ANALYTICAL NUMBER THEORY

M.A./M.Sc. Mathematics (Final)

MM-504 and 505
(Option-P_5)

Directorate of Distance Education
Maharshi Dayanand University
ROHTAK – 124 001

Maharshi Dayanand University
ROHTAK – 124 001

Developed & Produced by EXCEL BOOKS PVT. LTD., A-45 Naraina, Phase 1, New Delhi-110 028

Contents

M.A./M.Sc. Mathematics (Final)

ANALYTICAL NUMBER THEORY

MM-504-505 (P_5)

Max. Marks : 100

Time : 3 Hours

Note: Question paper will consist of three sections. Section I consisting of one question with ten parts covering whole of the syllabus of 2 marks each shall be compulsory. From Section II, 10 questions to be set selecting two questions from each unit. The candidate will be required to attempt any seven questions each of five marks. Section III, five questions to be set, one from each unit. The candidate will be required to attempt any three questions each of fifteen marks.

Unit I

Primes in certain arithmetical progressions. Fermat numbers and Mersenne numbers. Farey series and some results concerning Fary series. Approximtion of irrational numbers by rations. Hurwitz's theorem irrationality of e and n. The series of Fibonocci and Lucas. System of linear congruences Chinese Remainder Theorem. Congruence to prime power modulus.

Unit II

Quadratic residues and non-residues. Legender's Symbol. Gauss Lemma and its applications. Quadratic Law of Reciprocity jacobi's Symbol. The arithmetic in Z_p. The group U_n. Primitive roots. The group U_p^n (p-odd) and U_2^n. The existence of primitive roots. The group of quadratic residues. Quadratic residues for prime power moduli and arbitrary moduli.

Unit III

Riemann Zeta Function $\xi(s)$ and its convergence. Application to prime numbers. ξ (s) as Euler's product. Evaluation of $\xi(2)$ and $\xi(2k)$. Dirichlet series with simple properties. Dirichlet series as analytic function and its derivative. Eulers products. Introduction to modular forms.

Unit IV

Diophantine equations. $x^2 + y^2 = z^2$ and $x^4 + y^4 = z^4$. The representation of number by two or four squares. Waring's problem. Four square theorem. The number g(k) & G(k). Lower bounds for g(k) & G(k).

Algebraic number and Integers : Gaussian integers and its properties. Primes and fundamental theorem in the ring of Gaussian integers. Integers and fundamental theorem in Q (w) where w3 = 1, algebraic fields. Primitive polynomials. The general quadratic field Q($\sqrt{m}$), Units of Q ($\sqrt{2}$). Fields in which fundamental theorem is false. Real and complex Euclidean fields. Fermat" theorem in the ring of Gaussian integers. Primes of Q(2) and Q(5). Luca" test for the prmality of the Mersenne number.

Unit V

Arithmetical function $\phi(n)$, $\mu(n)$, d(n) and $\sigma(n)$ Mobius inversion formulae. Perfect numbers. Order and average order of d(n), $\phi(n)$. The functions $\vartheta(x)$, $\psi(x)$ and $\Delta(x)$. Betrand postulate. Sum p^{-1} and product $1+p^{-1}$. Merten's theorem Selberg's theorem. Prime number Theorem.

Unit-I

Primes in Certain Arithmetical Progressions and System of Congruences

Primes in certain arithmetical progressions.

Peano Axioms are

(1) $1 \in N$ where N is the set of natural numbers

(2) For every natural number n there exists its successor number $(n+1) \in N$

(3) 1 is not the successor of any natural number i.e. $o \notin N$.

(4) Principle of mathematical Induction : If p(n) is a mathematical statement which is true for n = 1 and p(n) is true for n = m + 1 whenever it is true for n = m then p(n) is true for all natural numbers.

Law of well ordering :- Every subset of N has a least element.
Theorem 1.1 Every natural number n > 1 has a prime divisor (factor)
Proof :- We shall prove the lemma by induction on n.
For n = 2, lemma is true (Θ 2 > 1, 2 has a prime divisor 2)

Suppose lemma is true for all natural number <n. Now consider n. If n is prime. Then the lemma is true because it has a prime divisor n itself. So assume 'n' to be composite. Then n has a positive divisor n_1, 1 < n, < n such that $n = n_1.n_2$ where $1 < n_2 < n$

Since $n_1 < n$ by induction hypothesis n_1 has a prime divisor say p. Then $p \mid n_1$ and $n_1 \mid n$

$\Rightarrow$ $p \mid n$. This proves the theorem.

Theorem 1.2 (Euclid) :- The number of primes are infinite

Proof :- If possible, suppose number of primes are finite. Let these be p_1, $p_2,\ldots p_r$.

Consider $N = p_1 p_2 \ldots p_r + 1$

Now N > 1, by above theorem N has a prime divisor say p>1. But only primes are $p_1, p_2,\ldots,p_r$ so $p = p_i$ for some i

Then $p \mid p_1 p_2 \ldots p_r$, Also $p \mid N \Rightarrow p \mid (N - p_1. p_2 \ldots p_r)$ or $p \mid 1$, which is a contradiction.

Hence number of primes are infinite

Note :- Let P = {2, 3, 5, 7, 11, 13,…} be the set of all primes and let S = {3, 5, 7,…} be the set of odd primes. Then S can be divided into two mutually

disjoint subsets having primes of the form 4n+1, 4n+3 and the set {5, 7, 11, 13; 17,…} can also be divided into two subsets having prime numbers of the form 6n+1 and 6n+5, n = 0, 1, 2,…

Theorem 1.3 The primes of the form (4n+3) are infinite in number.

Proof :- If possible, suppose primes of the form 4n+3 are finite and let they be $p_1 \cdot p_2,\ldots p_r$

Consider $N = 4\, p_1.p_2\ldots p_r - 1$. Then $N > 1$

So N can be written as the product of primes. Now N is odd, $N \neq 2$.

Thus N can be written as a product of odd primes, so N can be written as a product of primes of the form (4n+1) and (4n+3). But if N were divisible by primes of the form (4n+1) then N would also be of the form (4n+1). But N is of the form (4n+3), so N is divisible by atleast one prime of the form (4n+3) say p. But only primes of form (4n+3) are $p_1, p_2,\ldots, p_r$, Then $p = p_i$ for some i

Now $p \mid N$ and $p \mid p_1\ldots p_r \Rightarrow p \mid [4(p_1 \cdot p_2\ldots p_r) - N] \Rightarrow p \mid 1$, which is a contradiction

Hence, Number of primes of the form (4n+3) are infinite in number.

Theorem 1.4 The number of primes of the form (6n+5) are infinite in number.

Proof :- If possible, let number of primes of the form (6n+5) are finite and let these be $p_1, p_2\ldots p_r$.

Let $N = 6(p_1\ldots p_r) - 1$. Then $N > 1$ so N can be written as a product of primes.

$\therefore$ N can be written as a product of primes of the form (6n+1) and (6n+5). If N were divisible by primes of the form (6n+1) only, then N would be of the form (6n+1), so N is divisible by atleast one prime of the form (6n+5) say p.

But only primes of the form (6n+5) are $p_1, p_2,\ldots, p_r$, so $p = p_i$ for some i

Now $p \mid N$ and $p \mid p_i\, p_2\ldots p_r$, so $p \mid [6(p_1 \cdot p_2\ldots p_r) - N] \Rightarrow p \mid 1$, which is a contradiction

Hence number of primes of the form (6n+5) are infinite in number.

Note :- If gcd(a, b) = 1 Then every odd prime factor of $a^2 + b^2$ must be of the form 4n + 1.

For example gcd (4, 3) = 1, $4^2 + 3^2 = 25$ has an odd prime factor say 5 of the form 4n+1

Theorem 1.5 Primes of the type (4n+1) are infinite in number.

Proof :- If possible let $p_1, p_2,\ldots p_r$ be the only primes of the type (4n+1).

Consider $N = (2p_1\, p_2\ldots p_r)^2+1$

Now N is of the type $a^2 + b^2$ and gcd(a, b) = 1. Also N is odd so $2 \nmid N$ and all the prime factors of N are odd, so all the odd prime factors of N must be of the form (4n+1) Let $p \mid N$. Then p will be of the form (4n+1) But the only primes of the form (4n+1) are $p_1, p_2, \ldots, p_r$, $p = p_i$ for some i

Then $p \mid N$ and $p \mid (2p_1 \ldots p_r)^2$ i.e. $p \mid 1$, which is a contradiction. Hence number of primes of the form (4n+1) are infinite in number.

Theorem 1.6 Primes of the type 8n+5 are infinite in number

Proof :- If possible, let $p_1, p_2, \ldots, p_r$ be the only primes of the form (8n+5)

Consider $N = (p_1 p_2 \ldots p_r)^2 + 4 = (p_1 p_2 \ldots p_r)^2 + 2^2$

Then N is of the form $a^2 + b^2$ and $2 \nmid p_1 \cdot p_2 \ldots p_r$ implies g.c.d(a, b) = 1. Also N is odd, every prime factor of N must be of the form 4n+1. Now we know that square of every odd number is of the type 8n+1. Since $(2n+1)^2 = 4n^2 + 4n+1 = 4n(n+1)+1 = 8k + 1$, and so N is of the form 8k +5.

Now if every prime factor of N is of the type 8n+1 then their product N will also be of the form 8n+1 since $[(8n_1 + 1)(8n_2+1) = 64n_1n_2 + 8(n_1 + n_2) +1 = 8[8n_1n_2 + (n_1 + n_2)] + 1 = 8k + 1$

But N is of the form 8n+5 and so atleast one factor of N must be of the type 8n+5 say p. Therefore $p = p_1$ for some i. Now $p \mid N$ and $p \mid (p_1 \cdot p_2 \ldots P_r)^2$

$\Rightarrow$ $p \mid [N - (p_1 \cdot p_2 \ldots p_r)^2]$

$\Rightarrow$ $p \mid 4 \Rightarrow p \leq 4$.

But the smallest prime of the form 8n+5. So this is a contradiction and therefore primes of the type 8n+5 are infinite in number.

Fermat numbers

A French mathematician Fermat conjectured that $Fn = 2^{2^n} + 1$ represents primes for all values of $n \geq 0$

Note that $F_0 = 2^{2^0} + 1 = 3$

$F_1 = 2^{2^1} + 1 = 5$, $F_2 = 2^{2^2} + 1 = 17$

$F_3 = 2^{2^3} + 1 = 257$, $F_4 = 65537$ are all primes. These numbers are called Fermat numbers. A Fermat number which is a prime is called a Fermat prime. However no Fermat primes are known beyond F_4. In 1732, Euler proved that F_5 is composite. However his proof was very complicated. We give an easy proof due to Burmet.

Theorem 1.7 $F_5 = 2^{2^5} + 1$ is composite

Proof :- Let $a = 2^7 = 128$ and b = 5

then $a = b^3 + 3$ or $a - b^3 = 3$

Now $1 + ab - b^4 = 1+b(a-b^3)$

$= 1 + 3b = 16 = 2^4$

and $F_5 = 2^{2^5} + 1 = (2^{2^3})^{2^2} + 1 = (2^8)^4 + 1$

$= (2^1 \cdot 2^7)^4 + 1 = (2a)^4 + 1 = 16a^4 + 1 = (1+ ab-b^4)\, a^4 + 1$

$= (1+ab)\, a^4 + (1-a^4\, b^4)$

$= (1+ab)\, a^4 + (1 +ab)\, (1-ab)\, (1+a^2b^2)$

$= (1 +ab)\, [a^4 + (1-ab)\, (1+a^2\, b^2)]$

Thus $1 + ab = 1+128\cdot5 = 641$ is a divisor of F_5. Clearly $f_5 > 641$ and so F_5 is composite.

Remark :- We have not been able to find any Fermat prime number beyond F_4 and research is still on. However it is conjectured that F_n is not a prime for $n > 4$. But Fermat's number have very interesting properties.

Theorem 1.8 All Fermat numbers are relatively prime to each other i.e.,

$$\gcd(F_m, F_n) = 1 \text{ for } m \neq n$$

Proof :- W. L. O. G., we assume that $m > n$

Let $m = n + k$ where $k \geq 1$

Now $F_m = F_{n+k} = 2^{2^{n+k}} + 1 = (2^{2^n})^{2^k} + 1$

Set $x = 2^{2^n}$

Then $F_m = (x)^{2^k} + 1$

Now $$\frac{F_m - 2}{F_n} = \frac{(x)^{2^k} + 1 - 2}{x + 1}$$

$$= \frac{x^{2^k} - 1}{x + 1}$$

$$= \frac{(x^{2^{k-1}} + 1)(x^{2^{k-1}} - 1)}{x + 1}$$

$$= \frac{(x^{2^{k-1}} + 1)(x^{2^{k-2}} + 1)(x^{2^{k-3}} + 1)\ldots(x - 1)(x + 1)}{x + 1}$$

$\Rightarrow$ $F_n \mid (F_m - 2)$

Let $\gcd(F_m, F_n) = d$, then $d \mid F_m$, $d \mid F_n$ and $F_n \mid (F_m - 2)$

$\Rightarrow$ $d \mid (F_m - 2)$ and therefore $d \mid [F_m - (F_m - 2)]$ i.e., $d \mid 2$

$\Rightarrow$ d = 1 or 2. But $d \neq 2$ since all Fermat's number are odd.

Hence d = 1 and this proves the theorem.

Corollary 1 (Euclid) :- The number of primes is infinite.

Proof :- Let n be any natural number. Consider $F_1, F_2, \ldots F_n$. Each of $F_i > 1$ and so each F_i has a prime factor. Let $p_1 \mid F_1$, $p_2 \mid F_2, \ldots p_n \mid F_n$, where p_1, $p_2 \ldots p_n$ are primes.

Since all Fermat numbers are relatively prime i.e., $(F_i , F_j) = 1$ so $p_i \neq p_i$ for $i \neq j$

So all the p_i's are distinct primes. Thus given any natural number n, there exists at least n different primes and so the number of primes is infinite.

Corollary 2 :- $p_{n+1} \leq 2^{2^n} + 1 = F_n$, where p_i denotes the i th prime in ascending order

Proof :- Since each F_i is divisible by a different prime and $F_1 < F_2 < F_3 < \ldots < F_n$, so there exists at least n primes $\leq F_n$.

But all Fermat numbers are odd and prime 2 is less than all odd primes so at least (n+1) primes are less than F_n, i.e., $p_{n+1} \leq Fn$

Example :- Prove that for $n \geq 2$, $10 \mid F_n - 7$

or $F_n \equiv 7 \pmod{10}$

Solution :- We shall prove the exercise by induction on n.

For n = 2, $F_2 = 2^{2^2} + 1 = 17$

and $10 \mid (17 - 7)$

$\therefore$ exercise is true for n = 2

Assume that exercise is true for n = k

i.e., $10 \mid (F_k - 7)$

i.e., $10 \mid (2^{2^k} + 1 - 7)$

i.e., $10 \mid (2^{2^k} - 6)$

i.e., $2^{2^k} - 6 = 10r, \quad$ for $r \in Z$ …(1)

Now $2^{2^{k+1}} = (2^{2^k})^2 = (10r + 6)^2$

$= 100\, r^2 + 120r + 36.$

$= 10(10r^2 + 12r + 3) + 6$

$$= 10r^1 + 6 \text{ where } r^1 = 10r^2 + 12r + 3$$

$\therefore \quad 2^{2^{k+1}} - 6 = 10r^1 \quad \Rightarrow 10 \mid (2^{2^{k+1}} - 6)$

$\Rightarrow \quad 10 \mid [2^{2^{k+1}} + 1 - 7]$

$\Rightarrow \quad 10 \mid (F_{k+1} - 7)$

Thus by mathematical induction exercise is true for all natural numbers n.

Mersenne Numbers

Let p be any prime then number of the form

$M_p = 2^p - 1$ are called Mersenne numbers. A Mersenne number which is also a prime is called a Mersenne prime.

Theorem 1.9 Let $a \geq 2$ and $n \geq 2$ be natural number. Let $a^n - 1$ be a prime. Then $a = 2$ and $n = p$ for some prime number p or Any prime number of the type $a^n - 1$ must be a Mersenne prime

Proof :- Since $a^n - 1 = r$ is a prime so it cannot have any factor q such that $1 < q < r$

Now $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \ldots + a^2 + a + 1)$

i.e., $(a-1) \mid (a^n - 1)$

But $a \geq 2, n \geq 2$

If $a > 2$ then $a - 1 > 1$ is a factor of $a^n - 1$ giving a contradiction

$\Rightarrow \quad a = 2$

Again suppose n is composite

$\Rightarrow$ there exists p, q with $1 < p < n$, $1 < q < n$ such that $n = pq$

Now $a^n - 1 = a^{pq} - 1 = (a^q)^p - 1^p$

$$= (a^q - 1)[(a^q)^{p-1} + (a^q)^{p-2} + \ldots + a + 1)$$

Now since $a = 2$, $1 < q < n$

$\therefore \; 1 < a^q - 1 < a^n - 1$, is a factor of $a^n - 1$

This implies that $a^n - 1$ is composite which is a contradiction. So n must be prime.

Remark :- Converse of above theorem need not be true

For example.

$2^{11} - 1$ is not a prime. So $2^p - 1$ need not be a prime for all primes p

Remark :- In 1644, Mersenne conjectured that M_p is prime for

$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$

and composite for all other primes up to 257

Later on it was discovered that he has made some mistakes. In fact, today, we know that M_p is prime for

$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 257, 521, 607, 1279, 2281.$

as and so on and composite for all other primes ≤ 2281

Thus he had made five mistakes i.e., for

$p = 61, 67, 89, 107$ and 257, i.e., M_p is prime for

61, 89, 107 but composite for

$p = 67, 257.$

Theorem 1.10 If $a \geq 2$ and $n \geq 2$ and $a^n + 1$ is a prime, then $n = 2^k$ for some $k \geq 1$ and a is even.

Proof :- If a is odd then $a \geq 2 \Rightarrow a \geq 3$ and so $a^n + 1$ is an even number which is greater than or equal to 4 and so can not be a prime number. So for $a^n + 1$ to be a prime, a must be even.

Next we claim that no odd prime divides n, if possible, let an odd prime p divides n, then $n = pq$ where $1 < q < n$ and p is an odd prime. Therefore $a^n+1 = a^{pq} + 1 = (a^q)^p + 1^p$.

$\therefore \quad = (a^q+1)\,(a^{(p-1)} - a^{(p-2)} + \ldots - 1)$

Also $\quad 1 < a^q + 1 < a^n + 1$, so that $a^q + 1$ is a proper divisor of $a^n + 1$

$\Rightarrow \quad a^n + 1$ can not be a prime which is a contradiction.

$\therefore$ n must be a power of 2. [no odd prime divides n $\Rightarrow$ only $2 \mid n \Rightarrow n = 2^k$]

Theorem 1.11 Let $n > 1$ be a natural number, then n is composite iff n contains a prime factor $p \leq \sqrt{n}$

Proof :- Let n be composite and p be the smallest prime divisor of n where $n = pq$. Then $q \geq p$ Therefore $n = pq \geq p^2$

$[\Theta\ q \geq p]$

$\Rightarrow \quad p^2 \leq n \Rightarrow p \leq \sqrt{n}$

Thus to determine whether n is a prime number or not, it is sufficient to find out all primes $\leq \sqrt{n}$ and check whether any one of these primes divides n or not. If there is no divisor among these primes then n must be a prime number itself. In this sieve it is essential to find out all primes $\leq \sqrt{n}$.

Farey Series

Let $n \geq 1$ be any natural number. For every n, the set of fractions h/k such that $0 \leq h/k \leq 1$, $1 \leq k \leq n$ written in ascending order of magnitude is called Farey series of order n and will be denoted by Fn.

Construction of Farey Series :-

F_1 $\quad \frac{0}{1} \qquad\qquad\qquad\qquad\qquad\qquad \frac{1}{1}$

F_2 $\quad \frac{0}{1} \qquad\qquad \frac{1}{2} \qquad\qquad\qquad \frac{1}{1}$

F_3 $\quad \frac{0}{1} \qquad \frac{1}{3} \qquad \frac{1}{2} \qquad \frac{2}{3} \qquad\qquad \frac{1}{1}$

F_4 $\quad \frac{0}{1} \quad \frac{1}{4} \quad \frac{1}{3} \qquad \frac{1}{2} \qquad \frac{2}{3} \qquad \frac{3}{4} \qquad \frac{1}{1}$

Theorem 1.12 If $\frac{h}{k}, \frac{h}{k}$ are two consecutive members of Fn then

(a) $(k + k') > n$

(b) $k \neq k'$ if $n > 1$

Proof :- W.L.O.G. we assume that

$$\frac{h}{k} < \frac{h}{k}$$

We claim $\quad \frac{h}{k} < \frac{h+h}{k+k} < \frac{h}{k}$ …(1)

Now $\quad \frac{h}{k} < \frac{h+h}{k+k} \Leftrightarrow h\,k' < kh' \Leftrightarrow \frac{h}{k} < \frac{h}{k}$

and the last inequality is true by assumption. In a similar way,

$$\frac{h+h}{k+k} < \frac{h}{k}$$

so that the inequalities (1) are satisfied.

Proof (a) :- If possible, let $(k + k') \leq n$. Since $h \leq k$ and $h' \leq k' \Leftrightarrow h + h' \leq k + k'$

$\Rightarrow \quad \left(\frac{h+h}{k+k}\right) \in F_n$

$\Rightarrow$ A fraction $\frac{h+h}{k+k}$ lies between two consecutive fractions $\frac{h}{k}, \frac{h}{k}$ of Fn which is a contradiction

So $(k + k') > n$

Proof (b) :- If possible, let $k = k'$ where h/k and h'/k' are two consecutive fractions of Fn for some n. We note that $\frac{0}{1}$ and $\frac{1}{1}$ are the only two fractions with denominator 1.

Then $\frac{h}{k} \neq 1 \neq \frac{h}{k} = \frac{h}{k}$

$\therefore\ h < h' < k$

But h, h′, k are integers, so $h + 1 \leq h' \leq k - 1 < k$ …(II)

Now we claim

$$\frac{h}{k} < \frac{h}{k-1} < \frac{h+1}{k} \leq \frac{h}{k}$$ …(III)

To prove this we note $\frac{h}{k} < \frac{h}{k-1}$ and $\frac{h+1}{k} \leq \frac{h}{k}$ are clear

So it remains to prove that $\frac{h}{k-1} < \frac{h+1}{k}$

or $hk < (h+1)(k-1)$

or $hk < hk + k - h - 1$

i.e., $(k - h - 1) > 0$. i.e., $k > h + 1$ which is true by (II)

All the inequality in (III) are proved thus we have a fraction $\frac{h}{k-1}$ in Fn which lies between two consecutive fractions $\frac{h}{k}$ and $\frac{h}{k}$, which is a contradiction. So, we can not have $k = k'$ if $n > 1$

Theorem 1.13 Let h/k and h'/k' be two successive members of F_n

$$\frac{h}{k} < \frac{h}{k}$$

Then $h'k - h\,k' = 1$ …(I)

Proof :- Since $h/k < h'/k' \Rightarrow \frac{h}{k}$ is not the last function of fn

$$\Rightarrow \qquad 0 \le \frac{h}{k} < 1 \qquad \ldots(II)$$

Also g.c.d.(h, k) = 1

$\Rightarrow \exists$ integers x & y such that

$$kx - hy = 1 \qquad \ldots(III)$$

Now let (x_0, y_0) be a solution of (III). Then clearly $(x_0 + rh, y_0 + rk)$ is also a solution of (III) for every integer r. Then taking different values of r, the entire real line is divided into intervals of length k each

$$\underset{y_0-rk}{\times} \quad \underset{y_0-k}{\times} \quad \underset{y_0}{\times} \quad \underset{y_0+k}{\times} \quad \underset{y_0+rk}{\times}$$

Choose a value of r such that

$$0 \le n - k < y = y_0 + rk \le n \qquad \ldots(IV)$$

and such that

$$(x = x_0 + rh,\ y = y_0 + rk) \text{ is a solution of (III)}$$

Now dividing (III) by k, we get

$$x = \frac{1}{k} + \frac{h}{k} y \text{ so that } 0 < \frac{1}{k} \le x < 1+y$$

Thus $1 \le x \le y \le n$

Further from (III), g.c.d (x, y) = 1 so that

$$\frac{x}{y} \in F_n$$

Now dividing by ky in (III), we get

$$\frac{x}{y} = \frac{h}{k} + \frac{1}{ky} > \frac{h}{k}$$

$\therefore$ In F_n, $\frac{x}{y}$ occur after h/k

We claim, $\frac{x}{y} = \frac{h}{k}$

Suppose it is not true. Then x/y must occur after h′/k′, as h/k and h′/k′ are consecutive fraction of F_n. So that we must have x/y > h′/k′ > h/k

Now $$\frac{x}{y} - \frac{h}{k} = \frac{k\,x - h\,y}{k\,y} \ge \frac{1}{k\,y} \qquad \ldots(V)$$

as x/y > h′/k′ and so the numerator must be positive

Similarly, $h'/k' - h/k = \frac{h\,k - hk}{kk} \ge \frac{1}{kk}$ $\qquad \ldots(VI)$

Adding (V) & (VI) we get

$$\frac{x}{y}-\frac{h}{k}\geq\frac{1}{k\,y}+\frac{1}{kk}=\frac{k+y}{kk\,y}>\frac{n}{kk\,y} \qquad [\text{By (IV)}]$$

$$>\frac{1}{k\,y} \qquad (\Theta\ k'\leq n)$$

But by (III), $\frac{x}{y}-\frac{h}{k}=\frac{1}{k\,y}$, which is a contradiction

So, we must have $\frac{x}{y}=\frac{h}{k}$

Since $y > 0$, $k' > 0$, $\gcd(x,y) = 1$, $\gcd(h', k') = 1$

So, we must have

$$x = h'.\ y = k'$$

But (x, y) satisfies (III). So we must have $k\,h' - hk' = 1$, which proves (I)

Remark :- 1. The chice of r gives us an actual method to find next fraction h'/k' of F_n, if fraction h/k is given

2. $h/k < h'/k' \Leftrightarrow 1-h'/k' < 1-h/k$

Further h/k and h'/k' are consecutive fraction of F_n. So $1-h'/k'$ and $1-h/k$ are also consecutive fraction of F_n, in reverse order.

Theorem 1.14 Let $\frac{h}{k},\frac{h}{k}$ be two consecutive terms of F_n such that $\frac{h}{k},\frac{h}{k},\frac{h}{k}$ be consecutive terms of F_r such that $r > n$. Then

$$\frac{h}{k}=\frac{h+h}{k+k}$$

Proof :- Since $\frac{h}{k},\frac{h}{k}$ are consecutive terms of F_r with $\frac{h}{k}<\frac{h}{k}$ and so

$$h''k - hk'' = 1 \qquad \ldots(I)$$

Also $\frac{h}{k},\frac{h}{k}$ are consecutive terms of F_r and $\frac{h}{k}<\frac{h}{k}$

and so $h'\,k'' - h''\,k' = 1$ …(II)

From (I) and (II), we get

$$h''k - hk'' = h'k'' - h''k'$$

$\Rightarrow$ $h''(k + k') = k''(h + h')$

$$\Rightarrow \qquad \frac{h}{k} = \frac{h+h}{k+k}$$

Now consider $(h + h')k - (k + k')h = hk + h'k - kh - k'h$

$$= h'k - k'h = 1 \qquad \ldots(III)$$

From (III) we conclude that $\gcd(h + h', k + k') = 1$

Also $\gcd(h'', k'') = 1$ as $\frac{h}{k} \in F_r$ and so

$$\frac{h}{k} = \frac{h+h}{k+k} \Rightarrow h'' = h + h' \text{ and } k'' = k + k'.$$

Theorem 1.15 Let $\frac{h}{k}$ and $\frac{h}{k}$ be two consecutive Farey fractions with $\frac{h}{k} < \frac{h}{k}$, then $\frac{h+h}{k+k}$ is the unique fraction with the smallest denominator among all fractions between $\frac{h}{k}$ and $\frac{h}{k}$.

Proof :- Let $\frac{x}{y}$ be any fraction such that

$$\frac{h}{k} < \frac{x}{y} < \frac{h}{k}$$

Then
$$\frac{h}{k} - \frac{h}{k} = \left(\frac{h}{k} - \frac{x}{y}\right) + \left(\frac{x}{y} - \frac{h}{k}\right)$$

$$= \left[\frac{h\ y - k\ x}{k\ y}\right] + \left[\frac{kx - hy}{ky}\right]$$

Since $\frac{x}{y} < \frac{h}{k}$, $\left(\frac{h}{k} - \frac{x}{y}\right) > 0$ and so $(h'y - k'x) \geq 1$ as h', k', x, y are all integers.

Similarly $(kx - hy) \geq 1$

$$\therefore \qquad \frac{h}{k}\ \frac{h}{k} \geq \frac{1}{k\ y} + \frac{1}{ky} = \frac{k+k}{kk\ y} \qquad \ldots(1)$$

But $\frac{h}{k} - \frac{h}{k} = \frac{h\ k - k\ h}{k\,k} = \frac{1}{k\,k}$, since $\frac{h}{k}$ and $\frac{h}{k}$ are consecutive Farey fractions, $\ldots(2)$

From (1) and (2)

$$\frac{1}{kk} \geq \frac{k+k}{kk\ y} \Rightarrow y \geq (k + k') \qquad \ldots(3)$$

Since we know

$$\frac{h}{k} < \frac{h+k}{k+k} < \frac{h}{k}, \text{ so}$$

there exist a fraction lying with $\frac{h}{k}$ and $\frac{h}{k}$ whose denominator is $k + k'$

So if x/y is a fraction lying between $\frac{h}{k}$ and $\frac{h}{k}$, we should not have $y > (k+k')$.

So we must have, $y = k + k'$ in (3). But the equality in (3) will hold only when equality holds in (I) through out. $\Rightarrow$ We have

$$h'y - k'x = 1 \quad \text{and} \quad kx - hy = 1$$

or $$h'y - k'x = kx - hy \Rightarrow (k + k')x = (h + h')y$$

$\Rightarrow$ $$y = k + k'$$

Theorem 1.16 If $F_n = \left\{\frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_r}{b_r}\right\}$

Then (i) $$r = 1 + \sum_{j=1}^{n} \phi(j)$$

(ii) $$\sum_{i=1}^{r} \frac{a_i}{b_i} = \frac{1}{2}\left(1 + \sum_{j=1}^{n} \varphi(j)\right) \text{ and}$$

(iii) $$\sum_{j=1}^{r-1} (b_j \times b_{j+1})^{-1} = 1$$

Proof :- (i) $$r = 1 + \sum_{j=1}^{n} \phi(j)$$

We shall prove the result by induction on n and we know that $\frac{0}{1}$ and $\frac{1}{1}$ are the only terms in F_1 so that the result is true for n = 1. Assume that the result is true for all natural number <n.

Consider F_n. Now F_n contains all terms of F_{n-1} plus those fractions h/k such that gcd(h,n)=1,

$\therefore$ By definition the number of extra terms is $\phi(n)$

$\therefore$ Total number of terms on F_n = the number of terms in $F_{n-1} + \phi(n)$

$$= 1 + \sum_{j=1}^{n-1} \phi(j) + \phi(n)$$

$$= 1 + \sum_{j=1}^{n} \phi(j)$$

(ii) $$\sum_{i=1}^{r} \frac{a_i}{b_i} = \frac{1}{2}\left\{1 + \sum_{j=1}^{n} \varphi(j)\right\}$$

We know $\frac{h}{k} \in F_n \Leftrightarrow \left(1 - \frac{h}{k}\right) \in F_n$

So, we write the terms $\frac{a_i}{b_i}$ (i = 1, 2,…,r) in a row

$\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, ..., \frac{a_r}{b_r}$ and

$1 - \frac{a_1}{b_1}, 1 - \frac{a_2}{b_2}, ..., 1 - \frac{a_r}{b_r}$, in the second row, we write $1 - \frac{a_i}{b_i}$ underneath $\frac{a_i}{b_i}$

As $\frac{a_i}{b_i}$ runs over terms of F_n, $1 - \frac{a_i}{b_i}$ must also run over terms of F_n in the opposite order. Now adding the two rows horizontally.

So if $S = \sum_{i=1}^{r} \frac{a_i}{b_i}$ then $2S = r \Rightarrow S = \frac{1}{2} r = \frac{1}{2}\left\{1 + \sum_{j=1}^{n} \phi(j)\right\}$

(iii) We know that the last term of function is $\frac{1}{1}$ and the first term is $\frac{0}{1}$ so that

$$\frac{a_r}{b_r} = 1 \text{ and } \frac{a_1}{b_1} = 0$$

Now $1 = \frac{a_r}{b_r} = \left(\frac{a_r}{b_r} - \frac{a_{r-1}}{b_{r-1}}\right) + \left(\frac{a_{r-1}}{b_{r-1}} - \frac{a_{r-2}}{b_{r-2}}\right)$

$$+ \left(\frac{a_{r-2} - b_{r-3}}{b_{r-2} - b_{r-3}}\right) + ... + \left(\frac{a_2 - a_1}{b_2 - b_1}\right) + \frac{a_1}{b_1}$$

But we know that if $\frac{h}{k}, \frac{h}{k}$ are consecutive terms with $\frac{h}{k} < \frac{h}{k}$, then $h'k - hk' = 1$

Let us calculate,

$$\frac{a_i}{b_i} - \frac{a_{i-1}}{b_{i-1}} = \frac{a_i b_{i-1} - a_{i-1} b_i}{b_i b_{i-1}}$$

$$= \frac{1}{b_i b_{i-1}} = (b_i\, b_{i-1})^{-1}$$

Therefore, $1 = \sum_{j=1}^{r-1} (b_j\, b_{j+1})^{-1} + \frac{a_1}{b_1}$

$$\left[\Theta \frac{a_1}{b_1} = 0\right]$$

$$= \sum_{j=1}^{r-1} (b_j\, b_{j+1})^{-1}$$

Definition :- Let $\frac{h}{k}$ & $\frac{h}{k}$ be two consecutive Farey fractions of function such that $\frac{h}{k} < \frac{h}{k}$

Then $\frac{h+h}{k+k}$ is called a mediant of order n.

Note that g.c.d. $(h + h', k + k') = 1$ and $(k + k') \geq n + 1$

so the mediant of order n does not belong to F_n.

Further, we know

$$\frac{h}{k} < \frac{h+h}{k+k} < \frac{h}{k}$$

The mediant $\frac{1}{n+1} = \frac{0+1}{1+n}$ lying between $\frac{0}{1}$ and $\frac{1}{n}$ is called the first mediant of order n and the mediant

$$\frac{n}{n+1} = \frac{(n-1)+1}{n+1} \text{ lying between } \frac{n-1}{n} \& \frac{1}{1}$$

is called the last mediant of order n. If we represent all Farey fractions of order n on the unit circle, the totally of all these points on the unit circle is called Farey Dissection of the unit circle of order n.

Definition :- The arc of the unit circle bounded by mediant of order n of next mediant of order n is called a Farey arc of order n.

Remark :- Let $\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \frac{a_4}{b_4}$ be consecutive Farey fractions of order n.

Then $$\frac{a_1}{b_1} < \frac{a_1+a_2}{b_1+b_2} < \frac{a_2}{b_2} < \frac{a_2+a_3}{b_2+b_3} < \frac{a_3}{b_3} < \frac{a_3+a_4}{b_3+b_4} < \frac{a_4}{b_4}$$

Then the Farey arc bounded by $\frac{a_1+a_2}{b_1+b_2} \& \frac{a_2+a_3}{b_2+b_3}$ contains a Farey fraction $\frac{a_2}{b_2}$ and the Farey arc bounded by $\frac{a_2+a_3}{b_2+b_3} \& \frac{a_3+a_4}{b_3+b_4}$ contains the Farey fraction $\frac{a_3}{b_3}$ and so on.

Thus each Farey arc contains one & only one Farey fraction.

The Farey arc bounded by the last mediant n/n+1 and the first mediant 1/n+1 contains by convention the Farey fraction $\frac{0}{1}$

Theorem 1.17 Let $x = \frac{h}{k} \in F_n$ $(n > 1)$

Let x be represented by the point P_x on the unit circle. Suppose P_x lies on the Farey arc bounded by the points P_μ, $P_{\mu'}$, where μ and μ' are the mediants. Then the length of each of the arcs $P\mu\ Px$ and $P\mu'\ Px$ lies between

$$\frac{1}{k(2n-1)} \& \frac{1}{k(n+1)}$$

Proof :- We shall distinguish two cases

Case I :- $x = \frac{0}{1}$ or $\frac{1}{1}$

Then x lies on the Farey are bounded by $\frac{n}{n+1} \& \frac{1}{n+1}$. and the length of

$$P_\mu P_x = \frac{1}{n+1} = \text{length of } P_x P_{\mu'}$$

Case II $x \neq \frac{0}{1}$ & $x \neq \frac{1}{1}$

Then $x = \frac{h}{k}$ is neither the first fraction nor the last fraction of F_n. So $\exists$ Farey fractions $\frac{h_1}{k_1}$ & $\frac{h_2}{k_2}$ such that

$$\frac{h_1}{k_1} < \frac{h}{k} < \frac{h_2}{k_2}$$

Then $\frac{h}{k}$ lies on the Farey arc bounded by

$$\mu = \frac{h_1 + h}{k_1 + k} \text{ and } \frac{h + h_2}{k + k_2} = \mu'$$

Thus $$P\mu Px = \frac{h}{k} - \frac{h_1 + h}{k_1 + k} = \frac{h(k_1 + k) - k(h_1 + h)}{k(k_1 + k)}$$

$$= \frac{h k_1 - k h_1}{k(k_1 + k)} = \frac{1}{k(k_1 + k)}$$

Since $\frac{h_1}{k_1} \& \frac{h}{k}$ are consecutive fraction of function with

$$\frac{h_1}{k_1} < \frac{h}{k} \text{ and } k \neq k.$$

$\Rightarrow$ maximum value of $k + k_1$ is $2n-1$ and $(k + k_1) \geq n + 1$

$\Rightarrow$ $$\frac{1}{k(2n-1)} \leq P\mu Px \leq \frac{1}{k(n+1)}$$

Similarly, $\frac{1}{k(2n-1)} \leq Px\ P\mu' \leq \frac{1}{k(n+1)}$.

Remark :- We have already proved that given any real number α and an integer $t \geq 1$, there exists integers x & y such that

$$|\alpha x - y| < \frac{1}{t} \ \& \ 0 < x \leq t.$$

Theorem 1.18 Given any real number α and an integer $t \geq 1$, $\exists$ integers x & y such that $0 \leq x < t$ and $|\alpha x - y| \leq 1/t+1$

Proof :- Theorem is obvious if $\frac{1}{t+1} \geq |\alpha x - y|$

$$= |(\alpha + n)x - (nx + y)|$$

So if theorem is true for α, the above expression shows that it is also true for all real number $\alpha + n$, where n is any integer.

So w.l.o.g. assume $0 < \alpha < 1$. i.e., we shall consider only the fractional part of α if $0 < \alpha < 1$ is not satisfied. Since $t \geq 1$, we consider Farey series F_t. For $t = 1$, theorem is obvious.

Now assume $t > 1$. Since $0 < \alpha < 1$, there are two Farey fractions $\frac{h_1}{k_1}$ & $\frac{h_2}{k_2}$ such that $\frac{h_1}{k_1} < \alpha < \frac{h_2}{k_2}$, and $\exists$ mediants μ such that either $\alpha \in P_{\frac{h_1}{k_1}} P_\mu$ or

$$\alpha \in P_\mu \; P_{\frac{h_2}{k_2}}$$

where $P_\mu,\ P_{\frac{h_1}{k_1}},\ P_{\frac{h_2}{k_2}}$

represent the points on the unit circle respectively

$$\text{If } \alpha \in P_{\frac{h_1}{k_1}} P_\mu, \text{ then } P_{\frac{h_1}{k_1}} P_\mu \le \frac{1}{k_1(t+1)} \text{ and } 1 \le k_1 \le t$$

Since $\frac{h_1}{k_1}$ is a Farey fraction of order t.

Then $$\left| \alpha - \frac{h_1}{k_1} \right| \le \frac{1}{k_1(t+1)}$$

or $$|\alpha k_1 - h_1| \le \frac{1}{t+1}$$

Similarly, if $\alpha \in P_\mu P_{\frac{h_2}{k_2}}$, we can show

$$|\alpha k_2 - h_2| \le \frac{1}{t+1}$$

Hence the theorem.

Approximation of Irrational numbers by rationals.

Pigeon hole Principle :- This principle states that if (n+1) objects are to be divided into n classes (may be empty) then at least one class will contain at least two objects

Definition :- Let α be any real number. Then we define

$$\{\alpha\} = \text{Fractional part of } \alpha$$

$$= \alpha - [\alpha]$$

where $[\alpha]$ is greatest integer $\le \alpha$. Then by definition

$$0 \le \{\alpha\} < 1 \qquad \forall\ \alpha$$

Theorem 1.19 Let α be any given real number, then for every integer $t > 0$, there exists integer x, y such that

$$|\alpha x - y| < \frac{1}{t} \text{ and } 0 < x \le t$$

Proof :- Take the interval [0, 1). Divide this interval into t subintervals i.e.

$$\left[0, \frac{1}{t}\right), \left[\frac{1}{t}, \frac{2}{t}\right) \ldots \left[\frac{t-1}{t}, 1\right).$$ All these subintervals are mutually disjoint.

Consider the real numbers,

$$\{0 \cdot \alpha\}, \{1, \alpha\}, \ldots \{t \cdot \alpha\} \qquad \ldots(*)$$

These are (t +1) real numbers and we have only t sub-intervals. So at least one sub-interval consists at least two of (t + 1) real nos given in (*)

So there exists two distinct integers i & j such that

$$|\{j \cdot \alpha\} - \{i \cdot \alpha\}| < 1/t \text{ and } 0 \le i < j \le t$$

Now by definition $\{j \cdot \alpha\} = j\alpha - y_1$ for some integer y_1 and $\{i \cdot \alpha\} = i\alpha - y_2$ for some integer y_2

$$\therefore \quad \frac{1}{t} > |\{j \cdot \alpha\} - \{i \cdot \alpha\}| = |(j\alpha - y_1) - (i\alpha - y_2)|$$

$$= |(j - i)\alpha - (y_1 - y_2)|$$

Set $x = j - i$ and $y = y_1 - y_2$ Since $0 \le i < j \le t$, so $0 < j - i \le t$ i.e. $0 < x \le t$

and

$$|\alpha x - y| < 1/t$$

Remark :- Given real α and integer $t > 0$, we can find integers x & y such that

$$|\alpha x - y| < 1/t, \quad \text{g.c.d. } (x, y) = 1 \ \& \ 0 < x \le t$$

Proof :- By the theorem, we can find integers x_1 & y_1 such that

$$|\alpha x_1 - y_1| < \frac{1}{t} \text{ and } 0 < x_1 \le t$$

If g c d $(x_1, y_1) = 1$, we are through, so let gcd $(x_1, y_1) = d > 1$ and let $x_1 = dx$ & $y_1 = dy$

Then gcd (x, y) = 1

Now $|\alpha x - y| = \frac{1}{d} |\alpha x_1 - y_1| < \frac{1}{t d} < 1/t.$

Combining above theorem with remarks, we have

Theorem 1.20 Let α be any given real number and $t > 0$ be any given integer. Then there exists integers x and y such that gcd (x, y) = 1, $0 < x \leq t$ and

$$|\alpha x - y| < 1/t$$

Corollary :- Given any $\in > 0$, however small, there exists integers x and y such that $x > 0$

and $$\left| \alpha - \frac{y}{x} \right| < \in$$

(i.e. real number s are dense in rationals)

Proof :- Since $\in > 0$ is given choose an integer t such that $t > 1/\in$ Now there exists integers x & y, $x > 0$ such that

$$|\alpha x - y| < 1/t < \in$$

$\Rightarrow$ $$\left| \alpha - \frac{y}{x} \right| < \in / x < \in$$

Theorem 1.21 Given $\alpha > 0$, there exists integers x and y such that

$$\left| \alpha - \frac{y}{x} \right| < \frac{1}{x^2} \text{ \& gcd } (x, y) = 1$$

Proof :- We know that we can find integers x and y such that gcd(x, y) = 1, $0 < x \leq t$ (where $t > 0$ is any integer) and

$$|\alpha x - y| < 1/t$$

Then $$\left| \alpha - \frac{y}{x} \right| < \frac{1}{tx} \leq \frac{1}{x^2} \text{ since } x \leq t$$

Theorem 1.22 Let α be any rational number then $\exists$ only a finite number of pairs of integers (x, y) such that

$$x > 0, \text{ gcd}(x, y) = 1.$$

and $$\left| \alpha - \frac{y}{x} \right| < 1/x^2$$

Proof :- Since α is rational, let $\alpha = h/k$ where $k > 0$ & gcd (h, k) = 1 then

$$0 = |\alpha k - h| < 1/x^2$$

Thus there exists at least one pair (h, k) satisfying the given condition.

Let $\left|\alpha - \frac{y}{x}\right| < 1/x^2$ such that $x > 0$ & $(x, y) = 1$ …(1)

Then $|\alpha x - y| < 1/x$

$\Rightarrow$ $\alpha x - \frac{1}{x} < y < \alpha x + 1/x$

Here y lies in an interval of length $\frac{2}{x} \leq 2$, and so given x, y can take at most 3 values.

Further, setting $\alpha = \frac{h}{k}$ in (1) we get

$$\frac{1}{x^2} > \left|\frac{h}{k} - \frac{y}{x}\right| = \frac{|hx - ky|}{kx}$$

If $hx - ky \neq 0$, then $|hx - ky| \geq 1$

$\therefore$ $\frac{1}{x^2} > \frac{1}{kx} \Rightarrow k > x$

Also, $x > 0$

$\Rightarrow$ $0 < x < k$

and so x can take at most (k−1) values.

Thus the pair (x, y) can take at most 3(k−1) values

Theorem 1.23 Let α be any irrational number. Then $\exists$ infinitely many pairs (x, y) satisfying

$$\left|\alpha - \frac{y}{x}\right| < \frac{1}{x^2},\ x > 0 \text{ and } \gcd(x, y) = 1 \qquad \ldots(1)$$

Proof :- We know that there exists at least one pair (x, y) satisfying (1)

If possible, let there be only a finite number of pairs (x, y) satisfying (1) Let these pairs be

$(x_1, y_1), (x_2, y_2), \ldots, (x_r, y_r)$

Let $\in_i > |\alpha x_i - y_i|$ $(i = 1, 2, \ldots, r)$

Then each $\in_i > 0$ since α is irrational. Let $\in < \min(\in_1, \in_2 \ldots \in_r)$. Take $t > 1/\in$. Then there exists integers x, y such that

$$0 < x \le t,\ \gcd(x, y) = 1 \ \&\ |\alpha x - y| < 1/t < \in$$

Also $$\left|\alpha - \frac{y}{x}\right| < \frac{1}{tx} < \frac{1}{x^2} \qquad (\Theta\ 0 < x \le t)$$

$\therefore$ This pair (x, y) also satisfies (1) But $|\alpha x - y| < \in$ and so this pair $(x, y) \neq (x_i, y_i)$ for any i which is a contradiction

Combining all these results we get the following theorem

Theorem 1.24 Let α be any given real number then

(1) Given integer $t > 0$, there exists a pair of integers (x, y) such that $0 < x \le t$, $\gcd(x, y) = 1$ and

$$|\alpha x - y| \le 1/t$$

(2) Let α be any given real no. then $\exists$ pairs (x, y) such that $x > 0$, gcd (x, y) = 1 & $\left|\alpha - \frac{y}{x}\right| < 1/x^2$. Further the number of above pairs is finite if α i rational and the number of pairs is infinite if α is irrational.

Hurwitz's Theorem

Theorem 1.25 Given any irrational number ξ, there exist infinitely many pairs (h, k) of integers such that

$$\left|\xi - \frac{h}{k}\right| < \frac{1}{\sqrt{5}\,k^2} \qquad \ldots(I)$$

Proof :- Since $\left|\xi - \frac{h}{k}\right| < \frac{1}{\sqrt{5}k^2}$, $\Leftrightarrow$ $\left|(\xi + n) - \left(\frac{nk + h}{k}\right)\right| < \frac{1}{\sqrt{5}\,k^2}$

So w.l.o.g. we assume that $0 \le \xi < 1$. Further ξ is irrational, so $\xi \neq 0$, so we assume $0 < \xi < 1$

Let $n \in N$. Consider Farey series of order n.

Since ξ is irrational, $\exists$ two consecutive Farey fraction $\frac{a}{b}$ & $\frac{c}{d}$ of order n such that

$$\frac{a}{b} < \xi < \frac{c}{d}$$

Then either $$\xi < \frac{a + c}{b + d}$$

or $$\xi > \frac{a+c}{b+d}$$

First we shall prove that in either case at least one fraction out of a/b, $\frac{c}{d}$ & $\frac{a+c}{b+c}$ satisfy (1)

Suppose none of these fraction satisfy (1). Now to prove Hurtwitz theorem, we first prove a Lemma.

Lemma :- If x and y are positive integers then the following two inequalities

$$\frac{1}{xy} \geq \frac{1}{\sqrt{5}}\left(\frac{1}{x^2}+\frac{1}{y^2}\right) \qquad \ldots(2)$$

and $$\frac{1}{x(x+y)} \geq \frac{1}{\sqrt{5}}\left(\frac{1}{x^2}+\frac{1}{(x+y)^2}\right) \qquad \ldots(3)$$

can not hold simultaneously.

Proof of Lemma :- If possible, let both the inequalities (2) and (3) hold.

Then, we get

$$\sqrt{5}\ xy \geq x^2 + y^2 \qquad \ldots(4)$$

and $$\sqrt{5}\ x(x+y) \geq x^2 + (x+y)^2 \qquad \ldots(5)$$

Adding (4) and (5) we get

$$\sqrt{5}\,(x^2+2xy) \geq 3x^2 + 2y^2 + 2xy$$

or $$(3-\sqrt{5})\,x^2 + 2y^2 - 2(-1+\sqrt{5})\,xy \leq 0$$

Multiplying by 2, we get

$$(6-2\sqrt{5})\,x^2 + 4y^2 - 4(\sqrt{5}-1)xy \leq 0$$

$\Rightarrow$ $$((\sqrt{5}-1)\,x - 2y)^2 \leq 0$$

But a square quantity can not be less than zero i.e.

$\Rightarrow$ $$((\sqrt{5}-1)x - 2y)^2 = 0$$

$\Rightarrow \qquad (\sqrt{5}-1)x - 2y = 0$

$\Rightarrow$ $\sqrt{5}$ is a rational number which is not so. Thus (2) and (3) can not hold simultaneously. Hence the lemma.

Now to prove the theorem, we shall distinguish two cases

Case I $\xi < \dfrac{a+c}{b+d}$

Then we get $\left|\xi - \dfrac{a}{b}\right| \geq \dfrac{1}{\sqrt{5}b^2}$

But $\dfrac{a}{b} < \xi \quad \Rightarrow \left|\xi - \dfrac{a}{b}\right| = \xi - \dfrac{a}{b} \geq \dfrac{1}{\sqrt{5}b^2}$ …(6)

Also $\xi < \dfrac{a+c}{b+d} \Rightarrow \left|\xi - \dfrac{a+c}{b+d}\right| = \dfrac{a+c}{b+d} - \xi \geq \dfrac{1}{\sqrt{5}(b+d)^2}$ …(7)

and $\xi < \dfrac{c}{d} \Rightarrow \left|\xi - \dfrac{c}{d}\right| = \dfrac{c}{d} - \xi \geq \dfrac{1}{\sqrt{5}d^2}$ …(8)

Adding (6) and (8) we get

$$\frac{1}{\sqrt{5}}\left(\frac{1}{b^2}+\frac{1}{d^2}\right) \leq \frac{c}{d} - \frac{a}{b} = \frac{bc-ad}{bd} = \frac{1}{bd} \qquad \ldots(9)$$

(Θ $\dfrac{a}{b}$ & $\dfrac{c}{d}$ are consecutive Farey fractions)

Adding (6) and (7) we get

$$\frac{1}{\sqrt{5}}\left(\frac{1}{b^2}+\frac{1}{(b+d)^2}\right) \leq \frac{a+c}{b+d} \quad \frac{a}{b} = \frac{b(a+c)-a(b+d)}{b(b+d)}$$

$$= \frac{bc-ad}{b(b+d)} = \frac{1}{b(b+d)} \qquad \ldots(10)$$

But we have already proved that not both of the inequalities

$$\frac{1}{xy} \geq \frac{1}{\sqrt{5}}\left(\frac{1}{x^2}+\frac{1}{y^2}\right).$$

and $$\frac{1}{x(x+y)} \geq \frac{1}{\sqrt{5}}\left(\frac{1}{x^2}+\frac{1}{(x+y)^2}\right)$$

can hold simultaneously. So (9) and (10) violate the above Lemma and so in this case at least one of $\frac{a}{b}, \frac{c}{d}, \frac{a+c}{b+d}$ must satisfy (1)

Case II $\frac{a+c}{b+d} < \xi$

Since $\frac{a}{b} < \xi < \frac{c}{d}$. So (6), (8) and (9) also holds in this case

However $\frac{a+c}{b+d} < \xi$, so

$$\left| \xi - \frac{a+c}{b+d} \right| = \xi - \frac{a+c}{b+d} \geq \frac{1}{\sqrt{5}(b+d)^2} \qquad \ldots(11)$$

Adding (8) and (11) we get

$$\frac{1}{\sqrt{5}}\left(\frac{1}{d^2} + \frac{1}{(b+d)^2} \right) \leq \frac{c}{d} - \frac{a+c}{b+d}$$

$$= \frac{c(b+d) - d(a+c)}{d(b+d)} = \frac{bc - ad}{d(b+d)}$$

$$= \frac{1}{d(b+d)} \qquad \ldots(12)$$

Now (9) and (12) violate the condition of the Lemma, so at least one of $\frac{a}{b}, \frac{c}{d}, \frac{a+c}{b+d}$ must satisfy (1) in this case also.

Thus $\exists$ at least one fraction $\frac{h}{k}$ satisfying (1) and $\frac{h}{k}$ is either equal to $\frac{a}{b}$ or $\frac{c}{d}$ or $\frac{a+c}{b+d}$

Since $\frac{a}{b} < \xi < \frac{c}{d}$, so

$$\left| \xi - \frac{h}{k} \right| < \left| \frac{c}{d} - \frac{a}{b} \right| = \left| \left(\frac{c}{d} - \frac{a+c}{b+d} \right) + \left(\frac{a+c}{b+d} - \frac{a}{b} \right) \right|$$

$$= \left| \frac{c}{d} - \frac{a+c}{b+d} \right| + \left| \frac{a+c}{b+d} - \frac{a}{b} \right| = \frac{1}{d(b+d)} + \frac{1}{b(b+d)}$$

But $(b + d) \geq n + 1$, since $\frac{a}{b}$ & $\frac{c}{d}$ are consecutive Farey fractions.

$$\therefore \qquad \left|\xi - \frac{h}{k}\right| \le \frac{1}{d(n+1)} + \frac{1}{b(n+1)} \le \frac{2}{n+1} \quad (\Theta\ b \ge 1,\ d \ge 1)$$

Now to establish that (1) is satisfied by infinitely many rationals $\frac{h}{k}$, suppose there are only a finite number of $\frac{h}{k}$ satisfying (1)

Let $\varepsilon = \min\left|\xi - \frac{h}{k}\right|$, where minimum ranges over the finitely many rational numbers satisfying (1). Since ξ is irrational this minimum must be bigger than zero, i.e. $\varepsilon > 0$. Choose a rational number n such that

$$(n+1) > \frac{2}{\varepsilon}.$$

For this number n, as shown above $\exists$ a rational number $\frac{h_1}{k_1}$ satisfying (1) such that

$$\left|\xi - \frac{h_1}{k_1}\right| \le \frac{2}{n+1} < \varepsilon$$

and so $\frac{h_1}{k_1}$ must be different from the finitely many rational number considered above, which is a contradiction and so there must exist infinitely many rational number h/k satisfying (1)

This proves Hurwitz's theorem.

Theorem 1.26 Prove that $\sqrt{5}$ occurring in the statement of Hurwitz's theorem is best possible in the sense that if $\sqrt{5}$ is replaced by any larger real number say m then $\exists$ an irrational number ξ such that

$$\left|\xi - \frac{h}{k}\right| < \frac{1}{m k^2} \qquad \ldots(1)$$

does not hold for infinitely many rational number h/k.

Proof :- Take $\xi = \frac{1+\sqrt{5}}{2}$

then $\xi > 1$ and $\bar{\xi} = \frac{1-\sqrt{5}}{2} = \xi - \sqrt{5}$

We shall prove that if m is any real number with $\xi = \frac{1+\sqrt{5}}{2}$ and (1) is satisfied by infinitely many rational numbers $\frac{h}{k}$, the $m \le \sqrt{5}$

So we assume that (1) is satisfied by infinitely many rational numbers $\frac{h}{k}$

Now $(x-\xi)\,(x-\bar{\xi}) = (x-\xi)\,(x-\xi+\sqrt{5}) = x^2-x-1$ …(2)

Now for all integers h, k, $k > 0$

$$\left|\frac{h}{k}-\xi\right|.\left|\frac{h}{k}-\xi+\sqrt{5}\right| = \left|\frac{h^2}{k^2}-\frac{h}{k}-1\right| \ge \frac{1}{k^2}\ |h^2-hk-k^2|$$

Now, since any rational number h/k is not a root of $x^2-x-1 = 0$ so $|h^2 - hk - k^2| \ge 1$

$$\therefore \qquad \left|\frac{h}{k}-\xi\right|\left|\frac{h}{k}-\xi+\sqrt{5}\right| \ge \frac{1}{k^2} \qquad \ldots(3)$$

Since $\exists$ infinitely many rational numbers $\frac{h}{k}$ satisfying (1), $\exists$ sequence $\left\{\frac{h_i}{k_i},\ i = 1,2,3,\ldots\right\}$ of rational numbers satisfying (1)

Then $$\left|\frac{h_i}{k_i}-\xi\right| < \frac{1}{m k_i^2}$$

or $$|h_i - \xi k_i| < \frac{1}{m k_i}$$

But we know

$$|x-a| < \varepsilon \ \Rightarrow a-\varepsilon < x < a+\varepsilon$$

$$\therefore \qquad \xi k_i - \frac{1}{m k_i} < h_i < \xi k_i + \frac{1}{m k_i}$$

Then for each value of k_i, there exists a finite number of h_i's

Since (1) is satisfied by all $\frac{h_i}{k_i}$ s, so $k_i \to \infty$ as $i \to \infty$.

Further $$\frac{1}{k_i^2} \le \left|\frac{h_i}{k_i}-\xi\right|\left|\frac{h_i}{k_i}-\xi+\sqrt{5}\right|$$

$$\leq \left|\frac{h_i}{k_i}-\xi\right| \quad \left|\left|\frac{h_i}{k_i}-\xi\right|+\sqrt{5}\right|$$

$$\leq \frac{1}{m k_i^2}\left(\frac{1}{mk_i^2}+\sqrt{5}\right)$$

$(\Theta \frac{h_i}{k_i}$ satisfy (1))

Multiply by mk_i^2

$\Rightarrow \qquad m \leq \frac{1}{mk_i^2}+\sqrt{5} \quad \Rightarrow m \leq \sqrt{5}$, for all i large enough.

Theorem 1.27 e is irrational

Proof :- By definition

$$e = 1+\frac{1}{\lfloor\underline{1}}+\frac{1}{\lfloor\underline{2}}+\frac{1}{\lfloor\underline{3}}+\ldots..$$

If possible let e be rational and let $e = \frac{a}{b}$, $b > 0$ ad g.c.d. (a, b) = 1. Now consider $\lfloor\underline{b}\left[e-\left(1+\frac{1}{1}+\frac{1}{\lfloor\underline{2}}+\ldots+\frac{1}{\lfloor\underline{b}}\right)\right]=\alpha$

then α is an integer since, e = a/b is rational

Also by definition of e, $\alpha > 0$.

$$\alpha = \lfloor\underline{b}\left[\frac{1}{\lfloor\underline{b+1}}+\frac{1}{\lfloor\underline{b+2}}+\ldots..\right]$$

$$= \frac{1}{b+1}+\frac{1}{(b+1)(b+2)}+\ldots$$

$$< \frac{1}{b+1}+\frac{1}{(b+1)^2}$$

$$= \frac{1/(b+1)}{1-\frac{1}{b+1}} = \frac{1}{b} < 1 \qquad [\Theta\ b \geq 1]$$

Thus $0 < \alpha < 1$ is a contradiction since no integer lies between 0 and 1, so e is irrational.

Theorem 1.28 π is irrational

Let us first prove the following lemma

Lemma :- Let $f(x) = \dfrac{x^n(1-x)^n}{\lfloor n}$

then $f(0)$, $f(1)$ and $f^{(i)}(0)$, $f^{(i)}(1)$ are all integers for all $i \geq 0$. Also $0 < f(x) < 1/\lfloor n$ whenever $x \in (0, 1)$.

Proof of Lemma :- Clearly $f(0) = f(1) = 0$ (By definition of $f(x)$)

We can rewrite $f(x)$ as

$$f(x) = \frac{1}{\lfloor n}\left(\sum_{i=n}^{2n} c_i\, x^i\right)$$

Let $i \geq 1$. Now in $f^{(i)}(x)$, for $i < n$, we do not have any constant degree term and so

$$f^{(i)}(0) = 0 \text{ for } i < n$$

Further $f(x)$ is of degree $2n$, so

$$f^{(i)}(x) = 0 \text{ for } i > 2n$$

So let $n \leq i \leq 2n$

Then $f^{(i)}(0) = \sum_{i=n}^{2n} \dfrac{\lfloor i}{\lfloor n} c_i$

which is an integer since $n \leq i \leq 2n$

$\therefore$ $f^{(i)}(0)$ is an integer for all integers $i \geq 0$

Also by definition, $f(x) = f(1-x)$

$\therefore$ $f^{(i)}(1$ is also an integer $\forall\ i \geq 0$.

Proof of Theorem :- To prove the theorem, it is enough to prove that π^2 is irrational for if π^2 is irrational then π can not be rational. If possible, let $\pi^2 = \dfrac{a}{b}$ where g.c.d. $(a, b) = 1$, $b > 0$

Define a function

$$G(x) = b^n\{\pi^{2n} f(x) - \pi^{2n-2} f''(x) + \pi^{2n-4} f^{(IV)}(x) + \ldots + (-1)^n f^{(2n)}(x)\}$$

Then by lemma $f^m(0)$ & $f^m(1)$ are integers $\forall$ $m \geq 0$, so G(0) and G(1) are integers. Now consider

$$\frac{d}{dx}(G'(x) \sin \pi x - \pi G(x) \cos \pi x)$$

$$= G''(x) \sin \pi x + \pi G'(x) \cos \pi x, - \pi G'(x) \cos \pi x + \pi^2 G(x) \sin \pi x$$

$$= (G''(x) + \pi^2 G(x)) \sin \pi x \qquad \ldots(1)$$

Now

$$G''(x) = b^n \{\pi^{2n} f''(x) - \pi^{2n-2} f^{(IV)}(x) + \pi^{2n-4} f^{(VI)}(x) + \ldots + (-1)^n f^{(2n+2)}(x))$$

Also

$$\pi^2 G(x) = b^n \{\pi^{2n+2} f(x) - \pi^{2n} f''(x) + \pi^{2n-2} f^{(IV)}(x) + \ldots + (-1)^n \pi^2 f^{(2n)}(x)\}$$

Adding we get

$$G''(x) + \pi^2 G(x) = b^n \{\pi^{2n+2} f(x) + (-1)^n f^{(2n+2)}(x)\}$$

But f(x) is of degree 2n, so $f^{(2n+2)}(x) = 0$ and so

$$G^{II}(x) + \pi^2 G(x) = \pi^{2n+2} b^n f(x) \qquad \ldots(2)$$

But $\pi^2 = \frac{a}{b}$

$\Rightarrow$ $\pi^{2n+2} b^n = a^n \pi^2 \qquad \ldots(3)$

$\therefore$ From (1), (2) and (3) we get

$$\frac{d}{dx}(G'(x) \sin \pi x - \pi G(x) \cos \pi x)$$

$$= a^n \pi^2 f(x) \sin \pi x$$

$\therefore$ $a^n \pi^2 \int_0^1 f(x) \sin \pi x \, dx$

$$= [G'(x) \sin \pi x - \pi G(x) \cos \pi x]_0^1$$

$$= \pi G(1) \cos \pi + \pi G(0) \cos 0$$

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

$\therefore$ $G(0) + G(1) = \pi a^n \int_0^1 f(x) \sin \pi x \, dx \qquad \ldots(4)$

Now

$\sin \pi x$ is positive in (0, 1) and $0 < f(x) < 1/\lfloor n$ in (0, 1)

So by First mean value theorem of integral calculus, we have

$$0 < a^n \pi \int_0^1 f(x) \sin \pi x < \frac{a^n \pi}{\lfloor n} \int_0^1 \sin \pi x \, dx$$

$$= \frac{a^n}{\lfloor n} [-\cos \pi x]_0^1$$

$$= 2\frac{a^n}{\lfloor n} < 1$$

for n large enough since $\sum_{n=0}^{\infty} \frac{a^n}{\lfloor n}$ converges to e^a and to its nth term must tend to zero. But L.H.S. of (4) is an integer and so we get contradiction. $\therefore$ π^2 must be irrational.

Fibonacci Sequence

Definition :- A sequence in which first two terms are unity and then each term is the sum of the two that immediately precede it, is called Fibonacci sequence. Mathematically, this sequence can be formulated as

$u_1 = u_2 = 1$; $u_n = u_{n-1} + u_{n-2}$ for ≥ 3. Some initial terms of this sequence are

1, 1, 2, 3, 5, 8, 13, 21,…….

Lucas Sequence

Definition :- A sequence in which first two terms are 1 and 3 respectively and then each term is the sum of the two that immediately precede it, is called Lucas sequence. Mathematically, this sequence may be formulated as :

$L_1 = 1, L_2 = 3, L_n = L_{n-1} + L_{n-2}$ for $n \geq 3$

i.e. Lucus sequence is,

1, 3, 4, 7, 11, 18, 29, 47,……..

Note 1. Fibonacci numbers are sometimes denoted by F_n instead of u_n etc.

Note 2. Some authors use the term Fibonacci series and Lucas series in place of Fibonacci sequence and Lucas sequence. One should not get confused in two.

Some identities on Fibonacci and Lucas sequences :-

(I) $u_1 + u_3 + u_5 + \ldots + u_{2n-1} = u_{2n}$

(II) $u_2 + u_4 + u_6 + \ldots + u_{2n} = u_{2n+1} - 1$

(III) $L_1 + L_2 + L_3 + \ldots + L_n = L_{n+2} - 3,\ n \geq 1$

(IV) $L_1 + L_3 + L_5 + \ldots + L_{2n-1} = L_{2n} - 2,\ n \geq 1$

(V) $L_2 + L_4 + L_6 + \ldots + L_{2n} = L_{2n+1} - 1,\ n \geq 1$

(VI) $L_n = u_{n+1} + u_{n-1} = u_n + 2u_{n-1},\ n \geq 2$

(VII) $L_n = u_{n+2} - u_{n-2},\ n \geq 3$

Proof :- (1) We have

$u_1 = u_2$ (both are 1)

Also, $u_3 = u_4 - u_2$ ($\Theta\ u_4 = u_3 + u_2$)

Similarly, $u_5 = u_6 - u_4$

$u_7 = u_8 - u_6$

……

……

$u_{2n-3} = u_{2n-2} - u_{2n-4}$

$u_{2n-1} = u_{2n} - u_{2n-2}$

Adding all these equations, we get

$u_1 + u_3 + u_5 + \ldots + u_{2n-1} = u_{2n}$ (all other terms cancel)

(II) We have

$u_2 = u_2$

Also, $u_4 = u_5 - u_3$ ($\Theta\ u_5 = u_4 + u_3$)

Similarly, $u_6 = u_7 - u_5$

$u_8 = u_9 - u_7$

……..

……..

$u_{2n-2} = u_{2n-1} - u_{2n-3}$

$u_{2n} = u_{2n+1} - u_{2n-1}$

Adding all these equation, we get

$$u_2 + u_4 + u_6 + \ldots + u_{2n} = u_2 + u_3 + u_{2n+1}$$

$$\Rightarrow \quad u_2 + u_4 + u_6 + \ldots + u_{2n} = 1 - 2 + u_{2n+1}$$

$$= u_{2n+1} - 1.$$

(III) We shall prove the result by induction on n. For n = 1,

$$\text{L.H.S.} = L_1 = 1$$

and $\text{R.H.S.} = L_3 - 3 = 4 - 3 = 1$

Thus, the identity holds for n = 1.

Let us assume that, the identity holds for n = k i.e.

$$L_1 + L_2 + \ldots + L_k = L_{k+2} - 3 \qquad \ldots(*)$$

Now for n = k + 1, we have

$$L_1 + L_2 + \ldots + L_k + L_{k+1} = L_{k+2} - 3 + L_{k+1} \qquad [\text{By } (*)]$$

or $$L_1 + L_2 + \ldots + L_k + L_{k+1} = L_{k+3} - 3$$

or $$L_1 + L_2 + \ldots + L_k + L_{k+1} = L_{(k+1)+2} - 3$$

Thus, the identity holds for n = k + 1. Hence by Principle of mathematical induction, the identity holds for all natural numbers n.

(IV) We have

$$L_1 = L_1$$

Also, $L_3 = L_4 - L_2 \qquad (\Theta\ L_4 = L_3 + L_2)$

Similarly, $L_5 = L_6 - L_4$

$$L_7 = L_8 - L_6$$

……

……

$$L_{2n-3} = L_{2n-2} - L_{2n-4}$$

$$L_{2n-1} = L_{2n} - L_{2n-2}$$

Adding all these equations we get

$$L_1 + L_3 + L_5 + \ldots + L_{2n-1} = L_1 - L_2 + L_{2n}$$

$$= 1 - 3 + L_{2n}$$

$$= L_{2n} - 2$$

(V) We have $L_2 = L_2$

Also, $L_4 = L_5 - L_3$ $\quad (\Theta\ L_5 = L_4 + L_3)$

Similarly, $L_6 = L_7 - L_5$

$L_8 = L_9 - L_7$

……

$L_{2n-2} = L_{2n-1} - L_{2n-3}$

$L_{2n} = L_{2n+1} - L_{2n-1}$

Adding all these equations, we get

$$L_2 + L_4 + \ldots + L_{2n} = L_2 - L_3 + L_{2n+1}$$
$$= 3 - 4 + L_{2n+1} = L_{2n+1} - 1.$$

(VI) we shall prove the identity by induction on n.

For n = 2, L. H. S. $= L_2 = 3$

and R. H. S. $= u_3 + u_1 = 2+1 = 3$

Thus, the identity holds for n = 2

Let us assume that the identity holds for all natural numbers $k < n$

i.e. $L_k = u_{k+1} + u_{k-1} \ \forall\ k < n$

Now consider,

$L_n = L_{n-1} + L_{n-2}$ (by definition)

$= (u_n + u_{n-2}) + (u_{n-1} + u_{n-3})$

(by induction hypothesis for $n - 1$ and $n - 2$)

$\Rightarrow$ $L_n = (u_n + u_{n-1}) + (u_{n-2} + u_{n-3})$

$= u_{n+1} + u_{n-1} = (u_n + u_{n-1}) + u_{n-1} = u_n + 2\ u_{n-1}$

Hence the identity is established.

(VII) We shall prove the identity by induction on n.

For n = 3, L. H. S. = $L_3 = 4$

R. H. S. = $u_5 - u_1 = 5-1 = 4$

Thus, the identity holds for n = 3

Let us assume, that the identity holds for all natural numbers k < n.

i.e. $L_k = u_{k+2} - u_{k-2} \; \forall \; k < n$

Now, consider,

$$L_n = L_{n-1} + L_{n-2} = (u_{n+1} - u_{n-3}) + (u_n - u_{n-4})$$

(by induction hypothesis, for n − 1, n − 2)

$$= (u_{n+1} + u_n) - (u_{n-3} + u_{n-4})$$

$$= u_{n+2} - u_n - 2$$

Hence the identity is established.

Theorem 1.29. Prove that for the Fibonacci sequence,

$$\gcd(u_n, u_{n+1}) = 1 \text{ for every } n \geq 1$$

Proof :- Let, if possible, $\gcd(u_n, u_{n+1}) = d > 1$

$\Rightarrow$ $d \mid u_n, d \mid u_{n+1} \Rightarrow d \mid (u_{n+1} - u_n)$

$$\Rightarrow d \mid u_{n-1}$$

Again, $d \mid u_n, d \mid u_{n-1} \Rightarrow d \mid (u_n - u_{n-1})$

$$\Rightarrow d \mid u_{n-2}$$

Continuing like this, we can show that

$d \mid u_{n-3}, d \mid u_{n-4}, \ldots$ and finally $d \mid u_1$

But $u_1 = 1$ which is certainly not divisible by any d > 1.

Thus d = 1 and the proof is completed.

Lemma :- Prove that

$$u_{m+n} = u_{m-1}\, u_n + u_m\, u_{n+1} \quad \ldots(1)$$

Proof :- For fixed m, we shall prove the result (1) by induction on n.

For n = 1, (1) becomes, $u_{m+1} = u_{m-1}\, u_1 + u_m\, u_2$

$$= u_{m-1} + u_m \qquad (\Theta\ u_1 = u_2 = 1)$$

which is true by definition and the result is true for n = 1. Let us assume that result is true for n = 1, 2,…, k and now we shall prove it for n = k + 1.

By induction hypothesis, we have

$$u_{m+k} = u_{m-1}\, u_k + u_m\, u_{k+1}$$

and $$u_{m+(k-1)} = u_{m-1}\, u_{k-1} + u_m\, u_k$$

Adding these two, we get.

$$u_{m+k} + u_{m+(k-1)} = u_{m-1}\,(u_k + u_{k-1}) + u_m\,(u_{k+1} + u_k)$$

$$= u_{m-1}\, u_{k+1} + u_m\, u_{k+2}$$

So that the result holds for n = k + 1

Hence by induction principle the result is true for all the integers n. Now by changing m and by the above discussion, we conclude that the result (1) holds for all positive integers m and n.

Remark 1. If b | c, then gcd (a +c, b) = gcd (a, b)

Remark 2. If gcd (a, c) = 1, then gcd (a, b c) = gcd (a, b)

Theorem 1.30 Prove that for $m \geq 1$, $n \geq 1$, u_{mn} is divisible by u_m.

Proof :- We shall prove the result by induction on n. The result is trivial for n = 1. Let us assume, that the result is true for n = 1, 2,…, k i.e. u_{mn} is divisible by u_m for n = 1, 2,…k. Now we shall prove that $u_{m(k+1)}$ is divisible by u_m.

We have,

$$u_{m(k+1)} = u_{mk+m} = u_{mk-1}\, u_m + u_{mk}\, u_{m+1} \quad \ldots(1)$$

Now, by induction hypothesis, u_{mk} is divisible by u_m, so that R.H.S. of (1) and hence L.H.S. of (1) is divisible by u_m i.e. $u_{m(k+1)}$ is divisible by u_m. The proof is thus completed using principle of mathematical induction.

Lemma :- If m = qn+r, then prove that

$$\gcd(u_m, u_n) = \gcd(u_r, u_n)$$

Proof :- We have

$$\gcd(u_m, u_n) = \gcd(u_{qn+r}, u_n)$$

$$= \gcd(u_{qn-1}\, u_r + u_{qn}\, u_{r+1}, u_n)$$

…(1)

Now by above theorem $u_n \mid u_{qn} \Rightarrow u_n \mid u_{qn}\, u_{r+1}$,

so that by remark 1 stated above, we have

$$\gcd(u_{qn-1}\, u_r + u_{qn}\, u_{r+1}, u_n) = \gcd(u_{qn-1}\, u_r, u_n)$$

So that (1) becomes :

$$\gcd(u_m, u_n) = \gcd(u_{qn-1}\, u_r, u_n)$$

…(2)

Now, we claim that,

$$\gcd(u_{qn-1}, u_n) = 1.$$

Let $\gcd(u_{qn-1}, u_n) = d \Rightarrow d \mid u_{qn-1}$ and $d \mid u_n$

Now, $d \mid u_n$ and $u_n \mid u_{qn} \Rightarrow d \mid u_{qn}$ i.e. d is a common divisor of two successive Fibonacci numbers namely, u_{qn} and u_{qn-1} but successive Fibonacci number are coprime. So d = 1, the claim is thus completed. Hence using remark (2) stated above, we have

$$\gcd(u_{qn-1}\, u_r, u_n) = \gcd(u_r, u_n)$$

So that (2) becomes :

$$\gcd(u_m, u_n) = \gcd(u_r, u_n)$$ and proof is completed.

Theorem 1.31 The greatest common divisor of two Fibonacci numbers is again a Fibonacci number. More specifically,

$$\gcd(u_m, u_n) = u_d \text{ where } d = \gcd(m, n)$$

Proof :- W.L.O.G let us assume that $m \geq n$. Applying the division algorithm to m and n, we get the following system of equations.

$m = q_1 n + r_1$ $\quad 0 < r_1 < n$

$n = q_2\, r_1 + r_2$ $\quad 0 < r_2 < r_1$

$r_1 = q_3\, r_2 + r_3$ $\quad 0 < r_3 < r_2$

……. $\quad$ ……

……. $\quad$ ……

$r_{n-2} = q_n\, r_{n-1} + r_n$ $\quad 0 < r_n < r_{n-1}$

$r_{n-1} = q_{n+1}\, r_n + 0$

Now, by above lemma, we have

$$\gcd(u_m, u_n) = \gcd(u_{r_1}, u_n) = \gcd(u_{r_1}, u_{r_2})$$

$$\ldots, = \gcd(u_{r_{n-1}}, u_{r_n}) \qquad \ldots(1)$$

Now from the last equation of above system, we have

$r_n \mid r_{n-1}$ i.e. r_{n-1} is an integral multiple of r_n and hence $u_{r_{n-1}}$ is divisible by u_{r_n} (we have proved the theorem that u_{mn} is divisible by u_m $\forall$ $m \geq 1, n \geq 1$)

Hence $\gcd(u_{r_{n-1}}, u_{r_n}) = u_{r_n}$

So that (1) implies that $\gcd(u_m, u_n) = u_{r_n}$ …(2)

But it should be noted that in above system of equations r_n is the last non zero remainder in the division algorithm for m and n so that

$$\gcd(m, n) = r_n$$

Hence (2) provides that $\gcd(u_m, u_n) = u_{\gcd(m, n)}$

This completes the proof.

Corollary (1) :- Prove that if $\gcd(m, n) = 1$, then $\gcd(u_m, u_n) = 1$

Proof :- Taking $d = 1$ in the above theorem and noting that

$u_1 = 1$, we get the result.

Corollary (2) :- In the Fibonacci sequence, $u_m \mid u_n$ if and only if $m \mid n$.

Proof :- Firstly, let $m \mid n$, then $n = mk$ for any integers k. But we know that $u_m \mid u_{mk} \Rightarrow u_m \mid u_n$.

Conversely, let $u_m \mid u_n$ then $\gcd(u_m, u_n) = u_m$. But by above theorem, $\gcd(u_m, u_n) = u_{\gcd(m, n)}$

$\Rightarrow$ $\gcd(m, n) = m \Rightarrow m \mid n$.

Theorem 1.32 Prove that every positive integer can be represented as a finite sum of Fibonacci numbers, none used more than once. Or Prove that every positive integer can be written as a sum of distinct Fibonacci numbers.

Proof :- Clearly, we have

$1 = u_1$; $2 = u_3$; $3 = 1 + 2 = u_1 + u_3$ etc.

To prove the result for every natural number, we shall show that each of the integers 1, 2, 3,…, $u_n - 1$ is a sum of numbers from the set $\{u_1, u_2,\ldots, u_{n-2}\}$ and we shall prove this by induction on n.

Let us assume that the result holds for n = k i.e. each of the integers 1, 2, 3,…, u_{k-1} is a sum of numbers from the set $\{u_1, u_2\ldots u_{k-2}\}$ Now choose N such that

$$u_k - 1 < N < u_{k+1}$$

From this, we have $N - u_{k-1} < u_{k+1} - u_{k-1} = u_k$

$$\Rightarrow \quad N - u_{k-1} < u_k$$

$$\Rightarrow \quad N - u_{k-1} \leq u_k - 1$$

So by induction hypothesis $N - u_{k-1}$ is representable as a sum of distinct numbers from the set $\{u_1, u_2,\ldots, u_{k-2}\}$. This implies that N is representable as a sum of distinct numbers from the set $\{u_1, u_2,\ldots, u_{k-2}\}$. This implies that N is representable as a sum of distinct numbers from the set $\{u_1, u_2,\ldots, u_{k-2}, u_{k-1}\}$. Consequently each of the integers 1, 2, 3,… $u_{k+1} - 1$ can be expressed as a sum of numbers from the set $\{u_1, u_2, \ldots, u_{k-2}, u_{k-1}\}$. This completes the induction step and hence the theorem.

System of Linear Congruences

Definition :- Let m be a fixed positive integer. Two integers a and b are said to be congruent modulo m denoted by $a \equiv b \pmod m$ if m divides a–b i.e. a – b = km for some integer k.

Theorem 1.33 Let a, b, c, d, m be integers (m > 0), then

(i) If $a \equiv b \pmod m$, $b \equiv c \pmod m$, then $a \equiv c \pmod m$

(ii) If $a \equiv b \pmod m$, $c \equiv d \pmod m$, then $a + c \equiv b + d \pmod m$

(iii) If $a \equiv b \pmod m$, $c \equiv d \pmod m$, then $ac \equiv bd \pmod m$

(iv) If $a \equiv b \pmod m$, $d \mid m$ (d > 0), then $a \equiv b \pmod d$

(v) If $a \equiv b \pmod m$, then $ac \equiv bc \pmod{cm}$, c > 0

Proof :- (i) Given that $a \equiv b \pmod m \Rightarrow m \mid (a-b)$

$$b \equiv c \pmod m \Rightarrow m \mid (b-c)$$

$$\Rightarrow \quad m \mid [(a-b) + (b-c)] \Rightarrow m \mid (a-c)$$

$$\Rightarrow a \equiv c \pmod m$$

(ii) $a \equiv b \pmod m \Rightarrow m \mid (a-b)$

$c \equiv d \pmod m \Rightarrow m \mid (c - d)$

$$\Rightarrow \quad m \mid [(a-b) + (c-d)] \Rightarrow m \mid [(a+c) - (b+d)]$$

$\Rightarrow$ $(a + c) \equiv (b + d) \pmod m$

(iii) $a \equiv b \pmod m \Rightarrow m \mid (a-b)$

$c \equiv d \pmod m \Rightarrow m \mid (c-d)$

$\Rightarrow$ $a - b = mk$ and $c-d = mk'$ for some integers k, k'

$\Rightarrow$ $a = b + mk$ and $c = d + mk'$

Multiplying these two,

$$ac = bd + bm\,k^1 + dmk + m^2 kk'$$

$\Rightarrow$ $$ac = bd + m(bk' + dk + mkk')$$

$\Rightarrow$ $ac - bd = mk''$ where $k'' = bk' + dk + mkk'$ is an integer.

$\Rightarrow$ $m \mid (ac - bd)$

$\Rightarrow$ $ac \equiv bd \pmod m$

(iv) $a \equiv b \pmod m \Rightarrow m \mid (a-b)$

Also $d \mid m$ and $m \mid (a-b) \Rightarrow d \mid (a-b)$

Hence $a \equiv b \pmod d$

(v) $a \equiv b \pmod m$

$\Rightarrow$ $m \mid (a-b) \Rightarrow mc \mid (a-b)\,c \Rightarrow mc \mid (ac-bc)$

$\Rightarrow$ $ac \equiv bc \pmod{mc}$

Theorem 1.34 Let $f(x)$ be a polynomial with integral coefficients and $a \equiv b \pmod m$, then

$$f(a) \equiv f(b) \pmod m$$

Proof :- Let $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n x$, where $a_0, a_1, \ldots, a_n$ are integers.

Since $a \equiv b \pmod m$, so we must have …(1)

$a^2 \equiv b^2 \pmod m$ …(2)

$a^3 \equiv b^3 \pmod m$ …(3)

……

……

$a^n \equiv b^n \pmod m$

…(n)

Multiplying equation (1) by a_{n-1}, (2) by $a_{n-2}, \ldots$, (n) by a_0 we get

$a_{n-1}\, a \equiv a_{n-1}\, b \pmod m$

$a_{n-2}\, a^2 \equiv a_{n-2}\, b^2 \pmod m$

$$a_{n-3}\, a^3 \equiv a_{n-3}\, b^3 (\text{mod } m) \qquad \ldots(*)$$

……..

……..

$$a_0\, a^n \equiv a_0\, b^n \text{ (mod m)}$$

Also, we know that

$$a_n \equiv a_n (\text{mod } m)$$

Adding this with all the congruences in (∗), we get

$$a_n + a_{n-1}\, a + \ldots + a_0\, a^n \equiv a_n + a_{n-1}\, b + \ldots + a_0\, b^n \text{ (mod m)}$$

$\Rightarrow$ $f(a) \equiv f(b) \text{ (mod m)}$

Theorem 1.35 Prove that

(i) $ax \equiv ay (\text{mod } m) \quad \Leftrightarrow x \equiv y \bmod\left(\dfrac{m}{\gcd(a, m)}\right)$

(ii) If $ax \equiv ay (\text{mod } m)$ and $(a, m) = 1$ then $x \equiv y \text{ (mod m)}$

(iii) $x \equiv y \text{ (mod } m_i)$ for $i = 1, 2, \ldots, r$ iff, $x \equiv y (\text{mod } [m_1, m_2, \ldots, m_r])$

where $[m_1, m_2, \ldots, m_r]$ denotes the λ cm of $m_1, m_2, \ldots, m_r$.

Proof :- (i) Given that, $ax \equiv ay \text{ (mod m)} \Rightarrow m \mid (ax - ay)$

$\Rightarrow$ $ax - ay = mz$ for some integer z

$\Rightarrow$ $$\frac{a}{\gcd(a, m)}(x - y) = \frac{m}{\gcd(a, m)} z$$

So that, we get that

$$\frac{m}{\gcd(a,m)} \left| \frac{a}{\gcd(a,m)}(x - y) \right. \qquad \ldots(1)$$

But we know that, $\gcd\left(\dfrac{a}{\gcd(a,m)}, \dfrac{m}{\gcd(a,m)}\right) = 1$

$\therefore$ (1) implies that,

$$\frac{m}{\gcd(a,m)} \left| (x - y) \right.$$ (Using the result that if $a \mid bc$ and $(a, b) = 1$ then $a \mid c$)

$\Rightarrow$ $x \equiv y \bmod\left(\dfrac{m}{\gcd(a,m)}\right)$

Conversely, let $x \equiv y\left(\mod \frac{m}{\gcd(a,m)}\right)$

$\Rightarrow \quad \frac{m}{\gcd(a,m)} \mid (x-y)$

$\Rightarrow \quad m \mid \gcd(a, m)\,(x-y)$

$\Rightarrow \quad m \mid a(x-y) \qquad (\Theta\ \gcd(a, m) \mid a)$

$\Rightarrow \quad ax \equiv ay(\mod m)$

(ii) This is a special case of part (i), by taking gcd(a, m) = 1, we get the result

(iii) Let $x \equiv y(\mod m_i)$ for i = 1, 2,…, r

$\Rightarrow \quad m_i \mid (x-y)$ for i = 1, 2,…, r

i.e., x−y is a common multiple of $m_1, m_2,\ldots, m_r$ but $[m_1, m_2,\ldots, m_r]$ is least common multiple of $m_1, m_2,.., m_r$ so by definition of λcm, $[m_1, m_2,\ldots, m_r]$ is a divisor of (x−y)

i.e. $x \equiv y(\mod [m_1, m_2,\ldots, m_r])$

Conversely, let $x \equiv y\ (\mod [m_1, m_2,\ldots, m_r])$

Now $m_i \mid [m_1, m_2,\ldots, m_r]$

So $x \equiv y(\mod m_i)$

This completes the proof.

Definition :- (Complete Residue System)

A set $\{a_1, a_2,\ldots, a_m\}$ of integers is said to be complete residue system mod m if

(i) $a_i \not\equiv a_j(\mod m)$ for $i \neq j$

(ii) For each integer n, there exists a unique a_i such that $n \equiv a_i\ (\mod m)$

For example,

The set {1, 2,…, m−1, m} is a complete residue system mod m.

Definition :- (Reduced Residue System)

A set $\{b_1, b_2,\ldots, b_k\}$ of integers is said to be reduced residue system mod m if

(i) $(b_i, m) = 1$, i = 1, 2, …, k

(ii) $b_i \not\equiv b_j\ (\mod m)$ for $i \neq j$

(iii) If n is any integer which is coprime to m, then there exists a unique b_i such that $n \equiv b_i(\mod m)$

Remark :- It is clear from the two definitions that a reduced residue system mod m can be obtained by deleting those members from a complete residue system mod m which are not relatively prime to m.

Theorem 1.36 Let $\{r_1, r_2,\ldots, r_n\}$ be a complete (or reduced) residue system mod m and let (a, m) = 1 then $(ar_1, ar_2,\ldots, ar_n\}$ is a complete (or reduced) residue system mod m.

Proof :- If $(r_i, m) = 1$, then $(ar_i, m) = 1$

Clearly, the number of $ar_1, ar_2,\ldots, ar_n$ and of $r_1\ r_2,\ldots, r_n$ is same. Thus, we need only to show that $ar_i \not\equiv ar_j \pmod m$ if $i \neq j$.

Let, if possible, $ar_i \equiv ar_j \pmod m$, $i \neq j$

then $r_i \equiv r_j \pmod m$, $i \neq j$ $\quad (\Theta\ (a, m) = 1)$

a contradiction, since $\{r_1, r_2,\ldots, r_n\}$ is a complete (or reduced) residue system. This completes the proof

Remark :- In the case of complete residue system, we also have the following result.

Let $\{r_1, r_2,\ldots, r_n\}$ be a complete residue system mod m and let (a, m) = 1, then for any integer b, the set $\{ar_1 + b, ar_2 + b,\ldots, ar_n+b\}$ is also a completes residue system. This result does not hold in case of reduced residue system.

Definition :- (Euler's ϕ-Function)

Let m be any positive integer, then Euler's ϕ function is defined as :

$\phi(1) = 1$ and

$\phi(m)$ = number of natural number less than m which are relatively prime to m.

For example,

$$\phi(2) = 1,\ \phi(3) = 2,\ \phi(4) = 2,\ \phi(10) = 4 \text{ etc.}$$

Remark :- From the definitions of Euler's ϕ-function and reduced residue system, it is clear that reduced residue system mod m contains always $\phi(m)$ elements.

Theorem 1.37 (Euler's theorem) Prove that if (a, m) = 1

then $a^{\phi(m)} \equiv 1 \pmod m$

Proof :- Let $r_1, r_2,\ldots, r_{\phi(m)}$ be reduced residue system mod m. Since (a, m) = 1. So $ar_1, ar_2,\ldots, ar_{\phi(m)}$ is also a reduced residue system mod m. Hence, by definition, corresponding to each ri, there is one and only one ar_j such that

$$r_i \equiv ar_j \pmod m$$

Further, different r_i will have different corresponding ar_j. This implies that the numbers $ar_1, ar_2,\ldots, ar_{\phi(m)}$ are just the residue modulo m of $r_1, r_2,\ldots, r_{\phi(m)}$ but not necessarily in the same order. Thus multiplying these, we obtain :

$$\prod_{j=1}^{\phi(m)} (ar_j) \equiv \prod_{i=1}^{\phi(m)} r_i \pmod m$$

This implies that

$$a^{\phi(m)} \prod_{j=1}^{\phi(m)} r_j \equiv \prod_{j=1}^{\phi(m)} r_j \pmod m$$

Now $(r_j, m) = 1$, so cancelling r_j, we get

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

This completes the proof.

Corollary (Fermat's theorem) :- Let p be a prime such that $p \nmid a$, then prove that,

$$a^{p-1} \equiv 1 \pmod p$$

Proof :- Since p is prime, so every natural number less than p is coprime to p so that $\phi(p) = p-1$. Now given that p is prime and $p \nmid a \Rightarrow (p, a) = 1$

Hence by Euler's theorem,

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

$$\Rightarrow \quad a^{p-1} \equiv 1 \pmod p$$

This completes the proof

Remark :- Some time Fermat's theorem is stated as "Let p be a prime such that $p \nmid a$, then $a^p \equiv a \pmod p$" which is a trivial conclusion of above.

Theorem 1.38 If $(a, m) = 1$, then there is an x such that

$ax \equiv 1 \pmod m$ and conversely. Further this x is unique upto congruence i.e. any two such x are congruent (mod m).

Proof :- If $(a, m) = 1$, then there exists x and y such that

$ax + my = 1 \Rightarrow m \mid (ax-1) \Rightarrow ax \equiv 1 \pmod m$

Conversely, let $ax \equiv 1 \pmod m$, the there is a y such that $ax + my = 1$ so that $(a, m) = 1$

Now let $ax_1 \equiv 1 \pmod m$ and $ax_2 \equiv 1 \pmod m$

$$\Rightarrow \quad ax_1 \equiv ax_2 \pmod m$$

But $(a, m) = 1$, so it follows that

$$x_1 \equiv x_2 \pmod m$$

This completes the proof.

Theorem 1.39 (The Chinese Remainder Theorem). Let $m_1, m_2, \ldots, m_r$ denote r positive integers that are relatively prime in pairs i.e. $(m_i, m_j) = 1$, $i \neq$

j and let $a_1, a_2, \ldots, a_r$ denote any r integers. Consider the following congruences :

$$\left.\begin{aligned} &x \equiv a_1 \pmod{m_1} \\ &x \equiv a_2 \pmod{m_2} \\ &\ldots(*) \\ &\ldots\ldots\ldots\ldots \\ &x \equiv a_r \pmod{m_r} \end{aligned}\right)$$

then the congruences in (*) have a common solution. Further if x_0 and x_1 are two common solutions then $x_0 \equiv x_1 \pmod{m}$ where $m = m_1 m_2 \ldots m_r$ or we can say that if x_0 and x_1 are two common solutions, then $x_1 = x_0 + km$ for some integer k.

Proof :- Let $m = m_1 m_2 \ldots m_r$

then clearly, $\frac{m}{m_j}$ is an integer and $\left(\frac{m}{m_j}, m_j\right) = 1$

Also, we observe that $\frac{m}{m_j}$ is divisible by m_i for $i \neq j$

Now, since $\left(\frac{m}{m_j}, m_j\right) = 1$. So by last theorem, for each j there exists an integer b_j

such that $$\frac{m}{m_j} b_j \equiv 1 \pmod{m_j}$$

$$\Rightarrow \quad \frac{m}{m_j} b_j a_j \equiv a_j \pmod{m_j} \qquad \ldots(1)$$

Also, since $\frac{m}{m_j}$ is divisibly by m_i $(i \neq j)$, so we must have

$$\left(\frac{m}{m_j}\right) b_j = 0 \pmod{m_i} \text{ for } i \neq j \qquad \ldots(2)$$

Now, Put $x_0 = \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j$

$$= \frac{m}{m_1} b_1 a_1 + \frac{m}{m_2} b_2 a_2 + \ldots + \frac{m}{m_r} b_r a_r$$

then clearly we must have

$$x_0 \equiv \frac{m}{m_1} b_1 a_1 (\text{mod } m_1) \qquad \ldots(3)$$

(Θ all other terms of x_0 are divisible by m_1 by (2)

Putting j = 1 in (1),

$$\frac{m}{m_1} b_1 a_1 \equiv a_1 (\text{mod } m_1) \qquad \ldots(4)$$

Combining (3) and (4), we get that

$x_0 \equiv a_1 (\text{mod } m_1)$ i.e. x_0 is the solution of first congruence in $(*)$

Again, we must have

$$x_0 \equiv \frac{m}{m_2} b_2 a_2 (\text{mod } m_2) \qquad \ldots(5)$$

(Θ all other terms of x_0 ax divisible by m_2 by (2))

Putting j = 2 in (1) and combining with (5), we get

$x_0 \equiv a_2 (\text{mod } m_2)$ i.e. x_0 is the solution of second congruence in $(*)$

Continuing like this, we obtain that

$x_0 \equiv a_i (\text{mod } m_i)$ for i = 1, 2,.., r.

So that x_0 is common solution of congruences in $(*)$. Now, let x_0 and x_1 be two solutions of congruences in $(*)$, then,

$x_0 \equiv a_i (\text{mod } m_i)$ for i = 1, 2,…, r

and $x_1 \equiv a_i (\text{mod } m_i)$ for i = 1, 2,…, r

combining, $x_0 \equiv x_1 (\text{mod } m_i)$

$\Rightarrow$ $m_1 \mid (x_0 - x_1), m_2 \mid (x_0 - x_1), \ldots, m_r \mid (x_0 - x_1)$

But $(m_i, m_j) = 1$ for $i \neq j$ so

$m_1 m_2 \ldots m_r \mid (x_0 - x_1)$ [Θ If a | c, b | c and (a, b) = 1 then ab | c]

$\Rightarrow$ $m \mid (x_0 - x_1)$

$\Rightarrow$ $x_0 \equiv x_1 (\text{mod } m)$

This completes the proof.

Remark :- Converse of Fermat's theorem need not be true.

The converse of Fermat's theorem is not true i.e. if $m \nmid a$ and $a^{m-1} \equiv 1 (\text{mod } m)$, the m is not necessarily a prime.

For example, let m = 561 = 3.11.17 so m is not a prime. Now, let a be any integer such that gcd (a, 561) = 1

$\Rightarrow$ gcd (a, 3) = 1, gcd(a, 11) = 1, gcd(a, 13) = 1

i.e. $3 \nmid a$. $11 \nmid a$. $13 \nmid a$, so by Fermat's theorem,

$$a^2 \equiv 1 \pmod 3 \qquad (\Theta\ \phi(3) = 2)$$

$$\Rightarrow \quad (a^2)^{280} = a^{560} \equiv 1 \pmod 3$$

Similarly, $a^{10} \equiv 1 \pmod{11}$ $\qquad (\Theta\ \phi(11) = 10)$

$$\Rightarrow \quad a^{560} \equiv 1 \pmod{11}$$

and $\quad a^{16} \equiv 1 \pmod{17}$

$$\Rightarrow \quad a^{560} \equiv 1 \pmod{17}$$

using Chinese Remainder Theorem

$$A^{560} \equiv 1 \pmod{561}$$

Thus, the converse of Fermat's theorem is not true. In this regard, we prove the following theorem.

Theorem 1.40 For every odd a > 1, there exists infinitely many composite m satisfying,

$$a^{m-1} \equiv 1 \pmod m$$

Proof :- Let a > 1 be given odd number, choose an odd prime which does not divide $a(a^2-1)$ [we note that there are many such primes]

Take, $\quad m = \dfrac{a^{2p}-1}{a^2-1} == \dfrac{a^p-1}{a-1}.\dfrac{a^p+1}{a+1}$

So that m is clearly composite.

Now, $\quad m-1 = \dfrac{a^{2p}-1}{a^2-1} - 1 = \dfrac{a^{2p}-a^2}{a^2-1}$

$$\Rightarrow \quad (a^2-1)\,(m-1) = a^{2p} - a^2 = a(a^{p-1}-1)\,(a^p + a) \quad \ldots(1)$$

Since a and a^p are both odd so $a^p + a$ is even.

Also, $\quad p \mid (a^{p-1}-1)$ $\qquad$ (by Fermat's theorem)

and $\quad a^2-1 \mid (a^{p-1}-1)$ $\qquad (\Theta\ p-1$ is even)

Further, by choice of p, gcd $(p, a^2-1) = 1$

$\Rightarrow p\,(a^2-1) \mid (a^{p-1}-1) \Rightarrow 2p\,(a^2-1) \mid (a^{p-1}-1)\,(a^p + a)$ $\qquad (\Theta\ a^p + a$ is even)

$\Rightarrow 2p\,(a^2-1) \mid (a^2-1)\,(m-1)$ $\qquad$ [By (1)]

$\Rightarrow$ $2p \mid (m-1)$ $\Rightarrow \exists$ an integer μ such that $m = 1 + 2p\,\mu$. Now from (1), we have

$$a^{2p} = (a^2-1)(m-1) + a^2$$
$$= (a^2-1)m - (a^2-1) + a^2$$
$$\equiv 1 \pmod m$$

$\Rightarrow$ $a^{2p\mu} \equiv 1 \pmod m$

$\Rightarrow$ $a^{m-1} \equiv 1 \pmod m$

This is true for every choice of p and hence theorem is proved.

Remark :- The following theorem gives the correct converse of Fermat theorem., and is known as "Limited Converse of Fermat theorem", or "Modified Converse of Fermat theorem". But before that, we make a definition.

Definition (order of a mod m)

Let $m \geq 2$ be an integer and let (a, m) = 1, then by Euler's theorem we have $a^{\phi(m)} \equiv 1 \pmod m$.

Now, let $S = \{n \in N, a^n \equiv 1 \pmod m\}$, then $S \neq \phi$, since $\phi(m) \in S$. So by Law of well ordering S has a smallest element, say d. Then we say d is the order of a mod m and we write $\text{ord}_m^a = d$.

Theorem 1.41 (Limit converse or Modified converse of Fermat theorem)

If $m \geq 2$, $a^{m-1} \equiv 1 \pmod m$ and $a^x \not\equiv 1 \pmod m$ for any proper divisor x of m−1, then m is prime.

Proof :- Since $a^{m-1} \equiv 1 \pmod m \Rightarrow (a, m) = 1$

Now, let $\text{ord}_m^a = d$, then $d \mid (m-1)$ and $a^d \equiv 1 \pmod m$. But no proper divisor x of m−1 satisfies $a^x \equiv 1 \pmod m \Rightarrow d = m-1$

Also, by Euler theorem, $a^{\phi(m)} \equiv 1 \pmod m$

$\Rightarrow$ $d \mid \phi(m) \Rightarrow (m-1) \mid \phi(m) \Rightarrow m-1 \leq \phi(m)$

Also for $m \geq 2$, $\phi(m) \leq m-1$

$\Rightarrow$ $\phi(m) = m-1 \Rightarrow$ m is a prime.

Here, we give some examples based on Chinese Remainder Theorem

Example :- Find the least positive integer x such that

$$x \equiv 5 \pmod 7,\ x \equiv 7 \pmod{11},\ x \equiv 3 \pmod{13}$$

Solution :- We have by comparing with Chinese remainder theorem

$$a_1 = 5,\ a_2 = 7,\ a_3 = 3$$

$$m_1 = 7,\ m_2 = 11,\ m_3 = 13$$

Clearly m_1, m_2, m_3 are pairwise coprime and

$$m = 7.11.13 = 1001$$

Now, we find the values of b_1, b_2, b_3 using

$$\frac{m}{m_j} b_j \equiv 1 (\text{mod } m_j)$$

For j = 1, $\quad \frac{m}{m_1} b_1 \equiv 1 (\text{mod } m_1)$

$\Rightarrow \quad \frac{1001}{7} b_1 \equiv 1 (\text{mod } 7)$

$\Rightarrow \quad 143\, b_1 \equiv 1 (\text{mod } 7)$

$\Rightarrow \quad 3b_1 \equiv 1 (\text{mod } 7)$

which gives $b_1 = 5$

For j = 2, $\frac{m}{m_2} b_2 \equiv 1 (\text{mod } m_2)$

$\Rightarrow \quad 91\, b_2 \equiv 1 (\text{mod } 11)$

$\Rightarrow \quad 3\, b_2 \equiv 1 (\text{mod } 11)$

which gives $b_2 = 4$

For j = 3, $\quad \frac{m}{m_3} b_3 \equiv 1 (\text{mod } m_3)$

$\Rightarrow \quad 77\, b_3 \equiv 1 (\text{mod } 13)$

$\Rightarrow \quad -b_3 \equiv 1 \text{ (mod } 13)$

which gives $b_3 = 12$

Hence the common solution is

$$x_0 = \frac{m}{m_1} b_1 a_1 + \frac{m}{m_2} b_2 a_2 + \frac{m}{m_3}\, b_3\, a_3$$

$$= 143.5.5 + 91.4.7 + 77.12.3 = 8895$$

If x is another solution of given system of congruences then we must have :

$$x \equiv 8895 (\text{mod } 1001)$$

Also $\quad 8895 \equiv 887 (\text{mod } 1001)$

This gives $x \equiv 887$ (mod 1001)

Hence the required solution is 887.

Remark :- 1. In the Chinese Remainder Theorem, the hypothesis that m_j's should be pairwise coprime is absolutely essential. When this hypothesis fails, the existence of a solution x of the simultaneous system is no longer guaranteed. Further if such an x does exist, then it is unique modulo $[m_1, m_2,\ldots, m_r]$ and not modulo m, where $[m_1, m_2,\ldots, m_r]$ denotes the λcm of $m_1, m_2,\ldots, m_r$ 2. In case of no solution of given system, we call the system is inconsistent.

Example :- Show that there is no x for which both

$$x \equiv 29(\text{mod } 52) \text{ and } x \equiv 19(\text{mod } 72) \text{ hold simultaneously.}$$

Solution :- We have that, $52 = \lambda\text{cm } [13, 4]$

Thus the congruence $x = 29(\text{mod } 52)$ is equivalent to the simultaneous congruences,

$$x \equiv 29(\text{mod } 4) \text{ and } x \equiv 29(\text{mod } 13)$$

which reduces to : $x \equiv 1(\text{mod } 4)$ and $x \equiv 3 (\text{mod } 13)$

Also, we have that, $72 = \lambda\text{cm } [9, 8]$

Thus the congruence $x \equiv 19 (\text{mod } 72)$ is equivalent to

$$x \equiv 19(\text{mod } 9) \text{ and } x \equiv 19(\text{mod } 8)$$

By the Chinese Remainder theorem, we know that the constraints (mod 13) and (mod 9) are independent of those (mod 8), since 8, 9, 13 are pairwise coprime. We observe that there is no x for which both $x \equiv 1(\text{mod } 4)$ and $x \equiv 3(\text{mod } 8)$ holds. Thus the given system is inconsistent.

Example :- Determine whether the system

$$x \equiv 3 (\text{mod } 10), x \equiv 8(\text{mod } 15), x \equiv 5(\text{mod } 84)$$

has a solution and find the solution if exists.

Solution :- We have that the congruence, $x \equiv 3 (\text{mod } 10)$ is equivalent to

$$x \equiv 3(\text{mod } 5) \text{ and } x \equiv 3 (\text{mod } 2)$$

which give $x \equiv 3 (\text{mod } 5)$ and $x \equiv 1(\text{mod } 2)$ …(1)

Again, the congruence, $x \equiv 8(\text{mod } 15)$ is equivalent to

$$x \equiv 8 (\text{mod } 5) \text{ and } x \equiv 8(\text{mod } 3)$$

which give : $x \equiv 3(\text{mod } 5)$ and $x \equiv 2(\text{mod } 3)$ …(2)

Also we have that the congreunce $x \equiv 5 (\text{mod } 84)$ is equivalent to

$$x \equiv 5 (\text{mod } 4), x \equiv 5 (\text{mod } 3), x \equiv 5(\text{mod } 7)$$

which give $x \equiv 1(\text{mod } 4), x \equiv 2(\text{mod } 3), x \equiv 5 (\text{mod } 7)$ …(3)

Thus, the given system is equivalent to a system of seven congruences given by (1), (2) and (3).

Now, we observe that the congruence $x \equiv 1 \pmod 2$ in (1) and the congruence $x \equiv 1 \pmod 4$ in (3) are consistent but the second one implies the first so that the first one may be dropped. Further, we see that the congruence $x \equiv 3 \pmod 5$ is common in (1) and (2) and the congruence $x \equiv 2 \pmod 3$ is common in (2) and (3) so we take them once

Hence, we conclude that the system of seven congruences reduces to system of four congruences given by

$$\left.\begin{aligned} &x \equiv 1 \pmod 4, \quad x \equiv 2 \pmod 3 \\ &x \equiv 3 \pmod 5, \quad x \equiv 5 \pmod 7 \end{aligned}\right] \qquad \ldots(*)$$

Since the moduli 3, 4, 5, 7 are pairwise coprime so by Chinese Remainder theorem the given system is consistent. The solution is calculated as follows :

From (∗), we have $a_1 = 1,\ a_2 = 2, a_3 = 3,\ a_4 = 5$

$m_1 = 4, m_2 = 3, m_3 = 5, m_4 = 7$

So $m = 4.3.5.7 = 420$

Now, we find the values of b_1, b_2, b_3, b_4 as under.

We know that $\dfrac{m}{m_j} b_j \equiv 1 \pmod{m_j}$

$$\Rightarrow \qquad \frac{m}{m_1} b_1 \equiv 1 \pmod{m_1} \ \Rightarrow 105\ b, \equiv 1 \pmod 4$$

or $\qquad b_1 \equiv 1 \pmod 4$

which gives $b_1 = 5$

Again $\dfrac{m}{m_2} b_2 \equiv 1 \pmod{m_2} \ \Rightarrow 140\ b_2 \equiv 1 \pmod 3$

$$\Rightarrow 2\ b_2 \equiv 1 \pmod 3$$

which gives, $b_2 = 2$

Similarly we find $b_3 = 4$, $b_4 = 2$

Hence the solution is

$$x_0 = \frac{m}{m_1} b_1 a_1 + \frac{m}{m_2} b_2 a_2 + \frac{m}{m_3} b_3 a_3 + \frac{m}{m_4}\ b_4 a_4$$

$$= 105.5.1 + 140.2.2 + 84.4.3 + 60.2.5 = 2693$$

Let x be the another solution then

$$x \equiv 2693 \pmod{420}$$

which gives x = 173

This completes the solution.

Congruences with prime power moduli

Theorem 1.42 Let f be a polynomial with integer coefficients, let m_1, m_2,…, m_r be positive integers relatively prime in pairs, and let $m = m_1m_2\ldots m_r$.

Then the congruence

$$f(x) \equiv 0 \pmod{m} \qquad \ldots(1)$$

has a solution if, and only if, each of the congruences

$$f(x) \equiv 0 \pmod{m_i} \qquad (i = 1, 2,\ldots, r) \qquad \ldots(2)$$

has a solution. Moreover, if v(m) and $v(m_i)$ denote the number of solutions of (1) and (2), respectively, then

$$v(m) = v(m_1)\, v(m_2)\ldots v(m_r). \qquad \ldots(3)$$

Proof :- If $f(a) \equiv 0 \pmod{m}$ then $f(a) \equiv 0 \pmod{m_i}$ for each i. Hence every solution of (1) is also a solution of (2).

Conversely, let a_i be a solution of (2). Then by the Chinese remainder theorem there exists an integer a such that

$$a \equiv a_i \pmod{m_i} \text{ for } i = 1, 2,\ldots, r \qquad \ldots(4)$$

so

$$f(a) \equiv f(a_i) \equiv 0 \pmod{m_i}.$$

Since the moduli are relatively prime in pairs we also have $f(a) \equiv 0 \pmod{m}$. Therefore if each of the congruences in (2) gives rise to a unique integer a mod m satisfying (4). As each a_i runs through the $v(m_i)$ solutions of (2) the number of integers a which satisfy (4) and hence (2) is $v(m_1)\ldots v(m_r)$. This proves the theorem.

Theorem 1.42 shows that the problem of solving a polynomial congruence

$$f(x) \equiv 0 \pmod{m}$$

can be reduced to that of solving a system of congruences

$$f(x) \equiv 0 \pmod{p_i^{\alpha_i}} \qquad (i = 1, 2,\ldots, r),$$

where $m = p_1^{\alpha_1}\ldots p_r^{\alpha_r}$. Now we show that the problem can be further reduced to congruences with prime moduli plus a set of linear congruences.

Let f be a polynomial with integer coefficients, and suppose that for some prime p and some $\alpha \geq 2$ the congruence

$$f(x) \equiv 0 \pmod{p^{\alpha}} \qquad \ldots(1)$$

has a solution, say x = a, where a is chosen so that it lies in the interval

$$0 \le a < p^{\alpha}.$$

This solution also satisfies each of the congruences $f(x) \equiv 0 \pmod{p^{\beta}}$ for each $\beta < \alpha$. In particular, a satisfies the congruence

$$f(x) \equiv 0 \pmod{p^{\alpha-1}}. \qquad \ldots(2)$$

Now divide a by $p^{\alpha-1}$ and write

$$a = qp^{\alpha-1} + r, \text{ where } 0 \le r < p^{\alpha-1}. \qquad \ldots(3)$$

The remainder r determined by (3) is said to be generated by a. Since $r \equiv a \pmod{p^{\alpha-1}}$ the number r is also a solution of (2). In other words, every solution a of congruence (1) in the interval $0 \le a < p^{\alpha}$ generates a solution r of congruence (2) in the interval $0 \le r < p^{\alpha-1}$.

Now suppose we start with a solution r of (2) in the interval $0 \le r < p^{\alpha-1}$ and ask whether there is a solution a of (1) in the interval $0 \le a < p^{\alpha}$ which generates r. If so, we say that r can be lifted from $p^{\alpha-1}$ to p^{α}. The next theorem shows that the possibility of r being lifted depends on f(r) mod p^{α} on the derivative $f'(r) \bmod p$.

Theorem 1.43 Assume $\alpha \ge 2$ and let r be a solution of the congruence

$$f(x) \equiv 0 \pmod{p^{\alpha-1}} \qquad \ldots(4)$$

lying in the interval $0 \le r < p^{\alpha-1}$.

(a) Assume $f'(r) \not\equiv 0 \pmod{p}$. Then r can be lifted in a unique way from $p^{\alpha-1}$ to p^{α}. That is, there is a unique a in the interval $0 \le a < p^{\alpha}$ which generates r and which satisfies the congruence

$$f(x) \equiv 0 \pmod{p^{\alpha}}. \qquad \ldots(5)$$

(b) Assume $f'(r) \equiv 0 \pmod{p}$. Then we have two possibilities :

If $f(r) \equiv 0 \pmod{p^{\alpha}}$, r can be lifted from $p^{\alpha-1}$ to p^{α} in p distinct ways.

If $f(r) \not\equiv 0 \pmod{p^{\alpha}}$, r cannot be lifted from $p^{\alpha-1}$ to p^{α}.

Proof :- If n is the degree of f we have the identity (Taylor's formula)

$$f(x + h) = f(x) + f'(x)h + \frac{f''(x)}{2!}h^2 + \ldots + \frac{f^{(n)}(x)}{n!}h^n \qquad \ldots(6)$$

for every x and h. We note that each polynomial $f^{(k)}(x)/k\,!$ has integer coefficients. Now take x = r in (6), where r is a solution of (4) in the interval $0 \le r < p^{\alpha-1}$, and let $h = qp^{\alpha-1}$ where q is an integer to be specified presently. Since $\alpha \ge 2$ the terms in (6) involving h^2 and higher powers of h are integer multiples of p^{α}. Therefore (6) gives us the congruence

$$f(r + qp^{\alpha-1}) \equiv f(r) + f'(r)\, qp^{\alpha-1} \pmod{p^{\alpha}}.$$

Since r satisfies (4) we can write $f(r) = kp^{\alpha-1}$ for some integer k, and the last congruence becomes

$$f(r + qp^{\alpha-1}) \equiv \{qf'(r) + k\}p^{\alpha-1} \pmod{p^{\alpha}}.$$

Now let

$$a = r + qp^{\alpha-1}. \qquad \ldots(7)$$

Then a satisfies congruence (5) if, and only if, q satisfies the linear congruence

$$qf'(r) + k \equiv 0 \pmod{p}. \qquad \ldots(8)$$

If $f'(r) \not\equiv 0 \pmod{p}$ this congruence has a unique solution q mod p, and if we choose q in the interval $0 \le q < p$ then the number a given by (7) will satisfy (5) and will lie in the interval $0 \le a < p^{\alpha}$.

On the other hand, if $f'(r) \equiv 0 \pmod{p}$ then (8) has a solution q if, and only if, $p|k$, that is, if and only if $f(r) \equiv 0 \pmod{p^{\alpha}}$. If $p \nmid k$ there is no choice of q to make a satisfy (5). But if $p \mid k$ then the p values $q = 0, 1\ldots, p - 1$ give p solutions a of (5) which generate r and lie in the interval $0 \le a < p^{\alpha}$. This completes the proof.

Unit-2

Quadratic Residues and Non-Residues

Definition :- Let p be an odd prime and let (a, p) = 1. Then a is said to be a quadratic residue (mod p) if ∃ an integer x such that

$$x^2 \equiv a \pmod{p}$$

otherwise we say that a is a quadratic non-residue (mod p).

Remark :- If a is a quadratic residue (mod p) ∃ x ($1 \le x \le p-1$) such that $x^2 \equiv a \pmod{p}$

Definition :- (Legendre symbol)

The Legendre Symbol denoted by $\left(\frac{a}{p}\right)$, where (a, p) = 1 is defined as

$\left(\frac{a}{p}\right) = 1$ if a is a quadratic residue (mod p) and

$\left(\frac{a}{p}\right) = -1$, if a is a quadratic non-residue (mod p).

Remark :- If $a \equiv b \pmod{p}$, clearly $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ provided (a, b) = 1

Theorem 2.1 Let p be an odd prime and let gcd (a, p) = 1 then

$$\underline{|p-1} = -\left(\frac{a}{p}\right).a^{\frac{1}{2}(p-1)} \pmod{p}$$

Proof :- Let S = {1, 2,…, p−1} is a reduced set of residues (mod p).

Consider any x such that

$1 \le x \le p-1$ then

$xS = \{x, 2x, \ldots, (p-1)x\}$

is also a reduced set of residues (mod p)

So there exists y in S such that $xy \equiv a \pmod{p}$

Now distinguish two cases

Case I :- $\left(\frac{a}{p}\right) = 1$ then $\exists$ x such that $1 \le x \le p-1$ such that

$$x^2 \equiv a \pmod p$$

Let us find out all the solutions of the quadratic congruence

$$X^2 \equiv a \pmod p \quad \ldots(I)$$

Then (I) has at least one solution X = x. We know two solutions x_1 and x_2 are said to be same if $x_1 \equiv x_2 \pmod p$. Let x_1 & x_2 be two solutions of (I) then

$$x_1^2 \equiv a \pmod p$$

and $x_2^2 \equiv a \pmod p$

$\Rightarrow$ $x_1^2 \equiv x_2^2 \pmod p$

$\Rightarrow$ p divides $(x_1^2 - x_2^2)$

$\Rightarrow$ $p \mid (x_1 + x_2)(x_1 - x_2)$

Then $p \mid (x_1 + x_2)$ or $p \mid (x_1 - x_2)$ (Θ p is a prime)

$\Rightarrow$ either $x_1 + x_2 \equiv 0 \pmod p$

or $x_1 - x_2 \equiv 0 \pmod p$

Further $x_2 \equiv -x_1 \equiv p - x_1 \pmod p$

or $x_2 \equiv x_1 \pmod p$

Thus x and p–x are two solutions of (1) (mod p) since x is a solutions of (1) (mod p)

Further $x \ne p - x$

$\mid \Theta$ p is odd

So (I) has exactly two solutions (mod p)

Let us take y_1 in S such that $y_1 \ne x$ & $y_1 \ne (p - x)$

Now consider the set y_1 S. Then y_1 S is also a reduced residue system (mod p). So $\exists$ y_2 in S such that

$$y_1 y_2 \equiv a \pmod p$$

and further $y_1 \ne y_2$ since otherwise y_1 will also be a solution of (1). Thus for $y_1 \ne x$, $y_1 \ne p - x$, the remaining (p–3) elements in S can be divided into $\frac{p-3}{2}$ pairs (y_1, y_2) such that

$$y_1 y_2 \equiv a \pmod p$$

So

$$1.2.3\ldots\ldots\ldots(p-1) = x.\ (p-x)\ (y_1, y_2)$$

$$\equiv -x^2.\ a^{\frac{p-3}{2}} \pmod p$$

$$\equiv -a^{\frac{1}{2}(p-1)} \pmod p \qquad (\Theta\ x^2 \equiv a(\text{mod } p))$$

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

Case II $\left(\frac{a}{p}\right) = -1$

Then the congruence (1) has no solutions. So if we take $y_1 \in S$, we know $\exists\ y_2 \in S$ such that

$$y_1\ y_2 \equiv a(\text{mod } p) \text{ amd } y_1 \neq y_2$$

Thus we divide S into $(p-1)/2$ pairs (y_1, y_2) such that $y_1\ y_2 \equiv a(\text{mod } p)$

$$\therefore \qquad \underline{|\ (p-1)} \equiv a^{\frac{p-1}{2}} \pmod p \equiv -\left(\frac{a}{p}\right) a^{\frac{p-1}{2}} \pmod p \left(\therefore \left(\frac{a}{p}\right) = -1\right)$$

Thus theorem is proved completely.

Wilson's Theorem

Theorem 2.2 If p is any prime, then $\underline{|\ p-1} \equiv -1(\text{mod } p)$

Proof :- If p = 2 or p = 3; theorem is clearly true.

So let $p \geq 5$. Taking a = 1 in the last theorem we note $\left(\frac{1}{p}\right) = 1$ for all prime p.

Then we get

$$\underline{|\ p-1} \equiv -1 \pmod p$$

Converse of Wilson's Theorem :- The converse of Wilson's theorem is also true. Given that $\underline{|\ n-1} \equiv -1 \pmod n$, they must be a prime.

Proof :- If possible, suppose n is not a prime. Then there exists a divisor d of n such that

$$1 < d < n, \text{ then } \quad d \mid \underline{|\ n-1}$$

$$\therefore \qquad \underline{|\ n-1} \equiv 0 \pmod d$$

On the other hand

$$\underline{|\, n-1} \equiv -1 \pmod{n}$$

$$\Rightarrow \qquad \underline{|\, n-1} \equiv -1 \pmod{d}$$

$$\Rightarrow \qquad -1 \equiv 0 \pmod{d} \Rightarrow d \mid 1 \text{ which contradicts that } d>1.$$

So n must be a prime number.

Theorem 2.3 (Euler's Criterion) :- Let p be an odd prime and let gcd (a, p) ≡ 1. Then

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

Proof :- We know

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

We also know $\underline{|\, (p-1)} \equiv -1 \pmod{p}$

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

Multiplying by $\left(\frac{a}{p}\right)$ we get

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

Theorem 2.4 −1 is a quad reside of primes of the form 4k + 1 & a quad non-residue of primes of the form 4 k + 3.

Proof :- By Euler's Criterion

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

$$\Rightarrow \qquad p \left| \left[\left(\frac{-1}{p}\right) - (-1)^{\frac{1}{2}(p-1)} \right] \right.$$

The value of the quantity in brackets is either 0 or −2. But p is an odd prime and it divides the quantity in brackets, so we must have

$$\left(-\frac{1}{p}\right) - (-1)^{\frac{1}{2}(p-1)} = 0$$

$$\Rightarrow \qquad \left(-\frac{1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}$$

When p = 4k+1, $\left(-\frac{1}{p}\right) = (-1)^{\frac{4k}{2}} = (-1)^{2k} = 1$

and when p = 4k + 3,

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

Theorem 2.5 Let a & b be integers such that gcd (ab, p) =1, then

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

Proof :- By Euler's criterian,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{1}{2}(p-1)} \equiv a^{\frac{1}{2}(p-1)} b^{\frac{1}{2}(b-1)} \pmod{p} \qquad \ldots(1)$$

But gcd (ab, p) = 1 $\Rightarrow$ p $\nmid$ (a b)

$\Rightarrow$ b $\nmid$ a and p $\nmid$ b.

$\Rightarrow$ g c d(a, p) = 1 = gcd(b, p)

By Euler's criterion,

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

and $$\left(\frac{b}{p}\right) \equiv b^{\frac{1}{2}(p-1)} \pmod{p} \qquad \ldots(3)$$

From (2), (3), we get

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

$$\Rightarrow \qquad p \left| \left(\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - \left(\frac{ab}{p}\right) \right) \right.$$

$$\Rightarrow \qquad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \qquad (\ \Theta\ p \text{ is an odd prime})$$

Corollary :- The product of two quadratic residues (mod p) or two quadratic non-residues (mod p) is a quadratic residues (mod p) where as the product of a quadratic residue (mod p) and a quadratic non-residue (mod p) is quadratic non-residue (mod p)

Theorem 2.6 Let p be an odd prime and let p does not divide product ab where a & b are integers. Then $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$

Proof :- Since $p \nmid ab \Rightarrow b \nmid a$ & $p \nmid b$

$$\Rightarrow \qquad p \nmid b^2,$$

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right)$$

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

$[\ \Theta\ (\pm 1)^2 = 1$

Theorem 2.7 Given any odd prime p, there are $\frac{1}{2}(p-1)$quadratic residue & $\frac{1}{2}(p-1)$ quadratic non-residues.

Proof :- Let a be any quadratic residue then $\exists\ x\ (1 \le x \le p-1)$ such that

$$x^2 \equiv a \pmod{p}$$

But $\qquad x^2 \equiv (p-x)^2 \pmod{p}$

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

$$2^2 \equiv (p-2)^2 \pmod{p}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

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

Thus there are a maximum of $\frac{p-1}{2}$ quadratic residue (mod p)

But for $1 \le i, j \le \frac{p-1}{2}, i \ne j$

$$i^2 \not\equiv j^2 \pmod p$$

since if $i^2 \equiv j^2 \pmod p \Rightarrow p \mid (i^2 - j^2)$

$\Rightarrow$ $p \mid (i+j)(i-j) \Rightarrow p \mid (i+j)$ or $p \mid (i-j)$

which is not possible under the given condition. So there are exactly $\frac{1}{2}$ (p−1) quadratic residues.

The remaining $\frac{p-1}{2}$ numbers must be quadratic non−residues

Theorem 2.8 Given any prime p of the for 4k+1, ∃ x and on integers m such that

$$1 + x^2 = mp \text{ where } 1 \le m < p$$

Proof :- Since −1 is a quadratic residue of primes of the form 4k+1, ∃ x such that

$$x^2 \equiv -1 \pmod p$$

∴ W.L.O.G, we can assume $1 \le x \le \frac{p-1}{2}$.

Then ∃ an integer m such that

$$mp = x^2 + 1 \le 1 + \left(\frac{p-1}{2}\right)^2 < p^2$$

$\Rightarrow$ $m < p$

Clearly $m > 0$

$\Rightarrow$ $1 \le m < p$

Theorem 2.9 Given any prime p, there exist $x \ge 0$, $y \ge 0$ and m ($1 \le m < p$) such that $1 + x^2 + y^2 = mp$

Proof :- If p = 2, theorem is trivially true

$\Theta\ 1 + 1^2 = 2 = 1.\ 2$

So let p be an odd prime.

Consider $S = \left\{-x^2; x = 0,1,2,\ldots\ldots,\frac{p-1}{2}\right\}$

$$T = \left\{1+y^2; y = 0,1,2,\ldots.,\frac{p-1}{2}\right\}$$

Here elements of S are mutually incongruent (mod p).

Similarly elements of T are mutually incongruent. S contains $\frac{p+1}{2}$ elements and T also contain $\frac{p+1}{2}$ elements.

$\therefore$ SUT contains p + 1 district element . But there are only p residue classes (mod p)

Therefore at least two elements of SUT must be congruent to each other (mod p). However, no element of S is congruent to another element of S and no element of T is congruent to another element of T. So atleast one element of S must be congruent to an element of T i.e.,

$\exists$ x, y such that $0 \le x \le p-1/2$ and $0 \le y \le p-1/2$ such that

$$-x^2 \equiv 1 + y^2 \pmod{p}$$

or $$1 + x^2 + y^2 \equiv 0 \pmod{p}$$

So, $\exists$ an integer m such that

$$1 + x^2 + y^2 = mp$$

Clearly m > p

Now $$mp = 1+x^2+ y^2 \le 1 + \left(\frac{p-1}{2}\right)^2 + \left(\frac{p-1}{2}\right)^2$$

$$< 1 + \frac{p^2}{4} + \frac{p^2}{4} < p^2$$

$\Rightarrow$ $m< p$ and so $1 \le m < p$ which proves the theorem

Definition :- Let $m \ge 2$ be any given integer and let gcd (a, m) = 1 for some integer a. Then by Euler Fermat theorem,

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

Now take $S = \{n \in N;\ a^n \equiv 1 \pmod m\}$

then $S \neq \phi$ since $\phi(m) \in S$. So by L. W. O., S has a smallest element say 'd'. Then we say d is the order of a (mod m) and we write $d = \text{ord}_m^a$ (order a mod m)

Theorem 2.10 Let $\text{ord}_m^a = d$ then

$$a^n \equiv 1 \pmod m$$

$\Leftrightarrow$ $d \mid n$. In particular $d \mid \phi(m)$

Proof :- Since $a^{\phi} \equiv 1 \pmod m$, so if $d \mid n$, then

$$a^n \equiv 1 \pmod m$$

Now let $a^n \equiv 1 \pmod m$. By division algorithm theorem, write

$$n = dq + r, \quad 0 \leq r < d$$

then

$$1 \equiv a^n = a^{dq+r} = a^{dq} - a^r$$

$$= (a^d)^q \cdot a^r$$

$$\equiv a^r \pmod m \qquad (\Theta\ a^d \equiv 1 \pmod m)$$

So if $r \neq 0$, then we get a number $r < d$ such that $a^r \equiv 1 \pmod m$ which contradicts the definition of d

$\Rightarrow$ $r = 0 \Rightarrow d \mid n$

Theorem 2.11 Let $\text{ord}_m^a = d$. Then for any positive integer k,

$$\text{ord}_m^{a^k} = \frac{d}{\gcd(d,k)}$$

Proof :- Let gcd (d, k) = g and $\text{ord}_m^{a^k} = r$

Then $1 \equiv (a^k)^r \equiv a^{kr} \pmod m$

$\Rightarrow$ $d \mid kr$

$\Rightarrow$ $\frac{d}{g} \left| \left(\frac{k}{g}\right) r \right.$

But $\gcd\left(\frac{d}{g}, \frac{k}{g}\right) = 1$

$\Rightarrow$ $\frac{d}{q} \mid r \quad \Rightarrow \quad \frac{d}{q} \leq r$. Now since gcd (d, k) = q

$\Rightarrow$ $q \mid d, q \mid k$

Let $k = qk_1$

Now $(a^k)^{\frac{d}{q}} = (a^{qk_1})^{d/q} = a^{k_1 d} = (a^d)^{k_1}$

$\equiv 1 \pmod m$

$\Rightarrow$ $r \leq \frac{d}{g}$ [By definition of order]

So $\frac{d}{g} = r$

or $r = \frac{d}{q}$

Hence the theorem.

Gauss's Lemma 2.12 Let p be an odd prime and let gcd (a, p) = 1.

Let $S = \left\{1, 2, ..., \frac{p-1}{2}\right\}$

Let μ be the number of elements in the set S such that least positive residue of aS > p/2.

Then $\left(\frac{a}{p}\right) = (-1)^{\mu}$

Proof :- Consider any integer n where gcd (n, p) = 1 Apply division algorithm to n & p, $\exists$ q & r such that $n = qp + r$ where $0 \leq r \leq (p-1)$. Since gcd (n, p) = 1 $\Rightarrow p \nmid n \Rightarrow r \neq 0$

$\Rightarrow$ $1 \leq r \leq p-1$

Since p is odd, p/2 is not an integer. So either r < p/2 or r > p/2. If r < p/2, we leave it as it is If r > p/2, write $r = p - r'$ where $1 \leq r' < p/2$,

Thus $n = qp + (p - r') = (q+1)\, p - r' \equiv -r' \pmod p$.

Now we consider least positive residues of every element of aS. We are given that μ of those elements have least positive residues > p/2. Let k be the elements of aS with least positive residues < p/2.

Then $k + \mu = \frac{p-1}{2}$

If the least positive residues <p/2 are $r_1, r_2, \ldots, r_k$ and the least positive residues > p/2 are $-r_1, -r_2^1, \ldots, -r_\mu$ such that $1 \le r_\mu \le \frac{p-1}{2}$ then

$$\left\{r_1, \ldots, r_k, -r_1 - r_2, \ldots, -r_\mu\right\}$$

are the residues of elements of aS in some order such that

$$1 \le r \le \frac{p-1}{2} \text{ and } 1 \le r' \le \frac{p-1}{2}.$$

Since S is a subset of a reduced residue set {1, 2,…, p−1} and gcd (a, p) = 1, so {a, 2a,…, (p−1)a} is also a reduced residue set. Then first of all

$$r_i \neq r_j \text{ for } i \neq j$$

If possible, let $r_i = r_j$ for some pair (i, j)

Then $\exists\ x_i \in S$ and $x_j \in S$ such that

$$ax_i \equiv r_i \pmod p \ \&\ ax_j \equiv -r_j \pmod p$$

But $r_i = r_j$

$\Rightarrow$ $ax_i \equiv -ax_j \pmod p$

This means $a(x_i + x_j) \equiv 0 \pmod p$

$\Rightarrow$ $p \mid a(x_i + x_j)$

But gcd (a, p) = 1

$\Rightarrow$ $p \mid (x_i + x_j)$

But $1 < x_i \le \frac{p-1}{2}$

and $1 \le x_j \le \frac{p-1}{2}$

$\Rightarrow$ $2 \le x_i + x_j \le p-1$

$\Rightarrow \qquad p \nmid (x_i + x_j)$

which is a contradiction and so $\{r_1, r_2, \ldots, r_k, r_1, r_2, \ldots, r_\mu\}$ are all distinct.

But $\qquad \mu + k = \dfrac{p-1}{2}$

So there are $\dfrac{p-1}{2}$ distinct numbers lying between 1 & $\dfrac{p-1}{2}$

So $\qquad r_1, \ldots, r_k, r_1, \ldots, r_\mu$

are the natural numbers 1 to $\dfrac{p-1}{2}$ in some order. Therefore

$$\left\lfloor \frac{p-1}{2} \right\rfloor = r_1, \ldots r_k, r_1, \ldots, r_\mu \pmod p$$

Then by definition of $r_1, \ldots, r_k, r_1, \ldots, r_\mu$

$$\left\lfloor \frac{p-1}{2} \right\rfloor \equiv a \cdot 2a \ldots \frac{p-1}{2} \cdot a(-1)^\mu \pmod p$$

$$= (-1)^\mu \left(\left\lfloor \frac{p-1}{2} \right\rfloor \right) a^{\frac{p-1}{2}} \pmod p$$

But $\qquad \gcd\left(\left\lfloor \dfrac{p-1}{2} \right\rfloor, p \right) = 1$

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

But by Euler's criterion,

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

$\Rightarrow \qquad (-1)^\mu \left(\dfrac{a}{p} \right) \equiv 1 \pmod p$

$\Rightarrow \qquad \left(\dfrac{a}{p} \right) \equiv (-1)^\mu \pmod p$

But the value of $\left(\frac{a}{p}\right) - (-1)^{\mu}$ is either 2 or 0 or −2 and p is an odd prime

$$\Rightarrow \qquad \left(\frac{a}{p}\right) = (-1)^{\mu}$$

Application of Gauss's Lemma :-

Theorem 2.13 For every odd prime p,

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

where [x] means greatest integer

Proof :- Let $S = \left\{1, 2, ..., \frac{p-1}{2}\right\}$

Then $2S = \{2, 4, \ldots, p-1\}$

Let $x \in S$, then the number of elements of 2S with least positive value $< \frac{p}{2}$ is x $< \frac{p}{4}$.

But x is an integer $\Rightarrow$ x =[p/4]

$\therefore$ The number of elements of 2S with least positive value > p/2 is $\frac{p-1}{2} - \left[\frac{p}{4}\right]$

(i) If p is of the form 4k+1, then

$$\mu = \left(\frac{p-1}{2}\right) - \left[\frac{p}{4}\right]$$

$$= \frac{4k+1-1}{2} - \left[\frac{4k+1}{4}\right]$$

$$= 2k - k = k = \left[\frac{p-1}{4}\right] = \left[\frac{p+1}{4}\right]$$

(ii) If p is of the form, 4k + 3 then

$$\mu = \frac{p-1}{2} - \left[\frac{p}{4}\right] = \frac{4k+3-1}{2} - \left[\frac{4k+3}{4}\right]$$

$$= 2k + 1 - k = k + 1 = \left[\frac{k+1}{4}\right]$$

Thus in both cases, $\mu = \left[\frac{(p+1)}{4}\right]$

So by Gauss's Lemma

$$\left(\frac{2}{p}\right) = (-1)^{\mu} = (-1)^{\left[\frac{1}{4}(p+1)\right]}$$

Corollary :- 2 is a quadratic residue of primes of the form $8k \pm 1$ and quadratic non residues of primes of the form $8k \pm 3$.

Proof :- Let $p = 8k \pm 1$

Then $$\left[\frac{1}{4}(k+1)\right] = \left[\frac{1}{4}\left((8k \pm 1)+1\right)\right] = 2k$$

Therefore, in these two cases

$$\left(\frac{2}{p}\right) = (-1)^{\left[\left(\frac{p+1}{4}\right)\right]} = (-1)^{2k} = 1$$

Let $p = 8k \pm 3$

Then $$\left[\frac{1}{4}(p+1)\right] = \left[\frac{1}{4}(8k+4)\right] = 2k+1$$

and if $p = 8k-3$

Then $$\left[\frac{1}{4}(p+1)\right] = \left[\frac{1}{4}(8k-3+1\right]$$

$$= \left[\frac{1}{4}(8k-2)\right] = 2k-1$$

Therefore in these two cases

$$\left(\frac{2}{p}\right) = -1$$

Therefore 2 is a quadratic non–residue.

Corollary 2:- For every odd prime p

$$\left(\frac{2}{p}\right) = (-1)^{\left(\frac{p^2-1}{8}\right)}$$

Proof :- We know 2 is a quadratic residue of primes of the form $8k \pm 1$ & a quadratic non-residue of primes of the form $8k \pm 3$.

Let $p = 8k \pm 1$

Then $$\frac{p^2-1}{8} = \frac{(8k \pm 1)^2 - 1}{8} = \frac{64k^2 \pm 16k + 1 - 1}{8}$$

$$= 8k^2 \pm 2k$$

= an even number

$$\Rightarrow \quad (-1)^{\frac{p^2-1}{8}} = 1 = \left(\frac{2}{p}\right)$$

Let $p = \cdot 8k \pm 3$

Then $$\frac{p^2-1}{8} = \frac{(8k \pm 3)^2 - 1}{8}$$

$$= \frac{64k^2 \pm 48k + 9 - 1}{8}$$

$$= \frac{64k^2 \pm 48k + 8}{8}$$

$$= 8k^2 \pm 6k + 1$$

= An odd number.

Therefore $(-1)^{\frac{p^2-1}{8}} = -1 = \left(\frac{2}{p}\right)$

Thus in all cases

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Quadratic Law of Reciprocity :- For Legendre Symbols

Statement :- Let p & q be distinct odd primes then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = (-1)^{p'q'}$$

where $p' = \frac{p-1}{2}, q = \frac{q-1}{2}$

Alternative statements :-

(i) Let p or q be a prime of the form 4k + 1. Then either p′ is even or q′ is even

$\Rightarrow$ p′q′ is even

$\therefore$ $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1 \Rightarrow \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$

(ii) If both p & q are of the form 4k + 3 then both p′ & q′ are odd.

Therefore $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$

$\Rightarrow$ $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

So sometimes Quadratic Law of Reciprocity is also asked in the following form.

Theorem 2.14 Let p & q be two distinct odd primes. Then

$$\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$$ if either of p & q is of the form 4k + 1

and $$\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right)$$ if both of p & q are of the form 4k + 3.

Proof :- By Gauss's Lemma

$$\left(\frac{q}{p}\right)=(-1)^{\nu}$$

where ν is the number of integers x $\left(1 \le x \le \frac{p-1}{2}\right)$ such that

$$qx = py + r \text{ where } -\frac{p}{q} < r < 0$$

Since q > 0, x > 0 and r < 0

$\Rightarrow$ $(p\ y) > 0 \Rightarrow y \ge 1$

Further

$$p\ y = qx - r < \frac{p-1}{2}q + \frac{p}{2} < \frac{p}{2}\ (q+1)$$

$$\Rightarrow \quad y < \frac{q+1}{2}$$

$$\Rightarrow \quad y \le \frac{q-1}{2}$$

Similarly $\left(\frac{p}{q}\right)=(-1)^{\mu}$ where μ is the number of integers y $\left(1 \le y \le \frac{q-1}{2}\right)$

such that py = qx + s where $-\frac{q}{2} < s < 0$

Therefore $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\mu+\nu} \qquad \ldots(1)$$

where $\mu + \nu$ is the number of pairs of integers (x, y) such that $1 \le x \le \frac{p-1}{2}$

$$1 \le y \le \frac{q-1}{2}$$

and $$-\frac{p}{2} < r = qx - py = -s < \frac{q}{2}$$

Now, let us consider the following sets of pairs of integers (x, y)

$$S = \left\{(x, y) : 1 \le x \le \frac{p-1}{2}; 1 \le y \le \frac{q-1}{2}\right\}$$

$$S_1 = \left\{(x, y) \in S; qx - py) \le -\frac{p}{2}\right\}$$

$$S_2 = \left\{(x, y) \in S; -\frac{p}{2} < qx - py < \frac{q}{2}\right\}$$

$$S_1 = \left\{(x, y) \in S; (qx - py) \ge \frac{q}{2}\right\}$$

Then $$\#(S) = \#(S_1) + \#(S_2) + \#(S_1) \qquad \ldots(II)$$

Consider a mapping θ from S defined by

$$\theta((x, y)) = \left(\frac{p+1}{2} - x, \frac{q+1}{2} - y\right)$$

Since $$1 \le x \le \frac{p-1}{2} \;\&\; 1 \le y \le \frac{q-1}{2}$$

$\Rightarrow$ $$1 \le \frac{p+1}{2} - x \le \frac{p-1}{2}$$

and $$1 \le \frac{q+1}{2} - y \le \frac{q-1}{2}$$

So that θ is a mapping from S to S. Now, let $(x, y) \in S_1$

Then, by definition

$$\theta((x, y)) = \left(\frac{p+1}{2} - x, \frac{q+1}{2} - y\right) = (x', y') \text{ (say)}$$

Now $qx' - py' = q\left(\frac{p+1}{2} - x\right) - p\left(\frac{q+1}{2} - y\right)$

$= \frac{q}{2} - \frac{p}{2} - (qx - py)$

$\geq \frac{q}{2} - \frac{p}{2} - \left(-\frac{p}{2}\right)$ $\quad (\Theta\ (x, y) \in S_1)$

$= q/2$

$\Rightarrow$ $(x', y') \in S_1$

This means

$$\#(S_1) \leq \#(S_1) \qquad \ldots(III)$$

Now, let $(x, y) \in S_1$

then $qx' - py' = q\left(\frac{p+1}{2} - x\right) - p\left(\frac{q+1}{2} - y\right)$

$= \frac{q}{2} - \frac{p}{2} - (qx - py)$

$\leq \frac{q}{2} - \frac{p}{2} - \frac{q}{2}$ $\quad [\Theta\ (x, y) \in S_1$

$= -p/2$

$\Rightarrow$ $(x', y') \in S_1$

$\Rightarrow$ $\#(S_1) \leq \#(S_1)$ $\qquad \ldots(IV)$

From (III) & (IV) we get

$$\#(S_1) = \#(S_1) \qquad \ldots(V)$$

Therefore from (II) & (V) we get

$$\#(S) \equiv \#(S_2) \pmod 2$$

But $\#(S) = p'.\, q'$

$\Rightarrow$ $\#(S_2) = \mu + \nu$

$$\equiv p'\, q' \pmod 2$$

$\therefore$ From (I); $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{p'q'}$

Example :- Evaluate

$$\left(\frac{202}{257}\right)$$

or Determine Determine whether 202 is a quadratic residue of 257 or not? or

$x^2 \equiv 202 \pmod{257}$ is solvable or not.

Solution :- $202 = 2\times 101$

$$\left(\frac{202}{257}\right) = \left(\frac{2}{257}\right)\left(\frac{101}{257}\right)$$

$$\left(\frac{2}{257}\right) = 1 \text{ since}$$

$$257 \equiv 1 \pmod 8$$

$$\therefore \qquad \left(\frac{202}{257}\right)=\left(\frac{101}{257}\right)=\left(\frac{257}{101}\right)$$

$$\left|\Theta\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)\right.$$

$$=\left(\frac{55}{101}\right)$$

$$=\left(\frac{5}{101}\right)\left(\frac{11}{101}\right)$$

But $$\left(\frac{5}{101}\right)=\left(\frac{101}{5}\right)=\left(\frac{1}{5}\right)=1$$

and $$\left(\frac{11}{101}\right)=\left(\frac{101}{11}\right)$$ [

By Reciprocity law

$$=\left(\frac{2}{11}\right)$$

$$=-1$$

$$\therefore \qquad \left(\frac{202}{257}\right)=-1$$

Alternative $$\left(\frac{202}{257}\right)=\left(\frac{-55}{257}\right)$$

$$=\left(\frac{-1}{257}\right)\left(\frac{5}{257}\right)\left(\frac{11}{257}\right)$$

$\Rightarrow$

$$\left(\frac{-1}{257}\right)=1\left(\frac{5}{257}\right)=\left(\frac{257}{5}\right)-\left(\frac{2}{5}\right)=-1\left(\frac{11}{257}\right)=\left(\frac{257}{11}\right)=\left(\frac{4}{11}\right)=1$$

$\therefore \quad \left(\frac{202}{257}\right) = (1)\,(-1)\,(1) = -1$

Example :- $\left(\frac{650}{401}\right) = \left(\frac{26}{401}\right)\left(\frac{25}{401}\right)$

$$= \left(\frac{25}{401}\right)\left(\frac{2}{401}\right)\left(\frac{13}{401}\right)$$

$$= \left(\frac{13}{401}\right)$$

$$= \left(\frac{401}{13}\right) = \left(\frac{11}{13}\right) = \left(\frac{13}{11}\right)$$

$$= \left(\frac{2}{11}\right) = -1$$

Theorem 2.15 If p is an odd prime & gcd (a, 2p) = 1

then $\left(\frac{a}{p}\right) = (-1)^t$

where $t = \sum_{j=1}^{p-1} \left[\frac{j\,a}{p}\right]$

Also $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Proof :- Let $S = \left\{1, 2, ..., \frac{p-1}{2}\right\}$

Let $r_1, \ldots, r_\lambda$ and $r_1 ..., r_\mu$

be the least positive remainders of the elements of the set aS, which are < p/2 and > p/2 respectively.

Then as shown in the proof of Gauss's Lemma

$$r_1,\ldots, r_\lambda, p-r_1,...,p-r_\mu$$

are all distinct.

Since $\lambda + \mu = \frac{p-1}{2}$. Therefore $r_1,\ldots, r_\lambda, p-r_1...p-r_\mu^1$ are the integers $1, 2,\ldots, \frac{p-1}{2}$ in some order so that

$$\sum_{j=1}^{\frac{p-1}{2}} j = r_1 + r_2 +\ldots+ r_\lambda + \sum_{s=1}^{\mu} (p - r_j)$$

$$= \mu p + \sum_{i=1}^{\lambda} r_i - \sum_{j=1}^{\mu} r_j \qquad \ldots(I)$$

Further by definition of $r_1, \ldots r_\lambda, r_1,...,r_\mu$

$$\sum_{j=1}^{\frac{p-1}{2}} (j\,a) = \sum_{j=1}^{\frac{p-1}{2}} p\left[\frac{j\,a}{p}\right] + \sum_{i=1}^{\lambda} r_i + \sum_{j=1}^{\mu} r_j \qquad \ldots(II)$$

Subtracting (I) from (II), we get

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = p\,t + 2\sum_{j=1}^{\mu} r_j - \mu p \text{ where } t = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{j\,a}{p}\right] \qquad \ldots(III)$$

But $$\sum_{j=1}^{\frac{p-1}{2}} j = \frac{p^2-1}{8}$$

$\therefore$ $$(a-1)\left(\frac{p^2-1}{8}\right) = p(t-\mu) + 2\sum_{j=1}^{\mu} r_j \qquad \ldots(IV)$$

Since g.c.d. (a, 2p) = 1

$\Rightarrow$ a is odd.

$\Rightarrow$ $(a-1)$ is even. Also $\frac{p^2-1}{8}$ is an integers as p is odd

$\therefore$ From (IV), we get

$t - \mu \equiv 0 \pmod 2$ as p is odd

$\Rightarrow$ $\mu \equiv t \pmod 2$

By Gauss's Lemma

$$\left(\frac{a}{p}\right) = (-1)^{\mu}$$

Therefore $$\left(\frac{a}{p}\right) = (-1)^{t}$$

Now set a = 2 in (II) Since for j = 1, 2,…, $\frac{p-1}{2}$

$$\left[\frac{i\,j}{p}\right] = 0 \text{ for all } j \Rightarrow t = 0$$

$\therefore$ From (III), e get $\sum_{j=1}^{\frac{b-1}{2}} j + \mu p = 2\sum_{j=1}^{\mu} i\,j$

$\therefore$ $\sum_{j=1}^{\frac{p-1}{2}} j \equiv -\mu\, p \pmod 2$ 2\ RHS $\therefore$ 2\LHS

But $p \equiv -1 \pmod 2$

$\therefore$ $\mu \equiv \sum_{j=1}^{\frac{p-1}{2}} j \equiv \frac{p^2-1}{8} \pmod 2$

$\therefore$ By Gauss's Lemma

$$\left(\frac{2}{p}\right) = (-1)^{\mu} = (-1)^{\frac{p^2-1}{2}}$$

The Jacobi Symbol :- Let $Q > 1$ be an odd integer and $Q = q_1 q_2 \ldots q_s$ its prime factorization where $q_1, q_2, \ldots, q_s$ are odd primes, not necessarily distinct. Then the Jacobi symbol, denoted by $\left(\frac{P}{Q}\right)$, is defined as :

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s}\left(\frac{P}{q_i}\right) = \left(\frac{P}{q_1}\right)\left(\frac{P}{q_2}\right)\ldots\left(\frac{P}{q_s}\right)$$

where $\left(\frac{P}{q_j}\right)$ is the Legendre symbol.

Remarks 1. If Q itself is an odd prime then the Jacob symbol and Legendre symbol are same

(2) If gcd(P, Q) > 1, then $\left(\frac{P}{Q}\right) = 0$

For, $\gcd(P, Q) > 1 \Rightarrow q_i \mid P$ for some i $(1 \le i \le j)$

The corresponding Legendre symbol $\left(\frac{P}{q_i}\right) = 0$ and hence $\left(\frac{P}{Q}\right) = 0$

(3) If gcd(P, Q) = 1, then $\left(\frac{P}{Q}\right) = \pm 1$

(4) If P is a quadratic residue mod Q, then P is a quadratic residue mod each prime q_j dividing Q, so that $\left(\frac{P}{q_j}\right) = 1$ for each j and hence $\left(\frac{P}{Q}\right) = 1$. However $\left(\frac{P}{Q}\right) = 1$ does not imply that P is a quadratic residue of Q.

Theorem 2.16 Let Q and Q′ be odd and positive, then

(1) $\left(\frac{P}{Q}\right)\left(\frac{P}{Q}\right) = \left(\frac{P}{QQ}\right)$

(2) $\left(\frac{P}{Q}\right)\left(\frac{P}{Q}\right) = \left(\frac{PP}{Q}\right)$

(3) If gcd(P, Q) = 1, then $\left(\frac{P^2}{Q}\right)=\left(\frac{P}{Q^2}\right)=1$

(4) If gcd(PP′, QQ′) = 1, then $\left(\frac{P^1P^2}{Q^1Q^2}\right)=\left(\frac{P}{Q}\right)$

(5) $P' \equiv P \pmod{Q} \Rightarrow \left(\frac{P}{Q}\right)=\left(\frac{P}{Q}\right)$

Proof :- (1) Since Q and Q′ are odd, so QQ′ is odd. Let $Q = q_1 q_2 \ldots q_r$ and $Q' = q'_1 q'_2 \ldots q'_s$ where $q_1, q_2 \ldots, q_r, q'_1 \ldots, q'_s$ are all odd primes, not necessarily distinction then, we have,

$$QQ' = q_1 q_2 \ldots q_r q_1' q_2' \ldots q_s'$$

Hence, by definition

$$\left(\frac{P}{QQ}\right)=\left(\frac{P}{q_1}\right)\left(\frac{P}{q_2}\right)\ldots\left(\frac{P}{q_r}\right)\left(\frac{P}{q_1}\right)\left(\frac{P}{q_2}\right)\ldots\left(\frac{P}{q_s}\right)$$

$$= \prod_{i=1}^{r}\left(\frac{P}{q_i}\right)\prod_{j=1}^{s}\left(\frac{P}{q_j}\right)$$

$$= \left(\frac{P}{Q}\right)\left(\frac{P}{Q}\right)$$

(2) we have :

$$\left(\frac{PP}{Q}\right)=\left(\frac{PP}{q_1}\right)\left(\frac{PP}{q_2}\right)\ldots\left(\frac{PP}{q_r}\right)$$

$$= \prod_{i=1}^{r}\left(\frac{PP}{q_i}\right)=\prod_{i=1}^{r}\left(\frac{P}{q_i}\right)\left(\frac{P}{q_i}\right)$$

$$\left(\Theta \text{ in Legendre symbol}, \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)\right)$$

$$= \prod_{i=1}^{r}\left(\frac{P}{q_i}\right)\prod_{i=1}^{r}\left(\frac{P}{q_i}\right)$$

$$= \left(\frac{P}{Q}\right)\left(\frac{P}{Q}\right)$$

(3) We have

$$\left(\frac{P^2}{Q}\right) = \left(\frac{PP}{Q}\right) = \left(\frac{P}{Q}\right)\left(\frac{P}{Q}\right) \qquad \text{[By part (2)]}$$

$$= 1$$

$$\left(\Theta\,(P,Q) = 1 \Rightarrow \left(\frac{P}{Q}\right) = \pm 1\right)$$

Similarly $\left(\frac{P}{Q^2}\right) = \left(\frac{P}{Q}\right)\left(\frac{P}{Q}\right) = 1$

(4) we have

$$\left(\frac{P^1P^2}{Q^1Q^2}\right) = \left(\frac{P^1}{Q^1Q^2}\right)\left(\frac{P^2}{Q^1Q^2}\right) \qquad \text{[By part (2)]}$$

$$= \left(\frac{P^1}{Q^1}\right)\left(\frac{P^1}{Q^2}\right)\left(\frac{P^2}{Q^1}\right)\left(\frac{P^2}{Q^2}\right) \qquad \text{[By part (1)]}$$

$$= \left(\frac{P^1}{Q^1}\right)\left(\frac{P^1}{Q^2}\right)\left(\frac{P^2}{Q^1}\right)\left(\frac{P}{Q^2}\right)\left(\frac{P}{Q^2}\right) \qquad \text{[By part (2)]}$$

$$= \left(\frac{P}{Q}\right).1.1.1.1 = \left(\frac{P^1}{Q^1}\right) \qquad \text{[By part (3)]}$$

(5) We have

$$P' \equiv P \pmod{Q} \text{ and } Q = q_1\, q_2 \ldots q_r$$

$\Rightarrow$ $\quad P' \equiv P \pmod{q_i}\ \forall\ i = 1, 2, \ldots, r$

But in the case of Legendre symbol, we know that

if $a \equiv b \pmod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

Hence, $\left(\frac{P}{q_i}\right) = \left(\frac{P}{q_i}\right)$ for i = 1, 2,…, r

$$\Rightarrow \quad \prod_{i=1}^{r}\left(\frac{P}{q_i}\right) = \prod_{i=1}^{r}\left(\frac{P}{q_i}\right) \Rightarrow \left(\frac{P}{Q}\right) = \left(\frac{P}{Q}\right)$$

This completes the proof.

Theorem 2.17 If Q is positive and odd, then

(1) $$\left(\frac{-1}{Q}\right) = (-1)^{(Q-1)/2} \text{ and}$$

(2) $$\left(\frac{2}{Q}\right) = (-1)^{(Q^2-1)/8}$$

Proof :- We have

$$\left(\frac{-1}{Q}\right) = \prod_{j=1}^{s}\left(\frac{-1}{q_j}\right) \qquad \ldots(1)$$

where $Q = q_1 q_2 \ldots q_s$, q_i′s are prime, not necessarily distinct.
Now in the case of Legendre's symbol, we had proved that,

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

$$\Rightarrow \quad \left(\frac{-1}{q_j}\right) = (-1)^{(q_j-1)/2} \qquad 1 \le i \le s$$

Hence, (1) becomes:

$$\left(\frac{-1}{Q}\right) = \prod_{j=1}^{s}(-1)^{(q_j-1)/2} = (-1)^{\sum_{j=1}^{s}(q_j-1)/2} \qquad \ldots(2)$$

Now, if a and b are odd, then

$$\frac{ab-1}{2}-\left[\frac{a-1}{2}+\frac{b-1}{2}\right]=\frac{(a-1)(b-1)}{2}$$

Since a and b are odd, so (a−1) and (b−1) are even, hence $\frac{(a-1)(b-1)}{2}$ is a multiple of 2. This implies that

$$\frac{ab-1}{2}\equiv\left(\frac{a-1}{2}+\frac{b-1}{2}\right)\pmod 2$$

Applying this repeatedly, we obtain

$$\frac{q_1-1}{2}+\frac{q_2-1}{2}+\ldots+\frac{q_s-1}{2}\equiv\frac{q_1q_2\ldots q_s-1}{2}\pmod 2$$

$$\Rightarrow\qquad \sum_{j=1}^{s}\frac{q_j-1}{2}\equiv\frac{Q-1}{2}\pmod 2$$

$$\Rightarrow\qquad \sum_{j=1}^{s}\frac{q_i-1}{2}=\frac{Q-1}{2}+2\lambda \text{ for some integer } \lambda.$$

Putting in (2), we obtain

$$\left(\frac{-1}{Q}\right)=(-1)^{\frac{Q-1}{2}+2\lambda}=(-1)^{\frac{Q-1}{2}}$$

This proves part (1)

(2) we have

$$\left(\frac{2}{Q}\right)=\prod_{j=1}^{s}\left(\frac{2}{q_j}\right) \qquad \ldots(1)$$

But in the case of Legendre's symbol, we had proved that

$$\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}$$

$$\Rightarrow\qquad \left(\frac{2}{q_j}\right)=(-1)^{(q_j^2-1)/8} \qquad 1\le j\le s$$

so that (1) becomes :

$$\left(\frac{2}{Q}\right) = \prod_{j=1}^{s} (-1)^{(q_j^2-1)/8} = (-1)^{\sum_{i=1}^{s} (q_j^2-1)/8} \qquad \ldots(2)$$

Now, if a and b are odd, then

$$\frac{a^2b^2-1}{8} - \left[\frac{a^2-1}{8} + \frac{b^2-1}{8}\right] = \frac{(a^2-1)(b^2-1)}{8} = \frac{(a-1)(a+1)(b-1)(b+1)}{8}$$

Since a, b are odd, so a−1, a + 1, b−1, b + 1 are all even and hence $\frac{(a^2-1)(b^2-1)}{8}$ is a multiple of 2

$$\Rightarrow \qquad \frac{a^2-1}{8} + \frac{b^2-1}{8} \equiv \frac{a^2b^2-1}{8} \pmod 2$$

Applying this repeatedly, we obtain

$$\sum_{j=1}^{s} \frac{q_j^2-1}{8} \equiv \frac{q_1^2q_2^2\ldots q_s^2-1}{8} \pmod 2$$

$$\Rightarrow \qquad \sum_{j=1}^{s} \frac{q_j^2-1}{8} \equiv \frac{Q^2-1}{8} \pmod 2$$

$$\Rightarrow \qquad \sum_{j=1}^{s} \frac{q_j^2-1}{8} = \frac{Q^2-1}{8} + 2\lambda \text{ for some integer } \lambda.$$

Hence, (2) yields :

$$\left(\frac{2}{Q}\right) = (-1)^{\frac{Q^2-1}{8}+2\lambda} = (-1)^{\frac{Q^2-1}{8}} \text{ and the proof is completed.}$$

Theorem 2.18 If P and Q are odd and positive and if gcd(P, Q) = 1, then :

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$$

(This is quadratic law of reciprocity for Jacobi symbol)

Proof :- Writing $P = \prod_{i=1}^{r} p_i$ and $Q = \prod_{j=1}^{s} q_i$, we have

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s}\left(\frac{P}{q_j}\right) = \prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{p_i}{q_j}\right) \qquad \ldots(1)$$

By quadratic Law of reciprocity for Legendre Symbol we have

$$\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = (-1)^{\left(\frac{p_i-1}{2}\right)\left(\frac{q_j-1}{2}\right)}$$

$$\Rightarrow \qquad \left(\frac{p_i}{q_j}\right) = \left(\frac{q_j}{p_i}\right) = (-1)^{\left(\frac{p_i-1}{2}\right)\left(\frac{q_j-1}{2}\right)}$$

Putting this value in (1), we have :

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{q_j}{p_i}\right)(-1)^{\left(\frac{p_i-1}{2}\right)\left(\frac{q_i-1}{2}\right)}$$

$$= \left(\frac{Q}{P}\right)(-1)^{\sum_{j=1}^{s}\sum_{i=1}^{r}\left[\left(\frac{p_i-1}{2}\right)\left(\frac{q_j-1}{2}\right)\right]} \qquad \ldots(2)$$

But, we have

$$\sum_{j=1}^{s}\sum_{i=1}^{r}\left(\frac{p_i-1}{2}\right)\left(\frac{q_j-1}{2}\right) = \sum_{i=1}^{r}\frac{p_i-1}{2}\sum_{j=1}^{s}\frac{p_i-1}{2}$$

and we had earlier proved

$$\sum_{i=1}^{r}\frac{p_i-1}{2} \equiv \frac{P-1}{2} \pmod 2$$

and $$\sum_{j=1}^{s}\frac{q_j-1}{2} \equiv \frac{Q-1}{2} \pmod 2$$

which yields that $\sum_{i=1}^{r}\frac{p_i-1}{2} = \frac{P-1}{2} + 2\lambda$

and $$\sum_{j=1}^{s} \frac{q_j - 1}{2} = \frac{Q-1}{2} + 2\lambda'$$

For some integers λ and λ'

Putting these in (2), we obtain :

$$\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right)(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$$

or we can write

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$$

This completes the proof

Example :- Find the value of $\left(-\frac{42}{61}\right)$ or

Check whether -42 is a quadratic residue or quadratic no-residue mod 61.

Solution :- We have

$$\left(-\frac{42}{61}\right) = \left(\frac{-1\times 2\times 3\times 7}{61}\right) = \left(\frac{-1}{61}\right)\left(\frac{2}{61}\right)\left(\frac{3}{61}\right)\left(\frac{7}{61}\right) \quad \ldots(*)$$

Now, we have

$$\left(\frac{-1}{61}\right) = (-1)^{\frac{60}{2}} = 1$$

$$\left(\Theta\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}\right)$$

$$\left(\frac{2}{61}\right) = (-1)^{\frac{61^2-1}{8}} = -1$$

$$\left(\Theta\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}\right)$$

$$\left(\frac{3}{61}\right) = \left(\frac{61}{3}\right)(-1)^{(2/2)(60/2)}$$

$$\left(\Theta \text{ by Law of quadratic reciprocity.} \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\right)$$

$$= \left(\frac{61}{3}\right) = \left(\frac{60+1}{3}\right) = \left(\frac{1}{3}\right) = 1$$

and finally, $\left(\frac{7}{61}\right) = \left(\frac{61}{7}\right)(-1)^{\left(\frac{6}{2}\right)\cdot\left(\frac{60}{2}\right)}$

$$= \left(\frac{61}{7}\right) = \left(\frac{56+5}{7}\right) = \left(\frac{5}{7}\right)$$

$$= \left(\frac{7}{5}\right)(-1)^{\frac{4}{2}\cdot\frac{6}{2}} = \left(\frac{7}{5}\right) = \left(\frac{5+2}{5}\right)$$

$$= \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1$$

Putting all these in (∗), we have

$$\left(-\frac{42}{61}\right) = (1)\ (-1)\ (1)\ (-1) = 1$$

Hence −42 is quadratic residue mod 61.

Alternatively,

$$\left(\frac{-42}{61}\right)=\left(\frac{-61+19}{61}\right)=\left(\frac{19}{61}\right)$$

Since 19 and 61 are odd primes and 61 is of the form 4k + 1, so by quadratic Law of recipricity,

$$\left(\frac{19}{61}\right)=\left(\frac{61}{19}\right)=\left(\frac{57+4}{19}\right)=\left(\frac{4}{19}\right)$$

$$=\left(\frac{2}{19}\right)\left(\frac{2}{19}\right)=(-1)^{\frac{19^2-1}{8}}.(-1)^{\frac{19^2-1}{8}}$$

$$=1$$

Hence $\left(\frac{-42}{61}\right)=1,$ so -42 is quadratic residue mod 61.

The arithmetic in Z_p

We know that a linear congruence $ax \equiv b \bmod (n)$ has a unique solution mod (n) if gcd(a, n) = 1. Now if n is a prime p, then gcd(a, n) = gcd (a, p) is either 1 or p; in the first case, we have a unique solution mod (p), while in the second case (where $p \mid a$), either every x is a solution (when $p \mid b$) or no x is a solution (when $p \nmid b$).

One can view this elementary result as saying that if the polynomial $ax - b$ has degree d = 1 over Z_p (that is, if $a \not\equiv 0 \bmod (p)$), then it has at most one root in Z_p. Now in algebra we learn that a non-trivial polynomial of degree d, with real or complex coefficients, has at most d distinct roots in R or C; it is reasonable to ask whether this is also true for the number system Z_p, since we have just seen that it is true when d = 1. Our first main theorem, due to Lagrange, states that this is indeed the case.

Theorem 2.19 Let p be prime, and let $f(x) = a_d x^d + \ldots + a_1 x + a_0$ be a polynomial with integer coefficients, where $a_i \not\equiv 0 \bmod (p)$ for some i. Then the congruence $f(x) \equiv 0 \bmod (p)$ is satisfied by at most d congruence classes $[x] \in Z_p$.

Proof :-We use induction on d. If d = 0 then $f(x) = a_0$ with p not dividing a_0, so there are no solutions of $f(x) \equiv 0$, as required. For the inductive step, we now assume that $d \geq 1$, and that all polynomials $g(x) = b_{d-1} x^{d-1} + \ldots + b_0$ with some $b_i \not\equiv 0$ have at most $d-1$ roots $[x] \in Z_p$.

If the congruence $f(x) \equiv 0$ has no solutions, there is nothing left to prove, so suppose that [a] is a solution; thus $f(a) \equiv 0$, so p divides f(a). Now

$$f(x)-f(a) = \sum_{i=0}^{d} a_i x^i - \sum_{i=0}^{d} a_i a^i = \sum_{i=0}^{d} a_i (x^i - a^i) = \sum_{i=0}^{d} a_i (x^i - a^i) .$$

For each i = 1,…, d we can put

$$x^i - a^i = (x - a)\,(x^{i-1} + ax^{i-2} + \ldots + a^{i-2}\,x + a^{i-1}),$$

so that by taking out the common factor x−a we have

$$f(x) - f(a) = (x-a)g(x)$$

for some polynomial g(x) with integer coefficients, of degree at most d−1. Now p cannot divide all the coefficients of g(x) : if it did, then since it also divides f(a), it would have to divide all the coefficients of $f(x) = f(a) + (x-a)\,g(x)$, against our assumption. We may therefore apply the induction hypothesis to g(x), so that at most d−1 classes [x] satisfy $g(x) \equiv 0$. We now count classes [x] satisfying $f(x) \equiv 0$: if any class [x] = [b] satisfies $f(b) \equiv 0$, then p divides both f(a) and f(b), so it divides $f(b) - f(a) = (b-a)\,g(b)$; since p is prime, Lemma 2.1(b) implies that p divides b−a or g(b), so either [b] = [a] or $g(b) \equiv 0$. There are at most d−1 classes [b] satisfying $g(b) \equiv 0$, and hence at most 1 + (d−1) = d satisfying $f(b) \equiv 0$, as required.

Remarks :-

1. Note that this theorem allows the possibility that $a_d = 0$, so that f(x) has degree less than d; if so, then by deleting $a_d x^d$ we see that there are strictly fewer than d classes [x] satisfying $f(x) \equiv 0$. The same argument applies if we merely have $a_d \equiv 0 \bmod (p)$.
2. Even if $a_d \not\equiv 0$, f(x) may still have fewer than d roots in Z_p : for instance $f(x) = x^2 + 1$ has only one root in Z_2, namely the class [1], and it has no roots in Z_3.
3. The condition that $a_i \not\equiv 0$ for some i ensures that f(x) yields a non-trivial polynomial when we reduce it mod (p). If $a_i \equiv 0$ for all i then all p classes $[x] \in Z_p$ satisfy $f(x) \equiv 0$, so the result will fail if $d < p$.
4. In the theorem, it is essential to assume that the modulus is prime : for example, the polynomial $f(x) = x^2 - 1$, of degree d = 2, has four roots in Z_8, namely the classes [1], [3], [5] and [7].

A useful equivalent version of Lagrange's Theorem is the contrapositive :

Let $f(x) = a_d x^d + \ldots + a_1 x + a_0$ be a polynomial with integer coefficients, and let p be prime. If f(x) has more than d roots in Z_p, then p divides each of its coefficients a_i.

Lagrange's Theorem tells us nothing new about polynomials f(x) of degree d ≥ p : there are only p classes in Z_p, so it is trivial that at most d classes satisfy f(x) ≡ 0. The following result, useful in studying polynomials of high degree, is known as Fermat's Little Theorem though it was also known to Leibniz, and the first published proof was given by Euler.

Theorem 2.20 If p is prime and a ≢ 0 mod (p), then $a^{p-1} \equiv 1 \pmod p$.

Proof :- The integers 1, 2,…, p−1 form a complete set of non-zero residues (mod p).

If a ≢ 0 (mod p) then xa ≡ ya implies x ≡ y, so that the integers a, 2a,…, (p−1)a lie in distinct classes (mod p). None of these integers is divisible by p, so they also form a complete set of non-zero residues. It follows that a, 2a,…, (p−1)a are congruent to 1, 2,…, p−1 in some order. (For instance, if p = 5 and a = 3 then multiplying the residues 1, 2, 3, 4 by 3 we get 3, 6, 9, 12, which are respectively congruent to 3, 1, 4, 2.) The products of these two sets of integers must therefore lie in the same class, that is,

$$1 \times 2 \times \ldots \times (p-1) \equiv a \times 2a \times \ldots \times (p-1)a \pmod p,$$

or equivalently

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

Since (p−1)! is coprime to p, divide through by (p−1)! and deduce that $a^{p-1} \equiv 1 \mod (p)$.

This theorem states that all the classes in Z_p except [0] are roots of the polynomial $x^{p-1} - 1$. For a polynomial satisfied by all the classes in Z_p, we simply multiply by x, to get $x^p - x$:

Corollary :- It p is prime then $a^p \equiv a \mod(p)$ for every integer a.

Proof :- If a ≢ 0 then by above theorem $a^{p-1} \equiv 1$, so multiplying each side by a gives the result. If a ≡ 0 then $a^p \equiv 0$ also, so the result is again true.

Note :- This corollary shows that if f(x) is any polynomial of degree d ≥ p, then by repeatedly replacing any occurrence of x^p with x we can find a polynomial g(x) of degree less than p with the property that f(x) ≡ g(x) for all integers x. In other words, when considering polynomials (mod p), it is sufficient to restrict attention to those of degree d < p. Similarly, the coefficients can also be simplified by reducing them (mod p).

These two results are very useful in dealing with large powers of integers.

Example :- Let us find the least non-negative residue of $2^{68} \pmod{19}$. Since 19 is prime and 2 is not divisible by 19, we have p = 19 and a = 2, so that $2^{18} \equiv 1 \pmod{19}$. Now 68 = 18 × 3 + 14, so

$$2^{68} = (2^{18})^3 \times 2^{14} \equiv 1^3 \times 2^{14} \equiv 2^{14} \pmod{19}.$$

Since $2^4 = 16 \equiv -3 \pmod{19}$, we can write $14 = 4 \times 3 + 2$ and deduce that

$$2^{14} = (2^4)^3 \times 2^2 \equiv (-3)^3 \times 2^2 \equiv -27 \times 4 \equiv -8 \times 4 \equiv -32 \equiv 6 \text{ mod}(19),$$

so that $2^{68} \equiv 6 \pmod{19}$.

Example :- We will show that $a^{25} - a$ is divisible by 30 for every integer a. By factorising 30, we see that it is sufficient to prove that $a^{25} - a$ is divisible by each of the primes p = 2, 3 and 5. Let us deal with p = 5 first, applying abve Corollary twice, we have

$$a^{25} = (a^5)^5 \equiv a^5 \equiv a \pmod{5},$$

so 5 divides $a^{25} - a$ for all a. Similarly $a^3 \equiv a \pmod{3}$, so

$$a^{25} = (a^3)^8 \, a = a^8 \, a = a^9 = (a^3)^3 \equiv a^3 \equiv a \pmod{3},$$

as required. For p = 2 $a^2 \equiv a \pmod{2}$

$\therefore$ $$a^{25} = (a^2)^{12} \, a \equiv a^{12} \, a = (a^2)^6 \, a \equiv a^6 \, a = (a^2)^3 a$$

$$\equiv a^3 a = a^4 = (a^2)^2$$

$$\equiv a^2 \equiv a \pmod{2}.$$

Example :- Let us find all the roots of the congruence

$$f(x) = x^{17} + 6x^{14} + 2x^5 + 1 \equiv 0 \pmod{5}.$$

Here p = 5, so by replacing x^5 with x we can replace the leading term $x^{17} = (x^5)^3 \, x^2$ with $x^3 x^2 = x^5$, and hence with x. Similarly x^{14} is replaced with x^2, and x^5 with x, so giving the polynomial $x + 6x^2 + 2x + 1$. Reducing the coefficients (mod 5) gives $x^2 + 3x + 1$. Thus $f(x) \equiv 0$ is equivalent to the much simpler congruence

$$g(x) = x^2 + 3x + 1 \equiv 0 \pmod{5}.$$

Here we can simply try all five classes $[x] \in Z_5$, or else note that $g(x) \equiv (x-1)^2$; either way, we find that [x] = [1] is the only root of $g(x) \equiv 0$, so this class is the only root of $f(x) \equiv 0$.

As another application of Fermat's Little Theorem, we prove a result known as Wilson's Theorem, though it was first proved by Lagrange in 1770 :

Corollary :- An integer n is prime if and only if $(n-1)! \equiv -1 \pmod{n}$

Proof :- Suppose that n is a prime p. If p = 2 then $(p-1)! = 1 \equiv -1 \pmod{p}$, as required, so we may assume that p is odd. Define

$$f(x) = (1-x)\,(2-x)\ldots(p-1-x) + 1 - x^{p-1},$$

a polynomial with integer coefficients. This has degree $d < p-1$, since when the product is expanded, the two terms in f(x) involving x^{p-1} cancel. If a = 1, 2, …, p−1 then $f(a) \equiv 0 \pmod{p}$: the product (1−a) (2−a)…(p−1−a) vanishes since it has a factor equal to 0, and $1-a^{p-1} \equiv 0$ by Fermat's Little Theorem. Thus f(x) has more than d roots (mod p), so its coefficients are all divisible by p. In particular, p divides the constant term (p−1)! + 1, so $(p-1)! \equiv -1$.

For the converse, suppose that $(n-1)! \equiv -1 \pmod{n}$. We then have $(n-1)! \equiv -1 \pmod{m}$ for any factor m of n. If m < n then m appears as a factor of (n−1)!, so $(n-1)! \equiv 0 \pmod{m}$ and hence $-1 \equiv 0 \pmod{m}$. This implies that m = 1, so we conclude that n has no proper factors and is therefore prime.

Theorem 2.21 Let p be an odd prime. Then the quadratic congruence $x^2 + 1 \equiv 0 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.

Proof :- Suppose that p is an odd prime, and let k = (p−1)/2. In the product

$$(p-1)! = 1 \times 2 \times \ldots \times k \times (k+1) \times \ldots \times (p-2) \times (p-1),$$

we have $p-1 \equiv -1$, $p-2 \equiv -2$,…, $k+1 = p-k \equiv -k \pmod{p}$, so by replacing each of the k factors p − i with −i for i = 1, …, k we see that

$$(p-1)! \equiv (-1)^k.(k!)^2 \pmod{p}.$$

Now Wilson's Theorem gives $(p-1)! \equiv -1$, so $(-1)^k (k!)^2 \equiv -1$ and hence $(k!)^2 \equiv (-1)^{k+1}$. If $p \equiv 1 \pmod{4}$ then k is even, so $(k!)^2 \equiv -1$ and hence x = k! is a solution of $x^2 + 1 \equiv 0 \pmod{p}$.

On the other hand, suppose that $p \equiv 3 \pmod{p}$, so that k = (p−1)/2 is odd. If x is any solution of $x^2 + 1 \equiv 0 \pmod{p}$, then x is coprime to p, so Fermat's Little Theorem gives $x^{p-1} \equiv 1 \pmod{p}$. Thus $1 \equiv (x^2)^k \equiv (-1)^k \equiv -1 \pmod{p}$, which is impossible since p is odd, so there can be no solution.

Units in Z_n

Definition :- A multiplicative inverse for a class $[a] \in Z_n$ is a class $[b] \in Z_n$ such that [a] [b] = [1]. A class $[a] \in Z_n$ is a unit if it has a multiplicative inverse in Z_n. (In this case, we sometimes say that the integer a is a unit (mod n), meaning that $ab \equiv 1 \pmod{n}$ for some integer b.)

Lemma :-[a] is a unit in Z_n if and only if gcd(a, n) = 1.

Proof :- If [a] is a unit then ab = 1 + qn for some integers b and q; any common factor of a and n would therefore divide 1, so gcd(a, n) = 1. Conversely, if gcd(a, n) = 1 then 1 = au + nv for some u and v, so [u] is a multiplicative inverse of [a].

Example :- The units in Z_8 are [1], [3], [5] and [7] : in fact [1] [1] = [3] [3] = [5] [5] = [7] [7] = [1], so each of these units is its own multiplicative inverse.

In Z_9, the units are [1], [2], [4], [5], [7] and [8]: for instance [2] [5] = [1], so [2] and [5] are inverses of each other.

The group of units of U_n

Theorem 2.22 For each integer $n \geq 1$, the set U_n forms a group under multiplication mod (n), with identity element [1].

Proof :- We have to show that U_n satisfies the group axioms, namely closure, associativity, existence of an identity and of inverses. To prove closure, we have to show that the product [a] [b] = [ab] of two units [a] and [b] is also a unit. If [a] and [b] are units, they have inverses [u] and [v] such that [a] [u] = [au] = [1] and [b] [v] = [bv] = [1]; then [ab] [uv] = [aubv] = [au] [bv] = $[1]^2$ = [1], so [ab] has inverse [uv], and is therefor a unit. This proves closure. Associativity asserts that [a] ([b][c]) = ([a] [b]) [c] for all units [a], [b] and [c]; the left-and right-hand sides are the classes [a(bc)] and [(ab)c], so this follows from the associativity property a(bc) = (ab)c in Z. The identity element of U_n is [1], since [a][1] = [a] = [1][a] for all [a] $\in U_n$. Finally, if [a] $\in U_n$ then by definition there exists [u] $\in Z_n$ such that [a] [u] = [1]; now [u] $\in U_n$ (because the class [a] satisfies [u][a] = [1]), so [u] is the inverse of [a] in U_n.

Definition :- We say that a group G is abelian if its elements commute, that is, gh = hg for all g, h $\in$ G.

Lemma :- U_n is an abelian group under multiplication mod (n).

Proof of Lemma :-Let [a], [b] $\in Z_n$, then we have to prove that [a] [b] = [b] [a]

Now [a] [b] = [a b] = [b a] (by commutativity in Z)

= [b] [a]

Definition :- If G is a finite group with an identity element e, the order of an element g$\in$G is the least integer k > 0 such that g^k = e; then the integers *l* such that g^l = e are the multiples of k.

Example :- In U_5 the element 2 has order 4: its powers are $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 3$ and $2^4 \equiv 1$ (mod 5), so k = 4 is the least positive exponent such that 2^k = 1(the identity element) in U_5. Similarly, the element 1 has order 1, while the elements 3 and 4 have orders 4 and 2 respectively.

Example :- In U_8, the elements, 1, 3, 5, 7 have orders 1, 2, 2, 2 respectively.

Lemma :- If *l* and m are coprime positive integers, then $2^l - 1$ and $2^m - 1$ are coprime.

Proof :- Let n be the highest common factor of $2^l - 1$ and $2^m - 1$. Clearly n is odd, so 2 is a unit (mod n). Let k be the order of the element 2 in the group U_n. Since n divides $2^l - 1$ we have $2^l = 1$ in U_n, so k divides *l*. Similarly k divides m, so k divides gcd(*l*, m) = 1. Thus k = 1, so the element 2 has order 1 in U_n. This means that $2^1 \equiv 1$ mod(n), so n = 1, as required.

Corollary :- Distinct Mersenne numbers are coprime.

Proof :- In above lemma if we take l and m to be distinct primes we see that $M_l = 2^l - 1$ and $M_m = 2^m - 1$ are coprime.

Primitive roots

Definition :- If U_n is cyclic then any generator g for U_n is called a primitive root (mod n). This means that g has order equal to the order $\phi(n)$ of U_n, so that the powers of g yield all the elements of U_n. For instance, 2 and 3 are primitive roots (mod 5), but there are no primitive roots (mod 8) since U_8 is not cyclic.

Finding primitive roots in U_n (if they exist) is a non-trivial problem, and there is no simple solution. One obvious but tedious method is to try each of then $\phi(n)$ units $a \in U_n$ in turn, each time computing powers a^i (mod n) to find the order of a in U_n; if we find an element a of order $\phi(n)$ then we know that this must be a primitive root. The following result is a rather more efficient test for primitive roots :

Theorem 2.23 An element $a \in U_n$ is a primitive root if and only if $a^{\phi(n)/q} \neq 1$ in U_n for each prime q dividing $\phi(n)$.

Proof :- If a is a primitive root, then it has order $|U_n| = \phi(n)$, so $a^i \neq 1$ for all i such that $1 \leq i < \phi(n)$; in particular, this applies to $i = \phi(n)/q$ for each prime q dividing n.

Conversly, if a is not a primitive root, then its order k must be a proper factor of $\phi(n)$, so $\phi(n)/k > 1$. If q is any prime factor of $\phi(n)/k$, then k divides $\phi(n)/q$, so that $a^{\phi(n)/q} = 1$ in U_n, against our hypothesis. Thus a must be a primitive root.

Example :- Let n = 11, and let us see whether a = 2 is a primitive root (mod 11). Now $\phi(11) = 11-1 = 10$, which is divisible by the primes q = 2 and q = 5, so we take $\phi(n)/q$ to be 5 and 2 respectively. Now 2^5, $2^2 \not\equiv 1$ (mod 11), so above theorem implies that 2 is a primitive root (mod 11). To verify this, note that in U_{11} we have

$$2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 5,\ 2^5 = 10,$$

$$2^6 = 9,\ 2^7 = 7,\ 2^8 = 3,\ 2^9 = 6,\ 2^{10} = 1;$$

thus 2 has order 10, and its powers give all the elements of U_{11}. If we apply above theorem with a = 3, however, we find that $3^5 = 243 \equiv 1$ (mod 11), so 3 is not a primitive root (mod 11): its powers are 3, 9, 5, 4 and 1.

Example :- Let us find a primitive root (mod 17). We have $\phi(17) = 16$, which has only q = 2 as a prime factor. Above theorem therefore implies that an element $a \in U_{17}$ is a primitive root if and only if $a^8 \neq 1$ in U_{17}. Trying a = 2

first, we have $2^8 = 256 \equiv 1 \pmod{17}$, so 2 is not a primitive root. However, $3^8 = (3^4)^2 \equiv (-4)^2 = 16 \not\equiv 1 \pmod{17}$, so 3 is a primitive root.

Example :- To demonstrate the above theorem also applies when n is composite, let us take n = 9. We have $\phi(9) = 6$, which is divisible by the primes q = 2 and q = 3, so that $\phi(n)/q$ is 3 and 2 respectively. Thus an element $a \in U_9$ is a primitive root if and only if a^2, $a^3 \neq 1$ in U_9. Since 2^2, $2^3 \not\equiv 1 \pmod{9}$, we see that 2 is a primitive root.

Theorem 2.24 If p is prime, then the group U_p has $\phi(d)$ elements of order d for each d dividing p−1. Before proving this, we deduce.

Proof of the Theorem :- For each d dividing p−1 let us define

$$\Omega_d = \{a \in U_p | \text{ a has order d}\} \text{ and } \omega(d) = |\Omega_d|,$$

the number of elements of order d in U_p. Our aim is to prove that $\omega(d) = \phi(d)$ for all such d. The order of each element of U_p divides p−1, so the sets Ω_d form a partition of U_p and hence

$$\omega(d) = p-1.$$

99

Also $$\sum_{d \mid p-1} \phi(d) = p-1,$$

so $$\sum_{d \mid p-1} (\phi(d) - \omega(d)) = 0.$$

If we can show that $\omega(d) \leq \phi(d)$ for all d dividing p−1, then each summand in this expression is non-negative; since their sum is 0, the summands must all be 0, so $\omega(d) = \phi(d)$, as required.

The inequality $\omega(d) \leq \phi(d)$ is obvious if Ω_d is empty, so assume that Ω_d contains an element a. By the definition of Ω_d, the powers $a^i = a, a^2, \ldots, a^d$ (= 1) are all distinct, and they satisfy $(a^i)^d = 1$, so they are d distinct roots of the polynomial $f(x) = x^d - 1$ in Z_p; But f(x) has at most deg(f) = d roots in Z_p, so these are a complete set of roots of f(x). We shall show that Ω_d consists of those roots a^i with gcd(i, d) = 1. If $b \in \Omega_d$ then b is a root of f(x). so $b = a^i$ for some i = 1, 2,…, d. If we let j denote gcd(i, d), then

$$b^{d/j} = a^{id/j} = (a^d)^{i/j} = 1^{i/j} = 1$$

in U_p; but d is the order of b, so no lower positive power of b than b^d can be equal to 1, and hence j = 1. Thus every element b of order d has the form a^i

where $1 \le i \le d$ and i is coprime to d. The number of such integers i is $\phi(d)$, so the number $\omega(d)$ of such elements b is at most $\phi(d)$, and the proof is complete.

Corollary :- If p is prime then the group U_p is cyclic.

Proof :- Putting $d = p - 1$ in above therorem we see that there are $\phi(p-1)$ elements of order $p-1$ in U_p. Since $\phi(p-1) \ge 1$, the group contains at least one element of this order. Now U_p has order $\phi(p) = p-1$, so such an element is a generator for U_p, and hence this group is cyclic.

Example :- Let $p = 7$, so $U_p = U_7 = \{1, 2\ 3, 4, 5, 6\}$. The divisors of $p-1 = 6$ are $d = 1, 2, 3$ and 6, and the sets of elements of order d in U_7 are respectively $\{1\}, \{6\}, \{2, 4\}$ and $\{3, 5\}$; thus the numbers of elements of order d are 1, 1, 2 and 2 respectively, agreeing with the values of $\phi(d)$. To verify that 3 is a generator, note that

$$3^1 = 3,\ 3^2 = 2,\ 3^3 = 6,\ 3^4 = 4,\ 3^5 = 5,\ 3^6 = 1$$

in U_7, so every element of U_7 is a power of 3.

The group U_{p^e}, where p is an odd prime

Theorem 2.25 If p is an odd prime, then U_{p^e} is cyclic for all $e \ge 1$.

Proof :- We have already proved the case $e = 1$, so we may assume that $e \ge 2$. We use the following strategy to find a primitive root mod p^e:

(a) first we pick a primitive root g (mod p)

(b) next we show that either g or g + p is a primitive root mod (p^2);

(c) finally we show that if h is any primitive root mod p^2, then h is a primitive root mod p^e for all $e \ge 2$.

Since p is prime, so we have a primitive root g (mod p). Thus $g^{p-1} \equiv 1 \pmod p$, but $g^i \not\equiv 1 \pmod p$ for $1 \le i < p - 1$. We now proceed to step (b).

Since gcd(g, p) = 1 we have gcd $(g, p^2) = 1$, so we can consider g as an element of U_{p^2}. If d denotes the order of g (mod p^2), then Euler's theorem implies that d divides $\phi(p^2) = p(p-1)$. By definition of d, we have $g^d \equiv 1 \pmod{p^2}$, so $g^d \equiv 1 \pmod p$; but g has order $p-1 \pmod p$, so $p-1$ divides d. Since p is prime, these two facts imply that either $d = p(p-1)$ or $d = p - 1$. If $d = p(p-1)$ then g is a primitive root (mod p^2), as required, so assume that $d = p - 1$. Let $h = g + q$. Since $h \equiv g \pmod p$, h is a primitive root (mod p), so arguing as before we see that h has order $p(p-1)$ or $p-1$ in U_{p^2}. Since $g^{p-1} \equiv 1 \pmod{p^2}$, the Binomial Theorem gives

$$h^{p-1} = (g + p)^{p-1} = g^{p-1} + (p-1)\, g^{p-2}p + \ldots \equiv 1 - pg^{p-2} \pmod{p^2},$$

where the dots represent terms divisible by p^2. Since g is coprime to p, we have $pg^{p-2} \not\equiv 0 \pmod{p^2}$ and hence $h^{p-1} \not\equiv 1 \pmod{p^2}$. Thus h does not have ord a p − 1 in U_{p^2} so it must have order p(p−1) and is therefore a primitive root. This completes step (b).

Now we consider step (c). Let h be any primitive root (mod p^2). We will show, by induction on e, that h is a primitive root mod (p^e) for all e ≥ 2. Suppose, then, that h is a primitive root mod (p^e) for some e ≥ 2, and let d be the order of h (mod p^{e+1}). An argument similar to that at the beginning of step (b) shows that d divides $\phi(p^{e+1}) = p^e$ ((p−1) and is divisible by $\phi(p^e) = p^{e-1}$ (p−1), so $d = p^e$ (p−1) or $d = p^{e-1}$ (p−1). In the first case, h is a primitive root (mod p^{e+1}), as required, so it is sufficient to eliminate the second case by showing that $h^{p^{e-1}(p-1)} \not\equiv 1 \pmod{p^{e+1}}$.

Since h is a primitive root mod (p^e), it has order $\phi(p^e) = p^{e-1}$ (p−1) in U_{p^e}, so $h^{p^{e-2}(p-1)} \not\equiv 1 \pmod{p^e}$. However p^{e-2} (p−1) = $\phi(p^{e-1})$, so $h^{p^{e-2}(p-1)} \equiv 1 \pmod{p^{e-1}}$ by Euler's Theorem. Combining these two results, we see that $h^{p^{e-2}(p-1)} = 1 + kp^{e-1}$ where k is coprime to p, so the Binomial Theorem gives

$$h^{p^{e-1}(p-1)} = (1 + kp^{e-1})^p$$

$$= 1 + \binom{p}{1} kp^{e-1} + \binom{p}{2}(kp^{e-1})^2 + \ldots$$

$$= 1 + kp^e + \frac{1}{2} k^2 p^{2e-1} (p-1) + \ldots$$

The dots here represent terms divisible by $(p^{e-1})^3$ and hence by p^{e+1}, since 3(e −1) ≥ e + 1 for e ≥ 2, so

$$h^{p^{e-1}(p-1)} \equiv 1 + kp^3 + \frac{1}{2} k^2 p^{2e-1} (p-1) \pmod{p^{e+1}}.$$

Now p is odd, so the third term $k^2 p^{2e-1}(p-1)/2$ is also divisible by p^{e+1}, since 2e − 1 ≥ e + 1 for e ≥ 2. Thus

$$h^{p^{e-1}(p-1)} \equiv 1 + kp^e \bmod (p^{e+1}).$$

Since p does not divide k, we therefore have $h^{p^{e-1}(p-1)} \not\equiv 1 \bmod (p^{e+1})$, so step (c) is complete. (Notice where we need p to be od: if p = 2 then the third term $k^2 p^{2e-1}(p-1)/2 = k^2 2^{2e-2}$ is not divisible by 2^{e+1} when e = 2, so the first step of the induction argument fails.)

Example :- Let p = 5. We have seen that g = 2 is a primitive root (mod 5), since it has order $\phi(5) = 4$ as an element of U_5. If we regard g = 2 as an

element of $U_{p^2} = U_{25}$, then by the above argument its order d in U_{25} must be either $p(p-1) = 20$ or $p-1 = 4$. Now $2^4 = 16 \not\equiv 1 \pmod{25}$, so $d \neq 4$ and hence $d = 20$. Thus $g = 2$ is a primitive root (mod 25). (One can check this directly by computing the powers $2, 2^2, \ldots, 2^{20} \pmod{25}$, using $2^{10} = 1024 \equiv -1 \pmod{25}$ to simplify the calculations.) Suppose instead that we had chosen $g = 7$; this is also a primitive root (mod 5), since $7 \equiv 2 \pmod{5}$, but it is not a primitive root (mod 25): we have $7^2 = 49 \equiv -1 \pmod{25}$, so $7^4 \equiv 1$ and hence 7 has order 4 in U_{25}. Step (b) guarantees that in this case, $g + p = 12$ must be a primitive root.

The group U_{2^e}

Theorem 2.26 The group U_{2^e} is cyclic if and only if $e = 1$ or $e = 2$.

Proof :- The groups $U_2 = \{1\}$ and $U_4 = \{1, 3\}$ are cyclic, generated by 1 and by 3, so it is sufficient to show that U_{2^e} has no elements of order $\phi(2^e) = 2^{e-1}$ by showing that

$$a^{2^{e-2}} \equiv 1 \pmod{2^e} \quad \ldots(1)$$

for all odd a. We prove this by induction on e. For the lowest value $e = 3$, by (1) we have that $a^2 \equiv 1 \pmod 8$ for all odd a, and this is true since if $a = 2b + 1$ then $a^2 = 4b(b+1) + 1 \equiv 1 \pmod 8$. If we assume (1) for some exponent $e \geq 3$, then for each odd a we have

$$a^{2^{e-2}} = 1 + 2^e k$$

for some integer k. Squaring, we get

$$a^{2^{(e+1)-2}} = (1 + 2^e k)^2 = 1 + 2^{e+1} k + 2^{2e} k^2 = 1 + 2^{e+1}(k + 2^{e-1} k^2)$$

$$\equiv 1 \pmod{2^{e+1}},$$

which is the required form of (1) for exponent $e + 1$. Thus (1) is true for all integers $e \geq 3$, and the proof is complete.

Lemma :- $2^{n+2} \mid (5^{2^n} - 1)$ for all $n \geq 0$.

Proof :- We use induction on n. The result is trivial for $n = 0$. Suppose it is true for some $n \geq 0$. Now

$$5^{2^{n+1}} - 1 = (5^{2^n})^2 - 1 = (5^{2^n} - 1)(5^{2^n} + 1),$$

with $2^{n+2} \mid (5^{2^n} - 1)$ by the induction hypothesis, and with $2 \mid (5^{2^n} + 1)$ since $5^{2^n} \equiv 1 \pmod 4$. Combining the powers of 2 we get $2^{n+3} \mid (5^{2^{n+1}} - 1)$ as required.

Theorem 2.27 If $e \geq 3$ then $U_{2^e} = \{ \mu\ 5^i \mid 0 \leq i < 2^{e-2} \}$.

Proof :- Let m be the order of the element 5 in U_{2^e}. By Euler's Theorem, m divides $\phi(2^e) = 2^{e-1}$, so $m = 2^k$ for some $k \leq e-1$. Above theorem implies that U_{2^e} has no elements of order 2^{e-1} so $k \leq n-2$. Putting $n = e-3$ in the above theorem we see that $2^{e-1} \mid (5^{2^{e-3}} - 1)$, so $5^{2^{e-3}} \not\equiv 1 \pmod{2^e}$ and hence $k > e - 3$. Thus $k = e-2$, so $m = 2^{e-2}$. This means that 5 has 2^{e-2} distinct powers 5^i ($0 \leq i < 2^{e-2}$) in U_{2^e}. Since $5 \equiv 1 \pmod 4$, these are all represented by integers congruent to 1 mod (4). This accounts for exactly half of the 2^{e-1} elements 1, 3, 5,…, $2^e - 1$ of U_{2^e}, and the other half, represented by integers congruent to $-1 \pmod 4$, must be the elements of the form -5^i. This shows that every element has the form $\pm 5^i$ for some $i = 0, 1, \ldots, 2^{e-2}-1$, as required.

The existence of primitive roots

Lemma :- If $n = rs$ where r and s are coprime and are both greater than 2, then U_n is not cyclic.

Proof of Lemma :- Since $\gcd(r, s) = 1$ we have $\phi(n) = \phi(r)\,\phi(s)$. Since $r, s > 2$, both $\phi(r)$ and $\phi(s)$ are even. So $\phi(n)$ is divisible by 4. It follows that the integer $e = \phi(n)/2$ is divisible by both $\phi(r)$ and $\phi(s)$. If a is a unit (mod n), then a is a unit (mod r) and also a unit (mod s), so $a^{\phi(r)} \equiv 1 \pmod r$ and $a^{\phi(s)} \equiv 1 \pmod s$ by Euler's Theorem. Since $\phi(r)$ and $\phi(s)$ divide e, we therefore have $a^e \equiv 1 \pmod r$, that is $a^e \equiv 1 \pmod s$. Since r and s are coprime, this implies that $a^e \equiv 1 \pmod{rs}$, that is $a^e \equiv 1 \pmod n$. Thus every element of U_n has order dividing e, and since $e < \phi(n)$, this means that there is no primitive root (mod n).

Theorem 2.28 The group U_n is cyclic if and only if

$$n = 1, 2, 4, p^e \text{ or } 2p^e,$$

where p is an odd prime.

Proof :- The cases n = 1, 2 and 4 are trivial, and we have dealt with the odd prime-powers, so we may assume that $n = 2p^e$ where p is an odd prime. Now $\phi(n) = \phi(2)\,\phi(p^e) = \phi(p^e)$. Therefore there is a primitive root g (mod p^e). Then $g + p^e$ is also a primitive root (mod p^e), and one of g and $g + p^e$ is odd, so there is an odd primitive root h (mod p^e). We will show that h is a primitive root (mod $2p^e$). By its construction, h is coprime to both 2 and p^e, so h is a unit (mod $2p^e$). If $h^i \equiv 1 \pmod{2p^e}$, then certainly $h^i \equiv 1 \pmod{p^e}$; since h is a primitive root (mod p^e), this implies that $\phi(p^e)$ divides i. Since $\phi(p^e) = \phi(2p^e)$,

this shows that $\phi(2p^e)$ divides i, so h has order $\phi(2p^e)$ in U_{2p^e} and is therefore a primitive root.

Conversely, if $n \neq 1, 2, 4, p^e$ or $2p^e$, then either

(a) $n = 2^e$ where $e \geq 3$, or

(b) $n = 2^e p^f$ where $e \geq 2$, $f \geq 1$ and p is an odd prime, or

(c) n is divisible by at least two odd primes.

We have already proved that in case (a), U_n is not cyclic.

In case (b), in the above lemma, we can take $r = 2^e$ and $s = p^f$, while in case (c) we can take $r = p^e \mid n$ for some odd prime p dividing n, and $s = n/r$. In either case, $n = rs$ where r and s are coprime and greater than 2, so above lemma shows that U_n is not cyclic.

Example :- We know that $g = 2$ is a primitive root (mod 5^e) for all $e \geq 1$. Now g is even, so $h = 2 + 5^e$ is an odd primitive root (mod 5^e). Using the above theorem we see that h is also a primitive root (mod 2.5^e). For instance, 7 is a primitive root (mod 10), and 27 is a primitive root (mod 50).

The group of quadratic residues

Definition :- An element $a \in U_n$ is a quadratic residue (mod n) if $a = s^2$ for some $s \in U_n$; the set of such quadratic residues is denoted by Q_n. For small n one can determine Q_n simply by squaring all the elements $s \in U_n$.

Example 7.1 $Q_7 = \{1, 2, 4\} \subset U_7$, while $Q_8 = \{1\} \subset U_8$.

Theorem 2.29 Let $n = n_1 \ldots n_k$ where the integers n_i are mutually coprime, and let f(x) be a polynomaial with integer coefficients. Supose that for each $i = 1,\ldots, k$ there are N_i congruence classes $x \in Z_n$, such $f(x) \equiv 0 \pmod{n_i}$. Then there are $N = N_1 \ldots N_k$ classes $x \in Z_n$ such that $f(x) \equiv 0 \pmod{n}$.

Proof :- Since the moduli n_i are mutually coprime, we have $f(x) \equiv 0 \pmod{n}$ if and only if $f(x) \equiv 0 \pmod{n_i}$ for all i. Thus each class of solutions $x \in Z_n$ of $f(x) \equiv 0 \pmod{n}$ determines a class of solutions $x = x_i \in Z_{n_i}$ of $f(x_i) \equiv 0 \pmod{n_i}$ for each i. Conversely, if for each i we have a cass of solutions $x_i \in Z_{n_i}$ of $f(x_i) \equiv 0 \pmod{n_i}$, then by the Chinese Remainder Theorem there is a unique class $x \in Z_n$ satisfying $x = x_i \pmod{n_i}$ for all i, and this class satisfies $f(x) \equiv 0 \pmod{n}$. Thus there is a one-to-one correspondence between classes $x \in Z_n$ satisfying $f(x) \equiv 0 \pmod{n}$, and k-tuples of classes $x_i \in Z_{n_i}$ satisfying $f(x_i) \equiv 0 \pmod{n_i}$ for all i. For each i there are N_i choices for the class $x_i \in Z_{n_i}$, so there are $N_1 \ldots N_k$ such k-tuples and hence this is the number of classes $x \in Z_n$ satisfying $f(x) \equiv 0 \pmod{n}$.

Example :- Putting $f(x) = x^2 - 1$, let us find the number N of classes $x \in Z_n$ satisfying $x^2 \equiv 1 \pmod{n}$. We first count solutions of $x^2 \equiv 1 \pmod{p^e}$, where p

is prime. If p is odd, then there are just two classes of solutions: clearly the classes $x \equiv \pm 1$ both satisfy $x^2 \equiv 1$, and conversely if $x^2 \equiv 1$ then p^e divides $x^2 - 1 = (x-1)(x+1)$ and hence (since $p > 2$) it divides $x-1$ or $x+1$, giving $x \equiv \pm 1$. If $p^e = 2$ or 4 then there are easily seen to be one or two classes of solutions, but if $p^e = 2^e \geq 8$ then a similar argument shows that there are four, given by $x \equiv \pm 1$ and $x \equiv 2^{e-1} \pm 1$; for any solution x, one of the factors $x \pm 1$ must be congruent to 2 (mod 4), so the other factor must be divisible by 2^{e-1}. Now in general let n have prime-power factorization $n_1 \ldots n_k$, where $n_i = p_i^{e_i}$ and each $e_i \geq 1$. We have just seen that for each odd p_i there are $N_i = 2$ classes in Z_{n_i} of solutions of $x^2 \equiv 1 \pmod{n_i}$ whereas if $p_i = 2$ we may have $N_i = 1$, 2, or 4, depending on e_i. By above theorem there are $N = N_1 \ldots N_k$ classes in Z_n of solutions of $x^2 \equiv 1 \pmod{n}$, found by solving the simultaneous congruences $x^2 \equiv 1 \pmod{n_i}$. Substiutiting the values we have obtained for N_i, we therefore have

$$N = \begin{cases} 2^{k+1} & \text{if } n \equiv 0 \bmod (8), \\ 2^{k-1} & \text{if } n \equiv 2 \bmod (4) \\ 2^k & \text{otherwise.} \end{cases}$$

where k is the number of distinct primes dividing n. For instance, if $n = 60 = 2^2.3.5$ then $k = 3$ and there are $2^k = 8$ classes of solutions, namely $x \equiv \pm 1, \pm 11, \pm 19, \pm 29 \pmod{60}$.

Theorem 2.30 Let k denote the number of distinct primes dividing n. If $a \in Q_n$, then the number N of elements $t \in U_n$ such that $t^2 = a$ is given by

$$N = \begin{cases} 2^{k+1} & \text{if } n \equiv 0 \bmod (8), \\ 2^{k-1} & \text{if } n \equiv 2 \bmod (4) \\ 2^k & \text{otherwise.} \end{cases}$$

Proof :- If $a \in Q_n$ then $s^2 = a$ for some $s \in U_n$. Any element $t \in U_n$ has the form $t = sx$ for some unique $x \in U_n$, and we have $t^2 = a$ if and only if $x^2 = 1$ in U_n. Thus N is the number of solutions of $x^2 = 1$ in U_n, the above example gives the required formula for N.

Theorem 2.31 Q_n is a subgroup of U_n.

Proof :- We need to show that Q_n contains the identity element of U_n, and is closed under taking products and inverses. Firstly, $1 \in Q_n$ since $1 = 1^2$ with $1 \in U_n$. If $a, b \in Q_n$ then $a = s^2$ and $b = t^2$ for some $s, t \in U_n$, so $ab = (st)^2$ with $st \in U_n$, giving $ab \in Q_n$. Finally, if $a \in Q_n$ then $a = s^2$ for some $s \in U_n$; since a and s are units (mod n) they have inverses a^{-1} and s^{-1} in U_n, and $a^{-1} = (s^{-1})^2$so that $a^{-1} \in Q_n$.

Theorem 2.32 Let $n > 2$, and suppose that there is a primitive root g (mod n); then Q_n is a cyclic group of order $\phi(n)/2$, generated by g^2, consisting of the even powers of g.

Proof :- Since $n > 2$, $\phi(n)$ is even. The elements $a \in U_n$ are the powers g^i for $i = 1,\ldots, \phi(n)$, with $g^{\phi(n)} = 1$. If i is even, then $a = g^i = (g^{i/2})^2 \in Q_n$. Conversely, if $a \in Q_n$ then $a = (g^j)^2$ for some j, so $i \equiv 2j \pmod{\phi(n)}$ for some j; since $\phi(n)$ is even, this implies that i is even. Thus Q_n consists of the even powers of g, so it is the cyclic group of order $\phi(n)/2$ generated by g^2.

Quadratic residues for prime-power moduli

Theorem 2.33 Let p be an odd prime, let $e \geq 1$, and let $a \in Z$. Then $a \in Q_{p^e}$ if and only if $a \in Q_p$.

Proof :- We know that there is a primitive root g (mod p^e), so with $n = p^e$ we see that Q_{p^e} consists of the even powers of g. Now g, regarded as an element of U_p, is also a primitive root (mod p), and with $n = p$ we know that Q_p also consists of the even powers of g. Thus $a \in Q_{p^e}$ if and only if $a \in Q_{p^e}$. This completes the proof.

Note :- For odd primes p, we can find square roots in U_{p^e} for $e \geq 2$ by applying the iterative method to the polynomial $f(x) = x^2 - a$: we use a square root of a mod (p^i) to find the square roots mod (p^{i+1}). Suppose that $a \in Q_p$, and r is a square root of a mod (p^i) for some $i \geq 1$; thus $r^2 \equiv a \pmod{p^i}$, say $r^2 = a + p^i q$. If we put $s = r + p^i k$, where k is as yet unknown, then $s^2 = r^2 + 2rp^i k + p^{2i}k^2 \equiv a + (q + 2rk)\, p^i \pmod{p^{i+1}}$, since $2i \geq i + 1$. Now gcd (2r, p) = 1, so we can choose k to satisfy the linear congruence $q + 2rk \equiv 0 \pmod p$, giving $s^2 \equiv a \pmod{p^{i+1}}$ as required. An element $a \in Q_{p^{i+1}}$ has just two square roots in $U_{p^{i+1}}$ for odd p, so these must be $\pm$s. It follows that if we have a square root for a in U_p, then we can iterate this process to find its square roots in U_{p^e} for all e.

Example :- Let us take $a = 6$ and $p^e = 5^2$. In U_5 we have $a = 1 = 1^2$, so we can take r = 1 as a square root (mod 5). Then $r^2 = 1 = 6 + 5.(-1)$, so $q = -1$ and we need to solve the linear congruence $-1 + 2k \equiv 0 \pmod 5$. This has solution $k \equiv 3 \pmod 5$, so we take $s = r + p^i k = 1 + 5.3 = 16$, and the square roots of 6 in Z_{5^2} are given by ± 16, or equivalently $\pm 9 \pmod{5^2}$. If we want the square roots of 6 in Z_{5^3} we repeat the process: we can take r = 9 as a square root (mod 5^2), with $r^2 = 81 = 6 + 5^2.3$, so q = 3; solving $3 + 18k \equiv 0 \pmod 5$ we have $k \equiv -1$, so $s = 9 + 5^2.(-1) = -16$, giving square roots $\pm 16 \pmod{5^3}$.

Theorem 2.34 Let a be an odd integer. Then

(a) $a \in Q_2$;

(b) $a \in Q_4$ if and only if $a \equiv 1 \pmod 4$;

(c) if $e \geq 3$, then $a \in Q_{2^e}$ if and only if $a \equiv 1 \pmod 8$.

Proof :- Parts (a) and (b) are obvious: squaring the elements of $U_2 = \{1\} \subset Z_2$ and of $U_4 = \{1, 3\} \subset Z_4$, we see that $Q_2 = \{1\}$ and $Q_4 = \{1\}$. For part (c) we use the theorem which states that the elements of U_{2^e} all have the form $\pm 5^i$ for some i; squaring, we see that the quadratic residues are the even powers of 5. Since $5^2 \equiv 1 \pmod 8$, these are all represented by integers $a \equiv 1 \pmod 8$. Now both the even powers of 5 and the elements $a \equiv 1 \pmod 8$ account for exactly one quarter of the classes in Q_{2^e}; since the first set is contained in the second, these two sets are equal.

Example :- $Q_8 = \{1\}$, $Q_{16} = \{1, 9\}$, $Q_{32} = \{1, 9, 17, 25\}$, and so on.

Note :- One can find square roots in Q_{2^e} by adapting the iterative algorithm given earlier for odd prime-powers. Suppose that $a \in Q_{2^i}$ for some $i \geq 3$, say $r^2 = a + 2^i q$. If we put $s = r + 2^{i-1}k$, then $s^2 = r^2 + 2^i rk + 2^{2(i-1)}k^2 \equiv a + (q + rk)\, 2^i \pmod{2^{i+1}}$, since $2(i-1) \geq i + 1$. Now r is odd, so we can choose k = 0 or 1 to make $q + rk$ even, giving $s^2 \equiv a \pmod{2^{i+1}}$. Thus s is a square root of a in $U_{2^{i+1}}$. There are four square roots of a in $U_{2^{i+1}}$, and these have the form $t = sx$, where $x = \pm 1$ or $2^i \pm 1$ is a square root of 1. Since $a \equiv 1 \pmod 8$, we can start with a square root r = 1 for a in U_{2^3}, and then by iterating this process we can find the square roots of a in U_{2^e} for any e.

Example :- Let us find the square roots of $a = 17 \pmod{2^5}$; these exist since $17 \equiv 1 \pmod 8$. First we find a square root $\pmod{2^4}$. Taking r = 1 we have $r^2 = 1^2 = 17 + 2^3.(-2)$, so q = −2; taking k = 0 makes $q + rk = -2$ even, so $s = r + 2^2k = 1$ is a square root of 17 $\pmod{2^4}$. Now we repeat this process, using r = 1 as a square root $\pmod{2^4}$ to find a square root s $\pmod{2^5}$. We have $r^2 = 1 = 17 + 2^4.(-1)$, so now q = −1; taking k = 1 makes $q + rk = 0$ even, so $s = r + 2^3k = 9$ is a square root of 17 mod (2^5). The remaining square roots t are found by multiplying s = 9 by −1 and by $2^4 \pm 1 = \pm 15$, so we have $\pm 7, \pm 9$ as the complete set of square roots of 17 $\pmod{2^5}$.

Quadratic residues for arbitrary moduli

Theorem 2.35 Let $n = n_1 n_2 \ldots n_k$, where the integers n_i are mutually coprime. Then $a \in Q_n$ if and only if $a \in Q_{n_i}$ for each i.

Proof :- If $a \in Q_n$ then $a \equiv s^2 \pmod n$ for some $s \in U_n$. Clearly $a \equiv s^2 \pmod{n_i}$ for each i, with s coprime to n_i, so $a \in Q_{n_i}$. Conversely, if $a \in Q_{n_i}$ for

each i then there exist elements $s_i \in U_{n_i}$ such that $a = \equiv s_i^2 \pmod{n_i}$. By the Chinese Remainder Theorem there is an element $s \in Z_n$ such that $s \equiv s_i \pmod{n_i}$ for all i. Then $s^2 \equiv s_i^2 \equiv a \pmod{n_i}$ for all i, and hence $s^2 \equiv a \pmod{n}$ since the moduli n_i are comprime, so $a \in Q_n$.

We can now answer the questionof whether $a \in Q_n$ for arbitrary moduli n:

Theorem 2.36 Let $a \in U_n$. Then $a \in Q_n$ if and only if

(1) $a \in Q_p$ for each odd prime p dividing n, and

(2) $a \equiv 1 \pmod 4$ if $2^2 \mid n$, and $a \equiv 1 \pmod 8$ if $2^3 \mid n$.

(Note that condition (2) is relevant only when n is divisible by 4; in all other cases we can ignore it.)

Proof :- By Theorem 2.36, $a \in Q_n$ if and only if $a \in Q_{p^e}$ for each prime-power p^e in the factorisation of n. For odd primes p this is equivalent to $a \in Q_p$, by Theorem 2.33, giving condition (1); for $p = 2$ it is equivalent to condition (2), by Theorem 2.34.

Example :- Let $n = 144 = 2^4.3^2$. An element $a \in U_{144}$ is a quadratic residue if and only if $a \in Q_3$ and $a \equiv 1 \pmod 8$; since $Q_3 = \{1\} \subset Z_3$, this is equivalent to $a \equiv 1 \pmod{24}$, so $Q_{144} = \{1, 25, 49, 73, 97, 121\} \subset U_{144}$. Any $a \in Q_{144}$ must have $N = 8$ square roots. To find these, we first find its four square roots $\pmod{2^4}$ and its two square roots $\pmod{3^2}$ by the methods described earlier, and then we use the Chinese Remainder Theorem to covert each of these eight pairs of roots into a square root (mod 144). For instance, let $a = 73$; then $a \equiv 9 \pmod{2^4}$, with square roots $s \equiv \pm 3, \pm 5 \pmod{2^4}$, and similarly $a \equiv 1 \pmod{3^2}$, with square roots $s \equiv \pm 1 \pmod{3^2}$; solving these eight pairs of simultaneous congruences for s, we get the square roots $s \equiv \pm 19, \pm 35, \pm 37, \pm 53 \pmod{144}$.

Unit-3

Riemann Zeta Function and Dirichlet's Series

Riemann Zeta Function $\xi(s)$ and its convergence

Definition :- The Riemann zeta function denoted by $\xi(s)$, is defined as

$$\xi(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots. \qquad \text{where } s > 1.$$

Theorem 3.1 Prove that the function

$$\xi(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots.. \qquad \ldots(1)$$

converges for all real $s > 1$ and diverges for all real $s \leq 1$.

Proof :- Suppose first that $s > 1$. We group the terms together in blocks of length, 1, 2, 4, 8,…, giving

$$\xi(s) = 1 + \left(\frac{1}{2^s} + \frac{1}{3^s}\right) + \left(\frac{1}{4^s} + \ldots + \frac{1}{7^s}\right) + \left(\frac{1}{8^s} + \ldots + \frac{1}{15^s}\right) + \ldots$$

Now $$\frac{1}{2^s} + \frac{1}{3^s} \leq \frac{1}{2^s} + \frac{1}{2^s} = \frac{2}{2^s} = 2^{1-s},$$

$$\frac{1}{4^s} + \ldots + \frac{1}{7^s} \leq \frac{1}{4^s} + \ldots + = \frac{1}{4^s} = \frac{4}{4^s} = (2^{1-s})^2,$$

$$\frac{1}{8^s} + \ldots + \frac{1}{15^s} \leq \frac{1}{8^s} + \ldots + = \frac{1}{8^s} = \frac{8}{8^s} = (2^{1-s})^3, \text{ and so on.}$$

So we can compare (1) with the geometric series

$$1 + 2^{1-s} + (2^{1-s})^2 + (2^{1-s})^3 + \ldots \text{i.e. } 1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots \leq 1 + 2^{1-s} + 2^{(1-s)^2} + \ldots\ldots\ldots..$$

This converges since $0 < 2^{1-s} < 1$ and hence so does (1) by the comparison test. In fact, this argument shows that $1 \le \xi(s) \le f(s)$ for all $s > 1$, where

$$f(s) = \sum_{n=0}^{\infty} (2^{1-s})^n = \frac{1}{1-2^{1-s}}.$$

If $s \to +\infty$ then $2^{1-s} \to 0$ and so $f(s) \to 1$, giving $\lim_{s\to+\infty} \xi(s) = 1$.

We now show that (1) diverges for $s \le 1$. This is obvious if $s \le 0$, since than $\frac{1}{n^s} \to 0$ as $n \to \infty$, so let us assume that $s > 0$. By grouping the terms of (1) in blocks of length 1, 1, 2, 4,…, we have

$$\xi(s) = 1 + \frac{1}{2^s} + \left(\frac{1}{3^s} + \frac{1}{4^s}\right) + \left(\frac{1}{5^s} + \ldots + \frac{1}{8^s}\right) + \ldots$$

If $s \le 1$, then $\frac{1}{2^s} \ge \frac{1}{2}$, $\frac{1}{3^s} + \frac{1}{4^s} \ge \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$,

$\frac{1}{5^s} + \ldots + \frac{1}{8^s} \ge \frac{1}{8} + \ldots + \frac{1}{8} = \frac{1}{2}$, and so on, so (1) diverges by comparison with the divergent series $1 + \frac{1}{2} + \frac{1}{2} + \ldots$ In particular, by taking $s = 1$, we see that the harmonic series

$\sum \frac{1}{n}$ diverges.

Application to prime numbers.

Theorem 3.2 Using Riemann zeta function, prove that are infinitely many primes.

Proof :- Suppose there are only finitely many primes, say $p_1, p_2, \ldots p_k$. For each prime $p = p_i$, we have $\left|\frac{1}{p}\right| < 1$, so there is a convergent geometric series

$$1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \ldots = \frac{1}{1-p^{-1}}.$$

If follows that if we multiply these k different series together, their product

$$\prod_{i=1}^{k} \left(1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \ldots\right) = \prod_{i=1}^{k} \left(\frac{1}{1-p_i^{-1}}\right) \qquad \ldots(1)$$

is finite. Now there convergent series all consist of positive terms, so they are absolutely convergent. It follows that we can multiply out the series in (1) and rearrange the terms, without changing the product. If we take a typical term $\frac{1}{p_1^{e_1}}$ from the first series, $\frac{1}{p_2^{e_2}}$ from the 2nd series, and so on, where each $e_i \geq 0$, then their product

$$\frac{1}{p_1^{e_1}} \cdot \frac{1}{p_2^{e_2}} \cdots \frac{1}{p_k^{e_k}} = \frac{1}{p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}}$$

will represent a typical term in the expansion of (1). By the fundamental theorem of arithmetic, every integer $n \geq 1$ has a unique expansion $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ $(e_i \geq 0)$ as a product of powers of the primes p_i. Since we are assuming that these are the only primes; notice that we allow $e_i = 0$, in case n is not divisible by a particular prime p_i. This uniqueness implies that each n contributes exactly one term $\frac{1}{n}$ to (1), so the expansion takes the form

$$\prod_{i=1}^{k} \left(1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \cdots \right) = \sum_{n=1}^{\infty} \frac{1}{n} \qquad \ldots(2)$$

The right hand side is the harmonic series, which is divergent. However the LHS is finite, so this contradiction proves that there must be infinitely many primes.

ξ(s) as Euler's product

Theorem 3.3 If $s > 1$, then

$$\xi(s) = \prod_{p} \left(\frac{1}{1 - p^{-s}} \right), \text{ where the product is over all primes p.}$$

This is, infact, representation of Riemann zeta function as Euler's product.

Proof :- The method is to consider the product $p_k(s)$ of the factors corresponding to the first k primes, and to show that $P_k(s) \to \xi(s)$ as $k \to \infty$. Let $p_1, p_2 \ldots p_k$ be the first k primes. Now if $s > 0$ (so that the geometric series all converge) then

$$P_k(s) = \prod_{i=1}^{k} \left(\frac{1}{1 - p_i^{-s}} \right) = \prod_{i=1}^{k} \left(1 + \frac{1}{p_i^{s}} + \frac{1}{p_i^{2s}} + \cdots \right)$$

If we expand this product, the general term in the resulting series is $\frac{1}{n^s}$ where $n = p_1^{e1} p_2^{e2} ... p_k^{ek}$ and each $e_i \geq 0$. The Fundamental Theorem of Arithmetic implies that each such n contributes just one term to $P_k(s)$, so

$$P_k(s) = \sum_{n \in A_k} \frac{1}{n^s},$$

where $A_k = \left\{ n : n = p_1^{e1} p_2^{e2} ... p_k^{ek}, e_i \geq 0 \right\}$ is the set of integers n whose prime factor are among $p_1, p_2 \ldots p_k$. Each $n \notin A_k$ is divisible by same prime $p > p_k$, and so $n > p_k$. It follows that if $s > 1$ Then

$$|P_k(s) - \xi(s)| = \sum_{n \notin A_k} \frac{1}{n^s} \leq \sum_{n > p_k} \frac{1}{n^s} = \xi(s) - \sum_{n \leq p_x} \frac{1}{n^s}.$$

Since $s > 1$, the partial sum of the series $\sum \frac{1}{n^s}$ converges to $\xi(s)$, so in particular $\sum_{n \leq p_k} \frac{1}{n^s} \to \xi(s)$ as $k \to \infty$. Thus $|P_k(s) - \xi(s)| \to 0$ as $x \to \infty$, so $P_k(s) \to \xi(s)$ as required.

Evaluation of $\xi(2)$ and $\xi(2k)$.

Theorem 3.4 If $\xi(s)$ is Riemann zeta function, then $\xi(2) = \frac{\pi^2}{6}$

Proof :- We know that the function sin z can be expanded as

$$\sin z = z \prod_{n \neq 0} \left(1 - \frac{z}{n\pi}\right) = z \prod_{n \geq 1} \left(1 - \frac{z^2}{n^2 \pi^2}\right) \qquad \ldots(1)$$

The first product in (1) is over all non zero integers n, and the second product is obtained from the first by pairing the factors corresponding to $\pm n$.

Also the Taylor series expansion of sin z is

$$\sin z = z - \frac{z^3}{\underline{|3}} + \frac{z^5}{\underline{|5}} \ldots \qquad \ldots(2)$$

Comparing the coefficients of z^3 in (1) and (2), we see that

$$-\sum_{n\geq 1}\frac{1}{n^2\pi^2}=-\frac{1}{\underline{|3}}$$

Multiplying by $-\pi^2$, we get

$$\xi(2)=\frac{\pi^2}{6}.$$

Theorem 3.5 If $\xi(s)$ is a Riemann zeta function, then evaluate $\xi(2k)$ where $k \geq 1$.

Proof :- We know that sin z can be written as

$$\sin z = z\prod_{n\geq 1}\left(1-\frac{z^2}{n^2\pi^2}\right) \qquad \ldots(1)$$

Taking log . of (1), we have

$$\log\sin z = \log z + \sum_{n\geq 1}\log\left(1-\frac{z^2}{n^2\pi^2}\right)$$

and differentiating term by term

$$\cot z = \frac{1}{z}-\sum_{n\geq 1}\frac{2z}{n^2\pi^2}\left(1-\frac{z^2}{n^2\pi^2}\right)^{-1}.$$

Now $$\frac{2z}{n^2\pi^2}\left(1-\frac{z^2}{n^2\pi^2}\right)^{-1}=\frac{2z}{n^2\pi^2}\sum_{k\geq 0}\left(\frac{z^2}{n^2\pi^2}\right)^k$$

$$=2\sum_{k\geq 0}\frac{z^{2k+1}}{n^{2k+2}\pi^{2k+2}}=2\sum_{k\geq 1}\frac{z^{2k-1}}{n^{2k}\pi^{2k}}$$

and then collect powers of z, we get

$$\cot z=\frac{1}{z}-2\sum_{k\geq 1}\sum_{n\geq 1}\frac{z^{2k-1}}{n^{2k}\pi^{2k}}=\frac{1}{z}-2\sum_{k\geq 1}\frac{\xi(2k)z^{2k-1}}{\pi^{2k}} \qquad \ldots(2)$$

which is the Laurent series for cot z

We will now compare (2) with a second expansion of cot z. The exponential series

$$e^t = 1 + t + \frac{t^2}{\lfloor 2} + \frac{t^3}{\lfloor 3}$$

implies that

$$\frac{e^t - 1}{t} = 1 + \frac{t}{\lfloor 2} + \frac{t^2}{\lfloor 3} + \ldots$$

and the reciprocal of this has a Taylor series expansion which can be written in the form

$$\frac{t}{e^t - 1} = \left(1 + \frac{t}{\lfloor 2} + \frac{t^2}{\lfloor 3} + \ldots\right)^{-1} = \sum_{m \geq 0} \frac{B_m}{\lfloor m} t^m \qquad \ldots(3)$$

for certain constants $B_0, B_1 \ldots$ known as the Bernoulli numbers.

Now $$\frac{t}{e^t - 1} = \frac{t}{2}\left(\frac{e^t + 1}{e^t - 1} - 1\right) = \frac{t}{2}\left(\frac{e^{t/2} + e^{-t/2}}{e^{t/2} - e^{-t/2}} - 1\right)$$

$= \frac{t}{2}\left(\coth \frac{t}{2} - 1\right) = \frac{t}{2}\left(i \cot \frac{it}{2} - 1\right)$ where $i = \sqrt{-1}$. Putting $z = it/2$, we get

$$\frac{t}{e^t - 1} = z \cot z - \frac{z}{i} = z \cot z + iz.$$

Dividing by z and using (3), we have

$$\cot z = -i + \frac{1}{z} \sum_{m \geq 0} \frac{B_m}{\lfloor m} t^m = -i + \sum_{m \geq 0} \frac{B_m}{\lfloor m} \left(\frac{2}{i}\right)^m z^{m-1}$$

By comparing the coefficients of (2), we see that if $m = 2k \geq 2$,

then $$-2 \frac{\xi(2k)}{\pi^{2k}} = \frac{B_{2k}}{\lfloor (2k)} \left(\frac{2}{i}\right)^{2k},$$

so that $$\xi(2k) = \frac{(-1)^{k-1} 2^{2k-1} \pi^{2k} B_{2k}}{\lfloor 2k} \qquad \ldots(4)$$

Thus $$\xi(2) = \pi^2 B_2,\ \xi(4) = -\frac{\pi^4 B_4}{3},\ \xi(6) = \frac{2\pi^6 B_6}{45}$$ and so on.

We know that $B_0 = 1,\ B_1 = \frac{-1}{2},\ B_2 = \frac{1}{6},\ B_3 = 0$

$$B_4 = \frac{-1}{30},\ B_5 = 0,\ B_6 = \frac{1}{42}$$ and so on.

Thus $$\xi(2) = \frac{\pi^2}{6},\ \xi(4) = \frac{\pi^4}{90},\ \xi(6) = \frac{\pi^6}{945}$$ etc.

Dirichlet's Series with simple properties :-

Definition :- If f is an arithmetic function, then its Dirichlet series is the series

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

Example :- If f(n) = u(n), then $F(s) = \sum \frac{u(n)}{n^s} = \sum \frac{1}{n^s} = \xi(s)$ where u(n) = 1 $\forall\ n \in N$ is the unit function.

Example :- If f(n) = N(n) then $F(s) = \sum \frac{N(n)}{n^s} = \sum \frac{n}{n^s} = \sum \frac{1}{n^{s-1}} = \xi(s-1)$

where N(n) = n for all n.

Example :- If f(n) = μ(n), then

$$F(s) = \sum \frac{\mu(n)}{n^s} = \frac{1}{\xi(s)}$$ where μ(n) is Mobius function.

Notation. Following Riemann, we let s be a complex variable and write

$$s = \sigma + it,$$

where σ and t are real. Then $n^s = e^{s \log n} = e^{(\sigma + it)\log n}$. This shows that $|n^s| = n^\sigma$ since $|e^{i\theta}| = 1$ for real θ.

The set of points $s = \sigma + it$ such that $\sigma > a$ is called a half-plane. We will show that for each Dirichlet series there is a half-plane $\sigma > \sigma_c$ in which the

series converges, and another half-plane $\sigma > \sigma_a$ in which it converges absolutely. We will also show that in the half-plane of convergence the series represents an analytic function of the complex variable s.

The half-plane of absolute convergence of a Dirichlet series

First we note that if $\sigma \geq a$ we have $|n^s| = n^\sigma \geq n^a$ hence

$$\left|\frac{f(n)}{n^s}\right| \leq \frac{|f(n)|}{n^a} .$$

Therefore, if a Dirichlet series $\Sigma f(n)n^{-s}$ converges absolutely for $s = a + ib$, then by the comparison test it also converges absolutely for all s with $\sigma \geq a$.

Theorem 3.6 Suppose the series $\Sigma |f(n)n^{-s}|$ does not converge for all s or diverge for all s. Then there exists a real number σ_a, called the abscissa of absolute convergence, such that the series $\Sigma f(n)n^{-s}$ converges absolutely if $\sigma > \sigma_a$ but does not converge absolutely if $\sigma < \sigma_a$.

Proof. Let D be the set of all real σ such that $\Sigma |f(n)n^{-s}|$ diverges. D is not empty because the series does not converge for all s, and D is bounded above because the series does not diverge for all s. Therefore D has a least upper bound which we call σ_a . If $\sigma < \sigma_a$ then $\sigma \in D$, otherwise σ would be an upper bound for D smaller than the least upper bound. If $\sigma > \sigma_a$ then $\sigma \notin D$ since σ_a is an upper bound for D . This proves the theorem.

Note : If $\Sigma |f(n)n^{-s}|$ converges everywhere we define $\sigma_a = -\infty$. If the series $\Sigma |f(n)n^{-s}|$ converges nowhere we define $\sigma_a = +\infty$.

Example. Riemann zeta function. The Dirichlet series $\sum_{n=1}^{\infty} n^{-s}$ converges absolutely for $\sigma > 1$. When s = 1 the series diverges, so $\sigma_a = 1$. The sum of this series is denoted by $\zeta(s)$ and is called the Riemann zeta function.

Example. If f is bounded, say $|f(n)| \leq M$ for all $n \geq 1$, then $\Sigma f(n)n^{-s}$ converges absolutely for $\sigma > 1$, so $\sigma_a \leq 1$. In particular if χ is a Dirichlet character the L-series $L(s, \chi) = \Sigma \chi(n)n^{-s}$ converges absolutely for $\sigma > 1$.

Example. The series $\Sigma n^n n^{-s}$ diverges for every s so $\sigma_a = +\infty$.

Example. The series $\Sigma n^{-n} n^{-s}$ converges absolutely for every s so $\sigma_a = -\infty$.

The Function Defined by a Dirichlet series

Assume that $\Sigma f(n)n^{-s}$ converges absolutely for $\sigma > \sigma_a$ and let F(s) denote the sum function

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \quad \text{for } \sigma > \sigma_a .$$

This section derives some properties of F(s). First we prove the following lemma :

Lemma 1. If $N \geq 1$ and $\sigma \geq c > \sigma_a$ we have

$$\left| \sum_{n=N}^{\infty} f(n) n^{-s} \right| \leq N^{-(\sigma-c)} \sum_{n=N}^{\infty} |f(n)| n^{-c} .$$

Proof. We have

$$\left| \sum_{n=N}^{\infty} f(n) n^{-s} \right| \leq \sum_{n=N}^{\infty} |f(n)| n^{-\sigma} = \sum_{n=N}^{\infty} |f(n)| n^{-c} n^{-(\sigma-c)}$$

$$\leq N^{-(\sigma-c)} \sum_{n=N}^{\infty} |f(n)| n^{-c} .$$

The next theorem describes the behaviour of F(s) as $\sigma \to +\infty$.

Theorem 3.7 If $F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ for $\sigma > \sigma_a$, then

$$\lim_{\sigma \to +\infty} F(\sigma + it) = f(1)$$

uniformly for $-\infty < t < +\infty$.

Proof. Since $F(s) = f(1) + \sum_{n=2}^{\infty} f(n) n^{-s}$ we need only prove that the second term tends to 0 as $\sigma \to +\infty$. Choose $c > \sigma_a$. Then for $\sigma \geq c$ the lemma implies

$$\left| \sum_{n=2}^{\infty} \frac{f(n)}{n^s} \right| \leq 2^{-(\sigma-c)} \sum_{n=2}^{\infty} |f(n)| n^{-c} = \frac{A}{2^{\sigma}}$$

where A is independent of σ and t . Since $A/2^{\sigma} \to 0$ as a $\sigma \to +\infty$ this proves the theorem.

Examples. $\zeta(\sigma + it) \to 1$ and $L(\sigma + it, \chi) \to 1$ as $\sigma \to +\infty$.

We prove next that all the coefficients are uniquely determined by the sum function.

Theorem 3.8 Uniqueness theorem. Given two Dirichlet series

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \quad \text{and} \quad G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s},$$

both absolutely convergent for $\sigma > \sigma_a$. If $F(s) = G(s)$ for each s in an infinite sequence $\{s_k\}$ such that $\sigma_k \to +\infty$ as $k \to \infty$, then $f(n) = g(n)$ for every n.

Proof. Let $h(n) = f(n) - g(n)$ and let $H(s) = F(s) - G(s)$. Then $H(s_k) = 0$ for each k. To prove that $h(n) = 0$ for all n we assume that $h(n) \neq 0$ for some n_0 and obtain a contradiction.

Let N be the smallest integer for which $h(n) \neq 0$. Then

$$H(s) = \sum_{n=N}^{\infty} \frac{h(n)}{n^s} = \frac{h(N)}{N^s} + \sum_{n=N+1}^{\infty} \frac{h(n)}{n^s}.$$

Hence

$$h(N) = N^s H(s) - N^s \sum_{n=N+1}^{\infty} \frac{h(n)}{n^s}.$$

Putting $s = s_k$ we have $H(s_k) = 0$ hence

$$h(N) = -N^{s_k} \sum_{n=N+1}^{\infty} h(n) n^{-s_k}.$$

Choose k so that $\sigma_k > c$ where $c > \sigma_a$. Then Lemma 1 implies

$$|h(N)| \leq N^{\sigma_k} (N+1)^{-(\sigma_k - c)} \sum_{n=N+1}^{\infty} |h(n)| n^{-c} = \left(\frac{N}{N+1}\right)^{\sigma_k} A$$

where A is independent of k. Letting $k \to \infty$ we find $(N/(N+1))^{\alpha_k} \to 0$ so $h(N) = 0$, a contradiction.

The uniqueness theorem implies the existence of a half-plane in which a Dirichlet series does not vanish (unless, of course, the series vanishes identically).

Theorem 3.9 Let $F(s) = \Sigma f(n) n^{-s}$ and assume that $F(s) \neq 0$ for some s with $\sigma > \sigma_a$. Then there is a half-plane $\sigma > c \geq \sigma_a$ in which $F(s)$ is never zero.

Proof. Assume no such half-plane exists. Then for every $k = 1,2,\ldots$ there is a point s_k with $\sigma_k > k$ such that $F(s_k) = 0$. Since $\sigma_k \to +\infty$ as $k \to$

∞ the uniqueness theorem shows that f(n) = 0 for all n, contradicting the hypothesis that $F(s) \neq 0$ for some s .

The half-plane of convergence of a Dirichlet series

To prove the existence of a half-plane of convergence we use the following lemma :

Lemma 2. Let $s_0 = \sigma_0 + it_0$ and assume that the Dirichlet series $\Sigma f(n) n^{-s_0}$ has bounded partial sums, say

$$\left| \sum_{n \le x} f(n) n^{-s_0} \right| \le M$$

for all $x \ge 1$. Then for each s with $\sigma > \sigma_0$ we have

$$\left| \sum_{a < n \le x} f(n) n^{-s} \right| \le 2M a^{\sigma_0 - \sigma} \left(1 + \frac{|s - s_0|}{\sigma - \sigma_0} \right) \qquad \ldots(1)$$

Proof. Let $a(n) = f(n) n^{-s_0}$ and let $A(x) = \sum_{n \le x} a(n)$. Then $f(n)n^{-s} = a(n) n^{s_0 - s}$ so we can apply Abel's identity (to be proved in unit v) : For any arithmetical function a(n) and let

$$A(x) = \sum_{n \le x} a(n),$$

Where A(x) = 0 if x < 1. Assume f has a continuous derivative on the interval [y, x], where 0 < y < x. Then we have

$$\sum_{y < n \le x} a(n) f(n) = A(x) f(x) - A(y) f(y) - \int_y^x A(t) f'(t) dt$$

Theorem (with $f(x) = x^{s_0 - s}$) to obtain

$$\sum_{a < n \le b} f(n) n^{-s} = A(b) b^{s_0 - s} - A(a) a^{s_0 - s} (s - s_0) \int_a^b A(t) t^{s_0 - s - 1} \, dt .$$

Since $|A(x)| \le M$ this gives us

$$\left| \sum_{a < n \le b} f(n) n^{-s} \right| \le M b^{\sigma_0 - \sigma} + M a^{\sigma_0 - \sigma} + |s - s_0| M \int_a^b t^{\sigma_0 - \sigma - 1} \, dt$$

$$\leq 2M\, a^{\sigma_0-\sigma} + |s - s_0|\, M \left| \frac{b^{\sigma_0-\sigma} - a^{\sigma_0-\sigma-1}}{\sigma_0 - \sigma} \right|$$

$$\leq 2M\, a^{\sigma_0-\sigma} \left(1 + \frac{|s - s_0|}{\sigma - \sigma_0} \right).$$

Examples. If the partial sums $\sum_{n \leq x} f(n)$ are bounded, above Lemma 2 implies that $\Sigma\, f(n)n^{-s}$ converges for $\sigma > 0$. In fact, if we take $s_0 = \sigma_0 = 0$ in (1) we obtain, for $\sigma > 0$,

$$\left| \sum_{a<n\leq b} f(n)n^{-s} \right| \leq Ka^{-\sigma}$$

where K is independent of a. Let $a \to +\infty$ we find that $\Sigma\, f(n)n^{-s}$ converges if $\sigma > 0$. In particular, this shows that the Dirichlet series

$$\sum_{n=1}^{\infty} \frac{(-1)^n}{n^s}$$

converges for $\sigma > 0$ since $\left| \sum_{n\leq x} (-1)^n \right| \leq 1$.

Theorem 3.10 If the series $\Sigma\, f(n)n^{-s}$ converges for $s = \sigma_0 + it_0$ then it also converges for all s with $\sigma > \sigma_0$. If it diverges for $s = \sigma_0 + it_0$ then it diverges for all s with $\sigma < \sigma_0$.

Proof :- The second statement follows from the first. To prove the first statement, choose any s with $\sigma > \sigma_0$.Above Lemma shows that

$$\left| \sum_{a < n \leq b} f(n)n^{-s} \right| \leq Ka^{\sigma_0-\sigma}$$

where K is independent of a. Since $a^{\sigma_0-\sigma} \to 0$ as $\alpha \to +\infty$, the Cauchy condition shows that $\sum f(n)\, n^{-s}$ converges.

Theorem 3.11 If the series $\sum f(n)n^{-s}$ does not converge every where or diverge everywhere, then there exists a real number σ_c, called the abscissa of convergence, such that the series converges for all s in the half-plane $\sigma > \sigma_c$ and diverges for all s in the half-plane $\sigma < \sigma_c$.

Proof :- We argue as in the proof of Theorem 3.6, taking σ_c to be the least upper bound of all σ for which $\sum f(n)n^{-s}$ diverges.

Note. If the series converges everywhere we define $\sigma_c = -\infty$, and if it converges nowhere we define $\sigma_c = +\infty$.

Theorem 3.12 For any Dirichlet series with σ_c finite we have

$$0 \le \sigma_a - \sigma_c \le 1.$$

Proof :- It suffices to show that if $\sum f(n)\, n^{-s_0}$ converges for some s_0 then it converges absolutely for all s with $\sigma > \sigma_0 + 1$. Let A be an upper bound for the number $| f(n)\ n^{-s_0} |$. Then

$$\left|\frac{f(n)}{n^s}\right| = \left|\frac{f(n)}{n^{s_0}}\right| \left|\frac{1}{n^{s-s_0}}\right| \le \frac{A}{n^{\sigma-\sigma_0}}$$

so $\sum | f(n)n^{-s} |$ converges by comparison with $\sum n^{\sigma_0-\sigma}$.

Example The series

$$\sum_{n=1}^{\infty} \frac{(-1)^n}{n^s}$$

converges if $\sigma > 0$, but the convergence is absolute only if $\sigma > 1$. Therefore in this example $\sigma_c = 0$ and $\sigma_a = 1$.

Definition :- If f and g are arithmetic functions, then their Dirichlet product or convolution, is the arithmetic function $f * g$ given by

$$(f * g)(n) = \sum_{d/n} f(d)\, g\left(\frac{n}{d}\right);$$

equivalently, putting $e = \frac{n}{d}$, we have

$$(f * g)\,(n) = \sum_{de=n} f(d)\ g(e)].$$

Theorem 3.13 Suppose that

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}, \quad G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s} \text{ and}$$

$$H(s) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s} \text{ where } h = f * g.$$ Then $H(s) = F(s)\cdot G(s)$ for all s such that F(s) and G(s) both average absolutely.

Proof :- If F(s) and G(s) both converge absolutely, then we can multiply these series and re arrange their terms to give

$$F(g)\,G(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \cdot \sum_{n=1}^{\infty} \frac{g(n)}{n^s}$$

$$= \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \frac{f(m)g(n)}{(mn)^s} = \sum_{k=1}^{\infty} \sum_{mn=k} \frac{f(m)g(n)}{k^s}$$

$$= \sum_{k=1}^{\infty} \frac{(f * g)(k)}{k^s} = \sum_{k=1}^{\infty} \frac{h(k)}{k^s} = H(s)$$

Example :- If we take $f = \mu$, $g = u$, then

$h = f * g = \mu * u = I$. where I = identity function and $I(1) = 1$, $I(n) = 0\ \forall\ n > 1$.

Now $I(1) = 1$ and $I(n) = 0$ for all $n > 1$

so $H(s) = \sum \frac{I(n)}{n^s} = 1$ for all s.

We have $F(s) = \sum \frac{\mu(n)}{n^s}$ and

$G(s) = \sum \frac{u(n)}{n^s} = \sum \frac{1}{n^s} = \xi(s)$, both absolutely convergent for $s > 1$.

Using above theorem, we have

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \xi(s) = 1, \text{ so that}$$

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\xi(s)} \text{ for all } s > 1.$$

Example :- Let $f = \phi$ and $g = u$. Then $G(s) = \xi(s)$ is absolutely convergent for $s > 1$. Now $1 \le \phi(n) \le n$ for all n, so $F(s) = \sum \frac{\varphi(n)}{n^s}$ is absolutely convergent by comparison with $\sum \frac{n}{n^s} = \xi(s-1)$ for $s - 1 > 1$, that is, for $s > 2$

Also $\phi * u = N$, so

$$\sum_{n=1}^{\infty} \frac{\phi(n)}{n^s} \xi(s) = \sum_{n=1}^{\infty} \frac{N(n)}{n^s} = \sum_{n=1}^{\infty} \frac{n}{n^s} = \xi(s-1)$$

and hence $$\sum_{n=1}^{\infty} \frac{\phi(n)}{n^s} = \frac{\xi(s-1)}{\xi(s)} \text{ for all } s > 2.$$

Analytic properties of Dircichlet series

Convergence properties of Dirichlet series can be compared with those of power series. Every power series has a disk of convergence, whereas every Dirichlet series has a half-plane of convergence. For power series the interior of the disk of convergence is also the domain of absolute convergence. For Dirichlet series the domain of absolute convergence may be a proper subset of the domain of convergence. A power series represents an analytic function inside its disk of convergence. We show next that a Dirichlet series represents an analytic function inside its half-plane of convergence.

Analytic properties of Dirichlet series will be deduced from the following general theorem of complex function theory which we state as a lemma.

Lemma 3. Let $\{f_n\}$ be a sequence of functions analytic on an open subset S of the complex plane, and assume that $\{f_n\}$ converges uniformly on every compact subset of S to a limit function f. Then f is analytic on S and the sequence of derivatives $\{f'_n\}$ converges uniformly on every compact subset of S to be derivative f'.

Proof :- Since f_n is analytic on S we have Cauchy's integral formula

$$f_n(a) = \frac{1}{2\pi i}\int_{\partial D} \frac{f_n(z)}{z-a}\, dz$$

where D is any compact disk in S, ∂D is its positively oriented boundary, and a is any interior point of D. Because of uniform convergence we can pass to the limit under the integral sign and obtain

$$f(a) = \frac{1}{2\pi i}\int_{\partial D} \frac{f(z)}{z-a}\, dz$$

which implies that f is analytic inside D. For the derivatives we have

$$f_n'(a) = \frac{1}{2\pi i}\int_{\partial D} \frac{f_n(z)}{(z-a)^2}\, dz \text{ and}$$

$$f'(a) = \frac{1}{2\pi i}\int_{\partial D} \frac{f(z)}{(z-a)^2}\, dz$$

from which it follows easily that $f_n'(a) \to f'(a)$ uniformly on every compact subset of S as $n \to \infty$.

To apply the lemma to Dirichlet series we show first that we have uniform convergence on compact subsets of the half-plane of convergence.

Theorem 3.14 A Dirichlet series $\sum f(n)n^{-s}$ converges uniformly on every compact subset lying interior to the half plane of convergence $\alpha > \sigma_c$.

Proof: It is suffice to show that $\sum f(n)n^{-s}$ converges uniformly on every compact rectangle $R = [\alpha, \beta] \times [c, d]$ with $\alpha > \sigma_c$. To do this we use the estimate ,

$$\left| \sum_{a < n \le b} f(n)n^{-s} \right| \le 2Ma^{\sigma_0 - \sigma}\left(1 + \frac{|s - s_0|}{\sigma - \sigma_0}\right) \qquad \ldots(1)$$

where $s_0 = \sigma_0 + it_0$ is any point in the half-plane $\sigma > \sigma_c$ and s is any point with $\sigma > \sigma_0$. We choose $s_0 = \sigma_0$ where $\sigma_c < \sigma_0 < \alpha$.

Then if $s \in R$ we have $\sigma - \sigma_0 \ge \alpha - \sigma_0$ and $|s_0 - s| < C$, where C is a constant depending on s_0 and R but not on s. Then (1) implies

$$\left| \sum_{a < n \le b} f(n)n^{-s} \right| \le 2Ma^{\sigma_0 - \alpha}\left(1 + \frac{C}{\alpha - \sigma_0}\right) = Ba^{\sigma_0 - \alpha}$$

where B is independent of s. Since $\alpha^{\sigma_0 - \alpha} \to 0$ as $a \to +\infty$ the Cauchy condition for uniform convergence is satisfied.

Theorem 3.15 The sum function $F(s) = \sum f(n)n^{-s}$ of a Dirichlet series is analytic in its half-plane of convergence $\sigma > \sigma_c$, and its derivative $F'(s)$ is represented in this half-plane by the Dirichlet series

$$F'(s) = -\sum_{n=1}^{\infty} \frac{f(n)\log n}{n^s}, \qquad \ldots(1)$$

obtained by differentiating term by term.

Proof :- We apply above theorem 3.14 and Lemma 3 to the sequence of partial sums.

Notes :- The derived series in (1) has the same abscissa of convergence and the same abscissa of absolute convergence as the series for F(s).

Applying Theorem 3.15 repeatedly we find that the kth derivative is given by

$$F^{(k)}(s) = (-1)^k \sum_{n=1}^{\infty} \frac{f(n)(\log n)^k}{n^s} \text{ for } \sigma > \sigma_c.$$

Examples For $\sigma > 1$ we have

$$\zeta'(s) = -\sum_{n=1}^{\infty} \frac{\log n}{n^s} \qquad \ldots(2)$$

and

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}. \qquad \ldots(3)$$

Equation (2) follows by differentiating the series for the zeta function term by term, and (3) is obtained by multiplying the two Dirichlet series $\sum \Lambda(n)\, n^{-s}$ and $\sum n^{-s}$ and using the identity $\sum_{d \mid n} \Lambda(d) = \log n$.

Dirichlet series with nonnegative coefficients

Some functions which are defined by Dirichlet series in their half-plane of convergence $\sigma > \sigma_c$ can be continued analytically beyond the line $\sigma = \sigma_c$. For example, Riemann zeta function $\zeta(s)$ can be continued analytically beyond the line $\sigma = 1$ to a function which is analytic for all s except for a simple pole at s = 1. The singularity for the zeta function is explained by the following theorem of Landau which deals with Dirichlet series having nonnegative coefficients.

Theorem 3.16 Let F(s) be represented in the half-plane $\sigma > c$ by the Dirichlet series

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}, \qquad \ldots(1)$$

where c is finite, and assume that $f(n) \geq 0$ for all $n \geq n_0$. If F(s) is analytic in some disk about the point s = c, then the Dirichlet series converges in the half-plane $\sigma > c - \varepsilon$ for some $\varepsilon > 0$. Consequently, if the Dirichlet series has a finite abscissa of convergence σ_c, then F(s) has a singularity on the real axis at the point $s = \sigma_c$.

Proof :- Let a = 1 + c. Since F is analytic at a it can be represented by an absolutely convergent power series expansion about a,

$$F(s) = \sum_{k=0}^{\infty} \frac{F^{(k)}(a)}{k!}(s-a)^k, \qquad \ldots(2)$$

and the radius of convergence of this power series exceeds 1 since F is analytic at c, (see the figure 3.1 below). By theorem 3.16 the derivatives $F^{(k)}(a)$ can be determined by repeated differentiation of (1). This gives us

$$F^{(k)}(a) = (-1)^k \sum_{n=1}^{\infty} f(n)\, (\log n)^k\, n^{-a},$$

So (2) can be rewritten as

$$F(s) = \sum_{k=0}^{\infty} \sum_{n=1}^{\infty} \frac{(a-s)^k}{k!} f(n)\, (\log n)^k\, n^{-a}. \qquad \ldots(3)$$

Since the radius of convergence exceeds 1, this formula is valid for some real $s = c - \varepsilon$ where $\varepsilon > 0$ (see figure below). Then $a - s = 1 + \varepsilon$ for this s and the double series in (3) has nonnegative terms for $n \geq n_0$. Therefore we can interchange the order of summation to obtain

$$F(c-\varepsilon) = \sum_{n=1}^{\infty} \frac{f(n)}{n^a} \sum_{k=0}^{\infty} \frac{\{(1+\varepsilon)\log n\}^k}{k!} = \sum_{n=1}^{\infty} \frac{f(n)}{n^a} e^{(1+\varepsilon)\log n} = \sum_{n=1}^{\infty} \frac{f(n)}{n^{c-\varepsilon}}.$$

In other words, the Dirchlet series $\sum f(n)n^{-s}$ converges for $s = c - \varepsilon$, hence it also converges in the half-plane $\sigma > c - \varepsilon$.

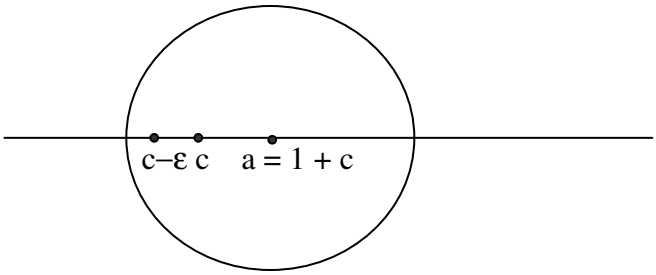


Figure 3.1

Definition :- An arithmetic function f is called multiplicative if f(mn) = f(m) f(n) where gcd (m, n) = 1.

Definition :- An arithmetic function f is completely multiplicative if f(mn) = f(m) f(n) for all positive integers m and n.

Euler Products

The product expansions of a function in which the factors are indexed by the primes are called Euler products. For example $\xi(s) = \prod_p \left(\frac{1}{1-p^{-s}}\right) \forall\ s > 1$, where the product is over all primes.

Theorem 3.17 (a) If f(n) is multiplicative and $\sum_{n=1}^{\infty} f(n)$ is absolutely convergent, then

$$\sum_{n=1}^{\infty} f(n) = \prod_p (1 + f(p) + f(p^2) + ...)$$

(b) If f(n) is completely multiplicative, and $\sum_{n=1}^{\infty} f(n)$ is absolutely convergent, then

$$\sum_{n=1} f(n) = \prod_{p} \left(\frac{1}{1-f(p)} \right).$$

Proof :- (a) Let $p_1, p_2, \ldots, p_k$ be the first k primes, and let

$$P_k = \prod_{i=1}^{k} (1 + f(p_i) + f(p_i^2) + \ldots)$$

The general term in the expansion of $P_k(s)$ is

$$f(p_1^{e1}) \ldots f(p_k^{ek}) = f(p_1^{e1} \ldots p_k^{ek}) \text{ , because f(n) is multiplicative}$$

Thus $$P_k = \sum_{n \in A_k} f(n)$$

where $$A_k = \{ n : n = p_1^{e1} \ldots p_k^{ek}, e_i \geq 0 \}.$$

We have $$\left| P_k - \sum_{n=1}^{\infty} f(n) \right| = \left| \sum_{n \notin A_k} f(n) \right| \leq \sum_{n \notin A_k} | f(n) |$$

$$\leq \sum_{n > p_k} | f(n) |, \text{ since } n > p_k \text{ for each } n \notin A_k.$$

Now $\sum_{n=1}^{\infty} | f(n) |$ converges, so as $k \to \infty$ we have $\sum_{n > p_k} | f(n) | \to 0$ and hence

$$\left| P_k - \sum_{n=1}^{\infty} f(n) \right| \to 0; \text{ thus } P_k \to \sum_{n=1}^{\infty} f(n) \text{ as } k \to \infty.$$

(b) If f(n) is completely multiplicative, then

$f(p^e) = f(p)^e$ for each prime power p^e, so part (a) gives

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} (1 + f(p) + f(p^2) + \ldots)$$

$$= \prod_{p} (1 + f(p) + f(p)^2 + \ldots)$$

$$= \prod_{p} \left(\frac{1}{1-f(p)} \right).$$

Applying Theorem 3.17, to absolutely convergent Dirichlet series we immediately obtain :

Theorem 3.18 Assume $\Sigma f(n)n^{-s}$ converges absolutely for $\sigma > \sigma_a$. If f is multiplicative we have

$$\sum_{n=1}^{\infty}\frac{f(n)}{n^s} = \prod_p\left\{1+\frac{f(p)}{p^s}+\frac{f(p^2)}{p^{2s}}+...\right\} \text{ if } \sigma > \sigma_a, \qquad ...(1)$$

and if f is completely multiplicative we have

$$\sum_{n=1}^{\infty}\frac{f(n)}{n^s} = \prod_p\frac{1}{1-f(p)p^{-s}} \text{ if } \sigma > \sigma_a . \qquad ...(2)$$

It should be noted that the general term of the product in (1) is the Bells series $f_p(x)$ of the function f with $x = p^{-s}$.

Examples. Taking $f(n) = 1$, $\mu(n)$, $\phi(n)$, $\sigma_\alpha(n)$, respectively, we obtain the following Euler products :

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s} = \prod_p\frac{1}{1-p^{-s}} \quad \text{if } \sigma > 1 .$$

$$\frac{1}{\zeta(s)}\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s} = \prod_p(1-p^{-s}) \quad \text{if } \sigma > 1 .$$

$$\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n=1}^{\infty}\frac{\phi(n)}{n^s} = \prod_p\frac{1-p^{-s}}{1-p^{1-s}} \qquad \text{if } \sigma > 2 .$$

$$\zeta(s)\,\zeta(s-\alpha) = \sum_{n=1}^{\infty}\frac{\sigma_\alpha(n)}{n^s} = \prod_p\frac{1}{(1-p^{-s})-(1-p^{a-s})} \text{ if } \sigma > \max\{1, 1+\mathrm{Re}(\alpha)\}$$

Example :- The mobius function $\mu(n)$ is multiplicative, with $\mu(p) = -1$ and $\mu(p^e) = 0$ for all $e \geq 2$, so

$$\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s} = \prod_p\left(1+\frac{\mu(p)}{p^s}+\frac{\mu(p^2)}{p^{2^s}}+...\right) = \prod_p(1-p^{-s}) = \frac{1}{\xi(s)}. \text{ for all } s > 1.$$

Unit-IV

Diophantine Equations and Quadratic Fields

Diophantine equations

Definition :- A Diaphantine equation is an equation in more than one variables and with integral coefficients such as

$$ax + by = c, \quad x^3 + y^3 = z^3, \qquad x^2 + y^2 = z^2$$

Our problem is to find all the integral solutions of a given Diophantine equation.

To find solutions of diaphantine equation

$$x^2 + y^2 = z^2 \qquad \ldots(1)$$

Let $x = 0$, then the equation becomes $y^2 = z^2 \Rightarrow y = \pm z$

Similarly if $y = 0$, then $x^2 = z^2$ and $x = \pm z$. Let $z = 0 \Rightarrow x^2 + y^2 = 0 \Rightarrow x = 0 = y$

Thus all the solutions are known if either $x = 0$ or $y = 0$ or $z = 0$

So we assume neither of x, y, z is equal to zero.

Further if (x, y, z) is a solution of (1), ($\pm$ x, $\pm$ y, $\pm$ z) is also a solution of (1) for all combinations. So we assume $x > 0$, $y > 0$, $z > 0$. Again if (x, y, z) is a solution of (1), (dx, dy, dz) is also a solution of (1) for all d. So W. L. O. G. we assume gcd (x, y, z) = 1

Let $\gcd(x, y) = d > 1$

then $\quad d \mid x, d \mid y \Rightarrow d^2 \mid x^2, \; d^2 \mid y^2$

$\Rightarrow \quad d^2 \mid x^2 + y^2 \Rightarrow d^2 \mid z^2 \Rightarrow d \mid z$

$\Rightarrow \quad \gcd(x, y, z) \geq d > 1$

Similarly if $\gcd(x, z) = d > 1$ then $\gcd(x, y, z) \geq d > 1$ and same holds if $\gcd(x, z) > 1$

So to consider solutions where $\gcd(x, y, z) = 1$, it is enough to assume that $\gcd(x, y) = 1$

Now since $\gcd(x, y) = 1$, so both of x & y can not be even.

Let both x & y be odd, then

$$x^2 = 1 \pmod 8,\ y^2 \equiv 1 \pmod 8$$

$$\Rightarrow \qquad z^2 = x^2 + y^2 \equiv 2 \pmod 8$$

But there is no integer z with

$$z^2 \equiv 2 \pmod 8$$

So if (x, y, z) satisfies (1) and gcd(x, y) = 1 then one of x & y must be odd and other must be even.

W. L. O. G. we assume that x is even and y is odd

Definition :- A solution (x, y, z) satisfying a Diaphantine equation is called a primitive solution if gcd(x, y, z) = 1

Theorem 4.1 All the positive primitive solutions of

$$x^2 + y^2 = z^2 \qquad \ldots(1)$$

where x is even, y is odd, is given

by $$x = 2ab,\ y = a^2 - b^2,\ z = a^2 + b^2 \qquad \ldots(2)$$

where a > b > 0 and a and b are of opposite parity and gcd (a, b) = 1

Proof :- Suppose (x, y, z) are given by (2) where a & b satisfy given conditions. Then we shall prove x, y, z are positive primitive solutions of (1)

Clearly x > 0, y > 0, z > 0 since a > b > 0

Setting $x = 2ab,\ y = a^2 - b^2$ we get

$$x^2 + y^2 = (2ab)^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2$$

Thus (x, y, z) satisfy (1)

To prove gcd (x, y, z) = 1, it is enough to prove that gcd (y, z) = 1 where y & z are given by (2). Let $d = \gcd(a^2 - b^2, a^2 + b^2)$

Then $$d \mid (a^2 - b^2) \ \&\ d \mid (a^2 + b^2)$$

$$\Rightarrow \qquad d \mid (a^2 + b^2) \pm (a^2 - b^2)$$

$$\Rightarrow \qquad d \mid 2a^2 \ \&\ d \mid 2b^2$$

$\Rightarrow$ $d \mid \gcd(2a^2, 2b^2)$

$\Rightarrow$ $d \mid 2 \gcd(a^2, b^2)$

But $\gcd(a, b) = 1 \Rightarrow \gcd(a^2, b^2) = 1 \Rightarrow d \mid 2 \Rightarrow d = 1$ or 2

Since a & b are of opposite parity, both of $a^2 - b^2$ & $a^2 + b^2$ are odd

$\Rightarrow d \neq 2 \quad \Rightarrow \quad d = 1$

Thus if (x, y, z) are given by (2) (x, y, z) is a primitive solution of (1)

Now let (x, y, z) be any positive primitive solution of (1). Then we know

$$\gcd(x, y) = 1 \ \gcd(y, z) = 1 \text{ and } \gcd(x, z) = 1$$

Now from (1), $x^2 = z^2 - y^2 = (z + y)(z - y)$ …(3)

Since, x is even, y is odd, so from (1) z is also odd

$\Rightarrow$ $z + y$ & $z - y$ are both even

$\Rightarrow$ $\frac{z+y}{2}$ & $\frac{z-y}{2}$ are natural numbers. (Note that $z > y$)

Writing (3) as

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right) \qquad \ldots(4)$$

Now we claim $\gcd\left(\frac{z+y}{2}, \frac{z-y}{2}\right) = d = 1$

Now $d \left| \frac{z+y}{2} \right.$ & $d \left| \frac{z-y}{2} \right. \Rightarrow d \left| \left(\frac{z+y}{2} + \frac{z-y}{2} \right) \right.$

$\Rightarrow$ $d \mid z$ & $d \mid y \Rightarrow d = 1$ since $\gcd(y, z) = 1$

Since x is even $\Rightarrow \frac{x}{2}$ is a integer

So from (4) we see that product of two coprime natural numbers $\frac{z+y}{2}$ & $\frac{z-y}{2}$ is the square of an integer.

$\Rightarrow$ Both of $\frac{z+y}{2}$ & $\frac{z-y}{2}$ are squares uof integers.

Let $\frac{z+y}{2} = a^2$ & $\frac{z-y}{2} = b^2$ where $a > 0$ & $b > 0$ …(5)

Since $y > 0 \Rightarrow a > b > 0$

Also $\gcd\left(\frac{z+y}{2}, \frac{z-y}{2}\right) = 1 \Rightarrow \gcd(a^2, b^2) = 1$

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

Now from (5) we get $z = a^2 + b^2$ & $y = a^2 - b^2$ …(6)

Substituting these values in (1) and noting that $x > 0$, we get $x = 2ab$.

Since y is odd so from (6) we get a & b are of opposite parity.

This proves the theorem.

Example :- Find all the solutions of

$$x^2 + y^2 = z^2 \text{ where } 0 < z \leq 30 \quad \text{...(I)}$$

Solution :- First we assume $x > 0$, $y > 0$, $z > 0$, $\gcd(x, y) = 1$ and $2 \mid x$ then we know that all the solution of (I) are given by

$$x = 2ab,\ y = a^2 - b^2,\ z = a^2 + b^2 \quad \text{…(II)}$$

where $a > b > 0$, $\gcd(a, b) = 1$ and a & b are of opposite parity

Now consider

$$0 < a^2 + b^2 \leq 30$$

Then $a = 1$ is not possible since $a > b > 0$. Let $a = 2$, Then $b = 1$, since $a > b > 0$

Then $x = 4,\ y = 3,\ z = 5$ i.e. (4, 3, 5) is the solution

Let $a = 3$ then $b = 2$ since $a > b > 0$ and a & b are of opposite parity

Then $x = 2 \cdot 3 \cdot 2 = 12,\ y = 5$

Then $z = 13$ i.e., (12, 5, 13) is the solution

Let $a = 4$ then $b = 1$ or 3, then for $b = 1$, $x = 8$, $y = 15$, $z = 17$

So (8, 15, 7) is the required solution

Now $a = 4, b = 3$

Then $x = 24, y = 7, z = 25$

i.e. (24, 7, 25) is the solution

Now, take a = 5 then b = 2 since a > b, 0, a & b are of opposite parity

and $(a^2 + b^2) \leq 30$

Therefore $x = 20, y = 21, z = 29$ i.e., $\therefore$ (20, 21, 29) is a solution

So, all solutions with $x > 0, y > 0, z > 0$, x, even and gcd (x, y) = 1 are

(4, 3, 5), (12, 5, 13), (8, 15, 17), (24, 7, 25), (20, 21, 29)

So all solutions of the required type are

(± 4, ± 3, 5), (± 12, ± 5, 13), (± 8, ± 15, 17), (± 24, ± 17, 25), (± 20, ±21, 29), (±3, ±4, 5), (±5, ±12, 13), (±15, ±8, 17), (±7, ±24, 25), (±21, ±20, 29), (±16, 8, 10), (±8, ±16, 10), (±9, ±12, 15), (±12, ±9, 15), (±12, ±16, 20), (±16, ±12, 20), (±15, ±20, 25), (±20, ±15, 25), (±18, ±24, 30), (±24, ±18, 30), (±24, ±10, 26), (±10, ±24, 26)

Example :- Prove that if x, y, z satisfy

$$x^2 + y^2 = z^2$$

then (i) $xyz \equiv 0 \pmod{60}$ …(I)

(ii) $xy(x^2 - y^2) \equiv 0 \pmod{84}$ …(II)

Solution :- W. L. O. G., we assume

$x > 0, y > 0, z > 0$; gcd (x, y) = 1 and $2 \mid x$

Then we assume know

$$x = 2ab, y = a^2 - b^2, z = a^2 + b^2$$

where $a > b > 0$; gcd (a, b) = 1 & a, b are opposite parity

Then setting $x = 2ab$, $y = a^2 - b^2$, we get

$$xy = 2ab(a^2 - b^2) \qquad \ldots(III)$$

Since a & b are of opposite parity, one of a & b must be even and other must be odd

Therefore $xy \equiv 0 \pmod 4$ {from (III)} …(IV)

If $3 \mid a$ or $3 \mid b$ then from (III)

$$xy \equiv 0 \pmod 3$$

So, assume $3 \nmid a$ and $3 \nmid b$

Then by Fermat's theorem

$$a^2 \equiv 1 \equiv b^2 \pmod 3$$

$\Rightarrow$ $a^2 - b^2 \equiv 0 \pmod 3$

So in this case also $xy \equiv 0 \pmod 3$ So in all cases,

$$xy \equiv 0 \pmod 3 \qquad \ldots(V)$$

From (IV) & (V), we get

$$xy \equiv 0 \pmod{12} \qquad \ldots(VI)$$

in all cases

Now $xyz = 2ab\,(a^2 - b^2)\,(a^2 + b^2)$

$= 2ab\,(a^4 - b^4)$ …(VII)

If 5/a or 5/b then from (VII)

$$xyz \equiv 0 \pmod 5 \qquad \ldots(VIII)$$

Then from (VI) & (VIII), we get

$xyz \equiv 0 \pmod{60}$ in this case

So let $5 \times a$ and $5 \times b$

By Fermat's theorem

$$a^4 \equiv 1 \equiv b^4 \pmod 5$$

From (VII) $xyz \equiv 0 \pmod 5$ …(IX)

and in this case also from (VI) and (IX)

$$xyz \equiv 0(\text{mod } 60)$$

This proves (i)

(ii) $xy(x^2 - y^2) \equiv 0(\text{mod } 84)$

As in (i), take $x = 2ab$, $y = a^2 - b^2$

$$\therefore \quad xy \equiv 0(\text{mod } 12) \qquad \ldots(*)$$

Now $xy(x^2-y) = 2ab\,(a^2 - b^2)\,((2ab)^2 - (a^2 - b^2)^2)$

$$= 2ab\,(a^2 - b^2)\,(4a^2b^2 - a^4 - b^4 + 2a^2b^2)$$

$$= 2ab\,(a^2-b^2)\,(6a^2\,b^2 - a^4 - b^4)$$

$$\equiv 2ab\,(a^2 - b^2)\,(-a^2\,b^2 - a^4 - b^4)(\text{mod } 7)$$

$$\equiv -2ab(a^2 - b^2)\,(a^4 + b^4 + a^2\,b^2)\,(\text{mod } 7)$$

$$\equiv -2ab(a^6 - b^6) \equiv 2ab\,(b^6 - a^6)\,(\text{mod } 7) \qquad \ldots(**)$$

If $7 \mid a$ or $7 \mid b$, thus from (**) and (*)

$$xy(x^2 - y^2) \equiv 0(\text{mod } 84)$$

If $7 \nmid a$ and $7 \nmid b$ then by Fermat's theorem

$$b^6 \equiv a^6 \equiv 1(\text{mod } 7)$$

and again from (**),

$$xy(x^2 - y^2) \equiv 0\ (\text{mod } 84)$$

Hence the result

Fermat's Last Theorem :- This states that $x^n + y^n = z^n$ $(n \geq 3)$ has no solutions for which $(x,y,z) \neq 0$

We shall give the proof of the result that

$$x^4 + y^4 = z^4$$

has no solution for which $(x, y, z) \neq 0$. In fact we shall prove a little more we shall prove

Theorem 4.2 $x^4 + y^4 = u^2$ has no non-trivial solutions. …(1)

Proof :- If possible suppose the given equation has solutions.

W. L. O. G assume $x > 0, y > 0, u > 0$

Let $S = \{u \in N; x^4 + y^4 = u^2 \text{ for } x, y \in N\}$

Then by assumption $S \neq \phi$. So by law of well ordering, S has a least element. Let u_0 be the least element of S.

Then $\exists\, x_0 \in N, y_0 \in N$, such that $x_0^4 + y_0^4 = u_0^2$ …(2)

Then first we claim that $\gcd(x_0, y_0, u_0 = 1$

Let $\gcd(x_0, y_0, u_0) = d > 1$. Then $d \mid x_0$ & $d \mid y_0$

$\Rightarrow$ $d^4 \mid x_0^4$ & $d^4 \mid y_0^4 \Rightarrow d^4 \mid x_0^4 + y_0^4$

$\Rightarrow$ $d^4 \mid u_0^2 \Rightarrow d^2 \mid u_0$

Then $$\left(\frac{x_0}{d}\right)^4 + \left(\frac{y_0}{d}\right)^4 = \left(\frac{u_0}{d^2}\right)^2$$

i.e., $\left(\frac{x_0}{y}, \frac{y_0}{d}, \frac{u_0}{d^2}\right)$ satisfies (1) and so $\frac{u_0}{d^2} \in S$

$\Rightarrow$ $\frac{u_0}{d^2} \geq u_0 \qquad \Rightarrow 1 \geq d^2$

$\Rightarrow d = 1$. So $\gcd(x_0, y_0, u_0) = 1$

Then x_0, y_0 can not be both even, since then u_0 is also even & $\gcd(x_0, y_0, u_0) \geq 2$.

But x_0 & y_0 can not be both odd either since in that case

$$u_0^2 = x_0^4 + y_0^4 \equiv 1 + 1 = 2 (\text{mod } 8)$$

which has no solution. So one of x_0, y_0 is odd & other is even. W.L.O.G. assume x_0 is even. Then y_0 must be odd. Also

$$(x_0^2)^2 + (y_0^2)^2 = u_0^2 \text{ and } \gcd(x_0^2, y_0^2, u_0) = 1$$

Then by previous theorem there exists positive integers a & b such that

$x_0^2 - 2ab,\ y_0^2 = a^2 - b^2,\ u_0 = a^2 + b^2$ where $a > b > 0$, $\gcd(a, b) = 1$. …(3)

and a & b are of opposite parity.

If possible let a be even then b must be odd.

Then from (3)

$$y_0^2 = a^2 - b^2 \equiv -1 \pmod 4$$

but there does not exist any integer n such that $n^2 \equiv -1 \pmod 4$

Then a must be odd & b must be even. Let $b = 2c$. Then from (3)

$$x_0^2 = 2ab = 4ac \Rightarrow \frac{x_0^2}{4} = ac$$

$$\Rightarrow \quad \left(\frac{x_0}{2}\right)^2 = ac \qquad \ldots(4)$$

Since $\gcd(a, b) = 1$ & $b = 2c$

$\Rightarrow$ $\gcd(a, c) = 1$

Now (4) gives us that square of an integer is equal to product of two positive integer where both are relatively prime So both a & c must be square of integers.

Let $a = f^2$ & $c = g^2$

Since $\gcd(a, b) = 1 \Rightarrow \gcd(f^2, 2g^2) = 1$. Again from (3)

$$y_0^2 = a^2 - b^2 = a^2 - 4c^2 = (f^2)^2 - 4(g^2)^2 = f^4 - 4g^4$$

$$\Rightarrow \quad y_0^2 + 4g^4 = f^4 \qquad \ldots(5)$$

But $\gcd(f^2, 2g^2) = 1$

$\Rightarrow$ $\gcd(y_0, 2g^2) = 1$

because a & b are of opposite parity, then from (3), y_0 must be odd.

Now (5) can be written as

$$(y_0^2)^2 + (2g^2)^2 = (f^2)^2$$

where $\gcd(2g^2, y_0) = 1$, y_0 is odd, $2g^2$ is even. They by previous theorem, there exists integer r, s, such that $2g^2 = 2rs$, $y_0 = r^2 - s^2$ $f^2 = r^2 + s^2$ …(6)

where $r > s > 0$, $\gcd(r, s) = 1$ & r, s are of opposite parity

Now from (6), $2g^2 = 2rs \quad \Rightarrow \quad g^2 = rs$

But $\gcd(r, s) = 1$, so we have product of two relatively prime integers is the square of an integer. $\Rightarrow$ r & s must themselves be squares.

Let $r = v^2$ & $s = w^2$ where $v > 0$, $w > 0$

Now from (6), $f^2 = r^2 + s^2 = (v^2)^2 + (w^2)^2 = v^4 + w^4$.

Then (v, w, f)0 is a solution of (1). So $f \in S$.

$\Rightarrow \quad f \geq u_0$

But $f \leq f^2 = a \leq a^2 < a^2 + b^2 = u_0$ which is a contradiction and contradiction arose because we assume (1) has a solution. So (1) has no solution.

The represent of number by two or four squares.

Theorem 4.3 Let n be a natural number of the form 4k+3, then n cannot be written as a sum of 2 squares.

Proof :- If possible let $n = x^2 + y^2$. Then

$$x^2 \equiv 0 \text{ or } 1 (\text{mod } 4) \text{ and } y^2 \equiv 0 \text{ or } 1 (\text{mod } 4)$$

Then $n = x^2 + y^2 \equiv 0$ or 1 or 2(mod 4)

Thus if $n \equiv 3(\text{mod } 4)$, it cannot be written as a sum of two squares.

Theorem 4.4 Let $n = x^2 + y^2$. Then primes of the type 4k + 3 can occur in the prime factorization of n to an even degree only.

In other words if a prime of the type 4k + 3 occurs to an odd degree in the prime factorization of a natural number n then n can not be written as a sum of squares of 2 numbers.

Proof :- Let p be a prime of the type 4k + 3.

Let $n = p^{2k+1}n$, where $k \geq 0$ and $\gcd(n_1, p) = 1$

and let $n = p^{2k+1}n_1 = x^2 + y^2$

Then $n = x^2 + y^2 \equiv 0 (\text{mod } p)$

Let $p \nmid x$. Then $\gcd(p, x) = 1$

Now $\gcd(p, x) = 1$

$\Rightarrow \exists$ an integer q such that $x\,q \equiv 1 \pmod p$

Now $y^2 \equiv -x^2 \pmod p$

$\Rightarrow$ $q^2 y^2 \equiv -q^2 x^2 \equiv -1 \pmod p$

$\Rightarrow$ $(qy)^2 \equiv -1 \pmod p$

$\Rightarrow$ -1 is a quadratic residues of p.

But p is a prime of the type $4k + 3$ and so -1 must be a quadratic non-residue of p, which is a contradiction. So p must divide x. Then p must also divide y, since $x^2 + y^2 = 0 \pmod p$

Let $x = px_1$ & $y = py_1$

Then $n = x^2 + y^2 = p^2 (x_1^2 + y_1^2) \backslash= p^{2k+1} n_1$

$\Rightarrow x_1^2 + y_1^2 = p^{2k-1} n_1$

If $p \nmid x_1$, we have contradiction as before.

So if $x_1 = px_2$, $y_1 = py_2$, then $x_2^2 + y_2^2 = p^{2k-3} n_1$ proceeding as before.

Proceeding like this and decreasing the power of p by 2 at a time, we get

$x_k^2 + y_k^2 = pn_1$ for some positive integers x_k & y_k

Also $\gcd(n_1, p) = 1$, proceeding as before we get $p^2 \mid pn_1$

$\Rightarrow$ $p \mid n_1$, which contradicts $\gcd(p, n_1) = 1$

Thus n can not be written as a sum of 2 squares.

Theorem 4.5 If all primes of the type $4k + 3$ occur to an even degree in the prime factorization of a natural number n, then n can be written as a sum of 2 squares.

To prove Theorem, we first shall prove the following lemmas

Lemma 1 :- If n_1 & n_2 are representable as a sum of 2 squares, then $n_1 n_2$ is also representable as a sum of 2 squares.

Proof :- Let $n_1 = a^2 + b^2$ and $n_2 = c^2 + d^2$

Then $n_1 n_2 = (a^2 + b^2)(c^2 + d^2)$

$$= (ac + bd)^2 + (ad - bc)^2$$

and this proves Lemma 1

Lemma 2 :- Given any prime p of the type 4k + 1, ∃ natural numbers x & m such that

$$x^2 + 1 = mp \text{ where } 0 < m < p$$

Proof :- Since p is a prime of the type 4k + 1, −1 is a quadratic residue of p.

So ∃ a natural number x such that $x^2 \equiv -1 \pmod p$ W. L. O. G. we may assume $0 < x < p$. If $p/2 \; x < p$, we note $(p-x)^2 \equiv x^2 \equiv -1 \pmod p$ and $0 < p - x < p/2$. So W. L. O. G. we assume $0 < x < p/2$. Then ∃ an integer m such that $m > 0$

and $$mp = x^2 + 1 < 1 + \left(\frac{p}{2}\right)^2 < p^2, \quad \Rightarrow \quad m < p.$$

Proof of Theorem :- Let m be the least positive integer such that, $a^2 + b^2 = mp$ for some positive integer a & b.

By Lemma 2, such an m exists & $0 < m < p$. If m = 1,

Then p can be written as a sum of 2 squares. Now we can write n as

$$n = p_1 \, p_2 \ldots p_k \, m^2$$

where each p_i is a prime of the form 4k + 1 and m is a product of primes of the type 4k + 3. If each p_i can be written as a sum of 2 squares, then theorem follows from Lemma 1. So assume ∃ at least one prime p of the form 4k + 1, such that p can not be written as a sum of 2 squares.

Then ∃ integers m, x, y such that $x^2 + y^2 = mp$

We take $2 \le m < p$ and m is the least positive integer

Now $$mp = x^2 + y^2 \equiv 0 \pmod m$$

Take integers u & v such that

$$x \equiv u \pmod m, \; y \equiv v \pmod m \qquad \ldots(1)$$

and $$|u| \le m/2, \; |v| \le m/2$$

Then $$u^2 + v^2 = x^2 + y^2 \equiv 0 \pmod m \qquad \ldots(2)$$

Let $$mr = u^2 + v^2 \le \frac{m^2}{4} + \frac{m^2}{4} = \frac{m^2}{2} < m^2$$

Then $mr < m^2 \Rightarrow 0 \le r < m$

Let $r = 0$. Then $u^2 + v^2 = 0 \quad \Rightarrow \quad u = 0, v = 0$

Then $x \equiv u \equiv 0 \pmod m$

$y \equiv v \equiv 0 \pmod m$

$\Rightarrow$ $m \mid x, m \mid y$. Then $m^2 \mid x^2, m^2 \mid y^2$

$\Rightarrow$ $m^2 \mid (x^2 + y^2) \Rightarrow m^2 \mid mp \Rightarrow m \mid p.$

But $2 \le m < p$, so $m \mid p$ is not possible

$\Rightarrow$ $r \neq 0$

Now $mp = x^2 + y^2$ and $mr = u^2 + v^2$

$\Rightarrow$ $m^2 rp = (x^2 + y^2)(u^2 + v^2) = (xu + yv)^2 + (xv - yu)^2 \quad \ldots(3)$

Now $xu + yv \equiv u^2 + v^2 \equiv mr \equiv 0 \pmod m$

and $xv - yu \equiv uv - uv \equiv 0 \pmod m$.

$\Rightarrow$ $m \mid (xu + yv)$ and $m \mid (xv - yu)$

$\Rightarrow$ $\dfrac{xu + yv}{m}$ & $\dfrac{xv - yu}{m}$ are integers

Dividing on both sides by m^2 in (3) we get

$$rp = \left(\frac{xu + yv}{m}\right)^2 + \left(\frac{xv - yu}{m}\right)^2$$

i.e., rp can be written as a sum of 2 squares.

But $0 < r < m$ and this contradicts the minimality of m. So $2 \le m < p$ is not possible

$\Rightarrow$ $m = 1$.

i.e., every prime of the form $4k + 1$ can be written as a sum of 2 squares.

Remark :- Combining Theorem 1 with Theorem 2 we get that a natural number n can be written as a sum of 2 square iff all the primes of the type 4k + 3 occur to an even degree in the prime factorization of n.

Theorem 4.6 If a prime $p = x^2 + y^2$, then apart from changes of signs and interchange of x & y, this representation of p as sum of two squares is unique.

Proof :- If p = 2, then $2 = (\pm 1)^2 + (\pm 1)^2$ is the only representation of 2 as sum of two squares.

Let p be an odd prime. Since no number of the form 4k + 3 can be written as sum of 2 squares so $p \neq 3 \pmod 4$. So $p \equiv 1 \pmod 4$

Let $p = x^2 + y^2$ & $p = X^2 + Y^2$

Since p is of the form 4k + 1, −1 is a quadratic residue of p.

So $\exists$ an integer h such that $h^2 \equiv -1 \pmod p$

Now $p = x^2 + y^2 \Rightarrow x^2 + y^2 \equiv 0 \pmod p$

$\Rightarrow \quad x^2 \equiv -y^2 \pmod p$

Since $h^2 \equiv -1 \pmod p \Rightarrow x^2 \equiv h^2 y^2 \pmod p$

$\Rightarrow \quad x \equiv \pm hy \pmod p$

By changing the signs of y if necessary, we can assume

$x \equiv hy \pmod p$

Similarly we assume $X = hY \pmod p$

Now $p^2 = (x^2 + y^2)(X^2 + Y^2)$

$= (xX + yY)^2 + (xY - yX)^2 \qquad \ldots(1)$

Now $xY - yX \equiv hyY - yhY \equiv 0 \pmod p$

$\Rightarrow \quad p \mid (xY - yX)$. Then from (1), $p \mid (xX + yY)$

Dividing both sides of (1) by p^2, we get

$$1 = \left(\frac{xX + yY}{p}\right)^2 + \left(\frac{xY - yX}{p}\right)^2 \qquad \ldots(2)$$

The only representation of (2) as sum of two squares are

$$1 = (\pm 1)^2 + 0^2 = 0^2 + (\pm 1)^2$$

So from (2) either $xX + yY = 0$ …(3)

or $xY - yX = 0$ …(4)

Case I $xY - yX = 0$

$\Rightarrow$ $xY = yX$ …(5)

Now $p = x^2 + y^2 \Rightarrow \gcd(x, y) = 1$, and $p = X^2 + Y^2 \Rightarrow \gcd(X, Y) = 1$

From (5), $x \mid (yX)$, but $\gcd(x, y) = 1 \Rightarrow x \mid X$ …(6)

Again from (5), $X \mid (xY)$, but $\gcd(X, Y) = 1 \Rightarrow X \mid x$ …(7)

Using (6) and (7)

$$x = \pm X.$$

But $x^2 + y^2 = X^2 + Y^2 = p$

$\Rightarrow$ $y^2 = Y^2 \Rightarrow y = \pm Y$

So in this case theorem is true.

Case II $xX + yY = 0$

In this case, we check that

$$x = \pm Y \ \& \ y = \pm X.$$

$$xX = -yY$$

$\Rightarrow$ $x \mid -yY \Rightarrow x \mid Y$

and $Y \mid -xX \Rightarrow Y \mid -x$

$\Rightarrow$ $x = \pm Y$

Similarly $y = \pm X$.

Four Square Theorem

Theorem 4.7 Every natural number n can be written as a sum of four squares.

Proof :- If n = 1, then $1 = 1^2 + 0^2 + 0^2 + 0^2$

So let n > 1

Let $n = p_1^{\alpha 1} p_2^{\alpha 2} ... p_k^{\alpha k}$ …(1)

be the prime factorization of n.

If every prime p can be written as a sum of four squares then the above theorem will follow from (1), if we are able to prove

Lemma 1 :- Product of two numbers, which can be written as sum of 4 squares, is also repreentable as sum of 4 squares.

Proof :- Let

$$n_1 = a^2 + b^2 + c^2 + d^2$$

and $$n_2 = x^2 + y^2 + z^2 + u^2$$

The $$n_1 n_2 = (a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + u^2) = (ax + by + cz + du)^2$$

$$+ (bx - ay + cu - dz)^2 + (cx + dy - az - bu)^2$$

$$+ (dx - cy + bz - au)^2$$

Thus after Lemma 1, it is enough to prove

Lemma 2 :- If p is an odd prime then ∃ integers x, y, m such that

$$1 + x^2 + y^2 = mp \text{ where } 1 \le m < p.$$

Proof of Lemma 2:- Let

$$S = \left\{1 + x^2 ; x = 0,1,2,..., \frac{p-1}{2}\right\}$$

and $$T = \left\{-y^2, y = 01,2,..., \frac{p-1}{2}\right\}$$

Then each of S & T contains $\frac{p+1}{2}$ elements. First we claim that elements of S are mutually incongruent (mod p)

If possible, let

$$1 + x_1^2 \equiv 1 + x_2^2 \pmod{p}$$

where $0 \le x_1 < x_2 \le \frac{p-1}{2}$.

Then $x_2^2 - x_1^2 \equiv 0 \pmod{p}$

$\Rightarrow$ $p \mid (x_2^2 - x_1^2)$ $\Rightarrow$ $p \mid (x_2 + x_1)(x_2 - x_1)$

But $1 \le x_1 + x_2 \le (p-1)$

and $1 \le x_2 - x_1 \ge \frac{p-1}{2}$

$\Rightarrow$ $p \nmid (x_1 + x_2)$ and $p \nmid (x_2 - x_1)$

So p does not divide $x_2^2 - x_1^2$. So elements of S are mutually incongruent (mod p)

Similarly elements of T are mutually incongruent (mod p).

Now consider SUT. SUT contains (p+1) distinct elements. But there are only (p−1) residue classes (mod p). So two elements of SUT must be congruent to each other (mod p). Since elements of S as well as elements of T are mutually incongruent (mod p), so there must exist an element of S which is congruent to an element of T

i.e. $\exists$ integers x, y; $0 \le x \le \frac{p-1}{2}$, $0 \le y \le \frac{p-1}{2}$ such that

$$1 + x^2 \equiv -y^2 \pmod{p}$$

i.e. $1 + x^2 + y^2 \equiv 0 \pmod{p}$ i.e. there exists an integer m such that

$$1 + x^2 + y^2 = mp$$

Then $mp = 1 + x^2 + y^2 \le 1 + \left(\frac{p-1}{2}\right)^2 + \left(\frac{p-1}{2}\right)^2 < p^2$

$\Rightarrow$ $m < p$.

Proof of Theorem :- Every prime can be written as four squares.

If $p = 2$, then $2 = 1^2 + 1^2 + 0^2 + 0^2$ and we are through.

By Lemma 2, given any odd prime p, $\exists$ integers a, b, c, d, m such that $a^2 + b^2 + c^2 + d^2 = mp$ where $1 \le m < p$, for we can take a = 1, b = x; c = y, d = 0.

Let m be the smallest positive integers such that

$$a^2 + b^2 + c^2 + d^2 = mp \qquad \ldots(1)$$

Then $a^2 + b^2 + c^2 + d^2 \equiv 0 (\text{mod } m)$

Now choose x, y, z , u such that

$$x \equiv a (\text{mod } m)$$

$$y \equiv b (\text{mod } m)$$

$$z \equiv c (\text{mod } m)$$

$$u \equiv d (\text{mod } m)$$

where $-\frac{m}{2} \le x, y, z, u \le \frac{m}{2}$

Then $x^2 + y^2 + z^2 + u^2 \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 (\text{mod } m)$

This is $\exists$ an integer r such that

$$x^2 + y^2 + z^2 + u^2 = mr \qquad \ldots(2)$$

Now $mr = x^2 + y^2 + z^2 + u^2 \le \left(\frac{m}{2}\right)^2 + \left(\frac{m}{2}\right)^2 + \left(\frac{m}{2}\right)^2 + \left(\frac{m}{2}\right)^2$

$= m^2 \Rightarrow r \le m$

Let $r = 0$

$\Rightarrow$ $x^2 + y^2 + z^2 + u^2 = 0$

$\Rightarrow$ $x = y = z = u = 0$

Then $mp = a^2 + b^2 + c^2 + d^2 \equiv 0 \ (\text{mod } m^2)$, since m/a, m/b, m/c and m/d

$\Rightarrow$ $m^2 \mid mp \Rightarrow m \mid p$

$\Rightarrow$ either m = 1 or m = p

Now $m \ne p$, since $m < p$. If m = 1, then

$a^2 + b^2 + c^2 + d^2 = p$ and p is representable as a sum of 4 squares. So we assume $r \ne 0$

Then $1 \le r \le m$ and $1 < m < p$

Let $r = m$

Then $x^2 + y^2 + z^2 + u^2 = m^2$. …(3)

Since $-\frac{m}{2} < x, y, z, u \leq \frac{m}{2}$

(3) is possible only if $x = y = z = u = \frac{m}{2}$.

Then $a \equiv \frac{m}{2}, b \equiv \frac{m}{2}, c \equiv \frac{m}{2}, d \equiv \frac{m}{2} \pmod{m}$

$\Rightarrow$ $\exists$ integers a_1, a_2, a_3, a_4 such that

$$a = \frac{m}{2} + a_1 m,\ b = \frac{m}{2} + a_2 m,\ c = \frac{m}{2} + a_3 m,\ d = \frac{m}{2} + a_4 m$$

Now $mp = a^2 + b^2 + c^2 + d^2$

$$= \left(\frac{m}{2} + a_1 m\right)^2 + \left(\frac{m}{2} + a_2 m\right)^2 + \left(\frac{m}{2} + a_3 m\right)^2 + \left(\frac{m}{2} + a_4 m\right)^2$$

$$= \frac{m^2}{4} + a_1 m^2 + a_1^2 m^2 + \frac{m^2}{4} + a_2 m^2 + a_2^2 m^2$$

$$+ \frac{m^2}{4} + a_3 m^2 + a_3^2 m^2 + \frac{m^2}{4} + a_4 m^2 + a_4^2 m^2$$

$$= m^2 (1 + a_1 + a_2 + a_3 + a_4 + a_1^2 + a_2^2 + a_3^2 + a_4^2)$$

$$\equiv 0 \pmod{m^2}$$

$\Rightarrow$ $m^2 \mid mp \Rightarrow m \mid p$

which is not possible since $1 < m < p$.

Now multiplying (1) & (2) we get

$$m^2 rp = (a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + u^2)$$

$$= (ax + by + cz + du)^2 + (bx - ay + cu - dz)^2$$

$$+ (cx + dy - az - bu)^2$$

$$+ (dx - cy + bz - au)^2 \text{ (By Lemma 1)} \quad \ldots(4)$$

But $ax + by + cz + du \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m}$

$$bx - ay + cu - dz \equiv ba - ab + cd - dc \equiv 0 \pmod{m}$$

$$cx + dy - az - bu \equiv ca + db - ac - bd \equiv 0 \pmod{m}$$

$$dx - cy + bz - au \equiv da - cb + bc - ad \equiv 0 \pmod{m}$$

$\therefore$ Dividing (4) by m^2 we get

$$rp = \left(\frac{ax + by + cz + du}{m}\right)^2 + \left(\frac{bx - ay + cu - dz}{m}\right)^2$$

$$+ \left(\frac{cx + dy - az - bu}{m}\right)^2 + \left(\frac{dx - cy + bz - au}{m}\right)^2 \quad \ldots(5)$$

where the expression in the R.H.S. of (5) are integers.

So we can write rp as a sum of 4 squares.

But $1 < r < m$ and this contradicts the minimality of m.

So $m > 1$ is impossible

$\Rightarrow$ $m = 1$

Hence the theorem

(It is called Langranges theorem)

Waring Problem :- Waring problem is about the representation of a natural numbers as a sum of fixed number of squares or cubes, or 4-th powers and so on.

In 1970, Waring stated without proof that a natural number can be written as a sum of 4 squares, 9 cubes, 19 biquradratics & 37 5-th powers & on. In 1909, Hilbert proved that given any natural number n and $k \geq 2$, $\exists$ a fixed number $s(k) = s$(say) such that n can be written as sum of s k-th powers.

The Waring problem has been established for all $k \neq 5$

The numbers g(k) and G(k)

Connected with Waring problem we define natural nos g(k) & G(k) in the following way:

g(k) : is defined as the smallest nos such that every natural number can be written as the sum of g(k) k-th power.

G(k) : is defined to be as the smallest natural number such that every natural number (except a finite number) can be written as a sum of G(k) k-th powers.

Theorem 4.8 $g(2) = 4$

Proof ;- By Lagrange Theorem, $g(2) \leq 4$

Now the most economical representation of 4 as a sum of 4 squares is

$$4 = 1^2 + 1^2 + 1^2 + 1^2$$

$\Rightarrow$ $g(2) \geq 4 \Rightarrow g(2) = 4$

Hence the theorem

Theorem 4.9 $G(2) = 4$

Proof :- We know

$$G(2) \leq g(2) = 4 \qquad \ldots(I)$$

By definition G(k) is the smallest natural numbers except a finite number that can be written as a sum of G(k) k-th powers. So to prove G(2) = 4, it is enough to prove that an infinite number of natural numbers can not be written as a sum of 3 squares.

For this, we shall prove that no natural number of the form 8k + 7 can be written as a sum of 3 square.

Let $n = a^2 + b^2 + c^2 \qquad \ldots(II)$

Then we distinguish following cases

(a) All the natural numbers a, b, c, are even then

$$a^2 \equiv 0 \text{ or } 4 \pmod 8$$

$$b^2 \equiv 0 \text{ or } 4 \pmod 8$$

and $c^2 \equiv 0 \text{ or } 4 \pmod 8$

$\therefore$ $n = a^2 + b^2 + c^2 \equiv 0 \text{ or } 4 \pmod 8$

(b) Two of the numbers a, b, c are even and one is odd. To be specific let a & b be even and c be odd.

Then $a^2 \equiv 0 \text{ or } 4 \pmod 8$

$$b^2 \equiv 0 \text{ or } 4 \pmod 8$$

$$c^2 \equiv 1 \pmod 8$$

$\therefore$ $n = a^2 + b^2 + c^2 \equiv 1 \text{ or } 5 \pmod 8$

(c) Two of a, b, c are odd and third is even

Let ‘a’ be even and b, c be odd.

then $a^2 \equiv 0 \text{ or } 4 \pmod 8$, $b^2 \equiv 1 \equiv c^2 \pmod 8$

$\therefore\ n \equiv a^2 + b^2 + c^2 \equiv 2 \text{ or } 6 (\text{mod } 8)$

(d) All of a, b, c are odd

then $a^2 \equiv b^2 \equiv c^2 = 1 (\text{mod } 8)$

$\therefore$ $n = a^2 + b^2 + c^2 \equiv 3 (\text{mod } 8)$

Therefore, for no choice of a, b, c

$n \equiv 7 (\text{mod } 8)$

$\therefore$ No number of the form 8k + 7 can be written as a sum of 3 square

$\Rightarrow$ $G(2) > 3$ …(III)

$\Rightarrow$ $G(2) \geq 4$

From (1) & (III) we get G(2) =4

Remarks:- It is clear from the proof that

if $n \equiv 0 (\text{mod } 4)$ and

$n \equiv a^2 + b^2 + c^2$, then a, b, c must be all even.

Example :- Prove that no number of the form $4^m (8k + 7)$; $(m \geq 0)$, $(k \geq 0)$ can be written as a sum of 3-squares.

Proof:- First we prove, no number of form 8k +7 can be written as a sum of 3 squares.

We shall prove the result by induction on m.

If m = 0, then $n = 4^m (8k + 7) = 8k + 7$ and we have proved that no number of the form 8k+7 can be written as a sum of 3- squares. So assume that no number of the form $4^{m-1} (8k + 7)$ $(m \geq 1)$ can be written as a sum of 3 squares

Now let $n = 4^m (8k + 7)$ when $m \geq 1$

Then $n \equiv 0 (\text{mod } 4)$

If possible, let $\exists$ numbers a, b, c such that $n = a^2 + b^2 + c^2$ then by the remark made earlier a, b, c, must be all even.

Therefore $$\frac{n}{4} = \frac{a^2}{4} + \frac{b^2}{4} + \frac{c^2}{4}$$

$$= \left(\frac{a}{2}\right)^2 + \left(\frac{b}{2}\right)^2 + \left(\frac{c}{2}\right)^2$$

i.e. $\frac{n}{4}$ can also be written as a sum of 3-squares.

But $$\frac{n}{4} = 4^{m-1}(8k + 7)$$

and this contradicts the assumption that no number of the form $4^{m-1}(8k + 7)$ can be written as a sum of 3-squares which proves the exercise.

Lower bounds for g(k) and G(k)

Theorem 4.10 $g(k) \geq \left[\left(\frac{3}{2}\right)^k\right] + 2^k - 2$

Proof :- Let $q = \left[\left(\frac{3}{2}\right)^k\right]$.

Let $N = 2^k q - 1$, then by definition, $N < 3^k$.

So if we want to represent N as a sum of kth powers, the 3^k cannot occur in this representation. Further $N < 2^k q$. So for the most economical representation of N as a sum of kth powers we must take $q-1$ powers of 2^k in its representation.

$\therefore$ $$N = 2^k q - 1 = 2^k q - 1 + 2^k - 2^k$$

$$= 2^k(q-1) + 2^k - 1$$

$$= (q-1)\, 2^k + (2^k - 1).\, 1^k$$

Thus we need exactly $q - 1 + 2^k - 1 = q + 2^k - 2$ kth powers to represent N as a sum of k-th powers in the most economical representation.

$\therefore$ $$g(k) \geq q + 2^k - 2 = \left[\left(\frac{3}{2}\right)^k\right] + 2^k - 2$$

Theorem 4.11 $G(k) \geq k + 1$

Proof :- To prove the theorem we first prove a lemma.

Lemma :- For every integer $k \geq 1$ and $r \geq 1$

$$\sum_{a=0}^{b} \frac{(a+1)(a+2)...(a+r-1)}{\lfloor r-1} = \frac{(b+1)(b+2)...(b+r)}{\lfloor r} \qquad ...(1)$$

Proof :- We shall prove the lemma by induction on b. However first we note that ($\lfloor n$) divides the product of n consecutive integers. So fractions appearing on both sides of (1) are integers.

Take b = 1, then L.H.S. of (1) for b = 1, is equal to

$$\frac{\lfloor r-1 + \lfloor r}{\lfloor r-1} = \frac{\lfloor r-1}{\lfloor r-1} + \frac{\lfloor r}{\lfloor r-1} = 1 + r = \frac{\lfloor r+1}{\lfloor r}$$

So assume that (1) holds for (b–1), where $b \geq 2$ and we shall prove its for b. Now L.H.S. of (1) is equal to

$$\sum_{a=0}^{b} \frac{(a+1)(a+2)...(a+r-1)}{\lfloor r-1}$$

$$=$$

$$\sum_{a=0}^{b-1} \frac{(a+1)(a+2)...(a+r-1)}{\lfloor r-1} + \frac{(b+1)(b+2)...(b+r-1)}{\lfloor r-1}$$

$$= \frac{b(b+1)...(b+r-1)}{\lfloor r} + \frac{(b+1)(b+2)...(b+r-1)}{\lfloor r-1}$$

$$= \frac{(b+1)(b+2)...(b+r-1)(b+r)}{\lfloor r} = \text{R.H.S. of (1)}$$

Thus lemma is true for b.

So by induction principle, lemma is true for every $b \geq 1$.

Proof of theorem :- For any given natural number N, let A(N) be the number of those natural numbers n such that $0 \leq n \leq N$ and n can be written as sum of k k-th powers i.e. A(N) is the number of natural numbers n such that

$$n = x_1^k + ... + x_k^k \text{ and } 0 \leq n \leq N \qquad ...(1)$$

is solvable

By interchanging $x_1, x_2, ..., x_k$ if necessary, we assume $0 \leq x_1 \leq x_2 \leq ... \leq x_k$ and $x_k \leq N^{1/k}$ ...(2)

Since $n \leq N$, then to every solution of (1), we must have a solution of (2), so that

$$A(N) \le B(N) \qquad \ldots(3)$$

where B(N) is the number of solutions of (2). Now, we have

$$B(N) = \sum_{x_k=0}^{\left[N^{1/k}\right]} \sum_{x_{k-1}=0}^{x_k} \ldots \sum_{x_3=0}^{x_4} \sum_{x_2=0}^{x_3} \sum_{x_1=0}^{x_2} 1$$

$$= \sum_{x_k=0}^{\left[N^{1/k}\right]} \sum_{x_{k-1}=0}^{x_k} \ldots \sum_{x_3=0}^{x_4} \sum_{x_2=0}^{x_3} (x_2+1)$$

Now applying the above lemma with $a = x_2$, $b = x_3$ and $r = 2$,

$$B(N) = \sum_{x_k=0}^{\left[N^{1/k}\right]} \sum_{x_{k-1}=0}^{x_k} \ldots \sum_{x_3=0}^{x_4} \frac{(x_3+1)(x_3+2)}{\underline{|2}}$$

Again, applying the Lemma with $a = x_3$, $b = x_4$, $r = 3$ and then continuing like this we obtain

$$B(N) = \sum_{x_k=0}^{\left[N^{1/k}\right]} \frac{(x_k+1)(x_k+2)\ldots(x_k+k-1)}{\underline{|k-1}}$$

$$= \frac{\left([N^{1/k}]+1\right)\left([N^{1/k}]+2\right)\ldots\left([N^{1/k}]+k\right)}{\underline{|k}} \qquad \ldots(4)$$

Now, if possible, let $G(k) \le k$, so that all but a finite number can be written as a sum of k kth powers, so there exists a finite number C such that

$$A(N) \ge N - C$$

But we have

$$A(N) \le B(N)$$

Combining, we have

$$A - C \le A(N) \le B(N) \qquad \ldots(5)$$

Now we know that

$$N^{1/k} - 1 \le [N^{1lk}] \le N^{1/k}$$

So that, we have from (4),

$$\frac{N^{1/k}(N^{1/k}+1)...(N^{1/k}+k-1)}{\lfloor k} \leq B(N) \leq \frac{(N^{1/k}+1)(N^{1/k}+2)...(N^{1/k}+k)}{\lfloor k} \qquad (6)$$

Then, we observe that for large N, L.H.S and R.H.S. of (6) tend to $N/\lfloor k$. Hence for large N, $B(N) \sim N/\lfloor k$. Thus it follows that from (5), we have for sufficiently large N,

$N \leq N/\lfloor k$, a contradiction for $k \geq 2$.

Thus, our assumption that $G(l) \leq k$ is not possible and hence, we must have :

$G(k) \geq k + 1$.

Theorem 4.12 Prove that,

$G(2^{\theta}) \geq 2^{\theta+2}$ for $\theta \geq 2$

Proof :- Firstly, let $\theta = 2$, then we have to show that

$G(4) \geq 16$

Let x be any integer, then

$x^4 \equiv 0$ or $1 (\text{mod } 16)$ …(1)

Thus, if we consider the numbers of the form 16m + 15, then any such number require at least 15 biquadrates. It follows that,

$G(4) \geq 15$

From (1), it follows that if 16n is the sum of 15 or fewer biquadrates, then each biquadrate must be a multiple of 16. Hence, we can write :

$$16n = \sum_{i=1}^{15} x_i^{\,4} = \sum_{i=1}^{15} (2y_i)^4$$

so that

$$n = \sum_{i=1}^{15} y_i^{\,4}$$

Hence, if 16n is the sum of 15 or fewer biquadrates, so is n. But, we observe that 31 is not the sum of 15 or fewer biquadrates. In fact the most economical representation contains 16 biquadrates given by, $31 = 2^4 + 15.1^4$.

So we must have

$$G(4) \geq 16$$

Now, let $\theta > 2$, then we have $k = 2^{\theta} > \theta + 2$

If x is even, then $x^{2^{\theta}} = (2y)^{2^{\theta}} = 2^{2^{\theta}} y^{2^{\theta}}$

Since, $\theta + 2 < 2^{\theta}$, so $2^{\theta+2} \mid 2^{2^{\theta}}$

So that we must have

$$x^{2^{\theta}} \equiv 0 \pmod{2^{\theta+2}}.$$

If x is odd, then $x^{2^{\theta}} = (2m+1)^{2^{\theta}}$

$$\Rightarrow \quad x^{2^{\theta}} = (1+2m)^{2^{\theta}} \equiv 1 + 2^{\theta+1} m + 2^{\theta+1} (2^{\theta} - 1) m^2$$

$$\equiv 1 + 2^{\theta+1} m + 2^{2\theta+1} m^2 - 2^{\theta+1} m^2$$

$$\equiv 1 + 2^{\theta+1} m - 2^{\theta+1} m^2$$

$$\equiv 1 - 2^{\theta+1} m(m-1) \equiv 1 \pmod{2^{\theta+2}}$$

Thus, we have obtained that,

$$x^{2^{\theta}} \equiv 0 \text{ or } 1 \pmod{2^{\theta+2}} \qquad \ldots(2)$$

Now, let n be any odd number and suppose that $2^{\theta+2}$ n is written as a sum of $2^{\theta+1} - 1$ or fewer k th powers where k = 2

$$2^{\theta+2}. N = x_i^k + x_2^k + \ldots + x_{2^{\theta+2}-1}^k.$$

then from (2), we get that each x_i must be even and hence divisible by 2^k. Hence, we obtain that $2^{k-\theta-2} \mid n$ which implies that n is even, a contradiction.

Hence, we must have

$$G(2^{\theta}) \geq 2^{\theta+2} \text{ for } \theta \geq 2.$$

This completes the proof

Theorem 4.13 Let p be a prime such that p > 2 (i.e. p is an odd prime), then

$$G[p^{\theta} (p-1)] \geq p^{\theta+1}$$

Proof :- Let $k = p^{\theta}(p-1)$.

Since p > 2, so we have $\theta + 1 \leq 3^{\theta} < k$

Hence, if $p \mid x$, then we have

$$x^k \equiv 0(\text{mod } p^{\theta+1})$$

and if $p \nmid x$, then we have

$$x^k = x^{p^\theta(p-1)} \equiv 1 \ (\text{mod } p^{\theta+1})$$

[Using the fact that $\phi(p^{\theta+1}) = p^\theta(p-1)$ and applying Euler's theorem]

Thus we obtain that

$$x^k \equiv 0 \text{ or } 1(\text{mod } p^{\theta+1})$$

Let n be a natural number such that (p, n) = 1 and suppose that $p^{\theta+1}.n$ is the sum of $p^{\theta+1}-1$ or fewer kth powers i.e.

$$p^{\theta+1}.n = x_1^{\,k} + x_2^{\,k} + \ldots + x^k_{p^{\theta+1}-1}$$

then each x_i must be divisible by p and hence each factor on R.H.S. must be divisible by p^k which implies that

$$p^k \mid p^{\theta+1}.n,$$

a contradiction, since $k > \theta + 1$ and (p, n) = 1

Hence, we must have

$$G(k) \geq p^{\theta+1}$$

i.e. $G(p^\theta(p-1)) \geq p^{\theta+1}$

This completes the proof.

Theorem 4.14 Let p be a prime such that $p > 2$ and $\theta \geq 0$ then

$$G\left\{\frac{1}{2}p^\theta(p-1)\right\} \geq \frac{1}{2}(p^{\theta+1}-1)$$

Proof :- Let

$$k = \frac{1}{2}p^\theta(p-1)$$

then we have $\theta + 1 < p^\theta \leq \frac{1}{2}p^\theta(p-1) = k$ (except in the trivial case, p = 3, θ = 0 and k = 1)

Hence we must have if p/x, then $x^k \equiv 0 \ (\text{mod } p^{\theta+1})$

and if $p \nmid x$, then we have

$$x^{2k} \equiv x^{p^\theta(p-1)} \equiv 1 \ (\text{mod } p^{\theta+1}) \quad \text{(By Euler's theorem)}$$

Hence, $p^{\theta+1} \mid (x^{2k}-1)$

$\Rightarrow$ $p^{\theta+1} \mid (x^k+1)(x^k-1)$.

Since $p > 2$, so p can not divide both x^k+1 and x^k-1 and so one of x^k-1 and x^k+1 is divisible by $p^{\theta+1}$. Thus, we have :

$$x^k \equiv 0, 1 \text{ or } -1 (\text{mod } p^{\theta+1})$$

If follows that number of the form $p^{\theta+1}m \pm \frac{1}{2}(p^{\theta+1}-1)$, requires at least $\frac{1}{2}(p^{\theta+1}-1)$ k th powers

$\Rightarrow$ $G(k) \geq \frac{1}{2}(p^{\theta+1}-1)$ and the proof is completed.

Theorem 4.15 If $\theta \geq 2$, the n,

$$G(3.2^{\theta}) \geq 2^{\theta+2}$$

Proof :- We have that, $G(3.2^{\theta}) \geq G(2^{\theta})$

$$\geq 2^{\theta+2} \text{ (proved earlier)}$$

This completes the proof.

Algebraic Number and integers

Definition :- (Rational Integers)

The numbers …, −3, −2, −1, 0, 1, 2, 3,… are called the "rational integers" or simply the "integers". The set of rational integers {…, −3, −2, −1, 0, 1, 2, 3,…} is denoted by Q(1).

Definition :- An algebraic number is a number x which satisfies an algebraic equation, i.e. an equation

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_n = 0,\ a_n \neq 0, \text{ where } a_0, a_1, \ldots, \text{ are integers}$$

If $x = \frac{a}{b}$, then $bx - a = 0$, so that any rational x is algebraic. Any quadratic surd is algebraic; thus $i = \sqrt{-1}$ is algebraic.

Definition :- If $a_0 = 1$ in the above definition, then x is called an algebraic integer .

Definition (Gaussian Integers)

Gaussian integer (or complex integer) is the number of the form, $\xi = a + bi$, where a and b are rational integers. The set of Gaussian integers, namely

$$\{a + bi : a, b \text{ are rational integers}\}$$

is denoted by Q(i) and Gaussian integers are also called as integers of Q(i)

Definition :- (Divisibility in Q(i))

An Gaussian integer ξ is said to be divisible by an Gaussian integer $\eta(\neq 0)$ if there exists an Gaussian integer σ such that $\xi = \eta\,\sigma$. Then, we say that η is a divisor of ξ and write $\eta \mid \xi$.

Remark :- 1. Any Gaussian integer ξ has eight trivial divisors namely, 1, –1, i, –i, ξ, –ξ, iξ and –iξ.

2. Basic properties of divisibility are satisfied in k(i), such as

$$\alpha \mid \beta, \beta \mid \gamma \Rightarrow \alpha \mid \gamma$$

$\alpha \mid \gamma_1, \alpha \mid \gamma_2, \ldots, \alpha \mid \gamma_n \Rightarrow \alpha \mid (\beta_1\gamma_1 + \beta_2\gamma_2 + \ldots + \beta_n\gamma_n)$ for all Gaussian integers.

Definition :- (Unity)

The integer $\in$ in Q(i) is said to be unity of Q(i) if $\in \mid \xi$ for every ξ of Q(i)

Alternatively, we may define a unity of Q(i) as any Gaussian integer which is a divisor of 1. The two definitions are equivalent, since 1 is a divisor of every Gaussian integer and $\in \mid 1$, $1 \mid \xi \Rightarrow \in \mid \xi$.

Definition (Norm of an Gaussian integer)

Let $\xi = a + ib$ is an Gaussian integer. The norm of ξ is defined as :

$$N(\xi) = N(a + ib) = a^2 + b^2$$

Remark :- It can be easily verified that $N(\xi)\,N(\eta) = N(\xi\eta)$ for all Gaussian integers ξ and η.

Theorem 4.16 In Q(i), the norm of a unity is 1 and any integer whose norm is 1 is a unity.

Proof :- If $\in$ is a unity, then, by definition, $\in \mid 1$

$\Rightarrow$ there exists an Gaussian integer η such that

$$1 = \in\eta$$

$$\Rightarrow \quad N(1) = N(\in\eta) = N(\in)\,N(\eta)$$

$$\Rightarrow \quad 1 = N(\in)\,N(\eta) \Rightarrow N(\in) \mid 1 \Rightarrow N(\in) = 1$$

On the other hand,

Let $N(a + ib) = 1$

$$\Rightarrow \quad a^2 + b^2 = 1 \Rightarrow (a + ib)\,(a - ib) = 1$$

$\Rightarrow$ $(a + ib) \mid 1$

$\Rightarrow$ $a + ib$ is a unity and proof is completed.

Theorem 4.17 The unities of Q(i) are $\in = i^s$ where S = 0, 1, 2, 3 or

Show that ± 1 and $\pm i$ are the only unities of Q(i).

Proof :- Let $\in = a + ib$ be a unity of Q(i), then by above theorem,

$$N(\in) = a^2 + b^2 = 1$$

But the only solutions of $a^2 + b^2 = 1$ are

$$a = \pm 1, b = 0 \text{ and } a = 0, b = \pm 1$$

So that, only choices of $\in$ are $1, -1, i, -i$

Hence the unities of Q(i) are of the form i^s (s = 0, 1, 2, 3)

Definition (Associate)

Let ξ be any Gaussian integer and $\in$ be unity of Q(i), then $\in\xi$ is said to be associate of ξ, or we say that $\in\xi$ is associated with ξ.

Remark :- (I) By above theorem, it is clear that the associates of ξ are ξ, $i\xi$, $-\xi$, $-i\xi$.

(II) The associates of 1 are the unities.

Definition (Primes in Q(i))

An integer in Q(i), neither zero nor unity, is said to be a prime in Q(i) if it is divisible only by associates of itself or by associates of I i.e. if π is a prime in Q(i), then it has no divisors except the eight trivial divisors $1, -1, i, -i, \pi, i\pi, -i\pi, -\pi$.

Theorem 4.18 A Gaussian integer whose norm is a rational prime (2, 3, 5, 7, 11…) is a prime in Q(i).

Proof :- Let ξ be any Gaussian integer such that

$N(\xi) = p$ where p is any rational prime. We have to show that ξ is a prime in Q(i).

Let $\xi = \eta\sigma$ where $\eta, \sigma \in$ Q(i) then $N(\eta\sigma) = N(\xi) = p$

$\Rightarrow$ $N(\eta)\, N(\sigma) = p$

But p is a prime so either $N(\eta) = 1$ or $N(\eta) = 1$. Hence either η or σ is a unity and therefore ξ is a prime in Q(i).

Remark :- Converse of above theorem is not true i.e. norm of a prime of Q(i) may not be a rational prime. For example, $3 = 3 + 0i, \in k(i)$ such that $N(3) = 9$ i.e. Norm of 3 is not a rational prime, but we show that 3 is a prime of Q(i)

Let $3 = (a + bi)(c + id)$

$$\Rightarrow \qquad N(3) = N(a + bi)\, N(c + id)$$

$$\Rightarrow \qquad 9 = (a^2 + b^2)(c^2 + d^2)$$

But, it is impossible that, $a^2 + b^2 = c^2 + d^2 = 3$ (since 31 is not the sum of two squares) and hence either $a^2 + b^2 = 1$ or $c^2 + d^2 = 1$ i.e. either $a + ib$ or $c + id$ is a unity. It follows that 3 is a prime of Q(i).

Theorem 4.19 Any Gaussian integer, neither zero nor unity, is divisible by a prime of Q(i)

Proof :- Let ξ be any Gaussian integer which is not equal to zero or unity. If ξ is a prime in Q(i), we have nothing to prove.

Let ξ be not a prime, then we must have $\xi = \alpha_1\beta_1$ for some $\alpha_1\ \beta_1 \in$ Q(i) such that, $N(\alpha_1) > 1$ and $N(\beta_1) > 1$ and so we have

$$1 < N(\alpha_1) < N(\xi) \qquad \ldots(I)$$

If α_1 (or β_1) is a prime, the proof is completed. If α_1 is not a prime, then

$\alpha_1 = \alpha_2\, \beta_2$ for some $\alpha_2, \beta_2 \in$ Q(i) such that,

$N(\alpha_2) > 1$ an $N(\beta_2) > 1$

then we have

$$1 < N(\alpha_2) < N(\alpha_1) \qquad \ldots(II)$$

Combining (1) and (II), we obtain

$$1 < N(\alpha_2) < N(\alpha_1) < N(\xi).$$

We may continue this process as long as α_r is not a prime. Since, $N(\xi) > N(\alpha_1) > N(\alpha_2)\ldots$ is a decreasing sequence of positive rational integers, we must come to a prime α_r and then we have

$$\xi = \alpha_1\, \beta_1 = \alpha_2\, \beta_2\, \beta_1 = \ldots = \alpha_r\, \beta_r \ldots \beta_1$$

Thus, α_r is a divisors of ξ and α_r is a prime in Q(i).

Theorem 4.20 Any Gaussian integer, neither zero nor unity, can be written as product of finite number of primes of Q(i)

Proof :- Let ξ be any Gaussian integer, not equal to zero or unity. If ξ itself is a prime, then the result is true.

We shall prove the result by induction on norm. We assume that result is true for all Gaussian integers (neither zero nor unity) with norm < $N(\xi)$.

Now, if ξ is not a prime, then, by last theorem, there exists a prime π such that $\pi \mid \xi$

or $\xi = \pi\alpha$ for some $\alpha \in Q(i)$ …(1)

and we have $N(\alpha) < N(\xi)$

Now if $N(\alpha) = 1$, then α is a unity and hence ξ is an associate of a prime π and hence, itself, is a prime, a contradiction. So $N(\alpha) > 1$, i.e. we have obtained $N(\alpha) < N(\xi)$ and α is neither zero nor unity. So by induction hypothesis, α can be written as a, product of primes of Q(i), say $\pi_1, \pi_2, \ldots, \pi_r$.

i.e. $\alpha = \pi_1 \pi_2 \ldots \pi_r$

Hence, from (1), we obtain

$\xi = \pi \pi_1 \pi_2 \ldots \pi_r$ where $\pi, \pi_1, \pi_2, \ldots, \pi_r$ are primes of Q(i)

Theorem 4.21 Given any two integers γ, γ_1 ($\gamma_1 \neq 0$) of Q(i), there exists integers ρ and γ_2 such that

$\gamma = \rho\gamma_1 \gamma_2$ where $N(\gamma_2) < N(\gamma_1)$

Proof :- Since $\gamma_1 \neq 0$, we have :

$\frac{\gamma}{\gamma_1} = R + Si$ where R and S are real (in fact R and S are rational). Then, we can find two rational integers x and y such that

$$|R - x| \leq \frac{1}{2} \text{ and } |S - y| \leq \frac{1}{2}$$

and then we have

$$\left| \frac{\gamma}{\gamma_1} - (x + iy) \right| = |R + iS) - x + iy|$$

$$= |(R - x) + i(S - y)| = [(R-x)^2 + (S-y)^2]^{1/2} \leq \frac{1}{\sqrt{2}}$$

Now, if we take

$\rho = x + iy$ and $\gamma_2 = \gamma - \rho\gamma_1$

Thus, we have

$$|\gamma - \rho\gamma_1| = |\gamma_1| \left| \frac{\gamma}{\gamma_1} - \rho \right| \leq \frac{1}{\sqrt{2}} |\gamma_1|$$

This implies that

$$N(\gamma_2) = N(\gamma - \rho\gamma_1) = |\gamma - \rho\gamma_1|^2 \leq \frac{1}{2}|\gamma_1|^2 = \frac{1}{2}N(\gamma_1) < N(\gamma_1)$$

Thus, we have obtained that

$$\gamma = \rho\gamma_1 + (\gamma - \rho\gamma_1)$$

$$= \rho\,\gamma_1 + \gamma_2 \text{ where } N(\gamma_2) < N(\gamma_1)$$

Remark :- (I) The above theorem is known as "Division Algorithm in Q(i)".

(II) Like the rational integers, the following result holds in Q(i).

"Let β and γ be Gaussian integers and π be prime of Q(i) such that $\pi \mid \beta\gamma$, then $\pi \mid \beta$ or $\pi \mid \gamma$.

The Fundamental Theorem of Arithmetic in Q(i)

Theorem 4.22 Every Gaussian integer (neither zero nor unity) is expressible as a product of finite numbers of primes of Q(i). This representation is unique apart from the order of the primes, the presence of unities and ambiguities between associated primes.

Proof :- Let ξ be any Gaussian integer, then ξ can be expressed as product of finite number of primes of Q(i).

Let $\xi = \pi_1\,\pi_2 \ldots \pi_r = \gamma_1\,\gamma_2 \ldots \gamma_s$ …(1)

be two representations of ξ where $\pi_1, \pi_2 \ldots, \pi r, \gamma_1, \gamma_2, \ldots, \gamma_s$ are all primes of Q(i).

Now, by (1), we have

$$\pi_1 \mid \gamma_1\,\gamma_2 \ldots \gamma_s$$

Since π_1 is a prime element of Q(i), so π, must divide some γ_i $(1 \leq i \leq s)$. Since γ_i is also a prime of Q(i), so we can say that π_1 and γ_1 are associates of each other

$\therefore \quad \gamma_i = \in_1 \pi_1$ for some unity $\in_1 \in$ Q(i)

Thus, (1) becomes :

$$\pi_1\,\pi_2 \ldots \pi_r = \gamma_1\,\gamma_2 \ldots \gamma_{i-1}\,(\in_1 \pi_1)\,\gamma_{i+1} \ldots \gamma_s$$

which implies that

$$\pi_1 (\pi_2 \ldots \pi_r - \gamma_1 \gamma_2 \ldots \gamma_{i-1} \in_1 \gamma_{i+1} \ldots \gamma_s) = 0$$

But π_1 is a prime, so $\pi_1 \neq 0$

$\Rightarrow$ $\pi_2 \ldots \pi_r = \in_1 \gamma_1 \gamma_2 \ldots \gamma_{i-1} \gamma_{i+1} \ldots \gamma_s$

Let, if possible, $r < s$, then continuing like above r times, we get :

$$1 = \in_1 \in_2 .. \in_r \gamma_{j1} \gamma_{j2} \ldots \gamma_{ji}$$

Since γ_{ji} is a prime and we get $\gamma_{ji} \mid 1$ which is a contradiction. Thus our supposition $r < s$ is wrong. Thus $r \not< s$. Similarly, we can prove that $s \not< r$. So we have $r = s$

By the process, we adopted, it also follows that π_i is associate of some γ_j and conversely.

Integers and fundamental Theorem in Q(w) where $w^3 = 1$.

Definition :-

The number of the form

$\xi = a + bw$ where a and b are rational integers and w is given by

$$w = e^{\frac{2}{3}\pi i} = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = \frac{-1+\sqrt{3}i}{2}$$

are called integers of Q(w).

Remark :- (1) If $w = e^{\frac{2}{3}\pi i} = \cos 2\pi/3 + i \sin 2\pi/3$

$$= \frac{-1+\sqrt{3}i}{2}$$

then, we have

$$w^2 = \frac{-1-\sqrt{3}i}{2}$$

(II) $w + w^2 = -1$ and $ww^2 = 1$

i.e. $1 + w + w^2 = 0$ and $w^3 = 1$

Definition :- (Norm in Q(w)).

Let $\xi = a + bw$ be any integer in Q(w), then norm of ξ is defined as :

$$N(\xi) = (a + bw)(a + bw^2) = a^2 - ab + b^2$$

Note (1) we have $N(\xi) = a^2 - ab + b^2 = \left(a - \frac{b}{2}\right)^2 + \frac{3}{4}b^2$

$\Rightarrow$ $N(\xi) = 0$ for $\xi = 0$ and $N(\xi) > 0$ otherwise

(II) We have :

$$N(a + bw) = a^2 - ab + b^2 = |a + bw|^2$$

(III) It can be easily verified that

$$N(\alpha\beta) = N(\alpha)\, N(\beta)$$

For all $\alpha, \beta \in Q(w)$.

Remark :- Definitions of divisor, unity, associate and prime in Q(w) are same as those in k(i).

Theorem 4.23 The unities of Q(w) are given by $\pm 1, \pm w, \pm w^2$

Proof :- Let a + bw be any unity of Q(w), hen

$$N(a + bw) = 1$$

$$\Rightarrow \quad a^2 - ab + b^2 = 1$$

$$\Rightarrow \quad (2a - b)^2 + 3b^2 = 4$$

The only solutions of this equation are

$$a = \pm 1,\ b = 0;\ a = 0,\ b = \pm 1;\ a = 1,\ b = 1;\ a = -1,\ b = -1$$

so that the unities are

$$\pm 1, \pm w, \pm(1 + w)$$

or $\pm 1, \pm w, \pm w^2$

Theorem 4.24 (1) The norm of a unity in Q(w) is 1 and any integer of Q(w) whose norm is 1 is unity.

(2) An integer whose norm is a rational prime is a prime in Q(w).

(3) Any integer in Q(w), not zero or a unity s divisible by a prime of Q(w).

(4) Any integer in Q(w), not zero or a unity, is a product of primes in Q(w).

Proof :- The proofs of these theorems are same as those given in the case of k(i), except for the difference in the form of the norm.

Remark :- Consider $1 - w \in Q(w)$

then by definition of norm, $N(1 - w) = 3$

So by theorem (2) given above, 1−w is a prime of Q(w)

2. Converse of theorem (2) may not be true i.e. norm of a prime of Q(w) may not be rational prime. For example, consider $2 = 2 + 0.w \in Q(w)$ then $N(2) = 3$ which is not a rational prime.

But, we show that 2 is a prime of Q(w)

Let $2 = (a + bw)(c + dw)$

$\Rightarrow$ $N(a + bw).\ N(c + dw) = 4$

Let, if possible

$$N(a + bw) = \pm 2$$

$\Rightarrow$ $a^2 - ab + b^2 = \pm 2 \Rightarrow (2a - b)^2 + 3b^2 = \pm 8$

which is impossible i.e $N(a + bw) \neq \pm 2$

Similarly $N(c + dw) \neq \pm 2$

Hence one of these must be 1 and other is 4 i.e. one of $(a + bw)$ and $(c + dw)$ is unity and hence 2 is a prime of Q(w).

Theorem 4.25 Given any two integers γ, γ_1 of Q(w) and $\gamma_1 \neq 0$, there exists two integers K and γ_2 in Q(w) such that

$$\gamma = K\gamma_1 + \gamma_2 \text{ where } N(\gamma_2) < N(\gamma_1)$$

(This is known as Division Algorith in Q(w))

Proof :- Let $\gamma = a + bw$ and $\gamma_1 = c + dw$ then consider,

$$\frac{\gamma}{\gamma_1} = \frac{a + bw}{c + dw} = \frac{(a + bw)(c + dw^2)}{(c + dw)(c + dw^2)}$$

$$= \frac{ac + bd - ad + (bc - ad)w}{c^2 - cd + d^2} = R + Sw \ (s \ \& \ y)$$

where, $R = \dfrac{ac + bd - ad}{c^2 - cd + d^2}$ and $S = \dfrac{bc - ad}{c^2 - cd + d^2}$

$\Rightarrow$ R and S are rational numbers.

We can find two rational integers x and y such that

$$|R - x| \leq \tfrac{1}{2} \text{ and } |S - y| \leq \tfrac{1}{2}$$

and then, we have

$$\left|\frac{\gamma}{\gamma_1} - (x + yw)\right|^2 = |(R-x) + (S-y)w|^2$$

$$= N[(R-x) + (s-y)\, w]$$

$$= (R-x)^2 - (R-x)\,(S-y) + (S-y)^2 \leq \frac{3}{4}$$

Hence, if we take

$$K = x + yw \text{ and } \gamma_2 = \gamma - K\,\gamma_1$$

then we obtain

$$\gamma = K\gamma_1 + \gamma_2$$

where $N(\gamma_2) = N\,(\gamma - K\,\gamma_1) \leq \frac{3}{4}\, N(\gamma_1) < N(\gamma_1)$

This completes the proof.

Fundamental Theorem of arithmetic in Q(w) :- The integer of Q(w) can be expressed as a product of primes of Q(w) and this expression is unique apart from the order of the primes, the presence of unities and ambiguities between associated primes.

Proof :- Same as given in the case of k(i)

Theorem 4.26 Show that $\lambda = 1-w$ is a prime and 3 is associated with λ^2

Proof :- It has been already proved (in a remark) that $\lambda = 1-w$ is a prime of Q(w).

Now $\lambda^2 = (1-w)^2 = 1-2w + w^2$

$$= 1-2w + (-1 -w)$$

$$= -3w$$

Hence 3 is associated with λ^2.

Algebraic fields

An algebraic field is the aggregate of al numbers

$$R(\vartheta) = \frac{P(\vartheta)}{P\,(\vartheta)},$$

Where ϑ is a given algebraic number, $P(\vartheta)$ and $P'(\vartheta)$ are polynomials in ϑ with rational coefficients, and $P'(\vartheta) \neq 0$. We denote this field by $Q(\vartheta)$. It is plain that sums and products of numbers of $Q(\vartheta)$ belong to $Q(\vartheta)$ and that α/β belongs to $Q(\vartheta)$ if α and β belong to $Q(\vartheta)$ and $\beta \neq 0$.

We defined an algebraic number ξ as any root of an algebraic equation

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_n = 0,$$

where a_0, a_1,… are rational integers, not all zero. If ξ satisfies an algebraic equation of degree n, but none of lower degree, we say that ξ is of degree n.

If n = 1, then ξ is rational and $Q(\xi)$ is the aggregate of rationals. Hence, for every rational ξ, $Q(\xi)$ denotes the same aggregate, the field of rationals, which we denote by Q(1). This field is part of every algebraic field.

If n = 2, we say that ξ is 'quadratic'. Then ξ is a root of a quadratic equation

$$a_0 x^2 + a_1 x + a_2 = 0$$

and so $$\xi = \frac{a + b\sqrt{m}}{c}, \quad \sqrt{m} = \frac{c\xi - a}{b}$$

for some rational integers a, b, c, m. Without loss of generality we may take m to have no squared factor. It is then easily verified that the field $Q(\xi)$ is the same aggregate as $Q(\sqrt{m})$. Hence it will be enough for us to consider the quadratic fields $Q(\sqrt{m})$ for every rational integer m, positive or negative (apart from m = 1).

Any member ξ of $Q(\sqrt{m})$ has the form

$$\xi = \frac{P(\sqrt{m})}{P(\sqrt{m})} = \frac{t + u\sqrt{m}}{v + w\sqrt{m}} = \frac{(t + u\sqrt{m})(v - w\sqrt{m})}{v^2 - w^2 m} = \frac{a + b\sqrt{m}}{c}$$

for rational integers t, u, v, w, a, b, c. We have $(c\xi - a)^2 = mb^2$, and so ξ is a root of

$$c^2x^2 - 2acx + a^2 - mb^2 = 0. \qquad (1)$$

Hence ξ is either rational or quadratic; i.e. every member of a quadratic field is either a rational or a quadratic number.

The field $Q(\sqrt{m})$ includes a sub-class formed by all the algebraic integers of the field. We defined an algebraic integer as any root of an equation

$$x^j + c_1 x^{j-1} + \ldots + c_j = 0, \qquad (2)$$

where $c_1,\ldots,c_j$ are rational integers. We appear then to have a choice in defining the integers of $Q(\sqrt{m})$. We may say that a number ξ of $Q(\sqrt{m})$ is an integer of $Q(\sqrt{m})$ (i) if ξ satisfies an equation of the form (2) for some j, or (ii) if ξ satisfies an equation of the form (2) with j = 2.

Primitive polynomials

We say that the integral polynomial

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

is a primitive polynomial if

$$a_0 > 0,\ \gcd(a_0, a_1, \ldots, a_n) = 1$$

Theorem 4.27 An algebraic number ξ of degree n satisfies a unique primitive equation of degree n. If ξ is an algebraic integer, the coefficient of x^n in this primitive equation is unity.

We first prove the following theorem :

Theorem 4.28 Let ξ be an algebraic number of degree n and let $f(x) = 0$ be a primitive equation of degree n satisfied by ξ. Let $g(x) = 0$ be any primitive equation satisfied by ξ. Then $g(x) = f(x)\, h(x)$ for some primitive polynomial $h(x)$ and all x.

By the definition of ξ and n there must be at least one polynomial $f(x)$ of degree n such that $f(\xi) = 0$. We may clearly suppose $f(x)$ primitive. Again the degree of $g(x)$ cannot be less than n. Hence we can divide $g(x)$ by $f(x)$ by means of the division algorithm of elementary algebra and obtain a quotient $H(x)$ and a remainder $K(x)$, such that

$$g(x) = f(x)\, H(x) + K(x), \qquad \ldots(1)$$

$H(x)$ and $K(x)$ are polynomials with rational coefficients, and $K(x)$ is of degree less than n.

If we put $x = \xi$ in (1), we have $K(\xi) = 0$. But this is impossible, since ξ is of degree n, unless $K(x)$ has all its coefficients zero. Hence

$$g(x) = f(x)\, H(x).$$

If we multiply this throughout by an appropriate rational integer, we obtain

$$cg(x) = f(x)h(x), \qquad \ldots(2)$$

where c is a positive integer and $h(x)$ is an integral polynomial. Let d be the highest common divisor of the coefficients of $h(x)$. Since g is primitive, we must have $d \mid c$. Hence, if $d > 1$, we may remove the factor d; that is, we may take $h(x)$ primitive in (2). Now suppose that $p \mid c$, where p is prime. It follows that $f(x)\, h(x) \equiv 0 \pmod p$ and so, either $f(x) \equiv 0$ or $h(x) \equiv 0 \pmod p$. Both are impossible for primitive f and h and so $c = 1$. This proves the theorem.

Proof of the theorem 4.27 The proof of Theorem 4.27 is now simple. If $g(x) = 0$ is a primitive equation of degree n satisfied by ξ, then $h(x)$ is a primitive polynomial of degree 0; i.e. $h(x) = 1$ and $g(x) = f(x)$ for all x. Hence $f(x)$ is unique.

If ξ is an algebraic integer, then ξ satisfies an equation of the form

$$x^j + c_1 x^{j-1} + \ldots + c_j = 0, \qquad \ldots(1)$$

where $c_1\ c_2 \ldots c_j$ are rational integers, for some $j \geq n$. We write $g(x)$ for the left-hand side of (1) and, by Theorem 4.28, we have

$$g(x) = f(x)\, h(x),$$

where $h(x)$ is of degree $j-n$. If $f(x) = a_0 x^n + \ldots$ and $h(x) = h_0 x^{j-n} + \ldots$, we have $1 = a_0 h_0$, and so $a_0 = 1$. This completes the proof of Theorem 4.27.

Definition :- A complex number α is called an algebraic number if $\exists$ integers $a_0, a_1, \ldots a_n$ $(a_n \neq 0)$ such that α satisfies a polynomial of the form

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

Further if $a_n = 1$ in above, then α is called on algebraic integer

Definition :- A monic polynomial $p(x)$ in $Q[x]$ is called a minimal polynomial of α if $p(x)$ is a polynomial of minimal degree which is satisfied by α.

Remark :- In modern algebra we have proved that if α is an algebraic integer then $Q[\alpha] = Q(\alpha)$ where $Q[\alpha]$ is the set of all polynomials in α with coefficient, from Q and $Q(\alpha)$ is the smallest field containing Q & α.

Remark :- We know $Q(\alpha)$ is a vector space over Q and degree $[Q(\alpha). Q]$ is the degree of minimal polynomial satisfied by α.

Theorem 4.29 Given an algebraic number α, $\exists$ a non-zero integer t such that $t\alpha$ is an algebraic integer.

Proof :- Since α is an algebraic number, $\exists$ integers $a_n, a_{n-1}, \ldots, a_1, a_0, a_n \neq 0$ such that

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} + \ldots + a_1 \alpha + a_0 = 0 \qquad \ldots(1)$$

Multiplying (1) by a_n^{n-1}, we get

$$a_n^n \alpha^n + a_{n-1} \alpha^{n-1} a_n^{n-1} + \ldots + a_1 \alpha a_n^{n-1} + a_0 a_n^{n-1} = 0$$

Then $(a_n \alpha)$ satisfies

$$f(x) = x^n + a_{n-1} x^n + \ldots + a_1\ a_n^{n-2} x + a_0\ a_n^{n-1}$$

$\Rightarrow$ $(a_n \alpha)$ is an algebraic integer. If we take $t = a_n$, we get the result.

The general quadratic field

Definition :- A field k of complex number is called a quadratic field if

$[K : Q] = 2$ and K is a vector space over Q.

Theorem 4.30 If K is a quadratic field, $\exists$ a non-zero square free integer m such that

$$K = Q(\sqrt{m})$$

Proof :- Since [K : Q] = 2, take any $c \in K$, $c \notin Q$. Now consider 1, c, c^2. These are three elements of K, so these must be linearly dependent over Q. So. $\exists$ a_0, a_1, a_2 in Q, not all zero, such that

$$a_0 c^2 + a_1 c + a_2 = 0$$

Now a_0 can not be equal to zero since otherwise $c \in Q$

$$\Rightarrow \qquad c^2 + \frac{a_1}{a_0} c + \frac{a_2}{a_0} = 0$$

$$\Rightarrow \qquad c^2 + \frac{a_1}{a_0} c = -\frac{a_2}{a_0}$$

Completing squares we get

$$c^2 + \frac{a_1}{a_0} c + \frac{a_1^2}{4a_0^2} = \frac{a_1^2}{4a_0^2} - \frac{a_2}{a_0} = \frac{a_1^2 - 4a_0 a_2}{4a_0^2}$$

Then $$\left(c + \frac{a_1}{2a_0} \right)^2 = \frac{a_1^2 - 4a_0 a_2}{4a_0^2}$$

Taking the square root we get

$$c + \frac{a_1}{2a_0} = \pm \frac{\sqrt{a_1^2 - 4a_0 a_2}}{2a_0}$$

i.e. $$c = -\frac{a_1 \pm \sqrt{a_1^2 - 4a_0 a_2}}{2a_0}$$

Then $$Q(c) = Q\left(\frac{-a_1 \pm \sqrt{a_1^2 - 4a_0 a_2}}{2a_0} \right)$$

But $2a_0 \in Q$

$\therefore$ $$Q(c) = Q(-a_1 \pm \sqrt{a_1^2 - 4a_0 a_2})$$

$$= Q(\pm \sqrt{a_1^2 - 4a_0 a_2})$$

$$= Q\left(\sqrt{a_1^2 - 4a_0a_2}\right)$$

$$= Q(b\sqrt{m}) = Q(\sqrt{m})$$

where m is a square free integer.

Now we claim $K = Q(\sqrt{m}) = Q(c)$

Suppose $K \neq Q(\sqrt{m})$

Then $\exists\ a \in K$, $a \notin Q(\sqrt{m})$. Then $1, \sqrt{m}$, a are linearly dependent over Q since $[K : Q] = 2$ and so $a \in Q(\sqrt{m})$.

Remark :- Since m is square free

$$m \not\equiv 0 \pmod 4$$

So either $m \equiv 1 \pmod 4$ or $m \equiv 2 \pmod 4$

or $m \equiv 3 \pmod 4$.

Theorem 4.31 Let $K = Q(\sqrt{m})$ be a quadratic field and let $\alpha \in K$. Then α is an algebraic integer of K.

$\Leftrightarrow \alpha$ can be written as

$$\alpha = a + b\tau$$

where $a, b \in Z$

and $\tau = \sqrt{m}$ if $m \equiv 2$ or $3 \pmod 4$

and $\tau = \dfrac{1+\sqrt{m}}{2}$ if $m \equiv 1 \pmod 4$

Proof :- Let $\alpha = a + b\tau$, where τ is given as above

Let $m \equiv 2$ or $3 \pmod 4$

Then $\alpha = a + b\sqrt{m}$

$\Rightarrow \alpha - a = b\sqrt{m}$

$\Rightarrow (\alpha - a)^2 = b^2m$

$\Rightarrow \alpha^2 - 2a\alpha + a^2 - b^2m = 0$

$\Rightarrow$ α satisfies $x^2 - 2ax + a^2 - b^2 m = 0$

$\therefore$ α is an algebraic integer by definition. Now let $m \equiv 1 (\text{mod } 4)$. Then

$$\alpha = a + b\left(\frac{1+\sqrt{m}}{2}\right)$$

i.e. $$\alpha = a + \frac{b}{2} + \frac{b\sqrt{m}}{2}$$

$\Rightarrow$ $$\alpha - \left(\frac{2a+b}{2}\right) = \frac{b\sqrt{m}}{2}$$

Squaring, we get

$$\alpha^2 - \alpha(2a+b) + a^2 + ab + \frac{b^2}{4} = \frac{b^2}{4} m$$

or $$\alpha^2 - (2a+b)\alpha + a^2 + ab - \frac{b^2}{4}(m-1) = 0$$

Thus α satisfies

$$x^2 - x(2a+b) + a^2 + ab - \frac{b^2}{4}(m-1) = 0$$

which has integral coefficients since $\frac{m-1}{4} \in Z$

$\Rightarrow$ α is a algebraic integer.

Conversely, let α be an algebraic integer. Since $\alpha \in K = Q(\sqrt{m})$ then we can write

$$\alpha = \frac{a + b\sqrt{m}}{c}, \text{ where } a, b, c \in Z, c \neq 0$$

W. L. O. G. we assume

$$c > 0 \text{ and } \gcd(a, b, c) = 1$$

Now $$\alpha = \frac{a + b\sqrt{m}}{c}$$

$\Rightarrow$ $$c\alpha - a = b\sqrt{m}$$

Squaring we get

$$(c\alpha - a)^2 = b^2 m$$

$$c^2\alpha^2 - 2ac\alpha + a^2 - b^2 m = 0$$

$$\Rightarrow \qquad \alpha^2 - \frac{2a}{c}\alpha + \frac{a^2 - b^2 m}{c^2} = 0$$

Then α satisfies

$$x^2 - \frac{2a}{c}x + \frac{a^2 - b^2 m}{c^2} = 0 \qquad \ldots(1)$$

Since α is an algebraic integer, so the coefficient in (1) must be integers. Then

(i) $\quad c \mid 2a$ and $c^2 \mid (a^2 - b^2 m)$ $\qquad \ldots(2)$

If $b = 0$ then $c^2 \mid a^2 \Rightarrow c \mid a$

In this case (1) becomes

$$x^2 - \frac{2a}{c}x + \frac{a^2}{c^2} = 0$$

$$\Rightarrow \qquad \left(x - \frac{a}{c}\right)^2 = 0 \Rightarrow x = \frac{a}{c}$$

i.e. $\quad \alpha = a/c$

But $\quad c \mid a \Rightarrow \frac{a}{c}$ is an integer

Then $\alpha = \frac{a}{c}$ and it is of the required form. i.e. $\alpha = \frac{a + 0.\sqrt{m}}{c}$

So let $\quad b \neq 0$

let $\quad \gcd(a, c) = d$

Then $\quad d \mid a , d \mid c \Rightarrow d^2 \mid a^2, d^2 \mid c^2$

But $\quad c^2 \mid (a^2 - b^2 m)$ and $d^2 \mid c^2$

$\Rightarrow \qquad d^2 \mid (a^2 - b^2 m)$

But $d^2 \mid a^2 \Rightarrow d^2 \mid b^2 m$

$\Rightarrow$ $d^2 \mid b^2$ (Θ m is square free)

$\Rightarrow$ $d \mid b$

Also $d \mid a, d \mid b, d \mid c \Rightarrow d \mid \gcd(a, b, c) = 1$

$\Rightarrow$ $d = 1$

$\Rightarrow$ $\gcd(a, c) = 1$

But $c \mid (2a) \Rightarrow c \mid 2 \Rightarrow c = 1$ or 2

If $c = 1$, then $\alpha = a + b\sqrt{m}$ where $a, b \in Z$.

$m \equiv 2$ or $m \equiv 3 \pmod 4$

Then α is of the required form

Now let $c = 2$

Then $\alpha = \dfrac{a + b\sqrt{m}}{2}$

Since $\gcd(a, c) = 1$ & $c = 2$

$\Rightarrow$ a must be odd.

From (2), $c^2 \mid (a^2 - b^2 m)$

$\Rightarrow$ $a^2 - b^2 m \equiv 0 \pmod 4$

Then $a^2 \equiv b^2 m \pmod 4$ …(3)

But a is odd and $m \equiv 1 \pmod 4$

$\Rightarrow$ $b^2 \equiv 1 \pmod 4$

$\Rightarrow$ b is odd.

The b can not be even.

$\Rightarrow$ $d = 1$

$\Rightarrow$ $bdc\ (a, c) = 1$

But $c/(2a) \Rightarrow c/2 \Rightarrow c = 1$ or 2

If $c = 1$, then $\alpha = a + b\sqrt{m}$ where $a, b \in Z$

and $m \equiv 2$ or $m \equiv 3 \pmod 4$

Then α of the required form

Now let $c = 2$

Then $\alpha = \dfrac{a + b\sqrt{m}}{2}$

Since $\gcd(a, c) = 1$ & $c = 2$

$\Rightarrow$ a must be odd.

From (2), $c^2/c^2 - b^2m$)

$\Rightarrow$ $a^2 - b^2 \equiv 0 \pmod 4$

Then $a^2 \equiv b^2m \pmod 4$ …(4)

But a is odd and $m \equiv 1 \pmod 4$

$\Rightarrow$ $b^2 \equiv 1 \pmod 4$

$\Rightarrow$ b is odd.

Then b can not be even.

Now $\alpha = \dfrac{a + b\sqrt{m}}{2} = b\left(\dfrac{1 + \sqrt{m}}{2}\right) + \dfrac{a - b}{2}$

Then α is of the form $x + y\tau$ where $x, y \in Z$ & $\tau = \dfrac{\sqrt{m} + 1}{2}$ since $\dfrac{a - b}{2}$ is an integer.

Hence, this proves the theorem

Remark :- If $m \equiv 1 \pmod 4$, then α is an algebraic integer of $Q(\sqrt{m})$

$\Leftrightarrow$ $\alpha = \dfrac{a + b\sqrt{m}}{2}$, where $a, b \in Z$ and of same parity.

Proof of remark :- If both a & b are even then

$\alpha = x + y\sqrt{m}$ where $x, y \in Z$

$$= 2y\left(\frac{1+\sqrt{m}}{2}\right) + x - y,$$

and if both a & b are odd,

$$\alpha = \frac{a+b\sqrt{m}}{2} = \frac{b(1+\sqrt{m})}{2} + \frac{a-b}{2}$$

and in either case, they can be written as $a + b\tau$, where a, b are integers and so they are algebraic integers

Conversely, if α is an algebraic integer

Let $\alpha = a + b\,\tau = a + b\left(\frac{1+\sqrt{m}}{2}\right)$

$$= \frac{(2a+b)+b\sqrt{m}}{2}$$

Then b & 2a + b are of the same parity and this prove the result.

Theorem 4.32 The algebraic integers of a quadratic field form a ring.

To prove this we shall prove that the product of two algebraic integers is an algebraic integer.

Proof :- If $m \equiv 2 \pmod 4$ or $m \equiv 3 \pmod 4$, the result is trivially true.

So let $m = 1 \pmod 4$.

Let $x_1 = a_1 + b_1\,\tau$ and $x_2 = a_2 + b_2\,\tau$

where $\tau = \frac{\sqrt{m}+1}{2}$

Now $x_1\,x_2 = (a_1 + b_1\,\tau)\,(a_2 + b_2\,\tau)$

$$= a_1\,a_2 + \tau\,(a_1\,b_2 + a_2\,b_1)$$

$$+ b_1\,b_2\,\tau^2$$

But $\tau = \frac{\sqrt{m}+1}{2} \quad \Rightarrow \tau - \frac{1}{2} = \frac{\sqrt{m}}{2}$

$\Rightarrow$ $\tau^2 - \tau + \frac{1}{4} = \frac{m}{4} \quad \Rightarrow \tau^2 = \tau + \frac{m-1}{4}$

Then $x_1 x_2 = a_1 a_2 + \tau(a_1 b_2 + a_2 b_1)$

$$+ b_1 b_2 \left(\tau + \frac{m-1}{4} \right)$$

$$= \tau(a_1 b_2 + a_2 b_1 + b_1 b_2)$$

$$+ a_1 a_2 + b_1 b_2 \frac{m-1}{4}$$

which is of the form $x + y\tau$ where $x, y \in Z$.

$\Rightarrow x_1 x_2$ is an algebraic integer.

Definition :- Let α and β be two algebraic integers, $\beta \neq 0$. We say $\beta \mid \alpha$ if $\exists$ an algebraic integer γ such that $\alpha = \beta\gamma$

Definition :- An algebraic integer $\alpha \neq 0$ is said to be a unity if $\alpha \mid 1$ i.e. if $\exists$ an algebraic integer β such that $\alpha\beta = 1$.

Theorem 4.33 The product of two unities is a unity

Proof :- Let α, and α_2 be two unities, then $\exists$ algebraic integers β_1 & β_2 such that $\alpha_1 \beta_1 = \alpha_2 \beta_2 = 1$ Then $(\alpha_1 \beta_1)(\alpha_2 \beta_2) = 1$ i.e. $(\alpha_1 \alpha_2)(\beta_1 \beta_2) = 1$

Also $\beta_1 \beta_2$ is an algebraic integer (since β_1 & β_2 are algebraic integer)

$\Rightarrow$ $\alpha_1 \alpha_2$ is a unity

Theorem 4.34 The inverse of a unity is a unity

Proof :- $\alpha\beta = 1 \Rightarrow \beta\alpha = 1 \Rightarrow \beta$ is also a unity

Remark :- The above two theorems prove that the unities of a quadratic field form a multiplicative group.

Definition :- Let $\alpha = x + y\sqrt{m} \in K = Q(\sqrt{m})$.

Then $x, y \in Q$.

We define norm of α as $N(\alpha) = N(x + y\sqrt{m}) = x^2 - my^2$

Clearly if $m < 0$; $(x^2 - my^2) \geq 0$

Remark :- Also $N(\alpha) , \neq 0$ if$(x, y) \neq (0, 0)$, i.e. if $\alpha \neq 0$

Proof :- If possible, let $N(\alpha) = 0$

$\Rightarrow$ $x^2 - my^2 = 0$

$\Rightarrow$ $x^2 = my^2$ …(1)

If $(x, y) \neq (0, 0)$ then (1) is not possible since m is square free.

Theorem 4.35 Norm is multiplicative i.e. if $\alpha, \beta \in K$; $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$

Proof :- Let $\alpha, \beta \in K$

Let $\alpha = x_1 + y_1\sqrt{m}$ and $\beta = x_2 + y_2\sqrt{m}$

Then $N(\alpha) = x_1^2 - m y_1^2$ and $N(\beta) = x_2^2 - m y_2^2$

Now $\alpha\beta = (x_1 + y_1\sqrt{m})(x_2 + y_2\sqrt{m})$

$= (x_1 x_2 + m y_1 y_2 + \sqrt{m}(x_1 y_2 + x_2 y_1))$ and

$N(\alpha\beta) = (x_1 x_2 + m y_1 y_2)^2 - m(x_1 y_2 + x_2 y_1)^2$

$= x_1^2 x_2^2 + m^2 y_1^2 y_2^2 + 2m x_1 x_2 y_1 y_2 - m x_1^2 y_2^2 - m x_2^2 y_1^2$

$- 2m x_1 x_2 y_1 y_2$

$= x_1^2 x_2^2 + m^2 y_1^2 y_2^2 - m x_1^2 y_2^2 - m x_2^2 y_1^2$

$= (x_1^2 - m y_1^2)(x_2^2 - m y_2^2) = N(\alpha) \cdot N(\beta)$

Theorem 4.36 The norm of a algebraic integer is an integer

Proof :- To prove this we have to distinguish two cases when $K = Q(\sqrt{m})$

Case I :- $m \equiv 2$ or $m \equiv 3 \pmod 4$

Let α be an algebraic integer of K. Then $\exists$ integers x & y such that $\alpha = x + y\sqrt{m}$

Then $N(\alpha) = x^2 - my^2$ is clearly an integer since x, y, m are integers

Case II :- $m \equiv 1 \pmod 4$

If α is an algebraic integer, then $\exists$ integers x and y such that

$$\alpha = x + y\left(\frac{1+\sqrt{m}}{2}\right)$$

$$= x + \frac{y}{2} + \frac{y}{2}\sqrt{m}$$

$$\therefore \quad N(\alpha) = \left(x + \frac{y}{2}\right)^2 - \frac{y^2}{4}m$$

$$= x^2 + \frac{y^2}{4} + xy - \frac{y^2}{4}m$$

$$= x^2 + xy - y^2\left(\frac{m-1}{4}\right) \text{ which is clearly an integer since } \frac{m-1}{4} \in Z$$

Theorem 4.37 The norm of a unity is ± 1

Proof :- Let α be a unity. Then $\exists$ an algebraic integer β such that $1 = \alpha\beta$

Then $1 = N(1) = N(\alpha\,\beta) = N(\alpha)\,N(\beta)$

But $N(\alpha)$ and $N(\beta)$ are integers $\Rightarrow N(\alpha) \mid 1$

$\Rightarrow$ $N(\alpha) = \pm 1$.

Definition :- Let α & β be algebraic integers. We say α is an associate of β if $\exists$ a unity $\in$ of K such that $\beta = \in \alpha$.

Remark :- We can check that the relation of associate ship is an equivalence relation in the set of all algebraic integers.

Definition :- An algebraic integer α is a said to be a prime of K if only divisor of α are associates of α.

Theorem 4.38 If $|N(\alpha)| = p$ where p is a prime no, then α is a prime of K.

Proof :- If possible let α be not a prime element of K. Then $\exists$ algebraic integers β, γ such that $\alpha = \beta\gamma$ and β, γ are not unities of K.

Now $N(\alpha) = N(\beta\gamma) = N(\beta) \cdot N(\gamma)$

$\therefore$ $p = |N(\alpha)| = |N(\beta) \cdot N(\gamma)| = |N(\beta)| \cdot |N(\gamma)|$

But both of β & γ are not unities of K.

Then $|N(\beta)| > 1$, $|N(\gamma)| > 1$

But only positive divisors of p are 1 & p

$\Rightarrow$ $|N(\beta)| = p = |N(\gamma)| \Rightarrow p = p \cdot p \Rightarrow p = 1$, which is not possible, since p is a prime number

$\Rightarrow$ Either β or γ must be a unity $\Rightarrow$ Divisors of α are associates of α. $\Rightarrow$ α is a prime element of K.

Theorem 4.39 If $|N(\alpha)| = 1$; then α must be a unity.

Proof :- We know if $\alpha = x + y\sqrt{m}$

Then $N(\alpha) = x^2 - my^2 = ((x + y\sqrt{m})\,(x - y\sqrt{m}) = \alpha\,\overline{\alpha}$

where $\overline{\alpha}$ denotes the algebraic conjugate of α.

Note that if α is an algebraic integer then $\overline{\alpha}$ is also an algebraic integer since α & $\overline{\alpha}$ are roots of same polynomial.

Now $|N(\alpha)| = 1 \Rightarrow N(\alpha) = \pm 1$, then $\pm 1 = N(\alpha) = \alpha\overline{\alpha} \Rightarrow \alpha \mid 1$

$\Rightarrow \alpha$ is a unity .

Theorem 4.40 Every non-zero non-unity algebraic integer of K can be written as product of prime elements of K.

Proof :- Let α be a non-zero, non-unity algebraic integer of K. Then $|N(\alpha)| > 1$

Now we shall prove the theorem by induction of $|N(\alpha)|$

If $|N(\alpha)| = 2$, then $|N(\alpha)|$ is a prime number and so α is a prime number of K.

Now assume the theorem is true for all α where $|N(\alpha)| < n$ where $n \in N$, $n > 2$.

Now let $|N(\alpha)| = n$. If α is a prime element of K, we are through.

So let α be not a prime element of K

Then $\exists$ algebraic integer β & γ of K such that. $\alpha = \beta\gamma$ where β & γ are not unities of K.

Then $|N(\beta)| > 1$, $|N(\gamma)| > 1$. But $|N(\alpha)| = |N(\beta)| \cdot |N(\gamma)| \Rightarrow |N(\beta)| < |N(\alpha)| = n$.

and $|N(\gamma)| < |N(\alpha)| = n$

Then by induction hypothesis, both β & γ can be written as product of prime elements of K.

$\Rightarrow \alpha = \beta\gamma$ can be written as product of prime elements of K.

Theorem 4.41 Prove that the unities of the field $K = Q(\sqrt{2})$ are $\pm \in^{\pm n}$ $(n = 0, 1, 2,\ldots)$ and $\in = 1+\sqrt{2}$.

Proof :- Let $\in$ be a unity of $K = Q(\sqrt{2})$. Now the algebraic integers of K are of the form $x + y\sqrt{2}$ where $x, y \in Z$

Since $\in$ is a unity of K, $N(\in) = \pm 1$, i.e. $x^2 - 2y^2 = \pm 1$ …(1)

Now by inspection, $x = 1$, $y = 1$ is a solution of (1)

i.e., $\in = 1 + \sqrt{2}$ is a solution of (1). Since product of two unities is a unity and inverse of a unity is a unity and negative of a unity is a unity, so $\pm \in^{\pm n}$ $(n = 0, 1, 2,\ldots)$ are all unities of K.

Let η be any unity of K. By taking $-\eta$, if necessary , we assume $\eta > 0$. Further by taking η^{-1}, if necessary, we assume $\eta > 1$.

Then we first find all unities of K, which are bigger than 1.

First we shall prove that there exists no unity η of K such that

$$1 < \eta < 1 + \sqrt{2}$$

Let $\eta = x + y\sqrt{2}$, then $-1 \le x^2 - 2y^2 \le 1$

But $$1 < x + y\sqrt{2} < 1 + \sqrt{2} \qquad \ldots(2)$$

So $$-1 < x - y\sqrt{2} < 1 \qquad \ldots(3)$$

Adding (2) & (3), we get

$$0 < 2x < 2 + \sqrt{2}$$

$$\Rightarrow \qquad 0 < x < 1 + \frac{1}{\sqrt{2}} < 2 \Rightarrow x = 1$$

Now from (2), $1 < 1 + y\sqrt{2} < 1 + \sqrt{2}$ and this has no solutions in y.

So $\exists$ no unity η such that $1 < \eta < 1 + \sqrt{2}$. Thus if η is any unity such that $\eta > 1$, then $\eta \ge \in$.

Let $\eta \ne \in^n$ for any n. Since $\in^n \to \infty$ as $n \to \infty$, $\exists$ a unique natural number n such that

$$\in^n < \eta < \in^{\eta+1} \Rightarrow 1 < \in^{-\eta} n < \in \qquad \ldots(4)$$

Since ε is a unity & η is a unity, $\varepsilon^{-\eta}\eta$ is also a unity.

Thus we have a unity of K lying between 1 & ε, which is a contradiction. So we must have

$$\eta = \varepsilon^n \text{ for some } < n.$$

By taking negative or inverse we see that all unities of K are of the form $\pm \varepsilon^{\pm n}$

Remark :- Similarly we can proves that unities of $Q(\sqrt{3})$ are infinite in number.

4.42 Fields in which the fundamental theorem is false. The fundamental theorem of arithmetic is true in Q(1), Q(i),Q(ρ), and in Q(√2). It is important to show by examples, that it is not true in every Q(√m). The simplest examples are m = −5 and (among real fields) m = 10.

(i) Since $-5 \equiv 3 \pmod 4$, the integers of $Q\{\sqrt{(-5)}\}$ are $a + b\sqrt{(-5)}$.

Now the four numbers

$$2, 3, 1 + \sqrt{(-5)}, 1 - \sqrt{(-5)}$$

are prime. Thus

$$1 + \sqrt{(-5)} = \{a + b\sqrt{(-5)}\}\ \{c + d\sqrt{(-5)}\}$$

implies $6 = (a^2 + 5b^2)\,(c^2 + 5d^2)$;

and $a^2 + 5b^2$ must be 2 or 3, if neither factor is a unity. Since neither 2 nor 3 is of this form, $1 + \sqrt{(-5)}$ is prime; and the other numbers may be proved prime similar. But

$$6 = 2.3 = \{1+\sqrt{(-5)}\}\ \{1-\sqrt{(-5)}\},$$

and 6 has two distinct decompositions into primes.

(ii) Since $10 \equiv 2 \pmod 4$, the integers of $Q(\sqrt{10})$ are $a + b\sqrt{10}$. In this case

$$6 = 2.3 = (4+\sqrt{10})\ (4-\sqrt{10}),$$

and it is again easy to prove that all four factors are prime. Thus, for example,

$$2 = (a + b\sqrt{10})\ (c + d\sqrt{10})$$

implies $4 = (a^2 - 10b^2)(c^2 - 10d^2)$,

and $a^2 - 10b^2$ must be ± 2 if neither factor is a unity. This is impossible because neither of ± 2 is a quadratic residue of 10.

Real and complex Euclidean fields

Let us find the unities of a quadratic field.

Theorem 4.43 Let $K = Q(\sqrt{m})$ be a quadratic field & let $m < 0$. Then the number of unities of K is

$$\begin{cases} 4 & \text{if } m = -1 \\ 4 & \text{if } m = -3 \\ 2 & \text{if } m \neq -1,\ m \neq -3. \end{cases}$$

Proof :- we shall distinguish two cases

Case I :- $m \equiv 2$ or $m \equiv 3 \pmod 4$

Let $\in$ be any unity of K. Then $\in$ is also an algebraic integer of K. So $\in = x + y\sqrt{m}$ for some integers x and y.

Since $m < 0$, norm of every norm-zero element of K is positive.

Since $\in$ is a unity, so $N(\in) = 1$, or $1 = N(\in) = N(x + y\sqrt{m}) = x^2 - my^2$ …(1)

Let $m \neq -1$

Then $|-my^2| \geq 2$ if $y \neq 0$

So for (1) to hold we must have $y = 0 \Rightarrow x^2 = 1 \Rightarrow x = \pm 1$

$\therefore \quad \in = x + y\sqrt{m} = \pm 1$

So for $m \neq -1$, $m \equiv 2$ or $3 \pmod 4$, ± 1 are the only unities of K.

Now let $m = -1$. Then from (1), $x^2 + y^2 = 1$

But its only solutions are $x = \pm 1$, $y = 0$ & $x = 0$, $y = \pm 1$

So for $m = -1, \pm 1$ & $\sqrt{-1} = \pm i$ are the only unities of K.

Case II :- $m \equiv 1 \pmod 4$

Let $\in$ be any unity of K. Then as above $N(\in) = 1$

Also, $\exists$ integers x & y such that

$$\in = x + y\left(\frac{1+\sqrt{m}}{2}\right) = x + \frac{y}{2} + \frac{y\sqrt{m}}{2}$$

Then $1 = N(\in) = N\left(x + \frac{y}{2} + \frac{y\sqrt{m}}{2}\right)$

$$= \left(x + \frac{y}{2}\right)^2 - \frac{my^2}{4} \qquad \ldots(2)$$

Since $m < 0$ and $m \equiv 1 \pmod 4 \Rightarrow m = -3, -7, -11, \ldots\ldots$

For $m < -3$, $\left(\frac{-my^2}{4}\right) > 1$ for $y \neq 0$

So for (2) to hold, we must have $y = 0$ and then as before

$$x = \pm 1$$

Now let $m = -3$ Then (2) becomes $1 = \left(x + \frac{y}{2}\right)^2 + \frac{3y^2}{4}$ $\qquad \ldots(3)$

If $|y| \geq 2$, $\frac{3y^2}{4} \geq 3$, so for (3) to hold, we must have

$$|y| \leq 1.$$

If $y = 0$, then as before $x = \pm 1$

If $y = 1$, then from (3), $1 = \left(x + \frac{1}{2}\right)^2 + \frac{3}{4} = x^2 + x + 1$

$\Rightarrow \quad x^2 + x = 0 \Rightarrow x = 0 \text{ or } -1$ …(4)

If $y = -1$, then from (3), $x^2 - x = 0 \Rightarrow x = 0 \text{ or } 1$ …(5)

Thus in this case there are six unities of K

These unities are $\pm 1, \frac{1+\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2}, -\frac{1+\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2},$

If we set $w = \frac{-1+\sqrt{-3}}{2}$

Then these unities are $\pm 1, \pm w, \pm w^2$

In all the cases the unities form a cyclic group.

Remark :- The above theorem shows that the number of unities in all complex quadratic fields is finite. However this is not true for real quadratic fields. In fact the number of unities in each real quadratic field is infinite.

Definition :- A quadratic field is called a simple quadratic field if every algebraic integer can be expressed as a product of prime element uniquely up to change of order and multiplication by units.

Definition :- We say Euclidean Algorithm holds in a quadratic field K if given α, β in K, $\beta \neq 0$, $\exists$ integers γ and δ such that

$$\alpha = \beta\gamma + \delta \quad \text{where either} \quad \delta = 0 \text{ or } |N(\delta)| < |N(\beta)|$$

Definition :- Let α, β be algebraic integers of a quadratic field K and $(\alpha, \beta) \neq (0, 0)$,

an algebraic integer γ is said to be greatest common divisor of α and β if

(i) $\gamma \mid \alpha, \gamma \mid \beta$ in K

(ii) If $\gamma_1 \mid \alpha$ and $\gamma_1 \mid \beta$ in K then $\gamma_1 \mid \gamma$ in K where γ_1 is any algebraic integer of K.

Theorem 4.44 If Euclidean algorithm holds in a quadratic field K then it must be a simple field.

Proof :- To prove the theorem, we first prove

Lemma 1 :- If ξ is greatest common divisor of two algebraic integer γ and γ_1 then $\exists$ algebraic integers η and η_1 such that

$$\xi = \gamma\eta + \gamma_1\eta_1 \; ; (\gamma, \gamma_1) \neq (0, 0)$$

where γ and γ_1 are algebraic integers of quadratic field in which Euclidean algorithm holds.

Proof :- W. L. O. G. take $\gamma_1 \neq 0$. Given γ and $\gamma_1 \in K$ and $\gamma_1 \neq 0$ and Euclidean algorithm holds in K, there exists algebraic integers k_1 and γ_2 such that

$$\gamma = k_1 \gamma_1 + \gamma_2 \text{ where either } \gamma_2 \equiv 0 \text{ or } |N(\gamma_2)| < |N(\gamma_1)|$$

If $\gamma_2 = 0$, $Y = k_1 \gamma_1$ and γ_1 is gcd of γ and γ_1

If $\gamma_2 \neq 0$ we apply Euclidean condition to γ_1 and γ_2 and we get

$$\gamma_1 = k_2 \gamma_2 + \gamma_3$$

for some algebraic integers k_2 and γ_3 and either $\gamma_3 = 0$ or

$$|N(\gamma_3)| < |N(\gamma_2)|$$

If $\gamma_3 \neq 0$, we continue as before and get a decreasing sequence

$$|N(\gamma_4)| < |N(\gamma_3)| < \ldots < |N(\gamma_1)|$$

But we can not get an infinite bounded sequence of positive integers and so the sequence of γ's must stop at some point say $\gamma_{n+1} = 1$. Then as in the corresponding proof for natural numbers, we can show that γ_n is the gcd of γ and γ_1.

Proof of Theorem :- Proceeding in the some manner as for natural numbers we can establish that the decomposition as a product of prime elements of K is unique up to change of order and multiplication by unities.

Theorem 4.45 The Euclidean algorithm is equivalent to the following hypothesis. Given any element δ of $Q(\sqrt{m})$, there is an algebraic integer k of $Q(\sqrt{m})$ such that

$$|N(\delta - k)| < 1$$

Proof :- Suppose, given hypothesis hold's i.e. let γ and γ_1 be two algebraic integers of $Q(\sqrt{m})$ and let $\gamma_1 \neq 0$. Take $\delta \in Q(\sqrt{m})$

Then by hypothesis $\exists$ an algebraic integer k such that

$$\left| N\left(\frac{\gamma}{\gamma_1} - k \right) \right| < 1 \text{ i.e., } \left| N\left(\frac{\gamma - \gamma_1 k}{\gamma_1} \right) \right| < 1$$

Multiply both sides by $|N(\gamma_1)|$, then

$$|N(\gamma_1)| \left| N\left(\frac{\gamma - \gamma_1 k}{\gamma_1}\right)\right| < |N(\gamma_1)|$$

But norm is multiplicative and so, $|N(\gamma - \gamma_1 k)| < |N(\gamma_1)|$

Take, $\eta = \gamma - \gamma_1 k$, then $\gamma = \eta + \gamma_1 k$ where $|N(\eta)| < |N(\gamma_1)|$ and so Euclidean algorithm holds.

Now conversely suppose Euclidean algorithm holds. Let δ be any element of $Q(\sqrt{m})$. If $\delta = 0$, take $k = 0$ and we are through. So let $\delta \neq 0$ then we know that δ is an algebraic number of $Q(\sqrt{m})$. Then $\exists$ a non-zero integer t such that $t\,\delta$ is an algebraic integer.

Now $t\,\delta$ and t are two algebraic integers of $Q(\sqrt{m})$ where $t \neq 0$

By Euclidean algorithm, $\exists$ an algebraic integer k & γ such that

$$t\,\delta = tk + \gamma \text{ where } \gamma = 0 \text{ or } |N(\gamma)| < |N(t)|$$

Then $$\left| N\left(\frac{\gamma}{t}\right)\right| |\, N(t)| = |N(\gamma)| < |N(\delta)|$$

$\Rightarrow$ $$\left| N\left(\frac{\gamma}{t}\right)\right| < 1$$

Now $t\,\delta = tk + \gamma$, $\delta = k + \frac{\gamma}{t} \Rightarrow \delta - k = \frac{\gamma}{t}$

and $|N(\delta - k)| = \left| N\left(\frac{\gamma}{t}\right)\right| < 1$, this proves equivalence.

Remark :- Thus to prove that a quadratic field is a simple field it is enough to prove that given any element δ of the field $\exists$ an algebraic integer k such that

$$|\, N(\delta - k)\,| < 1$$

Theorem 4.46. Euclidean algorithm holds in the quadratic field $K = Q(\sqrt{m})$ where

$$m = -1, -2, -3, -7, -11, 2, 3, 5, 13.$$

Proof. Now any element δ of $K = (\sqrt{m})$ can be written as

$$\delta = r + s\sqrt{m} \quad \text{where } r \in Q,\ s \in Q.$$

Let $m \not\equiv 1 \pmod 4$. Then any algebraic integer of $K = Q(\sqrt{m})$ can be written as $x + y\sqrt{m}$ where $x, y \in Z$

Now given s as above, select integers x & y such that $|r - x| \le \frac{1}{2}$, $|s-y| \le \frac{1}{2}$

Let $k = x + y\sqrt{m}$

Then $\delta - k = (r-x) + (s-y)\sqrt{m}$

$\therefore$ $N(\delta-k) = (r-x)^2 + (-m)(s-y)^2$

First let $m = -1$ or $m = -2$

Now $(r-x)^2 \le \frac{1}{4}$, $(s-y)^2 \le \frac{1}{4}$

Then $|N(\delta-k)| < 1$. Now if $m = 2$ or 3, again we have, $|N(\delta-k)| < 1$

Now let $m \equiv 1 \pmod 4$

Then we know that algebraic integers of K can be written as $a + b\tau$ where $a, b \in Z$

and $\tau = \frac{\sqrt{m}+1}{2}$

In this case select y such that

$$|2s - y| \le \frac{1}{2}$$

Having selected y, select an integer x such that

$$\left| r - \frac{1}{2}y - x \right| \le \frac{1}{2}$$

Now consider $k = x + y + \frac{1}{2}y(\sqrt{m}-1)$

$$= x + \frac{1}{2}y + \frac{1}{2}y\sqrt{m}$$

Then k is an algebraic integer of K and

$$\delta - k = \left(r - x - \frac{1}{2}y\right) + \sqrt{m}\left(s - \frac{1}{2}y\right)$$

For $m<0$, $$|N(\delta-k)| = \left| \left(r - x - \frac{y}{2}\right)^2 + (-m)\left(s - \frac{1}{2}y\right)^2 \right|$$

$$\le \left| \frac{1}{4}\frac{m}{16} \right| < 1, \text{ for } m = -3, -3, -11,$$

for $m > 0$, $\quad |N(\delta - k)| \le \left| -\frac{m}{16} \right| < 1$ for $m = 5$ and 13.

Remark :- There are exactly nine imaginary quadratic fields in which Euclidean algorithm holds

$$(m = -1, -2, -3, -7, -11, -19, -43, -67 \text{ and } -163)$$

Theorem 4.47 The number of real Euclidean fields $Q(\sqrt{m})$ where $m \equiv 2$ or $m \equiv 3 \pmod 4$ is finite.

Proof :- Let us suppose that $Q(\sqrt{m})$ is Euclidean and let $m \equiv 2$ or $3 \pmod 4$. The algebraic integers of K are of the form $x + y\sqrt{m}$ where $x, y \in Z$

Take care, $\quad \alpha = \frac{t}{m}\sqrt{m}$, then $\alpha \in Q(\sqrt{m})$

Since the field is Euclidean, there exists

$$k = x + y\sqrt{m} \text{ such that } |N(\alpha - k)| < 1$$

But $\quad \alpha - k = -x + \left(\frac{t}{m} - y\right)\sqrt{m}$

$\therefore \quad |N(\alpha - k)| < 1 \Rightarrow \left| x^2 - m\left(y - \frac{t}{m}\right)^2 \right| < 1$

$$\Rightarrow \left| x^2 - \frac{(my - t)^2}{m} \right| < 1 \Rightarrow |mx^2 - (my - t)^2| < m, \Rightarrow |(my - t)^2 - mx^2| < m$$

But $\quad (my - t)^2 - mx^2 \equiv t^2 \pmod m$,

So $\exists$ integers x & z such that

$$z^2 - mx^2 \equiv t^2 \pmod m \qquad \ldots(1)$$

and $\quad |z^2 - m x^2| < m \qquad \ldots(2)$

Now let $m \equiv 3 \pmod 4$.

It possible suppose $\exists$ infinitely many reals quadratic fields for which Euclidean algorithm holds in K.

Now select an odd integer t such that $5m < t^2 < 6m$, such a choice if t is possible.

But $\quad z^2 - mx^2 \equiv t^2 \pmod m$

and $\quad |z^2 - mx^2| < m$

$\Rightarrow$ Either $\quad |z^2 - mx^2| - t^2 = -5m$

or $\quad z^2 - mx^2 - t^2 = -6m$

$\Rightarrow$ $t^2 - 5m = z^2 - mx^2$

or $t^2 - 6m = z^2 - mx^2$

$\Rightarrow$ $t^2 - z^2 = m(5-x^2)$ …(3)

or $t^2 - z^2 = m(6-x^2)$ …(4)

But t is odd $\Rightarrow t^2 \equiv 1 \pmod 8$ and $x^2 \equiv 0$ or 1 or 4(mod 8) and $z^2 \equiv 0$ or 1 or 4(mod 8)

$\Rightarrow$ $t^2 - z^2 \equiv 0$ or 1 or 5 (mod 8)

and $5-x^2 \equiv 1$ or 4 or 5 (mod 8)

and $6-x^2 \equiv 2$ or 5 or 6 (mod 8)

$\therefore$ $m(5-x^2) \equiv 3$ or 4 or 7(mod 8) (Θ $m \equiv 3 \pmod 8$)

and $m(6-x^2) \equiv 2$ or 6 or 7 (mod 8)

$\therefore$ Neither (3) nor (4) can hold.

Now let $m \equiv 2 \pmod 4$. If possible suppose there are infinitely many real quadratic fields for which Euclidean algorithm holds. In this case, choose an odd integer t such that $2m < t^2 < 3m$

Then $t^2 \equiv 1 \pmod 8$ and $m \equiv 2$ or 6(mod 8)

Further $t^2 - 2m = z^2 - mx^2$ …(5)

or $t^2 - 3m = z^2 - mx^2$ …(6)

i.e. $t^2 - z^2 = m(2-x^2)$ or $t^2 - z^2 = m(3-x^2)$

Now $m(2-x^2) \equiv 2$ or 4 or 6(mod 8)

and $m(3-x^2) \equiv 2$ or 4 or 6(mod 8)

whereas $t^2 - z^2 \equiv 0$ or 1 or 5 (mod 8)

so neither (5) or (6) can hold

Theorem 4.48 Let $K = Q(\sqrt{m})$ be a simple field and let π be a prime of K then π divides one and only one rational prime

Proof :- Let $|N(\pi)| = n \Rightarrow N(\pi) = \pm n$

But $N(\pi) = \pi\ \bar{\pi}$ where $\bar{\pi}$ denotes the algebraic conjugate of π.

Since π is a prime $\Rightarrow n > 1$. Let $n = p_1\ p_2 \ldots p_r$ be the decomposition of n into primes.

Then $\pi\bar{\pi} = \pm\ p_1\ p_2 \ldots p_r$

But K is a simple field and so π must occur when we decompose n into prime elements of K and so π must divide at least one of $p_1, p_2, \ldots, p_r$.

If possible let π divides two different rational primes say p and q. Now in Z, gcd (p, q) = 1

$\Rightarrow \exists$ integers x & y such that

$$px + qy = 1$$

But $\pi \mid p$ and π/q in K.

$\Rightarrow$ $\pi \mid 1$ in K $\Rightarrow \pi$ is a unit which contradicts that π is a prime so π divides exactly one of p & q.

Theorem 4.49 The primes in Q(i) = K can be divided into 3 classes

(1) The prime 1 + i and its associates

(2) The rational primes of the form 4n+3 and their associates

(3) The prime factors a + bi of the rational primes of the form 4n+1 and their associates.

Proof :- Let π be any prime element of K. Then π divides exactly one rational prime say $\pi \mid p$.

Then we distinguish the following cases

Case I. p = 2

We know $2 = (1 + i)(1-i)$

Further we know 1, −1, i, −i are unities of K and

$(1-i) = -i(1+i)$ and 1 + i is not a unity of K

So $2 = -i(1 + i)^2$

Since we know that every rational prime can decomposed into at least of most 2 primes of a quadratic field and so 1 + i must be a prime number. So we get $\pi = 1+i$ or an associate of 1 + i

Case II :- $p \equiv 3 \pmod 4$

Since π is an element of K so π is an algebraic integer of K i.e. $\pi = x + yi$ for some integers x and y.

Now π divides $p \Rightarrow p = (x + yi)\alpha$ for some algebraic integer α of K.

i.e. p = (x + yi) (a + bi) for some integers a & b.

Further gcd (a, b) = 1 = gcd (x, y)

But the product of two complex numbers is a real number

$\Rightarrow$ $a + bi = x - yi$

$\Rightarrow$ $p = (x + yi)(x - yi) = x^2 + y^2$

But $p \equiv 3 \pmod 4$

$\Rightarrow$ $x^2 + y^2 \equiv 3 \pmod 4$

which is not possible as no number of the form 4n + 3 can be written as a sum of 2 squares.

So either $\pi = p$ or π is an associate of p.

Case III :- $p \equiv 1 \pmod 4$

Now we know -1 is a quadratic residue of primes of the form 4n +1, so $\exists$ an integer x such that

$$x^2 \equiv -1 \pmod p \text{ or } p \mid (x^2 + 1)$$

If possible, let π be an associate of p. Then p is also a prime element of K.

But $x^2 + 1 = (x + i)(x - i)$ and both $x + i$ and $x - i$ are algebraic integers of K.

Now K is a simple field and $p \mid (x + i)$ or $p \mid (x - i)$

$\Rightarrow$ $\frac{x}{p} + \frac{i}{p}i$ or $\frac{x}{p} - \frac{1}{p}i$ must be on algebraic integer of K, which is not so since algebraic integers of K are of the form a + bi where $a, b \in Z$.

So p can not be a prime element of K and so π must be a divisor of p. This gives rise to 3 classes of primes in K according to the nature of rational prime which they divide.

Definition :- Let α β, γ be algebraic integer in $Q(\sqrt{m})$, where m is square free. Then we say

$$\alpha \equiv \beta \pmod \gamma \text{ if } \gamma \mid (\alpha - \beta) \text{ in } Q(\sqrt{m})$$

Fermat's theorem in the ring of Gaussian integers Q(i).

Theorem 4.50 Let π be a prime in Q(i) such that π is not an associate of 1 + i. Let α be an algebraic integer of Q(i) such that $\gcd(\alpha, \pi) = 1$, Then

$$\alpha^{\phi(\pi)} \equiv 1 \pmod \pi$$

Proof :- since π is not an associate of 1 + i so either $\pi \mid p$, where p is a rational prime of the form

4n + 1 or $\pi = q$ where q is a rational prime of the form 4n + 3.

Since α is an algebraic integer of Q(i),

$$\alpha = \lambda + im, \text{ where } \lambda \in Z, m \in Z.$$

Now suppose $\pi \mid p$

Then $$(\lambda + im)^p \equiv \lambda^b + (i\, m)^p \pmod p$$

$$\equiv \lambda + i^p\, m(\text{mod } p)$$

But $i^p = (i)^{4n+1} = i^{4n}\, i = (i^4)^n\, i = i$

Therefore, $(\lambda + im)^p \equiv (\lambda + im)(\text{mod } p)$

$\Rightarrow$ $\alpha^p \equiv \alpha(\text{mod } p)$ in Q(i)

But $\pi \mid p \Rightarrow \alpha^\pi \equiv \alpha(\text{mod } \pi)$

But Q(i) is a simple field and $\gcd(\alpha, \pi) = 1$

$\Rightarrow$ $\alpha^{\pi-1} \equiv 1 \text{ (mod } \pi)$, i.e., $\alpha^{\phi(\pi)} \equiv 1(\text{mod } \pi)$ in this case

Let $\pi = q$, then $\phi(\pi) = \phi(q) \mid (g^2 - 1)$

Now $\alpha^q \equiv (\lambda + im)^q = \lambda^q + i^q\, m^q(\text{mod } q)$

But $i^q = i^{4n+3} = i^{4n+1}\, i^2 = -i$

$\therefore$ $\alpha^q = \lambda - im(\text{mod } q) = \overline{\alpha}$

Then $\alpha^{q^2} = (\alpha^q)^q = (\overline{\alpha})^q = (\overline{\overline{\alpha}}) = \alpha(\text{mod } q)$

But $\gcd(\alpha, q) = 1$ & Q(i) is a simple field, $\Rightarrow \alpha^{q^2-1} \equiv 1(\text{mod } q)$

i.e., $\alpha^{\phi(\pi)} \equiv 1(\text{mod } \pi)$ in this are also

Remark :- $Q(\sqrt{-3}) = Q(w)$ since $w = \dfrac{-1+\sqrt{-3}}{2}$ and the algebraic integers of $Q(\sqrt{-3})$ are of the form $a + b\omega$ since $a, b \in Z$ the units of $Q(\omega)$ are $\pm 1, \pm\omega, \pm\omega^2$.

Note :- -3 is a quadratic residue of primes of the form $6n + 1$ and quadratic non-residue of primes of the form $6n-1$

Theorem 4.51 The primes of Q(w) can be decomposed into 3 classes.

(1) $1 - w$ and its associates

(2) The rational primes of the form $3n + 2$ and their associates.

(3) The prime factor of the rational primes of the form $3n + 1$ and their associates.

Proof :- Let π be prime of Q(w)

Since $Q(w) = Q(\sqrt{3})$ is a simple field, π divides exactly one rational prime (say p)

Then we distinguish the following cases

Case I :- $p = 3$

Now we know $1 + w + w^2 = 0$

So $3 = (1-w)(1-w^2) = (1-w-w^2+w^3)$

But $w^3 = 1$ and $-w-w^2 = 1$, so

$$3 = (1-w)(1-w^2)$$
$$= (1+w)(1-w)^2$$
$$= -w^2(1-w)^2$$

Since Q(w) is a simple field, every rational prime can be decomposed into at most two primes of Q(w)

Now $-w^2$ is a unity and $(1-w)$ is not a unity. So $(1-w)$ must be prime of Q(w).

Case II :- $p \equiv 2 \pmod 3$

If possible, let p be not a prime of Q(w)

Since every rational prime in Q(w) can be decomposed into atmost two primes in Q(w).

$\exists$ primes π & η of Q(w) such that

$$p = \pi\eta$$

Then $p^2 = N(p) = N(\pi\eta)$

$$= N(\pi)\,N(\eta)$$

Consider $N(\pi)$

Now, only positive factor of p^2 are 1, p, p^2

$\Rightarrow$ $N(\pi) = 1$ or p or p^2

If $N(\pi) = 1$ then π is a unity of Q(w), contradicting π is a prime of Q(w)

If $N(\pi) = p^2$ then $N(\eta) = 1$, then η is a unity of Q(w), contradicting η is a prime of Q(w). So we must have

$$N(\pi) = p$$

Let $\pi = a + bw = a + b\left(\frac{\sqrt{-3}-1}{2}\right)$

$$= \left(a - \frac{b}{2}\right) + b\left(\frac{\sqrt{-3}}{2}\right)$$

Then $p = N(\pi) = \left(a - \frac{b}{2}\right)^2 + 3\frac{b^2}{4}$

$\Rightarrow$ $4p = (2a - b)^2 + 3b^2 \equiv (2a - b)^2 \pmod 3$ …(1)

Since $p \equiv 2 \pmod 3$

$\Rightarrow$ $4p \equiv 2 \pmod 3$

But $(2a - b)^2 \equiv 0 \text{ or } 1 \pmod 3$

So (1) is not possible for any value of a and b, which is a contradiction. So p must be prime of Q(w).

Case III :- $p \equiv 1 \pmod 3$

Here we claim that p can not be a prime of Q(w). If possible let p be a prime of Q(w)

Let $p = 3n+1$

If n is odd then p becomes an even number, greater than equal to 4.

$\therefore$ p can not be a prime

So n must be even

$\Rightarrow$ $p = 6m + 1$ for some $m > 0$, $m \in Z$

Then -3 is a quadratic residue of p.

$\Rightarrow \exists$ an integer x such that

$$x^2 \equiv -3 \pmod p$$

or $p \mid (x^2 + 3)$

But in Q(w), $x^2 + 3 - (x + \sqrt{3})\,(x - \sqrt{-3})$

$\Rightarrow$ $p \mid (x + \sqrt{-3})\,(x - \sqrt{-3})$ in Q(w)

But Q(w) is a simple field

$\Rightarrow$ $p \mid (x + \sqrt{-3})$ or $(x - \sqrt{-3})$ in Q(w)

$\Rightarrow$ Either $\quad \frac{x}{p}+\frac{1}{p}\sqrt{-3}$ or $\frac{x}{p}-\frac{1}{p}\sqrt{-3}$

must be an algebraic integer of Q(w), which is not so. So p can not be a prime of Q(w). So p must be divisible by a prime of Q(w).

Primes of Q($\sqrt{2}$)

Theorem 4.52 The prime of Q($\sqrt{2}$) can be divided into 3 classes

(1) The prime $\sqrt{2}$ and its associates

(2) The rational primes of the form $8n \pm 3$ and their associates

(3) The prime factor $a + h\sqrt{2}$ of the rational primes of the form $8n \pm 1$ and their associates.

Proof :- Let π be any prime of Q($\sqrt{2}$). Since, Q($\sqrt{2}$) is a simple field, π divides exactly one prime say p.

Now we distinguish the three classes

Case I :- $p = 2$

Now $2 = (\sqrt{2})^2$ and $\sqrt{2}$ is an algebraic integer of Q($\sqrt{2}$). But $\sqrt{2}$ is not a unity of Q($\sqrt{2}$) and every rational prime can be decomposed into at most 2 primes of Q($\sqrt{2}$)

So $\sqrt{2}$ must be a prime of Q($\sqrt{2}$).

Case II :- p is a rational prime of the form $8n \pm 3$. Then we claim that p must also be a prime of Q($\sqrt{2}$). If possible, let p be not a prime of Q($\sqrt{2}$), then we know that there exists a prime π of Q($\sqrt{2}$) such that

$$N(\pi) = p$$

Since π is a prime of Q($\sqrt{2}$), it is also an algebraic integer of Q($\sqrt{2}$)

So $\quad \pi = a + b\sqrt{2}$, for some integer $a, b \in Z$

Then $\quad p = N(\pi) = N(a + b\sqrt{2}) = a^2 - 2b^2 \qquad \ldots(1)$

Now $\quad a^2 \equiv 0$ or 1 or 4(mod 8)

and $\quad b^2 \equiv 0$ or 1 or 4(mod 8)

$\therefore \quad p \equiv 0$ or 1 or 2 or 4 or 6 or 7(mod 8)

But $\quad p \equiv 3$ or 5(mod 8)

So (1) does not hold for any value of a and b. So p must be a prime of Q($\sqrt{2}$)

Case III :- p is a rational prime of the form $8n \pm 1$.

We know 2 is a quadratic residue of primes of the form $8n \pm 1$. So there exists an integer x such that

$$x^2 \equiv 2 \pmod{p}$$

i.e. $p \mid (x^2 - 2)$, or $p \mid (x - \sqrt{2})(x + \sqrt{2})$

If p were a prime of $Q(\sqrt{2})$, then since $Q(\sqrt{2})$ is a simple field, p would divide either $x - \sqrt{2}$ or $x + \sqrt{2}$.

i.e. either $\frac{x}{p} - \frac{1}{p}\sqrt{2}$ or $\frac{x}{p} + \frac{1}{p}\sqrt{2}$ must be an algebraic integer of $Q(\sqrt{2})$, which is a contradiction since algebraic integer of $Q(\sqrt{2})$ are of the form $a+b\rho$ where $a,b \in Z$, $\rho = \frac{\sqrt{5}-1}{2}$.

Theorem 4.53 5 is a quadratic residue of prime of the form $5n \pm 1$ & a quadratic non-residue of primes of the form $5n \pm 2$.

Proof :- Let $p = 5n \pm 1$. Then $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{\pm 1}{5}\right) = 1$.

If $p = 5n \pm 2$ then $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{\pm 2}{5}\right) = \left(\frac{2}{5}\right) = -1$

Prime in $Q(\sqrt{5})$

Theorem 4.54 The primes of $Q(\sqrt{5})$ can be divided into three classes

(1) $\sqrt{5}$ and its associates

(2) The rational primes of the form $5n \pm 2$ & their associates

(3) The prime factors $a + h\lambda$ of rational primes of the form $5n \pm 1$.

Proof :- Let π be a prime of $Q(\sqrt{5})$. Since $Q(\sqrt{5})$ is a simple field, π divides exactly one prime of $Q(\sqrt{5})$ say p. Then we distinguish three cases

Case I :- $p = 5$

Now $5 = (\sqrt{5})^2$ and $\sqrt{5}$ is algebraic integer of $Q(\sqrt{5})$ and it is not a unity of $Q(\sqrt{5})$. But every rational prime can be written as a product of at most two primes of $Q(\sqrt{5})$ so $\sqrt{5}$ must be a prime of $Q(\sqrt{5})$

Case :- $p = 5n \pm 2$

If possible, suppose p is not a prime of $Q(\sqrt{5})$

Then there must exist a prime

$$\pi = a + b\lambda \text{ of } Q(\sqrt{5}),\ a, b \in Z$$

such that $p = N(\pi) = N(a + b\lambda)$

$$= N\left(a + b\frac{\sqrt{5}+1}{2}\right) = a^2 + ab - b^2$$

Then $4p = 4a^2 + 4ab - 4b^2$

$$= (2a + b)^2 - 5b^2 \equiv (2a + b)^2 \pmod 5 \qquad \ldots(1)$$

But $p = 5n \pm 2$

$\Rightarrow$ $4p \equiv \pm 3 \pmod 5$

where as $(2a + b)^2 \equiv 0$ or 1 or 4(mod 5) So (1) is not possible for any value a and b.

$\therefore$ p must be a prime of $Q(\sqrt{5})$.

Case III :- $p = 5n \pm 1$.

Then proceeding as in the last theorem, we can check that p is not a prime of $Q(\sqrt{5})$ and so its factors $a + b\lambda$ must be primes of $Q(\sqrt{5})$.

Notation :- Let p denote a rational primes of the form $5n \pm 1$ and q denote a rational prime of the form $5n \pm 2$.

Let π be any prime of $Q(\sqrt{5})$ such that π is not an associate of $\sqrt{5}$.

Then $\phi(\pi) = p-1$ if $\pi \mid p$

and $\phi(\pi) = q^2-1$ if $\pi = q$

Theorem 4.55 Let p and q be as denoted. Let π be any prime of $Q(\sqrt{5})$, π is not an associate of $\sqrt{5}$ and let α be any algebra integer of $Q(\sqrt{5})$ such that $\gcd(\alpha\ \pi) = 1$. Then

$$\alpha^{\phi(\pi)} \equiv 1 \pmod \pi \qquad \ldots(1)$$

$$\alpha^{p-1} \equiv 1 \pmod \pi \text{ if } \pi \mid p \qquad \ldots(2)$$

$$\alpha^{q+1} \equiv N(\alpha) \pmod q \qquad \ldots(3)$$

Further if $\bar{\pi}$ denotes the conjugate of π and

$$\text{g.c.d. } (\alpha, \bar{\pi}) = 1 \text{ then } \alpha^{p-1} \equiv 1 (\text{mod } p) \qquad \ldots(4)$$

Proof :- Since α is a algebraic integer of $Q(\sqrt{5})$,

let $\alpha = \dfrac{c + d\sqrt{5}}{2}$ where c & d are integers of the same parity.

Now $\alpha = \dfrac{c + d(\sqrt{5})}{2} \Rightarrow 2\alpha = c + d\sqrt{5}$

$\Rightarrow \quad 2\alpha^p \equiv (2\alpha)^p = (c + d\sqrt{5})^p = c^p + d^p(\sqrt{5})^p (\text{mod } p)$ ($\Theta (a + b)^p = a^b + b^p (\text{mod } p)$.)

$$= c^p + d^p 5^{\frac{1}{2}(p-1)} \sqrt{5} \ (\text{mod } p) \qquad \ldots(5)$$

Since p is of the form $5n \pm 1$, 5 is a quadratic residue of p.

By Euler's criterion

$$5^{\frac{1}{2}(p-1)} \equiv \left(\frac{5}{p}\right) \equiv 1 (\text{mod } p)$$

$\therefore \quad 2\alpha^p \equiv c^p + \sqrt{5}\, d^p (\text{mod } p) \qquad \ldots(6)$

But $c^p \equiv c \ (\text{mod } p)$ and $d^p \equiv d (\text{mod } p)$

$\Rightarrow \quad 2\alpha^p \equiv c + d\sqrt{5} \equiv 2\alpha (\text{mod } p)$

$\Rightarrow \quad \alpha^p \equiv \alpha (\text{mod } p)$, since gcd(2, p) = 1

But $\pi \mid p \Rightarrow \alpha^p \equiv \alpha (\text{mod } \pi)$

$\Rightarrow \quad \alpha^{p-1} \equiv 1 (\text{mod } \pi)$ as gcd $(\alpha, \pi) = 1$

Now let gcd$(\alpha\ \bar{\pi}) = 1$ then $(\alpha, p) = 1$ since $\pi\bar{\pi} = p$

$\therefore$ From (6), $\alpha^{p-1} \equiv 1 (\text{mod } p)$, which proves (4)

Now let $\pi = q$ where q is a rational prime of the form $5n \pm 2$.

First let $q > 2$

Now $2\alpha = c + d\sqrt{5}$

$\therefore \quad (2\alpha)^q = (c + d\sqrt{5})^q$

$$\equiv c^q + d^q(\sqrt{5})^q (\text{mod } q) \qquad \ldots(7)$$

Now $2^q \equiv 2(\text{mod } q)$,

$c^q \equiv c(\text{mod } q),\ d^q \equiv d(\text{mod } q)$

and $(\sqrt{5})^q = 5^{\frac{1}{2}(p-1)}\sqrt{5}$ …(8)

But 5 is a quadratic non –residue of primes of the form $5n \pm 2$, so

$$-1 = \left(\frac{5}{q}\right) \equiv 5^{\frac{1}{2}(p-1)} (\text{mod } q) \qquad \ldots(9)$$

Using (8) and (9) in (7)we get

$$2\alpha^q \equiv c - d\sqrt{5} (\text{mod } q)$$

But $c - d\sqrt{5} = 2\bar{\alpha}$, since $\alpha = \dfrac{c + d\sqrt{5}}{2}$

$\therefore$ $2\alpha^q \equiv 2\bar{\alpha} (\text{mod } q)$

But gcd (q, 2) = 1 since q is odd

$\Rightarrow$ $\alpha^q \equiv \bar{\alpha} (\text{mod } q)$ …(10)

$\Rightarrow$ $\alpha^{q+1} \equiv \alpha\bar{\alpha} (\text{mod } q)$

But $\alpha\bar{\alpha} = N(\alpha) \Rightarrow \alpha^{q+1} \equiv N(\alpha)(\text{mod } q)$ which proves (3) for $q > 2$

From (10) we get

$$\alpha^{q^2} \equiv (\bar{\alpha})^q \equiv \bar{\bar{\alpha}} \equiv \alpha(\text{mod } q)$$

But gcd(α, q) = 1 and so

$$\alpha^{q^2-1} \equiv 1(\text{mod } q)$$

i.e. $\alpha^{\phi(q)} \equiv 1(\text{mod } q)$

which proves (1) for $q > 2$.

Now let $\pi = 2$. Then we write

$$\alpha = e + f\lambda \text{ when } e, f \in Z$$

and we are given that gcd (α, π) = 1. Then one of e and f must be odd.

Now $\alpha^2 = \lambda^2 + f^2\rho^2 = e + fe^2(\text{mod } q)$ …(11)

Now $\rho = \dfrac{\sqrt{5}-1}{2} \Rightarrow \rho + \dfrac{1}{2} = \sqrt{5/2}$

$$\Rightarrow \qquad \rho^2 + \rho + \frac{1}{4} = \frac{5}{4} \quad \Rightarrow \rho^2 + \rho - 1 = 0$$

$$\Rightarrow \qquad \rho^2 = 1 - \rho$$

Then form (11) we get

$$\alpha^2 \equiv e + f(1-\lambda) (\text{mod } 2)$$

Now but $1-\lambda = 1 - \dfrac{\sqrt{5}-1}{2} = \dfrac{3}{2} - \dfrac{\sqrt{5}}{2} = -\dfrac{1}{2} - \dfrac{\sqrt{5}}{2} (\text{mod } 2) = \bar{\lambda}$

$$\therefore \qquad \alpha^2 = e + f(1-\lambda) \equiv e + f\bar{\lambda} (\text{mod } 2) = \bar{\alpha}$$

$$\Rightarrow \qquad \alpha^3 = \alpha\bar{\alpha} \equiv N(\alpha) (\text{mod } 2)$$

This proves (3) for q = 2.

But $$N(\alpha) = N(a + b\lambda) = N\left(a + b\frac{\sqrt{5}-1}{2}\right)$$

$$= a^2 - ab - b^2 \equiv 1 (\text{mod } 2) \qquad [\Theta$$

one of a & b is odd]

This proves (2) for q = 2

Definition :- Let

$$w = \frac{\sqrt{5}+1}{2},$$

then $$w - \frac{1}{2} = \frac{\sqrt{5}}{2}$$

$$\Rightarrow \qquad w^2 - w - 1 = 0 \text{ i.e. } w^2 = w + 1$$

Let its roots be w and $\bar{w}$.

Define $$r_m = w^{2^m} + \bar{w}^{2^m}$$

Since r_m is a symmetric function in the roots of the polynomial, $w^2 - w - 1 = 0$, r_m's are integers.

In fact $$r_m = \{3, 7, \ldots\ldots\}.$$

Further $$w\bar{w} = -1 \qquad \Rightarrow \bar{w} = -\frac{1}{w}$$

$$\therefore \qquad r_m^2 = (w^{2^m} + \bar{w}^{2^m})^2 = w^{2^{m+1}} + \bar{w}^{2^{m+1}} + 2(w\bar{w})^{2m}$$

$$= r_{m+1} + 2 \qquad [\Theta$$

$w\bar{w} = -1]$

$\Rightarrow \qquad r_{m+1} = r_m^2 - 2$

Lucas Test for Primality of the Mersenne Number :-

Theorem 4.56 Let $p = 4n + 3$ be a prime and Let $M = M_p = 2^p - 1$ be the corresponding Mersenne number.

Then M is prime $\Leftrightarrow$ $r_{p-1} \equiv 0 \pmod{M}$

Proof :- Suppose M is prime.

Now $M = 2^p - 1 = 2^{4n+3} - 1 = 8 \cdot 16^n - 1 = 2 \pmod 5$

Then M is a prime of the form $5n + 2$

Now $w = \dfrac{\sqrt{5}+1}{2} \Rightarrow N(w) = -1$

$\Rightarrow$ w is a unity of $Q(\sqrt{5})$. So if α is any algebraic integer of $Q(\sqrt{5})$ then

$\gcd(\alpha, w) = 1$

Now we apply the last theorem with $\alpha = w$, $q = M$

Then $w^{M+1} \equiv N(w) \pmod{M}$

But $M = 2^p - 1$

Therefore $w^{2p} = -1 \pmod{M}$ …(1)

By definition $r_{p-1} = w^{2^{p-1}} + \overline{w}^{2^{p-1}}$

$$= \overline{w}^{2^{(p-1)}} \left(\left(\frac{w}{\overline{w}} \right)^{2p-1} + 1 \right)$$

But $\overline{w} = -\dfrac{1}{w}$

$\Rightarrow \qquad r_{p-1} = \overline{w}^{2^{p-1}} ((-w^2)^{2^{p-1}} + 1)$

$= \overline{w}^{2^{p-1}} (1 + w^{2^p}) \equiv 0 \pmod{M}$ [From (1)]

Conversely

let $r_{p-1} \equiv 0 \pmod{M}$

Now $w^{2^p} + 1 = w^{2^{p-1}} \cdot r_{p-1} \equiv 0 \pmod{M}$

i.e., $w^{2^p} \equiv -1 \pmod{M}$ …(2)

$\Rightarrow \quad w^{2^{p+1}} \equiv 1 (\text{mod } M) \qquad \ldots(3)$

Let τ be any divisor of M then (2) and (3) are also true for γ instead of M.

Now by definition, $M \equiv 2 (\text{mod } 5) \Rightarrow 5 \nmid M$

So if M is composite then only divisor of M are either of the form $5k \pm 1$ or $5k \pm 2$.

But M is of the form $5n + 2$ so M must have at least one prime divisor of the form $5k \pm 2$ say k.

Let $M = p_1 p_2 \ldots q_1 q_2 \ldots..$

where p_i's are primes of the form $5k + 1$ and q_j's are prime divisor of the form $5k \pm 2$.

Let τ be any divisor of M.

Consider $S = \{x \in N; w^x \equiv 1 (\text{mod } \tau)\}$

Then $S \neq \phi$ since on the observation made above $2^{p+1} \in S$.

Now divisor of 2^{p+1} are 2^p, 2^{p-1}, 2, 1 and since, $w^{2^p} \equiv -1 (\text{mod } \tau)$

so $2^p \notin S$

$\Rightarrow \quad \text{ord}_\tau^2 = 2^{p+1}$

By last theorem,

$$w^{p_i - 1} \equiv 1 (\text{mod } p_i)$$

and $$w^{q_j + 1} \equiv N(w) \equiv -1 (\text{mod } q_j)$$

$\Rightarrow \quad w^{2(q_j+1)} \equiv 1 (\text{mod } q_j)$

$\Rightarrow$ $p_i - 1$ and $2(q_j + 1)$ are multiplies of 2^{p+1} since, $\text{ord}_\tau^2 = 2^{p+1} \Rightarrow p_i = 2^{p+1} h_i + 1$

and $q_j = 2^p h_j - 1$

for some h_i & h_j. The first hypothesis is impossible since

$p_i > M = 2^p - 1$ and the second hypothesis is possible only if $k_j = 1$

$\Rightarrow \quad M = q_j$ is prime.

Unit-V

Arithmetical Functions and Prime Number Theory

Arithmatical Functions :-

Definition :- A function f defined for all natural numbers n is called an arithmetic function and generally we shall write an arithmatical function as f(n).

Definition :- An arithmatical function f(n) is called a multiplicative function if

$$f(n_1 n_2) = f(n_1) f(n_2) \text{ for } n_1, n_2 \in N \text{ \& } \gcd(n_1, n_2) = 1$$

Definition :- An arithmatical function is called strongly multiplicative if

$$f(n_1 n_2) = f(n_1) f(n_2) \ \forall \ n_1, n_2 \in N.$$

Mobius Function

Mobius function denoted by $\mu(n)$ is defined as

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^r \text{ if } n = p_1 p_2 \ldots p_r \text{ where } p_i\text{'s are distinct primes} \\ 0 & \text{otherwise, In this case n will be divisible by square of a prime number} \end{cases}$$

For example

$$\mu(1) = 1, \mu(2) = \mu(3) = -1, \mu(4) = 0, \mu(5) = -1 \ \mu(6) = 1$$

Theorem 5.1 $\mu(n)$ is a multiplicative function

Proof :- Let $n_1, n_2 \in N$, $\gcd(n_1, n_2) = 1$

It either $n_1 = 1$ or $n_2 = 1$, clearly $\mu(n_1 n_2) = \mu(n_1) \mu(n_2)$

So let $n_1 > 1$ & $n_2 > 1$

If any one of n_1, n_2 is not-square free then $n_1 n_2$ is also not square and then $\mu(n_1 n_2) = 0 = \mu(n_1) \cdot \mu(n_2)$

So assume both n_1 & n_2 are square free.

Let $n_1 = p_1 p_2 \ldots p_r$, where $p_1, p_2, \ldots p_r$ are distinct primes

& $n_2 = q_1 \cdot q_2 \ldots q_s$ where $q_1, q_2, \ldots, q_s$ are distinct primes.

Then by definition

$$\mu(n_1) = (-1)^r \ \& \ \mu(n_2) = (-1)^s$$

Since $\gcd(n_1, n_2) = 1$, so no p_i is equal to a q_j or vice-versa

Now $n_1 n_2 = p_1 p_2 \ldots p_r \, q_1 \cdot q_2 \ldots q_s$

and $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ are distinct primes

$\Rightarrow$ $\mu(n_1 n_2) = -1)^{r+s} = (-1)^r \cdot (-1)^s = \mu(n_1) \cdot \mu(n_2)$

Thus in all cases

$$\mu(n_1 n_2) = \mu(n_1) \cdot \mu(n_2)$$

whenever $\gcd(n_1, n_2) = 1$

$\Rightarrow \mu$ is multiplicative

Theorem 5.2 If f(n) is a multiplicative function & $f \not\equiv 0$. Then f(1) = 1

Proof :- Since $f \not\equiv 0$, $\exists\ n \in N$ such that $f(n) \neq 0$.

Now $f(n) = f(n \cdot 1)$

$= f(n) \cdot f(1)$, since $\gcd(n, 1) = 1$

$\Rightarrow$ $f(1) = 1$ since $f(n) \neq 0$.

Theorem 5.3 If f(n) is a multiplicative function so is $\sum_{d|n} f(d)$

Proof :- Set $g(n) = \sum_{d|n} f(d)$

If $f \equiv 0$ then so is g and so g(n) is multiplicative

Let $f \not\equiv 0$. Then f(1) = 1. So by definition g(1) = f(1) = 1. Let $n_1, n_2 \in N$, $\gcd(n_1, n_2) = 1$

If $n_1 = 1$ or $n_2 = 1$. Then clearly $g(n_1 n_2) = g(n_1) \cdot g(n_2)$

So let $n_1 > 1$, $n_2 > 1$

Let $d \mid (n_1 n_2)$. Then we can write $d = d_1 d_2$ where d_1 / n_1 & d_2 / n_2

If $d_1 \neq 1$ or $d_2 \neq 1$ then $d_1 \neq d_2$ since $(n_1, n_2) = 1$. Now by definition

$$g(n_1, n_2) = \sum_{d|(n_1 . n_2)} f(d)$$

$$= \sum_{\substack{d_1 | n_1 \\ d_2 | n_2}} f(d_1 d_2)$$

$$= \sum_{\substack{d_1 | n_1 \\ d_2 | n_2}} f(d_1)\, f(d_2) \qquad \text{[f is multiplicative]}$$

Since $(n_1, n_2) = 1 \Rightarrow \gcd(d_1, d_2) = 1$.

$$\Rightarrow \qquad g(n_1 n_2) = \sum_{\substack{d_1 | n_1 \\ d_2 | n_2}} f(d_1)\, f(d_2)$$

$$= \left(\sum_{d_1 | n_1} f(d_1) \right) \left(\sum_{d_2 | n_2} f(d_2) \right)$$

$$= g(n_1)\, g(n_2)$$

Hence g(n) is multiplicative

Theorem 5.4 $\sum_{d|n} \phi(d) = n$

Proof :- Set $g(n) = \sum_{d|n} \phi(d)$

Since $\phi(n)$ is a multiplicative function of n, so by previous theorem g(n) is also multiplicative. If $n = 1$ the $d = 1$, $\therefore\ g(1) = \phi(1) = 1$

So let $n > 1$

Let $n = p_1^{\alpha 1}\, p_2^{\alpha 2} \ldots p_r^{r r}$ be the prime factorization of n. …(1)

Then $g(n) = g(p_1^{\alpha 1}\, p_2^{\alpha 2} \ldots p_r^{r r})$

$$= g(p_1^{\alpha 1})\, g(p_2^{\alpha 2}) \ldots g(p_2^{\alpha 2}) \qquad \ldots(2)$$

since g(n) is multiplicative.

If we are able to prove $g(p^\alpha) = p^\alpha$ for every prime p & $\alpha \geq 1$. Then clearly using (1) & (2), we are through.

Now only divisors of p^α are $1, p, p^2, \ldots, p^\alpha$

$\therefore$ By definition $g(p^\alpha) = \sum_{d | p^\alpha} \phi(d)$

$$= \phi(1) + \phi(p) + \ldots + \phi(p^\alpha)$$

$$= 1 \ (p-1) + (p^2 - p) + \ldots + (p^\alpha - p^{\alpha-1})$$

$$= p^\alpha \qquad (\Theta\ \phi(p^n) = p^n - p^{n-1})$$

Hence the theorem.

Theorem 5.5 $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$

Proof :- Clearly for n = 1, we have

$$\sum_{d/1} \mu(d) = 1$$

So let n > 1

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{r_r}$ be the prime factorization of n.

Let $g(n) = \sum_{d/n} \mu(d)$

Now divisors of n are of the form

$$p_1^{\beta_1}, p_2^{\beta_2}, \ldots p_r^{\beta_r} \text{ where } 0 \le \beta_i \le \alpha_i$$

If any $\beta_i \ge 2$, $\mu(p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}) = 0$, since in this case $p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}$ is not square free. So while considering the divisors of n we leave out all those divisors which are divisible by a square.

So the only divisors to be considered are $1, p_1, p_2, \ldots, p_r, \; p_1 p_2, p_1 p_3, \ldots p_1 p_r, \; p_1 p_2 p_3 \ldots \; p_1 p_2 p_3 p_r$

$$\therefore \quad g(n) = \mu(1) + \sum_{i=1}^{r} \mu(p_i) + \sum_{\substack{1 \le i, j \le r \\ i \ne j}} \mu(p_i p_j) + \ldots + \mu(p_1 p_2 \ldots p_r)$$

$$= 1 - {}^rc_1 + {}^rc_2 - {}^rc_3 \ldots + (-1)^r$$

$$= (1-1)^r = 0. \text{ Hence Proved.}$$

Example :- Let n>1 & let n have r distinct prime divisors. Then $\sum_{d|n} |\mu(d)| = 2^r$

Proof :- From above theorem, we see that

$$\sum_{d|n} |\mu(d)| = \mu(1) + \sum_{i=1}^{r} |\mu(p_i)| + \sum_{i \le i, j \le r} |\mu(p_i, p_j)| + \ldots + |\mu(p_1 p_2 \ldots p_r)|$$

$$= 1 + {}^rc_1 + {}^rc_2 + \ldots + {}^rc_3$$

$$= (1+1)^r = 2^r \quad \text{Hence Proved.}$$

Divisor Function :- d(n)

Definition :- Let $n \geq 1$. We define divisor function of n(to be denoted by d(n)) as

$$\sum_{d|n} 1 = \text{Number of divisors of n (including 1 \& n)}$$

Clearly $d(1) = 1$ & $d(p) = 2$ for every prime p.

Theorem 5.6 Prove that d(n) is a multiplicative function. Find a formula for d(n)

Proof :- The function $f(n) \equiv 1$ is a multiplicative function and so

$$\sum_{d|n} f(d) = \sum_{d|n} 1 = d(n) \text{ is a multiplicative function.}$$

If $n = 1$, Clearly $d(1) = 1$. So let $n > 1$.

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ be the prime power decomposition of n.

Since d is a multiplicative function, so

$$d(n) = d(p_1^{\alpha_1} ... p_k^{\alpha_k}) = d(p_1^{\alpha_1}) d(p_2^{\alpha_2}) ... d(p_k^{\alpha_k})$$

So to find d(n), it is enough to find $d(p^{\alpha})$ where p is any prime & $\alpha \geq 1$

By definition

$$d(p^{\alpha}) = \sum_{d|p^{\alpha}} 1$$

Now only divisors of p^{α} are $1, p, p^2, \ldots p^{\alpha}$ which are $\alpha + 1$ in number

$\therefore$ $$d(p^{\alpha}) = \alpha + 1$$

$$d(n) = \prod_{i=1}^{k} (\alpha_i + 1)$$

Sum function :- $\sigma(n)$

Definition :- Let $n \geq 1$ be any natural number we define

$$\sigma(n) = \sum_{d|n} d = \text{sum of all divisors of n (including 1 \& n)}$$

Clearly $\sigma(1) = 1$ and $\sigma(p) = p + 1$

Further $\sigma(n) > n \ \forall \ n > 1$ since there are at least 2 divisors of n namely 1 and n.

Theorem 5.7 Prove that $\sigma(n)$ is a multiplicative function of n. Find a formula for $\sigma(n)$.

Proof :- Since $f(n) \equiv n$ is a multiplicative function of n, so

$$\sum_{d|n} f(d) = \sum_{d|n} d = \sigma(n) \text{ is a multiplicative function.}$$

To find a formula for $\sigma(n)$, we not

$$\sigma(1) = 1. \text{ Let } n > 1$$

Let $n = p_1^{\alpha_1} ... p_k^{\alpha_k}$ be the prime power decomposition of n. Since σ is multiplicative function, so

$$\sigma(n) = \sigma(p_1^{\alpha_1} ... p_k^{\alpha_k}) = \sigma(p_1^{\alpha_1}) \sigma(p_2^{\alpha_2}) ... \sigma(p_k^{\alpha_k})$$

So to find $\sigma(n)$ it is enough to find $\sigma(p^{\alpha})$ where p is any prime and $\alpha \geq 1$,

Now $\sigma(p^{\alpha}) = \sum_{d|p^{\alpha}} d$. The only divisors of p^{α} an 1, p, … p^{α}

$\therefore$ $$\sigma(p^{\alpha}) = 1 + p + \ldots + p^{\alpha}$$

$$= \frac{p^{\alpha+1} - 1}{p - 1}$$

$\therefore$ $$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

Example :- Evaluate $\sum_{n=1}^{\infty} \mu(\underline{|} n)$

Solution :- $$\sum_{n=1}^{\infty} \mu(\underline{|} n) = \mu(1) + \mu(\underline{|} 2) + \mu(\underline{|} 3) + ... + \mu(\underline{|} 4) + \ldots\ldots$$

$$= 1 - 1 + 1 + 0 = 1.$$

Example :- Prove that $\mu(n)\, \mu(n+1)\, \mu(n+2)\, \mu(n+3) = 0 \ \forall\ n \geq 1$

Solution :- Since n, n +1, n + 2, n + 3 are four consecutive integers and so at least one of them is divisible by 4 and consequently μ of that number is equal to zero and so

$$\mu(n)\ (n+1)\ \mu(n+2)\ \mu(n+3) = 0. \text{ Definition Euler function } \phi(n)$$

Theorem 5.8 Prove that $\phi(n)$ is a multiplicative function of n.

i.e. $\phi(m\, n) = \phi(m)\, \phi(n)$ whenever gcd (m, n) = 1

Proof :- If m = 1 or n = 1, clearly

$$\phi(m\, n) = \phi(m) \cdot \phi(n)$$

So let $m > 1, n > 1$

Now $\phi(n)$ by definition is the number of natural numbers which are $\leq n$ and coprime to n. So to find out $\phi(m\ n)$, we write first mn natural numbers in n rows and m columns as

1	2	3….……m
m + 1	m + 2	m + 3……..2m
……		
……		
(n−1)m+1	(n−1)m+2	(n−1)m+3……nm

Now consider any natural number 'a' such that $1 \leq a \leq mn$

Now gcd (a, mn) = 1 $\Leftrightarrow$ gcd (a, m) = 1 = gcd(a, n)

So let (a, m) = 1, Then there exists r ($1 \leq r < m$) such that gcd(r, m) = 1 & $a \equiv r \pmod m$, with $1 \leq r < m$. Then this r is in the first row of the configuration such that gcd(r, m) = 1.

But {1, 2,…,m} is the set of all natural numbers $\leq m$ and so by definition, the first row contains $\phi(m)$ natural numbers which are coprime to m.

So by what we have proved above, 'a' can occur in those and only columns which are headed by a natural number r ($1 \leq r < m$) such that gcd(r, m) = 1

Now consider r where $a \equiv r \pmod m$ gcd(r, m) = 1 & $1 \leq r < m$.

Consider all the natural numbers headed by r. These are of the form mx + r where $0 \leq x \leq n-1$. Now the set {0, 1, 2, …, n−1} is a complete set of residues (mod n) and so {mx + r; $0 \leq x \leq n-1$} is also a complete and so it contains a reduced set of residues (mod n) which contains exactly $\phi(n)$ numbers and all these numbers are co-prime to n.

But these are also coprime to m. So these $\phi(n)$ numbers are coprime to mn. But there are $\phi(m)$ choices for r and so there are $\phi(m)\ \phi(n)$ elements in this configuration which are relatively coprime to mn and so by definition

$$\phi(m\ n) = \phi(m) \cdot \phi(n).$$

Mobius Inversion Formula

Theorem 5.9 Let $F(n) = \sum_{d|n} f(d)$

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

Also prove its converse.

Proof :- Clearly $\sum_{d|n} F(d)\mu\left(\frac{n}{d}\right)$

$$= \sum_{d|n}\mu(d)F\left(\frac{n}{d}\right) \text{ since } d \mid n \Leftrightarrow \frac{n}{d} \mid n$$

So let us prove

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

By definition, $F\left(\frac{n}{d}\right) = \sum_{c\left|\frac{n}{d}\right.} f(c)$

$$\therefore \quad \sum_{d|n}\mu(d)F\left(\frac{n}{d}\right) = \sum_{d|n}\mu(d) \sum_{c\left|\frac{n}{d}\right.} f(c) = \sum_{c|n} f(c) \left(\sum_{d\left|\frac{n}{c}\right.} \mu(d) \right)$$

$$= f(n)\left(\sum_{d|1}\mu(d)\right) + \sum_{\substack{c|n \\ c<n}} f(c)\left(\sum_{d\,|\frac{n}{c}} \mu(d) \right)$$

Now $\sum_{d\left|\frac{n}{c}\right.} \mu(d) = 0$ if $n > c$

and $\sum_{d\left|\frac{n}{c}\right.} \mu(d) = 1 \Leftrightarrow \frac{n}{c} = 1 \Leftrightarrow n = c$

So inner sum $\sum_{d\left|\frac{n}{c}\right.} \mu(d)$ vanishes unless $n = c$ and in case $n = c$, $\sum_{d\left|\frac{n}{c}\right.} \mu(d) = 1$

$$\therefore \quad \sum_{d|n} \mu(d)\ F\left(\frac{n}{d}\right) = f(n)$$

Conversely

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

Now $$\sum_{d|n} f(d) = \sum_{d|n} \left(\sum_{\delta|d} \mu(\delta) F\left(\frac{d}{\delta}\right) \right)$$ (By definition)

$$= \sum_{d|n} \sum_{\delta|n} \mu(\delta) F\left(\frac{d}{\delta}\right)$$

$$= \sum_{d|n} \sum_{\gamma|n} \mu\left(\frac{d}{\gamma}\right) F(\gamma) \qquad \left(\text{Set } \frac{d}{\delta} = \gamma\right)$$

Since $\gamma \mid d$, set $d = \beta\gamma$, So

$$\sum_{d|n} f(d) = \sum_{\gamma|n} \sum_{\beta\gamma|n} \mu(\beta) F(\gamma)$$

$$= \sum_{\gamma|n} F(\gamma) \left(\sum_{\beta|\frac{n}{\gamma}} \mu(\beta) \right)$$

$$= F(n)$$

since $\sum_{\beta|\frac{n}{\gamma}} \mu(\beta) = 0$ for $\frac{n}{\gamma} > 1$

Theorem 5.10 Prove that $\sum_{d|n} \frac{\mu(d)}{d} = \frac{\phi(n)}{n}$

Proof :- We know $\sum_{d|n} \phi(d) = n$

Then $$\phi(n) = \sum_{d|n} \mu(d).\frac{n}{d}$$ (By Mobius Inversion formula)

i.e. $$\frac{\phi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}$$

For n = 1 exercise is true. So let $n > 1$

and $$\sum_{d|n} \frac{\mu(d)}{d} = f(n)$$

Since $\mu(n)$ is a multiplicative function of n.

$\Rightarrow$ $\sum_{d|n} \frac{\mu(d)}{d} = f(n)$ is a multiplicative function of n.

Let $n = p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k}$ be the prime power factorization of n.

then $f(n) = f(p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k})$

$= f(p_1^{\alpha_1})\, f(p_2^{\alpha_2})...f(p_k^{\alpha_k})$.

Let us compute $f(p^\alpha)$ where p is any prime & $\alpha \geq 1$

Now only divisors of p^α are 1, p, p^2,..,p^α

$\therefore$ $f(p^\alpha) = \sum_{d|p^\alpha} \frac{\mu(d)}{d}$

$= \mu(1) + \frac{\mu(p)}{p} + 0$ $\quad (\Theta\ \mu(p^i) = 0 \text{ for } i \geq 2)$

$= \left(1 - \frac{1}{p}\right) = \frac{p-1}{p}$

$= \frac{p^{\alpha-1}}{p^\alpha}(p-1) = \frac{p^\alpha - p^{\alpha-1}}{p^\alpha}$

$= \frac{\varphi(p^\alpha)}{p^\alpha}$

$\therefore$ $f(n) = \prod_{i=1}^{k} \varphi\frac{(p_i^{\alpha_i})}{p_i^{\alpha_i}}$

$= \frac{\varphi(p_1^{\alpha_1}\, p_2^{\alpha_2}...p_k^{\alpha_k})}{p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k}} = \frac{\varphi(n)}{n}$

Hence the result.

Example :- prove

$$\sum_{\substack{i=1 \\ \gcd(i,n)=1}}^{n} i = \frac{n\varphi(n)}{2}$$

Solution :- Let $S = \sum_{\substack{i=1 \\ \gcd(i,n)=1}}^{n} i = a_1 + a_2 + \ldots + a_{\phi(n)}$ where $1 \le a_i \le n$, $\gcd(a_i, n) = 1$

But $\gcd(a_i, n) = 1 \Leftrightarrow \gcd(n - a_i, n) = 1$

$\therefore$ $S = (n - a_1) + (n - a_2) + \ldots + (n - a_{\phi(n)})$

and $2S = n\,\phi(n) \Rightarrow S = \frac{n\varphi(n)}{2}$ $(n > 1)$

Now $\frac{n\varphi(n)}{2}$ is always an integer $\forall\ n > 1$

$\Rightarrow \phi(n)$ is even for all odd $n \cdot > 1$

A General Principle :- Let there be N objects. Suppose N_α of these have property α, N_β have property β …. Suppose $N_{\alpha\beta}$ have both of these property α & β; …$N_{\alpha\beta\gamma}$ have the property α, β, γ… and so on. Then the number of objects which do not have any of the properties α, β, γ;……. is

$$N - N_\alpha + \sum N_{\alpha\beta} - \sum N_{\alpha\beta\gamma} + \ldots\ldots \qquad \ldots(1)$$

and consequently the number of objects having at least one property is

$$\sum N_\alpha - \sum N_{\alpha\beta} + \sum N_{\alpha\beta\gamma} \ldots\ldots\ldots \qquad \ldots(2)$$

Proof :- If is enough to prove (1) since (2) can be obtained by subtracting (1) from N. Let A be any one of these N objects. Then A contributes 1 to the term N of (1). Let A possess exactly k of these properties. If k = 0, then A does not contribute to any of the terms $\sum N_\alpha$, $\sum N_{\alpha\beta}$, $\sum N_{\alpha\beta\gamma}$,…and so A contributes exactly one 1 to (1). Now let $k \ge 1$(k is finite).

Then A contributes 1 to N, 1 to exactly k of the terms in $\sum N_\alpha$, 1 to exactly k/2 of the terms $\sum N_{\alpha\beta}$ and so on.

So the total contribution of A to (1) is

$$1 - k + \binom{k}{2} - \binom{k}{3} + \ldots.$$

$$= (1-1)^k = 0$$

and this proves the theorem.

Application of General Principle

Theorem 5.11 Let $n > 1$ and let $n = p_1^{\alpha 1} . p_2^{\alpha 2} \ldots p_k^{\alpha k}$ where $p_1, p_2, \ldots, p_k$ are distinct prime then

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_k}\right)$$

Proof :- To find out $\phi(n)$, by definition, we have to find the natural numbers $\leq$ n which are not divisible by any of $p_1, p_2,\ldots, p_k$.

Let $N_{\alpha i}(i = 1, 2,\ldots k)$ be the number of integers $\leq$ n divisible by $p_i(i = 1, 2, \ldots k)$ $N_{\alpha_i \alpha_j}$ be the number of natural numbers $\leq$ n divisible by $p_i\, p_j$ $(1 \leq i, j \leq k, i \neq j)$ and so on.

Clearly

$N\alpha_i = \frac{n}{p_i}$. Infact the natural numbers $\leq$ n divisible by p_i are $\left\{p_i, 2p_i, .., \frac{n}{p_i} p_i\right\}$.

Similarly $N\alpha_i\, \alpha_j = \frac{n}{p_i p_j}$ and so on

$\therefore$ By General principle number of natural numbers $\leq$ n and not divisible by any of $p_1, p_2,\ldots, p_k$ is

$$\phi(n) = n - \sum\frac{n}{p_i} + \sum\frac{n}{p_i p_j} \ldots$$

$$= n \prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$$

Example :- The sum of the squares of the integers which are $\leq$ n and relatively coprime to n is $\frac{1}{3}n^2\phi(n) + \frac{1}{6}n\,(1-p_1)\,(1-p_2)\ldots(1-p_k)$ where $n > 1$ and $p_1, p_2,\ldots,p_k$ are the only distinct prime dividing n.

Solution :- To find out the required sum we shall find the sum of squares $\leq$ n and not coprime to n i.e. sum of squares $\leq$ n of those natural numbers which are divisible by at least one p_i.

By General principle, this sum is equal to

$$\sum N_\alpha - \sum N_{\alpha\beta} + \sum N_{\alpha\beta\gamma} \qquad \ldots(1)$$

Now sum of squares of numbers $\leq$ n and divisible by p_i is

$$(p_i)^2 + (2p_i)^2 + \ldots + \left(\frac{n}{p_i}.p_i\right)^2$$

The sum of squares of numbers ≤ n and divisible by $p_i\, p_j$ is

$$(p_i\, p_j)^2 + (2p_i\, p_j)^2 + \ldots + \left(\frac{n}{p_i p_j} . p_i\, p_j\right)^2$$

and so on

So the sum (1) is equal to

$$\sum_{i=1}^{k}\left[(p_i)^2 + (2p_i)^2 + \ldots + \left(\frac{n}{p_i}\cdot p_i\right)^2\right]$$

$$- \sum_{\substack{1\le i,\, j\le k \\ i\ne j}}\left[(p_i\, p_j)^2 + (2p_i\, p_j)^2 + \ldots + \left(\frac{n}{p_i\, p_j} p_i\, p_j\right)^2\right] + \ldots..$$

$$+ (-1)^{k-1}\left[(p_i\, p_2 \ldots p_k)^2 + (2p_i\, p_2 \ldots p_k)^2 + \ldots + \left(\frac{n}{p_1\, p_2 \ldots p_k}\cdot p_1\, p_2 \ldots p_k\right)^2\right] \ldots (2)$$

Now let d be any divisor of n. Then the sum of squares of natural numbers ≤ n & divisible by d is

$$d^2 + (2d)^2 + \ldots + \left(\frac{n}{d}\cdot d\right)^2 = d^2\left[1^2 + 2^2 + \ldots + \left(\frac{n}{d}\right)^2\right]$$

$$= d^2 \cdot \frac{1}{6}\cdot\frac{n}{d}\left(\frac{n}{d}+1\right)\left(\frac{2n}{d}+1\right)$$

$$= \frac{n^3}{3d} + \frac{n^2}{2} + \frac{nd}{6} \qquad \ldots (3)$$

From (3), sum (2) is equal to

$$\frac{n^3}{3}\left[\Sigma\frac{1}{p_i} - \sum_{\substack{1\le i,\, j\le k \\ i\ne j}}\frac{1}{p_i p_j} + \ldots + (-1)^{k-1}\frac{1}{p_1 p_2 \cdots p_k}\right]$$

$$+ \frac{n^2}{2}\left[\sum_{i=1}^{k} 1 - \sum_{\substack{1\le i,\, j\le k \\ i\ne j}} 1 + \ldots + (-1)^{k-1}\right]$$

$$+ \frac{n}{6}[\sum p_i - \sum p_i p_j + \ldots + (-1)^{k-1} p_1 p_2 \ldots p_k] \qquad \ldots(4)$$

But the sum of squares of natural numbers ≤ n is

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

∴ Sum of squares of natural numbers ≤ n & coprime to n is

$$\frac{n^3}{3}\left[1 - \Sigma\frac{1}{p_i} + \Sigma\frac{1}{p_i p_j} + \ldots + (-1)^k \frac{1}{p_1 p_2 \cdots p_k}\right]$$

$$+ \frac{n^2}{2}\left[1 - k + \binom{k}{2} \ldots + (\phi - (-1)^k\right]$$

$$+ \frac{n}{6}[1 - \sum p_i + \sum p_i p_j \ldots + (-1)^k p_1 p_2 \ldots p_k]$$

$$= \frac{n^3}{3}\Pi\left(1 - \frac{1}{p_i}\right) + \frac{n^2}{2}(1-1)^k + \frac{n}{6}\prod_{i=1}^{k}(1 - p_i)$$

$$= \frac{1}{3} n^2 \phi(n) + \frac{n}{6}\prod_{i=1}^{k}(1 - p_i) \qquad \left| \; n \cdot \prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right) = \phi(n)\right.$$

Example :- Find the sum of the cubes of the integers ≤ n and relatively coprime to n. (n > 1)

Solution :- Let x be any natural number ≤ n and coprime to n.

Let $S = \sum x^3 = \sum (n-x)^3$

$$= \sum (n^3 - 3n^2 x + 3nx^2 - x^{3)}$$

$$2S = 2\sum x^3 = \sum n^3 - 3n^2 \sum x + 3n \sum x^2 = n^3 \phi(n) - 3n^2 \frac{n\varphi(n)}{2}$$

$$+ 3n\left(\frac{1}{3} n^2 \varphi(n) + \frac{n}{6}\Pi(1 - p_i)\right)$$

$$= n^3 \phi(n) - \frac{3}{2} n^3 \phi(n) + n^3 \phi(n) + \frac{1}{2} n^2 \Pi (1 - p_i)$$

$$= \frac{1}{2} n^3 \phi(n) + \frac{1}{2} n^2 \prod (1-p_i)$$

Perfect Numbers

Definition :- A natural number n is called a perfect number if $\sigma(n) = 2n$

For example 6 & 28 are perfect numbers.

as $\sigma(6) = 1+ 2 + 3 + 6 = 12 = 2.6$

$\sigma(28) = 1+ 2 + 4+ 7+ 14 + 28 = 56 = 2.28$

Theorem 5.12 If $2^{n+1}-1$ is a prime number then

$m = 2^n(2^{n+1}-1)$ is perfect.

Proof :- we have

$\sigma(2^n (2^{n+1}-1) = \sigma(2^n)\, \sigma(2^{n+1}-1)$

$= (1 + 2 +\ldots+ 2^n)\, (1+2^{n+1}-1)$ [Θ $\gcd(2^n, 2^{n+1}-1) = 1$]

$= (2^{n+1}-1)\, 2^{n+1}$

$= 2 \cdot 2^n.(2^{n+1}-1) = 2m$

Remark :- All the known perfect numbers are even. We don't know any odd perfect number and neither it has been proved that all perfect numbers. must be even.

Theorem 5.13 Every even perfect number must be of the form $2^n(2^{n+1}-1)$ where $2^{n+1}-1$ is a prime number.

Proof :- To prove the theorem, we first prove a lemma.

Lemma :- let $\sigma(m) = m\,\lambda$ where $1 \le \lambda < m$ & $\lambda \mid m$. Then $\lambda = 1$ and m is a prime number.

Proof of Lemma :- If possible, let $\lambda > 1$, then since $\lambda \mid m$ & $1 < \lambda < m$, so m has at least three divisors 1, λ & m

$\therefore$ $\sigma(m) \ge \lambda + m + 1$, which contradicts the hypothesis that $\sigma(m) = \lambda + m$

So $\lambda = 1$, then $\sigma(m) = m + 1$. Then m can have only two divisors 1 & m and so m must be a prime number.

Proof of Theorem :- Let k be a given even perfect number. Then k is of the form

$k = 2^n.\, m$ where $n \ge 1$ & m is odd (we can not have $k = 2^n$ since $\sigma(2^n) = 2^{n+1}-1 \ne 2.2^n$) …(1)

Let $\sigma(m) = m + \lambda$ where $\lambda \geq 1$

Now k is perfect, so

$$2^{n+1} \cdot m = 2 \cdot (2^n m) = 2k = \sigma(k)$$

$$= \sigma(2^n \cdot m) = \sigma(2^n)\, \sigma(m)$$

$$= (2^{n+1} - 1)\,(m + \lambda)$$

$$= 2^{n+1} m - m + \lambda\,(2^{n+1} - 1).$$

$$\Rightarrow \qquad m = \lambda(2^{n+1} - 1) \qquad \ldots(2)$$

$$\Rightarrow \qquad \lambda = \frac{m}{2^{n+1} - 1} \Rightarrow \lambda \mid m$$

Also $n \geq 1 \Rightarrow \lambda < m \Rightarrow 1 \leq \lambda < m$ & $\lambda \mid m$.

So by the lemma, $\lambda = 1$ & m is a prime number. Setting $\lambda = 1$ in (2) we get

$$m = 2^{n+1} - 1$$

and from (1)

$$k = 2^n(2^{n+1} - 1)$$

Example :- Prove that $\cdot(24m - 1) = 0 \pmod{24}\ \forall\ m \geq 1$

Solution :- we know $24 = 3 \cdot 8$

To prove the result, we shall in fact prove a little more. To be precise, we shall prove

(i) $\sigma(3m - 1) \equiv 0 \pmod 3$

(ii) $\sigma(8m - 1) \equiv 0 \pmod 8$.

(i) Let $n = 3m - 1$. Then $n \equiv -1 \equiv 2 \pmod 3$

So n can not be a perfect square since $k^2 \equiv 0$ or $1 \pmod 3$ for any natural number k.

So $d \mid n \Leftrightarrow \frac{n}{d} \mid n$ & $d \neq \frac{n}{d}$

Also $3 \nmid n$

$\therefore$ We write

$$\sigma(3m-1) = \sum_{\substack{d|n \\ d\neq\frac{n}{d} \\ 1\le d<\sqrt{n}}} \left(d+\frac{n}{d}\right) = \sum_{\substack{d|n \\ 1\le d<\sqrt{n} \\ d\neq\frac{n}{d}}} \left(\frac{d^2+n}{d}\right)$$

Since $3 \nmid n \Rightarrow 3 \nmid d \Rightarrow d^2 \equiv 1 (\text{mod } 3)$

$\Rightarrow \quad d^2 + n \equiv 0 (\text{mod } 3)$

Since $3 \nmid d$, $\left(d+\frac{n}{d}\right) \equiv 0 \text{ (mod 3)} \Rightarrow \frac{d^2+n}{d} \equiv 0 \text{ (mod 3)}$ for every divisor d of n, where $1 \le d < \sqrt{n}$

$\Rightarrow \quad \sigma 3m-1) \equiv 0 (\text{mod } 3)$

(ii) Let $n = 8m - 1 \Rightarrow n \equiv -1 \equiv 7 \text{ (mod 8)}$

Then $2 \nmid n$ and so every divisor d of n must be odd

$\Rightarrow d^2 \equiv 1 (\text{mod } 8)$ for every divisor d of n. Further n is not a perfect square since every odd square number must be $\equiv 1 (\text{mod } 8)$

Now $$\sigma(n) = \sigma(8m-1) = \sum_{\substack{d|n \\ d\neq\frac{n}{d} \\ 1\le d<\sqrt{n}}} \left(d+\frac{n}{d}\right) = \sum_{\substack{d/n \\ 1\le d<\sqrt{n}}} \frac{d^2+n}{d}$$

Since $2 \nmid d \Rightarrow d^2 \equiv 1 (\text{mod } 8)$

$\Rightarrow \quad d^2 + n \equiv 0 \text{ (mod 8) and } \frac{d^2+n}{d} \equiv 0 \text{ (mod 8)}$

$\Rightarrow \quad \sigma(n) \equiv 0 \text{ (mod 8)}$

Combining (i) & (ii) we get

$$\sigma(24m-1) \equiv 0 \text{ (mod 24)}$$

By similar methods we can prove

$$\sigma(4m-1) \equiv 0 (\text{mod } 4)$$

and $$\sigma(12m-1) \equiv 0 \text{ (mod 12)}$$

i.e. $$\sigma(48m-1) \equiv 0 (\text{mod } 48)$$

Example :- $$\sum_{m \mid n} d^3(m) = \left[\sum_{m \mid n} d(m)\right]^2$$

Solution :- Let $f(n) = \sum_{m|n} d^3(m)$

and $$g(n) = \left[\sum_{m|n} d(m)\right]^2$$

Clearly exercise is true for n = 1. So let n > 1

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ be the prime power decomposition of n.

Since d(n) is a multiplicative function of n.

So $d^3(n) = (d(n))^3$ is also a multiplicative function of n and so

$f(n) = \sum_{m|n} d^3(m)$ is also a multiplicative function.

Further $\sum_{m|n} d(m)$ is also a multiplicative function since d(n) is a multiplicative function and so

$$g(n) = \left[\sum_{m|n} d(m)\right]^2$$

is also a multiplicative function of n

So to prove f(n) = g(n), it is enough to prove

$$f(p^\alpha) = g(p^\alpha) \text{ for every prime } p \ \& \ \alpha \geq 1$$

Now $f(p^\alpha) = \sum_{m|p^\alpha} d^3(m)$

The only divisors of p^α are $1, p, p^2, \ldots, p^\alpha$

$\therefore \quad f(p^\alpha) = d^3(1) + d^3(p) + d^3(p^2) + \ldots + d^3(p^\alpha)$

$$= 1^3 + 2^3 + 3^3 + \ldots + (\alpha+1)^3 \qquad (\Theta\ d(i) = i + 1$$

$$= \left[\frac{(\alpha+1)(\alpha+2)}{2}\right]^2$$

= square of the sum of first $(\alpha + 1)$ natural numbers

i.e. $$[1 + 2 + \ldots + (\alpha+1)]^2$$

$$= [d(1) + d(p) + \ldots + d(p^\alpha)]^2$$

$$= g(p^\alpha).$$

Example :- For every natural number n > 1,

where $p_1, p_2, \ldots, p_k$ are the only prime divisors of n and f(n) is a multiplicative function of n.

Solution :- Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ be the prime power decomposition of n

Since $\mu(n)$ is a multiplication of n and f(n) is a multiplicative function of n

$\Rightarrow \mu(n) f(n)$ is a multiplicative function of n.

$\Rightarrow \sum_{d \mid n} \mu(d) f(d)$ is a multiplicative function of n

So to evaluate $\sum_{d \mid n} \mu(d) f(d)$, we evaluate $\sum_{d \mid p^{\alpha}} \mu(d) f(d)$ where p is a prime & $\alpha \geq 1$

Now only divisors of p^{α} are $1, p, p^2, \ldots, p^{\alpha}$

$$\therefore \sum_{d/p^{\alpha}} \mu(d) f(d) = \mu(1) f(1) + \mu(p) f(p) + \mu(p^2) f(p^2) + \ldots + \mu(p^{\alpha}) \& (p^{\alpha})$$

$$= 1 - f(p) \qquad (\Theta\ \mu(p^i) = 0\ \forall\ i \geq 2)$$

$$\therefore \sum_{d \mid n} \mu(d) f(d) = \prod_{i=1}^{k} (1 - f(p_i))$$

Corollary :- If f(n) = d(n). Then $d(p_i) = 2$

$$\Rightarrow \sum_{d \mid n} \mu(d) \tau(d) = (-1)^k$$

$$\sum_{d \mid n} \mu(d) \sigma(d) = \prod_{i=1}^{k} (1 - \sigma(p_i))$$

$$= (-1)^k p_1 p_2 \ldots p_k.$$

Example :- Prove that $\sigma(n)$ is odd $\Leftrightarrow n = m^2$ or $2m^2$

Proof :- Let n = 1. Then $\sigma(1) = 1$

Let $n > 1$ and $n = 2^r p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ where $r > 0$ & $p_1, p_2, \ldots, p_k$ are distinct odd primes.

Now $\sigma(n) = \sigma(2^r)\, \sigma(p_1^{\alpha_1}) \sigma(p_2^{\alpha_2}) \ldots \sigma(p_k^{\alpha_k})$

$$= (2^{r+1} - 1)\, (1 + p_1 + p_1^2 + \ldots + p_1^{\alpha_1}) \ldots (1 + p_k + p_k^2 + \ldots + p_k^{\alpha_k}) \ldots (1)$$

Now $\sigma(n)$ is odd $\Leftrightarrow$ Each factor on R.H. S of (1) is odd. But $(2^{r+1} - 1)$ is odd $\forall$ $r \geq 0$

However if α_i is odd for some i ($1 \le i \le k$) then $1 + p_i + p_i^2 + ... + p_i^{\alpha_i}$ is even, since number of terms in the sum is even while each term is odd.

$\therefore$ $\sigma(n)$ is odd $\Leftrightarrow$ each α_i is even. If r is also even, $n = m^2$ for some m and r is odd $n = 2m^2$ for some m.

Example :- Prove that $\sum_{d \mid n} (-1)^{d-1} \phi\left(\frac{n}{d}\right)$ = n or 0 according as n is odd or n is even.

Solution :- Let n be odd. Then each divisor d of n is odd and so d−1 is even

$$\Rightarrow \quad (-1)^{d-1} = 1 \text{ and } \sum_{d \mid n} (-1)^{d-1} \phi\left(\frac{n}{d}\right) = \sum_{d \mid n} \phi\left(\frac{n}{d}\right) = \sum_{d \mid n} \phi(d) = n$$

So let n be even and $n = 2^r p_1^{\alpha 1} p_2^{\alpha 2} ... p_k^{\alpha k}$ be the prime power decomposition of n.

$$\therefore \sum_{d \mid n} (-1)^{d-1} \phi\left(\frac{n}{d}\right) = \sum_{\substack{d \mid n \\ d \text{ is odd}}} \phi\left(\frac{n}{d}\right) - \sum_{\substack{d \mid n \\ d \text{ is even}}} \phi\left(\frac{n}{d}\right) = \sum_{\substack{d \mid n \\ d \text{ odd}}} \phi(d) - \sum_{\substack{d \mid n \\ d \text{ even}}} \phi(d) = n - n = 0$$

Order of Magnitude and Average Order :- d(n), σ(n) & ϕ(n).

Order of magnitude is simply how Large or how small is the magnitude of the function

We know d(1) = 1 & $d(n) \ge 2 \ \forall \ n \ge 2$.

Further d(p) = 2 for all primes p

Definition :- Let f(n) & g(n) be two functions of n.

(1) We say $f(n) = o(g(n))$

if $\lim_{n \to \infty} \frac{f(n)}{g(n)} = 0$

(2) We say $f(n) = O(g(n))$

if $\exists$ a positive constant A such that $|f(n)| < A\, g(n)$

(3) We say $f(n) \sim g(n)$

if $\lim_{n \to \infty} \frac{f(n)}{g(n)} = 1$

Remark :- If $f(n) = o(g(n))$

then $f(n) = O(g(n))$

and if $f(n) \sim g(n)$ even then

$$f(n) = O(g(n))$$

Some rules for addition

(1) $o(n) + o(n) = o(n)$

(2) $O(n) + O(n) = O(n)$

(3) $o(n) + O(n) = O(n)$

(4) $O(f(n)) + O(g(n)) = O[f(n) + g(n)]$

Theorem 5.14 $d(n) = O(n^s)$ for all positive δ, (δ however small)

Proof :- We know if $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$

Then $$d(n) = \prod_{i=1}^{k} (a_i + 1)$$

$\therefore$ $$\frac{d(n)}{d^{\delta}} = \prod_{i=1}^{r} \left(\frac{a_i + 1}{p_i^{a_i \delta}} \right)$$

$$= \prod_{p_i < 2^{1/\delta}} \left(\frac{a_i + 1}{p_i^{a_i \delta}} \right) \prod_{p_i \geq 2^{1/\delta}} \left(\frac{a_i + 1}{p_i^{a_i \delta}} \right)$$

Now for $p \geq 2^{1/s}$, $p^{\delta} \geq 2$, so

$$\frac{a+1}{p^{a\delta}} = \frac{a+1}{(p^{\delta})^a} \leq \frac{a+1}{2^a} \leq 1 \qquad \forall\ a$$

Also for all p,

$$a\,\delta \log 2 \leq e^{a\delta \log 2} = 2^{a\delta} \leq p^{a\delta} \qquad (\Theta\ 2 \leq p)$$

$\therefore$ $$\frac{a+1}{p^{a\delta}} = \frac{1}{p^{a\delta}} + \frac{a}{p^{a\delta}} \leq 1 + \frac{1}{\delta \log 2}$$

$$\leq \exp\left(\frac{1}{\delta \log 2} \right)$$

Using the above estimate for $p_i < 2^{1/\delta}$,

We get $$\frac{d(n)}{n^{\delta}} \leq \prod_{p_i < 2^{1/\delta}} \frac{a_i + 1}{p_i^{a_i \delta}} \leq \prod_{p_i < 2^{1/\delta}} \exp\left(\frac{1}{\delta \log 2} \right)$$

$$< \exp\left(\frac{2^{1/\delta}}{\delta \log 2}\right) = O(1)$$

$\therefore$ $\quad d(n) = O(n^{\delta})$.

Definition :- If f(n) and g(n) are two arithmetic functions of n, then we say f(n) is a average order of g(n) if $f(1) + f(2) + \ldots + f(n) \sim g(1) + g(2) + \ldots + g(n)$

Example :- Let us see when f(n) is of average order of n.

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

Thus if $f(n) \sim \frac{1}{2}n^2$, then f(n) is of average order of n

Theorem 5.15 d(n) is of average order of log n. In fact $d(1) + d(2) + \ldots + d(n) \sim n \log n$

Proof :- First we prove

$$\log (1) + \log (2) + \ldots + \log n \sim n \log n$$

Now $\quad \log (1) + \log (2) + \ldots + \log n$

$$= 1 \cdot \log 1 + 1 \cdot \log 2 + \ldots + 1 \cdot \log n$$

$$\sim \int_1^2 \log t \, dt + \int_2^3 \log t \, dt + \ldots + \int_n^{n+1} \log t \, dt$$

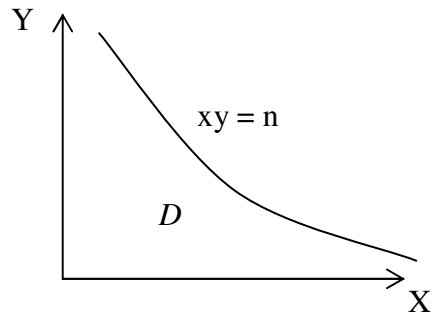
$$= \int_1^{n+1} \log t \, dt = \left[t \log t - t\right]_1^{n+1}$$

$$= (n + 1) \log (n+1) - n$$

$$\sim n \log n$$

Now to prove the theorem it is enough to prove

$$d(1) + d(2) + \ldots + d(n) \sim n \log n.$$



Consider the lattice whose vertices (x, y) are the points in the xy-plane with integral co-ordinates. Denote by *D* the region in the upper right hand corner contained between the rectangular axes & the rectangular hyperbola

xy = n leaving out the coordinate axes and counting the lattice points on the rectangular hyperbola.

We count the lattice point in this region in two different ways.

Let (x, y) be any lattice point in this region. Then x y ≤ n and xy is a natural number and so this lattice point lies on one of the rectangular hyperbolas xy = δ, where $1 \le \delta \le n$. Then total number of lattice points in this region will be

$$d(1) + d(2) + \ldots + d(n)$$

Also the number of lattice points in this region with x-coordinate equal to 1 will be $a = \left[\frac{n}{1}\right]$,

the number of lattice points in this region with x-coordinate equal to 2 will be $a = \left[\frac{n}{2}\right]$

……
……

∴ Total number of lattice points in this region will be

$$[n] + \left[\frac{n}{2}\right] + \left[\frac{n}{3}\right] + \ldots + \left[\frac{n}{n}\right]$$

∴ $d(1) + d(2) + \ldots + d(n)$

$$= [n] + \left[\frac{n}{2}\right] + \ldots + \left[\frac{n}{n}\right]$$

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

$$= n\left(1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}\right) + O(n)$$

$$= n\left(\log n + \gamma + O\left(\frac{1}{n}\right)\right) + O(n) \quad \text{(by Sterling formula)}$$

$$= n \log n + n\gamma + O(1) + O(n)$$

$$= n \log n + O(n) \sim n \log n$$

Theorem 5.16 Prove that

$$d(1) + d(2) + \ldots + d(n) = n \log n + (2\gamma - 1)\, n + O(\sqrt{n})$$

where γ is the Sterlings constant.

Proof :- Let D denote the region as defined in the previous theorem. Then we have already prove in previous then that the number of lattice points in this region is

$$d(1) + d(2) + \ldots + d(n)$$

Set $u = [\sqrt{n}\,] = \sqrt{n} + O(1)$

$\therefore$ $u^2 = (\sqrt{n} + O(1))^2 = n + O(\sqrt{n}) + O(1) = n + O(\sqrt{n})$

$= n + O(u)$

So $\log u = \log(\sqrt{n} + O(1)) = \log\left(\sqrt{n}\left(1 + O\left(\frac{1}{\sqrt{n}}\right)\right)\right)$

$$= \log(\sqrt{n}) + \log\left(1 + O\left(\frac{1}{\sqrt{n}}\right)\right)$$

$$= \log(\sqrt{n}) + O\left(\frac{1}{\sqrt{n}}\right)$$

$$= \frac{1}{2}\log n + O\left(\frac{1}{\sqrt{n}}\right) = \log u + O\left(\frac{1}{u}\right)$$

We know that the lattice points (x, y) with $x \neq 0$ & $y \neq 0$ is equal to

$$d(1) + d(2) + \ldots + d(n)$$

Since $x \neq 0$ and $y \neq 0$, the lattice points (x, y) be on the line $x = 1$, $x = 2$,… and $y = 1$, $y = 2$,….

Let A B C D be the square determined by the vertices (1, 1), (1, u), (u, u) & (u, 1). By symmetry the number of lattice points in the region ABCHGDA = number of lattice points in the region ADEFGBA

Since $[\sqrt{n}\,] = u$, there is no lattice point in the small triangle FGH.

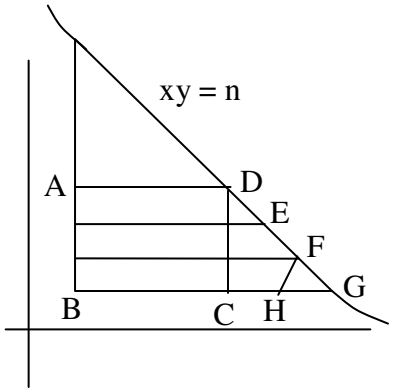
Further (square ABCD) ≤ Region (ABCHGDA) and Square (ABCD) ≤ Region (ABEFGDA).

∴ If we count the points on the lines x = 1, x = 2,… & y = 1, y = 2,…, the lattice points in the square ABCD are counted twice.

The number of lattice points in the square ABCD including on the boundary is equal to u^2

∴ Number of lattice points in the region under consideration = 2(number of Lattice points in the region ABCHGDA)– u^2

But as in the first part of the proof number of Lattice points in the region ABCHGDA



$$= \left[\frac{n}{1}\right] + \left[\frac{n}{2}\right] + \ldots + \left[\frac{n}{u}\right]$$

$$\therefore \quad \sum_{i=1}^{n} d(i) = 2\left(\left[\frac{n}{1}\right] + \left[\frac{n}{2}\right] + \ldots + \left[\frac{n}{4}\right]\right) - u^2.$$

But $$\left[\frac{n}{1}\right] + \left[\frac{n}{2}\right] + \ldots + \left[\frac{n}{u}\right] = \frac{n}{1} + \frac{n}{2} + \ldots + \frac{n}{u} + O(u)$$

$$\therefore \quad \sum_{i=1}^{n} d(i) = 2n\left(1 + \frac{1}{2} + \ldots + \frac{1}{u}\right) - u^2$$

$$= 2n\left(\log u + \gamma + O\left(\frac{1}{u}\right)\right) - u^2$$

$$= 2n \log u + 2n\gamma + O(u) - n + O(u)$$

$$= 2n\left(\frac{1}{2}\log n + O\left(\frac{1}{u}\right)\right) + (2\gamma - 1)n + O(u)$$

$$= n \log n + O(u) + (2\gamma - 1)n + O(u)$$

$$= n \log n + (2\gamma - 1)\, n + O(\sqrt{n}\,)$$

Magnitude and average order of σ(n).

We know σ(p) = p+1 and number of primes is infinite so all we can say about magnitude of σ(n) is σ(n) > n for n ≥ 2.

Theorem 5.17 The average order of σ(n) is $\frac{1}{6}\pi^2 n$, More precisely

$$\sigma(1) + \sigma(2) + \ldots + \sigma(n) = \frac{1}{12}\pi^2 n^2 + O(n \log n)$$

Proof :- Let as before, *D* be the region bounded by x-axis, y-axis & the rectangular hyperbola xy =n.

If x is a divisor of n, then ∃ a lattice point (x, y) lying in this region. Then this point will lie on one of the lines y = 1, y = 2, and xy ≤ n.

$\therefore$ $$\sum_{i=1}^{n} \sigma(i) = \sum_{x=1}^{n} \sum_{1 \le y \le \left[\frac{n}{x}\right]}^{n} y$$

$$= \frac{1}{2} \sum_{x=1}^{n} \left[\frac{n}{x}\right]\left(\left[\frac{n}{x}\right] + 1\right)$$

But $$\left[\frac{n}{x}\right] = \frac{n}{x} + O(1$$

$\therefore$ $$\sum_{i=1}^{n} \sigma(i) = \frac{1}{2} \sum_{x=1}^{n} \left(\frac{n}{x} + O(1)\right)\left(\frac{n}{x} + O(1)\right)$$

$$= \frac{1}{2} \sum_{x=1}^{n} \left(\frac{n^2}{x^2} + O\left(\frac{n}{x}\right) + O(1)\right)$$

$$= \frac{1}{2} n^2 \sum_{x=1}^{n} \frac{1}{x^2} + O\left(n \sum_{x=1}^{n} \frac{1}{x}\right) + O(n)$$

But $$\sum_{x=1}^{n} \frac{1}{x^2} = \sum_{x=1}^{\infty} \frac{1}{x^2} + O\left(\frac{1}{n}\right) = \frac{\pi^2}{6} + O\left(\frac{1}{n}\right)$$

and $$\sum_{x=1}^{n} \frac{1}{x} = \log n + 0\left(\frac{1}{n}\right).$$

$$\therefore \quad \sum_{i=1}^{n}\sigma(i) = \frac{1}{2}n^2\left(\frac{\pi^2}{6}+O\left(\frac{1}{n}\right)\right)+O\left(n\left(\log n+O\left(\frac{1}{n}\right)\right)\right)+O(n)$$

$$= \frac{1}{12}\pi^2 n^2 + O(n) + O(n \log n) + O(n)$$

$$= \frac{1}{12}\pi^2 n^2 + O(n \log n)$$

Magnitude and Average order of $\phi(n)$.

We know if $n > 1$, $\phi(n) < n$ On the other hand if $n = p^m$ and $p > 1/\varepsilon$ where $\varepsilon > 0$ is given

then $$\phi(n) = n\left(1-\frac{1}{p}\right) > n(1-\varepsilon)$$

$$\therefore \quad \frac{\varphi(n)}{n} > 1-\varepsilon \Rightarrow \overline{\lim}\,\frac{\varphi(n)}{n} = 1$$

Theorem 5.18 There exists a constant A, such that

$$A < \frac{\sigma(n)\varphi(n)}{n^2} < 1 \text{ for all } n > 1$$

Proof :- Let $n = \prod_p p^{\alpha}$, then we know

$$\sigma(n) = \prod_{p\mid n}\frac{p^{\alpha+1}-1}{p-1} = \prod_{p\mid n}\frac{p^{\alpha+1}\left(1-\frac{1}{p^{\alpha+1}}\right)}{p\left(1-\frac{1}{p}\right)} = \prod_{p\mid n}\frac{p^{\alpha}(-1p^{-\alpha-1})}{(1-p^{-1})}$$

$$= n\prod_{p\mid n}\frac{1-p^{\alpha-1}}{1-p^{-1}}$$

Also we know $\phi(n) = n\prod_{p\mid n}(1-p^{-1})$

$$\sigma(n)\,\phi(n) = n^2\prod_{p\mid n}1-p^{-\alpha-1}$$

$$\therefore \quad \frac{\sigma(n)\phi(n)}{n^2} = \prod_{p\mid n}(1-p^{-\alpha-1}) < 1.$$

Now for $\alpha \geq 1$, $p^2 \leq p^{\alpha+1}$

$$\Rightarrow \qquad \frac{1}{p^{\alpha+1}} \leq \frac{1}{p^2}$$

$$\Rightarrow \qquad 1-\frac{1}{p^{\alpha+1}} \geq 1-\frac{1}{p^2}$$

$$\therefore \qquad \frac{\sigma(n)\phi(n)}{n^2} = \prod_{p \mid n} (1-p^{-\alpha-1}) \geq \prod_{p \mid n}\left(1-\frac{1}{p^2}\right)$$

$$\geq \prod_{p}\left(1-\frac{1}{p^2}\right)$$

$$\geq \prod_{k=1}^{\infty}\left(1-\frac{1}{k^2}\right)$$

We know that the series $\sum a_n$ and the infinite product $\Pi(1-a_n)$ converge or diverge together

But $\sum \frac{1}{k^2}$ is convergent $\quad \Rightarrow \quad \prod_{k=1}^{\infty}\left(1-\frac{1}{k^2}\right)$ is also convergent]

So there exists a constant A such that

$$A < \frac{\sigma(n)\varphi(n)}{n^2} < 1.$$

Theorem 5.19 The average order of $\phi(n)$ is $\frac{6n}{\pi^2}$

In fact $\qquad \Phi(n) = \phi(1) + \phi(2) + \ldots + \phi(n) = \frac{3n^2}{\pi^2} + O(n \log n)$

Proof :- We have already prove $\sum_{d \mid n} \phi(d) = n$

So by Mobius inversion formula,

$$\Phi(n) = \sum_{m=1}^{n} \varphi(m) = \sum_{dd \leq n} d' \mu(d)$$

$$= \sum_{d=1}^{n} \mu(d) \cdot \sum_{d=1}^{\left[\frac{n}{d}\right]} d$$

$$= \frac{1}{2}\sum_{d=1}^{n}\mu(d)\left(\left[\frac{n}{d}\right]^2 + \left[\frac{n}{d}\right]\right) = \frac{1}{2}\sum_{d=1}^{n}\mu(d)\left(\left(\frac{n}{d}+O(1)\right)^2 + \left[\frac{n}{d}\right]\right)$$

$$= \frac{1}{2}\sum_{d=1}^{n}\mu(d)\left[\frac{n^2}{d^2}+O\left(\frac{n}{d}\right)\right]$$

$$= \frac{1}{2}n^2\sum_{d=1}^{n}\frac{\mu(d)}{d^2}+O\left(n\sum_{d=1}^{n}\frac{1}{d}\right)$$

But we know that

$$\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2} \text{ converges to } 6/\pi^2$$

$$\therefore \quad \Phi(n) = \frac{1}{2}n^2\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}+O\left(n\sum_{d=1}^{n}\frac{1}{d}\right) = \frac{1}{2}n^2\left[\frac{6}{\pi^2}+O\left(\frac{1}{n}\right)\right]O(n\log n)$$

$$= \frac{3n^2}{\pi^2} + O(n\log n)$$

Remark :- We know that the number of terms in Farey series function of order n is

$$1 + \sum_{i=1}^{n}\phi(i) = 1+\Phi(n)$$

$\therefore$ We get the number of terms in the Farey series of order n is approximately $\frac{3n^2}{\pi^2}$ for large n.

Thus an alternative statement of the last theorem is that the number of terms in Farey series of order n is approximately $3n^2/\pi^2$.

Theorem 5.20 The probability that the two given integers should be coprime to each other is $\frac{6}{\pi^2}$.

Proof :- Consider the pair of integers (p, q). Let $1 \le p \le q \le n$.

Now also consider the corresponding fraction $\frac{p}{q}$. For every n, there are almost n fractions. $\frac{p}{q}$ with $1 \le p \le q \le n$.

$\therefore$ Total number of such fractions with all $\frac{p}{q}(1 \le p \le q \le n)$ is $\sum_{i=1}^{n} i = \frac{1}{2}n(n+1) \sim \frac{1}{2}n$

But the number of fractions $\frac{p}{q}$, where $1 \le p \le q \le n$ and gcd(p, q) = 1 is $3n^2 / \pi^2$ for large n.

$\therefore$ Probability $= \frac{3n^2/\pi^2}{\frac{1}{2}n^2} = \frac{6}{\pi^2}$.

The Mangoldt function Λ(n)

We introduce next Mangoldt's function Λ which plays a central role in the distribution of primes.

Definition :- For every integer $n \ge 1$ we define

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^m \text{ fo some prime p and some } m \ge 1. \\ 0 & \text{otherwise} \end{cases}$$

Here is a short table of values of Λ(n) :

n:	1	2	3	4	5	6	7	8	9	10
Λ(n):	0	log2	log3	log2	log5	0	log7	log2	log3	0

Theorem 5.21 If $n \ge 1$ we have

$$\log n = \sum_{d \mid n} \Lambda(d). \qquad \ldots(1)$$

Proof :- The theorem is true if n = 1 since both members are 0. Therefore, assume that n > 1 and write

$$n = \prod_{k=1}^{r} p_k^{a_k}.$$

Taking logarithms we have

$$\log n = \sum_{k=1}^{r} a_k \log p_k.$$

Now consider the sum on the right of (1). The only nonzero terms in the sum come from those divisors d of the form p_k^m for m = 1, 2,…, a_k and k = 1, 2,…, r. Hence

$$\sum_{d|n} \Lambda(d) = \sum_{k=1}^{r} \sum_{m=1}^{a_k} \Lambda(p_k{}^m) = \sum_{k=1}^{r} \sum_{m=1}^{a_k} \log p_k = \sum_{k=1}^{r} a_k \log p_k = \log n,$$

which proves (1).

Now we use Mobius inversion to express $\Lambda(n)$ in terms of the logarithm.

Theorem 5.22 If $n \geq 1$ we have

$$\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d} = -\sum_{d|n} \mu(d) \log d.$$

Proof :- We know $\log n = \sum_{d \mid n} \Lambda(d)$ …(1)

Inverting (1) by the Mobius inversion formula we obtain

$$\Lambda(n) = \sum_{d \mid n} \mu(d) \log \frac{n}{d} = \log n \sum_{d \mid n} \mu(d) - \sum_{d \mid n} \mu(d) \log d$$

$$= \left[\frac{1}{n}\right] \log n - \sum_{d/n} \mu(d) \log d.$$

Since $\left[\frac{1}{n}\right] \log n = 0$ for all n the proof is complete.

Chebyshev's functions $\psi(x)$ and $\vartheta(x)$

Definition :- For $x > 0$ we define Chebyshev's ψ-function by the formula

$$\psi(x) = \sum_{n \leq x} \Lambda(n).$$

Since $\Lambda(n) = 0$ unless n is a prime power we can write the definition of $\psi(x)$ as follows :

$$\psi(x) = \sum_{n \leq x} \Lambda(n) = \sum_{\substack{m=1 \\ p^m \leq x}}^{\infty} \sum_{p} \Lambda(p^m) = \sum_{m=1}^{\infty} \sum_{p \leq x^{1/m}} \log p.$$

The sum on m is actually a finite sum. In fact, the sum on p is empty if $x^{1/m} < 2$, that is, if

$(1/m)\log x < \log 2$, or if

$$m > \frac{\log x}{\log 2} = \log_2 x.$$

Therefore we have

$$\psi(x) = \sum_{m \le \log_2 x} \sum_{p \le x^{1/m}} \log p.$$

This can be written in a slightly different form by introducing another function of Chebyshev.

Definition :- If $x > 0$ we define Chebyshev's ϑ-function by the equation

$$\vartheta(x) = \sum_{p \le x} \log p,$$

where p runs over all primes $\le x$.

The last formula for $\psi(x)$ can now be restated as follows :

$$\psi(x) = \sum_{m \le \log_2 x} \vartheta(x^{1/m}).$$

The next theorem relates the two quotients $\psi(x)/x$ and $\vartheta(x)/x$.

Theorem 5.23 For $x > 0$ we have

$$0 \le \frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \le \frac{(\log x)^2}{2\sqrt{x}\log^2}$$

Note :- This inequality implies that

$$\lim_{x \to \infty} \left(\frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \right) = 0 .$$

In other words, if one of $\psi(x)/x$ or $\vartheta(x)/x$ tends to a limit then so does the other, and the two limits are equal.

Proof :- we have $\psi(x) = \sum_{m \le \log_2 x} \vartheta(x^{1/m})$, so

$$0 \le \psi(x) - \vartheta(x) = \sum_{2 \le m \le \log_2 x} \vartheta(x^{1/m}).$$

But from the definition of $\vartheta(x)$ we have the trivial inequality

$$\vartheta(x) \le \sum_{p \le x} \log x \le x \log x$$

so

$$0 \le \psi(x) - \vartheta(x) \le \sum_{2 \le m \le \log_2 x} x^{1/m} \log(x^{1/m}) \le (\log_2 x)\sqrt{x} \log \sqrt{x}$$

$$= \frac{\log x}{\log 2} \cdot \frac{\sqrt{x}}{2} \log x = \frac{\sqrt{x}(\log x)^2}{2 \log 2}.$$

Now divide by x to obtain the theorem.

Relations connecting $\vartheta(x)$ and $\pi(x)$

In this section we obtain two formulas relating $\vartheta(x)$ and $\pi(x)$. where $\pi(x)$ is the number of primes $\leq x$. These will be used to show that the prime number theorem is equivalent to the limit relation

$$\lim_{x\to\infty} \frac{\vartheta(x)}{x} = 1.$$

Both functions $\pi(x)$ and $\vartheta(x)$ are step functions with jumps at the primes; $\pi(x)$ has a jump 1 at each prime p, whereas $\vartheta(x)$ has a jump of log p at p. Sums involving step functions of this type can be expressed as integrals by means of the following theorem.

Theorem 5.24 Abel's identity. For any arithmetical function a(n) let

$$A(x) = \sum_{n\leq x} a(n),$$

Where $A(x) = 0$ if $x < 1$. Assume f has a continuous derivative on the interval [y, x], where $0 < y < x$. Then we have

$$\sum_{y<n\leq x} a(n)\, f(n) = A(x)\, f(x) - A(y)\, f(y) - \int_y^x A(t)\, f'(t)\, dt. \qquad \ldots(1)$$

Proof :- Let $k = [x]$ and $m = [y]$, so that $A(x) = A(k)$ and $A(y) = A(m)$.

Then $$\sum_{y<n\leq x} a(n)f(n) = \sum_{n=m+1}^{k} a(n)f(n) = \sum_{n=m+1}^{k} \{A(n) - A(n-1)\}\, f(n)$$

$$= \sum_{n=m+1}^{k} A(n)f(n) - \sum_{n=m}^{k-1} A(n)f(n+1)$$

$$= \sum_{n=m+1}^{k-1} A(n)\ \{f(n)\ - f(n+1)\} + A(k)\ f(k)$$

$- A(m)f(m+1)$

$$= -\sum_{n=m+1}^{k-1} A(n) \int_n^{n+1} f'(t)dt + A(k)\, f(k) - A(m)f(m+1)$$

$$= -\sum_{n=m+1}^{k-1} \int_n^{n+1} A(t)\, f'(t)\, dt + A(k)\, f(k) - A(m)\, f(m+1)$$

$$= -\int_{m+1}^{k} A(t)\, f'(t)\, dt + A(x)\, f(x) - \int_k^x A(t)\, f'(t)\, dt$$

$$- A(y)\, f(y) - \int_y^{m+1} A(t)\, f'(t)dt$$

$$= A(x)\, f(x) - A(y)\, f(y) - \int_y^x A(t)\, f'(t)dt.$$

Theorem 5.25 For $x \geq 2$ we have

$$\vartheta(x) = \pi(x) \log x - \int_2^x \frac{\pi(t)}{t} dt \qquad \ldots(1)$$

and

$$\pi(x) = \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(t)}{t \log^2 t} dt. \qquad \ldots(2)$$

Proof :- Let a(n) denote the characteristic function of the primes; that is,

$$a(n) = \begin{cases} 1 & \text{if } n \text{ is prime,} \\ 0 & \text{otherwise.} \end{cases}$$

Then we have

$$\pi(x) = \sum_{p \leq x} 1 = \sum_{1 < n \leq x} a(n) \qquad \text{and } \vartheta(x) = \sum_{p \leq x} \log p = \sum_{1 < n \leq x} a(n) \log n.$$

Taking $f(x) = \log x$ in Abel's identity with $y = 1$ we obtain

$$\vartheta(x) = \sum_{1 < n \leq x} a(n) \log n = \pi(x) \log x - \pi(1) \log 1 - \int_1^x \frac{\pi(t)}{t} dt,$$

which proves (1) since $\pi(t) = 0$ for $t < 2$.

Next, let $b(n) = a(n) \log n$ and write

$$\pi(x) = \sum_{3/2 < n \leq x} b(n) \frac{1}{\log n}, \quad \vartheta(x) = \sum_{n \leq x} b(n).$$

Taking $f(x) = 1/\log x$ in Abel's identity with $y = 3/2$ we obtain

$$\pi(x) = \frac{\vartheta(x)}{\log x} - \frac{\vartheta(3/2)}{\log 3/2} + \int_{3/2}^x \frac{\vartheta(t)}{t \log^2 t} dt,$$

which proves (2) since $\vartheta(t) = 0$ if $t < 2$.

Some equivalent forms of the prime number theorem

Theorem 5.26 The following relations are logically equivalent :

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1. \qquad \ldots(1)$$

$$\lim_{x\to\infty} \frac{\vartheta(x)}{x} = 1. \qquad \ldots(2)$$

$$\lim_{x\to\infty} \frac{\psi(x)}{x} = 1. \qquad \ldots(3)$$

Proof :- From above theorem we obtain, respectively,

$$\frac{\vartheta(x)}{x} = \frac{\pi(x)\log x}{x} - \frac{1}{x}\int_2^x \frac{\pi(t)}{t}dt$$

and

$$\frac{\pi(x)\log x}{x} = \frac{\vartheta(x)}{x} + \frac{\log x}{x}\int_2^x \frac{\vartheta(t)dt}{t\log^2 t}.$$

To show that (1) implies (2) we need only show that (1) implies

$$\lim_{x\to\infty} \frac{1}{x}\int_2^x \frac{\pi(t)}{t}dt = 0.$$

But (1) implies $\frac{\pi(t)}{t} = O\left(\frac{1}{\log t}\right)$ for $t \geq 2$ so

$$\frac{1}{x}\int_2^x \frac{\pi(t)}{t}dt = O\left(\frac{1}{x}\int_2^x \frac{dt}{\log t}\right).$$

Now

$$\int_2^x \frac{dt}{\log t} = \int_2^{\sqrt{x}} \frac{dt}{\log t} + \int_{\sqrt{x}}^x \frac{dt}{\log t} \leq \frac{\sqrt{x}}{\log 2} + \frac{x-\sqrt{x}}{\log\sqrt{x}}$$

so $$\frac{1}{x}\int_2^x \frac{dt}{\log t} \to 0 \text{ as } x\to\infty.$$

This shows that (1) implies (2).

To show that (2) implies (1) we need only show that (2) implies

$$\lim_{x\to\infty} \frac{\log x}{x}\int_2^x \frac{\vartheta(t)dt}{t\log^2 t} = 0.$$

But (2) implies $\vartheta(t) = O(t)$ so

$$\frac{\log x}{x}\int_2^x \frac{\vartheta(t)dt}{t\log^2 t} = O\left(\frac{\log x}{x}\int_2^x \frac{dt}{\log^2 t}\right).$$

Now

$$\int_2^x \frac{dt}{\log^2 t} = \int_2^{\sqrt{x}} \frac{dt}{\log^2 t} + \int_{\sqrt{x}}^x \frac{dt}{\log^2 t} \le \frac{\sqrt{x}}{\log^2 2} + \frac{x-\sqrt{x}}{\log^2 \sqrt{x}}$$

hence

$$\frac{\log x}{x}\int_2^x \frac{dt}{\log^2 t} \to 0 \text{ as } x \to \infty.$$

This proves that (2) implies (1), so (1) and (2) are equivalent. We know already, that (2) and (3) are equivalent.

Theorem 5.27 Bertrand's Postulate. If x is a real number, $x > 1$, then there exists at least one prime number in the open interval (x, 2x).

Proof :- Suppose that the interval (x, 2x) contains no prime number. If p is prime then there is at most one value of k for which $p^k \in (x, 2x)$, since $p^{k+1}/p^k = p \ge 2$. Furthermore, $k > 1$, since the interval contains no primes. Hence

$$\psi(2x) - \psi(x) = \sum_{x < p^k \le 2x} \log p \le \psi(\sqrt{2x}) + \log 2x.$$

Here the last term on the right is required because 2x may be a prime number. We use $\psi(x) \ge a_0 x - 5 \log ex$ for $x \ge 6$, to provide a lower bound for $\psi(2x)$, and use $\psi(x) < b_0 x + 5 (\log ex)^2$ to provide upper bounds for $\psi(x)$ and $\psi(\sqrt{2x})$. Thus we find that

$$(2a_0 - b_0)\, x - 5 \log 2ex - 5 (\log ex)^2$$

$$\le b_0\sqrt{2x} + 5(\log e\sqrt{2x})^2 + \log 2x. \qquad \ldots(1)$$

Here the left side is comparable to x as $x \to \infty$, while the right side is comparable to $\sqrt{x}$. Hence the set of x for which this holds is bounded. In fact, we show that if (1) holds then $x < 1600$. That is, if $x \ge 1600$ hen

$$2a_0 - b_0 \ge 5(\log 2ex)/x + 5(\log ex)^2/x$$

$$+ 5(\log e\sqrt{2x})^2/x + (\log 2x)/x + b_0\sqrt{2}/\sqrt{x} \quad \ldots(2)$$

To this end let f(x) be a function of the form $f(x) = (\log ax^b)^c / x$ where a, b, c are positive real constants. Then $\log f(x) = c \log \log ax^b - \log x$, and by differentiating it follows that

$$\frac{f'(x)}{f(x)} = (bc/(\log ax^b) - 1)/x.$$

Thus if $ax^b > e^{bc}$, then $f(x) > 0$ and the above expression is negative, so that $f'(x) < 0$. In other words, f(x) is decreasing in the interval $[x_0, \infty)$ where $x_0 = e^c/a^{1/b}$. Thus in particular the first term on the right side of (2) is decreasing for $x \geq x_1 = ½$, the second is decreasing for $x \geq x_2 = e$, the third is decreasing for $x \geq x_3 = ½$, and the fourth is decreasing for $x \geq x_4 = e/2$. Since the last term on the right side of (2) is decreasing for all positive values of x, we conclude that the right side is decreasing for $x \geq x_2 = 2.71828\cdots$. By direct calculation we discover that the right side of (2) is less than 3/8 when x = 1600, while the left side is > 3/8. Since the right side is decreasing, it follows that (2) holds for all $x \geq 1600$.

We have shown that Bertrand's postulate is true for $x \geq 1600$. To verify it for $1 < x < 1600$ we note that the following thirteen numbers are prime : 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503. As each term of this sequence is less than twice the preceding member, Bertrand's postulate is valid for $1 < x < 2503$, and the proof is complete.

An asymptotic formula for the partial sums $\sum_{p \leq x}(1/p)$

Theorem 5.28 There is a constant A such that

$$\sum_{p \leq x} \frac{1}{p} = \log \log x + A + O\left(\frac{1}{\log x}\right) \text{ for all } x \geq 2 . \qquad \ldots(1)$$

Proof :- Let

$$A(x) = \sum_{p \leq x} \frac{\log p}{p}$$

and let

$$a(n) = \begin{cases} 1 & \text{if } n \text{ is prime,} \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$\sum_{p \leq x} \frac{1}{p} = \sum_{n \leq x} \frac{a(n)}{n} \qquad \text{and } A(x) = \sum_{n \leq x} \frac{a(n)}{n} \log n.$$

Therefore if we take $f(t) = 1/\log t$ in Abel's identity we find, since $A(t) = 0$ for $t < 2$,

$$\sum_{p\le x}\frac{1}{p}=\frac{A(x)}{\log x}+\int_2^x\frac{A(t)}{t\log^2 t}dt. \qquad \ldots(2)$$

But we know that $\sum_{p\le x}\frac{\log p}{p}=\log + O(1)$, so we have $A(x) = \log x + R(x)$, where $R(x) = O(1)$. Using this on the right of (2) we find

$$\sum_{p\le x}\frac{1}{p}=\frac{\log x+O(1)}{\log}+\int_2^x\frac{\log t+R(t)}{t\log^2 t}dt$$

$$=1+O\left(\frac{1}{\log x}\right)+\int_2^x\frac{dt}{t\log t}+\int_2^x\frac{R(t)}{t\log^2 t}dt. \qquad \ldots(3)$$

Now

$$\int_2^x\frac{dt}{t\log t}=\log\log x-\log\log 2$$

and

$$\int_2^x\frac{R(t)}{t\log^2 t}dt=\int_2^\infty\frac{R(t)}{t\log^2 t}dt-\int_x^\infty\frac{R(t)}{t\log^2 t}dt,$$

the existence of the improper integral being assured by the condition $R(t) = O(1)$. But

$$\int_x^\infty\frac{R(t)}{t\log^2 t}dt=O\left(\int_x^\infty\frac{dt}{t\log^2 t}\right)=O\left(\frac{1}{\log x}\right).$$

Hence Equation (3) can be written as follow :

$$\sum_{p\le x}\frac{1}{p}=\log\log x+1-\log\log 2+\int_2^\infty\frac{R(t)}{t\log^2 t}dt+O\left(\frac{1}{\log x}\right).$$

This proves the theorem with

$$A=1-\log\log 2+\int_2^\infty\frac{R(t)}{t\log^2 t}dt.$$

Theorem 5.29 For $x \ge 2$,

$$\sum_{m\le x}\psi\left(\frac{x}{m}\right)=\sum_{d\le x}\Lambda(d)\left[\frac{x}{d}\right]=x\log x-x+O(\log x).$$

Proof :- To prove this theorem, we use the following identity "Let f(n) be an arithmetic function and

$$F(x) = \sum_{n \le x} f(n).$$

Then
$$\sum_{m \le x} F\left(\frac{x}{m}\right) = \sum_{d \le x} f(d)\left[\frac{x}{d}\right]$$

$$= \sum_{n \le x} \sum_{d \mid n} f(d).$$

With $f(n) = \Lambda(n)$ in Theorem 6.15, we have

$$F(x) = \sum_{n \le x} \Lambda(n) = \psi(x),$$

and so

$$\sum_{m \le x} \psi\left(\frac{x}{m}\right) = \sum_{d \le x} \Lambda(d)\left[\frac{x}{d}\right]$$

$$= \sum_{n \le x} \sum_{d \mid x} \Lambda(d)$$

$$= \sum_{n \le x} \log n$$

$$= x \log x - x + O(\log x).$$

The last identity comes from the estimate $\sum_{n \le x} \log n = x \log x - x + O(\log x)$

Theorem 5.30 (Merten's formula) There exists a constant γ such that for $x \ge 2$,

$$\prod_{p \le x} \left(1 - \frac{1}{p}\right)^{-1} = e^{\gamma} \log x + O(1).$$

Proof:- We begin with two observations. First, the series $\sum_p \sum_{k=2}^{\infty} p^{-k}/k$ converges, since

$$\sum_p \sum_{k=2}^{\infty} \frac{1}{kp^k} < \sum_p \sum_{k=2}^{\infty} \frac{1}{p^k} = \sum_p \frac{1}{p(p-1)} < \sum_{n=2}^{\infty} \frac{1}{n(n-1)} < \infty.$$

Let

$$b_2 = \sum_p \sum_{k=2}^{\infty} \frac{1}{kp^k} > 0.$$

Second, for $x \geq 2$,

$$0 < \sum_{p>x} \sum_{k=2}^{\infty} \frac{1}{kp^k} < \sum_{p>x} \frac{1}{p(p-1)} < \sum_{n>x} \frac{1}{n(n-1)}$$

$$= \sum_{n=[x]+1}^{\infty} \left(\frac{1}{n-1} - \frac{1}{n} \right) = \frac{1}{[x]}$$

$$\leq \frac{2}{x}.$$

From the Taylor series

$$-\log(1-t) = \sum_{k=1}^{\infty} \frac{t^k}{k} \text{ for } |t| < 1$$

and using the estimate of $\sum_{p \leq x} \frac{1}{p}$ for $x \geq 2$, we obtain

$$\log \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = \sum_{p \leq x} \log\left(1 - \frac{1}{p}\right)^{-1}$$

$$= \sum_{p \leq x} \sum_{k=1}^{\infty} \frac{1}{kp^k}$$

$$= \sum_{p \leq x} \frac{1}{p} + \sum_{p \leq x} \sum_{k=2}^{\infty} \frac{1}{kp^k}$$

$$= \log\log x + b_1 + O\left(\frac{1}{\log x}\right) + b_2 - \sum_{p>x} \sum_{k=2}^{\infty} \frac{1}{kp^k}$$

$$= \log\log x + b_1 + b_2 + O\left(\frac{1}{\log x}\right) + O\left(\frac{1}{x}\right)$$

$$= \log\log x + b_1 + b_2 + O\left(\frac{1}{\log x}\right).$$

Let $\gamma = b_1 + b_2$. Then

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = e^{\gamma} \log x \exp\left(O\left(\frac{1}{\log x}\right)\right).$$

Since exp(t) = 1 + O(t) for t in any bounded interval [0, t_0], and since O(1/log x) is bounded for x ≥2, we have

$$\exp\left(O\left(\frac{1}{\log x}\right)\right) = 1 + O\left(\frac{1}{\log x}\right).$$

Therefore,

$$\prod_{p \le x}\left(1-\frac{1}{p}\right)^{-1} = e^{\gamma}\log x \exp\left(O\left(\frac{1}{\log x}\right)\right)$$

$$= e^{\gamma}\log x\left(1+O\left(\frac{1}{\log x}\right)\right)$$

$$= e^{\gamma}\log x + O(1).$$

This is Merten's formula.

Theorem 5.31 (Mertens Theorem) For x ≥ 1,

$$\sum_{n\le x}\frac{\Lambda(n)}{n} = \log x + O(1) \qquad \ldots(1)$$

and

$$\sum_{p\le x}\frac{\log p}{p} = \log x + O(1). \qquad \ldots(2)$$

Proof :- Since $\psi(x) = O(x)$ by Chebyshev's theorem, we have

$$x\log x - x + O(\log x) = \sum_{d\le x}\Lambda(d)\left[\frac{x}{d}\right]$$

$$= \sum_{d\le x}\Lambda(d)\left(\frac{x}{d} - \left\{\frac{x}{d}\right\}\right)$$

$$= x\sum_{d\le x}\frac{\Lambda(d)}{d} - \sum_{d\le x}\Lambda(d)\left\{\frac{x}{d}\right\}$$

$$= x\sum_{d\le x}\frac{\Lambda(d)}{d} + O(\psi(x))$$

$$= x \sum_{d \le x} \frac{\Lambda(d)}{d} + O(x).$$

We obtain equation (1) by dividing by x.

Next, we observe that

$$\sum_{n \le x} \frac{\Lambda(n)}{n} - \sum_{p \le x} \frac{\log p}{p} = \sum_{\substack{p^k \le x \\ k \ge 2}} \frac{\log p}{p^k}$$

$$\le \sum_{p \le x} \log p \sum_{k=2}^{\infty} \frac{1}{p^k}$$

$$\le \sum_{p \le x} \frac{\log p}{p(p-1)}$$

$$= O(1).$$

This proves (1).

Selberg's asymptotic formula

We deduce Selberg's formula by a method given by Tatuzawa and Iseki. It is based on the following theorem which has the nature of an inversion formula.

Theorem 5.32 Let F be a real or complex-valued function defined on (0, ∞), and let

$$G(x) = \log x \sum_{n \le x} F\left(\frac{x}{n}\right).$$

Then $$F(x) \log x + \sum_{n \le x} F\left(\frac{x}{n}\right)\Lambda(n) = \sum_{d \le x} \mu(d) G\left(\frac{x}{d}\right).$$

Proof :- First we write F(x)log x as a sum,

$$F(x)\log x = \sum_{n \le x} \left[\frac{1}{n}\right] F\left(\frac{x}{n}\right) \log \frac{x}{n} = \sum_{n \le x} F\left(\frac{x}{n}\right) \log \frac{x}{n} \sum_{d/n} \mu(d).$$

Then we use the identity,

$$\Lambda(n) = \sum_{d/n} \mu(d) \log \frac{n}{d}$$

to write

$$\sum_{n \le x} F\left(\frac{x}{n}\right)\Lambda(n) = \sum_{n \le x} F\left(\frac{x}{n}\right) \sum_{d \mid n} \mu(d) \log \frac{n}{d}.$$

Adding these equations we find

$$F(x)\log x + \sum_{n\le x} F\left(\frac{x}{n}\right)\Lambda(n) = \sum_{n\le x} F\left(\frac{x}{n}\right)\sum_{d\mid n} \mu(d)\left\{\log\frac{x}{n} + \log\frac{n}{d}\right\}$$

$$= \sum_{n\le x}\sum_{d\mid n} F\left(\frac{x}{n}\right)\mu(d)\log\frac{x}{d}.$$

In the last sum we write n = qd to obtain

$$\sum_{n\le x}\sum_{d\mid n} F\left(\frac{x}{n}\right)\mu(d)\log\frac{x}{d} = \sum_{d\le x}\mu(d)\log\frac{x}{d}\sum_{q\le x/d} F\left(\frac{x}{qd}\right) = \sum_{d\le x}\mu(d)G\left(\frac{x}{d}\right),$$

which proves the theorem.

Theorem 5.33 Selberg's asymptotic formula. For $x > 0$ we have

$$\psi(x)\log x + \sum_{n\le x}\Lambda(n)\psi\left(\frac{x}{n}\right) = 2x\log x + O(x).$$

Proof :- We apply above theorem to the function $F_1(x) = \psi(x)$ and also to $F_2(x) = x - C - 1$, where C is Euler's constant. Corresponding to F_1 we have

$$G_1(x) = \log x \sum_{n\le x}\psi\left(\frac{x}{n}\right) = x\log^2 x - x\log x + O(\log^2 x),$$

where we have used the relation $\sum_{n\le x}\psi\left(\frac{x}{n}\right) = x\log x - x + O(\log x)$. Corresponding to F_2 we have

$$G_2(x) = \log x \sum_{n\le x} F_2\left(\frac{x}{n}\right) = \log x \sum_{n\le x}\left(\frac{x}{n} - C - 1\right)$$

$$= x\log x \sum_{n\le x}\frac{1}{n} - (C+1)\log x \sum_{n\le x} 1$$

$$= x\log x\left(\log x + C + O\left(\frac{1}{x}\right)\right) - (C+1)\log x(x + O(1))$$

$$= x\log^2 x - x\log x + O(\log x).$$

Comparing the formulas for $G_1(x)$ and $G_2(x)$ we see that $G_1(x) - G_2(x) = O(\log^2 x)$. Actually, we shall only use the weaker estimate

$$G_1(x) - G_2(x) = O(\sqrt{x}).$$

Now we apply above Theorem to each of F_1 and F_2 and subtract the two relations so obtained. The difference of the two right members is

$$\sum_{d\le x} \mu(d)\left\{G_1\left(\frac{x}{d}\right) - G_2\left(\frac{x}{d}\right)\right\} = O\left(\sum_{d\le x} \sqrt{\frac{x}{d}}\right) = O\left(\sqrt{x}\sum_{d\le x} \frac{1}{\sqrt{d}}\right) = O(x)$$

Therefore the difference of the two left members is also $O(x)$. In other words, we have

$$\{\psi(x) - (x - C - 1)\}\log x + \sum_{n\le x}\left\{\psi\left(\frac{x}{n}\right) - \left(\frac{x}{n} - C - 1\right)\right\}\Lambda(n) = O(x).$$

Rearranging terms and using $\sum_{n \le x} \frac{\Lambda(n)}{n} = \log x + O(1)$ we find that

$$\psi(x)\log x + \sum_{n\le x} \psi\left(\frac{x}{n}\right)\Lambda(n) = (x - C - 1)\log x$$

$$+ \sum_{n\le x}\left(\frac{x}{n} - C - 1\right)\Lambda(n) + O(x)$$

$$= 2x \log x + O(x).$$

The Prime Number Theorem

The function $\pi(x)$ counts the number of prime numbers not exceeding x. The prime number theorem (conjectured independently around 1800 by Gauss and Legendre), states that $\pi(x)$ is asymptotic to x/log x, that is,

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1.$$

We define the remainder term R(x) for Chebyshev's function $\vartheta(x)$ by

$$R(x) = \vartheta(x) - x.$$

We shall prove the prime number theorem in the form $\vartheta(x) \sim x$, or, equivalently, $R(x) = o(x)$ as we have already proved in theorem 5.26 that $\vartheta(x) \sim x$ and $\pi(x) \sim x$ are equivalent. More precisely, we shall prove that there exist

sequences of positive real numbers $\{\delta_m\}_{m=1}^{\infty}$ and $\{u_m\}_{m=1}^{\infty}$ such that $\lim_{m\to\infty} \delta_m = 0$ and

$$|R(x)| < \delta_m x \quad \text{for } x \geq u_m.$$

We need the following lemmas [cf: Melvin B. Nathanson, *Elementary Methods in Number Theory*, Springer-Verlag, New York 1999].

Lemma 1. For every positive integer n,

$$\prod_{p \leq n} p < 4^n$$

Equivalently, for every real number $k \geq 1$

$$v(x) < x \log 4.$$

Lemma 2 :- There exists positive constants A and B such that

$$A(x) \leq v(x) \leq \psi(x) = \pi(x) \log x \leq B \text{ for } x \geq 2.$$

Moreover $$\liminf_{x\to\infty} \frac{v(x)}{x} = \liminf_{x\to\infty} \frac{\psi(x)}{x} = \liminf_{x\to\infty} \frac{\pi(x)\log x}{x} \geq 2$$

and

$$\limsup_{x\to\infty} \frac{v(x)}{x} = \limsup_{x\to\infty} \frac{\psi(x)}{x} = \limsup_{x\to\infty} \frac{\pi(x)\log x}{x} \leq \log 4$$

Lemma 3 For $x > e$,

$$\sum_{p \leq x} \frac{\log p}{p\left(1 + \log \frac{x}{p}\right)} = O(\log \log x).$$

Lemma 4 For $x \geq 1$

$$|R(x)| \leq \frac{1}{\log x} \sum_{n \leq x} \left| R\left(\frac{x}{n}\right) \right| + O\left(\frac{x \log\log x}{\log x}\right)$$

Lemma 5 Let $0 < \delta < 1$. There exist numbers $c_0 \geq 1$ and $x_1(\delta) \geq 4$ such that if $x \geq x_1(\delta)$, then there exists an integer n such that

$$x < n \leq e^{c_0/\delta} x$$

and $$|R(n)| < \delta n.$$

The constant c_0 does not depend on δ.

Lemma 6 Let $c_0 \geq 1$ be the number constructed in Lemma 3 and let $0 < \delta < 1$. There exists a number $x_2(\delta)$ such that if $x \geq x_2(\delta)$, then the interval $(x, e^{c_0/\delta}x]$ contains a subinterval $(y, e^{\delta/2}y]$ such that

$$|R(t)| < 4\delta t$$

for all $t \in (y, e^{\delta/2}y]$.

Theorem 5.34 (Prime number theorem) For Chebyshev's function $\vartheta(x)$,

$$\vartheta(x) \sim x$$

as $x \to \infty$.

Proof :- By lemma 1,

$$\limsup_{x\to\infty} \frac{R(x)}{x} = \limsup_{x\to\infty} \frac{\vartheta(x)}{x} - 1 \leq \log 4 - 1 < 0.4.$$

By lemma 2,

$$\liminf_{x\to\infty} \frac{R(x)}{x} = \liminf_{x\to\infty} \frac{\vartheta(x)}{x} - 1 \geq \log 2 - 1 > -0.4.$$

It follows that there exist numbers M and u_1 such that

$$|R(x)| < Mx \quad \text{for all } x \geq 1,$$

and $$|R(x)| < \delta_1 x \quad \text{for all } x \geq u_1,$$

where $$\delta_1 = 0.4.$$

We shall construct sequences of positive real numbers $\{\delta_m\}_{m=1}^{\infty}$ and $\{\varepsilon_m\}_{m=1}^{\infty}$, such that

$$\delta_1 > \delta_2 > \delta_3 > \ldots$$

and

$$\lim_{m\to\infty} \varepsilon_m = 0. \qquad \ldots(1)$$

Let $m \geq 1$, and suppose that we have constructed the number δ_m. Let $c_0 \geq 1$ be the number defined in Lemma 5. Choose ε_m such that

$$0 < \varepsilon_m < 1/m$$

and

$$(1 + \varepsilon_m)\left(1 - \frac{\delta_m^2}{256c_0}\right) < 1.$$

We define

$$\delta_{m+1} = (1 + \varepsilon_m)\left(1 - \frac{\delta_m^2}{256c_0}\right)\delta_m. \qquad \ldots(2)$$

Then $0 < \delta_{m+1} < \delta_m$. This determines the sequences $\{\delta_m\}_{m=1}^{\infty}$ and $\{\varepsilon_m\}_{m=1}^{\infty}$ inductively.

We shall prove that for every m there exists a number u_m such that

$$|R(x)| < \delta_m x \text{ for all } x \geq u_m. \qquad (3)$$

Let us show that this suffices to prove the prime number theorem. The sequence $\{\delta_m\}_{m=1}^{\infty}$ is a strictly decreasing sequence of positive real numbers, so the sequence converges to some non negative number $\delta < 1$. Then (1) and (2) imply that

$$\delta = \left(1 - \frac{\delta^2}{356c_0}\right)\delta = 0.$$

Inequality (3) implies that $R(x) = o(x)$, which is equivalent to the prime number theorem.

We construct the numbers u_m inductively. There exists u_1 such that $|R(x)| < \delta_1 x$ for $x \geq u_1$. Suppose that u_m has been determined. We shall prove that there exists a number u_{m+1} such that $|R(x)| < \delta_{m+1}x$ for all $x \geq u_{m+1}$.

Define $\delta'_m = \dfrac{\delta_m}{8}$

and $\rho = e^{c_0/\delta_m}$.

Let $x_2(\delta_m)$ be the number constructed in Lemma 6, and let

$$x_3(m) = \max\,(x_2(\delta_m), u_m).$$

If

$$x \geq x_3(m) \geq x_2(\delta_m),$$

then by Lemma 6, every interval $(x, \rho x]$ contains a subinterval $(y, e^{\delta_m/2}y]$ such that

$$|R(t)| < 4\,\delta_m t = \frac{\delta_m t}{2}$$

for all $t \in (y, e^{\delta_m/2}y]$. Let k be the greatest integer such that $\rho^k \le x/x_3(m)$. Then

$$k \le \frac{\log x/x_3(m)}{\log \rho} < k+1,$$

and so

$$\begin{aligned} k &= \frac{\log(x/x_3(m))}{\log\rho} + O(1) \\ &= \frac{\delta_m \log(x/x_3(m))}{c_0} + O(1) \\ &= \frac{\delta_m \log x}{8c_0} + O(1). \end{aligned}$$

By lemma 4,

$$\begin{aligned} |R(x)| &\le \frac{1}{\log x}\sum_{n\le x}\left|R\left(\frac{x}{n}\right)\right| + o(x) \\ &= \frac{1}{\log x}\sum_{n\le \rho^k}\left|R\left(\frac{x}{n}\right)\right| + \frac{1}{\log x}\sum_{\rho^k < n \le x}\left|R\left(\frac{x}{n}\right)\right| + O(x) \\ &\le \frac{1}{\log x}\sum_{n\le \rho^k}\left|R\left(\frac{x}{n}\right)\right| + \frac{Mx}{\log x}\sum_{\rho^k < n \le x}\frac{1}{n} + O(x) \\ &\le \frac{1}{\log x}\sum_{n\le \rho^k}\left|R\left(\frac{x}{n}\right)\right| + o(x), \end{aligned}$$

since

$$\sum_{\rho^k < n \le x}\frac{1}{n} \le \sum_{x/(\rho x_3(m)) < n \le x}\frac{1}{n} = \log(\rho x_3(m)) + O(1/x) = O(1).$$

If $1 \le n \le \rho^k$, then

$$\frac{x}{n} \ge \frac{x}{\rho^k} \ge x_3(m) \ge u_m$$

and

$$\left|R\left(\frac{x}{n}\right)\right| < \frac{\delta_m x}{n},$$

by the definition of u_m.

For $j = 1,\ldots,k$, we have

$$\frac{x}{\rho^j} \geq \frac{x}{\rho^k} \geq x_3(m) \geq x_2(\delta_m),$$

and so each interval $\left(\frac{x}{\rho^j}, \frac{x}{\rho^{j-1}}\right]$ contains a subinterval $I_j = (y_j, e^{\delta_m/2} y_j]$

such that $|R(t)| < 4\delta_m t = \frac{\delta_m t}{2}$ for all $t \in I_j$.

Therefore,

$$\sum_{n \in (\rho^{j-1}, \rho^j]} \left| R\left(\frac{x}{n}\right)\right| = \sum_{n \in (\rho^{j-1}, \rho^j] \setminus I_j} \left| R\left(\frac{x}{n}\right)\right| + \sum_{n \in]_j} \left| R\left(\frac{x}{n}\right)\right|$$

$$< \delta_m x \sum_{n \in (\rho^{j-1}, \rho^j] \setminus I_j} \frac{1}{n} + \frac{\delta_m x}{2} \sum_{n \in I_j} \frac{1}{n}$$

$$= \delta_m x \sum_{n \in (\rho^{j-1}, \rho^j] \setminus} \frac{1}{n} - \frac{\delta_m x}{2} \sum_{n \in I_j} \frac{1}{n}.$$

Then

$$\sum_{n \leq \rho^k} \left| R\left(\frac{x}{n}\right)\right| = R(x) + \sum_{j=1}^{k} \sum_{n \in (\rho^{j-1}, \rho_j]} \left| R\left(\frac{x}{n}\right)\right|$$

$$= \delta_m x + \sum_{j=1}^{k} \left(\delta_m x \sum_{n \in (\rho^{j-1}, \rho_j]} \frac{1}{n} - \frac{\delta_m x}{2} \sum_{n \in I_j} \frac{1}{n} \right)$$

$$= \delta_m x \sum_{n \leq \rho^k} \frac{1}{n} - \frac{\delta_m x}{2} \sum_{j=1}^{k} \sum_{n \in I_j} \frac{1}{n}.$$

We have

$$\delta_m x \sum_{n \leq \rho^k} \frac{1}{n} = \delta_m x \left(k \log \rho + O\left(\frac{1}{\rho^k}\right)\right)$$

$$= \delta_m x \log x + O(x).$$

Moreover,

$$\sum_{n\in I_j}\frac{1}{n}=\sum_{n\in(y_j,e^{\delta_m/2}y_j]}\frac{1}{n}=\frac{\delta_m}{2}+O\left(\frac{1}{y_j}\right)=\frac{\delta_m}{2}+O\left(\frac{\rho^j}{x}\right),$$

and so

$$\begin{aligned}\sum_{j=1}^{k}\sum_{n\in I_j}\frac{1}{n}&=\frac{\delta_m k}{2}+O\left(\sum_{j=1}^{k}\frac{\rho^j}{x}\right)\\&=\frac{\delta_m}{2}\left(\frac{\delta_m\log x}{8c_0}+O(1)\right)+O(1)\\&=\frac{\delta_m\log x}{128c_0}+O(1),\end{aligned}$$

since

$$\sum_{j=1}^{k}\frac{\rho^j}{x}=\frac{\rho(\rho^k-1)}{x(\rho-1)}<\frac{2\rho^k}{x}\le\frac{2}{x_3(m)}=O(1).$$

Therefore,

$$\frac{\delta_m x}{2}\sum_{j=1}^{k}\sum_{n\in I_j}\frac{1}{n}=\frac{\delta_m^3 x\log x}{256c_0}+O(x).$$

Combining these results, we obtain, for $x\ge x_3(m)$,

$$\begin{aligned}\sum_{n\le\rho^k}\left|R\left(\frac{x}{n}\right)\right|&\le(\delta_m x\log x+O(x))-\left(\frac{\delta_m^3 x\log x}{256c_0}+O(x)\right)\\&=\left(1-\frac{\delta_m^2}{256c_0}\right)\delta_m x\log x+O(x),\end{aligned}$$

and

$$\begin{aligned}|R(x)|&\le\frac{1}{\log x}\sum_{n\le\rho^k}\left|R\left(\frac{x}{n}\right)\right|+o(x)\\&=\left(1-\frac{\delta_m^2}{256c_0}\right)\delta_m x+o(x).\end{aligned}$$

We choose u_{m+1} sufficiently large that for all $x \geq u_{m+1}$ we have

$$o(x) < \varepsilon_m \left(1 - \frac{\delta_m^2}{256c_0}\right) \delta_m x.$$

Then $$|R(x)| < (1+\varepsilon_m) \left(1 - \frac{\delta_m^2}{256c_0}\right) \delta_m x = \delta_{m+1} x.$$

This completes the proof of the prime number theorem.