**SHRI GOVIND GURU UNIVERSITY**
**B.Sc.Sem-5 Material**
**BSCSE506:Mathematics(Theory)**
**Number Theory(E.C)**

## Unit-I

**Unit-I:** Some Preliminary Consideration: Well-Ordering Principle, Mathematical Induction, the Binomial Theorem & binomial coefficients.
Divisibility Theory: the division algorithm, divisor, remainder, prime, relatively prime, the greatest common divisor, the Euclidean algorithm (Without proof), the least common multiple, the linear Diophantine equation & its solution.

# 1 Some Preliminary Consideration

**Well-Ordering Principle :-** Every non-empty set $S$ of non-negative integers contains a least element; That is there is some integer $a$ in $S$ such that $a \leqslant b$ for all $b$ belonging to $S$.

**Theorem 1** *State and Prove First Principal of Mathematical Induction*
***Statement :-*** *Let $S$ be a set of positive integers with the following properties:*

*(a) The integer 1 belongs to $S$.*

*(b) Whenever the integer $k$ in $S$, the next integer $k+1$ must also be in $S$.*

*Then $S$ is the set of all positive integers.*

***Proof:-*** *Let $T$ be the set of all positive integers not in $S$, and assume that $T$ is non-empty.*
*The Well-Ordering Principle tells us that $T$ possesses a least element, which we denote by $a$.*
*Because 1 is in $S$, certainly $a > 1$, and so $0 < a - 1 < a$.*
*The choice of $a$ is the smallest positive integer in $T$ implies that $a - 1$ is not a member of $T$, or equivalently that $a - 1$ belongs to $S$.*
*By hypothesis, $S$ must also contain $(a-1)+1 = a$, which contradicts the fact that $a$ lies in $T$.*
*We conclude that the set $T$ is empty and in consequence that $S$ contains all the positive integers.*

**Example 1** *Prove That*

$$1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

***Solution:-*** *Here we use principle of Mathematical induction to establish the formula.*

$$p(n) : 1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6} \tag{1}$$

*First we check for* $n = 1$

$$\begin{aligned} L.H.S. &= p(1) = 1^2 = 1 \\ R.H.S. &= \frac{n(n+1)(2n+1)}{6} \\ &= \frac{1(1+1)(2(1)+1)}{6} \\ &= \frac{(1)(2)(3)}{6} \\ &= \frac{6}{6} \\ &= 1 \\ \therefore\ L.H.S. &= R.H.S. \end{aligned}$$

*so, equation (1) is true for* $n = 1$
*Now. we check for* $n = 2$

$$\begin{aligned} L.H.S. &= p(1) = 1^2 + 2^2 = 5 \\ R.H.S. &= \frac{n(n+1)(2n+1)}{6} \\ &= \frac{2(2+1)(2(2)+1)}{6} \\ &= \frac{(2)(3)(5)}{6} \\ &= \frac{30}{6} \\ &= 5 \\ \therefore\ L.H.S. &= R.H.S. \end{aligned}$$

*so, equation (1) is true for* $n = 2$
*Now, suppose equation (1) is true for* $n = k$ *where* $k \in \mathbb{N}$.

$$p(k) : 1^2 + 2^2 + 3^2 + \ldots + k^2 = \frac{k(k+1)(2k+1)}{6} \tag{2}$$

*and we have to show that equation (1) is true for* $n = k + 1$.
*To obtain that sum of the first* $k + 1$ *squares we add the next one* $(k + 1)^2$ *to both side of equation (2).*
*This gives*

$$\begin{aligned} 1^2 + 2^2 + 3^2 + \ldots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\ &= (k+1)\left[\frac{k(2k+1)}{6} + (k+1)\right] \\ &= (k+1)\left[\frac{k(2k+1)+6(k+1)}{6}\right] \\ &= (k+1)\left[\frac{2k^2+k+6k+6}{6}\right] \\ &= (k+1)\left[\frac{2k^2+7k+6}{6}\right] \end{aligned}$$

$$1^2+2^2+3^2+\ldots+k^2+(k+1)^2=(k+1)\left[\frac{(k+2)(2k+3)}{6}\right]$$
$$=\left[\frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}\right]$$

*So, the equation is true for* $n=k+1$
$p(k)$ *is true* $\Rightarrow p(k+1)$ *is true.*
*By principle of mathematical induction our result is true for* $\forall\ n\in\mathbb{N}$.
*Hence,*

$$1^2+2^2+3^2+\ldots+n^2=\frac{n(n+1)(2n+1)}{6}$$

**Theorem 2** *State and Prove Binomial Theorem*
***Statement:-***

$$(a+b)^n=\binom{n}{0}a^n+\binom{n}{1}a^{n-1}b+\binom{n}{2}a^{n-2}b^2+\ldots+\binom{n}{n-1}ab^{n-1}+\binom{n}{n}b^n$$

***Proof:-*** *We use the principle of mathematical induction to establish this formula*

$$(a+b)^n=\binom{n}{0}a^n+\binom{n}{1}a^{n-1}b+\binom{n}{2}a^{n-2}b^2+\ldots+\binom{n}{n-1}ab^{n-1}+\binom{n}{n}b^n \tag{3}$$

*First we check this formula is true for* $n=1$

$$L.H.S.=(a+b)^1=(a+b)$$
$$R.H.S.=\binom{1}{0}a^1+\binom{1}{1}a^{1-1}b^1$$
$$=(a+b)$$

*so result is true for* $n=1$
*Now, suppose this equation (3) is true for* $n=m$

$$(a+b)^m=\binom{m}{0}a^m+\binom{m}{1}a^{m-1}b+\binom{m}{2}a^{m-2}b^2+\ldots+\binom{m}{m-1}ab^{m-1}+\binom{m}{m}b^m \tag{4}$$

*we have to prove that equation (3) is true for* $n=m+1$
*multiply both side of equation (4) by* $(a+b)$

$$\begin{aligned}(a+b)^m(a+b)&=\left[\binom{m}{0}a^m+\binom{m}{1}a^{m-1}b+\binom{m}{2}a^{m-2}b^2+\ldots+\binom{m}{m-1}ab^{m-1}+\binom{m}{m}b^m\right](a+b)\\
&=\binom{m}{0}a^{m+1}+\binom{m}{1}a^mb+\binom{m}{2}a^{m-1}b^2+\ldots+\binom{m}{m-1}a^2b^{m-1}+\binom{m}{m}ab^m+\\
&\binom{m}{0}a^mb+\binom{m}{1}a^mb^2+\binom{m}{2}a^{m-1}b^3+\ldots+\binom{m}{m-1}a^2b^m+\binom{m}{m}b^{m+1}\\
&=\binom{m+1}{0}a^{m+1}+\binom{m}{1}a^mb+\binom{m}{2}a^{m-1}b^2+\ldots+\binom{m}{m-1}a^2b^{m-1}+\binom{m}{m}ab^m+\\
&\binom{m}{0}a^mb+\binom{m}{1}a^mb^2+\binom{m}{2}a^{m-1}b^3+\ldots+\binom{m}{m-1}a^2b^m+\binom{m+1}{m+1}b^{m+1}\end{aligned}$$

$$\left[\because\ \tbinom{m}{m}=\tbinom{m+1}{m+1}=1,\tbinom{m}{0}=\tbinom{m+1}{0}=1\right]$$

$$(a+b)^{m+1} = \binom{m+1}{0}a^{m+1} + \left[\binom{m}{1} + \binom{m}{0}\right]a^m b + \left[\binom{m}{2} + \binom{m}{1}\right]a^{m-1}b^2 +$$
$$\left[\binom{m}{3} + \binom{m}{2}\right]a^{m-2}b^3 + \ldots + \left[\binom{m}{m} + \binom{m}{m-1}\right]ab^m + \binom{m+1}{m+1}b^{m+1}$$

*from Pascal's Rule*

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$$

$$(a+b)^{m+1} = \binom{m+1}{0}a^{m+1} + \binom{m+1}{1}a^m b + \binom{m+1}{2}a^{m-1}b^2 + \ldots + \binom{m+1}{m}ab^m + \binom{m+1}{m+1}b^{m+1}$$

*so, the formula is true for* $n = m+1$
*By Principle of mathematical induction we establish binomial theorem*

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n$$

**Example 2** *Show that*

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n} = 2^n$$

***Solution:-*** *The Binomial theorem is*

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n}b^n$$

*Put* $a = b = 1$ *in above equation*
*we get*

$$(1+1)^n = \binom{n}{0}(1)^n + \binom{n}{1}(1)^{n-1}1 + \binom{n}{2}(1)^{n-2}1^2 + \ldots + \binom{n}{n}(1)^n$$
$$2^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n}$$

**Example 3** *Show that*

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \ldots + (-1)^n\binom{n}{n} = 0$$

***Solution:-*** *The Binomial theorem is*

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n}b^n$$

*Put* $a = 1, b = -1$ *in above equation*
*we get*

$$(1-1)^n = \binom{n}{0}(1)^n + \binom{n}{1}(1)^{n-1}(-1) + \binom{n}{2}(1)^{n-2}(-1)^2 - \ldots + \binom{n}{n}(-1)^n$$
$$0 = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \ldots + \binom{n}{n}$$

**Example 4** *Show that*

$$\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \ldots + n\binom{n}{n} = n\ 2^{n-1}$$

***Solution:-*** *The Binomial theorem is*

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n}b^n$$

*Put $a = 1, n = n-1$ in above equation*

$$\begin{aligned}(1+b)^{n-1} &= \binom{n-1}{0}1^{n-1} + \binom{n-1}{1}1^{n-2}b + \binom{n-1}{2}1^{n-3}b^2 + \ldots + \binom{n-1}{n-1}b^{n-1} \\ &= \binom{n-1}{0} + \binom{n-1}{1}b + \binom{n-1}{2}b^2 + \ldots + \binom{n-1}{n-1}b^{n-1}\end{aligned}$$

*Now, multiplying both side above equation by $n$, we get*

$$n(1+b)^{n-1} = n\binom{n-1}{0} + n\binom{n-1}{1}b + n\binom{n-1}{2}b^2 + \ldots + n\binom{n-1}{n-1}b^{n-1}$$

*Now, put $b = 1$, we get*

$$\begin{aligned}n\ 2^{n-1} &= n\binom{n-1}{0} + n\binom{n-1}{1}1 + n\binom{n-1}{2}1^2 + \ldots + n\binom{n-1}{n-1}1^{n-1} \\ &= n\binom{n-1}{0} + n\binom{n-1}{1} + n\binom{n-1}{2} + \ldots + n\binom{n-1}{n-1}\end{aligned}$$

*Now,*

$$n\binom{n-1}{k} = (k+1)\binom{n}{k+1}$$

$$n\ 2^{n-1} = (0+1)\binom{n}{0+1} + (1+1)\binom{n}{1+1} + (2+1)\binom{n}{2+1} + \ldots + (n-1+1)\binom{n}{n-1+1}$$

*so, we get*

$$n\ 2^{n-1} = \binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \ldots + n\binom{n}{n}$$

# 2 Divisibility Theory

**Theorem 3** *State and Prove Division Algorithm*

***Statement:-*** *Given integer $a$ and $b$, with $b > 0$ there exist unique integer $q$ and $r$ satisfying*

$$a = qb + r \qquad 0 \leqslant r < b$$

*The integers $q$ and $r$ are called respectively the quotient and reminder in the division of $a$ by $b$.*

***Proof:-*** *Let $S = \{a - bx \mid x \in \mathbb{Z}, q - bx \geqslant 0\}$*
*i.e. $S$ is a set of non-negative integers.*

$$\begin{aligned}Now \quad b > 0 &\Rightarrow b \geqslant 1 \\ &\Rightarrow \mid a \mid b \geqslant \mid a \mid\end{aligned} \tag{5}$$

*Taking* $x = -\mid a \mid \in \mathbb{Z}$

$$\begin{aligned} a - bx &= a - b(-\mid a \mid) \\ &= a + \mid a \mid b \\ &\geqslant a + \mid a \mid \qquad (\because\ by\ (5)) \\ &\geqslant 0 \end{aligned}$$

$$\therefore\ a - bx \in S$$

$$\therefore\ S \neq \Phi$$

*Thus* $S$ *is a non-empty set of non-negative integers.*

$\therefore$ *By well-ordering principle* $S$ *contains a smallest integers say* $r$,

*i.e.* $r \in S$ $\therefore\ q \in \mathbb{Z}$ *such that*

$$r = a - qb \quad and \quad 0 \leqslant r$$

$$a = qb + r \quad and \quad 0 \leqslant r \tag{6}$$

*Now, we prove that* $r < b$.

*If possible suppose* $r \nless b$.

$\therefore\ r > b$

$\therefore\ r - b > 0$

*Hence*

$$\begin{aligned} a - b(q+1) &= a - bq - b \\ &= (a - bq) - b \\ &= r - b \\ &\geqslant 0 \end{aligned}$$

$$\therefore\ a - b(q+1) \in S$$

$$\therefore\ r - b \in S$$

*Which is not possible because* $r$ *is the smallest integer in* $S$.

$\therefore$ *our supposition* $r \nless b$ *is wrong*

$$\therefore\ r < b \tag{7}$$

*So,from equation (6) and (7) we get*

$$a = qb + r, \qquad 0 \leqslant r < b$$

*Now, we prove that* $q$ *and* $r$ *are unique integer*

*If suppose not then*

$$a = qb + r, \qquad 0 \leqslant r < b$$

$$a = q'b + r', \qquad 0 \leqslant r' < b$$

$$\therefore\ bq + r = bq' + r'$$

$$\therefore\ bq - bq' = r' - r$$

$$\therefore\ b(q - q') = r' - r$$

$$\therefore \mid b(q - q') \mid = \mid r' - r \mid$$

$$\therefore \mid b \mid\mid q - q' \mid = \mid r' - r \mid$$

$$\therefore\ b \mid q - q' \mid = \mid r' - r \mid \quad (\because\ b > 0) \tag{8}$$

*Now,*

$$0 \leqslant r < b \quad and \quad 0 \leqslant r' < b$$
$$\Rightarrow \quad -b < -r \leqslant 0 \quad and \quad 0 \leqslant r' < b$$

*Adding*

$$\begin{aligned}
&\Rightarrow \quad -b < r' - r < b \\
&\Rightarrow \quad \mid r' - r \mid < b \\
&\Rightarrow \quad b \mid q - q' \mid < b \qquad (\because \ by \ equation \ (8)\ ) \\
&\Rightarrow \quad \mid q - q' \mid < 1 \\
&\Rightarrow \quad \mid q - q' \mid \leqslant 0 \\
&\Rightarrow \quad \mid q - q' \mid = 0 \qquad (\because \ \mid q - q' \mid \nless 0\ ) \\
&\Rightarrow \quad q - q' = 0 \\
&\Rightarrow \quad q = q'
\end{aligned}$$

*By equation (8) we get*

$$\mid r' - r \mid = 0$$
$$\therefore \ r - r' = 0$$
$$\therefore \ r = r'$$

*Hence $q$ and $r$ are unique integers.*

**Definition 2.1** *An integer $b$ is said to be divisible by an integer $a \neq 0$, if there exist some integer $c$ such that $b = ac$.And it is denoted by $a \mid b$.*
*we write $a \nmid b$ to indicate that $b$ is not divisible by $a$.*

**Theorem 4** *For Integers $a, b, c$ the following hold:*

*(a)* $a \mid 0, \quad 1 \mid a, \quad a \mid a$

*(b)* $a \mid 1$*, if and only if* $a \pm 1$

*(c) If $a \mid b$ and $c \mid d$ then $ac \mid bd$*

*(d) If $a \mid b$ and $b \mid c$ then $a \mid c$*

*(e) If $a \mid b$ and $b \mid a$ if and only if $a \pm b$.*

*(f) If $a \mid b$ and $b \neq 0$, then $\mid a \mid \leqslant \mid b \mid$*

*(g) If $a \mid b$ and If $a \mid c$, then $a \mid (bx + cy)$ for arbitrary integers $x$ and $y$.*

***Proof:-***

*(a) By above definition (2.1) if $a \mid b$ then there exist an integer $c$ such that $b = ac$*
*Now,* $a \mid 0 \ \Rightarrow 0 = ac \ \ take \ \ c = 0$
*Now,* $a \mid 1 \ \Rightarrow a = 1c \ \ take \ \ c = a$
*Now,* $a \mid a \ \Rightarrow a = ac \ \ take \ \ c = 1$

*Therefore (a) is hold.*

*(b) By above definition (2.1) if $a \mid b$ then there exist an integer $c$ such that $b = ac$*

*($\Rightarrow$) suppose $a \mid 1$*

$\Rightarrow \quad 1 = ac$

*So, it is possible when $a = 1 \quad \& \quad c = 1$*

*or $\quad a = -1 \quad \& \quad c = -1$*

$\Rightarrow \; a = \pm 1$

($\Leftarrow$) *conversely suppose $a \pm 1$*

$\Rightarrow \quad a = 1 \quad or \quad a = -1$

$1.1 = 1 \quad and \quad (-1)(-1) = 1$

$\Rightarrow 1 \mid 1 \quad and \quad \Rightarrow -1 \mid 1$

$\Rightarrow a \mid 1 \quad and \quad \Rightarrow a \mid 1$

*Therefore (b) is hold.*

*(c) By above definition (2.1) if $a \mid b$ then there exist an integer $c$ such that $b = ac$ so,*

$$a \mid b \Rightarrow b = ac_1 \quad where\ c_1\ is\ an\ integer \tag{9}$$

$$c \mid d \Rightarrow d = cc_2 \quad where\ c_2\ is\ an\ integer \tag{10}$$

*Now,equation (9) multiply with equation (10)*

$$\begin{aligned} bd &= (ac_1)(cc_2) \\ \Rightarrow bd &= (ac)(c_1c_2) \\ \Rightarrow bd &= (ac)c_3 \quad (where\ c_3 = c_1c_2,\ c_3\ is\ an\ integer) \\ \Rightarrow ac &\mid bd \end{aligned}$$

*Therefore (c) is hold.*

*(d) By above definition (2.1) if $a \mid b$ then there exist an integer $c$ such that $b = ac$ so,*

$$a \mid b \Rightarrow b = ac_1 \qquad where\ c_1\ is\ an\ integer \tag{11}$$

$$b \mid c \Rightarrow c = bc_2 \qquad where\ c_2\ is\ an\ integer \tag{12}$$

$$\begin{aligned} &\Rightarrow c = ac_1c_2 \quad (from\ equation\ (11)\ ) \\ &\Rightarrow c = ac_3 \qquad where\ c_3 = c_1c_2\ is\ an\ integer \\ &\Rightarrow a \mid c \end{aligned}$$

*Therefore (d) is hold.*

*(e) By above definition (2.1) if $a \mid b$ then there exist an integer $c$ such that $b = ac$*

($\Rightarrow$) *so,*

$$a \mid b \Rightarrow b = ac_1 \qquad where\ c_1\ is\ an\ integer \tag{13}$$

$$b \mid a \Rightarrow a = bc_2 \qquad where\ c_2\ is\ an\ integer \tag{14}$$

$$\begin{aligned} &\Rightarrow a = ac_1c_2 \quad (from\ equation\ (13)\ ) \\ &\Rightarrow a = a(c_1c_2) \\ &\Rightarrow c_1c_2 = 1 \end{aligned}$$

*It is possible only when* $c_1 = 1$ & $c_2 = 1$ *or* $c_1 = -1$ & $c_2 = -1$

$$\begin{aligned} If\ c_1 = c_2 = 1 \Rightarrow a = b \qquad & (From\ equation\ (13)) \\ If\ c_1 = c_2 = -1 \Rightarrow a = -b \qquad & (From\ equation\ (14)) \\ \Rightarrow a = \pm b \end{aligned}$$

$(\Leftarrow)$ *conversely if* $a = \pm b$ *then* $a = b$ *or* $a = -b$

$$\begin{aligned} a = b \Rightarrow b = a1 \Rightarrow a \mid b \\ a = -b \Rightarrow a = b(-1) \Rightarrow b \mid a \end{aligned}$$

*Therefore (e) is hold.*

(f) *By above definition (2.1) if* $a \mid b$ *then there exist an integer* $c$ *such that* $b = ac$ *so,*

$$\begin{aligned} a \mid b &\Rightarrow b = ac \\ &\Rightarrow \mid b \mid = \mid ac \mid \qquad (taking\ modulas\ both\ sides) \\ &\Rightarrow \mid b \mid = \mid a \mid\mid c \mid \end{aligned}$$

*since* $b \neq 0 \Rightarrow c \neq 0$
$\because\ c \neq 0$ *it follows that*

$$\begin{aligned} \mid c \mid \geqslant 1 \\ \Rightarrow \mid a \mid\mid c \mid \geqslant \mid a \mid \\ \Rightarrow \mid b \mid \geqslant \mid a \mid \\ \Rightarrow \mid a \mid \leqslant \mid b \mid \end{aligned}$$

*Therefore (f) is hold.*

(g) *By above definition (2.1) if* $a \mid b$ *then there exist an integer* $c$ *such that* $b = ac$ *so,*

$$a \mid b \Rightarrow b = ar \qquad (where\ r\ is\ an\ integer) \tag{15}$$
$$a \mid c \Rightarrow c = as \qquad (where\ s\ is\ an\ integer) \tag{16}$$

*But the choice of* $x$ *and* $y$ *is*

$$\begin{aligned} bx + cy &= (ar)x + (as)y \qquad (By\ equation\ (15)\ and\ (16)\ ) \\ bx + cy &= a(rx + sy) \\ &\Rightarrow a \mid (bx + cy) \qquad (\because\ (rx + sy)\ is\ an\ integer) \end{aligned}$$

*Therefore (g) is hold.*

## 3 Greatest Common Divisor

**Definition 3.1** *Let $a$ and $b$ be given integers with at least one of them not zero,then Greatest common divisor of $a$ and $b$, denoted by $\gcd(a, b)$ is the positive integer $d$ satisfies the following:*

*(i)* $d \mid a$ *and* $d \mid b$

*(ii) If* $c \mid a$ *and* $c \mid b$*, then* $c \leqslant d$*.*

**Theorem 5** *Prove that given integers $a$ and $b$ not both of zero, then there exist integers $x$ and $y$ such that* $\gcd(a.b) = ax + by$

***Proof:-*** *Consider the set $S$ of all positive linear combination of $a$ and $b$.*

$$S = \{au + bv \mid au + bv > 0, u, v \in \mathbb{Z}\}$$

*First we show $S \neq \phi$.*
*If $a \neq 0$, then the integer $\mid a \mid = au + b0$ lies in $S$, where we choose $u = 1$ or $u = -1$ according as $a$ is positive or negative.*
*So, $S \neq \phi$*
*Now, we prove $d = \gcd(a, b)$*
*By, well-ordering principle $S$ must contain a smallest element $d$*
*Now, by definition of $S$ there exist integer $x$ and $y$ for which $d = ax + by$*
*then we have to prove that $d \mid a$ and $d \mid b$.*
*If $d \nmid a$ then by Division Algorithm there exist integer $q$ and $r$ such that*

$$\begin{aligned} a &= dq + r, \quad where\ \ 0 \leqslant r < d \\ Now, \quad d &= ax + by \\ \Rightarrow\ dq &= aqx + bqy \\ \Rightarrow\ a - r &= aqx + bqy \\ \Rightarrow\ r &= a - aqx - bqy \\ \Rightarrow\ r &= a(1 - qx) + b(-qy) \\ \Rightarrow\ r &\in S\ \ \&\ \ r < d \end{aligned}$$

*which is contradiction as $d$ is the smallest element of $S$.*
*so, $d \mid a$.*
*Similarly by above we can prove $d \mid b$.*
*so, $d$ is common divisor of $a$ and $b$.*
*Let $c$ is an arbitrary positive common divisor of the integer $a$ and $b$.*
*Then $c \mid a$ and $c \mid b$.*
$\Rightarrow\ c \mid (ax + by) \quad (\because\ from\ theorem\ 4(g)\ )$
$\Rightarrow\ c \mid d\ \ and\ \ d \neq 0$
$\Rightarrow \mid c \mid \leqslant \mid d \mid \qquad (\because\ from\ theorem\ 4(f)\ )$
$\Rightarrow\ c \leqslant d.$
*so, $d$ is a greatest common divisor of $a$ and $b$.*
*so, $d = \gcd(a, b)$*

**Theorem 6** *If $a$ and $b$ are given integers not both zero then the set*

$$T = \{ax + by \mid x, y\ are\ integers\}$$

*is precisely the set of all multiples of $d = \gcd(a, b)$*

***Proof:-*** *Here we have to prove*

$$T = \{ax + by \mid x, y \; are \; integers\}$$

*is the precisely of the multiple of* $nd$.
*Here* $d = \gcd(a, b) \Rightarrow \; d \mid a$ *and* $d \mid b$
$\Rightarrow \; d \mid (ax + by)$ *for all integers* $x, y$.
*Thus every member of* $T$ *is a multiple of* $d$.

*Conversely* $d$ *may be written as* $d = ax_0 + by_0$ *for suitable integers* $x_0$ *and* $y_0$
*so, that any multiple* $nd$ *of* $d$ *is of the form*

$$nd = n(ax_0 + by_0)$$
$$nd = a(nx_0) + b(ny_0)$$

*Hence,* $nd$ *is a linear combination of* $a$ *and* $b$.
*so,* $nd \in T$.

**Definition 3.2** *Two integers* $a$ *and* $b$*, not both of which are zero are said to be relatively prime whenever* $\gcd(a, b) = 1$

**Theorem 7** *Let* $a$ *and* $b$ *be integers not both zero.Then* $a$ *and* $b$ *are relatively prime if and only if there exist integers* $x$ *and* $y$ *such that* $1 = ax + by$.

***Proof:-*** *If* $a$ *and* $b$ *are relatively prime so* $\gcd(a, b) = 1$*, then by theorem(5) there exist integers* $x$ *and* $y$ *satisfying* $1 = ax + by$

*conversely suppose that* $1 = ax + by$ *for some choice of* $x$ *and* $y$.
*Suppose that* $d = \gcd(a, b) \; \Rightarrow \; d \mid a$ *and* $d \mid b$
*So, by theorem 4 (g),* $\; d \mid (ax + by) \Rightarrow d \mid 1$
*Now,* $d$ *is a positive integer, so* $d = 1$

$$\therefore \gcd(a, b) = 1$$

*Thus, integers* $a$ *and* $b$ *are relatively prime.*

**Theorem 8** *If* $\gcd(a, b) = d$ *then* $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

***Proof:-*** *Here First we show* $\frac{a}{d}$ *and* $\frac{b}{d}$ *are integer*
*Here* $\gcd(a, b) = d$ *then* $d \mid a$ *and* $d \mid b$.
$d \mid a$ *then there exist integer* $n_1$ *such that* $a = n_1 d$
$\therefore \; \frac{a}{d} = n_1$.
$d \mid b$ *then there exist integer* $n_2$ *such that* $b = n_2 d$
$\therefore \; \frac{b}{d} = n_2$.
*so, both* $\frac{a}{d}$ *and* $\frac{b}{d}$ *are integers.*
*Now,* $\gcd(a, b) = d$ *then there exist integers* $x$ *and* $y$ *such that* $d = ax + by$
*Dividing both side by* $d$*, we get*

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

*Because* $(\frac{a}{d})$ *and* $(\frac{b}{d})$ *both are integer*
*So,* $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

**Theorem 9** *If* $a \mid c$ *and* $b \mid c$, *with* $\gcd(a,b) = 1$ *then* $ab \mid c$.

***Proof:-*** *If* $a \mid c$ *then there exist an integer such that* $r$ *such that*

$$c = ar \tag{17}$$

*If* $b \mid c$ *then there exist an integer such that* $s$ *such that*

$$c = bs \tag{18}$$

*Now,* $\gcd(a,b) = 1$ *then there exist integer* $x$ *and* $y$ *such that*

$$1 = ax + by \tag{19}$$

*Multiply equation (19) by* $c$

$$\begin{aligned} &\Rightarrow\ c = acx + bcy \\ &\Rightarrow\ c = a(bs)x + b(ar)y \qquad (from\ equation\ (17)\ and\ (18)) \\ &\Rightarrow\ c = ab(sx + ry) \\ \because\ &sx + ry\ is\ an\ integer \\ &\therefore ab \mid c \end{aligned}$$

**Theorem 10** *State and Prove Euclid's Lemma*

***Statement:-*** *If* $a \mid bc$ *with* $\gcd(a,b) = 1$, *then* $a \mid c$

***Proof:-*** *Here it is given that* $\gcd(a,b) = 1$, *then there exist integers* $x$ *and* $y$ *such that*

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

$$1 = ax + by \tag{20}$$

*Multiply equation (20) by* $c$

$$\therefore\ c = acx + bcy \tag{21}$$

*Now,* $a \mid bc$ *and also* $a \mid ac$
*it follows that* $a \mid acx + bcy$ *for any integers* $x$ *and* $y$

$$\Rightarrow\ a \mid c \qquad\qquad (from\ eqution\ (21))$$

**The Euclidean Algorithm:-** For given integers $a$ and $b$ both not zero then find the $\gcd(a,b)$ we procedure the following system equations:

$$\begin{aligned} a &= q_1 b + r_1 \qquad 0 < r_1 < b \\ b &= q_2 r_1 + r_2 \qquad 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 \qquad 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \qquad 0 < r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n + 0 \end{aligned}$$

This division process continue until some zero remainder appears, say at the $(n+1)^{th}$ stage where $r_{n-1}$ is divided by $r_n$
The last nonzero remainder $r_n$ is equal to $\gcd(a,b)$.

**Example 5** *Find* $\gcd(12378, 3054)$ *and obtain integers* $x$ *and* $y$ *satisfy following:*

$$\gcd(12378, 3054) = 12378x + 3054y$$

***Solution:-*** *Here we use Euclidean Algorithm*

$$12378 = 4(3054) + 162 \tag{22}$$
$$3054 = 18(162) + 138 \tag{23}$$
$$162 = 1(138) + 24 \tag{24}$$
$$138 = 5(24) + 18 \tag{25}$$
$$24 = 1(18) + 6 \tag{26}$$
$$18 = 3(6) + 0 \tag{27}$$

*So,* $\gcd(12378, 3054) = 6$

*To represent 6 as a linear combination of the integers 12378 and 3054 we start with the next to last of the displayed and successively eliminate the remainders 18,24,138 and 162.*

$$\begin{aligned}
6 &= 24 - 1(18) && (from\ equation\ (26))\\
6 &= 24 - 1(138 - 5(24)) && (from\ equation\ (25))\\
6 &= 6(24) - 1(138) \\
6 &= 6(162 - 1(138)) - 1(138) && (from\ equation\ (24))\\
6 &= 6(162) - 7(138) \\
6 &= 6(162) - 7(3054 - 18(162)) && (from\ equation\ (23))\\
6 &= 132(162) - 7(3054) \\
6 &= 132(12378 - 4(3054)) - 7(3054) && (from\ equation\ (22))\\
6 &= 12378(132) + 3054(-535)
\end{aligned}$$

*And we have* $\gcd(12378, 3054) = 6$

$$\gcd(12378, 3054) = 12378(132) + 3054(-535)$$

*So,* $x = 132$ *and* $y = -535$

**Example 6** *Find* $\gcd(1106, 497)$ *and obtain integers* $x$ *and* $y$ *satisfy following:*

$$\gcd(1106, 497) = 1106x + 497y$$

***Solution:-*** *Here we use Euclidean Algorithm*

$$1106 = 2(497) + 112 \tag{28}$$
$$497 = 4(112) + 49 \tag{29}$$
$$112 = 2(49) + 14 \tag{30}$$
$$49 = 3(14) + 7 \tag{31}$$
$$14 = 2(7) + 0 \tag{32}$$

*So,* $\gcd(1106, 497) = 7$

*To represent 7 as a linear combination of the integers 1106 and 497 we start with the next to last of the displayed and successively eliminate the remainders 14,49 and 112*

$$
\begin{aligned}
7 &= 49 - 3(14) && (from\ equation\ (31)) \\
7 &= 49 - 3(112 - 2(49)) && (from\ equation\ (30)) \\
7 &= 7(49) - 3(112) \\
7 &= 7(497 - 4(112)) - 3(112) && (from\ equation\ (29)) \\
7 &= 7(497) - 31(112) \\
7 &= 7(497) - 31(1106 - 2(197)) && (from\ equation\ (28)) \\
7 &= 497(69) + 1106(-31)
\end{aligned}
$$

*And we have* $\gcd(1106, 497) = 7$

$$\gcd(1106, 497) = 1106(69) + 497(-31)$$

*So,* $x = 69$ *and* $y = -31$

**Definition 3.3** *The least common multiple of two nonzero integers* $a$ *and* $b$ *denoted by lcm(a,b) is the positive integer* $m$ *satisfying the following:*

*(i)* $a \mid m$ *and* $b \mid m$

*(ii) If* $a \mid c$ *and* $b \mid c$ *with* $c > 0$*, then* $m \leqslant c$*.*

**Theorem 11** *For positive integers* $a$ *and* $b$ *then prove that*

$$\gcd(a, b).lcm(a, b) = ab$$

**Proof:-** We know that for any positive integer $a$ and $b$, $\gcd(a, b) = d$
This implies that $d \mid a$ and $d \mid b$
If $d \mid a \Rightarrow a = dr;\ \ where\ r\ is\ an\ integer$
If $d \mid b \Rightarrow b = ds;\ \ where\ s\ is\ an\ integer$
If $m = \dfrac{ab}{d}$
Then,

$$
\begin{aligned}
m &= \frac{(dr)b}{d} \quad \& \quad m = \frac{(ds)a}{d} \\
&= br \qquad \& \qquad = as \\
\Rightarrow b &\mid m \qquad \& \qquad a \mid m
\end{aligned}
$$

Which shows that $m$ is a positive common multiple of $a$ and $b$.
Now, let $c$ be any positive integer that is common multiple of $a$ and $b$
$\Rightarrow a \mid c$ and $b \mid c$
$\Rightarrow c = au$ and $c = bv$ (where $u$ and $v$ are integers)
Also, we know that there exist integer $x$ and $y$ satisfying $d = ax + by$
Now,

$$
\begin{aligned}
\frac{c}{m} &= \frac{cd}{ab} \\
&= \frac{c(ax + by)}{ab} \\
&= \frac{cax}{ab} + \frac{cby}{ab} \\
&= \frac{cx}{b} + \frac{cy}{a} \\
&= (\frac{c}{b})x + (\frac{c}{a})y
\end{aligned}
$$

$$\begin{aligned}\frac{c}{m} &= vx + uy \\ c &= m(vx + uy) \\ \Rightarrow m &\mid c\end{aligned}$$

It conclude that $m \leqslant c$

Thus by definition (3.3),

$$\begin{aligned}& m = lcm(a, b) \\ & \Rightarrow \frac{ab}{d} = lcm(a, b) \\ & \Rightarrow \frac{ab}{\gcd(a, b)} = lcm(a, b) \\ & \Rightarrow \gcd(a, b).lcm(a, b) = ab\end{aligned}$$

# 4 Linear Diophantine Equation

**Definition 4.1** *The general form of a linear Diophantine equation in two unknown $x$ and $y$ is*

$$ax + by = c$$

*where $a, b$ and $c$ are integers and $a, b$ are not both zero.*

**Theorem 12** *Prove that the linear Diophantine equation $ax + by = c$ has a solution if and only if $d \mid c$, where $d = \gcd(a, b)$*
*Further, if $x_0, y_0$ is any particular solution of this equation then all other solutions are given by*

$$x = x_0 + (\frac{b}{d})t \quad and \quad y = y_0 + (\frac{a}{d})t$$

*Where, $t$ is an arbitrary integer*

***Proof:-***($\Rightarrow$) *Suppose that the equation $ax + by = c$ has a solution say $x_0, y_0$.*

$$\therefore ax_0 + by_0 = c$$

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

$$\therefore d \mid a \quad and \quad d \mid b$$

$$\therefore a = dr \quad and \quad b = ds, \quad where\ r, s \in \mathbb{Z}$$

*Now,*

$$\begin{aligned}c &= ax_0 + by_0 \\ c &= (dr)x_0 + (ds)y_0 \\ c &= d(rx_0 + sy_0) \\ \Rightarrow d &\mid c\end{aligned}$$

($\Leftarrow$) *conversely suppose $d \mid c$*

$$\therefore c = dt \quad where\ t \in \mathbb{Z}$$

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

$$\therefore d = au + bv, \qquad where\ u, v \in \mathbb{Z}$$
$$\therefore dt = tau + tbv$$
$$\therefore dt = a(ut) + b(vt)$$
$$\therefore dt = ax_0 + by_0$$

*where* $x_0 = ut$ *and* $y_0 = vt$ *is a particular solution of* $ax + by = c$
$\therefore$ *the equation* $ax + by = c$ *has a solution.*

***Further Proof:-*** *Suppose* $x_0, y_0$ *is any particular solution of the equation* $ax + by = c$ *and* $x', y'$ *any other solution of* $ax + by = c$.
*Hence*

$$ax_0 + by_0 = c \quad and \quad ax' + by' = c$$

$$\Rightarrow ax' + by' = ax_0 + by_0$$
$$\Rightarrow ax' - ax_0 = by_0 - by'$$
$$\Rightarrow a(x' - x_0) = b(y_0 - y') \tag{33}$$

*Now,*

$$\gcd(a, b) = d$$
$$\therefore \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$
$$\therefore \gcd(r, s) = 1$$
$$where\ r = \frac{a}{d} \quad and \quad s = \frac{b}{d}$$
$$\therefore a = dr \quad and \quad b = ds$$

*Putting these values of* $a$ *and* $b$ *in equation (33)*
*we get*

$$dr(x' - x_0) = ds(y_0 - y')$$
$$\therefore r(x' - x_0) = s(y_0 - y') \tag{34}$$
$$\Rightarrow r \mid s(y_0 - y')$$

*But,* $\gcd(r, s) = 1$

$$\therefore r \mid y_0 - y' \qquad (By\ Euclid's\ Lemma)$$
$$\therefore y_0 - y' = rt \qquad For\ some\ integer\ t \tag{35}$$

*From equation (34) we get*

$$r(x' - x_0) = s(rt)$$
$$\therefore x' - x_0 = st$$
$$\therefore x' = x_0 + st$$
$$\therefore x' = x_0 + (\frac{b}{d})t \tag{36}$$

*From equation (35) we get*

$$\therefore y' = y_0 - rt$$
$$\therefore y' = y_0 - (\frac{a}{d})t \tag{37}$$

*Hence for any integer* $t$

$$
\begin{aligned}
ax' + by' &= a\left[x_0 + (\frac{b}{d})t\right] + b\left[y_0 - (\frac{a}{d})t\right] \quad (from\ equation\ (36)\ and\ (37)) \\
&= ax_0 + a(\frac{b}{d})t + by_0 - b(\frac{a}{d})t \\
&= ax_0 + by_0 \\
&= c \qquad (\because\ x_0, y_0\ is\ a\ solution\ of\ the\ equation\ ax + by = c)
\end{aligned}
$$

*Hence all other solution are given by*

$$
\begin{aligned}
x &= x_0 + (\frac{b}{d})t \\
y &= y_0 - (\frac{a}{d})t \quad where\ t\ is\ an\ integer
\end{aligned}
$$

**Example 7** *Find the General Solution of the linear Diophantine equation*

$$172x + 20y = 1000$$

***Solution:-*** *First we find* $\gcd(172, 20)$

$$
\begin{aligned}
172 &= 8(20) + 12 \qquad (38) \\
20 &= 1(12) + 8 \qquad (39) \\
12 &= 1(8) + 4 \qquad (40) \\
8 &= 2(4) + 0
\end{aligned}
$$

*Hence* $\gcd(172, 20) = 4$ *and* $4 \mid 1000$
$\therefore$ *The Solution of the given equation exists.*
*Now,*

$$
\begin{aligned}
4 &= 12 - 1(8) \qquad (fron\ equation\ (40)) \\
4 &= 12 - 1(20 - 1(12) \qquad (fron\ equation\ (39)) \\
4 &= 2(12) - 1(20) \\
4 &= 2(172 - 8(20)) - 1(20) \qquad (fron\ equation\ (38)) \\
4 &= 2(172) - 17(20) \qquad (41)
\end{aligned}
$$

*Multiplying equation (41) by 250 we get*

$$1000 = 172(500) + 20(-4250)$$

*Thus one solution of the given Diophantine equation is given by*

$$x_0 = 500 \quad \& \quad y_0 = -4250$$

*Now,general solution of given Diophantine equation is given by*

$$
\begin{aligned}
x &= x_0 + (\frac{b}{d}t) \\
&= 500 + (\frac{20}{4})t \\
x &= 500 + 5t \qquad (42) \\
y &= y_0 - (\frac{a}{d}t) \\
&= (-4250) - (\frac{172}{4})t \\
y &= -4250 - 43t \qquad (43)
\end{aligned}
$$

*Now from equation (42) we get*

$$\begin{aligned} 5t + 500 &> 0 \\ t &> -100 \end{aligned} \tag{44}$$

*And from equation (43) we get*

$$\begin{aligned} -4250 - 43t &> 0 \\ \frac{-4250}{43} &> t \\ -98.83 &> t \end{aligned} \tag{45}$$

*From equation (44) and (45) we get*

$$-100 < t < -98.83$$

*Thus we get* $t = -99$
*Put* $t = -99$ *in equation (42) and (43) we get unique positive solution of Diophantine equation is* $x = 5$ *and* $y = 7$

**Example 8** *A customer bought a dozen pieces of fruit, apples and oranges,for* $\$1.32 = [132\ cents]$. *If an apple 3 cents more than an orange and more apples then oranges were purchased, how many pieces of each kind were bought?*

***Solution:-*** *Suppose* $x$ *is the number of apples purchased.*
*And* $y$ *is the number of oranges purchased*

$$\therefore\ x + y = 12 \tag{46}$$

*Suppose* $z$ *is the cost of an orange in cent.*
*And* $z + 3$ *is the cost of an apple in cent.*
$\therefore$ *we get*

$$\begin{aligned} (z+3)x + zy &= 132 \\ \therefore zx + 3x + zy &= 132 \\ \therefore z(x+y) + 3x &= 132 \\ \therefore 3x + z(x+y) &= 132 \\ \therefore 3x + 12z &= 132 \qquad (from\ equation\ (46)) \\ \therefore x + 4z &= 44 \end{aligned} \tag{47}$$

*Now,* $\gcd(1, 4) = 1$ *and* $1 \mid 44$ *therefore the solution of this equation exists.*

$$1 = 1(-3) + 4(1)$$

*Multiply above equation by (44) we get*

$$\begin{aligned} 44 &= 1(-132) + 4(44) \\ \therefore\ x_0 &= -\,132 \quad \& \quad z_0 = 44 \end{aligned}$$

*This is one solution of the equation.*
*All the solution are of the form*

$$x = -132 + 4t \tag{48}$$

$$z = 44 + (-1)t \quad where\ t \in \mathbb{Z} \tag{49}$$

*Now, apples are more than oranges*
*Therefore we get*

$$
\begin{aligned}
x &> y \qquad and \\
x + y &= 12 \\
\therefore x &\geqslant 12 \qquad (\because\ y \geqslant 0)
\end{aligned}
\tag{50}
$$

*Now,*

$$
\begin{aligned}
x &> 12 - x \\
\therefore 2x &> 12 \\
\therefore x &> 6
\end{aligned}
\tag{51}
$$

*Now, from equation (50) and (51) we get,*

$$
\begin{aligned}
6 < x &\leqslant 12 \\
\therefore 6 < -132 + 4t &\leqslant 12 \qquad (from\ equation\ (48)) \\
\therefore 138 < 4t &\leqslant 144 \\
\therefore 34.5 < t &\leqslant 36
\end{aligned}
$$

$\therefore t = 35$ *and* $t = 36$
*Now,* $t = 35$ *and from equation (48) we get* $x = 8, y = 4\ and\ z = 9$
*Now,* $t = 36$ *and from equation (48) we get* $x = 12, y = 0\ and\ z = 8$
*So, there are two possible purchase:*
*(i) 8 apples at 12 cents each and 4 apples at 9 cents each.*
*(ii) 12 apples at 11 cents each.*

# 5 Exercises

1. By Principle of Mathematical induction Show that
$$1 + 2 + 2^2 + 2^3 + \ldots + 2^{n-1} = 2^n - 1$$
2. By Principle of Mathematical induction Show that
$$1.2 + 2.3 + 3.4 + \ldots + n.(n+1) = \frac{n(n+1)(n+2)}{3}$$
3. Find $\gcd(726, 275)$ and obtain integers $x$ and $y$ satisfy following:
$$\gcd(726, 275) = 726x + 275y$$
4. Find $\gcd(1769, 2378)$ and obtain integers $x$ and $y$ satisfy following:
$$\gcd(1769, 2378) = 1769x + 2378y$$
5. Find (i) $lcm(306, 257)$ and (ii) $lcm(272, 1479)$
6. Find General solution of the linear Diophantine equation
$$54x + 21y = 906$$
7. If a cook is worth 5 coins, a hen 3 coins and three chicks together 1 coin, how many cocks,hens and chicks totaling 100, can be bought for 100 coins?