5. Bigger number cannot divide the smaller positive number.
6. Only zero is divisible by zero.

6.1.2 Prime Numbers :

- Any integer p such that $p > 1$ is called as prime number if p is divisible by 1 and itself.
- An integer, which is not prime number is called as composite.

Prime number theorem :

Let $\pi(x)$ denotes the number of primes less than x then

$$\pi(x) \approx \frac{x}{\ln x}$$

And the ratio $\pi(x) \mid (x \mid \ln x) \rightarrow 1$ as $x \rightarrow \infty$.

- Every positive integer can be expressed as the product of prime numbers raised to different powers.

  Example $9720 = 2^3 3^5 5$, $504 = 3^2 \times 2^3 \times 7$
- This factorization into primes is unique and reordering of factors can be done.
- If a prme p, divides a product ab.....z then p must divide one of the factors a, b ....z.
- If the product of two integers is even then one of the integers must be even.

6.1.3 Greatest Common Divisor (gcd) :

- The greatest common division of 'a' and 'b' is denoted by gcd (a, b) or (a, b). It is the largest positive integer that divides both 'a' and 'b'.
- If gcd (a, b) = 1 then integers 'a' and 'b' are called as **relative prime numbers.**
- To find gcd of integers 'a' and 'b' ; factorize 'a' and 'b' into primes. Then take a common prime divisor having smallest exponent. It is gcd.

Example : gcd (9720, 504) = gcd $(2^3 3^5 5, 3^2 2^3 7)$

Here gcd is 2^3.

- If it is not easy to factorize, then **Euclidean algorithm** is used.

Ex. 6.1.1 : Suppose we want gcd (385, 1270)

Soln. :

Divide 1270 by 3 and 5

$$\therefore \quad 385 \overline{)\,1270\,(3} \qquad \text{(E-1281)}$$
$$\underline{1155}$$
$$115$$

Here quotient is 3 and remainder is 115

$$\therefore \quad 1270 = 3.385 + 115$$

Then divide 385 by 115

$$115 \overline{)\,385\,(3} \qquad \text{(E-1282)}$$
$$\underline{345}$$
$$40$$

Quotient is 3 and remainder is 40

$$\therefore \quad 385 = 3.115 + 40$$

Now divide 115 by 40

$$\begin{array}{r|l} 40 & 115 \quad (2 \\ & \underline{80} \\ & 35 \end{array} \qquad \text{(E-1283)}$$

The quotient is 2 and remainder is 35

$$\therefore \quad 115 = 2.40 + 35$$

Divide 40 by 35

$$\begin{array}{r|l} 35 & 40 \quad (1 \\ & \underline{35} \\ & 5 \leftarrow \text{Last nonzero remainder} \end{array} \qquad \text{(E-1284)}$$

Here quotient is 1 and remainder is 5

$$\therefore \quad 40 = 1.35 + 5$$

Divide 35 by 5

$$\begin{array}{r|l} 5 & 35 \quad (7 \\ & \underline{35} \\ & 0 \leftarrow \text{zero remainder} \end{array} \qquad \text{(E-1285)}$$

Now we have got zero remainder

$$\therefore \quad 35 = 7.5 + 0$$

The last non zero remainder is gcd. It is 5.

Thus gcd (385, 1270) = 5

- The generalized form can be expressed as follows :
- Suppose we want to calculate gcd (a, b) and a > b. If a is not greater than 'b' then simply change the positions of 'a' and 'b'.
- Initially express 'a' as

$$a = q_1 b + r_1$$

- Here q_1 is the quotient and r_1 is remainder. If r_1 is zero then gcd is b. But if $r_1 \neq 0$ then b as,

$$b = q_2 r_1 + r_2$$

- This procedure is continued, till zero remainder is obtained.

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \quad\quad \vdots \\ r_{k-2} &= q_k r_{k-1} + r_k \\ r_{k-1} &= q_{k+1} r_k + 0 \end{aligned} \qquad \text{(E-1286)}$$

The gcd is r_k.

$$\gcd(a, n) = 1.$$

- Since these are four integers; we can write,

$$\phi(n) = \phi(10) = 4$$

- This function 'ϕ' is called as Euler's function.
- If 'p' is prime number and $n = p^r$ then the following condition is satisfied.

$$\phi(n) = \phi(p^r) = \left(1 - \frac{1}{p}\right) p^r$$

- Consider that 'n' is product of two distinct primes that means $n = p \cdot q$. Then the following condition is satisfied :

$$\phi(n) = \phi(pq) = (p - 1)(q - 1)$$

- Consider $n = 10$ and let two distinct primes be $p = 2$ and $q = 5$.

$$\therefore \phi(10) = (2 - 1)(5 - 1) = 4$$

Statement :

$$\text{If } \gcd(a, n) = 1 \text{ then,}$$
$$a^{\phi(n)} \equiv 1 \pmod{n}$$

- If $n = p$, where 'p' is prime number then Euler's theorem is same as Fermat's theorem.
- If we want to calculate mod n; we should do the calculations for mod $\phi(n)$ in the exponent.

6.7 Prime Number Generation :

New Syll. : MU : May 14

- The prime number generation is required in many public key algorithms.
- It is basically required to obtain key pairs during various cryptographic setup.
- Few simple and effective algorithms can be used to generate prime numbers.
- Start with integer 2 and then start selecting each successive integer as a potential prime (pp).
- Then check for the prime property that whether it can be factored by any previous prime or not.
- Make an array and store each newly verified prime in the prime set array (ps).
- The algorithm is as follows :

```
pp = 2
ps = [pp]
lim = raw – input
while
   pp < int (lim)
   ppt = 1
For a in ps :
   if pp % a = 0
        break
   else : ps. append (pp)
   return ps
```

6.8 Random Number Generation :

New Syll. : MU : May 14

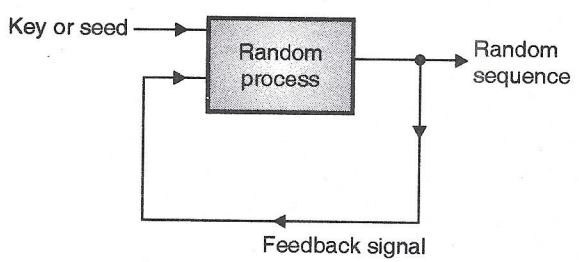
- Random number generator (RNG) is a physical device that generates a sequence of number randomly that means in this sequence there is no fixed pattern.
- Random numbers are required in applications, where it is required to produce the unpredictable results.
- Some of the applications are cryptography computer simulation, statistical sampling etc.
- There are two methods for random number generation :
  1. True random numbers
  2. Pseudo-random numbers

1. True Random Number Generator (TRNG) :

- The true random number generation is based on observations of random physical process.
- This method measures some physical phenomenon which is supposed to be random.
- Then the possible biasing in the measurement process is calculated.
- In this measurement a random source called as entropy source is used.
- For example, the radioactive decay which is measured for small time period is used as entropy source.
- The entropy of the source is dependent on the physical phenomenon that is to be measured.
- This process is usually slow and there is no guarantee that second time, the same random number will be generated.

2. Pseudo-Random Number Generator (PRNG) :

- TRNG makes use of entropy source based on random phenomenon to be measured.
- In PRNG, a short initial input is selected. It is called as **key or seed.**
- This method makes use of computer algorithm which is not time limited by external source.
- The algorithm produces a long sequence of random numbers by using deterministic calculations.
- But if all key (seed) values are known then any one can generate the same random numbers.
- The general block diagram is shown in Fig. 6.8.1.



(E-1274) **Fig. 6.8.1**

- The output random bits are used as feedback. They by using feedback data and key value; a long sequence of random numbers is generated.

- One of the most commonly used algorithm is a linear congruential generator.
- It makes use of recursive (feedback) technique as :

$$X_{n+1} = (a X_n + b) \bmod m$$

- The maximum numbers that can be generated is governed by mod m. Here a is multiplier value.
- Many such random generators with different values of 'a' are connected in parallel.
- The master generator is used to select any one of random generators.

6.9 Primitive Roots :

Introduction to BCH Codes :

- The long form of BCH is Bose-Chaudhari-Hocquenghem. The BCH codes are one of the most important, powerful linear block codes.
- BCH codes are cyclic codes with a wide variety of parameters.
- These codes can correct multiple errors. They are easy to encode and decode.
- Till now we used to construct a code, then find its minimum distance d_{min} to know the error correcting capability of the code.
- But in case of BCH codes. We go the other way. The number random errors to be corrected is specified first and accordingly we construct the generator polynomial; for the code.
- Reed Solomon code is a subclass of BCH codes. The RS code also has been discussed in this chapter.
- The Hamming code with a single error correcting capability is a BCH code. The block lengths and the code. The block lengths and the code rates of BCH codes are variable. In this sense they provide a high flexibility.
- For block lengths of a few hundred, the BCH codes are among the best known codes of the same block length and code rate.

6.9.1 Primitive Elements :

Definition :

A primitive element of GF(q) is defined as the element (α) such that every element in the field except zero can be expressed as a power of α.

The concept of primitive elements is clear from the following example.

Ex. 6.9.1 : Obtained the various primitive elements for the field GF(5).

Soln. :

For GF(5) the value of q is 5 which is a prime number. So we can use the modulo arithmetic.

The elements of GF(5) are as follows :

$$GF(5) = \{0, 1, 2, 3, 4\}.$$

Out of these elements any one or more can be the primitive elements. Let us try out for 2.

1. Consider the element 2 :

We should be able to express all the elements i.e. 1, 2, 3, 4 except 0 in terms of powers of $\alpha = 2$.

$\therefore \quad 2^{\circ} = 1 \pmod 5 = 1 \div 5$, $\theta = 0$, Remainder = 1

$\therefore \quad 2^{\circ} = 1$ ...Considering the remainder

Similarly $2^{1} = 2 \pmod 5 = 2$

$2^{2} = 4 \pmod 5 = 4$

$2^{3} = 8 \pmod 5 = 8 \div 5, Q = 1, R = 3$

$\therefore 2^{3} = 3$ ...Considering the remainder.

Thus we can express all the elements of GF (5) in terms of power of 2.

$\therefore$ 2 is a primitive element of GF (5).

2. Consider the element 3 :

$3^{0} = 1 \pmod 5 = 1$

$3^{1} = 3 \pmod 5 = 3$

$3^{2} = 9 \pmod 5 = 4$

$3^{3} = 27 \pmod 5 = 2$

Thus we can express all the elements of GF(5) except.

0 as power of 3. So 3 also is a primitive elements of GF(5).

3. Consider the element 1 :

$1^{0} = 1 \pmod 5 = 1$ ...O.K.

$1^{1} = 1 \pmod 5 = 1$

$1^{2} = 1 \pmod 5 = 1$

Thus we cannot express the elements 2, 3, 4 in terms of powers of 1. Hence 1 is **not** the primitive elements of GF (5).

4. Consider the element 4 :

$4^{0} = 1 \pmod 5 = 1$ ...O.K.

$4^{1} = 4 \pmod 5 = 4$ ...O.K.

$4^{2} = 16 \pmod 5 = 1$ ...O.K.

$4^{3} = 64 \pmod 5 = 4$

Thus we cannot express the elements 2 and 3 in terms of powers of 4. So 4 is **not** the primitive elements of GF(5).

Conclusion :

- From Ex. 6.9.1 we conclude that there can be more than 1 primitive elements in a field.
- It is not necessary that there are always more than 1 primitive elements but there is a guarantee of finding at least one primitive element.

Importance of primitive element :

- Primitive elements are used to build (construct) a field.
- If we know a primitive elements of a field, we can find all other elements of the field by calculating the power of α.

6.9.2 Primitive Polynomial :

- A primitive polynomial p(x) over GF(q) is a prime polynomial over GF(q) with the property that in the extension field constructed modulo p(x), the field element represented by x is a prime element.
- An irreducible polynomial is called as a primitive polynomial. The examples of primitive polynomials are $(x^3 + x + 1)$ or $(x^4 + x + 1)$
- Primitive polynomials of every degree will be present over every GF. A primitive polynomial is useful in construction of an extension field. This is illustrated in the following example.

Ex. 6.9.2 : Compute all the element of GF(8) using the primitive polynomial $p(x) = x^3 + x + 1$, assuming that the primitive element of GF (8) is $\alpha = y$.

Soln. :

- We can obtain all the elements of GF(8). As powers of $\alpha = y$ evaluated module p(x).
- Since q = 8, we have to go only upto the 7^{th} power of α i.e. y.

1. y^0 :

$$y^0 = 1 \bmod p(x) = 1 \div p(x),\ Q = 0,\ R = 1$$
$$= 1 \quad \text{...Considering the remainder.}$$

2. y^1 :

$$y^1 = y \bmod b(x) = y \div p(x)$$
$$= y$$

3. y^2 :

$$y^2 = y^2 \bmod p(x) = y^2$$

4. y^3 :

$$y^3 = y^3 \bmod p(x) = y^3 \div (y^3 + y + 1)$$
$$= Q = 1, R = (y + 1)$$
$$\therefore \quad y^3 = (y + 1) \quad \text{...Considering the remainder.}$$

Similarly we can obtained the values of y^4, y^5, y^6, y^7. The remainders are used as the elements of the field GF(8). They are listed in Table P. 6.9.2.

Importance of primitive element :

- Primitive elements are used to build (construct) a field.
- If we know a primitive elements of a field, we can find all other elements of the field by calculating the power of α.

6.9.2 Primitive Polynomial :

- A primitive polynomial p(x) over GF(q) is a prime polynomial over GF(q) with the property that in the extension field constructed modulo p(x), the field element represented by x is a prime element.
- An irreducible polynomial is called as a primitive polynomial. The examples of primitive polynomials are $(x^3 + x + 1)$ or $(x^4 + x + 1)$
- Primitive polynomials of every degree will be present over every GF. A primitive polynomial is useful in construction of an extension field. This is illustrated in the following example.

Ex. 6.9.2 : Compute all the element of GF(8) using the primitive polynomial $p(x) = x^3 + x + 1$, assuming that the primitive element of GF (8) is $\alpha = y$.

Soln. :

- We can obtain all the elements of GF(8). As powers of $\alpha = y$ evaluated module p(x).
- Since q = 8, we have to go only upto the 7^{th} power of α i.e. y.

1. y^0 :

$$y^0 = 1 \bmod p(x) = 1 \div p(x),\ Q = 0,\ R = 1$$
$$= 1 \quad \text{...Considering the remainder.}$$

2. y^1 :

$$y^1 = y \bmod b(x) = y \div p(x)$$
$$= y$$

3. y^2 :

$$y^2 = y^2 \bmod p(x) = y^2$$

4. y^3 :

$$y^3 = y^3 \bmod p(x) = y^3 \div (y^3 + y + 1)$$
$$= Q = 1, R = (y + 1)$$
$$\therefore \quad y^3 = (y + 1) \quad \text{...Considering the remainder.}$$

Similarly we can obtained the values of y^4, y^5, y^6, y^7. The remainders are used as the elements of the field GF(8). They are listed in Table P. 6.9.2.

Table P. 6.9.2

Power of y	Element of GF(8)
y^0	1
y^1	y
y^2	y^2
y^3	y + 1
y^4	$y^2 + y$
y^5	$y^2 + y + 1$
y^6	$y^2 + 1$
y^7	1

Theorem :

If $b_1, b_2 \ldots, b_{q-1}$ are the non zero field elements of GF(q) then it can be proved that

$$x^{(q-1)} - 1 = (x - b_1)(x - b_2) \ldots (x - b_{q-1})$$

For example consider GF(5). The non zero elements in GF(5) are {1, 2, 3, 4}.

$$\therefore \quad b_1 = 1, b_2 = 2, b_3 = 3, b_4 = 4$$

$$\therefore \quad x^{(5-1)} - 1 = (x-1)(x-2)(x-3)(x-4)$$

$$\therefore \quad x^4 - 1 = (x-1)(x-2)(x-3)(x-4)$$

6.9.3 Minimal Polynomials :

- In the chapter on cyclic codes, we have seen that in order to find the generator polynomial of a cyclic code, of block length n, we have to find the factors of $(x^n - 1)$.
- So $(x^n - 1)$ can be expressed as a product of its p prime factors as follows.

$$(x^n - 1) = f_1(x) \cdot f_2(x) \ldots . f_p(x) \qquad \ldots (6.9.1)$$

  Where $f_1(x)$, $f_2(x)$ ... etc are the prime factors of $(x^n - 1)$.
- We can obtain the generator polynomial g(x) by multiplying any of these prime factors together.
- The procedure for constructing the generator polynomial g(x) is as follows :
  1. Decide the desirable zeros in the extension field.
  2. Using these desirable zeros in the extension field.
  3. Multiply the prime polynomials together to construct the desirable generator polynomial g(x).

Primitive block length :

If the block length n is of the form $n = q^m - 1$, then it is called as the primitive block length for a code over GF(q).

Primitive cyclic code :

A cyclic code over GF(q) of primitive block length is called as a primitive cyclic code.

- The field $GF(q^m)$ is known as the extension field of GF(q). If we assume that the primitive block length $n = q^m - 1$ then the factorisation of $x^n - 1$ over the field GF(q) is given by,

$$(x^n - 1) = x^{(q^m - 1)} - 1 = f_1(x) \cdot f_2(x) \ldots f_p(x) \quad \ldots(6.9.2)$$

- Note the factorisation of $(x^n - 1)$ will be valid over the extension field $GF(q^m)$.
- It is known that the generator polynomial g(x) divides $(x^n - 1)$ i.e. $x^{q^m - 1} - 1$. So we can say that g(x) should be equal to the product of some of the terms on RHS of Equation (6.9.2).
- Also every non zero element of $GF(q^m)$ is zero of $x^{qm - 1} - 1$. So we can factorize $x^{q^m - 1}$ in the extension field $GF(q^m)$ to write,

$$x^{qm-1} - 1 = \prod_j (x - \beta j) \quad \ldots(6.9.3)$$

Where βj ranges over all the non zero elements of $GF(q^m)$.

- This means that each polynomial $f_1(x)$, $f_2(x)$ ... can be represented in $GF(q^m)$ as a product of some linear terms.
- It also means that each βj is a zero of only one $f_i(x)$ i.e. $f_1(x)$, $f_2(x)$ ...etc.
- This $f_i(x)$ is called a **Minimal Polynomial** of βj.

Definition of minimal polynomial :

- The minimal polynomial of βj is defined as the smallest degree polynomial with coefficients in the base field GF(q) that has a zero in the extension field $GF(q^m)$.

Ex. 6.9.3 : For the subfield GF(2) and its extension field GF(8). Obtain the minimal polynomials $f_i(x)$ and corresponding values of elements βj in GF(8).

Soln. :

The subfield is GF(2) so q = 2 and the extension field is $GF(8) = GF(2^3)$ so m = 3.

Step 1 : Factorize $x\, q^{m-1} - 1$:

We have to factorize $x^{q^m - 1} - 1$ in the subfield or extension field.

$$\therefore \quad x^{q^m - 1} = x^{2^3} - 1 = x^7 - 1$$

$$= (x - 1)(x^3 + x + 1)(x^3 + x^2 + 1) \quad \ldots(1)$$

Step 2 : Write down the elements of GF(8) :

The elements of GF(8) are as follows,

$0, 1, y, (y + 1), y^2, (y^2 + 1), (y^2 + y), (y^2 + y + 1)$

Step 3 : Factorize $(x^7 - 1)$ in terms of elements of GF(8)

The factors of $(x^7 - 1)$ in terms of the elements of GF(8).

$$x^7 - 1 = (x - 1)(x - y)(x - y - 1)(x - y^2)(x - y^2 - 1)(x - y^2 - y)(x^2 - y^2 - y - 1)$$

$$\therefore \quad x^7 - 1 = (x - 1)[(x - y)(x - y^2)(x - y^2 - y)] \cdot [(x - y - 1)(x - y^2 - 1)(x - y^2 - y - 1)]$$

It can be proved that over GF(8),

$$(x^3 + x + 1) = (x - y)(x - y^2)(x - y^2 - y) \text{ and}$$

$$(x^3 + x^2 + 1) = (x - y - 1)(x - y^2 - 1)(x - y^2 - y - 1)$$

All the multiplications and additions are performed over GF(8).

- Table P. 6.9.3 lists the minimal polynomials $f_i(x)$ and the corresponding elements βj in GF(8).

Table P. 6.9.3

Sr. No.	Minimal polynomial $f_i(x)$	Corresponding elements βj in GF(8)	Elements in terms of powers of α
1.	$(x-1) = f_1(x)$	1	α^0
2.	$(x^3+x+1) = f_2(x)$	y, y^2 and (y^2+y)	$\alpha^1, \alpha^2, \alpha^4$
3.	$(x^3+x^2+1) = f_3(x)$	$(y+1)$, (y^2+1) and (y^2+y+1)	$\alpha^3, \alpha^6, \alpha^5 (= \alpha^{12})$

- Note that the elements in terms of powers of the primitive elements α correspond to the same minimal polynomial.
- In this example the zeros of the minimal polynomial $f_2(x) = x^3 + x + 1$ are α^1, α^2 and α^4.
- And the zeros of the minimal polynomial $f_3(x) = x^3 + x^2 + 1$ are α^3, α^6 and α^{12}.

Definition of conjugates :

- If two or more elements in $GF(q^m)$ share the same minimal polynomial over GF(q) then they are called as conjugates with respect to GF(q).
- For example, the elements $\{\alpha^1, \alpha^2, \alpha^4\}$ in Table P. 6.9.3.

6.10 Legendre and Jacobi Symbols :

- Consider that 'p' is odd prime number. Also consider an integer 'a' such that,

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

- The congruence $x^2 \equiv a \pmod{p}$ has a solution if and only if

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

- Legendre and Jacobi symbols give a simple method to determine whether or not a number is square mod p.
- Consider a odd prime number p and let $a \not\equiv 0 \pmod{p}$ then Legendre symbol is defined as :

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } x^2 \equiv a \pmod{p} \text{ has a solution} \\ -1 & \text{if } x^2 \equiv a \pmod{p} \text{ has no solution} \end{cases}$$

Properties of Legendre symbol :

1. If $a \equiv b \not\equiv 0 \pmod{p}$ then,

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

2. If $a \cdot b \not\equiv 0 \pmod{p}$ then,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

3. If $a \not\equiv 0 \pmod{p}$ then,

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

4. $(-1)^{(p-1)/2} = \left(-\frac{1}{p}\right)$

- The Jacobi symbol is definition based on Legendre symbol.
- Consider an odd positive integer 'n' and let 'a' is non-zero integer such that gcd (a, n) = 1.
- Let the prime factors of n are,

$$n = p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \ldots\ldots p_r^{b_r} \text{ then we have,}$$

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{b_1} \cdot \left(\frac{a}{p_2}\right)^{b_2} \cdot \left(\frac{a}{p_3}\right)^{b_3} \ldots\ldots \left(\frac{a}{p_r}\right)^{b_r}$$

- The R.H.S. represents Legendre symbol. But if n = p then at R.H.S. we will get only one Legendre symbol. It is called as Jacobi symbol.

Properties of Jacobi symbols :

1. When $a \equiv b \pmod n$ and gcd (a, n) = 1 then

$$\left(\frac{a}{b}\right) = \left(\frac{b}{n}\right)$$

2. Let gcd (ab, n) = 1 then,

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$$

3. $$\left(\frac{2}{n}\right) = \begin{cases} +1 \text{ if } n \equiv 1 \\ -1 \text{ if } n \equiv 3 \end{cases}$$

4. $$(-1)^{(n-1)/2} = \left(\frac{-1}{n}\right)$$

5. Consider 'q' is odd with gcd (q, n) = 1 then,

$$\left(\frac{q}{n}\right) = \begin{cases} -\left(\frac{n}{q}\right) \text{ if } q \equiv n \equiv 3 \pmod 4 \\ +\left(\frac{n}{q}\right) \text{ otherwise} \end{cases}$$

- The last property is called as law of quadratic reciprocity.

6.11 Discrete Probability :

New Syll. : MU : May 14

6.11.1.1 Introduction :

The probability theory is used in the analysis of non-deterministic or random signals and systems. Let us begin our discussion on probability by defining some important terms.

6.11.1.2 Set Theory :

- For learning the probability it is necessary to have the background of set theory.
- The various operations such as union, subtraction, intersection of sets, definition of subset etc. is essential.
- We assume that being a second year student of engineering you have the basic knowledge of the set theory and go ahead.