Unit 1

1

DIVISIBILITY THEORY OF INTEGERS AND ARITHMETIC FUNCTIONS

Unit Structure :

1.0 Objectives

After reading this chapter, you will know about.

- Division Algorithm.
- The Greatest common divisor of two integers.
- The Euclidean Algorithm as a repetition of division algorithm.
- Solution to linear Diophantine equations.
- The concept of Congruence.
- Cardano's method to solve a general cubic equation.
- Quadratic Residues.
- Number - Theoretic functions like Möbius inversion formula, The greatest integer function etc.

1.1 INTRODUCTION

The theory of numbers starts with many properties of the integers and particularly with the positive integers 1, 2, 3…. when it comes to a question of checking whether a given integer *b* divides another integer *a*, we look for some integer *q* such that *a* = *bq* and conclude that the division is possible with $q = \frac{b}{a}$, one important theorem, explaining the division process in the integers is the division algorithm, roughly it states that an integer a can be divided by another integer *b* in such a way that the remainder has a magnitude smaller than *b*. Let us prove this theorem.

1.2 Theorem : Division Algorithm

Given integers *a* and *b*, with *b* > 0, there exist unique integers *q* and *r* satisfying $a = bq + r, 0 \le r \le b$. The integers *q* and *r* are called, quotient and remainder in the division of *a* by *b*.

Proof :

We show that the set $S = \{a - xb \,|\, x \text{ is an integer}, a - xb \ge 0\}$ is a non-empty set. For this, it is enough to exhibit a value of *x*, making *a – xb* nonnegative. Since the integer $b \ge 1$, we have $|a|\, b \ge |a|$ and therefore $a - (-|a|)\, b = a + |a|\, b \ge a + |a| \ge 0$. Hence, for $x = -|a|, a - xb \in S$. By applying the well-ordering principle, the set *S* contains a smallest integer, call it *r*. By definition of S, there exists an integer *q* satisfying $r = a - qb, 0 \le r$, we argue that *r* < *v*. If $r \ge b$ then $a - (q+1)\, b = (a - qb) - b = r - b \ge 0 \Rightarrow a - (q+1)\, b \in S$. But $a - (q+1)\, b = r - b < r$, violating the fact that *r* is the smallest member of S. Hence *r* < *b*. We shall show that such *q* and *r* are unique. Suppose *a* can be represented by two expressions, say $a = qb + r = q'b + r'$, where $0 \le r < b, 0 \le r' < b$ then $r' - r = b(q - q') \Rightarrow 1r' - r' = b|q - q'|$. Also $-b < -r \le 0$ and therefore $0 - b < r' - r < b - 0 \Rightarrow -b < r' - r < b$, equivalently, $|r' - r| < b$. Thus $b|q - q'| < b \Rightarrow 0 \le |q - q'| < 1$. Now $|q - q'|$ is a nonnegative integer, therefore the only possibility is that $|q - q'| = 0, \Rightarrow q - q' = 0 \Rightarrow q = q'$, this gives that $r = r'$.

To understand the Division Algorithm, when $b<0$, take $b=-7$. Then for the choices of a = 1, – 2, 61 and – 59, we get the expressions

$$1 = 0\ (-1) + 1$$

$$-2 = 1\ (-7) + 5$$

$$61 = (-8)\ (-7) + 5$$

$$-59 = 9\ (-7) + 4.$$

As one of the application of the division algorithm, we show that the square of any odd integer is of the form $8k + 1$.

By division algorithm, any integer is described as one of the four forms $4k$, $4k + 1$, $4k + 2$, $4k + 3$. In this form only those integers of the form $4k + 1$ and $4k + 3$ are odd.

$$\because (4k+1)^2 = 8\left(2k^2+k\right)+1 = 8k'+1 \text{ and similarly}$$

$$(4k+3)^2 = 8\left(2k^2+3k+1\right)+1 = 8k'+1.$$

For example, the square of the odd integer 7 is $7^2 = 49 = 8.6+1$.

1.3 The Greatest Common Divisor

When the remainder $r = 0$ in the division algorithm, such cases are of special significance.

Definition of divisibility:

An integer b is divisible by an integer $a \neq 0$, symbolically $a \mid b$, if there exists some integer c such that $b = ac$. We write $a \nmid b$ to indicate that b is not divisible by a.

For example, – 12 is divisible by 4, since –12 = 4 (–3). However, 10 is not divisible by 7; for there is no integer c, which makes the statement $10 = 7c$ true. When a divides b, we say that b is a multiple of a whenever $a \mid b$, a also divides $-b$. Therefore to find all divisers of a given integer, it is sufficient to obtain the positive divisers and then adjoin them with the corresponding negative integers. Let us state the consequences of the above definition.

Theorem : For integers *a*, *b*, *c* the following hold :

1) a / 0, 1 /a, a / a.
2) a / 1 if and only if $a = \pm 1$.
3) If a / b and c / d then ac / bd.
4) IF a / b and b / c, then a / c.
5) if a / b and b / a then $a = \pm b$.
6) If a / b and b # 0, then $|a| \le |b|$.
7) If a / b and a / c, then a / (bx + cy) for any choice of integers x and y.

Proof :

We shall prove only (6) and (7).

If a / b then there exists on integer C. such that b = ac; also $b \neq 0 \Rightarrow c \neq 0$. Taking absolute values, $\because |b| = |ac| = |a||c|$. Since c # 0, it follows that $|c| \ge 1$. $\because |b| = |a||c| \ge |a| \Rightarrow |a| \le |b|$. To prove (7), a/b and $a / c \Rightarrow b = ar$ and c = as for some integers r and s. Then $bx + cy = arx + asy = a(rx + sy)$, for any choice of integers x and y. This shows that $a \mid (bx + cy)$.

Definition :

If a and b are integers, then an integer d is said to be a common divisor of a and b if both d / a and d / b. Since 1 is a divisor of every integer, 1 is a common divisor of a and b, hence the set of positive divisions for a and b is not empty when, at least one of a or b is different from zero, there are only a finite number of positive common divisions among these, there is largest one, called the greatest common divisor of a and b.

Definition :

Let a and b be given integers, with atleast one of them different from zero. The greatest common divisor of a and b is denoted by gcd (a, b), it is the positive integer d satisfying

1) d / a and d / b.
2) If c / a and c / b, then c / d.

For example the positive divisors of - 12 are 1, 2, 3, 4, 6, 12, while the positive divisors of 30 are 1,2,3,5,6,10,15,30; hence, the positive common divisors of - 12 and 30 are 1,2,3,6 since 6 is the largest, it follows that gcd (-12, 30) = 6. In the same way, one can show that gcd (-5, 5) = 5, gcd (8, 17) = 1 and gcd (-8, -36) = 4. The next theorem shows that gcd(a,b) = ax + by for some integers x and y, say gcd (-8, -36) = 4 = (-8) 4 + (-36) (-1).

Theorem :

Given integers a and b, not both of which are zero, there exist integers x and y such that gcd(a, b) = ax + by.

Proof :

Consider the set S of all positive linear combinations of a and b. $S = \{au + b\upsilon / au + b\upsilon > 0, u, \upsilon \text{ are integers}\}$. Notice that S is not empty. For example, if a # 0, then $|a| = au + b0$ will lie in S, if we choose u = 1 or u = -1, according to as a is positive or negative. By virtue of the well-ordering principle, s must contain a smallest element d.

$\therefore$ There exist integers x and y, for which d = ax + by. We claim that d = gcd(a, b) using the division algorithm, one can find q and r such that a = qd + r, $o \le r < d$.

Then r can be written in the form $\begin{aligned} r = a - qd &= a - q\,(ax + by) \\ &= a(1 - qx) + b\,(-qy) \end{aligned}$

$\Rightarrow r \in S$ and r < d, a contradiction to assumption that d is the smallest member of S. therefore $r = 0 \Rightarrow a = qd$ or d / a. By similar reasoning $d / b \Rightarrow d$ is a common divisor of both a and b.

If c/a and c/b then $c / ax + by \Rightarrow c / d \Rightarrow c = |c| \le |d| = d$ so that d is greater than every positive common divisor of a and b. $\Rightarrow d = \gcd(a, b)$.

It may happen that 1 and -1 are the only common divisors of a given pair of integers a and b $\Rightarrow \gcd(a,b) = 1$. For example, $\gcd(2,5) = \gcd(-9,16) = 1$.

Definition :

Two integers a and b, not both zero, are said to be relatively prime, whenever gcd(a, b) = 1.

Theorem :

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

Proof :

Let a, b be relatively prime numbers, then $\gcd(a,b) = 1 \Rightarrow$. There exist integers x and y such that 1 = ax + by. Conversely, if $1 = ax + by$ for some choice of integers x and y and $d = \gcd(a,b) \Rightarrow d / ax + by$ or d / 1, $d \geq 0 \Rightarrow d = 1$.

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

Proof :

If $d = \gcd(a,b) \Rightarrow$ these exist integers x and y such that $d = ax + by$, after dividing throughout by d, we get $1 = \left(\frac{a}{d}\right) xf \left(\frac{b}{d}\right) y$. $\Rightarrow \left(\frac{a}{d}\right)$ and $\left(\frac{b}{d}\right)$ are relatively prime $\therefore \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

For example, gcd(-12, 30) = 6 and gcd(-12/6, 30/6) = gcd(-2,5) = 1.

Theorem : (Euclid's lemma) :

If a / bc, with gcd(a, b) = 1, then a/c.

Proof :

$\gcd(a,b) = 1 \Rightarrow$ There exist integers x and y such that $1 = ax + by$ multiplying throughout by C gives $c = 1.c = (ax + by)\, C = acx + bcy$. Since a / ac and $a / bc \Rightarrow a / (acx + bcy) \Rightarrow a / c$.

If a and b are not relatively prime, then the conclusion may fail to hold. For example, 12/9.8 but 12 doesn't divide 8 or 9.

Theorem :

Let a, b be integers, not both zero. For a positive integer d, $d = \gcd(a,b)$ if and only if

1) d/a and d/b.

2) Whenever c/a and c/b then c/d.

Proof :

Suppose that $d = \gcd(a,b) \Rightarrow$ d/a and $d \,/\, b \Rightarrow d$ is expressible as d = ax + by for some integers x and y. Thus, if c/a and c/b then $c \,/\, (ox + by)$ or c/d. conversely, let d be any positive integer such that d/a and d/b and whenever c/a and c/b then $c \,/\, d \Rightarrow d \geq c \Rightarrow d$ is the greatest common divisor of both a and b.

1.4 Euclidean Algorithm

A more efficient process, involving repeated application of the division algorithm is known as the Euclidean Algorithm. The Euclidean algorithm can be described as following :

Let a and b be two integers, whose gcd is to be calculated. Since $\gcd(|a|,|b|) = \gcd(a,b)$. Assume that $a \geq b > o$. The first step is to apply the division algorithm to a and b to get $a = q_1 b + r, o \leq r_1 < b$. Were $r_1 = o$ or $r_1 > 0, r_1 = 0 \Rightarrow b \,/\, a$ and gcd(a,b) = b. when $r_1 \neq o$, divide b by r_1 find integers q_2 and r_2 such that $b = q_2 r_2 + r_2, o \leq r_2 < r_1$.

If $r_2 = o$ then stop, otherwise proceed as before to obtain r_3 and q_3 such that $r_1 = q_3 r_2 + r_3, o \leq r_3 < r_2$. This process continues until some zero remainder appears, say at (n + 1)th step, r_{n-1} is divided by r_n.

The result is the following system :

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

We claim that r_n, the last nonzero remainder in these steps, is equal to gcd(a,b).

Lemma : If a = qb + r, then $\gcd(a,b) \Rightarrow \gcd(b,r)$.

Proof : Let . $\Rightarrow d / a$ and $d / b \Rightarrow d / (a - qb)$ or d/r. Thus d is a common divisor of both b and r on the other hand, if c is an arbitrary common divisor of b and r, then $c / (qb + r) \Rightarrow c / a$. This make c a common divisor of a and $b \Rightarrow c \le d$. Therefore d = gcd(b,r) using this lemma, for the given system.

$$\because \gcd(a,b) = \gcd(b,r_1) = \gcd(r_{n-1}, r_n)$$
$$= \gcd(r_n, o) = r_n$$

Example

To calculate gcd (12378, 3054)

Write $12378 = 4 \times 3054 + 162,$

$$3054 = 18 \times 162 + 138,$$
$$162 = 1 \times 138 + 24,$$
$$138 = 5 \times 24 + 18,$$
$$24 = 1 \times 18 + 6,$$
$$18 = 3 \times 6 + 0$$

$$\Rightarrow 6 = \gcd(12378, 3054)$$

To express 6 as a linear combination of 12378 and 3054, following is the procedure.

$$\therefore 6 = 24 - 18$$
$$= 24 - (138 - 5 \times 24)$$
$$= 6 \times 24 - 138$$
$$= 6(162 - 138) - 138$$
$$= 6 \times 162 - 7 \times 138$$
$$= 6 \times 162 - 7(3054 - 18 \times 162)$$
$$= 132 \times 162 - 7 \times 3054$$
$$= 132(12378 - 4\,3054) - 7 \times 3054$$
$$= 132 \times 12378 + (-535) \times 3054$$

Thus, we get $6 = \gcd(12378, 3054) = 12378x + 3054y$ where x = 132 and y = -535.

An important consequence of the Euclidean Algorithm is the following theorem.

Theorem :

If k > 0, then gcd (ka, kb) = k gcd (a,b).

Proof :

Let $d = \gcd(ka, kb) \Rightarrow$ There exist integers x and y such that $d = (ka)x + (kb)y = k(ax + by \Rightarrow k / d$ suppose that $d = k\ell$ for some integer ℓ. We shall claim that $\ell = \gcd(a,b)$.

Since $d = \gcd(ka, kb) \Rightarrow d / ka$ and $d / kb \Rightarrow \left(\frac{d}{k}\right) / a$ and $\left(\frac{d}{k}\right) / b$. Hence ℓ / a and ℓ / b. Assume that some integer c/a and $c / b \Rightarrow c / ax + by$. Therefore c/d. Applying the theorem on gcd, we obtain $\frac{d}{k} = \ell = \gcd(a,b)$

$$\Rightarrow d = R \gcd(a,b)$$

$$\Rightarrow \gcd(ka, kb) = k \gcd(a,b)$$

There is a concept parallel to that of the gcd of two integers, known as their least common multiple.

Definition :

An integer *C* is said to be a common multiple of two non zero integers *a* and *b* whenever *a/c* and *b/c*. 0 is a common multiple of *a* and *b*. The products *-(ab)* and *ab* are both common multiples of a and b. By well-ordering principle, the set of positive common multiples of a and b must contain a smallest integer, we call it the least common multiple of and b. here we define it formally.

Definition :

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

1) *a/m* and *b/m,*

2) If *a/c* and *b/c*, with *c>0*, then $m \leq c$.

For example, the positive common multiples of the integers - 12 and 30 are 60, 120, 180, …., hence *lcm(-12, 30) = 60.*

Note : Given nonzero integers a and b, *lcm(a,b)* always exists and $lcm(a,b) \le |ab|$.

To connect *gcd* and *lcm* of integers a and b, the following is a theorem.

Theorem :

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

Proof :

Let d = gcd(a,b) write a = dr, b = ds for integers r and s. If $m = ab/d$, then $m = as = rb \Rightarrow m$ is a common multiple of a and b. let *c* be any positive integer that is common multiple of a and b, say $c = au = b\upsilon$. As we know, there exist integers x and y satisfying $d = ax + by$. In consequence, $\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax+by)}{ab} = \left(\frac{a}{b}\right)x + \left(\frac{c}{a}\right)y = \upsilon x + uy \Rightarrow m/c \Rightarrow m \le c$. By definition $m = lcm(a,b)$, that is $lcm(a,b)\frac{ab}{d} = \frac{ab}{\gcd(a,b)} \Rightarrow \gcd(a,b) \times lcm(a,b) = ab$.

Corollary : Given positive integers a and b, $l.c.m.(a,b) = ab$ if any only if $g.c.d.(a,b) = 1$.

For example, we know that gcd(3054, 12378) = 6

$$\Rightarrow lcm(3054, 12378) = \frac{3054 \times 12378}{6} = 6,300,402.$$

We shall now take up the study of Diophantine equations. Any equation in one or more unknown, which is to be solved in the integers, is taken as the Diophantine equation. The simplest type of Diophantine equation that we will consider is the linear Diophantine equation in two unknowns $ax + by = c$, where a, b, c are given integers and a, b not both zero. A solution of this equation is a pair of integers x_0, y_0 such that $ax_0 + by_0 = c$. A given linear Diophantine equation can have a number of solutions, for example $3x + 6y = 18$ has many solutions.

$3 \times 4 + 6 \times 1 = 18;$
$3 \times (-6) + 6 \times 6 = 18;$
$3 \times 10 + 6 \times (-2) = 18$

Whereas the equation $2x+10y=17$ has no solution so, we shall discuss the circumstances under which a solution is possible to such a linear Diophantine equation.

1.5 Solving Linear Diophantine Equations

The Diophantine equation $ax+by=c$ has a solution if and only if *d/c*, where $d=\gcd(a,b)$.

Theorem :

The linear Diophantine equation $ax+by=c$ has a solution if and only if d/c, where $d=\gcd(a,b)$. If x_0, y_0 is any particular solution of this equation then all other solutions are given by $x=x_0+\left(\frac{b}{d}\right)t$, $y=y_0+\left(\frac{a}{d}\right)t$ for varying integers t.

Proof : Let $d=\gcd(a,b) \Rightarrow$ There exists integers r and s for which a = dr and b = ds. If a solution of $ax+by=c$ exists, so that $ax_0+by_0=c$ for suitable x_0 and y_0, then $c=ax_0+by_0=drx_0+dsy_0 \quad =d(rx_0+sy_0) \quad \Rightarrow d/c$. Conversely assume that d/c, say $c=dt \Rightarrow$ There exists integers x_0, y_0 satisfying $d=ax_0+by_0$, when this relation is multiplied by t, we get.

$c=dt=(ax_0+by_0)t=a(tx_0)+b(ty_0) \quad \Rightarrow$ the Diophantine equation $ax+by=c$ has $x=tx_0$ and $y=ty_0$ as particular solution.

Let us now suppose that a solution x_0, y_0 of the given equation is known if x^1, y^1 is any other solution, then $ax_0+by_0=c=ax^1+by^1$, which is equivalent to $a\left(x^1-x_0\right)=b\left(y_0-y^1\right)$.

By theorem, there exist relatively prime integers r and s such that a = dr, b = ds substituting these values in the last equation and canceling the common factor d, we find that $r\left(x^1-x_0\right)=s\left(y_0-y^1\right) \Rightarrow r/s\left(y_0-y^1\right)$ with $\gcd(r,s)=1$. $\therefore$ By Euclid's lemma, $r\left(y_0-y^1\right). \Rightarrow y_0-y^1=rt$ for some integer t.

$\Rightarrow x^1-x_0=st$

$$\Rightarrow x^1 - x_0 + st = x_0 + \left(\frac{b}{d}\right)t.$$

$$y^1 = y_0 - r^t = y_0 - \left(\frac{a}{d}\right)t.$$

It can be seen that these values satisfy the Diophantine equation,

$$\because ax^1 + by^1 = a\left[x_0 + \left(\frac{b}{d}\right)t\right] + b\left[y_0 - \left(\frac{a}{d}\right)t\right]$$

$$= \left(ax_0 + by_0\right) + \left(\frac{ab}{d} - \frac{ab}{d}\right)t$$

$$= c + ot = c$$

Thus there are an infinite number of solutions of the given equation, one for each value of *t.*

Example :

Consider the linear Diophantine equations $172x + 20y = 1000$.

To find $\gcd(172, 20)$. Apply Euclid's Algorithm,

$$\because 172 = 8 \times 20 + 12,$$
$$20 = 1 \times 12 + 8,$$
$$12 = 1 \times 8 + 4,$$
$$8 = 2 \times 4 + 0$$

$\Rightarrow \gcd(172, 20) = 4$. Since $4 / 1000$ a solution to this equation exists. To obtain 4 as a linear combination of 172 and 20,

$$4 = 12 - 8$$

$$= 12 - (20 - 12)$$
$$= 2 \times 12 - 20$$
$$= 2(172 - 8 \times 20) - 20$$
$$= 2 \times 172 + (-17) \times 20$$

By multiplying throughout by 250, we obtain

$$1000 = 250 \times 4 = 250 \times [2 \times 172 + (-17) \times 20]$$
$$= 500 \times 172 + (-4250) \times 20$$

$\Rightarrow x = 500$ and y = - 4250 is a solution. All other solutions are given by

$$x = 500 + \left(\frac{20}{4}\right)t = 500 + 5t$$

$$y = -4250 - \left(\frac{172}{4}\right)t = -4250 - 43t \text{ form integer t.}$$

If we put t = - 99, we get a positive solution x = 5, y= 7.

Corollary :

If gcd(a, b) = 1 and if x_0, y_0 is a particular solution of the linear Diophantine equation $ax + by = c$ then all solutions are given by $x = x_0 + bt$, $y = y_0 - at$ for integral values of t.

For example, the equation 5x + 22y = 18 has $x_0 = 8, y_0 = -1$ as one solution, from the corollary, a complete solution is given by $x = 8 + 22t, y = -1 - 5t$ for arbitrary t.

In the following section, we shall see the cardanos method for finding roots of cubic polynomials.

1.6 Cardanos Method

Given a cubic polynomial in unknown x, $x^3 + ax^2 + bx + c = 0$, eliminate the square term by using the substitution $x = t - \frac{a}{3}$

$$\Rightarrow \left(t - \frac{a}{3}\right)^3 + a\left(t - \frac{a}{3}\right)^2 + b\left(t - \frac{a}{3}\right) + c = 0.$$

Therefore

$$t^3 - 3t^2\left(\frac{a}{3}\right) + 3t\left(\frac{a}{3}\right)^2 - \left(\frac{a}{3}\right)^3 + a\left[t^2 - \frac{2at}{3} + \left(\frac{a}{3}\right)^2\right] + bt - \frac{ab}{3} + c = 0$$

$$\Rightarrow t^3 - 3\left(\frac{at^2}{3}\right) + \frac{3a^2t}{9} - \frac{a^3}{27} + at^2 - \frac{2a^2t}{3} + \frac{a^3}{9} + bt - \frac{ab}{3} + c = 0$$

$$\Rightarrow t^3 + \left(b - \frac{a^2}{3}\right)t + c + \left(\frac{2a^3 - 9ab}{27}\right) = 0$$

Put $p = b - \frac{a^2}{3}$ and $q = c + \left(\frac{2a^3 - 9ab}{27}\right)$.

Then $t^3 + pt + q = 0$ is the reduced form of the given cubic equation. Now, let $t = \mu + \upsilon$ and rewrite the above equation as $(\mu + \upsilon)^3 + p(\mu + \upsilon) + q = 0$ or $\mu^3 + \upsilon^3 + (\mu + \upsilon)(3\mu\upsilon + p) + q = 0$. Set $3\mu\upsilon + p = 0$, then the above equation becomes $\mu^3 + \upsilon^3 = -q$. And we are left with these two equations.

$$\mu^3 + \upsilon^3 = -q$$

$$\mu^3\upsilon^3 = -p^3/27$$

Since these equations are the product and sum of μ^3 and υ^3 therefore these exist a quadratic equation $t^2 + qt - \frac{p^3}{27} = 0$ with roots μ^3 and υ^3. Therefore this equation has solutions as following.

$$\mu^3 = \left(\frac{-q}{2}\right) + \upsilon\left(\frac{-q^2}{4}\right) + \left(\frac{p^3}{27}\right)$$

$$\upsilon^3 = \left(\frac{-q}{2}\right) - \upsilon\left(\frac{q^2}{4}\right) + \left(\frac{p^3}{27}\right)$$

We must find the cube roots of these equations to solve for μ^3 and υ^3.

If $27q^2 + 4p^3 < 0$ then the roots will complex number. If $27q^2 + 4p^3 \geq 0$ then the roots are real numbers. Let us solve certain cubic polynomials by this method.

For example, consider the cubic equation $x^3 - 0.75x^2 + 0.1875x - 0.015625 = 0$; this equation has a form $x^3 + qx^2 + bx + c = 0$; therefore substitute $x = t - \frac{a}{3}$, to eliminate the x^2 term we get a new equation $t^3 + pt + q = 0$, where $p = b - \frac{a^2}{3}, q = c + \left(\frac{2a^3 - 9ab}{27}\right)$.

Here $p = 0.1878 - \frac{(-0.75)^2}{3} = 0$

$$q = -0.015625 + \frac{2(-0.75)^3 - 9(-0.75)(0.1875)}{27} = 0$$

So, the new equation is $t^3 + ot + 0 = 0$, that is $t^3 = 0$. Since $27q^2 + 4p^3 = 0 \geq 0$, therefore all roots are real and equal to $-\frac{a}{3}$ because $x = t - \frac{a}{3} \Rightarrow x = -\frac{a}{3}(t = 0)$. $\therefore$ The roots are $x_1 = 0.25, x_2 = 0.25, x_3 = 0.25$. Let us consider another example, $x^3 + 6x^2 + 11x + 6 = 0$, after putting $x = t - \frac{a}{3}$, to eliminate x^2 term, we get new equation $t^3 + pt + q = 0, p = b - \frac{a^2}{3}, q = c + \left(\frac{2a^3 - 9qb}{27}\right)$.

Here $p = 11 - \frac{6^2}{3} = -1$,

$$q = 6 + \left(\frac{2\left(6^3\right) - 9(6)11}{27}\right) = 0$$

So, the new equation is $t^3 - 1t + 0 = 0$. $\Rightarrow t^3 - t = 0$, has a solution $t = 0$ or $t = \pm 1$.

If $t = 0$, $x = -\frac{a}{3} = -\frac{6}{3} = -2$, hence $x = -2$ is a root of the given equation. If $t = 1, x = 1 - \frac{6}{3} = -1$, hence $x = -1$ is another root of the given equation. For

$t=-1, x=-1-\frac{6}{3}=-3$, hence $x=-3$ is the third root of the given equation.

Gauss has introduced the concept of congruence and the notation, which makes it such a useful technique. According to Gauss. If a number *n* measures the difference between two numbers a and b, then a and b are said to be congruent with respect to *n*, if not then they are use called incongruent. Let us start with the definition of congruence relation.

1.7 Congruence Relations

Let *n* be a fixed positive integer. Two integers a and b are said to be congruent modulo *n*, write by $a \equiv b \pmod{n}$, if n divides the difference a - b; that is $a-b=kn,$ for some integer k.

For example, consider *n* = 7. we can see that $3 \equiv 24 \pmod 7), 7 / (24-3)$.

$-31 \equiv 11 \pmod 7), 7 / 11(-31)$

$-15 \equiv -64 \pmod 7), 7 / -64-(-15)$

If $n \chi(a-b)$, then we say that a is incongruent to b modulo n and in this case we write $a \not\equiv b \pmod{n}$. For example,e $25 \not\equiv 12 \pmod 7)$, because 7 doesnot divide 25 - 12 = 13.

Given an integer a, let q and r be it's quotient and remainder upon division by n, so that $a=qn+r, 0 \le r < n$.

Then by definition of congruence, $a \equiv r \pmod{n}$, because $n / (a-r) = qn$. Since there are *n* choices for r, we observe that every integer is congruent modulo n to exactly one of the values $0,1,2,\ldots,n-1$. The set of *n* - integers $\{0,1,2,..,\nu-1\}$ is called the set of least positive residues modulo *n*.

In general, a collection of *n* - integers $a_1, a_2, \ldots, a_n$ is said to form a complete set of residues modulo *n* if every integer is congruent modulo *n* to one and only one of the a_k. For example, $-12,-4,11,13,22,82,91$ form a complete set of residues modulo 7; here $\because -12 \equiv 2 \pmod 7), -4 \equiv 3 \pmod 7), 11 \equiv 4 \pmod 7), 13 \equiv 6 \pmod 7),$

$22 \equiv 1 \pmod 7), 82 \equiv 5 \pmod 7), 91 \equiv 0 \pmod 7)$.

We shall prove a theorem, which gives a useful characterization of congruence modulo *n* in terms of remainders upon division by *n*.

Theorem :

For arbitrary integers a and b, $a \equiv b \pmod{n}$ if and only if a and b leave the some non-negative remainder, when divided by *n*.

Proof :

Assume that $a \equiv b \pmod{n}$

$\Rightarrow a = b + kn$ for some integer *k*.

Let $b = qn + r, 0 \leq rcn$.

Then $a = b + kn = qn + r + kn = (q + k)n + r.$

$\Rightarrow a = \ell n + r, \ell = q + k$.

$\Rightarrow$ a leaves the same remainder *r,* upon division by *n*.

Conversely, assume that $a = q_1 n + r$ and $b = q_2 n + r$, with the same remainder $r(0 \leq r < n)$.

Then $\because a - b = q_1 n + r - (q_2 n + r) = (q_1 - q_2)n$.

$\Rightarrow n / a - b \Rightarrow a \equiv b \pmod{n}$. For example, - 56 and -11 can be expressed in the form - 56 = (-7) 9 + 7, -11 = (-2) 9 + 7 with the same remainder 7, hence from the above theorem, $-56 \equiv -11 \pmod{9}$ congruence relation can be considered as a generalized form of equality. Some of the basic properties of equality holds true in case of congruence's we propose to prove these properties as the next theorem.

Theorem :

Let *n > 0* be fixed and a, b, c, d be arbitrary integers. Then the following properties hold.

1. $a \equiv a \pmod{n}$.
2. If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.
3. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

4. If $a \equiv b(\text{mod}\, n)$ and $c \equiv d(\text{mod}\, n)$, then $a + c \equiv b + d(\text{mod}\, n)$ and $ac \equiv bd(\text{mod}\, n)$.

5. If $a \equiv b(\text{mod}\, n)$, then $a + c \equiv b + c(\text{mod}\, n)$ and $ac \equiv bc(\text{mod}\, n)$.

6. If $a \equiv b(\text{mod}\, n)$, then $a^k \equiv b^k (\text{mod}\, n)$ for any positive integer *k*.

Proof :

1. For any integer a, we have a - a = 0.*n*, so that $a \equiv a(\text{mod}\, n)$.

2. If $a \equiv b(\text{mod}\, n)$, then $a - b = kn$ for some integer *k*, Hence $b - a = -kn = (-k)n$, since $-k$ is an integer $\Rightarrow b \equiv a(\text{mod}\, n)$.

3. If $a \equiv b(\text{mod}\, n)$ and $b \equiv c(\text{mod}\, n)$ then $\exists$ integers k and ℓ satisfying, $a - b = kn$ and $b - c = \ell n$

   $\Rightarrow a - c = (a - b) + (b - c) = kn + \ell n = (k + \ell)n.$
   $\Rightarrow a - c = pn (p = k + \ell \text{ is an integer})$
   $\Rightarrow n / a - c \Rightarrow a \equiv c(\text{mod}\, n)$

4. If $a \equiv b(\text{mod}\, n)$ and $c \equiv d(\text{mod}\, n)$. Then $a - b = kn$, $c - d = qn$ for some integers *k* and *q*. Therefore, we obtain $(a + c) - (b + d) = (a - b) + c(-d) = kn + qn = (k + q)n$.

   $\Rightarrow n / (a + c) - (b + d)$
   $\Rightarrow a + c \equiv b + d(\text{mod}\, n)$

   Similarly $\because ac = (b + kn)(d + qn)$

   $$= bd + bqn + dkn + kqn^2$$

   $\Rightarrow ac = bd + (bq + dk + kqn)n.$

   $\Rightarrow ac - bd = pn,$ where $p = bq + dk + kqn$ is some integer.

   $\Rightarrow n / ac - bd \Rightarrow ac \equiv bd(\text{mod}\, n)$

5. Given that $a \equiv b(\text{mod}\, n)$, we know that $c \equiv c(\text{mod}\, n)$, by (4) we get, $a + c \equiv b + c(\text{mod}\, n)$ & $ac \equiv bc(\text{mod}\, n)$.

6. $a^k \equiv b^k \pmod{n}$ is true if $k = 1$. By induction hypothesis, assume that the result is true for $k = m$

$\Rightarrow a^m \equiv b^m \pmod{n}$

$\because a \equiv b \pmod{n}$ and applying (4), we get $a^{m+1} \equiv b^{m+1} \pmod{n}$. Therefore the result hold true for every positive integer $k, \Rightarrow a^k \equiv b^k \pmod{n}$, whenever $a \equiv b \pmod{n}$

For example, to show that 41 divides $2^{20} - 1$. Note that $2^5 \equiv -1 \pmod{41} \Rightarrow (25)^4 \equiv (-9)^4 \pmod{41} \Rightarrow 2^{20} \equiv 81.81 \pmod{41}$.

But $81 \equiv -1 \pmod{41} \Rightarrow 2^{20} \equiv 1 \pmod{41} \Rightarrow 41 / 2^{20} - 1$.

Theorem :

If $ca \equiv cb \pmod{n}$, then $a \equiv b \left(\bmod \frac{n}{d} \right)$, where $d = \gcd(c, n)$.

Proof :

$\because ca \equiv cb \pmod{n} \Rightarrow ca - cb = kn$ for some integer k.

Since $d = \gcd(c, n) \Rightarrow \exists$ relatively prime integers r and s s.t. $c = dr, n = ds$.

$\Rightarrow dra \equiv drb \pmod{n}$
$\Rightarrow dr(a - b) = kds$

$\Rightarrow r(a - b) = ks$. Hence $s / r(a - b)$.

Since $\gcd(r, s) = 1 \Rightarrow s / a - b$

$\Rightarrow a \equiv b \pmod{s}$. (B7 Eudid's Lemma).

For example, consider the congruence $33 \equiv 15 \pmod{9}$. $\Rightarrow 3.11 \equiv 3.5 \pmod{9}$. Since $\gcd(3, 9) = 3 \Rightarrow 11 \equiv 5 \pmod{3}$.

Now let us consider the congruence relation $ax^2 + bx + c \equiv 0 \pmod{p}$ whose p is a prime greater than 2 and $a \not\equiv 0 \pmod{p}$, that is, $\gcd(a, p) = 1$. The assumption that p is an odd prime implies that $\gcd(4a, p) = 1$. Therefore the given congruence is equivalent to $4a(ax^2 + bx + c) \equiv 0 \pmod{p}$.

$$\because 4a(ax^2+bx+c)=(2ax+b)^2-(b^2-4ac)$$
$$\Rightarrow (2ax+b)^2 \equiv (b^2-4ac)(\text{mod } p)$$

Now, put $y=2ax+b$ and $d=b^2-4ac$ to get $y^2 \equiv d(\text{mod } p)$.

If $x \equiv x_0(\text{mod } p)$ is a solution of the congruence $ax^2+bx+c \equiv 0(\text{mod } p)$, then $y \equiv (2ax_0+b) \bmod p$ satisfies the congruence $y^2 \equiv d(\text{mod } p)$.

Conversely, if $y \equiv y_0(\text{mod } p)$ is a solution of the congruence $y^2 \equiv d(\text{mod } p)$, then $2ax \equiv (y_0-b)(\text{mod } p)$ can be solved to obtain a solution of the congruence $ax^2+bx+c \equiv 0(\text{mod } p)$.

Thus a problem of finding a solution to the quadratic congruence $ax^2+bx+c \equiv 0(\text{mod } p)$ is same as that of finding a solution to a linear congruence and a quadratic congruence of the form $x^2 \equiv a(\text{mod } p)$.

If p/a then this congruence has $x \equiv 0(\text{mod } p)$ as the only solution. So, let us assume that $p \chi a$ consider a simple example of the congruence $5x^2-6x+2 \equiv 0(\text{mod}13)$. To obtain the solution, replace this congruence by $y^2 \equiv 9(\text{mod}13)(b^2-4ac=9)$.

Now this congruence has solutions $y \equiv 3 \bmod 13, y \equiv 10 \bmod 13$. Next, we solve the linear congruence $10x \equiv 9(\text{mod}13),\ \ 10x \equiv 16(\text{mod}13)$.

If can be checked that $x \equiv 10(\text{mod}13)$ and $x \equiv 12(\text{mod}13)$ satisfy these equations. Hence solving a linear congruence $2ax \equiv (y_0-b)(\text{mod } p)$ for x required a test for the existence of solutions of the congruence $x^2 \equiv a(\text{mod } p)$, $\gcd(a,p)=1$. In other words, we wish to find those integers a, which are perfect squares modulo p.

Definition :

Let p be an odd price and $\gcd(a,p)=1$. If the congruence $x^2 \equiv a(\text{mod } p)$, has a solution, then a is said to be a quadratic residue of p. otherwise, a is called a quadratic non residue of p.

For example, consider the case of the prime p = 13 we must know, which of the congruence $x^2 \equiv a(\text{mod}13)$ has a solution, when a runs through the set $\{1,2,..,12\}$. Modulo 13, the squares of the integers 1,2,3,…,12 are :

$1^2 \equiv 12^2 \equiv 1,$
$2^2 \equiv 11^2 \equiv 4,$
$3^2 \equiv 10^2 \equiv 9,$
$4^2 \equiv 9^2 \equiv 3,$
$5^2 \equiv 8^2 \equiv 12,$
$6^2 \equiv 7^2 \equiv 10$

Therefore, the quadratic residues of 13 are 1,3,4,9,10,12, while the non-residues are 2,5,6,7,8,11.

Euler stated a simple criterion for deciding whether an integer a is a quadratic residue of a given price p or not.

Theorem : (EULER'S CRITERION) :

Let p be an odd price and $\gcd(a, p) = 1$. Then a is a quadratic residue of p if and only if $a^{(p-1)/2} \equiv 1 (\text{mod}\, p)$.

Proof :

Suppose that a is a quadratic residue of p, so that $x^2 \equiv a(\text{mod}\, p)$ has a solution call it x_1. Since $\gcd(a, p) = 1 \Rightarrow \gcd(x_1, p) = 1$.

$\therefore$ By Fermat's theorem $a^{\frac{p-1}{2}} \equiv \left(x_1^2\right)^{(p-1)/2} \equiv x_1^{p-1} \equiv 1(\text{mod}\, p)$

$\Rightarrow a^{(p-1)/2} \equiv 1(\text{mod}\, p)$.

(Note : Fermats theorem says that, if p is a prime and $p \chi a$, then $a^{p-1} \equiv 1(\text{mod}\, p)$). Conversely, assume that $a^{(p-1)/2} \equiv 1(\text{mod}\, p)$.

Let r be a primitive root of p, that is $\gcd(r, p) = 1$ and $r^{\varnothing(p)} \equiv 1(\text{mod}\, p)$ $\Rightarrow a \equiv r^k (\text{mod}\, p)$ for some integer $k, 1 \le k \le p-1$.

$\Rightarrow r^{k(p-1)/2} \equiv a^{(p-1)/2} \equiv 1 \pmod{p}$

$\Rightarrow r^{k(p-1)/2} \equiv 1 \pmod{p}$

$\Rightarrow p-1 / (k(p-1)/2)$

$\therefore k$ is an even integer let $k = 2j$.

Hence $(rj)^2 = r^{2j} = r^k \equiv a \pmod{p}$

1.8 Quadratic Residue

Hence $x = r^j$ is a solution of the congruence $x^2 \equiv a \pmod{p}$. This prove that *a* is a quadratic residue of the prime *p*.

Corollary :

Let p be an odd prime and $\gcd(a, p) = 1$. Then a is a quadratic residue or non residue of p according as $a^{(p-1)/2} \equiv 1 \pmod{p}$ or $a^{(p-1)/2} \equiv -1 \pmod{p}$.

Proof :

If p is an odd prime and $\gcd(a, p) = 1$, then $\left(a^{(p-1)/2} - 1\right)\left(a^{(p-1)/2} + 1\right) = a^{p-1} - 1 \equiv 0 \pmod{p}$.

Hence either $a^{(p-1)/2} \equiv 1 \pmod{p}$ or $a^{(p-1)/2} \equiv -1 \pmod{p}$ but not both.

For example, if *p = 13*, we find that $2^{(13-1)/2} = 2^6 = 64 \equiv 12 \equiv -1 \pmod{13}$.

$\therefore 2$ is a quadratic non-residue of 13.

Since $3^{(13-1)/2} = 3^6 = (27)^2 \equiv 1^2 \equiv 1 \pmod{13}$, the corollary indicates that 3 is a quadratic residue of 13 and so the congruence $x^2 \equiv 3 \pmod{13}$ is solvable.

Certain functions are of special importance in connection with the study of the divisors of an integer. Any function whose domain is the set of positive integers is said to be an arithmetic function. In the following section, we shall study certain number - theoretic functions.

1.9 Number Theoretic/Arithmetic Functions

Definition :

Given a positive integer *n*, let of $\tau(n)$ denote the number of positive divisors of *n* and $\sigma(n)$ denote the sum of these divisors.

For example, consider *n* = 12, since 12 has the positive divisors $1, 2, 3, 4, 6, 12$ we find that $\sigma(12) = 6$ and $\sigma(12) = 1+2+3+4+6+12 = 28$.

Let us introduce a notation $\sum_{d/n} f(d)$ to mean, the sum of values of $f(d)$ as *d* runs over all positive divisors of the positive integers *n*. For instance, we have

$\sum_{d/20} f(d) = f(1) + f(2) + f(4) + f(5) + f(10) + f(20)$ with these understanding, of and $\sigma(n) = \sum_{d/n} 1$, $\sigma(n) = \sum_{d/n} d$. If $n = 10$, $\tau(n) = \tau(10) = \sum_{d/10} 1 = 1+1+1+1 = 4$, because there are just four positive divisors of 10 namely 1,2,5,10. Also, we obtain $\sigma(10) = 1+2+5+10 = 18$ whenever $n = p_1^{k_1} p_2^{k_2} .... p_r^{k_r}$ is the prime factorization of $n > 1$, then the positive divisors of *n* are precisely those integers d of the form $d = p_1^{a_1} p_2^{a_2} .... p_r^{a_r}$, where $0 \le a_i \le k_i \ (i = 1, 2, ..., r)$.

Now, let us find the formulae for $\tau(n)$ and $\sigma(n)$ in terms of prime factorization of a positive integer n > 1.

Theorem :

If $n = p_1^{k_1} p_2^{k_2} .... p_r^{k_r}$ is the prime factorization of n > 1, then

a) $\tau(n) = (k_1 + 1)(k_2 + 1)...(k_r + 1)$ and

b) $\sigma(n) = \left(\frac{p_1^{k_1+1} - 1}{p_1 - 1}\right)\left(\frac{p_2^{k_2+1} - 1}{p_2 - 1}\right)...\left(\frac{p_r^{k_r+1} - 1}{p_r - 1}\right)$

Proof :

a) The positive divisors of *n* are precisely those integers $d = p_1^{a_1} p_2^{a_2} .... p_r^{a_r}$, where $0 \le a_i \le k_i$; There are $k_1 + 1$ choices for the exponent $a_1, k_2 + 1$ choices for

the exponent $a_2,....,k_r+1$ choices for a_r, hence there are $(k_1+1)(k_2+1).....(k_r+1)$ possible divisors of n.

In order to evaluate $\sigma(n)$, consider the product.

$(1+p_1+p_1^2+...+p_1^{k_1})(1+p_2+...+p_2^{k_2})(1+p_r+p_r^2+...+p_r^{k_r})$. Each positive divisors of n appears once and only once as a term in the expansion of this product, so that $\sigma(n)=(1+p_1+p_1^2+...+p_1^{k_1})....(1+p_r+p_r^2+...+p_r^{k_r})$

Using the geometric series formula, $1+p_i+p_i^2+..+p_i^{k_i}=\frac{p_i^{k_i+1}-1}{p_i-1}$

If follows that $\sigma(n)=\left(\frac{p_1^{k_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{k_2+1}-1}{p_2-1}\right)...\left(\frac{p_r^{k_r+1}-1}{p_r-1}\right)$

A notation for the products is defined by the Greek capital letter p_i, denoted by Π for example.

$$\prod_{1\le d\le 5} f(d)=f(1)f(2)f(3)f(4)f(5)$$
$$\prod_{d/q} f(d)=f(1)f(3)f(9)$$

In this notations.

$$\sigma(n)=\prod_{1\le i\le r}(k_i+1)$$
$$\sigma(n)=\prod_{1\le i\le r}\frac{p_i^{k_i+1}-1}{p_i-1}$$

For example, the number $180=2^2.3^2.5$ has $(180)=(2+1)(2+1)(1+1)=18$ positive divisors the sum of these 18 integers is $\sigma(180)=\left(\frac{2^3-1}{2-1}\right)\left(\frac{3^3-1}{3-1}\right)\left(\frac{5^2-1}{5-1}\right)=7\times13\times6=546$.

Definition :

An arithmetic function *f* is said to be multiplicative if $f(mn)=f(m)f(n)$, whenever $\gcd(m,n)=1$.

Theorem :

The functions τ and σ are both multiplication function.

Proof :

Let m and n be relatively prime integers. Assume that $m>1$ and $n>1$. If $m=p_1^{k_1}p_2^{k_2}....p_r^{k_r}$ and $n=q_1^{j_1}q_2^{j_2}....q_s^{j_s}$ are the prime factorizations of m and n then, since $(m,n)=1\Rightarrow p_i\neq q_j$ for any j.

$$\Rightarrow mn=m=p_1^{k_1}....p_r^{k_r}...q_1^{j_1}....q_s^{j_s}$$

$$\therefore \text{of}(mn)=(k_r+1)(j_i+1)(j_s+1)=of(m)\,of(n)$$

Similarly, $\sigma(mn)=\left(\frac{p_1^{\Re_1+1}-1}{p_1-1}\frac{p_r^{\Re_r+1}-1}{p_r-1}\right)\left(\frac{q_1^{j_1+1}-1}{q_1-1}\frac{q_s^{j_s+1}-1}{q_s-1}\right)$

$$=\sigma(m)\sigma(n)$$

Thus, τ and σ are multiplicative functions we introduce another naturally defined functions on the positive integers, the mobius μ-function.

Definition : for a positive integer *n,* define μ by the rules.

$\mu(n)=1$ if $n=1$

$=0$ if p^2/n for some prime P.

$=(-1)^r$ if $n=p_1p_2...p_r$ where p_i are distinct primes.

For example, $\mu(n)=(-1)^r$, if n is square free with r prime factors.

$$\mu(30)=\mu(2.3.5)=(-1)^3=-1.$$

The first few values of μ are $\mu(1)=-1,\mu(2)=-1,\mu(3)=-1,$ $\mu(4)=0,\mu(5)=-1,\mu(6)=1,$ .. If p is a prime number, it is clear than $\mu(p)=-1$, also $\mu(p^{\Re})=0$ for $\Re\geq 2$. We can observe that the Mobius μ-function is multiplicative.

Theorem : The function μ is a multiplicative function.

Proof :

Assume that both m and n are square free integers. Say $m = p.p_2...p_r, n = q_1q_2....q_s$, the primes p_i and q_i being all distinct. Then $\mu(mn) = \mu(p_1...p_r\ q_1...q_s) = (-1)^{r+s}$

$$= (-1)^r (-1)^s = \mu(m)\mu(n).$$

Let us see what happens if $\mu(d)$ is evaluated for all the positive divisors d of an integer n and the results added.

If $n = 1,\ \because \sum_{d/n} \mu(d) = \sum_{d/1} \mu(d) = \mu(1) = 1$

Suppose $n > 1$, put $F(n) = \sum_{d/n} \mu(d)$.

If $n = p^k$ the power or prime, then the positive divisors of p^k are just the k+1 integers $1, p, p^2, p^{\aleph}$ so that

$$F\left(p^{\aleph}\right) = \sum_{d/p^{\aleph}} \mu(d) = \mu(1) + \mu(p) + \mu\left(p^2\right) + ... + \mu\left(p^{\aleph}\right)$$

$$= \mu(1) + \mu(p) = 1 + (-1) = 0$$

If n has a prime factorization $n = p_1^{k_1} p_2^{k_2} .... p_r^{k_r}$, then $F(n)$ is the product of the values assigned of F for the prime powers in this representation :

$F(n) = F\left(p_1^{k_1}\right) F\left(p_2^{k_2}\right).... F\left(p_r^{k_r}\right) = 0$, since F is a multiplicative function.

$\therefore$ For each positive integer $n \geq 1$, $\sum_{d/n} \mu(d) = 1$ if $n = 1 = 0$ if $n > 1$ where d runs through the positive divisors of n.

For example, consider $n=10$. The positive divisors of 10 are $1,2,5,10$ and the desired sum is

$$\sum_{d/10} \mu(d) = \mu(1) + \mu(2) + \mu(5) + \mu(10)$$

$$= 1 + (-1) + (-1) + 1 = 0.$$

Theorem : (MOBIUS INVERSION FORMULA) :

Let F and f be two arithmetic functions related by the formula.

$$F(n)=\sum_{d/n} f(d)$$

Then $F(n)=\sum_{d/n}\mu(d)\,F\left(\frac{n}{d}\right)=\sum_{d/n}\mu\left(\frac{n}{d}\right)F(d)$

Proof :

Consider $\sum_{d/n}\mu(d)\,F\left(\frac{n}{d}\right)=\sum_{d/n}\left(\mu(d)\sum_{c(n/d)} f(c)\right)$

$$=\sum_{d/n}\left(\sum_{c(n/d)}\mu(d)f(c)\right)$$

It can be verified that *d/n* and *c/(n/d)* if and only if *o/n* and *d/(n/c)*

$$\therefore\sum_{d/n}\left(\sum_{c/(n/d)}\mu(d)\,f(c)\right)=\sum_{c/n}\left(\sum_{d/(n/c)} f(c)\,\mu(d)\right)$$

$$=\sum_{c/n}\left(f(c)\sum_{d/(n/c)}\mu(d)\right)$$

Now, the sum $\sum_{d/(n/c)}\mu(d)$ vanishes except when $\frac{n}{c}=1$ (that is $n=c$), in this case $\mu(d)=1$.

$$\therefore\sum_{c/n}\left(f(c)\sum_{d/(n/c)}\mu(d)\right)=\sum_{c/n} f(c).1=f(n).$$

Definition :

For an arbitrary real number x, we denote by [x], the largest integer less than or equal to x, that is, [x] is the unique integer satisfying $x-1<[x]\le x$.

For example, $\left[-\frac{3}{2}\right]=-2,[\sqrt{2}]=1,\left[\frac{1}{3}\right]=0\,[\pi]=3,[-\pi]=-4$.

Note $[x]=x$ if and only if x is an integer.

1.10 Let Us Sum Up

1) Division Algorithm :

Given integers a and b, with *b>0* there exist unique integers *q* and *r* satisfying $a = bq + r, 0 \le r \le b$ the integers *q* and *r* are called quotient and remainder in the division of a by b.

2) The gcd of two integers a and b can be computed by the Euclidean algorithm as follows :

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

Here the last step involves a complete division, hence giving us r_n as the gcd of integers a and b.

3) A Linear Diophantine equation $ax + by = c$ can be solved for *x* and *y* only if $\gcd(a,b)$ divided c. If x_0 and y_0 are particular solution of $ax + by = c$, then all other solutions are given by :

$$x = x_0 + \left(\frac{b}{d}\right)t, \; y = y_0 + \left(\frac{a}{d}\right)t \text{ for varying integer t.}$$

4) Cardanos method helps us solve a cubic equation $x^3 + ax^2 + bx + c = 0$ by reducing the equation to $t^3 + pt + q = 0$. If $t = \mu + \upsilon$ then the equation $t^2 + qt + \frac{p^3}{27} = 0$ has roots μ^3 and υ^3 given by $u^3 = \left(\frac{-q}{2}\right) + \upsilon\left(\frac{q^2}{4}\right) + \left(\frac{p^3}{27}\right)$,

$\upsilon^3 = \left(\frac{-q}{2}\right) - \upsilon\left(\frac{q^2}{4}\right) + \left(\frac{p^3}{27}\right)$.

5) Two integers a and b are said to be congruent modulo n, written by $a \equiv b \pmod{n}$, if $n/(a-b)$ congruence is a general form in equality.

6) A problem of finding a solution to the quadratic congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ is some as that of finding a solution to a linear congruence and a quadratic congruence of the form $x^2 \equiv a \pmod{p}$. If p is an odd prime and $\gcd(a, p) = 1$ and the congruence $x^2 \equiv a \pmod{p}$ is solvable then a is called as the quadratic residue of p otherwise, a is called a quadratic non residue of p.

7) Euler's criterion is helpful to decided whether a is a quadratic residue of an add prime p or not. It states that if $\gcd(a, p) = 1$, then a is a quadratic residue of p if and only if $a^{((p-1)/2)} \equiv 1 \pmod{p}$.

8) Given a positive integer *n*, of *(n)* and $\sigma(n)$ denote the number of positive divisions of n and the sum of these divisors respectively. If $n = p_1^{k_1} p_2^{k_2} .... p_r^{k_r}$ is the factorization of *n>1*, then

$$of(n) = (\Re_1 + 1)(\Re_2 + 1)...(\Re_r + 1)$$

$$\sigma(n) = \left(\frac{p_1^{\Re_1+1} - 1}{p_1 - 1}\right)\left(\frac{p_2^{\Re_2+1} - 1}{p_2 - 1}\right)...\left(\frac{p_r^{\Re_r+1} - 1}{p_r - 1}\right)$$

9) One of the very important arithmetic function is the Mobius μ-function defined by :

$\mu(n) = 1$ if $n = 1$

$= 0$ if $p^2 n$ for some prime p.

$= (-1)^r$ if $n = p_1 p_2 ... p_r$ where p_i are distinct primes.

10) Mobius Inversion formula :

Let f and F be two arithmetic functions related by the formula

$F(n) = \sum_{d/n} f(d)$ Then

$$f(n) = \sum_{d/n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d/n} \mu\left(\frac{n}{d}\right) F(d).$$

1.11 Solved Numericals

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

Solution :

According to the Division Algorithm, every integer a is of the form $3q, 3q+1, 3q+2$. If $a = 3q$ then $\frac{a\left(a^2+2\right)}{3} = q\left(9q^2+1\right)$ which is clearly an integer. Similarly, if $a = 3q+1$, then

$(3q+1)\left(\left((3q+1)^2+2\right)/3\right) = (3q+1)\left(3q^2+2q+1\right)$ and $\frac{a\left(a^2+2\right)}{3}$ is an integer in this case. Finally, if $a = 3q+2$ then we get

$$\frac{a\left(a^2+2\right)}{3} = \frac{(3q+2)}{3}\left((3q+2)^2+2\right)$$

$$= (3q+2)\left(3q^2+4q+2\right) \text{ an integer once again.}$$

2) Use the division Algorithm to establish that the square of any integer is either of the form $3\Re$ or $3\Re+1$.

Solution :

Given any integer a, by the Division Algorithm,

$a = 3q, a = 3q+1$ or $a = 3q+2$

If $a = 3q \Rightarrow a^2 = (3q)^2 = 9q^2 = 3\left(3q^2\right) = 3\Re$

If $a = 3q+1 \Rightarrow a^2 = (3q+1)^2 = 9q^2+6q+1 = 3\left(3q^2+2q\right)+1 = 3\Re+1$

If $a = 3q+2 \Rightarrow a^2 = (3q+2)^2 = 9q^2+6q+4 = 3\left(3q^2+2q+1\right)+1$

$= 3\Re+1/$

3) Prove that $3a^2-1$ is never a perfect square.

Solution :

If $3a^2-1=b^2$ for some integer b then $3a^2-1=3\Re$ or $3a^2-1=3\Re+1$, by problem (2)

$$\Rightarrow 3a^2-3k=1 \text{ or } 3a^2-3k=2$$
$$\Rightarrow 3\left(a^2-\Re\right)=1 \text{ or } 3\left(a^2-\Re\right)=2$$

Neither case is possible, because $a^2-\Re$ is an integer $\Rightarrow 3a^2-1$ can't be perfect square for some integer b.

4) If a, b are integer, not both of which are zero, verify that

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

Solution :

Let $d=\gcd(a,b)$ and $c=\gcd(-a,b)$

$\Rightarrow c/-a$ and c/b

$\Rightarrow c/a$ and c/b, but $d=\gcd(a,b)$

$\Rightarrow c/d$ similarly d/c, hence $c=d \Rightarrow \gcd(a,b)=\gcd(-a,b)$

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

Putting a as -a on both the sides $\because \gcd(-a,b)=\gcd(a,b)$

Let $d=\gcd(-a,b)$ and $c=\gcd(a,-b)$

$\Rightarrow c/a$ and $c/-b$

$\Rightarrow c/a$ and c/b but d is the gcd of a & b $\Rightarrow c/d$.

Similarly $d/c \Rightarrow c/d$.

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

Let $d=\gcd(a,b)$ and $c=\gcd(-a,-b)$

$\Rightarrow c/-a$ & $c/-b$

$\Rightarrow c / a$ & $c / -b$ but d being the gcd of a & b $\Rightarrow c / d$. Similarly, we can show that $d / c \Rightarrow c = d$.

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

5) Use the eudidean algorithm to obtain integers *x* and *y* satisfying.

a) gcd (56, 72) = 56x + 72y

b) gcd (119, 272) = 119x + 272y

Solution :

a) Write $72 = 1 \times 56 + 16$

$$56 = 3 \times 16 + 8$$
$$16 = 2 \times 8 + 0$$

$\therefore$ The last nonzero remainder is 8.

$\therefore$ gcd(56,72) = 9

$$\because 8 = 56 - 3 \times 16$$
$$= 56 - 3(72 - 1 \times 56)$$
$$= 56 - 3 \times 72 + 3 \times 56$$
$$= 4 \times 56 - 3 \times 72$$
$$\therefore \gcd(56,72) = 56(4) + 72(-3)$$

6) Prove that if gcd(a,b) = 1, then gcd (a+n, ab) = 1.

Solution :

Let d = gcd (a+b, ab)

$\Rightarrow$ $d / a+b$ and d/ab

$\Rightarrow$ $a + b = dm$ and $ab = dn$ for some integers m,n

$\Rightarrow$ $a = dm - b$, $ab = dn$

$\Rightarrow$ $(dm - b)\ b = dn$

$\Rightarrow$ $dmb - b^2 = dn \Rightarrow d(mb - n) = b^2$

Hence d/b^2. similarly d/a^2

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

But d is the gcd of *a + b* & *ab* and *gcd(a,b) = 1*. So, by definition $d/1 \Rightarrow d = +1$ or $d = -1$, being gcd $d = 1$.

$$\Rightarrow \gcd(a+b, ab) = 1$$

7) Use cardanos method to solve the cubic equation $x^3 + 3x^2 + 3x - 2 = 0$.

Solution :

Substituting $x = t - \frac{a}{3} = t - \frac{3}{3} = t - 1$, to eliminate the x^2 term, we obtain new equation $t^3 + pt + q = 0$.

Where $p = b - \frac{a^2}{3}$ and $q = c + \left(\frac{2a^3 - 9ab}{27}\right)$

$\because p = 3 - \frac{3^2}{3} = 0,$

$\because q = -2 + \left(\frac{2(3^3) - 9(3)(3)}{27}\right) = -2 + (2 - 3)$

$\Rightarrow q = -3$

So, the new equation is $t^3 + ot - 3 = 0$.

$\Rightarrow t = \sqrt[3]{3}$

So $x = \sqrt[3]{3} - 1$.

In summary, the roots for the cubic.

$x^3 + 3x^2 + 3x - 2$ are

$x_1 = 0.4422495703$

$x_2 = -1.7211247852 + 1.2490247665i$

$x_3 = -1.7211247852 - 1.2490247665i$

8) Use Cardanos method to find the roots of the cubic $64x^3 - 48x^2 + 12$.

Solutions :

Substitute $x - 1x = t - \frac{9}{3}$. In the cubic $x^3 - 0.75x^2 + 0.1875x - 0.015625$, to get a new equation $t^3 + pt + q = 0$, $p = b - \frac{a^2}{3}, q = c + \left(\frac{2a^3 - 9qb}{27}\right)$

$$\therefore p = 0, q = 0$$

So, the new equation is $t^3 + ot + 0 = 0$

$\Rightarrow t = 0 \Rightarrow x = \dfrac{-9}{3} = 0.25.$

$\therefore$ All three roots are real equal to 0.25.

9) A customer bought a dozen pieces of fruit, apples and oranges for \$1.32. If an apple costs 3 cents more than an orange and more apples than oranges were purchased, how many pieces of each kind were bought?

Solution :

Let x be the number of apples and y be the number of oranges purchased, also, let z represents the cost (in cents) of an orange. Then the condition of the problem lead to $(z+3)x + zy = 132$ or $3x + (x+y)z = 132$.

Since $x + y = 12$, the above equation may be replaced as $3x + 12z = 132$, which in turn simplifies to $x + 4z = 44$.

As $\gcd(1, 4) = 1$ is a divisor of 44, there is a solution to this equation.

$\because 1 = 1(-3) + 4(1)$, upon multiplying by 44, we get

$44 = 1(-132) + 4.44.$

$\Rightarrow x_0 = -132, z_0 = 44$ is a solution.

All other solutions are of the form

$x = -132 + 4t$

$z = 44 - t$, t is any integer we want x s.t. $12 \geq x > 6.$

$\Rightarrow 12 \geq -132 + 4t > 6$

$\Rightarrow t \leq 36 \;\&\; -132 + 4t > 6$

$\Rightarrow t > \dfrac{34}{2}$

$\therefore t = 35$ and $t = 36$

$\therefore$ These are two possible choices.

12 apples costing 11 cents per piece or 8 apples at 12 cents each and 4 oranges at 9 cents each.

10) Solve the following puzzle :

Alcuin of York : A hundred bushels of grain are distributed among 100 persons in such a way that each man receives 3 bushels, each woman 2 bushels and each child ½ bushels. How many men, women & children are there?

Solution :

Let there be z men, y women and z children.

$\Rightarrow 3x + 2y + \frac{1}{2}z = 100$ and there are 100 persons in all. Therefore

$x + y + z = 100$

$\Rightarrow z = 100 - x - y$

$\therefore 3x + 2y + \frac{1}{2}(100 - x - y) = 100$

$\Rightarrow \left(\frac{5}{2}\right)x + \left(\frac{3}{2}\right)y = 50$

$\Rightarrow 5x + 3y = 100$

As $\gcd(5,3) = 1$, is a divisor of 100, there is a solution to this equation $\because 1 = (-1) \times 5 + 2 \times (3) \therefore$ multiplying the above equation throughout by 100, we obtain

$\therefore 100 = (-100) \times 5 + (200) \times 3$

$\therefore x_0 = -100$ and $y_0 = 200$ is a solution, All other solutions are of the form

$x = -100 + 3t$

$y = 200 - 5t$, t is any integer, if we put t = 34, we get

$x = -100 + 5 \times 34 = -100 + 102 = 2$

$y = 200 - 5 \times 34 = 200 - 170 = 30$

$\therefore$ A possible solution is that there are 2 men, 30 women and $100 - 32 = 68$ number of children.

11) Find the remainder, when 2^{50} and 41^{65} are divided by 7.

Solution :

$\because 2^{10} = 2^5 \times 2^5 = 32 \times 32$

$\therefore 2^{10} \equiv 32 \times 32 \bmod 7$

$\equiv 32 \bmod 7 \times 32 \bmod 7$

$\equiv 4 \bmod 7 \times 4 \bmod 7$

$\equiv 16 \bmod 7 \equiv 2 \bmod 7$

$\therefore \left(2^{10}\right)^5 \equiv 2^5 \bmod 7 \equiv 32 \bmod 7 \equiv 4 \bmod 7$

$\therefore$ The remainder, when 2^{50} is divided by 7 comes out to be (4).

Next, we know that $41 \equiv 6 \bmod 7$.

$\therefore 41^{65} \equiv 6^{65} \bmod 7$

$\because 6^5 = 7776 \equiv 6 \bmod 7.$

$\therefore \left(6^5\right)^{13} \equiv 6^{13} \bmod 7$

$\equiv 6^{13} \bmod 7$

$\equiv \left[\left(6^5\right)^2 + 6^3\right] \bmod 7$

$\equiv 6^5 \bmod 7\, 6^5 \bmod 7 \times 216 \bmod 7$

$\equiv 6 \bmod 7 \times 6 \bmod 7 \times 6 \bmod 7$

$\equiv 6^3 \bmod 7 \equiv 6 \bmod 7$

$\therefore$ The remainder, when 41^{65} is divided by 7 found to be (6)

12) Solve the quadratic congruence $x^2 + 7x + 10 \equiv 0 \,(\text{mod}\, 11)$.

Solution :

Here $a = 1, b = 7, c = 10, p = 11$

$\therefore$ Replace this congruence by the simpler one $y^2 \equiv d \,(\text{mod}\ p)$

$y = 29x + b \;\&\; d = b^2 - 4ac$

$\therefore y = 2x + 7 \; and \; d = 7^2 - 40 = 9$

$\Rightarrow y^2 \equiv 9 \bmod 11$, this has two solution $y \equiv 3 \bmod 11$ and $y \equiv 8 \pmod{11}$, next we solve the linear congruences,

$2ax \equiv y_0 - b \pmod{p}$ for

$y_0 = 3 \;\&\; y_0 = 8$

$\Rightarrow 2x \equiv 7 \bmod 11 \;\&\; 2x \equiv 1 \bmod 11$

It can be seen that $x \equiv 9 \bmod 11$ & $x \equiv 6 \bmod 11$ are solutions of these congruences respectively.

$\therefore x \equiv 9 \bmod 11$ and $x \equiv 6 \bmod 11$ are solutions of the given congruence $x^2 + 7x + 10 \equiv 0 \pmod{11}$.

13) Show that 3 is a quadratic residue of 23, but non-residue of 31.

Solution :

By Eulen's criterion, a is a quadratic residue of P iff $\gcd(a, p) = 1$ and $a^{\frac{p-1}{2}} \equiv 1 \bmod p$.

$\therefore$ Consider $3^{\left(\frac{23-1}{2}\right)} = 3^{11} = \left(3^2\right)^5 - 3$

$\therefore 3^{\frac{23-1}{2}} \equiv \left(3^2\right)^5 .3 \bmod 23$

$\equiv 9^5 . 3 \bmod 23$

$\equiv 81^2 . 9.3 \bmod 23$

$\equiv 81^2 \bmod 23\, 4 \bmod 23$

$\equiv 81 \bmod 23\, 81 \bmod 23\, 4 \bmod 23$

$\equiv 12^2 \bmod 23 \times 4 \bmod 23$

$\equiv 8 \bmod 23 \times 4 \bmod 23$

$\equiv 24 \bmod 23 \equiv 1 \bmod 23$

Hence $3^{\frac{23-1}{2}} \equiv 1 \bmod 23$. Therefore 3 is a quadratic residue of 23.

If $p = 31, \because 3^{\frac{p-1}{2}} = 3^{\frac{31-1}{2}} = 3^{15}$

$\therefore 3^{\frac{31-1}{2}} \equiv 3^{15} \bmod 31 \equiv \left(3^2\right)^5 .3^5 \bmod 31$

$\equiv 9^5 \bmod 31.3^5 \bmod 31$

$\equiv 25 \bmod 31.26 \bmod 31$

$\equiv 650 \bmod 31 \equiv 30 \bmod 31$

$\equiv 30 \bmod 31$

$\Rightarrow 3^{\frac{31-1}{2}} \not\equiv 1 \bmod 31$

$\Rightarrow 3$ is a quadratic non-residue of 31.

14) Knowing that 2 is a primitive root of 19, find all quadratic residues of 19.

Solution :

In the proof of Euler's criterion, we saw that, if r is a primitive root of p then $k \equiv r^k \bmod p$ for some integer

$\Re, 1 \le k \le p-1$ and $K = 2j$

$\therefore$ consider even powers of $r = 2$

$2^0 \equiv 1, 2^2 \equiv 4, 2^4 \equiv 16, 2^6 \equiv 64 \equiv 7, 2^8 \equiv 28 \equiv 9, 2^{12} \equiv 36 \equiv 17, 2^{14} \equiv 68 \equiv 11,$
$2^{16} \equiv 44 \equiv 6, 2^{18} \equiv 24 \equiv 5$

$\Rightarrow 1,4,16,7,9,17,11,6,5$ are the quadratic residues of 19.

15) Find the $\gcd(12378, 3054)$ and $lom(12378, 3054)$

Solution :

$\because 12378 = 2 \times 3 \times 2060$

$\because 3054 = 2 \times 3 \times 509$

$\Rightarrow 12378 = 2^1 \times 3^1 \times 509^0 \times 2063^1$ &

$3054 = 2^1 \times 3^1 \times 509^1 \times 2063^0$

$\therefore$ By the theorem,

$$\gcd(12378, 3054) = 2^{\min 1,1} \times 3^{\min 1,1} \times 509^{\min 0,1} \times 2063^{\min 0,1}$$
$$= 2^1 \times 3^1 \times 509^0 \times 2063^0$$
$$\& \; lom\,(12378, 3054) = 2^{\max 1,1} \times 3^{\max 1,1} \times 509^{\max 0,1} \times 2063^{\max 0,1}$$
$$= 2 \times 3 \times 504 \times 2063$$
$$= 6,18,400$$

1.12 Check Your Progress

Unit End Exercises:

1) Show that the product of any set of *n* consecutive ingeters is divisible by *n*.

(Hint : any product of *n* consecutive integers looks like

$\Re(k+1)(k+\Re)(\Re+(n-1))$ for some integer k).

2) Find the quadratic residues of 29 & 31.

3) Let *m* & *n* be positive integers and $p_1, p_2, .., p_r$ be distinct primes, which divide atleast one of m or n. Then m & n can be written in the form

$m = p_1^{k_1} p_2^{k_2} \; p_r^{k_r}$, with $\Re_i \geq 0 \; i = 1, 2, r$

$n = p_1^{j_1} p_2^{j_2} \; p_r^{j_r} \; j_i \geq 0$ for $i = 1, 2, r$

Then prove that

$\gcd(m,n) = p_1^{u_1} p_2^{u_2} \; p_r^{u_r}$ & $lcm\,(m,n) = p_1^{\upsilon_1} p_2^{\upsilon_2} \; p_r^{\upsilon_r}$ where

$\mu_i = \min\{\Re_i, j_i\}$,
$\upsilon_i = \max\{\Re_i, j_i\}$

4) Solve the following quadratic congruence $3x^2 + 9x + 7 \equiv 0 \,(\mathrm{mod}\, 13)$.

5) Using cardanos method solve the following cubic polynomial equation $x^3 - 2x^2 - 5x + 6 = 0$.

6) Determine all solutions in the integers for the following Diophantine equation $24x+138y=18$.

7) Show that the cube of any integer is of the form $7\mathfrak{R}$ or $7\mathfrak{R}\pm 1$. (Hint : Apply division algorithm).

8) Given an odd integer a, establish that $a^2+(a+2)^2+(a+4)^2+1$ is divisible by 12.

9) Find $\gcd(119,272)$ and $lcm(143,227)$.

Unit 1

2

BASIC PRINCIPLES OF COUNTING

Unit Structure :

2.0 Objectives

After going through this chapter, you will come to know about

* Basic concepts in set theory
* Counting Techniques like the sum rule and the product rule
* Two way counting the size of the set
* Permutations as on arrangement of finitely many objects in a line
* Combinations or selection of r objects form given n – distinct objects
* Binomial and Multinomial theorem to count the size of a set defined by certain constraints
* Some identities like Pascal's identity by using two way counting

2.1 Introduction

We shall understand sets and functions as basic requirements to formulate certain counting techniques we deal only with the sets consisting of only finitely many objects in it. We will regard the word set as synonymous with the word "Class" "collection" and "family"

2.2 Elementary Set Theory

In this section, we shall review of the terminology and notation that will be used in this text. If an element x is in a set A, we write $x \in A$ and say that x is a member of A or that x belongs to A. If x is not in A, we write $x \notin$.A. If every element of a set A also belongs to a set B, we say that A is a subset of B and write $A \subseteq B$ or $B \supseteq A$.

Definition : Two sets A and B are said to be equal and we write $A = B$, if they both contain the same elements.

Thus, to prove that the sets A and B are equal, we must show that

$A \subseteq B$ and $B \subseteq A$

If Principal denotes a property that is meaningful and unambiguous for elements of a set S, then we write $\{x \in s : P(x)\}$ for the set of all elements x in s for which the property p is true.

For example, the set of natural numbers

$= \{1, 2, 3, ...\}$The set of integers

$\square = \{0, 1, -1, 2, -2, ...\}$ The set of rational numbers $\square$

$\square = \{\frac{m}{n} : m, n \in \square, n \neq 0\}$ The set of all real numbers $\square$

Set operations :-

a) The union of sets A and B is the set

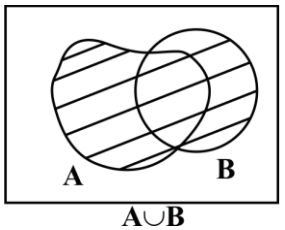
$A \cup B = \{x : x \in A \text{ or } x \in B\}$

b) The intersection of the sets A and B is the set

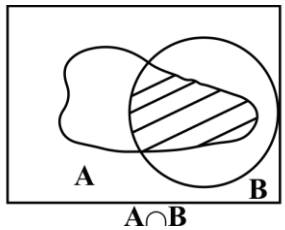
$A \cap B = \{x : x \in A \text{ or } x \in B\}$

c) The complement of B relative to A is the set

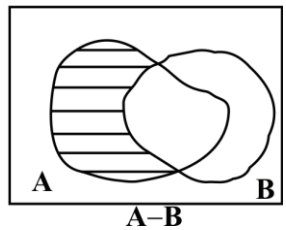
$A - B := \{x : x \in A \text{ or } x \notin B\}$



$A \cup B$



$A \cap B$



$A - B$

The set that has no elements is called the empty set and it is denoted by the symbol ∅. Two sets A and B are said to be disjoint, if they have no elements in common, symbolically, use write $A \cap B = \varnothing$

Theorem :- (De Morgan's laws)

If A, B, C are sets, then

a) $A - (B \cap C) = (A - B) \cup (A - C)$

b) $A - (B \cup C) = (A - B) \cap (A - C)$

For a finite collection of sets $\{A_1, A_2, \ldots, A_n\}$, their union is denoted by $\bigcup_{k=1}^{n} A_r$ consisting of all elements that belong to atleast one of the sets A_R and their intersection is denoted by $\bigcup_{k=1}^{n} A_r$ consists of all elements that belong to all of the sets A_R.

Cartesian Products :

In order to discuss functions, we define the Cartesian product of two sets.

Definition :- If A and B are nonempty sets, then the Cartesian product $A \times B$ of A and B is the set of all ordered pairs (a, b) with $a \in A$ and $b \in B$. That is

$A \times B = \{(a, b) : a \in A, b \in B\}$

Thus if $A = \{1, 2, 3\}$ and $B = \{1, 5\}$

Then A × B consists of the ordered pairs (1, 1), (1, 5), (2, 1), (2, 5), (3, 1), (3, 5) we will not discuss the fundamental notion of a function or a mapping. To the

mathematician of the early nineteenth century, the word function meant a definite formula, such as $f(x) = x^2 + 3x - 5$, which associates to each real number x, another number $f(x)$. Here $f(0) = -5, f(1) = -1, f(5) = 35$

A function f from a set A into a set B is a rule of correspondence that assigns to each element x in A, a uniquely determined element $f(x)$ in B.

Definition :- Let A and B be sets. Then a function from A to B is a set f of ordered pairs in $A \times B$ such that for each a $\in$ A there exists a unique b $\in$ B with $(a, b) \in f$. The set A of first elements of a function f is called the domain of f, denoted by $D(f)$. The set of all second elements in f is called the range of f and it's often denoted by $R(f)$. Note that $D(f) = A$, we only have $R(f) \subseteq B$.

The essential condition that $(a, b) \in f$ and $(a, b') \in$ f implies that $b = b^1$. The notation $f : A \to B$ is often used to indicate that f is a function from A into B we will also say that f is a mapping of A into B or f maps A into B. It is customary to write $b = f(a)$ or $a \mapsto b$

Direct and Inverse Images :

Let $f : A \to$ B be a function with domain

$D(f) = A$ and range $R(f) \subseteq B$.

Definition : If E is a subset of A, then the direct image of E under f is the subset $f(E)$ of B given by

$f(E) = \{f(x): x \in E\}$.

If H is a subset of B, then the inverse image of H under f is the subset

$f^{-1}(H)$ of A given by

$f^{-1}(H) = \{x \in A : f(x) \in H\}$

Special types of functions :

The following definitions identify some very important types of functions.

Definitions : Let $f : A \to B$ be a function from A to B

a) The function f is said to be injective or one –to-one) if whenever $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$. If f is an injective function, we say that f is on injection.

b) The function f is said to be surjective (or onto B) if $f(A) = B$, that is, if the range $R(f) = B$. If f is a surjective function, we say that f is a surjection.

c) If f is both injective and surjective, then f is said to be bijective. If f is bijective, we say that f is a bijection.

For example, Let $A = \{x \in \square : x \neq 1\}$, define $f(x) = \frac{2x}{x-1}$ for all $x \in A$. Then if is injective for $\frac{2x_1}{x_1 - 1} = \frac{2x_2}{x_2 - 1}$ implies that $x_1(x_2 - 1) = x_2(x_1 - 1) \Rightarrow x_1 = x_2$. To determine the range of f, we solve the equation $y = \frac{2x}{x-1}$ for x, in terms of y we obtain $x = \frac{y}{y-2}$, which is meaningful if $y \neq 2$. Thus the range of f is the set $B = \{y \in \square : y \neq 2\}$. Thus f is a bijection of A onto B.

Inverse functions :

If $f : A \to B$ is a bijection then we can define another function $g : B \to A$ such that $g(b) = a$ whenever $f(a) = b$. Here g is called the inverse function of f, denoted by $g = f^{-1}$.

Definition :-

If $f : A \to B$ is a bijection of A on to B, then $g = \{(b, a) \in B \times A : (a, b) \in f\}$ is a function of B into A, denoted by $g = f^{-1}$

For example, the function $f(x) = \frac{2x}{x-1}$ is a bijection of $A = \{x \in \square : x \neq 1\}$ on to the set $B = \{y \in \square : x \neq 2\}$. The function inverse to f is given by

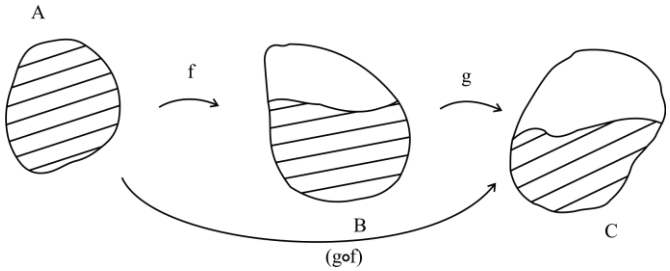
$f^{-1}(y) = \frac{y}{y-2}$ for $y \in B$.

Composition of Functions :

If often happens that we want to compose two functions f, g by first finding $f(x)$ and then applying g to get $g(f(x))$. However, this is possible only when $f(x)$ belongs to the domain of g.

Definition :- If $f : A \to B$ and $g: B \to C$ and if $R(f) \subseteq D(g) = B$, then the composite function $(g \circ f)$ is the function from A into C defined by

$(g \circ f)(x) = g(f(x))$ for all $x \in A$



For example, let $f(x) = 1 - x^2$ and $g(x) = \sqrt{x}$, then since $D(g) = \{x : x \geq 0\}$ the composition function (g of) is given by the formula

$(g \circ f)(x) = g(f(x))$

$= \sqrt{f(x)} = \sqrt{1 - x^2}$

Only for $x \in D(f)$ that satisfy $f(x) \geq 0$, that is for x satisfying $-1 \leq x \leq 1$.

Restrictions of functions :

If $f : A \to B$ is a function and if $A_1 \subset A$, we can define a function $f_1 : A_1 \to B$ by $f_1(x) = f(x)$ for $x \in A_1$, denoted by $f_1 = f/A_1$.

Principles of Mathematical Induction :

1) Let s be a subset of $\mathbb{N}$ that possesses the following properties :

   a) The number $1 \in s$

   b) For every $k \in \mathbb{N}$, if $k \in s$ then $k + 1 \in s$

   Then we have $s = \mathbb{N}$

2) Let s be a subset of $\mathbb{N}$ such that

   a) $1 \in s$

   b) For every $k \in \mathbb{N}$, if $\{1, 2, ..., k\} \subseteq s$, then $k + 1 \in s$

   Then $s = \mathbb{N}$

The above two principles of mathematical induction are used to prove a result P(n) is true for every positive integer n.

Now, let us start with elementary counting techniques, based on the simple observations summarized as the sum role and the product rule.

2.3 The Sum Rule

Suppose Task 1 can be done in m different ways and Task 2 in n different ways. Also there is no way of doing both the tasks together, then the number of ways of doing either Task 1 or Task 2 can be done in (m + n) different ways.

For example, if there are 80 mathematics and 40 statistics book. Then there are $80 + 50 = 130$ ways of selecting either a Mathematics or an English book,

The General form of this sum Rule can be stated as follows :

If there are n_1 ways of performing an event, n_2 ways of performing second event and n_r ways of doing r^{th} event. Then either of these r-events can be performed in $(n_1 + n_2 + ... + nr)$ different ways.

2.4 The Product Rule

Suppose a procedure can be divided into a first step followed by the second step and that there are m-different ways of performing step-1 and n-different ways of performing step-2, independent of the first step. Then a procedure can be accomplished in $m \times n$ ways.

For example, two dice are thrown, then there are 6 different outcomes of a given dice. So there are $6 \times 6 = 36$ possible outcomes of throwing two dice, the generalised form of the product rule can be stated as follows.

Suppose a procedure can be broken into r stages with n_1 outcomes in the first stage, r_2 outcomes in the second stage, n_r outcomes in the r^{th} stages. If all these outcomes at every stage are independent of each other then the procedure can be performed in $n_1, n_2, ... n_r$ different ways. For examples, if we are to decide how many different 3-digit eve numbers are there, in writing such a number the first digit can't be zero, so there are 9 ways to choose the first digit, the second digit can be zero, so there are 10 ways to form second digit and the last digit can be 0, 2, 4, 6 or 8, so thee are 5 choices for the third digit. Therefore the product $9 \times 10 \times 5 = 450$ is the total number of 3-digit even numbers,

Definition :-

A set x is said to be an n-set consisting of n number of elements, if x has n different objects.

For example, $A = \{1, 2, 3, 4, 5\}$ is a 5-set consisting of 5-district objects.

$B = \{0, 1\}$ is a 2-set consisting of 2-distinct elements.

One of the important question is to count the number of arrangements of an n-set x in order. For example, if three people Ms. Jordan, Mr. Harper and Ms. Gabler are scheduled for job interviews. In how many different orders can they be interviewed ?

Let us list all possible orders, as follows :

1. Jordan, Harper, Gabler
2. Jordan, Gabler, Harper,
3. Harper, Jorden, Gabler
4. Harper, Gabler, Jordan
5. Gabler, Jordan, Harper
6. Gabler, Harper, Jordan

We can see that there are total 6 possible orders. Alternatively, we can observe that there are 3 choices for the first person being interviewed. For each of these 3 choices there are 2 remaining choices for second person. For each of these choices, there is only 1 choice remaining for third person. Hence by the product rule, the number of possible order is $3 \times 2 \times 1 = 6$.

If there are 5 people to be interviewed then there are 5 choices possible for first person, 4 choices for second and so on, resulting in $5 \times 4 \times 3 \times 2 \times 1 = 120$ possible order in all.

The number of permutations of an n-set x is given by
$n \times (n-1) \times (n-2) \times \ldots \times 2 \times 1 = n!$

2.5 Double Counting / Two Way Counting

In combinatorics, two way counting is a proof technique for showing that two expressions are equal by demonstrating that they are two ways of counting the size of one set,

For example if X is the collection of all committees that can be formed from η people. Then $|X| = \underbrace{2 \times 2 \times ..... \times 2}_{n} = 2^n$

Alternatively, one may observe that the size of the committee must be some number between 0 and n. For each possible size k, the number of ways, in which a committee of k people can be formed from n people is the binomial co-efficient $\binom{n}{k}$. Therefore the total number of possible committees is the sum of the binomial co-efficients over k = 0, 1, 2, …, n. Equating the two expressions gives the identity

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Another way we can make use of double counting in proving Vandermonde's Identity, that states that if m, n, r $\in$ □ $^{+}$ $\cup\{0\}$ then

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k}$$

This identity can be formulated as a problem of forming a committee of r senators in the US senote consisting m Democrats and n Republicans. Then the number of ways of forming a committee of r-senotors is $\binom{m+n}{r}$

Now, every typical committee of r-senators contain K Democrats and consequently r-k Republicans, so by the product rule the number of subcommittees consisting k Democrats and r – k Republicans is $\binom{m}{k}\binom{n}{r-k}$.

Therefore there are $\sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k}$ distinct ways of forming a committee of r-senotors. It implies that $\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k}$

Next example, we wish to find the number of ways, we can select 3 students from a student body of 3n, where n are singers, n are dancers, n are musicians ? There are two answers to this question. From the total group of 3n students, choose 3 in $\binom{3n}{3}$ ways.

Case 1 – Choose all 3 students from the same group we can choose the group in 3 ways, then the students in $\binom{n}{3}$ ways.

By the multiplication principles, there are $3\binom{3n}{3}$ ways to do this.

Case 2 – Choose 2 groups, then 1 student from the first group and 2 students from the second group. Since order matters, there are 6 ways to choose a ranked pair of groups and $\binom{n}{1}$ and $\binom{n}{2}$ ways to choose the students fro those groups. Thus Case 2 is covered in $6n\binom{n}{2}$ ways.

Case 3 – Choose 1 student from each group. By the multiplication principle / the product rule, this can be done in $\binom{n}{1}\binom{n}{1}\binom{n}{1} = n^3$ ways. By above these cases, which are not occurring simultaneously.

$$\because \quad \binom{3n}{3} = 3\binom{n}{3} + 6n\binom{n}{2} + n^3$$

2.6 r – Permutations :

Given an n-set x, suppose we wish to pick r elements and arrange them in order such on arrangement is called r-permutation of the n-set x. For example, the number of three letter words without repeated letters can be calculated by noticing that we want to choose three letters out of 26 and arrange them in order the first letter of a three letter word can be chosen in 26 ways, having done this the second letter has $26 - 1 = 25$ choices left and consequently the third letter can be chosen in $25 - 1 = 24$ ways. Hence by the product rule there are $26 \times 25 \times 24$ different three letter words without repetition. Let $P(n, r)$ be the number of r-permutations of an n-set X. Hence $P(26, 3) = 26 \times 25 \times 24$

Theorem : $n \geq r$ then the number of r-permutations of an n-set x without repeatition is given by

$$P(n, r) = \frac{n!}{(n - r)!}$$

Proof : Consider a typical r permutation of an n-set x,

$$b_1 b_2 \; b_{r-1} \; br$$

Here b_1 has n – choices hence b_2 has n – 1 choices left, b_3 can be chosen from n – 2 objects and so on b_{r-1} can be chosen from $n–(r–2)$ objects and there fore there are n–(r−1) choices left for br. Hence by the product rule, there are

$$n \times (n-1) \times (n-2) \times \ldots \times (n-x)\ (n-(r-1))$$

Such r - permutations of an n-set X

$$\Rightarrow \quad p(n, r) = n(n-1)(n-2)\ (n-r)\ (n-r+1)$$

If $n > r$ this can be simplified as

$$p(n, r) = \frac{n(n-1)n(-2).....(n-2+2)(n-r+1)}{1 \times 2 \times 3 \times .... \times (n-r-1) \times (n-r)}$$

$$\Rightarrow \ p(n, r) = \frac{n!}{(n-r)!}$$

Subset of an n-set X :-

Consider the set $\{a, b, c\}$. Let us ask how many subsets are there for this set. The answer can be obtained by enumeration, and we find that these are 8 such subsets:

$\varnothing, \{a\}, \{b\}, \{0\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}$

The answer can also be obtained using the product rule. We think of building up a subset in steps, First, we think of either including element a or not. There are 2 choices. Then we either include element b or not. Thee are again 2 choice, Finally, we either include element C or not. There are again 2 choices. The total number of ways of building up the subset is, by the product rule.

$$2 \times 2 \times 2 = 2^3 = 8$$

Similarly the number of subsets of a 4-set is $2 \times 2 \times 2 \times 2 = 2^4 = 16$. Hence the number of subsets of on n-set is

$$\underbrace{2 \times 2 \times ..... \times 2}_{n \text{ times}} = 2^n$$

2.7 Combinations

r-combinations :-

An r – combination of an n-set x is a selection of r-elements from the set, which means that order doesn't matter, Thus, an r-combination is an r-element subset, C(n, r) denotes the number of r-combinations of an n-set. For example the number of ways to choose a committee of 3 from a set of 4 people is given by $C(4, 3)$, If

the four people are Dewey, Evans, Grange and Howe, then the possible committees are {Dewey, Evans, Grange}, {Howe, Evans, Grange}, {Dewey, Howey, Grange}, {Dewey, Evans, Howe}. Hence *C(4, 3) = 4* Note that *C(n, r)=0* if $n < r$, there are no r-combinations of an n-set in this case.

Theorem :

$P(n, r) = C(n, r) \times P(r, r)$

Proof : An ordered arrangement of r-objects out of n can be obtained by first choosing r-objects (this can be done in *C(n, r)* ways) and then ordering them (this can be done in $p(r, r) = r!$ ways)

Therefore by product rule, there are $C(n, r) \times P(r, r)$ such ordered arrangements of r-objects out of n – objects

Corollary : $C(n,r) = \dfrac{n!}{r!(n-r)!}$

Proof :- Since we know that

$P(n, r) = C(n, r) \times P(r, r)$

$$\Rightarrow C(n,r) = \frac{P(n,r)}{p(n,r)} = \frac{p(n,r)}{r!}$$

But, we know that $p(n,r) = \dfrac{n!}{(n-r)!}$

$$\Rightarrow C(n,r) = \frac{n!}{r!(n-r)!}$$

Corollary :- $C(n, r) = C(n, n - r)$

Proof :- $\dfrac{n!}{r!(n-r)!} = \dfrac{n!}{(n-r)!r!} = \dfrac{n!}{(n-r)![n-(n-r)]!}$

$\Rightarrow C(n, r) = C(n, n - r)$

Note :- The number $\dfrac{n!}{r!(n-r)!}$ is often denoted by $\binom{n}{r}$ and called the binomial co-efficient

2.8 Pascal's Identity

$C(n, r) = C(n - 1, r - 1) + C(n - 1, r)$

Theorem :-

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

Proof :- Given an n-set $X = \{x1, x2, \ldots. xn\}$. Any r-combinations of this n-set X can be of either category.

1) containing x_1 as object or

2) not containing x_1, as object

There are $\binom{n-1}{r-1}$ r- combinations of n-et X containing x_1 and $\binom{n-1}{r}$ r-combinations of n-set X, not containing x_1.

Therefore by the sum rule, there are in all $\binom{n-1}{r-1} + \binom{n-1}{r}$ r-combination of an n-ser X.

$$\Rightarrow \binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$$

This is a combinatorial proof, relying on counting arguments. This theorem can also be proved by algebraic manipulation. Here is the proof.

$$C(n-1, r-1) + (C(n-1, r) = \frac{(n-1)!}{(r-1)![(n-1)-(r-1)]!} + \frac{(n-1)!}{r![(n-1)-r]!}$$

$$= \frac{(n-1)!}{(r-1)!(n-r)!} + \frac{(n-1)!}{r!(n-r-1)!}$$

$$= \frac{r(n-1)!}{r!(n-r)!} + \frac{(n-r)(n-1)!}{r!(n-r)!}$$

$$= \frac{r(n-1)! + (n-r)(n-1)!}{r!(n-r)!}$$

$$= \frac{(n-1)!(r+n-r)}{r!(n-r)!}$$

$$= \frac{n(n-1)!}{r!(n-r)!} == \frac{n!}{r!(n-r)!} = C(n,r)$$

A convenient method of computing the number C(n, r) is to use the following array

n = 0				1			← r = 0
n = 1			1		1		← r = 1
n = 2		1		2		1	← r = 2
n = 3	1		3		3		1 ← r = 3
n = 4	1		4		6		4 1 ← r = 4
n = 5	1	5		10		10	5 1

For example, *C(5, 2)* is given by summing the numbers 4 and 6. The above array of binomial numbers is called as the Pascal's triangle.

2.9 Binomial and Multinomial Coefficients

The number $\frac{n!}{r!(n-r)!}$ is denoted by $\binom{n}{r}$, which equals the number of r-combinations of an n-set x.

$$\binom{n}{r} = \frac{n(n-1)(n-2).....(n-r+1)}{r!} \quad \text{if } r > 0$$

$$= 1 \quad \text{if } r > 0$$

OCCUPANCY PROBLEM :

In the history of combinatorics and probability theory, problems of placing balls into cells or urns have played an important role such problems are called occupancy problems. In this section, we consider the situation, where we distribute n-distinguishable balls into R-distinguishable cells. In particular, we consider the situation where we distribute n_1 balls into the first cell, n_2 into the second cell, nk into the k^{th} cell. Let C(n, n_1, n_2, , n_k) denote the number of ways this can be done. This number is also written as $\binom{n}{n_1, n_2, ..., n_k}$ and called the multinational coefficient. Let us consider one example. The University Registrat's office is having a problem. It has 11 new students to squeeze into 4 sections of an introductory course : 3 in the first, 4 in the second and third, and 0 in the forth. In

how many ways this can be done ? The answer is $C(11, 3, 4, 4, 0)$. Now there are $\binom{11}{3}$ choices for the first section, for each of these choices there are $\binom{11-3}{4}=\binom{8}{4}$ choices for the second section; for each of these choices, there are $\binom{8-4}{4}$ choices for the third section and $\binom{0}{0}$ choices for the fourth section. Hence, by the product rule, the number of ways to assign section is

$$C(11, 3, 4, 4, 0) = C(11, 3) \times C(8, 4) \times C(4, 4) \times C(0, 0)$$

$$= \frac{11!}{3!8!} \times \frac{8!}{4!4!} \times \frac{4!}{4!0!} \times \frac{0!}{0!0!}$$

$$= \frac{11!}{3!4!4!} \qquad (0! = 1)$$

Continuing with our example, suppose that suddenly, spaces in the fourth section become available. The registrar's office now wishes to put 3 people each into the first, second and third sections and 2 into the fourth. In how many ways can this be done ? Of the 11 students, 3 must be chosen for the first section; of the remaining 8 student, 3 must be chosen for the second section, of the remaining 5 students, 3 must be chosen for the third section; finally, the remaining 2 must be put into the fourth section. The total number of ways of making the assignments is

$$C(11, 3, 3, 3, 2) = C(11, 3) \times C(8, 3) \times C(5, 3) \times C(2, 2)$$

$$= \frac{11!}{3!8!} \times \frac{8!}{3!5!} \times \frac{5!}{3!2!} \times \frac{2!}{2!0!}$$

$$\Rightarrow \quad C(11, 3, 3, 3, 2) = \frac{11!}{3!3!3!2!}$$

Let us derive the formula for

$C(n, n_1, n_2, \ldots, n_k)$

$C(n, n_1, n_2, \ldots, n_k) = C(n, n_1) \times C(n - n_1, n_2) \times C(n - n_1 - n_2, \ldots, n_k) \times \ldots\ldots \times C(n - n_1 - n_2, \ldots, n_{k-1}, n_k)$

$$\Rightarrow \quad C(n, n_1, n_2, \ldots, n_k) = \frac{n!}{n! \times (n - n_1)} \times \ldots\ldots \times \frac{(n - n_1 - n_2 - \ldots - n_{k-1})!}{n_k!(n - n_1 - \ldots - n_k)!}$$

$$= \frac{n!}{n_1! n_{2!} ! \ldots\ldots n_k!(n - n_1 - n_2 - \ldots\ldots n_k)!}$$

Theorem

$$C(n, n_1, n_2, \ldots, n_k) = \frac{n!}{n_1! n_2! \ldots .. n_k!}$$

$$n = n_1 + n_2 + \ldots\ldots + n_k \quad (0! = 1)$$

For example, an NHL hockey season consists of 82 games. The number of ways the season can end in 41 wins, 27 losses and 14 ties is

$$C(82, 41, 27, 14) = \frac{82!}{41!27!14!}$$

Note :- $C(n, n_1, n_2) = C(n, n_1)$

The number of 5-digit numbers consisting of two 2's, two 3's and one 1 is C(5, 2, 2, 1) = $\frac{5!}{2!2!1!} = 30$

2.10 Binomial and Multinomial Theorme :

In elementary algebra, the binomial theorem describes the algebraic expansion of powers of a binomial. According to the theorem, it is possible to expand the power $(x + y)^n$ into a sum involving terms of the form ax^by^c, where the exponents b, c are non negative integers with b + c = n.

For example

$$(x+y)^4 = x^4 + 4x^3y^2 + 4x$$

$$= x^4 + 4x^3y + 5x^2y^2 + 4xy^3 + y^4$$

The coefficient a in the term x^by^c is known as the binomial coefficient $\binom{n}{b}$ or $\binom{n}{c}$

Theorem :- (Binomial Expansion)

For $n \geq 0$

$$(x+y)^n = \sum_{k=0}^{n} C(n,k) x^k y^{n-k}$$

$$= \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Proof :-

$$\because (x+y)^n = \underbrace{(x+y)\ (x+y) \qquad\qquad (x+y)}_{n \text{ times}}$$

In multiplying out, we pick one term from each factor (x + y). Hence we only obtain terms of the form $x^k y^{n-k}$. To find the coefficient of $x^k y^{n-k}$, to obtain $x^k y^{n-k}$, we need to choose k of the terms from which we choose x. This can be done in $\binom{n}{k}$ ways.

In particular, we have

$(x + y)^2 = \binom{2}{0}x^2 + \binom{2}{1}xy + \binom{2}{2}y^2$

$= x^2 + 2xy + y^2$

$(x + y)^3 = \binom{3}{0}x^3 + \binom{3}{1}x^2y + \binom{3}{2}xy^2 + \binom{3}{3}y^3$

$= x^3 + 3x^2y + 3xy^2 + y^3$

Let us give few of the applications of binomial theorem. The coefficient of x^{20} in the expansion of $(1 + x)^{30}$ is obtained by taking y = 1 in the above theorem and n = 30, we are looking for the coefficient of 1^{10}, x^{20}, that is,

$$C(30,10) = \binom{30}{10} = \binom{30}{20}$$

Theorem :- For $n \geq 0$,

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

Proof :- Note that $2^n = (1 + 1)^n$

Hence putting x = y = 1 in the binomial expansion we get

$$2^n = \sum_{k-0}^{n} \binom{n}{k} 1^k 1^{n-k}$$

$$\Rightarrow \qquad 2^n = \sum_{k-0}^{n} \binom{n}{k}$$

$$\binom{n}{0}+\binom{n}{1}+.....+\binom{n}{n}$$

Theorem :- For n > 0

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

Proof :-

$$\because 0=(1-1)^n=(-1+1)^n=\sum_{k=0}^{n}\binom{n}{k}(-1)^k 1^{n-k}$$

$$\Rightarrow \qquad 0=\binom{n}{0}-\binom{n}{1}+.....+(-1)^n\binom{n}{n}$$

Corollary :- For n > 0

$$\binom{n}{0}+\binom{n}{2}+.....=\binom{n}{1}+\binom{n}{3}+.....$$

The interpretation of this corollary is that the number of ways to select on even number of objects from n equals the number of ways to select an odd number.

The multinomial theorem says how to expand a power of a sum in terms of the terms in the sum. It is the generalization of the Binomial expansion.

Theorem :- For any positive integer m and any non-negative integer n, the multinomial formula tells us how a sum with m terms expands, when raised to an arbitrary power n.

$$(x_1+x_2+.....+x_m)^n=\sum_{k_1+k_2+...+k_m=n}\binom{n}{k_1,k_2,.....,km}x_1^{k_1}x_2^{k_2}\quad x_m^{k_m}$$

where

$$\binom{n}{k_1,k_2,.....,km}=\frac{n!}{k_1!k_2!.....k_m!}$$

Multinomial coefficient. The sum is taken over all combinations of nonnegative integer.

In the case m = 2, this statement reduces to that of Binomial theorem.

For example, the third power of the trinomial x + y + z is given by

$(x + y + z)^3 = x^3 + y^3 + z^3 + 3x^2y + 3x^2z + 3y^2x + 3y^2z + 3z^2x + 3z^2y + 6\,xyz$

$x^2y^0x^1$ has coefficient $\binom{3}{2,0,1} = \frac{3!}{2!\,0!\,1!} = 3$

$x^1y^1x^1$ has coefficient $\binom{3}{1,1,1} = \frac{3!}{1!\,1!\,1!} = 6$

Proof :-

This proof of the multinomial theorem uses the binomial theorem and induction on m. For m = 1, both sides equal x_1^n.

Suppose the theorem hold for m. Then

$(x_1 + x_2 + \ldots.. + x_m + x_{m+1})^n = (x_1 + x_2 + \ldots.. + x_m + x_{m+1})^n$

$$= \sum_{k_1+k_2+\ldots.+k_{m-1}+k=n} \binom{n}{k_1,k_2,\ldots\ldots,k_{m-1},k} x_1^{k_1} x_2^{k_2} \quad x_{m-1}^{k_{m-1}}$$

(By the Induction hypothesis)

Applying the Binomial theorem to the last factor,

$$= \sum_{k_1+k_2+\ldots..+k_{mr}+k=n} \binom{n}{k_1,k_2,\ldots\ldots k_{m-1},k} x_1^{k_1} x_2^{k_2} \quad x_{m-1}^{k_{m-1}}$$

$$\sum_{k_m+k_{m+1}=k} \binom{k}{k_m,k_{m+1}} x_m^{k_m} \; x_{m+1}^{k_{m+1}}$$

$$= \sum_{k_1+k_2+\ldots+k_{mr}+k_{m+1}=n} \binom{n}{k_1,k_2,\ldots k_m,k_{m+1}} x_1^{k_1} x_2^{k_2} x_{m-1}^{k_{m-1}} x_m^{k_m} x_{m+1}^{k_{m+1}}$$

The last step holds true, because

$$\binom{n}{k_1,k_2,\ldots,k_{m-1},k}\binom{k}{k_m,k_{m+1}} = \binom{n}{k_1,k_2,\ldots,k_{m-1},k_{m+1}}$$

In factorial notation,

$$\frac{n!}{k_1!k_2!\ldots.k_{m-1}!k!}\;\frac{k!}{k_m!k_{m+1}!} = \frac{n!}{k_1!k_2!\ldots.k_m!k_{m+1}}$$

Note :- The substitution of x = 1 for all into

$$\sum_{k_1+k_2+....+k_m=n} \binom{n}{k_1, k_2, ..., k_m} x_1^{k_1} x_2^{k_2} \ldots \; x_m^{k_m}$$

gives that

$$\sum_{k_1+k_2+....+k_m=n} \binom{n}{k_1, k_2, ..., k_m} = \underbrace{(1+1+.....+1)^n}_{m \text{ times}}$$

$$= m^n$$

Let us see one of the application of the multinomial theorem

Suppose that there are n objects,

n_1 objects of type 1, n_2 objects of type *2, ..., n_k* objects of type k with

$n_1 + n_2 + ….. + n_k = n$. Then the number of distinct permutations of these objects is the multinomial co-efficient

$$C(n, n_1, n_2, ... n_k) = \frac{n!}{n_1! n_2! .....n_k!}$$

For instance, suppose that *n = 3* and there are two type 1 objects, a and a and one type 2 object b. Then there are *3! = 6* permutations of the three objects, but some of these are indistinguishable.

b_a, a_2 is same as ba_2a_1. Therefore there are only $\frac{3!}{2!1!} = 3$ distinguishable permutations baa, aba aab, As an another example, there are $\frac{9!}{3!1!1!2!1!1!}$ different words that can be formed using all letters of the word “excellent”.

2.11 Let Us Sum Up/Summary

1) The sum rate states that if thee are n, ways of performing task 1, n_2 ways of performing task 2 and so on, nr ways of performing task r then either of these r-tasks can be executed in $n_1 + n_2 + ... + n_r$ ways.

2) The product rule state that if there is procedure consisting of performing r different tasks together, if first task can be completed in n_1 ways, second task can be completed in n_2 ways and similarly r^{th} task can be completed in n_r

ways, all r-tasks are performed independent of each other. Then the procedure can be performed in $n_1 \times n_2 \times ..... \times n_r$ different ways.

3) Let n ≥ r, then the number of r-permutations can be given by $P(n, r)$

$$P(n,r) = \frac{n!}{(n-r)!}$$

4) The number of all subsets of an n-set X is 2^n.

5) The number of r – combinations of an n-set X is given by $C(n, r)$ and $C(n,r) = \frac{n!}{r!(n-r)!}$

6) Pascal's Identity :

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

7) Binomial co-efficient is denoted by $C(n,r) = \binom{n}{r} \frac{n!}{r!(n-r)!}$ and multinomial coefficient is denoted by $C(n, n_1, n_2, \ldots n_k)$

$$C(n, n_1, n_2, ... n_k) = \binom{n}{n_1, n_2, ... n_k} \frac{n!}{n_1! n_2! ..... n_k!}$$

8) Binomial Expansion :-

For n ≥ 0

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

9) Multinomial Expansion

$$(x_1 + x_2 + ... + x_m)^n = \sum_{k_1+k_2+....+k_m=n} \binom{n}{k_1, k_2, ..., k_m} x_1^{k_1} x_2^{k_2} \quad x_m^{k_m}$$

10) The number of permutations of an n-number of objects with n_1 objects of type 1, n_2 objects of type 2, and n_k objects of type k ($n_1 + n_2 + ... + n_k = n$) is given by the multinomial co-efficient

$$C(n, n_1, n_2, ... n_k) = \frac{n!}{n_1! n_2! ..... n_k!}$$

2.12 Solved Numericals

1) There are 80 mathematics and 50 statistics books. How many ways we can pick either type of book ?

   Solution :- One book, either of mathematics or statistics can be selected in $80 + 50 = 130$ ways (by the sum rule)

2) How many ways, we can select either a Heart card or a diamond card from 52 playing cards ?

   Solution :- There are 13 Heart cards and 13 diamond cards. Therefore there are $13 + 13 = 26$ ways to pick a card of Heart or diamond. (by the sum rule)

3) At one time, a local telephone number was given by a sequence of two letters followed by five numbers. How many different telephone numbers were there?

   Solution :- Using the product rule, there are $26 \times 26 \times 10 \times 10 \times 10 \times 10 \times 10 = 26^2 \times 10^5$ different telephone numbers available.

4) Show that in a graph G, the sum of degrees over all vertices is even.

   Solution :- We count all the incidences between vertices are edges in two ways. The number of edges incident with a vertex ν is the degree of ν, denoted by d(ν). So basically, we want to know parity of ∑ d(ν). Since every edge is incident with exactly two vertices, the sum of all degrees is same as twice the number if edges, Hence ∑ d(ν) is always an even number.

5) Let A, B be two finite nonempty sets then show that

   $|A \cup B| = |A| + |B| - |A \cap B|$

   Solution :- Let $A = \{a_1, a_2, \ldots, a_m\}$

   $B = \{b_1, b_2, \ldots, b_n\}$ and $|A \cap B| = r$

   $\Rightarrow$ exactly r of the ai's and bj's are same. Assume that

   $a_1 = b_1, a_2 = b_2, a_r = b_r$

   $\Rightarrow$ $|A \cup B| = m + n - r$

   $\therefore$ $|A| = m,\ |B| = n$ & $|A \cap B| = r$

   $\therefore$ $|A \cup B| = |A| + |B| - |A \cap B|$

6) Find the total number of signals that can be made by five flags of different color, when any number of them may be used in any signal.

Solution :-

Case 1 – When only one flag is used

No. of signals made = $5p_1 = 5$

Case 2 – When only two flags are used

No. of signals made = $5p_2 = 5 \times 4 = 20$

Case 3 – When only three flags are used

No. of signals made = $5p_3 = 5 \times 4 \times 3 = 60$

Case 4 – When only four flags are used

No. of signals made = $5p_4 = 120$

Case 5 – When only five flags are used

No. of signals made = $5p_5 = 5! = 120$

Hence, by the sum rule, the required number is =

$5 + 20 + 60 + 120 + 120 = 325$

7) If there are 5 men and 6 women in how many ways a committee consisting of four persons can be formed such that it contains atleast one woman ?

Solution :- A typical committee of four persons consisting of atleast one woman will look like

1) one women, three men

2) two women, two men

3) three women, one man

4) All four women

There are ${}^6C_1 \times {}^5C_3$ to form committee, of case 1 There are ${}^6C_2 \times {}^5C_2$ ways to form committee of Case 2, there are ${}^6C_3 \times {}^5C_1$ ways to form committee of Case 3 and ${}^6C_4 \times {}^5C_0$ ways to form a committee of case 4. Therefore by the sum rule, there are

${}^6C_1 \times {}^5C_3 + {}^6C_2 \times {}^5C_2 + {}^6C_3 \times {}^5C_1 + {}^6C_4 \times {}^5C_0$

Different ways to form a committee of four persons consisting of atleast one women.

8) Find $\sum_{k=1}^{n} k\binom{n}{k}$

Solution :- By Binomial theorem, we know that

$$(x+1)^n = \sum_{k=1}^{n} {}^nC_k x^k 1^{n-k}$$

$\therefore$ Differentiating with respect to x, we get

$$n(x+1)^{n-1} = \sum_{k=1}^{n} {}^nC_k k\, x^{k-1}$$

Putting x = 1 $\Rightarrow$

$$n(1+1)^{n-1} = \sum_{k=1}^{n} k\,{}^nC_k$$

Therefore

$$\sum_{k=1}^{n} k\binom{n}{k} = n2^{n-1}$$

9) What is the co-efficient of a^3bc^2 in the expansion of $(a + b + c)^6$?

Solution :- By multinomial theorem, the coefficient of $a^3b^1c^2$ in the expansion of $(a + b + c)^6$ is the multinomial coefficient

$$C(6,3,1,2) = \binom{6}{3,1,2} = \frac{6!}{3!1!2!}$$

$$= 60$$

10) In a kennel that is short of space, 12 dogs must be put into 3 cages, 4 in cage 1, 5 in cage 2 and 3 in cage 3. In how many ways can this be done?

Solution :- n = 12, with $n_1 = 4$, $n_2 = 5$, $n_3 = 3$, n_1 dogs are of the same type, n_2 objects are of the same type and n_3 objects are of the same type. So, there are

$C(12,4,5,3) = \frac{12!}{4!5!3!}$ ways to put dogs into 3 cages.

2.13 Unit end Excercises

1) How many bit strings have length 3, 4 or 5!

   (Hints :- Use sum rule, A bit string is made up of 0's and 1's)

2) In how many ways we can get a sum of 3 or a sum of 4, when two dice are rolled? (Use sum rule).

3) How many ways are these to rank five potential basketball recruits of different heights if the tallest one must be ranked first and the shortest one last?

4) A value function on a set A assigns 0 or 1 to each subset of A.

   a) If A has 3 elements, how many different value functions are there on A?

   b) What if A has n elements?

5) A company is considering 6 possible new computer systems and it's system manager would like to try out at most 3 of them. In how many ways can the systems manager choose the systems to be tried out?

6) Show that

$$\binom{n+m}{r} = \binom{n}{o}\binom{m}{r} + \binom{n}{1}\binom{m}{r-1} + \ldots\ldots + \binom{n}{r}\binom{m}{o}$$

7) How many different 11- letters words can be made from the letters of the word ABRACADABRA?

   (Use multinomial theorem)

8) Find the co-efficient of $a^3bc^4d^2$ in the expansion of $(a + b + c + d)^{10}$. (Use multinomial theorem)

9) Suppose there are 6 candidates for job interviews, how many different ways are there for 2 of them to be interviewed on Monday, 2 on Wednesday, and 2 on Saturday?

   (Use multinomial theorem)

10) Let $P_n(k)$ denotes the number of permutations of the set {1, 2, …, n}, which fixes exactly k numbers. Prove that

$$\sum_{k=0}^{n} kP_n(k) = n!$$

(Hint - The LHS is the total number of fixed points in all $(n! = \underbrace{(n-1)! + (n-1)! + ... + (n-1)!}_{n \text{ times}})$ permutations of {1, 2, …, n}

❖❖❖❖

Unit 1

3

ADVANCE COUNTING

Unit Structure :

3.0 Objective

After going through this chapter you can able to known that

- Different methods of counting problems.
- Occupancy problems.
- Different types of occupancy problems.
- Number of solutions of equation by using occupancy problems.

3.1 Introduction:

Combinatorics, which is also refer as combinatorial mathematics is the field of mathematics consent with problems of selections, arrangement and operation with a finite or discrete system. Its objective is how to count without ordinary counting.one of the basic problem of Combinatorics is to determine the number of possible configurations of objects of a given type. This chapter includes

numerous quite elementary topics such as enumerating all permutation or combination of a finite set.

There are three essential problems in combinatorics. These are the existence problem, the counting problem, and the optimization problem. This course deals primarily with the first two in reverse order.

3.2 Occupancy problems:

The purpose of this ultimate section is to show that some basic counting exercises can be re-phrased as so-called occupancy problems. A consequence will be that we can easily introduce occupancy problems which are not amenable to the elementary tactics we have dealt with so far.

The basic occupancy problem has us placing *n* objects into *k* containers / boxes. To classify the type of occupancy problem we have, we must answer three yes/no questions. There will therefore be 8 =2^3 basic occupancy problems. The three questions are:

1) Are the objects distinguishable from one another?

2) Are the boxes distinguishable from one another?

3) Can a box remain unoccupied?

If the answer to all three questions is yes, then the number of ways to place the *n* objects in to the *k* boxes is clearly the number of functions from an *n*-set to a *k*-set, which is k^n.

If, on the other hand the answer to the first question is no, but the other two answers

are yes, then we have the basic donut Shoppe problem. So the number of ways to distribute *n* identical objects among *k* distinguishable boxes is the number of solutions in non-negative whole numbers to $x_1 + x_2 + x_3 + \cdots \ldots \ldots + x_k = n$ where x_i is the number of objects placed in the *i*th box.

If we change the answer to the third question to no, then we have the more realistic donut Shoppe problem. Now we need the number of solutions in positive integers to $x_1 + x_2 + x_3 + \cdots \ldots \ldots + x_k = n$ or equivalently the number of solutions in non-negative integers to$y_1 + y_2 + \cdots \ldots \ldots \ldots + y_k = n - k$. This is $C((n-k)+k-1, n-k) = C(n-1, n-k) = C(n-1, k-1)$.

So it might appear that there is nothing really new here. That every one of our occupancy problems can be solved by an elementary counting technique. However if we define $S(n, k)$ to be the number of ways to distribute n distinguishable objects into k indistinguishable boxes we will defining

$$S(n,k)=\frac{1}{k!}\sum_{i=0}^{k}(-1)^i\binom{k}{i}(k-i)^n$$

Upon making this definition we can answer three more of our eight basic occupancy

problems. This is summarized in the table.

Objects distinguished	Box distinguished	Empty box allowed	Number of ways to complete
Y	Y	Y	k^n
Y	Y	N	$k!\,S(n,k)$
N	Y	Y	$\binom{k+n-1}{k}$
N	Y	N	$\binom{n-1}{k-1}$
Y	N	Y	$\sum_{i=1}^{k} S(n,i)$
Y	N	N	$S(n,k)$

The numbers $S(n, k)$ are called the Stirling numbers of the second kind. The table indicates their relative importance for counting solutions to occupancy problems.

3.3 Basic Combinatorial Numbers:

Let throughout this this chapter X stand for the n-set {1, 2, 3, ….., n } and A stand for the m-set $\{a_1, a_2, a_{3,\ldots\ldots}, a_m\}$. Let X stands for a set of n distinct objects to be distributed or sorted into the m boxes. Consider a map $\emptyset: X \to A$. There are m^n such possible maps. Every such map allows several interpretations. We can think $\emptyset$ as

$$\begin{pmatrix} 1 & 2 & 3 & \ldots\ldots\ldots\ldots & n \\ \phi(1) & \phi(2) & \phi(3) & \ldots\ldots\ldots\ldots\ldots & \phi(n) \end{pmatrix}.$$

$\emptyset$ describes a way of sorting the n objects into the m boxes. With this interpretation, we says that the object j goes into the box a_{ij} . This way of sorting shall be called as combinatorial distribution or simply distribution.

General guideline for modeling distribution problems are:

Distributions of distinct objects are equivalent to arrangements and distributions of identical objects are equivalent to selections.

3.3.1 Basic Modals for distribution:

The distribution of n distinct objects into m distinct boxes and the distribution of n identical objects into m distinct boxes are the two basic modals for distribution. There are m^n distributions of the n distinct objects in m distinct boxes. and $C(n+m-1,n)$ distributions of the n-identical objects in m distinct boxes.

Theorem: Let M and N be two sets such that $|M| = m$ and $|N| = n$. Then the total number of function $f: M \to N$ equals m^n.

Proof: Let $M = \{a_1, a_2, a_3, \ldots\ldots, a_m\}$ and $N = \{b_1, b_2, b_3, \ldots\ldots b_n\}$.

Since the function is determined as soon as we know the value of $f(a_i) = a_i$ for $1 \le i \le m$, a function $f: M \to N$ has the from

$$\begin{pmatrix} a_1 & a_2 & a_3 & \ldots\ldots\ldots\ldots & a_m \\ f(a_1) & f(a_2) & f(a_3) & \ldots\ldots\ldots\ldots & f(a_m) \end{pmatrix}$$

Where $f(a_i) \in \{b_1, b_2, \ldots\ldots, b_n\}$ for $1 \le i \le m$. As there is no restriction on the function f, $f(a_1)$ has n choices $b_1, b_2, \ldots\ldots, b_n$.

Similarly $f(a_2)$ has n choices $b_1, b_2, \ldots\ldots, b_n$ and so on. Thus the total number of function $f: M \to N$

is $\xrightarrow[m \ \ times]{n \times n \times n \times \ldots\ldots\ldots \times n} = n^m$.

Example 1: How many ways are there to distribute four identical balls and six distinct balls into five distinct boxes?

Solution: There are $C(4+5-1,4)=70$ ways to distribute four identical balls into five distinct boxes and $5^6=15625$ ways to put six distinct balls in five distinct boxes. These processes are disjoint, and so there are $70\times 15625=1{,}093{,}750$ ways to distribute the four identical and six distinct balls.

Example 2: How many solution does the following equation $x_1+x_2+x_3+x_4=15$ have, x_1, x_2, x_3 and x_4 are non-negative integers?

Solution: We assume we have four types labeled x_1, x_2, x_3 and x_4. There are 15 items or units (since we are looking for an integer solution). Every time an item (unit) is selected it adds one to the type it picked it up. Observe that a solution corresponds to a way of selecting 15 items (units) from a set of four elements. Therefore, it is equal to 1combinations with repetition allowed from a set with four elements. we have

$$C(4+15-1,15)=C(18,15)=C(18,3)=\frac{18\times 17\times 16}{3\times 2\times 1}=816.$$

Example 3: How many different ways can we distribute n indistinguishable balls into

k distinguishable boxes?

Solution: Every distribution of balls can be represented as a sequence of bullets and lines.

••|•••|•|••

••|•••||••

••••••••|||

So putting *n* balls in to *k* boxes boils down placing *k* -1 vertical lines in a line of *n* bullets.

There are total of *n*+*k*-1 possible positions for the bars.

Hence there are $\binom{n+k-1}{k-1}=\binom{n+k-1}{n}$ ways of selecting k-1 positions.

So it can be done by $\binom{n+k-1}{n}$.

The number of ways to place n indistinguishable objects into k indistinguishable boxes if no box is empty is the number of partitions of n into exactly k parts. If we denote this by $p_k(n)$, then we see that $p_2(5) = 2$. Also $p_1(n) = p_n(n) = 1$ for all positive integers n.

Meanwhile $p_k(n) = 0$ is $k > n$. Finally $p_2(n) = \left|\frac{(n-1)}{2}\right|$.

The final occupancy problem is to place n indistinguishable objects into k indistinguishable boxes if some boxes may be empty. The number of ways this can be done by

$$\sum_{i=1}^{k} p_i(n)$$

This is the number of partitions of n into k or fewer parts.

Example 4: Determine the number of ways of putting k indistinguishable balls into n indistinguishable boxes with the restriction that no box is empty?

Solution: Since the balls are indistinguishable balls, the problem reduces to counting the number of balls in each box with the condition that no box is empty. As the boxes are also indistinguishable, they can be arranged in such a way that the number of balls inside them are in non-increasing order. Hence, we have the answer as $S(k, n)$.

Example 5: Determine the number of ways to put k indistinguishable balls into n indistinguishable boxes.

Solution: The problem can be rephrased as follows: "suppose that each box already has 1 ball, i.e., initially, each of the n boxes are non-empty. Now let us determine the number of ways of putting k indistinguishable balls into the n indistinguishable boxes that are already non-empty." This new problem is same as "in how many ways can $k + n$ indistinguishable balls be put into n indistinguishable boxes with the restriction that no box is empty". Therefore, the answer to our problem reduces to computing $S(m + n, n)$.

3.3 INDISTINGUISHABLE BALLS IN INDISTINGUISHABLE BOXES:

Till now, we have been looking at problems that required arranging the objects into a row.

That is, we differentiated between the arrangements ABCD and BCDA. In this section, we briefly study the problem of arranging the objects into a circular fashion. That is, if we are arranging the four distinct chairs, named A,B,C and D, at a round table then the arrangements ABCD and the arrangement BCDA are the same. That is, the main problem that we come across circular arrangements as compared to problems in the previous sections is "there is no object that can truly be said to be placed at the number 1 position".

So, to get distinct arrangements at a round table, we need to fix an object and assign it the number 1 position and study the distinct arrangement of the other $n - 1$ objects relative to the object which has been assigned position 1. We will look at two examples to understand this idea.

Example 6: Determine the number of ways to sit 8 persons at a round table.

Solution: Let us number the chairs as 1, 2, . . . , 8. Then, we can pick one of the person and ask him/her to sit on the chair that has been numbered 1. Then relative to this person, the other persons (7 of them) can be arranged in 7! ways. So, the total number of arrangements is 7!.

Example 7: Suppose we are now interested in making the 4 couples sit in a round table.

Find the number of seating arrangements.

Solution: The 4 cohesive units can be arranged in 3! ways. But we can still have the couples to sit either as "wife and husband" or "husband and wife'. Hence, the required answer is $2^4 \cdot 3!$.

3.4 Permutations of Sets with Indistinguishable Objects:

Let us now generalized the above example. Assume there are n objects with n_1 indistinguishable objects of type 1, n_2 objects of type 2... ....n_k indistinguishable objects of type k. The number of different permutations are

$$\frac{n!}{n_1!n_2!\ldots\ldots n_k!}$$

There are many ways to prove this result. For example, we know that there $n!$ permutations, but many of these permutations are the same since we have$k$

classes of indistinguishable objects. How many permutations are the same due to n_1 indistinguishable objects. Obviously, there are $n_1!$ uch permutations of type 1,$n_2!$ of type 2,…..$n_k!$ of type k . Thus the result follows.

Balls-and-Urns Model

Finally, we consider throwing n distinguishable balls (objects) into k distinguishable urns (boxes).

Consider the following example. There are n balls, and three boxes. We want to know in how many ways we can throw these n balls such that there are n_1 balls in the first box, n_2 in the second box, and n_3 balls in the third box. Of course, there are $C(n, n_1)$ of ways putting n_1 balls from a set of n balls into the first box. For every such an arrangement, the remaining $n - n_1$ balls can be thrown in $C(n - n_1, n_2)$ ways into the second box so that it contains n_2 balls. Finally, the last box will have n_3 balls on $C(m - n_1 - n_2, n_3)$ ways. Therefore, by the multiplication rule we have

$$C(n, n_1)C(n - n_1, n_2)C(m - n_1 - n_2, n_3) = \frac{n!}{n_1!n_2!n_3!(n-n_1-n_2-n_{3)!}}.$$

In general, let n distinguishable objects be thrown into k distinguishable boxes with n_i objects in the ith box, $i = 1,2,3,..k$. Then, generalizing our example, we obtain

$$\frac{n!}{n_1!n_2!n_3!\ldots\ldots\ldots n_k!(n-n_1-n_2-n_3\ldots\ldots\ldots n_k)!}$$ ways to distribute these n n objects among k k boxes.

Example 8: In how many ways we can distribute hands of 55 cards to each of four players from the deck of 52 2 cards?

Solution: We may represent this problem as throwing 52 52 objects into four boxes each containing 5 cards. since every hand has 4 cards, and after the distribution of 4.5 = 20 5 cards there remain 32 cards.

Thus the solution is $= \frac{52!}{5!5!5!5!32!}$.

3.5 Counting combinations with repetitions allowed:

There exists a bijection between any two of the following sets:

a. The set of increasing words of length n on m ordered letters,

b. The set of distributions of n non-distinct objects in to m distinct boxes,

c. The set of combinations of m symbols taken n at a time, with repetitions permitted.

The cardinality of each of these sets is $\frac{[m]^n}{n!} = C(m,n)$. The number is taken to be 1 if either
m = 1 or n = 0.

Proof: Let $a_1 a_1 \ldots\ldots, a_2 a_2 a_2 \ldots\ldots$ Be an increasing word of length n on m ordered letters. In a_1 repeated i_1 times, a_2 repeated i_2 times, and so on. Now put i_1 of the objects into the first box, i_2 of the objects into the second box, and so on.

This process and its inverse give a bijection between the sets (a) and (b) of the proposition. Since the word itself is a combination of the m symbols with repetitions permitted according to a partition $i_1 + i_2 + i_3 + \cdots \ldots \ldots$ of n , bijection between (a) and (c) is established.

To calculate the number required, note that each distribution of the n non-distinct objects into the boxes according to a partition $i_1 + i_2 + i_3 + \cdots \ldots \ldots$ of n , gives n! distributions of n-labeled objects into the boxes with the same partition.

Example 9: The Reserve bank of India print currency notes in denominations of Five Rupees, Ten Rupees, Twenty Rupees, Fifty Rupees, One Hundred Rupees, Five Hundred rupees and One Thousand Rupees. In how many ways an it display ten currency notes not necessarily denominations?

Solution: This problem is same as counting the combinations when repetitions are allowed. We need to find the number of 10 combinations of the seven denominations, with repetitions permitted. Hence the number of ways

$$C(m,n) = \frac{[m]^n}{n!} = \frac{[7]^{10}}{10!} = 8008.$$

3.6 Partition of the integer:

What remains now, is the distribution of n non-distinct objects into m non-distinct boxes, with or without exclusion principle. With each such distribution for which no box is empty, we can associate the m-tuple ($x_1, x_2, \ldots\ldots, x_m$) satisfying

$$x_1 + x_2 + x_3 + \cdots\ldots\ldots + x_m = n, \quad x_1 \geq x_2 \geq \cdots\ldots\ldots \geq x_m \geq 1.$$

Such an m-tuple is called a partition of the integer n.

Notation: The number of partitions of the integer n into exactly m classes is denoted by

$$P_n^m = P(m, n).$$

The partition above is usually written it as $x_1\ x_2 \ldots\ldots\ldots x_m$ without commas and parentheses.

If $x_1\ x_2 \ldots\ldots\ldots x_m$ is a partition of n then we write it as $x = (x_1, x_2, \ldots\ldots\ldots, x_m)$.

x may be written as $1^{r_1}2^{r_2}\ldots\ldots\ldots\ldots$

Where r_i is the number of parts equal to i in , i varying in {1, 2, 3,……}. This is explained below, the partition, 4+3+3+2+2+1 of 15 may be written as 433221 or $12^2 3^2 4$.

Hence the number of distributions of n non-distinct objects in m identical boxes (boxes could be empty or with more than one object) is $P_n^1 + P_n^2 + \cdots\ldots\ldots + P_n^m$.

This is the total number of partitions of n into m or fewer parts. If m = n, this number is denoted by $P(n)$, the number of all partitions of the integer n.

Example 10: How many distinct partitions 7 into 4 parts?

Solution: The distinct partitions 7 into 4 parts are given by 4+1+1+1, 2+3+1+1, 2+2+2+1.

Hence $P_n^m = P_4^7 = 3$.

Note: By convention, we let $P_n^m = P_0^0 = 1$ and $P_n^m = 0$ whenever n > m.

Example 11: Determine the number of ways of putting m indistinguishable balls into n indistinguishable boxes with the restriction that no box is empty?

Solution: Since the balls are indistinguishable balls, the problem reduces to counting the number of balls in each box with the condition that no box is empty. As the boxes are also indistinguishable, they can be arranged in such a way that the number of balls inside them are in non-increasing order. Hence, we have the answer as P_n^m.

Example 12: Determine the number of ways to put m indistinguishable balls into indistinguishable boxes.

Solution: The problem can be rephrased as follows: "suppose that each box already has 1 ball, i.e., initially, each of the n boxes are non-empty. Now let us determine the number of ways of putting m indistinguishable balls into the n indistinguishable boxes that are already non-empty." This new problem is same as "in how many ways can m + n indistinguishable balls be put into n indistinguishable boxes with the restriction that no box is empty". Therefore, the answer to our problem reduces to computing P(m + n, n).

3.7 Summary:

- There are three essential problems in Combinatorics.
- This is summarized in the table.

Objects distinguished	Box distinguished	Empty box allowed	Number of ways to complete
Y	Y	Y	k^n
Y	Y	N	$k!\,S(n,k)$
N	Y	Y	$\binom{k+n-1}{k}$
N	Y	N	$\binom{n-1}{k-1}$
Y	N	Y	$\sum_{i=1}^{k} S(n,i)$
Y	N	N	$S(n,k)$

3.8 Unit end exercise:

1. Determine the number of ways of selecting r distinguishable objects from n distinguishable objects when $n \geq r$?

2. How many ways are there to distribute 20 distinguishable toys among 4 children so that each children gets the same number of toys?

3. In how many ways can m distinguishable balls be put into n indistinguishable boxes, such that NO box is empty?

4. In how many ways can m distinguishable balls be put into n indistinguishable boxes?

5. How many ways are there to distribute 8 balls into 6 boxes with the first 2 boxes collectively having at most 4 ball if:
   a. The balls are identical.
   b. The balls are distinct.

6. How many distinct ways are there to make a 5 letter word using the ENGLISH alphabet
   a. With ONLY consonants?
   b. With ONLY vowels?
   c. With a consonant as the first letter and a vowel as the second letter?
   d. If the vowels appear only at odd positions?

7. How many ways are there to distribute 20 distinguishable toys among 4 children so that each children gets the same number of toys?

8. In how many ways can m distinguishable balls be put into n indistinguishable boxes?

9. How many nonnegative integer solutions are there to the equation

$$x_1 + x_2 + x_3 + x_4 + x_5 = 67?$$

10. With repetition allowed and order counting, how many ways are there to select r things from n distinguishable things?

11. Determine the number of ways to sit 5 men and 7 women at a round table with NO 2 men sitting next to each other?

12. Determine the number of ways to sit 8 persons, including Ram and Shyam, at a round table with Ram and Shyam NOT sitting diametrically opposite to each other?

13. Determine the number of ways to select 6 men from 25 men who are sitting at a round table if NO adjacent men are to be chosen?

14. Find all partitions of 8 into four or fewer parts.

15. How many solutions in non-negative integers are there to $x1 + x2 + x3 + x4 = 18$ which satisfy $1 \leq xi \leq 8$ for $i = 1, 2, 3, 4$?

4

ADVANCED COUNTING - II

Unit Structure :

4.0 Objectives

After going through this chapter you will be able to:

- define Stirling's number of first and second kind
- solve problems based on Stirling's numbers
- define the statement of Principle of inclusion-exclusion
- use inclusion-exclusion principle to solve derangement problems

4.1 INTRODUCTION

In the previous chapter we have studied about distinguishable balls put into distinguishable/indistinguishable boxes. Let $f : X \to Y$ such that |X| = n and |Y| = k.

Consider the problem of determining the number of ways of putting n distinguishable balls into k indistinguishable boxes, with the condition that no box

remains empty. Let X = $\{x_1, x_2, x_3, \ldots, x_n\}$ be the set of n balls. Since the boxes are indistinguishable, we can assume that the number of balls in each of the boxes is in a non-increasing order. Let X_i denote the set of balls in the i-th box, $1 \le i \le k$. Then $|X_1| \ge |X_2| \ge \ldots \ge |X_k|$ and $\bigcup_{i=1}^{k} X_i = X$. Since each box is non-empty, $X_i \neq \phi$, for all $1 \le i \le k$. Thus, we have obtained a partition of the set X, consisting of n elements, into k-parts, $X_1, X_2, \ldots, X_k$. The number of required ways here, is given by $S(n, k)$, that is the Stirling number of second kind. We shall see the formal definition in the following section.

4.3 Stirling's number

Let us recollect first the definition of a *partition* of a set. Let X be a non-empty set. Then a partition Π of X into k parts, is a collection of non-empty subsets X_1, $X_2, \ldots, X_k$, of X such that :

(i) $X_i \cap X_j = \phi$

(ii) $\bigcup_{i=1}^{k} X_i = X$

4.3.1 Stirling number of second kind:

Let $|X| = n$. The number of partitions of the set X into k-parts is denoted by $S(n, k)$ and is called as *Stirling number of the second kind*.

Remark:

1. The number of partitions of a n-set into n-parts is 1.
2. The number of partitions of a n-set into 0 parts is 0.
3. The number of partitions of a n-set into k-parts with $k > n$ is also 0.
4. The above three can be summed as follows:

$$S(n,k) = \begin{cases} 1 & \text{if } n = k \\ 0 & \text{if } k = 0 \\ 0 & \text{if } k > n \end{cases}$$

Lemma: Let X and Y be two finite sets with $|X| = m$ and $|Y| = n$. Then the total number of onto functions $f : X \to Y$ is $n!S(m, n)$.

4.3.2 Stirling's number of first kind

Definition: The Stirling number of first kind, denoted by $s(n, k)$ is the number of permutations of an n-set with precisely k cycles.

We define $s(0, 0) = 1$ and $s(0, k) = 0$ for $k > 0$.

Several different notations for the Stirling numbers are in use. Stirling numbers of the first kind are denoted with a small s, and those of the second kind with a capital S. The Stirling numbers of the second kind are never negative, but those of the first kind can be negative; hence, there is a separate notation for the unsigned Stirling numbers of the first kind.

4.4 Principle of Inclusion-Exclusion

Example 1: In a set $S = \{1, 2, 3, \ldots, 100\}$, one out of every 7 is a multiple of 7, so that the total number of multiples of 7 in S is $\left[\frac{100}{7}\right] = 14$ ($[x]$ means the integer part of x). Similarly, the total number of multiples of 3 in S is $\left[\frac{100}{3}\right] = 33$.

The question now is, how many are multiples of 7 or 3?

Is the answer 14 + 33 = 47? Well, no. The reason is that 14 + 33 counts those numbers twice which are multiples of 7 **as well as of** 3, for e.g. 21. How many such numbers are there in S which are multiples of 7 **and** 3? They are $\left[\frac{100}{21}\right] = 4$.

Hence the correct answer to the above question is 14 + 33 – 4 = 43.

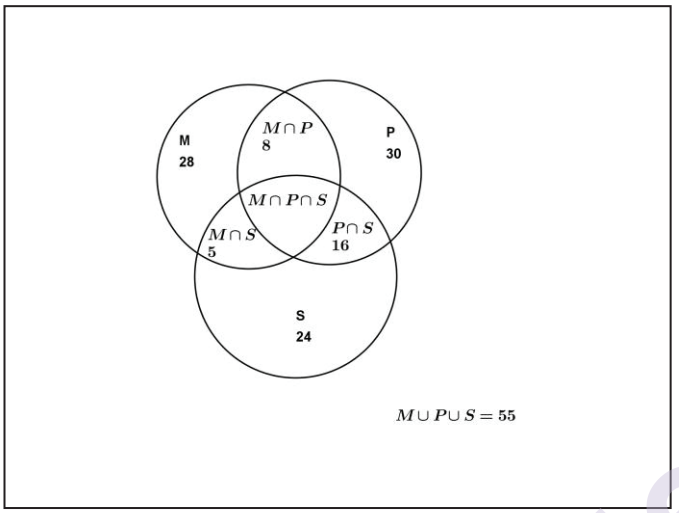
Now, if we want to know how many numbers in S are not multiples of 7 or 3, then we need to just subtract 43 from 100, i.e. 100 – 43 = 47 numbers in S are not multiples of either 7 or 3.

Example 2: Let us consider another example. In a College there are:

- 28 students in Mathematics
- 30 students in Physics
- 24 students in Statistics

- 8 students in both Mathematics and Physics
- 16 students in both Physics and Statistics
- 5 students in both Mathematics and Statistics
- And 55 students in either Mathematics, Physics or Statistics

How many students are there in all three subjects in the College?



Such problems can be solved using the principle of Inclusion and Exclusion stated below:

Statement: Consider a set of N objects and a set of n properties $\alpha_1, \alpha_2, \ldots, \alpha_n$. Some of the N objects may have none of these properties. Some may have more than one of these. Let $N(\alpha_1 \alpha_2 \ldots \alpha_n)$ denote the number of objects having any of the properties $\alpha_1, \alpha_2, \ldots, \alpha_n$ and $N(\alpha_1' \alpha_2' \ldots \alpha_n')$ denote the number of objects having none of the properties $\alpha_1, \alpha_2, \ldots, \alpha_n$ then,

$$N(\alpha_1' \alpha_2' \ldots \alpha_n') = N - N(\alpha_1) - N(\alpha_2) - \ldots - N(\alpha_n) + N(\alpha_1 \alpha_2) + N(\alpha_1 \alpha_3) + \ldots + N(\alpha_{n-1} \alpha_n)$$

$$- N(\alpha_1 \alpha_2 \alpha_3) - N(\alpha_1 \alpha_2 \alpha_4) - \ldots - N(\alpha_{n-2} \alpha_{n-1} \alpha_n)$$

$$+ \ldots$$

$$+ (-1)^n N(\alpha_1 \alpha_2 \ldots \alpha_n)$$

Thus, the solution to the Example 2 is;

$$N(A \cup B \cup C) = N(A) + N(B) + N(C) - N(A \cap B) - N(A \cap C) - N(B \cap C) + N(A \cap B \cap C)$$

$$55 = 28 + 30 + 24 - 8 - 16 - 5 + N(A \cap B \cap C)$$

$$N(A \cap B \cap C) = 55 - 53 = 2$$

Remark: The proof of the principle of inclusion and exclusion can be done using principle of mathematical induction on *n*.

Example 3: In a sports club with 54 members, 34 members play cricket, 22 play squash and 11 play chess. Of these 10 play cricket and squash, 6 play cricket and chess and 4 play squash and chess. If 2 members play all the games, find how many play none of the games?

Solution: Let A: member playing cricket, B: member playing squash and C: member playing chess.

We are given that, N = 54, N(A) = 34, N(B) = 22, N(C) = 11, N(AB) = 10, N(AC) = 6,

N(BC) = 4 and N(ABC) = 2.

We want to find $N(A'B'C')$.

Now $N(A'B'C')$ = N – N(A) – N(B) – N(C) + N(AB) + N(AC) + N(BC) – N(ABC)

$$= 54 - 34 - 22 - 11 + 10 + 6 + 4 - 2$$

Thus $N(A'B'C') = 5$

Check your progress

1. Find the number of integers between 1 and 250, that are not divisible by 2, 3 and 5.

2. In a survey of students it was found that 80 students knew Marathi, 60 knew English, 50 knew Sanskrit, 30 knew Marathi and English, 20 knew English and Sanskrit, 15 knew Marathi and Sanskrit and 10 knew all the three languages. How many students knew:

   (i) At least one language

   (ii) Marathi only

   (iii)English and one but not both English and Sanskrit

3. Determine the number of primes not exceeding 100. (Hint: Observe that primes not exceeding 100 are those positive integers greater than 1 and not exceeding 100 which are not divisible by 2, 3, 5 or 7)

4.4.1 Application to Derangement problems

Definition: A **derangement** is a permutation of objects that leaves no object in its original position.

As an application of the principle of inclusion and exclusion, we will find a formula for derangements of n symbols. Let D_n denote the number of derangements on n symbols.

Theorem: The number of derangements of a set of n elements is :

$$D_n = n!\left[1-\frac{1}{1!}+\frac{1}{2!}-\frac{1}{3!}+\ldots+(-1)^n\frac{1}{n!}\right]$$

Proof: The total number of permutations on n symbols is n!. So let $N = n!$.

For $i = 1, 2, 3, \ldots, n$, let α_i denote the property that i occurs in its original place in a permutation.

Thus, by definition of derangement and by principle of inclusion-exclusion, we have,

$$D_n = N(\alpha_1'\alpha_2'\ldots\alpha_n') = N - N(\alpha_1)-N(\alpha_2)-\ldots-N(\alpha_n) + N(\alpha_1\alpha_2)+N(\alpha_1\alpha_3)+\ldots+N(\alpha_{n-1}\alpha_n)$$

$$-N(\alpha_1\alpha_2\alpha_3)-N(\alpha_1\alpha_2\alpha_4)-\ldots-N(\alpha_{n-2}\alpha_{n-1}\alpha_n)$$

$$+\ldots+(-1)^n N(\alpha_1\alpha_2\ldots\alpha_n) \quad (*)$$

Now, N = n!

$N(\alpha_1)$ = number of permutations in which α_1 is in its original place

= number of permutations in which α_1 is fixed

= number of permutations on $(n - 1)$ symbols

$= (n - 1)!$

Thus, $N(\alpha_i) = (n-1)!$ for each $i = 1, 2, 3, \ldots, n$.

Each such α_i can be selected from $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$ in ${}^nC_1$ ways.

Thus, $N(\alpha_1) + N(\alpha_2) + N(\alpha_3) + \ldots + N(\alpha_n) = {}^nC_1 (n-1)! = \dfrac{n!}{1!}$

Similarly,

$N(\alpha_1\alpha_2)$ = number of permutations in which α_1 and α_2 are fixed.

= number of permutations on $n - 2$ symbols

Thus $N(\alpha_1\alpha_2) = (n-2)!$

Each such pair can be selected from $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$ in ${}^nC_2$ ways.

Thus, $N(\alpha_1\alpha_2) + N(\alpha_1\alpha_3) + \ldots + N(\alpha_{n-1}\alpha_n) = {}^nC_2 (n-2)! = \dfrac{n!}{2!}$

On the same lines we have,

$$N(\alpha_1\alpha_2\alpha_3) + N(\alpha_1\alpha_2\alpha_4) + \ldots + N(\alpha_{n-2}\alpha_{n-1}\alpha_n) = {}^nC_3 (n-3)! = \frac{n!}{3!}$$

Substituting all such values in (*), we get,

$$D_n = n! - \frac{n!}{1!} + \frac{n!}{2!} - \frac{n!}{3!} + \ldots + (-1)^n \frac{n!}{n!}$$

Thus, $D_n = n!\left[1 - \dfrac{1}{1!} + \dfrac{1}{2!} - \dfrac{1}{3!} + \ldots + (-1)^n \dfrac{1}{n!}\right]$

Check your progress

A new employee checks the hats of *n* people visiting a restaurant, forgetting to put claim check numbers on the hats. When customers return for their hats, the checker gives them back hast chosen at random from the remaining hats. What is the probability that no one receives the correct hat? What is the probability as *n* tends to infinity?

4.5 Let Us Sum Up

In this chapter we have seen learned about Stirling number of first and second kind. Also we have seen principle of inclusion-exclusion and its application to derangement problems.

4.6 Unit End Exercises

1. In a class of 150 students 70 have opted Maths, 80 have opted Physics and 90 have opted Stats. Of these

2. In how many ways can the digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 be arranged so that no even digit is in its original position?

3. How many derangements of {1, 2, 3, 4, 5, 6} begin with the integers 1, 2, and 3 in some order?

4. n persons pick up their hats at random in a club. Show that the probability that no one gets a right hat is $1/e$ as n tends to infinity.

Unit 2

5

PIGEON-HOLE PRINCIPLE

Unit Structure :

5.1 Objectives

After going through this chapter you will be able to:

- Pigeon-hole principle and its generalised.
- Application of pigeon-hole principle.
- Monotone subsequences and Erdos-Szekers theorem.
- Remsay number and its application.

5.2 Introduction

The pigeonhole principle is one of the most used tools in combinatorics, and one of the simplest ones. It is applied frequently in graph theory, enumerative combinatorics and combinatorial geometry. The pigeonhole principle seems trivial and in some ways it is. So it's astonishing that it can be used to solve such a wide variety of interesting problems. This week we will focus on these kinds of

problems. In practice, it is often quite easy to identify a problem as one requiring the use of the pigeon hole principle. But it is often challenging to determine what part of the problem should play the role of the pigeons and what should play the role of the holes. here we are going to learn few application of pegionhole principle like Monotone subsequences in Erdos-Szekers theorem. and ramsey number.

5.3 Pigeon-Hole Principle

We represent the basic principle of counting which is easily derived and extremely useful.

Statement:

If there n-pigeons to be placed in m-pigeonhole where $m \leq n$. Then there is at least one pigeonhole which receives more then one pigeon. Here is a simple consequence of the pigeonhole principle.

In one set 13 or more people there are at least two whose birthdays fall in the same month. In this case we have to think of putting the people in to pigeonhole. It can be January, February, March, and so no. Since there are 13 people and only 12 months (i.e. pigeonhole) one of the pigeonholes must contain at least two people.

Theorem 5.3.1 :

Suppose n pigeons are placed into k holes. If $n \delta k$ then some hole contains more than one pigeon.

Proof :

We prove the contra positive. Assume no hole contains more than one pigeon. Let $a_1, a_2, ..., a_k$ be the number of objects in each class. then $a_1 \leq 1, a_2 \leq 2, ..., a_k \leq 1$.

Thus, the total number of objects, $n = \sum_{i=1}^{k} a_i = a_1 + a_2 + ... a_k \leq 1 + 1 + ... + 1 = k$.

Hence nik our assumption is wrong some hole contains more than one pigeon.

Note : The pigeonhole principle is also called the Dirichlet drawer principle.

Example 1 :

If eight people are chosen in any way then show that atleast two of them are born on the same day of a week.

Solution:

Here each person (pigeon) is assigned the day of the week (pigeonhole) on which he and she was born since there are eight people and only seven days of the week, the pigeonhole principal tells us that atleast two people must be assigned to the same day.

Example 2 :

Consider the area shown it is bounded by a regular hexagon. Whose sides have length 1 units? Show that if any seven points are chosen with in this area then two of them must be on further apart then 1 unit.

Solution:

Suppose that the area is divided in to six equilateral triangles as shown in figure 1:1 If seven points are chosen we can assigned each one to a triangle that contains it. If the point belongs to several triangles, assigns it arbitrarily to one of them. The seven points one assigned to six triangles so by pigeonhole principal, at least two points must belong to same triangle. These two can not be more then 1 unit apart.

Example 3 :

Five points are located inside a square whose sides are of length 2 show that two of the points are within a distance of each other.

Solution:

Divide up the square into four square regions of area 1 unit. As indicated in figure 1.2. By pigeonhole principal, it follows that at least one of this regions will contain at least two points. The result now follows since two points in a square of radius 1. Can not be further apart then length of the diagonal of the square is which (by Pythagoras theorem).

Example 4 :

If any five numbers from 1 to 8 are chosen, then show that two of them will add to 9.

Solution:

Constructs four different sets each contains two numbers that 8 to 9, as follows A1 = 1, 8, A2 = 2, 7, A3 = 3, 6, A4 = 4, 5. Each of the five numbers chosen will

be assigned to the set that contains it. Since there are only four sets. The pigeonhole principal tells that two of the chosen numbers will be assigned to the same sets. These two numbers will add to 9.

Example 5 :

Fifteen children together 100 nuts. Prove that some pairs of children gathered the same number of nuts.

Solution:

Now to prove that we use method of contradiction. Suppose all the children gathered a different number of nuts. Then the fewest total number is 0 + 1 + 2 + 3 + 4 + 5 … + 14 = 105 but this is more then 100. Which is contradiction to our assumption.
There for at least pair of children gathered same number of nuts.

Example 6 :

Show that in any set of 10 integers there are at least pair of integers who have same remainder when divided by 9.

Solution:

Set of 10 integers , when it divided by 9,lie in the same residue classes of modulo 9.i.e. the remainder is 0,1,2,3,4,5,6,7,8. Here there will be 9 remainder and 10 integers. There fore by pigeonhole principal, at least one integer has same remainder.

Check Your Progress :

1. Show that for every integer n there is a multiple of n that has only 0s and 1s in its decimal expansion.
2. Show that if there are 30 students in a class, then at least two have last names that begin with the same letter.
3. Show that among any group of five integers, there are two with the same remainder when divided by 4.
4. Let T be an equilateral triangle whose sides has length 1 unit. Show that if any five points are chosen lying on insides T, then two of them will be more then$\frac{1}{2}$ unit apart.
5. Write the statement of pigeonhole principle and explain with one example.

6. There are n married couples. Out of the 2n people, how many have to be chosen so that we choose a married couple?

7. In any group of n people there are at least two persons having the same number friends.

5.3.1 The extended pigeonhole principle :

Theorem 5.3.2 :

If there are n pigeons assigned to m pigeonholes, then one of the pigeon-hole must contain at least $\left[\frac{n-1}{m}\right]+1$ pigeons.

Proof :

If each contain number more then $\frac{n-1}{m}$ pigeons, then there are at most $\frac{n-1}{m} \le m\frac{n-1}{m} = n-1$. A pigeon in all this contradicts our assumption. so one of the pigeonholes must contain at least $\left[\frac{n-1}{m}\right]+1$ pigeond.

Example 7 :

Show that if 30 dictionaries in a library contains a total of 61,327 pages, then one of the dictionaries must have at least 2045 pages.

Solution:

Let the pages be the pigeons and the dictionaries are te pigeonholes. Assigns each to the dictionaries in which it appears then by the extended pigeonhole principle are dictionaries must contain at least $\left[\frac{(n-1)}{m}\right]+1 = \frac{(61,327-1)}{30}+1 = 2045$ pages.

Example 8 :

Show that if any 29 people are selected then one may choose subset of 5. So that all 5 were born on the same day of the week.

Solution:

Assign each person to the day of week on which ha and she was born. Then n = 29 persons are being assigned to m = 7 pigeonholes. By the extended pigeonholes principle at least $\frac{n-1}{m}+1 = \frac{29-1}{7}+1 = 5$ persons.

Check Your Progress :

1. Show that if seven colours are used to paint 50 bicycles at least eight bicycles must have the same colours.
2. In any group of 1500 people, Show that there are at least 5 persons having the same birthday.
3. There are 50 baskets of apple, Each baskets contain no more than 24 apples. Show that there are at least 3 baskets containing the same number of apples.
4. 15 boys gathered 100 nuts. Prove that two of them gathered same number of nuts.
5. Show that there must be atleast 90 ways t choose six integers from 1 to 15 so that all the choices have the same sum.
6. How many friends must you have to guarantee atleast five of them will have birthdays in the same months?

5.4 Strong form of Pegionhole Principle

Theorem 5.4.1 :

Let $q_1, q_2, \ldots q_n$ be a positive integers. If $q_1 + q_2 \ldots + q_n - n + 1$ objects are put in to the n-boxes, then either 1st box contain at least q_1 objects, 2nd box contain at least q_2 objects, … , the nth box contain at least q_n objects.

Proof :

Suppose it is not true that is, the ith box contain at most $q_i - 1$ objects, $i = 1, 2, \ldots . n$ then the total number of objects contain in n boxes can be at most $(q_1 - 1) + (q_2 - 1) + \ldots + (q_n - 1) = q_1 + q_2 + \ldots + q_n - n$. Which is one less then the number of object distributed. This is a contradiction. The simple from of pigeonhole principle is obtained from the strong from by taking $q_1 = q_2 = \ldots = q_n = 2$. Then $q_1 + q_2 + q_3 + \ldots + q_n - n + 1 = 2n - n + 1 = n + 1$. In elementary mathematics the strong from of pigeonhole principle is most often applied in the special case when $q_1 = q_2 = \ldots = q_n = r$. In this case pigeonholes principle becomes : note :

- If n (r - 1) + 1 objects are put into n boxes, then at least one box contain r or more then r objects.

- If the averages of n non-negative integers, $a_1.a_2 \ldots a_n$ is greater then r - 1 objects, then at least one of integer is greater then or equal to r.

Theorem 5.4.2 :

Given n integers $a_1.a_2 \ldots a_n$ not necessarily distinct, there crist integers k and l with $0 \le k < l \le n$ such that the sum $a_{k+1} + a_{k+2} + \ldots + a_l$ is multiple of n.

Proof :

Consider the n integers $a_1, a_1 + a_2, a_1 + a_2 + a_3, \ldots a_1 + a_2 + \ldots + a_n$. Dividing these integers by n we get $a_1 + a_2 + \ldots + a_i = q_i n + r_i$ where $0 \le r_i \le n-1, i = 1,2,3, \ldots n$. If one of the remainder $r_1, r_2, \ldots r_n$ is zero, say $r_k = 0$ is multiple of n. If none of $r_1, r_2, \ldots r_n$ is zero, then two of them must have same say $r_k = r_t$ with $k < l$. This means $a_1 + a_2 + \ldots + a_k$ and $a_1 + a_2 + \ldots + a_t$ have the same remainder. Thus $a_{k+1} + a_{k+2} + \ldots + a_l$ is multiple of n.

Example 9

Show that among any n +1 numbers one can find two members so that their difference is divisible by n.

Solution:

Here, since there are only n possible remainder on divisible by n, and we have n +1 member, by pigeonhole principal some two of them have same remainder on division by n. Thus we can write this two as $n_1 = nk_1 + r$ and $n_2 = nk_2 + r$ where r is the remainder when division by n. $n_1 - n_2 = (nk_1 + r) - (nk_2 + r) = nk_1 + r - nk_2 - r = n(k_1 - k_2)$ which is divisible by n.

Theorem 5.4.3 :

Let m and n be relative prime positive integer. then the system this $x \equiv a \pmod m$ and $x \equiv b \pmod n$ has a solution.

Proof :

We may assume that $0 \le a < m$ and $0 \le b < n$. Let us consider the n integers $a, (m+a), (2m+a), a, (3m+a), \ldots .'(n-1)m + a$. Each of these integers has

remainder a when divide by m. Suppose that two of them has same remainder r when divide by n. Let the two number be im + a and jm + a where $0 \le i < j \le (n-1)$. Then there are integers q_j and q_j such that im + a = q_jn + r and jm + a = q_jn + r. Subtracting the first equation from the second, we get (j - i) m = (q_j - q_i)n. Since the gcd (m, n) = 1, we conclude that $n \mid (j-i)$. Npte that $0 \le i < j \le (n-1)$. This is a contradiction. Thus the n integers $a, (m+a), (2m+a), (3m+a), \ldots .'(n-1)\,m+a$ have distinct remainder when divide by n. That is each of the n numbers 0, 1, 2, 3, …, (n - 1) occur as a remainder. In particular, the number b does. Let p be the integer with $0 \le p \le (n-1)$ such that the number x = pm + a has remainder b when divide by n. Then for some integer q, x = qn + b. So x = pm + a = qn + b and x has the required property.

Example 10. :

51 points are placed in an arbitrary way, into a square of side 1. Prove that some 3 of these points can be covered by a circle of radius $\frac{1}{7}$.

Solution:

Divide the square into 25 smaller squares of the side $\frac{1}{5}$ then at least one of the small square would contain at least 3 points. Indeed, if this is not true then every small square contains 2 points or less; but the total number of points can not be more then 2 x 25 = 50. This contradicts to the assumption that we have 51 points. Now the circle circumvented around the square with the 3 points inside also contains these 3 points and has radius,

$$r = \sqrt{\left(\frac{1}{10}\right)^2 + \frac{1^2}{10}} = \sqrt{\frac{2}{100}} = \sqrt{\frac{1}{50}} < \sqrt{\frac{1}{49}} = \frac{1}{7}.$$

Check Your Progress :

1. Show that among any n + 1 positive integers not exceeding 2n there must be an integer that divides one of the other integers.

2. Prove that among any 52 integers, two can always be found such that the difference of their squares is divisible by 100.

3. Prove that, given any 12 natural numbers, we can choose two of them and such that their difference is divisible by 11.

4. 2001 flies are inside the cube of side 1. Prove that 3 of them are within the sphere of radius.

5. Show that among any 4 numbers one can find 2 numbers so that their difference is divisible by 3.

5.5 Erdos-Szekeres Theorem

Let assume we have m people standing in a line. We want to ask u of them to stand forward, such that, in the new line, if we look at them from left to right, their height is monotone increasing. Namely, every person is taller than the person to their left, and lower to the person to their right. Or alternatively, their heights are monotonically decreasing, namely, every person is shorter than the person to their left, and taller than to the person to their right. What is the largest u that we can nd such a subsequence?

Definition 1 :

Subsequence: A subsequence of a sequence of numbers $a_1, a_2, ..., a_m$ is a sequence formed by selecting some of the elements of the sequence in the same order as the original sequence. Formally, we have indices $1 \le i_1 < i_2 < ... < i_k \le m$, and the subsequence is $a_{i1}, a_{i2}, ... a_{ik}$.

Definition 2 :

Monotone sequence: A sequence of numbers a_1, a_2, a_3, is monotonically increasing if $a_i \le a_{i+1}$ for all i. Similarly, it is monotonically decreasing if $a_i \ge a_{i+1}$ for all i. A sequence which is either monotonically decreasing or monotonically increasing is called a monotone sequence.

Theorem 5.5.1 :

Every sequence $a_1, a_2, a_3, ... a_{n^2+1}$ of $n^2 + 1$ real numbers contains either an increasing subsequence of length n + 1 or a decreasing subsequence of length n + 1.

Proof :

If $b_1, b_2, ..., b_m$ is a sequence, then $b_{i1}, b_{i2}, ..., b_{ik}$ is a subsequence, provided that $1 \le i_1 < i_2 < ... < i_k < m$. Thus b_2, b_4, b_5, b_6 is a subsequence of $b_1, b_2, ..., b_8$ but

b_2, b_6, b_5 is not. The subsequence $b_{i1}, b_{i2}, ..., b_{ik}$ is increasing $b_{i1}, b_{i2}, ..., b_{ik}$ and decreasing if $b_{i1}, b_{i2}, ..., b_{ik}$. Using contradiction method, we assume that there is no increasing subsequence of length n + 1 and show that there must be a decreasing subsequence of length n + 1. For each $k = 1, 2 ...., n^2 + 1$, let m_k be the length of the longest increasing subsequence that being with a_k. Suppose $m_k \le n$ for each $k = 1, 2 ...., n^2 + 1$, let m_k, so that there is no increasing subsequence of length n + 1. Since $m_k \ge 1$ for each $k = 1, 2 ...., n^2 + 1$, let m_k, the numbers m_1, m_2, m_3, m_{n^2+1} are $n^2 + 1$ integers each between 1 and n. By the strong from of the pigeonhole principle n + 1 of the number $m_1, m_2, ... m_{n^2+1}$ are equal. Let $m_{k1} = m_{k2} = ... = m_{k_{n+1}}$, where $1 \le k_1 < k_2 < k_{n+1} \le n^2 + 1$. Suppose that for some $i = 1, 2, .. n, a_{ki} < ak_{i+1}$. Then, since $k_i < K_{i+1}$ we could take a longest increasing subsequence beginning with a_{ki+1}. Since this implies that $m_{ki} < mk_{i+1}$, we conclude that $a_{ki} > ak_{i+1}$. Since this is true for each $i = 1, 2, ..., n$, we have $a_{ki} \ge a_{i2} \ge ..... \ge a_{k_{n+1}}$, and we conclude that $a_{k1}, a_{k2}, ... \ge a_{k_{n+1}}$ is a decreasing subsequence of length n + 1.

Example 11 :

A Chess master who has 11 weeks to prepare for a tournament decides to play at least one game every day but, order not to tire himself, he decides not to play more than 12 games during any calendar weeks. Show that there exist a succession of consecutive days during which the chess master will have played exactly 21 games.

Solution :

Let a_1 be the number of games played on the first day, a_2 the total number of games played on the first and the second day, a_3 the total number of games played on first, second and the third day, and so on. Since at least one game is played in each day, the sequence of numbers $a_1, a_2, a_3, ... a_7 7$ is strictly increasing, that is $a_1 < a_2 < a_3 < ... < a_7 7$. Moreover $a_1 \ge 1$:and since at most 12 games are played during any one week there for $a_1 7 \ge 12 * 11 = 132$. Thus $1 \le a_1 < a_2 < ... < a_1 7 \le 132$. Note that sequence $a_1 + 21, a_2 + 21, ... a_7 7 + 21$ is also strictly increasing, and $1 + 21 \le a_1 + 21 < a_2 + 21 < .... < a_7 7 + 21$ each of these between 1 to 153. It follows that two of them must be equal. Since

$a_1, a_2, ... a_7 7$ are distinct and $a_1 + 21, a_2 + 21, ..., a_7 7 + 21$ are also distinct, then two equal member of must be from a_i and $a_j + 21$. Since the number of games played on i_th day is $a_i = a_j + 21$ we conclude that on the day j + 1, j + 2, ….i the chess master played total of 21 games.

5.6 Ramsey Number

Definition 3 :

The Ramsey number R(m, n) gives the solution to party problem, which asks the minimum number of guests R(m, n) that must be invited so that at least m will know each other or at least n will not know each other.

By symmetry, it is true that R(m, n) = R(n, m). It also must be true that R(m, 2) = m. A generalized Ramsey number is written $R(m_1, m_2, m_3, ..., m_k; n)$ and is the smallest integer r such that, no matter how each n-element subset of an r-element set is colored with k colors, there exists an i such that there is a subset of sizein, all of whose n-element subsets arei color. The usual Ramsey numbers are then equivalent to R(m, n) = R(m, n; 2).

5.6.1 Ramsey party problem :

Given K there is n so large that is any party of at least n people there is either a set of K mutual friends or K mutual enemies. Of course we cannot know which option will pertain since for some parties all might be friends or other might be enemies. The statement above rather unwieldy, so we shall introduce some notation in our discussion we will write $n \to (k_1, k_2)$. If n has the property that it is so large that in any party of n people there are either k_1 mutual friends or k_2 mutual enemies.

Example 12 :

Assume that in a group of 6 people, each pair of individuals consists of two friends or two enemies. Show that there are either 3 mutual friends or 3 mutual enemies in the group.

Solution :

Let a be a any person. By the pigionhole principle, of the remaining 5 persons, either 3 or more are friends of a or 3 or more are enemies of a. When 5 object are divided into two sets, therefore by generalization of pegionhole principle, one of

the set containedat least $\left(\frac{5}{2}=3\right)$ elements. Suppose first that b, c and d are friends of a. If any 2 of these persons are friends, these 2 and a from a group of 3 mutual friends. If none of b, c and d are friends, then b, c and d from a group of mutual enemies. The argument is similar if we suppose that b, c and d are enemies odf a.

5.7 Summary

Pegionhole principle: n pigeons are placed into k holes. If $n \delta k$ then some hole contains more than one pigeon.

The extended pigeonhole principle: If there are n pigeons assigned to m pigeonholes, then one of the pigeonhole must contain at least $\left[\frac{n-1}{m}\right]+1$ pigeons.

Strong from of pegionhole principle: Let q_1, q_2, ...q_n be a positive integers. If q_1 + q_2.... + q_n - n + 1 objects are put in to the n-boxes, then either 1st box contain at least q_1 objects, 2nd box contain at least q_2 objects, …., the nth box contain at least q_n objects.

Erdos-Szekeres theorem and its application.

Ramsey number and its application in pegionhole principle.

5.8 Chapter End Exercise

1. 7.Given 8 different natural numbers, none greater than 15, show that at least three pairs of them have the same positive difference.
2. Show that every sequence of n^2 + 1 distinct real numbers contains a subsequence of length n + 1 that is either strictly increasing or decreasing.
3. During a month with 30 days a baseball team plays at least one game a day, but no more than 45 games. Show that there must be a period of some number of consecutive days during which the team must play exactly 14 games.
4. Show that among any n +1 positive integers not exactly 2n there must be an integers that divides one of the other integer.
5. Show hat given any set of 5 numbers, there are 3 numbers in the set whose sum is divisible by 3.

6. Prove that of any 10 point chosen within an equilateral triangle of side length 1, there are two points whose distance apart is at most $\frac{1}{3}$.

7. Show that in a group of 10 people there are either a set of 3 mutual strangers or a set of 4 mutual friends.

8. Prove that any 11 integers selected from the set 1, 2, …. , 100 there are at least 2 integers say x and y that $0 < \left|\sqrt{x} - \sqrt{y}\right| < 1$.

9. Fifty-one points are scattered inside a square with a side of 1 meter. Prove that some set of three of these points can be covered by a square with side length equal to 20 centimeters.

10. Prove that among 52 natural numbers, one can find two numbers m and n such that either the sum m + n or difference m n is divisible by 100.

11. The digits 1, 2, …., 9 are divided in three groups. Prove that product of the numbers in one of the groups must exceed 71.

12. Show that in a party there are always two persons who have shaken hands with the same number of persons.

13. Show that if 6 points are placed in the plane and they are joined with blue or green segments, then at least two monochromatic triangles are formed with vertices in the 6 points.

14. A class of 32 students is organized in 33 teams. Every team consists of three students and there are no identical teams. Show that there are two teams with exactly one common student.

15. Give any sequence of mn + 1 distinct real numbers then prove that there exist either an increasing sequence of length m + 1 or decreasing sequence of length n + 1 or both.

16. Give any six integers in 1, 2,...., 10 prove that there exist atleast two that adds upto 11.

17. If (n + 1) numbers are picked from $a+1, \ldots a+2n \; n \in \square, a \in F$ then prove that there are two numbers which are co-prime.

18. There are 280 students in the class. Without knowing anybody's birthday, what is the largest value of n for which we can prove that at least n students must have been born in the same month?

19. From the integers 1, 2, 200, we choose 101 integers. Show that among the integers chosen there are two such that one of them is divisible by the other.

20. Basket of fruit is being arranged out of apples, bananas, and oranges. What is the smallest number of pieces of fruits that should be put in the basket in order to guarantee that either there are at least 8 apples or at least 6 bananas or at least 9 oranges?

5.9 References

V. Krishnamurthy: Combinatorics Theory and application, Affiliated East-West Press. Richard A. Brualdi: Introductory Combinatorics, John Wiley and son.

A. Tucker: Applied Combinatorics, Oxford University press.

Kenneth Rosen : Discrete Mathematics and its application, Tata McGraw Hills.

Unit 3

6

GENERATING FUNCTION

Unit Structure:

6.1 Objectives

After going through this chapter students will be able to understand:

- Ordinary generating Functions algebraic manipulations with power series
- Exponential Generating Functions algebraic manipulations with power series
- Generating functions for counting combinations with and without repetitions.
- Applications to counting, use of generating functions for solving homogeneous and non-homogeneous recurrence relations.

6.2 Introduction

The concept of a generating function is one of the most useful and basic concepts in the theory of combinatorial enumeration. The power of the generating function rests upon its ability not only to solve the kinds of problem we have considered so

far but also to aid us in new situations where additional restrictions may be involved.

Now we see some important polynomial expansions, which are often used in this chapter. **Polynomial Identities:**

i) $\frac{1-x^{n+1}}{1-x} = 1 + x + x^2 + x^3 + \cdots \ldots \ldots + x^n$

ii) $\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots \ldots \ldots$

iii) $(1 + +x)^n = 1 + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots \ldots \ldots + \binom{n}{n}x^n$

iv) $(1 - x^m)^n = 1 - \binom{n}{1}x^m + \binom{n}{2}x^{2m} - \cdots \ldots \ldots + (-1)^n\binom{n}{n}x^{nm}$

v) $\frac{1}{(1-x)^n} = 1 + \binom{1+n-1}{1}x + \binom{2+n-1}{2}x^2 +$
$\cdots \ldots \ldots \ldots + \binom{r+n-1}{r}x^r + \cdots$

vi) If $h(x) = f(x)g(x)$ where $f(x) = a_0 + a_1x + a_2x^2 + \cdots \ldots$ and $g(x) = b_0 + b_1x + b_2x^2 + \cdots \ldots$ then

$h(x) = a_0b_0 + (a_1b_0 + a_0b_1)x + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + \cdots \ldots \ldots +$
$(a_rb_0 + a_{r-1}b_1 + \ldots \ldots + a_0b_r)x^r + \cdots$.

6.3 Generating function

Let $a_0, a_1, a_2, \ldots \ldots \ldots$ be a sequence of real numbers. The function

$g(x) = a_0 + a_1x + a_2x^2 + \cdots \ldots \ldots = \sum_{i=0}^{\infty} a_ix^i$

is called the ordinary generating function or generating function for the given sequence.

Example 1: Generating function for the binomial theorem.

Solution: For any $n \in Z^+$,

$$(1 + x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots \ldots + \binom{n}{n}x^n,$$

So $(1 + x)^n$ is the generating function for the sequence

$$\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \ldots \ldots \ldots, \binom{n}{n}, 0,0,0, \ldots$$

$f(x) = (1 + x)^n$ is the generating function for $a_r = C(n, r)$, the number of ways to select an *r*-subset from an *n*-set.

Example 2: Generating function for Maclaurian series.

Solution: For any $n \in Z^+$, the Maclaurin series expansion for $(1+x)^{-n}$ is given by

$$(1+x)^{-n} = 1 + (-n)x + (-n)(-n-1)\frac{x^2}{2!} + \cdots \ldots ..$$

$$= 1 + \sum_{r=1}^{\infty} \frac{-n(-n-1)(-n-2)\ldots.(-n-r+1)}{r!}\, x^r$$

$$= \sum_{r=0}^{\infty} (-1)^n \binom{n+r-1}{r} x^r$$

Hence $(1+x)^{-n} = \binom{-n}{0} + \binom{-n}{1}x + \binom{-n}{2}x^2 + \cdots \ldots . = \sum_{r=0}^{\infty}\binom{-n}{r}x^r$.

This generalizes the binomial theorem and shaws that $(1+x)^{-n}$ is the generating function for the sequence $\binom{-n}{0}, \binom{-n}{1}, \binom{-n}{2}, \ldots \ldots$

Example 3: Generating function for a sequence.

Solution: For any $n \in Z^+$, $(1-x^{n+1}) = (1-x)(1+x+x^2+\cdots \ldots \ldots + x^n)$.

So $\frac{(1-x^{n+1})}{(1-x)} = (1+x+x^2+\cdots \ldots \ldots + x^n)$, and $\frac{(1-x^{n+1})}{(1-x)}$ is the generating function for the sequence 1,1,1,…….,0,0,0……, where the first *n+1* terms are 1.

Extending the above example we find that $1 = (1-x)(1+x+x^2+\cdots \ldots \ldots + x^n)$,

So $\frac{1}{(1-x)}$, is the generating function for the sequence 1,1,1,…..

Note: $\frac{1}{(1-x)} = 1+x+x^2+\cdots \ldots \ldots$ is valid for all real *x* where $|x| < 1$; it is for this range of values that the geometric series $1+x+x^2+\cdots \ldots \ldots$ converges. However convergence is not the main idea of this concept.

Consider the formal expansion of $(1+x)^3 = (1+x)(1+x)(1+x)$

$$= 111 + 11x + 1x1 + 1xx + x11 + x1x + xx1 + xxx$$

This formal expansion lists all ways of multiplying a term in the first factor times a term in the second factor times a term in the third factor.

The problem of determining the coefficient of x^r in $(1+x)^3$, and more generally in $(1+x)^n$, reduce to the problem of counting the number of different formal products with exactly r x's and $(n-r)$ 1's. So the coefficient of x^r in $(1+x)^3$ is $C(3,r)$, and in $(1+x)^n$ is $C(n,r)$.

The following examples illustrate the use and efficiency of generating functions to solve combinatorial problems.

Example 4: Determine the number of ways to select 4-letter combination from the set { A,B,C} if A can be included at most once, B at most twice, and C at most three times.

Solution: The list of all possible combinations is:

{C.B,B,A}, {C,C,B,B}, {C,C,B,A}, {C,C,C,A}, {C,C,C,A}

This situation can be modeled with a generating function by expressing each letter's possibilities with a polynomial.

(1+A) represents A occurring 0 times or 1 time. $(1+B+B^2)$ represents B occurring 0,1, or 2 times. $(1+C+C^2+C^3)$ represents C occurring 0, 1, 2, or 3 times.

Then the expansion $(1+A)\,(1+B+B^2)\,(1+C+C^2+C^3)$ will list all the ways to create

K-element sets with A or B or C with the constraints of the problem.

Since the problem does not require all the possibilities, we use the generating function $(1+x)\,(1+x+x^2)\,(1+x+x^2+x^3)$ to find the number of ways to select a 4-letter combination. Expanding the above product, we get $1+3x+5x^2+6x^3+5x^4+3x^5+x^6$. The coefficient of the term x^4, 5 represents the number of ways to select 4- element set under the given condition of the problem.

Example 5: Using a generating function modal the problem of counting all selections of six objects chosen from three types of objects with repetition of upto four objects of each type.

Solution: This problem can be modeled as the number of integer solution to

$$e_1 + e_2 + e_3 = 6, \quad 0 \le e_i \le 4.$$

This problem does not ask for the general solution of the ways to select r objects.

This problem requires the coefficient of x^6, that is the ways of $x^{e_1}x^{e_2}x^{e_3}$ can equal x^6.

Thus the desired generating function is $(1 + x + x^2 + x^3 + x^4)^3$ and the coefficient of x^6 in the expansion gives the required result.

Example 6: In how many ways 25 identical pens can be distributed among four children.

Solution: We can model the above problem as the number of integer solutions for the equation $c_1 + c_2 + c_3 + c_4 = 25$ if $0 \leq c_i$ for all $1 \leq i \leq 4$?

For each child the possibilities can be described by the polynomial $1 + x + x^2 + \cdots \ldots . . + x^{25}$. Then the answer to this problem is the coefficient of x^{25} in the generating function

$$f(x) = (1 + x + x^2 + \cdots . + x^{25})^4.$$

The answer can also be obtained as the coefficient of x^{25} in the generating function

$$f(x) = (1 + x + x^2 + \cdots . + x^{25} + x^{26} + \cdots . .)^4$$

Note that if the distribution is to only one child then the generating function is

$f(x) = 1 + x + x^2 + \cdots . + x^{25}$.

Example 7: At a small shop, pencils sell for Rs. 2 and pen for Rs. 3. For *r* rupees, how many different ways can pens and pencils be ordered?

Solution: For 8 rupees, we note that there are two orders that can be placed:

i) One pencil and two pens or
ii) Four pencil and no pen

A generating function that provides a solution is

$$(1 + x^2 + x^4 + x^6 + \cdots \ldots . .)(1 + x^3 + x^6 + x^9 + \cdots \ldots \ldots .)$$

Whose expansion is

$1 + x^2 + x^3 + x^4 + x^5 + 2x^6 + 2x^7 + 2x^8 + 2x^9 + 2x^{10} + 2x^{11} + 3x^{12} + 2x^{13} + 3x^{14} + 3x^{15} + \cdots \ldots \ldots ..$

The coefficient of x^r in the above expansion gives the number of orders for *r* rupees.

6.3.1Calculating coefficients of generating functions:

When determining the sequence generated by a generating function, you will want to get a formula for the n^{th} term (that is, for the coefficient of x^n), rather than just computing numerical values for the first few coefficients.

$$(1+x)^{-1} = 1 + x + x^2 + x^3 + \cdots \ldots \ldots \ldots$$

The second fact above says that $\frac{1}{1-x}$ is the generating function for the sequence 1, 1, 1, 1,.... It also lets you determine the sequence generated by many other functions.

Theorem : The coefficient of x^r in the power series $\frac{1}{(1+x)^n}$ is $(-1)^r \binom{n+r-1}{r}$.

Proof: Given power series $\frac{1}{(1+x)^n}$ can be written as $(1+x)^{-n}$. To avoid the minus signs we shall consider $(1-x)^{-n}$.

$$(1+x)^{-1} = 1 + x + x^2 + x^3 + \cdots \ldots \ldots \ldots$$

It follows that $(1+x)^{-n}$ is the product of *n* factors,

$(1+x)^{-n} = (1 + x + x^2 + + \cdots)(1 + x + x^2 + x^3 + \cdots) \ldots (1 + x + x^2 + x^3 + \cdots .)$ n times.

Now we have to show that the coefficient of x^r in the product of these *n* factors is equal to the number of un-order selections of *r* of *n* factors, with repetition allowed.

Suppose that each factor has a Marker, initially positioned at the term 1, and that we make an un-order selection, with repetition, of size *r* from the *n* factors.

Each time a particular factor is selected we move its marker to the next term, So that if that factor is selected *i* times in all the marker will finish up at x^i.

Thus for each one of the $\binom{n+r-1}{r}$ possible selections we obtain a set of marked terms, one from each factor, with total exponent *n*.

So the coefficient of x^r is $\binom{n+r-1}{r}$.

Replacing *x* by –*x* we get,

The coefficient of x^r in the power series $\frac{1}{(1+x)^n}$ is $(-1)^r \binom{n+r-1}{r}$.

Example 8: Find the coefficient of x^5 in $(1-2x)^{-7}$.

Solution: Using generating function for Maclaurin series, we write

$(1-2x)^{-7} = (1+y)^{-7} = \sum_{r=0}^{\infty}\binom{-7}{r}(-2x)^r$ where $y = -2x$.

Consequently, the coefficient of x^5 is

$$\binom{-7}{5}(-2x)^5 = (-1)^5\binom{7+5-1}{5}(-32) = 32\binom{11}{5} = 14{,}784.$$

Example 9: Find the coefficient of x^{16} in $(x^2+x^3+x^4+\cdots.)^5$.Also find the general coefficient . i.e. the coefficient of x^r.

Solution: To simplify the expression, we extract x^2 from each polynomial factor and then apply the polynomial identity.

$$(x^2+x^3+x^4+\cdots.)^5 = [x^2(1+x+x^2+\cdots..)]^5$$

$$= [x^{10}(1+x+x^2+\cdots..)^5] = x^{10}\frac{1}{(1-x)^5}$$

Thus the coefficient of x^{16} in $(x^2+x^3+x^4+\cdots.)^5$ is the coefficient of x^{16} in $x^{10}(1-x)^{-5}$.

But the coefficient of x^{16} in this letter expression will be the coefficient of x^6 in $(1-x)^{-5}$. i.e. the x^6 term in $(1-x)^{-5}$ is multiply by x^{10} to become the x^{16} term in $x^{10}(1-x)^{-5}$.

From the polynomial identity

$$\frac{1}{(1-x)^n} = 1+\binom{1+n-1}{1}x+\binom{2+n-1}{2}x^2+$$
$$\cdots\ldots\ldots..+\binom{r+n-1}{r}x^r+\cdots$$

We see that the coefficient of x^6 in $(1-x)^{-5} = \binom{6+5-1}{6} = 210$.

More generally, the coefficient of x^r in $x^{10}(1-x)^{-5}$ equals the coefficient of x^{r-10} in $(1-x)^{-5}$ is $\binom{(r-10)+5-1}{r-10}$.

Proposition: In how many ways can we select, with repetition allowed, *r* objects from *n* distinct objects?

Proof: To prove this we need the following identity.

$$\frac{1}{(1-x)^n} = 1 + \binom{1+n-1}{1}x + \binom{2+n-1}{2}x^2 + \cdots \ldots \ldots + \binom{r+n-1}{r}x^r + \cdots$$

$$= \sum_{r=0}^{\infty} \binom{n+r-1}{r} x^r$$

Now coming to our main result, the possible choices for the object to choose namely, none, one, two, …..($r = 0,1,2,3, \ldots$) are nothing but the coefficients of powers of corresponding x's in the geometric series $1 + x + x^2 + \cdots$ ... for each of *n* distinct objects.

Considering all of the n distinct objects, the generating function is

$$g(x) = (1 + x + x^2 + \cdots)^n,$$

And the required answer is the coefficient of x^r in $f(x)$. Now using the above identity we have

$$(1 + x + x^2 + \cdots)^n = \left(\frac{1}{(1-x)}\right)^n = \frac{1}{(1-x)^n} = \sum_{r=0}^{\infty} \binom{n+r-1}{r} x^r$$

Therefore the coefficient of x^r is $\binom{n+r-1}{r}$.

Example 10: How many ways are there to distribute 25 identical balls into Seven distinct boxes if the first box can have no more than 10 balls but any number can go into each of the other Six boxes?

Solution: The generating function for the number of ways to distribute r balls into seven boxes with at most 10 balls in first box is

$$h(x) = (1 + x + x^2 + \cdots + x^{10})(1 + x + x^2 + \cdots)^6$$
$$= (1 - x^{11})(1 - x)^{-7}$$

By the identity (1) and (2)

Let $f(x) = (1 - x^{11})$ and $g(x) = (1 - x)^{-7}$

Using identity (5) , we have

$$g(x) = (1 - x)^{-7}$$
$$= 1 + \binom{1+7-1}{1}x + \binom{2+7-1}{2}x^2 + \cdots \ldots + \binom{r+7-1}{r}x^r + \cdots$$

We need the coefficient of x^{25} (25 ball distributed) in $h(x) = f(x)g(x)$. We need to consider only the terms in the product of the two polynomials $(1 - x^{11})$ and $(1 - x)^{-7}$ that yields an x^{25} term. The only nonzero coefficients in $f(x) = (1 - x^{11})$ are $a_1 = 1$ and $a_{11} = -1$. So the coefficient of x^{25} in $f(x)g(x)$ is

$$a_0 b_{25} + a_{11} b_{14} = 1 \times \binom{25 + 7 - 1}{25} + (-1)\binom{14 + 7 - 1}{14} = 6{,}97{,}521$$

Example 11: Find the number of ways to collect 15 rupees from 20 distinct people if each of the 19 people can give a rupee (or nothing) and the twentieth person can give a 1-rupee or 5-rupees (or nothing).

Solution: This collection problem is equivalent to finding the number of integer solutions to

$$x_1 + x_2 + \cdots \ldots + x_{20} = 20$$

Where each x_i represents the i^{th} person,

When x_i= 0 or 1, and the corresponding polynomial expression is

$$(1 + x)^{19}$$

$i = 1,2, \ldots \ldots 19$ and $x_{20} = 0, 1 \; or \; 5$ and the corresponding polynomial is

$$1 + x + x^5.$$

The answer is the coefficient of x^{15} in the generating function of the product of $(1 + x)^{19}$ and $(1 + x + x^5)$,

$h(x) = (1 + x)^{19}(1 + x + x^5)$.

Now we find the required answer as follows.

Let
$f(x) = (1 + x)^{19}$ and $g(x) = (1 + x + x^5)$.

Let a_r and b_r be the coefficient of x^r in $f(x)$ and $g(x)$ respectively, then we know that

$a_r = \binom{19}{r}$ and $b_0 = b_1 = b_5 = 1$ and other b_i's are zero.

Now the coefficient of x^{15} in $h(x)$ is

$$a_{15} b_0 + a_{14} b_1 + a_{13} b_2 + \cdots \ldots . . + a_0 b_{15}$$

Which reduce to $a_{15}b_0 + a_{14}b_1 + a_{10}b_5$.

Substituting the values of $a_i's$ and $b_i's$ we get

$$a_{15}b_0 + a_{14}b_1 + a_{10}b_5 = \binom{19}{15} \times 1 + \binom{19}{14} \times 1 + \binom{19}{10} \times 1$$

$$= \binom{19}{15} + \binom{19}{14} + \binom{19}{10}$$

Example 12: Using generating functions to show that $\sum_{r=0}^{n} C(n,r)^2 = C(2n,n)$ whenever *n* is a positive integer.

Solution: First note that by the Binomial Theorem $C(2n,n)$ is the coefficient of x^n in $(1+x)^{2n}$.

However we also have

$$(1+x)^{2n} = [(1+x)^n]^2$$

$$= [C(n,0) + C(n,1)x + C(n,2)x^2 + \cdots \ldots + C(n,n)x^n]^2$$

The coefficient of x^n in this expression is

$$C(n,0)C(n,n) + C(n,1)C(n,n-1) + C(n,2)C(n,n-2) + \cdots \ldots + C(n,n)C(n,0)$$

$= \sum_{r=0}^{n} C(n,r)^2 \quad \because C(n,n-r) = C(n,r).$

Here both $C(2n,n)$ and $\sum_{r=0}^{n} C(n,r)^2$ represent the coefficient of x^n in $(1+x)^{2n}$.

Therefore $\sum_{r=0}^{n} C(n,r)^2 = C(2n,n)$.

6.4 Exponential Generating Function

The Exponential generating function arise in selection problems where order was not important i.e combination.

However, turning to the problems of arrangement (Permutations), where order is important , we seek a comparable tool, namely the " Exponential Generating Function".

Definition: For a sequence $a_0, a_1, \ldots$ Of real numbers,

$$g(x) = a_0 + a_1 x + a_2 \frac{x^2}{2!} + a_2 \frac{x^3}{3!} + \cdots \ldots = \sum_{r=0}^{\infty} a_r \frac{x^r}{r!}$$

is called the exponential generating function for the given sequence. Note that $a_i's$ may be constants or functions of reals.

For example; In the Maclaurin's series expansion of e^x, we find

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots \ldots = \sum_{r=0}^{\infty} \frac{x^r}{r!}.$$

Therefore e^x is the ordinary generating function for the sequence $1, 1, {}^1/_{2!}, {}^1/_{3!}$,….and is the exponential generating function for sequence 1, 1, 1, …..

Proposition: The expansion of $(1 + x)^n$ is an exponential generating function for the sequence $P(n, r)$, where $0 \leq r \leq n$.

Solution: We know that,

$\binom{n}{r} = C(n, r)$ is the number of combinations of *n* objects taken *r* at a time, and $P(n, r)$ is the number of permutations of *n* objects taken *r* at a time with $0 \leq r \leq n$.

Consequently, $(1 + x)^n$ generates the sequence $C(n, 0), C(n, 1), \ldots \ldots, C(n, n), 0, 0, 0 \ldots$

Now by Making use of the relation between $C(n, r)$ and $P(n, r)$ we write

$$(1 + x)^n = C(n, 0) + C(n, 1)x + C(n, 2)x^2 + \cdots \ldots + C(n, n)x^n$$

$$= P(n, 0) + P(n, 1)\frac{x}{1!} + P(n, 2)\frac{x^2}{2!} + \cdots + P(n, n)\frac{x^n}{n!}.$$

Where $C(n, r) = \frac{P(n,r)}{r!}$.

Hence $(1 + x)^n$ generates the sequence $P(n, 0), P(n, 1), \ldots \ldots, P(n, n)$ as the coefficient of $\frac{x^r}{r!}$.

Therefore the expansion of $(1 + x)^n$ is an exponential generating function for the sequence $P(n, r)$, where $0 \leq r \leq n$.

Example 13: A company hires 11 new employees, each of whom is to be assigned one of four subdivisions. Each subdivision will get atleast one new employee. In how many ways can these assignments be made?

Solution: Assuming the subdivisions A, B, C and D, we can equivalently count the number of 11 letter sequences in which there is atleast one occurrence of each of the letters A, B, C and D. The exponential generating function for these arrangements is

$$f(x) = \left(x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots.\right)^4 = (e^x - 1)^4$$

$$= e^{4x} - 4e^{3x} + 6e^{2x} - 4e^x + 1$$

Now the required answer is the coefficient of $\frac{x^{11}}{11!}$ in $f(x)$.

$$4^{11} - 4(3^{11}) + 6(2^{11}) - 4(1^{11}) = \sum_{r=0}^{4} (-1)^r \binom{4}{r} (4-r)^{11}.$$

Example 14: A ship carries 48 flags, 12 each of the colors red, white, blue and green. 12 of these flags are placed on a vertical pole in order to communicate a signal to other ships. How many of these signals use an even number of blue flags and an odd number of green flags?

Solution: The exponential generating function for this problem is

$$f(x) = \left(1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots\right)\left(1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \cdots\right)\left(x + \frac{x^3}{3!} + \frac{x^5}{5!} + \cdots\right)$$

Consider all such signals made up of n flags, where $n \geq 1$. The last two factors in $f(x)$ restrict the signals to an even number of blue and an odd number of green flags, respectively.

Since $f(x) = (e^x)^2 \left(\frac{e^x + e^{-x}}{2}\right)\left(\frac{e^x - e^{-x}}{2}\right)$

$$= \frac{1}{4}(e^{2x})(e^{2x} - e^{-2x}) = \frac{1}{4}(e^{4x} - 1)$$

$$= \frac{1}{4}\left(\sum_{r=0}^{\infty} \frac{(4x)^r}{r!} - 1\right) = \frac{1}{4}\sum_{r=0}^{\infty} \frac{(4x)^r}{r!}$$

The coefficient of $\frac{x^{12}}{12!}$ in the expansion of $f(x)$ yield $\frac{1}{4}4^{12} = 4^{11}$ signals made up of 12 flags with an even number of blue flags and an odd number of green flags.

6.5 Use of generating functions for Solving homogeneous and Non-homogeneous recurrence relations:

Now we demonstrate the procedure to solve a given recurrence relation with the help of generating functions in the following example in a systematic procedure.

Example15: Solve the recurrence relation

$$a_{n+2} - 5a_{n+1} + 6a_n = 2,\ n \geq 0.$$
$$a_0 = 3, a_1 = 7$$

Solution:

Step 1

Multiply the given relation by x^{n+2}, because $n + 2$ is largest subscript in the relation. This gives us

Step 2

Sum all the equations represented by the result in step (1) and we get

$$\sum_{n=0}^{\infty} a_{n+2} x^{n+2} - 5\sum_{n=0}^{\infty} a_{n+1} x^{n+2} + 6\sum_{n=0}^{\infty} a_n x^{n+2} = 2\sum_{n=0}^{\infty} x^{n+2}.$$

Step 3

In order to have each of the subscripts on a match the corresponding exponent on x, we rewrite the equation in step (2) as

$$\sum_{n=0}^{\infty} a_{n+2} x^{n+2} - 5x\sum_{n=0}^{\infty} a_{n+1} x^{n+2} + 6x^2\sum_{n=0}^{\infty} a_n x^{n+2} = 2x^2\sum_{n=0}^{\infty} x^{n+2}.$$

Step 4

Let $f(x) = \sum_{n=0}^{\infty} a_n x^n$ be the generating function for the solution. The equation in step (3) now takes the form

$$(f(x) - a_0 - a_1 x) - 5(f(x) - a\delta) + 6x^2 f(x) = \frac{2x2}{1-x}$$

Or

$$(f(x) - 3 - 7x) - 5(f(x) - 3) + 6x^2 f(x) = \frac{2x2}{1-x}$$

Step 5

Solving for $f(x)$ we have

$$(1 - 5x + 6x^2) f(x) = 3 - 8x + \frac{2x2}{1-x}$$

$$= \frac{3-11x+10x2}{1-x},$$

Form which it follows that

$$f(x) = \frac{3-11x+10x2}{(1-5x+6x2)(1-x)}$$

$$= \frac{(3-5x)(1-2x)}{(1-3x)(1-2x)(1-x)}$$

$$= \frac{3-5x}{(1-3x)(1-x)}$$

Partial fraction decomposition gives us

$$f(x) = \frac{2}{1-3x} + \frac{1}{1-x}$$

$$= 2\sum_{n=0}^{\infty}(3x)^n + \sum_{n=0}^{\infty}(x)^n$$

Consequently, $a_n = 2(3^n) + 1$, $n \geq 0$,

6.6 Let us sum up

In this chapter we have learnt the following:

- For the sequence of real numbers, $a_0, a_1, a_2, \ldots \ldots \ldots$ the function

  $$g(x) = a_0 + a_1x + a_2x^2 + \cdots \ldots \ldots = \sum_{i=0}^{\infty} a_i x^i$$

  is called the ordinary generating function or generating function for the given sequence.

- For a sequence $a_0, a_1, \ldots$ Of real numbers,

  $$g(x) = a_0 + a_1x + a_2\frac{x^2}{2!} + a_2\frac{x^3}{3!} + \cdots \ldots \ldots = \sum_{r=0}^{\infty} a_r \frac{x^r}{r!}$$

  is called the exponential generating function for the given sequence.

- Finding the coefficient of x^r in the expansion of a polynomial.
- Solving various recurrence relations and the method of generating functions.

6.7 Unit end Exercise

1. What is the generating function for the sequence 1,1,1,1,1?
2. Find the generating function for $(1+x)^{-n}$ and $(1-x)^{-n}$ when n is a positive integer. Using the extended Binomial theorem.
3. In how many different ways can 8 balls be distributed among three distinct boys. If each boy receives atleast two balls and no more than four balls?
4. Using the generating functions to find the number of *r*-combinations of a set with *n*- elements.
5. Use generating function to find the number of ways to select r-objects of n different kinds, if we must select atleast one object of each kind.
6. Determine the generating function for the number of ways to distribute a large number of identical balls to four children so that the first two children receive an odd number of balls, the third child receives at least three balls, and the fourth child receives at most two balls.
7. Determine the generating function for the number of n-combinations of apples, bananas, oranges, and pears where in each n-combination the number of apples is even, the number of bananas is odd, the number of oranges is between 0 and 4, and the number of pears is at least two.
8. Let a_n denote the number of nonnegative integral solutions of the equation $2x_1 + 3x_2 + 4x_3 + 5x_4 = n$ .Find the generating function.
9. Determine the number a_n of *n* digit (under base 10) numbers with each digit odd where the digit 1 and 3 occur an even number of times.
10. What is the number of distinct *r*-letter words based on *n*-letter alphabet (repetition allowed, order matters)
11. Determine the number of ways to colors the square of a 1 by-n chess board using colors red, white and blue. If an even number of squares are to be colored red.
12. Determine generating function for the sequence of squares 0,1,4,…..,n^2.
13. Solve the recurrence relation using generating function

    $a_n = 5a_{n-1} - 6a_{n-2}\,, \quad n \geq 2, \quad a_0 = 1, a_1 = -1.$

14. Find an exponential generating function for the number of permutations with repetition of length n of the set {a,b,c}, in which there are an odd number of a's, an even number of b's, and any number of c's.

15. In how many ways can we paint the 10 rooms of a hotel if at most three can be painted red, at most 2 painted green, at most 1 painted white, and any number can be painted blue or orange? (The rooms are different, so order matters.)

6.8 References

1. Applied Combinatorics, Alan Tucker.

2. Combinotorial Techniques, Sharad S. Sane

3. Discrete mathematics its Application, Keneth H. Rosen TMG.

4. Discrete mathematics, Norman L. Biggs.

5. Discrete structures by B. Kolman HC Busby, S Ross PHI Pvt. Ltd.

6. Discrete mathematics, Schaum's outlines series, Seymour Lip Schutz, Marc Lipson, TMG.

Unit 4

7

POLYA'S THEORY OF COUNTING

Unit Structure:

7.1 Objective

After going through this chapter students will be able to understand:

- Equivalence relations and orbits under a permutation group action.
- Orbit Stabiliser theorem.
- Polya theorem.
- Burnside theorem and its application.
- Cycle index of a permutation.
- Polya's formula and its application in counting theory.

7.2 Introduction

The section needs a good understanding of some basic facts from group theory, particularly those connected with permutation groups. The Polya Theory in its enumerative applications to permutations groups. The discussion includes the notion of the power group, the Burnside's Lemma along with the notions on groups, stabilizer, orbits and other group theoretic terminologies which are so fundamentally used for a good introduction to the Polya Theory. These in turn, involve the introductory concepts on weights, patterns, figure and configuration

counting series along with the extensive discussion of the cycle indexes associated with the permutation group at hand. Shows that the special figure series $c(x) = 1 + x$ is useful to enumerate the number of G-orbits of r -subsets of any arbitrary set X. Further more, the paper also shows that this special figure series simplifies the counting of the number of orbits determined by any permutation group which consequently determines whether or not the said permutation group is transitive. Here we shall be studying a financial theorem of conservative combinations called Polya's theorem.

7.3 Equivalence relations and orbits under a permutation group action

Let X be a set, which may be finite or infinite (but will usually be finite). We denote by $Sym(X)$ the symmetric group on X, the group whose elements are all the permutations of X (the bijective maps from X to itself), with the operation of composition. If X is finite, say $|X| = n$, we often write $Sym(X)$as S_n.

We compose permutations from left to right, so that $g_1 g_2$ means "apply first g_1 , then g_2". This goes naturally with writing a permutation on the right of its argument: $\alpha(g_1 g_2) = (\alpha g_1) g_2$.

Now a permutation group on X is simply a subgroup of $Sym(X)$ that is, a permutation group G is a set of permutations of X which is closed under composition, contains the identity permutation, and contains the inverse of each of its elements.

Remark : Let S be a mathematical structure of virtually any type built on the set X . Then the automorphism group of S is usually a permutation group on X. (A little care is required: if S is a topology, then taking "automorphism" to mean "continuous bijection" does not work; we should take "automorphism" to be "homeomorphism" in this case.)

There is a related concept, that of a group action. Let G be a group (in the abstract sense of group theory, a set with a binary operation). Then an action of G on X is a homomorphism from G to $Sym(X)$in other words, it associates a permutation with each element of G. The image of a group action is a permutation group; the extra generality is that the action may have a kernel. The extra flexibility is important, since the same group may act on several different sets.

For e.g. Let G be the group of symmetries of a cube,

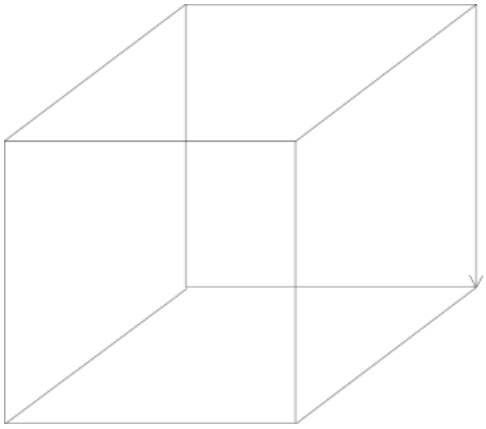


Fig. 7.1

Let X be the set of size 26 consisting of the 8 vertices, 12 edges, and 6 faces of the cube. Then G acts on Ω; the action is faithful (no symmetry can fix all the vertices except the identity), so we can regard G as a permutation group on X. It is often the case, as in the examples below, that when we say "Let G be a permutation group on ", we could as well say "Let the group G act on X ". For example, any permutation group property immediately translates to group actions.

7.3.1 Orbits and transitivity:

In above example, the group G contains permutations which map any vertex to another vertex; we cannot map a vertex to an edge. We formalize this by the notion of orbits.

Let G be a permutation group on X. Define a relation ~ on X by the rule $\alpha \sim \beta$ if and only if there exists $g \in G$ such that $\alpha g = \beta$.

Definition: Equivalence relation: Let 'R' be a relation on 'A', 'R' is said to be an equivalence relation on A iff 'R' is reflexive, symmetric and transitive.

Example 1: Show that ~ is an equivalence relation on X.

Solution: Define relation ~ on X by the rule,

$x \sim y \iff g(x) = y$ for some $g \in G$.

Reflexivity: Since identity belong to any group, and $id(x) = x$ for all $x \in X$, we have $x \sim x$.

Symmetry: Suppose $x \sim y$, so that $g(x) = y$ for some $g \in G$. Since G is a group, $g^{-1} \in G$, and since $g^{-1}(y) = x$ we have $y \sim x$.

Transitivity: If $x \sim y$ and $y \sim z$ we must have $y = g_1(x)$, and $z = g_2(y)$ for some g_1 and g_2 in G. Since G is a group , $g_2 g_1$ is in G and since $g_2 g_1(x) = z$ we have $x \sim z$.

Hence $\sim$ is an equivalence relation on X.

Since $\sim$ is an equivalence relation, X decomposes as a disjoint union of its equivalence classes. These classes are called orbits.

Definition: The Orbit of x contains all the members of X which are of the form $g(x)$ for some $g \in G$, it is denoted by Gx. Explicitly,

$$Gx = \{y = g(x) \ \ for \ \ some \ g \in G\}.$$

Therefore in above example of cube, the sets of vertices, edges and faces form the three orbits of G.

Note: If a permutation group has just a single orbit, we say that it is transitive.

Definition: Stabilizers: Given an element x in X, we define the stabilizer G_x of x (in G) by

$$G_x = \{g \in G \mid gx = x\}$$

As can be readily checked, the stabilizer G_x is a subgroup of G. There is a nice relationship

between the stabilizers of points that belong to the same orbit: if $y = gx$ for some $g \in G$ for points y and x of X, then, as can be readily checked

$$G_{gx} = gG_x g^{-1}$$

The most fundamental theorem about group actions is the Orbit-Stabilizer Theorem, which states that the size of the orbit of an element is equal to the index of its stabilizer in the group. This applies to any situation in which the relevant orbit is finite, although for simplicity we state it only for finite groups

The Orbit-Stabilizer Theorem: Let G be a finite group acting on a set X, and let $x \in X$. Then the number of elements in the orbit Gx is equal to $[G: G_x]$.

i.e. $|Gx| = \frac{|G|}{|G_x|}$

Proof: we say that $\frac{|G|}{|G_x|}$ is the index of G_x in G. which is the number of distinct left cosets of G_x in G.

Let g and h be elements of G and consider when the elements gx and hx of Gx are equal.

$$gx = hx \Leftrightarrow g^{-1}gx = g^{-1}hx$$

Thus $gx = x$ if and only if $g^{-1}h = s$ for some $s \in G_x$.

This occurs if and only if $h = gs$ which means that h belongs to the left coset of G_x determined by g, which means that g and h determine the same left coset of G_x .

Thus the number of distinct elements of the orbit of x is equal to the number of distinct left cosets of G_x in G, as required.

Example 2: Let *T* be a regular tetrahedron in 3-dimensional space. Find the order of the group of rotational symmetries of *T*. (Fig. 7.2)

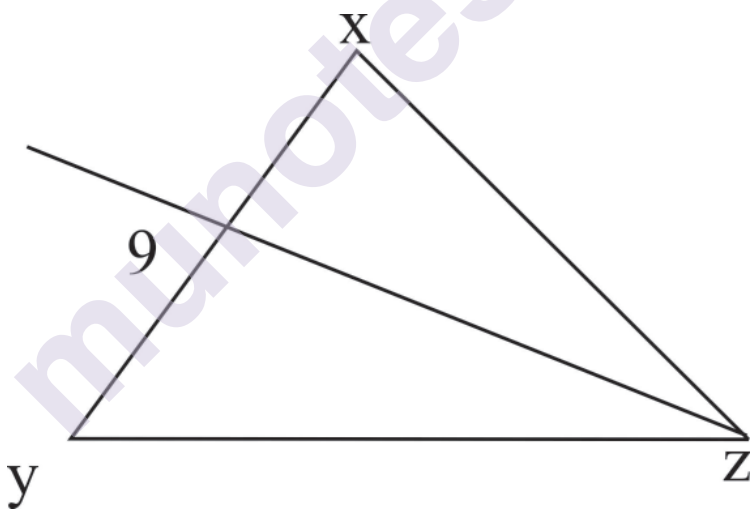


Figure 7.2

Solution: Let *G* be the group of permutations of the corners which correspond to rotational symmetries, and let *x* be any corner of *T*. Given any other corner *y* there is an edge *yx* of *T* and there are two faces of *T* which are bounded by *yx*. Let *a* be the centroid of one of these faces and let *z* be the opposite corner of *T*. Then a rotation of 120° about the axis *az* take *x* to *y*. Hence the orbit Gx contains all four vertices, and we have $|Gx| = 4$.

The only rotational symmetries which fix x are the rotations through $0^\circ, 120^\circ$ and 240° about the altitude passing through x, and so the stabilizer G_x has order 3. Hence by the Orbit-Stabilizer Theorem,

$$|Gx| = \frac{|G|}{|G_x|}$$

$\therefore |G| = |Gx| \times |G_x| = 4 \times 3 = 12.$

The number of orbits:

We turn now to the problem of counting the number of orbits when we are given a group G of permutations of a set X. each orbit is a subset of X whose members are indistinguishable under the action of G, and so the number of orbits tells us the number of distinguishably different types of object in X.

Given any group G of permutations of a set X we define, for each g in G, a set

$$F(g) = \{x \in X \mid g(x) = x\}$$

Thus $F(g)$ is the set of objects fixed by g. The next theorem says that the number of orbits is equal to the average size of the sets $F(g)$ is called Burnside's Lemma.

7.4 Burnside's Lemma

We now develop a theory for counting the number of different (non-equivalent) 2-colorings of the square. More generally, in a set T of colorings of the corners (edges or faces) of same figure, we seek the number N of equivalence classes of T induced by a group G of symmetries of this figure.

Suppose there is a group of s symmetries acting on the c-colorings in T. Let E_c be the equivalence class consisting of C and all colorings C' equivalent to C, that is, all C' such that for some $\pi \in G, \pi(C) = C'$. If each of the $s\pi'$s takes C to a different coloring $\pi(C)$, then E_c would have s colorings. Note that the set of $\pi(C)'$s includes C since $\pi_I(C) = C$ (π_I is the identify symmetry). If every equivalence class is like this with s colorings, then $sN = c$ (number of symmetries) $\times$ (number of equivalence classes) = (total number of colorings)

Solving for N, we have $N = \frac{c}{s}$.

We can use Burnside's Lemma to enumerate the number of distinct objects, however, sometimes we will also want to know more information about the

characteristics of these distinct objects.

Theorem: The number of orbits of G on X is $\frac{1}{|G|}\sum_{g\in G} |F(g)|$. Where $F(g)$ is the set of object fixed by g.

Proof: We use method of counting pairs. Let $E = \{(g, x) | g(x) = x\}$.

Then the row total $r_g(E)$ is equal to the number of x fixed g, that is $|F(g)|$.

Also, the column total $c_g(E)$ is equal to the number of g which fix x, that is $|G_x|$.

Hence the two methods for counting E lead to the equation

$$\sum_{g\in G} |F(g)| = \sum_{x\in X} |G_x|$$

Suppose there are t orbits, and let z be a chosen element of X. If x belong to the orbit G_z then $|G_x| = |G_z|$. Hence on the right hand side of the equation above there are $|Gz|$ terms equal to $|G_z|$, one for each x in Gz. The total contribution from these terms is $|Gz| = \frac{|G|}{|G_x|}$,

Since there are t orbits altogether the right hand side is equal to $t|G|$, and on rearranging the equation we obtain

$$t = \frac{1}{|G|}\sum_{g\in G} |F(g)|.$$

Example 3: Necklaces are manufactured by arranging 13 white beads and 3 black beads on a loop of string. How many different necklaces can be produced in this way?

Solution:

Total number of beads = 13 + 3 = 16 beads, can placed at the corners of a regular polygon with 16 sides.

Now, each configuration is specified by the choice of the 3 corners which are occupied by black beads, therefore $(16\ 3) = 560$ configuration in all.

Two configurations give the same necklace if one can be obtained from the other by a symmetry transformation of the polygon by either a rotation or a reflection, the latter being equivalent to overturning the polygon.

There are 32 symmetries in all, as given below,

i) The identity fixes all 560 configurations.

ii) There are 15 rotations through angles $\frac{2\pi n}{16}$ where $n = 1,2, \ldots\ldots, 15$ and each of them has no fixed configurations.

iii) There are 8 reflections in axes joining the mid-points of opposite sides, and each of them has no fixed configurations.

iv) There are 8 reflections in axes passing through opposite corners. The positions of the 3 black beads are unchanged by such a reflection only if one of the beads occupies one of the 2 corners lying on the axis, and the other pair occupies one of the 7 pairs of corners symmetrically placed with respect to this axis.

Hence there are $2 \times 7 = 14$ fixed configurations for each reflection of this kind.

Therefore the number of different necklaces $= \frac{1}{32}\ [\ 560 + (8 \times 14)] = 21.$

Example 4: A stick is painted with equal sized cylindrical bands. Each band can be painted black or white. If the stick is un-oriented as when spun in the air, how many different 2-coloring of the stick are possible if the stick has i) 2 band? ii) 3 bands?

Solution:

i) The stick with 2 bands is shown in figure below:

Fig.7.3

There are two symmetries of a stick: first(x) is a 0° revolution and second(y) is a 180° revolution.

For the 2-band stick, the set of 2-colorings left by x is all 2-colorings of the stick. There are $2^2 = 4$. The set of 2-colorings left fixed by y consists of the all black and all white coloring, and so 2.

Therefore by Burnside's theorem,

The number of different colorings $= \frac{1}{2}[4 + 2] = 3.$

ii) The stick with 3 bands is shown in figure below:

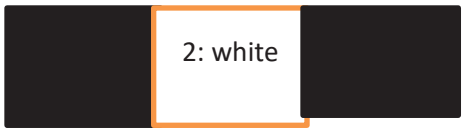


Fig.7.4

There are two symmetries of a stick: first(x) is a 0° revolution and second(y) is a 180° revolution.

For the 3-band stick, the set of 2-colorings left by x is all 2-colorings of the stick. There are $2^3 = 8$. The set of 2-colorings left fixed by y can have any color in the middle band and common color in the two end bands, and so $2 \times 2 = 4$.

Therefore by Burnside's theorem,

The number of different colorings $= \frac{1}{2}[8 + 4] = 6$.

7.5 The Cycle Index

In applying Burnside's theorem we have been faced with computing $F(g)$ for each $g \in G$, where G is permutation group acting on a set X of configurations. We now develop the theory for the simplified calculation of $F(g)$ in Burnside's theorem to use it efficiently in terms of 2-colorings of a square.

Definition: Let G be a group whose elements are the permutations of X, where $|X| = m$. We define the polynomial in m variables $x_1, x_2, \ldots\ldots, x_m$, if $\{a_1, a_2, a_3, \ldots\}$ in the type of g.then the polynomial

$$P_G(x_1, x_2, \ldots\ldots, x_m) = \frac{1}{|G|}\sum_{g \in G} x_1^{a_1} x_2^{a_2} \ldots\ldots x_m^{a_m}$$

is called the cycle index of G.

More generally we have the following result.

Let X be the set of all configurations obtained by a permutation group G. then for any m, $P_G(m, m, m \ldots, m)$ will be the number of non-equivalent m-colorings of X.

Example 5: Suppose a necklace can be made from beads of three colors black, white, and red. How many different necklaces with *n* beads are there?

Solution: Here beads on the necklace can rotate freely around the circle but reflections are not permitted and that the number of different 3-colored strings of n beads is equal to the number of 3-colorings of a cyclically un-oriented n-gon. For $n = 3$, the rotations are of $0^{\circ}, 120^{\circ}$ and 240° with cycle structure representations of x_1^3, x_3, and x_3 respectively. Thus,

$P_G = \frac{1}{3}(x_1^3 + x_3)$.

The number of 3-colored strings of three beads is

$$P_G = \frac{1}{3}[3^3 + 2 \times 3] = 11.$$

More generally, the number of m-colored necklace of three beads is

$$P_G(m, m, m) = \frac{1}{3}[m^3 + 2m].$$

7.6 Polya's Formula

In many instances, the direct application of the Burnside's Lemma is not practically efficient to permit us to enumerate the distinct G −orbits induced by a permutation group. The difficulty perfectly stems from the computation of the number of invariances for a large ordered group.

It is an elegant combination of theory of groups of permutations and the powerful method of generating function. We are now ready to address our ultimate goal of a formula for the pattern inventory. Recall that the pattern inventory is a generating function that tells how many colorings of an unoriented figure are using different possible collections of colors.

The Polya's theorem provides a tool necessary to facilitate this computation. To formulate and prove Polya's theorem in an abstract and more concise manner, it is somehow convenient to require the notion of functions and patterns as its enumerations are basically performed over sets whose elements are functions. In the rest of discussion, we consider X be a set of elements called "places", and Let Y be a set of elements called "figure". Also we consider the usual permutation

group G acting on X, which is called Configuration group. Moreover, an element *f* in Y^X will be called Configuration.

Definition: On Y^X ,the set of all configurations from X to Y, define the relation $f_1 \sim f_2$, to mean that for some $\pi \in G$; $f_1(\pi(x)) = f_2(x) \quad \forall x \in X$.

Definition: Let $w: Y \to \{0, 1, 2, \ldots \ldots\}$ called weight function whose range is set of non-negative integers. For each $k = 0, 1, 2, \ldots$..Let $c_k = |w^{-1}(k)|$ be the number of figures with weight *k*. Further the series in the indeterminate *x*,

$$c(x) = \sum_{k=0}^{\infty} \quad c_k x^k$$

Definition: Let X and R be finite sets, and G be permutation group of X. We will assign a weight to each element $r \in R$ call it $w(r)$. The weight $W(f)$ of a function $f \in R^X$ is the product

$$W(f) = \prod_{x \in X} \quad w[f(x)].$$

Note that if $f_1 \sim f_2$, that is, if they belong to the same pattern, then they have the same weight.

Therefore, we may define the weight of the pattern as a common value. Thus if *F* denotes a pattern, we will denote the weight of *F* by *W(F)*.

Definition: The pattern inventory written P.I is defined by $P.I. = \sum_f \quad W(f)$ where the sum is over all the patterns *f* (in the action of a group *G* acting on the domain *X*)

Polya's Fundamental theorem:

Statement: Let *G* be a permutation group acting on the domain set *X* and let *w* be a weight assignment on the range *R*. then the pattern inventory is given by

$$P.I = P_G\left[\sum_{r \in R} \quad w(r), \sum_{r \in R} \quad w(r)^2, \quad \ldots \ldots, \sum_{r \in R} \quad w(r)^j\right]$$

$$= P_G(x_1, x_2, \ldots \ldots, x_j, \ldots) \mid \left\{x_j = \sum_{r \in R} \quad w(r)^j\right\} \quad \forall\, j$$

That is the pattern inventor is obtained by replacing each variable x_j in the cycle index of the group G by the sum $\sum_{r\in R} \quad w(r)^j$.

Proof: Let $W_1, W_2, \ldots\ldots, W_i, \ldots$ be the distinct entities that occur as weights of patterns. Let m_i denote the number of patterns whose weight is W_i. Then by definition, we have $P.I = \sum_i \quad m_i W_i$.

Now fix an i and consider the set T of all the functions f whose weight W_i.If $F_1, F_2, \ldots\ldots, F_i$ denotes the m_i patterns whose weight is W_i then $T = F_1 \cup F_2 \cup \ldots\ldots \cup F_i$. Let $f \in T$ and let $\alpha \in G$. Then $a_\alpha(f) \in T$ and hence $a_\alpha|T$ is a permutation on T. Therefore, we may restrict the action of the Permutation group G to T and that gives us m_i orbits of G on T. using Burnside's lemma , we have

$$m_i = |G|^{-1} \sum_{\alpha\in G} \quad \left|(F(ix)_{\alpha,i}\right|$$

Where $F(ix)_{\alpha,i} = \{f: f \in T \; and \; a_\alpha(f) = f\}$

And we get $F(ix)_{\alpha,i} = \{f: f \in R^X \; and \; a_\alpha(f) = f\}$

Hence the pattern inventory is given by summing over all i.

$$P.I = \sum_i \quad m_i W_i$$

$$= \sum \quad W_i \, |G|^{-1} \left\{ \sum_{\alpha\in G} \quad \left|(Fix)_{\alpha,i}\right| \right\}$$

$$= |G|^{-1} \sum_{\alpha\in G} \quad \left\{ \sum_i \quad \left|(Fxi)_{\alpha,i}\right| W_i \right\}$$

We now interpret the expression in the parentheses. Fix an $\alpha \in G$. Then we are summing over all i. Thus $\sum_i \quad \left|(Fxi)_{\alpha,i}\right| W_i$ is the sum of weights of all the functions that are fixed by α. Let

$$S_\alpha = \{f: a_\alpha(f) = f\}$$

Then the expression of the pattern inventory simplifies to

$$P.I = |G|^{-1} \sum_{\alpha \in G} W(S_\alpha)$$

To simplifies the notation, Let $S = S_\alpha$. Let cycle type of α be $(b_1, b_2, \dots, b_j, \dots)$. Let $X_{j,t}$ denote the t^{th},j-cycle in the cycle of decomposition of α.Thus $\cup_j \cup_{t=1}^{b_j} X_{j,t}$ is the partition of X. Let $X_{j,t} = (a_1, a_2, \dots\dots, a_j, \dots)$. Then α fixed f if and only if $f(a_i) = f(\alpha(a_i)) = a_{i+1}$ where we read subscripts modulo j. Thus $f \in S$ if and only if f is constant on each $X_{j,t}$. That gives the weight of S to be $w(s) = \prod_j \prod_{t=1}^{b_j} \sum_{r \in R} w(r)^{|X_{j,t}|} = \prod_j \left\{\sum_{r \in R} w(r)^j\right\}^{b_j}$ Because $|X_{j,t}| = j$ and b_j cycles of the length j. it just remains to interpret the right hand side of the equation just obtained. Since α has cycle type $(b_1, b_2, \dots, b_j, \dots)$, the monomial of α is

$$(x_1)^{b_1}(x_2)^{b_2} \dots\dots (x_j)^{b_j} \dots = \prod_j (x_j)^j$$

Thus $w(S_\alpha) = w(S) = \prod_j (x_j)^j$ where the variable x_j is replace by the expression $\sum_{r \in R} w(r)^j$. Thus $w(S_\alpha)$ is nothing but the monomial of α with the j^{th} variable x_j is replace by $\sum_{r \in R} w(r)^j$.

Since *P.I* is obtained by summing all $w(S_\alpha)$ and dividing by $|G|$, by using the definition of cycle index we get

$$P.I = |G|^{-1} \sum_{\alpha \in G} (monomial\ of\ \alpha)$$

$$P.I = P_G\left[\sum_{r \in R} w(r), \sum_{r \in R} w(r)^2, \dots\dots, \sum_{r \in R} w(r)^j\right]$$

$$= P_G(x_1, x_2, \dots\dots, x_j, \dots)\Big| \left\{x_j = \sum_{r \in R} w(r)^j\right\} \forall\, j$$

Example 6: Find the number of 7-bead necklaces distinct under rotations using 3 black and 13 white beads.

Solution: we need to determine the coefficient of b^3w^4 in the pattern inventory. Each rotation except the 0° rotation, is a cyclic permutation when the number of beads is prime, so

$$P_G = \frac{1}{7}(x_1^7 + 6x_7).$$

The pattern inventory is $\frac{1}{7}[(b+w)^7 + 6(b^7 + w^7)]$.

Since the factor $6(b^7 + w^7)$ in the pattern inventory contributes nothing to the b^3w^4 term, we can neglect it. Thus the number of 3-black , 4- white necklaces is simply

$$\frac{1}{7}[\,coefficient\ of\ \ b^3w^4\ in(b+w)^7] = \frac{1}{7}(7\,3\,) = 5.$$

Example 7: Consider of colorings the 12 faces of a regular dodecahedron in two colors black and white with the weights of black and white *b* and *w* respectively. Computed the cycle index of the rotation group of a regular dodecahedron. Using Polya's theorem the pattern inventory is given by

$$P.I = \frac{1}{60}\,[(b+w)^{12} + 20(b^3 + w^3)^4 + 15(b^2 + w^2)^6 + 24(b+w)^2(b^5 + w^5)^2].$$

i) How many patterns have 4 faces black?

ii) How many patterns have 9 faces white?

iii) Find the total number of patterns.

Solution: Polya's theorem the pattern inventory is given by

$$P.I = \frac{1}{60}\,[(b+w)^{12} + 20(b^3 + w^3)^4 + 15(b^2 + w^2)^6 + 24(b+w)^2(b^5 + w^5)^2]$$

i) Patterns have 4 faces black,. i.e. it have 8 faces white. Therefore it has coefficient b^4w^8 in the $P.I$ is given by

$$P.I = \frac{1}{60}\{(12\,4\,) + 15 \times (6\,2\,)\} = \frac{1}{60}\{495 + 225\} = \frac{720}{60} = 60$$

ii) patterns have 9 faces white i.e. it have 3 faces black. Therefore it has coefficient b^3w^9 in the $P.I$ is given by

$$P.I = \frac{1}{60}\{(12\,9\,) + 20 \times (4)\} = \frac{1}{60}\{220 + 80\} = \frac{300}{60} = 5$$

iii) The total number of patterns is

$$P.I = \frac{1}{60}\left[(2)^{12} + 20(2)^4 + 15(2)^6 + 24(4)^4\right]$$

$$= \frac{1}{60}\left[4096 + 20 \times 16 + 15 \times 64 + 24 \times 16\right]$$

$$= \frac{1}{60}\left[4096 + 320 + 960 + 384\right] = 96$$

Example 8: In how many ways, can we color the corners of the square with two colors?

Solution:

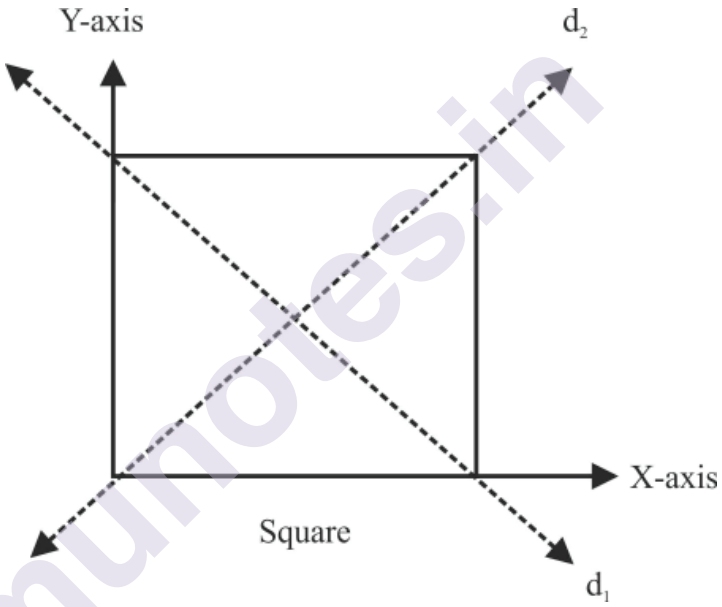


Fig. 7.5

Here the permutation group isD_4. We have two colors. First we find all possible permutations under the action of rotation and reflection, and set of all permutations are isomorphic toD_4.

So,

$$\varepsilon = (1\,2\,3\,4 \quad 1\,2\,3\,4 \quad) = (1)(2)(3)(4)$$

Possible ways (Number of coloring of square's corners) under action ε are

$$|X_\varepsilon| = 2^4 = 16$$

We have,

$\rho_1 = (1\,2\,3\,4 \quad 2\,3\,4\,1\ ) = (1234)$ (90° counter clockwise)

$\rho_2 = (1\,2\,3\,4 \quad 3\,4\,1\,2\ ) = (13)(24)$ (180° counter clockwise)

$\rho_3 = (1\,2\,3\,4 \quad 4\,1\,2\,3\ ) = (1432)$ (90° clockwise)

So, possible ways (Number of coloring of square's corners) under action ρ_1, ρ_2, ρ_3 are

$$\left|X_{\rho_1}\right| = \left|X_{\rho_3}\right| = 2^1 = 2, \quad \left|X_{\rho_2}\right| = 2^2 = 4$$

By reflections of square along axis, we have

$\sigma_x = (1\,2\,3\,4 \quad 4\,3\,2\,1\ ) = (14)(23)$ (rotation along x-axis)

$\sigma_y = (1\,2\,3\,4 \quad 2\,1\,4\,3\ ) = (12)(34)$ (rotation along y-axis)

So, possible ways (Number of coloring of square's corners) under action σ_x and σ_y are

$$|\sigma_x| = \left|\sigma_y\right| = 2^2 = 4$$

By reflections of square along diagonals, we have

$\sigma_{d_1} = (1\,2\,3\,4 \quad 3\,2\,1\,4\ ) = (13)(2)(4)$ (rotation along d_1 diagonal)

$\sigma_{d_2} = (1\,2\,3\,4 \quad 1\,4\,3\,2\ ) = (1)(3)(24)$ (rotation along d_2 diagonal)

So, possible ways (Number of coloring of square's corners) under action σ_{d_1} and σ_{d_2} are

$$\left|\sigma_{d_1}\right| = \left|\sigma_{d_1}\right| = 2^3 = 8.$$

we have,

Required number of colorings $= \frac{1}{8}(16 + 2 \times 2 + 4 + 2 \times 4 + 2 \times 8) = 6.$

Now, we are going to use Polya's theorem for two colors in a square. From above, we have the following cycle structures of permutations

$$(1)(2)(3)(4)$$

$$(1234)$$

$(13)(24)$

(1432)

$(14)(23)$

$(12)(34)$

$(13)(2)(4)$

$(1)(3)(24)$

Cycle structure of D_4

so the cycle index of D_4 is

$$Z(D_4) = \frac{1}{8}(1 \times a_1^4 + 3a_2^2 + 2a_1^2 a_2 + 2a_4)$$

Generating function coloring one corner is

$$F(X, Y) = 1.X + 1.Y$$

We can use color X or Y to color a corner in the square. By Polya's Enumeration Theorem (PET), we have

$$P.I = \frac{1}{8}[(X+Y)^4 + 3(X^2+Y^2)^2 + 2(X+Y)^2(X^2+Y^2) + 2(X^4+Y^4)]$$

Generating function for the colorings of the square. We have

$$Z(D_4)(X, Y) = X^4 + Y^4 + X^3Y + XY^3 + 2X^2Y^2$$

$$Z(D_4)(1,1) = 1 + 1 + 1 + 1 + 2 = 6$$

So, total number of colorings = 6. Hence, the possible colorings are:

1- All corners have color X,

1- All corners have color Y,

1- Three corners have color X, and one has Y,

1- One corner has color X and three have Y,

2- Two corners have color X and two have Y

Example 9: One of the important applications of the content version of Polya's theorem is the finding of different possible isomers of a chemical compound. Recall that isomers are chemical compounds with the same chemical formula with a different arrangement of the atoms.

a) Find the number of benzene rings with Cl substituted in the place of H.

Solution: The symmetry group of the benzene ring is D_6 (i.e., the symmetries of a regular hexagon).

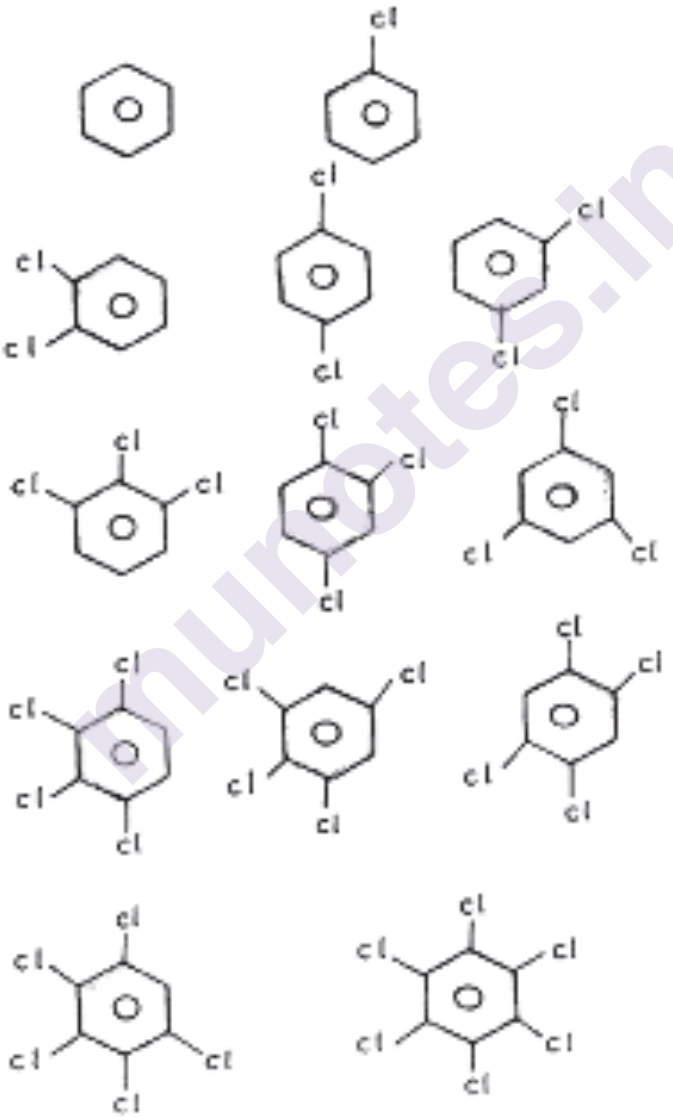


Fig 7.6

Now, $Z(D_6) = \frac{1}{12}[S_1^6 + 4S_2^3 + 2S_3^2 + 3S_1^2S_2^2 + 2S_6]$

Here, $D = \{1,\ 2, 3, 4, 5, 6\}$ $R = \{H, Cl\}$

Let content $(H) = 0$, content $(Cl) = 1$,

So $c(x) = 1 + x$.

$$P.I = \frac{1}{12}[(1+x)^6 + 4(1+x^2)^3 + 2(1+x^3)^2 + 3(1+x)^2(1+x^2)^2 + 2(1+x^6)]$$

$$= 1 + x + 3x^2 + 3x^3 + 3x^4 + x^5 + x^6$$

Replace $x = 1$ we get,

The number of benzene rings with $Cl = 1 + 1 + 3 + 3 + 3 + 1 + 1 = 13$

Therefore there are 13 chemical compounds obtained in this manner.

Example 10: Find the number of (simple, undirected) graphs upto isomorphism on a set of *4* vertices.

Solution: Here D is the set of (4 2) pairs of vertices. If there is an edge between a pair of vertices,

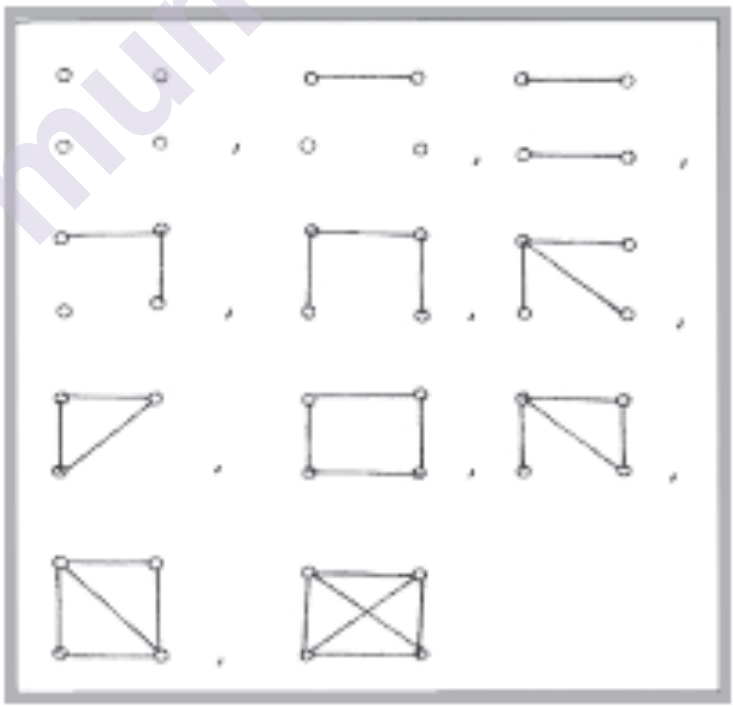


Fig. 7.7

Let it have content 1, if it has no edge, then let it have content 0.

So, a configuration is a graph, and its content is the number of edges.

Then $c(x) = 1 + x$.

Now, two labelled graphs are isomorphic if there exists a bijection between the vertices that preserves adjacency (therefore, two graphs are equivalent if they are isomorphic). Now, the group G of symmetries of the set of pairs of vertices is called $s_n^{(2)}$ and its cycle index is

$$Z\left(s_4^{(2)}\right) = \frac{1}{24}\left[s_1^6 + 9s_1^2s_2^2 + 8s_3^2 + 6s_2s_4\right]$$

Counting series for such graphs

$$P.I = [(1+x)^6 + 6(1+x)^2(1+x^2)^2 + 8(1+x^3)^2 + 6(1+x^2)(1+x^4)]$$

$$= 1 + x + 2x^2 + 3x^3 + 2x^4 + x^5 + x^6$$

Replace $x = 1$ we get,

Total number of unlabelled graphs on 4 vertices$= 1 + 1 + 2 + 3 + 2 + 1 + 1 = 11$.

Therefore total number of unlabelled graphs on 4 vertices = 11

Let us Sum up:

In this unit we have learnt the following:

- Equivalence relations and orbits under a permutation group action.
- Basic concept of Orbits and stabiliser, Orbit stabiliser theorem.
- Burnside Lemma and its applications base examples.
- Polya's counting theory with Cycle index, Polya's theorem and its application.

Unit End Exercise

1. Calculate the group of rotational symmetries, and count its orbits on the set of dimples on the golf ball.

2. How many different 3-colorings of the bands of an *n*-band stick are there if the stick is un-oriented?

3. Suppose a necklace can be made from beads of three colors black, white, and red. How many different necklaces with *n* beads are there?

4. How many necklaces can be made from a string of 3 black beads and 13 white beads?

5. Each face of a cube is painted in one of the following five colors: red, green, blue, yellow, or white. Determine the number of cubes that can be generated this way, if the color red has to be used exactly two times. Cubes are considered distinct if they cannot be obtained from each other using rotations.

6. Find the number of distinct squares that can be obtained by painting each edge of a given square in either red or green. Squares are considered distinct if they cannot be obtained from each other using rotations or reflections.

7. A disc lies in a plane. Its Centre is fixed but it is free to rotate. It has been divided into *n* sectors of angle $\frac{2\pi}{n}$. Each sector is to be colored Red or Blue. How many different colorings are there?

8. How many necklaces of n beads can be made in m colors, if the group acting on them is the cyclic group C_n?

9. Compute the number of distinct colorings of the vertices of a square with 3 colors, under the following equivalencies:

   a) Rotations are not distinct.

   b) Rotations and reflections are not distinct.

   c) Rotations, reflections, and color permutations are not distinct.

10. How many distinct organic molecules can be formed under the following stipulation? The geometry of a typical organic molecule has a carbon atom at the center of a regular tetrahedron with four valencies going towards the four comers of the regular tetrahedron.

Reference:

1. Applied Combinatorics, Alan Tucker.
2. Combinotorial Techniques, Sharad S. Sane
3. Discrete mathematics its Application, Keneth H. Rosen TMG.
4. Discrete mathematics, Norman L. Biggs.
5. Discrete structures by B. Kolman HC Busby, S Ross PHI Pvt. Ltd.
6. Discrete mathematics, schaum's outlines series, seymour Lip Schutz, Marc Lipson, TMG.