Contents

Notation:

$\mathbb{N}$ = the set of natural numbers,
$\mathbb{Z}$ = the set of integers,
$\mathbb{Q}$ = the set of rational numbers,
$\mathbb{R}$ = the set of real numbers,
$\mathbb{C}$ = the set of complex numbers.

Special courses in Mathematics

• Students with keen interest in Mathematics can get scholarships to do an integrated 3-year course in Mathematics and Computer Science leading to a B.Sc. degree at Chennai Mathematical Institute (C.M.I.), 92, G. N. Chetty Road, Chennai 600 017. The applications are to be sent by 31st March and the Entrance Exam. is held in May in major cities of India each year. The B.Sc. programme is supported by NBHM and ISRO. Since 2001, C.M.I. has also started a 2-year M.Sc. course with research component. For further information visit the website `http://www.cmi.ac.in` .

• The Indian Statistical Institute has started a 3-year B. Math. (Hons.) Programme at its Bangalore Centre from 2000. The selection is through a written test at various centres all over India followed by an interview. Successful candidates will receive a stipend of Rs. 500/- per month. Limited hostel facilities are available. The emphasis of B. Math. will be on mathematics, however, the programme includes four computer science courses and a course in discrete mathematics which will give a solid foundation for pursuing computer science more seriously at a later stage. There are also courses in physics, probability and statistics which will enable students to take up these fields later if they so desire. The Institute has also started a master's programme in mathematics as a follow-up of this programme. For further information visit the website `http://www.isibang.ac.in` or send e-mail to : `bmath@isibang.ac.in`.

The INMO awardees can get an NBHM scholarship of Rs. 1200 p.m. for the above programmes.

Chapter 1

Number Theory

1.1 Divisibility of Integers

In this section, we see some elementary properties of integers. The reader is familiar with properties of integers such as divisibility, greatest common divisor (highest common factor), least common multiple, prime and composite numbers. In this chapter, we will give definitions and then proofs of the properties which reader quite often have used without proof. Many of the proofs depend on two principles (i) Well Ordering Principle, and (ii) Principle of Mathematical Induction. We first state these two principles.

(i) Well Ordering Principle: Any non-empty subset of non-negative integers has a smallest element.

In other words, if S is a non-empty subset of non-negative integers then there is $a \in S$ such that $a \leq s$ for any s in S.

Principle of Mathematical Induction is a logical consequence of the well ordering principle.

(ii (a)) Principle of Mathematical Induction: If a subset S of positive integers contains 1, and contains $n+1$ whenever it contains n, then S contains all the positive integers.

(ii (b)) Principle of Mathematical Induction(Strong Form): If a subset S of positive integers contains 1, and contains $n+1$ whenever it contains $1, 2, \ldots, n$, then S contains all the positive integers.

Definition 1.1 An integer b is said to be divisible by a non-zero integer a if there is an integer x such that $b = ax$, and we then write $a|b$. In case b is not divisible by a we write $a \nmid b$. The property $a|b$ may also be expressed by saying that 'a divides b' or 'a is a divisor of b' or 'b is a multiple of a'.

Note that 5 divides 10 as $10 = 5 \times 2$. But 5 does not divide 13. We may write this as $5|10$ but $5 \nmid 13$. If an integer is divisible by 2, we say that it is an even integer, otherwise we say that it is an odd integer. Thus, $0, \pm 2, \pm 4$ are even integers while $\pm 1, \pm 3, \pm 5$ are odd integers.

Theorem 1 Let a, b, c, m, x, y be integers.

(*i*) If $a|b$ then $a|bc$ for any integer c.

(*ii*) If $a|b$ and $b|c$ then $a|c$.

(*iii*) If $a|b$ and $a|c$ then $a|bx + cy$ for any integers x and y.

(*iv*) If $a|b$, and $b \neq 0$ then $|a| \leq |b|$.

(*v*) If $a|b$ and $b|a$ then $a = \pm b$.

(*vi*) If $m \neq 0$ then $a|b$ if and only if $ma|mb$.

Proof.

(*i*) If $a|b$, then $b = aq$ where q is an integer. Hence $bc = a(qc)$ for any integer c. Hence, $a|bc$.

(*ii*) If $a|b$ and $b|c$, then $b = aq$ and $c = bq_1$ where q, q_1 are integers. Thus $c = (aq)q_1 = a(qq_1)$. Hence, $a|c$.

(*iii*) If $a|b$ and $a|c$, then $b = aq, c = aq_1$ for $q, q_1 \in \mathbb{Z}$. Hence, $bx + cy = a(qx + q_1y)$. Hence, $a|bx + cy$.

(*iv*) If $a|b$, $b \neq 0$, then $b = aq, q \neq 0$. Hence, $|b| = |aq| = |a||q|$. As $q \neq 0, |q| \geq 1$, hence $|a| \leq |b|$.

(*v*) If $a|b$ then $|a| \leq |b|$. Also, $b|a$, implies $|b| \leq |a|$. Thus, $|a| = |b|$. Hence $a = \pm b$.

(*vi*) If $a|b$, then $b = aq$. Suppose $m \neq 0$. Then $mb = (ma)q$. Hence $ma|mb$. Conversely, if $ma|mb$, then $mb = maq$. Since, $m \neq 0$, we get $b = aq$, that is, $a|b$.

Theorem 2 (Division Algorithm) Given any integers a and b with $a \neq 0$, there exist unique integers q and r such that $b = qa + r, 0 \leq r < |a|$. If $a \nmid b$, then r satisfies the stronger inequality $0 < r < |a|$.

Proof. Consider, $S = \{b - ak | b - ak \geq 0,\ k \in \mathbb{Z}\}$. Clearly, $b + |ab| \in S$. Hence, S is non-empty. By well ordering principle, S has a least element, say r. Since $r \in S, r \geq 0$ and there exists an integer q such that $r = b - aq$. If $r \geq |a|$ then $0 \leq r - |a| < r$ and $r - |a| \in S$, a contradiction. Hence $0 \leq r < |a|$.

Next we prove the uniqueness of q and r. Suppose $b = aq_1 + r_1$ and also $b = aq_2 + r_2$ with $0 \leq r_1 < |a|,\ 0 \leq r_2 < |a|$. If $r_1 \neq r_2$, let $r_1 < r_2$.

Then $0 < r_2 - r_1 < |a|$. But $r_2 - r_1 = a(q_1 - q_2)$. Thus $a|(r_2 - r_1)$. But this contradicts (iv) of the theorem 1. Hence $r_2 = r_1$ and so $q_2 = q_1$.

Example 1 Show that the square of any integer is of the form $4k$ or $8k + 1$.

Solution. By division algorithm (take $a = 2$), any integer b is representable as $2q$ or $2q+1$. If $b = 2q$, then $b^2 = 4q^2$. Thus, b^2 is of the form $4k$. If $b = 2q+1$, then $b^2 = 4q^2 + 4q + 1 = 4q(q + 1) + 1$. Since $q(q + 1)$ is divisible by 2, we get that b^2 is of the form $8k + 1$.

Example 2 Find all integers n such that $n^2 + 1$ is divisible by $n + 1$.

Solution. Let n be an integer such that $(n + 1)|n^2 + 1$. Observe that $n^2 - 1 = (n+1)(n-1)$. Hence $(n+1)|(n^2-1)$ so that $(n+1)|\left[(n^2 + 1) - (n^2 - 1)\right]$ i.e. $(n + 1)|2$. Hence, $n + 1 = \pm 1, \pm 2$. Hence, $n = -3, -2, 0, 1$.

Definition 1.2 An integer d is called a common divisor of a and b in case $d|a$ and $d|b$. Let a, b be integers, not both zero. A positive integer g is said to be the **greatest common divisor** of a and b if and only if the following two conditions are satisfied: (i)$g|a$ and $g|b$ and (ii) if $d|a$ and $d|b$ then $d|g$. The greatest common divisor of a and b is denoted by $\gcd(a, b)$ or (a, b).

In other words, if at least one of a and b is not equal to zero, the greatest among their common divisors is called the greatest common divisor of a and b. It can be shown that such an integer g is unique, if it exists. The existence of g is proved in the following theorem. While, uniqueness follows from the definition.

Theorem 3 (Bezout's Theorem) If a, b are any integers, not both zero, then $\gcd(a, b)$ exists and there exist integers x_0, y_0 such that $\gcd(a, b) = ax_0 + by_0$.

Proof. Consider, $S = \{ax + by | x, y \in \mathbb{Z},\ ax + by > 0\}$. S is non-empty as $a^2 + b^2 \in S$. By well ordering principle, S has a smallest element, say g. Since, $g \in S$, we can write g as $g = ax_0 + by_0$.

Now if $d|a$ and $d|b$ then $d|ax_0 + by_0$ i.e. $d|g$. Secondly, suppose $g \nmid a$. Then $a = gq + r$, $0 < r < g$. Hence $r = a - gq = a(1 - qx_0) + b(-qy_0)$ and $r \in S$. This is a contradiction since $r < g$ and g is the smallest element of S. Hence, $g|a$. Similarly $g|b$. Hence by definition of gcd, we see that g is the gcd of a and b.

Definition 1.3 Two integers a, b which are not both zero, are said to be *relatively prime* or *coprime* if $(a, b) = 1$.

Thus a and b are coprime if and only if their only common divisors are ± 1.

Example 3 Note that 9 and 16 are relatively prime integers. Similarly, 8 and 15 are coprime, while 6 and 15 are not. Any two consecutive integers are relatively prime. Further, any two consecutive odd integers are relatively prime.

Corollary 1 Let a, b be integers, not both zero. Then a, b are coprime if and only if there are integers x, y such that $ax + by = 1$.

Proof. Let a, b be coprime integers. Then $(a, b) = 1$. So, by the Bezout's theorem there exist integers x, y such that $ax + by = (a, b) = 1$. Conversely, if for some integers x and y, we have $ax + by = 1$ and $(a, b) = d$, then $d|a$ and $d|b$ so that $d|(ax + by)$ or $d|1$. Hence $0 < d \leq 1$. So, $d = 1$, that is, x, y are coprime integers.

Corollary 2 If a, b are coprime integers, then every integer n can be expressed as $n = ax + by$ for some integers x, y.

Proof. Let a, b be coprime integers. Then by Bezout's theorem, there exist integers u, v such that $1 = au + bv$. Hence $n = a(nu) + b(nv)$ so that $x = nu, y = nv$ are as required.

Corollary 3 If $d = \gcd(a, b)$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Proof. Let $(a, b) = d$. Then $d|a$ and $d|b$. So $a = rd, b = sd$ for some integers r, s. Now by the above theorem there are integers x, y such that $ax + by = d$. So $rdx + sdy = d$ or $rx + sy = 1$. Hence by Corollary 1, $(r, s) = 1$.

Example 4 Show that there are no integers a, b such that $\gcd(a, b) = 3$ and $a + b = 100$.

Solution. Suppose there exist integers a, b such that $\gcd(a, b) = 3$ and $a + b = 100$. Then $3|a, 3|b$. Hence, $3|a + b$. But $a + b = 100$ and $3 \nmid 100$. Thus, we get a contradiction. Hence, there are no such integers.

Example 5 If $(a, n) = 1$ and $(b, n) = 1$, then $(ab, n) = 1$.

Solution. As $(a, n) = 1$ and $(b, n) = 1$, by Corollary 1, there are integers x, y and u, v such that $ax + ny = 1$ and $bu + nv = 1$. Hence multiplying these we get $ab(xu) + n(vax + ybu + ynv) = 1$. So $(ab, n) = 1$ by Corollary 1.

Or $ax = 1 - ny, bu = 1 - nv$. Hence, $(ab)(xu) = 1 - n(y + v - yv)$. Hence, $(ab)(xu) + n(y + v - yv) = 1$. Hence, $(ab, n) = 1$.

Example 6 For any $x \in \mathbf{Z}$, $\gcd(a, b) = \gcd(a, b + ax)$.

Solution. For let $(a, b) = d, (a, b + ax) = e$. Then for some integers r, s, u, v,

$$\text{(i)}\quad ar + bs = d \quad \text{(ii)}\quad au + (b + ax)v = e.$$

Now $d|a$ and $d|b$ so that $d|e$ by (ii). Similarly, $e|a$ and $e|(b+ax)$ so that $e|b$. Hence $e|d$ by (i). So $d = e$.

Remark 1.1 Thus, if $b = aq + r, 0 \leq r < |a|$ then $(a, b) = (a, r)$.

Theorem 4 (The Euclidean algorithm) Given integers b and $c, c > 0$, we make a repeated application of the division algorithm to obtain a series of equations :

$$\begin{array}{lcll} b & = & cq + r_1, & 0 < r_1 < c, \\ c & = & r_1q_1 + r_2, & 0 < r_2 < r_1, \\ r_1 & = & r_2q_2 + r_3, & 0 < r_3 < r_2, \\ \vdots & & \vdots & \\ r_{j-2} & = & r_{j-1}q_{j-1} + r_j, & 0 < r_j < r_{j-1}, \\ r_{j-1} & = & r_jq_j. & \end{array}$$

Then the $\gcd(b, c)$ of b and c is r_j, the last non-zero remainder in the division process. Moreover, if $(b, c) = bx_0 + cy_0$ then the values of x_0 and y_0 can be obtained by eliminating $r_{j-1}, ..., r_2, r_1$ from the above set of equations.

Proof. If $g = (b, c)$ then $g|b$ and $g|c$. Hence, $g|b - cq$. But, $b - cq = r_1$. Hence, $g|r_1$. Now, $g|c$, $g|r_1$. Hence, $g|r_2$. Continuing this way, we see that $g|r_i$ for $1 \leq i \leq j$. In particular, $g|r_j$. Conversely, note that $r_j|r_{j-1}$. Hence, $r_j|r_{j-1}q_{j-1} + r_j$ i.e. $r_j|r_{j-2}$. Similarly, $r_j|r_{j-3}$. Continuing in this way, we get that $r_j|r_{j-2}, \cdots, r_j|r_1, r_j|c, r_j|b$. Hence, r_j is a common divisor of b and c. Hence, $r_j|(b, c)$ i.e. $r_j|g$. But, $g|r_j$ and both g and r_j are positive integers. Hence $g = r_j$.

Equivalently, one can use Remark (1.1) to prove that $g = r_j$. For

$$(b, c) = (c, r_1) = (r_1, r_2) = \cdots = (r_{j-1}, r_j) = (r_j, 0) = r_j.$$

Remark 1.2

1. We note that in the above theorem, there is no loss of generality in assuming that c is positive for $(b, c) = (b, -c) = (-b, c) = (-b, -c)$ and $(b, 0) = |b|$, as $b \neq 0$.

2. Further, the values of x_0 and y_0 are not unique. For example, $(2, 3) = 1$ and $1 = -1(2) + 1(3)$ and $1 = 2(2) - 3$.

Example 7 Find gcd of 4840 and 1512. Also find x_0, y_0 such that

$$(4840, 1512) = 4840x_0 + 1512y_0.$$

Solution. We have

$$\begin{aligned} 4840 &= 3(1512) + 304 && (1)\\ 1512 &= 4(304) + 296 && (2)\\ 304 &= 1(296) + 8 && (3)\\ 296 &= 37(8) + 0 && (4) \end{aligned}$$

The last nonzero remainder is 8, hence (4840,1512) = 8. Now to find x_0, y_0 such that $8 = 4840x_0 + 1512y_0$, we write (3) as 8 = 304 − 296. Substituting for 296 from (2),

$$8 = 304 - (1512 - 4(304)) = 5(304) - 1512$$

Substituting for 304 from (1),

$$8 = 5(4840 - 3(1512)) - 1512 = 5(4840) - 16(1512)$$

so that $x_0 = 5$, $y_0 = -16$.

Example 8 Prove that the fraction $\dfrac{21n+4}{14n+3}$ is irreducible for every natural number n.

Solution. We want to show that the fraction $\dfrac{21n+4}{14n+3}$ is irreducible for every natural number n, that is, we should show that $(21n + 4, 14n + 3) = 1$ for every natural number n. Now,

$$\begin{aligned} 21n + 4 &= 1(14n + 3) + (7n + 1)\\ 14n + 3 &= 2(7n + 1) + 1\\ 7n + 1 &= 1(7n + 1) \end{aligned}$$

Hence, by Euclidean algorithm, $(21n + 4, 14n + 3) = 1$. Hence, the fraction $\dfrac{21n+4}{14n+3}$ is irreducible for every natural number n.

Definition 1.4 An integer $p > 1$ is called a prime number, or a prime, if it has no divisor d such that $1 < d < p$. If an integer is not a prime then it is called a composite number.

Note that 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 are prime numbers, while 4, 6, 8, 15, 20 are composite numbers.

Example 9 If p is a prime and $p \nmid a$, then $\gcd(p, a) = 1$.

Solution. Let $\gcd(p, a) = d$. Then $d|p$ and $d|a$. But p is a prime. Hence $d = 1$ or $d = p$. Since $p \nmid a$, we cannot have $d = p$. Thus $d = 1$.

Remark 1.3 From the above example, we get that if p is a prime and a is an integer then $(a, p) = \begin{cases} p & \text{if } p|a \\ 1 & \text{otherwise.} \end{cases}$ Further, we get that if p and q are distinct primes then $(p, q) = 1$. Thus, p and q are relatively prime.

Theorem 5 (Euclid's Lemma) If $(a, m) = 1$ and $m|ab$ then $m|b$.
Proof. Since $(a, m) = 1$, there exist integers x, y such that $ax + my = 1$ Hence, $abx + mby = b$. Since, $m|ab$ we get $m|(abx + mby)$. Hence, $m|b$.

Corollary 4 If p is a prime and $p|ab$ then $p|a$ or $p|b$.
Proof. If $p|a$ then we are done. Otherwise, $p \nmid a$. Hence, $(p, a) = 1$. Since, $p|ab$ and $(p, a) = 1$, by Euclid's lemma, we get that $p|b$.

Euclid's lemma can also be generalised for the product of n integers. This proof is based on Principle of Mathematical Induction. Induction is on the number of terms occurring in the product.

Corollary 5 If p is a prime such that $p|a_1a_2 \cdots a_n$, then p divides at least one factor a_i of the product.
Proof. Let $n = 2$. If $p|a_1a_2$ and $p \nmid a_1$. Then $p \mid a_2$ by Euclid's lemma. Hence, the result holds for $n = 2$. Assume that the result holds for the product of n integers. Suppose $p|a_1 \cdots a_na_{n+1}$, then $p|(a_1a_2 \cdots a_n)(a_{n+1})$. Hence, either $p|a_1a_2 \cdots a_n$ or $p|a_{n+1}$. If $p|a_{n+1}$ then we are done. Otherwise, $p|a_1a_2 \cdots a_n$. Hence, by induction hypothesis, $p|a_i$ for some i, $1 \leq i \leq n$. Hence, by principle of mathematical induction, we get the result.

Corollary 6 If $a|m$ and $b|m$ and $(a, b) = 1$, then $ab|m$.
Proof. Let $a|m$. Then $m = an$ for some integer n. Now $b|an$ and $(a, b) = 1$. Hence by the above theorem, $b|n$. Thus $n = bk$ for some integer k and so $m = an = abk$ or $ab|m$.

Example 10 Show that, if p is a prime then $p|\binom{p}{r}$ for $0 < r < p$.

Solution. Note that $\binom{p}{r} = \frac{p!}{r!(p-r)!}$. Hence, $p! = \binom{p}{r} r!(p-r)!$. Note that $p|p!$ and as, $1 \leq r \leq p-1$, $p \nmid r!$ and $p \nmid (p-r)!$. Hence, using Euclid's lemma, we get $p|\binom{p}{r}$.

Thus, if p is an odd prime then p divides $\sum_{r=1}^{p-1} \binom{p}{r}$ i.e. $p|(2^p - 2)$. Further, we can use principle of Mathematical induction and Binomial theorem[1] to prove that $p|(n^p - n)$ for $n \in \mathbb{N}$ and in fact for every integer n. This result is called Fermat's Little theorem.

Example 11 Prove that if p is a prime, then $\sqrt{p}$ is an irrational number.

Solution. Suppose $\sqrt{p}$ is a rational number, say $\frac{a}{b}$, where a, b are relatively prime integers. Hence, $p = \frac{a^2}{b^2}$. Thus, $pb^2 = a^2$. Hence, $p|a^2$. By Euclid's lemma, $p|a$. Hence, $p^2|a^2$. But $a^2 = pb^2$. Hence, $p|b^2$. Hence, $p|b$, a contradiction. Hence, $\sqrt{p}$ is an irrational number.

Similarly, we can prove that if p is a prime, then $\sqrt[n]{p}$ is an irrational number, where n is an integer greater than or equal to 2. More generally if a is a positive integer which is not a perfect n-th power, then $\sqrt[n]{a}$ is irrational.

Fermat Numbers. The integers $F_n = 2^{2^n} + 1$, $n \geq 0$, are called Fermat Numbers. $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ and $F_4 = 65537$ are primes, but $F_5 = 4,294,967,297$ is divisible by 641. Primes among Fermat numbers are called Fermat primes. Gauss (1801) proved that if m is a Fermat prime then a regular polygon of m sides can be constructed just using ruler and compass. It is not known whether there are infinitely many Fermat primes. In fact, $F_0, F_1, \ldots, F_4$ are the only known Fermat primes.It is known that F_n is composite if $5 \leq n \leq 32$.

Example 12
(*i*) $F_n - 2 = F_0 F_1 \cdots F_{n-1}$, $n \geq 1$.
(*ii*) Any two Fermat numbers are relatively prime.

Solution. (i) (Induction on n) The result is true for $n = 1$. Assuming it true for $n-1$, we get

$$\begin{aligned} F_n - 2 = 2^{2^n} - 1 &= (2^{2^{n-1}} + 1)(2^{2^{n-1}} - 1) = F_{n-1}(F_{n-1} - 2) \\ &= F_{n-1} \cdot F_{n-2} \cdots F_0 \text{ by induction assumption.} \end{aligned}$$

[1] Binomial Theorem $(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r}$

Hence by induction (i) holds for all $n \geq 1$.
(ii) Let $m < n$. If $d|F_n$ and $d|F_m$, then by (i), $d|(F_n - 2)$. Hence $d|2$ as $F_n-(F_n-2) = 2$. Thus, $d = 1$ or 2. As F_n is odd, $d = 1$. Thus, $(F_m, F_n) = 1$.

Lemma 1.1 Every integer $n > 1$ can be expressed as a product of primes (with perhaps only one factor).

Proof. If the integer $n = 2$ then it is a prime, hence the integer itself stands as a product with a single prime factor. Suppose the result holds for all the integers k such that $2 \leq k \leq m$.

If the integer $n = m + 1$ is a prime, the integer itself stands as a product with a single prime factor. Otherwise n can be factored into, say, $n_1 n_2$, where $1 < n_1 < n$ and $1 < n_2 < n$. As $2 \leq n_1 \leq m, 2 \leq n_2 \leq m$, by induction hypothesis, n_1, n_2 can be written as product of primes. Hence, $n_1 n_2$ can be written as product of primes. Hence, by induction, the result holds for all the integers $n \geq 2$.

Remark 1.4 In this proof, we have used strong form of Principle of Mathematical Induction.

We now state the following important theorem. The proof of this theorem uses Euclid's Lemma and is left as an exercise to the reader.

Theorem 6 (The Fundamental theorem of Arithmetic) Every positive integer $n > 1$ can be expressed as product of primes in a unique way except for the order of the prime factors.

Remark 1.5 Fundamental theorem of Arithmetic implies that every integer $n > 1$ can be written as $n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$, where $p_i \neq p_j$ whenever $i \neq j$. In fact, one may assume that $p_i < p_j$ whenever $i < j$.

Notes.

1. A number $n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ is a perfect square if and only if each of $a_1, a_2, \dots, a_r$ is even. If $n = p_1 p_2 \dots p_r$ (i.e. if each of $a_1, a_2, \dots, a_r$ is equal to 1) then n is called a square-free integer. (Note that $p_1, p_2, \dots p_r$ are distinct primes.)

2. If a, b are positive integers such that $ab = c^2$ and $(a, b) = 1$, then a and b are both perfect squares.

Proof of 2. Let $ab = c^2$ for some $c \in \mathbb{N}$. Then the result clearly holds if one of a, b equals 1. Hence let $a > 1$ and $b > 1$ so that $c > 1$. Write a, b, c in canonical form thus :

$$a = p_1^{d_1} \cdots p_m^{d_m}, \quad b = q_1^{e_1} \cdots q_n^{e_n}, \quad c = s_1^{k_1} \cdots s_r^{k_r}.$$

Then $ab = c^2$ becomes

$$p_1^{d_1} \cdots p_m^{d_m} \cdot q_1^{e_1} \cdots q_n^{e_n} = s_1^{2k_1} \cdots s_r^{2k_r}.$$

Now note that since $(a, b) = 1$, the primes $p_1 \ldots, p_m$ are all different from the primes $q_1 \ldots, q_n$. Hence by the unique factorisation theorem, it follows that $p_1, \ldots p_m, q_1 \ldots, q_n$ is only a rearrangement of $s_1, \ldots, s_r$ and that the indices $d_1, \ldots, d_m, e_1, \ldots, e_n$ form a similar rearrangement of $2k_1, \ldots, 2k_r$. Hence each of d_i and e_j is an *even* number and so both a and b are perfect squares. Similarly, if $ab = c^n$ for some $c, n \in \mathbb{N}$, and $(a, b) = 1$, then $a = x^n$ and $b = y^n$ for some $x, y \in \mathbb{N}$.

3. Using unique factorisation we can express the gcd of two numbers in terms of their prime factors. For this we allow zero indices for the prime powers so that the *same* set of primes can be used to represent both the positive integers, say a, b. Thus let

$$a = p_1^{d_1} \cdots p_n^{d_n}, \quad b = p_1^{e_1} \cdots p_n^{e_n}, \qquad \text{(i)}$$

where $p_1, \ldots, p_n$ are distinct primes and $d_i \geq 0, e_i \geq 0$. Then

$$(a, b) = \gcd(a, b) = p_1^{\min\{d_1, e_1\}} \ldots p_n^{\min\{d_n, e_n\}} \qquad \text{(ii)}$$

For example, for $a = 819$, $b = 658$,

$$a = 2^0 \cdot 3^2 \cdot 7^1 \cdot 13^1 \cdot 47^0, b = 2^1 \cdot 3^0 \cdot 7^1 \cdot 13^0 \cdot 47^1,$$

so that $\gcd(a, b) = 2^0 \cdot 3^0 \cdot 7^1 \cdot 13^0 \cdot 47^0 = 7.$

Definition 1.5 Let a, b be non-zero integers. An integer m is called a common multiple of a and b in case $a|m$ and $b|m$. A positive integer l is said to be **least common multiple** (lcm) of a and b if and only if the following two conditions are satisfied: (i) $a|l$ and $b|l$ and (ii) if $a|m$ and $b|m$ then $l|m$.

The least common multiple of a and b is denoted by $[a, b]$.

In other words, the least integer among all the positive common multiples of a and b is called the least common multiple of a and b.

First, it can be shown that the lcm of a, b is unique, if it exists. Secondly, lcm$[a, b]$ always exists. To prove this, express a, b as in (i) above. Then it is easy to see that the integer

$$h = p_1^{\max\{d_1,e_1\}} \cdots p_n^{\max\{d_n,e_n\}} \quad \text{(iii)}$$

satisfies the properties (i) and (ii) above and so $h = [a, b]$. For example, for the above factorisation of $a = 819$ and $b = 658$, we get

$$[a, b] = 2^1 \cdot 3^2 \cdot 7^1 \cdot 13^1 \cdot 47^1 = 76986.$$

Finally, multiplying (ii) and (iii) and comparing the result with the factorisation of the product ab, namely, $p_1^{d_1+e_1} \cdots p_n^{d_n+e_n}$, it follows that

$$ab = (a, b)[a, b].$$

Example 13 The sum of two positive integers is 52 and their lcm is 168. Find the numbers.

Solution. Let the positive integers be a and b and $a \leq b$. Let $d = (a, b)$ so that $a = dm$, $b = dn$ and $(m, n) = 1$. Thus (i) $a + b = d(m + n) = 52 = 4 \times 13$ and (ii) l.c.m. of $a, b = dmn = 168 = 4 \times 2 \times 7 \times 3$. But $((m+n)d, mnd) = d$, since $(m, n) = 1$. Hence by (i) and (ii), $d = 4$. So $m + n = 13$ and $mn = 42$. Hence, $m = 6, n = 7$ and $a = dm = 24$, $b = dn = 28$.

Theorem 7 There are infinitely many primes.

Proof. (Euclid) Assume that there are finitely many primes, say $2 = p_1, p_2, \cdots, p_r$. Let $N = p_1 p_2 \cdots p_r + 1$. Note that $N > 1$ hence N has a prime factor. Clearly none of the p_j's divide N. Hence, the prime factor of N is is a new prime, a contradiction. Hence, there are infinitely many primes.

(Kummer) Assume that there are finitely many primes, say $2 = p_1, p_2, \cdots, p_r$. Let $N = p_1 p_2 \cdots p_r - 1$. Clearly $N > 2$ hence N has a prime factor. None of the p_j's divide N. Hence, this prime is a new prime, a contradiction. Hence, there are infinitely many primes.

(Using Fermat Numbers, Pölya) Let p_i be a prime divisor of the Fermat number F_i, $i \geq 0$. For $i \neq j$, $(F_i, F_j) = 1$, so $p_i \neq p_j$. This gives us infinitely many primes $\{p_i\}_{i \geq 0}$.

Example 14 There are infinitely many primes of the type $4n - 1$.

Solution. Assume that there are finitely many primes of the type $4n - 1$, say $p_1 = 3, p_2, \cdots, p_r$. Let $N = 4p_1 p_2 \cdots p_r - 1$. Clearly $N > 2$ and is odd. Moreover, none of the p_j's divide N. Further, since N is of the type $4n - 1$, N

must have a prime factor of the type $4n-1$. Hence, this prime is a new prime of the type $4n-1$, a contradiction. Hence, there are infinitely many primes of the type $4n-1$.

Theorem 8 Given any positive integer n, there exist n consecutive composite integers.

Proof. Consider the n integers

$$(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+n, (n+1)!+(n+1).$$

Note that k divides $(n+1)!+k$ if $2 \leq k \leq (n+1)$ and $(n+1)!+k > k$. Thus, every number of the sequence is a composite number. Hence, we get n consecutive composite numbers. Thus, there are arbitrarily large gaps in the sequence of primes.

Example 15 If p is a prime greater than 3 then show that $2p+1$ and $4p+1$ cannot be primes simultaneously.

Solution. Since p is a prime greater than 3, p is either of the type $3k+1$ or $3k+2$. If p is of the type $3k+1$ then $2p+1 = 2(3k+1)+1 = 6k+3 = 3(2k+1)$. Hence, $3|(2p+1)$ and $2p+1$ cannot be a prime. Similarly, if p is of the type $3k+2$ then 3 divides $4p+1$ and it cannot be a prime.

Exercise Set - 1.1

1. Prove that no integer in the sequence 11, 111, 1111, ... is a perfect square.

2. Show that for any positive integer m, $(ma, mb) = m(a,b)$.

3. Show that if $d|a$ and $d|b$ and $d > 0$ then $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a,b)}{d}$.

4. Let d be any positive integer not equal to 2, 5 or 13. Show that one can find distinct a, b in the set $2, 5, 13, d$ such that $ab-1$ is not a perfect square (I.M.O. 1986).

5. By using Euclidean algorithm find the gcd of (i) 7645 and 2872 (ii) 3645 and 2357. Also express the gcd as the linear combination of the given numbers.

6. Find $(a^{2^m}+1, a^{2^n}+1)$. Hence, show that there are infinitely many primes. (Due to Pölya.)

7. Let a, b, c be integers such that $(a, b) = 1,\ c > 0$. Prove that there is an integer x such that $(a + bx, c) = 1$.

8. Show that there are infinitely many primes of the type $6n - 1$.

9. Show that product of three consecutive integers is divisible by 3! while the product of four consecutive integers is divisible by 4!.

10. Suppose m, n are integers and $m = n^2 - n$. Then show that $m^2 - 2m$ is divisible by 24.

11. A printer numbers the pages of a book starting with 1 and uses 3189 digits in all. How many pages does the book have?

12. Show that any integer divisible by 3 can be written as a sum of cubes of four integers. (Example. $6 = 2^3 + (-1)^3 + (-1)^3 + 0^3$.)

13. Let $p > 3$ be an odd prime. Suppose $\sum_{k=1}^{p-1} \frac{1}{k} = \frac{a}{b}$, where $(a, b) = 1$. Prove that a is divisible by p.

14. Prove that if $n \geq 4$ then $n, n + 2, n + 4$ cannot all be primes.

15. If $2 = p_1 < p_2 < \ldots < p_n$ where p_i are primes, show that the number $p_1 p_2 \cdots p_n + 1$ can never be a perfect square.

16. Prove that, if $n > 4$, then the number $1! + 2! + 3! + \cdots n!$ is never a square.

17. The gcd of two positive integers is 81 and their l.c.m. is 5103. Find the numbers.

18. Prove that there are infinitely many positive integers a such that $2a$ is a square, $3a$ is a cube and $5a$ is a fifth power.

19. If a, b are positive integers such that the number $(a + 1)/b + (b + 1)/a$ is also an integer, then prove that gcd $(a, b) \leq \sqrt{a + b}$.

20. If $2^n - 1$ is a prime, show that n is a prime.

21. If $2^n + 1$ is a prime, show that n is a power of 2.

22. Find all integers x and y such that $(x, y) = 8$ and $[x, y] = 64$.

23. If $(a, b) = [a, b]$ then show that $a = \pm b$.

24. Show that if n is an odd integer, then $16|n^4 + 4n^2 + 11$.

25. Find all integers which leave remainder 1 when divided by 3, remainder 2 when divided by 4, ..., remainder 8 when divided by 10.

26. Show that an integer $n > 1$ is a composite number if and only if it has a prime divisor d such that $d \leq \sqrt{n}$.

27. If $(a, 4) = (b, 4) = 2$ then show that 4 divides $a + b$.

28. Show that there are infinitely many integers a, b such that $(a, b) = 5$ and $a + b = 100$.

29. Given any non-zero integers a, b and n, prove that there exist integers k, l whose gcd is 1 and for which $n|ak + bl$.

30. Let a, b, m, n be natural numbers, $a > 1$, and suppose that a, b have no common factor. Prove that if $a^m + b^m$ is divisible by $a^n + b^n$, then m is divisible by n.

1.2 Congruences

A *congruence* is a convenient statement about divisibility. The notion of congruence was introduced by C. F. Gauss (1777-1855) in his famous book Disquisitions Arithmeticae, written at age 24. It gained ready acceptance as a fundamental tool for the study of number theory.

Definition 1.6 Let m be a non-zero integer. The integers a and b are said to be congruent *modulo* m if and only if $m|a - b$, and written $a \equiv b \pmod{m}$.

Since, $a - b$ is divisible by m if and only if $a - b$ is divisible by $-m$, we will confine our attention to a positive modulus.

For example, $19 \equiv 1 \pmod{6}$. We can also say that x is even if $x \equiv 0 \pmod{2}$ and x is odd if $x \equiv 1 \pmod{2}$. Further, if x is even then $x^2 \equiv 0 \pmod{4}$ and if x is odd then $x^2 \equiv 1 \pmod{4}$.

Theorem 9 Let a, b, c, d, x, y denote integers. Then,

1. $a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$, and $a - b \equiv 0 \pmod{m}$ are equivalent statements.

2. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

3. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$ax + cy \equiv bx + dy \pmod{m}.$$

4. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$. In particular, if $a \equiv b \pmod{m}$ then $a^k \equiv b^k \pmod{m}$ for every positive integer k.

5. If $a \equiv b \pmod{m}$ and $d|m$, then $a \equiv b \pmod{d}$.

Proof:

1. Suppose $a \equiv b \pmod{m}$. Then, by definition, $m|a-b$. Now, $m|a-b$ if and only if $m|b-a$ if and only if $m|a-b-0$. Hence, $a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$, and $a - b \equiv 0 \pmod{m}$ are equivalent statements.

2. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $m|a-b$ and $m|b-c$. Hence, $m|a-c$ i.e. $a \equiv c \pmod{m}$.

3. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $m|a-b$ and $m|c-d$. Hence, $m|(a-b)x$ and $m|(c-d)y$. Hence, $m|(ax+cy)-(bx+dy)$ i.e.

$$ax + cy \equiv bx + dy \pmod{m}.$$

4. $m|(a-b)$ and $m|(c-d) \Rightarrow m|[c\cdot(a-b)+b\cdot(c-d)] \Rightarrow$ $m|(ac-bd) \Rightarrow ac \equiv bd \pmod{m}$.

   Equivalently, we can take $x = c$ and $y = b$ in 3 above to get the same result.

5. If $a \equiv b \pmod{m}$ then $m|a-b$. But $d|m$, hence, $d|a-b$ i.e. $a \equiv b \pmod{d}$.

Theorem 10 Let $f(x)$ denote a polynomial with integral coefficients. If $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$.

Proof: Assume that $f(x) = c_0 + c_1x + \cdots + c_nx^n$, where c_i's are integers. Since, $a \equiv b \pmod{m}$, we get $a^2 \equiv b^2 \pmod{m}, \ldots, a^n \equiv b^n \pmod{m}$. Hence, for every $j, 0 \le j \le n$, we get $c_ja^j \equiv c_jb^j \pmod{m}$. Hence,

$$\sum_{j=0}^{n} c_ja^j \equiv \sum_{j=0}^{n} c_jb^j \pmod{m},$$

that is $f(a) \equiv f(b) \pmod{m}$.

Theorem 11 Let $a, b, x, y, m, m_1, \ldots, m_r$ be integers. Then,

1. $ax \equiv ay \pmod{m}$ if and only if $x \equiv y \pmod{\frac{m}{(a,m)}}$.
2. If $ax \equiv ay \pmod{m}$ and $(a,m) = 1$ then $x \equiv y \pmod{m}$.
3. $x \equiv y \pmod{m_i}$ for $i = 1, 2, \ldots, r$ if and only if $x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}$.

Proof.

1. If $ax \equiv ay \pmod{m}$ then $ax - ay = mq$ for some integer q. Hence, we have
$$\frac{a}{(a,m)}(x-y) = \frac{m}{(a,m)}q$$
and thus $\frac{m}{(a,m)} \mid \frac{a}{(a,m)}(x-y)$. But $\left(\frac{a}{(a,m)}, \frac{m}{(a,m)}\right) = 1$. Hence, we get $\frac{m}{(a,m)} \mid (x-y)$, that is, $x \equiv y \pmod{\frac{m}{(a,m)}}$.

   Conversely, if $x \equiv y \pmod{\frac{m}{(a,m)}}$ then $\frac{m}{(a,m)} \mid (x-y)$. This implies that $m \mid a(x-y)$, that is, $ax \equiv ay \pmod{m}$.

2. If $ax \equiv ay \pmod{m}$ and $(a,m) = 1$ then $x \equiv y \pmod{\frac{m}{(a,m)}}$. But $(a,m) = 1$ hence we get $x \equiv y \pmod{m}$.

3. If $x \equiv y \pmod{m_i}$ for $i = 1, 2, \ldots, r$ then $m_i \mid x - y$ for $i = 1, 2, \ldots, r$. That is, $x - y$ is a common multiple of $m_1, \ldots, m_r$ and therefore $x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}$.

   Conversely, if $x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}$ then $m_i \mid [m_1, \ldots, m_r]$ for $1 \leq i \leq r$. Hence, $x \equiv y \pmod{m_i}$ for $i = 1, 2, \ldots, r$.

Proposition 1 If $b \equiv c \pmod{m}$ then $(b,m) = (c,m)$.

Proof. Since, $b \equiv c \pmod{m}$ we get $b = c + qm$. Hence, $(c,m) \mid b$ and hence, $(c,m) \mid (b,m)$. Also, $c = b - qm$ implies that $(b,m) \mid c$ and hence $(b,m) \mid (c,m)$. As both (b,m) and (c,m) are positive, we get $(b,m) = (c,m)$.

Example 16 Find the remainder when $13^{73} + 14^3$ is divided by 11.

Solution. We note that $13 \equiv 2 \pmod{11}$ and $14 \equiv 3 \pmod{11}$. Hence,

$$14^3 \equiv 3^3 \equiv 5 \pmod{11}. \qquad (1)$$

Also, $2^5 \equiv -1 \pmod{11}$. Hence, $2^{70} \equiv 1 \pmod{11}$ and $2^{73} \equiv 8 \pmod{11}$. Thus,

$$13^{73} \equiv 2^{73} \equiv 8 \pmod{11}. \qquad (2)$$

Adding the congruences (1) and (2), we get

$$13^{73} + 14^3 \equiv 8 + 5 \equiv 2 \pmod{11}.$$

Hence, 2 is the remainder when $13^{73} + 14^3$ is divided by 11.

Example 17 Show that a number is divisible by 3 if and only if the sum of its digits is divisible by 3.

Solution. Let n be a given number. n can be written as

$$n = n_0 + 10n_1 + \cdots + 10^k n_k,$$

where $0 \leq n_0, n_1, \ldots, n_k \leq 9$. Note that $10 \equiv 1 \pmod{3}$. Hence, for every positive integer m $10^m \equiv 1 \pmod{3}$. Hence, $n \equiv n_0 + n_1 + \cdots + n_k \pmod{3}$. This implies that n is divisible by 3 if and only if the sum of its digits is divisible by 3.

The above argument also works if we replace 3 by 9 i.e. a number is divisible by 9 if and only if the sum of its digits is divisible by 9.

Example 18 If p and q are primes such that $p = q + 2$, prove that $p^p + q^q$ is a multiple of $p + q$.

Solution. We note that as p and q are primes such that $p = q + 2$, both p and q are odd primes. Hence, $q - 1$ is even. Consider

$$\begin{aligned} p^p + q^q = (p + q - q)^p + q^q &\equiv (-q)^p + q^q \pmod{p+q} \\ &\equiv -q^q(q^2 - 1) \pmod{p+q} \end{aligned}$$

Now $p + q = 2q + 2$ and $2|q - 1$. Hence, $p + q = 2(q + 1)$ divides $q^2 - 1$. Hence, $p^p + q^q \equiv 0 \pmod{p+q}$, that is, $p^p + q^q$ is a multiple of $p + q$.

Example 19 If a, b are integers, p a prime, then show that

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

Solution. We note that

$$\begin{aligned} (a+b)^p &= a^p + \binom{p}{1} a^{p-1}b + \cdots + \binom{p}{p-1} ab^{p-1} + b^p \\ &\equiv a^p + b^p \pmod{p} \end{aligned}$$

as $\binom{p}{1}, \cdots, \binom{p}{p-1}$ are divisible by p. Thus, in particular,

$$(a+1)^p \equiv a^p + 1 \pmod{p}.$$

Further, if $a = 1$ then $2^p \equiv 2 \pmod{p}$. Thus, by induction, we can prove that $n^p \equiv n \pmod{p}$ for every integer n. [2]

Example 20 Prove that for any natural number n the expression $A = 2903^n - 803^n - 464^n + 261^n$ is divisible by 1897.

Solution. Let n be a natural number. Note that $1897 = 7 \times 271$. Consider the expression $A = 2903^n - 803^n - 464^n + 261^n$. Now $2903 \equiv 803 \pmod{7}$ and $464 \equiv 261 \pmod{7}$. Also, $2903 \equiv 464 \pmod{271}$ and $803 \equiv 261 \pmod{271}$. Hence, A is divisible by 7 as well as 271. Since $(7, 271) = 1$, we get that A is divisible by 1897.

Example 21 Let a be a rational number. Show that if $11 + 11\sqrt{11a^2+1}$ is an odd integer, then it must be a perfect square.

Solution. As $11 + 11\sqrt{11a^2+1}$ is an odd integer, $11a^2 + 1$ must be the square of a rational number b of the form $b = c/11$ where c is an integer. Now $11a^2 + 1 = c^2/11^2$, hence a can have 11 in the denominator. Let $a = d/11$. Then $11d^2 + 11^2 = c^2$. Hence $11 \mid c$, i.e. b is an integer and $11a^2 + 1 = b^2$. Now $11\dfrac{d^2}{11^2} + 1 = b^2$ i.e. $d^2 = 11(b^2 - 1)$, so that $11 \mid d$. Hence a is an integer.

If $11 + 11\sqrt{11a^2+1}$ is an odd integer, then $11a^2 + 1$ must be the square of an even integer. Let $11a^2 + 1 = 4m^2$, so that $11a^2 = (2m-1)(2m+1)$. Now $(2m-1, 2m+1) = 1$ hence, by Note 2 §1, either $2m - 1 = 11e^2$ and $2m + 1 = f^2$ or $2m - 1 = e^2$ and $2m + 1 = 11f^2$. In the first case, $f^2 - 11e^2 = 2$, so that $f^2 \equiv 2 \pmod{11}$. This is impossible, as the only squares (mod 11) are 1, 3, 4, 5, 9. Hence $2m - 1 = e^2$ and $2m + 1 = 11f^2$. Hence

$$11 + 11\sqrt{11a^2+1} = 11 + 11(2m) = 11 + 11(11f^2 - 1) = (11f)^2,$$

which is a perfect square.

Example 22 Prove that $2^p + 3^p$ is not a perfect power (i.e. a perfect square, cube etc.) if p is a prime number.

[2] This is called Fermat's Little Theorem.

Solution. If $p = 2$, then $2^2 + 3^2 = 13$ is not a perfect power.

Suppose that p is odd. Then $2^p + 3^p = (2+3)\sum_{k=0}^{p-1}(-1)^k 2^{p-1-k}3^k$.

Now $3 \equiv -2 \pmod 5$. Hence, modulo 5, the sum

$$\sum_{k=0}^{p-1}(-1)^k 2^{p-1-k}3^k \equiv \sum_{k=0}^{p-1}(-1)^k 2^{p-1-k}(-2)^k \equiv p2^{p-1} \pmod 5.$$

Hence, if $p \neq 5$, then $2^p + 3^p = 5n$, where $n \not\equiv 0 \pmod 5$, so that $2^p + 3^p$ is not a perfect power. Finally, $2^5 + 3^5 = 275$ is not a perfect power.

Example 23 Let $f(m,n) = 36^m - 5^n$, where m, n are natural numbers. Find the smallest value of $|f(m,n)|$. Justify your answer.

Solution. We note that $f(1,2) = 11$. Further $f(m,n)$ is odd, $f(m,n)$ is not a multiple of 3 and $f(m,n) \equiv 1 \pmod 5$. Thus the only possible value less than 11 that $|f(m,n)|$ can take is 1. We now show that $|f(m,n)| \neq 1$. Now

$$|f(m,n)| = 1 \Rightarrow 36^m - 5^n = \pm 1 \Rightarrow 36^m \pm 1 = 5^n.$$

But modulo 5, $36^m + 1 = 5^n$ gives $2 \equiv 0 \pmod 5$, a contradiction and going modulo 4, $36^m - 1 = 5^n$ gives $-1 \equiv 1 \pmod 4$, a contradiction. Thus, the smallest value of $|f(m,n)| = 11$.

Exercise Set -1.2

1. Show that the square of an odd integer is $\equiv 1 \pmod 8$.
2. Show that the square of an integer is $\equiv 0$ or $1 \pmod 3$.
3. Find all primes p such that both p and $p^2 + 8$ are primes.
4. Show that the square of an integer is $\equiv 0,\ 1,\ -1 \pmod 5$.
5. Show that if $2n + 1$ and $3n + 1$ are both perfect squares then $40|n$.
6. If an integer n is coprime to 6 then show that $n^2 \equiv 1 \pmod{24}$.
7. Let n be an integer. Show that if $2 + 2\sqrt{28n^2 + 1}$ is an integer, then it must be a perfect square.
8. If $a \equiv b \pmod{m^n}$ then prove that $a^m \equiv b^m \pmod{m^{n+1}}$.
9. If $(a,b) = 1$, then show that $\gcd\left(\frac{a^p - b^p}{a-b}, a-b\right) = 1$ or p.

1.3 Theorems of Fermat, Euler, Wilson and Lagrange

Definition 1.7 If $x \equiv y \pmod{m}$ then y is called a residue of x modulo m. A set $x_1, \ldots, x_m$ is called a **complete residue system** modulo m if for every integer y there exists unique x_j such that $y \equiv x_j \pmod{m}$.

Definition 1.8 A **reduced residue system** modulo m is a set of integers r_i such that $(r_i, m) = 1$, $r_i \not\equiv r_j \pmod{m}$ if $i \neq j$, and such that every x prime to m, is congruent to some member r_i of the set.

Example 24 Let m be any positive integer. Then $\{0, 1, 2, \ldots, m-1\}$ is a complete residue system modulo m. If $m = p$, a prime then $\{1, 2, \ldots, p-1\}$ is a reduced residue system modulo p. $\{1, 5\}$ is a reduced residue system modulo 6 while $\{1, 3, 7, 9\}$ is a reduced residue system modulo 10. We also note that $\{1, 3, 3^3, 3^3\}$ is also a reduced residue system modulo 10.

Theorem 12 Let $(a, m) = 1$. Let $r_1, \ldots, r_n$ be a complete or reduced residue system modulo m. Then $ar_1, \ldots, ar_n$ is a complete or reduced residue system modulo m.

Definition 1.9 The number $\phi(m)$ is the number of positive integers less than or equal to m and relatively prime to m.

Equivalently, $\phi(m)$ is the number of elements in a reduced residue system modulo m. For example, $\phi(6) = 2, \phi(8) = 4, \phi(11) = 10$ and $\phi(p) = p - 1$ if and only if p is a prime.

Theorem 13 For $n \geq 1$, $\sum_{d|n} \phi(d) = n$.

Proof. Let $S = \{1, 2, \ldots, n\}$. For every positive divisor d of n, let

$$S_d = \{m \in S \mid \gcd(m, n) = d\}.$$

Then, clearly, these sets S_d are pairwise disjoint and their union is S. Also $\gcd(m, n) = d$ if and only if $\gcd(m/d, n/d) = 1$. Hence the number of integers in the set S_d is equal to the number of positive integers $\leq n/d$ which are relatively prime to n/d; i.e. equal to $\phi(n/d)$. Hence $n = \sum_{d|n} \phi\left(\frac{n}{d}\right)$. But as d runs through all positive divisors of n, so does n/d. Hence

$$\sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d) = n.$$

Theorem 14 (Euler's theorem) Let a, m be integers such that $(a, m) = 1$. Then

$$a^{\phi(m)} \equiv 1 \pmod{m}. \tag{5}$$

Proof. Let $r_1, r_2, \cdots, r_{\phi(m)}$ be a reduced residue system modulo m. Since $(a, m) = 1$, using Theorem 12, $ar_1, ar_2, \cdots, ar_{\phi(m)}$ is also a reduced residue system modulo m. Hence we get,

$$\prod_{i=1}^{\phi(m)} ar_i = a^{\phi(m)} \prod_{i=1}^{\phi(m)} r_i \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m}.$$

That is, $m \mid \prod_{i=1}^{\phi(m)} r_i(a^{\phi(m)} - 1)$. Since, $(\prod_{i=1}^{\phi(m)} r_i,\ m) = 1$, using Euclid's lemma we get $m \mid a^{\phi(m)} - 1$. Hence, the theorem.

Theorem 15 (Fermat's theorem) Let p be a prime and a be an integer. Then

$$a^p \equiv a \pmod{p}. \tag{6}$$

Proof. If $p \mid a$ then $a^p \equiv a \pmod{p}$. If $p \nmid a$ then $(a, p) = 1$. Since, $\phi(p) = p - 1$, using (5) we get $a^{p-1} \equiv 1 \pmod{p}$, hence $a^p \equiv a \pmod{p}$.

Example 25 If $n \in \mathbb{N}$ and $(n, 35) = 1$, prove that $n^{12} \equiv 1 \pmod{35}$.
Solution. Since n and $35 = 5 \times 7$ have no common factor, we see that $5 \nmid n$ and $7 \nmid n$. Hence by Euler's theorem, $n^4 \equiv 1 \pmod{5}$ and $n^6 \equiv 1 \pmod{7}$ since $5, 7$ are primes. Now

$$n^{12} - 1 = (n^4 - 1)(n^8 + n^4 + 1) \text{ and } n^{12} - 1 = (n^6 - 1)(n^6 + 1).$$

So, $5 \mid (n^{12} - 1)$ and $7 \mid (n^{12} - 1)$ and so 5×7 i.e. 35 divides $(n^{12} - 1)$ since $(5, 7) = 1$.

Example 26 Find the last two digits of the number $7^{100} - 3^{100}$.
Solution. To find the last two digits of a number means to find the remainder when that number is divided by 100. Note that $100 = 25 \times 4$ and $(25, 4) = 1$.

Also, $7 \equiv 3 \pmod{4}$ and this implies that $7^{100} \equiv 3^{100} \pmod{4}$. Now $(7, 25) = (3, 25) = 1$. By Euler's theorem $7^{20} \equiv 1 \pmod{25}$ and $3^{20} \equiv 1 \pmod{25}$. Thus, $7^{20} \equiv 3^{20} \pmod{25}$ and we get $7^{100} \equiv 3^{100} \pmod{25}$. Since, $(25, 4) = 1$ we get that $7^{100} \equiv 3^{100} \pmod{100}$. Thus, the last two digits of the number $7^{100} - 3^{100}$ are 00.

Example 27 If p, q are odd primes such that $2p = q + 1$, and a is relatively prime to 2, p and q, prove that $a^{2(p-1)} \equiv 1 \pmod{16pq}$.
Solution. Note that a is odd as a is relatively prime to 2. Now, $a^{2(p-1)} - 1 = (a^{p-1} - 1)(a^{p-1} + 1)$. Since, p is an odd prime, $p - 1$ is even and $a^{p-1} - 1$ is divisible by 8. Also, $a^{p-1} + 1$ is divisible by 2. Thus,

$$a^{2(p-1)} \equiv 1 \pmod{16} \qquad (1).$$

Since, a is relatively prime to p, we get $a^{p-1} \equiv 1 \pmod{p}$. Hence,

$$a^{2(p-1)} \equiv 1 \pmod{p} \qquad (2).$$

Since, a is relatively prime to q and $q - 1 = 2p - 2 = 2(p - 1)$, we get

$$a^{2(p-1)} \equiv 1 \pmod{q} \qquad (3).$$

Using the fact that $2, p$ and q are relatively prime in pairs and combining (1), (2) and (3) we get $a^{2(p-1)} \equiv 1 \pmod{16pq}$.

Example 28 Prove that $504 | n^9 - n^3$, where n is an integer.
Solution. We note that $504 = 7 \times 8 \times 9$. If n is even then $8 | n^3$ while if n is odd then $8 | n^2 - 1$. Hence, for every n $8 | n^3(n^2 - 1)$. But $n^3(n^2 - 1) | n^3(n^6 - 1)$. Hence, $8 | n^9 - n^3$ for every integer n.

Now either $3 | n$ or $3 \nmid n$. If $3 | n$ then $9 | n^2$. Hence, $9 | n^3$. If $3 \nmid n$ then $(3, n) = 1$. This implies that $(9, n) = 1$. By Euler's theorem, we get $9 | n^6 - 1$. Thus, in either case $9 | n^9 - n^3$.

Similarly, either $7 | n$ or $7 \nmid n$. If $7 | n$ then $7 | n^3$. If $7 \nmid n$ then $(7, n) = 1$. By Euler's theorem, we get $7 | n^6 - 1$. Thus, in either case $7 | n^9 - n^3$.

Since, 7, 8 and 9 are relatively prime in pairs and each divides $n^9 - n^3$ we get that their product 504 divides $n^9 - n^3$.

Definition 1.10 Let $m \neq 0$. If $(a, m) = 1$, an integer a' such that $aa' \equiv 1 \pmod{m}$, is called an inverse of a modulo m.

Example 29 The following table shows the inverses of $1, \ldots, 12$ modulo 13.

number	1	2	3	4	5	6	7	8	9	10	11	12
inverse	1	7	9	10	8	11	2	5	3	4	6	12

Observe that $11! \equiv 1[(2)(7)][(3)(9)][(4)(10)][(5)(8)][(6)(11)] \equiv 1 \pmod{13}$ and hence $12! \equiv 12 \equiv -1 \pmod{13}$.

Remark 1.6 Since $(a, m) = 1$, there exist integers b, c such that $ab + mc = 1$. Hence, $ab \equiv 1 \pmod{m}$. This shows that if $(a, m) = 1$, a has an inverse modulo m. Further, if b and c are inverses of $a \pmod{m}$ then $m|a(b-c)$. Using Euclid's lemma, we get $b \equiv c \pmod{m}$. Thus, the inverse is unique modulo m

Let b and c be integers congruent $\pmod{m}$ and b' be the inverse of $b \pmod{m}$. Then $cb' \equiv bb' \equiv 1 \pmod{m}$. Hence, both b and c have the same inverse modulo m. Hence, the integers congruent modulo m have the same inverse modulo m.

Theorem 16 (Wilson's theorem) Let p be a prime. Then

$$(p-1)! \equiv -1 \pmod{p}. \tag{7}$$

Proof. The result can easily be verified for $p = 2$ and $p = 3$. We assume that $p \geq 5$. Now, given an integer i such that $1 \leq i \leq p-1$ there exists a unique j such that $ij \equiv ji \equiv 1 \pmod{p}$, $1 \leq j \leq p-1$. Moreover $i = j$ if and only if $i = 1$ or $p-1$. Hence, $(p-2)! \equiv 1 \pmod{p}$. Hence,

$$(p-1)! \equiv p-1 \equiv -1 \pmod{p}.$$

Remark 1.7 Note that n is prime if and only if $(n-1)! \equiv -1 \pmod{n}$.

Theorem 17 Let p denote a prime. Then $x^2 \equiv -1 \pmod{p}$ has solutions if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.

Proof. If $p = 2$ we have the solution $x = 1$. For any odd prime we can write Wilson's theorem in the form $\prod_{j=1}^{(p-1)/2} j(p-j) \equiv -1 \pmod{p}$. But $j(p-j) \equiv -j^2 \pmod{p}$, and we get

$$(-1)^{(p-1)/2} \prod_{j=1}^{(p-1)/2} j^2 \equiv -1 \pmod{p}.$$

Hence for $p \equiv 1 \pmod{4}$, we get a solution of $x^2 \equiv -1 \pmod{p}$.

Suppose $p \neq 2$ or $p \not\equiv 1 \pmod{4}$ then $p \equiv 3 \pmod{4}$. In this case, if for some integer x, we have $x^2 \equiv -1 \pmod{p}$, then

$$(x^2)^{(p-1)/2} \equiv -1^{(p-1)/2} \pmod{p}.$$

Hence $x^{p-1} \equiv -1 \pmod{p}$. Since $(p, x) = 1$ we get $p|2$, a contradiction.

Theorem 18 (Lagrange's Theorem) [3] Let $p > 3$ be an odd prime and let

$$(x-1)\cdots(x-(p-1)) = x^{p-1} - A_1x^{p-2} + \cdots - A_{p-2}x + A_{p-1}. \quad (8)$$

Then, $A_{p-1} \equiv -1 \pmod{p}$ and $p^2 | A_{p-2}$.

Proof. Replace x by $x-1$ in (2) and multiply both sides by $x-1$. Hence, we get

$$\begin{aligned} & \{(x-1)(x-2)\cdots(x-(p-1))\}(x-p) \\ = \; & (x-1)^p - A_1(x-1)^{p-1} + \cdots - A_{p-2}(x-1)^2 + A_{p-1}(x-1). \end{aligned}$$

Hence,

$$\begin{aligned} & (x^{p-1} - A_1x^{p-2} + \cdots - A_{p-2}x + A_{p-1})(x-p) \\ = \; & (x-1)^p - A_1(x-1)^{p-1} + \cdots - A_{p-2}(x-1)^2 + A_{p-1}(x-1). \end{aligned}$$

Expanding R.H.S. using binomial theorem and comparing the coefficients, we get

$$\begin{aligned} -p + A_1 &= p + A_1 \quad \text{Identity} \\ pA_1 + A_2 &= \binom{p}{2} + \binom{p-1}{1}A_1 + A_2 \\ pA_2 + A_3 &= \binom{p}{3} + \binom{p-1}{2}A_1 + \binom{p-2}{1}A_2 + A_3 \\ &\vdots \qquad\qquad \vdots \\ pA_{p-2} + A_{p-1} &= \binom{p}{p-1} + \binom{p-1}{p-2}A_1 + \binom{p-2}{p-3}A_2 + \cdots + A_{p-1} \\ pA_{p-1} &= 1 + A_1 + A_2 + \cdots + A_{p-1} \end{aligned}$$

From this, we successively get $p|A_1, p|A_2, \cdots, p|A_{p-2}$ and $p|A_{p-1}+1$. If we put $x = 0$ in (2) then we get $A_{p-1} = (p-1)!$. Thus, we get $(p-1)! \equiv -1 \pmod{p}$ (Wilson's Theorem). If we put $x = p$ in (2) then we get $p^2|A_{p-2}$.

We also note that $x^{p-1} - 1 - \{(x-1)\cdots(x-(p-1))\}$ is a polynomial with integer coefficients such that its coefficients are divisible by p. If x is not divisible by p then $(x-1)\cdots(x-(p-1))$ is divisible by p. Hence, we get $x^{p-1} - 1$ is divisible by p and thus we get Fermat's Little Theorem.

Definition 1.11 Let $r_1, ..., r_m$ denote a complete residue system modulo m. The number of solutions of $f(x) \equiv 0 \pmod{m}$ is the number of r_i such that $f(r_i) \equiv 0 \pmod{m}$.

[3] The proof of this theorem may be skipped for the first reading.

Theorem 19 Let g denote (a, m). Then $ax \equiv b \pmod{m}$ has no solutions if $g \nmid b$. If $g|b$, it has g solutions $x \equiv (b/g)x_0 + t(m/g) \pmod{m}$, where $t = 0, 1, ..., g-1$ where x_0 is any solution of $(a/g)x \equiv 1 \pmod{m/g}$.

Proof. Suppose $ax \equiv b \pmod{m}$ has a solution, say x_0. Then $ax_0 \equiv b \pmod{m}$ i.e. $ax_0 - b = qm$ for some integer q. Hence, $ax_0 - qm = b$ which implies that $g|b$ (where $g = (a, m)$) if $ax \equiv b \pmod{m}$ has a solution. Thus, if $g \nmid b$ then $ax \equiv b \pmod{m}$ has no solution.

Suppose $g|b$. Since $(a, m) = g$ there exist integers λ, μ such that $\lambda a + \mu m = g$. As $g|b$ there exists q such that $b = gq$. Hence, $q(\lambda a + \mu m) = qg = b$. Thus, $q\lambda a \equiv b \pmod{m}$. Hence, $ax \equiv b \pmod{m}$ has a solution if $g|b$. It is easy to see that if $g = 1$ then $ax \equiv b \pmod{m}$ has unique solution.

Further, if x_0 is any solution of $(a/g)x \equiv 1 \pmod{m/g}$ then $(b/g)x_0 + t(m/g), t = 0, 1, \ldots, g-1$ are solutions of $ax \equiv b \pmod{m}$.

Theorem 20 (Chinese Remainder Theorem) Let $m_1, m_2, \ldots, m_r$ denote r positive integers that are relatively prime in pairs, and let $a_1, \ldots, a_r$ denote any r integers. Then the congruences $x \equiv a_i \pmod{m_i}$, $i = 1, \ldots, r$ have common solutions. Any two solutions are congruent modulo $m_1 m_2 \cdots m_r$.

Proof. Let $m = m_1 m_2 ... m_r$. Note that m/m_j and m_j are coprime. Hence there exists b_j such that $(m/m_j)b_j \equiv 1 \pmod{m_j}$. Clearly,

$$\frac{m}{m_j} b_j \equiv 0 \pmod{m_i} \text{ for } i \neq j.$$

Define $x_0 = \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j$. Now $\frac{m}{m_j} b_j \equiv 1$ or $0 \pmod{m_i}$ according as $j = i$ or $j \neq i$. Hence x_0 is a solution of the system of congruences.

If x_0 and y_0 are solutions of the system, then $x_0 - y_0 \equiv a_i - a_i \equiv 0 \pmod{m_i}$ for each i. As $m_1, \ldots, m_r$ are coprime in pairs, we get $x_0 - y_0 \equiv 0 \pmod{m}$ as required.

Example 30 Find all solutions of the system

$$x \equiv 2 \pmod{4},\ x \equiv 3 \pmod{5},\ x \equiv 1 \pmod{7}.$$

Solution. Here $m_1 = 4$, $m_2 = 5$, $m_3 = 7$; $M = m_1 m_2 m_3 = 140$, $M_1 = M/m_1 = 35$, $M_2 = M/m_2 = 28$, $M_3 = M/m_3 = 20$. $M_1 \equiv 3 \pmod{4}$, hence $M_1' \equiv 3 \pmod{4}$. $M_2 \equiv 3 \pmod{5}$, hence $M_2' \equiv 2 \pmod{5}$. $M_3 \equiv 6 \pmod{7}$, hence $M_3' \equiv 6 \pmod{7}$. Consider

$$\begin{aligned} x_0 &= 2M_1M_1' + 3M_2M_2' + 1M_3M_3' \\ &= 2 \times 35 \times 3 + 3 \times 28 \times 2 + 20 \times 6 = 498 \equiv 78 \pmod{140}. \end{aligned}$$

Hence all the solutions of the system are $78 + 140k,\ k \in \mathbf{Z}$.

We note that there are many possibilities to choose M_i'. For example, we may choose $M_1' = -1, M_2' = 2$ and $M_3' = -1$. Then $x_0 \equiv 78 \pmod{140}$.

Example 31 Find the last three digits of the 100 th powers of the first 100 natural numbers.

Solution. Let m be a natural number and r be the last digit of m. Then $m = r + 10k$ for some integer k. Hence

$$\begin{aligned} m^{100} = (r+10k)^{100} &= r^{100} + 100r^{99}(10k) + \frac{100 \times 99}{2} r^{98}(10k)^2 + \ldots \\ &\equiv r^{100} \pmod{1000} \end{aligned}$$

[We can prove this as follows: (Exercise Set 1.2 Prob. No.8)

$$\begin{aligned} m \equiv r \pmod{10} &\Rightarrow m^{10} \equiv r^{10} \pmod{10^2} \\ &\Rightarrow (m^{10})^{10} \equiv (r^{10})^{10} \pmod{10^3} \\ \text{i.e.} \quad & m^{100} \equiv r^{100} \pmod{1000}] \end{aligned}$$

(a) If $r = 0$, then $r^{100} = 0$.
(b) If $r = 1, 3, 7, 9$, then $r^2 \equiv 1 \pmod 8$, so $r^{100} \equiv 1 \pmod 8$. Also, $\phi(125) = 100$ By Euler's theorem, as $(r, 5) = 1, r^{100} \equiv 1 \pmod{125}$. Hence, $r^{100} \equiv 1 \pmod{1000}$.
(c) If $r = 5$ then $r^2 \equiv 1 \pmod 8$. Hence, $r^{100} \equiv 1 \pmod 8$ and $r^{100} \equiv 0 \pmod{125}$. Using Chinese remainder theorem, $r^{100} \equiv 625 \pmod{1000}$.
(d) If $r = 2, 4, 6, 8$, $r^{100} \equiv 0 \pmod 8$. Since, $(r, 5) = 1$ we get $r^{100} \equiv 1 \pmod{125}$. By Chinese remainder theorem, $r^{100} \equiv 376 \pmod{1000}$.

Thus in the above 4 cases, the last 3 digits of m^{100} are 000, 001, 625 and 376 respectively.

Definition 1.12 Let a, m be integers such that $(a, m) = 1$. An integer n is called the order of a modulo m if n is the smallest integer such that $a^n \equiv 1 \pmod m$. An integer a relatively prime to m is called a primitive root modulo m if order of a modulo m is $\phi(m)$.

For example, order of 2 modulo 7 is 3 while the order of 3 modulo 7 is 6. Thus, 3 is a primitive root modulo 7.

Remark 1.8 The integers $1, 2, 4, p^e, 2p^e$ (p an odd prime) are the only integers which have a primitive root.

Example 32 Find all pairs of prime numbers (p, q) satisfying the condition that pq divides $2^p + 2^q$.

Solution. Let us assume that p, q are odd primes such that $pq|2^p + 2^q$. Let m and n denote order of 2 modulo p and modulo q respectively and $m = 2^a m_1$ and $n = 2^b n_1$ where $2 \nmid m_1$ and $2 \nmid n_1$. We have $2^p \equiv -2^q \pmod{pq}$. Hence, we get $2^p \equiv -2 \pmod{q}$ and $2^q \equiv -2 \pmod{p}$. Hence, we get $2^{p-1} \equiv -1 \pmod{q}$ and $2^{q-1} \equiv -1 \pmod{p}$. But $m|p-1$ and $n|q-1$. We may assume that $a \geq b$. Hence, we get

$$(2^{p-1})^{n_1} \equiv (-1)^{n_1} \equiv -1 \pmod{q}.$$

But $n|p-1$. Hence $(2^{p-1})^{n_1} \equiv 1 \pmod{q}$ which implies that $q|2$, a contradiction. Hence, at least one of p and q equals 2. Suppose $p = 2$ then it is easy to see that $q = 2$ or $q = 3$. Similarly, if $q = 2$ then $p = 2$ or $p = 3$. Hence, all pairs satisfying the given condition are $(2, 2)$, $(2, 3)$ and $(3, 2)$.

Exercise Set - 1.3

1. Find the remainders when 2^{50} and 41^{65} are divided by 7.
2. Find the units digit of 3^{100}.
3. Show that $11|(5^{10} - 3^{10})$. More generally, if p is a prime such that $p \nmid a$ and $p \nmid b$, then show that $p|(a^{p-1} - b^{p-1})$.
4. Prove that (i) $39|(53^{103} + 103^{53})$ and (ii) $7|(111^{333} + 333^{111})$.
5. If p and q are distinct primes, show that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.
6. Find the remainder when $7^{200} + 11^{800}$ is divided by 101.
7. Show that $89|(2^{44} - 1)$ and $97|(2^{48} - 1)$.
8. Show that there are infinitely many primes of the type $4n + 1$.
9. Show that there are infinitely many primes of the type $6n + 1$.
10. Show that if a prime p divides an integer of the form $16a^4 + 1$ then p is of the type $8n + 1$. Hence, or otherwise show that there are infinitely many primes of the type $8n + 1$.
11. Show that $\sum_{r=1}^{n-3} r(r)!$ is divisible by n if and only if n is prime.

12. Prove that if p is a prime and a, b are any positive integers, then

$$\text{(i)} \quad \binom{2p}{p} \equiv 2 \pmod{p}, \quad \text{(ii)} \binom{2p}{p} \equiv 2 \pmod{p^2},$$

$$\text{(iii)} \quad \binom{pa}{pb} \equiv \binom{a}{b} \pmod{p}, \quad \text{(iv)} \binom{pa}{pb} \equiv \binom{a}{b} \pmod{p^2}.$$

13. Solve the following equations in $\mathbb{Z}$: $(i) y^2 = x^3 + 7$, $(ii) y^2 = 41x + 3$.

14. Prove that for each positive integer n there exist n consecutive positive integers none of which is an integral power of a prime number.

15. If p is a prime and $0 < r < p$, prove that $(p-r)!(r-1)! + (-1)^{r-1} \equiv 0 \pmod{p}$. Show also that $18! \equiv -1 \pmod{437}$.

16. Show that $1^5 + 2^5 + \ldots + 100^5$ is divisible by 10100, however it is not divisible by 3.

17. Let $(a, b) = 1$. Show that there exists an integer l such that $a^l + b^l \equiv 1 \pmod{ab}$.

18. Prove that if $p > 5$ is a prime, then $p^4 \equiv 1 \pmod{240}$.

19. Prove that if p is an odd prime different from 3 and 7, then $p^6 \equiv 1 \pmod{168}$. Is it true that $p^6 \equiv 1 \pmod{504}$?

20. Prove that if for integers a and b we have $7|a^2 + b^2$,then $7|a$ and $7|b$.

1.4 Greatest Integer Function

For real x, the symbol $[x]$ denotes the greatest integer less than or equal to x. Thus, we note that $[\pi] = 3, [e] = 2, [-\pi] = -4$.

Theorem 21 Let x and y be real numbers. Then we have

(i) $[x] \leq x < [x] + 1$ and $x - 1 < [x] \leq x$, $0 \leq x - [x] < 1$.

(ii) If $x \geq 0$, $[x] = \sum_{1 \leq i \leq x} 1$.

(iii) $[x + m] = [x] + m$ if m is an integer.

(iv) $[x] + [y] \leq [x + y] \leq [x] + [y] + 1$.

(v) $[x]+[-x]=\begin{cases}0 & \text{if } x \text{ is an integer,}\\ -1 & \text{otherwise.}\end{cases}$

(vi) $\left[\frac{[x]}{m}\right]=\left[\frac{x}{m}\right]$ if m is a positive integer.

(vii) $x-[x]$ is the fractional part of x and is denoted by $\{x\}$.

(viii) $-[-x]$ is the least integer $\geq x$.

(ix) $[x+0.5]$ is the nearest integer to x. If two integers are equally near to x, $[x+0.5]$ denotes the larger of the two.

(x) If a and b are positive integers, $[b/a]$ is the number of integers among $1,2,\ldots,n$ that are divisible by a. Thus, $b=aq+r, 0\leq r<a$ can also be written as

$$b=a\left[\frac{b}{a}\right]+r.$$

Example 33 For every positive integer n, show that

$$[\sqrt{n}+\sqrt{n+1}]=[\sqrt{4n+1}]=[\sqrt{4n+2}]=[\sqrt{4n+3}].$$

Solution. Note that $(\sqrt{n}+\sqrt{n+1})^2=2n+1+2\sqrt{n(n+1)}$ and as $n\geq 1$, $n<\sqrt{n(n+1)}<n+1$. Consequently $4n+1<(\sqrt{n}+\sqrt{(n+1)})^2<4n+3$, which gives

$$\sqrt{4n+1}<\sqrt{n}+\sqrt{(n+1)}<\sqrt{4n+3}. \tag{9}$$

Also, there always exist an integer k such that

$$k^2\leq 4n+1<(k+1)^2.$$

Since a square cannot be congruent to 2 or 3 (mod 4), we have

$$k^2\leq 4n+1<4n+2<4n+3<(k+1)^2,$$

$$\text{i.e.}\quad k\leq\sqrt{4n+1}<\sqrt{4n+2}<\sqrt{4n+3}<(k+1). \tag{10}$$

Combining (9) and (10), we get the required result.

Theorem 22 (de Polignac's Formula) Let p be a prime. Let e be the largest exponent of p such that p^e divides $n!$. Then $e=\sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right]$.

Proof. Induction on n or one can also prove this using elemenary counting principles.

1.5 Arithmetic Functions

Definition 1.13 A function $f : \mathbb{N} \to \mathbb{C}$ is called an arithmetic function.

For example, .
$d(n)$ = the number of positive divisors of n,
$\sigma(n)$ = the sum of positive divisors of n,
$\sigma_k(n)$ = the sum of k^{th} powers of positive divisors of n,
$\phi(n)$ = the number of positive integers $\leq n$ and relatively prime to n.
$\omega(n)$ = the number of distinct primes dividing n.

Proposition 2 If $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, then $d(n) = (a_1+1)(a_2+1)\dots(a_k+1)$.
Proof. If d is a divisor of n, then $d = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$ where $0 \leq b_i \leq a_i$, $1 \leq i \leq k$. For each i, we have $a_i + 1$ choices for b_i and so

$$d(n) = (a_1 + 1)\dots(a_k + 1).$$

Definition 1.14 An arithmetic function f is said to be multiplicative if f is not identically zero and $f(mn) = f(m)f(n)$ whenever m and n are coprime i.e. $(m, n) = 1$.

For example, $f(n) = n$, $f(n) = d(n)$ are multiplicative functions.

Theorem 23 If $f(n)$ is multiplicative, then so is $F(n) = \sum_{d|n} f(d)$.

Definition 1.15 The Möbius function $\mu(n)$ is defined as follows:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } a^2 | n \text{ for some } a > 1, \\ (-1)^k & \text{if } n = p_1 \dots p_k, \ p_i \text{ being distinct primes.} \end{cases}$$

Thus, $\mu(p) = -1$, where p is a prime, $\mu(6) = 1, \mu(24) = 0$.

Example 34 Find $\sum(\mu(n!)$ i.e $\mu(1!) + \mu(2!) + \mu(3!) + \cdots$.
Solution. We note that $4|n!$ if $n \geq 4$. Hence, $\mu(n!) = 0$ if $n > 4$. It follows that $\sum(\mu(n!) = \mu(1!) + \mu(2!) + \mu(3!) = 1$.

Theorem 24 (Möbius Inversion Formula) If $F(n) = \sum_{d|n} f(d)$ for every positive integer n, then $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d})$, for every positive integer n.

Note. The converse of this is also true.

Theorem 25 $\phi(n) = n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)$, where $n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$.

Proof. Since $\sum_{d|n}\phi(d) = n$ we have, by Möbius inversion formula,

$$\phi(n) = \sum_{d|n}\mu(d)\cdot(n/d). \text{ Hence, } \frac{\phi(n)}{n} = \sum_{d|n}\frac{\mu(d)}{d}$$

Now $\mu(d)/d$ is a multiplicative function. So $\phi(n)/n$ is a multiplicative function. Thus $\phi(n)$ **is a multiplicative function.** For a prime p

$$\begin{aligned}\phi(p^e) &= \sum\mu(d)\left(\frac{p^e}{d}\right) = \sum_{f=0}^{e}\mu(p^f)\left(\frac{p^e}{p^f}\right)\\ &= \mu(1)p^e + \mu(p)p^{e-1} = p^e - p^{e-1} = p^e\left(\frac{p-1}{p}\right)\\ \text{Hence } \phi(n) &= n\cdot\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)\end{aligned}$$

Remark 1.9 The multiplicativity of Euler's totient function can also be established using Chinese Remainder theorem and also by elementary counting method. We give a proof by elementary counting method.

Proof. Let us write the numbers from 1 to mn in an $n \times m$ array.

$$\begin{array}{cccc} 1 & 2 & \cdots & m \\ m+1 & m+2 & \cdots & 2m \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ m(n-1)+1 & m(n-1)+2 & \cdots & mn \end{array}$$

Circle those numbers in the first row which are relatively prime to m. Since $(m,n) = 1$ and any two elements in the same column differ by multiple of m we get that these are the only elements from 1 to mn which are relatively prime to m. Thus, we get $\phi(m)$ such columns.

Now, if $1 \le r \le m$ and $(r,m) = 1$, then $r, r+m, \ldots, r+m(n-1)$ form a complete residue system modulo n. Hence, out of these elements exactly, $\phi(n)$ are relatively prime to n. But these elements are relatively prime to m also.

Hence, there are exactly $\phi(m)\phi(n)$ elements less than or equal to mn which are relatively prime to both m and n, hence to mn. Thus, we get $\phi(mn) = \phi(m)\phi(n)$.

Example 35 Let $\sigma(n)$ be the sum of all positive divisors of a positive integer n (including 1 and n) and $\phi(n)$ the number of positive integers less than n and prime to n. Prove that $\sigma(n) + \phi(n) \geq 2n$.

Solution. Since $\sigma(1)+\phi(1) = 2$, let $n > 1$. Let $1 = d_1 < d_2 < \cdots < d_k = n$, be all the divisors of n. Note that

$$d_1 + \cdots + d_k = \sigma(n), \quad \frac{n}{d_2} = d_{k-1}, \quad \frac{n}{d_3} = d_{k-2}, \quad \cdots, \quad \frac{n}{d_k} = d_1.$$

The number of positive integers $\leq n$ and divisible by d_i is n/d_i. So, the number of positive integers $\leq n$ and *not* coprime with n is

$$n - \phi(n) \leq \frac{n}{d_2} + \frac{n}{d_3} + \cdots + \frac{n}{d_k} = d_{k-1} + \cdots + d_1 = \sigma(n) - n.$$

Exercise Set - 1.4

1. How many zeros are there at the end of 400! ?
2. Show that n is a perfect square if and only if $d(n)$ is odd.
3. There are n students standing in a row as per their roll numbers $1, \ldots, n$. The drill-master asks all the students to sit down. Then he asks *every second* student to stand up. Next he asks *every third* student to change his position from standing to sitting and vice-versa. Then he asks *every fourth* student to change his existing position and so on. Finally, he asks the nth student to change his existing position. Find which students are found in the sitting position at the end of this drill.
4. If $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$, then show that $\sigma(n)$ and $\sigma_k(n)$ are multiplicative functions and hence show that

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1}, \quad \sigma_k(n) = \prod_{i=1}^{k} \frac{p_i^{k(a_i+1)} - 1}{p_i^k - 1}.$$

5. A natural number n is said to be *perfect* if $\sigma(n) = 2n$. Prove the following theorem of Euclid: If $2^k - 1$ is a prime, then $2^{k-1}(2^k - 1)$ is a perfect number. (This is the case when e.g. $k = 2, 3, 5, 7, 13, 17, 19$).

Conversely, prove that every even perfect number is of the form $2^{k-1}(2^k-1)$, where 2^k-1 is a prime (Euler). (No odd perfect numbers are known).

6. Prove that for $n = 1,2,3,\ldots$

$$\left[\frac{n+1}{2}\right]+\left[\frac{n+2}{4}\right]+\left[\frac{n+4}{8}\right]+\left[\frac{n+8}{16}\right]+\ldots = n.$$

7. Let $\langle a_n\rangle_{n=1}^{\infty}$ be a sequence of positive integers defined by $\sum_{d|n} a_d = 2^n$ for every $n \in \mathbb{N}$. (For example, $a_1 = 2, a_1+a_2 = 2^2, a_1+a_3 = 2^3$.) Prove the following statements:

   (a) If p, q are distinct primes then $pq|a_{pq}$.

   (b) For every prime p and positive integer m, $p^m|a_{p^m}$.

1.6 Pythagorean Triples

If (x_1, y_1, z_1) is a solution of $x^2+y^2 = z^2$ in positive integers then the triple (x_1, y_1, z_1) is called a Pythagorean triple. If the gcd of x_1, y_1, z_1 is 1, then such a triple is called a primitive Pythagorean triple. For example, (3,4,5), (5,12,13), (8,15,17) are primitive Pythagorean triples.

Theorem 1 A primitive Pythagorean triple (x_1, y_1, z_1) with y_1 even is given by $x_1 = r^2-s^2$, $y_1 = 2rs$, $z_1 = r^2+s^2$ where r and s are arbitrary positive integers of opposite parity with $r > s$ and $(r,s) = 1$.

Proof. Since the gcd of x_1, y_1, z_1 is 1, then x_1, y_1 cannot both be even. If x_1, y_1 are both odd then $x_1^2 \equiv 1 \pmod 4$ and $y_1^2 \equiv 1 \pmod 4$, so that $x_1^2+y_1^2 = z_1^2 \equiv 2 \pmod 4$, a contradiction. Hence x_1, y_1 cannot both be odd. We assume that y_1 is even and x_1 is odd. Now, $y_1^2 = z_1^2-x_1^2 = (z_1+x_1)(z_1-x_1)$. So $(y_1/2)^2 = y_1^2/4 = [(z_1-x_1)/2][(z_1+x_1)/2]$. Now since the g.c.d of x_1, y_1, z_1 is 1, we have $((z_1-x_1)/2, (z_1+x_1)/2) = 1$ and hence $(z_1-x_1)/2 = s^2$ and $(z_1+x_1)/2 = r^2$ for some positive integers r, s. Obviously $(r,s) = 1$; since the g.c.d of x_1, y_1, z_1 is 1, we get that one of r, s is odd and the other is even. Hence we get that the integers x_1, y_1, z_1 must be of the form $x_1 = r^2-s^2, y_1 = 2rs, z_1 = r^2+s^2$ with $r > s > 0$, $(r,s) = 1$ and r, s are of opposite parity. Conversely, if integers x_1, y_1, z_1 are of the above form, then (x_1, y_1, z_1) is a primitive Pythagorean triple.

Example 36 If (x, y, z) is a primitive Pythagorean triple then show that one of x, y is divisible by 3. Further, show that xyz is divisible by 60.

Solution. By the above theorem we have (assuming y even) $x = r^2 - s^2$, $y = 2rs$, $z = r^2 + s^2$. If $3|r$ or $3|s$ then $3|y$. If $3 \nmid r$ and $3 \nmid s$ then by Fermat's theorem $r^2 \equiv 1 \pmod 3$ and $s^2 \equiv 1 \pmod 3$. Thus $x = r^2 - s^2 \equiv 0 \pmod 3$ i.e. $3|x$.

Since r and s are of opposite parity $4|y$. If $5|rs$ then $5|y$. If $5 \nmid rs$ then $r^4 \equiv 1 \pmod 5$ and $s^4 \equiv 1 \pmod 5$. Hence, $xz = r^4 - s^4 \equiv 0 \pmod 5$. Since, 3, 4, 5 are pairwise coprime, their product i.e. 60 divides xyz.

Example 37 Let a, b, c be integer sides of a right-angled triangle, where $a < b < c$. Show that $ab(b^2 - a^2)$ is divisible by 84.

Solution. Let $a = xt, b = yt$ and $c = zt$ where (x, y, z) is a primitive Pythagorean triple and t is a positive integer. We may assume that y is even, hence we get $x = r^2 - s^2$, $y = 2rs$, $z = r^2 + s^2$ where r and s are arbitrary positive integers of opposite parity with $r > s$ and $(r, s) = 1$. Note that $84 = 4 \times 3 \times 7$. Hence,

$$\begin{aligned} xy(x^2 - y^2) &= 2rs(r^2 - s^2)[(r^2 - s^2)^2 - 4r^2s^2] \\ &= 2rs(r^2 - s^2)[r^4 + r^2s^2 + s^4) - 7r^2s^2] \\ &= 2rs[(r^6 - s^6) - 7(r^2 - s^2)r^2s^2] \end{aligned}$$

is divisible by 4 as one of r and s is even. Either rs is divisible by 3 or otherwise $r^2 \equiv s^2 \equiv 1 \pmod 3$. Hence, $3|r^2 - s^2$. If $7 \nmid rs$ then $r^6 \equiv s^6 \equiv 1 \pmod 7$. Hence, $7|xy(x^2 - y^2)$. Since, 3,4 and 7 are relatively prime in pairs, we get the required result.

1.7 Representation of a positive integer

Let n be a positive integer, b be any positive integer > 1. Then n can be written *uniquely* as

$$n = n_s b^s + n_{s-1} b^{s-1} + \ldots + n_1 b + n_0 \tag{11}$$

where $0 \leq n_i < b$, $n_s \neq 0$. We also write (11) as

$$n = (n_s, n_{s-1}, \ldots, n_1, n_0)_b \tag{12}$$

(11) and (12) are called a digital representation of n in base b. The n_i are called the digits. The above n may also be written (for $k > s$) as,

$$n = (n_k, n_{k-1}, \ldots, n_2, n_1, n_0)_b \tag{13}$$

where we must take $n_k = n_{k-1} = \ldots = n_{s+1} = 0$. We may thus write $n = (\ldots n_i \ldots n_s \ldots n_0)_b$, with $n_i = 0$ for every $i > s$. We have the following conventions:

Binary representation : base 2	Decimal representation : base 10
Ternary representation : base 3	Duodecimal representation : base 12
Octal representation : base 8	Hexadecimal representation : base 16.

Thus,

$$\begin{aligned} n = 210 &= 2 \times 10^2 + 1 \times 10^1 + 0 \times 10^0 = (2\,1\,0)_{10}. \\ &= 1 \times 5^3 + 3 \times 5^2 + 2 \times 5 = (1320)_5. \end{aligned}$$

To convert $210 = (2\ \ 1\ \ 0)_{10}$ to base 2, we divide 210 by 2, and note the remainder, and repeat the process with 210 replaced by the quotient. Continue the process till we get the quotient to be zero. Then starting at the bottom, the remainders give us the binary digits for 210, read from left to right. Thus we have the following table.

$n = 210$

divisor	quotient	remainder	
2	105	0	
2	52	1	
2	26	0	
2	13	0	
2	6	1	
2	3	0	↑
2	1	1	↑
2	0	1	↑

Hence $(210)_{10} = (11010010)_2$. Check:

$$\begin{aligned} (11010010)_2 &= 1 \times 2^7 + 1 \times 2^6 + 1 \times 2^4 + 1 \times 2^1 \\ &= 128 + 64 + 16 + 2 = 210. \end{aligned}$$

The same procedure works for any base b. Note that for representation to base b, the 'digits' are the numbers $0, 1, \ldots, b-1$. Thus in base 2 the digits are 0, 1 and in base 5 they are 0, 1, 2, 3, 4. If $b > 10$, then we have to use new symbols to designate the digits ≥ 10. E.g. if $b = 12$, the digits are $0, 1, \ldots, 10, 11$. The new digits 10 and 11 may be designated by symbols such

as t and e or they may be underscored. Thus $(1\ t)_{12} = (2\ 2)_{10}$ or $(\underline{11}\ 1)_{12} = (1\ 3\ 3)_{10}$. When hexadecimal representation is used, we denote the numbers 10, 11, 12, 13, 14 and 15 by A, B, C, D, E, F respectively.

Note. We have $0 = (0)_b$ and $1 = (1)_b$ for any base b.

Exercise set- 1.5

1. Show that if $x_1^2 + y_1^2 = z_1^2$, then the following are equivalent:
   (i) gcd of x_1, y_1, z_1 is 1 (ii) $(x_1, y_1) = 1$ (iii) $(y_1, z_1) = 1$
   (iv) $(x_1, z_1) = 1$ (v) $(x_1, y_1) = 1,\ (y_1, z_1) = 1,\ (x_1, z_1) = 1$.

2. If (x, y, z) is a pythagorean triple such that each x, y, z can be written as sum of two squares then show that $180|xyz$.

3. Verify the following: (i) $(5\ 5\ 6)_{10} = (4\ 2\ 1\ 1)_5$
   (ii) $(5\ 5\ 6)_9 = (4\ 5\ 6)_{10}$ (iii) $(1\ 3\ 7\ 6)_8 = (5\ 3\ t)_{12}$.

4. Show that every positive integer is congruent modulo $b-1$ to sum of its digits in base b. Show further that if $n = (n_s, n_{s-1}, \ldots n_1, n_0)_b$, then $n \equiv n_0 - n_1 + n_2 \ldots + (-1)^s n_s \pmod{(b+1)}$. Hence, derive a divisibility test for 11.

5. Noting that 37 divides 999, devise a test for divisibility by 37. Noting that $1001 = 7 \times 11 \times 13$, devise a test of divisibility by these primes.

6. Let n be a five-digit number and let m be a 4-digit number formed from n by deleting its middle digit. Determine all n such that n/m is an integer.

7. Prove that sum of all the $n-$ digit integers $(n > 2)$ is
   $49499\ldots95500\ldots0$ [digit 9 $(n-3)$ times and 0 $(n-2)$ times.]

8. Prove that a triangle with sides of lengths 5,5,6 has the same area as the triangle with sides 5,5, 8. Find all other pairs of noncongruent isosceles triangles, with integer sides, having equal areas.

9. Show that the highest power of a prime p that divides $n!$ is
   ($n-$ sum of the digits of n when n is written in base p)$/(p-1)$.

10. Find all the right-angled isosceles triangles with integer sides.

11. Determine all three digit numbers N, such that N is divisible by 11 and $\frac{N}{11}$ is equal to the sum of the squares of the digits of N.

12. Find the smallest natural number n with 6 as the last digit in its decimal representation and such that if the last digit is erased and kept in front of the remaining digits, the resulting number is four times as large as the original number n.

13. When 4444^{4444} is written in decimal notation, the sum of its digits is A. Let B be the sum of the digits of A. Find the sum of the digits of B.

14. A divisor $d > 0$ of a positive integer n is said to be a *unitary divisor* if $(d, n/d) = 1$. Suppose n is a positive integer such that the sum of its unitary divisors is equal to $2n$. Prove that n cannot be an odd integer. (Note that 1, 3, 4, 12 are the unitary divisors of 12.)

15. Let $n \geq 2$ be an integer. Show that $\sum_{k=1}^{n} \frac{1}{k}$ is not an integer.

16. Consider the set $\{1, 2, \ldots, 100\}$. Is it possible to split this set into three groups such the sum of the elements of the first group is divisible by 100, the sum of the elements of the second group is divisible by 201 and the sum of the elements of the third group is divisible by 302.

17. Consider the set $\{1, 2, \ldots, 100\}$. Is it possible to split this set into three groups such the sum of the elements of the first group is divisible by 102, the sum of the elements of the second group is divisible by 203 and the sum of the elements of the third group is divisible by 304.

18. For each real number r, $[r]$ denotes the largest integer less than or equal to r. Indicate on the $(x, y)-$plane the set of all points (x, y) for which $[x]^2 + [y]^2 = 4$.

19. Find all the real solutions of the equation

$$[x] + [2x] + [4x] + [8x] + [16x] + [32x] = 12345.$$

20. Find all real solutions to the equation $4x^2 - 40[x] + 51 = 0$. Here, if x is a real number, then $[x]$ denotes the greatest integer that is less than or equal to x.

21. Let p and q be distinct odd primes. Show that

$$\sum_{j=1}^{(p-1)/2} \left[\frac{qj}{p}\right] + \sum_{j=1}^{(q-1)/2} \left[\frac{pj}{q}\right] = \frac{(p-1)(q-1)}{4}.$$

22. There are ten bags with coins. Some of them contain only counterfeit coins, each of which is 1 gram lighter than a genuine coin. One of the bags is known to be filled with the genuine coins. Using only one weighing on a balance with one pan and an arrow showing showing the weight on the pan, determine which bags are "counterfeit" and which are not.

23. Find all the natural numbers N such that the reduced residue system consisting of least positive residues modulo N form an arithmetic progression (I.M.O. 1991).

24. Find all integers $x \neq 3$ such that $x-3|x^3-3$.

25. Prove that their exist infinitely many positive integers n such that $4n^2+1$ is divisible both by 5 and 13.

26. Find two least composite numbers n such that $n|2^n-2$ and $n|3^n-3$.

27. Find the least positive integer n such that $n|2^n-2$ but n not divides 3^n-3.

28. Find least integer n such that n not divide 2^n-2 but $n|3^n-3$.

29. Prove that :

    (a) every positive integer has at least as many divisor of the form $4k+1$ as divisor of the form $4k+3$;

    (b) there exist infinitely many positive integers which have as many divisors of the form $4k+1$ as divisors of the form $4k+3$;

    (c) there exists infinitely many positive integers which have more divisors of the form $4k+1$ than divisors of the form $4k+3$.

30. Let p be an odd prime. Show that there exits an integer x such that. $x^8 \equiv 16 \pmod{p}$.

Solutions to Exercise Set-1.1

1. A typical term $11\ldots11$ is of the type $4k+3$. The perfect squares are either of the form $4k$ or of the form $4k+1$. Hence, the number $11\ldots111$ cannot be a perfect square.

2. Note that

$$\begin{aligned}(ma,\ mb) &= \text{least positive value of } max + mby \\ &= m(\text{least positive value of } ax+by) = m(a,b).\end{aligned}$$

3. Note that $d \cdot (\frac{a}{d}, \frac{b}{d}) = (a, b)$. Hence, we get the required result.

4. Suppose $2d-1 = x^2, 5d-1 = y^2$ and $13d-1 = z^2$. Since, $2d-1 = x^2$ we get that d must be odd. Hence y and z must be even. Also, $z^2 - y^2 = (z-y)(z+y) = 8d$. Hence, $\frac{(z+y)}{2}\frac{(z-y)}{2} = 2d$. Now either $\frac{(z+y)}{2}$ or $\frac{(z-y)}{2}$ must even. Moreover, these two numbers differ by y, an even number. Hence their product $2d$ must be divisible by 4. Hence, d must be even, a contradiction. Hence, one can find distinct $a,\ b \in \{2, 5, 13, d\}$ such that $ab - 1$ is not a perfect square.

5. $(7645, 2872) = 1 = 3543(2872) - 1331(7645)$ and $(3645, 2357) = 1$.

6. Note that $x + 1 | x^{2k} - 1$ if k is a positive integer. We may assume that $m < n$. Put $x = a^{2^m}$ and $k = 2^{n-m}$. Hence, $a^{2^m} + 1 | (a^{2^m})^{2^{n-m}} - 1$. Hence, we get that $(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1 & \text{if } a \text{ is even,} \\ 2 & \text{if } a \text{ is odd.} \end{cases}$

   Let a be even and p_m denote the prime dividing $a^{2^m} + 1$. Then as p_m, p_n are distinct primes, we have $(p_m, p_n) = 1$ whenever $m \neq n$. Hence, there are infinitely many primes.

7. Let a, b, c be integers such that $(a, b) = 1,\ c > 0$. Let P denote the product of primes common to both a and c and $P = 1$ if there are no primes common to both. Let Q denote the product of primes common to both b and c and $Q = 1$ if there are no primes common to both. Let R denote the product of primes which divide c but do not divide ab and $R = 1$ if there are no such primes. Note that $(P, Q) = (P, R) = (Q, R) = 1$. It is now easy to see that $(a + bQR, c) = 1$.

8. Assume that there are finitely many primes of the type $6n - 1$, say $p_1 = 5, p_2, \cdots, p_r$. Let $N = 6p_1p_2 \cdots p_r - 1$. Clearly $N > 2$ and 2, 3 and none of the p_j's divide N. Moreover, since N is of the type $6n - 1$, N must have a prime factor of the type $6n - 1$. Hence, this prime is a new prime of the type $6n - 1$, a contradiction. Hence, there are infinitely many primes of the type $6n - 1$.

9. If $k, k+1, k+2$ are consecutive integers, then at least one of them is even and one of them is divisible by 3. If there are four consecutive integers, then there are two even integers and one of them is divisible by 4 as well.

10. Since $m = n^2 - n = n(n-1)$ and $m - 2 = (n-2)(n+1)$ and $m^2 - 2m = (n-2)(n-1)n(n+1)$. Hence, $m^2 - 2m$ is product of 4 consecutive integers and hence $24|m(m-2)$.

11. It can be easily seen that the book has more than 1000 pages. Suppose the book has $999 + x$ pages. Then, we get the equation $9 + 2(90) + 3(900) + 4x = 3189$. Hence, $x = 75$. Hence, the book has 1074 pages.

12. Note that $6k = (k+1)^3 + (k-1)^3 - k^3 - k^3$ and $6k - 15 = (2k)^3 - (2k+1)^3 + (k-2)^3 - (k+2)^3$.

13. Let $p > 3$ be an odd prime. Note that $\sum_{k=1}^{p-1} \frac{1}{k} = \sum_{k=1}^{p-1/2} \frac{p}{k(p-k)}$. Hence, the numerator is divisible by p.

    Challenge. Show that the numerator is divisible by p^2

14. Note that if $n \geq 4$ then $3|n(n+2)(n+4)$.

15. Since 2 is the only even prime, the product $a = p_1 p_2 \cdots p_n$ is of the form $a = 2k$ where k is odd. But if $a + 1 = q^2$, then q^2 and hence q is odd and so $a = (q+1)(q-1)$ is divisible by 4. This is a contradiction. So $a + 1$ cannot be a square.

16. The units digit of the square of an integer must be one of 1,4,5,6,9. But when $n > 4$, the number $a = 5! + \cdots n!$ is divisible by 10 and so the units digit of $b = 1! + 2! + 3! + 4! + a = 33 + a$ is 3.. Hence b is not a square.

17. Let $a < b$ and $a = 81m$, $b = 81n$ so that by data $(m, n) = 1$. Also, then l.c.m. of $a, b = 81mn = 5103 = 81 \times 63$, so that $mn = 63 = 7 \times 9$. But $(m, n) = 1$. Hence we may take $m = 7$, $n = 9$. Thus $a = 81m = 567$, $b = 81n = 729$.

18. Let $a = 2^x 3^y 5^z b$ where b is coprime to 2,3 and 5. Then given conditions imply that (i) $x + 1$, y, z are divisible by 2 and (ii) x, $y + 1$, z are divisible by 3 and (iii) x, y, $z + 1$ are divisible by 5. so by trial, the smallest values of x, y, z are 15, 20, 24 respectively. Also, for any integer n, $b = n^{30}$ is a square, cube and a fifth power. Hence, we may take $a = 2^{15} 3^{20} 5^{24} n^{30}$.

19. Let $(a, b) = d$ so that $a = dm$, $b = dn$ and $(m, n) = 1$. Then $\frac{a+1}{b} + \frac{b+1}{a} = c$, an integer. This implies that $a^2 + a + b^2 + b = abc$

or $(a+b)^2+a+b = abc+2ab$ or $d(m^2+n^2)+m+n = dmnc+2dmn$, so that d divides $m+n$ and so $d \leq (m+n)$ as all numbers are positive. Hence, $d^2 \leq d(m+n) = a+b$, as was to be proved.

20. If n is composite then $n = n_1 n_2$ where $n_1 > 1$ and $n_2 > 1$. Hence, $2^{n_1} - 1 > 1$ and $2^{n_1} - 1 | 2^n - 1$.

21. If $n = 2^\alpha n_1$, where n_1 is an odd integer greater than 1 then $2^\alpha + 1 | 2^n + 1$, a contradiction.

22. $x = 8$ and $y = 64$ or $x = 64$ and $y = 8$.

23. Suppose $(a, b) = d$. Then $d|a$ and $d|b$. Since, $(a, b) = [a, b]$, we get that $a|d$ and $b|d$. Hence, $a = \pm d$ and $b = \pm d$. Hence, $a = \pm b$.

24. Note that $n^4+4n^2+11 = (n^4+4n^2-5)+16 = (n^2+5)(n^2-1)+16$. Since, n is odd $8|n^2 - 1$ and $2|n^2 + 5$.

25. x is a solution if and only if $x + 2$ is divisible by $3, 4, \ldots, 10$. Hence, smallest positive solution is given by $[3, \ldots, 10] - 2$ and all solutions are given by $[3, \ldots, 10] - 2 + k \cdot [3, \ldots, 10]$, where $k \in \mathbb{Z}$.

26. Suppose an integer $n > 1$ is a composite number. Then $n = ab$ where both a and b are greater than one. Suppose both a and b are greater than $\sqrt{n}$. Then ab is greater than n, a contradiction. Hence, one of a and b is smaller than or equal to $\sqrt{n}$. Hence,it has a prime divisor d such that $d \leq \sqrt{n}$.

27. $a = 4k + 2, b = 4l + 2$. Hence, $(a + b, 4) = 4$.

28. Take $a = 5 - 100k, b = 95 + 100k$. Now $a + b = 100$ and $(a, b) = (a, a + b) = (5 - 100k, 100) = (5, 100) = 5$.

29. Let $d = (a, b)$ and let $a = a'd$ and $b = b'd$ so that $\gcd(a', b') = 1$. Hence there exist integers x, y such that

$$a'x + b'y = 1. \tag{14}$$

So, on multiplying this equality by dn, we get $a'dnx + b'dny = dn$, or $anx + bny = dn$. But since $ab' = a'b = a'b'd$, this can be rewritten as

$$a(nx - b') + b(ny + a') = dn \quad \text{or} \quad ak + bl = dn, \tag{15}$$

where $k = nx - b'$ and $l = ny + a'$. Now the g.c.d. of k, l is 1. For, if c is the g.c.d. of k and l, then c also divides

$$xl - ky = nxy + a'x - nxy + b'y = a'x + b'y,$$

so that by (14), c divides 1; hence $c = 1$. Thus by (15), k, l are the required integers.

Solutions to Exercise Set -1.2

1. Note that $b = 2q + 1$ for some integer q. Hence, $b^2 = 4q(q + 1) + 1$. Since $2|q(q + 1)$, we get that $b^2 \equiv 1 \pmod 8$.

2. An integer b can be written as $3q$ or $3q \pm 1$. If $b = 3q$, then $b^2 \equiv 0 \pmod 3$. If $b = 3q \pm 1$, then $b^2 \equiv 1 \pmod 3$. Hence, the square of an integer is $\equiv 0, 1 \pmod 3$.

3. If $p \neq 3$ then $3 \nmid p$ then $p^2 \equiv 1 \pmod 3$. Thus, $3|p^2 + 8$. Hence, $p = 3$ is the only prime.

4. An integer b can be written as $5q$ or $5q \pm 1$ or $5q \pm 2$. If $b = 5q$, then $b^2 \equiv 0 \pmod 5$. If $b = 5q \pm 1$, then $b^2 \equiv 1 \pmod 5$. If $b = 5q \pm 2$, then $b^2 \equiv -1 \pmod 5$. Hence, the square of an integer is $\equiv 0, 1, -1 \pmod 5$.

5. Put $2n + 1 = a^2$ and $3n + 1 = b^2$. Since, $2n + 1$ is a perfect square then n is divisible by 4. Hence, $3n + 1 \equiv 1 \pmod 8$. Hence, $8|n$. Since, the square of an integer is $\equiv 0, 1, -1 \pmod 5$. We get $2n + 1 \equiv 0, 1, -1 \pmod 5$ and $3n + 1 \equiv 0, 1, -1 \pmod 5$. If $2n + 1 \equiv 0 \pmod 5$ then $3n + 1 \equiv 2 \pmod 5$, a contradiction. If $2n + 1 \equiv -1 \pmod 5$ then $3n + 1 \equiv 3 \pmod 5$, a contradiction. Hence, $2n + 1 \equiv 1 \pmod 5$ and $5|n$. Since, $(8, 5) = 1$ we get $40|n$.

   Challenge. Show that if $3n + 1$ and $4n + 1$ are both perfect squares then n is divisible by 56.

6. Since, $(n, 6) = 1$, $n^2 \equiv 1 \pmod 8$ and $n^2 \equiv 1 \pmod 3$.

7. We note that $2 + 2\sqrt{28n^2 + 1}$ is an even integer. Hence, $28n^2 + 1$ is a perfect square of an odd integer, say m. Now $28n^2 = m^2 - 1 = (m-1)(m+1)$ and $7n^2 = \left(\frac{m-1}{2}\right)\left(\frac{m+1}{2}\right)$. Hence, $\frac{m-1}{2} = 7a^2$ and $\frac{m+1}{2} = b^2$ or $\frac{m+1}{2} = 7a^2$ and $\frac{m-1}{2} = b^2$.

If $\frac{m+1}{2} = 7a^2$ and $\frac{m-1}{2} = b^2$ then $b^2 \equiv -1 \pmod 7$, a contradiction. Hence, $\frac{m-1}{2} = 7a^2$ and $\frac{m+1}{2} = b^2$. Hence, $2 + 2m = 2 + 2(2b^2 - 1) = 4b^2$, a perfect square.

8. Note that $a^m - b^m = (a-b)(a^{m-1} + a^{m-2}b + \cdots + ab^{m-2} + b^{m-1})$. Since, $a \equiv b \mod m^n$, $a \equiv b \mod m$. Hence, $a^{m-i}b^i \equiv b^m \mod m$ and $a^{m-1} + a^{m-2}b + \cdots + ab^{m-2} + b^{m-1} \equiv mb^m \equiv 0 \pmod m$. Hence, $a^m - b^m$ is divisible by m^{n+1}.

9. Note that $\frac{a^p - b^p}{a-b} = \sum_{i=0}^{p-1} a^i b^{p-1-i} \equiv pb^{p-1} \equiv pa^{p-1} \pmod{a-b}$. It follows that the gcd $\left(\frac{a^p - b^p}{a-b}, a-b\right)$ divides pa^{p-1} and pb^{p-1}. Since a and b are coprime the gcd is 1 or p.

Solutions to Exercise Set - 1.3

1. When 2^{50} is divided by 7 the remainder is 4. Note that $41 \equiv -1 \pmod 7$ Hence, $41^{65} \equiv -1 \equiv 6 \pmod 7$.

2. The unit's digit of 3^{100} is 1.

3. Observe that $a^{p-1} \equiv 1 \pmod p$ and $b^{p-1} \equiv 1 \pmod p$.

4. (i) Note that $53 \equiv -1 \pmod 3$ and $103 \equiv 1 \pmod 3$. Hence,

$$(53)^{103} \equiv -1 \pmod 3 \text{ and } (103)^{53} \equiv 1 \pmod 3.$$

This shows that $(53)^{103} + (103)^{53} \equiv 0 \pmod 3$. Also, $53 \equiv 1 \pmod{13}$ and $103 \equiv -1 \pmod{13}$. Hence, $(53)^{103} \equiv 1 \pmod{13}$ and $(103)^{53} \equiv -1 \pmod{13}$. This shows that $(53)^{103} + (103)^{53} \equiv 0 \pmod{13}$. But $(3, 13) = 1$. Hence, $(53)^{103} + (103)^{53} \equiv 0 \pmod{39}$.

Also, $111 \equiv 3 \pmod 6$. Hence, $333^{111} \equiv 4^3 \equiv 1 \pmod 7$.

(ii) Note that $111 \equiv -1 \pmod 7$ and $333 \equiv 4 \pmod 7$. Also, $111 \equiv 3 \pmod 6$. Hence, $333^{111} \equiv 4^3 \equiv 1 \pmod 7$.

5. Note that p, q are primes, hence using Euler's theorem we get $p^{q-1} \equiv 1 \pmod q$ and $q^{p-1} \equiv 1 \pmod p$.

6. Use Euler's theorem and note that 101 is a prime. Hence, $7^{200} \equiv 1 \pmod{101}$ and $11^{800} \equiv 1 \pmod{101}$. Hence, the remainder is 2.

7. Note that $2^{11} \equiv 1 \pmod{89}$ and $2^{24} = (2^{12})^2 \equiv (-22)^2 \pmod{97}$.

8. Assume that there are finitely many primes of the type $4n+1$, say $p_1, p_2, \cdots, p_r$. Let $N = (2p_1p_2 \cdots p_r)^2 + 1$. Clearly $N > 2$ and is odd. Moreover, none of the p_j's divide N. Since N is of the type k^2+1, N must have a prime factor of the type $4n+1$. Hence, this prime is a new prime of the type $4n+1$, a contradiction. Hence, there are infinitely many primes of the type $4n+1$.

9. Assume that there are finitely many primes of the type $6n+1$, say $p_1, p_2, \cdots, p_r$. Let

$$N = (2 \cdot 3p_1p_2 \cdots p_r)^2 + (2 \cdot 3p_1p_2 \cdots p_r) + 1.$$

Clearly $N > 2$ and is odd. Moreover, 2 , 3 and none of the p_j's divide N. Since $N > 1$, N has a prime factor, say p. Moreover, $p > 3$ and $p \nmid (2 \cdot 3p_1p_2 \cdots p_r) - 1$. Now, $p | (2 \cdot 3p_1p_2 \cdots p_r)^3 - 1$. Suppose $p = 6k-1$, then $((2 \cdot 3p_1p_2 \cdots p_r)^3)^{2k} \equiv 1 \pmod{p}$. Using Fermat's little theorem, we get $p | (2 \cdot 3p_1p_2 \cdots p_r)^2 - 1$. hence $p | (2 \cdot 3p_1p_2 \cdots p_r) + 1$. This implies that $p | (2 \cdot 3p_1p_2 \cdots p_r)^2$, a contradiction. Hence, this prime is a new prime of the type $6n+1$, a contradiction. Hence, there are infinitely many primes of the type $6n+1$.

10. Note that a prime p divides an integer of the form $16a^4 + 1$ then we observe that $p \equiv 1 \pmod{4}$. If $p = 8k+5$ then $((2a)^4)^{2k+1} = (2a)^{p-1} \equiv -1 \pmod{p}$. Hence, by Fermat's little theorem, we get $p|2$. a contradiction. Hence, p is of the type $8n+1$. There are infinitely many primes of the type $8n+1$ can be proved as in the earlier example.

11. Note that $\sum_{r=1}^{n-3} r(r)! = \sum_{r=1}^{n-3} (r+1)! - (r)! = (n-2)! - 1$. Using Wilson's Theorem, we get that $(n-2)! - 1$ is divisible by n if and only if n is prime.

12. Note that $\binom{2p}{p} = 2 + \sum_{r=1}^{p-1} \binom{p}{r}\binom{p}{p-r} \equiv 2 \pmod{p^2}$ as $p | \binom{p}{r}$ for $1 \le r \le p-1$. Also, note that

$\binom{pa}{pb} = \sum_{r_1+\cdots+r_a=pb} \binom{p}{r_1}\binom{p}{r_2}\cdots\binom{p}{r_a}$. As $p | \binom{p}{r}$ for $1 \le r \le p-1$,

$$\binom{pa}{pb} \equiv \binom{a}{b} \pmod{p^2}.$$

Challenge. Show that if $p \geq 5$ is a prime then

$$\binom{2p}{p} \equiv 2 \pmod{p^3} \text{ and } \binom{pa}{pb} \equiv \binom{a}{b} \pmod{p^3}.$$

13. (i) Suppose $y^2 = x^3 + 7$. Hence, $y^2 + 1 = x^3 + 8$. Hence, x must be odd and y must be even. Moreover, $y^2 + 1 = (x+2)(x^2 - 2x + 4) = (x+2)((x-1)^2 + 3)$. Now, $(x-1)^2 + 3$ is of the type $4n-1$ and hence it has a prime factor p of the type $4n-1$. Hence, $y^2 \equiv -1 \pmod{p}$. But, $p \equiv -1 \pmod{4}$, a contradiction.

(ii) Let (x, y) be a solution of $y^2 = 41x + 3$. Then $y^2 \equiv 3 \pmod{41}$. But 3 is not a square modulo 41. Hence, there are no such solutions.

14. Let $p_1, \ldots, p_n, q_1, \ldots, q_n$ denote $2n$ distinct primes. Consider, the system of congruences given by, $x \equiv -r \pmod{p_r q_r}$ for $1 \leq r \leq n$. Since, $(p_r q_r, p_s q_s) = 1$ by Chinese remainder theorem, this system has a common solution. Hence, for each positive integer n there exist n consecutive positive integers none of which is an integral power of a prime number.

15. If p is a prime and $0 < r < p$, we have by Wilson's theorem $(p-1)! = (p-r)!(p-(r-1))(p-(r-2))\cdots(p-1) \equiv -1 \pmod{p}$. Hence, $(p-r)!(r-1)! \times (-1)^{r-1} \equiv -1 \pmod{p}$. Thus,

$$(p-r)!(r-1)! + (-1)^{r-1} \equiv 0 \pmod{p}.$$

Note that 19 and 23 are primes and by Wilson's theorem $18! \equiv -1 \pmod{19}$ and by the above result, $18! \times 4! \equiv -1 \pmod{23}$. Hence, $18! \equiv -1 \pmod{23}$. Since, $(19, 23) = 1$, we get $18! \equiv -1 \pmod{437}$.

16. Let $M = 1^5 + 2^5 + \ldots + 100^5$. Note that $101 | r^5 + (101 - r)^5$ for $1 \leq r \leq 50$. Hence, $101 | \sum_{r=1}^{50} r^5 + (101 - r)^5$. Hence, M is divisible by 101. Also, $100 | r^5 + (100 - r)^5$ for $1 \leq r \leq 49$ and $100 | 50^5$ and $100 | 100^5$. Hence, M is divisible by 100. However, $3 | r^5 + (99 - r)^5$ for $0 \leq r \leq 49$. Hence, $1^5 + 2^5 + \ldots + 99^5$ is divisible by 3. But 100^5 is not divisible by 3. Hence, M is not divisible by 3.

17. Note that $(a, b) = 1$. hence, by Euler's theorem, $a^{\phi(b)} \equiv 1 \pmod{b}$ and $b^{\phi(a)} \equiv 1 \pmod{a}$. Let $\{\phi(a) + \phi(b)\} = l$. Hence, $a^l \equiv 1 \pmod{b}$ and $b^l \equiv 1 \pmod{a}$. Since, $a | a$ and $b | b$, we get $a^l + b^l \equiv 1 \pmod{a}$ and $a^l + b^l \equiv 1 \pmod{b}$. Since, $(a, b) = 1$, $a^l + b^l \equiv 1 \pmod{ab}$.

18. Observe that $240 = 3 \times 5 \times 8$. If p is a prime greater than 5, then $(p,3) = (p,5) = (p,8) = 1$. Hence, by Euler's theorem $p^2 \equiv 1 \pmod 3$ which implies that $p^4 \equiv 1 \pmod 3$. Also, by Euler's theorem $p^4 \equiv 1 \pmod 5$ and $p^2 \equiv 1 \pmod 8$. Now $p^4 - 1 = (p^2-1)(p^2+1)$. Since $8|p^2-1$ and $2|p^2+1$ $p^4 \equiv 1 \pmod{16}$. Since, $3, 5, 16$ are relatively prime in pairs, we get $p^4 \equiv 1 \pmod{240}$.

19. Note that $168 = 3 \times 7 \times 8$. If p is an odd prime different from 3 and 7, then $p^2 \equiv 1 \pmod 3$, $p^2 \equiv 1 \pmod 8$ and $p^6 \equiv 1 \pmod 7$. Since, $3, 7, 8$ are relatively prime in pairs, we get $p^6 \equiv 1 \pmod{168}$.

    It is easy to see that $p^6 \equiv 1 \pmod{504}$.

Solutions to Exercise Set - 1.4

1. We want to find the number of zeros at the end of 400! in the decimal expansion i.e. the highest power of 10m which divides 400!. Since, $10 = 5 \times 2$, we will find the highest power of 5 and highest power of 2 which divides 400! and take the least among the 2. Hence, the highest power of 10 which divides 400! is 99.

2. Note that $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ is a perfect square if and only if each α_i is even if and only if $d(n) = \prod_{i=1}^{k} (1+\alpha_i)$ is odd.

3. The k-th student has to change his position at the d-th stage if and only if d is a divisor of k. Hence, the students whose roll numbers are perfect squares are in sitting position at the end of the drill.

4. Note that $\sigma(n) = \sum_{d|n} d$ and $\sigma^k(n) = \sum_{d|n} d^k$. Hence, $\sigma(n)$ and $\sigma^k(n)$ are multiplicative functions. Hence, the required result.

5. Sppose first that $p = 2^k - 1$ is a prime number, and $n = 2^{k-1}(2^k - 1)$. To show n is perfect we need only show $\sigma(n) = 2n$. Since σ is multiplicative and $\sigma(p) = p + 1 = 2^k$, we know $\sigma(n) = \sigma(2^k - 1).\sigma(p) = (2^k - 1)2^k = 2n$. This shows that n is a perfect number.

    On the other hand, suppose n is any even perfect number and write n as $2^{k-1}m$ where m is an odd integer and $k \geq 2$. Again σ is multiplicative so $\sigma(2^{k-1}m) = \sigma(2^{k-1}).\sigma(m) = (2^k - 1).\sigma(m)$. Since n is perfect we also know that $\sigma(n) = 2n = 2^k m$. Together these two criteria give $2^k m = (2^k - 1).sigma(m)$, so $2^k - 1$ divides $2^k m$ hence $2^k - 1$ divides

m, say $m = (2^k - 1)M$. Now substitute this back into the equation above and divide by $2^k - 1$ to get $2^k M = sigma(m)$. Since m and M are both divisors of m we know that $2^k M = \sigma(m) \geq m + M = 2^k M$, so $\sigma(m) = m + M$. This means that m is prime and its only two divisors are itself (m) and one (M). Thus $m = 2^k - 1$ is a prime and we have proved that the number n has the prescribed form.

6. Note that $[x] = \left[\frac{x}{2}\right] + \left[\frac{x+1}{2}\right]$. Hence,

$$\begin{aligned} n &= \left[\frac{n}{2}\right] + \left[\frac{n+1}{2}\right], \\ \left[\frac{n}{2}\right] &= \left[\frac{n}{4}\right] + \left[\frac{n+2}{4}\right], \\ \left[\frac{n}{4}\right] &= \left[\frac{n}{8}\right] + \left[\frac{n+4}{8}\right], \\ &\vdots \quad\quad \vdots \end{aligned}$$

Adding these equations, we get the required result.

7. Let $\langle a_n \rangle_{n=1}^{\infty}$ be a sequence of positive integers defined by $\sum_{d|n} a_d = 2^n$ for every $n \in \mathbb{N}$. We note that $a_1 = 2$ and if p is an odd prime, then $a_p = 2^p - 2$. If p, q are distinct primes then $a_{pq} = 2^{pq} - (a_1 + a_p + a_q)$. Using Fermat's little theorem, it is easy to see that $pq | a_{pq}$. It is easy to show that for every prime p and positive integer m, $a_{p^m} = 2^{p^m} - 2^{p^{m-1}}$. If $p = 2$ then $2^m | 2^{2^m - 1}$ as well as $2^m | 2^{2^m}$ Hence, $2^m | a_{2^m}$. If p is an odd prime, then using Euler's theorem, we get $p^m | a_{p^m}$.

Challenge. Show that $n | a_n$.

Solutions to Exercise Set -1.5

2. We have already proved that $60 | xyz$. Hence, 3 divides one of x, y, z. Since, each of x, y, z is a sum of two squares, if 3 divides one of x, y, z then 9 also divides it.

3. Since we are not conversant with calculations in base 8, we first convert $(1\ 3\ 7\ 6)_8$ to base 10 to obtain $(7\ 7\ 6)_{10}$ and then convert the base 10 representation to base 12.

4. If $n = (n_s, n_{s-1}, \ldots n_1, n_0)_b$, then $n = n_s b^s + n_{s-1} b^{s-1} + \cdots + n_1 b + n_0$ and

$$\begin{aligned} n &\equiv n_s + n_{s-1} + \cdots + n_1 + n_0 \pmod{b-1} \\ &\equiv (-1)^s n_s + (-1)6s - 1n_{s-1} + \cdots - n_1 + n_0 \pmod{b+1}. \end{aligned}$$

6. $n = 10^3 N$, where $10 \leq N \leq 99$.

10. There are no such triangles.

13. Let $N = 4444^{4444}$. The maximum number of digits in $N < 4444 \times 4 = 17776$. Hence, the maximum possible value of A is $17776 \times 9 = 159984$. Similarly, the maximum possible value of $Bis45$ and sum of digits of $B \leq 12$. Observe that $N \equiv A \equiv B \pmod 9$ and $4444 \equiv 7 \pmod 9$. Since, $7^3 \equiv 1 \pmod 9$, we get $4444^{4444} \equiv 7^{4444} \equiv 7 \pmod 9$ as $4444 \equiv 1 \pmod 3$. Hence, the sum of digits of $B = 7$.

15. We know that there exists l such that $2^l len < 2^{l+1}$. Now, we take the lcm and do the addition. All the terms except $\frac{1}{2^l}$ are even while $\frac{1}{2^l}$ will be odd. Thus, numerator is odd and denominator is even. Hence, the given sum is not an integer.

Challenge. Show that $\sum_{k=1}^{n} \frac{1}{2k-1}$ is not an integer.

21. Let $S = \{(x, y) | x, y \in \mathbb{N},\ 1 \leq x \leq (p-1)/2, 1 \leq y \leq (q-1)/2\}$. We note the set S can be partitioned into two sets S_1 and S_2 according as $qx > py$ or $qx < py$. Note that there are no pairs in S such that $qx = py$. The set S_1 can be described as the set of all pairs (x, y) satisfying $1 \leq x \leq (p-1)/2, 1 \leq y < qx/p$. Then S_1 has $\sum_{j=1}^{(p-1)/2} \left[\frac{qj}{p}\right]$ elements. Similarly S_2 has $\sum_{i=1}^{(q-1)/2} \left[\frac{pi}{q}\right]$. Hence, we get the required result.

Problem. This is a problem for those who know Analytical geometry. Consider the unit circle (i.e. $x^2 + y^2 = 1$) and consider a line having slope m passing through $(-1, 0)$. Find the point of intersection of the line and the circle excluding $(-1, 0)$. What can you say about the point if m is a rational number? See that this point is a point having both the coordinates as rational numbers. Are you familar with this point?

♣♣♣

Chapter 2

Algebra

2.1 Polynomials

We denote the set of rational numbers by $\mathbb{Q}$. Thus,

$$\mathbb{Q} = \left\{ \frac{m}{n} | m, n \text{ are integers}, n \neq 0 \right\}.$$

Also, we denote the set of real numbers by $\mathbb{R}$ and the set of complex numbers by $\mathbb{C}$. Let $\mathbb{F}$ denote any one of the sets $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. If n is a non-negative integer, then an expression of the form

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n, \tag{1}$$

where $a_0, a_1, \ldots, a_n$ are in $\mathbb{F}$ (or in $\mathbb{Z}$), is called a *polynomial* in x with coefficients $a_0, \ldots, a_n$. We express this by saying that $f(x)$ is a polynomial *over* $\mathbb{F}$ (or $\mathbb{Z}$). If $f(x)$ is a polynomial over $\mathbb{Z}$ then $f(x)$ is called a polynomial with integer coefficients. Similarly, we can define a polynomial with real or rational coefficients. If all the coefficients are zero, then $f(x)$ is called the *zero* polynomial and is denoted by 0. If $a_0 \neq 0$, then $f(x)$ is called a polynomial of *degree* n and a_0 is called *its leading coefficient* . The polynomial is said to be *monic* if its leading coefficient is 1. If $n = 0$ and $a_0 \neq 0$, then $f(x) = a_0$ is a polynomial of degree zero. We do not define the degree of the zero polynomial. Two non-zero polynomials are called (*identically*) *equal* if the coefficients of respective powers of x in them are equal.

Theorem 1 (Division Algorithm) Let $f(x)$ and $g(x)$ be polynomials with coefficients in $\mathbb{F}$ and let $g(x)$ be non-zero. Then there exist *unique* polynomials $q(x)$ and $r(x)$ with coefficients in $\mathbb{F}$ such that,

$$f(x) = q(x)g(x) + r(x), \tag{2}$$

where $r(x)$ is either the zero polynomial or a non-zero polynomial of degree less than the degree of $g(x)$.

Here $q(x)$ is called the *quotient* and $r(x)$ the *remainder*, obtained on dividing $f(x)$ by $g(x)$. If $r(x)$ is the zero polynomial, we say that $f(x)$ is *divisible* by $g(x)$ *over* $\mathbb{F}$ or that $g(x)$ is a *factor* of $f(x)$ *over* $\mathbb{F}$.

We note that if $f(x)$ and $g(x)$ are over $\mathbb{Z}$ i.e. if they have integer coefficients, then $q(x)$ and $r(x)$ are, in general, over $\mathbb{Q}$. But if the leading coefficient of $g(x)$ is 1 or -1, then $q(x)$ and $r(x)$ *also* have integer coefficients.

Theorem 2 (Remainder Theorem) Let $a \in \mathbb{F}$. If $f(x)$ is a polynomial, then the remainder after dividing $f(x)$ by $x - a$ is $f(a)$.

Proof: Since the degree of $g(x) = x - a$ is 1, by (2) we get,

$$f(x) = (x - a)q(x) + r,$$

where r is *independent* of x. Hence putting $x = a$ we get $f(a) = r$.

Definition: Let $a \in \mathbb{F}$. Then a is said to be a *root* of a polynomial $f(x)$ (or of the polynomial equation $f(x) = 0$) if $f(a) = 0$.

Theorem 3 (Factor Theorem) A number a is a root of a polynomial $f(x)$ if and only if $x - a$ divides $f(x)$.

Proof: We have $f(x) = (x - a)q(x) + f(a)$. Hence a is a root of $f(x)$ if and only if $f(a) = 0$ if and only if $x - a$ divides $f(x)$ (by theorem 2).

We now state the following theorem without proof.

Theorem 4 (Fundamental Theorem of Algebra) If $f(x)$ is a polynomial of degree $n \geq 1$ with complex coefficients, then $f(x)$ has at *least one complex* root.

We can restate the Fundamental Theorem of Algebra as follows:

Theorem 5 If $f(x)$ is a polynomial of degree $n \geq 1$ with coefficients in $\mathbb{C}$, then $f(x)$ has exactly n roots, not necessarily distinct, in $\mathbb{C}$. Further, if these roots are $b_1, b_2, \ldots, b_n$ then $f(x)$ has the factorization

$$f(x) = a_0(x - b_1)\ldots(x - b_n), \tag{3}$$

where a_0 is the leading coefficient of $f(x)$.

Theorem 6 Let $f(x)$ be a polynomial, as in (1), having integer coefficients and degree $n \geq 1$ and $a_n \neq 0$. Let $p \neq 0$ and $q > 0$ be integers without a common factor. Then if $\frac{p}{q}$ is a rational root of $f(x)$, then p divides a_n and q divides a_0. If $a_0 = \pm 1$, then every rational root of $f(x)$ must be an integer and must divide a_n.

Proof: Let $\frac{p}{q}$ be a root of $f(x)$. Then $f(\frac{p}{q}) = 0$ i.e.

$$a_0(\frac{p}{q})^n + a_1(\frac{p}{q})^{n-1} + \ldots + a_n = 0$$

$$\text{or} \quad -p(a_0p^{n-1} + \ldots + a_{n-1}q^{n-1}) = a_nq^n \tag{4}$$

$$\text{and} \quad a_0p^n = -q(a_1p^{n-1} + \ldots + a_nq^{n-1}). \tag{5}$$

By (4), $p|a_nq^n$ and so $p|a_n$ since p and q are coprime. Similarly (5) shows that $q|a_0$.

Note 1. If $f(x)$ has integer coefficients and a is an integer root of $f(x)$ and m is any integer different from a, then $a - m$ divides $f(m)$.
Proof: On dividing $f(x)$ by $x - m$ we get

$$f(x) = (x - m)q(x) + f(m),$$

where $q(x)$ has integer coefficients. So for $x = a$, we get

$$0 = f(a) = (a - m)q(a) + f(m) \quad \text{or} \quad f(m) = -(a - m)q(a).$$

Hence $(a - m)$ divides $f(m)$.

Example 1 Let $f(x)$ be a polynomial, as in (1), having integer coefficients and let $f(0) = 1989$ and $f(1) = 9891$. Prove that $f(x)$ has no integer roots.

Solution : If a is an integer root, then $a \neq 0$ as $f(0) \neq 0$. Also a must be odd since it must divide $f(0) = a_n = 1989$. But $a \neq 1$ as $f(1) \neq 0$. So taking $m = 1$ in Note 1, we see that the *even* number $(a - 1)$ divides the *odd* number $f(1) = 9891$, a contradiction.

Example 2 Find all polynomials p satisfying $p(x + 1) = p(x) + 2x + 1$.

Solution. Observe that $p(x) = x^2$ satisfies the given condition. We substitute $p(x) = f(x) + x^2$. Hence, the given condition gets transformed to

$$f(x + 1) = f(x).$$

Since, $p(x)$ and x^2 are polynomials, $f(x)$ is also a polynomial and since $f(x + 1) = f(x)$ for all x, we get that $f(x)$ is a constant polynomial. Hence,

$$p(x) = x^2 + c.$$

Note 2. The roots of the equation $ax^2 + bx + c = 0, a \neq 0$ are given by

$$\alpha = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \text{ and } \beta = \frac{-b - \sqrt{b^2 - 4ac}}{2a}.$$

Let us denote the expression $b^2 - 4ac$, i.e. the quantity under the radical sign, by the letter Δ (delta of the Greek alphabet). Then

$$\alpha = \frac{-b + \sqrt{\Delta}}{2a} \text{ and } \beta = \frac{-b - \sqrt{\Delta}}{2a}.$$

We also note that $(\alpha - \beta)^2 = \dfrac{b^2 - 4ac}{a^2} = \dfrac{\Delta}{a^2}$. Hence, it is clear that whether the roots will be real or complex, equal or unequal, depends on Δ. Thus $\Delta = b^2 - 4ac$ discriminates the nature of the roots of the equation. Hence, Δ is called the *discriminant* of the equation.

The nature of the roots of the quadratic equation $ax^2 + bx + c = 0, a, b, c \in \mathbb{R}$ is decided as follows:

1. If $\Delta > 0$, $\sqrt{\Delta}$ is real and $\sqrt{\Delta} \neq 0$. Hence the roots $\dfrac{-b + \sqrt{\Delta}}{2a}$ and $\dfrac{-b - \sqrt{\Delta}}{2a}$ are real and distinct. Note that $(\alpha - \beta)^2 = \dfrac{b^2 - 4ac}{a^2} = \dfrac{\Delta}{a^2}$. Thus, conversely, if the roots are real and unequal, then $\Delta > 0$.

   In particular, suppose $a, b, c \in \mathbb{Q}$ i.e. a, b, c are rational numbers, $a \neq 0$. Now, if Δ is a perfect square of a rational number, say $\Delta = k^2$ then the roots are rational, namely $\dfrac{-b \pm k}{2a}$. On the other hand if Δ is not a perfect square of a rational number, then $\sqrt{\Delta}$ is irrational and so the roots are irrational and they are $\dfrac{-b}{2a} + \dfrac{\sqrt{\Delta}}{2a}$ and $\dfrac{-b}{2a} - \dfrac{\sqrt{\Delta}}{2a}$, i.e they are always of the form $m + \sqrt{n}$ and $m - \sqrt{n}$, where $m = \dfrac{-b}{2a}$ and $n = \Delta 4a^2$ are rational numbers. Thus, **if $a, b, c \in \mathbb{Q}$ then the roots $m + \sqrt{n}$ and $m - \sqrt{n}$ always occur in pairs.**

2. If $\Delta = 0$ then the roots $\dfrac{-b \pm \sqrt{\Delta}}{2a} = \dfrac{-b}{2a}$ are real and equal. Conversely, it is easy to see that if the roots are real and equal, then $\Delta = 0$.

3. If $\Delta < 0$. $\sqrt{\Delta}$ is imaginary and the roots are complex numbers. Let $\Delta = -k^2$ where $k > 0$. Hence the roots $\dfrac{-b}{2a} + \dfrac{k}{2a}i$ and $\dfrac{-b}{2a} - \dfrac{k}{2a}i$, i.e.

they are complex conjugate numbers of the form $m+it$ and $m-it$, where $m = \frac{-b}{2a}$ and $t = k2a$ are real numbers. $(\alpha - \beta)^2 = \frac{b^2 - 4ac}{a^2} = \frac{\Delta}{a^2}$. Thus, conversely, if the roots are non-real, then $\Delta < 0$.

Note 3. If $f(x)$ has real coefficients and if $c = a + ib$ (where $a, b \in \mathbb{R}$ and $b \neq 0$) is a complex root of $f(x)$, then the conjugate $\bar{c} = a - ib$ of c is also a root of $f(x)$.

Proof: On dividing $f(x)$ by $g(x) = (x - c)(x - \bar{c}) = (x - a)^2 + b^2$, we get

$$f(x) = (x - c)(x - \bar{c})q(x) + ex + d, \tag{6}$$

where $q(x)$ and $ex + d$ have real coefficients. Now

$$f(c) = 0 = e(a + ib) + d \text{ and so } ea + d = 0 \text{ and } eb = 0.$$

This gives $e = 0$ as $b \neq 0$. Hence $d = 0$. So by (6), $f(\bar{c}) = 0$.

Note 4. It can be shown that every polynomial of *odd* degree n with real coefficients has at least one real root.

Note 5. If a real quadratic surd $a + \sqrt{b}$ is a root of a polynomial $f(x)$ with rational coefficients, then $a - \sqrt{b}$ is also a root of $f(x)$.

An expression in variables $a, b, \ldots$, is said to be *symmetric* in $a, b \ldots$ if it is unchanged under all permutations of $a, b, \ldots$.

Thus $a + b$ and $a/b + b/a$ are symmetric in a, b but $a - b$ is not symmetric. The simplest symmetric polynomials in a, b and c are the following : $a + b + c$, $ab + ac + bc$, abc. These are respectively the sum of products of a, b, c taken one at a time, two at a time and three at a time. The first two of these are usually denoted respectively by $\sum a, \sum ab$. These three polynomials are called *elementary symmetric polynomials* in a, b, c. Similarly the elementary symmetric polynomials in a, b, c, d are

$$\sum a = a + b + c + d, \quad \sum ab = ab + ac + ad + bc + bd + cd,$$
$$\sum abc = abc + abd + acd + bcd \text{ and } abcd.$$

We have

Theorem 7 (Newton) Every symmetric polynomial in $a_1, a_2, \ldots, a_n$ with integer coefficients (coefficients in $\mathbb{F}$) can be expressed as a polynomial in the elementary symmetric polynomials in $a_1, a_2, \ldots, a_n$ with integer coefficients (respectively with coefficients in $\mathbb{F}$).

For example, $a^2+b^2+c^2 = (a+b+c)^2-2(ab+bc+ca) = (\sum a)^2-2\sum ab$ and

$$\begin{aligned} a^3+b^3+c^3 &= (a+b+c)(a^2+b^2+c^2-ab-bc-ca)+3abc \\ &= (a+b+c)((a+b+c)^2-3(ab+bc+ca))+3abc \end{aligned}$$

Now consider the cubic equation $f(x)=0$, where

$$f(x) = a_0x^3+a_1x^2+a_2x+a_3, a_0 \neq 0.$$

Let α, β, γ be its roots. Then by (3),
$f(x) = a_0(x-\alpha)(x-\beta)(x-\gamma)$. Hence,

$$a_0x^3+a_1x^2+a_2x+a_3 = a_0[x^3-(\sum\alpha)x^2+(\sum\alpha\beta)x-\alpha\beta\gamma].$$

Hence equating coefficients of various powers of x on the two sides we obtain

$$\sum\alpha = -\frac{a_1}{a_0}, \quad \sum\alpha\beta = \frac{a_2}{a_0}, \quad \alpha\beta\gamma = -\frac{a_3}{a_0}. \tag{7}$$

These give the values of the elementary symmetric polynomials of the roots of $f(x)$ in terms of its coefficients. Similarly, for a fourth degree polynomial $f(x)$ with roots $\alpha, \beta, \gamma, \delta$ we have

$$\sum\alpha = -\frac{a_1}{a_0}, \quad \sum\alpha\beta = \frac{a_2}{a_0}, \quad \sum\alpha\beta\gamma = -\frac{a_3}{a_0}, \quad \alpha\beta\gamma\delta = \frac{a_4}{a_0}. \tag{8}$$

Example 3 Find the roots of $4x^3-16x^2-9x+36=0$, given that one root is the negative of another.

Solution. If the roots are a, b, c, we have $b=-a$, say. So by (7), $a-a+c=4$, $-a^2+ac-ac=-9/4$ and $-a^2c=-9$. Hence $c=4$ and $a=3/2=-b$. Hence, the roots are $\pm\frac{3}{2}, 4$.

Example 4 Let $a, b, c \in \mathbb{R}, a \neq 0$, such that a and $4a+3b+2c$ have the same sign. Show that the equation $ax^2+bx+c=0$ cannot have both roots in the interval $(1,2)$.

Solution. Let α, β be roots of the given quadratic equation. We have

$$\begin{aligned} 0 \leq \frac{4a+3b+2c}{a} &= 4+3\frac{b}{a}+2\frac{c}{a} = 4-3(\alpha+\beta)+2\alpha\cdot\beta \\ &= (\alpha-1)(\beta-2)+(\alpha-2)(\beta-1). \end{aligned}$$

If α, β both belong to $(1,2)$ then each term of the sum will be negative, which is a contradiction.

Example 5 Consider all lines which meet the graph of $y = 2x^4+7x^3+3x-5$ in four distinct points, say $(x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4)$. Then, show that $\dfrac{x_1+x_2+x_3+x_4}{4}$ is independent of the line and find its value.

Solution. Let $y = mx + c$ be any line which intersects the graph $y = 2x^4 + 7x^3 + 3x - 5$ at $(x_i, y_i), 1 \le i \le 4$. Then x_i are roots of $mx + c = 2x^4 + 7x^3 + 3x - 5$. (Note that x_i's are distinct as $x_i = x_j$ would imply $y_i = y_j$.) The above equation reduces to an equation of degree 4, namely $2x^4 + 7x^3 + (3 - m)x - 5 - c = 0$. Hence,

$$\frac{x_1+x_2+x_3+x_4}{4} = -\frac{7}{8}.$$

Example 6 The product of two of the four roots of $x^4 - 20x^3 + kx^2 + 590x - 1992 = 0$ is 24. Find k.

Solution. Let the given equation be written as $f(x) = 0$, and let the roots of the equation be r_1, r_2, r_3, r_4 with $r_1r_2 = 24$. Now $r_1r_2r_3r_4 = -1992$, so $r_3r_4 = -1992/24 = -83$. Also,

$$\begin{aligned} f(x) &= (x - r_1)(x - r_2)(x - r_3)(x - r_4) \\ &= (x^2 - cx + r_1r_2)(x^2 - dx + r_3r_4) \\ &= (x^2 - cx + 24)(x^2 - dx - 83), \end{aligned}$$

with $c = r_1 + r_2, d = r_3 + r_4$. Comparing coefficients of x^3 and x we get $c + d = 20$ and $83c - 24d = 590$. This gives $c = 10, d = 10$. Comparing coefficients of x^2, $k = cd - 83 + 24 = 100 - 83 + 24 = 41$.

Example 7 If α and β are roots of $x^2+px+q = 0$, where p and q are integers with $q|p^2$, then show that

(i) $\alpha^n + \beta^n$ is an integer $(n \ge 1)$,

(ii) $\alpha^n + \beta^n$ is an integer divisible by q $(n \ge 2)$.

Solution. Since α, β are the roots of $x^2 + px + q = 0$, we get

$$\alpha + \beta = -p, \tag{9}$$

$$\alpha\beta = q. \tag{10}$$

Note that $\alpha^2 = -p\alpha - q$. For $n \ge 2$, multiplying this equation by α^{n-2}, we get $\alpha^n = -p\alpha^{n-1} - q\alpha^{n-2}$. Similarly, $\beta^n = -p\beta^{n-1} - q\beta^{n-2}$. Hence,

$$\alpha^n + \beta^n = -p(\alpha^{n-1} + \beta^{n-1}) - q(\alpha^{n-2} + \beta^{n-2}). \tag{11}$$

Also for $n = 2$, $\alpha^2 + \beta^2 = (-p)^2 - 2q = p^2 - 2q.$ (12)

1. By (9) and (12), $\alpha+\beta$ and $\alpha^2+\beta^2$ are both integers. Hence, by (11), it follows by induction on n that $\alpha^n+\beta^n$ is an integer for $n \geq 1$.

2. Since $q|p^2$, (12) shows that $q|(\alpha^2+\beta^2)$. Further,

$$\alpha^3+\beta^3 = -p(\alpha^2+\beta^2) - q(\alpha+\beta)$$

and so $q|(\alpha^3+\beta^3)$. Hence, by (11), it follows by induction on n that $q|(\alpha^n+\beta^n)$ for $n \geq 2$.

Example 8 Find all integers a such that the equation $x^3 - 3x + a = 0$, has three integer roots.

Solution. Let the integer roots of the given equation be α, β, γ. Then

$$\alpha+\beta+\gamma = 0, \alpha\beta+\beta\gamma+\gamma\alpha = -3, \alpha\beta\gamma = -a. \tag{13}$$

Hence, $\alpha^2+\beta^2+\gamma^2 = (\alpha+\beta+\gamma)^2 - 2(\alpha\beta+\beta\gamma+\gamma\alpha) = 6.$ (14)

So, $0 \leq \alpha^2, \beta^2, \gamma^2 \leq 6$ and so the solutions of (14) are essentially the following :

$$\alpha = 2, \beta = -1, \gamma = -1 \tag{15}$$

$$\text{and } \alpha = -2, \beta = 1, \gamma = 1. \tag{16}$$

Both these sets satisfy (13). Hence the required values of a are $a = -2, 2$ corresponding to the roots in (15) and (16) respectively.

Example 9 Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial of degree n with real coefficients $a_0, \ldots, a_n$ such that $a_n = 1$ and $a_i^2 = 1$ for $i = 0, 1, \ldots, n-1$. Suppose that all the roots $c_1, \ldots, c_n$ of the equation $p(x) = 0$ are integers. Find $c_1^2 + c_2^2 + \cdots + c_n^2$. Hence find all such polynomials $p(x)$.

Solution. Since $p(x)$ is a monic polynomial and $a_0 = \pm 1$, we have that each root $c_i = \pm 1$. Therefore $\sum c_i^2 = n$. For $n = 1$, $p(x) = x+1$, or $p(x) = x-1$ are the required polynomials. So let $n \geq 2$. Now

$\left(\sum c_i\right)^2 = \sum c_i^2 + 2\sum_{i<j} c_i c_j$. Hence, $\left(\frac{-a_{n-1}}{a_n}\right)^2 = n + 2\left(\frac{a_{n-2}}{a_n}\right)$.

Hence $1 = n \pm 2$, i.e., $n = 1 \pm 2$ so that $n = 3$ as $n \geq 2$. Therefore

$$p(x) = x^3 + ax^2 + bx + c, \text{ where } a^2 = b^2 = c^2 = 1.$$

As $-a = c_1 + c_2 + c_3 = \pm 1$, and each $c_i = \pm 1$, it follows that

$$p(x) = (x-1)(x-1)(x+1) = x^3 - x^2 - x + 1,$$
$$p(x) = (x+1)(x+1)(x-1) = x^3 + x^2 - x - 1.$$

We also note that in these polynomials all coefficients are ± 1. Hence these are the required polynomials.

Example 10 Find the remainder when $(x+1)^n$ is divided by $(x-1)^3$.

Solution. Dividing $(x+1)^n$ by $(x-1)^3$ we get

$$(x+1)^n = f(x)(x-1)^3 + Ax^2 + Bx + C.$$

Put $x - 1 = y$ or $x = y + 1$. Hence,

$$(y+2)^n = f(y+1)y^3 + A(y+1)^2 + B(y+1) + C.$$

Using Binomial theorem, we get

$$\begin{aligned} y^n + \cdots + y^2\left(\frac{n(n-1)}{2}2^{n-2}\right) + y(n2^{n-1}) + 2^n \\ = f(y+1)y^3 + Ay^2 + (2A+B)y + A + B + C \end{aligned} \tag{17}$$

Now, equating coefficients of y^2, y^1, y^0 we get

$$A = n(n-1)2^{n-3}, 2A + B = n2^{n-1}, A + B + C = 2^n.$$

Solving these equations, we get

$$A = n(n-1)2^{n-3},\ B = n(3-n)2^{n-2},\ C = (n^2 - 5n + 8)2^{n-3}.$$

Hence, the remainder is

$$n(n-1)2^{n-3}x^2 + n(3-n)2^{n-2}x + (n^2 - 5n + 8)2^{n-3}.$$

Example 11 Suppose a, b, c are rational numbers and all the roots of

$$x^4 - ax^2 + bx + c = 0$$

are rational and distinct. Let p, q, r, s be these roots. Prove that the number $4(a + pq) - 3(p+q)^2$ is the square of a rational number.

Solution. Using the relations between roots and coefficients we have

$$p+q+r+s=0 \text{ or } p+q=-(r+s), \quad pq+pr+ps+qr+qs+rs=-a.$$

Hence substituting for a and $p+q$,

$$\begin{aligned} & 4(a+pq)-3(p+q)^2 \\ = \; & 4[-(pq+pr+ps+qr+qs+rs)+pq]-3(r+s)^2 \\ = \; & 4[-(p+q)(r+s)-rs]-3(r+s)^2 \\ = \; & 4(r+s)^2-4rs-3(r+s)^2=(r-s)^2, \end{aligned}$$

which is the square of the rational number $r-s$.

Example 12 For any positive integer n, prove that there exists a polynomial $P(x)$ of degree at least $8n$, such that

$$\sum_{k=1}^{(2n+1)^2} |P(k)| < |P(0)|. \tag{18}$$

Solution: Consider the polynomial

$$\begin{aligned} P(x) &= \prod_{k=2}^{(2n+1)^2} (x-k) \\ &= (x-2)(x-3)\cdots(x-[4n^2+4n])(x-[2n+1]^2). \end{aligned} \tag{19}$$

Clearly,

$$|P(0)| = (4n^2+4n+1)!, \quad |P(1)| = (4n^2+4n)!$$

and $$P(k)=0 \text{ for } 2 \le k \le (2n+1)^2.$$

So (18) holds because then

$$\sum_{k=1}^{(2n+1)^2} |P(k)| = (4n^2+4n)! < (4n^2+4n+1)! = |P(0)|.$$

Also, since the degree of the polynomial in (19) is $d=4n^2+4n=4n(n+1)$ and since either n or $n+1$ is an even integer, we see that $d \ge 8n$.

2.1.1 Complex Numbers

Consider a complex number $z = x + iy$, where x, y are real. Then the real number $r = +\sqrt{x^2 + y^2}$ is called the *modulus* of z, denoted by $|z|$. Clearly $r = |z| \geq 0$ and $r = 0$ if and only if $z = 0$. Let $z \neq 0$ and let θ be any angle such that

$$\cos\theta = \frac{x}{r}, \quad \sin\theta = \frac{y}{r}. \tag{20}$$

Then θ is called an *amplitude* or *argument* of z. Clearly, the angles $\theta \pm 2\pi$, $\theta \pm 4\pi, \ldots$ also satisfy (20). But there is a unique angle θ_0 which satisfies (20) and is such that $-\pi < \theta_0 \leq \pi$. θ_0 is called the *principal argument* of z. Note that $z = x + iy = r(\cos\theta + i\sin\theta)$ and this last expression is called the *polar form* of z. For example, if $z = -1 + i\sqrt{3}$, then $r = 2$ and $\theta_0 = 2\pi/3$, and so $z = 2[\cos(2\pi/3) + i\sin(2\pi/3)]$.

Definition: If n is a positive integer and w, z are complex numbers such that $w^n = z$, then w is called an n^{th} root of z and we say that w is a value of $z^{1/n}$.

For example, $w = (-1 + i\sqrt{3})/2$ is a cube root of 1 (i.e. a value of $1^{1/3}$) because $w^3 = 1$. Similarly, if p, q are integers, $q > 0$, and $w^q = z^p$, then we say that w is a value of $z^{p/q}$.

Theorem 8 (De Moivre) If n is an integer, then

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta.$$

If p, q are integers and $q > 0$, then $\cos(p\theta/q) + i\sin(p\theta/q)$ is one of the values of $(\cos\theta + i\sin\theta)^{\frac{p}{q}}$.

Roots of unity: Let n be a positive integer. Then the n roots of the equation $z^n = 1$ are

$$w_r = \cos\left(\frac{2\pi r}{n}\right) + i\sin\left(\frac{2\pi r}{n}\right),$$

where $r = 0, 1, \ldots, n-1$ and are called the n^{th} roots of unity. These are all non-real except the root 1 when n is odd and except the roots $1, -1$ when n is even. It is easy to see that the sum of all the roots of unity is 0.

Problem 1 Let $f(x) = x^2 + ax + b$ where a, b are real numbers. Prove that there exist quadratic polynomials $p(x)$ and $q(x)$ (with real coefficients) having all roots real and such that $f(x) = \frac{1}{2}[p(x) + q(x)]$.

Problem 2 If the equation $\sum_{i=1}^{n}(x+i-1)(x+i) = 10n$, has roots r and $r+1$, find n.

Problem 3 Let $a, b, c, d \in \mathbf{R}$ and $p(x) = ax^3 + bx^2 + cx + d, a \neq 0$.
(i) Show that the cubic equation $p(x) = 0$ has one real and two purely imaginary roots if and only if $bc = ad$ and $ac > 0$.
(ii) Show that all roots of the cubic equation $p(x) = 0$ are real and two of them are equal but of opposite sign if and only if $bc = ad$ and $ac < 0$.

Exercise Set 2.1

1. Find numbers a, b such that the roots of $x^2 + ax + b = 0$ are a, b.

2. Suppose α, a, b are integers and $b \neq -1$. Show that if α satisfies the equation $x^2 + ax + b + 1 = 0$, then $a^2 + b^2$ is composite.

3. Find all positive integers a, b such that each of the equations

$$x^2 - ax + b = 0 \quad \text{and} \quad x^2 - bx + a = 0$$

has distinct positive integral roots.

4. Let $f(x) = ax^2 + bx + c$ be a quadratic polynomial with integral coefficients, where $a \neq 0$. Show that

(i) if $f(x)$ is factorisable into linear factors with integral coefficients, then there are integers d and e such that

$$d + e = b \quad \text{and} \quad de = ac; \tag{1}$$

and (ii) if integers d and e can be found such that (1) holds, then

$$f(x) = \frac{(ax + d)}{g} \frac{(ax + e)}{a/g},$$

where g is the g.c.d. of a and d and each of the linear factors has integral coefficients.

5. Prove that if $x^2 + px - q$ and $x^2 - px + q$ both factorise into linear factors with integral coefficients, then the positive integers p and q are respectively the hypotenuse and area of a right triangle with sides of integer length. Show further that if

$$x^2 + px - q = (x - \alpha)(x - \beta) \quad \text{and} \quad x^2 - px + q = (x - \gamma)(x - \delta),$$

where $p, q, \alpha, \beta, \gamma, \delta$ are integers, then $\alpha, \beta, \gamma, \delta$ are numerically the radii of the incircle and the three excircles of the triangle.

6. If $a \neq b, c \neq 0$ and if the equations $x^2+ax+bc = 0$ and $x^2+bx+ca = 0$ have a common root, then show that their other roots satisfy the equation $x^2 + cx + ab = 0$.

7. If $2(a + b + c) = \alpha^2 + \beta^2 + \gamma^2$, and the roots of $x^2 + \alpha x - a = 0$ are β, γ and the roots of $x^2 + \beta x - b = 0$ are γ, α, show that the equation whose roots are α, β is $x^2 + \gamma x - c = 0$.

8. Find the cubic in x which vanishes when $x = 1$ and $x = -2$ and has values 4 and 8 when $x = -1$ and $x = 2$ respectively.

9. Suppose $a_0, a_1, \cdots, a_n$ are integers and $a_0 \neq 0$ and $a_n \neq 0$. Consider the polynomial

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n.$$

If $p \neq 0, q > 0$ are coprime integers and p/q is a rational root of the equation $f(x) = 0$, then show that $p|a_n$ and $q|a_0$, and that if $q > 1$, then $p - mq$ divides $f(m)$ for any integer m.

10. Prove that a polynomial $f(x)$, with integral coefficients, has no integral roots if $f(0)$ and $f(1)$ are both odd integers.

11. Given that $x = 2$ is a root of $84x^3 - 157x^2 - kx + 78 = 0$, find the value of k and the other roots.

12. Find an integer root of

(i) $x^3 - 6x^2 + 15x - 14 = 0$ (ii) $x^4 - 2x^3 - 8x^2 + 13x - 24 = 0$.

13. Find all integer roots of

(i) $x^3 + 8x^2 + 13x + 6 = 0$ (ii) $x^3 - 5x^2 - 2x + 24 = 0$.

(iii) $x^5 - 29x^4 - 31x^3 + 31x^2 - 32x + 60$.

14. Find all rational roots of

(i) $4x^3 - 16x^2 - 9x + 36 = 0$ (ii) $2x^3 + 11x^2 + 10x - 8 = 0$

(iii) $8x^3 + 36x^2 + 22x - 21 = 0$ (iv) $x^4 + 4x^3 - 7x^2 - 22x + 24 = 0$

(v) $12x^3 + 4x^2 - 53x + 30 = 0$.

15. Find the square-roots of (i) $-16+30i$ (ii) $5-12i$ (iii) $7+24i$ (iv) $9+40i$.

16. Find real numbers a, b if $x^2 + x + 1$ is a factor of $2x^6 - x^5 + ax^4 + x^3 + bx^2 - 4x - 3$.

17. Find real numbers p, q if $1+i$ is a root of $x^3+px^2+qx+6=0$. Also, solve the equation.

18. Solve the equation if the given number is a root.

(i) $2x^3-7x^2-52x-55=0,\ \ 3-2\sqrt{5}.$

(ii) $x^4-2x^3-x^2-2x-2=0,\ \ 1+\sqrt{3}.$

(iii) $3x^3-7x^2-60x+140=0,\ \ 2\sqrt{5}.$

(iv) $x^4-4x^3+4x-1=0,\ \ 2+\sqrt{3}.$

(v) $x^3-3x^2-6x-20=0,\ \ -1+i\sqrt{3}.$

(vi) $x^4-4x^3+5x^2-2x-2=0,\ \ 1-i.$

19. Solve the given system of equations :

(i) $x+y+z=1,\ \ xy+yz+zx=-4,\ \ xyz=-4.$

(ii) $x+y+z=1,\ \ x^2+y^2+z^2=29,\ \ xyz=-24.$

(iii) $x+y+z=-2,\ \ x^2+y^2+z^2=6,\ \ x^3+y^3+z^3=-8.$

(iv) $x+y+z=18,\ \ x^2+y^2+z^2=110,\ \ x(y+z)=65.$

(v) $x+y+z=-xyz,\ xy+yz+zx=-1,\ (1+x^2)(1+y^2)(1+z^2)=20.$

(vi) $x^2+y^2+z^2=6,\ \ x^3+y^3-xyz=4,\ \ xy+yz+zx=-3.$

20. Find numbers a, b, c such that the roots of $x^3-ax^2+bx-c=0$ are a, b, c.

21. Find a necessary and sufficient condition on real numbers a, b, c so that $x^3+ax^2+bx+c=0$ has three real roots which are in arithmetic progression. (Ans. $2a^3-9ab+27c=0$ and $a^2\geq 3b$.)

22. If α, β are the roots of $2x^2-5x-4=0$, find the simplest quadratic equation whose roots are $\alpha+1/\alpha, \beta+1/\beta$.

23. If α, β, γ are the roots of $x^3+px-q=0$, find the simplest cubic equation whose roots are $\alpha+\beta, \beta+\gamma, \gamma+\alpha$.

24. If α, β, γ are the roots of $x^3-x^2+4x+7=0$, find the simplest cubic equation whose roots are $\alpha+\beta, \beta+\gamma, \gamma+\alpha$.

25. Find the polynomial of degree 3 whose roots are the cubes of the roots of $x^3-x-1=0$.

26. Let $f(x)$ be a polynomial with integer coefficients. If a, b, c are distinct integers such that $f(a) = f(b) = f(c) = -1$, show that the equation $f(x) = 0$ has no integral roots.

27. (i). If a, b, c, d are the roots of $x^4 + x + 1 = 0$, find the equation whose roots are ab, ac, ad, bc, bd, cd.

    (ii). If a, b are two of the roots of $x^4 + x^3 - 1 = 0$, prove that ab is a root of $x^6 + x^4 + x^3 - x^2 - 1 = 0$.

28. Solve the equation $4x^4 - 4x^3 - 13x^2 + 9x + 9 = 0$, given that the sum of two of the roots is zero.

29. Solve the equation $x^4 + 2x^3 - 21x^2 - 22x + 40 = 0$, given that the roots are in arithmetic progression.

30. If the roots of $x^3 - 5x^2 + qx + 8 = 0$ are real and are in geometric progression, then show that $q = -10$.

31. If one root of the equation $x^3 + 2ax^2 - b = 0$, is equal to the sum of the other two, then show that $a^3 = b$.

32. If α is a non-real root of $x^7 = 1$, find the equation whose roots are $\alpha + \alpha^6,\ \alpha^2 + \alpha^5,\ \alpha^3 + \alpha^4$.

33. Prove that if $f(x)$ is a polynomial such that $f(x^n)$ is divisible by $x - 1$, then $f(x^n)$ is divisible by $x^n - 1$.

34. Let $f(x), g(x)$ be polynomials having real coefficients such that $F(x) = f(x^3) + xg(x^3)$ and $F(x)$ is divisible by $x^2 + x + 1$. Prove that $f(x)$ and $g(x)$ are divisible by $x - 1$.

35. Solve the system $x^2 - yz = 3, y^2 - zx = 4, z^2 - xy = 5$.

36. Factorise $(kx - y + z)(x + ky - z)(x - y - kz) - (kx + y - z)(x - ky - z)(x - y + kz)$.

37. For what integer a, does $x^2 - x + a$ divide $x^{13} + x + 90$?

38. Let $f(x), g(x)$ be polynomials with real coefficients. If $f(x)g(x) = f(x^2 + x + 1)$ for all $x \in \mathbb{R}$, show that $f(x)$ is of even degree.

39. Prove Ptolemy's theorem: Let $ABCD$ be a cyclic quadrilateral in the plane of complex numbers. A, B, C, D are represented using complex numbers z_1, z_2, z_3 and z_4. Then, show that

$$|(z_1 - z_2)(z_3 - z_4)| + |(z_2 - z_3)(z_4 - z_1)| = |(z_1 - z_3)(z_2 - z_4)|.$$

40. If 1 and $2+i$ are solutions of $x^5 - 11x^4 + 46x^3 - 94x^2 + 93x - 35 = 0$, find the other solutions.

41. Find the common solutions of the following equations:

$$x^3 + 2x^2 + 2x + 1 = 0 \text{ and } x^{1990} + x^{200} + 1 = 0.$$

42. Solve (i) $x^2 - |3x + 15| - 55 = 0$. (ii) $x^2 + x + 3ix - 8 - i = 0$. (iii) $\sqrt{x^2 - 4x + 3} \geq 2 - x$.

43. Solve the system of equations $x+y+z = a$, $x^2+y^2+z^2 = b^2$, $xy = z^2$ where a and b are constants. Give the conditions on a and b so that x, y, z are distinct positive numbers.

44. Let the polynomial $f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n$ have integral coefficients. If there exist four distinct integers a, b, c and d such that $f(a) = f(b) = f(c) = f(d) = 5$, show that there is no integer k such that $f(k) = 8$.

45. Determine all solutions in real numbers of the system

$$x + y + z = w, \quad \frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{1}{w}.$$

46. Let $a_1, a_2, \ldots, a_n$ be non-zero real numbers and $b_1, b_2, \ldots, b_n$ be real numbers. Find the discriminant of the quadratic equation

$$(a_1x - b_1)^2 + (a_2x - b_2)^2 + \cdots + (a_nx - b_n)^2 = 0.$$

What can you say about the discriminant?

47. Determine all the triangles with integer sides such that area equals semi-perimeter?

48. Let a, b, c be real numbers. Consider the equation

$$(x - a)(x - b) + (x - b)(x - c) + (x - c)(x - a) = 0.$$

Prove that the roots of this equation are always real. Further, show that the roots are equal if and only if $a = b = c$.

2.2 Inequalities

Among the basic properties of order relation in $\mathbb{R}$, we have the following:

For all $a, b, c \in \mathbb{R}$,

(I) Exactly one of the following is true: $a < b$, $a = b$, $a > b$.

(II) If $a < b$ and $b < c$ then $a < c$.

(III) If $a < b$ then $a + c < b + c$.

(IV) If $a < b$ and $c > 0$ then $ac < bc$.

These properties imply the following important results.

1. $a > 0$ and $b > 0 \Rightarrow ab > 0$.
2. $a < b$ and $c < 0 \Rightarrow ac > bc$.
3. For every $a \in \mathbb{R}$, $a^2 \geq 0$, and equality occurs if and only if $a = 0$. This is equivalent to the following:
   (i) $a \neq 0 \Rightarrow a^2 > 0$, and (ii) $a = 0 \Rightarrow a^2 = 0$.
4. If a, b, c, d are all positive, and if $a > b$ and $c > d$, then,
   (i) $ac > bd$ (ii) $(a/d) > (b/c)$.
5. Let $a > 0$, $b > 0$ and $m \in \mathbb{N}$. Then $a > b \Leftrightarrow a^m > b^m$.
6. Let $a > 0$. Then $f(x) = ax^2 + bx + c \geq 0$, for all $x \in \mathbb{R}$ if and only if $b^2 - 4ac \leq 0$.

   We note that

$$f(x) = a\left[(x + \frac{b}{2a})^2 + \frac{4ac - b^2}{4a^2}\right] \ ].$$

Examples

1. If $a > 0$ then show that $a + \frac{1}{a} \geq 2$, with equality if and only if $a = 1$.
2. If a, b, c, d are positive, then show that

$$\sqrt{(a + c)(b + d)} \geq \sqrt{ab} + \sqrt{cd}. \qquad (1)$$

3. If $a, b, c > 0$ and $a + b + c = 1$, then show that $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} \geq 9$.

4. If a, b, c are positive, then show that $(a + b)(b + c)(c + a) \geq 8abc$.

Solutions

1. This follows because the inequality is equivalent to $(a - 1)^2 \geq 0$.

2. Since all terms are positive, the inequality is equivalent to that obtained by squaring both sides. Hence (1) is equivalent to $(a + c)(b + d) \geq ab + cd + 2\sqrt{abcd}$ i.e. to $ad + bc \geq 2\sqrt{abcd}$

$$\text{i.e. to } (\sqrt{ad} - \sqrt{bc})^2 \geq 0. \tag{2}$$

But (2) is true as square of any real number is non-negative. Hence (1) is proved.

3. For, on dividing $a + b + c = 1$ by a, b, c in turn, we get

$$1 + \frac{b}{a} + \frac{c}{a} = \frac{1}{a}, \quad \frac{a}{b} + 1 + \frac{c}{b} = \frac{1}{b}, \quad \frac{a}{c} + \frac{b}{c} + 1 = \frac{1}{c}.$$

$$\text{Adding, } \frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 3 + \left(\frac{a}{b} + \frac{b}{a}\right) + \left(\frac{b}{c} + \frac{c}{b}\right) + \left(\frac{a}{c} + \frac{c}{a}\right)$$
$$\geq 3 + 2 + 2 + 2, \text{ by Ex.1.}$$

Note that equality occurs if and only if $a = b = c$.

4. By Ex. 1, $\frac{\sqrt{a}}{\sqrt{b}} + \frac{\sqrt{b}}{\sqrt{a}} \geq 2$ or $\frac{a+b}{\sqrt{ab}} \geq 2$. Similarly, $\frac{b+c}{\sqrt{bc}} \geq 2$ and $\frac{c+a}{\sqrt{ca}} \geq 2$. Multiplying these three inequalities the result follows.

The Three Means: If a, b are positive real numbers, we define their arithmetic mean (A.M.), geometric mean (G.M.) and harmonic mean (H.M.) as follows

$$\text{A.M.} = A = \frac{a+b}{2}, \text{ G.M.} = G = +\sqrt{ab}, \text{ H.M.} = H = \left(\frac{\frac{1}{a} + \frac{1}{b}}{2}\right)^{-1}.$$

Remark 2.1 Note that the H.M. is the reciprocal of the A.M. of the reciprocals of the given numbers. Further, H.M. of a and b is $\frac{2ab}{a+b}$. We also note that the A.M. can be defined for any real numbers (not necessarily positive) but to define G.M. and H.M. we require necessarily positive real numbers.

Theorem 9 If a, b are positive, then $A \geq G \geq H$. Also, equality occurs if and only if $a = b$.

Proof: First let $a \neq b$. Then $\sqrt{a}$ and $\sqrt{b}$ are unequal and so $(\sqrt{a} - \sqrt{b})^2 > 0$. Hence the identities $A - G = \dfrac{a+b}{2} - \sqrt{ab} = \frac{1}{2}(\sqrt{a} - \sqrt{b})^2$, $G - H = \sqrt{ab} - \dfrac{2ab}{a+b} = \dfrac{\sqrt{ab}(\sqrt{a} - \sqrt{b})^2}{a+b}$ respectively show that $A > G$ and $G > H$.

If $a = b$, it is clear that $A = G = H = a$.

Corollary: If $a > b > 0$, then $a > A > G > H > b$.

Example 5 If $a_1, a_2, \ldots, a_n$ are all positive, then show that

$$\sqrt{a_1 a_2} + \sqrt{a_1 a_3} + \ldots + \sqrt{a_{n-1} a_n} \leq \frac{(n-1)}{2}(a_1 + a_2 + \ldots + a_n).$$

Solution. Add the $n(n-1)/2$ inequalities

$$\sqrt{a_1 a_2} \leq \frac{a_1 + a_2}{2}, \sqrt{a_1 a_3} \leq \frac{a_1 + a_3}{2}, \ldots, \sqrt{a_{n-1} a_n} \leq \frac{a_{n-1} + a_n}{2}$$

and note that in the sum on the right each a_i occurs $n-1$ times.
[For example, for $n = 4$, we have to consider 6 terms:
$\sqrt{a_1 a_2}$, $\sqrt{a_1 a_3}$, $\sqrt{a_1 a_4}$, $\sqrt{a_2 a_3}$, $\sqrt{a_2 a_4}$, $\sqrt{a_3 a_4}$.]

If $a_1, \ldots, a_n$ are n positive real numbers, we define their arithmetic mean A_n, geometric mean G_n and harmonic mean H_n as follows:

$$A_n = \frac{a_1 + \ldots + a_n}{n}, \; G_n = (a_1 a_2 \ldots a_n)^{1/n}, \; H_n = \frac{n}{\frac{1}{a_1} + \ldots + \frac{1}{a_n}}.$$

We observe that one can have a remark similar to Remark 2.1 here. We also have the following generalization of theorem 9.

Theorem 10 If $a_1, \ldots, a_n$ are positive real numbers, then

$$A_n \geq G_n \geq H_n,$$

and equality occurs if and only if $a_1 = a_2 = \ldots = a_n$.

Proof: First we prove by induction on n that $A_n \geq G_n$ with equality if and only if all the n numbers are equal. The result is true for $n = 2$. Assume the result for $n = m - 1$. Suppose $0 < a_1 \leq a_2 \leq \ldots \leq a_m$. We note that the result is true if $a_1 = a_m$. Suppose $a_1 < a_m$. Then clearly

$$m a_1 < a_1 + a_2 + \ldots + a_m < m a_m,$$

so that $a_1 < A_m < a_m$. Hence

$$A_m(a_1 + a_m - A_m) - a_1 a_m = (a_1 - A_m)(A_m - a_m) > 0$$

and so

$$a_1 + a_m - A_m > \frac{a_1 a_m}{A_m} \tag{3}$$

Now since the A.M. of the $m-1$ numbers $a_2, \ldots, a_{m-1}, a_1 + a_m - A_m$ is A_m, we have by induction hypothesis,

$$\begin{aligned} A_m^{m-1} &\geq a_2 \ldots a_{m-1}(a_1 + a_m - A_m) \\ &> a_2 \ldots a_{m-1} \frac{a_1 a_m}{A_m} \qquad \text{[by (3)]} \end{aligned}$$

Hence $A_m^m > a_1 a_2 \ldots a_m$ i.e. $A_m > G_m$.

Thus the result is true for $n = m$ and the induction is complete. We also observe that when the a_i's are unequal, the arithmetic mean is strictly greater than the geometric mean. Hence, if the arithmetic mean and the geometric mean are equal then all the a_i's must be equal.

Finally, applying this result to the n positive numbers $1/a_1, \ldots, 1/a_n$ we see that $G_n \geq H_n$, with equality if and only if $a_1 = \ldots = a_n$.

Example 6 If $b_1, \ldots, b_n$ is a permutation of the n positive numbers $a_1, \ldots, a_n$, then

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} + \ldots + \frac{a_n}{b_n} \geq n.$$

Solution. Using AM-GM inequality for the numbers $\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}$, we get

$$\frac{1}{n}\left(\frac{a_1}{b_1} + \frac{a_2}{b_2} + \ldots + \frac{a_n}{b_n}\right) \geq \left(\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} \ldots \frac{a_n}{b_n}\right)^{1/n} = 1.$$

Example 7 Let x, y, z be positive real numbers satisfying $x+y+z = 1$. Prove that

$$xy(x+y)^2 + yz(y+z)^2 + zx(z+x)^2 \geq 4xyz.$$

Solution. As $x + y + z = 1$, the given inequality holds if and only if

$$\begin{aligned} & xy(1-z)^2 + yz(1-x)^2 + zx(1-y)^2 \geq 4xyz \\ \text{if and only if} \quad & xy + yz + zx - 6xyz + xyz^2 + yzx^2 + zxy^2 \geq 4xyz \\ \text{if and only if} \quad & \frac{1}{z} + \frac{1}{x} + \frac{1}{y} + x + y + z \geq 10 \\ \text{if and only if} \quad & \frac{1}{x} + \frac{1}{y} + \frac{1}{z} \geq 9 \text{ or } \frac{1}{3} \geq \frac{3}{\frac{1}{x} + \frac{1}{y} + \frac{1}{z}} \end{aligned}$$

which is true since $x + y + z = 1$ and A.M. $\geq$ H.M. applies.

Theorem 11 Let a, b be positive real numbers and α, β be positive rational numbers such that $\alpha + \beta = 1$. Then

$$\alpha a + \beta b \geq a^{\alpha} \cdot b^{\beta} \tag{4}$$

and equality occurs if and only if $a = b$.

Proof: We may assume that $\alpha = r/u$, $\beta = s/u$ where $r, s, u \in \mathbf{N}$. Then $\alpha + \beta = 1$ gives $u = r + s$. Applying the A.M.-G.M. inequality to the $r + s$ numbers

$$a_1 = a_2 = \ldots = a_r = a, \quad a_{r+1} = \ldots = a_{r+s} = b,$$

we see that

$$\frac{ra + sb}{r + s} \geq \left(a^r b^s\right)^{1/(r+s)}$$

i.e. $\alpha a + \beta b \geq a^{\alpha} \cdot b^{\beta}$, with equality if and only if $a = b$.

Note.

(i) With the notation of theorem 11, if α, β are given and a, b vary so that $a\alpha + b\beta = c$ =constant, then (4) shows that the product $a^{\alpha}\, b^{\beta}$ attains its *maximum* value, c, when $a = b = c$.

(ii) With the notation of theorem 10, if $a_1, \ldots, a_n$ vary so that $a_1 + \ldots + a_n = c$, then, $A_n \geq G_n$ implies that the product $a_1 a_2 \ldots a_n$ attains its *maximum* value, $(c/n)^n$, when $a_1 = \ldots = a_n = c/n$. Similarly, if $a_1 a_2 \ldots a_n = c$, then $A_n \geq G_n$ implies that the sum $a_1 + \ldots + a_n$ attains its *minimum* value $n \cdot c^{1/n}$, when $a_1 = \ldots = a_n = c^{1/n}$.

Cauchy-Schwarz Inequality:
For any real numbers a, b, c, d, we have the identity

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (bc - ad)^2. \tag{5}$$

Now suppose that c and d are non-zero. From (5) we obtain the inequality

$$(a^2 + b^2)(c^2 + d^2) \geq (ac + bd)^2, \tag{6}$$

because $(bc - ad)^2 \geq 0$. Also equality holds in (6) if and only if

$$(bc - ad)^2 = 0 \text{ or } bc = ad \text{ or } \frac{a}{c} = \frac{b}{d}.$$

Theorem 12 Let a_i and b_i $(i = 1, \ldots, n)$ be any real numbers. Then

$$(a_1^2 + \ldots + a_n^2)(b_1^2 + \ldots + b_n^2) \geq (a_1 b_1 + \ldots + a_n b_n)^2 \quad (7)$$

and equality occurs if and only if either

1. all the a_i's are zero or
2. all the b_i's are zero or
3. the a_i's are proportional to the b_i's i.e., there exists $k \neq 0$ such that $a_i = kb_i$ for all i.

Proof: We have the identity

$$\begin{aligned} & (a_1^2 + \cdots + a_n^2)(b_1^2 + \cdots + b_n^2) - (a_1 b_1 + \cdots + a_n b_n)^2 \\ = \; & (a_1 b_2 - a_2 b_1)^2 + (a_1 b_3 - a_3 b_1)^2 + \ldots + (a_{n-1} b_n - a_n b_{n-1})^2. \quad (8) \end{aligned}$$

This is called Cauchy-Lagrange identity. From it (7) follows immediately and further, equality occurs in (7) if and only if

$$a_1 b_2 - a_2 b_1 = \ldots = a_{n-1} b_n - a_n b_{n-1} = 0.$$

This condition may be written as the set of conditions in the statement of the theorem. (7) is called Cauchy-Schwartz inequality.

Remark 2.2 Another proof of Cauchy-Schwartz inequality follows using exercise 46 from exercise set 2.1. We observe that the discriminant is less than or equal to 0. By actual computation of the discriminant, we get Cauchy-Schwartz inequality. One may also prove the Cauchy-Schwartz inequality using principle of mathematical induction.)

Example 8 If a, b, c are positive, then

$$(a^2 b + b^2 c + c^2 a)(ab^2 + bc^2 + ca^2) \geq 9a^2 b^2 c^2.$$

Solution. This follows from (7) if we put

$$a_1^2 = a^2 b,\ a_2^2 = b^2 c,\ a_3^2 = c^2 a,\ b_1^2 = bc^2,\ b_2^2 = ca^2,\ b_3^2 = ab^2,$$

$n = 3$, where we take a_i, b_i to be positive.

Example 9 If $c_1, \ldots, c_n$ are positive real numbers, then

$$\Big(\sum_{i=1}^{n} c_i\Big)\Big(\sum_{i=1}^{n} \frac{1}{c_i}\Big) \geq n^2.$$

Solution. Put $a_i = \sqrt{c_i}$ and $b_i = \frac{1}{\sqrt{c_i}}$ in (7).

Example 10 For real numbers x, y, z, prove that

$$\left(\frac{x}{2} + \frac{y}{3} + \frac{z}{6}\right)^2 \leq \frac{x^2}{2} + \frac{y^2}{3} + \frac{z^2}{6},$$

with equality only when $x = y = z$.

Solution. Equivalently, we have to show that

$$(3x + 2y + z)^2 \leq 6(3x^2 + 2y^2 + z^2).$$

This follows by applying the Cauchy-Schwarz inequality to the sequences

$$x,\ x,\ x,\ y,\ y,\ z \text{ and } 1,\ 1,\ 1,\ 1,\ 1,\ 1.$$

Theorem 13 (Tchebycheff's Inequality) If $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ are any real numbers such that

$$a_1 \geq a_2 \geq \ldots \geq a_n \text{ and } b_1 \geq b_2 \geq \ldots \geq b_n \tag{9}$$

then

$$\frac{a_1 + \ldots + a_n}{n} \cdot \frac{b_1 + \ldots + b_n}{n} \leq \frac{a_1 b_1 + \ldots + a_n b_n}{n}, \tag{10}$$

where equality holds if and only if either all the a's are equal or all the b's are equal.

Proof: We have the identity

$$n\sum_{i=1}^{n} a_i b_i - \left(\sum_{i=1}^{n} a_i\right)\left(\sum_{i=1}^{n} b_i\right) = \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}(a_i - a_j)(b_i - b_j) \tag{11}$$

To prove this, note that

$$\sum_{i=1}^{n}\sum_{j=1}^{n}(a_i - a_j)(b_i - b_j) = \sum_{i=1}^{n}\sum_{j=1}^{n}\left[a_i b_i + a_j b_j - a_i b_j - a_j b_i\right] \tag{12}$$

$$\text{Now} \quad \sum_{i=1}^{n}\sum_{j=1}^{n} a_i b_i = \sum_{i=1}^{n}\sum_{j=1}^{n} a_j b_j = n\sum_{i=1}^{n} a_i b_i$$

$$\text{and} \quad \sum_{i=1}^{n}\sum_{j=1}^{n} a_i b_j = \sum_{i=1}^{n}\sum_{j=1}^{n} a_j b_i = \left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{n} b_j\right).$$

Using these relations we get (11) from (12).

Now if $i < j$ or if $i > j$, then

$$(a_i - a_j)(b_i - b_j) \geq 0,$$

since both the factors are ≥ 0 or both are ≤ 0 by (9). Hence the right side of (11) is ≥ 0 and so (10) follows. Now suppose that at least two a's are unequal and at least two b's are unequal. Then by (9), $a_1 > a_n$ and $b_1 > b_n$. Hence $(a_1 - a_n)(b_1 - b_n) > 0$ and so the right side of (iii) is > 0 and hence there is strict inequality in (10).

Corollary : Taking $a_i = b_i$ we see that

$$(a_1 + \ldots + a_n)^2 \leq n(a_1^2 + \ldots + a_n^2), \tag{13}$$

where equality holds only when all the a's are equal.

Remark . Assume that $a_1, \ldots, a_n$ be any real numbers. Note that from (13) we get

$$\frac{a_1 + \ldots + a_n}{n} \leq \sqrt{\frac{(a_1^2 + \ldots + a_n^2)}{n}} \tag{14}$$

$\sqrt{\frac{a_1^2 + \ldots + a_n^2}{n}}$ is called root-mean square (RMS) of the given numbers and the inequality (14) is called as RMS-AM inequality.

Remark . If $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ are any real numbers such that

$$a_1 \geq a_2 \geq \ldots \geq a_n \text{ and } b_1 \leq b_2 \leq \ldots \leq b_n \tag{15}$$

$$\text{or } a_1 \leq a_2 \geq \ldots \leq a_n \text{ and } b_1 \geq b_2 \geq \ldots \geq b_n \tag{16}$$

then

$$\frac{a_1 + \ldots + a_n}{n} \cdot \frac{b_1 + \ldots + b_n}{n} \geq \frac{a_1 b_1 + \ldots + a_n b_n}{n}, \tag{17}$$

where equality holds if and only if either all the a's are equal or all the b's are equal.

Remark . Let $r \geq 3$ be any integer. Then if we have r decreasing sequences of *non-negative* real numbers, say

$$\begin{aligned} a_1 &\geq a_2 \geq \cdots \geq a_n \geq 0, \\ b_1 &\geq b_2 \geq \cdots \geq b_n \geq 0, \\ &\vdots \\ l_1 &\geq l_2 \geq \cdots \geq l_n \geq 0, \end{aligned}$$

then by repeated applications of theorem 13, we get

$$\frac{\sum a}{n} \cdot \frac{\sum b}{n} \cdots \frac{\sum l}{n} \leq \frac{\sum (abc \cdots l)}{n}, \tag{18}$$

where equality holds only when $(r-1)$ of the r sequences are constant sequences. In particular,

$$\left(\frac{\sum a}{n}\right)^r \leq \frac{\sum a^r}{n}. \tag{19}$$

Further, let $p, q, r, \ldots$ be a finite sequence of positive real numbers whose sum is m. Then applying (19) to the sequences

$$a_1^p, a_2^p, \ldots, a_1^q, a_2^q, \ldots, a_1^r, a_2^r, \ldots$$

we get

$$\frac{\sum a^p}{n} \frac{\sum a^q}{n} \frac{\sum a^r}{n} \cdots \leq \frac{\sum a^m}{n}, \tag{20}$$

where equality holds only when all the a's are equal.

Example 11 Let $a_1 \leq a_2 \leq \cdots a_n$ be n real numbers such that $\sum_{j=1}^{n} a_j = 0$.

Show that $na_1a_n + \sum_{j=1}^{n} a_j^2 \leq 0$.

Solution. For $1 \leq j \leq n$, put $a_j = a_1 + r_j$. Then $0 = r_1 \leq r_2 \leq \cdots \leq r_n$, and $r_1 + r_2 + \cdots + r_n + na_1 = 0$. Now,

$$\begin{aligned} \sum_{j=1}^{n} a_j^2 &= \sum_{j=1}^{n} (a_1 + r_j)^2 = na_1^2 + 2a_1 \sum_{j=1}^{n} r_j + \sum_{j=1}^{n} r_j^2 \\ &= na_1^2 + 2a_1(-na_1) + \sum_{j=1}^{n} r_j^2 = -na_1^2 + \sum_{j=1}^{n} r_j^2 \end{aligned}$$

$$\begin{aligned} \text{Hence, } na_1a_n + \sum_{j=1}^{n} a_j^2 &= na_1(a_n - a_1) + \sum_{j=1}^{n} r_j^2 \\ &= (-\sum_{j=1}^{n} r_j) r_n + \sum_{j=1}^{n} r_j^2 = \sum_{j=1}^{n} r_j(r_j - r_n) \leq 0. \end{aligned}$$

Example 12 If a, b, c, d, e are real numbers, prove that the roots of

$$x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$$

cannot *all* be real if $2a^2 < 5b$.

Solution. Suppose all the roots α_i $(i = 1, 2, \ldots, 5)$ of the given equation are real. Then $\sum \alpha_i = -a$ and $\sum_{i<j} \alpha_i \alpha_j = b$. Hence

$$a^2 = (\sum \alpha_i)^2 = \sum \alpha_i^2 + 2 \sum_{i<j} \alpha_i \alpha_j = \sum \alpha_i^2 + 2b,$$

so that $\sum \alpha_i^2 = a^2 - 2b$. But by (13) above, $(\sum \alpha_i)^2 \leq 5 \sum \alpha_i^2$. So, $(-a)^2 = (\sum \alpha_i)^2 \leq 5(a^2 - 2b)$ or $10b \leq 4a^2$ or $5b \leq 2a^2$.

Example 13 Prove that if a, b, c are positive then

$$bc(b + c) + ca(c + a) + ab(a + b) \leq 2(a^3 + b^3 + c^3).$$

Solution. By the symmetry of the result we may assume that $a \geq b \geq c$. Then by Tchebycheff's Inequality, we have

$$(a + b + c)(a^2 + b^2 + c^2) \leq 3(a^3 + b^3 + c^3),$$

from which the result follows.

Example 14 If a, b, c are distinct positive numbers, show that

$$\frac{a^8 + b^8 + c^8}{a^3 b^3 c^3} > \frac{1}{a} + \frac{1}{b} + \frac{1}{c}.$$

Solution. By (15) above [extension of theorem 13],

$$\begin{aligned} \left(\frac{a^8 + b^8 + c^8}{3}\right) &> \left(\frac{a + b + c}{3}\right)^8 \\ &> \left(\sqrt[3]{abc}\right)^6 \cdot \frac{\sum a^2 + 2 \sum ab}{9} > (abc)^2 \cdot \frac{3(\sum ab)}{9}. \end{aligned}$$

Weighted means. The ordinary A.M., G.M. and H.M. are special cases of the *weighted mean* which is denoted by $M_r(a)$ or $M_r(a, p)$ and is defined as follows:

Let $p_1, \ldots, p_n$ and $a_1, \ldots, a_n$ be *positive* real numbers and let r be a real number. Then for $r \neq 0$, we define

$$M_r(a) = M_r(a, p) = \left(\frac{p_1 a_1^r + \cdots + p_n a_n^r}{p_1 + \cdots + p_n}\right)^{1/r}.$$

For $r = 0$, we define $M_0(a, p)$ to be the generalized G.M. thus:

$$M_0(a,p) = \left(a_1^{p_1} a_2^{p_2} \cdots a_n^{p_n}\right)^{1/P_n},$$

where $P_n = p_1 + \cdots + p_n$. Here the p_i's are called the weights associated with the a_i's.

In particular, putting $r = 1, p_1 = \cdots = p_n = 1$, we see that

$$M_1(a,p) = \frac{a_1 + \cdots + a_n}{n}, \quad M_{-1}(a,p) = \left(\frac{\frac{1}{a_1} + \cdots \frac{1}{a_n}}{n}\right)^{-1}$$

are the ordinary A.M. and H.M. Also, the number

$$RMS = M_2(a,p) = \left(\frac{p_1 a_1^2 + \cdots + p_n a_n^2}{p_1 + \cdots + p_n}\right)^{1/2}$$

is called the *generalized root-mean square*. Clearly, if $r > 0$, then

$$M_{-r}(a,p) = \left(\frac{p_1 a_1^{-r} + \cdots + p_n a_n^{-r}}{p_1 + \cdots + p_n}\right)^{-1/r} = \frac{1}{M_r(\frac{1}{a}, p)}.$$

We state the following result without proof.

Theorem 14 Let $p_1, \ldots, p_n$ and $a_1, \ldots, a_n$ be *positive* real numbers and let r, s be real numbers. Then, if $r < s$, then

$$M_r(a) \leq M_s(a),$$

where equality holds if and only if all the a_i's are equal. In particular,

$$M_{-1}(a) \leq M_0(a) \leq M_1(a) \leq M_2(a),$$

i.e. H.M. $\leq$ G.M. $\leq$ A.M. $\leq$ RMS,

$$\text{i.e.} \quad \left(\frac{p_1 + \cdots + p_n}{p_1 a_1^{-1} \cdots + p_n a_n^{-1}}\right) \leq \left(a_1^{p_1} a_2^{p_2} \cdots a_n^{p_n}\right)^{1/P_n}$$

$$\leq \left(\frac{p_1 a_1 + \cdots + p_n a_n}{p_1 + \cdots + p_n}\right) \leq \left(\frac{p_1 a_1^2 + \cdots + p_n a_n^2}{p_1 + \cdots + p_n}\right)^{1/2}.$$

Example 15 If a, b, c are non-negative real numbers such that $a + b + c = 1$, then show that

$$\frac{a}{1+bc} + \frac{b}{1+ca} + \frac{c}{1+ab} \geq \frac{9}{10}.$$

Solution. The result clearly holds if one of a, b, c is zero. So let a, b, c be positive. Since $a+b+c=1$, by AM-GM inequality,

$$\frac{1}{3} = \frac{a+b+c}{3} \geq \sqrt[3]{abc} \text{ or } \frac{1}{9} \geq 3abc.$$

Hence, $\frac{1}{1+3abc} \geq \frac{9}{10}$. Now on letting $r=1, n=3$,

$$p_1 = a, p_2 = b, p_3 = c, a_1 = \frac{1}{1+bc}, a_2 = \frac{1}{1+ca} \text{ and } a_3 = \frac{1}{1+ab},$$

and noting that $p_1+p_2+p_3 = a+b+c = 1$, theorem 14 gives

$$\begin{aligned} M_1(a) &\geq M_{-1}(a), \text{ i.e.} \\ \left(\frac{p_1a_1+p_2a_2+p_3a_3}{p_1+p_2+p_3}\right) &\geq \left(\frac{p_1+p_2+p_3}{p_1a_1^{-1}+p_2a_2^{-1}+p_3a_3^{-1}}\right), \\ \text{Hence, } \frac{a}{1+bc}+\frac{b}{1+ca}+\frac{c}{1+ca} &\geq \frac{1}{a(1+bc)+b(1+ca)+c(1+ab)} \\ &= \frac{1}{1+3abc} \geq \frac{9}{10}. \end{aligned}$$

Example 16 Let x, y, and z be non-negative real numbers satisfying $x+y+z=1$. Show that

$$x^2y+y^2z+z^2x \leq \frac{4}{27},$$

and find when equality occurs.

Solution: By cyclic changes, if necessary, assume that y is between x and z. Then $(y-x)(y-z) \leq 0 \leq xy$. So $(y-x)(y-z)z \leq xyz$ and adding x^2y, to both sides we get

$$\begin{aligned} x^2y+(y-x)(y-z)z &\leq x^2y+xyz \\ x^2y+y^2z+z^2x &\leq x^2y+yz^2+2xyz = y(x+z)^2 = (1-y)^2y \\ &\leq 4\left[\frac{\frac{1}{2}(1-y)+\frac{1}{2}(1-y)+y}{3}\right]^3 = \frac{4}{27}, \end{aligned}$$

by the A.M.-G.M. inequality, when $0 \leq y \leq 1$.

Example 17 If a, b, c are real numbers with $a<b<c$ and

$$\begin{aligned} a+b+c &= 6, \\ ab+bc+ca &= 9, \end{aligned}$$

then prove that $0<a<1<b<3<c<4$.

Solution. we have

$$a+b+c = 6, \quad (21)$$
$$ab+bc+ca = 9. \quad (22)$$

Substitute $a+b=6-c$ in (22) to get $ab+c(6-c)=9$. Hence,

$$ab=(c-3)^2. \quad (23)$$

[We get the perfect square on the right side of (23) because of the particular numbers 6 and 9 in (21),(22).] Similarly,

$$ac = (b-3)^2, \quad (24)$$
$$bc = (a-3)^2. \quad (25)$$

Now $c>0$, by (21), since $a<b<c$. If $a=0$, then $c=3$ by (23) and $b=3$ by (24). This is false since $b<c$ by data. Hence $a\neq 0$. Similarly, $b\neq 0$. As $a\neq 0$ and $c\neq 0$, $ac=(b-3)^2\neq 0$ and so $ac>0$. Hence $a>0$, as $c>0$. As, $b>a$ b is positive. Multiplying (23),(24),(25), we have $(a-3)^2(b-3)^2(c-3)^2=a^2b^2c^2$. Hence,

$$(a-3)(b-3)(c-3)=abc+9(a+b+c)-3(ab+bc+ca)-27=abc>0 \quad (26)$$

Since $0<a<b<c, b\geq 3 \Rightarrow c>3$, and this contradicts (21). Thus $b<3$. Hence $b-3<0, a-3<0$ and so $c-3>0$, by (26). Thus $c>3$.

If $b\leq 1$, then $a<1$ so that $ab<1$ and so $(c-3)^2<1$, by (23). Hence $2<c<4$. But then $a+b+c<1+1+4=6$, contradicting (21). Hence $b>1$. If $a\geq 1$, then $ab>1$ and so $(c-3)^2>1$. by (23). Then either $c<2$ or $c>4$. If $c<2$, then we get $a<2$ and $b<2$, contradicting (21). If $c>4$, then again (21) is contradicted since $a\geq 1$ and $b>1$. Thus

$$0<a<1<b<3<c.$$

If $c\geq 4$, then $(c-3)^2\geq 1$ and so $ab\geq 1$, by (23). Hence $a+b>2\sqrt{ab}\geq 2$, so that $a+b+c>2+4=6$, contradicting (21). Hence $c<4$.

Example 18 If a, b, c, d are all positive real numbers, prove that

$$\frac{1}{a^3}+\frac{1}{b^3}+\frac{1}{c^3}+\frac{1}{d^3}\geq \frac{1}{abc}+\frac{1}{bcd}+\frac{1}{cda}+\frac{1}{dab}.$$

Since a, b, c, d are all positive real numbers, by A. M.- G. M. inequality, we get

$$\frac{1}{a^3}+\frac{1}{b^3}+\frac{1}{c^3}\geq\frac{3}{abc},\quad \frac{1}{a^3}+\frac{1}{b^3}+\frac{1}{d^3}\geq\frac{3}{abd},$$
$$\frac{1}{a^3}+\frac{1}{c^3}+\frac{1}{d^3}\geq\frac{3}{acd},\quad \frac{1}{b^3}+\frac{1}{c^3}+\frac{1}{d^3}\geq\frac{3}{bcd}.$$

Adding the last four inequalities and dividing both the sides by 3 we get the result. Moreover, equality holds it any only $a=b=c=d$.

Example 19 If a, b, c denote the three sides of a triangle, prove that

$$a(b-c)^2+b(c-a)^2+c(a-b)^2+4abc>a^3+b^3+c^3.$$

Solution. One observes that if a, b, c are sides of a triangle then

$$a+b>c, b+c>a \text{ and } c+a>b.$$

We have

$$\begin{aligned}
& a(b-c)^2+b(c-a)^2+c(a-b)^2+4abc-[a^3+b^3+c^3]\\
= \;& ab^2+ac^2+bc^2+ba^2+ca^2+cb^2-2abc-a^3-b^3-c^3\\
= \;& c^2(a+b-c)+ab(a+b-c)+ca^2+cb^2-abc-a^3-b^3\\
= \;& c^2(a+b-c)+ab(a+b-c)+(a^2+b^2-ab)(c-a-b)\\
= \;& (a+b-c)[c^2+ab-a^2-b^2+ab]\\
= \;& (a+b-c)(c^2-(a-b)^2)\\
= \;& (a+b-c)(c+b-a)(a+c-b).
\end{aligned}$$

As a, b, c are sides of a triangle, each factor is positive. Hence the required inequality is also valid.

Example 20 If x, y, z are positive real numbers such that $x\geq y\geq z$, prove that

$$\frac{x^2y}{z}+\frac{y^2z}{x}+\frac{z^2x}{y}\geq x^2+y^2+z^2.$$

Solution. As $x\geq y\geq z$, let $z=a$, $y=a+b$, $x=a+b+c$ where b, c are non-negative. Then the given inequality is equivalent to

$$x^3y^2 + y^3z^2 + z^3x^2 \geq x^3yz + y^3zx + z^3xy,$$

i.e. to $x^3y(y-z) + z^3x(x-y) \geq y^3z(x-z),$

or to $(a+b+c)^3(a+b)b + a^3c(a+b+c) \geq a(a+b)^3(b+c),$

or to $[(a+b)^3 + 3c(a+b)^2 + 3(a+b)c^2 + c^3](ab+b^2)$
$+ a^3c(a+b+c) \geq ab(a+b)^3 + ac(a+b)^3,$

or to $\underline{ab(a+b)^3} + b^2(a+b)^3 + [c^3 + 3(a+b)c^2](ab+b^2) + \underline{3a^3bc}$
$+\underline{9a^2b^2c} + \underline{9ab^3c} + 3b^4c + \underline{a^4c} + a^3bc + 3a^3c^2$
$\geq ab(a+b)^3 + a^4c + 3a^3bc + 3a^2b^2c + acb^3,$

which is true since the underlined terms on the left side together contain all the terms on the right side.

We now state the **Rearrangement Inequality** (RI for short) as follows:

Theorem 15. Let $a_1 \leq a_2 \leq \cdots \leq a_n$ and $b_1 \leq b_2 \leq \cdots \leq b_n$ be real numbers. Let (a) denote the ordered n-tuple $(a_1, a_2, \ldots, a_n)$. Then for any permutation $(a') = (a'_1, a'_2, \cdots, a'_n)$ of (a), we have

$$a_1b_n + a_2b_{n-1} + \cdots + a_nb_1 \leq a'_1b_1 + a'_2b_2 + \cdots + a'_nb_n \qquad (1)$$

and

$$a'_1b_1 + a'_2b_2 + \cdots + a'_nb_n \leq a_1b_1 + a_2b_2 + \cdots + a_nb_n \qquad (2)$$

[Thus RI says that the sum $\sum a_ib_i$ is maximum when the sequences (a) and (b) are *similarly ordered* and it is minimum when they are *oppositely ordered.*]

Equality holds in (2) if and only if

$$(a'_k - a'_i)(b_k - b_i) \geq 0 \text{ for all } k, i \text{ where } 1 \leq k < i \leq n.$$

[Thus when $a'_k > a'_i$, the condition $(a'_k - a'_i)(b_k - b_i) \geq 0$ forces the difference $b_k - b_i$ to be zero since $b_k - b_i \leq 0$.]
Similarly, equality holds in (1) if and only if

$$(-a'_k + a'_i)(b_k - b_i) \geq 0 \text{ for all } k, i \text{ where } 1 \leq k < i \leq n.$$

Example 21 Prove that for all positive numbers a, b, c,

$$\frac{a}{b+c}+\frac{b}{c+a}+\frac{c}{a+b}\geq\frac{3}{2}.$$

Solution: Since the inequality to be proved is symmetric in a, b, c, we may assume that $a\leq b\leq c$. Then we get $a+b\leq a+c$ and $a+c\leq b+c$. Hence we get $\frac{1}{a+b}\geq\frac{1}{a+c}\geq\frac{1}{b+c}$. Now by the rearrangement inequality, we get

$$\begin{aligned}\frac{c}{a+b}+\frac{b}{a+c}+\frac{a}{b+c} &\geq \frac{a}{a+b}+\frac{c}{a+c}+\frac{b}{b+c},\\ \frac{c}{a+b}+\frac{b}{a+c}+\frac{a}{b+c} &\geq \frac{b}{a+b}+\frac{a}{a+c}+\frac{c}{b+c}.\end{aligned}$$

Adding these we get

$$2\Big[\frac{c}{a+b}+\frac{b}{a+c}+\frac{a}{b+c}\Big]\geq\Big[\frac{a+b}{a+b}+\frac{c+a}{a+c}+\frac{b+c}{b+c}\Big]=3,$$

from which the result follows.

Example 22 If x, y, z are positive real numbers such that $x^2+y^2+z^2=1$, prove that

$$E\equiv\frac{x}{1-x^2}+\frac{y}{1-y^2}+\frac{z}{1-z^2}\geq\frac{3\sqrt{3}}{2}.$$

Solution: By the RMS inequality we have

$$\frac{(x+y)^2}{2}\leq x^2+y^2=1-z^2 \text{ so that } \frac{z}{1-z^2}\geq\frac{2z}{(x+y)^2}.$$

Hence it follows that

$$E\geq\frac{2x}{(y+z)^2}+\frac{2y}{(z+x)^2}+\frac{2z}{(x+y)^2}. \tag{1}$$

By the Cauchy-Schwarz inequality,

$$\begin{aligned}(x+y+z)\Big(\frac{x}{(y+z)^2}+\frac{y}{(z+x)^2}+\frac{z}{(x+y)^2}\Big)&\\ \geq\Big(\frac{x}{y+z}+\frac{y}{z+x}+\frac{z}{x+y}\Big)^2.&\end{aligned} \tag{2}$$

By Example 21 above, for $x, y, z>0$, we have

$$\frac{x}{y+z}+\frac{y}{z+x}+\frac{z}{x+y}\geq\frac{3}{2}. \tag{3}$$

Further, by the RMS inequality we have

$$\left(\frac{x+y+z}{3}\right)^2 \leq \frac{x^2+y^2+z^2}{3} = \frac{1}{3}$$

$$\Rightarrow \quad x+y+z \leq \sqrt{3} \quad \Rightarrow \quad \frac{1}{x+y+z} \geq \frac{1}{\sqrt{3}}. \qquad (4)$$

Hence (1) gives, using (2),(3), that

$$E \geq \frac{2}{x+y+z}\left(\frac{x}{y+z}+\frac{y}{z+x}+\frac{z}{x+y}\right)^2$$

$$\geq \frac{2}{\sqrt{3}}\left(\frac{3}{2}\right)^2 = \frac{3\sqrt{3}}{2}. \quad \text{[by (4)]}$$

Example 23 If a, b, c are positive real numbers, prove that

$$\frac{\sqrt{a+b+c}+\sqrt{a}}{b+c} + \frac{\sqrt{a+b+c}+\sqrt{b}}{c+a} + \frac{\sqrt{a+b+c}+\sqrt{c}}{a+b} \geq \frac{9+3\sqrt{3}}{2\sqrt{a+b+c}}.$$

Solution: Let $s = a+b+c$ and $x = a/s, y = b/s, z = c/s$. Then the given inequality can be written as

$$\frac{\sqrt{s}+\sqrt{a}}{b+c} + \frac{\sqrt{s}+\sqrt{b}}{c+a} + \frac{\sqrt{s}+\sqrt{c}}{a+b} \geq \frac{9+3\sqrt{3}}{2\sqrt{s}},$$

and on multiplying by $\sqrt{s}$,

$$\frac{s+\sqrt{sa}}{b+c} + \frac{s+\sqrt{sb}}{c+a} + \frac{s+\sqrt{sc}}{a+b} \geq \frac{9+3\sqrt{3}}{2},$$

hence on dividing each numerator and denominator on the left by s,

$$\frac{1+\sqrt{x}}{y+z} + \frac{1+\sqrt{y}}{z+x} + \frac{1+\sqrt{z}}{x+y} \geq \frac{9+3\sqrt{3}}{2},$$

or since $x+y+z = 1$,

$$\frac{1+\sqrt{x}}{1-x} + \frac{1+\sqrt{y}}{1-y} + \frac{1+\sqrt{z}}{1-z} \geq \frac{9+3\sqrt{3}}{2}. \qquad (1)$$

Now $[(1-x)+(1-y)+(1-z)] = 3-(x+y+z) = 2$ and so by the Cauchy-Schwarz inequality,

$$((1-x)+(1-y)+(1-z))\left(\frac{1}{1-x}+\frac{1}{1-y}+\frac{1}{1-z}\right) \geq (1+1+1)^2,$$

$$\text{or } \frac{1}{1-x}+\frac{1}{1-y}+\frac{1}{1-z} \geq \frac{9}{2}. \tag{2}$$

Also, on replacing x, y, z by $\sqrt{x}, \sqrt{y}, \sqrt{z}$ in Example 22 above, we have

$$\frac{\sqrt{x}}{1-x}+\frac{\sqrt{y}}{1-y}+\frac{\sqrt{z}}{1-z} \geq \frac{3\sqrt{3}}{2}. \tag{3}$$

Adding (2) and (3), we get (1).

Exercise Set 2.2

1. Show that, if $a, b, c > 0$, then (i) $\frac{a^3+b^3}{2} \geq \left(\frac{a+b}{2}\right)^3$

   (ii) $\frac{a^2+b^2}{2} \geq \left(\frac{a+b}{2}\right)^2$ (iii) $\frac{a^2+b^2+c^2}{3} \geq \left(\frac{a+b+c}{3}\right)^2$.

2. Show that, if a, b, c, d are positive then

   $$\frac{ab}{a+b}+\frac{cd}{c+d} \leq \frac{(a+c)(b+d)}{a+b+c+d}.$$

3. If $a_1, a_2, \ldots, a_n$ are positive and if $a_1 a_2 \ldots a_n = 1$, then show that

   $$(1+a_1)(1+a_2)\ldots(1+a_n) \geq 2^n.$$

4. If $p, q > 0$ and $p+q = 1$, show that $\left(p+\frac{1}{p}\right)^2+\left(q+\frac{1}{q}\right)^2 \geq \frac{25}{2}$.

5. Show that for every integer $n \geq 2$,

   (i) $n! < \left(\frac{n+1}{2}\right)^n$ (ii) $1 \cdot 3 \cdot 5 \ldots (2n-1) < n^n$

   (iii) $\sum_{i=1}^{n} \sqrt{\binom{n}{i}} \leq \sqrt{n(2^n-1)}$.

6. If p, q are real, prove that any real root α of $x^3+px+q = 0$ satisfies $p^2-4\alpha q \geq 0$.

7. If $a_1, \ldots, a_n$ are positive numbers less than 1 and $S_n = a_1 + \cdots + a_n$, then show that

$$1 - S_n < (1 - a_1)(1 - a_2)\ldots(1 - a_n) < \frac{1}{1 + S_n}.$$

8. If x, y, z are all positive real numbers, then prove that

$$x(1 + y) + y(1 + z) + z(1 + x) \geq 6\sqrt{xyz}.$$

9. Let $x_1, x_2, \ldots, x_n$ be real numbers. If $x_1 + x_2 + \ldots + x_n \leq 1/2$, each $x_i \geq 0$, prove that $(1 - x_1)(1 - x_2)\ldots(1 - x_n) \geq 1/2$.

10. (a) Let $a_1, \ldots a_n$ be any real numbers. Using the fact that $(na_k - \sum_{i=1}^{n} a_i)^2 \geq 0$ for each k, verify that the square of the A.M. of $a_1, \ldots a_n$ is $\leq$ the A.M. of the squares of $a_1, \ldots a_n$.

    (b) (ii) If a, b, c, d, e are real numbers such that $a + b + c + d + e = 8$ and $a^2 + b^2 + c^2 + d^2 + e^2 = 16$, determine the maximum and minimum values of e. Show that they are attained.

2.3 Functional Equations

In this section, we discuss some functional equations. The different techniques used to solve functional equations are illustrated with the help of solved examples. For further discussion, refer to the book written by B. J. Venkatachala listed in the bibliography.

1. If $f : \mathbb{R} \to \mathbb{R}$ is a function satisfying the properties
   (i) $f(-x) = -f(x)$, (ii) $f(x + 1) = f(x) + 1$,
   (iii) $f(1/x) = f(x)/x^2$ for $x \neq 0$, prove that $f(x) = x$, for all $x \in \mathbb{R}$.

2. Find all polynomials $P(x)$ such that $P(F(x)) = F(P(x))$, $P(0) = 0$, where $F(x)$ is a given function satisfying $F(x) > x$ for all $x \geq 0$.

3. Prove that $f(n) = 1 - n$ is the only integer valued function defined on integers such that
   (i) $f(f(n)) = n$ for all $n \in \mathbb{Z}$ and
   (ii) $f(f(n + 2) + 2) = n$ for all $n \in \mathbb{Z}$ and (iii) $f(0) = 1$.

4. Determine all the functions $f : \mathbb{R} \to \mathbb{R}$ such that

$$f(x)f(y) - f(xy) = x + y \text{ for all } x, y \in \mathbb{R}.$$

Solutions

1. The identity function $f(x) = x$, clearly satisfies the given conditions. Conversely. let f be any function which satisfies these conditions.

Putting $x = 0$ in (i) we get $f(0) = 0$. Let $x > 0$. Replacing x by $\frac{1}{x}$ in (ii) we get

$$f\left(\frac{x+1}{x}\right) = f\left(1+\frac{1}{x}\right) = f\left(\frac{1}{x}\right) + 1 = \frac{1}{x^2}f(x) + 1 \text{ [by (iii)]}$$

$$\text{and } f\left(\frac{x+1}{x}\right) = f\left(\left[\frac{x}{x+1}\right]^{-1}\right) = \left[\frac{x}{x+1}\right]^{-2} f\left(\frac{x}{x+1}\right) \text{ [by (iii)]}$$

$$= \left(\frac{x+1}{x}\right)^2 f\left(1-\frac{1}{x+1}\right)$$

$$= \left(\frac{x+1}{x}\right)^2 \left[f\left(\frac{-1}{x+1}\right) + 1\right] \text{ [by (ii)]}$$

$$= \left(\frac{x+1}{x}\right)^2 \left[-f\left(\frac{1}{x+1}\right) + 1\right] \text{ [by (i)]}$$

$$= \left(\frac{x+1}{x}\right)^2 \left[-\frac{1}{(x+1)^2}f(x+1) + 1\right] \text{ [by (iii)]}$$

$$= \left(\frac{x+1}{x}\right)^2 \left[1 - \frac{f(x)+1}{(x+1)^2}\right] \text{ [by (ii)].}$$

Hence,

$$\frac{1}{x^2}f(x) + 1 = \left(\frac{x+1}{x}\right)^2 - \frac{f(x)}{x^2} - \frac{1}{x^2}.$$

$\therefore f(x) = x$, if $x > 0$. If $x < 0$, then $-x > 0$ and so $f(-x) = -x$. Hence by (i). $f(x) = -f(-x) = -(-x) = x$. Hence $f(x) = x$, for all $x \in \mathbb{R}$.

Note: When the domain of f is the set of *rationals*, we have the following alternative method.

Let $f : \mathbb{Q} \to \mathbb{R}$ be a function which satisfies the above conditions. Putting $x = 0$ in (i) we get $f(0) = 0$. By (i) it is enough to prove that $f(x) = x$ for every positive rational x.

By (ii) it follows by induction on n that $\forall\, x \in \mathbb{Q}$ and $\forall\, n \in \mathbb{N}$,

$$f(x+n) = f(x) + n. \tag{iv}$$

In particular, $f(n) = f(0+n) = f(0)+n = n$. Hence by (iii) $\forall\, n \in \mathbb{N}$,

$$f\left(\frac{1}{n}\right) = \frac{1}{n^2}f(n) = \frac{n}{n^2} = \frac{1}{n}. \tag{v}$$

Next, $\forall\, m, n \in \mathbf{N}$, (iii) gives

$$f\left(\frac{m}{n}\right) = \frac{m^2}{n^2} f\left(\frac{n}{m}\right). \tag{vi}$$

Now, by induction on m, we prove that $\forall\, m, n \in \mathbf{N}$,

$$f\left(\frac{m}{n}\right) = \frac{m}{n}. \tag{vii}$$

This is true for $m = 1$ by (v). Now let $m > 1$ and assume that $f(m'/n) = m'/n$ for all $m' < m$ and all n. Then for a given integer n we have either (1) $n < m$ or (2) $n \geq m$. If (1) holds, then by induction hypothesis, $f(n/m) = n/m$ and so by (vi), $f(m/n) = m/n$. If (2) holds, divide n by m to get $n = mq + r$, $0 \leq r < m$. Then

$$\begin{aligned} f\left(\frac{n}{m}\right) &= f\left(q + \frac{r}{m}\right) = f\left(\frac{r}{m}\right) + q \text{ [by (iv)]} \\ &= \frac{r}{m} + q \text{ [as in case (1)]} = \frac{n}{m}. \end{aligned} \tag{viii}$$

Hence (vii) follows.

2. Let $F(0) = a_0$. Then $P(a_0) = P(F(0)) = F(P(0)) = F(0) = a_0$ and $a_0 > 0$. Let $F(a_0) = a_1$. Then, as before, $P(a_1) = a_1$ and $a_1 > a_0$. By induction, if $F(a_n) = a_{n+1}$ then $P(a_n) = a_n$ and $a_{n+1} > a_n$. But this means that the polynomial equation $P(x) - x = 0$ has infinitely many roots $a_0, a_1, \ldots$ Hence $P(x) - x = 0$ for all x, i.e. $P(x) = x$.

3. The function $f(n) = 1 - n$ clearly satisfies conditions (i), (ii) and (iii). Conversely, suppose a function $f : \mathbb{Z} \to \mathbb{Z}$ satisfies (i), (ii) and (iii). Applying f to (ii) we get,

$$f(f(f(n+2)+2))) = f(n)$$

and this gives, because of (i),

$$f(n+2) + 2 = f(n), \tag{iv}$$

for all $n \in \mathbb{Z}$. Now using (iv) it is easy to prove by induction on n that for all $n \in \mathbb{Z}$,

$$f(n) = \begin{cases} f(0) - n, & \text{if } n \text{ is even} \\ f(1) + 1 - n, & \text{if } n \text{ is odd} \end{cases}$$

Also by (iii), $f(0) = 1$. Hence by (i), $f(1) = 0$. Hence $f(n) = 1 - n$ for all $n \in \mathbb{Z}$.

4. We have,

$$f(x)f(y) - f(xy) = x + y \text{ for all } x, y \in \mathbb{R}. \qquad (v)$$

Put $x = y = 0$ in (v). Hence, $f(0)f(0) - f(0) = 0$. This implies that $f(0) = 0$ or $f(0) = 1$. If $f(0) = 0$ then $f(x)f(0) - f(0) = x + 0$. Hence, $x = 0$ for all $x \in \mathbb{R}$, a contradiction. Hence, $f(0) = 1$.
Substituting $y = 0$, in (v) we get $f(x)f(0) - f(0) = x$ i. e. $f(x) = x + 1$.

If we substitute $f(x) = x + 1$ in (v), we get $(x+1)(y+1) - (xy+1) = x + y$. Hence, $f(x) = x + 1$ is the only solution of (v).

Example 5: Show that if $n \equiv 2, 3 \pmod 4$, it is not possible to get a rearrangement $(x_1, \ldots, x_n)$ of $(1, 2, \ldots, n)$ such that $|x_1 - 1|, |x_2 - 2|, \ldots, |x_n - n|$ are all distinct.

Solution. Note that $|x_i - i| = \pm(x_i - i) \equiv (x_i - i) \pmod 2$, and so

$$\sum_{i=1}^{n} |x_i - i| \equiv \sum_{i=1}^{n} x_i - \sum_{i=1}^{n} i = 0 \pmod 2.$$

Now if $|x_1 - 1|, \ldots, |x_n - n|$ are all distinct, then they must be a rearrangement of $0, 1, \ldots, n-1$. (Note: $0 \le |x_i - i| \le n - 1$.) In that case,

$$\sum_{i=1}^{n} |x_i - i| = n(n-1)/2.$$

If $n(n-1)/2$ is even, then $n \equiv 0, 1 \pmod 4$. This shows that if $n \equiv 2, 3 \pmod 4$, then $|x_1 - 1|, \ldots, |x_n - n|$ cannot all be distinct.

Example 6: Let $f(x) = (x - a_1) \ldots (x - a_n) + 1$, where $a_1, \ldots, a_n$ are distinct integers. Show that (i) if n is odd, then $f(x)$ is irreducible over $\mathbb{Z}$ i.e. $f(x)$ cannot be factorised in the form $f(x) = p(x)q(x)$ where $p(x)$ and $q(x)$ are polynomials with integer coefficients and their degrees are less than the degree of $f(x)$ (Here the degree of $f(x)$ is n.) and (ii) if n is even, then either $f(x)$ is irreducible over $\mathbb{Z}$ or is the square of a polynomial with integer coefficients.

Solution. (i) Let $n = 2m + 1$ and let, if possible, $f(x) = p(x)q(x)$ where $p(x)$ and $q(x)$ are polynomials with integer coefficients and their degrees, say r and s, are both less than n. But then, clearly,

$$f(a_i) = 1 \text{ i.e. } p(a_i)q(a_i) = 1 \text{ for } i = 1, \ldots, n \qquad (1)$$

Now $n = r + s = 2m + 1$ and so r, s cannot both be greater than m. So let $r \leq m$. Now by (1), $p(a_i) = 1$ or -1 for $i = 1, 2, \ldots, 2m + 1$. Hence $p(a_i) = 1$ for $m + 1$ values of i or $p(a_i) = -1$ for $m + 1$ values of i. But the degree of $p(x) = r \leq m$. Hence $p(x)$ is the constant polynomial 1 or -1. This is a contradiction. Hence $f(x)$ is irreducible over $\mathbf{Z}$.

(ii) Let $n = 2m$. Let $f(x)$ be reducible over $\mathbf{Z}$ so that $f(x) = p(x)q(x)$ as before. Then $r = s = m$, because if $r < m$ say, then $p(a_i) = \pm 1$ for $i = 1, 2, \ldots, 2m$. Hence $p(a_i) = 1$ (or $p(a_i) = -1$) for atleast m values of i. Hence $p(x)$ is a constant polynomial: contradiction. Hence $r = s = m$. Now since the leading coefficient of $f(x)$ is 1, we may assume that the leading coefficients of $p(x)$ and $q(x)$ are both 1 or both -1. Hence the degree of the polynomial $p(x) - q(x)$ is less than m. But $p(a_i) = q(a_i) = \pm 1$ for $i = 1, 2, \ldots, 2m$. Hence $p(x) - q(x) = 0$ has more than m roots. Hence $p(x)$ and $q(x)$ are equal polynomials, so that $f(x) = [p(x)]^2$.

Exercise Set 2.3

1. Determine the function $f : \mathbb{R} \to \mathbb{R}$ which satisfies
   $x^2 f(x) + f(1 - x) = 2x - x^4, x \in \mathbb{R}$.
2. If $f : \mathbf{Q} \to \mathbb{R}$ satisfies $f(x + y) = f(x) + f(y) \forall x, y \in \mathbf{Q}$, prove that $f(x) = f(1)x, \forall x \in \mathbf{Q}$.
3. Find all $f : \mathbb{R} \to \mathbb{R}$ such that $f(x^2 + f(y)) = (f(x))^2 + y, \forall x, y \in \mathbb{R}$.
4. Let a, b and c be lengths of the sides of a triangle. Show that if $a^2 + b^2 + c^2 = bc + ca + ab$, the triangle is equilateral.
5. If $f(x)$ denotes a polynomial of degree n such that $f(k) = 1/k$ for $k = 1, 2, \ldots, (n + 1)$, determine $f(n + 2)$.
6. For what real values of the variable x does the following inequality hold:
   $$\frac{4x^2}{\left(1 - \sqrt{1 + 2x}\right)^2} < 2x + 9 \quad ?$$
7. Solve the equation $\cos^2 x + \cos^2 2x + \cos^2 3x = 1$.
8. Let a, b, c be real numbers such that
   $$(bc - a^2)^{-1} + (ca - b^2)^{-1} + (ab - c^2)^{-1} = 0.$$
   Prove that $a(bc - a^2)^{-2} + b(ca - b^2)^{-2} + c(ab - c^2)^{-2} = 0$.

9. a, b and c are natural numbers such that the sum of any two of them is greater than the third number. Prove that

$$\left[1-\frac{b-c}{a}\right]^a\left[1-\frac{c-a}{c}\right]^b\left[1-\frac{a-b}{c}\right]^c \leq 1.$$

Hints to Problems

Pr. 1 If $b \geq 0$, take $p(x) = x^2 + kx + \frac{5}{2}b$ and $q(x) = x^2 + (2a-k)x - \frac{1}{2}b$ where the real number k is chosen so that $k^2 - 10b \geq 0$. If $b < 0$, take $p(x) = x^2 + ax + \frac{3}{2}b$ and $q(x) = x^2 + ax + \frac{1}{2}b$.

Pr. 2 The equation is

$$x^2 + nx + \frac{1}{3}(n^2 - 31) = 0.$$

Hence the sum of the roots is $2r + 1 = -n$ and product of roots is $r(r+1) = (n^2-31)/3$. So $n = 11, r = -6$.

Pr. 3 (i) Suppose p, q are real and the roots are $p, qi, -qi$ where $q \neq 0$. (Here the non-real roots have to be complex conjugates.) Then we have the factorization $p(x) = a(x-p)(x-qi)(x+qi) = a(x^3 - px^2 + q^2x - pq^2)$ so that $b = -ap, c = aq^2, d = -apq^2$. These numbers clearly satisfy the given condition. Conversely, let the given condition hold. Then multiplying by b, equation becomes $abx^3 + b^2x^2 + adx + bd = 0$ or $abx^2(x + \frac{b}{a}) + ad(x + \frac{b}{a}) = 0$ or $(x + \frac{b}{a})(x^2 + \frac{c}{a}) = 0$. As $ac > 0$, a and c have the same sign so that $c/a > 0$. So $-b/a$ is the real root and $\pm i\sqrt{c/a}$ are the purely imaginary roots.

(ii) Suppose p, q are real and the roots are $p, q, -q$. Then we have the factorization $p(x) = a(x-p)(x-q)(x+q) = a(x^3 - q^2x - px^2 + pq^2)$ so that $b = -ap, c = -aq^2, d = apq^2$. These numbers clearly satisfy the given condition. Conversely, let the given condition hold. Then multiplying by b, equation becomes $abx^3 + b^2x^2 + adx + bd = 0$ or $(x + \frac{b}{a})(x^2 + \frac{c}{a}) = 0$. So the roots are $-b/a$ and $\pm\sqrt{-c/a}$ which are as required.

Solutions to Exercise Set 2.1

1. $a = b = 0$ or $a = 1, b = -2$.

3. Let integers $\alpha > \beta > 0$ be the roots of (i) $x^2 - ax + b = 0$ and let integers $\gamma > \delta > 0$ be the roots of (ii) $x^2 - bx + a = 0$. For definiteness, let $a \geq b$. Now

$$\alpha + \beta = a, \quad \alpha\beta = b, \quad \text{and} \quad \gamma + \delta = b, \quad \gamma\delta = a.$$

Hence $a-b=1-(\alpha-1)(\beta-1)$. Hence $0 \leq 1-(\alpha-1)(\beta-1) \leq 1$. So $\beta=1$ since α, β are positive integers and $\beta<\alpha$. Thus $a-b=1$. Further, $a-b=(\gamma-1)(\delta-1)-1$, so that $(\gamma-1)(\delta-1)=2$. So since $\gamma>\delta>0$ are integers, we see that $\gamma-1=2$ and $\delta-1=1$, so that $\gamma=3, \delta=2$. Hence, $a=\gamma\delta=6$ and $b=\gamma+\delta=5$. Also, therefore, $\alpha=5$, $\beta=1$.

5. Suppose that $f(x)=x^2+px-q$ and $g(x)=x^2-px+q$ both factorize into linear factors with integer coefficients i.e. both the equations $f(x)=0$ and $g(x)=0$ have integer roots. Then the integers $p^2 \pm 4q$ are both perfect squares, say $d_1^2=p^2+4q$ and $d_2^2=p^2-4q$ where d_1, d_2 are positive integers. So $d_1^2-p^2$ is even so that d_1, p are both even or both odd; similarly for d_2, p. Thus d_1, d_2, p are all even or all odd. Hence $a=(d_1+d_2)/2$ and $b=(d_1-d_2)/2$ are both integers and $d_1=a+b, d_2=a-b$. But then $2p^2=d_1^2+d_2^2=2a^2+2b^2$ and $8q=d_1^2-d_2^2=4ab$ so that $p^2=a^2+b^2$ and $q=\frac{1}{2}ab$. Hence p is the hypotenuse of a right triangle with legs a, b and q is the area of this triangle. Further, if the roots are $\alpha=(-p+d_1)/2$, $\beta=(-p-d_1)/2$, $\gamma=(p+d_2)/2, \delta=(p-d_2)/2$, then the semi-perimeter of the triangle is $s=(a+b+p)/2=(p+d_1)/2=-\beta$, and $q=\alpha\beta=\gamma\delta=$ the area of the triangle. Hence (except for sign) the inradius and exradii are respectively given by $q/s=\alpha\beta/\beta=\alpha$, $q/(s-a)=\gamma\delta/\delta=\gamma$, $q/(s-b)=\gamma\delta/\gamma=\delta$, $q/(s-p)=\alpha\beta/\alpha=\beta$.

8. $\frac{1}{3}(4x^3+2x^2-10x+4)$. **11.** $k=61, -3/4, 13/21$.

12. (i) 2 (ii) -3. **13.** (i) $-1, -1, -6$ (ii) $-2, 3, 4$ (iii) $1, -2, 30$.

14. (i) $4, \pm 3/2$ (ii) $1/2, -2, -4$ (iii) $-7/2, -3/2, 1/2$ (iv) $-4, -3, 1, 2$.
(v) $2/3, 3/2, -5/2$. **15.** $\pm(3+5i)$, $\pm(3-2i)$, $\pm(4+3i)$, $\pm(5+4i)$.

16. $a=4$, $b=1$. **17.** $p=1$, $q=-4$, $1 \pm i$, -3.

18. (i) $3 \pm 2\sqrt{5}, -5/2$. (ii) $1 \pm \sqrt{3}, \pm i$ (iii) $\pm 2\sqrt{5}, 7/3$ (iv) $2 \pm \sqrt{3}, \pm 1$ (v) $-1 \pm i\sqrt{3}, 5$ (vi) $1 \pm i, 1 \pm \sqrt{2}$.

19. (i) $-2, 1, 2$ (ii) $-4, 2, 3$ (iii) $-2, -1, 1$ (iv) $5, 6, 7$
(v) $-1, 1, \pm 2$. (vi) $1, 1, -2$.

20. $(a, b, c)=(a, 0, 0), (-1, -1, 1)$.

21. First suppose that the roots are in A.P., say $p = k-d, q = k, r = k+d$. Then $3k = \sum p = -a$. So $k = -a/3$ is a root. Next, $\sum pq = b$ gives (i) $3k^2 - d^2 = b$, and $pqr = -c$ gives (ii) $k(k^2 - d^2) = -c$. Since $k = -a/3$ is a root, we get $(-a/3)^3 + a(-a/3)^2 + b(-a/3) + c = 0$ i.e. (iii) $2a^3 - 9ab + 27c = 0$. Further, since the roots are real, (i) shows that $0 \le d^2 = 3k^2 - b$ so that $3k^2 \ge b$ i.e. $3(-a/3)^2 \ge b$ or (iv) $a^2 \ge 3b$. Conversely, conditions (iii) and (iv) are sufficient for the roots to be real numbers in A.P. To see this, let (iii),(iv) hold. Then (iii) shows that $r = -a/3$ is a root. Also, by (iv), $a^2 - 3b \ge 0$ or $9r^2 - 3b \ge 0$ so that $t = +\sqrt{3r^2 - b}$ is a real number. Thus $t^2 = 3r^2 - b$. Hence $r - t$ is a root because

$$\begin{aligned} & (r-t)^3 + a(r-t)^2 + b(r-t) + c \\ = \; & r^3 - 3r^2t + 3rt^2 - t^3 + ar^2 - 2art + at^2 + br - bt + c \\ = \; & (r^3 + ar^2 + br + c) - t(3r^2 + t^2 + b + 2ar) + t^2(3r + a) \\ = \; & 0 - t(3r^2 + 3r^2 - b + b + 2r(-3r)) + t^3(0) = 0. \end{aligned}$$

Similarly, $t + r$ is a root. Hence the roots are $r - t, r, r + t$ which are real and are in A.P.

22. $8x^2 - 10x - 61 = 0$. **23.** $x^3 + px + q = 0$.

24. $x^3 - 2x^2 + 5x - 11 = 0$. **25.** $x^3 - 3x^2 + 2x - 1$.

25. Hint: Let α, β, γ be the roots of $x^3 - x - 1 = 0$. Then $\alpha^3 = \alpha + 1$, $\beta^3 = \beta + 1$, $\gamma^3 = \gamma + 1$. So we need to find the equation with roots $\alpha + 1, \beta + 1, \gamma + 1$.

26. Hint: Let, if possible, $x = m$ is an integer root of $f(x)$. Then $f(x) = (x-m)g(x)$ where $g(x)$ is a polynomial with integer coefficients. Hence $-1 = f(a) = (a-m)g(a)$ so that $a - m$ divides 1, hence $a - m = \pm 1$. Similarly, $b - m = \pm 1$, $c - m = \pm 1$. Now two of the differences $a - m$, $b - m$, $c - m$ must have the same sign. For example, let $a - m = -1$ and $b - m = -1$. So $a = b$, a contradiction.

27. (i) Since a, b, c, d are the roots of the equation $x^4 + (0)x^3 + (0)x^2 + x + 1 = 0$, we have

$$\begin{aligned} a + b + c + d &= 0, && (1) \\ ab + ac + ad + bc + bd + cd &= 0, && (2) \\ abc + abd + acd + bcd &= -1, \text{ and} && (3) \\ abcd &= 1. && (4) \end{aligned}$$

Rewrite (2) as

$$\begin{aligned} ab + a(c+d) + b(c+d) + cd &= 0. \text{ Then} \\ \text{by (1), (4),} \quad ab - (a+b)^2 + \frac{1}{ab} &= 0. \end{aligned} \tag{5}$$

Next, rewrite (3) as

$$\begin{aligned} ab(c+d) + cd(a+b) &= -1. \text{ Then} \\ \text{by (1), (4),} \quad -ab(a+b) + \frac{1}{ab}(a+b) &= -1, \\ \text{so } (a+b)(ab - \frac{1}{ab}) = 1 \text{ or } a+b &= \frac{ab}{(ab)^2 - 1}. \end{aligned}$$

Hence on substituting this value of $a+b$ in (5) we get

$$ab + \frac{1}{ab} = \frac{(ab)^2}{((ab)^2-1)^2}.$$

Hence replacing ab by x and simplifying we see that ab satisfies the equation

$$x^6 - x^4 - x^3 - x^2 + 1 = 0.$$

This shows that, in fact, *each* of the *six* products ab, ac, ad, bc, bd, cd satisfies the above *sixth* degree equation. Hence the above equation has exactly these six products as its roots.

28. $\pm 3/2,\ (1 \pm \sqrt{5})/2$. **29.** $-5, -2, 1, 4$.

30 Let $a/r, a, ar$ be the roots. Then $a^3 =$ the product of roots $= -8$. So $a = -2$, as the roots are real. **32.** $x^3 + x^2 - 2x - 1 = 0$.

35. $(x, y, z) = (-11/6, 1/6, 13/6), (11/6, -1/6, -13/6)$.

36. $2(k^2-1)(x-y)(y-z)(z-x)$. **37.** $a = 2$.

38. If $f(x)$ is of odd degree, then it has a real root, say x_1. But then by the given condition it follows that $x_2 = x_1^2 + x_1 + 1$ is also a root. Further, $x_2 \geq |x_1|$ because $x_1^2 + 1 \geq 2\sqrt{x_1^2 \cdot 1} = 2|x_1|$ so that $x_1^2 + x_1 + 1 \geq 2|x_1| + x_1 \geq |x_1|$. Similarly, $x_3 = x_2^2 + x_2 + 1$ is also a root and $x_3 > x_2$ and so on. Hence $f(x) = 0$ has infinitely many roots, a contradiction.

45. (One guesses possible solutions as $x = -y, z = w$ etc.) From 2nd equation, $\dfrac{xy+yz+xz}{xyz} = \dfrac{1}{w}$, so that from 1st equation,

$$(x+y+z)(xy+yz+xz) = xyz.$$

$$\text{Hence, } x^2y + x^2z + y^2z + y^2z + z^2x + z^2y + 2xyz = 0$$

$$\text{i.e. } (x+y)(x+z)(y+z) = 0.$$

Thus, two of x, y, z are opposite of each other and the remaining quantity is equal to w. (Such values of x, y, z, w are clearly a solution of the two equations.)

Solutions to Exercise Set 2.2

1. (i) and (ii) are equivalent to $(a-b)^2 \geq 0$. For (iii), note that $a^2+b^2+c^2-ab-bc-ca = \frac{1}{2}[(a-b)^2+(b-c)^2+(c-a)^2]$.

2. Equivalent to $(ad-bc)^2 \geq 0$. **4.** Hint: By Ex. 1 (ii) above,

$$\text{L.H.S.} = \left(p+1+\frac{q}{p}\right)^2 + \left(q+1+\frac{p}{q}\right)^2 \geq \frac{1}{2}\left(p+1+\frac{q}{p}+q+1+\frac{p}{q}\right)^2.$$

5. (iii) Use (13). **6.** For, then α is a root of $\alpha x^2 + px + q = 0$.

10. (a)

$$\begin{aligned}\sum_{k=1}^{n}(na_k - \sum_{k=1}^{n} a_i)^2 &= n^2\sum_{k=1}^{n} a_k^2 + n(\sum a_i)^2 - 2n(\sum a_i)^2 \\ &= n^2(\sum a_k^2) - n(\sum a_i)^2.\end{aligned}$$

As this must be ≥ 0, we get the result.
(b) $(a+b+c+d)^2 \leq 4(a^2+b^2+c^2+d^2)$ $\therefore (8-e)^2 \leq 4(16-e^2)$ $\therefore 64 - 16e + e^2 \leq 64 - 4e^2$ $\therefore e(5e-16) \leq 0$ $\therefore 0 \leq e \leq 16/5$. $e = 0$ is attained for $a = b = c = d = 2$ and $e = 16/5$ is attained for $a = b = c = d = 6/5$ (These values are easily located by observation.)

Solutions to Exercise Set 2.3

3. $f(x) = x$. **5.** $(1+(-1)^n)/(n+2)]$.

♣♣♣

Chapter 3

Geometry

3.1 Some Important Theorems

Given any two distinct points A and B on a straight line, they determine a line segment of definite length. When we associate with this segment the *direction from A to B*, we obtain the *directed line segment* denoted by AB. Thus directed segments AB and BA have the same length but opposite direction and we denote this by the equation $AB = -BA$, or equivalently by $AB + BA = 0$.

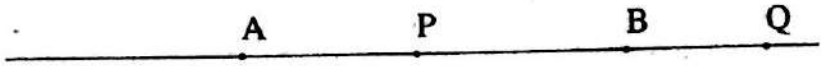


Fig. 3.1

If P is a point on the line AB lying between A and B, P is said to divide the segment AB *internally* and the ratio $AP : PB$ of the division is *positive*. If Q is a point on the line AB lying outside the segment AB, Q is said to divide the segment AB *externally* and the ratio $AQ : QB$ of the division is *negative*. (See Fig. 3.1).

Definition 1 Two polygons are defined to be *similar* if there is a one to one correspondence between their vertices such that their corresponding angles are equal and their corresponding sides are proportional.

Theorem 1 In any triangle ABC, the line joining the midpoints B' and C' of the sides CA and AB respectively, is parallel to BC and $B'C' = \frac{1}{2}BC$.

Theorem 2 Let ABC be a triangle. If a straight line is drawn parallel to BC through the midpoint C' of AB, then it passes through the midpoint of CA.

Theorem 3 If a straight line is drawn parallel to one side of a triangle, then it divides the other two sides (produced, if necessary,) proportionally. Conversely, if a straight line divides two sides (produced, if necessary,) of a triangle proportionally, then it is parallel to the third side.

Theorem 4 The areas of triangles with equal altitudes are proportional to the bases of the triangles. The areas of triangles with equal bases are proportional to the altitudes of the triangles.

Problem 1 Choose point P on side AB of $\triangle ABC$. Let the line parallel to BC through P meet AC in Q, the line parallel to AB through Q meet BC in R, the line parallel to CA through R meet AB in S, the line parallel to BC through S meet AC in T, and the line parallel to AB through T meet BC in U. Prove that PU is parallel to AC. (See Fig. 3.2)

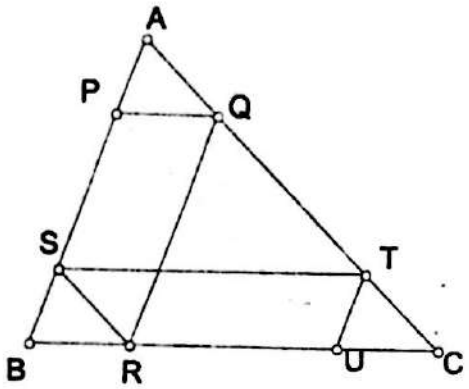


Fig 3.2

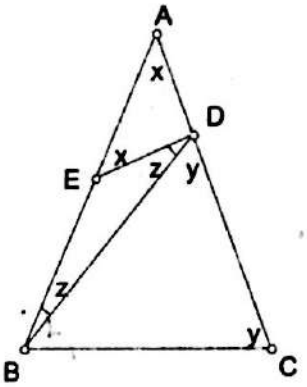


Fig 3.3

Problem 2 In $\triangle ABC$, $AB = AC$. If points D, E are on sides AC, AB respectively such that $BC = BD$ and $AD = DE = EB$, find $\angle A$ (See Fig. 3.3).

Example 1 In a triangle ABC points D and E respectively divide the sides BC and CA in the ratios $\dfrac{BD}{DC} = m$, and $\dfrac{AE}{EC} = n$. The segments AD and BE intersect in a point X. Find the ratio $\dfrac{AX}{XD}$.

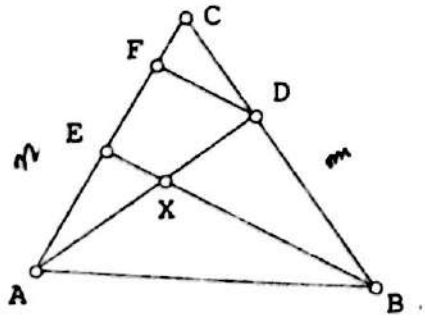


Fig. 3.4

Solution. Draw DF parallel to BE as in Fig.3.4. Then by theorem 3, from $\triangle EBC$ we get

$$\frac{EF}{FC} = \frac{BD}{DC} = m, \text{ and so}$$

$$\frac{EF}{EC} = \frac{BD}{BC} = \frac{m}{m+1}.$$

From $\triangle ADF$ we get

$$\frac{AX}{XD} = \frac{AE}{EF} = \frac{AE}{EC} \cdot \frac{EC}{EF} = n \cdot \frac{m+1}{m}.$$

Example 2 On the sides BC, CA, AB of a triangle ABC points D, E, F are taken in such a way that $\frac{BD}{DC} = \frac{CE}{EA} = \frac{AF}{FB} = 2$. Show that the area of the triangle determined by the lines AD, BE, CF is $\frac{1}{7} \times \Delta$ where Δ is the area of $\triangle ABC$.

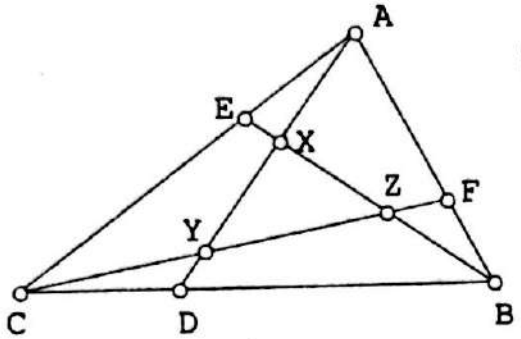


Fig 3.5

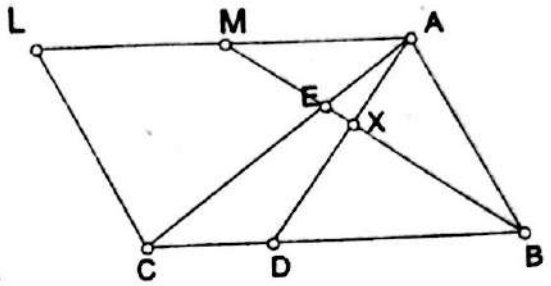


Fig 3.6

Solution. Let XYZ be the triangle formed by the lines AD, BE, CF. Then by Example 1, $AX/XD = \frac{1}{2}\frac{3}{2} = \frac{3}{4}$. Hence $AX/AD = \frac{3}{7}$. Now the triangles ABD and ABC have the same height and so by theorem 4, $\frac{\triangle ABD}{\triangle ABC} = \frac{BD}{BC} = \frac{2}{3}$. Again, the triangles ABX and ABD have the same height and so

$$\frac{AX}{AD} = \frac{\triangle ABX}{\triangle ABD} = \frac{\triangle ABX}{\frac{2}{3}\Delta}.$$

Thus $\triangle ABX = \frac{2}{7} \cdot \Delta$. Similarly, $\triangle BCZ = \triangle CYA = \frac{2}{7} \cdot \Delta$. But clearly,

$$\triangle ABX + \triangle BCZ + \triangle CAY + \triangle XYZ = \Delta,$$

and so $\triangle XYZ = \Delta - 6\Delta/7 = \Delta/7$.

Direct solution by M. R. Railkar

As shown in Fig. 3.6, complete the parallelogram $ABCL$ and let BE meet AD in X and AL in M. Then $\angle AEM = \angle CEB$ and $\angle EAM = \angle ECB$ so that $\triangle AEM \sim \triangle CEB$. Hence that $AM/BC = AE/CE = 1/2$. Similarly, $\triangle AXM \sim \triangle DXB$ so that $BX/XM = BD/AM = \frac{2}{3}BC/\frac{1}{2}BC = 4/3$. Hence $BX/BM = 4/7$. Therefore, since triangles AXB and AMB have bases BX and BM and the same height, we get $\triangle AXB/\triangle AMB = BX/BM = 4/7$. Finally, since M is the mid-point of AL and $AM \parallel BC$, it follows that $\triangle AMB = \frac{1}{2}\triangle ABC$. Hence $\triangle AXB = \frac{4}{7} \cdot \frac{1}{2}\triangle ABC = \frac{2}{7}\triangle ABC$, and the solution can be completed as before.

Theorem 5 If two triangles are equiangular, then their corresponding sides are proportional, and so they are similar. Conversely, if two triangles have corresponding sides proportional, then they are equiangular and hence they are similar.

Theorem 6 Let ABC and DEF be triangles such that $\frac{AB}{DE} = \frac{AC}{DF}$ and $\angle BAC = \angle EDF$. Then the triangles ABC and DEF are similar.

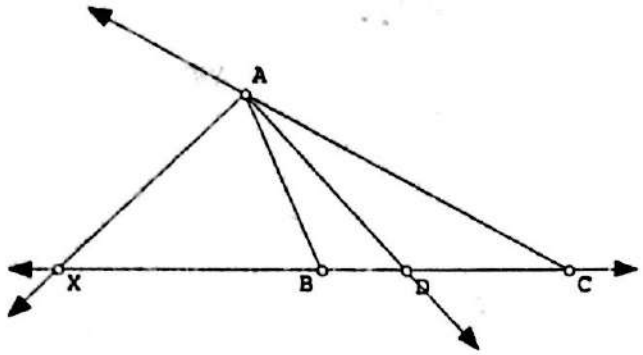


Fig 3.7

Theorem 7 In any $\triangle ABC$, the internal bisector AD of $\angle A$ divides the opposite side BC internally in the ratio $\frac{BD}{DC} = \frac{AB}{AC}$; the external bisector AX of $\angle A$ divides BC externally in the ratio $\frac{BX}{XC} = -\frac{AB}{AC}$. (See Fig. 3.7).

Theorem 8 The straight line that passes through the point of intersection of the diagonals of a trapezium and through the point of intersection of its non-parallel sides, bisects each of the parallel sides of the trapezium.

Theorem 9 Angles in the same segment of a circle are equal. In fact, as in Fig. 3.8, $\angle APB = \angle AQB = (1/2)\angle AOB$, O being the centre of the circle. Conversely, if line segment AB subtends equal angles at two points P, Q on the same side of it, then A, B, P, Q are concyclic. (See Fig. 3.9).

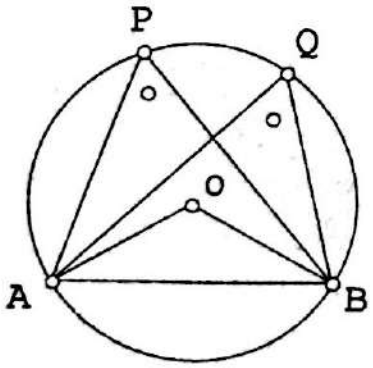


Fig 3.8

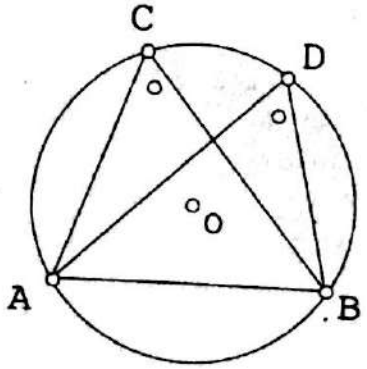


Fig.3.9

Theorem 10 The opposite angles of a quadrilateral inscribed in a circle are supplementary. Conversely, if the opposite angles of a quadrilateral are supplementary, the quadrilateral is cyclic (See Fig. 3.10).

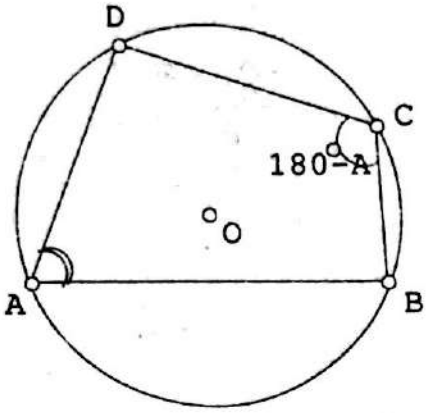


Fig. 3.10

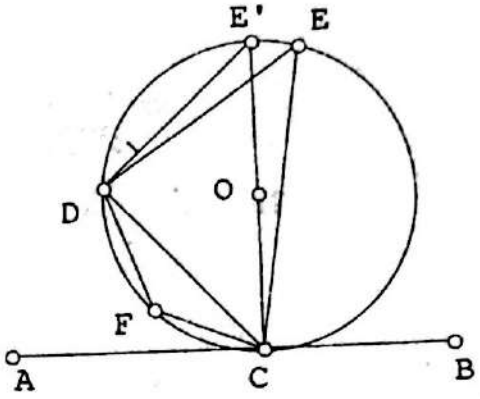


Fig. 3.11

Theorem 11 If as in Fig. 3.11, line AB touches a circle at point C, then for any chord CD through C we have $\angle ACD = \angle CED$ and $\angle BCD = \angle CFD$.

Theorem 12 If (see Fig. 3.12) AA' and BB' are chords of a circle through a point P inside the circle, then $PA \cdot PA' = PB \cdot PB'$.

Proof. Note that the result follows by observing that $\triangle PAB \sim \triangle PB'A'$.

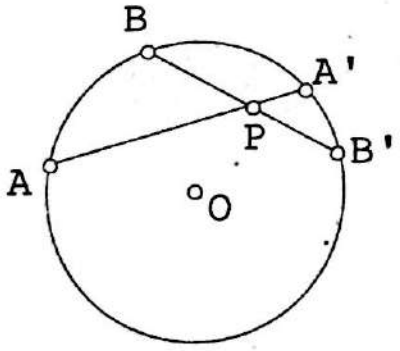


Fig. 3.12

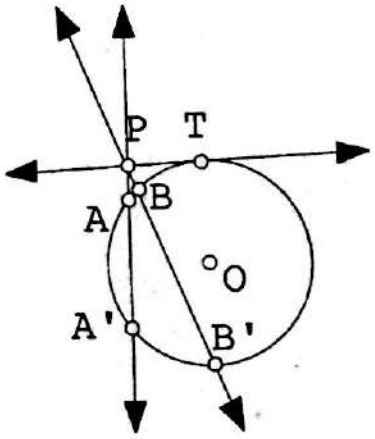


Fig 3.13

Theorem 13 If (see Fig. 3.13) P is a point outside a circle and a tangent from P to the circle touches it at T and secants through P cut it at A, A' and B, B', then

$$PA \cdot PA' = PB \cdot PB' = PT^2.$$

Problem 3 If straight line OT touches a circle at T, and OAB is a ray cutting it at A and B, and the bisector of angle BOT meets TA, TB at X, Y, find out what you can about X and Y and prove it.

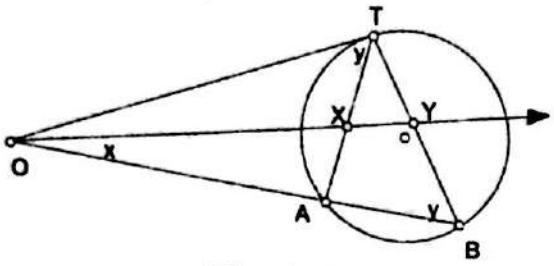


Fig. 3.14

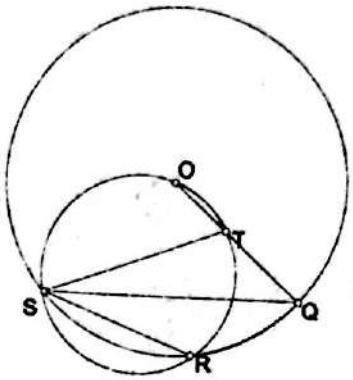


Fig. 3.15

Problem 4 O is the centre of a circle QRS and T is a point within the circle. A second circle passes through O and T and intersects the first circle at R and S, R being the nearer to T. OT is produced to meet the first circle at Q and TS, QS and RS are joined. Prove that $\angle QSR = \angle QST$.

3.2 Concurrency and collinearity

Theorem 14 (Ceva) If points D, E, F are taken on the sides BC, CA, AB of $\triangle ABC$ so that the lines AD, BE, CF are concurrent at a point O, then

$$\frac{BD}{DC} \cdot \frac{CE}{EA} \cdot \frac{AF}{FB} = 1. \tag{1}$$

Proof. There are two possible cases depending on whether O lies inside or outside $\triangle ABC$. First note that in Fig. 3.16 (i), *all* the ratios BD/DC etc. are positive, while in Fig. 3.16 (ii) *exactly* two are negative and so the product in (1) is *positive* in *all* cases. Hence we now ignore the signs of the segments and prove that the numerical value of the product in (1) is 1.

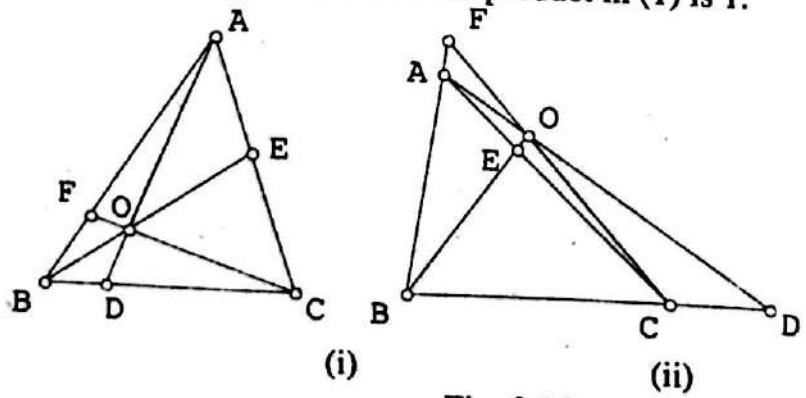


Fig. 3.16

In Fig. 3.16, since the triangles ABD, ADC have the same altitude and also the triangles OBD, ODC have the same altitude, by theorem 4 we get

$$\frac{BD}{DC} = \frac{\triangle ABD}{\triangle ADC} = \frac{\triangle OBD}{\triangle ODC} = \frac{\triangle ABD - \triangle OBD}{\triangle ADC - \triangle ODC} = \frac{\triangle ABO}{\triangle CAO}.$$

Similarly,

$$\frac{CE}{EA} = \frac{\triangle BCO}{\triangle ABO}, \quad \frac{AF}{FB} = \frac{\triangle CAO}{\triangle BCO}.$$

Multiplying these three equations we get (1).

Example 3 D, E, F are points on the sides BC, CA, AB respectively, of $\triangle ABC$ such that AD, BE, CF are concurrent at O. Show that

(i) $\dfrac{OD}{AD} + \dfrac{OE}{BE} + \dfrac{OF}{CF} = 1.$ (ii) $\dfrac{AO}{AD} + \dfrac{BO}{BE} + \dfrac{CO}{CF} = 2$

(iii) $\dfrac{AO}{OD} = \dfrac{AF}{FB} + \dfrac{AE}{EC}.$

Solution. (i) We have, as in the above,

$$\frac{OD}{AD} = \frac{\triangle OBD}{\triangle ABD} = \frac{\triangle ODC}{\triangle ADC} = \frac{\triangle OBD + \triangle ODC}{\triangle ABD + \triangle ADC} = \frac{\triangle OBC}{\triangle ABC},$$

etc. Hence

$$\frac{OD}{AD} + \frac{OE}{BE} + \frac{OF}{CF} = \frac{\triangle OBC}{\triangle ABC} + \frac{\triangle OCA}{\triangle ABC} + \frac{\triangle OAB}{\triangle ABC} = \frac{\triangle ABC}{\triangle ABC} = 1.$$

(ii) Use the relations $\dfrac{AO}{AD} = \dfrac{AD - OD}{AD} = 1 - \dfrac{OD}{AD}$, etc. and (i).

(iii) We have

$$\begin{aligned} \frac{AO}{OD} &= \frac{\triangle AOB}{\triangle BOD} = \frac{\triangle AOC}{\triangle COD} = \frac{\triangle AOB + \triangle AOC}{\triangle BOD + \triangle COD} \\ &= \frac{\triangle AOB + \triangle AOC}{\triangle BOC} = \frac{\triangle AOB}{\triangle BOC} + \frac{\triangle AOC}{\triangle BOC} = \frac{AE}{EC} + \frac{AF}{FB}. \end{aligned}$$

Theorem 15 (Converse of Ceva's theorem.) If three points D, E, F taken on the sides BC, CA, AB of $\triangle ABC$ are such that equation (1) holds, then AD, BE, CF are concurrent.

Proof. Suppose AD and BE meet in O and CO meets AB in F'. Then since AD, BE, CF' are concurrent, we get by Ceva's theorem,

$\frac{BD}{DC} \cdot \frac{CE}{EA} \cdot \frac{AF'}{F'B} = 1$. Hence by (1) we get $\frac{AF}{FB} = \frac{AF'}{F'B}$.

Hence $\frac{AF}{AF+FB} = \frac{AF'}{AF'+F'B}$ or $\frac{AF}{AB} = \frac{AF'}{AB}$.

Thus $AF = AF'$ and so the points F and F' coincide. Hence CF also passes through O.

Trigonometric form of Ceva's Theoem: Let points D, E, F be taken on the sides BC, CA, AB of $\triangle ABC$. Then the lines AD, BE, CF are concurrent if and only if

$$\frac{\sin \angle BAD}{\sin \angle DAC} \cdot \frac{\sin \angle CBE}{\sin \angle EBA} \cdot \frac{\sin \angle ACF}{\sin \angle FCB} = 1.$$

Corollary 1. The medians of a triangle are concurrent.

[For in this case, (Fig. 3.20(i)), $BD/DC = 1$ etc. and so (1) holds.]

Corollary 2. The altitudes of a triangle are concurrent.

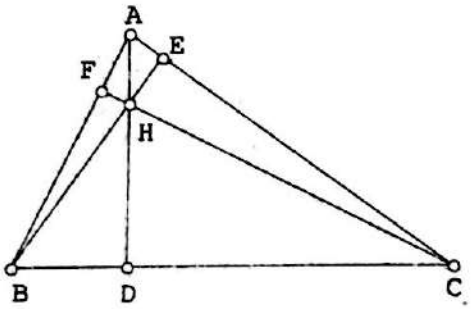


Fig. 3.17

[For acute-angled triangle ABC, (Fig. 3.17) $BE \perp CA$ and $CF \perp AB$ and so $\triangle AEB \sim \triangle AFC$ as $\angle A$ is common to them. Hence $\frac{AE}{AF} = \frac{AB}{AC}$. Similarly, if $AD \perp BC$, then $\frac{BF}{BD} = \frac{BC}{BA}$ and $\frac{CD}{CE} = \frac{CA}{CB}$. So

$$\frac{BD}{DC} \cdot \frac{CE}{EA} \cdot \frac{AF}{FB} = \frac{AB}{BC} \cdot \frac{BC}{CA} \cdot \frac{CA}{AB} = 1,$$

and so (1) holds. A similar proof holds for obtuse-angled triangles.]

Corollary 3. The internal bisectors of the angles of a triangle are concurrent.

[For in this case, (Fig. 3.7) $\frac{BD}{DC} = \frac{AB}{AC} = \frac{c}{b}$, etc. where a, b, c respectively denote the lengths of the sides BC, CA, AB of $\triangle ABC$. Hence

$$\frac{BD}{DC}\cdot\frac{CE}{EA}\cdot\frac{AF}{FB}=\frac{c}{b}\cdot\frac{a}{c}\cdot\frac{b}{a}=1,$$ and so (1) holds.]

Corollary 4. The external bisectors of any two angles of a triangle and the internal bisector of the third angle are concurrent.

[For in this case, (Fig. 3.7)

$$\frac{BD}{DC}=\frac{c}{b},\ \frac{CE}{EA}=\frac{-a}{c},\ \frac{AF}{FB}=\frac{-b}{a},$$ and so (1) holds.]

Corollary 5. If the incircle of $\triangle ABC$ touches BC, CA, AB at X, Y, Z respectively, then AX, BY, CZ are concurrent (the point of concurrence is called the *Gergonne point* of $\triangle ABC$.)

[For in this case, (Fig. 3.18 (i)) $BX = BZ$, etc. and so

$$\frac{BX}{XC}\cdot\frac{CY}{YA}\cdot\frac{AZ}{ZB}=\frac{BX}{CY}\cdot\frac{CY}{AZ}\cdot\frac{AZ}{BX}=1,$$ and so (1) holds.]

Corollary 6. If the excircles of $\triangle ABC$, opposite the vertices A, B, C touch BC, CA, AB at X_1, Y_2, Z_3 respectively, then AX_1. BY_2, CZ_3 are concurrent (the point of concurrence is called the *Nagel point* of $\triangle ABC$.)

Proof. Let the excircle opposite A touch CA at Y_1 and AB at Z_1. Then, (Fig. 3.18 (ii)) $BX_1 = BZ_1$, $CX_1 = CY_1$, $AZ_1 = AY_1$. Hence $AB + BX_1 = AB+BZ_1 = AZ_1$ and $AC+CX_1 = AC+CY_1 = AY_1$. Thus $AB+BX_1 = AC+CX_1 = 1/2(AB+BX_1+X_1C+CA) = 1/2(AB+BC+CA)$. Hence X_1 *bisects* the perimeter of $\triangle ABC$. Similarly, Y_2, Z_3 bisect the perimeter. Hence by Example 9 below, AX_1, BY_2, CZ_3 are concurrent.

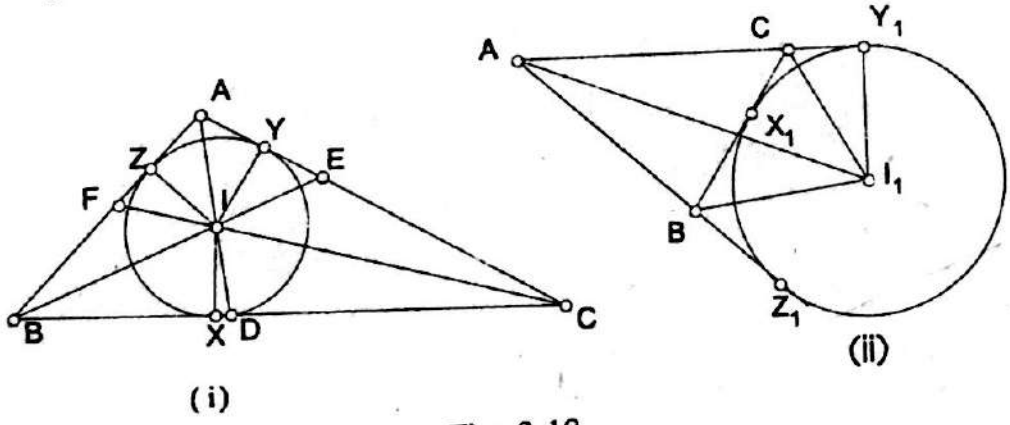


Fig. 3.18

Note: With regard to the Gergonne point it is interesting to note the following more general result called Problem of Joseph Diez Gergonne: If through the vertices of a $\triangle ABC$, two lines AP, BQ of arbitrary length are drawn in the direction of C, AP parallel to BC, BQ parallel to AC, and if lines PD and

QD are drawn respectively parallel to BQ and AP, meeting in D, then the lines AQ, BP, and CD are concurrent.

To prove this, let AQ cut BC in X, BP cut AC in Y, and let AQ, BP intersect at W as in Fig. 3.19. Let DC meet AB in Z. Then since $\triangle QXB \sim \triangle AXC$ and $\triangle BYC \sim \triangle PYA$, we get

$$\frac{BX}{XC} = \frac{QB}{CA} \text{ and } \frac{CY}{YA} = \frac{BC}{AP}. \tag{2}$$

Let DP, BA meet in E and let DQ, AB meet in F. Then, since triangles EAP and BFQ are both similar to $\triangle ABC$, we have

$$\frac{EA}{AB} = \frac{AP}{BC} = \frac{PE}{CA} = \lambda, \text{ and } \frac{BF}{AB} = \frac{FQ}{BC} = \frac{QB}{CA} = \mu. \tag{3}$$

Hence $\dfrac{EA}{BF} = \dfrac{\lambda}{\mu}$. Next, since $\triangle AZC \sim \triangle EZD$ and $\triangle ZBC \sim \triangle ZFD$, we get

$$\frac{AZ}{EZ} = \frac{ZC}{ZD}, \quad \frac{ZB}{ZF} = \frac{ZC}{ZD}.$$

Hence

$$\frac{AZ}{ZB} = \frac{EZ}{ZF} = \frac{EZ - AZ}{ZF - ZB} = \frac{EA}{BF} = \frac{\lambda}{\mu}. \tag{4}$$

Hence by (4), (3) and (2),

$$\frac{AZ}{ZB} \cdot \frac{BX}{XC} \cdot \frac{CY}{YA} = \frac{\lambda}{\mu} \cdot \mu \cdot \frac{1}{\lambda} = 1.$$

Hence by Ceva's theorem, the lines AQ, BP, and CD are concurrent.

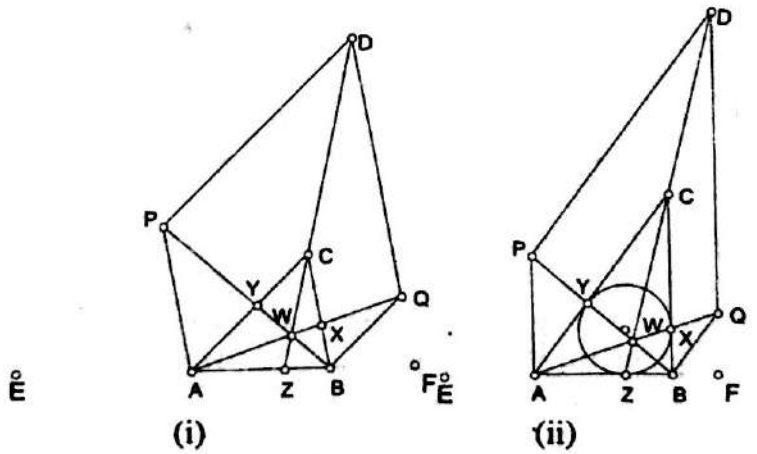


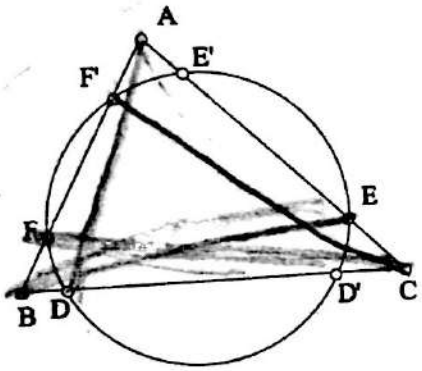
Fig. 3.19

If we take $AP = BQ = AB$, then

$$\frac{AZ}{ZB} = \frac{\lambda}{\mu} = \frac{AP}{BC}/\frac{QB}{CA} = \frac{CA}{CB}, \text{ and } \frac{BX}{XC} = \frac{QB}{AC} = \frac{AB}{AC},$$

so that W is the *incentre* of $\triangle ABC$. If we take $AP = BC$ and $BQ = AC$, it is easy to see that W is the *centroid* of $\triangle ABC$. Finally, if P is taken as the point at which BY cuts the parallel through A, and Q the point at which AX cuts the parallel through B, where X and Y are the points of contact of the incircle, then W is the Gergonne point of $\triangle ABC$.[1]

Example 4 A circle cuts the sides of $\triangle ABC$ internally as follows: BC at D, D'; CA at E, E' and AB at F', F. If AD, BE, CF are concurrent, prove that AD', BE', CF' are concurrent.



Solution. Let AD, BE, CF be concurrent, so that by Ceva's theorem, we have $\frac{BD}{FB} \cdot \frac{CE}{DC} \cdot \frac{AF}{EA} = 1$.

By theorem 12, using signed segments we have

$$BD \cdot BD' = BF \cdot BF',$$
$$CE \cdot CE' = CD' \cdot CD$$
$$\text{and } AE' \cdot AE = AF \cdot AF'.$$

$$\text{Hence } \frac{BD}{FB} = \frac{F'B}{BD'}, \frac{CE}{DC} = \frac{D'C}{CE'}, \frac{AF}{EA} = \frac{E'A}{AF'}.$$

$$\text{Thus, } \frac{F'B}{BD'} \cdot \frac{D'C}{CE'} \cdot \frac{E'A}{AF'} = \frac{BD}{FB} \cdot \frac{CE}{DC} \cdot \frac{AF}{EA} = 1.$$

Hence by the converse of Ceva's theorem, AD', BE', CF' are concurrent.

Example 5 Let ABC be a triangle and let D, E, F be points on its sides such that, starting at A, D divides the perimeter of the triangle into two equal parts, starting at B, E divides the perimeter of the triangle into two equal parts, and starting at C, F divides the perimeter of the triangle into two equal parts. Prove that D, E, F lie on the sides BC, CA, AB respectively and the lines AD, BE, CF are concurrent.

[1] **Ref.:** Laura Guggenbuhl, *Note on the Gergonne point of a triangle*, Amer. Math. Monthly, 1957, p. 192-193.

Solution. Let $2s = a+b+c$ be the perimeter of $\triangle ABC$. Now $c < a+b$, $b < c+a$. Hence $2c < a+b+c < 2c+2a$ and so $c < s = AB+BD < c+a = AB+BC$. Therefore D lies on BC. Similarly, E lies on CA and F on AB. Next, $c+BD = s = DC+b$, $a+CE = s = EA+c$, $b+AF = s = FB+a$. Hence

$$\frac{BD}{DC}\cdot\frac{CE}{EA}\cdot\frac{AF}{FB} = \frac{s-c}{s-b}\cdot\frac{s-a}{s-c}\cdot\frac{s-b}{s-a} = 1.$$

So, by the converse of Ceva's theorem, AD, BE and CF are concurrent.

Theorem 16 (Menelaus) If a transversal cuts the sides BC, CA, AB (suitably extended) of $\triangle ABC$ in points D, E, F, respectively, then

$$\frac{BD}{DC}\cdot\frac{CE}{EA}\cdot\frac{AF}{FB} = -1. \tag{5}$$

Proof. There are two cases depending on whether the transversal cuts one side externally or all three sides externally. Note that *only one* ratio (as in Fig.3.20 (i)) or else *all the three* ratios (as in Fig.3.20 (ii)) in (5) are negative. Thus the product in (5) is *always* negative. Hence we now ignore the signs of the segments and prove that the numerical value of the product in (5) is 1.

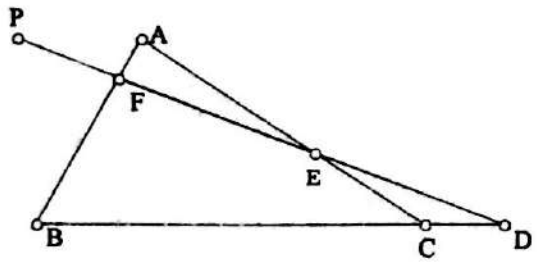


Fig. 3.20 (i)

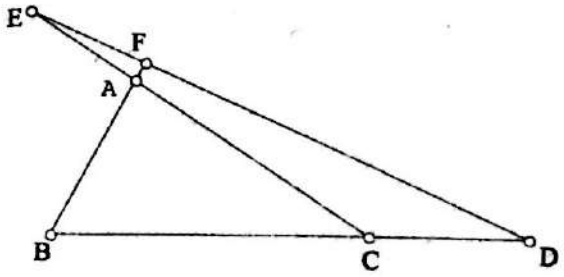


Fig. 3.20 (ii)

With the notation of Fig. 3.20 (i), draw AP parallel to DB meeting DF in P. Then, since $\triangle APF \sim \triangle BDF$, $\frac{AF}{FB} = \frac{PA}{BD}$ and since $\triangle CDE \sim \triangle APE$, $\frac{DC}{AP} = \frac{CE}{EA}$. Hence

$$\frac{BD}{DC}\cdot\frac{CE}{EA}\cdot\frac{AF}{FB} = \frac{BD}{DC}\cdot\frac{DC}{AP}\cdot\frac{PA}{BD} = 1, \quad \text{numerically.}$$

Note: We can deduce Ceva's theorem from Menelaus' theorem as follows: See Fig. 3.16. Apply Menelaus' theorem to $\triangle ABD$, and to $\triangle ADC$ with line CF as transversal. This gives

$$\frac{BC}{CD}\cdot\frac{DO}{OA}\cdot\frac{AF}{FB} = -1 \text{ and } \frac{CE}{EA}\cdot\frac{AO}{OD}\cdot\frac{DB}{BC} = -1.$$

Multiplying these equations we get Ceva's theorem.

Conversely, we can deduce Menelaus' theorem from Ceva's theorem as follows: As shown in Fig. 3.21, let a transversal cut the sides BC, CA, AB of $\triangle ABC$ in points D, E, F respectively. Let CF meet BE in P and AD in Q, and let AD and BE meet in R. Apply Ceva's theorem to each of the six triangles in Fig. 3.21 as follows:

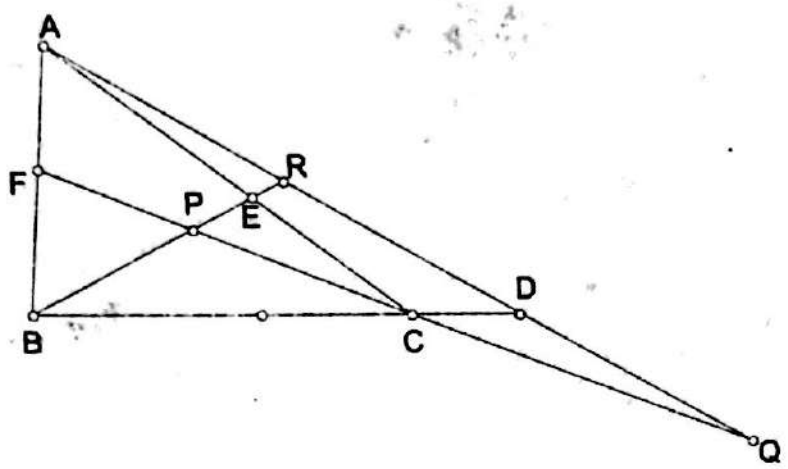


Fig. 3.21

For $\triangle DAB$ lines DF, AC, BR are concurrent at E and so

$$\frac{BC}{CD} \cdot \frac{DR}{RA} \cdot \frac{AF}{FB} = 1.$$

For $\triangle EBC$ lines ED, BA, CP are concurrent at F and so

$$\frac{BD}{DC} \cdot \frac{CA}{AE} \cdot \frac{EP}{PB} = 1.$$

For $\triangle FCA$ lines FE, CB, AQ are concurrent at D and so

$$\frac{CE}{EA} \cdot \frac{AB}{BF} \cdot \frac{FQ}{QC} = 1.$$

For $\triangle DEA$ lines DC, ER, AF are concurrent at B and so

$$\frac{AR}{RD} \cdot \frac{DF}{FE} \cdot \frac{EC}{CA} = 1.$$

For $\triangle EFB$ lines EF, FP, BD are concurrent at C and so

$$\frac{FA}{AB} \cdot \frac{BP}{PE} \cdot \frac{ED}{DF} = 1.$$

For $\triangle FDC$ lines FB, DQ, CE are concurrent at A and so

$$\frac{DB}{BC} \cdot \frac{CQ}{QF} \cdot \frac{FE}{ED} = 1.$$

By multiplying the last six equations we get

$$\left(\frac{BD}{DC} \cdot \frac{CE}{EA} \cdot \frac{AF}{FB}\right)^2 = 1.$$

From this Menelaus' theorem follows because the transversal cuts either one side externally or three sides externally.

Theorem 17 (Converse of Menelaus' Theorem.) If points D, E, F are taken on the sides of $\triangle ABC$ such that equation (5) holds, then D, E, F are collinear.

Proof. Let DE meet AB in F'. Then by Menelaus' theorem, we get

$\frac{BD}{DC} \cdot \frac{CE}{EA} \cdot \frac{AF'}{F'B} = -1$. Hence by (5) we get $\frac{AF}{FB} = \frac{AF'}{F'B}$ and so $F = F'$.

Hence F lies on DE, as required.

Corollary. The external bisectors of the three angles of a scalene triangle meet their respective opposite sides at three collinear points. (A triangle is called *scalene* if no two of its sides are equal.)

Example 6 The incircle of $\triangle ABC$ has centre I and touches the side BC at D. Let the midpoints of AD and BC be M and N respectively. Prove that M, I, N are collinear.

Solution. Let NI meet AD at M'. Join A and I and let AI meet BC at L. For $\triangle ADL$, with NIM' as transversal, Menelaus' theorem gives

$$\frac{DN}{NL} \times \frac{LI}{IA} \times \frac{AM'}{M'D} = -1 \qquad (6)$$

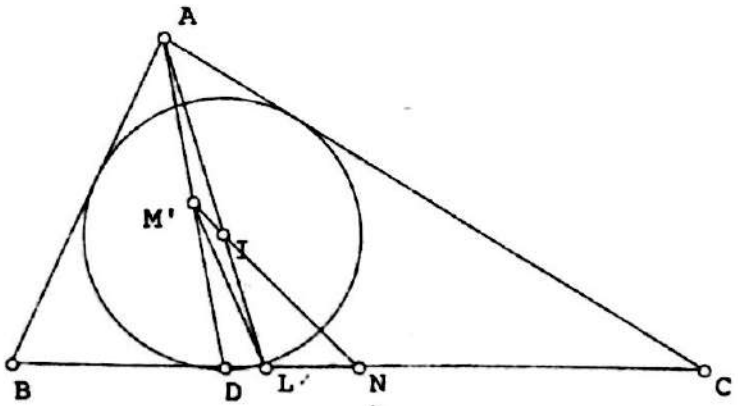


Fig. 3.22

$$\text{Now} \quad \frac{LI}{IA} = \frac{LC}{CA} = \frac{ab}{(b+c)b} = \frac{a}{b+c} \tag{7}$$

$$\text{and} \quad \frac{DN}{LN} = \frac{BN - BD}{BN - BL} = \frac{\frac{a}{2} - (s-b)}{\frac{a}{2} - \frac{ac}{b+c}} = \frac{b+c}{a} \tag{8}$$

Substituting (7) and (8) in (6), we get $\frac{AM'}{M'D} = 1$. Hence, M' coincides with M.

Exercise Set- 3.1

1. A transversal cuts the sides AB, BC, CD, DA of a quadrilateral $ABCD$ at P, Q, R, S respectively. Prove that

$$\frac{AP}{PB} \cdot \frac{BQ}{QC} \cdot \frac{CR}{RD} \cdot \frac{DS}{SA} = +1.$$

2. Points X, Y are taken on the sides CA, AB of $\triangle ABC$. If BX, CY meet at P and

$$\frac{AX}{XC} = \frac{BY}{YA} = \frac{1}{2},$$

find the value of the ratio BP/PX. [Ans. $BP/PX = 3/4$.]

3. In $\triangle ABC, BC = 2CA$; the internal bisector of angle C meets AB at X and AA' is a median. If $A'X$ meets CA produced at Z, prove that A is the midpoint of CZ. If also AA', CX intersect at O and BO cuts CA at Y, prove that Y is a point of trisection of CA.

4. Points E, F on the sides CA, AB of $\triangle ABC$ are such that FE is parallel to BC; BE, CF intersect at X. Prove that AX is a median of $\triangle ABC$.

5. The external bisector of angle A of $\triangle ABC$ meets BC produced at L, and the internal bisector of angle B meets CA at M. If LM meets AB at R, prove that CR bisects the angle C.

6. AD, BE, CF are concurrent lines drawn from the vertices of $\triangle ABC$ to points D, E, F on the opposite sides. If AD is the altitude of $\triangle ABC$, show that AD bisects $\angle FDE$.

3.3 Pythagoras Theorem

Theorem 18 (Pythagoras.) In any right-angled triangle, the square on the hypotenuse is equal to the sum of the squares on the other sides.

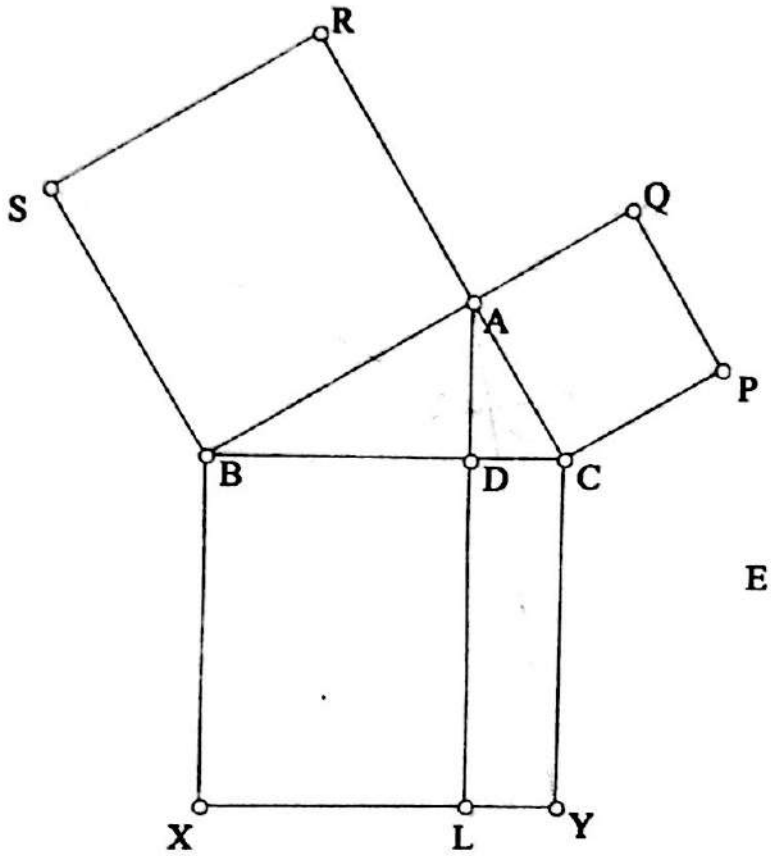


Figure 3.23

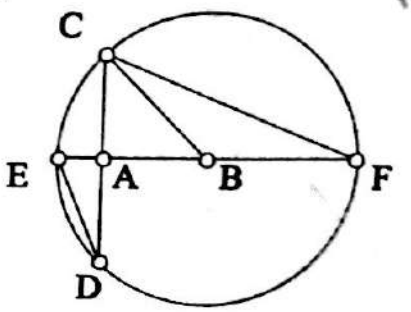


Fig. 3.24

Proof. Let ABC be a triangle having $\angle A = 90°$. Construct squares $BXYC$ on BC, $CPQA$ on CA and $ARSB$ on AB as shown in Fig. 3.23. Draw $AL \parallel BX$ meeting XY in L. Join AY, BP.

Then, since $\angle BAC = \angle CAQ = 90°$, BAQ is a straight line. For similar reason, CAR is a straight line. In triangles ACY and PCB, $CA = CP$, $CY = CB$ and $\angle ACY = \angle PCB$ because each $= \angle ACB + 90°$. Hence triangles ACY and PCB are congruent. Now parallelogram $CDLY$ and $\triangle ACY$ are on common base CY and are between the parallel lines CY and AL and so

$$\text{area } CDLY = 2 \cdot \text{area } \triangle ACY.$$

Similarly,

$$\text{area of sq. } CPQA = 2 \cdot \text{area } \triangle PCB.$$

Hence,

$$\text{area } CDLY = \text{area of sq. } CPQA.$$

Similarly, by joining SC and AX, it can be seen that

$$\text{area } BXLD = \text{area of sq. } BARS.$$

Hence, adding the expressions for area $CDLY$ and area $BXLD$, we get

$$\text{area of sq. } BXYC = \text{area of sq. } CPQA + \text{area of sq. } ARSB,$$

as was to be proved.

Another Proof. Let ABC be a triangle having $\angle A = 90°$. Construct a circle with B as centre and a as radius. Let AC intersect the circle at D and AB intersect the circle at E and F as shown in the fig 3.24. By theorem 12, we have $CA \cdot AD = EA \cdot AF$. Hence, $b^2 = (a - c)(a + c) = a^2 - c^2$ i.e. $a^2 = b^2 + c^2$ as was to be proved.

Exercise Set- 3.2

1. In Fig. 3.23 show that
   (a) $AB^2 = BD \cdot BC$, $AD^2 = BD \cdot DC$, $AD \cdot BC = CA \cdot AB$
   (b) $\frac{1}{AD^2} = \frac{1}{AB^2} + \frac{1}{AC^2}$, $AY \perp BP$.
   (c) Triangles SBX, PCY, RAQ and ABC have the same area.
   (d) AL, SC, and BP are concurrent and S, A, P are collinear.
2. (a) In $\triangle ABC$, $\angle C$ is obtuse and AD is perpendicular to BC produced. Prove that $AB^2 = BC^2 + CA^2 + 2BC \cdot CD$.
   (b) In $\triangle ABC$, $\angle C$ is acute and AD is perpendicular to BC. Prove that $AB^2 = BC^2 + CA^2 - 2BC \cdot CD$.

   This is a form of Cosine Rule.
3. If point D divides the base BC of $\triangle ABC$ in the ratio $BD/DC = n/m$, then show that

   $$m \cdot AB^2 + n \cdot AC^2 = m \cdot BD^2 + n \cdot CD^2 + (m + n) \cdot AD^2.$$

   This is called as Stewart's theorem .

   [Draw $AX \perp BC$. Then applying Ex. 2 to $\triangle ABD$ we get

   $$AB^2 = BD^2 + AD^2 \pm 2BD \cdot DX$$

   and applying Ex. 2 to $\triangle ADC$ we get

   $$AC^2 = AD^2 + DC^2 \mp 2DC \cdot DX.$$

   Multiply these equations by m and n respectively and add.]

4. Let in $\triangle ABC$, D be the midpoint of BC. Prove that

$$AB^2 + AC^2 = 2AD^2 + 2DC^2.$$

This is called Apollonius' Theorem.

5. In $\triangle ABC$, AD is perpendicular to BC. Prove that for any point P on AD,

$$BP^2 - PC^2 = BD^2 - DC^2 \qquad (1)$$

and conversely, if P satisfies (1), then P lies on AD. Hence prove that the altitudes of a triangle are concurrent.

6. On the sides of $\triangle ABC$, equilateral triangles APB, BQC, CRA are drawn outwards . Show that $AQ = BR = CP$. Further, if $\angle BAC = 90°$, show that the area of the triangle on the hypotenuse is equal to the sum of the areas of the other two triangles.

7. ABC is any triangle; any parallelograms $BADE$, $BCFG$ are placed on BA, BC; DE, FG produced meet in H. Show that the sum of the areas of parallelograms $BADE$ and $BCFG$ is equal to the area of the parallelogram $ACIJ$ having sides CI, AJ equal to and parallel to BH. (Pappus' extension of Pythagoras' theorem.)

3.4 Properties of triangles

Centroid. Let ABC be a triangle and A', B', C' be the mid-points of the sides BC, CA, AB. The medians AA', BB', CC' are concurrent and the point of concurrence G is called the *centroid* of the triangle. G trisects every median, the larger segment being toward the vertex. Thus $AG : GA' = 2 : 1$.

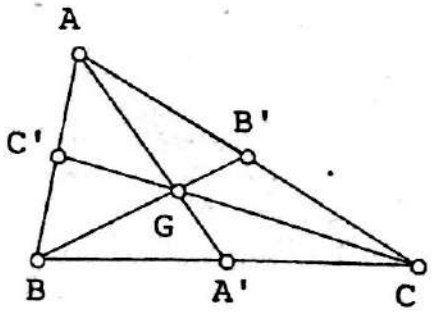


Figure 3.25

The concurrence of the medians has been proved in Corollary 1 of the converse of Ceva's theorem. Now, as in Fig. 3.25, for $\triangle ABA'$ with transversal CGC', we get by Menelaus' theorem that

$$\frac{BC}{CA'} \cdot \frac{A'G}{GA} \cdot \frac{AC'}{C'B} = -1.$$

Moreover, $BC = -2CA'$ and $AC' = C'B$, and so we get $AG = 2GA'$ as stated.

Example 7 A line from vertex C of $\triangle ABC$ bisects the median from A. Prove that it divides the side AB in the ration 1 : 2.

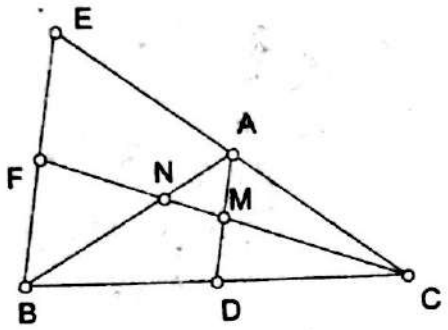


Figure 3.26

Solution. Through B draw a line parallel to the median AD meeting CA extended in E. Let M be the midpoint of AD and let CM extended meet BE in F and AB in N. Then as in $\triangle CBE, DA$ is drawn through mid point D of CB parallel to base BE, it follows that A is mid point of CE. Hence F is the mid point of BE as $BF = 2DM = 2MA = FE$. Hence AB and CF are medians of $\triangle CBE$ and so they divide each other in the ratio 1:2, i.e., $BN = 2NA$.

Equivalntly, one may apply Menelaus' theorem to $\triangle ABA'$ with line CMN as transversal.

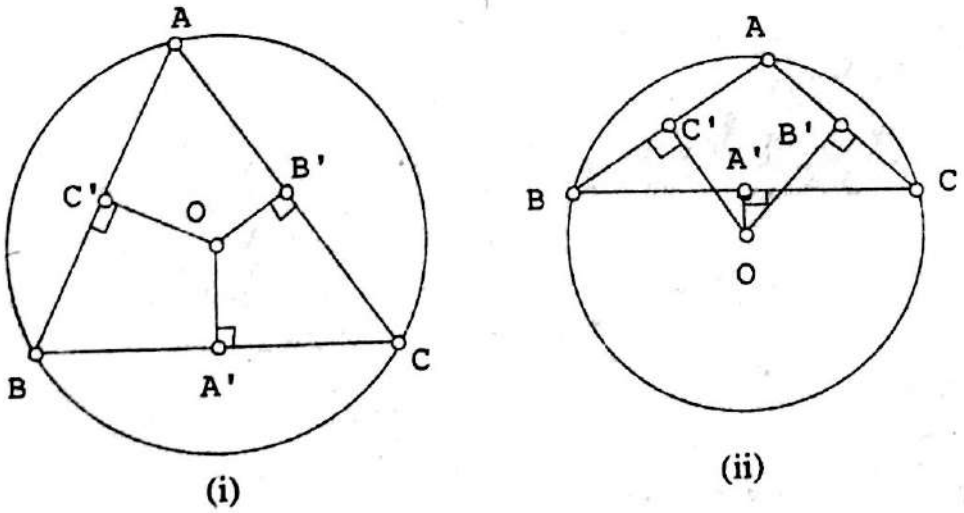


Figure 3.27

Circumcentre. In $\triangle ABC$, the perpendicular bisectors of the sides are concurrent and the point of concurrence O is equidistant from the vertices. Let R

be the common distance. The circle with centre O and radius $OA = R$, passes through the vertices A, B, C and is called the *circumcircle* of the triangle and O is called the *circumcentre* of the triangle. See Fig. 3.27.

For an obtuse-angled triangle, the circumcentre is *outside* the triangle: see Fig. 3.27(ii). Clearly, $\angle BOA' = \angle A'OC = \angle A$ etc.

Orthocentre. The altitudes AD, BE, CF of $\triangle ABC$ are concurrent and the point of concurrence H is called the *orthocentre* of $\triangle ABC$. The triangle DEF formed by the feet of the altitudes is called the *pedal triangle* of $\triangle ABC$. See Fig. 3.28(i).

For an obtuse-angled triangle, the orthocentre is *outside* the triangle: see Fig. 3.28(ii).

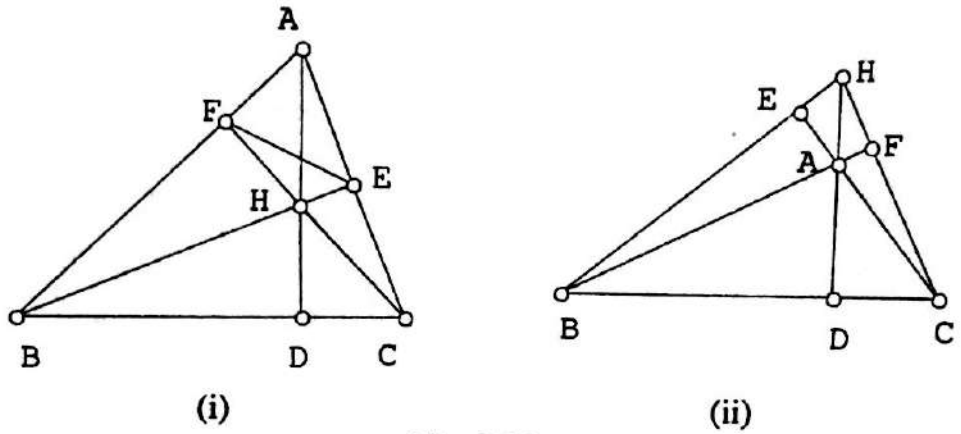


Fig. 3.28

When $\triangle ABC$ is an acute-angled triangle, as in Fig. 3.28(i), we have the following results.

(i) As $BCEF$ is a cyclic quadrilateral, $\angle AFE = C$, $\angle AEF = B$. Similarly, $\angle BDF = A$, etc.

(ii) Since $\angle ADF = 90° - \angle BDF = 90° - A$ and $\angle ADE = 90° - \angle CDE = 90° - A$, we see that AD bisects $\angle EDF$ and $\angle EDF = 180° - 2A$. Similarly, BE, CF bisect angles DEF and DFE. Thus, H is the incentre of the pedal triangle DEF. When $\angle A$ is obtuse, as in Fig. 3.21(ii), we have $\angle ADE = A - 90°$ and H is the excentre of the pedal triangle DEF opposite to vertex D.

Theorem 19 If H is the orthocentre of $\triangle ABC$ and AP is a circumdiameter, then PH and BC bisect each other. If $OA' \perp BC$, where O is the circumcentre of $\triangle ABC$, then $AH = 2OA'$.

Proof. As in Fig. 3.29, $BE \perp AC$ and $PC \perp AC$. Hence $BH \parallel PC$. Similarly, $BP \parallel HC$. Thus $BPCH$ is a parallelogram and so its diagonals BC and PH bisect each other at A'. Next, A' is the midpoint of PH. Hence from $\triangle APH$, we get $AH = 2OA'$.

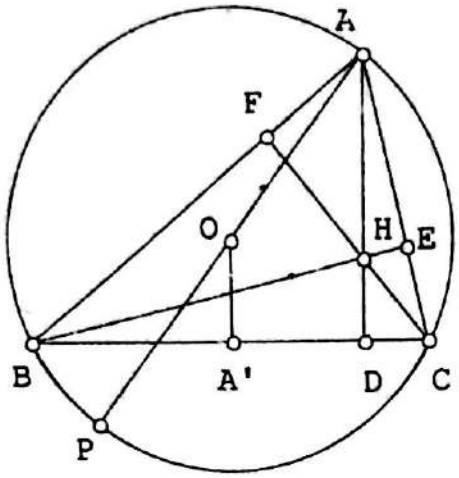


Fig. 3.29

Theorem 20 (Euler line) The circumcentre O, the centroid G and the orthocentre H of a non-equilateral triangle are collinear and $GH = 2 \cdot OG$. Also OG is called the Euler line of the triangle.

Proof. See Fig. 3.30. Let AA' cut OH in G'. Since $\angle AG'H = \angle A'G'O$ and $\angle AH'G' = \angle A'OG'$, triangles HAG' and $OA'G'$ are similar. Hence

$$\frac{AG'}{G'A'} = \frac{HG'}{G'O} = \frac{AH}{OA'}.$$

But $AH/OA' = 2$ by the last theorem. Hence $AG'/G'A' = 2$, so that G' is the same as the centroid G. Thus O, G, H are collinear. Further, $GH/OG = 2$, as required.

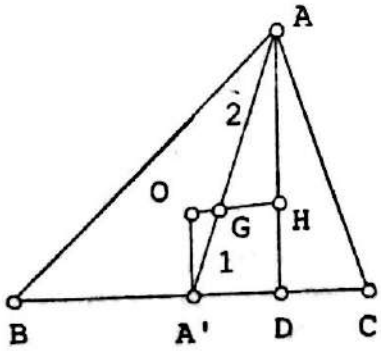


Fig. 3.30

Theorem 21 If H is the orthocentre of $\triangle ABC$ and AH produced meets BC at D and the circumcircle of $\triangle ABC$ at P, then $HD = DP$. (Fig. 3.31)

Proof. Since $\angle PBC = \angle PAC$ (same segment) and $\angle DBE = \angle 90° - \angle C = \angle PAC$, we see that $\angle PBD = \angle DBH$. Since $\angle BDH = \angle BDP = 90°$ and BD is a common side, the triangles PBD and DBH are congruent. Hence $HD = DP$.

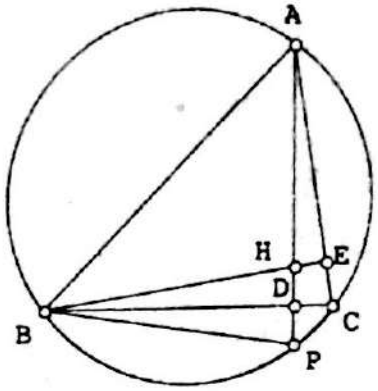


Fig. 3.31

Incentre. The internal bisectors of the angles of $\triangle ABC$ are concurrent and the point of concurrence I is equidistant from the sides. Let r be the common distance. See Fig. 3.32 (i). The circle with centre I and radius r touches the sides BC, CA, AB and is called the *inscribed circle* or the *incircle* of $\triangle ABC$. I is called the *incentre* and r is called the *inradius* of the triangle. Let $2s = a + b + c$, so that s is the semiperimeter of the triangle. Then, as shown in figure below, since tangents from a point to a circle are equal in length, we have $AZ = AY$, $BZ = BX$ and $CX = CY$. Hence

$$AZ + BX + XC = \frac{1}{2}(a + b + c) = s,$$

and so $AZ + a = s$ or $AZ = AY = s - a$. Similarly, $BZ = BX = s - b$ and $CX = CY = s - c$.

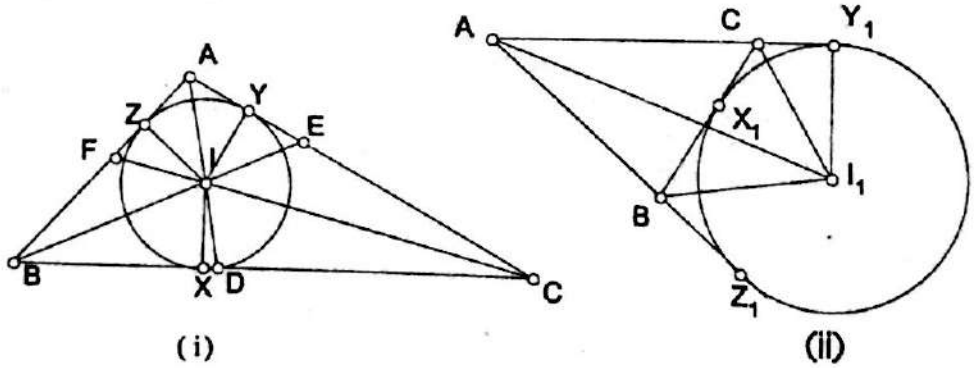


Fig. 3.32

As shown in the figure (ii) above, the internal bisector of $\angle A$ and the external bisectors of angles B and C are concurrent at I_1. I_1 is equidistant from the sides BC, CA, AB. Let r_1 be the common distance. Then the circle with centre I_1 and radius r_1 touches BC internally and CA, AB externally

at X_1, Y_1, Z_1 respectively. This circle is called the *escribed circle* opposite A and I_1 is called an *excentre* of $\triangle ABC$. Similarly, there are escribed circles with centres I_2, I_3 and radii r_2, r_3 (say) opposite B and C respectively. Again, using the equal tangents property, we get $AY_1 = AZ_1$, $BX_1 = BZ_1$ and $CY_1 = CX_1$. Hence

$$2s = \text{perimeter} = AB + BX_1 + X_1C + CA = AZ_1 + AY_1,$$

and so $AZ_1 = AY_1 = s$ and $BX_1 = AZ_1 - AB = s - c, CX = s - b$.

Also $\angle BIC = 90° + \frac{A}{2}$, etc. Further, if AD is the bisector of $\angle A$, then

$$\frac{BD}{DC} = \frac{AB}{AC} = \frac{c}{b}, \text{so that } BD = \frac{ac}{b+c}, \quad DC = \frac{ab}{b+c}.$$

Hence by Ex.3 of Exercise Set-3.2, we get

$$AD^2 = bc\left[1 - \frac{a^2}{(b+c)^2}\right].$$

Also, if Δ denotes the area of triangle ABC, then

$$\Delta = rs = r_1(s-a) = r_2(s-b) = r_3(s-c),$$

$$\text{Hence, } \frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3} = \frac{1}{r}.$$

Example 8 If A, B are two fixed points and P is a moving point such that $\frac{PA}{PB}$ is constant, then prove that the locus of P is a circle.

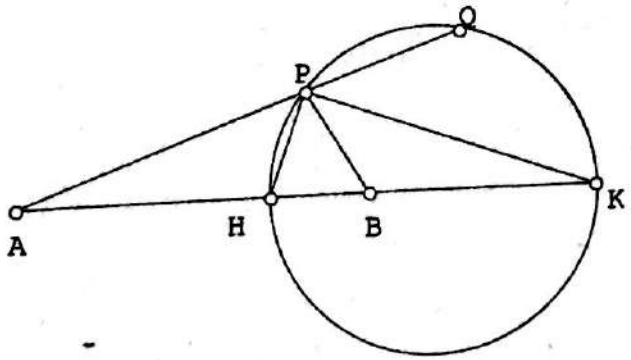


Fig. 3.33

Solution. Produce AP to Q. Let $\frac{PA}{PB} = \lambda$. Divide AB internally at H and externally at K in the ratio λ. Since $\frac{AH}{HB} = \lambda = \frac{AP}{PB} = \frac{AK}{BK}$, PH and PK are the internal and external bisectors of $\angle APB$. Hence, $\angle HPK = \frac{1}{2}[\angle APB + \angle BPQ] = 90^0$. Thus, P lies on the circle whose diameter is HK. This circle is called the circle of *Apollonius*.

Theorem 22 (Nine - point circle) The circle through the midpoints of the sides of a triangle passes through the feet of the altitudes and the midpoints of the lines joining the orthocentre to the vertices. This circle is called the nine-point circle of the triangle.

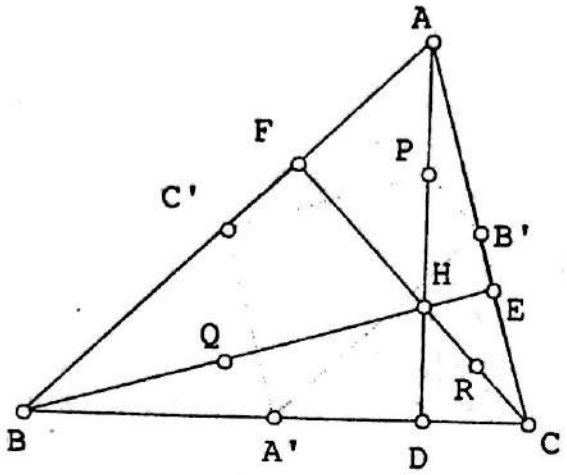


Fig. 3.34

In Figures 3.34, 3.35 and 3.36 A', B', C' are midpoints of BC, CA, AB and D, E, F are the feet of the altitudes AD, BE, CF and P, Q, R are midpoints of AH, BH, CH where H is the orthocentre of $\triangle ABC$. Let O be the circumcentre and R be the circumradius of $\triangle ABC$.

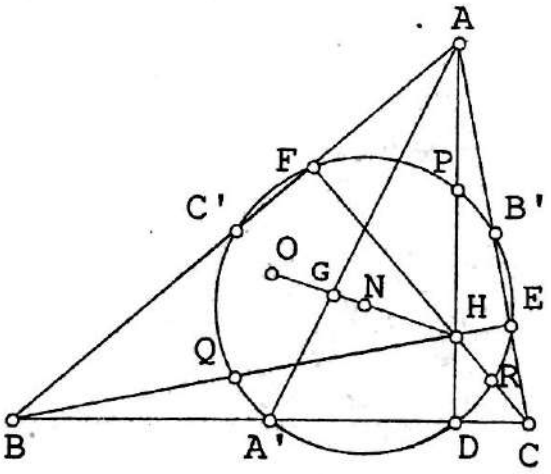


Fig. 3.35

Proof. As in Fig. 3.34, $C'P \parallel BE$, since in $\triangle ABH$, $C'P$ joins the midpoints C' and P of AB and AH respectively. Similarly, $C'A' \parallel AC$. Hence $\angle A'C'P = 90^0$, since $BE \perp AC$. Similarly, $\angle A'B'P = 90^0$. Also $\angle A'DP = 90^0$. Hence the circle having $A'P$ as a diameter, passes through B', C', D.

Hence the circle $A'B'C'$ passes through P and D, and similarly through Q, E and F, R. Also $B'Q$ and $C'R$ are diameters of the nine-point circle.

Next, as in Fig. 3.36, the perpendicular bisectors of the chords $A'D$ and $C'F$ meet in the midpoint of OH, say N. Hence N is the centre of the nine-point circle. Hence from $\triangle AOH$, $R = OA = 2NP$. This shows that the radius of the nine-point circle is half the circumradius.

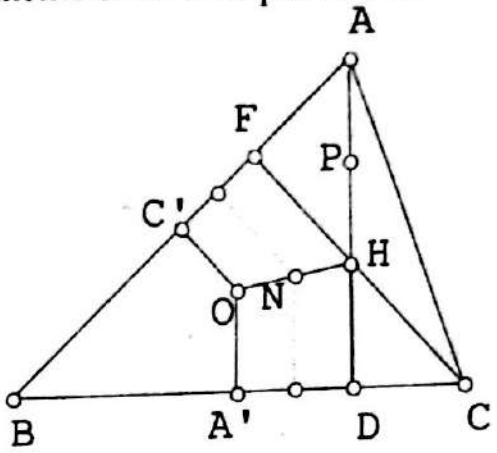


Fig. 3.36

Nine-Point Circle another proof. We note that from the proof of Euler line Theorem 20, we get that $AH = 2OA'$. As P is midpoint of AH, we get that $PH = OA'$. Join A' and P. Suppose $A'P$ intersects OH at N. Then triangles $OA'N$ and HPN are congruent to each other. Hence, N is midpoint of OH as well as of $A'P$. Further, as $\angle A'DP = 90°$, there is a circle with $A'P$ as diameter passing through D. The radius of this circle is NP. Since, P is midpoint of AH and N is midpoint of OH, we get that $PN = \frac{1}{2}OA$. Similarly, we can show that there is a circle with $B'Q$ as diameter passing through E and having center N and radius $\frac{1}{2}OB$ and a circle with $C'R$ as diameter passing through F and having center N and radius $\frac{1}{2}OC$. But, $OA = OB = OC$. Hence, the three circles are the same. Hence, the nine points are concyclic.

Yet another proof. Observe that $A'CB'C'$ is a parallelogram. Also, DB' is a median of the right angled triangle ADC and hence $DB' = \frac{1}{2}AC$. Thus, $\angle B'C'A' = \angle B'CD = \angle B'DC$. Hence, A', B', C', D are concyclic. Similarly, A', B', C', E and A', B', C', F are concyclic. Hence, A', B', C', D, E, F are concyclic. Thus, the midpoints of the sides and feet of the altitudes of a triangle lie on a circle. Applying this observation for triangle HBC, we get that A', Q, R, D, E, F are concyclic. Similarly, in triangle HAB, we get that C', P, Q, D, E, F are concyclic. Hence, A', B', C', D, E, F are concyclic.

Notes.

(i) See Fig. 3.36. Since D, E, F are the feet of the altitudes of $\triangle ABC$, it

follows that A is the orthocentre of $\triangle HBC$ and that the triangles ABC and HBC have the same nine-point circle.

(ii) In Fig. 3.35, triangles $A'B'C'$ and PQR are congruent.

(iii) As in Fig. 3.37, the excentres I_1, I_2, I_3 of $\triangle ABC$ form a triangle whose sides pass through the vertices A, B, C. Since angle-bisectors of an angle are at right angles, we see that the incentre I of $\triangle ABC$ is the orthocentre of $\triangle I_1I_2I_3$.

Also, as A, B, C are the feet of the altitudes of $\triangle I_1I_2I_3$, it follows that the circumcircle of $\triangle ABC$ is the nine-point circle of $\triangle I_1I_2I_3$. Hence the circumcircle of $\triangle ABC$ bisects the lines I_2I_3, I_3I_1, I_1I_2 and also the lines II_1, II_2 and II_3.

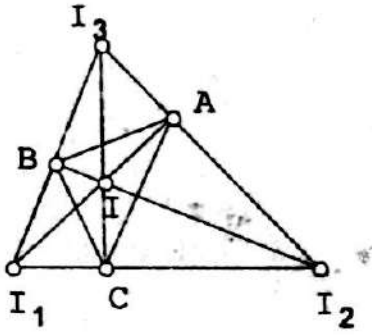


Fig. 3.37

Theorem 23 The angle between the altitude AD and the circumdiameter AL drawn from the vertex A of $\triangle ABC$ is equal to difference of angles at vertices B and C and is bisected by the angle - bisector AX of $\angle A$. Thus, the angle bisector of $\angle BAC$ is also an angle bisector of $\angle OAH$.

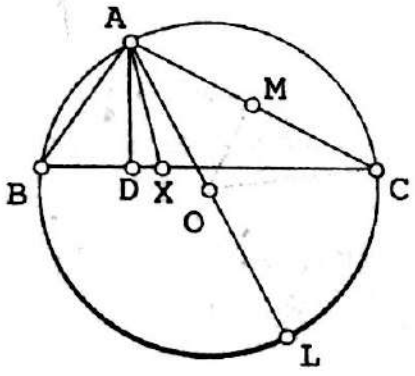


Fig. 3.38

Proof. See Fig. 3.38. Since $\angle AOC = 2B$, we get $\angle CAO = 90° - B$. Also $\angle DAB = 90° - B$. So $\angle CAO = \angle DAB$. Since $\angle XAB = \angle XAC$, we get $\angle XAD = \angle XAO$, i.e. AX bisects $\angle DAL$. Also, in Fig. 3.38,

$$\angle DAL = 2(\angle XAB - \angle DAB) = B - C.$$

Theorem 24 (Euler) In any $\triangle ABC$, $OI^2 = R^2 - 2Rr$, where O, I are the centres and R, r are the radii, respectively, of the circumcircle and incircle of $\triangle ABC$.

Proof. See Fig. 3.39. Since $\angle MBC = \angle MAC = A/2$, we get

$$\angle MBI = (A + B)/2 = \angle IBA + \angle BAI = \angle BIM.$$

Hence $BM = MI$.

Let the internal and external bisectors of $\angle A$ meet the circumcircle in M and N. Then $\angle MAN = 90^0$. Hence MN is a diameter. Now if XY is the diameter containing O and I, then $AI \cdot IM = XI \cdot IY$ and so

$$AI \cdot IM = (R+OI)(R-OI) = R^2 - OI^2.$$

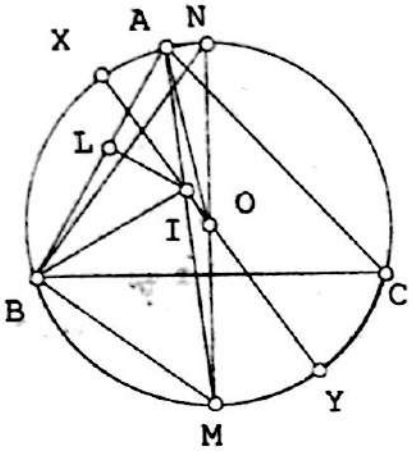


Fig. 3.39

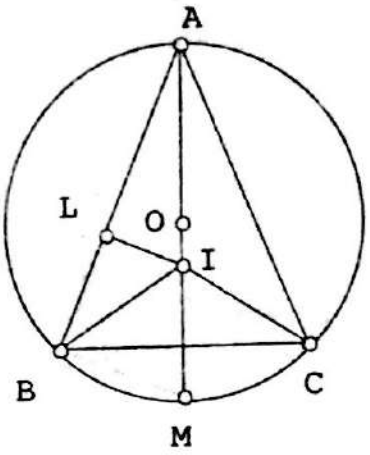


Fig. 3.40

Let $IL \perp AB$. Also, since $\angle LAI = \angle BNM$ and $\angle ALI = \angle MBN = 90^0$, we see that $\triangle ALI \sim \triangle NBM$. Hence $\frac{AI}{IL} = \frac{MN}{MB}$, and so, since $BM = IM$, we get $AI \cdot IM = MN \cdot IL = 2Rr$.

Remark. The proof of $BM = MI$ is immediate if we use the note just before theorem 23. Also, it can be proved that $OI_1^2 = R^2 + 2R \cdot r_1$. $OI_1^2 - R^2 = OI_1^2 - OP^2 = I_1P \cdot I_1A = PB \cdot I_1A = 2R \cdot r_1$.

Example 9 Consider an isosceles triangle, Let r be the radius of its circumscribed circle and p the radius of the inscribed circle. Prove that the distance d between the centres of these circles is $d = \sqrt{r(r-2p)}$.

Solution. See Fig. 3.40. Draw $IL \perp AB$ and join BM. Then, as in Theorem 24, $BM = IM = r - d$. Since $BD = \frac{a}{2}$, equating the two expressions for the area of $\triangle ABI$, we get $\frac{1}{2}cp = \frac{1}{2}AI \cdot \frac{a}{2}$, or $2cp = (r+d)a$. Similarly, $\triangle ABM$ gives $c \cdot BM = ar = c(r-d)$. Hence, eliminating a, we get $2cp = (r+d)c(r-d)/r$ or $r^2 - d^2 = 2rp$, as required.

Theorem 25 (Simson line) The feet L, M, N of the perpendiculars on the sides BC, CA, AB, of any $\triangle ABC$ from any point X on the circumcircle of

the triangle are collinear. The line LMN is called the *Simson line* or the *pedal line* of the point X with respect to $\triangle ABC$.

Proof: Let $XN \perp AB$ and $XM \perp AC$ as in Fig. 3.41. Let NM meet BC in L. Then to prove that L, M, N are collinear, it is enough to show that $XL \perp BC$. For this, join XA, XC. Then the quadrilateral $XMNA$ is cyclic because $\angle ANX = \angle AMX = 90^0$. Hence $\angle XML = \angle XAN$. Also the quadrilateral $XABC$ is clearly cyclic and so $\angle XAB = \angle XCL$. Hence $\angle XML = \angle XCL$. Therefore the quadrilateral $XMCL$ is cyclic. Also $XM \perp AC$. Hence $\angle XLC = 180^0 - \angle XMC = 90^0$, as required.

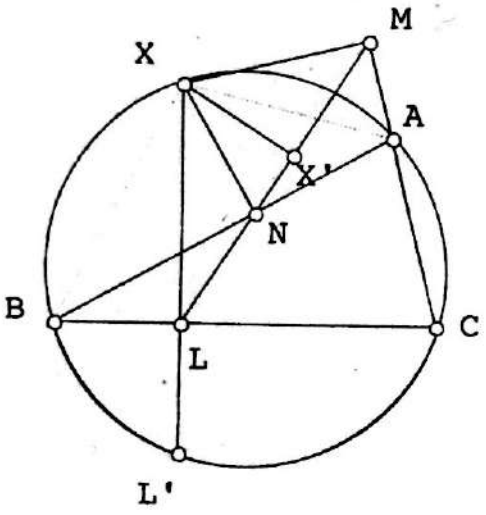


Fig. 3.41

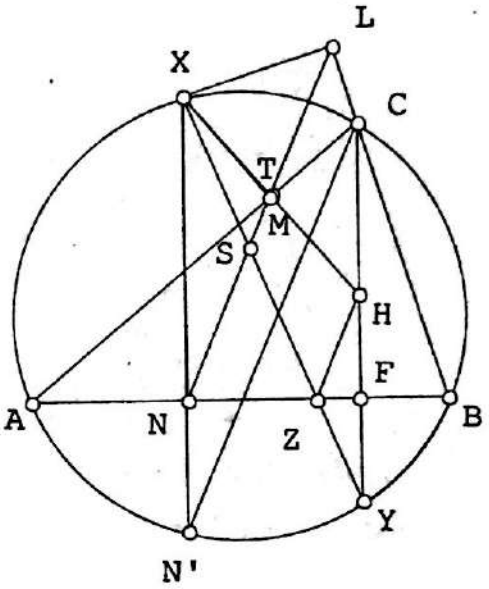


Fig. 3.42

Corollary 1. If the perpendicular XL on BC meets the circumcircle again at L', then AL' is parallel to the Simson line of X. (See Fig. 3.41).

Proof. Let XL produced meet the circumcircle at L'. Then $\angle XCA = \angle XL'A$. Also $\angle XCA = \angle XLM$, since the quadrilateral $XLCM$ is cyclic. Hence $\angle XL'A = \angle XLM$ so that $AL' \parallel LMN$.

Corollary 2. The Simson line of any point bisects the join of the point and the orthocentre.

Proof. As shown in Fig. 3.42, let the altitude CF produced meet the circumcircle at Y. Let XY cut the Simson line at S and AB at Z. Let XH cut the Simson line at T. Let XN produced meet the circumcircle at N'. Then $CN' \parallel LN$, by Cor. 1. Since $HF = FY$, we have

$$\angle ZHF = \angle ZYF = x, \ \angle HZF = \angle YZF = y, \text{ say.}$$

Since XN' and CY are parallel chords, $\angle YXN' = \angle XN'C = \angle XYC = x$. Hence HZ is parallel to CN' and hence to the Simson line. Hence $\angle SNZ = \angle SZN$ so that $SN = SZ$. Also $\angle YXN' = \angle XN'C = \angle XNS$, so that $XS = SN$. Hence S the mid-point of XZ. Therefore, as ZH is parallel to the Simson line, T is the mid-point of XH.

Example 10 With the notation of Fig. 3.41, we have

$$\text{(i)} \quad \frac{XL \cdot MN}{BC} = \frac{XM \cdot NL}{CA} = \frac{XN \cdot LM}{AB} = XX',$$

where $XX' \perp LMN$, and (ii) one of the ratios

$$\frac{BC}{XL}, \quad \frac{CA}{XM} \text{ and } \frac{AB}{XN}$$

is equal to the sum of the other two.

Proof. (i) Clearly, as in Fig. 3.41, $\triangle XNM \sim \triangle XBC$, and $\triangle XNX' \sim \triangle XBL$. Hence

$$\frac{XN}{XB} = \frac{MN}{BC}, \quad \frac{XN}{XB} = \frac{XX'}{XL},$$

so that

$$\frac{XL \cdot MN}{BC} = XX'.$$

Similarly, since $\triangle XNL \sim \triangle XAC$, $\triangle XAM \sim \triangle XNX'$ etc. we obtain the remaining ratios.

Theorem 26 (Ptolemy) The rectangle contained by the diagonals of a cyclic quadrilateral is equal to the sum of the rectangles contained by pairs of its opposite sides.

Proof. As in Fig. 3.43(i), draw AE making $\angle BAE = \angle CAD$. Then, since $\angle ABE = \angle ACD$ (same segment) and $\angle BAE = \angle CAD$ (by construction), it follows that the triangles BEA and CDA are similar. Also, $\angle BAC = \angle BAE + \angle EAC = \angle EAC + \angle CAD = \angle EAD$ and $\angle BCA = \angle BDA$, it follows that the triangles AED and ABC are similar. Hence

$$\frac{AC}{AB} = \frac{CD}{BE} \quad \text{and} \quad \frac{AC}{AD} = \frac{BC}{ED}.$$

So $AC \cdot BE = AB \cdot CD$ and $AC \cdot ED = AD \cdot BC$.

Adding these equations and noting that $BE + ED = BD$, we get

$$AC \cdot BD = AB \cdot CD + AD \cdot BC.$$

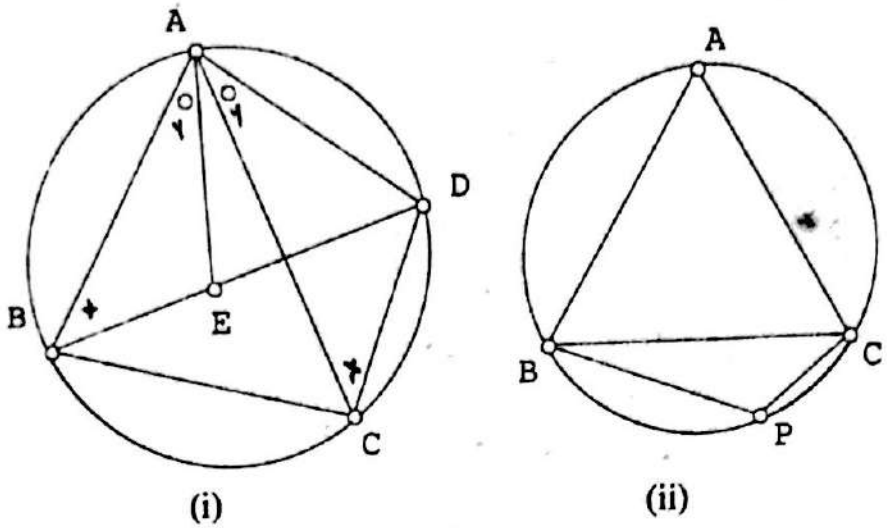


Fig. 3.43

Corollary. If a point be taken anywhere on the circumcircle of an equilateral triangle, its distance from one of the vertices is equal to the sum of its distances from the remaining vertices.

Proof. As in Fig. 3.43(ii), let P be a point on the minor arc BC of the circumcircle of the equilateral triangle ABC. Then applying Ptolemy's theorem to the cyclic quadrilateral $ABPC$, we get $PA \cdot BC = AB \cdot PC + AC \cdot PB$. So $PA = PB + PC$, since $AB = BC = CA$.

Theorem 27 (Extension of Ptolemy's Theorem.) Let $ABCD$ be a quadrilateral which is not cyclic. Then $BC.AD + AB.CD > AC.BD$.

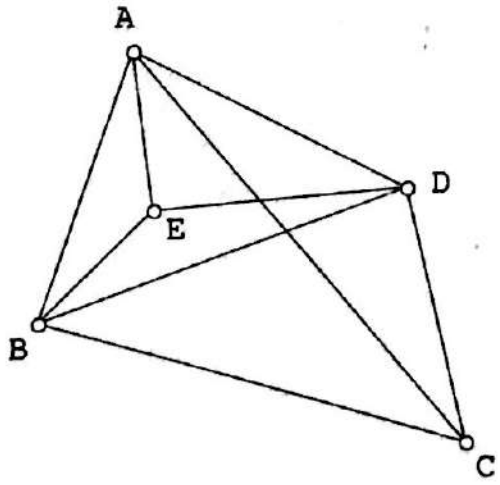


Fig. 3.44

Proof. See Fig. 3.44. Let $ABCD$ be a quadrilateral which is *not* cyclic so that angles ABD and ACD are *not* equal. Make $\angle BAE = \angle CAD$ and

$\angle ABE = \angle ACD$. Join ED. Then $\triangle ABE \sim \triangle ACD$ and so

$$\frac{AB}{BE} = \frac{AC}{CD} \quad \text{or} \quad AB \cdot CD = AC \cdot BE.$$

Also, since $\triangle ABE \sim \triangle ACD$, $\frac{AB}{CA} = \frac{AE}{AD}$.
Also, $\angle BAC = \angle EAD$. So, by theorem 6, we see that $\triangle ABC \sim \triangle AED$ and so

$$\frac{BC}{AC} = \frac{ED}{AD} \quad \text{or} \quad BC \cdot AD = AC \cdot ED.$$

Hence

$$AB \cdot CD + BC \cdot AD = AC \cdot (BE + ED) > AC \cdot BD$$

because BED is not a straight line.

Theorem 28 (Brahmagupta.) If in $\triangle ABC$, AD is the altitude and AE is the diameter of the circumcircle through A, then

$$AB \cdot AC = AD \cdot AE.$$

Proof: As shown in Fig. 3.45 $\triangle ABD \sim \triangle AEC$ so that $\frac{AB}{AE} = \frac{AD}{AC}$.

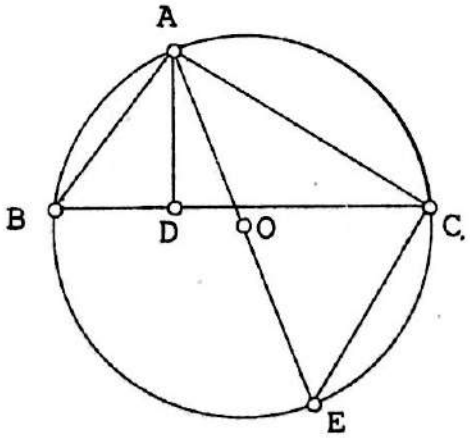


Fig. 3.45

Example 11 If $ABCD$ is a cyclic quadrilateral, then

$$AC \cdot [AB \cdot BC + CD \cdot DA] = BD \cdot [DA \cdot AB + BC \cdot CD].$$

Proof: See Fig. 3.46. By the last theorem, we have

$$\begin{aligned} AB \cdot BC &= 2R \cdot BM, \\ DA \cdot DC &= 2R \cdot DN, \end{aligned}$$

where R is the radius of the circle. Hence

$$\begin{aligned} & AC \cdot [AB \cdot BC + CD \cdot DA] \\ = \; & AC \cdot 2R \cdot BM + AC \cdot 2R \cdot DN \\ = \; & 2R[2\triangle ABC + 2\triangle ACD] \\ = \; & 4RS, \end{aligned}$$

where S =the area of the quadrilateral $ABCD$.

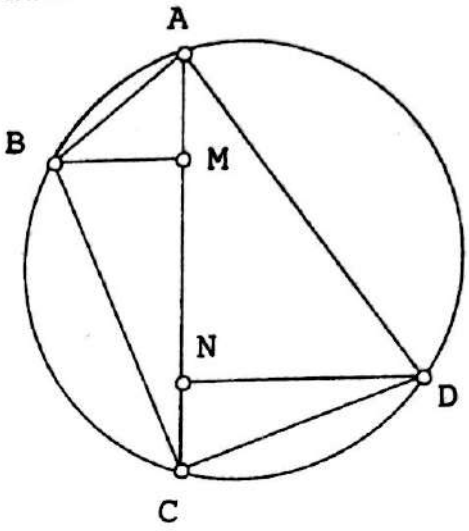


Fig. 3.46

Similarly, $BD \cdot [DA \cdot AB + BC \cdot CD] = 4RS$, and the result follows.

Example 12 D, E, F are the midpoints of the sides BC, CA, AB of $\triangle ABC$. Through D, E, F straight lines are drawn meeting in a point P; and through A, B, C lines are drawn parallel to DP, EP, FP respectively. Prove that these lines also meet in a point. (You may assume that P is inside $\triangle ABC$.)

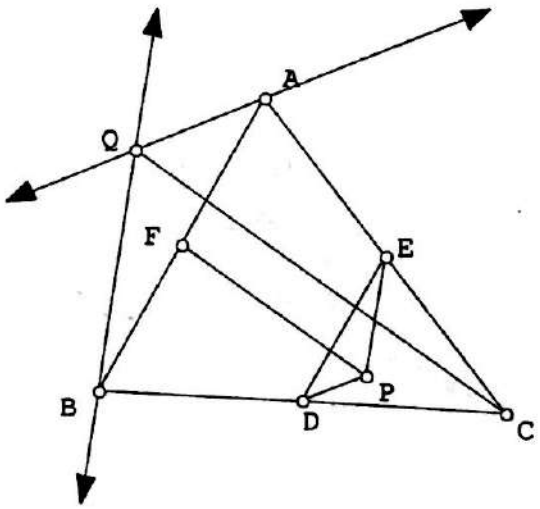


Fig. 3.47

Solution. Let the lines through A and B parallel to DP and EP respectively meet in Q. Join CQ. Since $DP \parallel QA$, $EP \parallel BQ$ and $AB \parallel ED$, triangles QAB and PDE are similar. So $QB/EP = AB/DE = 2$. Also $BC/FE = 2$. Hence $QB/EP = BC/FE$. Also, $\angle QBC = x + \angle ABC = x + \angle DEF = \angle FEP$. Hence $\triangle QBC \sim \triangle PEF$. Hence $QC \parallel PF$ and the result follows.

Example 13 D is the midpoint of the side BC of $\triangle ABC$. The line joining D and the incentre I of the triangle intersects the altitude AA' at the point P. Prove that $l(AP)$ is equal to the radius of the incircle of the triangle.

Solution. In $\triangle ABC$, let D be the midpoint of BC, I the incentre and P the intersection of DI with the altitude AA'. Draw the circumcircle with centre O. Now X, the midpoint of arc BC of the circumcircle, lies on AI, and OX is the perpendicular bisector of BC. Draw $IQ \perp AC$.

Since $\angle IAQ = \angle BAX = \angle BCX = \frac{1}{2}\angle A$, the right triangles AIQ and CXD are similar.Also since $\angle IAP = \angle IXD$ and $\angle AIP = \angle XID$, triangles AIP and XID are similar. Hence

$$\frac{AP}{XD} = \frac{AI}{IX} \text{ and } \frac{AI}{XC} = \frac{IQ}{XD}.$$

But we know that $IX = XC$. Hence $AP = IQ$, as required.

Exercise Set-3.3

1. **Heron's formula:** In $\triangle ABC$, let a, b, c denote the lengths of the sides BC, CA, AB respectively. Let $2s = a + b + c$, so that s is the semi-perimeter of $\triangle ABC$. Then show that the area $\triangle$ of $\triangle ABC$ is given by
$$\triangle = \sqrt{s(s-a)(s-b)(s-c)}.$$
Hence, or otherwise show that among all the triangles having the same perimeter, equilateral triangle has the maximum area.

2. The centroid G of $\triangle ABC$, is such that $AG = BC$. Show that $\angle BGC = 90°$.

3. In $\triangle ABC$, G is the centroid. Prove that
$$AB^2 + BC^2 + CA^2 = 3(GA^2 + GB^2 + GC^2).$$

4. **Theorem:** In any triangle, the sum of any two sides is greater than the third side.

5. $PQRS$ is a quadrilateral in which $\angle PQR = \angle QRS$. Prove that $\angle RSP$ is greater than, equal to, or less than $\angle SPQ$ according as PQ is greater than, equal to, or less than RS.

6. E is the mid-point of segment AD, which is drawn through A to meet the side BC of the equilateral triangle ABC at any point D. Show that $AE < CE$.

7. **Theorem:** In $\triangle ABC$, straight lines are drawn from the vertices B, C to intersect at a point Q within the triangle. Prove that

   (i) $AB + AC > OB + OC$. (ii) $\angle BOC > \angle BAC$.

   (iii) $AB + AC - [OB + OC] < 2 \cdot OA$.

8. **Theorem:** In triangles ABC and DEF, $AB = DE$, $AC = DF$ and $\angle BAC > \angle EDF$. Prove that $BC > EF$. [Conversely, if $AB = DE$, $AC = DF$ and $BC > EF$, then $\angle BAC > \angle EDF$.]

9. Square $ABCD$ is divided into two parts by the diagonal AC. Show that if O is any point within triangle ABC, then $OB < OD$.

10. In $\triangle ABC$, $AB > AC$. Show that median $BE >$ median CF.

11. Suppose $ABCD$ is a rectangle and P, Q, R, S are points on the sides AB, BC, CD, DA respectively. Show that

$$PQ + QR + RS + SP > \sqrt{2} \cdot AC.$$

12. In $\triangle ABC$, $m_a + m_b + m_c < a + b + c < \frac{4}{3}(m_a + m_b + m_c)$.

13. In $\triangle ABC$, O is the circumcentre and H is the orthocentre. If $AO = AH$, prove that $\angle A = 60°$. Also, if the circle BOC passes through H, prove that $\angle A = 60°$.

14. In $\triangle ABC$, O is the circumcentre and H is the orthocentre . Then, prove that $AH^2 + BC^2 = 4AO^2$.

15. The incircle of $\triangle ABC$ touches BC at D. Show that the circles inscribed in triangles ABD and CAD touch each other.

16. In $\triangle ABC$, let AD be the internal bisector of $\angle A$. Show that, $AD^2 = AB \cdot AC - BD \cdot DC$.

17. P and P' are points on the circumcircle of $\triangle ABC$ such that PP' is parallel to BC. Prove that $P'A$ is perpendicular to the Simson line of P.

18. P is a point on the circumcircle of $\triangle ABC$ and O is its circumcenctre. Prove that $\angle APO =$ angle between the Simson line of P and BC.

19. If, as in Fig. 3.43(i), the diagonals AC, BD intersect in M, then prove that

$$\frac{AB \cdot BC}{AD \cdot DC} = \frac{BM}{DM}.$$

20. Two circles intersect in points A and B. PQ is a line segment through A and terminating on the two circles. Prove that BP/BQ is constant for all allowable configurations of PQ.

21. A hexagon inscribed in a circle has three consecutive sides of length a and three consecutive sides of lengths b. Determine the radius of the circle.

22. Consider a triangle $P_1P_2P_3$ and a point P within the triangle. Lines P_1P, P_2P, P_3P, intersect the opposite sides in points Q_1, Q_2, Q_3 respectively. Prove that out of the numbers

$$\frac{P_1P}{PQ_1}, \frac{P_2P}{PQ_2}, \frac{P_3P}{PQ_3},$$

at least one is ≤ 2 and at least one is ≥ 2.

23. If a quadrilateral $ABCD$ circumscribes a circle, show that $AB+CD = BC + DA$. Conversely, show that if a convex quadrilateral $ABCD$ is such that $AB + CD = BC + DA$, then a circle can be inscribed in the quadrilateral.

24. A quadrilateral inscribes a circle and it also circumscribes another circle. If the sides of the quadrilateral are a, b, c, d, show that the area of the quadrilateral is $\sqrt{abcd}$.

25. Show that the harmonic mean of the altitudes of a triangle is equal to 3 times its inradius.

26. $ABCD$ is a square. E is a point inside the square such that $m\angle EBC = m\angle ECB = 15°$. Show that $\triangle AED$ is equilateral.

27. In the triangle ABC, $AB = AC$; the altitude AD of the triangle meets the circumcircle at P; prove that $AP.BC = 2AB.BP$.

28. P is a point on the minor arc AB of the circumcircle of the square $ABCD$; prove that $\dfrac{PA+PC}{PB+PD} = \dfrac{PD}{PC}$.

29. P is a point on the minor arc AB of the circumcircle of the regular pentagon $ABCDE$; prove that $\dfrac{PA+PD}{PB+PD} = \dfrac{PE}{PC}$.

30. P is a point on the minor arc AB of the circumcircle of the regular hexagon $ABCDEF$; prove that $PE + PD = PA + PB + PC + PF$.

31. P is a point on the minor arc AB of the circumcircle of the regular pentagon $ABCDE$; prove that $PA + PB + PD = PC + PE$.

32. P is a point inside a parallelogram $ABCD$, such that

$$\angle APB + \angle CPD = 180°;$$

prove that $AP \cdot CP + BP \cdot DP = AB \cdot BC$.

33. If P, Q, R are points on the sides BC, CA, AB of a triangle, such that the perpendiculars to the sides at these points are concurrent; then show that

$$BP^2 + CQ^2 + AR^2 = PC^2 + QA^2 + RB^2.$$

34. Two circles of radii a and b touch each other externally and they also touch a line. A circle of radius c is inscribed in the region in between the circles and the line to touch the both the circles and the line. Show that

$$\frac{1}{\sqrt{c}} = \frac{1}{\sqrt{a}} + \frac{1}{\sqrt{b}}.$$

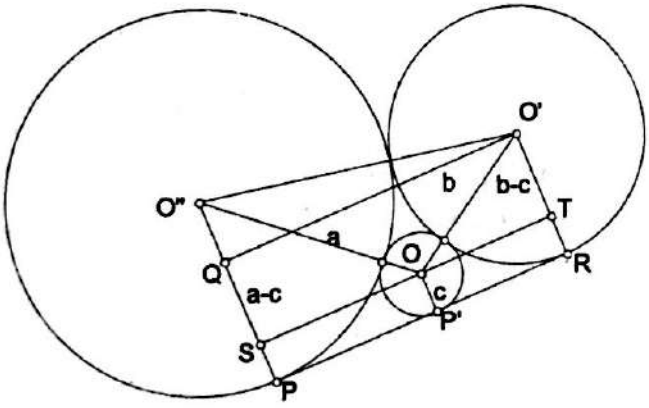


Fig. (a)

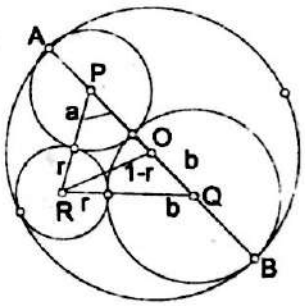


Fig. (b)

35. Two circles C_1, C_2 of radii a and b touch each other externally and they both touch a unit circle C internally. A circle C_3 of radius r is inscribed to touch the circles C_1, C_2 externally and the circle C internally. Show that

$$r = \frac{ab}{1 - ab}.$$

3.5 Constructions

Notation. In $\triangle ABC$, we denote by (i) a, b, c the lengths of the sides opposite to A, B, C; (ii) h_a, h_b, h_c the altitudes on BC, CA, AB; (iii) m_a, m_b, m_c medians to BC, CA, AB; (iv) t_a, t_b, t_c, the bisectors of angles A, B, C.

I. To construct $\triangle ABC$ when the stated elements are given.

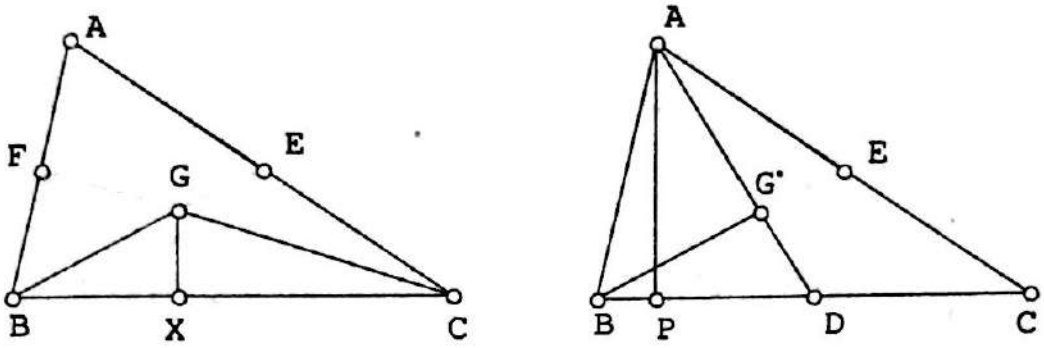


Fig. 3.48

(a) Given m_b, m_c, h_a. (See Fig. 3.48(i)). Construct $\triangle GBC$ with altitude $GX = h_a/3$ and sides $GB = 2m_b/3$, $GC = 2m_c/3$. Then $\triangle ABC$ can be easily completed.

(b) Given m_a, m_b, h_a (See Fig. 3.40(ii)). First construct right angled triangle APD with side $AP = h_a$ and hypotenuse $AD = m_a$. Divide AD at G in the ratio $2 : 1$. Take B on PD such that $GB = 2\ m_b/3$ and produce BD to C such that $BD = DC$. Join A to B and C.

(c) Given m_a, m_b, m_c.
First construct $\triangle BGG'$ with sides GG', BG, BG' equal to $2/3$ times m_a, m_b and m_c. Find midpoint D of GG'. Produce BD to C so that $BD = DC$. Produce $G'G$ to A so that $G'G = GA$. Join AB and AC.

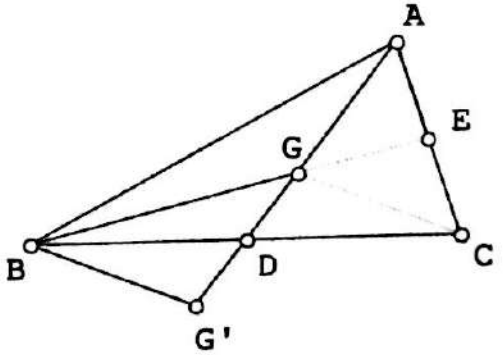


Fig. 3.49

(d) Given h_a, h_b, h_c. Since $a.h_a = b.h_b = c.h_c$ = twice the area of $\triangle ABC$, we see a, b, c are inversely proportional to the altitudes h_a, h_b, h_c. So first construct line segments inversely proportional to h_a, h_b, h_c as follows. As in Fig.

3.50(ii), draw a circle of sufficiently large radius. In it take a point P sufficiently close to the circumference. Find points A_1, B_1, C_1 on the circle at distances h_a, h_b, h_c from P. Let the lines meet the circle again at A_2, B_2, C_2. Then by theorem 12, we see that PA_2, PB_2, PC_2 are the required segments. Construct $\triangle AMN$ with sides MN, AM, AN equal to these segments. Enlarge or reduce $\triangle AMN$ to obtain $\triangle ABC$ with given altitude h_a.

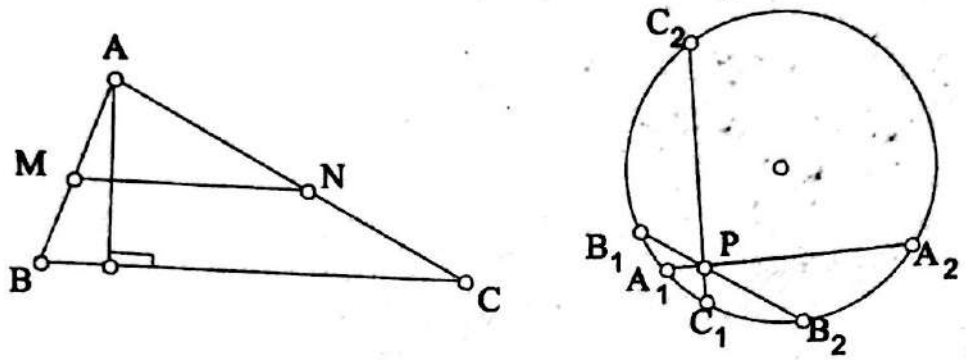
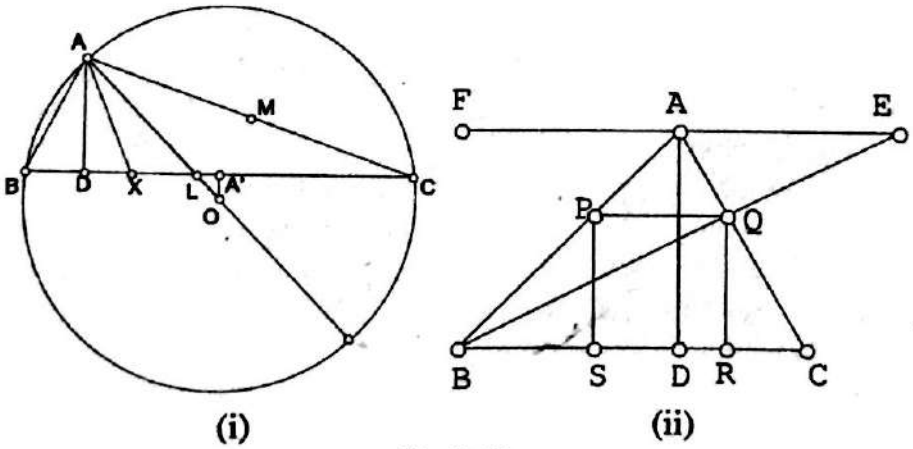


Fig. 3.50

(e) Given m_a, h_a, t_a. First construct right angled triangle ADX with $AD = h_a$ and hypotenuse $AX = t_a$. Draw AL so that $\angle XAL = \angle DAX$. Find A' on DX (produced if necessary) such that $AA' = m_a$. Then by theorem 23, we see that the perpendicular to DX through A' meets AL at O, where O is the circumcentre of the required $\triangle ABC$. Hence the circle with centre O and radius OA cuts DX at B and C. See Fig. 3.51 (i)



(i) (ii)

Fig.3.51

II. To inscribe a square $PQRS$ in a given triangle ABC such that P is on AB, Q is on AC and R, S are on BC. For this draw FE parallel to BC through A. Find E such that $AE =$ altitude AD as in Fig. 3.51 (ii). Let EB cut AC in Q. Then rectangle $PQRS$ is as required.

III. To inscribe in a given $\triangle ABC$ a triangle similar to a given $\triangle XYZ$. For this, as in Fig. 3.52, draw EF parallel to YZ. Then draw $DF \parallel XZ$ and $DE \parallel XY$ to meet in D. Produce CD to meet AB in P. Draw $PR \parallel DF$ and $PQ \parallel DE$. Join QR. Then $\triangle PQR$ is as required.

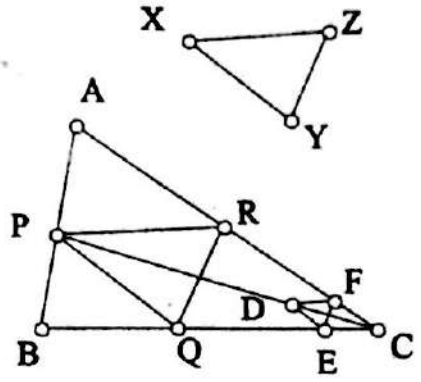
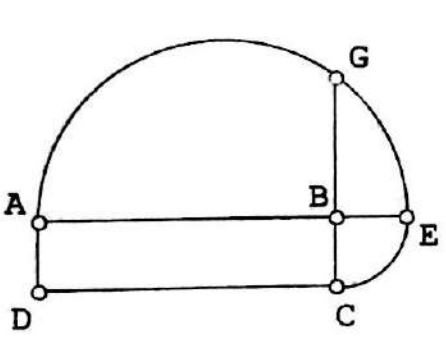


Fig.3.52

IV. To construct a square whose area is equal to the area of a given rectangle $ABCD$ using unmarked ruler and compass only. As in Fig. 3.53(i) produce AB to E so that $BC = BE$. Draw a semicircle with AE as diameter and let it meet CB produced at G. Then BG equals a side of the required square.



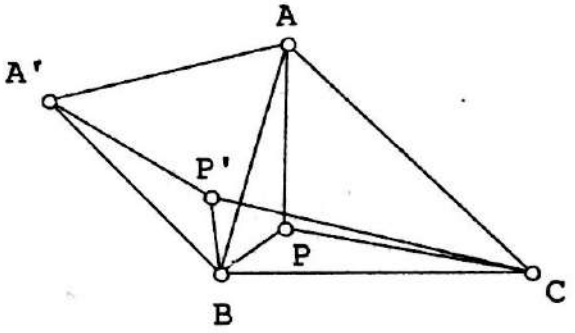


Fig.3.53

V. To find a point P in a given acute-angled triangle ABC such that $PA + PB + PC$ is minimum. Take any point P inside $\triangle ABC$. Join P to A, B, C and as in Fig. 3.53 (ii), rotate $\triangle APB$ through $60°$ about B to obtain $\triangle A'P'B$. Then $\triangle ABA'$ and $\triangle PBP'$ are equilateral. Hence $PA+PB+PC = A'P' + P'P + PC$ and three segments $A'P', P'P$ and PC form a path from A' to C. This path, in general, has angles at P' and P and it has minimal length when it is straight, in which case $\angle BPC = 120°$ and $\angle APB = \angle A'P'B = 120°$. Thus the required point P, for which $PA+PB+PC$ is minimum, is the point at which each of the sides BC, CA, AB makes an angle of $120°$. This point P can be constructed thus: P is the second intersection of line CA' with the circumcircle of the equilateral $\triangle ABA'$.

VI. L is a line and A, B are points not on L and lying on the same side of L. To find a point P on L such that $AP+PB$ is minimum. As in Fig. 3.45, let A' be the reflection of A in L. Let $A'B$ meet L in P. Then P is the required point.

For if R is any other point on L, then $AR + RB = A'R + RB > A'B = A'P + PB = AP + PB$.

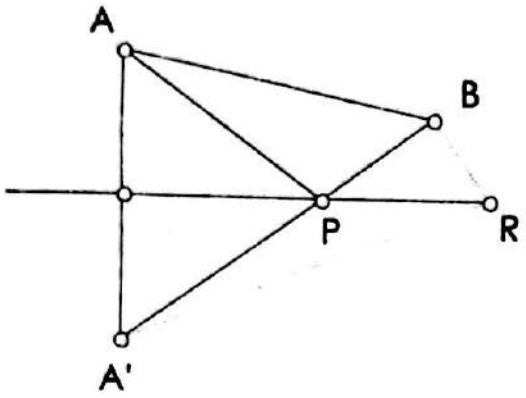


Fig.3.54

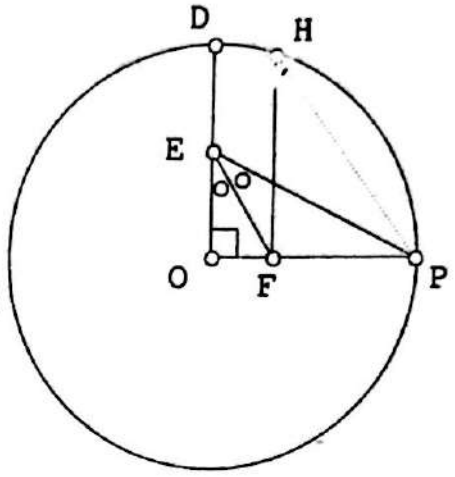


Fig.3.55

VII. To inscribe a regular pentagon in a given circle. See Fig. 3.55.
Draw the circle with centre O and let P be a point on it. Construct $OB \perp OP$ meeting the circle in B. Bisect OB at D. Bisect $\angle ODP$ and let the bisector meet OP at N. Construct $NQ \perp OP$ meeting the circle in Q. Then PQ is a side of a regular pentagon inscribed in the given circle.

Exercise Set-3.4

1. ABC is a given triangle; construct a point P such that $PA : PB : PC = 1 : 2 : 4$.

2. $ABCD$ are four collinear points; construct a point P at which AB, BC, CD subtend equal angles.

3. Given the base, vertical angle and the ratio of the sides containing it, construct the triangle.

4. Construct a triangle, given the lengths of one side and two medians.

5. Given A, N, H construct the triangle ABC.

6. Three distinct concurrent lines are given. Construct an equilateral triangle having exactly one vertex on each of the given lines. You are allowed to use unmarked ruler and compass only. Justify your construction.

3.6 Solved Problems

Example 14 A straight line cuts two concentric circles in points A, B, C and D in that order. AE and BF are parallel chords, one in each circle. If CG is perpendicular to BF and DH is perpendicular to AE, prove that $GF = HE$.

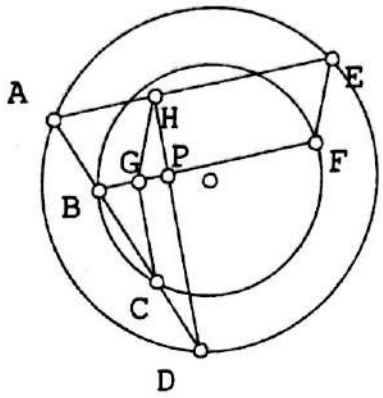


Fig. 3.56

Solution. Let DH intersect BF at P. Let $AB = m$. Then $CD = m$, since the chords AD and BC have a common perpendicular bisector as the circles are concentric. Then in right angled triangle GPH,

$$GH^2 = GP^2 + PH^2 = m^2 \sin^2 D + m^2 \sin^2 A = m^2,$$

since angles A, D are complementary. So $GH = m$ and the trapezium $ABGH$ is isosceles. (Note that $BG < AH$). Since AE and BF are parallel chords in two concentric circles, they have a common perpendicular bisector. Hence the trapezium $ABFE$ is also isosceles. Hence $EFGH$ is a parallelogram and $GF = HE$.

Example 15 Construct $\triangle ABC$, given $\angle A$, side AC and the radius r of the inscribed circle. Justify your construction.

Solution. Analysis: Let I be the incentre. Let ID, IE, IF be the perpendiculars from I to the sides BC, CA and AB.
Then $\angle FIE = 180^0 - \angle A$. Also the tangents CE and CD are equal.

Construction: Draw a circle with centre I and radius r. Draw radii IE and IF such that $\angle FIE = 180^0 - A$. Draw the tangents at F and E meeting in A. Produce AE to C so that AC is as given. With centre C draw an are with radius CE to cut the incircle at D. Produce CD to meet AF in B. Then ABC is the required triangle.

Example 16 $\triangle ABC$ is right angled at C. The internal bisectors of $\angle A$ and $\angle B$ meet BC and CA at P and Q respectively. M and N are the feet of the perpendiculars from P and Q to AB. Find $\angle MCN$.

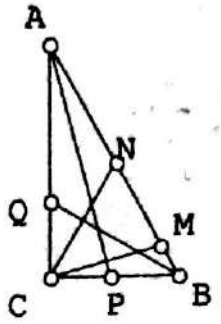


Fig. 3.57

Solution. Since $\angle BNQ = \angle BCQ = 90°$, B, C, Q, N are concyclic and so $\angle CNQ = \frac{B}{2} = \angle NCQ$. Similarly, A, P, M, C are concyclic. Hence, $\angle MCP = \frac{A}{2} = \angle PMC$. Hence, $\frac{A}{2} + \angle MCN + \frac{B}{2} = \angle ACB = 90°$. Since $\angle A + \angle B = 90°$, we get $\angle MCN = 45°$.

Example 17 Three circles C_1, C_2, C_3 with radii r_1, r_2, r_3 $(r_1 < r_2 < r_3)$ respectively are given. They are placed such that C_2 lies to the right of C_1 and touches it externally; C_3 lies to the right of C_2 and touches it externally. Further, there exist two straight lines each of which is a direct common tangent simultaneously to all the three circles. Find r_2 in terms of r_1 and r_3.

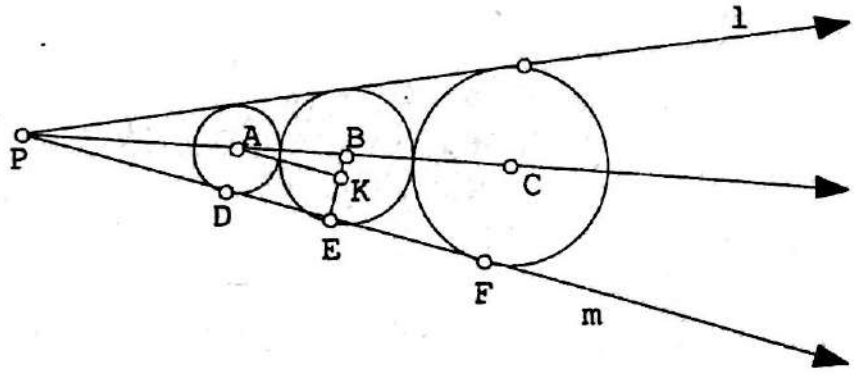


Fig. 3.58

Solution. Let the given common tangents l, m meet at P. We observe that the centres, say A, B, C of the given circles will lie on the angle-bisector of the angle between l and m. Let these circles touch m at D, E, F respectively. Draw $AK \perp BE$. We have

$$\begin{aligned} DE &= AK = \sqrt{(AB)^2 - (BK)^2} \\ &= \sqrt{(r_2 + r_1)^2 - (r_2 - r_1)^2} = 2\sqrt{r_1 r_2}. \end{aligned}$$

Similarly $EF = 2\sqrt{r_2 r_3}$. Let $m\angle APD = \theta$ and $PD = x$. Then

$$\begin{aligned} \tan\theta &= \frac{AD}{PD} = \frac{BE}{PE} = \frac{CF}{PF} \\ &= \frac{r_1}{x} = \frac{r_2}{x + 2\sqrt{r_1 r_2}} = \frac{r_3}{x + 2\sqrt{2r_1 r_2} + \sqrt{r_2 r_3}} \end{aligned}$$

$$\text{Hence, } \frac{r_2 - r_1}{2\sqrt{r_1 r_2}} = \frac{r_3 - r_2}{2\sqrt{r_2 r_3}}.$$

Thus, $\sqrt{r_3}(r_2 - r_1) = \sqrt{r_1}(r_3 - r_2)$. Therefore,

$$r_2(\sqrt{r_3} + \sqrt{r_1}) = \sqrt{r_1 r_3}(\sqrt{r_1} + \sqrt{r_3}).$$

Hence, $r_2 = \sqrt{r_1 r_3}$.

Example 18 Let ABC be a triangle with unequal sides. The medians of $\triangle ABC$, when extended, intersect its circumcircle in points L, M, N. If L lies on the median through A and $LM = LN$, prove that

$$2BC^2 = CA^2 + AB^2.$$

Solution. We note that the triangles AGB and MGL are similar because $\angle GAB = \angle GML$ (same segment) and $\angle AGB = \angle MGL$. Hence

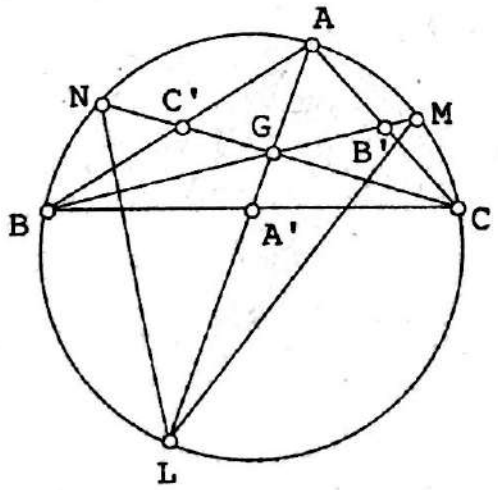


Fig. 3.59

$$\frac{AG}{MG} = \frac{AB}{LM} \text{ i.e. } AG = MG \cdot \frac{c}{LM}. \qquad (1)$$

Similarly, $\triangle AGC \sim \triangle NGL$ and so

$$\frac{AG}{NG} = \frac{AC}{NL} \text{ i.e. } AG = NG \cdot \frac{b}{NL}. \tag{2}$$

Also, by data, $LM = LN$. Hence by (1),(2) we get

$$\frac{MG}{GN} = \frac{b}{c}. \tag{3}$$

Since the chord BM and CN intersect at G, we have

$$BG \cdot GM = CG \cdot GN.$$

So by (3), $BG \cdot b = CG \cdot c$ and so

$$\frac{2}{3}BB' \cdot b = \frac{2}{3}CC' \cdot c \text{ or } 2BB'^2 \cdot b^2 = 2CC' \cdot c^2.$$

So, applying Apollonius' theorem twice we get

$$\begin{aligned} b^2(c^2 + a^2 - 2AB'^2) &= c^2(a^2 + b^2 - 2AC'^2), \\ b^2(c^2 + a^2 - \frac{1}{2}b^2) &= c^2(a^2 + b^2 - \frac{1}{2}c^2), \\ a^2(b^2 - c^2) &= \frac{1}{2}(b^4 - c^4), \\ 2a^2 &= b^2 + c^2, \quad \text{as } b \neq c. \end{aligned}$$

Solutions to Problems

Problem 1 By Theorem 3, since $PQ \parallel BC$, we get the equality $AP/PB = AQ/QC$. Similarly, we have, the equalities $CR/RB = CQ/QA$,

$$BR/RC = BS/SA,\ AT/TC = AS/SB, \text{ and } CT/TA = CU/UB.$$

Multiplying these five equalities we get $AP/PB = CU/UB$. So, by Theorem 3, $PU \parallel AC$.

Problem 2 Let $\angle BAC = x$, $\angle BDC = y$, and $\angle EDC = z$. Then by data, we get $\angle AED = x$, $\angle BCD = \angle ABC = y$, and $\angle EBD = z$. Now for $\triangle EBD$, exterior angle AED = the sum of the interior opposite angles EDC and EBD i.e. $x = z + z = 2z$. Similarly, from $\triangle ABD$ we get $y = x + z$ so that $y = 3z$. Finally, from $\triangle ABC$ we get $x + 2y = 180°$ so that $2z + 6z = 180°$ i.e. $z = 22.5°$. Hence $\angle A = x = 2z = 45°$.

Problem 3: We will show that $TX = TY$. Let $\angle TOX = \angle XOA = x$ and $\angle OTA = y$. Then since OT touches the circle at T, $\angle TBA = y$. So from $\triangle TOX$, $\angle TXY = x + y$ and from $\triangle YOB$, $\angle TYX = x + y$. Thus $\angle TXY = x + y = \angle TYX$ so that $\triangle TXY$ is isosceles.

Problem 4: Hint: Join OR.

Solutions to Exercise Set-3.3

11. Assume that $AB \geq BC$. Then $AC^2 = AB^2 + BC^2 \leq 2AB^2$ so that $AC \leq \sqrt{2} \cdot AB$. Also, $SP + PQ > SQ$, $QR + RS > SQ$. Hence $SP + PQ + QR + RS > 2 \cdot SQ \geq 2 \cdot AB = 2 \cdot AC/\sqrt{2} = \sqrt{2} \cdot AC$.

12. Let D, E, F be the midpoints of BC, CA, AB and G be the centroid. Then in $\triangle ADE$, $AD < AE + ED$ or $m_a < (b/2 + c/2)$. Similarly we get $m_b < (c/2 + a/2)$ and $m_c < (a/2 + b/2)$. Adding these three inequalities we get $m_a + m_b + m_c < a + b + c$. Next from $\triangle BCG$, $BG + GC > BC$ or $\frac{2}{3}m_b + \frac{2}{3}m_c > a$ or $2(m_b + m_c) > 3a$. Similarly we get two more inequalities and adding them we get $3(a + b + c) < 4(m_a + m_b + m_c)$.

16. Let AD produced meet the circumcircle of $\triangle ABC$ in L. Then, clearly, $\triangle ABD$ is similar to $\triangle ALC$. Hence $AB/AL = AD/AC$. Hence,

$$\begin{aligned} AB \cdot AC = AD \cdot AL &= AD(AD + DL) \\ &= AD^2 + AD \cdot DL = AD^2 + BD \cdot DC. \end{aligned}$$

23. First, suppose that the quadrilateral $ABCD$ circumscribes a circle so that its sides AB, BC, CD, and DA touch the circle respectively at points P, Q, R, and S, say. Then $AP = AS$, $BP = BQ$, $CQ = CR$, and $DR = DS$. Hence $AB + CD = AP + PB + CR + RD = AS + BQ + QC + SD = AD + BC$.

Conversely, let convex quadrilateral $ABCD$ be such that

$$AB + CD = BC + DA. \tag{i}$$

If $AB = BC$, then by (i), $DA = CD$, so that $ABCD$ is a kite and the internal bisectors of angles A and C meet on BD, by symmetry, at O, say. Then clearly a circle can be inscribed in the quadrilateral with centre O. Otherwise, let $AB > BC$. (Fig. 3.60) Then by (i), $DA - CD = AB - BC$ and so $DA > CD$, also. Take point X on side AB such that $BX = BC$ and point Y on side DA such that $DY = DC$. Then by (i), $AX = AY$. The internal bisectors of the angles B, A, D bisect at right angles the bases of the isosceles triangles BCX, DCY and AXY and so they meet at the circumcentre say O', of $\triangle CXY$. The point O' is equidistant from all the sides and lies within the quadrilateral. Hence a circle with centre O' can be inscribed in the quadrilateral.

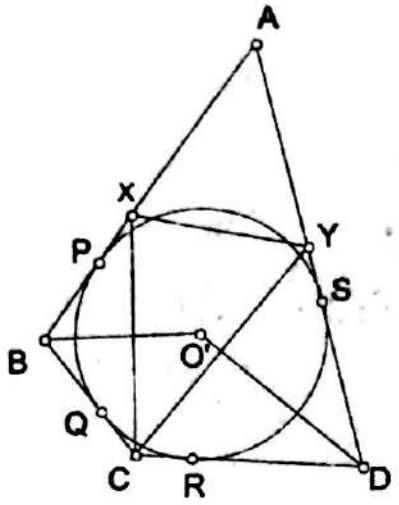


Fig. 3.60

24. First, consider a general convex quadrilateral $ABCD$. Denote the lengths of its sides and diagonals thus: $AB = a$, $BC = b$, $CD = c$, $DA = d$, $AC = x$, and $BD = y$. Let S be the area and $s = \frac{1}{2}(a+b+c+d)$ be the semi-perimeter of the quadrilateral. Then $S = \triangle ABC + \triangle ACD$ so that

$$4S = 2ab\sin B + 2cd\sin D. \tag{1}$$

Also, $a^2 + b^2 - 2ab\cos B = x^2 = c^2 + d^2 - 2cd\cos D$ so that

$$a^2 + b^2 - c^2 - d^2 = 2ab\cos B - 2cd\cos D. \tag{2}$$

From (1) and (2) by squaring and adding,

$$\begin{aligned}
16S^2 \; + \; (a^2+b^2-c^2-d^2)^2 &= 4a^2b^2 + 4c^2d^2 - 8abcd\cos(B+D) \\
&= (2ab+2cd)^2 - 8abcd[1+\cos(B+D)]. \text{ Hence} \\
16S^2 &= (2ab+2cd)^2 - (a^2+b^2-c^2-d^2)^2 - 16abcd\cos^2\frac{B+D}{2} \\
&= [(a+b)^2-(c-d)^2]\,[(c+d)^2-(a-b)^2] \\
&\qquad - 16abcd\cos^2\frac{B+D}{2} \\
&= (a+b+c-d)(a+b-c+d)(c+d+a-b)(c+d-a+b) \\
&\qquad - 16abcd\cos^2\frac{B+D}{2} \\
&= (2s-2d)(2s-2c)(2s-2b)(2s-2a) - 16abcd\cos^2\frac{B+D}{2}
\end{aligned}$$

So

$$S^2 = (s-a)(s-b)(s-c)(s-d) - abcd\cos^2\frac{B+D}{2}. \qquad (3)$$

When the lengths of the sides of the quadrilateral are given, (3) shows that the area of the quadrilateral is greatest when $\cos\frac{1}{2}(B+D) = 0$ i.e. when $B+D = 180°$ i.e. when the quadrilateral is cyclic. Also, when the quadrilateral is cyclic, its area is given by

$$S = \sqrt{(s-a)(s-b)(s-c)(s-d)}. \qquad (4)$$

If the quadrilateral is cyclic and also has an inscribed circle, then as seen above, we have $a+c = b+d = \frac{1}{2}(a+b+c+d) = s$. Hence $s-a = c$, $s-c = a$, $s-b = d$, and $s-d = b$. So (4) gives

$$S = \sqrt{abcd}.$$

31.

$$\begin{aligned} PA\cdot DE + PD\cdot AE &= PE\cdot AD = PE\cdot BD; \\ PE\cdot BD + PB\cdot DE &= PD\cdot BE = PD\cdot EC; \\ PD\cdot EC &= PE\cdot DC + PC\cdot DE; \end{aligned}$$

add all the three results; then

$$PA\cdot DE + PD\cdot AE + PB\cdot DE = PE\cdot DC + PC\cdot DE,$$

but $DE = AE = DC$.

34. Hint: Let $O'Q \perp O''P$ and TS be the common perpendicular to $O''P$ and $O'P$ through O. Then $PP'^2 = SO^2 = OO''^2 - O''S^2 = (a+c)^2 - (a-c)^2 = 4ac$ so that $PP' = 2\sqrt{ac}$. Similarly, $P'R = 2\sqrt{bc}$. Also $PR^2 = QO'^2 = O'O''^2 - O''Q^2 = (a+b)^2 - (a-b)^2 = 4ab$ so that $PR = 2\sqrt{ab}$. Now $PR = PP' + P'R$.

35. Hint: First, $2a + 2b = AB = 2$ so that $a + b = 1$. Using cosine rule for triangles PRO and PRQ, we get

$$\begin{aligned} (1-r)^2 &= (a+r)^2 + (1-a)^2 - 2(a+r)(1-a)\cos\alpha, \\ \text{and } (b+r)^2 &= (a+r)^2 + (a+b)^2 - 2(a+r)(a+b)\cos\alpha. \end{aligned}$$

Now put $a + b = 1$ and eliminate α.

Solutions to Exercise Set-3.4

5. Observe that N is midpoint of OH. Hence, we get OA, the circumradius of $\triangle ABC$. Also, observe that $OA' \parallel AH$ and $OA' = \frac{1}{2}AH$.

6. Let the given lines be denoted by l, m, n and be concurrent at O.

Construction:

- Choose any point P, other than O, on m.
- Draw $\angle APO = \angle CPO = 60°$ such that A and C lie on l and n respectively.Complete the triangle APC.
- Draw the circumcircle of triangle APC. Let it intersect m again at B. Then $\triangle ABC$ is as required.

Justification: Note that $ABCP$ is a cyclic quadrilateral and

$$\angle ABC = \angle ACB = 60°$$

as they are inscribed in the arcs having measure 60°. Hence $\triangle ABC$ is equilateral as desired.

♣♣♣

Chapter 4

Combinatorics

Combinatorics is concerned with arrangements of the objects of a set into patterns. Thus in combinatorics we deal with the problems of existence, counting and generation of arrangements of a specified kind. Two basic counting principles, namely the Addition Principle (A.P.) and the Multiplication Principle (M.P.) are already known to the reader. In this chapter, we apply A.P. and M.P. to count permutations and combinations of objects with or without repetition. Then we introduce the Bijection Principle, the Inclusion-Exclusion Principle, the Pigeonhole Principle and the method of recurrence relations.

4.1 Basic Counting Principles

Addition Principle (A.P.): If a finite set S of objects is divided into two disjoint subsets S_1, S_2, then the number of objects in S (denoted as $|S|$) can be determined by finding the number of objects in S_1 and S_2 and adding them, i.e. $|S| = |S_1| + |S_2|$.

This principle can be extended, by induction, to the case of more than two subsets as follows:
If a finite set S of objects is divided into mutually disjoint subsets $S_1, \ldots, S_m$, then the number of objects in S can be determined by finding the number of objects in $S_1, \ldots, S_m$ and adding them, i.e. $|S| = |S_1| + \ldots + |S_m|$.

The addition principle can be stated in terms of choices as follows:
If a set S contains m objects and a set T contains n objects and S and T are disjoint sets, then the total number of ways of choosing one object from S *or* T is $m + n$.

Multiplication Principle (MP): If an action A has m different outcomes and a second action B has n different outcomes, then on performing *both* the actions A and B, in that order, we get mn composite outcomes, provided all these composite outcomes are distinct.

This principle can also be stated as follows:

If A, B are finite sets containing m and n objects respectively, then the Cartesian product $A \times B = \{(x, y) \mid x \in A, y \in B\}$ contains mn ordered pairs.

The multiplication principle can be extended, by induction, to any finite number of actions as follows:

Multiplication Principle (MP): Suppose a procedure can be broken into m successive *ordered* stages, with r_1 outcomes in the first stage, r_2 outcomes in the second stage, $\ldots$, r_m outcomes in the m^{th} stage. If all these composite outcomes are distinct, then the total procedure has $r_1 \cdot r_2 \cdots r_m$ different composite outcomes.

In solving problems, we shall apply one or both of the above principles. In general, the method is as follows:

If the given problem can be divided into mutually exclusive cases, then we apply AP and the total count is the sum of the counts obtained in the various cases. If we have to perform 2 or more actions, in succession, then we apply MP and the total count is the product of the counts obtained in the various stages. Also, we must note carefully whether *repetition* is allowed and whether *order* is to be taken into consideration.

Example 1 Find the number of 2-digit numbers which are even and have different digits.

Solution. Since the number $10x+y$ is to be even, its units digit y must be even: $0, 2, 4, 6, 8$. So, y can be chosen in 5 ways. Also, the tens digit x must be non-zero and different from the units digit. Hence we have 2 mutually exclusive cases: (a) Let $y = 0$. Then x can be chosen in 9 ways. This gives 9 numbers. (b) Let y be non-zero. Then y can be chosen in 4 ways and x can be chosen in 8 ways. This gives, by the multiplication principle, $4 \times 8 = 32$. Hence, by the addition principle, the total number of required numbers is $9 + 32 = 41$. Note that if we *first* choose x from $\{1, 2, \ldots, 9\}$, then we have to proceed differently. In fact, we then have the following 2 mutually exclusive cases: (i) x odd (ii) x even. In case (i), x can be chosen in 5 ways and y in 5 ways giving in all $5 \times 5 = 25$ numbers and in case (ii), x can be chosen in 4 ways and y in 4 ways giving in all $4 \times 4 = 16$ numbers. Hence, by the addition principle, the total number of required numbers is again $25 + 16 = 41$.

Example 2 How many numbers can be formed from some or all of the digits 2,3,4,5 if no number is to have repeated digits?

Solution. The number can be of 1, 2, 3 or 4 digits. Of these types there are respectively, 4, 4×3, $4\times3\times2$ and $4\times3\times2\times1$ numbers that can be formed from the digits 2, 3, 4, 5 without repetition. So, in all, there are $4+12+24+24 = 64$ numbers.

Example 3 A *binary word* or a *binary sequence* of length n is a sequence of length n such that each of its terms is 0 or 1.
(i) How many binary words of length n are there ?
(ii) How many binary words of length 10 begin with three 0s ? How many end with two 1s ?
Solution. (i) Each of the n terms in the word can be chosen in 2 ways: 0 or 1. Hence, by MP, there are 2^n binary words of length n.
(ii) Let A = set of binary words of length 10 which begin with three 0's and let B = set of binary words of length 10 which end with two 1's. A word in A is of the form $000-------$ where each of the 7 dashes is either 0 or 1. Hence $|A| = 2^7$. Similarly, a word in B is of the form $--------11$ where each of the 8 dashes is either 0 or 1. Hence $|B| = 2^8$.

We now state the third basic counting principle:

Bijection Principle (BP): If two finite sets S and T can be put into one-to-one correspondence with each other, then they contain the *same* number of elements, i.e. $|S| = |T|$.

Hence, the number of elements in a given finite set S can sometimes be found in the following way: discover a set T which is in one-to-one correspondence with S and the number of elements in T is known, say n. Then the number of elements in S is also n.

For example, consider an n-set $S = \{a_1, a_2, \ldots, a_n\}$. Let A be the family of all subsets of S and B the family of all binary words of length n. We define a correspondence between A and B in the following way: a subset T of S corresponds to the binary word $t = (x_1, \ldots, x_n)$ where $x_i = 1$ if a_i is in T and $x_i = 0$ if a_i is not in T. (for example, if $n = 4$, the subset $\{a_2, a_4\}$ corresponds to the binary word $(0, 1, 0, 1)$ of length 4.) Clearly, the binary word t is uniquely defined when T is given. Conversely, *every* binary word of length n uniquely corresponds to a subset of S. (For example, if $n = 5$, the binary word $(1, 0, 0, 1, 1)$ corresponds to the subset $\{a_1, a_4, a_5\}$.) Thus $T \leftrightarrow t$ is a one-to-one correspondence between the families A and B and so, by BP, $|A| = |B|$. But as seen in Example 3 (i) above, $|B| = 2^n$. Hence $|A| = 2^n$.

Note. In a standard pack of playing cards, there are 52 cards. These are divided into 4 *suits* of 13 cards each: spades (♠), hearts (♡), diamonds (♢) and clubs (♣). Each card has a *rank*. The ranks of the 13 cards in each suit are $2, 3, 4, \ldots$ 10, Jack, Queen, King and Ace. Two or more cards are said to be of the same *kind* if they are of the same rank. A *pair* is a set of two cards of the same kind (i.e. 2 twos or 2 eights or 2 kings etc.).

Exercise Set- 4.1

1. A new club flag is to be designed with 6 vertical stripes using some or all of the colours yellow, green, blue and red. In how many ways can this be done so that no two adjacent stripes have the same colour ?

2. (i) How many different five-digit numbers are there (leading zeros, e.g. 00144, not allowed) ?

   (ii) How many even 5-digit numbers are there ?

   (iii) How many 5-digit numbers are there with exactly one 3 ?

   (iv) How many 5-digit numbers are there that are the same when the order of their digits is inverted (e.g. 14341) ?

3. How many times is the digit 0 written when listing all numbers from 1 to 3333?

4. How many times is the digit 5 written when listing all numbers from 1 to 10^5 ?

5. How many non-empty collections of letters can be formed from three A's and five B's ?

6. Show that the number of ways of making a non-empty collection by choosing some or all of $n_1 + n_2 + \cdots + n_k$ objects where n_1 are alike of one kind, n_2 alike of second kind, ... ,n_k alike of k^{th} kind, is

$$(n_1 + 1)(n_2 + 1)\cdots(n_k + 1) - 1.$$

7. Show that the total number of subsets of a set S with n elements is 2^n.

8. How many positive integers are factors of 30030?

9. Let $A = \{1, 2, \ldots, m\}$ and $B = \{1, 2, \ldots, n\}$ where m, n are positive integers. How many functions are there from A to B ? How many one-one functions are there from A to B ?

10. $A = \{a_1, a_2, a_3, \ldots, a_n\}$ and $B = \{b_1, b_2\}$. Find the number of *onto* functions that can be defined from A to B.

11. How many functions are there from the set $\{1, 2, \ldots, n\}$ to the set $\{0, 1\}$ (i) that are one-to-one ? (ii) that assign 0 to both 1 and n? (iii) that assign 1 to exactly one of the positive integers $< n$?

Solutions to Exercise Set 4.1

1. Let $abcdef$ denote the 6 vertical stripes in order from the left. Then a can be of any one of the 4 colours; then b can be of any one of the *other* 3 colours; then c can be again of any one of 3 colours since the colour used for a is now available. Similarly, there are 3 possible colours for each of d, e, f. Hence, by MP, there are 4×3^5 ways of designing the flag.

2. (i) A 5-digit number is of the form $abcde$ where $a, \ldots, e$ are the digits in it and a is the *leading* digit. Now a cannot be 0 and so can be chosen in 9 ways (any one of $1, \ldots, 9$). Each of the remaining digits can be chosen in 10 ways since repetition is allowed. So, in all 9×10^4 ways.
(ii) The number $abcde$ is even if and only if the units digit e is even; so there are 5 choices for e : 0,2,4,6,8. So in all $9 \times 10^3 \times 5$ ways.
(iii) Two cases: either only $a = 3$ or exactly one of $b, c, d, e = 3$. There are 9^4 ways in the first case and $8 \times 9^3 \times 4$ in the second case (factor 4 for the 4 subcases $b = 3$ or $c = 3$ etc,); so in all $9^4 + 8 \times 9^3 \times 4$ ways.
(iv) By the given condition, the values of a, b, c fix the values of d, e : $e = a, d = b$. Hence, the number of ways is 9×10^2.

3. We are considering the integers t such that $1 \leq t \leq 3333$. Clearly, the largest number t having 0 in the units place is 3330. So there are 333 numbers t having 0 in the units place: they are $10, 20, \ldots, 3330$. We can describe these numbers as $t = x0$ where x is any one of $1, 2, \ldots 333$. Similarly, numbers $t = x0y$ i.e. numbers having 0 in the tens place are in all 33×10 because x can be any one of $1, 2, \ldots 33$ and y can be any one of $0, 1, 2, \ldots 9$. Thus there are $33 \times 10 = 330$ numbers like $x0y$. In the same way, there are $3 \times 10^2 = 300$ numbers with 0 in the hundreds place (i.e. $x0yz$ where $1 \leq x \leq 3$, $0 \leq y, z \leq 10$). Hence the total number of times 0 is written is $333 + 330 + 300 = 963$.

   [We assume in this solution that the number such as 11 is written as 11 and not as 0011.]

4. Since we are counting the occurrences of digit 5, consider integers t such that $1 \leq t \leq 10^5$. Clearly, the largest number t having 5 in the units place is 99995. So there are $1 + 9999 = 10^4$ numbers t having 5 in the units place: they are $5, 15, 25, \ldots, 99995$. We can describe these numbers as $t = x5$ where x is any one of $0, 1, 2, \ldots 9999$. Similarly, numbers $t = x5y$ i.e. numbers having 5 in the tens place are in all $(1 + 999) \times 10 = 10^4$ because x can be any one of $0, 1, 2, \ldots 999$ and y can be any one of $0, 1, 2, \ldots 9$. In the same way, there are 10^4 numbers

in each of the following cases: numbers with 5 in the hundreds place or thousands place or ten thousands place. Hence the total number of times 5 is written is $10^4 \times 5$.

5. A collection is determined once we know the number of times A occurs in it and the number of times B occurs in it. Let these numbers be i and j respectively. Then i takes values from 0 to 3 and j from 0 to 5. Hence to obtain a collection we have 4 choices for i and 6 choices for j so that there are $4 \times 6 = 24$ collections (for example, $i = 1, j = 2$ gives the collection $\{A, B, B\}$). The empty collection corresponds to letting $i = j = 0$; so that omitting this case there are $24 - 1 = 23$ non-empty collections. The next problem gives the general case of this result.

6. To make a collection we have to select a certain number of objects of each kind. Now for each value of r, $1 \leq r \leq k$, from n_r like objects we can choose $0, 1, \ldots,$ or n_r objects; i.e. there are $n_r + 1$ choices. Hence, by MP, there are in all $(n_1 + 1)(n_2 + 1) \cdots (n_k + 1)$ collections and so the number of non-empty collections is $(n_1+1)(n_2+1) \cdots (n_k+1) - 1$.

   As an application, let us answer the following question: How many different numbers can be formed by the product of two or more of the numbers 3,4,4,5,5,6,7,7,7 ? The numbers formed by products whose factors are taken from the given numbers exactly correspond with non-empty collections made from the 9 objects 3,4,4,5,5,6,7,7,7: for example, the number $4 \times 5^2 \times 7^2$ corresponds with the collection 4,5,5,7,7. Hence, by the last example, the total number of such numbers is

   $$(n_1+1) \cdots (n_k+1) - 1 = (1+1)(2+1)(2+1)(1+1)(3+1) - 1 = 143.$$

   Hence, on omitting the 9 given numbers, the numbers formed by products of *two or* more numbers are in all $143 - 9 = 134$.

7. Let $S = \{a_1, a_2, \ldots, a_n\}$. Note that we form a subset T of S, in n stages as follows: we have 2 choices for a_1 : either a_1 *is* included in T or a_1 *is not* included in T. Similarly, we have 2 choices for a_2 : either a_2 *is* included in T or a_2 *is not* included in T, etc. Finally, we have 2 choices for a_n : either a_n *is* included in T or a_n *is not* included in T. (For example, if $n = 4$, then the subset $\{a_2, a_4\}$ corresponds to the sequence of choices no, yes, no, yes.) Hence, by MP, the total number of subsets is $2 \times 2 \times \cdots \times 2$ (n factors) i.e. 2^n.

8. Here $m = 30030 = 2 \times 3 \times 5 \times 7 \times 11 \times 13$, and each prime factor occurs only once. Hence every factor of m corresponds to the product of

elements of a particular subset of the 6-set $S = \{2, 3, 5, 7, 11, 13\}$. Note that the empty subset corresponds to the factor 1. Hence the number of factors of m is equal to the number of subsets of S, namely 2^6, by the last problem.

9. A function f from A to B corresponds to the ordered set given by $(f(1), \ldots, f(m))$ of m elements where $f(i)$ is the value of f at i. Now for each i in A, $f(i)$ can be chosen in n ways from B. Hence, by the multiplication principle, there are $n \times n \times \ldots \times n$ (m factors) $= n^m$ functions from A to B.

   The number of one-one functions will be $n(n-1)\cdots(n-m+1)$. Thus, if $n < m$ then the number of one-one functions is zero and if $n \geq m$ then the number of one-one functions is $\dfrac{n!}{(n-m)!}$.

   Remark. We will obtain a formula for the number of functions from A *onto* B in §4.4 below, by using the Inclusion-Exclusion Principle. The next problem is a special case.

10. The function is to be onto B and so it must take on both the values b_1 and b_2. So there are 2 choices for the value of the function at each of the n elements of A, namely b_1 or b_2, excepting the case when all values are equal to b_1 and the case when all values are equal to b_2. Hence the number of required functions is $2^n - 2$.

11. (i) If $n = 1$, the number of one-to-one functions from A to B is 2: the function which maps 1 to 0 and the function which maps 1 to 1. If $n = 2$, the number of one-to-one functions from A to B is again 2: the function which maps 1 to 0 and 2 to 1 and the function which maps 1 to 1 and 2 to 0. If $n \geq 3$, the number of one-to-one functions from A to B is 0.
    (ii) The number of required functions is 1 if $n = 1$. If $n > 1$, it is 2^{n-2}, since $f(1) = 0$, $f(n) = 0$ and each of $f(2), \ldots, f(n-1)$ can be 0 or 1.
    (iii) The number of required functions is $2(n-1)$, since for each number $k = 1, 2, \ldots, (n-1)$, we have the function f for which $f(k) = 1$ and $f(i) = 0$ for every $i, 0 \leq i \leq (n-1), i \neq k$, and $f(n) = 0$ or 1.

4.2 Permutations - Combinations

By an r-permutation of a set $S = \{1, 2, \ldots, n\}$, we mean an ordered arrangement of r of the n elements of S in a row.

Theorem 1. The number of $r-$permutations of a set S containing n different objects is denoted by $P(n,r)$ or ${}^nP_r$ and is given by

$$ {}^nP_r = n(n-1)(n-2)\dots(n-r+1) = \frac{n!}{(n-r)!}. $$

By an r-combination of a set $S = \{1, 2, \dots, n\}$, we mean an unordered selection of r of the n elements of S.

Theorem 2. The number of r- combinations of an $n-$ element set is denoted by $\binom{n}{r}$ or ${}^nC_r$ or $C(n,r)$ and is given by

$$ {}^nC_r = \frac{n!}{r!(n-r)!}. $$

Theorem 3 (Binomial Theorem). For every positive integer n, we have

$$ \begin{aligned} (x+a)^n &= {}^nC_0x^n + {}^nC_1x^{n-1}a + {}^nC_2x^{n-2}a^2 + \\ &+ \dots + {}^nC_rx^{n-r}a^r + \dots + {}^nC_na^n. \end{aligned} \tag{1} $$

Before giving a combinatorial proof of this theorem we consider an example: To evaluate the power $(x+y)^3$ i.e. the product

$$ (x+y)(x+y)(x+y) $$

we have the following procedure:

1. Choose *one* term from *each* factor (2 choices: x or y) and multiply the 3 chosen terms together to obtain a *monomial*. For example, taking x from the first factor, y from the second factor and x from the third factor, we get the monomial xyx or x^2y. There are in all 2^3 such monomials.

2. Take the sum of all the 2^3 monomials to obtain the expansion of the above product. Thus

$$ (x+y)^3 = xxx + xxy + xyx + yxx + xyy + yxy + yyx + yyy. $$

3. Simplify the sum by pulling together the monomials which occur more than once. Thus

$$ (x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3. $$

Proof of theorem 3: To evaluate the product

$$(x+y)^n = (x+y)(x+y)\cdots(x+y) \ [n \text{ factors}]$$

we have to add the 2^n monomials obtained thus: a monomial is formed by choosing one term from each factor and multiplying them together. Now if we choose y from r of the factors and x from the remaining $n-r$ factors, then we get the monomial $x^{n-r}y^r$. Here r takes values from 0 to n to account for all possible monomials. But r of the n factors (from which we take y) can be chosen in ${}^nC_r$ ways. Hence the monomial $x^{n-r}y^r$ occurs ${}^nC_r$ times. Therefore the simplified expansion of the above product is given by

$$(x+y)^n = {}^n C_0 x^n + {}^n C_1 x^{r-1} y + \cdots + {}^n C_r x^{n-r} y^r + \cdots + {}^n C_n y^n.$$

Some properties of ${}^nC_r$ are collected in the following theorem. These can be easily proved algebraically. Here we give combinatorial proofs of properties (f) and (g).

Theorem 4. For any positive integers n, r $(r \leq n)$, we have

(a) ${}^nC_r = {}^nC_{n-r}$, if $0 \leq r \leq n$.

(b) ${}^nC_r + {}^nC_{r-1} = {}^{n+1}C_r$, if $1 \leq r \leq n$.

(c) ${}^nC_r = \frac{n}{r} \times^{n-1} C_{r-1}$, if $1 \leq r \leq n$.

(d) ${}^nC_0 + {}^nC_1 + {}^nC_2 + \ldots + {}^nC_n = 2^n$.

(e) ${}^nC_0 + {}^nC_2 + {}^nC_4 + \ldots = {}^nC_1 + {}^nC_3 + {}^nC_5 + \ldots = 2^{n-1}$.

(f) $\sum_{r=0}^{k} {}^nC_r \, {}^mC_{k-r} = {}^{m+n}C_k$.

(g) $\binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{k-m}$.

Proof: (f) This is known as Vandermonde's identity. This is obtained by counting the k-subsets of an $(m+n)$-set in two ways. Let S be an $(m+n)$-set of which m elements are red and n blue. Fix k such that $0 \leq k \leq m+n$. Then the total number of k-subsets of S is ${}^{m+n}C_k$. Now we can make a k-subset of S using any r red elements and $k-r$ blue elements where $0 \leq r \leq k$. So the total number of ways of making a k-subset with r red elements is ${}^mC_r \, {}^nC_{k-r}$. Hence the total number of k-subsets is, by addition principle, $\sum_{r=0}^{k} {}^mC_r \, {}^nC_{k-r}$. Hence (f) follows.

(g) Let S be an n-set. Consider the set T of all ordered pairs (A, B) where A is a k-subset of S and B is an m-subset of A. We prove (g) by counting the elements in T in two ways. First, set $A \subseteq S$ can be chosen in $\binom{n}{k}$ ways and set $B \subseteq A$ can be chosen in $\binom{k}{m}$ ways and so $|T| = \binom{n}{k}\binom{k}{m}$. Secondly, an m-subset B of S can be chosen in $\binom{n}{m}$ ways. For each choice of set B, choose a $(k-m)$-subset C of $S - B$ and let $A = B \cup C$. Then A is a k-subset of S and $B \subseteq A$. Thus the number of ways of choosing set A=the number of ways of choosing set C=$\binom{n-m}{k-m}$. Hence $|T| = \binom{n}{m}\binom{n-m}{k-m}$ and so (g) follows. In particular, if we take $k = r$ and $m = 1$, then we get the property (c).

Example 1 Evaluate

$$\binom{n}{0} + \binom{n}{3} + \binom{n}{6} + \cdots$$

Solution: We note that

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n.$$

Put $x = 1$,

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

Put $x = \omega = \frac{-1+i\sqrt{3}}{2}$.

$$(1+\omega)^n = \binom{n}{0} + \binom{n}{1}\omega + \binom{n}{2}\omega^2 + \cdots$$

Put $x = \omega^2 = \frac{-1-i\sqrt{3}}{2}$

$$(1+\omega^2)^n = \binom{n}{0} + \binom{n}{1}\omega^2 + \binom{n}{2}(\omega^2)^2 + \cdots$$

Adding the equations for $x = 1,\ \omega,\ \omega^2$, we get,

$$2^n + (1+w)^n + (1+w)^n = 3[\binom{n}{0} + \binom{n}{3} + \binom{n}{6} + \cdots]$$

using $1 + w + w^2 = 0$. But

$$\begin{aligned} 1 + w &= -w^2 = \frac{1 + i\sqrt{3}}{2} = \cos 60^0 + i \sin 60^0, \text{ and} \\ 1 + w^2 &= -w = \frac{1 - i\sqrt{3}}{2} = \cos 60^0 - i \sin 60^0. \end{aligned}$$

$$\begin{aligned} \text{Hence} \quad & 2^n + (1 + w)^n + (1 + w^2)^n \\ = \; & 2^n + (\cos 60^0 + i \sin 60^0)^n + (\cos 60^0 - i \sin 60^0)^n \\ = \; & 2^n + 2 \cos(n60^0) \end{aligned}$$

$$\text{But } \cos(n60^0) = \begin{cases} 1 & \text{if } n = 6k \\ \frac{1}{2} & \text{if } n = 6k \pm 1 \\ -\frac{1}{2} & \text{if } n = 6k \pm 2 \\ -1 & \text{if } n = 6k + 3. \end{cases}$$

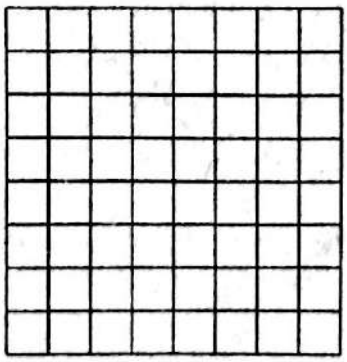
This gives

$$\binom{n}{0} + \binom{n}{3} + \binom{n}{6} + \cdots = \begin{cases} \dfrac{2^n + 2}{3} & \text{if } n = 6k, \\ \dfrac{2^n + 1}{3} & \text{if } n = 6k \pm 1 \\ \dfrac{2^n - 1}{3} & \text{if } n = 6k \pm 2. \end{cases}$$

Example 2 Given an 8×8 chessboard, (i) how many squares of all sizes are there on it ? (ii) how many rectangles of all sizes are there on it ?

Solution. (i) We count the squares according to their size. For example, on an 8×8 chessboard, there are 9 vertical lines and so there are 7 sets of 3 *successive* vertical lines, namely 123, 234, . . . , 789. Each such set gives a 2×9 strip. Each such strip contains 7 2×2 squares; the figure shows one such square. Hence there are 7^2 squares of size 2×2. Similarly,there are 8^2 squares of size 1×1, 6^2 squares of size 3×3 etc. Hence the total number of squares is

$$8^2 + 7^2 + \cdots + 1^2 = 204.$$



Now let us consider an $n \times n$ chessboard. For $r = 1, 2, \ldots, n+1$, there are $n-(r-1)$ sets of $r+1$ *successive* vertical lines, namely. For *any* such $r+1$-set, there are $n-(r-1)$ sets of $r+1$ successive horizontal lines, giving $n-(r-1)$ squares of size $r \times r$. Hence, by MP, there are in all $[n-(r-1)]^2$ squares of size $r \times r$. Thus the total number of squares is

$$\sum_{r=1}^{n}[n-(r-1)]^2 = \frac{1}{6}n(n+1)(2n+1).$$

(ii) Similarly, for $r = 1, 2, \ldots, n+1$, there are $n-(r-1)$ sets of $r+1$ successive vertical lines. For *any* such $r+1$-set, there are $n-(s-1)$ sets of $s+1$ successive horizontal lines, giving $n-(r-1) \times n-(s-1)$ rectangles of size $r \times s$. Hence, by MP, there are in all $[n-(r-1)][n-(s-1)]$ squares of size $r \times s$. Thus the total number of rectangles is

$$\sum_{s=1}^{n}\sum_{r=1}^{n}[n-(r-1)][n-(s-1)] = \frac{1}{4}n^2(n+1)^2.$$

Example 3 How many 7−digit numbers are there such that the digits are distinct integers taken from the set $S = \{1, 2, \ldots, 9\}$ and such that the integers 5 and 6 do not appear consecutively in either order ?

Solution. We first find the number n_1 of 7−permutations of the 9-element set S which do contain 56 or 65. Consider 7 places as follows:

$$\cdot \quad a \quad b \quad c \quad d \quad e \quad f \quad g$$

There are 6 pairs of *consecutive* places, namely ab, bc, $\ldots$, fg in which we can place 56 or 65. Thus each of 56 and 65 can be placed in 6 ways. In each case there are P_5^7 ways of filling the remaining 5 places. Hence $n_1 = 2 \times 6 \times P_5^7$. Also, the number of 7-permutations of S is $n_2 = P_7^9$. So the number of required permutations is $n_2 - n_1 = 151200$.

Example 4 In a group of 15 boys, there are 7 scout-boys. In how many ways can 12 boys be selected so as to include (i) exactly 6 scout-boys (ii) at least 6 scout-boys?

Solution. (i) (a) 6 scout-boys out of 7 can be chosen in ${}^7C_6$ ways and (b) 6 other boys out of 8 others can be chosen in ${}^8C_6$ ways. Now any 6-combination from (a) can be combined with any 6-combination from (b) to make a required type of group of 12 boys. So, by MP, the total number of ways is ${}^7C_6 \times {}^8C_6 = 196$.

(ii) The 12-combination can include either 6 or 7 scout-boys. As in (i), there are ${}^7C_6 \times {}^8C_6$ 12-combinations with exactly 6 scout-boys. Also, if we include all the 7 scout-boys, then the remaining 5 boys can be chosen from the other 8 boys in ${}^8C_5$ ways. So there are ${}^8C_5$ 12-combinations with exactly 7 scout-boys. Hence, by AP, the total number of ways is ${}^7C_6 \times {}^8C_6 + {}^8C_5$.

Example 5 Suppose n is a positive integer and let $S = \{1, 2, \ldots, n\}$. Find the number of ordered pairs (A, B), where A and B are subsets of S, in the following cases.
(i) A is a subset of B (ii) A is a proper subset of B.

Solution. (i) To get a pair (A, B) with $A \subseteq B$, every element x of S must be treated in one of the following *three* ways:
(a) x is put in both A and B
(b) x is put in B but not in A
(c) x is put in neither of A, B.
Hence, as there are n elements in S, the number of pairs of subsets, (A, B), with $A \subseteq B$ is, by MP, 3^n.
(ii) The number of pairs (A, B), with $A = B$ is the number of subsets of S and is therefore $= 2^n$. Hence the number of pairs (A, B), where A is a proper subset of B, is $3^n - 2^n$.

Second solution for (i): For a given r, $0 \leq r \leq n$, a subset B with r elements can be chosen in ${}^nC_r$ ways. For each such B, a subset A of B can be chosen 2^r ways. Hence, for r-element subsets B, there are ${}^nC_r \cdot 2^r$ pairs (A, B), $A \subseteq B$. Hence the total number of pairs is

$$\sum_{r=0}^{n} {}^nC_r \cdot 2^r = (2+1)^n = 3^n,$$

using the binomial theorem.

Second solution for (ii): For a given r, $0 \leq r \leq n$, a subset B with r elements can be chosen in ${}^nC_r$ ways. For each such B, a subset A of B can be chosen $2^r - 1$ ways. Hence, for r-element subsets B, there are ${}^nC_r \cdot (2^r - 1)$ pairs (A, B), $A \subseteq B$. Hence the total number of pairs is

$$\sum_{r=0}^{n} {}^nC_r \cdot (2^r - 1) = (2+1)^n - 2^n = 3^n = 2^n.$$

Example 6 In how many ways can $2n$ players be grouped into n tennis pairs?

Solution. Here we want to *partition* a set S of $2n$ elements into n 2-element subsets (i.e. these n 2-element subsets are pairwise disjoint and their union is S). For example, let $n = 5$ and $S = \{a_1, a_2, \ldots, a_{10}\}$. Then one possible partition or *pairing* is

$$P : p_1 = (a_1, a_3),\ p_2 = (a_2, a_5),\ p_3 = (a_4, a_7),$$
$$p_4 = (a_6, a_9),\ p_5 = (a_8, a_{10}).$$

To find the number of all possible parings, note that first, 2 players can be chosen out of $2n$ in ${}^{2n}C_2$ ways. After that 2 players can be chosen from the remaining $2n-2$ players in ${}^{2n-2}C_2$ ways, etc. Continuing in this manner, after $n-1$ steps, 2 players remain and of these 2 can be chosen in ${}^{2}C_2$ ways. Also, the *order* in which the n pairs are chosen is not important. So the total number N of ways of obtaining n pairs is the product of above n numbers divided by $n!$ i.e.

$$\begin{aligned} N &= [{}^{2n}C_2 \cdot {}^{2n-2}C_2 \cdots {}^{4}C_2 \cdot {}^{2}C_2]/n! \\ &= \frac{(2n)(2n-1)}{2} \cdot \frac{(2n-2)(2n-3)}{2} \cdots \frac{4 \cdot 3}{2} \cdot \frac{2 \cdot 1}{2} \cdot \frac{1}{n!} \\ &= (2n-1)(2n-3) \cdots 3 \cdot 1. \end{aligned}$$

Example 7 (a) Ten boys are to be grouped into 5 tennis pairs. In how many ways can this be done ? (b) The same 10 boys are going to 5 seaside places A,B,C,D,E, two to each place. In how many ways can this be done ? Explain the difference between your answers.

Solution. The difference between (a) and (b) is this: In (a), only the pairings are important; not the order in which the pairs occur in a pairing. But in (b), for each pairing, such as P in the last example, the order in which the pairs of boys are sent to 5 places A,...,E makes a difference. Hence for (a) the answer is, by the last example, $n = 9 \times 7 \times 5 \times 3 \times 1 = 945$. But for (b), the number n must be multiplied by 5! since each pairing corresponds to 5! different ways of visiting the 5 places. So the answer is $n \times 5! = 945 \times 5! = 113400$.

Circular permutations

By a *circular permutation* of the set $S = \{1, 2, \ldots, n\}$, we mean an ordered arrangement of the n elements of S around a circle.

Theorem 5. The number of distinct circular permutations of n different objects is $(n-1)!$.

Corollary: Let $n \geq 3$ be a positive integer. The number of different circular necklaces that can be made from n different beads is $\frac{1}{2}[(n-1)!]$.

Example 8 There are 8 persons.
(i) In how many ways can they be seated at a round table ?
(ii) With the further condition that 2 of them, a and b, must not sit in adjacent seats ?
(iii) If 4 of the persons are men and 4 ladies and if no two men are to be in adjacent seats ?
(iv) If the 8 persons are 4 married couples and if no husband and wife, as well as no two men, are to be in adjacent seats ?

Solution. (i) The number of ways is $(8-1)! = 7!$ by theorem 5 above.
(ii) Regard a, b as one person: ab or ba. Then in each of these cases we are to seat 7 persons round the table and this can be done in $(7-1)! = 6!$ ways. Hence a, b are seated *together* in $2 \times 6!$ arrangements. Hence the number of arrangements in which they are *not* together is $7! - (2 \times 6!)$.
(iii) The 4 ladies can be seated in 3! ways. There are 4 places between the successive ladies and for each arrangement of the ladies the men can be seated in these 4 places in 4! ways. So the total number of required ways is $3! \times 4!$.
(iv) The 4 wives can be seated in 3! ways. There are 4 places between the successive wives and for each arrangement of the wives the men can be seated in these 4 places in exactly 2 ways counterclockwise:

$$w_1, m_4, w_2, m_1, w_3, m_2, w_4, m_3, \quad w_1, m_3, w_2 m_4, w_3, m_1, w_4, m_2.$$

So the answer is 12.

Exercise 4.2

1. How many ways can 12 identical white and 12 identical black pawns be placed on the black squares of an 8×8 chessboard ?
2. How many ways are there to place 2 identical rooks in a common row or column of an 8×8 chessboard ?
3. How many ways are there to place 2 identical kings on an 8×8 chessboard so that the kings are not in adjacent squares ? On an $n \times m$ chessboard ?
4. How many necklaces can be made using 7 beads of which 5 are identical red beads and 2 are identical blue beads ?
5. There are 12 members in a committee who sit around a table. There is one place specially designated for the chairman. Besides the chairman there are 3 people who constitute a subcommittee. Find the number of

seating arrangements if (i) the subcommittee sit together as a block, and (ii) no 2 of the subcommittee sit next to each other.

6. Prove that the number of ways of arranging p 1's and q 0's in a line such that no two 1's are adjacent is $\binom{q+1}{p}$.

7. Prove that the number of r-subsets of the set $S = \{1, 2, \ldots, n\}$ that do not contain a pair of consecutive integers is $\binom{n-r+1}{r}$.

Hints and Answers to Exercise Set 4.2

1. There are 32 black squares and of these 12 can be chosen to put the 12 white pawns in $\binom{32}{12}$ ways. Then out of the remaining 20 black squares 12 can be chosen to put the 12 black pawns in $\binom{20}{12}$ ways. So the answer is $\binom{32}{12} \times \binom{20}{12}$.

2. Since the 2 rooks are identical, the order in which they are placed in a row (or column) is not important. First a row can be chosen in 8 ways. In any row, 2 of the 8 squares can be chosen in ${}^8C_2$ ways. Hence the 2 rooks can be placed in a row in $8 \times {}^8C_2$ ways. Similarly, 2 rooks can be placed in a column in $8 \times {}^8C_2$ ways. So the total number is $2 \times 8 \times {}^8C_2$. For an $n \times m$ board the answer is $n \times {}^mC_2 + m \times {}^nC_2$.

3. A row can be chosen in 8 ways. In a row, there are in all ${}^8C_2$ pairs of squares of which 7 are pairs of *adjacent* squares. So there are $[{}^8C_2 - 7]$ pairs of places in any of which the two identical kings can be placed. Hence the kings can be placed in a row in $8 \times [{}^8C_2 - 7]$ ways and in the same number of ways in a column. So the total number of ways is $2 \times 8 \times [{}^8C_2 - 7]$. For an $n \times m$ board, the number is

$$n[{}^mC_2 - (m-1)] + m[{}^nC_2 - (n-1)].$$

4. The different necklaces are determined by the number of red beads *between* the two blue beads, taking both arcs into consideration. So there are exactly 3 distinct necklaces:

$$bbrrrrr, \quad brbrrrr, \quad brrbrrr.$$

5. Ans: (i) $9! \times 3!$ (ii) $8! \times {}^9P_3$.

6. There are $q+1$ places between the q 0's (namely, $q-1$ places between the q successive 0's and 2 places at the ends). The required arrangements are obtained by putting the p 1's in p of these $q+1$ places; and this can be done in $\binom{q+1}{p}$ ways.

7. An r-subset T of S corresponds, in a one-to-one way, to an arrangement $a_1, a_2, \ldots, a_n$ of r 1's and $n-r$ 0's in a row as follows: $a_i = 1$ if $i \in T$ and $a_i = 0$ if $i \notin T$. Hence the r-subsets of $S = \{1, 2, \ldots, n\}$ that do not contain a pair of consecutive integers exactly correspond to the arrangements of r 1's and $n-r$ 0's in a line such that no two 1's are adjacent. Hence, by the last problem, the number of required r-subsets is $\binom{n-r+1}{r}$.

4.2.1 Permutations with repetitions:

Theorem 6. Suppose there are n objects, of which n_1 are identical of first type, n_2 are identical of second type, $\ldots$, n_k are identical of k^{th} type so that $n = n_1 + n_2 + \ldots + n_k$. Then the number of permutations of these n objects, taken all at a time, is denoted by $P(n; n_1, n_2, \ldots, n_k)$ and is given by

$$P(n; n_1, n_2, \ldots n_k) = \frac{n!}{n_1! n_2! \ldots n_k!}.$$

Combinations with repetitions:

Suppose $S = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$ is a set containing 7 different objects. Then a 5-combination of S, with repetitions allowed, is $t = a_2a_2a_2a_5a_7$. To count the number of such 5-combinations of S, note first that each combination uniquely corresponds to a table with $7 - 1 = 6$ columns in which 5 dots have been placed in the columns. Thus the combination t corresponds to the table

a_1	a_2	a_3	a_4	a_5	a_6	a_7
	•••			•		•

Also, each such table uniquely corresponds to a permutation of 6 vertical lines and 5 dots. Thus the combination t corresponds to the permutation $|•••|||•||•$.

Conversely, every such permutation (say, $•||••|||•|•$) uniquely corresponds to a table of the type described above (namely,

a_1	a_2	a_3	a_4	a_5	a_6	a_7
•		••			•	•

in this case) which in turn uniquely corresponds to a 5-combination with repetitions (namely, $a_1a_3a_3a_6a_7$, in this case).

Now there are $\frac{(6+5)!}{6!5!} = \binom{11}{6} = \binom{7-1+5}{6}$ permutations of 6 vertical lines and 5 dots.

Hence the number of 5-combinations of S, with repetitions allowed, is the same as the number of such permutations, and so it is $\binom{7-1+5}{6}$.

More generally, the same method of proof can be used to obtain the following

Theorem 7. Let S be a set having n different objects. Then the number of $r-$combinations of S, with repetitions allowed, is $\binom{n-1+r}{r}$.

Corollary 1. Let n, r be given positive integers. Then the number $A_{n,r}$ of *non-negative integer* solutions $(x_1, x_2, \ldots, x_n)$ of the equation

$$x_1 + x_2 + \cdots + x_n = r, \tag{1}$$

is $\binom{n-1+r}{r}$.

Proof. Let $S = \{a_1, \ldots, a_n\}$ be a set with n distinct elements. Given any r-combination t of S, with repetitions allowed, (say, $t = a_2a_2a_2a_5a_7$, $n = 7, r = 5$) let x_i be the number of times a_i occurs in t. Then t corresponds to the solution $(x_1, x_2, \ldots, x_n)$ of equation (1) in non-negative integers.
(Thus the above 5-combination $t = a_2a_2a_2a_5a_7$ corresponds to the solution $(0, 3, 0, 0, 1, 0, 1)$ of the equation $x_1 + x_2 + \cdots + x_7 = 5$).

Conversely, every non-negative integer solution of (1) corresponds to a unique r-combination of S, with repetitions allowed. Hence, by the above theorem, $A_{n,r} = \binom{n-1+r}{r}$.

Corollary 2. Let $r \geq n > 0$ be integers. The number $B_{n,r}$ of solutions $(x_1, x_2, \ldots, x_n)$ of equation (1) in *positive integers* is $\binom{r-1}{n-1}$.

Proof. Given any solution $(y_1, \ldots, y_n)$ of (1) in positive integers, let $x_i = y_i - 1$. Then substituting in (1), we get

$$x_1 + \ldots + x_n = y_1 + \ldots + y_n - n = r - n, \tag{2}$$

so that $(x_1, x_2, \ldots, x_n)$ is a non-negative integer solution of (2). Conversely, every non-negative integer solution of (2) corresponds to a unique

positive integer solution $(y_1, \ldots, y_n)$ of (1) with $y_i = x_i + 1$. Hence,

$$B_{n,r} = \binom{n-1+r-n}{r-n} = \binom{r-1}{n-1}.$$

Corollary 3. Let $r, n > 0$ be integers. Let $a_1, \ldots, a_n$ be given integers. Then the number of integer solutions of equation (1) such that $x_i > a_i$, $1 \leq i \leq n$, is $\binom{r-a_1-\cdots-a_n-1}{n-1}$.

Proof. Given any solution $(y_1, \ldots, y_n)$ of (1) in integers, such that $y_i > a_i$, $1 \leq i \leq n$, so that $y_1 + \ldots + y_n = r$. Let $x_i = y_i - a_i$. Then substituting for y's we get

$$x_1 + \ldots x_n = r - (a_1 + \cdots a_n),$$

so that $(x_1, x_2, \ldots, x_n)$ is a positive integer solution of the last equatio conversely. So, the number of required solutions is $\binom{r-a_1-\cdots-a_n-1}{n-1}$.

Example 9 If n identical dice are rolled, how many different outcomes can be recorded ?

Solution. Since the dice are identical, the order in which the n scores appear is not important. So we want the number of n-combinations, with repetition, of the set $\{1, 2, 3, 4, 5, 6\}$ and it is $\binom{6-1+n}{n}$.

Example 10 A shop sells 6 different flavours of ice-cream. In how many ways can a customer choose 4 ice-cream cones if
(i) they are all of different flavours;
(ii) they are not necessarily of different flavours;
(iii) they contain only 3 different flavours;
(iv) they contain only 2 or 3 different flavours?

Solution. Let the flavours be denoted by a, b, c, d, e and f.
(i) Here we want the number of ways of choosing 4 ice-cream cones of *different* flavours from cones of 6 *different* flavours. That is, we want the number of 4-combinations of 6 distinct objects without repetition. So the number is $\binom{6}{4} = 15$.
(ii) By theorem 1, the number of 4-combinations of 6 objects a, b, c, d, e, f, with repetitions allowed, is $\binom{6-1+4}{4} = \binom{9}{4} = 126$.
(iii) The number of ways of choosing 4 cones of exactly 3 different flavours, with repetitions = (the number of ways of choosing 3 flavours out of 6)×(the

number of ways of choosing 4 cones of 3 chosen flavours) $= \binom{6}{3} \times 3 = 60$, because there are $\binom{6}{3}$ ways of choosing 3 flavours out of 6 and for each choice, say a, b, c, there are 3 ways of choosing 4 cones of the 3 chosen flavours, namely a, b, c, c or a, b, b, c or a, a, b, c.
(iv) As in (iii), the number of ways of choosing 4 cones of exactly 2 different flavours, with repetitions $= \binom{6}{2} \times 3 = 45$, because for each choice of 2 flavours, say a, b, there are 3 ways of choosing 4 cones of the 2 chosen flavours, namely a, a, a, b or a, a, b, b or a, b, b, b. Hence the ways of choosing cones of 2 or 3 flavours are in all $60 + 45 = 105$. *Alternatively*, the number of ways of choosing 4 cones of only 2 or 3 different flavours, with repetitions allowed = the number of ways of choosing 4 cones, with repetitions allowed, when 6 flavours are available $-$[(the number of ways of choosing 4 cones of only 1 flavour) + (number of ways of choosing 4 cones of 4 different flavours]$= 126 - (6 + 15) = 105$, because there are 6 ways of choosing 4 cones of only 1 flavour, namely *aaaa*, *bbbb*, etc.

Example 11 Given integers $1, 2, \ldots, 11$, two groups (not necessarily disjoint) are selected; the first group contains 5 integers and the second group contains 2 integers. In how many ways, allowing repetitions, can the selection be made if
(i) there are no further conditions ?
(ii) each group contains either all odd integers or all even integers ?

Solution. (i) The first group G_1 of 5 integers from the 11 integers can be chosen in $\binom{11-1+5}{5} = \binom{15}{5}$ ways. Similarly, the group G_2 of 2 integers from the 11 integers can be chosen in $\binom{11-1+2}{2} = \binom{12}{2}$ ways. Therefore the two groups G_1 and G_2 can be chosen in $\binom{15}{5} \times \binom{12}{2}$ ways.
(ii) We have 4 mutually exclusive cases: (a) G_1 all odd, G_2 all even
(b) G_1 all odd, G_2 all odd (c) G_1 all even, G_2 all odd (d) G_1 all even, G_2 all even. Hence the total number of ways is

$$\binom{10}{5}\binom{6}{2} + \binom{10}{5}\binom{7}{2} + \binom{9}{5}\binom{7}{2} + \binom{9}{5}\binom{6}{2}.$$

Example 12 Find the number of non-negative integer solutions of the equation $x_1 + x_2 + x_3 = 15$ subject to the given conditions.
(i) $x_1 \geq 0,\ x_2 \geq 0,\ x_3 \geq 0$
(ii) $x_1 > 0,\ x_2 > 0,\ x_3 > 0$
(iii) $x_1 \geq 3,\ x_2 \geq 2,\ x_3 \geq 7$.

Solution. (i) By theorem 1, the required number is $\binom{3-1+15}{15} = 136$. (ii) By corollary 1 above the required number is $\binom{15-1}{3-1} = 91$. (iii) If (y_1, y_2, y_3) is

a solution of the required type, let $x_1 = y_1 - 3$, $x_2 = y_2 - 2$, $x_3 = y_3 - 7$. Then (x_1, x_2, x_3) is a non-negative integer solution of $x_1 + x_2 + x_3 = 15 - (3 + 2 + 7) = 3$. So the required solutions are in all $\binom{3-1+3}{3} = 10$.

Example 13 Find the number of integer solutions of $x_1 + x_2 + x_3 + x_4 = 48$ with the conditions $x_1 > 5$, $x_2 > 6$, $x_3 > 7$, $x_4 > 8$.

Solution. If $y_1, \ldots, y_4$ is a solution of the required type, put $x_1 = y_1 - 5, x_2 = y_2 - 6, x_3 = y_3 - 7$ and $x_4 = y_4 - 8$. Then $y_1 + \cdots + y_4 = 48$ becomes $x_1 + \cdots + x_4 = 48 - 26 = 22$ and we want positive integer solutions. So the number of solutions is $\binom{22-1}{4-1}$.

Example 14 Find the number of isosceles triangles with integer sides if no side exceeds 1994.

Solution. Let the sides of the isosceles triangle be a, a, b. There will such a unique triangle if and only if $2a > b$. Hence, for any a, b can vary from 1 to $2a - 1$. We have additional restrictions: $a \leq 1994$ and $b \leq 1994$.
(i) If $a \leq \frac{1994}{2} = 997, b$ varies from 1 to $2a - 1$, i.e. b can take $2a - 1$ values. Hence the number of isosceles triangles obtained is the sum of the first 997 odd natural numbers which equals $(997)^2$.

(ii) If $998 \leq a \leq 1994, b$ can take any value between 1 and 1994, i.e. there are 1994 choices for b. In this case a has 997 possibilities. So the number of isosceles triangle s in this case is
$997 \times 1994 = 2 \times (997)^2$. The total numbers of isosceles triangles is thus $3 \times (997)^2 = 3 \times 994009 = 2982027$.
(Note: $(997)^2 = (10^3 - 3)^2 = 10^6 - 6 \times 10^3 + 9 = 1000009 - 6000 = 994009$.)

Example 15 How many ways are there to split a group of $2n$ α s, $2n$ β s, and $2n$ γ s in half (into two groups of $3n$ letters)?

Solution. Count the ways to select $3n$ letters from the 3 types of letters and then subtract outcomes with $2n+1$ or more of one letter $-C(3n+3-1, 3n) - 3 \times C((n-1)+3-1, n-1)$. Since each split forms two groups of $3n$ letters, it appears we should divide this count of $3n$-letter groups by 2. However, the split in which each group consists on n letters of each type contains two copies of the same group (this split is not double counted). So the answer is $\frac{1}{2}[C(3n+3-11, 3n) - 3 \times C((n-1)+3-1, n-4) - 1] + 1$.

Exercise Set- 4.3

1. Find the number of arrangements of any 3 letters from the 11 letters of the word *combination*.

2. Find the number of integer solutions of the given equation with given conditions.
   (i) $x+y+z=7;\ x>0, y>0, z>0$
   (ii) $x+y+z=9;\ x\geq 0, y\geq 0, z\geq 0$
   (iii) $x+y+z=24;\ x>1, y>1, z>1$
   (iv) $x+y+z=24;\ x>1, y>2, z>3$
   (v) $x+y+z+t+w=36;\ x, y, z, t, w\geq 0$

3. Show that the equations $x_1+\cdots+x_7=13$ and $x_1+\cdots+x_{14}=6$ have the same number of non-negative integer solutions.

4. Show that the equations $x_1+x_2+x_3=12$ and $x_1+\cdots+x_{10}=12$ have the same number of positive integer solutions.

5. How many integers between 100 and 1,000,000 have sum of digits (a) equal to 5 (b) less than 5 ?

6. How many different collections of 3 coins can be formed if the coins can be pennies, nickels, dimes, quarters or half-dollars ? How many different collections of 5 coins can be formed with the same types of coins ?

7. Find the number of integer solutions of the given equation with given conditions.
   (i) $x+y+z+w=40;\ x, y, z, w>5$
   (ii) $x_1+\cdots+x_6=72;$
   (a) $x_i>0, x_1>10$ (b) $x_i>0, x_1>10, x_5>5$
   (iii) $x+y+z=1;\ x>-5, y>-5, z>-5.$

8. How many ways are there to invite 1 of 3 friends over for dinner on 6 successive nights such that no friend is invited more than 3 times ?

Solutions to Exercise Set- 4.3

1. $3\times 21 +^8 P_3$.

2. (i) $\binom{7-1}{3-1}=15$. (ii) $\binom{3-1+9}{9}=55$. (iii) Put $X=x-1$ etc. Then the equation becomes $X+Y+Z+3=24$ or $X+Y+Z=21$. Hence the number of solutions is $\binom{21-1}{3-1}=190$. (iv) $\binom{3-1+15}{3-1}$. (v) $\binom{5-1+36}{5-1}$.

5. (a) Let $x_i, 1\leq i\leq 6$, be the digits of a number with at most 6 digits. Then the number of non-negative integer solutions of $x_1+\cdots+x_6=5$ is $\binom{6-1+5}{5}=252$. But the number is to be >100. So the 6 numbers 5,14,41,23,32,50 are to be omitted. Thus the required number is $252-6=246$. (b) For $1\leq k\leq 4$, the number of non-negative integer solutions of $x_1+\cdots+x_6=5-k$ is $\binom{6-1+5-k}{5-k}=\binom{10-k}{5}$. Again we have to omit the

15 numbers 1,10,2,20,11,3,30,12,21,4,40,13,31,22,100, and so the answer is $[\sum_{k=0}^{4} \binom{10-k}{5}] - 15 = 194$.

6. Let x, y, z, t, w respectively denote the numbers of coins of given types to form a collection of 3 coins. Then the required number is the number of non-negative integer solutions of $x + y + z + t + w = 3$ which is $\binom{5-1+3}{3} = 35$. Second part: $\binom{5-1+5}{5} = 126$.

7. (i) Put $x = a + 5$, etc. so that the equation becomes $a + b + c + d = 20$ and its positive integer solutions are in all $\binom{20-1}{4-1} = 969$. (ii) (a) Put $x_1 = x_1' + 10$ so that the equation becomes $x_1' + x_2 + \cdots + x_6 = 62$ and its positive integer solutions are in all $\binom{62-1}{6-1}$. (b) $\binom{57-1}{6-1}$. (iii) 105.

8. Let x, y, z be the friends and let (a, b, c) denote the case where x is invited a times, y b times and z c times. For example, one possible arrangement corresponding to the triplet $(3, 2, 1)$ is

$$x, x, y, x, y, z$$

Then we have the following possibilities: (i) $(a, b, c) = (1, 2, 3);\ (1, 3, 2);\ (2, 3, 1);\ (2, 1, 3);\ (3, 1, 2);\ (3, 2, 1)$. (ii) $(a, b, c) = (3, 3, 0);\ (3, 0, 3);\ (0, 3, 3)$. (iii) $(a, b, c) = (2, 2, 2)$. So the total number of ways is

$$6 \times 6!/1!2!3! + 3 \times 6!/3!3! + 6!/2!2!2!.$$

4.3 The Pigeonhole Principle

The **pigeonhole principle (PP)**, also called **Dirichlet's box principle**, states that if more than n objects are distributed into n boxes, then at least one box must receive more than one object. We will abbreviate this as (PP1).

Second form of the pigeonhole principle (PP2): For any positive integers n, t, if $tn + 1$ or more objects are placed in n boxes, then at least one box will contain *more* than t objects.

Third form of the pigeonhole principle (PP3): If the average of n positive numbers is t, then at least one of the numbers is greater than or equal to t. Further, at least one of the numbers is less than or equal to t.

Proof: Let $a_1, a_2, \ldots, a_n$ be the numbers. Then by data,

$$\frac{a_1 + \cdots + a_n}{n} = t \text{ so that } a_1 + \cdots + a_n = tn. \tag{3}$$

Hence if each of the n numbers $a_1, \ldots, a_n$ is less than t, then the sum of these numbers would be less that nt, contradicting (4).

A similar argument shows that at least one of the numbers is less than or equal to t.

Remark: If the numbers $a_1, a_2, \ldots, a_n$ are *integers*, then PP3 says that at least one of them is $\geq t_0$, where t_0 is the smallest integer not less than t; and at least one is $\leq [t]$ where $[t]$ is the integral part of t.

Strong form of the pigeonhole principle: Let $q_1, q_2, \ldots, q_n$ be positive integers. If $(q_1 + q_2 + \ldots + q_n - n + 1)$ objects are put into n boxes, then either the first box contains at least q_1 objects or the second box contains at least q_2 objects,...,or the nth box contains at least q_n objects.

We will abbreviate this form as (PP4).

Proof. Suppose we distribute $(q_1 + q_2 + \ldots + q_n - n + 1)$ objects in n boxes and if for each $i = 1, 2, \ldots, n$, the ith box contains less than q_i objects, then the total number of objects in the n boxes is

$$\leq (q_1 - 1) + (q_2 - 1) + \ldots + (q_n - 1) = q_1 + q_2 + \ldots + q_n - n.$$

But this number is less than the number of objects placed in the n boxes. Hence, for at least one i, ith box must contain at least q_i objects,

Solutions to the following problems use this principle as the key-step in the argument.

Examples

1. Given m integers $a_1, a_2, \ldots, a_m$, show that there exist integers k, s with $0 \leq k < s \leq m$ such that $a_{k+1} + a_{k+2} + \ldots + a_s$ is divisible by m.
2. Among the integers 1,2, ..., 200, if 101 integers are chosen then show that there are two among the chosen, such that one is divisible by the other.
3. Prove that if 100 integers are chosen from the set $1, 2, \cdots, 200$ such that atleast one of them is smaller than 15, then there exist two of the chosen integers such that one divides the other.
4. Suppose numbers 1 to 20 are placed in any order around a circle. Show that

   (i) the sum of some 3 consecutive numbers must be at least 32

   (ii) the sum of some 4 consecutive numbers must be at least 42.
5. A storekeeper's list consists of 115 items, each marked "available" or "unavailable". There are 60 available items. Show that there are at least 2 *available* items in the list exactly 4 items apart.
   (For example, available items at positions 5 and 9 or at positions 36 and 40 satisfy the condition.)

6. A chess master who has 11 weeks to prepare for a tournament decides to play at least one game every day, but not more than 12 games during a week. Show that there exists a succession of days during which the chess master will have played exactly 21 games.

7. Prove that if in a group of 6 persons, each pair is either of mutual friends or mutual enemies, then there are either three mutual friends or three mutual enemies. Also show that the result is not true in case of a group of 5 persons.

8. Let $\langle a_1, a_2, \ldots, a_{1995} \rangle$ be a sequence of positive integers whose sum is 3989. Show that there is a block of r successive a_i's ($r \geq 1$) whose sum is 95.

9. Let (x_i, y_i), $1 \leq i \leq 5$, be a set of five distinct points with integer co-ordinates in the x-y plane. Show that the mid-point of the line joining at least one pair of these points has integer co-ordinates.

10. Let $a_1, a_2, \ldots, a_{100}$ and $b_1, b_2, \ldots, b_{100}$ be any two permutations of the integers from 1 to 100. Prove that among the hundred products

$$a_1b_1, a_2b_2, \ldots, a_{100}b_{100},$$

there are two products whose difference is divisible by 100.

11. Prove that no 7 integers, not exceeding 24, can have sums of all subsets different.

Solutions

1. Consider the sequence $a_1, a_1 + a_2, \ldots, a_1 + a_2 + \ldots + a_m$. If anyone of these m sums is divisible by m then we are through. Otherwise, suppose that none of them is divisible by m. So each leaves a non-zero remainder $1, 2, \ldots, (m-1)$. Since there are m sums and $(m-1)$ possible values of the remainders, by the pigeonhole principle two of the sums leave the same remainder after division by m. So let

$$\begin{aligned} & a_1 + a_2 + \ldots + a_k = bm + r \\ \text{and} \quad & a_1 + a_2 + \ldots + a_s = cm + r. \end{aligned}$$

This gives (if $k < s$), $a_{k+1} + a_{k+2} + \ldots + a_s = m(c - b)$. Thus m divides $a_{k+1} + a_{k+2} + \ldots + a_s$.

2. Let the 101 integers chosen among 1,2, ..., 200 be written as $m_i = 2^{k(i)}a_i$ for $i = 1, 2, \ldots, 101$, where a_i is an odd number which is the *greatest* odd divisor of m_i and it is one of the 100 odd numbers 1,3,5, ..., 199. Thus by pigeonhole principle, among the chosen 101 numbers m_i, at least two have equal odd parts after removing the power of 2. Thus let $m_t = 2^{k(t)} \cdot a_t$ and $m_s = 2^{k(s)}a_s$ with $a_t = a_s$. Then if $k(t) < k(s)$ then m_t divides m_s and if $k(t) > k(s)$ then m_s divides m_t

3. Let us suppose that we have chosen 100 positive integers, not exceeding 200, none of which is divisible by any other. Let us prove that none of the numbers from 1 to 15 is contained among these 100 numbers.

   Let us consider all the *greatest* odd divisors of the chosen numbers (as in the last example). It is obvious that these divisors form the set of all odd numbers not exceeding 200. In particular, these odd divisors include the numbers 1,3,9,27,81. Since among the numbers corresponding to these odd divisors there are no two numbers one of which is divisible by the other, the number containing the odd factor 27 must be divisible by a power of 2 whose exponent is atleast 1,the number containing the odd factor 9 must be divisible by a power of 2 whose exponent is atleast 2, the number containing the odd factor 3 must be divisible by a power of 2 whose exponent is atleast 3, the number containing the odd factor 1 must be divisible by a power of 2 whose exponent is atleast 4. This means that the numbers 1, $2 = 1 \cdot 2$, 3, $4 = 1 \cdot 2^2$, $6 = 2 \cdot 3$, $8 = 1 \cdot 2^3$, 9 and $12 = 3 \cdot 2^2$ are not contained among the 100 chosen numbers.

   In just the same way we can consider those of the given numbers whose greatest odd divisors are 5, 15 and 45 and prove that the given numbers do not contain 5, $10 = 5 \cdot 2$ and 15. Similarly, if we consider the numbers 7, 21 and 63 we can show that the numbers 7 and 14 are not among the 100 chosen integers; while if we consider the numbers 11 and 33, we can show that 11 is not among the 100 chosen integers and if we consider the numbers 13 and 39, we can show that 13 is not among the 100 chosen integers.

4. (i) Let $a_1, \ldots, a_{20}$ be the numbers placed around the circle. Since the mean of the 20 sums of 3 consecutive numbers, namely $a_1+a_2+a_3$, $a_2+a_3+a_4$, $\ldots, a_{19}+a_{20}+a_1$, $a_{20}+a_1+a_2$ is

$$\frac{1}{20}[3(a_1 + a_2 + \cdots + a_{20})] = \frac{3(20)(21)}{2(20)} = 31 \cdot 5,$$

   we see by PP3, that at least one of the sums must be ≥ 32. A similar proof holds for (ii).

5. Let the positions of the available items be $a_1, a_2, \ldots, a_{60}$. Since $a_{60} \leq 115$, we see that the 120 numbers

$$a_1 < a_2 < \cdots < a_{60}$$

$$\text{and } a_1 + 4 < a_2 + 4 < \ldots < a_{60} + 4$$

lie between 1 and 119. Hence by PP, two of these numbers must be equal. But the numbers in the first row are all distinct and similarly the numbers in the second row are all distinct. Hence some number in the first row must be equal to a number in the second row i.e. for some i, j we must have $a_i = a_j + 4$, so that $a_i - a_j = 4$, as required.

Second method: By data, there are $115 - 60 = 55$ unavailable items. Label the items in the list thus: $i_1, \ldots, i_{115}$. Then we have the following set of 111 pairs of items in each of which the two items are 4 items apart:

$$S = \{(i_1, i_5),\ (i_2, i_6),\ (i_3, i_7),\ (i_4, i_8),\ (i_5, i_9), \ldots, (i_{111}, i_{115})\}.$$

Now call a pair (i_r, i_s) from the above set a *good* pair if the items i_r and i_s are both available, and a *bad* pair otherwise. Then, clearly, the pair (i_r, i_s) is bad if at least one of the items i_r and i_s is unavailable. Note that if, for example, item i_5 is unavailable, then *both* the pairs (i_1, i_5) and (i_5, i_9) are bad.

We want to show that there is at least one good pair. Suppose, if possible, that all the 111 pairs in S are bad. This implies, since $111 = (2 \times 55) + 1$, that there are at least $55 + 1 = 56$ unavailable items. This contradicts the fact that there are only 55 items which are unavailable. So there is at least one good pair.

6. For $1 \leq r \leq 77$, let a_r denote the total number of games played on the first r days.

Hence $1 \leq a_1 < a_2 \ldots < a_{77}$. Now the chess master plays at least one game per day so that $a_{i+1} \geq a_i + 1$. Also, since at most 12 games are played during a week, $a_{77} \leq 132 (= 12 \times 11)$. Thus $a_{77} + 21 < 154$.

Consider the sequence of 154 positive numbers, $a_1, a_2, \ldots, a_{77}, a_1 + 21$, $a_2 + 21, \ldots, a_{77} + 21$ such that a_i and $a_i + 21 \leq 153$ for all i. So by the pigeonhole principle, at least two of the elements in the sequence are equal. But $a_1 < a_2 < \ldots < a_{77}$ and $a_1 + 21 < a_2 + 21 < \ldots < a_{77} + 21$. Hence $a_i = a_j + 21$ for some $j < i$. Hence $a_i - a_j = (j+1)$ th day games $+ \ldots + (i)$ th day games $= 21$.

Thus games played on $(j+1)$th, $(j+2)$ th, $\ldots$, (i) th day total upto exactly 21.

Note: By the same method, the following general result can be proved.

Suppose a chess master decides to play on d consecutive days, playing at least one game a day and a total of no more than b games where $d < b < 2d$. Then for each $i \leq 2d - b - 1$ there is a succession of days on which, in total, the chess master plays exactly i games.

7. First part: Consider a fixed person A. Of the other five, by PP, there are either three who are friends of A or three who are not. In the first case, the three friends of A are either mutual enemies or two of them are friends and form a triplet of friends with A. The other case is similar.
Second part: Consider a group of 5 persons and suppose that exactly the following are pairs of friends: AB, BC, CD, DE, EA. Then it is easy to see that no three are mutual friends or mutual enemies.

Remark. In fact, one can show that in a group of six people there are two triplets of mutual friends or two triplets of mutual enemies or one triplet of mutual friends and one triplet of mutual enemies.

8. For $1 \leq r \leq 1995$, let $b_r = \sum_{i=1}^{r} a_i$. Hence $1 \leq b_1 < b_2 \ldots < b_{1995} = 3989$. Distribute b_i's into 95 boxes $0, 1, 2, \ldots, 94$ such that b_i is in box j if j is the remainder when b_i is divided by 95.

Case (i) None of the b_i's is divisible by 95. Then the 1995 b_i's are put in only 94 boxes $1, 2, \ldots, 94$. Hence, by pigeonhole principle, there is one box which contains atleast 22 integers. Suppose $b_{i_1} < b_{i_2} < \ldots < b_{i_{22}}$ are in the same box. If $|b_{i_s} - b_{i_t}| = 95$, for some s, t, then we are done. Otherwise,

$$\begin{aligned} b_{i_2} &\geq b_{i_1} + 2(95), \\ b_{i_3} &\geq b_{i_2} + 2(95) \geq b_{i_1} + 4(95), \\ \ldots & \quad \ldots \\ b_{i_{22}} &\geq b_{i_21} + 2(95) \geq b_{i_1} + 42(95) \geq 3990 \end{aligned}$$

But $b_{i_{22}} \leq 3989$, a contradiction. Hence, there is a block of r successive a_i's $(r \geq 1)$ whose sum is 95.

Case (ii) Atleast one of the b_i's is divisible by 95. If there is one box which contains atleast 22 integers, then as in Case (i), we get a block of r successive a_i's $(r \geq 1)$ whose sum is 95. Otherwise, each box contains

exactly 21 integers. Suppose $b_{i_1} < b_{i_2} < \ldots < b_{i_{21}}$ are in the box 0. If $b_{i_s} = 95$ or $|b_{i_s} - b_{i_t}| = 95$ then we are done. Otherwise,

$$\begin{aligned} b_{i_1} &\geq 2(95), \\ b_{i_2} &\geq b_{i_1} + 2(95) \geq 4(95), \\ \ldots & \quad \ldots \\ b_{i_{21}} &\geq b_{i_{20}} + 2(95) \geq 42(95) \geq 3990 \end{aligned}$$

But $b_{i_{21}} \leq 3989$, a contradiction.

9. Since an integer must be either even or odd, every point (a, b) with integer co-ordinates must be put in one of the *four* pigeonholes:

(even,even), (even,odd),(odd,even) and (odd,odd).

Hence, two of the given five points (say, $A(x_1, y_1)$ and $B(x_2, y_2)$) must lie in the same pigeonhole, so that their x co-ordinates must have the same *parity* (i.e. they are either both even or both odd) and their y co-ordinates must have the same parity. Hence, $x_1 + x_2$ and $y_1 + y_2$ are even. Thus $(x_1 + x_2)/2$ and $(y_1 + y_2)/2$ are both integers, so that the mid-point of AB has integer co-ordinates.

10. Suppose that the 100 products $a_i b_i$ leave 100 different remainders when divided by 100. Then 50 of the products must be odd and the remaining 50 must be even since their remainders must now be a permutation of $1, 2, \ldots, 100$. The 50 odd products use up all the odd a_i and all the odd b_i. Hence the even products are products of even numbers and are therefore divisible by 4. But then none of the products will be of the form $4k + 2$, which is a contradiction.

11. Let S be any $7-$subset of $\{1, 2, \ldots, 24\}$. The number of non-empty subsets of S having at most 4 elements is

$$\binom{7}{1} + \binom{7}{2} + \binom{7}{3} + \binom{7}{4} = 98.$$

If T is any one of these subsets, then the sum of elements in T is between 1 and $21 + 22 + 23 + 24 = 90$. Since $90 < 98$, by PP1 it follows that the sums corresponding to the above 98 subsets cannot all be different. [Note that for the $6-$element subset $\{11, 17, 20, 22, 23, 24\}$ sums corresponding to all subsets are different.]

Exercise Set - 4.4

1. True or false? Justify your answer.

   If there are *more* than m objects and there are m boxes,

   (i) there will be at least 1 box with no objects,

   (ii) there will be at least 1 box with at least 2 objects,

   (iii) there will be at least 2 boxes with the same number of objects.

2. Given a group of n women and their husbands, how many people must be chosen from this group of $2n$ people to guarantee that the set contains a married couple ?

3. Thirteen persons have first names Bapu, Chandru and Damu and last names Kale, Late, Mate and Natu. Show that at least two persons have the same first and last names.

4. Eighteen persons have first names Eknath, Ganesh and Hari and last names Patil, and Rathi. Show that at least three persons have the same first and last names.

5. The members of a class of 27 pupils each go swimming on some of the days from Monday to Friday in a certain week. If each pupil goes at least twice, show that there must be two pupils who go swimming on exactly the same days.

6. Let A be any set of 20 distinct integers chosen from the arithmetic progression $1, 4, 7, \ldots, 100$. Prove that there must be two distinct integers in A whose sum is 104.

7. Let $S = \{3, 7, 11, \ldots, 103\}$. How many elements must we select from S to ensure that there will be at least two distinct integers among them whose sum is 110 ?

8. If 11 integers are selected from $\{1, 2, 3, \ldots, 100\}$, prove that there are at least two, say x, y, such that $0 < |\sqrt{x} - \sqrt{y}| < 1$.

9. How many times must we roll a single die in order to get the same score (i) at least twice (ii)at least three times (iii) at least n times $(n \geq 4)$?

10. (i) Let k be a positive integer. Prove that there is a positive integer m such that $k|m$ and the only digits in m are 0's and 1's.
    (ii) Let k be a positive integer. Prove that there is a positive integer n such that $k|n$ and the only digits in n are 0's and 3's.

11. Let n be an odd positive integer. If $i_1, i_2, \ldots, i_n$ is a permutation of $1, 2, \ldots, n$, prove that $(1 - i_1)(2 - i_2) \cdots (n - i_n)$ is an even integer.

12. In any set S of ten 2-digit numbers, show that there always exist 2 non-empty, disjoint subsets A and B such that the sum of elements in A equals the sum of elements in B.

13. Let S be a set of 7 positive integers the maximum of which is at most 24. Prove that the sums of the elements in all the non-empty subsets of S cannot be distinct.

14. Let S be a set of 5 positive integers the maximum of which is at most 9. Prove that the sums of the elements in all the non-empty subsets of S cannot be distinct.

15. Let $n \geq 3$ be an odd number. Show that there is a number in the set $\{2^1 - 1,\ 2^2 - 1,\ \ldots, 2^{n-1} - 1\}$ which is divisible by n.

16. At registration time, 750 students were required to select exactly five courses from a total of 10. Show that among all such combinations of courses, there was at least one not selected by more than two students.

17. An urn contains 100 balls: 28 red, 20 green, 12 yellow, 20 blue, 10 white and 10 black. What is the smallest number of balls that must be drawn from the urn, without looking, if the collection contains atleast 15 balls of the same colour ?

18. Given 8 distinct positive integers from the set $\{1, 2, \ldots, 16\}$ prove that there exists k such that $a_i - a_j = k$ has at least 3 distinct solutions (a_i, a_j).

19. A storekeeper's list consists of 80 items, each marked "available" or "unavailable". There are 50 available items. Show that there are at least 2 *unavailable* items in the list either 3 or 6 items apart.

20. Show that given 52 integers, there exist two of them whose sum or difference is divisible by 100.

21. (a) Show that of any 5 points chosen within a square of side length 2, there are two whose distance apart is atmost $\sqrt{2}$.

    (b) Show that of any $(n^2 + 1)$ points chosen in an equilateral triangle with side-length 1, there are two whose distance apart is atmost $1/n$.

22. Prove that when a rational number a/b, in lowest terms is expressed as a decimal, the decimal must either terminates or recurs.

23. Every point on a straight line is coloured with one of two colours. Prove that there is a segment whose ends and mid-point have the same colour.

24. If the points of the plane are colored in two colours, then show that there are three points of the same colour that form vertices of an equilateral triangle.

25. Show that among any 8 composite integers selected from the first 360 natural numbers, there will always be two which are not relatively prime.

26. If $n + 1$ integers are chosen, show that there exist two integers whose difference is divisible by n, where n is a positive integer.

27. In a round-robin tournament, show that there must be two players with the same number of wins if no player loses all matches and there are no drawn matches.

28. Show that given any set of seven distinct integers, there must exist two integers in this set whose sum or difference is a multiple of 10.

29. Show that any collection of eight positive integers whose sum is 20 has a subset summing to 4.

30. Show that if $(n + 1)$ integers are chosen from the set $1,2, \ldots, 2n$, then (i) there is a pair of coprime numbers among the chosen numbers; (ii) there exists a pair among the chosen integers which adds upto $2n + 1$; (iii) there exists a pair among the chosen integers such that one of them divides the other.

31. In a gathering of n people every two individuals either know each other or do not know each other. Show that there must exist two individuals who know the same number of people.

32. A set of numbers is called a sum-free set if no two of them add up to a member of the same set and if no member is double of another member. What is the maximum size of a sum-free subset of

$$S = \{1, 2, \ldots, 2n + 1\}?$$

33. There are 1958 computers which can communicate among themselves in 6 languages with the provision that any two computers can communicate only in one language out of the 6 languages. Prove that there exist at least 3 computers whose mutual language of communication, two by two, is the same.

34. Two disks, one smaller than the other, are each divided into 200 congruent sectors. In the larger disk 100 of the sectors are chosen arbitrarily and painted red; the other 100 sectors are painted blue. In the smaller disk each sector is either painted red or blue with no condition on the number of red and blue sectors. The smaller disk is then placed on the larger disk so that their centres coincide. Show that it is possible to align the two disks so that the number of the sectors of the smaller disk whose colour matches the corresponding sector of the larger disk is at least 100.

35. Show that every sequence $a_1, a_2, \ldots a_{mn+1}$ of $mn+1$ distinct real numbers contains either an increasing subsequence of length $m+1$ or a decreasing subsequence of length $n+1$. (Recall that if $\mathbf{b} : b_1, b_2 \ldots, b_m$ is a sequence, then $\mathbf{b}' : b_{i_1}, b_{i_2}, \ldots b_{i_k}$ is called a *subsequence* of $\mathbf{b}$ provided $1 \leq i_1 < i_2 < \ldots < i_k \leq m$.)

    [For example, let $m = 3$, $n = 4$. Then in a sequence of $mn+1 = 3(4)+1 = 13$ distinct real numbers, there is either an increasing subsequence of length $3+1 = 4$ or a decreasing subsequence of length $4+1 = 5$. In the sequence

    $$4, 3, 2, 1, 8, 7, 6, 5, 12, 11, 10, 9, 16,$$

    $4, 8, 12, 16$ is an increasing subsequence of length 4 but there is no decreasing subsequence of length 5.]

36. Show that among any seven distinct positive integers not greater than 126, one can find two of them, say x and y, such that $1 < y/x \leq 2$.

37. Show that given any set A of 13 distinct real numbers, there exist $x, y \in A$ such that

    $$0 < \frac{x-y}{1+xy} \leq 2 - \sqrt{3}.$$

Hints and Answers

1. (i) False; for if the number of objects is $m+r$, $r > 0$, then it is possible that $m-1$ of the boxes contain 1 object each and the m^{th} box contains all the remaining $r+1$ objects so that no box is empty. (ii) True; this is

PP1. (iii) False; for if the number of objects is $m(m-1)/2$, $m > 3$, then $m(m-1)/2 > m$ and it is possible that the m boxes contain respectively $0, 1, 2, \ldots, (m-1)$ objects so that all the boxes contain different number of objects. [Note that $1 + \cdots + (m-1) = m(m-1)/2 =$ the total number of objects given.]

2. Ans. $n + 1$.

3. By the multiplication principle, there are $4 \times 3 = 12$ possible names such as Bapu Kale, Bapu Late etc. Now regard the 13 persons as 13 'objects' and the 12 names as 12 'boxes'. Then by PP1, it follows that at least 2 'objects' are in the same box i.e. at least 2 persons have the same name.

4. By the multiplication principle, there are $3 \times 2 = 6$ names such as Eknath Patil etc. Now since there are 18 persons and $18 = 3 \times 6$, it follows, by PP2, that at least 3 persons have the same first and last names.

5. The set $\{Monday, \ldots, Friday\}$ of 5 days has $\binom{5}{5} + \binom{5}{4} + \binom{5}{3} + \binom{5}{2} = 1 + 5 + 10 + 10 = 26$ subsets each containing 2 or more days. Regard the 27 pupils as 'objects' and these 26 subsets as 'boxes'. Then by PP1, there must be at least one box containing at least 2 pupils i.e. at least 2 pupils must go swimming on the same days.

6. The given A.P. $1, 4, \ldots, 100$ has n^{th} term $3n - 2$ and hence contains 34 terms. Arrange these terms in 18 boxes as follows:

$$\boxed{1}\ \boxed{52}\ \boxed{4\ \ 100}\ \boxed{7\ \ 97}\ \ldots\ \boxed{49\ \ 55}$$

Note that the sum of the numbers in each of the last 16 boxes is 104. Then by PP1, if 20 numbers are taken from these 18 boxes, then at least *two* of the numbers must come from the same box (and that box must be one of the last 16 boxes since the first two contain only 1 number each) and their sum is 104 as required.

7. Ans: 15. To see this note that the set S contains 26 elements which form an A.P. These numbers can be put in the following 14 boxes

$$\boxed{3}\ \boxed{55}\ \boxed{7\ \ 103}\ \boxed{11\ \ 99}\ \ldots\ \boxed{51\ \ 59}$$

where the sum of the numbers in each of the last 12 boxes is 110. Hence by PP1 is enough to select 15 elements from S.

8. Consider the integral part $[t]$ of the positive real number t. Then $t-[t]=f$ is the fractional part of t and $0 \le f < 1$. Now since $1 \le x \le 100$, we have $1 \le \sqrt{x} \le 10$ and so $1 \le [\sqrt{x}] \le 10$. Thus for elements x of S, $[\sqrt{x}]$ must be one of the 10 numbers $1, 2, \ldots, 10$. Hence if 11 numbers are taken from S, then by PP1, at least two of them, say x, y, must be such that $\sqrt{x}$ and $\sqrt{y}$ have the *same* integral part, say i. So if $\sqrt{x} = i + f_1$ and $\sqrt{y} = i + f_2$, $0 \le f_1, f_2 < 1$, then $0 < |\sqrt{x} - \sqrt{y}| = |f_1 - f_2| < 1$.

9. The score is one of the 6 numbers $1, 2, \ldots, 6$ in one roll of the die. (i) So, by PP1, we must roll the die 7 times to be sure to get the same score twice. (ii) Since $13 = 2 \times 6 + 1$, by PP2, if we roll the die 13 times, then we must get the same score at least 3 times. (iii) $6(n-1)+1$.

10. (i) The $9k+1$ numbers $10^1, 10^2, \ldots, 10^{9k+1}$, when divided by $9k$, can leave only $9k$ different remainders $0, 1, \ldots, 9k-1$. Hence, by PP1, two of these numbers , say 10^r and 10^s $(r > s)$, leave the same remainder on division by $9k$. Thus $9k$ divides $10^r - 10^s$ so that $10^r - 10^s = 10^s(10^{r-s} - 1) = 9kl$, for some integer l. Now the integer $10^{r-s} - 1$ consists of digit 9 only. Hence $(10^{r-s} - 1)/9$ is an integer Thus $m = 10^s(10^{r-s} - 1)/9$ is an integer consisting of digits 0 and 1 only and $k|m$ since $m = kl$ by the above.
(ii) Find the number m as in (i). Then $n = 3m$ is as required.

11. Since n is odd, let $n = 2m + 1$ where m is a non-negative integer. Then the set $S = \{1, 2, \ldots, n\}$ contains $m+1$ odd numbers, namely $1, 3, \ldots, 2m+1$ but only m even numbers, namely $2, 4, \ldots, 2m$. The same is true of the permutation $i_1, i_2, \ldots, i_n$ of S. Consider the $m+1$ numbers $1 - i_1, 3 - i_3, \ldots, n - i_n$ which are of the form $r - i_r$ where r is *odd*. Since i_s is even for only m values of s, by PP1, one of the $m+1$ numbers $i_1, i_2, \ldots, i_n$, say i_t, is odd where t is also odd. Hence $t - i_t$ is even and so the product $(1 - i_1)(2 - i_2) \cdots (n - i_n)$ is even.

12. Let $s(T)$ denote the sum of the numbers in any non-empty subset T of S. Then by data, the largest number in S can be at most 99 and so $s(T) \le 90 + 91 + \cdots + 99 = 945$. Thus $s(T)$ has at most 945 different values. But the number of non-empty subsets of S is $2^{10} - 1 = 1023$. Hence, regarding the sums $s(T)$ as 'boxes' and the non-empty subsets T of S as 'objects', we see that there are more objects than boxes. So, by PP1, there exist 2 distinct non-empty subsets A_1 and B_1 such that $s(A_1) = s(B_1)$. If A_1, B_1 are disjoint, they are the required subsets. If $A_1 \cap B_1$ is non-empty, we can remove the common part from each of them to get the required subsets.

13. Let $s(T)$ denote the sum of the numbers in any non-empty subset T of S. Since the largest number in T can be at most 24 we have $s(T) \leq 18+19+\cdots+24 = 147$. Thus $s(T)$ can have 147 different values. But we cannot argue as in the last problem because in this case the number of non-empty subsets of S is $2^7 - 1 = 128 - 1 = 127$ which is less than the number of possible sums, namely 147. So we consider non-empty subsets A of S such that $|A| \leq 5$. There are in all $2^7 - (1+7+1) = 119$ such subsets T because we have to exclude the empty set and the $\binom{7}{6} = 7$ subsets with 6 elements each and the set S itself. Now for such a subset A we have $s(A) \leq 20+21+22+23+24 = 110$. Hence, as in the last problem, by PP1 we see that there exist 2 non-empty subsets A, B with at most 5 elements such that $s(A) = s(B)$.

14. Consider non-empty subsets A of S such that $|A| \leq 3$ and proceed as in the last problem.

15. Consider the n numbers $2^0.2^1, \ldots, 2^{n-1}$. Since n is odd, none of these numbers is divisible by n and so, modulo n, they can leave only $n-1$ different remainders: $1, 2, \ldots, n-1$. Hence, by PP1, two of them, say 2^r and 2^s, $0 \leq s < r \leq n-1$, must leave the same remainder modulo n so that n divides $2^r - 2^s = 2^s(2^{r-s} - 1)$. Hence n divides $2^{r-s} - 1$ since n is odd and so n and 2^s are coprime. So the result follows since $1 \leq r - s \leq n-1$.

16. There are $\binom{10}{5} = 252$ different 5-combinations of the 10 courses available to the 750 students. Hence the *average* number of times a combination is chosen by a student is $750/252 = 2.97...$ Hence, by PP3, there is a combination which was chosen by at most 2 students.

17. By PP4, it is enough to draw $(14+14+12+14+10+10)+1 = 75$ balls.

18. Let $a_1, \ldots, a_8$ be the chosen numbers. Without loss, we may suppose that these are arranged in decreasing order:

$$a_1 > a_2 > a_3 > a_4 > a_5 > a_6 > a_7 > a_8.$$

Now we have $\binom{8}{2} = 28$ differences of the form $a_i - a_j$ with $i < j$. We have to show that at least three of these differences are equal with common value k, say. We will, in fact, show that at least three of the following seven *successive* differences

$$a_1 - a_2,\ a_2 - a_3,\ a_3 - a_4,\ a_4 - a_5,\ a_5 - a_6,\ a_6 - a_7,\ a_7 - a_8 \quad \text{(i)}$$

are equal. Since $1 \leq a_i \leq 16$, the sum of these differences is $a_1 - a_8 \leq 16 - 1 = 15$. Suppose, if possible, that any difference can occur at the most twice. Then the sequence of differences having *minimum sum* is clearly the following:

$$1,\ 1,\ 2,\ 2,\ 3,\ 3,\ 4;$$

and the sum of these differences is 16. This contradicts the fact that the sum of the differences is always ≤ 15. Hence at least three of the seven differences in (i) must be equal.

19. Let the positions of the unavailable items be $a_1, a_2, \ldots, a_{30}$. Since $a_{30} \leq 80$, we see that the 90 numbers

$$\begin{aligned} & a_1 < a_2 < \cdots < a_{30} \\ \text{and} \quad & a_1 + 3 < a_2 + 3 < \ldots < a_{30} + 3 \\ \text{and} \quad & a_1 + 6 < a_2 + 6 < \ldots < a_{30} + 6 \end{aligned}$$

lie between 1 and 80. Hence by PP1, two of these numbers must be equal. But the numbers in the first row are all distinct and similarly the numbers in the second row and those in the third row are all distinct. Hence some number in one of the rows must be equal to a number in some other row. So, for some i, j we have *either* $a_i = a_j + 3$, or $a_i = a_j + 6$ or $a_i + 3 = a_j + 6$. Hence either, $a_i - a_j = 3$ or $a_i - a_j = 6$, as required.

22. We obtain the decimal for a/b by long division as follows: Divide a by b to obtain $a = xb + r,\ 0 \leq r < b$. Next, divide $10r$ by b to obtain $10r = x_1 b + r_1,\ 0 \leq r_1 < b$. Next, divide $10r_1$ by b to obtain $10r_1 = x_2 b + r_2,\ 0 \leq r_2 < b$; next divide $10r_2$ by b to obtain $10r_2 = x_3 b + r_3,\ 0 \leq r_3 < b$, and so on. Then, we get $a/b = x \cdot x_1 x_2 x_3 \cdots$. Now if the decimal does not terminate, then we must obtain a non-zero remainder at each stage. Since there are only $b - 1$ possible different non-zero remainders, by PP1, some remainder must be repeated after at most b steps. Hence the expansion will recur from this point onward.

23. Suppose every point on a straight line is coloured with one of 2 colours, say red and blue. Then there exist 2 distinct points, A and B, with the same colour, say red.

Let C be the mid-point of AB. (i) Let C be red. Then segment ACB is as required. (ii) Let C be blue. In this case, take a point A' on the A-side of C such that $AA' = AB$ and a point B' on the B-side of C such

that $BB' = AB$. If A' and B' are both blue, then segment $A'CB'$ is as required. If A' is red, then segment $A'AB$ is as required. If B' is red, then segment ABB' is as required. Thus the result holds in all cases.

24. Suppose the points of the plane are colored in two colours, say red and blue. Then, as shown in the last problem, there exists a segment ADB such that D is the mid-point of AB and the points, A, D, B have the same colour, say red. Consider an equilateral triangle ABC. Let E, F be respectively, the mid-points of BC and CA. If E (respectively F) is red, then $\triangle DBE$ (respectively $\triangle DFA$) is as required. So, suppose both E, F are blue. Then if C is red, then $\triangle ABC$ is as required and if C is blue, then $\triangle CFE$ is as required.

25. Let $a_1, \ldots, a_8$ be eight composite numbers from the numbers $1, \ldots, 360$. Now for $1 \leq i \leq 8$, $a_i \leq 360 < 361 = 19^2$. Hence, if p is the smallest prime divisor of any a_i, then $p \leq \sqrt{a_i} < 19$. Now there are only 7 primes less than 19: $2, 3, 5, 7, 11, 13, 17$. So, by PP1, at least 2 a_i's must have a common prime divisor.

33. Let C_1 be any one of the given 1958 computers. Then since C_1 communicates with the remaining $1957 = 326 \times 6 + 1$ computers in 6 languages, it follows by PP2 that C_1 communicates with at least 327 computers in the *same* language, say L_1. If two of these 327 computers communicate with each other in this language L_1, the the result holds. Otherwise these 327 computers communicate with each other in the 5 remaining languages. Now we can repeat the above argument: Let C_2 be any one of the above 327 computers. Then C_2 communicates with the remaining $326 = 65 \times 5 + 1$ computers in 5 languages, so that C_2 communicates with at least 66 computers in the *same* language, say L_2. If two of these 66 computers communicate with each other in this language L_2, then the result holds. Otherwise these 66 computers communicate with each other in the 4 remaining languages, and since $65 = 16 \times 4 + 1$, we are reduced to the case of 17 computers which communicate with each other in the same language out of the 4 languages. Next, since $16 = 3 \times 5 + 1$, we have the case of 6 computers which communicate with each other in 2 languages. Now the result follows by solved Ex. 7 above.

34 Let $S_1, S_2, \ldots, S_{200}$ denote the successive sectors of the smaller disk. As the smaller disk rotates, sector S_1 matches in colour with 100 sectors of the larger disk in one complete rotation. Similarly, sector S_2 matches 100 times and so on for each of the 200 sectors of the smaller disk. Hence

in all there are $100 \times 200 = 20000$ colour matches for the 200 sectors of the smaller disk. Therefore the average number of colour matches per position is $20000/200 = 100$. So the result follows by PP3.

35 Let $\mathbf{a} : a_1, a_2, \ldots, a_{mn+1}$ be the given sequence. Let x_i denote the length of the longest *increasing* subsequence of a beginning at a_i and let y_i be the length of the longest *decreasing* subsequence of a beginning at a_i. Consider the $mn+1$ ordered pairs $(x_i, y_i), 1 \leq i \leq mn+1$. We will prove that

(*) All these $mn + 1$ ordered pairs are distinct.

For any distinct integers i, j such that $1 \leq i, j \leq mn + 1$, we are given that $a_i \neq a_j$ since the terms of the sequence are distinct. Let $i < j$. First let $a_i < a_j$. Then it follows that $x_i > x_j$ since we can append a_i at the beginning of every increasing subsequence beginning with a_j and obtain a *longer* subsequence of the same type. (To see this, let $\mathbf{a}' : a_{j_1}, a_{j_2}, \ldots a_{j_r}$, where $j_1 = j$, be any increasing subsequence of a starting with a_j. Then since $i < j = j_1$, the sequence $\mathbf{a}'' : a_i, a_{j_1}, a_{j_2}, \ldots a_{j_r}$ obtained by appending a_i to $\mathbf{a}'$ is a *subsequence* of a starting with a_i. Further, this last subsequence is also increasing because by supposition $a_i < a_{j_1}$.)

Similarly, if $a_i > a_j$, then $y_i > y_j$. Hence, if $i \neq j$, then (x_i, y_i) and (x_j, y_j) are *distinct* ordered pairs. This proves (*).

Now suppose that the stated result is not true. Then for each i, we must have $1 \leq x_i \leq m$ and $1 \leq y_i \leq n$. Thus there are only m possible different values of x_i and only n possible different values of y_i. Hence, by the multiplication principle, only mn of the $mn + 1$ ordered pairs (x_i, y_i) can be *distinct*. Hence by PP1, at least 2 of the $mn + 1$ ordered pairs must be equal: contradiction to (*). Hence the result is true.

4.4 Principle of Inclusion and Exclusion

The **Principle of Inclusion and Exclusion (PIE)** is the most general form of the addition principle for enumeration. Let S be a finite set of objects. Let A and B be two subsets of S, then to count the number of elements in $A \cup B$ is to count the number of elements of A and those of $B - A$ and add. But $|B - A| = |B| - |A \cap B|$. Hence

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

In other words, while counting elements of A and of B separately, elements common to both A and B are counted twice and so in order to nullify this double counting one has to remove the $A \cap B$ count once from $|A| + |B|$.

General form of PIE Let $A_1, A_2, \ldots, A_m$ be subsets of an n-element set S. Let $A_i' = S - A_i$ = the complement of A_i in S. Then the number of elements not belonging to any of the sets $A_1, A_2, \ldots, A_m$ is given by

$$|A_1' \cap A_2' \cap \ldots \cap A_m'| = n - S_1 + S_2 - S_3 + \ldots + (-1)^m S_m,$$

$$\text{where} \qquad S_r = \sum |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_r}|$$

and the sum is taken over the $C(n, r)$ choices of r integers $i_1, \ldots, i_r$ such that $1 \leq i_1 < i_2 < \ldots < i_r \leq m$.

To understand this better let us take $m = 3$. Then

$$\begin{aligned} |A_1' \cap A_2' \cap A_3'| &= n - (|A_1| + |A_2| + |A_3|) \\ &+ (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) - |A_1 \cap A_2 \cap A_3|. \end{aligned}$$

Example 1 Find the number of positive integers between 1 and 1000 which are divisible neither by 2 nor by 5.

Solution. Let $S = \{1, 2, \ldots, 1000\}$, $A = \{x \in S | 2 \text{ divides } x\}$, $B = \{x \in S |\ 5 \text{ divides } x\}$. We are interested in finding $|A' \cap B'|$. Recall the De Morgan laws, $(A \cup B)' = A' \cap B', (A \cap B)' = A' \cup B'$. Thus if $[x]$ denotes the integral part of x,

$$\begin{aligned} |A' \cap B'| &= |(A \cup B)'| = |S| - |A \cup B| = |S| - (|A| + |B| - |A \cap B|) \\ &= 1000 - ([1000/2] + [1000/5] - [1000/10]) = 400. \end{aligned}$$

Example 2 A party is attended by n persons and every party-goer leaves his hat at the counter. In how many ways can the hats be given back so that nobody receives his own hat?

Solution. Let 1,2,3, $\ldots, n$ be these persons and $\hat{1}, \hat{2}, \ldots, \hat{n}$ denote their corresponding hats. Let A_i denote the set of all distributions so that i gets his own hat for $i = 1, 2, \ldots n$.

The number of distributions in which i gets $\hat{i}$ is clearly $(n-1)!$ as the remaining $(n-1)$ hats can be distributed arbitrarily among the remaining $(n-1)$ persons. Thus $|A_i| = (n-1)!$.

Next for each choice of k distinct integers $i_1, i_2 \ldots, i_k$ from 1,2, $\ldots, n$ let $A_{i_1 i_2 \ldots i_k} = A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}$ = the set of all distributions so that i_1 gets

i_1, i_2, gets $i_2, \ldots, i_k$ gets i_k, then again $|A_{i_1 i_2 \ldots i_k}| = (n-k)!$. Note that this counting is independent of the choice of $i_1, i_2, \ldots, i_k$. The number of ways in which we can choose k distinct symbols from 1,2, ... n is $C(n,k)$.

Thus $S_k = \sum |A_{i_1 i_2 \ldots i_k}| = C(n,k) \cdot (n-k)! = \frac{n!}{k!}$. Now by PIE

$$\begin{aligned} |A_1' \cap A_2' \cap \ldots \cap A_n'| &= n! - C(n,1)(n-1)! + C(n,2)(n-2)! - \cdots \\ &+ (-1)^k C(n,k)(n-k)! + \ldots + (-1)^n C(n,n) \\ &= n!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \ldots + \frac{(-1)^n}{n!}\right] \end{aligned}$$

This number is denoted by D_n. Thus the probability that no one gets his own hat is $D_n/n!$. Note that D_n is the number of derangements of $S = (1, 2, \ldots n)$, where a derangement of S is a permutation $(i_1, i_2, \ldots i_n)$ such that $i_k \neq k$ for $k = 1, 2, \ldots n$.

Example 3 Find the number of integer solutions of $x_1 + x_2 + x_3 = 24$ subject to the conditions $1 \leq x_1 \leq 5$, $12 \leq x_2 \leq 18$, $-1 \leq x_3 \leq 12$.

Solution. Let $y_1 = x_1 - 1$, $y_2 = x_2 - 12$, $y_3 = x_3 + 1$, so that the equation becomes $y_1 + y_2 + y_3 = 12$, and we want non-negative integer solutions subject to the conditions $y_1 \leq 4$, $y_2 \leq 6$, $y_3 \leq 13$. Let A, B, C be respectively the sets of all solutions (y_1, y_2, y_3) such that $y_1 > 4$, $y_2 > 6$, $y_3 > 13$. Then $A \cap B$ is the set of solutions with $y_1 > 4$ and $y_2 > 6$, with similar meaning for $A \cap C$, $B \cap C$ and $A \cap B \cap C$. Now the number of non-negative integer solutions of $y_1 + y_2 + y_3 = 12$ is $n = \binom{3-1+12}{12} = 91$. Further, $|A| = \binom{3-1+7}{7} = 36$, $|B| = \binom{3-1+5}{5} = 21$ and $|C| = 0$, since $y_3 \leq 13$; and similarly $|A \cap B| = 1$, $|A \cap C| = |B \cap C| = 0$, $|A \cap B \cap C| = 0$. Hence, by PIE, the required number of solutions is $91 - (36 + 21 + 0) + (1) - 0 = 35$.

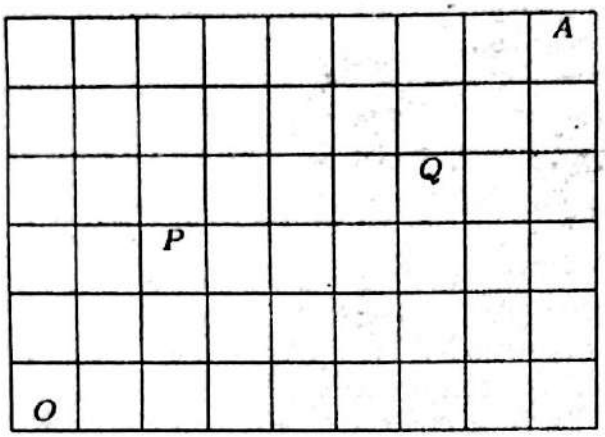
Example 4 A person starts from the origin $O(0,0)$ in the X-Y plane. He takes steps of **one unit** along the **positive** X-axis or the **positive** Y-axis. Travelling in this manner, find the total number of ways he can reach $A(9,6)$ avoiding both the points $P(3,3)$ and $Q(6,4)$.

Solution. We use the following formula: the number of paths from $(0,0)$ to (m,n) is $\binom{m+n}{m}$. Let $T(O,A)$ be the set of all paths from $O(0,0)$ to $A(9,6)$, $T(O,P,A)$ be the set of all paths from O to A via P, etc. Hence $|T(O,P,A)| = |T(O,P)| \times |T(P,A)|$, where $|T(P,A)|$ is to be evaluated by shift of origin to P. Now,

$$\begin{aligned} |T(O,A)| &= \binom{9+6}{6} = 5005, \\ |T(O,P,A)| &= \binom{3+3}{3} \times \binom{6+3}{3} = 20 \times 84 = 1680, \end{aligned}$$

$$|T(O,Q,A)| = \binom{6+4}{4} \times \binom{3+2}{2} = 210 \times 10 = 2100,$$

$$|T(O,P,Q,A)| = \binom{3+3}{3} \times \binom{3+1}{1} \times \binom{3+2}{2} = 20 \times 4 \times 10 = 800.$$



By the inclusion-exclusion principle, the required number of paths is given by

$$\begin{aligned} & |T(O,A)| - (|T(O,P,A)| + |T(O,Q,A)|) + |T(O,P,Q,A)| \\ = \; & 5005 - 1680 - 2100 + 800 = 2025. \end{aligned}$$

Exercise Set-4.5

1. Find the number of integers between 1 and 1000 inclusive which are not divisible by any of 2,3, and 7.

2. How many integers between 1 and 1000,000 inclusive are neither perfect squares, nor perfect cubes, nor perfect fourth powers?

3. (a) Show that for $n \geq 2$, $D_n = (n-1)(D_{n-1} + D_{n-2})$.

   (b) Show that D_n is even, if n is odd.

   (c) Show that $D_n = nD_{n-1} + (-1)^n, n \geq 2$.

4. In how many ways can the letters M, A, D, I, S, O, N be written down so that the word spelled completely disagrees with $MADISON$?

5. Prove that there exist $2^n - 2$ numbers that have n digits made up only of the numbers 1 and 2 and contain each digit at least once.

6. Find the number of positive integer solutions of $x_1 + x_2 + x_3 = 15$ subject to the conditions $x_1 \leq 5$, $x_2 \leq 6$, $x_3 \leq 8$.

7. Three identical black balls, four identical red balls and five identical white balls are to be arranged in a row. Find the number of ways that can be done if all the balls with the same colour do not form a single block.

Solutions to Exercise set-4.5

1. 286 2. Hint: The numbers between 1 and 10^6 which are perfect k^{th} powers are the integers n such that $1 \leq n \leq 10^{6/k}$. Ans. 998910.

4.5 Recurrence Relations

Definition: A recurrence relation for the sequence $a_0, a_1, \ldots$ is an equation that relates a_n to certain of its predecessors $a_0, a_1, \ldots, a_{n-1}$.

A recurrence relation defines the n th term of a sequence indirectly. We give two examples of recurrence relations.

1. Fibonacci Sequence: $F_0 = 1$, $F_1 = 1$ and for $n \geq 2$, $F_n = F_{n-1} + F_{n-2}$. This sequence is 1, 1, 2, 3, 5, 8, 13, ...

2. Derangements: $D_n = (n-1)(D_{n-1} + D_{n-2})$

The following examples illustrate how to obtain the recurrence relations.

Examples

1. Find the number of regions n lines in general position in the plane divide the plane into.

   Solution. Here it is assumed that no two of the n lines are parallel and no three intersect at the same point. Let a_n denote the required number of regions into which the plane is divided. Then $a_0 = 1, a_1 = 2, a_2 = 4$, $a_3 = 7$. In fact, for $n \geq 1$, $a_n = a_{n-1} + n$. This happens because the nth line is cut by the previous $n-1$ lines in n segments and each segment cuts a region into two new regions. Hence n regions are added to a_{n-1} giving a_n. Now

   $a_1 = 1 + 1, \quad a_2 = a_1 + 2, \quad \ldots \quad \ldots, \quad a_n = a_{n-1} + n.$

   Adding these equations we get $a_n = 1 + \frac{1}{2}n(n+1)$.

2. Find the number of binary sequences of length n having no 11. (In a binary sequence every term is 0 or 1).

Solution. Consider the set S_n of all $n-$ bit sequences with no 11. Let $n \geq 3$. Decompose S_n into $S_{n,0}$ and $S_{n,1}$ as follows:
$S_{n,0} = n-$ bit sequences starting with a zero and without 11,
$S_{n,1} = n-$ bit sequences starting with a one and without 11.
Clearly $S_{n,0}$ is obtained by appending a zero at the beginning of elements of S_{n-1}. Also in every element of $S_{n,1}$ the second digit has to be 0 and the remaining $n-2$ bit-sequence must come from S_{n-2}. Let a_n denote the number of elements in S_n. Then we get $a_n = a_{n-1} + a_{n-2}, \quad n \geq 3$. (The recurrence relation is same as that for the Fibonacci sequence, however the sequence a_n is different as the initial values are different: $a_1 = 2, a_2 = 3$.)

3. There are n necklaces such that the first necklace contains 5 beeds, the second necklace contains 7 beeds, and in general the ith necklace contains i beeds more than the number of beeds in the $(i-1)st$ necklace. Find the total numbers of beeds in all the n necklaces.

Solution. Let T_i denote the number of beeds in the ith necklace. Thus for $2 \leq i \leq n$

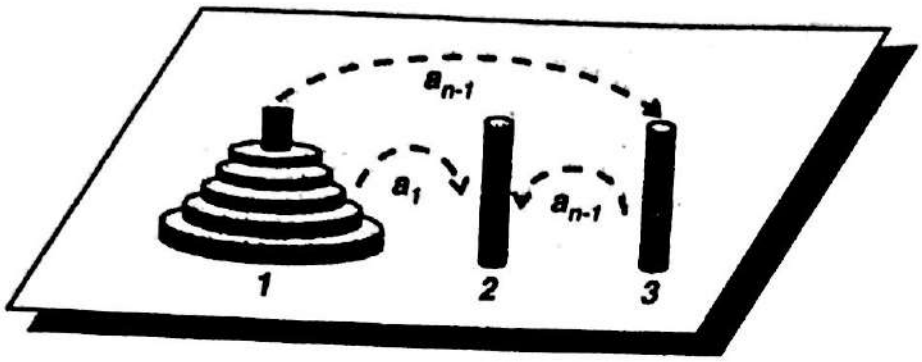
$$\begin{aligned} T_2 &= T_1 + 2 \\ T_3 &= T_2 + 3 \\ &\vdots \quad\quad \vdots \\ T_i &= T_{i-1} + i \end{aligned}$$

Adding, $T_i = T_1 + 2 + 3 + \cdots + i = 4 + \frac{i(i+1)}{2}$ i.e. $T_i = 4 + \frac{1}{2}(i^2 + i)$
This holds for $1 \leq i \leq n$. Adding, we get

$$\begin{aligned} \sum_{i=1}^{n} T_i &= \sum_{i=1}^{n} 4 + \frac{1}{2}\sum_{i=1}^{n} i^2 + \frac{1}{2}\sum_{i=1}^{n} i \\ &= 4n + \frac{1}{2}\frac{n(n+1)(2n+1)}{6} + \frac{1}{2}\frac{n(n+1)}{2} \\ &= 4n + \frac{n(n+1)(n+2)}{6} = \frac{n}{6}[n^2 + 3n + 26] \end{aligned}$$

4. **Tower of Hanoi:** This is a puzzle consisting of three pegs mounted on a board and n disks of different sizes. Initially all the n disks are stacked on the first peg so that any disk is always above a larger disk. The problem is to transfer all these disks to peg 2 with minimum number

of moves, each move consisting of transferring one disk from any peg to another so that on the new peg the transferred disk will be on top of a larger disk. (Keeping a disk on a smaller disk is not allowed).



Tower of Hanoi

Solution. To accomplish this, let C_i denote the minimum number of moves required to transfer a heap of i disks from one peg to another under the given conditions. First transfer uppermost $n-1$ disks from first peg to peg 3. This can be done in C_{n-1} moves (minimum number). Now transfer the n^{th} disk from peg 1 to peg 2. Place the $n-1$ disks from peg 3 to peg 2 using C_{n-1} moves. Thus we get the recurrence relation, $C_n = 2C_{n-1} + 1$.

Exercise Set-4.6

1. Determine the recurrence relation for a_n:

   (i) a_n is the number of regions into which the plane is divided by n circles, where each pair of circles intersects in exactly two points and no three circles meet in a single point.

   (ii) In a singles tennis tournament, $2n$ players are paired off in n matches; a_n denotes the number of different ways in which this pairing can be done.

2. n points are given on the circumference of a circle, and the chords determined by them are drawn. If no three chords have a common point, how many triangles are there all of whose vertices lie inside the circle? (E.g. one triangle when $n = 6$).

3. Let n be an integer ≥ 3. Find a direct combinatorial interpretation of the identity $\binom{\binom{n}{2}}{2} = 3\binom{n+1}{4}$.

4. Suppose 5 points are given in the plane, not all on a line, and no 4 on a circle. Prove that there exists a circle through three of them such that of the remaining 2 points, one lies in the interior and the other is in the exterior of the circle.

5. Show that for each $n \geq 6$, a square can be subdivided into n non-overlapping squares.

6. If n is a power of 2, say 2^k, find the largest value of m such that there is an $m-$element subset A of $\{1, 2, 3, \ldots, 2^k\}$ such that
(i) The set A does not contain a power of 2 (not even $2^0 = 1$), and
(ii) No two elements of A adds upto a power of 2.

Solutions to Exercise Set-4.6

1. (i) $a_n = a_{n-1} + 2n - 2$, $a_1 = 2$. (ii) $a_n = (2n-1)a_{n-1}$, $a_1 = 1$.
2. $\binom{n}{6}$.
4. Take n points on a circle with centre O. The number of chords formed from these points is $\binom{n}{2}$ and the number of pairs of chords is $\binom{\binom{n}{2}}{2}$. Now consider the $n+1$ points including given n points and the centre O. We can choose 4 points out of these $n+1$ points to get $\binom{n+1}{4}$ combinations. If such a combination contains O, then we get 6 line segments of which 3 are radii and 3 are earlier chords.

The 3 chords give rise to $\binom{3}{2} = 3$ pairs of chords *with exactly one point common to a given pair*. E.g. $\{O, A, B, C\}$ gives AB, AC, BC as three chords and $\{AB, AC\}$, $\{AB, BC\}$ and $\{AC, BC\}$ as three pairs of chords.

We next consider a collection of 4 points not including O. This gives $\binom{4}{2} = 6$ chords and hence $\binom{6}{2} = 15$ pairs of chords. Out of these we take into account *only those pairs having no point common*. (The pairs with one point common have already been considered). These are again exactly 3. E.g. $\{A, B, C, D\}$ gives rise to the pairs $\{AB, CD\}$, $\{AD, BC\}$ and $\{AC, BD\}$. In this way, we have counted all the earlier pairs of chords. Hence the second method of counting pairs of chords gives their number as $3\binom{n+1}{4}$.

Hint for 5. First show that two of the points, say A and B, can be chosen so that the remaining points, say P, Q, R, lie on the same side of the line AB. Show that the angles $\angle APB$, $\angle AQB$, $\angle ARB$ are all of different sizes. We may suppose then that $\angle APB < \angle AQB < \angle ARB$. Hence the circle through A, B and Q contains R in its interior and P in its exterior.

Generalization: Consider $2n + 3$ points. (5 is the case $n = 1$) then there is a circle through 3 of the points with n points inside and n points outside the circle.

Hint for 6. Consider the set $A = \{2^{k-1}+1, 2^{k-1}+2, \ldots, 2^k - 1\}$. Ans. $m = 2^{k-1} - 1$.

4.6 Miscellaneous Problems

Example 5 Let $a_1, \ldots, a_{10}$ be ten real numbers such that each is greater than 1 and less than 55. Prove that there are three among the given numbers which form the lengths of the sides of a triangle.

Solution: Without loss of generality, we may take

$$1 < a_1 \leq a_2 \leq \ldots \leq a_{10} < 55. \qquad \text{(i)}$$

Let, if possible, no three of the given numbers be the lengths of the sides of any triangle. We will consider the triplets a_i, a_{i+1}, a_{i+2}, $1 \leq i \leq 8$. As these numbers do not form the lengths of the sides of a triangle, the sum of the smallest two numbers should not exceed the largest number i.e. $a_i + a_{i+1} \leq a_{i+2}$. Hence,

$i = 1$ gives $a_1 + a_2 \leq a_3$ giving $2 < a_3$.
$i = 2$ gives $a_2 + a_3 \leq a_4$ giving $3 < a_4$.
$i = 3$ gives $a_3 + a_4 \leq a_5$ giving $5 < a_5$.
$i = 4$ gives $a_4 + a_5 \leq a_6$ giving $8 < a_6$.
$i = 5$ gives $a_5 + a_6 \leq a_7$ giving $13 < a_7$.
$i = 6$ gives $a_6 + a_7 \leq a_8$ giving $21 < a_8$.
$i = 7$ gives $a_7 + a_8 \leq a_9$ giving $34 < a_9$.
$i = 8$ gives $a_8 + a_9 \leq a_{10}$ giving $55 < a_{10}$,

contradicting (i).
Hence there exist three numbers among the given numbers which form the lengths of the sides of a triangle.

Example 6 In a collection of 1234 persons any two persons are mutual friends or enemies. Each person has at most 3 enemies. Prove that it is possible to divide this collection into two parts such that each person has at most 1 enemy in his subcollection.

Solution. Let C denote the collection of given 1234 persons. Let $\{C_1, C_2\}$ be a partition of C. Let $e(C_1)$ denote total number of enemy pairs in C_1. Let $e(C_2)$ denote the total number of enemy pairs in C_2.
Let $e(C_1, C_2) = e(C_1) + e(C_2)$ denote the total number of enemy pairs *corresponding* to this partition $\{C_1, C_2\}$ of C. Note $e(C_1, C_2)$ is an integer ≥ 0. Hence by Well-ordering principle there exists a partition having the least value

of $e(C_1, C_2)$.
Claim: This is a required partition.
If not, without loss of generality suppose there is a person P in C_1 having at least 2 enemies in C_1. Construct a new partition $\{D_1, D_2\}$ of C as follows: $D_1 = C_1 - \{P\}$ and $D_2 = C_2 \cup \{P\}$. Now
$e(D_1, D_2) = e(D_1) + e(D_2) \leq [e(C_1) - 2] + [e(C_2) + 1] = e(C_1, C_2) - 1$
Hence, $e(D_1, D_2) < e(C_1, C_2)$, contradicting the minimality of $e(C_1, C_2)$.

Example 7 A barrel contains $2n$ balls, numbered 1 to $2n$. Choose three balls at random, one after the other, and with the balls replaced after each draw.

What is the probability that the three element sequence obtained has the properties that the smallest element is odd and that only the smallest element, if any, is repeated?

Solution: The total number of possible outcomes is $N = 2n \times 2n \times 2n = 8n^3$. To find the total number of favourable outcomes we proceed as follows:

Let a be any odd integer such that $1 \leq a \leq 2n - 1$ and let us count the sequences having a as least element.

(i) There is only one sequence (a, a, a) with a repeated thrice.

(ii) There are $2n - a$ sequences of the form (a, a, b) with $a < b \leq 2n$. For each such sequence there are three distinct permutations possible. Hence there are in all $3(2n - a)$ sequences with a repeated twice.

(iii) When $n > 1$, for values of a satisfying $1 \leq a \leq (2n - 3)$, sequences of the form (a, b, c) with $a < b < c \leq 2n$ are possible and the number of such sequences is $r = 1 + 2 + \cdots + (2n - a - 1) = \frac{1}{2}(2n - a)(2n - a - 1)$. For each such sequence there are six distinct permutations possible. Hence there are $6r = 3(2n - a)(2n - a - 1)$ sequences in this case.

Hence, for odd values of a between 1 and $2n - 1$, the total counts of possibilities S_1, S_2, S_3 in the above cases are respectively

$$S_1 = 1 + 1 + \cdots + 1 = n, \quad S_2 = 3\,[\,1 + 3 + 5 + \cdots + (2n - 1)\,] = 3n^2,$$
$$S_3 = 3\,[\,2 \times 3 + 4 \times 5 + \cdots + (2n - 2)(2n - 1)\,] = n(n - 1)(4n + 1).$$

Hence the total number A of favourable outcomes is $A = S_1 + S_2 + S_3 = n + 3n^2 + n(n - 1)(4n + 1) = 4n^3$. Hence the required probability is

$$\frac{A}{N} = \frac{4n^3}{8n^3} = \frac{1}{2}.$$

♣♣♣

Regional Mathematical Olympiads in India

With a view to locate and then nurture Mathematical talent among school going children in India, an elaborate scheme has been drawn up by the National Board for Higher Mathematics (NBHM). Under this scheme, Regional Mathematical Olympiads (RMO) are held in various regions across the country. More information and the exact date can be obtained from the concerned regional/group coordinators. The list of the coordinators is given at the end of this write up. Primarily, students of Std. XI and XII (first and second year of Junior College) can appear for RMO. But the students of Std. VIII, IX or X are also eligible to appear for RMO. The top 15 to 30 students from each region/group selected in RMO, including at most 6 students from Std. XII, will be invited to write the Indian National Mathematical Olympiad (INMO).There is no fixed syllabus for RMO or INMO. Problems asked are of a non-routine type but within the capacity of a bright talented 15 year old student. The top 30 students of INMO (called INMO Awardees) would be invited to a Summer Camp at HBCSE, Mumbai in May-June. All these students, and also INMO-awardees of the previous years who are still pre-university students and who show good performance in postal correspondence during the academic year, would be eligible to be selected to the Indian team for participation in International Mathematical Olympiad (IMO). The selection of the team is done during the Summer Camp.

INMO awardees may take up any branch of study in future and if they give evidence of their continued interest in mathematics, they will be eligible for NBHM scholarships. NBHM organises Nurture Programs every year in summer vacation for these talented students.

National Coordinator, Prof. R. B. Bapat
Indian Statistical Institute, 7, S.J.S. Sansanwal Marg, New Delhi-110016.
email: *rbb@isid.ac.in*

List of Regional Co-ordinators

1. **Region Costal AP & Rayalaseema** Prof. David Kumar, Commissionerate of Collegiate Education, Govt. of Andhra Pradesh, Opp. To Latha complex, Namapally (Station), Hyderabad -500 001
   Ph.: 040 - 2461 7469 Fax: 040 - 2460 2285, 2461 7469
   E-mail: rdkumar1729@yahoo.com rdkumar1729@gmail.com
2. **Region Telangana Prof. R. Kedareshwar Rao** Dept. of Mathematics, Acharya Aryabhata University,Vignan Vidyalayam, Nizampet, opp.

JNTU Kikatpally,Hyderabad - 500 072. Ph. (040) - 2461 7469, (040) - 2301 1853, e-mail:kedar_rudra@yahoo.co.in

3. **Region South Bihar Prof R K Das** Lal Bagh, Tilakamanjhi, Police Line Road Bhagalpur 812 001, Bihar Ph.: (0641) - 2611 236.

4. **Region North Bihar Azhar Hussain** Dept. of Mathematics Veer Kunwar Singh University Ara (Bihar) Email: hussainazhar@yahoo.com

5. **Region Delhi Prof Amitabh Tripathi** Dept of Mathematics IIT, Hauz Khas, New Delhi 110 016 Ph.: (011) - 2689 6831 (011)- 2659 1486 E-mail: atripath@maths.iitd.ernet.in at1089@rediffmail.com

6. **Region Gujarat Prof. I. H. Sheth** Dept of Mathematics, School of Sciences Gujarat University Navrangpura, Ahmedabad 380 009.
Ph.: (079) - 2630 1154 (O)
E-mail: ganit_spardha@yahoo.co.in, yisheth@yahoo.co.in

7. **Region Jharkhand Dr. K. C. Prasad** Dean faculty of science Ranchi University, Dept. of Mathematics,Morabadi Campus, Ranchi 834 008 Ph.: 0651 -2233 877 / 2233 127 (O) Fax: 0651 - 2233 877.
e-mail: kcprasad1@rediffmail.com

8. **Region Karnataka Dr. B. Sury** (RMO) Stat math Unit Indian Statistical Institute 8th Mile Mysore Road, RV College Post Bangalore 560059 Ph: (080) 28483002/ 06 Extn. 445 (O) (080) 28484265 (F)
Email: sury@isibang.ac.in

9. **Region Karnataka Dr. A. K. Nandakumaran (INMO)** Dept of Mathematics IISc Bangalore 560 012 Ph.: (080) - 2293 2265
e-mail: nands@math.iisc.ernet.in

10. **Region Kerala Dr. Ambat Vijaykumar** Reader Dept of Mathematics Cochin University of Science & Technology Cochin 682 022 Ph.: (0484) - 2577 518 (O) e-mail: ambatvijay@rediffmail.com vijayambat@member.ams.org vijay@cusat.ac.in

11. **Region MP Shri Anantram R. Pathak** Director, State Institute of Science Education (SISE) P. S. M. Campus, Jabalpur 482 001 Ph.: (0761) - 2625 776 (O) Dr. Rajendra Pandey Fax: 0761 4004206

12. **Region Chhattisgarh Dr. V. K. Pathak,** Asst. Professor (Mathematics) Govt. P.G. College, Dhamtari Chattisgarh : 493773 Ph. 07722-Fax: 07722- 237933 Email: vkpath21162@yahoo.co.in

13. **Region Maharashtra & Goa Dr. V. V. Acharya** c/o Bhaskaracharya Pratishthan 56/14, Erandawane, V. Damle Path Off Law College Road Pune 411 004. Ph.: (020) -2543 4547/2541 0724 (O)
E-mail: vvacharya@yahoo.com, rmomaha@yahoo.co.in, rmomaths@gmail.com

14. **Region Mumbai Prof. Arvind Kumar / Prof. H. C. Pradhan** HBCSE, TIFR, V N Purav Road, Mankhurd 400 088.
E-mail: arvindk@hbcse.tifr.res.in, hcp@hbcse.tifr.res.in

15. **Region North East Prof. M. B. Rege** Dept of Mathematics, North-Eastern Hill University Permanent Campus Mawlai, Shillong, Meghalaya 793 022. Ph.: (0364) - 2550083.
e-mail: mb29rege@yahoo.co.in

16. **Region Tripura Prof. Dipankar De,** Asstt.Prof. (Sel. Gr.) Department of Mathematics Ramthakur College Agartala-799003, Tripura L-line:03812230295 Fax: (0381)2326503
E-mail: rtc_tu@yahoo.com; dipankardee@yahoo.co.in.

17. **Region North West Dr. V. K. Grover** Dept of Mathematics,Punjab University, Chandigarh 160 014. Ph.: 0172 - 2534 510 (O) 2711 317 (R) 98884 86387 (m) e-mail: grovervk@pu.ac.in vk_gvr@yahoo.com

18. **Region Rajasthan Dr. A. K. Mathur** Regional Coordinator, INMO, Dept of Mathematics, University of Rajasthan, Jaipur 302 004
Ph.: 0141 - 3708 392 (O) 2550 377 (R) 93145 29855 (M)

19. **Region Orissa Prof. Sudarshan Padhy** Dept of Mathematics,Utkal University, Bhubaneshwar 751 004
Ph.: (0674) - 2582 301 (O) E-mail: spadhy@sancharnet.in

20. **Tamilnadu Prof. K. N. Ranganathan** Dept of Mathematics Ramkrishna Mission's Vivekananda College, Chennai 600 004 Ph.: (044) - 28342651 e-mail: hurrrahs@vsnl.com knranga@dataone.in

21. **UP Prof. D. P. Shukla** Dept of Mathematics & Astronomy Lucknow University Lucknow 226 007. Ph.: (0522) - 2740 019 (O) Email dpshukla3@gmail.com

22. **Region Uttarakhand Prof. M. C. Joshi** Dept of Maths, Stats & Comp. Science, Gobind Ballabh Pant Agri. & Tech. University, Pantnagar 263 145, Uttaranchal. Ph.: (05944) - 234 559 (R).
e-mail: mcjoshi69@gmail.com, mcjoshi@gmail.com

23. **Region WB Dr. Pradipta Bandyopadhyay** ISI, 202 B T Road, Kolkata 700 108. Ph. (033) - 2575 3422, Fax : 91 - 33 - 2577-3071. e-mail: pradipta@isical.ac.in e-mail: pradiptabandyo@yahoo.co.uk

24. **Region J & K Dr. Bashir Ahmed Zargar** Department of Mathematics University of Kashmir Srinagar - 190006 Ph. (0952) 257347 e-mail : zargarba3@yahoo.co.in

25. **Region KVS Mr. G.S. Lawania** KVS Mathematics Olympiad, Kendriya Vidyalaya NTPC, Badarpur New Delhi 110 044. Ph.: 98914 26013 E-mail: gslawania@rediffmail.com

26. **Region CBSE Director (Academic)** Central Board of Secondary Education Shiksha Kendra Bhavan 2, Commercial Centre, New Delhi 110 092. Ph: 2322 0154 (Dir) / 2251 5829

27. **Region NVS Prof. H.N.S. Rao** Dy. Commissioner, Navodalaya Vidyalaya of Navodaya Vidyalaya Samiti Regional Office A-28, Kailash Colony New Delhi 110 048. Ph.: (011) 2642 4162(O)

Bibliography

Recommended Books

1. **V. K. Balakrishnan**, Combinatorics, Schuam Series, 1995.

2. **S. Barnard and J.M. Child**, Higher Algebra, Macmillan and Co., London, 1939; reprinted Surjeet Pbl. Delhi, 1990.

3. **W.S. Burnside and A.W. Panton**, The Theory of Equations: Vol 1 (13th Ed.), S. Chand and Co. Ltd., New Delhi 1990.

4. **David M. Burton**, Elementary Number Theory (Second Ed.), Universal Book Stall, New Delhi, 1991.

5. **H.S.M. Coxeter and S.L. Greitzer**, Geometry Revisited: New Mathematical Library 19, The Mathematical Association of America, New York, 1967.

6. **Clement V. Durell**, Modern Geometry, Macmillan and Co., London, 1961.

7. **H.S. Hall and S. R. Knight**, Higher Algebra, Macmillan and Co., London, (Metric Ed.) Delhi, 1983.

8. **V. Krishnamurthy, K.N. Ranganathan, B.J. Venkatachala and C.R. Pranesachar**, Challenges and Thrills of Pre-College Mathematics, Wiley Eastern Ltd., New Delhi, 2007.

9. **I. Niven and H.S. Zuckerman**, An Introduction to the Theory of Numbers (Fifth Ed.), Wiley Eastern Ltd., New Delhi, 1991.

10. **A. Subramanian and S. Murlidharan**, Triangles: Construction and Inequalities, The Association of Mathematics Teachers of India, Madras, 1992.

11. **Dimitri Fomin**, Mathematical Circles, University Press, 2005.

Books for further reading

1. **J.W. Archbold**, Algebra (Fourth Ed.), ELBS and Pitman Publishing, London, 1970.

2. **V. K. Balakrishnan**, Introductory Discrete Mathematics, Prentice Hall, 1991.

3. **Richard A. Brualdi**, Introductory Combinatorics, Elsevier, North-Holland, New York, 1977.

4. **Ross Honsberger**, Mathematical Gems I, 1973, II, 1976, III, 1985, The Mathematical Association of America (Inc.), New York.

5. **Nicholas D. Kazarinoff**, Geometric Inequalities: New Mathematical Library 4, Random House and The L.W. Singer Co., New York, 1961.

6. **P.P. Korovkin**, Inequalities: Little Mathematics Library, MIR Publishers, Moscow, 1975.

7. **I.S. Sominsky**, The Method of Mathematical Induction, MIR Publishers, Moscow, 1975.

8. **Alan Tucker**, Applied Combinatorics (Second Ed.), John Wiley and Sons, New York, 1984.

9. **G. N. Yakovlev**, (Ed.) High School Mathematics, Part II, MIR Publishers, Moscow, 1984.

Books on Problems

1. **Samuel L. Greitzer**, International Mathematical Olympiads 1959-1977: New Mathematical Library 27, The Mathematical Association of America, New York (1978), Indian Edition, Mathematical Association of India, New Delhi (1992).

2. **J.N.Kapur**, Mathematical Olympiad Problems Book I (1991), Books II, III (1992), Books IV, V, VI (1993), Mathematical Sciences Trust Soc., New Delhi.

3. **G. Kessler and L. Zimmerman**, NYSML-ARML Contests (1983 - 1988), National Council of Teachers of Mathematics Virginia, 1989, Indian Edition, 1991, Distributed by Math. Sci. Trust Soc, New Delhi.

4. **Murray S. Klamkin**, USA Mathematical Olympiads 1972-86: New Mathematical Library 33, The Mathematical Association of America, New York (1988), Indian Edition, Mathematical Association of India, New Delhi (1992).

5. **Murray S. Klamkin**, International Mathematical Olympiads I 1950-1977 and II 1978-1985: New Mathematical Library 31, The Mathematical Association of America, New York, (1986), Indian Edition, Mathematical Association of India, New Delhi (1992).

6. **V.A. Krechmar**, A Problem Book in Algebra, MIR Publishers, Moscow, 1974.

7. **C. R. Pranesachar, B. J. Venkatachala and C. S. Yogananda**, Problem Primer for the Olympiad, Interline Publishing, Bangalore, (Second Edition) 2007.

8. **I.F. Sharygin**, Problems in Plane Geometry, MIR Publishers, Moscow, 1988.

9. **D.O. Shklyarsky, N.N. Chentsov** and **I.M. Yaglom**, Selected Problems and Theorems in Elementary Mathematics, MIR Publishers, Moscow, 1979.

10. **A.M. Yaglom and I.M. Yaglom**, Challenging Mathematical Problems with Elementary Solutions, Vol. 1, Holden Day Inc., San Fransisco, London, Amsterdam, 1964.

11. **B. J. Venatachala**, Functional Equations, Prism, 2003.

12. **Arthur Engel**, Problem Solving Strategies, Springer, 1999.

Some Useful Mathematical Periodicals

1. **Bona Mathematica**, Bhaskaracharya Pratishthana, 56/14, Vishnupant Damle Path, Erandavana, Pune- 411 004.

2. **Crux Mathematicorum**, Canadian Mathematical Society, Ottawa, Canada.

3. **Mathematical Education**, (Quarterly), Journals division, Wiley Eastern Ltd.

4. **Mathematics Magazine**, Mathematical Association of America, Washington, USA.

5. **Samasyā**, The Secretary, Leelavati Trust, No.24, 21st Main, II Block, B. S. K. I stage, Bangalore - 560 050, India.

6. **The American Mathematical Monthly**, Mathematical Association of America, Washington, USA.

7. **The Mathematics Teacher**, The Association of Mathematics Teachers of India.

Index