2$ be a fixed integer. We say the two integers m_1 & m_2 are congruent modulo n denoted by

$$m_1 \equiv m_2 \pmod{n}$$

If and only if $n \mid (m_1 - m_2)$.

Ex: $3n \equiv 0 \pmod 3$

$3n+1 \equiv 1 \pmod 3$

$3n+2 \equiv 2 \pmod 3$.

Ex: If $n = 4$

Ans: $4n \equiv 0 \pmod 4$

$4n+1 \equiv 1 \pmod 4$

$4n+2 \equiv 2 \pmod 4$

$4n+3 \equiv 3 \pmod 4$

Ex: Find the smallest +ve integer m such that:

$$2370 \equiv m \pmod{11}$$

Ans: $m = 5$

$\therefore 2370 \equiv 5 \pmod{11}$

Theorem: Let $n \geq 2$ be a fixed integer. For any two integer m_1 & m_2,

$m_1 \equiv m_2 \pmod n$ iff $m_1 \bmod n \equiv m_2 \bmod n$

($m_1 \bmod n$: Remainder; $m_2 \bmod n$: Remainder.)

Proof:

Let $m_1 \equiv m_2 \pmod n$

$\Rightarrow n \mid m_1 - m_2$

$m_1 - m_2 = nq$. — ①

Assume $m_1 \bmod n = r_1$

$m_2 \bmod n = r_2$

$\Rightarrow m_1 = nq_1 + r_1 \qquad 0 \leq r_1 < n$

$\Rightarrow m_2 = nq_2 + r_2 . \qquad 0 \leq r_2 < n .$

Substitute m_1, m_2 in ①

$\Rightarrow nq_1 + r_1 - nq_2 - r_2 = nq .$

$(r_1 - r_2) + n(q_1 - q_2) = nq$

$= (r_1 - r_2) = n[q - q_1 + q_2]$

$\Rightarrow n \mid (r_1 - r_2)$

$r_1 - r_2 = 0$ only when $r_1 - r_2 = 0 \therefore r_1 = r_2 .$

$\Rightarrow m_1 \bmod n = m_2 \bmod n .$

Conversely:

$m_1 \bmod n = m_2 \bmod n = r$

$m_1 = q_1 n + r$

$m_2 = q_2 n + r$

$\Rightarrow m_1 - m_2 = n(q_1 - q_2)$

$\Rightarrow n \mid (m_1 - m_2)$

$m_1 \equiv m_2 \pmod n .$

Eg: $m_1 = 42$

$m_2 = 18$

$42 \equiv 18 \pmod 4$ iff $42 \bmod 4 = 2 = 18 \bmod 4 .$

$n \geq 2$

If $a \equiv b \pmod n$ & $c \equiv d \pmod n$

then

$a + c \equiv b + d \pmod n$

$ac \equiv bd \pmod n$

Proof: $a \equiv b \pmod n$ $\quad$ $c \equiv d \pmod n$

$\Rightarrow n \mid (a - b)$ $\quad$ $n \mid (c - d)$

$\Rightarrow nq_1 = (a - b)$ $\quad$ $nq_2 = (c - d)$

Adding them: $n(q_1 + q_2) = (a + c) - (b + d)$

$\Rightarrow n \mid (a + c) - (b + d)$

$= (a + c) \equiv (b + d) \bmod n$.

Multiply them

$$\begin{array}{r} cnq_1 = ac - bc \\ bnq_2 = bc - bd \\ + \\ \hline n(cq_1 + bq_2) = ac - bd \end{array}$$

$\Rightarrow n \mid ac - bd$

$\therefore ac \equiv bd \bmod (n)$

$a = b + nq_1$

$c = d + nq_2$

$\Rightarrow ac = (b + nq_1)(d + nq_2)$

$ac = bd + n(\quad)$

$\Rightarrow ac - bd = n(\quad)$

$\Rightarrow n \mid ac - bd$

$\therefore ac \equiv bd$

Ex: Find the smallest +ve integer m such that

$37^2 \cdot 41 - 53 \cdot 2 \equiv m \pmod 7$

Ans: $37 \equiv 2 \pmod 7$ $\quad -①$

$41 \equiv 6 \pmod 7$ $\quad -②$

$53 \equiv 4 \pmod 7$ $\quad -③$

$2 \equiv 2 \pmod 7$ $\quad -④$

$①^2 \cdot ② - ③ \cdot ④$

$\Rightarrow 37^2 \cdot 41 - 53 \cdot 2 \equiv 2^2 \cdot 6 - 4 \cdot 2 \pmod 7$

$\equiv (24 - 8) \pmod 7$

$\equiv 16 \pmod 7 \equiv 2 \pmod 7$

$\therefore m = 16 \cdot 2$

Ex: Evaluate:

$56^3 \cdot 22 \cdot 17 - 35 \cdot 481 \equiv m \pmod 9$

Ans: $56 \equiv 2 \pmod 9$

$22 \equiv 4$ "

$17 \equiv 8$ "

$35 \equiv 8$ "

$481 \equiv 4$ "

$\Rightarrow 2^3 \cdot 4 \cdot 8 - 8 \cdot 4 \equiv 256 - 32 = 224 \equiv 8 \pmod 9$

Ans: $\underline{8} \pmod 9$