1. NUMBER SYSTEMS
1.1.1 Natural Numbers

The Peano Postulates
In this section, we propose to develop the system of natural numbers assuming only a few of its simpler properties. These simple properties, known as the Peano Postulates (Axioms) after the Italian mathematician who in 1899 inaugurated the program, may be stated as follows:

Postulate I: $1 \in$ N

Postulate II: For each n$\in$N there exists a unique $n^* \in$N, called the successor of n.

Postulate III: For each n$\in$N we have $n^* \neq 1$ ie.1 is the first Natural number.

Postulate IV: If m, n$\in$N and $m^* = n*$, then m=n.

Postulate V: Any subset K of N having the properties $1 \in$K, $k^* \in K$ whenever k$\in K$ is equal to N

First we shall check to see that these are in fact well-known properties of the natural numbers. Postulates I and II need no elaboration; III states that there is a first natural number 1; IV states that the distinct natural numbers m and n have distinct successors m+1 and n+1;V states essentially that any natural number can be reached by beginning with 1 and counting consecutive successors. It will be well noted that, in the definitions of addition and multiplication on N which follow, nothing beyond these postulates is used.

Definition 1

The set of natural or counting numbers is {1, 2, 3, …………) The natural numbers are closed under addition and multiplication. Let N be a natural number and n, m $\in$N, then n + m $\in$M and nm $\in$ N, that is the sum and product of two natural numbers are also natural numbers.

For any natural numbers, a, b, c, we have

(+) Addition	Mutiplication	
a + (b + c) = (a + b) + c	a(bc) = (ab)c	(associativity)
a + b = b + a	ab = ba	(commutativity)
a(b + c) = ab + ac	(a + b)c = ac + bc.	(Distributive)

1.1.2 Integers
Considering subtraction and division, we extend the set of natural numbers to the set of integers

………-3, -2, -1, 0, 1, 2, 3 ………

The set of integers are closed under addition, multiplication and subtraction. We use the additive inverse to derive subtraction eg. a – b means a + (-b)

<u>Properties of integers</u>

(i) Associative
(ii) Commutative
(iii) Distributive
(iv) Identity element (ie, a + 0 = a = 0 + a and a.1 = a = 1.a)
(v) Transitivity, (ie, a > b and b > c $\Rightarrow$ a > c)
(vi) Trichotomy: either a > b, a < b or a = b
(vii) Cancellation law: If a.c = b.c and c $\neq$ 0 then a = b

1.1.3 Rational Numbers

The set of integers, Z is not closed under multiplication.

In particular, the problem: ux = 1 where u$\in Z$, is known or has no solution x in Z. If however, Z is enlarged to include the reciprocals $\frac{1}{u}$ for each nonzero u, as well as their negatives, then, we obtain a new larger set of numbers Q, the Rationals, which is closed under multiplication. It is clear that every rational number can be written as: u.$\left(\frac{1}{v}\right)$ or $u/_v$, where u,v$\in Z$ and v $\neq 0$.

Q is closed under all the four arithmetic operations. In the case of closure under $\div$, division by 0 must be avoided, as the result is indeterminate $\left(0/_0\right)$

Note that;

0$\in Q$, since $\frac{0}{b}$, b $\neq 0$ is 0.

Z$\in Q, since\ \frac{a}{1} = a$ for all a $\in Z$

It is clear that N$\in Z \in Q$

Note: The Set of Irrational Numbers

There are numbers which do not belong to Q, that is, they cannot be expressed in the form $\frac{a}{b}\ where\ a, b\ \in Z$. There are however, points on the number line which correspond to these numbers. The set of such numbers is called the set of **Irrational Numbers**.

Examples of such numbers are: $\sqrt{2}, \sqrt{3}, \sqrt{5}, \pi\ etc.$

Exercise: Prove that the following are irrational numbers, $\sqrt{2}, \sqrt{3}, \pi$.

Remember that every rational number may be expressed either as a terminating decimal or as a recurring decimal. E.g. $\frac{1}{2}$ = 0.5, $\frac{1}{3} = 0.333\ldots\ldots or 0.\bar{3}$.

Again every irrational number can only be expressed as a non-terminating and non-recurring decimal number.

1.1.4 Real Numbers

Nevertheless, we find that the set of Rationals, Q is not closed under the extraction of some roots. In particular, the problem of $x^2 = 2$ has no solution x in Q. (Exercise)

Note, however, that √2 can be geometrically constructed (Exercise).

Furthermore, a geometrically realizable constant like $\pi = {}^{C}/_{2r}$ where c is the circumference of a circle and r is its radius is not a rational number.

These non rational (or irrational) numbers can be written as the limit of an infinite series of rational numbers. If the set of rational numbers, Q is enlarged to include all limits of convergent series of rational numbers, the resulting set is called the set of *real numbers* and is denoted R.

Operations with Real Numbers

Let a, b, c$\in R$, then

a + b and ab all belong to R.	closure law
a + b = b + a	commutative law of addition
(a + b) + c = a + (b + c)	associative law
ab = ba	commutative law of multiplication
(ab) c = a (bc)	associative law of multiplication
a(b + c) = ab + ac	distributive law of multiplication over addition
a + 0 = 0 + a = a	existence of an identity under addition
a1 = 1a = a	existence of an identity under multiplication
a + x = x + a = 0	existence of an inverse under + x is denoted by(-a).
$aa^{-1} = a^{-1} a = 1$	existence of an inverse under x . a^{-1} is denoted by $\frac{1}{a}$

Any set, such as R, which satisfies the above rules is called a field.

1.1.5 Principle of Mathematical Induction

If it is known that

(1) some statement is true for n = 1
(2) assumption that statement is true for n implies that the statement is true for (n + 1) then the statement is true for all positive integers

Modifications of the Principle of Mathematical Induction

If it is known that

(1) Some statement is true for $n = n_0$ (positive integer)
(2) assumption that statement is true for n implies that the statement is true for (n + 1) then the statement is true for all positive integers greater or equal to n_0

If it is known that

(1) some statement is true for n = 1
(2) assumption that statement is true for all positive integers k, $1 \leq k \leq n$ implies that the statement is true for (n + 1) then the statement is true for all positive integers

(Backward induction)

If it is known that

(1) some statement is true for n = 1
(2) assumption that statement is true for n > 1 implies that the statement is true for 2n and (n-1) then the statement is true for all positive integers

Example:
Use mathematical induction to establish the following formula:
$1+2+3+\cdots+n = {}^{n}\!/_{2}\ (n+1)$

Solution:
Let $S_n = 1+2+3+\cdots+n = {}^{n}\!/_{2}\ (n+1)$ and
Let $n=1$
then $1 = {}^{1}\!/_{2}\ (1+1) = 1$
when $n=k$
We have $1+2+3+\cdots+k = {}^{k}\!/_{2}\ (k+1)$.
Hence for $n=k+1$
We have $S_{k+1} = 1+2+3+\cdots+k+k+1 = \frac{k}{2}\ (k+1) + (k+1)$

$$S_{k+1} = 1+2+3+\cdots+k+k+1 = \frac{k}{2}\ ((k+1) + 2\ (k+1))$$
$$= \frac{k+1}{2}\ (k+2)$$
$$= \frac{k+1}{2}[(k+1)+1]$$

Consider
$1^2 + 2^2 + 3^2 + \ldots + n^2 = n(2n+1)(n+1)$ for $n = 1, 2, \ldots .1$
Let S denote the set of all positive integers n for which the above equation is true. We observe that when n= 1, the formula becomes

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

This shows that $1 \in S$. Next assume that $k \in S$ (where k is fixed but unspecified integer) so that
$1^n + 2^2 + 3^2 + - - - + k^2 = \frac{k(2k+1)(K+1)}{6}$
Next assume $(k+1) \in S$, we have $\frac{k(2k+1)(K+1)}{6}$

$$*1^2 + 2^2 + -- + k^2 + (k+1)^2 = \frac{k(2k+1)(K+1)}{6}\ (K+1)^2 \qquad ----- (1)$$
$$= \frac{1}{6}\ (k+1)(k\ (2k+1) + 6(k+1))$$
$$= \frac{1}{6}\ (k+1)\ (2k^2 + k + 6k + 6)$$
$$= \frac{1}{6}\ (k+1)\ (2k^2 + 4k + 3k + 6)$$
$$= \frac{1}{6}\ (k+1)\ [2k\ (k+2) + 3(k+2)]$$
$$= \frac{1}{6}\ (k+1)[(k+2)(2k+3)]$$
$$= \frac{1}{6}\ (k+1)\ [\{(k+1) + 1\}\{2(k+1\}]$$

or from equation (1) we have $(k+1)\ \frac{[k(2k+1)+6(k+1)]}{6}$

$$= (k+1)\ \frac{[2k^2 + 7k + 6]}{6}$$

$$= \frac{(k+1)\ (2k+3)\ (k+2)}{6}$$

Generally in mathematical induction we assume the question to be true for the integer 1, and if it is true for the integer k, then it should also true for k + 1

Questions:
Establish the formulae below by mathematical induction
A $.1 + 3 + 5 + \cdots + (2n-1) = n^2$ for all $n \geq 1$

b $1.2 + 2.3 + 3.4 + \cdots + n\,(n+1) = \frac{n(n+1)(n+2)}{3}$ for all $n \geq 1$
$c.\ 1^2 + 3^2 + 5^2 + \ldots \ldots . + (2n-1)^2 = \frac{n(2n-1)(2n+1)}{3}$ for all $n \geq 1$

Well ordering principle
Every nonempty set S of nonnegative integers contains a least element, that is, there is some integer a $\in$ S such that a $\leq$ b for all b belonging to S.
From the above we can therefore say that the set of positive integers has what is known as the Archimedean property.

Theorem 1: Archimedean property:
If a and b are any positive integers, then there exists a positive integer n such that n.a $\geq$ b.

Proof: Assume that the statement of the theorem is not true, so that for some a and b, n.a < b for every positive integer n.
Then the set S={ b- n a/ n a positive integer} consists entirely of positive integers.

By the Well-ordering principle, S will possess a least element say, b- ma.

But notice that $b-(m+1)$ a also lies in S, since S contains all integers of this form.

We have $b-(m+1)a = (b-ma) - a < b - ma$ contrary to the choice of $b = ma$ as the smallest integer in S. This is because the assumption refuted the Archimedean property, hence the proof.

Note that this method of proof is what is called "proof by contraction".

Theorem 2: Principle of finite induction:
Let S be a set of positive integers with the following properties.

I. The integer 1 belongs to S
II. Whenever the integer k is in S, the next integer, k + 1 must also be in S.
Then S is the set of **all** positive integers.

Theorem 3: Division Algorithm
Given integers a and b with $b > 0$, there exist a unique integer q and r satisfying $a = qb + r \;\; 0 \le r \le b$. The integers q and r are called the quotient and the remainder respectively in the division of a and b. $0 \le r < b$

Corollary 1
If a and b are integers, with $b \neq 0$, then there exist unique integers q and r such that $a = qb + r, 0 \le r < |b|$

Example:
When $b < 0$, let us take $b = -7$. Then for the choices of $a = 1, -2, 61$ and -59, we obtain the expression

$$1 = 0\,(-7) + 1$$
$$-2 = 1(-7) + 5$$
$$61 = -8(-7) + 5$$
$$-59 = 9(-7) + 4$$

Definition 2.
An integer b is said to be divisible by an integer $a \neq 0$, thus $a|b$, if there exists some integer c such that b = ac. We write $a \nmid b$ to indicate that b is not divisible by a.
When $a|b$, we can also say that:

(i)a is a divisor of b
(ii) a is a factor of b or
(iii) b is a multiple of a

Example:
-12 is divisible by 4, since $-12 = 4(-3)$. However, 10 is not divisible by 3.

Theorem 4:.
For integers a, b, c, the following hold,

(a) $a|0, 1|a, a|a$
(b) $a|1 \Leftrightarrow a = \pm 1$
(c) If $a|b$ and $c|d$, then $ac|bd$
(d) If $a|b\, and\; b|c, then\; a|c$
(e) $a|b$ and $b|a \Leftrightarrow a = \pm b$
(f) If $a|b$ and $b \neq 0$, then $|a| \le |b|$
(g) If $a|b$ and $a|c$, then $a|(bx + cy)$ for arbitrary integers x and y

Proof

If $a|b$, then there exists an integer c such that $b = ac$; also, $b \neq 0 \Rightarrow c \neq 0$.
Taking absolute values, we get $|b| = |ac| = |a||c|$ since $c \neq 0$, if follows that $|c| \ge 1$,hence $|b| = |a||c| \ge |a|$.
If $a|b$ and $a|e$, then $\exists$ integers r and s such that $b = ar, c = as$ choose x and y s.t $bx + cy = arx + asy = a(rx + sy)$ since $rx + sy$ is an integer, it implies $a|(bx + cy)$.

Take the rest as exercise.

Definition 2:

(1) If a and b are arbitrary integers, then an integer d is said to be a common divisor of a and b if both $d|a$ and $d|b$. Since 1 is a divisor of every integer, 1 is a common divisor of a and b.

(2) Let a and b be positive integers.

(i) An integer c is called a common factor of a and b, if c is a factor of a and c is $also\ a$ factor of b.

(ii) A positive integer h is called the highest common factor of a and b if h is a common factor of a and b and c divides h for every common factor c of a and b.

(3) eg. Find the $h\ c\ f$ of 18 and 24

solution

$18 = \{1, 2, 3, 6, 9, 18\}$

$24 = \{1, 2, 3, 4, 6, 8, 12, 24\}$

Common factors $= \{1, 2, 3, 6\}$

$\therefore\ h\,cf = 6$

Definition 3:

A positive integer p is called a prime number if $p \geq 2$ and every positive integer which is a factor of p is either 1 or p. eg. $2, 3, 7, \ldots$ .... {A prime number p has two factors, 1 and p}

Definition 4:

Two integers a and b not both of which are zero, are said to be relatively prime whenever $g\,cd\,(a, b) = 1$.

Theorem 5:

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 $1 = ax + by$.

Theorem 6:.

For integers a, b and c, if $a|c$ and $b|c$ and a and b are co prime, then $ab|c$.

Proof:

Since a and b divide c, there exist integers x and y such that $x = by = c$.

By theorem x there exist integers u and v such that

$1 = au + bv. \Rightarrow c = auc + bvc = auby + bvax = ab(uy + vx) \Rightarrow ab|c$

Theorem 7:

If u and v are positive integers and p is a prime number such that p divides uv, then either p divides u or p divides v.

Proof:

Let $uv = gp$ where p is an integer. If p does not divide u then $\gcd(p, u) = 1 \Rightarrow 1 = px + uy$ where x and y are integers , then,

$$v = pxv + uyv$$
$$= pxv + gyp$$
$$= p(xv + gy)$$

Therefore p divides v if p does not divide u.

The Euclidean Algorithm

The greatest common divisor of two integers can of course be found by using all their positive divisors and choosing the largest one common to each; but this is cumbersome for large numbers. A more efficient process, involving repeated application of the Division Algorithm is used. This process is referred to as the Euclidean Algorithm.

Let a and b be two integers whose greatest common divisor is desired.
Since $\gcd(|a|,|b|) = \gcd(a,b)$, we assume a $\geq b > 0$.
Applying Division Algorithm to a and b, we get $a = qx_1 \ \ b + r_1 \ 0 \ \leq \ r_1 < b$. If $r_1 = 0$,
then $b|a$ and the $\gcd(a,b) = b$, if $r_1 \neq 0$, divide b by r_1. $\Rightarrow b = \ q_2\, r_1 + \ r_2 \quad 0 \ \leq \ r_2 \ \leq r$

$$r_1 = \ q_3\, r_2 + \ r_3 \quad 0 \ \leq \ r_3 < \ r_2$$
$$\vdots$$
$$r_{n-2} = \ q_n\, r_{n-1} + \ r_n \quad 0 < \ r_n < \ r_{n-1}$$

Example

By the Euclidean algorithm calculate the gcd $(12378, 3054)$

$$12378 = 4(3054) + \ 162$$
$$3054 = 18\,(162) + \ 138$$
$$162 = 1(138) + \ 24$$
$$138 = 5(24) + \ 18$$
$$24 = 1(18) + 6$$
$$18 = 3(6) + \ 0$$
$$\Rightarrow \gcd(12378, 3054) = 6$$

Exercise

Find gcd $(143, 227)$ and $\gcd(272, 1479)$

Definition 5.

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

$a|m$ and $b|m$

If $a|c$ and $b|c$, with $c > 0$, then $m \ \leq c$

Example:

The positive common multiplies of the integers -12 and 30 are $60, 120, 180, \ldots \ldots$

$$\therefore \ LCM \ (-12, 30) = \ 60$$

Theorem 8.

For positive integers a and b ,$\gcd(a,b)\ lcm(a,b) = ab$.
Let gcd (a,b)=d

$\Rightarrow lcm\,(a,b) = \dfrac{ab}{d}$

Example:
Find the $lcm\,(3054, 12378)$

$$lcm\,(3054, 12378) = \frac{3054\ x\ 12378}{6} = 6{,}300{,}402$$

Exercise:
Find the greatest common divisors of the following pairs of numbers.
1. gcd(56,72)
2. gcd(119,272)
3. gcd(1769,2378)

We can express the greatest common divisor (gcd) of a and b in the form
gcd(a,b)=ax+by

Example:
Express the gcd(56,72) in the form gcd(56,72)=56x+72y
Solution: $72 = 1(56) + 16$
$56 = 3(16) + 8$
$16 = 2(8) + 0$

Now we have

$$\begin{aligned} 8 &= 56 - 3(16) \\ &= 56 - 3[72 - 1(56)] \\ &= 4(56) - 3(72) \end{aligned}$$

Hence x=4 and y=-3

Exercise:
Express the following pairs of numbers in the form ax+by:
(1) gcd(119,272)
(2) gcd(1769,2379)
(3) gcd(78,143)