USOSCMTHOS

V.P. & R.P.T.P. SCIENCE COLLEGE
V.V.NAGAR

T.Y. B.Sc.
MATHEMATICS

US05CMTH05

M-305

(NUMBER THEORY

&

~~COMPLEX ANALYSIS~~)

Name :..

Address : ....

....

Contact No.: ....

Sem IV

UNIT-1 Pg. 1 to 52

UNIT-2 Pg-53 to 62
Pg-87 to 93
Pg-125 to 146
Pg-187 to 196

UNIT-3 Pg. 153 to 185
Pg-63 to 76
~~Pg-93 to 102~~
~~Pg-146 to 152~~

UNIT-4 Pg. 77 to 85
Pg. 93 to 102, 146 [illegible]
Pg-103 to 124

Pg. 93, 94, 99

SARDAR PATEL UNIVERSITY ,VALLABH VIDYANAGAR
SYLLABUS FOR B.Sc.(MATHEMATICS) SEMESTER - V
US05CMTH05 (Number Theory)
THREE HOURS PER WEEK (3 CREDIT)
Effective from June 2012

Marks:-100(30 internal+70 external)

UNIT-1 Divisibility . Fundamental theorem of divisibility , G.C.D.: definition and examples , L.C.M. : definition and examples , Prime numbers , Factorization in prime numbers , Unique factorization theorem .

UNIT-2 Perfect numbers : definition and examples , Mersenne numbers : definition and examples , Fermat numbers : definition and examples ,Gauss function : definition and examples , Mobius function : definition and examples .

UNIT-3 Linear indeterminate equations and its solution , Shang-gao indeterminate equation and its solution , Congruences : Definition and examples , Properties of congruences .

UNIT-4 Complete residue system(mod m) , Reduced residue system(mod m) Euler's function , Congruence in one unknown , Solution of Linear congruence in one unknown and two unknown Chinese theorem , Wilson's theorem .

Recommended texts :

C.Y.Hsiung, Elementary Theory of numbers, Allied publishers Ltd.(1992) Chapter 1, 2, 3(only article 3.1 and 3.2), 4 (only article 4.1).

Reference Books:

(1) D.Burton , elementary Number Theory, Universal Book stall, new Delhi

(2) I.Niven And H.Zuckermar , An Introduction to the theory of Numbers, Wiley-Eastern Publication.

(3) S.Barnard and J.N.Child , Higher Algebra, Mc Millan and Co. Ltd.

B.Sc.(MATHEMATICS) SEMESTER - V
QUESTION BANK OF US05CMTH05
(Number Theory)
Effective from June 2012

Marks:-100(30 internal + 70 external)

Unit-1

1. Divisor , Proper divisor , Common divisor , G.C.D , L.C.M.
2. Prove that $(a-s)/(ab+st) \Rightarrow (a-s)/(at+sb)$ [2]
3. State and prove Fundamental theorem of divisibility. [6]
4. Let g be a positive integer greater than 1 then prove that every positive integer a can can be written uniquely in the form $a = c_n g^n + c_{n-1} g^{n-1} + ... + c_1 g + c_0$, where $n \geq 0, c_i \in \mathbb{Z}, 0 \leq c_i < g, c_n \neq 0$. [7]
5. Find gcd of two numbers by using Euclidean algorithm . [3]
6. Find (525 , 231) , (1235 , 237) , (4678 , 362) , (3054 , 12379). [2]
7. Prove that $(a, b) = d$ iff $\exists\, x, y \in \mathbb{Z}$ such that $xa + yb = d$. [5]
8. Prove that (a , b) = d iff the following conditions are satisfied :
   (i) d/a , d/b
   (ii) whenever c/a and c/b then c/d . [3]
9. Prove that any common divisor of a and b is the divisor of their gcd . [2]
10. Prove that (a , b) = (a , b + ka) , for $k \in Z$. [3]
11. Prove that $(a, b)c = (ac, bc), \ \forall\ c > 0$ [3]
12. Prove that $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$. [5]
13. Prove that $[a, b](a, b) = ab, \ \forall\ ab > 0$. [5]
    OR : State and prove the relation between gcd and lcm of two numbers .
14. Prove that common multiple of a and b is a multiple of their lcm . [4]
15. If $k > 0$ is a common multiple of a and b then prove that $\left(\frac{k}{a}, \frac{k}{b}\right) = \frac{k}{[a, b]}$. [4]
16. If a and b are relatively primes and d/ab then prove that there exist unique d_1/a , d_2/b such that $d = d_1 d_2$. [4]
17. If a/bc and (a,b)=1,then prove that a/c. [2]
18. Prove that $(a+b)[a, b] = b[a, a+b]$,$\forall\ a, b > 0$. [3]
19. Prove that $[a, b, c] = [[a, b], c]$ [2]
20. Prove that $[a, b, c] = \dfrac{abc}{(ab, bc, ca)}$, for all $a, b, c > 0$. [3]
21. Find (136,221,391) and [136,221,391] . [4]
22. If m is composite integer and $n_m = 1111\ldots$(m times) then prove that n_m is also composite number . [4]

24. Prove that there are infinitely many prime number of the form $4n - 1$.

25. If P_n is nth prime number then prove that $P_n < 2^{2^n}$, for all $n \in \mathbb{N}$.

26. If p is prime then prove that there exist no positive integer a and b such that $a^2 = pb^2$. [5]
OR : If p is prime then prove that $a^2 \neq p\,b^2$, $\forall\ a, b \in \mathbb{N}$.

27. State and prove unique factorization theorem for positive integers.
OR State and prove fundamental theorem of arithmetic .

USO5CMTH05
Unit-2

1. If $a = p_1{}^{a_1} p_2{}^{a_2} p_3{}^{a_3} \ldots p_k{}^{a_k}$, where all p_i are primes and $a_i > 0$, then prove the following

   (a) $T(a) = \prod_{i=1}^{k} (a_i + 1)$ [2]

   (b) $S(a) = \prod_{i=1}^{k} \left[\frac{p_i^{a_i+1} - 1}{p_i - 1} \right]$ [2]

   (c) $P(a) = a^{T(a)/2}$ [2]

2. If a and b are relatively prime numbers then prove the following :
(i) T(ab) = T(a)T(b) . [2]
(ii) S(ab) = S(a) S(b) . [2]
(iii) P(ab) = $P(a)^{T(b)} P(b)^{T(a)}$. [2]

3. (i) If a is a square number then prove that S(a) is odd integer . [3]

   (ii) If a is not square number but odd integer then prove that S(a) is even integer . [2]

4. Prove that $S(a) < a\sqrt{a}$, $\forall\ a > 2$. [5]

5. Define Mersenne number.Prove that any prime factor of M_p is greater than p. [5]

6. Prove that odd prime factor of $M_p (p > 2)$ has the form 2pt+1,for some integer t. [5]

7. Prove that odd prime factor of $a^{2^n} + 1 (a > 1)$ is of the form $2^{n+1}t + 1$,for some integer t . [6]

8. Define Fermat's number.Prove that every prime factor of $F_n (n > 2)$ is of the form $2^{n+2}t + 1$,for some integer t. [7]

9. Prove that the necessary and sufficient condition that a positive integer a can be even perfect number is $a = 2^n(2^{n+1} - 1)$, $(n > 1)$ and $2^{n+1} - 1$ is prime. [6]

10. Define Gauss function (or : Greatest integer value function). Prove that $[x] + [y] \leq [x + y] \leq [x] + [y] + 1$. [3]

that among the integers from 1 to x the number of multipliers of n is $\left[\frac{x}{n}\right]$. [3]

12. Prove that in the product n! the highest power of prime p is $\sum_{k=1}^{m}\left[\frac{n}{p^k}\right]$, where $p^m \le n < p^{m+1}$. [5]
OR
In usual notation prove that $P(n!) = \sum_{k=1}^{m}\left[\frac{n}{p^k}\right]$, where $p^m \le n < p^{m+1}$.

13. **Find highest power of 2 in 50! i.e 2(50!) , Find 3(50!).** [2]

14. **Define Mobious function.Prove that Mobious function is multiplicative function.** [4]

15. **Prove that** $\sum_{d/a}\mu(d) = 0 = \sum_{d/a}\mu(\frac{a}{d})$, if $a > 1$. [4]

16. **Define Fibonacci numbers.Prove that the successive Fibonacci numbers are relatively prime.** [2]

17. **In usual notation prove that** $u_{m+n} = u_{m-1}u_n + u_m u_{m+1}$, $\forall\ m, n \in \mathbb{N}$ [4]

18. **Prove that** u_m/u_{mn}. [2]

19. **Prove that** $m/n \Rightarrow u_m/u_n$. [2]

20. **If** $m = qn + r$ **then prove that** $(u_m, u_n) = (u_n, u_r)$. [3]

21. Prove that g.c.d of two Fibonacci numbers is also a Fibonacci number. [4]
OR : Prove that $(u_m, u_n) = u_{(m,n)}$.
OR : Prove that $(u_m, u_n) = u_d$, where $d = (m, n)$.

22. **Prove that** $u_m/u_n \Leftrightarrow m/n$. [2]

23. **Find** (u_{16}, u_{12}) , (u_{15}, u_{25}) [2]

24. **Prove that** $u_{n+3} = 3u_{n+1} - u_{n-1}$, $\forall\ n \ge 2$. [3]

25. **Prove that** $\sum_{i=1}^{n} u_i{}^2 = u_n u_{n+1}$. [3]

26. Prove that $u_{n+1}^2 = u_n^2 + 3u_{n-1}^2 + 2[u_{n-2}^2 + u_{n-3}^2 + \cdots + u_1]$ [4]

US05CMTH05
Unit-3

1. (i)Prove that the indeterminate equation $ax + by = c$ has solution iff d/c,where (a,b)=d. [2]
(ii)If $x = x_0, y = y_0$ is a particular solution of $ax + by = c$ then prove that general solution can be written as [4]

$$x = x_0 + \frac{b}{d}t; y = y_0 - \frac{a}{d}t, \text{where } t \in \mathbb{Z}.$$

2. **If (a,b)=1 then prove that any solution of ax+by=c can be written as** $x = x_0 + bt, y = y_0 - at, t \in \mathbb{Z}$**,where** $x = x_0; y = y_0$ **are particular a solution of** $ax + by = c$. [4]

(i) [illegible] $+ 231y = 42$
(ii) $7x + 19y = 231$
(iii) $19x + 20y = 1909$
(iv) $x^2 + xy - 6 = 0$

4. Find general solution of equation [4]
(i) 50x+45y+36z=10
(ii) 8x-18y+10z=16 [3]

5. Prove that the positive integer solution of $x^{-1}+y^{-1} = z^{-1}$,(x,y,z)=1 has and must have the form $x = a(a+b), y = b(a+b), z = ab$,where $a, b > 0, (a, b) = 1$. [6]

6. Prove that the general integer solution of $x^2 + y^2 = z^2$ with $x, y, z > 0$, $(x, y) = 1$ and y even is given by $x = a^2 - y^2, y = 2ab, z = a^2 + b^2$,where $a, b > 0, (a, b) = 1$ and one of a,b is odd and the other is even. [6]

7. Prove that the integer solution of $x^2 + 2y^2 = z^2$,(x,y)=1 can be expressed as $x = \pm(a^2 - 2b^2), y = 2ab, z = a^2 + 2b^2$. [6]

8. **Prove that the integer solution of $x^{-2} + y^{-2} = z^{-2}$,(x,y,z)=1 is given by $x = (a^4 - b^4), y = 2ab(a^2 + b^2), z = 2ab(a^2 - b^2)$,where $a > b > 0, (a, b) = 1$ and a,b both can not be odd or even .** [6]

9. **Prove that a general integer solution of $x^2 + y^2 + z^2 = w^2$,(x,y,z,w)=1 is given by**
$x = (a^2 - b^2 + c^2 - d^2), y = 2ab - 2cd, z = 2ad + 2bc, w = a^2 + b^2 + c^2 + d^2$. [7]

10. Prove that the equation $x^4 + y^4 = z^2$ has no solution with nonzero positive integers x,y,z. [6]
OR : Prove that $x^4 + y^4 = z^2$ has no nonzero positive integer solution.

11. Define Congruent modulo n .

12. Prove that $a \equiv b(modn)$ iff a and b have the same nonnegative remainder when divided by n. [3]

13. **Prove that congruent is an equivalent relation.** [2]

14. **If $a_1 \equiv b_1(modn)$ and $a_2 \equiv b_2(modn)$,then prove the following:**

(a) $a_1 + a_2 \equiv b_1 + b_2(modn)$ [2]
(b) $ca_1 \equiv cb_1(modn)$,$\forall c \in \mathbb{Z}$. [2]
(c) $c + a_1 \equiv c + b_1(modn)$,$\forall c \in \mathbb{Z}$ [2]
(d) $a_1a_2 \equiv b_1b_2(modn)$ [2]
(e) $a_1{}^m \equiv b_1{}^m(modn)$,$\forall m \in \mathbb{N}$,by using mathematical induction method. [3]

15. If $ca \equiv cb(modn)$ and (c,n)=1 then prove that $a \equiv b(modn)$ [3]

16. Prove that $x^2 + y^2 = z^2$ has no prime solution. [3]
OR: Prove that Pythagoras equation has no prime solution.

17. Prove that a positive integer n is divided by 3 iff the sum of its digits is divisible by 3. [4]

18. Prove that a positive integer n is divided by 9 iff the sum of its digits is divisible by 9. [4]

by 11. [4]

20. Find a necessary and sufficient condition that a positive integer is divisible by 7. [4]

21. Prove that every number containing more than two digits can be divided by 4 iff the number formed by last two digits can be divided by 4. [4]

22. Is 765432 divided by 3,4,5,7,9,11,13? [2]

USO5CMTH05
Unit-4

1. **Define complete residue system modulo m and reduced residue system modulo m.** [2]

2. **Prove that a set of k integers $a_1, a_2, a_3 \ldots, a_k$ is a complete residue system modulo m iff (i)k=m (ii)$a_i \not\equiv a_j (mod m), \forall i \neq j$.** [5]

3. **If $a_1, a_2, a_3 \ldots, a_k$ is CRS modulo m and (a,m)=1,then prove that $aa_1 + b, aa_2 + b, aa_3 + b, \ldots, aa_k + b$ forms a CRS mod m,where b is any integer.** [2]

4. **Prove that a set of k integers $a_1, a_2, a_3, \ldots, a_k$ is a reduced residue system modulo m iff (i)$k = \Phi(m)$ (ii)$(a_i, m) = 1$, $\forall i$ (iii) $a_i \neq a_j (modm)$, $\forall i \neq j$.** [3]

5. **If $a_1, a_2, a_3 \ldots, a_{\Phi(m)}$ is RRS modulo m and (a,m)=1,then prove that** [3+3]

   (i)$aa_1, aa_2, aa_3 \ldots, aa_{\Phi(m)}$ is RRS mod m.
   (ii)$aa_1 + b, aa_2 + b, aa_3 + b \ldots, aa_{\Phi(m)} + b$ is not RRS mod m,where b is any integer.

6. **State and prove Euler's theorem.** [3]

7. **State and prove Fermat's theorem.** [2]
   OR: State and prove Fermat's little theorem.

8. **If $a^n \equiv 1 (modm)$ and d is order of a modulo m then prove that d/n.** [2]

9. **Define Euler's function . Prove that Euler's function is multiplicative function.** [5]
   OR :If (a,b)=1 then prove that $\phi(ab) = \phi(a)\phi(b)$. [5]

10. **Find all positive integers m and n such that $\phi(mn) = \phi(m) + \phi(n)$.** [5]

11. **Prove that $\Phi(p^k) = p^k - p^{k-1}$,where p is prime.** [4]

12. **Find $\phi(128)$,$\phi(625)$,$\phi(81)$.** [2]

13. **$\sum_{i=0}^{k} \Phi(p^i) = p^k$,where p is prime.** [4]

14. **Find $\phi(32) + \phi(16) + \phi(8) + \phi(4) + \phi(2) + \phi(1)$** [2]
    OR Find $\sum_{i=0}^{5} \Phi(2^i)$.

15. **If $m = p_1^{m_1} p_2^{m_2} p_3^{m_3} \ldots p_k^{m_k}$,where all p_i are primes then prove that**
    $$\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right).$$ [4]

17. Prove that the sum of $\phi(m)$ positive integers less than m $m > 1$ and relatively prime to m is $\frac{m}{2}\phi(m)$.

18. If m is positive integer then prove that $\phi(m) = m \sum_{d/m} \frac{\mu(d)}{d} = \sum_{d/m} \mu\left(\frac{m}{d}\right) d$. [5]

19. Prove that $\sum_{d/m} \mu(d)\phi(d) = 0$ iff m is even. [5]

20. Prove that m is prime iff $\phi(m) + S(m) = mT(m)$. [7]

21. Define Congruence in one unknown .

22. Prove that $ax + b \equiv 0(modm)$, where (a,m)=1 has exactly one solution $x \equiv -a^{\phi(m)-1}(modm)$. [2]

23. Prove that $ax + b \equiv 0(modm)$,where (a,m)=d,$d > 1$ has solution iff d/b. Also prove that it has d solutions $x_i \equiv a + i\frac{m}{d}(modm), i = 0, 1, 2, \ldots d - 1$, of which $x \equiv a\left(mod\frac{m}{d}\right)$ is unique solution of $\frac{a}{d}x + \frac{b}{d} \equiv 0\left(mod\frac{m}{d}\right)$. [6]

24. Prove that $ax + by + c \equiv 0(modm)$ has solution iff d/c,where d=(a,b,m) . Also prove that it has md solutions. [3]

25. Prove that the system of congruences , $x \equiv a(modm); x \equiv b(modn)$ has solution iff $a \equiv b(mod(m, n))$.
Also prove that system has unique solution with respect to modulo [m,n]. [5]

26. Solve the equation [4]
(i) $12x + 15 \equiv 0(mod\ 45)$.
(ii) $18x \equiv 30(mod\ 42)$.
(iii) $9x \equiv 21(mod\ 30)$
(iv) $103x \equiv 57(mod\ 211)$.

27. State and prove Chinese remainder theorem. [6]
OR
State and prove Sun-Tsu theorem.

28. Solve the system of congruences [5]
(i) $x \equiv 2(mod\ 3); x \equiv 3(mod\ 5); x \equiv 2(mod\ 7)$.
(ii) $x \equiv 1(mod\ 4); x \equiv 3(mod\ 5); x \equiv 2(mod\ 7)$.
(iii) $2x \equiv 1(mod\ 5); 3x \equiv 1(mod\ 7)$.
(iv) $x \equiv -2(mod\ 12); x \equiv 6(mod\ 10); x \equiv 1(mod\ 15)$.

SARDAR PATEL UNIVERSITY
B.Sc.(MATHEMATICS) SEMESTER - V
Multiple Choice Question Of US05CMTH05
(Number Theory)
June 2013

Unit-1

Que. Fill in the following blanks.

(1) Square of any odd number is of the form ....
(a) 5k + 1 (b) 3k + 1 (c) 7k + 1 (d) 8k + 1 .

(2) Square of any even number is of the form ....
(a) 4k (b) 5k (c) 7k (d) 6k

(3) If n is even integer then $3^n + 1$ is divisible by ....
(a) 5 (b) 2 (c) 3 (d) 4

(4) If n is odd integer then $3^n + 1$ is divisible by ....
(a) 5 (b) 3 (c) 4 (d) 6

(5) Every square is of the form ....
(a) 9k or 3k + 1 (b) 2k (c) 3k or 9k + 1 (d) 9k or 3k

(6) If k is any positive integer then $k^2 + k + 1$ is .... number .
(a) prime (b) not a square (c) square (d) even

(7) $(-2, -6) =$ ....
(a) -2 (b) 12 (c) 2 (d) -12

(8) $(a, 0) =$ .... , $\forall\ a \in \mathbb{Z}$
(a) $-a$ (b) $|a|$ (c) a (d) 0

(9) $(a, 1) =$ .... , $\forall\ a \in \mathbb{Z}$
(a) $-a$ (b) $|a|$ (c) a (d) 1

(10) If a/b then $(a, b) =$ .... $\forall\ a, b \in \mathbb{Z}$.
(a) a (b) $|a|$ (c) $|b|$ (d) b

(11) If b/a then $(a, b) =$ .... $\forall\ a, b \in \mathbb{Z}$.
(a) a (b) $|a|$ (c) $|b|$ (d) b

(12) $(a, b) \geq$ .... $\forall\ a, b \in \mathbb{Z}$.
(a) a (b) b (c) 0 (d) 1

(13) If $a = qb + r$, $0 \leq r < b$ then $(a, b) =$ ....
(a) (b, r) (b) (q, r) (c) (a, r) (d) r

(14) If a/bc and $(a, b) = 1$ then ....
(a) a (b) a/c (c) b/c (d) c/a

(15) If $(a, ka + b) =$ .... $\forall\ k \in \mathbb{Z}$
(a) b (b) (a, ka) (c) (a, b) (d) 1

(16) If $(b, a + kb) =$ .... $\forall\ k \in \mathbb{Z}$
(a) b (b) (b, kb) (c) (a, b) (d) 1

(17) $(ac, bc) =$ .... $\forall\ c \neq 0$.
(a) $c(a, b)$ (b) (a, b) (c) $(a, b)c$ (d) $(a, b)|c|$

(18) $(a, c) = (b, c) = 1$ then ....
(a) $(ab, c) = 1$ (b) $(a, b) = 1$ (c) $(a, b)c = 1$ (d) $a = b = 1$

(19) $(a, b) = 1$ then $(ab , a + b) =$ ....
(a) a (b) 1 (c) b (d) $a + b$

(20) $(a, b)[a, b] =$ .... $\forall\ a, b \in \mathbb{Z}$.
(a) 1 (b) ab (c) $|ab|$ (d) (a, b)

(21) If a/k, b/k , $k > 0$ then $\left(\frac{k}{a}, \frac{k}{b}\right) =$ ....
(a) 1 (b) $k\,(a, b)$ (c) $\frac{k}{(a, b)}$ (d) $\frac{k}{[a, b]}$

(22) (525, 231) = ...
(a) 10 (b) 31 (c) 21 (d) 7

(23) (1235, 237) = ...
(a) 3 (b) 31 (c) 5 (d) 1

(24) (4676, 366) = ...
(a) 2 (b) 6 (c) 4 (d) 1

(25) [12, 30] = ...
(a) 6 (b) 60 (c) 360 (d) 30

(26) [25, 30] = ...
(a) 750 (b) 60 (c) 150 (d) 5

UNIT-2

(27) T(20) = ...
(a) 3 (b) 4 (c) 5 (d) 6

(28) T(10) = ...
(a) 3 (b) 12 (c) 18 (d) 4

(29) T(11) = ...
(a) 3 (b) 12 (c) 2 (d) 11

(30) S(10) = ...
(a) 18 (b) 12 (c) 20 (d) 10

(31) S(11) = ...
(a) 3 (b) 12 (c) 2 (d) 11

(32) P(10) = ...
(a) 100 (b) 80 (c) 18 (d) 10

(33) P(11) = ...
(a) 3 (b) 2 (c) 100 (d) 11

(34) If a is prime then T(a) = ...
(a) a (b) 2 (c) 1 (d) 3

(35) If a is prime then S(a) = ...
(a) a (b) $a-1$ (c) $a+1$ (d) $a+2$

(36) If a is prime then P(a) = ...
(a) a (b) a - 1 (c) 1 (d) a + 1

(37) T(60) = ...
(a) 60 (b) 12 (c) 18 (d) 61

(38) S(60) = ...
(a) 61 (b) 60 (c) 12 (d) 168

(39) P(60) = ...
(a) 120 (b) 60 (c) 60^6 (d) 60^5

(40) P(20) = ...
(a) 6 (b) 80 (c) 800 (d) 8000

(41) If a is square number then S(a) is ....
(a) even (b) odd (c) prime (d) 0

(42) .... is a Merseine number .
(a) 16 (b) 6 (c) 15 (d) 31

(43) .... is a Mersenne number .
(a) 100 (b) 127 (c) 1 (d) 125

(44) Any prime factor of M_p is .... p
(a) $<$ (b) $=$ (c) $>$ (d) $\leq$

(45) .... is Fermat's number .
(a) 5 (b) 6 (c) 7 (d) 15

(46) .... is Fermat's number .
(a) 4 (b) 6 (c) 17 (d) 15

(47) .... is Fermat's number .
(a) 100 (b) 116 (c) 327 (d) 257

(48) .... is Perfect number .

(a) 12 (b) 6 (c) 9 (d) 25

(49) $F_0F_1F_2 .... F_{n-1} =$ ....

(a) $F_n + 2$ (b) F_{n+2} (c) $F_n - 2$ (d) F_{n-2}

(50) $\mu(6) =$ ....

(a) 1 (b) 0 (c) -1 (d) 2

(51) $\mu(12) =$ ....

(a) 1 (b) 0 (c) -1 (d) 3

UNIT-3

(52) $a \equiv b(mod\, n)$ then ....

(a) n/a (b) n/b (c) n / a - b (d) (a - b) / n .

(53) If $ca \equiv cb(modn) \Rightarrow a \equiv b(mod\, n)$ only if ....

(a) (c , a) = 1 (b) (c , a) = b (c) (c , b) = 1 (d) (c , n) = 1 .

(54) $ax + by = c$ has integer solution if and only if ....

(a) (a , b) = a (b) (a , b) = b (c) $(a, b)/c$ (d) $c/(a, b)$.

(55) $\phi(m) + S(m) = mT(m)$ iff m is ....

(a) not prime (b) odd (c) even (d) prime

(56) Prove that a positive integer n is divided by 3 iff the .... of its digits is divisible by 3.

(a) Subtraction (b) multiplication (c) sum (d) division

(57) Prove that a positive integer n is divided by 9 iff the .... of its digits is divisible by 9.

(a) Subtraction (b) sum (c) multiplication (d) division

(58) Prove that every number containing more than two digits can be divided by 4 iff the number formed by .... digits can be divided by 4.

(a) last two (b) last three (c) first two (d) first three

(59) 765432 is divided by ....

(a) 5 (b) 3 (c) 11 (d) 13

(60) 765432 is divided by ....

(a) 5 (b) 13 (c) 11 (d) 9

(61) 765432 is divisible by ....

(a) 4 (b) 13 (c) 11 (d) 5

(62) 765432 is not divisible by ....

(a) 4 (b) 3 (c) 5 (d) 9

(63) 765432 is not divisible by ....

(a) 4 (b) 3 (c) 9 (d) 13

(64) 765432 is not divisible by ....

(a) 7 (b) 3 (c) 4 (d) 9

UNIT-4

(65) $\phi(m) \leq$ .... , $\forall \cdot m > 1$.

(a) m-1 (b) m (c) m+1 (d) m - 2

(66) If m is prime then $\phi(m)$..................$m - 1$.

(a) $\neq$ (b) $>$ (c) $<$ (d) $=$

(67) If m is not prime then $\phi(m)$..................$m - 1$.

(a) $\neq$ (b) $<$ (c) $>$ (d) $=$

(68) Reduced residue modulo m contains .... elements .

(a) m (b) $\phi(m+1)$ (c) $\phi(m)$ (d) $\phi(m-1)$

(69) If (a , m) = 1 then $a^{\phi(m)} \equiv$ ....$(mod\, m)$.

(a) 1 (b) m (c) 2 (d) 0

(70) If a is any integer and p is prime then $a^p \equiv$ ....$(mod\, p)$.

(a) 1 (b) p (c) a (d) a^{p-1}

(71) If $a^n \equiv 1(mod\, m)$ and d is order of a modulo m then ....

(a) $n < d$ (b) d/n (c) d = n (d) n/d

(72) Any prime factor of M_p is ....

(a) $\geq p$ (b) $= p$ (c) $> p$ (d) $< p$

(73) $\phi\,(300) =$ ....

(a) 80 (b) 90 (c) 60 (d) 300

(74) $\phi\,(128) =$ ....

(a) 128 (b) 16 (c) 64 (d) 32

(75) Odd prime factor of M_p , $(p > 2)$ is of the form ....

(a) 2pt (b) 2pt + 1 (c) 2pt - 1 (d) 2pt + 2

(76) $\{6, 8, 10, 12, 14, 16, 18\}$ is CRS modulo ....

(a) 2 (b) 6 (c) 7 (d) 18

(77) $a^p \equiv a(mod\, p)$ only if p is ....

(a) even (b) prime (c) odd (d) not prime

(78) $a^{\phi(m)} \equiv 1(mod\, m)$ only if ....

(a) (a , m) = a (b) (a , m) = m (c) $(a, m) = 1$ (d) $\phi(m) = m$

(79) $12x + 15 \equiv 0(mod\, 45)$ has only .... solutions.

(a) 3 (b) 12 (c) 15 (d) 1

(80) $18x \equiv 30(mod\, 42)$ has only .... solutions.

(a) 3 (b) 2 (c) 1 (d) 6

(81) $2x + 7y \equiv 5(mod\, 12)$ has only .... solutions.

(a) 1 (b) 2 (c) 12 (d) 5

(82) $(p-1)! + 1 \equiv 0(mod\, p)$ iff p is ....

(a) 4 (b) prime (c) odd (d) even

THEORY OF DIVISIBILITY

Date: 15/01/10

* Divisibility :-

A nonzero integer b divides an integer a if $\exists$ an integer $c \ni a = bc$.

'b divides a' is denoted by b/a

b/a means b is divisor of a <u>or</u> b is factor of a <u>or</u> a is divisible by b <u>or</u> a is multiple of b.

Remarks:-

(1) Clearly $1/a$, $\forall a \in \mathbb{Z}$.

(2) If $b \neq 0$ then $b/0$ and $b/\pm b$.

(3) If $b > 1$ then $b \nmid 1$

(4) If a/b then $a \leq b$ ($\forall a, b > 0$)

* Proper divisor:-

b is said to be a proper divisor of a if $\exists\, c \in \mathbb{Z}$, $c \neq \pm 1$, $c \neq \pm a \ni a = bc$

e.g. (i) -1 is not proper divisor of 3.

because $3 = (-1)(-3) \Rightarrow c = -3 = -a$

(ii) 3 is proper divisor of 6.

because $6 = 3 \times 2 \Rightarrow c = 2 \neq \pm 1$ or ± 6

* Theorems and examples:-

(1) P.T. square of any odd no. is of the form $8k+1$.

proof:- Let $2n+1$ be any odd no. then

$$
\begin{aligned}
(2n+1)^2 &= 4n^2 + 4n + 1 \\
&= 4n(n+1) + 1 \\
&= 4(2k) + 1 \quad (\because n(n+1) \text{ is even} \\
&= 8k + 1, \text{ for some } k \in \mathbb{Z}
\end{aligned}
$$

(2) P.T. square of even no. is of the form $4k$.

proof :- Let $2n$ be any even no. then

$(2n)^2 = 4n^2$

$= 4k$, for some $k \in Z$.

(3) If $b \neq 0$, $c \neq 0$, then prove the following results :

(i) c/b & $b/a \Rightarrow c/a$

proof :-

Here $c/b \Rightarrow b = ck_1$, $b/a \Rightarrow a = bk_2$ $\Big\}$ for some $k_1, k_2 \in$

Now,

$a = bk_2 \Rightarrow a = ck_1k_2$

$\Rightarrow a = ck$, for some $k = k_1 k_2 \in$

$\Rightarrow c/a$

(ii) $b/a \Rightarrow bc/ac$.

proof : Here, $b/a \Rightarrow a = bk$, $k \in Z$

$\Rightarrow ac = bck$ ($\because c \neq 0$

$\Rightarrow bc/ac$.

(iii) If c/a, c/b then $c/(ma+nb)$, $\forall\, m, n \in Z$.

proof :- $c/a \Rightarrow a = ck_1$, $c/b \Rightarrow b = ck_2$ $\Big\}$ for some $k_1, k_2 \in Z$

we have to p.t. $c/(ma+nb)$

i.e p.t. $ma + nb = ck$, $k \in Z$

LHS $= ma + nb = mck_1 + nck_2$

$= c(mk_1 + nk_2)$

$= ck$, for some $k = mk_1 + nk_2$.

$=$ RHS.

(iv) b/a, $a/b \Rightarrow a = b$ or $-b$.

proof :- $b/a \Rightarrow a = bk_1$ } (*) , for some $k_1, k_2 \in \mathbb{Z}$.
$a/b \Rightarrow b = ak_2$ }

Now, $b = ak_2$
$\Rightarrow b = bk_1k_2$
$\Rightarrow k_1k_2 = 1$ $(\because b \neq 0$
$\Rightarrow k_1 = 1, k_2 = 1$ or
$k_1 = -1, k_2 = -1$.

putting this value in (*), we get
$a = b$ & $a = -b$.

(4) State and prove fundamental theorem of divisibility.

Statement :-

For any two integers a, b ($b \neq 0$)* $\exists$ unique $q, r \in \mathbb{Z} \ni a = qb + r$, where $0 \leq r < |b|$. * or $b > 0$

proof :-

We can easily say that, 'a' lies between two consecutive integers of the sequence

$\ldots, -2|b|, -|b|, 0, |b|, 2|b|, \ldots$

Assume that, $q|b| \leq a < (q+1)|b|$ then
$a - q|b| \geq 0$ & $a - (q+1)|b| < 0$
$\Rightarrow a - q|b| < |b|$

$\therefore 0 \leq a - q|b| < |b|$ — (1)

Let $r = a - q|b|$ then by (1), $0 \leq r < |b|$
also $a = q|b| + r$, where $0 \leq r < |b|$ — (2)

If $b > 0$ then $|b| = b$

$\therefore a = qb + r$, where $0 \leq r < |b|$

If $b < 0$ then $|b| = -b$.

$\therefore$ By (2) $a = q(-b) + r = (-q)b + r \Rightarrow a = q_1b + r$,
where $0 \leq r < |b|$

Thus we say that $\exists\ q, r \in \mathbb{Z} \ni a = qb + r$,
where $0 \le r < |b|$ — (3)

Now we prove that q and r are unique.
Suppose, $a = q_1 b + r_1$, where $0 \le r_1 < |b|$ — (4)
be the another representation of a then
by (3) & (4),

$$qb + r = q_1 b + r_1$$
$$\Rightarrow (q - q_1) b = r_1 - r, \text{ where } 0 \le |r - r_1| < |b| \quad \text{— (5)}$$
$$\Rightarrow |(q - q_1) b| = |r_1 - r|$$
$$\Rightarrow |q - q_1| |b| < |b|$$
$$\Rightarrow |q - q_1| < 1$$
$$\Rightarrow q - q_1 = 0$$
$$\Rightarrow q = q_1$$

On putting $q = q_1$ in (5)
$$0 = r_1 - r \Rightarrow r = r_1$$

Thus q & r are unique
Hence theorem is proved

(5) Prove that, $(a-s) / (ab + st) \Rightarrow (a-s) / (at + sb)$.

proof:- We can write,
$$(ab + st) - (at + sb) = a(b - t) - s(b - t)$$
$$\Rightarrow (ab + st) - (at + sb) = (b - t)(a - s)$$
$$\Rightarrow (at + sb) = (ab + st) + (b - t)(a - s)$$

Now,
$$(a-s) / (ab + st) \quad \& \quad (a-s) / (a-s)(b-t)$$
$$\Rightarrow (a-s) / [(ab + st) + (a-s)(b-t)]$$
$$\Rightarrow (a-s) / (at + sb).$$

(6) Prove that product of any three consecutive integers is a multiple of 3.

Proof:-

For any positive integer 'a', we have to p.t. $3 / (a+1)(a+2)(a+3)$.

we know that, $\dfrac{(a+1)(a+2)(a+3)}{6}$

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

$$= \frac{(a+3)!}{3!\,a!}$$

$$= {}^{(a+3)}C_3 = K \text{ (say) } \in Z.$$

Thus $(a+1)(a+2)(a+3) = 6K$, $K \in Z$

$\Rightarrow 6 / (a+1)(a+2)(a+3)$

also $3/6$ & $6 / (a+1)(a+2)(a+3)$

$\Rightarrow 3 / (a+1)(a+2)(a+3)$

$\Rightarrow (a+1)(a+2)(a+3)$ is multiple of 3, if $a>0$.

Similarly we can prove this result for any -ve integer 'a' and also for $a=0$.

Hint * for -ve integer,

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

(7) (i) If n is even integer then prove that, 3^n+1 is divisible by 2.

(ii) If n is odd integer then prove that, 3^n+1 is divisible by 2^2.

(iii) If n is any integer then prove that, 3^n+1 is not divisible by 2^m, where $m \geq 3$.

proof :-

(i) If n is even integer then $n=2n_1$

we have to p.t $2 / 3^n+1$.

i.e. p.t $(3^n+1)=2k$, for some $k \in Z$.

$$\begin{aligned}
L.H.S. = 3^n+1 &= 3^{2n_1}+1 \\
&= (3^{n_1})^2+1 \\
&= (8k_1+1)+1 \quad \text{(By result (1)} \\
&= 8k_1+2 \\
&= 2(4k_1+1) \quad \text{— (*)} \\
&= 2k, \text{ where } 4k_1+1=k \in Z
\end{aligned}$$

Thus 3^n+1 is divisible by 2.

(ii) If n is odd no. integer then $n=2n_1+$

we have to p.t, $2^2 / 3^n+1$

i.e p.t $3^n+1=4k$, for some $k \in$

$$\begin{aligned}
L.H.S. &= 3^n+1 \\
&= 3^{2n_1+1}+1 \\
&= (3^{n_1})^2 \cdot 3+1 \\
&= (8k_1+1) \cdot 3+1 \\
&= 24k_1+3+1 \\
&= 24k_1+4 \\
&= 4(6k_1+1) \quad \text{— (**)} \\
&= 4k, \text{ where } k=6k_1+1 \in Z
\end{aligned}$$

Thus 3^{n+1} is divisible by 2^2 if n is odd

(iii) If n is even then by (*)

$$3^n+1 = 2(4k_1+1) \quad \&$$

If n is odd then by (**)

$$3^n+1 = 4(6k_1+1)$$

Clearly $4k_1+1$ & $6k_1+1$ both are odd no's.

$\therefore$ they are not multiple of 2

$$\therefore \; 2^m \nmid 3^n+1 \quad \text{for } m \geq 3.$$

* Square number :-

An integer 'a' is said to be a square number if it is a square of some other integers. i.e. $a = b^2$, for some $b \in \mathbb{Z}$, $b \neq 0$.

e.g. $1 = (-1)^2$, $4 = (2)^2$, $9 = (3)^2$, --- are square numbers.

(8) P.T. every square no. is of the form $9k$ or $3k+1$, for some $k \in \mathbb{Z}$.

proof:-

We know that any integer can be written in the form $3n$ or $3n \pm 1$, $n \in \mathbb{Z}$.

Now, $(3n)^2 = 9n^2 = 9k$

$$(3n \pm 1)^2 = 9n^2 \pm 6n + 1$$

$$= 3(3n^2 \pm 2n) + 1$$

$$= 3k+1, \quad \text{where } k = 3n^2 \pm 2n \in \mathbb{Z}$$

Thus every square no. is of the form $9k$ or $3k+1$, for some $k \in \mathbb{Z}$.

(9) If a positive odd integer n can be decomposed in a product of two divisi[illegible] then prove that n can be written as a difference of two square numbers.

proof:-

Here n is odd integer

let $n = ab$, for some odd integers a & [illegible]

clearly $\frac{a+b}{2}$ and $\frac{a-b}{2}$ are integers.

also we know that $n = ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)$

Thus n is difference of two square no[illegible]

(10) If k is any positive integer then prove that, k^2+k+1 is not a square number.

proof:-

Here k is positive integer.

$\therefore k^2 < k^2+k+1 < k^2+2k+1$

$\Rightarrow k^2 < k^2+k+1 < (k+1)^2$

Since $(k+1)^2$ is a square no which is next to k^2

$\therefore k^2+k+1$ is not a square no.

(11) Let g be a +ve integer greater than 1 then prove that every +ve integer 'a' can be written uniquely in the form

$a = c_n g^n + c_{n-1} g^{n-1} + \dots + c_1 g + c_0$ —(1)

where $n \geq 0$, $c_i \in Z$, $0 \leq c_i < g$, $c_n \neq 0$.

[Here g is called the base of 'a' and a is denoted by $(c_n c_{n-1} c_{n-2} \cdots)_g$]

Proof:- We prove this result by using mathematical induction method on 'a'.

For $a=1$, we can write $a=c_0$, where $c_0=1$

Suppose result (1) is true for any positive integer less than 'a' then we have to p.t. result is true for +ve integer 'a'.

We know that, $g>1$ & $a>0$.

Clearly 'a' lies between two consecutive numbers of the following sequence

$$g^0, g^1, g^2, g^3, \ldots, g^n, \ldots$$

$\therefore \exists$ unique $n \ni g^n \le a < g^{n+1}$

Now by division algorithm property for a & g we can write, $a = c_n g^n + r,\ 0 \le r < g^n$

where $c_n, r \in Z$

— (2)

Clearly $0 < c_n < g$

because,

if $c_n > g$ then

$c_n = g+k$

$\Rightarrow a = (g+k)g^n + r$

$\Rightarrow a = g^{n+1} + kg^n + r$

$\Rightarrow a > g^{n+1}$ ※ $(\because a < g^{n+1}$

If $r=0$ then by (2) $a = c_n g^n$.

i.e. $a = c_n g^n + 0g^{n-1} + \cdots + 0g + 0$

Thus result (1) is true when $r=0$.

If $0 < r < g^n$ then by (2)

$r = a - c_n g^n < a$

Thus $r < a$

$\therefore$ Result (1) is true for 'r'

$\therefore$ We can write, $r = b_t g^t + b_{t-1} g^{t-1} + \cdots + b_1 g + b_0$, Now by (2), we get

$$a = c_n g^n + b_r g^r + b_{r-1} g^{r-1} + \cdots + b_1 g + b_0$$

Thus result (1) is true for 'a'.

Hence by induction method we say that result (1) is true for all +ve integers 'a'

Now we p.t 'a' can be represented uniquely.

Suppose another representation of 'a' is

$$a = d_m g^m + d_{m-1} g^{m-1} + d_{m-2} g^{m-2} + \cdots + d_1 g + d_0 \quad \text{—(3)}$$

where $m \geq 0$, $d_i \in \mathbb{Z}$, $0 \leq d_i < g$, $d_m \neq 0$.

We have to p.t $n = m$ and $c_i = d_i$, $\forall i$.

By comparing (1) & (3), we get

$$e_s g^s + e_{s-1} g^{s-1} + \cdots + e_1 g + e_0 = 0 \quad \text{—(4)}$$

s is the largest where $e_s = c_s - d_s$ | If

true i.e. $\exists\ e_s \neq 0$

suppose If $e_s = c_s - d_s \neq 0$ $e_i = c_i - d_i \neq 0$ for some i

If $s = 0$ then by (4) $e_0 = 0$

$\Rightarrow c_0 - d_0 = 0$

$\Rightarrow c_0 = d_0$ ✗ ($\because e_s \neq 0$)

$\therefore s > 0$

also we can write,

$$|e_i| = |c_i - d_i| < g \quad (\because c_i < g,\ d_i < g)$$

$$\Rightarrow \boxed{|e_i| \leq g-1,\ \forall i}$$

also from (4)

$$e_s g^s = -[e_{s-1} g^{s-1} + e_{s-2} g^{s-2} + \cdots + e_1 g + e_0] \quad \text{—(5)}$$

we know that $g^s < |e_s g^s|$ $(\because e_s \in \mathbb{Z})$

$= | e_{s-1} g^{s-1} + e_{s-2} g^{s-2} + \cdots + e_1 g + e_0 |$

$\leq |e_{s-1}||g^{s-1}| + |e_{s-2}||g^{s-2}| + \cdots + |e_1||g| + |$

(by (5))

$\leq (g-1)[g^{s-1} + g^{s-2} + \cdots + g + 1]$ $(\because g > 1)$

$(\& |e_i| \leq g-1)$

$= g^s - 1.$

Thus $g^s < g^s - 1$ ※

$\therefore$ we say that $e_i = c_i - d_i = 0, \forall i.$

~~i.e. $c_s = d_s, \forall s$~~

i.e $c_i = d_i, \forall i.$

$\therefore n = m.$ and $c_i = d_i, \forall i.$

Hence uniqueness is proved

* Remark:-

If $g=2$ then by above thm we say that every +ve integer 'a' can be expressed uniquely in the form, $a = c_n 2^n + c_{n-1} 2^{n-1} + \cdots + c_1 2 + c_0.$

$c_n \neq 0.$

i.e. $c_i = 0$ or 1

In symbol $a = (c_n c_{n-1} c_{n-2} \cdots c_1 c_0)_2.$

(12) Express the following nos in the base as mentioned :-

(i) 2107 in the base of 2, 12, 8.

Soln :- * $2107 = 2^{11} + 59$

$= 2^{11} + 2^5 + 27$

$= 2^{11} + 2^5 + 2^4 + 11$

$= 2^{11} + 2^5 + 2^4 + 2^3 + 3$

$= 2^{11} + 2^5 + 2^4 + 2^3 + 2^1 + 1$

$\therefore 2107 = (100000111011)_2$

which is required binary form.

* $2107 = 12^3 + 379$

$= 12^3 + 2\times 12^2 + 91$

$= 12^3 + 2\times 12^2 + 7\times 12 + 7$

$\therefore (2107) = (1277)_{12}$

* $2107 = 4\times 8^3 + 59$

$= 4\times 8^3 + 7(8) + 3$

$\therefore (2107) = (4073)_8$.

(ii) 17872 in base of 8.

Sol^n:- $17872 = 4\times 8^4 + 1488$

$= 4\times 8^4 + 2\times 8^3 + 464$

$= 4\times 8^4 + 2\times 8^3 + 7\times(8)^2 + 16$

$= 4\times 8^4 + 2\times 8^3 + 7\times 8^2 + 2\times 8 + 0$

$= (42720)_8$.

* Common divisor:-

Let $a, b \in \mathbb{Z}$, d is said to be common divisor of a and b if d/a & d/b

* Greatest common divisor:-

Let $a, b \in \mathbb{Z}$ with atleast one of them different from zero then d is said to be greatest common divisor (g.c.d) of a & b if it satisfies the following condition.

(1) d/a & d/b.

(2) if c/a & c/b, then $c \le d$

g.c.d. of a and b is denoted by (a, b) or g.cd.(a, b)

eg. $(2, -6) = 2$, $(-14, 21) = 7$

$(5, 21) = 1$

* Remark :-

$(a,1) = 1 , \forall a \in Z$ $\qquad (a,b) \geq 1, \forall a,b$

$(a,0) = |a| , \forall a \in Z$

$(-3,0) = 3 .$

if a/b then $(a,b) = |a| , \forall a \in Z$.

if b/a then $(a,b) = |b| , \forall b \in Z$.

$(a,b) \geq 1$

(13) If $a = qb + r$, $0 \leq r < b$ then prove that,
$(a,b) = (b,r)$. $\quad$ P.T $(b,r) = d$

proof :- Let $(a,b) = d$ then by definition

d/a & $d/b \Rightarrow d/qb$.

also d/a & $d/qb \Rightarrow d/a-qb \Rightarrow d/r$.

Thus d/b & d/r.

Now, whenever c/b and c/r then

c/qb and c/r.

$\Rightarrow c/qb+r \Rightarrow c/a$

Thus c/a and c/b & g.c.d. $(a,b) = d$

$\therefore c \leq d$

Thus $(b,r) = d$

Hence $(a,b) = (b,r)$.

Discuss Euclidean algo. to find gcd of two nos.

or

(14) Find g.c.d. of two nos. by using Euclidian algorithm.

solⁿ :-

Let a and b $(a \geq b)$ be any +ve integers.

then by divison algorithm property,

$$a = q_1 b + r_1 \quad , 0 \le r_1 < b$$
$$b = q_2 r_1 + r_2 \quad , 0 \le r_2 < r_1$$
$$r_1 = q_3 r_2 + r_3 \quad , 0 \le r_3 < r_2$$
$$\vdots$$
$$r_{n-2} = q_n r_{n-1} + r_n , \quad 0 \le r_n < r_{n-1}$$
$$r_{n-1} = q_{n+1} r_n + 0$$

By above ex (prove it)

$$(a,b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = \cdots$$
$$= (r_{n-1}, r_n) = (r_n, 0)$$

Thus $(a,b) = r_n$.

(15) Find g.c.d of the following numbe by using Euclidian algorithm.

(i) $(525, 231)$.

Sol^n.

$$525 = (2)(231) + 63$$
$$231 = (3)(63) + 42$$
$$63 = (1)(42) + 21$$
$$42 = (2)(21) + 0.$$
$$\therefore (525, 231) = 21$$

(ii) $(1235, 237)$.

Sol^n.

$$1235 = (5)(237) + 50$$
$$237 = (4)(50) + 37$$
$$50 = (1)(37) + 13$$
$$37 = (2)(13) + 11$$
$$13 = (1)(11) + 2$$
$$11 = (5)(2) + 1$$
$$2 = (1)(1) + 1 \qquad \therefore (1235, 237) = 1.$$

(iii) $(4676, 366)$.

Sol^n.

$$4676 = (12)(366) + 284$$
$$366 = (1)(284) + 82$$
$$284 = (3)(82) + 38$$
$$82 = (2)(38) + 6$$
$$38 = (6)(6) + 2$$
$$6 = (3)(2) + 0$$
$$\therefore (4676, 366) = 2$$

(iv) $(3054, 12379)$.

Sol^n.

$$12379 = (4)(3054) + 163$$
$$3054 = (18)(163) + 120$$
$$163 = (1)(120) + 43$$
$$120 = (2)(43) + 34$$
$$43 = (1)(34) + 9$$
$$34 = (3)(9) + 7$$
$$9 = (1)(7) + 2$$
$$7 = (2)(3) + 1$$
$$2 = (1)(1) + 1$$
$$1 = 1 + 0$$
$$\therefore (3054, 12379) = 1$$

(16) If $(a,b) = d$ then p.t. $\exists\ x, y \in Z \ni xa + yb = d$.

or

If $(a,b) = 1$ then p.t. $\exists\ x, y \in Z \ni xa + yb = 1$.

Proof:

Here $(a,b) = d$

By divison algorithm property

$a = q_1 b + r_1 \quad , 0 \le r_1 < b$

$b = q_2 r_1 + r_2 \quad , 0 \le r_2 < r_1$

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

$\vdots$

$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \quad , 0 \le r_{n-1} < r_{n-2}$

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

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

then

$(a,b) = r_n$

$\therefore r_n = d$

Now by $(*)$ we can write,

$r_n = r_{n-2} - q_n r_{n-1}$.

$\Rightarrow d = r_{n-2} - q_n (r_{n-3} - q_{n-1} r_{n-2})$

$(\because r_{n-3} = q_{n-1} r_{n-2} + r$

$\Rightarrow d = (1 + q_n q_{n-1}) r_{n-2} - q_n r_{n-3}$

$\Rightarrow d = x_1 r_{n-2} + y_1 r_{n-3}$

Thus d is linear combination of r_{n-2} and r_{n-3}.

Continuing this process in reverse orde finally we get d is linear combination of a & b.

$\therefore d = xa + yb$ for some $x, y \in Z$

On putting $d = 1$ we can easily p.t.

$xa + yb = 1$ for some $x, y \in Z$.

(17) $(a,b) = 1$ iff $\exists \, x, y \in Z \ni xa + yb = 1$.

proof:- If $(a,b) = 1$ then by above thm.

$\exists \, x, y \in Z \ni ax + by = 1$.

converse part:-

If $\exists\ x, y \in Z \ni ax+by=1$ then we have to p.t. $(a,b)=1$.

suppose $(a,b)=d$ then $d/a, d/b$

$\Rightarrow d/ax, d/by$

$\Rightarrow d/ax+by$

$\Rightarrow d/1$

$\Rightarrow d=1$

Thus $(a,b)=1$.

(18) corrolary:- If $(a,b)=d$ then p.t. $\left(\frac{a}{d}, \frac{b}{d}\right)=1$.

proof:-

$(a,b)=d \Rightarrow d/a, d/b$

$\Rightarrow a=k_1 d, b=k_2 d$, for some $k_1, k_2 \in Z$

$\Rightarrow \frac{a}{d}=k_1, \frac{b}{d}=k_2$

i.e. $\frac{a}{d}, \frac{b}{d} \in Z$.

also $(a,b)=d$

$\therefore$ By thm $\exists\ x, y \in Z \ni ax+by=d$

$\Rightarrow \frac{a}{d}x+\frac{b}{d}y=1$

$\Rightarrow \left(\frac{a}{d}, \frac{b}{d}\right)=1$ (by above thm)

(19) corollary:- If a/c, b/c and $(a,b)=1$ then p.t ab/c.

proof:- $\left.\begin{array}{l} a/c \Rightarrow c=k_1 a \\ b/c \Rightarrow c=k_2 b \end{array}\right\}$ for some $k_1, k_2 \in Z$.

also $(a,b)=1 \Rightarrow ax+by=1$ for some $x, y \in Z$.

we have to p.t ab/c.
i.e p.t $c = kab$, for some $k \in Z$.

Now, $c = c \cdot 1$
$= c(ax+by)$
$= cax + cby$.
$= k_2 bax + k_1 aby$
$= ab(k_2 x + k_1 y)$
$= kab$, where $k = k_2 x + k_1 y \in Z$

(20) If a/bc and $(a,b)=1$ then a/c

proof:-
$a/bc \Rightarrow bc = k_1 a$, for some $k_1 \in Z$.
$(a,b)=1 \Rightarrow ax+by=1$ " " $x, y \in Z$
we have to p.t a/c
i.e. $c = ak$, for some $k \in Z$.

Now, $c = c \cdot 1$
$= c \cdot (ax+by)$
$= cax + cby$
$= cax + k_1 ay$
$= a(cx + k_1 y)$
$= ak$, where $k = cx + k_1 y$

(21) P.T. $(a,b)=d$ iff the following cond. are satisfied:
(i) d/a & d/b.
(ii) whenever c/a, c/b then c/d.

proof:-
If $(a,b)=d$ then d/a & d/b

and $ax+by=d$ for some $x,y \in Z$.

if c/a, c/b then c/ax, c/by

$\Rightarrow c/ax+by$

$\Rightarrow c/d$

converse part:-

If given two conditions are satisfied then by condition (i) d/a & d/b. &

" " (ii) whenever c/a, c/b then c/d

$\Rightarrow c \le d$

Hence $(a,b)=d$

(22) P.T. common divisor of two numbers is also the divisor of their g.c.d

Proof:-

we have to p.t. if c/a, $c/b \Rightarrow c/(a,b)$

Let $(a,b)=d$ then $ax+by=d$ for some $x,y \in Z$.

$c/a \Rightarrow c/ax$

$c/b \Rightarrow c/by$

Now c/ax, c/by

$\Rightarrow c/ax+by \Rightarrow c/d$

(23) P.T. $(a,b)=(a,ka+b)$, for $k \in Z$.

Proof:- Let $(a,b)=d$ and $(a,ka+b)=d'$.

Now, $(a,b)=d \Rightarrow d/a$, d/b

$\Rightarrow d/a$, d/ka, d/b

$\Rightarrow d/a$, $d/ka+b$

$\Rightarrow d/(a,ka+b)$.

also, $(a, ka+b) = d'$

$\Rightarrow d'/a,\ d'/ka+b$

$\Rightarrow d'/a,\ d'/ka,\ d'/ka+b$

$\Rightarrow d'/a,\ d'/ka+b-ka$

$\Rightarrow d'/a,\ d'/b$

$\Rightarrow d'/(a,b)$

$\Rightarrow d'/d$

$\Rightarrow d' \leq d$ — (**)

By (*) & (**), $d = d'$

i.e $(a,b) = (a, ka+b),\ k \in Z$

(24) $(a,b) = (b, a+kb)$, $k \in Z$

proof:- Let $(a,b) = d$ & $(b, a+kb) = d'$

Now,

$(a,b) = d \Rightarrow d/a,\ d/b$

$\Rightarrow d/a,\ d/b,\ d/kb$

$\Rightarrow d/b,\ d/a+kb$

$\Rightarrow d/(b, a+kb)$

$\Rightarrow d/d' \Rightarrow d \leq d'$ —(*)

also, $(b, a+kb) = d'$.

$\Rightarrow d'/b,\ d'/a+kb$

$\Rightarrow d'/b,\ d'/kb,\ d'/a+kb$

$\Rightarrow d'/b,\ d'/a$

$\Rightarrow d'/(a,b)$

$\Rightarrow d'/d \Rightarrow d' \leq d$ —(**)

(25) P.T. $(a,b) = (a+b, a)$

proof:- $(a,b) = d$ & $(a+b, a) = d'$

$(a,b) = d \Rightarrow d/a,\ d/b$

$\Rightarrow d/a,\ d/a+b$

$\Rightarrow d/(a, a+b)$

$\Rightarrow d/d' \Rightarrow d \leq d'$

$(a+b, a) = d'$

$\Rightarrow d'/a+b,\ d'/a$

$\Rightarrow d'/a,\ d'/b$

$\Rightarrow d'/(a,b)$

$\Rightarrow d'/d \Rightarrow d' \leq d.$

Hence, $d = d'$.

→ Similarly, $(a,b) = (b, a-kb)$

$= (100a+b, a)$

$= (a+100b, b).$

(26) P.T. $(a,b)c = (ac, bc)$. if $c>0$.

proof:-

Let $(a,b) = d$ & $(ac, bc) = d'$

then we have to p.t. $dc = d'$.

Now,

$(a,b) = d \Rightarrow d/a,\ d/b$

$\Rightarrow dc/ac,\ dc/bc \quad (\because c \neq 0)$

$\Rightarrow dc/(ac, bc)$

$\Rightarrow dc/d'$

$\Rightarrow dc \leq d'.$

also, $(ac, bc) = d'$

$\Rightarrow d'/ac,\ d'/bc$

$\Rightarrow d'/acx,\ d'/bcy \quad \left(\because (a,b) = d \Rightarrow xa + yb = d,\ x, y \in Z\right)$

$\Rightarrow d'/acx+bcy$

Date: / /

$\Rightarrow d' / c(ax+by)$

$\Rightarrow d' / cd$

$\Rightarrow d' \leq cd$

Hence, $dc = d'$ i.e. $(a,b)c = (ac, bc)$, (if $c>0$)

(27) Prove or disprove:

(i) $(a,b)c = (ac, bc)$

Sol^n:- let $a=2$, $b=4$, $c=-3$ then

$$
\begin{aligned}
L.H.S. &= (a,b)c \\
&= (2,4)(-3) \\
&= 2(-3) \\
&= -6
\end{aligned}
$$

$$
\begin{aligned}
R.H.S. &= (ac, bc) \\
&= (2(-3), 4(-3)) \\
&= (-6, -12) \\
&= 6
\end{aligned}
$$

Thus $L.H.S. \neq R.H.S.$

$\therefore$ Given statement is not true

(ii) $(a,b)|c| = (ac, bc)$, $\forall c \neq 0$.

Sol^n: we will prove above result

case-1 :-

If $c>0$ then by above result

$(a,b)c = (ac, bc)$ (proveit)

$\Rightarrow (a,b)|c| = (ac, bc)$. ($\because c>0$)

case-2 :-

If $c<0$ then $|c| = -c > 0$.

Now, $RHS = (ac, bc)$

$= (a(-c), b(-c))$

$= (a,b)|c|$ $(\because |c|>0$, by case (i))

Hence, $(a,b)|c| = (ac,bc)$, $\forall c \neq 0$.

(28) If $(a,b)=1$ then p.t. $(ac,b)=(c,b)$.

proof:

Let $(ac,b)=d$ & $(c,b)=d'$ then we have to p.t. $d=d'$.

Now, $(ac,b)=d \Rightarrow d/ac,\ d/b$

$\Rightarrow d/ac,\ d/b,\ d/bc$

$\Rightarrow d/(ac,bc),\ d/b$

$\Rightarrow d/|c|(a,b),\ d/b$.

$\Rightarrow d/|c|,\ d/b$ $(\because (a,b)=1$

$\Rightarrow d/c,\ d/b$

$\Rightarrow d/(c,b)$

$\Rightarrow d/d'$

$\Rightarrow d \leq d'$.

also,

$(c,b)=d' \Rightarrow d'/c,\ d'/b$

$\Rightarrow d'/ac,\ d'/b$

$\Rightarrow d'/(ac,b)$

$\Rightarrow d'/d$

$\Rightarrow d' \leq d$

$\therefore \boxed{d=d'}$

Date : / /

(29) P.T. $(a,b)=1 \Rightarrow (a,bc)=(a,c)$.

proof:- Let $(a,bc)=d$ & $(a,c)=d'$.

$(a,bc)=d \Rightarrow d/a,\ d/bc$

$\Rightarrow d/ac,\ d/a,\ d/bc$

$\Rightarrow d/(ac,bc),\ d/a$

$\Rightarrow d/|c|(a,b),\ d/a$

$\Rightarrow d/|c|,\ d/a$

$\Rightarrow d/a,\ d/c$

$\Rightarrow d/(a,c)$

$\Rightarrow d/d'$

$\Rightarrow d \le d'$

$(a,c)=d' \Rightarrow d'/a,\ d'/c$

$\Rightarrow d'/a,\ d'/c,\ d'/bc$

$\Rightarrow d'/(a,bc)$

$\Rightarrow d'/d$

$\Rightarrow d' \le d$

$\therefore d=d'$.

(30) If $(a,c)=1=(b,c)$ then p.t. $(ab,c)=1$

proof:- $(a,c)=1$ then by above result (prove:

$(ab,c)=(b,c)=1$

(31) P.T. $(a,b)=1 \Rightarrow (ab,a+b)=1$.

proof:- we know that, $(a,b)=(a,ka+b)$

$=(b,a+kb)$

for $k=1$, $(a,b)=(a,a+b)=(b,a+b)$

$\Rightarrow (a, a+b) = (b, a+b) = 1 \quad (\because (a,b) = 1$

$\Rightarrow (ab, a+b) = 1 \quad$ (by above ex)

(32) If $c>0$ is common divisor of a & b then p.t. $\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{(a,b)}{c}$.

proof:- Here $c>0$ then $\left(\frac{a}{c}, \frac{b}{c}\right)c = \left(\frac{a}{c}c, \frac{b}{c}c\right)$

$= (a,b)$

$\Rightarrow \left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c}(a,b)$

(33) P.T. $(a,b) = c$ iff $\left(\frac{a}{c}, \frac{b}{c}\right) = 1 \quad (\forall c>0)$

proof:- $\left(\frac{a}{c}, \frac{b}{c}\right) = 1$

$(a,b) = c \Leftrightarrow \frac{(a,b)}{c} = 1$

$\Leftrightarrow \left(\frac{a}{c}, \frac{b}{c}\right) = 1$.

(34) Prove that, $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$, $\forall a > 1$, m, n are +ve integers.

proof:- case-1 :- If $m=n$ then

$L.H.S. = (a^n - 1, a^n - 1) = a^n - 1$

$R.H.S. = a^{(n,n)} - 1 = a^n - 1$

Thus. L.H.S. = R.H.S.

case-2 :-

If $m \neq n$, let $(m,n) = r_n$

Let $m>n$ then by divison algorithm property, we say that

$m = qn + r. \quad 0 \le r < n. \quad -(1)$

also we can write

$a^m - 1 = (a^n-1)a^{m-n} + a^{m-n} - 1$ &

$a^{m-n} - 1 = (a^n-1)a^{m-2n} + a^{m-2n} - 1$

$\therefore a^m - 1 = (a^n-1)(a^{m-n} + a^{m-2n}) + a^{m-2n} - 1.$

continuing this process, we get

$a^m - 1 = (a^n-1)(a^{m-n} + a^{m-2n} + a^{m-3n} + \dots + a^{m-}$

$+ a^{m-qn} - 1$

$\therefore a^m - 1 = p(a^n-1) + (a^r - 1).$

then by Euclidian algorithm, we say that,

(a^m-1, a^n-1)

$= (a^n-1, a^r-1)$

$= (a^r-1, a^{r_1}-1)$

$= (a^{r_1}-1, a^{r_2}-1)$

$\vdots$

$= (a^{r_n}-1, 0)$

$= a^{r_n} - 1$

$= a^{(m,n)} - 1$

Hence result is proved.

* Remarks:-

(1) we can also find g.c.d of more than two integers say $a_1, a_2, \dots, a_n$.
It is denoted by $(a_1, a_2, \dots, a_n)$

(2) $a_1, a_2, \dots, a_n$ are said to be mutual relatively prime if $(a_1, a_2, \dots, a_n) = 1$

(3) $a_1, a_2, \dots, a_n$ are said to be pairwise relatively prime if $(a_i, a_j) = 1, \ \forall i \neq j$.
$(i, j = 1, 2, \dots, n)$.

e.g. $(2,4,6,7)=1$

$\therefore$ 2, 4, 6 & 7 are mutually relatively prime

but $(2,4)=2$

$\therefore$ ~~2, 6, 6, 4, 7~~ $\therefore$ 2, 4, 6 & 7 are not pairwis

relatively prime

~~also~~,

e.g. $(3,4)=1,\ (4,5)=1,\ (3,5)=1,\ (5,7)=1,$

$(4,7)=1,\ (3,7)=1$

$\therefore$ 3, 4, 5, 7 are pairwise relatively prin

also

$(3,4,5,7)=1$

$\therefore$ 3, 4, 5 & 7 are mutually relatively pri

* Thus pairwise relatively prime no^s. are always mutually relatively prime

proof:-

Let $a_1, a_2, \cdots, a_n$ are pairwise relatively prime $\therefore (a_i, a_j)=1, \forall i \neq j$

$(i,j=1,2,\cdots n$

since $(a_i, a_j)=1, \forall i \neq j\ (i.j=1,2,\cdots n)$,

$(a_1, a_2, \cdots, a_n)=1$

$\therefore a_1, a_2, \cdots, a_n$ are also mutually relatively prime.

(35) Prove that, $(a,b,c)=((a,b),c)$.

proof: Let $(a,b,c)=d$ and $((a,b),c)=d'$

Now, $\underbrace{(a,b,c)}_{=d} \Rightarrow d/a,\ d/b,\ d/c$

$\Rightarrow d/(a,b),\ d/c$

$\Rightarrow d/((a,b),c)$

$\Rightarrow d/\ \ \Rightarrow d \leq d'$

also,

$$((a,b),c) = d' \Rightarrow d'/(a,b) \,,\; d'/c$$

$$\Rightarrow d'/a \,,\; d'/b \,,\; d'/c$$

$$\Rightarrow d'/(a,b,c)$$

$$\Rightarrow d'/d$$

$$\Rightarrow d' \leq d$$

$\therefore\ d = d'$

Hence $(a,b,c) = ((a,b),c)$.

(35) P.T. $(a,b,c) = (a,(b,c))$.

proof :- Let $(a,b,c) = d$, $(a,(b,c)) = d'$.

Now, $(a,b,c) = d \Rightarrow d/a \,,\; d/b \,,\; d/c$

$$\Rightarrow d/a \,,\; d/(b,c)$$

$$\Rightarrow d/(a,(b,c))$$

$$\Rightarrow d/d'$$

$$\Rightarrow d \leq d'.$$

also, $(a,(b,c)) = d' \Rightarrow d'/a \,,\; d'/(b,c)$

$$\Rightarrow d'/a \,,\; d'/b \,,\; d'/c$$

$$\Rightarrow d'/(a,b,c)$$

$$\Rightarrow d' \leq d.$$

Hence $d = d'$.

Similarly

$$(a,b,c) = ((a,c),b)$$

(36) P.T $d/(a,b) \Rightarrow d/a,\ d/b$

proof :- Let $(a,b) = d'$

Now, $d/(a,b) \Rightarrow d/d'$

Since, d/d' & d'/a

$\therefore d/a$

also, d/d' & d'/b

$\therefore d/b$

$\therefore d/(a,b) \Rightarrow d/a,\ d/b$

(37) If $a = qc + r$ & $b = q_1 c + r_1$ $(0 \le r < c,\ 0 \le r_1 < c)$ then p.t. $(a,b,c) = (r, r_1, c)$.

proof :-

$a = qc + r \Rightarrow (a,c) = (c,r)$

$b = q_1 c + r_1 \Rightarrow \cancel{(b, a_1) = (q_1, r)}\ (b,c) = (c, r_1)$

$$
\begin{aligned}
LHS = (a,b,c) &= ((a,c),b) \\
&= ((c,r),b) \\
&= (c,r,b) \\
&= ((b,c),r) \\
&= ((c,r_1),r) \\
&= (c, r_1, r) \\
&= (r, r_1, c) = R.H.S.
\end{aligned}
$$

Least common multiple (L.C.M.) :-

A positive integer m is said to be a least common (~~[illegible]~~) multiple of a & b if (i) $a/m,\ b/m$

(ii) whenever $a/m_1,\ b/m_1$ then $m \le m_1$ (with $m_1 > 0$)

L.C.M. of a & b are denoted by $[a, b]$ or $l.c.m.(a, b)$.

e.g. * $[12, 30] = 60$

$12 = 2 \times 2 \times 3$

$30 = 2 \times 3 \times 5$

$[12, 30] = 2 \times 2 \times 3 \times 5 = 60$

6	12	30
2	2	5
5	1	5
	1	1

* $[25, 30] = 150$

$25 = 5^2$

$30 = 5 \times 3 \times 2$

$[25, 30] = 5^2 \times 3 \times 2 = 150$

5	25	30
5	5	6
6	1	6
	1	1

(38) P.T. common multiple of two non zero integers is also a multiple of their l.c.m.

proof :- Let $[a, b] = m$

then we have to p.t

$a/m', \; b/m' \Rightarrow m/m'$

or P.T. $a/m', \; b/m' \Rightarrow [a,b]/m'$

clearly $m \leq m'$.

also by divison algorithm prop.

we can write, $m' = qm + r, \; 0 \leq r < m$

if $0 < r < m$ then we know that

$a/m', \; a/m, \; b/m', \; b/m$

$\Rightarrow a/m', \; a/qm, \; b/m', \; b/qm$

$\Rightarrow a/m'-qm, \; b/m'-qm$

$\Rightarrow a/r, \; b/r$

$\Rightarrow m \leq r \; (\because m = [a, b]$

$\therefore r = 0$

$\therefore$ By (1) $m' = qm$

$\Rightarrow m / m'$

i.e. $[a,b] / m'$.

(39) State and prove relation between L.C.M. & g.c.m. of two numbers.

or

If $ab > 0$ then p.t. $[a,b](a,b) = ab$.

proof :-

Let $[a,b] = m$ & $(a,b) = d$ then we have p.t. $md = ab$.

Now,

$[a,b] = m \Rightarrow a/m,\ b/m$

$\Rightarrow ab/mb,\ ab/ma$

$\Rightarrow ab/(ma, mb)$

$\Rightarrow ab/m(a,b)$ $(\because m > 0$

$\Rightarrow ab/md$

$\Rightarrow ab \le md$

also,

$(a,b) = d \Rightarrow d/a,\ d/b$

$\Rightarrow a = k_1 d,\ b = k_2 d,\ k_1, k_2 \in Z$

$\Rightarrow \frac{a}{d}$ & $\frac{b}{d} \in Z$

Now, $a/a,\ b/b$

$\Rightarrow a/a\left(\frac{b}{d}\right),\ b/b\left(\frac{a}{d}\right)$

$\Rightarrow a/\frac{ab}{d},\ b/\frac{ab}{d}$

$\Rightarrow [a,b] / \frac{ab}{d}$

$$\Rightarrow \quad m \,/\, \frac{ab}{d}$$

$$\Rightarrow \quad md/ab \Rightarrow md \le ab$$

Thus $md = ab$

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

Ex P.T. $(a,b)[a,b] = |ab|$

(4?) corollary :-

For any +ve integers a & b $[a,b] = ab$ iff $(a,b) = 1$.

proof :- we know that,

$[a,b](a,b) = ab$ (prove it)

Now,

$$[a,b] = ab \Leftrightarrow \frac{ab}{(a,b)} = ab$$

$$\Leftrightarrow \frac{1}{(a,b)} = 1$$

$$\Leftrightarrow (a,b) = 1.$$

$(a,b) = 1$ iff $[a,b] = |ab|$

(Q1) Find $[3054, 12378]$.

sol^n: first we find $(3054, 12378)$

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

$\therefore (3054, 12378) = 6$

$$\therefore [3054, 12378] = \frac{3054 \times 12378}{(3054, 12378)} = 6300402$$

(42) Find $[525, 235]$.

Sol^n:

first we find $(525, 235)$

$$525 = 2(235) + 55$$
$$235 = 4(55) + 15$$
$$55 = 3(15) + 10$$
$$15 = 1(10) + 5$$
$$10 = 2(5) + 0$$
$$\therefore (525, 235) = 5$$

$$\therefore [525, 235] = \frac{525 \times 235}{5} = 24675.$$

(43) If $k > 0$ is a common multiple of a & b then p.t. $\left(\frac{k}{a}, \frac{k}{b}\right) = \frac{k}{[a,b]}$.

Proof:
$$\left(\frac{k}{a}, \frac{k}{b}\right)|ab| = \left(\frac{k}{a}(ab), \frac{k}{b}(ab)\right)$$
$$= (kb, ka)$$
$$= k(a,b) \quad (\because k > 0)$$
$$\Rightarrow \left(\frac{k}{a}, \frac{k}{b}\right)|ab| = \frac{k|ab|}{[a,b]} \quad (\because (a,b)[a,b] = |ab|)$$

$$\Rightarrow \left(\frac{k}{a}, \frac{k}{b}\right) = \frac{k}{[a,b]}$$

(44) Find, $\left(\frac{90}{45}, \frac{180}{60}\right)$

$$\left(\frac{90}{45}, \frac{180}{60}\right) = \left(\frac{180}{90}, \frac{180}{60}\right)$$

$\therefore$ By above thm, $\left(\frac{90}{45}, \frac{180}{60}\right) = \frac{180}{[60,90]}$

$$= \frac{180}{180} = 1$$

Date: / /

(95) P.T. $[a,b]=k$ iff $\left(\frac{k}{a},\frac{k}{b}\right)=1$, if $k>0$ is common multiple of a & b.

proof:- we know that, $\left(\frac{k}{a},\frac{k}{b}\right)=\frac{k}{[a,b]}$ —(*) (prove it)

If $[a,b]=k$ then by (*)

$$\left(\frac{k}{a},\frac{k}{b}\right)=\frac{k}{k}=1.$$

If $\left(\frac{k}{a},\frac{k}{b}\right)=1$ then by (*)

$$1=\frac{k}{[a,b]} \Rightarrow [a,b]=k$$

(96) P.T. $(a+b)[a,b]=b[a,a+b]$, $\forall a,b>0$.

proof:-

$$\begin{aligned} R.H.S. &= b[a,a+b] \\ &= b\,\frac{a(a+b)}{(a,a+b)} \\ &= \frac{ab(a+b)}{(a,b)} \quad (\because (a,b)=(a,a+b)) \\ &= (a+b)[a,b] \\ &= L.H.S. \end{aligned}$$

(97) P.T. $[a,b,c]=[[a,b],c]$

proof:- Let $[a,b,c]=m$ & $[[a,b],c]=m'$.

Now, $[a,b,c]=m \Rightarrow a/m,\ b/m,\ c/m$

$$\Rightarrow [a,b]/m,\ c/m$$

$$\Rightarrow [[a,b],c]/m$$

$$\Rightarrow m'/m$$

$$\Rightarrow m'\le m$$

also, $[[a,b],c] = M'$

$\Rightarrow [a,b]/M' , c/M'$

$\Rightarrow a/M' , b/M' , c/M'$

$\Rightarrow [a,b,c]/M'$

$\Rightarrow M \leq M'$

Thus $M = M'$ i.e $[a,b,c] = [[a,b],c]$

(98) P.T. $[a,b,c] = \dfrac{abc}{(ab,bc,ca)}$, $\forall\ a,b,c > 0$.

Proof: $L.H.S = [a,b,c]$

$= [[a,b],c]$

$= \dfrac{[a,b]c}{([a,b],c)}$

$= \dfrac{ab}{(a,b)} \times \dfrac{c}{([a,b],c)}$

$= \dfrac{abc}{((a,b)[a,b],(a,b)c)}$

$= \dfrac{abc}{(ab,(ac,bc))}$

$= \dfrac{abc}{(ab,bc,ca)} = R.H.S.$

Find $(136,221,391) = 17$

(99) Find $[136,221,391]$ by three different ways

Sol (i)

$\therefore [136,221,391]$

$= 90664$

8	136	221	391
17	17	221	391
13	1	13	23

(ii) $[136, 221, 391]$

$= [[136, 221], 391]$

$= \left[\dfrac{136 \times 221}{(136, 221)}, 391\right]$

$= \left[\dfrac{30056}{17}, 391\right]$

$= [1768, 391]$

$1768 = 4(391) + 204$
$391 = 204 + 187$
$204 = 187 + 17$
$187 = 11 \times 17 + 0$

$= \dfrac{1768 \times 391}{(1768, 391)}$

$= \dfrac{1768 \times 391}{17}$

$= 40664.$

(iii) $[136, 221, 391] = \dfrac{136 \times 221 \times 391}{(136 \times 221, 221 \times 391, 391 \times 13}$

$= \dfrac{11751896}{(30056, 86411, 53176)}$

$30056 = 17 \times 17 \times 13 \times 8$
$86411 = 17 \times 13 \times 23 \times 17$
$53176 = 17 \times 8 \times 23 \times 17$

$\therefore (30056, 86411, 53176) = 17^2$

$\therefore [136, 221, 391] = 40664$

* Prime no :-

An integer $p>1$ is said to be a prime no. if its only +ve divisors are 1 & p itself.

An integer greater than 1 which is not a prime is called composite number.

→ Every prime no. greter than $\cancel{a}$ 3 is of the for $3k+1$ or $3k-1$.

(50) State and prove fundamental property of prime number.

* If p is prime no. & p/ab then either p/a or p/b.

proof :-

Here p is prime & p/ab.

if p/a then result is proved.

if $p \nmid a$ then $(p,a)=1$ ($\because$ p is prime)

Thus $(p,a)=1$ & $p/ab \Rightarrow p/b$

Hence either p/a or p/b.

(51) If a is composite no. & q is its least +ve divisor then p.t. $q \le \sqrt{a}$

proof :-

we have given that, q/a

$\therefore a = kq, k \in Z$

$\Rightarrow k/a \Rightarrow q \le k$ ($\because$ q is least +ve div)

$\Rightarrow q^2 \le kq$

$\Rightarrow q^2 \le a$ ($\because q>0$)

$\Rightarrow q \le \sqrt{a}$

Date: / /

(52) Let p be a prime integer greater than 3 then prove that $2p+1$ & $4p+1$ can not be prime simultaneously

soln:-

we know that every prime no. greater than 3 is of the form $3k+1$ or $3k-1$

If $p = 3k+1$ then

$$2p+1 = 2(3k+1)+1$$
$$= 6k+2+1$$
$$= 3(2k+1)$$

Thus $2p+1$ is not prime no.

$\therefore$ $2p+1$ & $4p+1$ cannot be prime simultaneously when $p=3k+1$

If $p=3k-1$ then

$$4p+1 = 4(3k-1)+1$$
$$= 12k-3$$
$$= 3(4k-1)$$

which is not prime

Thus $2p+1$ & $4p+1$ can not be prime simultaneously.

Hence result is proved.

* Above result is not true for $p=3$ because $2p+1=7$ & $4p+1=13$

$\therefore$ Both are prime.

(53) If m is composite no. and $n_m = 111\ldots1$ (m times) then p.t. n_m is also composite no.

proof:-

Here m is composite no.

$\therefore m = a \times b$ for some $a, b \in \mathbb{Z}$
and $a, b \neq 1, m$

Now, $10^m - 1 = 10^{ab} - 1$

$= (10^a)^b - 1$

$= (10^a - 1)\left[(10^a)^{b-1} + (10^a)^{b-2} + \dots + 10^a + 1\right]$

$\therefore 10^m - 1 = [999\ldots 9 \text{ (a-times)}]\, K$

where $K = (10^a)^{b-1} + \dots + 10^a + 1$

$\Rightarrow 999\ldots 9 \text{ (m times)} = [999\ldots 9 \text{ (a times)}]\, K$

$\Rightarrow \cancel{9}(111\ldots 1 \text{ m times}) = \cancel{9}(111\ldots 1 \text{ a times})\, K$

$\Rightarrow n_m = n_a \times K$

$\Rightarrow n_m$ is a composite no.

(54) If n_m is prime no. then p.t. m is also prime no. where $n_m = 1111\ldots$ (m times)

proof:-

we have given that n_m is prime.
we have to p.t. m is prime.
suppose m is not prime then m is composite

$\therefore$ by above thm. n_m is composite. $\times$

(proveit)

Hence m is prime

(55) 111111 is prime or not.

sol: Here $n_6 = 111111 \quad \therefore m = 6$ which is composite $\therefore n_6$ is composite.

(56) Prove or disprove:

If m is prime then n_m is prime

where $n_m = 111\ldots m$ times.

sol:- let $n_3 = 111$ where $n=3$ is prime

but $n_3 = 111 = 37\times 3$ is not prime

$\therefore$ statement is not true always.

(57) P.T. there are n consecutive comp. integers for all $n>3$

solⁿ:- Clearly $(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1)$

are n consecutive nos. and also all are composite nos. because $2 \mid (n+1)!+2$,

$3 \mid (n+1)!+3$

Hence thm is proved

(58) Give 15 consecutive composite nos.

sol:- Take $n=15$

$\therefore n+1 = 16 \Rightarrow 16!+2, 16!+3, \ldots, 16!+16$

are 15 consecutive composite nos.

(59) Give 10 consecutive comp. no.

sol:- Take $n=10 \Rightarrow n+1 = 11$

$\therefore 11!+2, 11!+3, \ldots, 11!+11$

are 10 cosecutive composite numbers

(60) State & prove Euclid's result for prime no.

→ Statement:-

There are infinitely many prime no.

proof:-

Let p be any prime no.
and let $a = p!+1$
let q be any prime divisor of a
i.e. q is prime and $q \mid (p!+1)$.

Clearly $q \nmid p!$ **.

i.e $q \nmid (1 \cdot 2 \cdot 3 \cdots p)$

$\therefore$ $q > p$.
also q is prime

Thus q is prime no. greater than p.
Continue this process,
Hence we say there are infinitely many prime no.

(61) P.T. the no. of the prime of the form $4n-1$ is infinite

or

P.T. there are infinite prime no^s. of the form $4n-1$.

proof:-

Suppose $\exists$ only finitely many prime of the form $4n-1$ (say)
↓
$q_1, q_2, \ldots, q_k$

Consider the no. $a = 4(q_1 q_2 \cdots q_k) - 1$.
clearly a is odd no.
let p be any odd prime divisor of a
i.e. p is odd prime & p / a
$\therefore p \neq q_i \; (i = 1, 2, \ldots, k)$

($\because$ If $p = q_i$ then $q_i / 4q_1q_2 \cdots q_k$.
& $q_i \nmid 4q_1q_2 \cdots q_k - 1$
$\Rightarrow q_i \nmid a$
$\Rightarrow p \nmid a$ *)

we know that, every odd no. can be written in the form $4n+1$ or $4n-1$.
also we know that product of two or more integers of the form $4n+1$ is also of the form $4n+1$.

If all prime divisors of a are of the form $4n+1$ then a is also of the form $4n+1$
but a is of the form $4n-1$ *
$\therefore$ we get contradiction

$\therefore$ all prime divisors of a cannot be of ~~a~~ the same form $4n+1$.
$\therefore$ There are some prime divisors p of a which are of the form $4n-1$.
(Also $p \neq q_i$)

∴ Continue the process, finally we say that there are infinitely many prime no^s. of the form $4n-1$

(62) There are infinitely many prime no. of the form $4n+3$.

proof:

Suppose there $\exists$ only finitely many primes of the form $4n+3$.

say $q_1, q_2, \cdots q_k$

Consider a no. $a = 4(q_1 \cdot q_2 \cdots q_k) - 4 + 3$.

i.e. $a = 4(q_1 \cdot q_2 \cdots q_k - 1) + 3$. —(*)

Clearly a is odd no.

let p be any odd prime divisor of a. we know that every odd no. are of the form $4n+1$ or $4n+3$.

also we know that product of integers of the form $4n+1$ is also of the form $4n+1$

Clearly $p \neq q_i$, $i = 1, 2, \cdots k$

If all prime divisors of a are of the form $4n+1$ then a is also of the form $4n+1$ X.

∴ There are some prime divisors of a of the form $4n+3$. Also $P \neq q_i$

∴ ~~Continue the process, finally~~ we say that there are infinitely many prime

(63) If P_n is the n^{th} prime no. then prove that $P_n < 2^{2^n}, \forall n \in N$.

proof:

We will prove this result by using mathematical induction n.

For $n=1$, $P_1 = 2$ & $2^{2^n} = 2^{2^1} = 4$

Thus $P_1 < 2^{2^1}$.

Thus result is true for $n=1$.

Suppose result is true for n

i.e. $P_n < 2^{2^n}$.

then we have to p.t. result is tr

for n+1

i.e. we have to p.t. $P_{n+1} < 2^{2}$

we know that,

$$P_{n+1} \leq P_1 P_2 \ldots P_n + 1.$$
$$< 2^{2^1} \cdot 2^{2^2} \cdot \ldots 2^{2^n} + 1$$
$$= 2^{[2 + 2^2 + \ldots + 2^n]} + 1$$
$$= 2^{2[1 + 2 + 2^2 + \ldots + 2^{n-1}]} + 1$$
$$= 2^{2[(2^n - 1)/(2-1)]} + 1.$$
$$= 2^{2^{n+1} - 2} + 1$$
$$< 2^{2^{n+1} - 2} + 3 \cdot 2^{2^{n+1} - 2} \quad (\because 1 < 3 \cdot 2$$
$$= 4 \cdot 2^{2^{n+1} - 2}$$
$$= 2^2 \cdot 2^{2^{n+1} - 2}$$
$$= 2^{2^{n+1}}$$

Thus $P_{n+1} < 2^{2^{n+1}}$

Thus result is true for $n+1$,

Hence by mathematical induction method we say that $P_n < 2^{2^n}$, $\forall n$

(64) If P_n is the n^{th} prime no. then p.t. $P_n \leq 2^{2^{n-1}}$, $\forall n$.

proof:-

For $n=1$, $P_1 = 2$, & $2^{2^{n-1}} = 2^{2^{1-1}} = 2^{2^0} = 2$

Thus result is true for $n=1$.

Suppose result is true for n

i.e $P_n \leq 2^{2^{n-1}}$

then we have to p.t. result is true for $n+1$.

i.e we have to p.t.

$$P_{n+1} \leq 2^{2^n}.$$

we know that $P_{n+1} \leq P_1 P_2 \dots P_n + 1$

$$\leq 2^{2^0} \cdot 2^{2^1} \dots 2^{2^{n-1}} + 1$$

$$= 2^{[1+2+2^2+\dots+2^{n-1}]} + 1$$

$$= 2^{[(2^n-1)/(2-1)]} + 1$$

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

$$< 2^{2^n-1} + 2^{2^n-1}$$

$$(\because 1 \leq 2^{2^n-1}.$$

$$= 2 \cdot 2^{2^n-1}$$

$$= 2^{2^n}.$$

Thus $P_{n+1} < 2^{2^n}$.

i.e. $P_{n+1} \leq 2^{2^n}$.

Thus result is true for $n+1$

(65) P.T. $P_n < 2^{2^{n-1}}$ $\forall n > 1$.

proof:- We will prove this result by mathematical induction

for $n=2$, $P_2 = 3$

and $2^{2^{2-1}} = 2^2 = 4$

Thus $P_2 < 2^{2^{2-1}}$.

Thus result is true for $n=2$.

Suppose result is true for n

i.e $P_n < 2^{2^{n-1}}$, $\forall n > 1$

we have to p.t. result is true for $n+1$

i.e $P_{n+1} < 2^{2^n}$, $\forall n > 1$

we know that,

$$
\begin{aligned}
P_{n+1} &< P_1 P_2 P_3 \cdots P_n + 1 \\
&< 2^{2^0} \cdot 2^{2^1} \cdot 2^{2^2} \cdots 2^{2^{n-1}} + 1 \\
&= 2^{(2^0 + 2^1 + 2^2 + \cdots + 2^{n-1})} + 1 \\
&= 2^{((2^n - 1)/(2-1))} + 1 \\
&= 2^{2^n - 1} + 1 \\
&< 2^{2^n - 1} + 2^{2^n - 1} \qquad (\because 1 < 2^{2^n - 1}) \\
&= 2 \cdot 2^{2^n - 1} \\
&= 2^{2^n}.
\end{aligned}
$$

$\therefore P_{n+1} < 2^{2^n}$, $\forall n > 1$

Thus result is true for $n+1$, $\forall n > 1$

Hence by mathematical induction we say that,

$P_n < 2^{2^{n-1}}$, $\forall n > 1$.

* Remark:-

(1) P is prime then $P/ab \Rightarrow$ either P/a or P/b

$P/a_1 a_2 \cdots a_n \Rightarrow P/a_1$ or P/a_2 or $\cdots$ P/a_n.

Date: 77

(2) If $p / p_1 p_2 \cdots p_n$, where p & p_i are prime, $i = 1, 2, \cdots$

p/p_i, for some i.

i.e. $p = p_i$ for some i.

(66) If p is prime then pt. $\exists$ no +ve integer $a, b \ni a^2 = pb^2$ (OT)

If p is prime then $a^2 \neq pb^2, \forall a, b \in N$.

proof:- Suppose $\exists$ two +ve integers a & $b \ni$
$a^2 = pb^2$.

Let $(a, b) = d$ then

d/a & $d/b \Rightarrow a = a_1 d$, $b = b_1 d$.
for some $a_1, b_1 \in Z$.

clearly $(a_1, b_1) = 1$. *

Now $a^2 = pb^2 \Rightarrow a_1^2 d^2 = p b_1^2 d^2$
$\Rightarrow a_1^2 = p b_1^2$ —(*)
$\Rightarrow p/a_1^2$
$\Rightarrow p/a_1$
$\Rightarrow a_1 = kp$
$\Rightarrow a_1^2 = k^2 p^2$
$\Rightarrow p b_1^2 = k^2 p^2$
$\Rightarrow b_1^2 = k^2 p$
$\Rightarrow p/b_1^2$
$\Rightarrow p/b_1$

* If $(a_1, b_1) = d' > 1$
then
d'/a_1, d'/b_1
$\Rightarrow a_1 = k_1 d'$, $b_1 = k_2 d'$
$\Rightarrow a = k_1 dd'$, $b = k_2 dd'$
$\Rightarrow dd'/a$, dd'/b X
($\because d$ is g.c.d. of a & b & $dd' > d$)

Thus p/a_1 & p/b_1 X
($\because (a_1, b_1) = 1$)

$\therefore$ our supposition is wrong
i.e. $\exists$ no +ve integers a & $b \ni$

Date : / /

(61) State & prove unique factorization thm for +ve integers or
State & prove fundamental thm of arithmetic

* Statement :-

Every +ve integer greater than 1 can expressed uniquely as a product of pri upto the order of the factor

proof:

Let $a > 1$ be any +ve integer.

If a is prime then result is prove.

If a is not prime

Let $p_1 (>1)$ be the least +ve divisor.

then clearly p_1 is prime

and $a = p_1 a_1$ ($\because p_1 / a$

If a_1 is prime then result is true.

If a_1 is not prime, let $p_2 (>1)$ be the smallest divisor of a_1 then

clearly p_2 is prime

and $a_1 = p_2 a_2$ ($\because p_2 / a_1$)

$\therefore a = p_1 p_2 a_2$, where $a_1 > a_2$

continue this process, after a finite no. of steps we must have

$a = p_1 p_2 \cdots p_r$ —(1) ($\because a_1 > a_2 > a_3 \cdots$

Hence, every integer greater than 1 can be expressed as product of pri

Now, we p.t this factorization of a is unique.

Suppose a can be expressed as

$a = q_1 q_2 \cdots q_s$, where q_i are prim -(2)

then we have to prove that

$r = s$ & $p_i = q_i, \forall i$

If $r \neq s$ let $r > s$

by (1) & (2) we get

$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ -(3)

we know that,

$q_1 / q_1 q_2 \cdots q_s$

$\therefore q_1 / p_1 p_2 \cdots p_r$

$\Rightarrow q_1 = p_i$, for some i

assume $q_1 = p_1$ then by (3)

$p_1 p_2 \cdots p_r = p_1 q_2 \cdots q_s$

$\Rightarrow p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$.

continue this process, we get

$q_2 = p_2, q_3 = p_3, \cdots q_s = p_s$.

&

$p_{s+1} \cdot p_{s+2} \cdots p_r = 1 \rightarrow (\because r > s)$ X

$\therefore r = s$

and $p_i = q_i, \forall i$

Hence uniqueness is proved and hence the theorem

* Standard factorization of $a > 1$:

If some prime no's are repeated then we have, $p_i \neq p_j, \forall i, j$

Date: / /

This representation of a is called <u>standard factorization of a</u> or standard representation of a

→ If $p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_r^{a_r}$ be the standard factorization of a then d is positive divisor of a iff $d = p_1^{d_1} \cdot p_2^{d_2} \cdots p_r^{d_r}$ where $0 \leq d_i \leq a_i$.

→ If $a = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_r^{a_r}$ &

$b = p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdots p_r^{b_r}$, where all p_i are prime $\forall a_i \geq 0, b_i \geq 0$

then $(a, b) = p_1^{c_1} \cdot p_2^{c_2} \cdots p_r^{c_r}$,

where $\forall c_i = \min\{a_i, b_i\}$ &

$[a, b] = p_1^{d_1} \cdot p_2^{d_2} \cdots p_r^{d_r}$ where

$\forall d_i = \max\{a_i, b_i\}$.

(68) Find $(142, 150, 155)$ & $[142, 150, 155]$.

<u>Sol</u>:-

$142 = 71 \times 2 = 5^0 \times 3^0 \times 2^1 \times 71^1 \times 31^0$

$150 = 75 \times 2 = 5 \times 5 \times 3 \times 2 = 5^2 \times 3^1 \times 2^1 \times 71^0 \times 3$

$155 = 31 \times 5 = 5^1 \times 3^0 \times 2^0 \times 31^1 \times 71^0$.

$\therefore (142, 150, 155) = 1$ &

$[142, 150, 155] = 2 \times 3 \times 5^2 \times 31 \times 71$

$= 330150$

* Remark:-

Let $a = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$,

$b = p_1^{b_1} p_2^{b_2} \dots p \; q_1^{b_1} q_2^{b_2} \dots q_s^{b_s}$, $\forall a_i > 0$

$\forall b_i > 0$

p_i & q_i are primes

If $(a,b)=1$. then all primes p_i & q_i are distinct and also,

$ab = p_1^{a_1} \dots p_r^{a_r} q_1^{b_1} \dots q_s^{b_s}$.

(69) If a and b are relatively prime & d/ab then prove that $\exists$ unique d_1/a, d_2/b $\ni$ $d = d_1 d_2$.

Sol^n: ~~If~~ Let $a = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ &

$b = q_1^{b_1} q_2^{b_2} \dots q_s^{b_s}$, where

$\forall a_i > 0, b_i > 0$,

p_i, q_i are primes

Here $(a,b) = 1$.

$\therefore$ All primes p_i & q_i are distinct and $ab = p_1^{a_1} \dots p_r^{a_r} q_1^{b_1} \dots q_s^{b_s}$.

Since d/ab, $d = p_1^{l_1} p_2^{l_2} \dots p_r^{l_r} q_1^{k_1} \dots q_s^{k_s}$,

$\forall$ $0 \le l_i \le a_i$ & $0 \le k_i \le b_i$.

let $d_1 = p_1^{l_1} \dots p_r^{l_r}$,

$d_2 = q_1^{k_1} \dots q_{\cancel{ks}}^{k_s}$ then

~~d_1/d~~ d_1/a, d_2/b & $d = d_1 d_2$

also clearly d_1 & d_2 are unique

Date: / /

(70) Goldback's problem (conjecture) :-

Every odd no. greater than 9 can be expressed as the sum of three o[illegible] primes and every even no. greater than 6 can be expressed as sum o[illegible] two odd primes.

This problem is called Goldback problem. Sometimes the 1st problem is called odd G.B. problem and 2nd called even G.B. problem.

In 1937, L.M. Dinogradov, prove the odd Goldback's problem by the cycle method but the even goldback's pr[illegible] is still not proved.

eg.

151 =

17 = 3+7+7

11 = 5+3+3.

8 = 3+5.

24 = 11+13.

30 = 11+19

* Twin primes :-

Two consecutive odd no. are called twin primes if both are primes

eg. 3,5 ; 5,7 ; 11,13 ; 17,19 ; 29,31

(71) Twin Prime Problem: There are infinite pairs of twin primes.

This problem is still unsolved

(71) Twin prime problem:

There are infinite pairs of twin primes
This problem is still unsolved

UNIT-2 UNIT-2 (Stead)

* Def^n:-
Let a be any +ve integer then the total no. of +ve divisior of a is denoted by $T(a)$ or $d(a)$ and defined as

$$T(a) = \sum_{d/a} 1$$

→ Find $T(20)$

Sol^n:- $a = 20$, $d = 1, 2, 4, 5, 10, 20$

$$\therefore \sum_{d/a} 1 = 1+1+1+1+1+1 = 6.$$

→ Find $T(100)$ & $T(110)$

$a = 100$, $d = 1, 2, 4, 5, 10, 20, 25, 50, 100$

$$\therefore \sum_{d/a} 1 = \sum_{9} 1 = 1+1+1+1+1+1+1+1+1 = 9$$

* Def^n:-
Let a be any +ve integer then the sum of all positive divisor of a is denoted by $S(a)$ or $\sigma(a)$ and defined as

d/a

e.g. $S(20) = \sum_{d/a} d = 1+2+4+5+10+20 = 42.$

* Def^n :-

The product of all +ve divisor of a i[illegible]
denoted by $p(a)$ & defined as

$$p(a) = \prod_{d/a} d$$

e.g. $p(20) = \prod_{d/a} d = 1 \times 2 \times 4 \times 5 \times 10 \times 20 = 8$[illegible]

→ Find $P(12), S(12), T(12)$.

* Remark :-

a	1	2	3	4	5	6	7	8	9	10	11
T(a)	1	2	2	3	2	4	2	4	3	4	2
S(a)	1	3	4	7	6	12	8	15	13	18	12
p(a)	1	2	3	8	5	36	7	64	27	100	11

from above table if a is prime no. T(a)[illegible]
$S(a)$[illegible]
$p(a)$[illegible]

$T(a) = 2$
$S(a) = (a+1)$
$P(a) = a$

Date: 1/3/08

(12) If $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. where all p_i are primes and $a_i > 0$.

then prove the following:

(i) $T(a) = \prod_{i=1}^{k} (a_i+1)$.

(ii) $S(a) = \prod_{i=1}^{k} \left[\frac{p_i^{a_i+1} - 1}{p_i - 1}\right]$

(iii) $P(a) = a^{T(a)/2}$

proof:- Here $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$.

If d/a then $d = p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k}$.

where $0 \le l_i \le a_i$.

(i)

$$T(a) = (a_1+1)(a_2+1)\cdots(a_k+1)$$
$$= \prod_{i=1}^{k} (a_i+1)$$

(ii) $$S(a) = \sum_{t_1=0}^{a_1} p_1^{t_1} \times \sum_{t_2=0}^{a_2} p_2^{t_2} \times \cdots \times \sum_{t_k=0}^{a_k} p_k^{t_k}.$$

$$= \frac{p_1^{a_1+1} - 1}{p_1 - 1} \times \frac{p_2^{a_2+1} - 1}{p_2 - 1} \times \cdots \times \frac{p_k^{a_k+1} - 1}{p_k - 1}$$

$\left(\because 1 + x + x^2 + \cdots + x^{n-1} = \frac{x^n - 1}{x - 1} \right.$

$$\therefore S(a) = \prod_{i=1}^{k} \left[\frac{p_i^{a_i+1} - 1}{p_i - 1}\right].$$

(iii) Let $d_1, d_2, \ldots, d_r$ be all +ve divisors of a then $T(a) = r$.

Now d_i/a, $\forall i = 1, 2, \ldots, r$.

Date : / /

$\Rightarrow a = d_i d_i'$ for some $d_i' \in \mathbb{Z}$

$\Rightarrow d_i' / a \quad , \forall i = 1, 2, \ldots, r$

Thus $d_1', d_2', \ldots d_r'$ are also divisors of a

Now, $p(a)$ = product of all divisors

$\therefore p(a) = d_1 \cdot d_2 \cdots d_r$ &

$p(a) = d_1' \cdot d_2' \cdots d_r'$

$\therefore [p(a)]^2 = p(a) p(a)$

$= (d_1 d_2 \cdots d_r)(d_1' d_2' \cdots d_r')$

$= (d_1 d_1')(d_2 d_2') \cdots (d_r d_r')$

$= a \cdot a \cdot a \cdots a$ (r times)

$\therefore [p(a)]^2 = a^r = a^{T(a)}$

$\Rightarrow p(a) = [a^{T(a)}]^{1/2} = a^{T(a)/2}$

(73) Find $P(20)$.

No. divisors of $20 = 6 \Rightarrow T(a) = 6$

$\therefore p(20) = 20^{6/2} = 20^3 = 8000$

(74) Find $T(60)$, $S(60)$, $P(60)$.

$60 = 2^2 \times 3^1 \times 5^1$.

$T(a) = \prod_{i=1}^{k} (a_i + 1)$

$\Rightarrow T(60) = (2+1)(1+1)(1+1)$

$= 3 \times 2 \times 2 = 12$.

$$S(a) = \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1}$$

$$\Rightarrow S(60) = \left[\frac{2^3 - 1}{2 - 1}\right]\left[\frac{3^2 - 1}{3 - 1}\right]\left[\frac{5^2 - 1}{5 - 1}\right]$$

Date:

$$= \frac{7}{1} \times \frac{8}{2} \times \frac{24}{4}$$

$$= 7 \times 4 \times 6 = 24 \times 7 = 168$$

$$P(a) = a^{T(a)/2}$$

$$\Rightarrow P(60) = 60^{12/2} = 60^{6} =$$

(75) Find $T(75)$, $S(75)$, $T(75)$.

(76) If a & b are relatively prime then prove the following

~~(i) $P(ab) = P(a)P(b)$.~~

(i) $T(ab) = T(a)T(b)$

(ii) $S(ab) = S(a)S(b)$

(iii) $P(ab) = P(a)^{T(b)} P(b)^{T(a)}$. or

In usual notation p.t. T is a multiplicati

Date: / / 08

proof :- Let $a = p_1^{a_1} \cdots p_r^{a_r}$

$b = q_1^{b_1} \cdots q_s^{b_s}$.

where $\forall a_i > 0, b_i > 0$, p_i & q_i a[re] pr[ime]

since $(a,b) = 1$, all p_i & q_i are distinct and

$$ab = p_1^{a_1} \cdots p_r^{a_r} \cdot q_1^{b_1} \cdots q_s^{b_s} \quad \text{— } (*)$$

(i) $$T(ab) = \left[\prod_{i=1}^{r} (a_i+1)\right]\left[\prod_{i=1}^{s} (b_i+1)\right]$$

$$= T(a)\,T(b).$$

(ii) By $(*)$

$$S(ab) = \prod_{i=1}^{r}\left[\frac{p_i^{a_i+1} - 1}{p_i - 1}\right]\prod_{i=1}^{s}\left[\frac{q_i^{b_i+1} - 1}{q_i - 1}\right]$$

$$= S(a)S(b).$$

(iii) By $(*)$

$$P(ab) = ab^{T(ab)/2}$$

$$= (ab)^{\frac{T(a)T(b)}{2}}$$

$$= a^{\frac{T(a)T(b)}{2}} \cdot b^{\frac{T(a)T(b)}{2}}$$

$$= \left[a^{\frac{T(a)}{2}}\right]^{T(b)}\left[b^{\frac{T(b)}{2}}\right]^{T(a)}$$

$$= P(a)^{T(b)}\,P(b)^{T(a)}.$$

(78) If a is square no. then p.t. $S(a)$ is an odd integer. If a is not a square no. but odd integer then p.t. $S(a)$ is even

Sol:- (i) If a is squa no then
$a = x^2$ for some $x \in N$.
Let $x = p_1^{a_1} \cdots p_r^{a_r}$ where $\forall a_i$, p_i re p

Now,
$$a = x^2 = [p_1^{a_1} \cdots p_r^{a_r}]^2$$
$$\Rightarrow a = p_1^{2a_1} \cdots p_r^{2a_r}.$$
$$\Rightarrow \cancel{s(a) = \sum_{i=0}^{2a_1} p_1^i}$$
$$\Rightarrow s(a) = \sum_{i=0}^{2a_1} p_1^i \cdots \sum_i p_r^i$$

We know that,
sum of od no in ld me is always odd.
$\therefore$ Every factor of s(a) odd.

$\therefore$ s(a) must be odd.

(ii) If a is not a square no. but an odd integer.
$$a = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}.$$
Since a is not a square no,
atleast one a_i say a_1 is odd
and all p_i are odd primes
$$\therefore s(a) = \sum_{i=0}^{a_1} p_1^i \cdots \sum_i p_r^i.$$
Clearly the 1st factor of s(a) is even
($\because a_1$ odd).
$\therefore$ s(a) is even.

Date: / /

(79) Prove that, $\sigma(a) < a\sqrt{a}$, $\forall a > 2$. or

$\sigma(a) < a^{3/2}$, $\forall a > 2$

Soln:-

case-1 :- If $a = 2^k$ $(k \geq 2)$ then

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

Thus $\sigma(a) = 2^{k+1} - 1$

$< 2^{k+1}$

$= 2^k \cdot 2^1$

$\leq 2^k \cdot 2^{k/2}$ $\left(\because 2 \leq 2^{k/2} \; (k \geq 2)\right)$

$= a\sqrt{a}$

Thus $\sigma(a) < a\sqrt{a}$ if $a = 2^k$.

case-2 :- If $a = p^k$, where p is odd prime $(k \geq 1)$.

then

$$\sigma(a) = \frac{p^{k+1} - 1}{p-1}$$

$$= \frac{p^k - 1/p}{1 - 1/p}$$

$$= \frac{p^k}{1 - 1/p} - \frac{1/p}{1 - 1/p}$$

$$< \frac{p^k}{1 - 1/p}$$

$$= \frac{a}{1 - \frac{1}{p}}$$

$\leq a \cdot \frac{3}{2}$ $\left(\because p \geq 3 \Rightarrow 1/p \leq 1/3 \Rightarrow 1 - 1/p \geq 2/3\right)$

Thus

Date: 7 /

$\Rightarrow \boxed{S(a) < \frac{3}{2}a}$ — (*)

$\Rightarrow S(a) < \sqrt{3}\,a \quad (\because \frac{3}{2} < \sqrt{3})$.

$\Rightarrow S(a) < \sqrt{a}\,a \quad (\because p \geq 3$
$\Rightarrow p^k \geq 3 \Rightarrow a \geq 3$
$\Rightarrow \sqrt{a} \geq \sqrt{3}$
$\Rightarrow \sqrt{3} \leq \sqrt{a}$

Thus $S(a) < a\sqrt{a}$, if $a = p^k$, where p is odd prim, $a \geq 1$.

<u>case-3</u> :-

If a is any integer greater than 2

then we can write.

$a = 2^{a_0} \cdot p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$, where $a_0 = 0$ or $a_0 \geq 1$. — (**)

If $a_0 = 0$ or $a_0 > 1$. then

$S(a) = S(2^{a_0})\, S(p_1^{a_1}) \cdots S(p_r^{a_r})$.

$< 2^{a_0}\sqrt{2^{a_0}} \cdot p_1^{a_1}\sqrt{p_1^{a_1}} \cdots p_r^{a_r}\sqrt{p_r^{a_r}}$

(by case 1 & 2)

$= [2^{a_0} \cdot p_1^{a_1} \cdots p_r^{a_r}] \sqrt{2^{a_0} \cdot p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}}$

$= a\sqrt{a}$

Thus $S(a) < a\sqrt{a}$ when $a_0 = 0$ or $a_0 > 1$.

$S(2) = 3$

$S(p_1^{a_1}) < \frac{3}{2}p_1^{a_1}$

Now, if $a_0 = 1$ then by (**)

$a = 2 \cdot p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$

$\therefore S(a) = S(2) \cdot S(p_1^{a_1}) \cdots S(p_r^{a_r})$

$< 3 \cdot \frac{3}{2} p_1^{a_1} \cdot p_2^{a_2}\sqrt{p_2^{a_2}} \cdots p_r^{a_r}\sqrt{p_r^{a_r}}$

Date: / /

$< 2\sqrt{2}\sqrt{p_1^{a_1}} \cdot p_1^{a_1} p_2^{a_2} \sqrt{p_2^{a_2}} \cdots p_r^{a_r} \sqrt{p_r^{a_r}}$

$\left(\because \frac{9}{2} < 2\sqrt{2}\sqrt{3} < 2\sqrt{2}\sqrt{p_1} \right.$

$= (2 p_1^{a_1} \cdots p_r^{a_r}) \sqrt{2 p_1^{a_1} \cdots p_r^{a_r}}$

$= a\sqrt{a}$

Thus, $s(a) < a\sqrt{a}$ if $a_0 = 1$

Hence by case-1, 2 & 3 we say that $s(a) < a\sqrt{a}, \forall a > 2$

~~Unit 2 contd. on pg. 87~~

* Mersenne number :-

Any integer of the form $2^p - 1$ is called a Mersenne number, where p is prime. It is denoted by M_p

Thus, $M_p = 2^p - 1$, p is prime

ex- 3, 7, 31, 127

(24) check which are of following are mersenne numbers.

8, 10, 15, 18, 20, 24, 31

8 is not M_p.

also 10, ~~10~~ 15, 18, 20, 24 are not M_p.

but 31 is M_5 as $2^5 - 1$

$\therefore$ 31 is mersenne no.

~~15 is Mersenne~~ no.

(25) P.T. any prime factor of M_p is greater than p. or

If p is prime and q is any prime factor of M_p then p.t. ~~M_p~~ q is greater than ~~M_p~~ p.

* case-1 :- If p is even prime then p 2

$\therefore M_2 = 2^2 - 1 = 3$

Clearly prime factor of 3 is 3 itself

$\therefore q = 3$

$\therefore q > p$.

$\therefore$ Result is proved if p is even prime

Date: / /

* **Case-2 :-** If p is odd prime

Let q be any prime factor of M_p
then q / M_p.

$\Rightarrow q / 2^p - 1$.

$\Rightarrow 2^p \equiv 1 \pmod q$.

If d is order of $2 \bmod q$ then

$d / p \Rightarrow d = 1$ or p ($\because p$ is prime)

$\Rightarrow d = p$ ($\because$ If $d=1$ then $2^1 \equiv 1 \pmod q$ $\Rightarrow q / 1$ ※)

Clearly q is odd prime ($\because q / 2^p - 1$, $2^p - 1$ is odd)

also $(2, q) = 1$. then by Euler's thm

$2^{\phi(q)} \equiv 1 \pmod q$.

$\Rightarrow 2^{q-1} \equiv 1 \pmod q$.

Since d is order of 2, $d / q-1$

$\Rightarrow p / q-1$ ($\because d = p$)

$\Rightarrow p \leq q-1 < q$

$\Rightarrow p < q$

$\Rightarrow q > p$.

Hence, thm is proved

(26) Prove that odd prime factor of M_p (p
has the form, $2pt+1$, for some integer

proof:-

Let q be any odd prime factor of M_p $(p>2$
then q is odd prime & q / M_p.

$$\Rightarrow q / 2^p - 1$$

$$\Rightarrow 2^p \equiv 1 \pmod q$$

$$\Rightarrow p \text{ is order of } 2 \bmod q$$

($\because$ p is prim

also $(2,q)=1$

$\therefore$ By Euler's thm,

$$2^{\phi(q)} \equiv 1 \pmod q$$

$$\Rightarrow 2^{q-1} \equiv 1 \pmod q$$

$$\Rightarrow p / q-1 \quad (\because p \text{ is order of } 2 \bmod q)$$

Thus $p / q-1$ & $2 / q-1$

$$\Rightarrow 2p / q-1 \quad (\because (2,p)=1$$

$$\Rightarrow q-1 = 2pt$$

$$\Rightarrow q = 2pt+1, \text{ for some } t \in Z.$$

(27) P.T. the odd prime factor of $a^{2^n}+1$ $(a>1$
is of the form $2^{n+1}t+1$ for some $t \in Z$.

proof:

We shall prove this result by using P.M.I. on n.

for $n=0$ $\therefore$ $a^{2^n}+1 = a+1$

we know that, every odd prime no.

can be written in the form $2t+1$, $t \in Z$

Let q be the odd prime factor of $a+1$ then $q = 2t+1$ for some $t \in Z$.

i.e $q = 2^{n+1}t + 1$ (for $n=0$).

Thus result is true for $n=0$.

Suppose result is true for $n-1$. then we have to p.t result is true for n

Let q be any odd prime factor of $a^{2^n}+1$, then

$q / a^{2^n}+1$ & q is odd prime

$\Rightarrow q / ((a^2)^{2^{n-1}}+1)$ & q is odd prime

Thus $q = 2^n t_1 + 1$, for some $t_1 \in Z$ —(*)

(∵ result is true for $n-1$)

also $q / a^{2^n}+1$

$\Rightarrow a^{2^n} \equiv (-1) \pmod q$

$\Rightarrow (a^{2^n})^{t_1} \equiv (-1)^{t_1} \pmod q$

$\Rightarrow a^{2^n t_1} \equiv (-1)^{t_1} \pmod q$ —(**)

Since q is prime,

By Fermat's thm $a^q \equiv a \pmod q$

$\Rightarrow a^{q-1} \equiv 1 \pmod{q}$. $(\because (q,a)=1)$

$\Rightarrow a^{2^n t_1} \equiv 1 \pmod{q}$ (by (*))

$\Rightarrow 1 \equiv (-1)^{t_1} \pmod{q}$

$\Rightarrow q / 1-(-1)^{t_1}$ — (***)

If t_1 is odd, then $(-1)^{t_1} = -1$.

$\therefore q / 1-(-1)$ (by ***)

$\Rightarrow q/2$ $\times$ ($\because$ q is odd prime

$\therefore t_1$ must be even

$\therefore t_1 = 2t$ for some $t \in \mathbb{Z}$

$\therefore$ by (*), $q = 2^n \cdot 2t + 1$

$\Rightarrow q = 2^{n+1} t + 1$ for $t \in \mathbb{Z}$

Thus result is true for n

Hence by P.M.I. we say that, thm. is proved

* Fermat's number :.

An integer of the form $2^{2^n}+1$ is called Fermat's number. It is denoted by F_n.

i.e. $F_n = 2^{2^n}+1$.

e.g. 5, 17, 257

(28) Every prime factor of F_n $(n>2)$ is of the form $2^{n+2}t+1$ for some $t \in \mathbb{Z}$.

Let q be any prime factor of F_n then q / F_n.

we have to p.t. $q = 2^{n+2}t + 1$, for some $t \in \mathbb{Z}$

we know that,

$$[F_{n-1}]^{2^{n+1}} = [(F_{n-1})^2]^{2^n}$$

$$= [[2^{2^{n-1}} + 1]^2]^{2^n}$$

$$= [(2^{2^{n-1}})^2 + 2 \cdot 2^{2^{n-1}} + 1]^{2^n}$$

$$= [2^{2^n} + 2^{2^{n-1}+1} + 1]^{2^n}$$

Thus, $$(F_{n-1})^{2^{n+1}} = [F_n + 2^{2^{n-1}+1}]^{2^n} \quad \text{—} (*)$$

also we know that F_n / F_n

$$\Rightarrow F_n \equiv 0 \pmod{F_n}$$

$$\Rightarrow F_n + 2^{2^{n-1}+1} \equiv 2^{2^{n-1}+1} \pmod{F_n}$$

$$\Rightarrow [F_n + 2^{2^{n-1}+1}]^{2^n} \equiv (2^{2^{n-1}+1})^{2^n} \pmod{F_n}$$

$$\Rightarrow (F_{n-1})^{2^{n+1}} \equiv (2^{2^{n-1}})^{2^n} (2^1)^{2^n} \pmod{F_n}$$

$$\Rightarrow (F_{n-1})^{2^{n+1}} \equiv (2^{2^n})^{2^{n-1}} (2^{2^n}) \pmod{F_n}$$

$$\Rightarrow (F_{n-1})^{2^{n+1}} \equiv (2^{2^n})^{2^{n-1}+1} \pmod{F_n}$$

$$\Rightarrow (F_{n-1})^{2^{n+1}} \equiv (-1)^{2^{n-1}+1} \pmod{F_n}$$

$$\Rightarrow (F_{n-1})^{2^{n+1}} \equiv (-1) \pmod{F_n}$$

$$\Rightarrow (F_{n-1})^{2^{n+1}} + 1 \equiv 0 \pmod{F_n}$$

$$\Rightarrow F_n / \quad {}^{n+1}$$

F_4 / F_4

$F_4 / 2^{2^4} + 1$

$\Rightarrow 2^{2^4} \equiv -1 \pmod{F_4}$

$\Rightarrow q / (F_{n-1})^{2^{n+1}} - 1$

also q is prime & odd

∴ by Last thm, we see that

$q = 2^{n+2}t + 1$,

for some $t \in \mathbb{Z}$

Hence theorem is proved

$\Rightarrow q \,/\, (F_{n-1})^{2^{n+1}} + 1$, also q is prime & odd

then by last thm, we say that

$q = 2^{n+2}t + 1$, for some $t \in Z$

Hence the thm is proved

(29) Prove that, $\phi(p^k) = p^k\left(1 - \frac{1}{p}\right) \left(= p^k - p^{k-1}\right)$ where p is prime

U-4

proof :-

Here p is prime $\therefore \phi(p) = p-1$.
In a CRS modulo p^k, the only multipliers of p are, $p, 2p, 3p, \ldots, p^{k-1}.p$.
These numbers are not relatively prime to p. thus there are total p^{k-1} elements which are not relatively prime to p.
Hence the remaining $p^k - p^{k-1}$ elements are relatively prime to p^k
Hence, by def^n

$$\phi(p^k) = p^k - p^{k-1}$$

$$= p^k\left[1 - \frac{1}{p}\right].$$

U-4

(30) Find $\phi(128)$, $\phi(625)$, $\phi(81)$.

sol^n: $\phi(128) = \phi(2^7) = 2^7 - 2^6 = 128 - 64 = 64$

(1) Prove that, $\phi(m) \geq \frac{m}{T(m)}$. or

$$\phi(m)T(m) \geq m.$$

sol^n:-

Let $m = p_1^{m_1} \cdot p_2^{m_2} \cdots p_k^{m_k}$, where all p_i are primes.

$$\Rightarrow \phi(m) = m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).$$

$$\& \quad T(m) = (m_1+1)(m_2+1)\cdots(m_k+1).$$

Now,

$$\phi(m)T(m) = m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)(m_1+1)(m_2+1)\cdots(m_k+1).$$

$$\geq m\left(\frac{1}{2}\right)^k \cdot 2^k \quad \left(\because 1-\frac{1}{p_i} \geq \frac{1}{2} \; \forall \text{ prim} \;\; \& \;\; m_i+1 \geq 2.\right)$$

$$= m$$

Thus, $\phi(m)T(m) \geq m$.

$$\Rightarrow \phi(m) \geq \frac{m}{T(m)}$$

U-1 (conts)

* Perfect Number :-

Positive number 'a' is said to be perfect number if $S(a) = 2a$.

e.g. $S(6) = 1+2+3+6 = 12$ $\therefore$ 6 is perfect no.

$S(12) = 1+2+3+4+6+12 = 28 \neq 2 \times 12$

$\therefore$ 12 is not perfect no.

→ A square no. is not a perfect no. because

$S(q^2)$ is odd ~~no~~

Date: / /

(2) P.T. the necessary and sufficient condition that a positive integer 'a' can be even perfect is,

$$a = 2^n(2^{n+1}-1) \quad (n>1) \text{ and } 2^{n+1}-1 \text{ is}$$

prime.

OR

P.T. the necessary and sufficient condition for 'a' to be an even perfect number is

$$a = \frac{1}{2} m_p(m_p+1), \text{ where } m_p \text{ is prime}$$

Proof:- we have to p.t. 'a' is even perfect no. iff $a = \frac{1}{2} m_p(m_p+1)$

$$\Rightarrow a = \frac{1}{2}(2^p-1)2^p$$

$$\Rightarrow a = 2^{p-1}(2^p-1), \text{ where } 2^p-1 \text{ is prime.} \quad -(1)$$

If a is even perfect no. then we can write, $a = 2^n \cdot k$, for some $n \geq 1$ & k is odd ~~prime prime~~

Clearly $(2, k) = 1$

Since 'a' is perfect no.,

$$S(a) = 2a$$

$$\Rightarrow S(2^n \cdot k) = 2 \cdot 2^n \cdot k$$

$$\Rightarrow S(2^n)S(k) = 2^{n+1}k$$

$$\Rightarrow \left(\frac{2^{n+1}-1}{2-1}\right) S(k) = 2^{n+1}k$$

$$\Rightarrow S(k) = \frac{2^{n+1}k}{2^{n+1}-1}$$

$$\Rightarrow S(k) = k + \frac{k}{2^{n+1}-1}$$

Since $s(k)$ is integer, $\dfrac{k}{2^{n+1}-1}$ is also integer.

$\therefore$ It is also divisor of k. $\left[* \ \dfrac{k}{2^{n+1}-1} \Big/ k \quad \Rightarrow \dfrac{k}{\frac{k}{2^{n+1}-1}} = 2^{n+1}- \right.$

but $s(k)$ is sum of all divisors of ~~'a'~~ 'k'

×[~~less than k and itself~~]×

$\therefore \dfrac{k}{2^{n+1}-1}$ is sum of all divisors of k

less than k and itself.

There is no other than 1 (~~∵ it is odd~~

i.e. $\dfrac{k}{2^{n+1}-1} = 1$

$\Rightarrow \quad k = 2^{n+1}-1$

also k is prime no. because its diviso[rs] are 1 & k itself.

Hence,

$a = 2^n(2^{n+1}-1)$ $(n>1)$, and $2^{n+1}-1$ is prime

replacing n by $p-1$ we will get result (1)

* Converse part:-

If $a = 2^n(2^{n+1}-1)$ $(n>1)$ and $2^{n+1}-1$ is pri[me]

let $k = 2^{n+1}-1$ then $a = 2^n \cdot k$ which is even number.

Now we p.t. $s(a) = 2a$

$s(a) = s(2^n \cdot k)$

$= s(2^n)\, s(k)$

$= \left(\dfrac{2^{n+1}-1}{2-1}\right)(k+1).$ $\left(\because k \text{ is prime} \Rightarrow s(k) = k+1 \quad s(11) = 1+11\right.$

Date: / /

$= (2^{n+1}-1)(2^{n+1}-1+1)$

$= 2^{n+1}(2^{n+1}-1)$

$= 2.2^{n}(2^{n+1}-1)$

$= 2a.$

Hence a is even perfect number.

(3) If $2^m - 1$ is prime then p.t. m is also prime. Does the converse hold? verify it?

Proof:-

Suppose m is not prime then we can write, $m = qt$, for some $1 < q, t < m$.

Now, $2^m - 1 = 2^{qt} - 1$

$= (2^t)^q - 1$

$= (2^t - 1)\left((2^t)^{q-1} + \dots + 1\right)$

$= (2^t - 1)k$, where $k = (2^t)^{q-1} + \dots + 1$.

where $1 < t < m$

$\Rightarrow 2^t - 1 / 2^m - 1$ ※

because $2^m - 1$ is prime

Hence m is prime

Converse need not be true

i.e if m is prime then $2^m - 1$ need not be prime because for $m = 11$.

$2^m - 1 = 2^{11} - 1$

$= 2047 = 23 \times 89$

$\therefore 2^m - 1$ is not prime.

(4) If m is composite number then p.t. $2^m - 1$ is also composite

proof:- Since m is composite, we can write $m = qt$, for some $1 < q, t < m$.

Now,

$$2^m - 1 = 2^{qt} - 1$$
$$= (2^t)^q - 1$$
$$= (2^t - 1)((2^t)^{q-1} + \cdots + 1)$$
$$= (2^t - 1)k, \quad k = (2^t)^{q-1} + \cdots + 1$$

$\Rightarrow 2^t - 1 / 2^m - 1.$

$\Rightarrow 2^m - 1$ is composite number.

(5) If $2^m + 1$ is prime then p.t. $m = 2^k$ for some $k \in \mathbb{Z}$ (i.e. m is some power of 2). Does the converse hold? verify it?

proof:-

If $2^m + 1$ is prime then we have to p.t. $m = 2^k$, for some $k \in \mathbb{Z}$.

Suppose $m \neq 2^k$, $\forall k \in \mathbb{Z}$.

then there exists some odd ~~prime~~ no. q such that q / m $\left(\because m \neq 2^k. \ \therefore m = 2^k \cdot q \ (q \text{ is odd}) \right.$

$\Rightarrow m = qr$, for some $r \in \mathbb{Z}$, $1 < q, r < m$

Now, $2^m + 1$

$$= 2^{qr} + 1$$
$$= (2^r)^q + 1$$
$$= (2^r + 1)((2^r)^{q-1} + \cdots + 1)$$
$$= (2^r + 1)k, \quad \text{where } k = (2^r)^{q-1} + \cdots + 1$$

$\Rightarrow (2^r + 1) / (2^m + 1)$

$\Rightarrow 2^m + 1$ is not prime -X-

Date : / /

converse need not be true

i.e. if $m = 2^k$ for some $k \in \mathbb{Z}$ then $2^m + 1$ need not be prime

* for $m = 2^5$.

$$2^m + 1 = 2^{2^5} + 1$$
$$= 2^{32} + 1$$
$$= 2^4 \cdot 2^{28} + 1$$
$$= 2^4 (2^7)^4 + 1$$
$$= [2^7 \cdot 5 + 1 - 5^4](2^7)^4 + 1$$
$$= (2^7 \cdot 5 + 1)(2^7)^4 - (5^4)(2^7)^4 + 1$$
$$= (2^7)^4 (1 + 2^7 \cdot 5) + 1 - 5^4 (2^7)^4$$
$$= (2^7)^4 (1 + 5 \cdot 2^7) + (1 - 5 \cdot 2^7)(1 + 5 \cdot 2^7)(1 + 5^2 \cdot (2^7)^2)$$
$$= (1 + 5 \cdot 2^7)\left[(2^7)^4 + (1 - 5 \cdot 2^7)(1 + 5^2 \cdot (2^7)^2)\right]$$

$$2^4 = 16$$
$$2^7 \cdot 5 + 1 - 5^4$$
$$= 128 \times 5 + 1 - 625$$
$$= 640 + 1 - 625$$
$$= 16$$

$\Rightarrow 2^m + 1 = (1 + 5 \cdot 2^7) k$

$\Rightarrow 2^m + 1$ is not prime.

(6) P.T. F_5 is composite no.

sol: we know that $F_5 = 2^{2^5} + 1$ (converse of above)

(7) P.T. $F_0 \cdot F_1 \cdots F_{n-1} = F_n - 2$

Proof: we will prove this result by mathematical induction method

for $n = 1$.

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

also $F_1 - 2 = 2^{2^1} + 1 - 2$

$$= 4 + 1 - 2 = 3$$

Thus result is true for $n = 1$.

Suppose the result is true for $n-1$ then we have to p.t. it is true for n.

i.e $F_0 \cdot F_1 \cdots F_{n-1} = F_n - 2$.

L.H.S. $= F_0 \cdot F_1 \cdots F_{n-2} \cdot F_{n-1}$

$= (F_{n-1} - 2)\, F_{n-1}$ ($\because$ result is true $n-1$

$= \left(2^{2^{n-1}} + 1 - 2\right) F_{n-1}$

$= \left(2^{2^{n-1}} - 1\right)\left(2^{2^{n-1}} + 1\right)$

$= \left(2^{2^{n-1}}\right)^2 - 1$ $\qquad \cancel{2^{2(2^n-1)}}$ $\quad 2^{2^{(n-1)} \cdot 2}$

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

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

$= F_n - 2$

$=$ R.H.S.

Hence by Mathematical induction, we say that result is proved

(8) P.T. any two distinct mersene numbers are relatively prime

proof :-

We have to p.t $(M_p, M_q) = 1$, $\forall\, p \neq q$. where p, q are primes.

Clearly $(p, q) = 1$.

Now, ~~let~~ $(m_p, m_q) = (2^p - 1, 2^q - 1)$

$= 2^{(p,q)} - 1$ $\quad \left(\because (a^m - 1, a^n - 1) = a^{(m,n)} - 1\right)$

$= 2^1 - 1$

$= 1$

Hence, any two distinct mersenne numbers are relatively prime

Date: / /

(9) P.T. two distinct Fermat's numbers are relatively prime.

Proof:-

We have to p.t. $(F_m, F_n) = 1, \forall m \neq n$.

Suppose $(F_m, F_n) = d, m \neq n$

let $m < n$.

Now,

$F_0 \cdot F_1 \cdot \ldots F_{n-1} = F_n - 2$

$\therefore F_0 \cdot F_1 \cdot \ldots F_m \cdots F_{n-1} = F_n - 2$.

$\Rightarrow d / 2 \quad \left(\because d = (F_m, F_n) \Rightarrow d / F_m, d / F_n \right.$

$\left. \Rightarrow d / F_0 \cdot F_1 \cdots F_m \cdots F_{n-1} \ \& \ d / F_n \right)$

$\Rightarrow d = 1$ or 2

$\Rightarrow d = 1 \quad \left(\because F_m \ \& \ F_n \text{ are odd} \Rightarrow (F_m, F_n) = \text{o} \right.$

$\therefore (F_m, F_n) \neq 2$.

$\Rightarrow (F_m, F_n) = 1, \ \forall m \neq n$

Hence, the result is proved

* Greatest integer (integer value) function

or

Gauss function

The greatest integer function of any real number x is denoted by $[x]$ and defined as,

$[x]$ = the greatest integer not greater than x

e.g.

$[1.8] = 1, \quad [2.1] = 2, \quad [3.999] = 3$

$[-4.1234] = -5, \quad [0.5] = 0, \quad [-5] = -5$.

(3) $[[x]] = [x]$

→ Remark :-

(1) $x = [x] + a, \quad 0 \leq a < 1$

(2) $x < [x] + 1 \quad \& \quad [x] \leq x \Rightarrow [x] \leq x < [x] + 1$

(10) P.T. $[x]+[y] \le [x+y] \le [x]+[y]+1$.

proof:-

Let $x = [x]+a$, $y = [y]+b$ for some $0 \le a, b < 1$.

$x+y = [x]+[y]+a+b$, $0 \le a+b < 2$.

$\Rightarrow [x+y] = [x]+[y]+[a+b]$ — (1)

$\Rightarrow [x+y] \ge [x]+[y]$ — (2)

Since, $0 \le a+b < 2$.

$[a+b] = 0$ or 1

by (1) $[a+b] \le 1$.

$\Rightarrow [x+y] \le [x]+[y]+1$ — (3)

By (2) & (3),

$[x]+[y] \le [x+y] \le [x]+[y]+1$.

(11) Let x be any real no. and n be any positive integer then p.t.

(i) $\left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right]$.

(ii) $\left[\frac{\left[\frac{a}{b}\right]}{c}\right] = \left[\frac{a}{bc}\right]$, $\forall\, a, b \in R$, $c \in N$.

proof:-

We know that,

$[x] \le x < [x]+1$, $\forall x \in R$

$\Rightarrow \left[\frac{x}{n}\right] \le \frac{x}{n} < \left[\frac{x}{n}\right]+1$.

$\Rightarrow p \le \frac{x}{n} < p+1$, where $p = \left[\frac{x}{n}\right] \in Z$.

$\Rightarrow np \le x < n(p+1)$

$\Rightarrow np \le [x] < n(p+1)$

$\Rightarrow p \le \frac{[x]}{n} < p+1$

$\Rightarrow \left[\frac{[x]}{n}\right] = p.$

$\Rightarrow \left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right] \quad —(*)$

On replacing x by $\frac{a}{b}$ and n by c in (*), we get

$$\left[\frac{\left[\frac{a}{b}\right]}{c}\right] = \left[\frac{\frac{a}{b}}{c}\right]$$

$$\Rightarrow \left[\frac{\left[\frac{a}{b}\right]}{c}\right] = \left[\frac{a}{bc}\right].$$

(12) State and prove Hermite identity.

* Let x be any ~~integer~~ positive real number and n be a +ve integer then,

$$[x] + \left[x+\frac{1}{n}\right] + \left[x+\frac{2}{n}\right] + \dots + \left[x+\frac{n-1}{n}\right] = [nx]$$

Proof :-

Let $f(x) = [nx] - [x] - \left[x+\frac{1}{n}\right] - \dots - \left[x+\frac{n-1}{n}\right] \quad -(1)$

then it is sufficient to p.t.

$f(x) = 0, \forall x \in R$

Now, $f\left(x+\frac{1}{n}\right) = \left[n\left(x+\frac{1}{n}\right)\right] - \left[x+\frac{1}{n}\right] - \left[x+\frac{2}{n}\right] -$

$\dots - [x+1]$ (comma)

$$= [nx] + [1] - \left[x + \frac{1}{n}\right] - \dots - \left[x + \frac{n-1}{n}\right] - [x] - 1$$

$$= [nx] - [x] - \left[x + \frac{1}{n}\right] - \dots - \left[x + \frac{n-1}{n}\right]$$

$$= f(x).$$

Thus,

$$f\left(x + \frac{1}{n}\right) = f(x), \forall x \in R, n \in N \quad -(2)$$

If $0 \leq x \leq \frac{1}{n}$ then

$f(x) = 0$ $\left(\because 0 \leq x \leq \frac{1}{n} \text{ then for } n=2,\ 0 \leq x \leq \right.$

$\Rightarrow f(x) = [2x] - [x] - \left[x + \frac{1}{2}\right]$

$= 0, \forall\ 0 \leq x \leq \frac{1}{2}$

If $0 \leq x \leq \frac{2}{n}$ then

again $f(x) = 0$ $\left(\because x = \frac{2}{n} \Rightarrow f(x) = f\left(\frac{2}{n}\right) \right.$

$= f\left(\frac{1}{n} + \frac{1}{n}\right) = f\left(\frac{1}{n}\right) = 0$

(by (2))

If $0 \leq x \leq \frac{3}{n}$ then again $f(x) = 0$.

continuing the process finally we get $f(x) = 0, \forall x \in R^+$.

Hence result is proved.

(13) Let x be any +ve real number and n is +ve integer then p.t. among the integers from 1 to x the no. of multipliers of n is $\left[\frac{x}{n}\right]$.

Date: / /

roof :- we know that,

$$[x] \le x < [x]+1 \Rightarrow \left[\frac{x}{n}\right] \le \frac{x}{n} < \left[\frac{x}{n}\right]+1$$

$$\Rightarrow \left[\frac{x}{n}\right]n \le x < \left(\left[\frac{x}{n}\right]+1\right)n.$$

$\Rightarrow$ The greatest multiple of n which is less than or equal to x. is $\left[\frac{x}{n}\right]n$

Thus among the integers from 1 to x, the multipliers of ~~n~~ are,

$n, 2n, \ldots, \left[\frac{x}{n}\right]n$

Hence, the total number of multipliers of n in 1 to x is $\left[\frac{x}{n}\right]$.

(14) Find no. of multipliers of 7 among the integers from 200 to 500.

sol^n :-

No. of multiples of 7 among 1 to 500.

is, $\left[\frac{500}{7}\right] = 71$

No. of mult. of 7 among 1 to 199

is, $\left[\frac{199}{7}\right] = 28.$

No. of mult. of 7 among ~~1~~ 200 to 500 is

$71 - 28 = 43.$

(15) Find the number of multiples of 11 among the integers 300 to 1000.

Sol^n:

No. of multiples of 11 among 1 to 1000 $= \left[\frac{1000}{11}\right] = 90$

" " " " " " 1 to 299 $= \left[\frac{299}{11}\right] = 27$

$\therefore$ " " " " " " 300 to 1000 is $90 - 27 = 63$.

(16) P.T., In the product $n!$ the highest power of prime p (denoted by $p(n!)$) is $\sum_{k=1}^{m} \left[\frac{n}{p^k}\right]$, where $p^m \leq n < p^{m+1}$.

OR

In usual notation p.t.

$$p(n!) = \sum_{k=1}^{m} \left[\frac{n}{p^k}\right], \text{ where } p^m \leq n < p^m$$

OR

Let $n \in N$, p be prime then p.t the exponent of the highest power of p that divided $n!$ is,

$$\sum_{k=1}^{m} \left[\frac{n}{p^k}\right], \text{ where } p^m \leq n < p^{m+1}.$$

Date: / /

Here p is prime and

$n! = 1.2 \ldots p \ldots n$

clearly $p / n!$

We know that,

Total no. of multiples of p among 1 to n is $\left[\frac{n}{p}\right]$ which are

$p, 2p, 3p, \ldots \left[\frac{n}{p}\right] p$.

$\therefore$ In $n!$, product of all multiples of p

$$= p \cdot 2p \cdot 3p \cdots \left[\frac{n}{p}\right] p$$

$$= p^{\left[\frac{n}{p}\right]} \left(1 \cdot 2 \cdots \left[\frac{n}{p}\right]\right)$$

$$= p^{\left[\frac{n}{p}\right]} \left(\left[\frac{n}{p}\right]!\right)$$

$\therefore$ Highest power of p in $n!$ is,

$$p(n!) = \left[\frac{n}{p}\right] + p\left(\left[\frac{n}{p}\right]!\right) \quad \text{—(1)}$$

Similarly

$$p\left(\left[\frac{n}{p}\right]!\right) = \left[\frac{\left[\frac{n}{p}\right]}{p}\right] + p\left(\left[\frac{\left[\frac{n}{p}\right]}{p}\right]!\right)$$

$$\Rightarrow p\left(\left[\frac{n}{p}\right]!\right) = \left[\frac{n}{p^2}\right] + p\left(\left[\frac{n}{p^2}\right]!\right) \quad \text{—(2)}$$

putting in (1), we get

$$p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + p\left(\left[\frac{n}{p^2}\right]!\right).$$

continuing this process, we get

$$p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \dots + \left[\frac{n}{p^m}\right] + \left[\frac{n}{p^{m+1}}\right] + p\left(\left[\frac{n}{p^{m+1}}\right]!\right).$$

$$= \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \dots + \left[\frac{n}{p^m}\right]$$

$$\boxed{\therefore p(n!) = \sum_{k=1}^{m} \left[\frac{n}{p^k}\right]}$$

$\left(\because p^m \le n < p^{m+1} \right.$
$\Rightarrow \frac{n}{p^{m+1}} < 1$
$\Rightarrow \left[\frac{n}{p^{m+1}}\right] = 0.$

(17) In usual notation p.t.,

$$p(p^r!) = \frac{p^r - 1}{p - 1}$$

proof :-

from the above thm,

$$\text{L.H.S. } p(p^r!) = \left[\frac{p^r}{p}\right] + \left[\frac{p^r}{p^2}\right] + \dots + \left[\frac{p^r}{p^r}\right]$$

$$= p^{r-1} + p^{r-2} + \dots + 1$$

$$= \frac{p^r - 1}{p - 1}.$$

$= R.H.S.$

(18) Find highest power of 2 in 50!, also find 3(50!), 4(50!), 8(50!).

Sol^n:-

$n = 50$.

Now, $2(50!) = \left[\frac{50}{2}\right] + \left[\frac{50}{4}\right] + \left[\frac{50}{8}\right] + \left[\frac{50}{16}\right] + \left[\frac{50}{32}\right]$

$= 25 + 12 + 6 + 3 + 1$

$= 47$.

Now, $50! = 2^{47} \times k$, k is odd

$= 2^{46} \cdot 2k$

$= (2^2)^{23} \cdot 2k$

$= 4^{23} \cdot 2k$

$\therefore 4(50!) = 23$.

also, $50! = 2^{47} \times k$, k is odd

$\Rightarrow 50! = 2^{45} \cdot 2^2 \times k$

$= (2^3)^{15} \cdot 2^2 \times k$

$= 8^{15} \times 4k$

$\therefore 8(50!) = 15$

again,

$3(50!) = \left[\frac{50}{3}\right] + \left[\frac{50}{9}\right] + \left[\frac{50}{27}\right]$

(19) P.T. $2^{47} \mid 50!$ & $2^{48} \nmid 50!$

proof :- we know that,

$$2(50!) = 47 \quad \text{(prove it)}$$

$\Rightarrow 50! = 2^{47}.k$, k is odd integer

$\Rightarrow 2^{47} \mid 50!$ but $2^{48} \nmid 50!$

($\because$ k is odd)

(20) If p is not prime then prove that above theorem (16) is need not be true

solⁿ :-

If n=50 and p=4 (not prime) then

$$4(50!)\ 23 \text{ (prove it)}.$$

but by above thm,

highest power,

$$4(50!) = \left[\frac{50}{4}\right] + \left[\frac{50}{16}\right] + \left[\frac{50}{64}\right]$$

$$= 12 + 3 = 15.$$

Thus above thm. is not true when p is not prime

(21) P.T. Product of n consecutive +ve intege[rs] can be divided by n!

proof:

Let a be any +ve integer then we have to prove that,

product of n consecutive integers a+1, a+2, ---, a+[n]

i.e. we have to prove that,

$$\frac{(a+1)(a+2)\cdots(a+n)}{n!} \in \mathbb{Z}.$$

Now,

$$\frac{(a+1)(a+2)\cdots(a+n)}{n!}$$

$$= \frac{1\cdot 2\cdot 3\cdots a(a+1)\cdots(a+n)}{1\cdot 2\cdot 3\cdots a\cdot n!}$$

$$= \frac{(a+n)!}{a!\,n!}$$

$$= {}^{(a+n)}C_n \in \mathbb{Z}$$

(22) Prove that, $a!\cdot b! \,/\, (a+b-1)!$

if $(a,b)=1$. (or) P.T. $\frac{(a+b-1)!}{a!b!}$ is +ve integ

Proof:- we know that, $\frac{(a+b-1)!}{(a-1)!\,b!}$

$$= {}^{(a+b-1)}C_b = p \in \mathbb{Z} \quad -(1)$$

& $\frac{(a+b-1)!}{a!(b-1)!} = {}^{(a+b-1)}C_a = q \in \mathbb{Z}. \quad -(2)$

By (1) & (2) we say that,

$$(a+b-1)! = (a-1)!\,b!\,p = a!\,(b-1)!\,q$$

$\Rightarrow (a-1)!\, b(b-1)!\, p = a(a-1)!\,(b-1)!\, q$

$\Rightarrow bp = aq$

$\Rightarrow a / bp$

$\Rightarrow a/p \quad (\because (a,b)=1$

$\Rightarrow p = ak$, for some $k \in \mathbb{Z}$.

then by (3),

$$(a+b-1)! = (a-1)!\, b!\, ak.$$
$$= a!\, b!\, k$$
$$\Rightarrow \boxed{a!\,b! \,/\, (a+b-1)}$$

Mobious function:- of the integer m

Mobious function is denoted by $\mu(m)$ & defined as,

$$\mu(m) = \begin{cases} 1, & \text{if } m=1 \\ (-1)^r, & \text{if } m \text{ is product of } r \text{ distinct prime} \\ 0, & \text{if } m \text{ has atleast a squre factor.} \end{cases}$$

m	1	2	3	4	5	6	7	8	9	10	11	1[illegible]
$\mu(m)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0

from the above table,

$\mu(p) = -1$, if p is prime

$\mu(m) \le 1, \ \forall m \geq 1$

Date: / /

(23) Prove that, μ is multiplicative function

Proof:-

We have to prove that,

$$\mu(ab) = \mu(a)\mu(b) \quad , \quad \text{if } (a,b)=1$$

case-1 :- If either $a=1$ or $b=1$ then clearly $\mu(ab)=\mu(a)\mu(b)$.

case-2 :- If any of a or b has a square factor then ab also has a square factor.

$$\therefore \mu(ab) = \mu(a)\mu(b) = 0.$$

case-3 :- If both a & b have no square factor then we can write $a = p_1 p_2 \cdots p_k$

$b = q_1 \cdot q_2 \cdots q_m$

where all p_i & q_i are distinct prime

$[\because (a,b)=1$

$\therefore \mu(a) = (-1)^k$

$\mu(b) = (-1)^m$

& $\mu(ab) = (-1)^{k+m} = (-1)^k \cdot (-1)^m = \mu(a)\mu(b)$

Hence, $\mu(ab) = \mu(a)\mu(b)$ if $(a,b)=1$.

(24) If $a>1$, then prove that,

$$\sum_{d/a} \mu(d) = 0 = \sum_{d/a} \mu\left(\frac{a}{d}\right)$$

proof :- Let $a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$.
where all p_is are primes

Let $F(a) = \sum_{d/a} \mu(d)$

First we prove that,
$F(bc) = F(b)F(c)$. if $(b,c) = 1$. — (1)

L.H.S. =

$$F(bc) = \sum_{d/bc} \mu(d)$$

$$* = \mu(1) + \mu(b) + \mu(c) + \mu(bc)$$
$$= 1 + \mu(b) + \mu(c) + \mu(b)\mu(c).$$
$$= [1 + \mu(b)][1 + \mu(c)]$$
$$= [\mu(1) + \mu(b)][\mu(1) + \mu(c)].$$
$$= F(b)F(c).$$
$$= R.H.S.$$

We know that,
$$a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}.$$

$$F(a) = F(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k})$$
$$= F(p_1^{a_1}) F(p_2^{a_2}) \cdots F(p_k^{a_k}) \quad \text{— (2)}$$

Now,
$$F(p_i^{a_i}) = \sum_{d/p_i^{a_i}} \mu(d)$$

$$= \mu(1) + \mu(p_i) + \mu(p_i^2) + \cdots + \mu(p_i^{a_i})$$

By (2) we say that,

$$F(a) = \sum_{d/a} \mu(d) = 0.$$

Since, d takes all factors of 'a',

$\frac{a}{d}$ also takes all the factors of 'a.

$$\left(\because \begin{array}{l} a=12, \; d = 1, 2, 3, 4, 6, 12 \\ \frac{a}{d} = 12, 6, 4, 3, 2, 1 \end{array} \right.$$

$\therefore$ We can write, $\sum_{d/a} \mu\left(\frac{a}{d}\right) = 0.$

(see pg. 187 for U4 t 2

U-4

x (25) If m is +ve integer then p.t.

$$\phi(m) = m \sum_{d/m} \frac{\mu(d)}{d} = \sum_{d/m} \mu\left(\frac{m}{d}\right) \cdot d.$$

$$\left[\because m \sum_{d/m} \frac{\mu\left(\frac{m}{d}\right)}{\frac{m}{d}} \right]$$

proof :-

Let $m = p_1^{m_1} p_2^{m_2} \cdots p_k^{a_k}$.

where all p_i's are primes

Now, define a function,

$$F(m) = \sum_{d/m} \frac{\mu(d)}{d}.$$

first we prove that,

$F(bc) = F(b) F(c)$, if $(b, c) = 1$.

$$LHS = F(bc) = \sum \frac{\mu(d)}{d}$$

Date: 18-7

(52) P.T. for any +ve integer n, the eq^n. $x^n+y^n=z^n$ has no +ve integer sol^n $< n$.

proof:-

Suppose, $x^n+y^n=z^n$ has +ve integer sol^n. such that $x \le y$ & $x < n$.

Since, $x^n+y^n=z^n$

$$\Rightarrow z^n \geq x^n \text{ \& }$$
$$z^n \geq y^n.$$
$$\therefore z > x \text{ \& } z > y$$

also, $x^n = z^n - y^n$

$$= (z-y)(z^{n-1}+yz^{n-2}+y^2z^{n-3}+\cdots+y^{n-1})$$
$$> x^{n-1}+x^{n-2}\cdot x+x^{n-3}x^2+\cdots+x^{n-1}$$
$$= n\,x^{n-1}.$$
$$> x\cdot x^{n-1} \quad (\because n > x).$$
$$= x^n$$

Thus $x^n > x^n$ ✗.

Hence, $x^n+y^n=z^n$ has no +ve integer sol^n. $< n$.

* Fibonacci Numbers:-

The sequence 1, 1, 2, 3, 5, 8, 13, 21, ... is called Fibonacci sequence and its terms are called Fibonacci numbers.

The n^{th} (term) Fibonacci number is denoted by u_n.

The general formula for n^{th} term is,

$$u_n = u_{n-1} + u_{n-2}, \forall n \geq 3$$

i.e. $u_{n+1} = u_n + u_{n-1}, \forall n \geq 2$

$\Rightarrow u_n = u_{n+1} - u_{n-1}, \forall n \geq 2.$

(53) P.T. $(u_n, u_{n+1}) = 1, \forall n \geq 1.$

OR

P.T. the successive Fibonacci numbers are relatively prime.

proof:- we know that,

$$u_{n+1} = 1 \cdot u_n + u_{n-1}$$
$$u_n = 1 \cdot u_{n-1} + u_{n-2}$$
$$u_{n-1} = 1 \cdot u_{n-2} + u_{n-3}$$
$$\vdots$$
$$u_4 = u_3 + u_2$$
$$u_3 = 2u_2 + 0$$

Hence, by Eulcidean algorithm we say that,

$$(u_{n+1}, u_n) = u_2 = 1$$

(54) In usual notation p.t.

$u_{m+n} = u_{m-1} u_n + u_m u_{n+1}, \forall m, n \in N.$

proof:- We can prove this result by using mathematical induction.

Date: 1/10/1

on n (for fix m)

for $n=1$

$LHS = u_{m+1}$

$RHS = u_{m-1} u_1 + u_m u_2$

$= u_{m-1} + u_m \quad (\because u_1 = 1 = u_2)$

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

$= LHS.$

Thus result is true for $n=1$

Suppose result is true for all $n < k+1$ then we have to p.t. result is true for $n=k+1$.

i.e. we have to p.t

$u_{m+(k+1)} = u_{m-1} u_{k+1} + u_m u_{k+2}$

Since result is true for $n=k$ & $n=k-1$

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

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

By adding these results, we get

$u_{m+k} + u_{m+(k-1)}$

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

$u_m(u_{k+1} + u_k)$

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

Thus result is true for $n=k+1$

Hence, by PMI we say that

Page No.:
Date: / /

(c) P.T. u_m / u_{mn}

proof:- We prove this result by using P.M.I. on n

for $n = 1$

u_m / u_m which is true

$\therefore$ result is true for $n = 1$

suppose result is true for $n = k$

i.e u_m / u_{mk}

then we have to PT.

result is true for $n = k+1$

i.e we have to p.t

$u_m / u_{m(k+1)}$

W.K.T.

$u_{m(k+1)} = u_{mk+m}$

$= u_{mk-1} u_m + u_{mk} u_{m+1}$

$\Rightarrow u_m / u_{m(k+1)}$

$(\because u_m / u_m \;\&\; u_m / u_{mk})$

Thus result is true for $m = k+1$

Hence by PMI we say that

$u_m / u_{mn}, \; \forall m, n \geq 1$.

(56) P.T. $m/n \Rightarrow u_m/u_n$

proof :- W.K.T. u_m/u_{mn}

Here,

Now, $m/n \Rightarrow n = mk$

By above thm, u_m/u_{mk}

$\Rightarrow u_m/u_n$

(57) If $m = qn + r$ then p.t.

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

proof :-

$LHS = (u_m, u_n)$

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

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

$= (u_{qn-1} u_r, u_n)$ — (i)

($\because$ if $b/c \Rightarrow (a+c, b) = (a,b)$

& Here u_n/u_{qn}

If $(u_{qn-1}, u_n) = d$ then

d/u_{qn-1} & d/u_n

Since, u_n/u_{qn}, d/u_{qn}

Thus, d/u_{qn-1} & d/u_{qn}

$\Rightarrow d = 1$ ($\because (u_{qn}, u_{qn-1}) = 1$

$\therefore$ By (i)

$$LHS = (u_{qn-1}u_r, u_n)$$
$$= (u_r, u_n) \quad (\because (u_{qn-1}, u_n) = 1)$$
$$= RHS$$

(58) P.T. $(u_m, u_n) = u_d$, where $d = (m, n)$ <u>or</u>

g.c.d. of two Fibonacci no^s. is also a Fibonacci number.

<u>or</u>

$$(u_m, u_n) = u_{(m,n)}$$

Proof:- Let u_m & u_n be two Fibonacci no^s. with $m \geq n$ then by Euclidean algorithm we say that,

$$m = q_1 n + r_1, \quad 0 \leq r_1 < n.$$
$$n = q_2 r_1 + r_2 \quad 0 \leq r_2 < r_1$$
$$r_1 = q_3 r_2 + r_3 \quad 0 \leq r_3 < r_2$$
$$\vdots$$
$$r_{n-2} = q_n r_{n-1} + r_n, \quad 0 \leq r_n < r_{n-1}.$$
$$r_{n-1} = q_{n+1} r_n$$
$$\therefore (m, n) = r_n,$$

also by above lemma,

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

(63) P.T. $\sum_{i=1}^{n} u_i^2 = u_n u_{n+1}$

Sol. W.K.T.

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

$\Rightarrow u_n u_{n+1} = u_n^2 + u_n u_{n-1}$

$\Rightarrow u_n^2 = u_n u_{n+1} - u_n u_{n-1}$

NOW,

$LHS = \sum_{i=1}^{n} u_i^2$

$= u_1^2 + u_2^2 + \cdots + u_n^2$

$= u_1^2 + (u_2 u_3 - u_2 u_1) +$
$(u_3 u_4 - u_3 u_2) + \cdots +$

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

$= u_1^2 - u_2 u_1 + u_n u_{n+1}$

$= 1 - 1 \cdot 1 + u_n u_{n+1} = u_n u_{n+1} = RH$

(64) P.T.

$u_{n+1}^2 = u_n^2 + 3u_{n-1}^2 + 2[u_{n-2}^2 + u_{n-3}^2 + \cdots + u_2^2 + u_1^2]$.

proof :- W.K.T

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

$u_n = u_{n+1} - u_{n-1}$ —(1)

$\sum_{i=1}^{n} u_i^2 = u_n u_{n+1}$ —(2)

Page No.:
Date: / /

Now,

$$RHS = u_n^2 + 3u_{n-1}^2 + 2(u_{n-2}^2 + u_{n-3}^2 + \dots + u_2^2 + u_1^2)$$

$$= 2(u_1^2 + u_2^2 + \dots + u_n^2) - u_n^2 + u_{n-1}^2$$

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

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

(by (1) & (2))

$$= 2u_n u_{n+1} + \cancel{u_{n-1}^2} - u_{n+1}^2 + 2u_{n+1}u_{n-1} - \cancel{u_{n-1}^2}$$

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

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

$$= u_{n+1}^2 = LHS.$$

(65) Prove the following:

(i) $2 / u_n \Leftrightarrow 3 / n$

proof :- $2 / u_n \Leftrightarrow u_3 / u_n \Leftrightarrow 3 / n$

(ii) $5 / u_n \Leftrightarrow 5 / n$.

proof :- $5 / u_n \Leftrightarrow u_5 / u_n \Leftrightarrow 5 / n$

— x —

355

* Indeterminate eq^n:-

An equation which has two or more than two unknown is called indetermin eq^n. Or Diophantine eq^n.

e.g $x+y=7$, $2x+y+z=8$.

A system of indeteminate eq^n is called indeteminate system if the no. of eq^n is less than that of the unknowns.

e.g (1) $\begin{Bmatrix} x+2y+z=6 \\ 2x-5y+3z=5 \end{Bmatrix}$

(2) $\begin{Bmatrix} x-2y+z=5 \\ 3x-y+2z=7 \end{Bmatrix}$.

Th-(28) (i) Prove that, the linear indeteminate eq^n $ax+by=c$ $(a,b,c \in Z)$ has integer sol^n iff d/c where $(a,b)=d$.

(ii) moreover if $x=x_0$, $y=y_0$ is a perticular sol^n then p.t. general sol^n can be written as.

$x = x_0 + \frac{b}{d}t$, $y = y_0 - \frac{a}{d}t$, where $t \in Z$.

Proof:- (i)

If $ax+by=c$ has sol^n.

let $d=(a,b)$ then d/a, d/b.

$\Rightarrow d/ax$, d/by

$\Rightarrow d/ax+by \Rightarrow d/$

Date : / /

Converse part :-

as $c = kd$

$ax_1 + by_1 = d$

c

$a(kx_1) + b(ky_1) = kd$

$\Rightarrow a(kx_1) + b(ky_1) = c$

$\Rightarrow ax + by = c$

has sol

If d/c then we have to p.t. $ax+by=c$ has sol^n.

i.e. p.t.

$$\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d} \text{ has } sol^n$$

$$\left(\because \frac{a}{d}, \frac{b}{d}, \frac{c}{d} \in Z\right)$$

i.e. $a'x + b'y = c'$ has sol^n.

where $a' = \frac{a}{d}$, $b' = \frac{b}{d}$, $c' = \frac{c}{d}$

we know that, $(a, b) = d$

$$\therefore \left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

$$\therefore (a', b') = 1.$$

$\therefore \exists\ x_0, y_0 \in Z \ni a'x_0 + b'y_0 = 1$.

$$\Rightarrow a'c'x_0 + b'c'y_0 = c'.$$

$\Rightarrow x = c'x_0,\ y = c'y_0$ is sol^n of $a'x + b'y = c'$.

Hence, $ax + by = c$ has sol^n.

(ii) If $x = x_0$ & $y = y_0$ is perticular sol^n of $ax+by=c$ then

$$ax_0 + by_0 = c.$$

$$\Rightarrow \frac{a}{d}x_0 + \frac{b}{d}y_0 = \frac{c}{d}$$

$$\Rightarrow a'x_0 + b'y_0 = c' \quad \text{—— (1)}$$

also, $ax+by=c$

$$\Rightarrow \frac{a}{d}x+\frac{b}{d}y=\frac{c}{d}.$$

$$\Rightarrow a'x+b'y=c'. \quad -(2)$$

Subtraction of (2) from (1) gives,

$$a'(x_0-x)+b'(y_0-y)=0$$

$$\Rightarrow b'(y_0-y)=a'(x-x_0) \quad -(3)$$

$$\Rightarrow a' / b'(y_0-y).$$

$$\Rightarrow a' / (y_0-y) \quad (\because (a',b')=1)$$

$$\Rightarrow y_0-y=a't, \quad t\in\mathbb{Z}. \quad -(4)$$

$$\Rightarrow \boxed{y=y_0-\frac{a}{d}t}.$$

By (3) & (4), we get

$$a'(x_0-x)+b'a't=0$$

$$\Rightarrow x_0-x+b't=0$$

$$\Rightarrow x=x_0+\frac{b}{d}t, \quad t\in\mathbb{Z}$$

or

$$a'(x-x_0)=b'a't$$

$$x-x_0=b't$$

$$\Rightarrow x=x_0+b't$$

$$\boxed{x=x_0+\frac{b}{d}t}$$

Thus general sol^n of $ax+by=c$ can be written as,

$$x=x_0+\frac{b}{d}t, \quad y=y_0-\frac{a}{d}t, \quad t\in\mathbb{Z}.$$

Date: / /

(29) If $(a,b)=1$ then prove that,

Th-2 any sol^n. of $ax+by=c$ can be written as $x=x_0+bt$, $y=y_0-at$, $t\in Z$. where $x=x_0$ and $y=y_0$ are perticular sol^n. of $ax+by=c$.

Proof:-

Here $x=x_0$ and $y=y_0$ are perticular sol^{ns}. of $ax+by=c$.

$$\therefore ax_0+by_0=c \quad -(1) \quad \text{also}$$
$$ax+by=c \quad -(2)$$

Subtraction of (2) from (1) gives

$$a(x_0-x)+b(y_0-y)=0 \quad (3)$$
$$\Rightarrow b(y_0-y)=a(x-x_0)$$
$$\Rightarrow a / b(y_0-y)$$
$$(\because (a,b)=1$$
$$\Rightarrow a/(y_0-y)$$
$$\Rightarrow y_0-y=at, \quad t\in Z.$$
$$\Rightarrow y=y_0-at, \quad t\in Z$$

putting $y_0-y=at$ in (3)

$$a(x_0-x)+bat=0$$
$$\Rightarrow x_0-x+bt=0$$
$$\Rightarrow x=x_0+bt, \quad t\in Z.$$

Hence, $x=x_0+bt$, $y=y_0-at$, $t\in Z$ is general sol^n of $ax+by=c$.

* Remark:-

(1) If co-efficient of $ax+by=c$ are not large then we can find its solⁿ by inspection method.

(2) Also we can solve the eqⁿ. $ax+by=c$ by applying the process of successively deminishing the coeffic

(30) solve the eqⁿ. $525x+231y=42$.

solⁿ :-

Here,

$525 = 3\times5^2\times7$

$231 = 3\times7\times11$

$\therefore (525, 231) = 3\times7 = 21$

also $21/42$.

$\therefore$ Given eqⁿ has solⁿ.

Now, $525x+231y=42 \quad -(1)$

$\Rightarrow 25x+11y=2 \quad -(2)$

$\Rightarrow 11(2x+y)+3x-2=0$

$\Rightarrow 11u+3x-2=0$; where $u=2x+y \quad -(3)$

$\Rightarrow u=1,\ x=-3$

$\therefore$ from (3)

$1 = 2(-3)+y$

$\Rightarrow y=7$

is a perticular solⁿ.

Thus $x_0=-3$ & $y_0=7$ is a perticular solⁿ of given eqⁿ.

Date : / /

Hence, reqd. general solⁿ is,

$$x = x_0 + \frac{b}{d}t \quad , \quad y = y_0 - \frac{a}{d}t \quad , \quad t \in \mathbb{Z}$$

$$\Rightarrow x = -3 + 11t \quad , \quad y = 7 - 25t \quad , \quad t \in \mathbb{Z}$$

([redacted]) Find the +ve integer solns of following eqns (by using method of successive diminishing the coefficien

(31) $7x + 19y = 213$.

solⁿ:- Here $(7,19) = 1$ & $1 / 213$.

$\therefore$ given eqⁿ has solⁿ.

Now, $7x + 19y - 213 = 0$.

$$\Rightarrow 7(x + 3y - 30) - 2y - 3 = 0$$

$$\Rightarrow 7u - 2y - 3 = 0 \text{, where } u = x + 3y - 30 \quad -(1)$$

$$\Rightarrow u = 1, \quad y = 2$$

from (1)

$$1 = x + 3(2) - 30$$

$$\Rightarrow x = 25.$$

$$x = x_0 + \frac{b}{d}t \quad , \quad y = y_0 - \frac{a}{d}t \quad , t \in \mathbb{Z}$$

$$\therefore x = 25 + 19t \quad , \quad y = 2 - 7t \quad -(2)$$

Now, for +ve integer solⁿ $x > 0$ & $y > 0$

Now,

$x > 0$	$y > 0$
$\Rightarrow 25 + 19t > 0$	$\Rightarrow 2 - 7t > 0$
$\Rightarrow 19t > -25$	$\Rightarrow 2 > 7t$
$\Rightarrow t > -\frac{25}{19} \Rightarrow t > -1.3$	$\Rightarrow t < \frac{2}{7} \Rightarrow t < 0.28$

$\therefore\ -1.3 < t < 0.28$

$\Rightarrow\ t = -1, 0.$

putting these values in (2), we get

$t=0 \Rightarrow x = 25,\ y = 2$

$t=-1 \Rightarrow x = 6,\ y = 9$

$\therefore$ (25, 2) & (6, 9) are the only +ve solns of given eq.

(32) $19x + 20y = 1909.$

soln. $(19, 20) = 1$ & $1 / 1909$

Now, $19x + 20y = 1909$

$\Rightarrow 19(x + y - 100) + y - 9 = 0$

$\Rightarrow 19u + y - 9 = 0.$, where $u = x + y - 100$ —(*)

$\Rightarrow u = 1,\ y = -10$

$\Rightarrow 1 = x - 10 - 100$ (by (*))

$\Rightarrow x = 111$

$\therefore x_0 = 111,\ y_0 = -10$ is perticular soln.

Now, general soln is,

$x = x_0 + \frac{b}{d}t,\quad y = y_0 - \frac{a}{d}t$

$\Rightarrow x = 111 + 20t,\quad y = -10 - 19t.\ ,\ t \in Z$ —(**)

Now for +ve solns

$x > 0,\quad y > 0$

$\Rightarrow 111 + 20t > 0 \qquad \Rightarrow -10 - 19t > 0$

$\Rightarrow 20t > -111 \qquad \Rightarrow -19t > 10$

$\Rightarrow t > \frac{-111}{20} \qquad \Rightarrow 19t < -10$

$\qquad \Rightarrow t < \frac{-10}{19}$

$\Rightarrow t > -5.5$

Date: / /

$\therefore -5.5 < t < -0.53$

$t = -5, -4, -3, -2, -1$.

$\therefore$ By (**)

for $t=-5$, $x = 111 + 20(-5) = 11$

$y = -10 - 19(-5) = 85$

for $t=-4$, $x = 111 + 20(-4) = 31$

$y = -10 - 19(-4) = 66$

for $t=-3$, $x = 111 + 20(-3) = 51$

$y = -10 - 19(-3) = 47$

for $t=-2$, $x = 111 + 20(-2) = 71$

$y = -10 - 19(-2) = 28$

for $t=-1$, $x = 111 + 20(-1) = 91$

$y = -10 - 19(-1) = 9$.

(33)* $x^2 + xy - 6 = 0$.

sol^n:- Here $x^2 + xy - 6 = 0$

$\Rightarrow x^2 + xy = 6$

$\Rightarrow x(x+y) = 6$

$\Rightarrow x = 6, \quad x+y = 1 \Rightarrow y = -5$

$x = 1, \quad x+y = 6 \Rightarrow y = 5$

$x = 3, \quad x+y = 2 \Rightarrow y = -1$

$x = 2, \quad x+y = 3 \Rightarrow y = 1$

Hence, (1,5) & (2,1) are req^d +ve integer sol^{ns}.

Date: 1, 6, 1

(34) $y - \dfrac{x+3y}{x+2} = 1$.

Soln. Here, $y = 1 + \dfrac{x+3y}{x+2}$

$$= \frac{x+2+x+3y}{x+2}$$

$$\Rightarrow y = \frac{2x+3y+2}{x+2}.$$

$$\Rightarrow xy+2y = 2x+3y+2.$$
$$\Rightarrow xy - y = 2x+2$$
$$\Rightarrow y(x-1) = 2(x+1).$$
$$\Rightarrow y = \frac{2(x-1+2)}{x-1}$$
$$\Rightarrow y = 2 + \frac{4}{x-1} \quad -(*)$$

Since, y is integer, $\dfrac{4}{x-1} \in Z$.

$\therefore x-1 / 4$

$\Rightarrow x-1 = \pm1, \pm2, \pm4.$

$\Rightarrow x = 1\pm1, 1\pm2, 1\pm4.$

$\Rightarrow x = 2, 0, 3, -1, 5, -3.$

Since, x is positive,

$x = 0, 2, 3, 5.$

By (*)

for $x=0$, $y=-2$

for $x=2$, $y=6$

for $x=3$, $y=4$

for $x=5$, $y=3$

Thus, (2, 6), (3, 4) & (5, 3) are reqrd +ve integer sol^{ns}.

Date: / /

(35) Solve, $8x-18y+10z=16$

sol^n

Here, $(8,-18,10)=2$ & $2/16$

$\therefore$ given eq^n has sol^n.

Now,

$8x-18y+10z=16$

$\Rightarrow 4x-9y+5z-8=0$

$\Rightarrow 4(x-2y+z-2)-y+z=0$

$\Rightarrow 4u-y+z=0$, where $u=x-2y+z-2$ — (*)

$\Rightarrow u=1, y=1, z=-3$

from (*)

$1=x-2-3-2$

$\Rightarrow x=8$

Hence, $(8,1,-3)$ is req^{rd} sol^n.

(36) Solve, $50x+45y+60z=10$.

sol^n - Here $(50,45,60)=5$ & $5/10$

$\therefore$ given eq^n has sol^n.

Now, $50x+45y+60z=10$

$\Rightarrow 10x+9y+12z=2$

$[\Rightarrow 9(x+y+z)+x+3z-2=0]$

$\Rightarrow 10(-1)+9(0)+12(+1)=2$,

$\Rightarrow x=-1,\ y=0,\ z=+1$

Hence,

$(-1,0,1)$ is the sol^n of given eq^n

(31) Find general solⁿ $50x+45y+36z=1$

solⁿ :-

Here, $(50,45,36)=1 \ \&\ 1/10$.

$\therefore$ given eqⁿ has a solⁿ.

Now,

$$50x+45y+36z=10$$
$$\Rightarrow 36(x+y+z)+14x+9y=10$$
$$\Rightarrow 36k_1+14x+9y=10,$$
where $k_1 = x+y+z$ —(1)

$$\Rightarrow 9(4k_1+x+y)+5x=10$$
$$\Rightarrow 9\cdot 5k_2+5x=10,$$ where
$5k_2 = 4k_1+x+y.$ —(2)
$$\Rightarrow 9k_2+x=2$$
$$\Rightarrow x=2-9k_2.$$

By (2),
$$5k_2 = 4k_1+x+y.$$
$$\Rightarrow y = 5k_2-4k_1-2+9k_2$$
$$\Rightarrow y = 14k_2-4k_1-2$$

putting these values of x & y in (1), we get

$$k_1 = \cancel{2}-9k_2+14k_2-4k_1-\cancel{2}+z$$
$$\Rightarrow z = 5(k_1-k_2).$$

Hence, general solⁿ is,

$$x = 2-9k_2,$$
$$y = 14k_2-4k_1-2$$
$$z = 5(k_1-k_2)$$, where $k_1,k_2 \in \mathbb{Z}$

Date : / /

(38) Find sol^n of $8x-18y+10z=16$

sol^n:-

Here $(8,-18,10)=2$ & $2/16$.

$\therefore$ given eq^n has sol^n.

Now,

$$8x-18y+10z=16$$
$$\Rightarrow 4x-9y+5z=8$$
$$\Rightarrow 4(x-2y+z)-y+z=8$$
$$\Rightarrow 4k_1-y+z=8, \text{ where } k_1=x-2y+z \quad -(1)$$
$$\Rightarrow k_2+z=8, \text{ where } k_2=4k_1-y$$
$$\therefore y=4k_1-k_2$$
$$\Rightarrow z=8-k_2$$

putting these values of z & y in (1)

$$k_1=x-8k_1+2k_2+8-k_2$$
$$\Rightarrow x=9k_1-k_2-8.$$

$\therefore x=9k_1-k_2-8, \ y=4k_1-k_2, \ z=8-k_2$

is general sol^n of given eq^n.

(39) Find general sol^n of
$$50x+45y+60z=10.$$

sol^n:- Here $(50,45,60)=5$ & $5/10$

Now, $50x+45y+60z=10$
$$\Rightarrow 10x+9y+12z=2$$
$$\Rightarrow 9(x+y+z)+x+3z=2$$

$\Rightarrow 9k_1 + x + 3z = 2$, $k_1 = x + y + z$ — (1)

$k_2 + x = 2$, $k_2 = 9k_1 + 3z$

$\Rightarrow 3(3k_1 + z) + x = 2$

$\Rightarrow 3k_2 + x = 2$, $k_2 = 3k_1 + z$

$\Rightarrow x = 2 - 3k_2$ $\Rightarrow z = k_2 - 3k_1$

& from (1) $y = k_1 - 2 + 3k_2 - k_2 + 3k_1$

$= 4k_1 + 2k_2 - 2.$

Hence, req^rd. general sol^ns are,

$x = 2 - 3k_2,\ y = 4k_1 + 2k_2 - 2,\ z = k_2 - 3k_1.$

(40) P.T. the linear indeterminant eq^n.

(*) $a_1x_1 + a_2x_2 + \dots + a_nx_n = c$ has integer sol^n, iff d/c, where $d = (a_1, a_2, \dots, a_n)$

proof:-

Suppose, $a_1x_1 + a_2x_2 + \dots + a_nx_n = c$ — (1) has sol^n. then $d = (a_1, a_2, \dots, a_n)$

$\Rightarrow d/a_1,\ d/a_2, \dots, d/a_n.$

$\Rightarrow d/a_1x_1,\ d/a_2x_2, \dots\ d/a_nx_n$

$\Rightarrow d/(a_1x_1 + \dots + a_nx_n)$

$\Rightarrow d/c.$

If d/c then $c = kd$, for $k \in \mathbb{Z}$.

Here $(a_1, a_2, \dots, a_n) = d$

$\therefore \exists\ y_1, y_2, \dots, y_n \in \mathbb{Z} \ni$

$a_1y_1 + a_2y_2 + \dots + a_ny_n = d$

$\Rightarrow a_1(ky_1) + a_2(ky_2) + \dots + a_n(ky_n) = kd$
$= c$

$\Rightarrow x_1 = ky_1, \dots, x_n = ky_n$ is sol^n of eq^n (1)

Date: / /

(91) Solve, $2x+10y+202z=5$.

sol^n:- $(2, 10, 202) = 2 \nmid 5$.

$\therefore$ given eq^n has no sol^n.

(92) P.T. the +ve integer sol^n of $x^{-1}+y^{-1}=z^{-1}$ $(x,y,z)=1$ has & must have the form $x=a(a+b)$, $y=b(a+b)$, $z=ab$, where $a,b>0$. $(a,b)=1$.

Th-3

Proof:-

First we p.t. $x=a(a+b)$, $y=b(a+b)$, $z=ab$ is sol^n of $x^{-1}+y^{-1}=z^{-1}$.

$$L.H.S. = x^{-1}+y^{-1}$$

$$= \frac{1}{a(a+b)} + \frac{1}{b(a+b)}$$

$$= \frac{b+a}{ab(a+b)}$$

$$= \frac{1}{ab}$$

$$= z^{-1}. = RHS$$

Now we p.t every sol^n of $x^{-1}+y^{-1}=z^{-1}$. $(x,y,z)=1$ is of the form, $x=a(a+b)$, $y=b(a+b)$, $z=ab$,

$(a,b)=1$, $a,b>0$

If x,y,z is any sol^n of $x^{-1}+y^{-1}=z^{-1}$ & $(x,y)=c$ then c/x & c/y.

$\Rightarrow x=ac$, $y=bc$, for some $a,b\in$

& $(a,b)=1$

Now, $z^{-1} = x^{-1} + y^{-1}$

$$= \frac{1}{ac} + \frac{1}{bc}$$

$$= \frac{a+b}{abc}$$

$$\Rightarrow z = \frac{abc}{a+b} \quad -(*)$$

since $z \in \mathbb{Z}$, $a+b / abc$

also $(a,b) = 1$

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

$\therefore a+b / abc \Rightarrow a+b / c$

$\Rightarrow c = c'(a+b)$ for some $c' \in \mathbb{Z}$

putting this value of c in $(*)$, we get

$$z = \frac{abc'(a+b)}{a+b}$$

$$= abc'.$$

also,

$x = ac \Rightarrow x = \cancel{ab}\ ac'(a+b)$

$y = bc \Rightarrow y = bc'(a+b).$

Now, $(x, y, z) = 1$

$\Rightarrow (a(a+b)c', b(a+b)c', abc') = 1$

$\times \Big[\Rightarrow ((a(a+b)c', b(a+b)c'), abc') = 1$

$\Rightarrow (c'($

$\Rightarrow ((a+b)c'(a,b), abc')$

$\Rightarrow ((a+b)c', abc') \quad (\because (a,b) = 1$

Date: / /

Hence,

$x = a(a+b)$, $y = b(a+b)$, $z = ab$.

$a, b > 0$, $(a,b) = 1$.

* Pythagoras equation or Shang-gao eq^n :-

The indeterminate eq^n of 2^{nd} degree of the form $x^2+y^2=z^2$ is called Pythagoras equation.

* Lemma (without proof) :-

If $xy = z^n$, $(x,y)=1$ then $\exists$ +ve integer a, b $\ni$ $x = a^n$, $y = b^n$, $(a,b)=1$.

(43) P.T. the general integer sol^n of $x^2+y^2=z^2$ with $x,y,z>0$, $(x,y)=1$ and y even is given by $x=a^2-b^2$, $y=2ab$, $z=a^2+b^2$ where $a>b>0$, $(a,b)=1$ and one of a,b is odd & the other is even

Imp

Proof :-

First we prove that, $x = a^2-b^2$, $y = 2ab$, $z = a^2+b^2$ is sol^n of $x^2+y^2=z^2$.

$$
\begin{aligned}
L.H.S. &= x^2+y^2 \\
&= (a^2-b^2)^2 + (2ab)^2 \\
&= a^4 - 2a^2b^2 + b^4 + 4a^2b^2 \\
&= (a^2+b^2)^2 \\
&= z^2
\end{aligned}
$$

Now, we prove that,
every sol^n of $x^2+y^2=z^2$ is of the form
$x=a^2-b^2$, $y=2ab$, $z=a^2+b^2$.

Let x, y, z be any sol^n of given eq^n
$x^2+y^2=z^2$ with $x, y, z>0$, $(x,y)=1$ &
y is even

Now, $x^2+y^2=z^2$

$$\Rightarrow y^2=z^2-x^2.$$

$$\Rightarrow \left(\frac{y}{2}\right)^2=\left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right)$$

($\because$ y is even $\Rightarrow \frac{y}{2}$ is in

If $\left(\frac{z+x}{2}, \frac{z-x}{2}\right)=d$

then $d \,/\, \left(\frac{z+x}{2}\right)$, $d \,/\, \left(\frac{z-x}{2}\right)$.

(~~$\because (x,y)=1$ odd even~~ y eve $(x,y)=$ $\because x$ od
& $x^2+y^2=z^2$
odd even $\Rightarrow$ odd

$\Rightarrow d/z$ & d/x (by add & sub. $\frac{z+x}{2}$, $\frac{z-x}{2}$

$\Rightarrow d=1$ ($\because (x,y)=1$ & $x^2+y^2=z^2$
$(x^2, y^2)=1 \Rightarrow (x^2, x^2+y^2)=1$
$\Rightarrow (x^2, z^2)=1$
$\Rightarrow (x, z)=1$

Thus, $\left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right)=\left(\frac{y}{2}\right)^2$ & —(1)

$$\left(\frac{z+x}{2}, \frac{z-x}{2}\right)=1$$

$\therefore$ By above lemma, we say that,

$\exists$ +ve integers $a, b \ni \frac{z+x}{2} = a^2, \frac{z-x}{2} = b^2$

& $(a,b)=1$

$\Rightarrow z+x = 2a^2, \ z-x = 2b^2, \quad (a,b)=1.$

and $a>b>0$.

$\Rightarrow z = a^2+b^2, \quad x = a^2-b^2.$

also, by (1)

$$\left(\frac{y}{2}\right)^2 = a^2b^2$$

$$\Rightarrow y^2 = (2ab)^2 \Rightarrow y = 2ab.$$

Thus,

$x = a^2-b^2, \quad y = 2ab, \quad z = a^2+b^2.$

$(a,b)=1, \quad a>b>0.$

Since y is even,

x is odd $(\because (x,y)=1)$

$\therefore z^2 = x^2+y^2 \Rightarrow z$ is odd

$\Rightarrow z = a^2+b^2$ is odd

$\Rightarrow$ one of a & b is odd and the other is even.

Hence the thm. is proved

(44) Find all relatively prime solns of $x^2+y^2=z^2$ with $0<z<30$.

Soln:- From above thm, we say that, soln is,

$x = a^2-b^2, \quad y = 2ab, \quad z = a^2+b^2$

Now, $0 < a^2+b^2 < 30$ $(\because a > b > 0)$

$\Rightarrow a \leq 5$.

Now.

a	b	$x = a^2-b^2$	$y = 2ab$	$z = a^2+b^2$
2	1	3	4	5
3	2	5	12	13
4	1	15	8	17
4	3	7	24	25
5	2	21	20	29

Thus, $(3,4,5)$, $(5,12,13)$, $(15,8,17)$, $(7,24,25)$, $(21,20,29)$ are reqrd. relatively prime sol^n.

(95) P.T. the integer sol^n of $x^2+2y^2=z^2$, $(x,y)=1$ can be expressed as $x = \pm(a^2-2b^2)$, $y = 2ab$, $z = a^2+2b^2$.

Th-5

proof:-

Here given eq^n. is,

$x^2+2y^2=z^2$

$\Rightarrow 2y^2 = z^2-x^2$

$\Rightarrow 2y^2 = (z+x)(z-x)$ —— $(*)$

we know that, $(x,y)=1$, $(x,z)=1$

also x, z are odd.

$\therefore$ $z+x$ & $z-x$ are even.

If $(z+x, z-x) = d$ then $d/z+x$ & $d/z-x$.

$\Rightarrow d/2z$

$\Rightarrow d/2$ $(\because d$ is even & z is odd$)$

$\Rightarrow d=1$ or $d=2$

$\Rightarrow d=2 \quad (\because d$ is even$)$

Thus $(z+x, z-x)=2$.

$\therefore$ $z+x$ & $z-x$ both are not multiples of 4.

* case-I

If $z+x$ is not multiple of 4 then $\frac{z+x}{2}$ is odd &, also $z-x$ is even.

$\therefore \left(\frac{z+x}{2}, z-x\right)=1 \quad (\because (x,z)=1)$

Thus by (*) $y^2=\left(\frac{z+x}{2}\right)(z-x)$ &

$\left(\frac{z+x}{2}, z-x\right)=1$.

$\therefore$ By lemma we say that, $\exists$ +ve integers $a, b \ni \frac{z+x}{2}=a^2,\ z-x=(2b)^2$.

$\left(\begin{array}{l}\because z-x \text{ is even} \\ \therefore \text{we can write } (2b)^2\end{array}\right)$

$\Rightarrow z+x=2a^2$ — (1)

$z-x=4b^2$ — (2)

Addition of (1) & (2) gives,

$2z=2(a^2+2b^2) \Rightarrow z=a^2+2b^2$

Subtraction of (2) from (1) gives,

$2x=2(a^2-2b^2)$

By $(*)$ $y^2 = (a^2)(4b^2)$

$\Rightarrow y = 2ab$

Thus, $x = a^2 - 2b^2$, $y = 2ab$, $z = a^2 + 2b^2$ is one of the solⁿ of $x^2 + 2y^2 = z^2$.

* <u>Case-II</u>

If $z - x$ is not multiple of 4 then $\frac{z-x}{2}$ is odd & also $z + x$ is even

$$\therefore \left(z+x, \frac{z-x}{2}\right) = 1.$$

Thus by $(*)$

$$y^2 = (z+x)\left(\frac{z-x}{2}\right)$$

$$\& \left(z+x, \frac{z-x}{2}\right) = 1.$$

$\therefore$ By lemma,

$\exists$ +ve integers $a, b \ni z + x = (2b)^2$ & $\frac{z-x}{2} = a^2$.

$\Rightarrow z + x = 4b^2 \quad -(3) \qquad z - x = 2a^2 \quad -(4)$

$(3) + (4) \Rightarrow 2z = 4b^2 + 2a^2$

$\Rightarrow z = a^2 + 2b^2$.

again,

$(3) - (4) \Rightarrow 2x = 4b^2 - 2a^2$

$\Rightarrow x = -(a^2 - 2b^2)$.

By $(*)$, $y^2 = (4b^2)(a^2) \Rightarrow y = 2ab$.

Thus, $x = -(a^2 - 2b^2)$, $y = 2ab$, $z = a^2 + 2b^2$

Page No.: Date: / /

Hence,

$$x = \pm(a^2 - 2b^2),\ y = 2ab,\ y = a^2 + 2b^2$$

are reqrd solns.

(46) P.T. the integer soln. of the eqn. $x^{-2} + y^{-2} = z^{-2}$. $(x, y, z) = 1$ is given

Th 6. by $x = a^4 - b^4$, $y = 2ab(a^2 + b^2)$,

$z = 2ab(a^2 - b^2)$, where $a > b > 0$, $(a, b) = 1$

& a, b both can not be odd or even.

Proof:-

Here, $(x, y, z) = 1$

$\therefore (x^2, y^2, z^2) = 1$

Now,

$$x^{-2} + y^{-2} = z^{-2}$$

$$\Rightarrow (x^2)^{-1} + (y^2)^{-1} = (z^2)^{-1}$$

$\therefore$ It's soln. is of the form,

$x^2 = r(r+s)$, $y^2 = s(r+s)$, $z^2 = rs$. — (1)

where $r, s > 0$, $(r, s) = 1$

Now, $z^2 = rs$ & $(r, s) = 1$

$\therefore$ By lemma, $\exists$ +ve integer $r_1, s_1 \ni$

$r = r_1^2$, $s = s_1^2$. — (*)

and $(r_1, s_1) = 1$

also,

$x^2 = r(r+s)$, $(r, r+s) = 1$

$\therefore$ By lemma, we say that,

$\exists$ +ve integers r_1 & $t_1 \ni$

$r = r_1^2$, $r+s = t_1^2$, $(r_1, t_1) = 1$ — (2)

also, $y^2 = s(r+s)$ & $(s, r+s) = 1$

$\therefore$ By lemma, $\exists$ +ve integers s_1 & t_1 $\ni$ $s = s_1^2$, $r+s = t_1^2$. & $(s_1, t_1) = 1$

Thus, $r_1^2 + s_1^2 = t_1^2$, $(r_1, t_1) = 1$.
$r_1 > 0$, $t_1 > 0$.

$\therefore$ By Pythagoras thm,
we say that,
its sol^n is,
$r_1 = a^2 - b^2$, $s_1 = 2ab$, $t_1 = a^2 + b^2$ — (3)
where $a > b > 0$.
$(a, b) = 1$ & one of a & b is odd.

Now, by (1)

$x^2 = r(r+s) \Rightarrow x^2 = r_1^2 t_1^2$ (by (2))
$\Rightarrow x = r_1 t_1$
$\Rightarrow x = (a^2 - b^2)(a^2 + b^2)$ (by (3))
$\Rightarrow x = a^4 - b^4$.

Now,
$y^2 = s(r+s)$
$\Rightarrow y^2 = s_1^2 t_1^2$ (by (*) & (2))
$\Rightarrow y = s_1 t_1$
$\Rightarrow y = 2ab(a^2 + b^2)$ (by (3))

Now, $z^2 = rs = r_1^2 s_1^2$ (by (*))
$\Rightarrow z = r_1 s_1$
$\Rightarrow z = 2ab(a^2 - b^2)$ (by (3))

Hence, $x = a^4 - b^4$, $y = 2ab(a^2 + b^2)$
$z = 2ab(a^2 - b^2)$.

Page No.:
Date: / /

(47) P.T. a general integer solⁿ. of the eqⁿ $x^2+y^2+z^2=\omega^2$, $(x,y,z,\omega)=1$ is given by $x=a^2-b^2+c^2-d^2$, $y=2ab-2c$ ...
$z=2ad+2bc$, $\omega=a^2+b^2+c^2+d^2$.

R-7

Solⁿ :-

Assume, that, y & z both are even & x & ω both are odd.

Let $\left(\frac{y}{2},\frac{z}{2}\right)=r$ & $(x,\omega)=s$ then

$r/\frac{y}{2}$, $r/\frac{z}{2}$ & s/x, s/ω.

$\Rightarrow y=2ry_1$, $z=2z_1r$ & $(y_1,z_1)=1$

& $\Rightarrow x=x_1s$, $\omega=\omega_1s$, $(x_1,\omega_1)=1$
where x_1 & ω_1 are odd

Now, $x^2+y^2+z^2=\omega^2$

$\Rightarrow y^2+z^2=\omega^2-x^2$

$\Rightarrow y^2+z^2=(\omega-x)(\omega+x)$

$\Rightarrow 4r^2(y_1^2+z_1^2)=s^2(\omega_1+x_1)(\omega_1-x_1)$

$(\because$ by $(*))$

$\Rightarrow y_1^2+z_1^2=\frac{s^2}{r^2}\left[\frac{\omega_1+x_1}{2}\right]\left[\frac{\omega_1-x_1}{2}\right].$

Let $r=r_1r_2$ & $(r_1,r_2)=1$.

$\therefore y_1^2+z_1^2=s^2\left[\frac{\omega_1+x_1}{2r_1^2}\right]\left[\frac{\omega_1-x_1}{2r_2^2}\right]$ — (1)

We know that,

the odd prime factors of $y_1^2+z_1^2$ are of the form $4k+1$ and also we know that, $4k+1$ can be expressed

Date: 17-7

as the sum of two square nos.

$\therefore$ By (1), we can write,

$$\frac{w_1 + x_1}{2r_1^2} = 4k_1 + 1 = a_1'^2 + c_1'^2 \quad \text{--- (2)}$$

$$\frac{w_1 - x_1}{2r_2^2} = 4k_2 + 1 = b_1'^2 + d_1'^2 \longrightarrow (3)$$

putting these values in (1), we get

$$y_1^2 + z_1^2 = s^2(a_1'^2 + c_1'^2)(b_1'^2 + d_1'^2)$$
$$y_1^2 + z_1^2 = (sa_1'^2 + sc_1'^2)(sb_1'^2 + sd_1'^2)$$

$$\Rightarrow y_1^2 + z_1^2 = (a_1^2 + c_1^2)(b_1^2 + d_1^2) \quad \text{--- (4)}$$

where $b_1^2 = sb_1'^2$, $d_1^2 = sd_1'^2$,
$a_1^2 = sa_1'^2$, $c_1^2 = sc_1'^2$.

Suppose,

$$y_1^2 + z_1^2 = (y_1 + \sqrt{-1}\, z_1)(y_1 - \sqrt{-1}\, z_1)$$

Let

$$\left.\begin{aligned} (y_1 + \sqrt{-1}\, z_1) &= (a_1 + \sqrt{-1}\, c_1)(b_1 + \sqrt{-1}\, d_1) \\ (y_1 - \sqrt{-1}\, z_1) &= (a_1 - \sqrt{-1}\, c_1)(b_1 - \sqrt{-1}\, d_1) \end{aligned}\right\} \text{--- (5)}$$

By solving eq^n. (5), we get

$$\left.\begin{aligned} y_1 &= a_1 b_1 - c_1 d_1 \\ z_1 &= a_1 d_1 + b_1 c_1 \end{aligned}\right\} \text{--- (6)}$$

By solving eq^{ns}. (2) & (3), we get

$$2w_1 = 2r_1^2(a_1'^2 + c_1'^2) + 2r_2^2(b_1'^2 + d_1'^2).$$

Page No.:
Date: / /

$$\Rightarrow w_1 = r_1^2\left(\frac{a_1^2}{5}+\frac{c_1^2}{5}\right)+r_2^2\left(\frac{b_1^2}{5}+\frac{d_1^2}{5}\right)$$

$(\because$ by

$$= \frac{1}{5}\left[r_1^2(a_1^2+c_1^2)+r_2^2(b_1^2+d_1^2)\right]$$

and

$$2x_1 = 2r_1^2(a_1'^2+c_1'^2) - 2r_2^2(b_1'^2+d_1'^2)$$

$$\Rightarrow x_1 = \frac{1}{5}\left(r_1^2(a_1^2+c_1^2)-r_2^2(b_1^2+d_1^2)\right) \quad (\because \text{by}$$

On putting all these values of x_1, y_1, z_1 & w_1 in (*), we get,

$$x = 5x_1 = r_1^2(a_1^2+c_1^2) - r_2^2(b_1^2+d_1^2)$$

$\Rightarrow x = a^2+c^2-b^2-d^2$, where,

$a = r_1a_1$, $b = r_2b_1$

$c = r_1c_1$, $d = r_2d_1$

$$y = 2ry_1 = 2r_1r_2(a_1b_1 - c_1d_1)$$

$\Rightarrow y = 2ab - 2cd$, where,

$a = a_1r_1$

$b = b_1r_2$

$c = c_1r_1$

$d = d_1r_2$

$z = 2rz_1 \Rightarrow z = 2r_1r_2(a_1d_1+c_1b_1)$

$\Rightarrow z = 2ad+2bc.$

$w = w_1 5 \Rightarrow r_1^2(a_1^2+c_1^2)+r_2^2(b_1^2+d_1^2) = a^2+b^2+c^2+d^2.$

Hence, general integer solⁿ of the given eqⁿ is* given by,

$x = a^2-b^2+c^2-d^2$, $y = 2ab+2cd$,

(98) If x, y, z is solⁿ of $x^2+y^2=z^2$, $(x,y,z)=1$ then one of x, y there is a multiple of 3 and a multiple of 4. Also p.t. one of x, y, z is multiple of 5.

Th-8

i.e. prove that, ~~xyz~~ xyz is a multiple of 60.

proof:

Suppose that both x, y are not multiples of 3.

Since an integer not a multiple of 3 is of the form $3n \pm 1$, with square,

$(3n\pm1)^2 = 9n^2 \pm 6n + 1$

$= 3(3n^2 \pm 2n) + 1$

$= 3k + 1$

Now, $z^2 = x^2 + y^2 = (3k_1+1) + (3k_2+1)$

$= 3(k_1+k_2) + 2$

$= 3k_3 + 2$

which is not a square number.

It is impossible since z^2 is a square number.

Thus one of x, y is a multiple of 3

Again suppose x, y are both not multiples of 4.

An integer not a multiple of 4 is of the form $4n\pm1$, $4n+2$.

Now,

$$(4n+2)^2 = \cancel{16}+\cancel{16}\ 16n^2+16n+4$$
$$= 16(n^2+n)+4$$
$$= 8k'+4$$

If x, y are both of the form $4n\pm1$ then

$$z^2 = x^2+y^2 = (8k_1+1)+(8k_2+1)$$
$$= 8(k_1+k_2)+2$$
$$= 8k_3+2$$

which is not a sqare no.

If one of x, y is of the form $4n\pm1$ and the other is of the form $4n+2$ then,

$$z^2 = x^2+y^2$$
$$= (8k_1+1)+(8k_4+4)$$
$$= 8(k_1+k_4)+5$$
$$= 8k_5+5$$

$$z^2 = 8k_5+4 + 8k_6+4 = 8(k_5+k_6+1) =$$

which is not a square no

It is impossible since z^2 is a sqare no.
Hence, one of x, y must be a multiple of 4.

Finally if none of x, y, z is a multiple of 5 then they must have the forms $5n\pm1$, $5n\pm2$.

Now,

$$(5n\pm1)^2 = 25n^2\pm10n+1$$
$$= 5(5n^2\pm2n)+1$$
$$= 5k+1$$

&

$$(5n\pm2)^2 = 25n^2\pm20n+4 \qquad 5k'+4$$

$\therefore z^2 = x^2+y^2$

$= (5k_1+1)^2 + (5k_2+1)$

$= 5k_3+2$

Which is not a square no.

also

$z^2 = x^2+y^2$

$\Rightarrow z^2 = (5k_1'-1) + (5k_2'-1)$

$= 5(k_1'+k_2') - 2$

$= 5k_4 - 2$

Which is not square no.

and

$z^2 = x^2+y^2$

$= (5k_1+1) + (5k_2'-1)$

$= 5(k_1+k_2')$

$= 5k_5$

which is multiple of 5

These contradict the assumption.

Hence one of x, y, z is multiple of 5

Hence, xyz is multiple of 60.

(19) Find integer solⁿ of $x^2+xy-y^2-3x+4y-6=0$

solⁿ:

Given eqⁿ is,

$x^2+xy-y^2-3x+4y-6=0$ —— (1)

$\Rightarrow x^2+x(y-3)+(-y^2+4y-6)=0$

$$\Rightarrow x = \frac{(3-y) \pm \sqrt{(y-3)^2 - 4(-y^2+4y-6)}}{2}$$

~~$x = (3-y) \pm \sqrt{(y-3)^2 - 4(-y^2+4y-6)}$~~

Page No.:
Date: / /

$$\Rightarrow x = \frac{(3-y) \pm \sqrt{y^2-6y+9+4y^2-16y+24}}{2}.$$

$$\Rightarrow x = \frac{(3-y) \pm \sqrt{5y^2-22y+33}}{2}$$

Since, x is an integer,

$5y^2-22y+33$ must be a square number

It is easy that,
when $y=1 \Rightarrow 5y^2-22y+33 = 16 = 4^2$.

$y=2 \Rightarrow 5y^2-22y+33$
$= 5(4)-22(2)+33$
$= 20-44+33$
$= 53-44 = 9 = 3^2$.

$y=4 \Rightarrow 5(16)-22(4)+33$
$= 80-88+33$
$= 113-88 = 25 = 5^2$.

$y=6 \Rightarrow 5(36)-22(6)+33$
$= 180-132+33$
$= 213-132 = 81 = 9^2$

Now, by eq^n. (1)

for $y=1$, $x^2+x-1-3x+4-6=0$
$\Rightarrow x^2-2x-3=0$
$\Rightarrow (x-3)(x+1)=0$
$\Rightarrow x=3,-1$
$\therefore (3,1), (-1,1)$.

for $y=2$,

$$x^2+2x-4-3x+8-6=0$$

$$\Rightarrow x^2-x-2=0$$

$$\Rightarrow (x-2)(x+1)$$

$$\Rightarrow x=2,-1$$

$$\therefore (2,2),(-1,2)$$

for $y=4$,

$$x^2+4x-16-3x+16-6=0$$

$$\Rightarrow x^2+x-6=0$$

$$\Rightarrow (x+3)(x-2)=0$$

$$\Rightarrow x=-3,2.$$

$$\therefore (-3,4),(2,4)$$

for $y=6$,

$$x^2+6x-36-3x+24-6=0$$

$$\Rightarrow x^2+3x-18=0$$

$$\Rightarrow (x+6)(x-3)=0$$

$$\Rightarrow x=-6,3$$

$$\therefore (-6,6),(3,6).$$

Hence,
$(3,1)$ & $(-1,1)$, $(2,2)$ & $(-1,2)$,
$(2,4)$ & $(-3,4)$, $(3,6)$ & $(-6,6)$
are req^rd integer sol^ns.

(50) P.T. the Diophantine eq^n.
$x^4+y^4=z^2$. has no sol^n. with non zero
Th-q
+ve integers x, y & z.

OR

P.T. $x^4+y^4=z^2$ has no non-zero +ve integer

Page No.:
Date: / /

proof:- Suppose, $x^4+y^4=z^2$ has +ve integer solⁿ.
we may suppose that,
$(x,y)=1$ & y is even.
and z is smallest solⁿ of z.

Now, given eqⁿ is,
$(x^2)^2+(y^2)^2=z^2$.
∴ By Pythagoras thm,

$x^2=a^2-b^2$, $y^2=2ab$, $z=a^2+b^2$.
where $a>b>0$, $(a,b)=1$ &
one of a & b is odd
and other is even
If a is even and b is odd then clearly
$a^2-b^2+1=4k$, for some $k\in\mathbb{Z}$

∴ $4-25+1=4k$
$\Rightarrow -20=4k$
~~$9-36+1=4k$~~
$\Rightarrow 36-9+1$
$=28=4k$

$\Rightarrow 4/(a^2-b^2+1)$

$\Rightarrow a^2-b^2\equiv(-1)\pmod 4$
$\Rightarrow x^2\equiv(-1)\pmod 4$ —(1)

Since, x is odd $x^2-1=4k$.
$\Rightarrow 4/(x^2-1)$

$\Rightarrow x^2\equiv 1\pmod 4$ —(2)

By (1) & (2), we say that,

Date: 18/5/10

$1 \equiv (-1) \pmod 4$

$\Rightarrow 4/2$ ✗

$\therefore$ a must be odd & b must be even

Now,

$x^2 = a^2 - b^2$

$\Rightarrow x^2 + b^2 = a^2$

$\therefore$ By Pythagoras thm, we get

$x = p^2 - q^2$, $b = 2pq$, $a = p^2 + q^2$.

where $p > q > 0$, $(p, q) = 1$ &

one of p, q is odd and the other is even.

also $y^2 = 2ab$.

$\Rightarrow y^2 = 2(p^2+q^2)2pq$

$\Rightarrow y^2 = 4pq(p^2+q^2)$, where $(p, q, p^2+q^2) = 1$.

then by lemma, we say that

$\exists$ +ve integers r, s, t $\ni$

$p = r^2$, $q = s^2$, $p^2+q^2 = t^2$.

$\Rightarrow r^4 + s^4 = t^2$

Thus, r, s & t are solns of $x^4 + y^4 = z^2$.

but $z = a^2 + b^2 > a = p^2 + q^2 = t^2 > t$.

Thus $z > t$. ✗

($\because z$ is the smallest soln. of z in all solns.)

Hence $x^4 + y^4 = z^2$ has no soln

(5) P.T. following eq^n has no +ve integer sol^n. (i) $x^4+y^4=z^4$.

Th-1) (ii) $x^{-4}+y^{-4}=z^{-4}$

(iii) $x^4-4y^4=z^2$.

Proof:

(i) Suppose, $x^4+y^4=z^4$ has +ve integer sol^n. then

$x^4+y^4=(z^2)^2$ has also +ve integer sol^n. ✗ ($\because$ Diophantine eq^n, $x^4+y^4=Z^2$ has no sol^n, where $z^2=Z$)

Hence, $x^4+y^4=z^4$ has no sol^n.

(ii) Given eq^n is,

$$x^{-4}+y^{-4}=z^{-4}$$

$$\Leftrightarrow (xyz)^4[x^{-4}+y^{-4}] = [(xyz)^4 z^{-4}]$$

$$\Leftrightarrow (yz)^4+(xz)^4=(xy)^4.$$

which has no +ve integer sol^n (by thm)

$\therefore x^{-4}+y^{-4}=z^{-4}$ has no +ve integer sol^n.

(iii) $x^4-4y^4=z^2$.

$$\Leftrightarrow (x^4-4y^4)^2=z^4$$

$$\Leftrightarrow x^8-8x^4y^4+16y^8=z^4.$$

$$\Leftrightarrow x^8+8x^4y^4+16y^8=z^4+16x^4y^4$$

$$\Leftrightarrow (x^4+4y^4)^2=(z^4+(2xy)^4)$$

$$\Leftrightarrow z^4+(2xy)^4=(x^4+4y^4)^2$$

which has no +ve integer sol^n.

CONGRUENCES

* Congruent modulo n :-

Let n be a fixed +ve integer. Two integers a & b are said to be congruent modulo n if $n/a-b$.

i.e. if $a-b=kn$, for some $k \in Z$

In symbol $a \equiv b \pmod n$ means " a and b are congruent modulo n or "a is congruent to b". modulo n

(1) Prove that, $a \equiv b \pmod n$ iff a & b have the same non negative remainder when divided by n

proof :-

If $a \equiv b \pmod n$ then by defn.

$n/a-b \Rightarrow a-b=kn$

$\Rightarrow a=kn+b$, for some $k \in$ —(*)

If r is the remainder when b divided by n.

$\therefore b=qn+r$, where $0 \le r < n$

Now by (*)

$a=kn+qn+r$, where $0 \le r < n$

$\Rightarrow a=(k+q)n+r$, " "

$\Rightarrow a=q_1n+r$, " "

Thus a & b have same remainder

Converse part :-

If a & b have same remainer when divided by n then we have

Now, $a = q_1 n + r$

$b = q_2 n + r$

$a - b = (q_1 - q_2)n$

$\Rightarrow n / a-b$

$\Rightarrow a \equiv b \pmod n$

* Equivalent relation:-

The relation '$\sim$' is said to be equivalence relation if it satisfies the following conditions

(1) Reflexivity :-

$a \sim a, \forall a$

(2) Symmetry:-

$a \sim b \Rightarrow b \sim a, \forall a, b$.

(3) Transitivity:-

$a \sim b \ \& \ b \sim c \Rightarrow a \sim c, \forall a, b, c$.

(2) P.T congruent is equivalent relat

proof:-

(1) Reflexivity:-

clearly. $n/0 \Rightarrow n/a-a$

$\Rightarrow a \equiv a \pmod n$.

(2) symmetry:-

$a \equiv b \pmod n$

$\Rightarrow n / a-b$

$\Rightarrow n / -(a-b)$

(3) Transitivity :-

$$a \equiv b \pmod{n} \;\&\; b \equiv c \pmod{n}$$

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

$$\Rightarrow n / (a-b)+(b-c)$$

$$\Rightarrow n / a-c$$

$$\Rightarrow a \equiv c \pmod{n}.$$

Thus congruent is an equivalence relation.

(3) If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$ then prove the following results:

(1) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$

proof:-

we have $n / a_1 - b_1$ & $n / a_2 - b_2$

$$\Rightarrow n / (a_1-b_1)+(a_2-b_2)$$

$$\Rightarrow n / (a_1+a_2)-(b_1+b_2)$$

$$\Rightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod{n}.$$

(2) $a_1 - a_2 \equiv b_1 - b_2 \pmod{n}$

(iii) $ca_1 \equiv cb_1 \pmod{n}$, $c \in \mathbb{Z}$

proof:-

$$n / a_1 - b_1 \Rightarrow n / c(a_1 - b_1), \; c \in \mathbb{Z}$$

$$\Rightarrow n / ca_1 - cb_1$$

$$\Rightarrow ca_1 \equiv cb_1 \pmod{n}.$$

(iv) $a_1 + c \equiv b_1 + c \pmod{n}$, $c \in \mathbb{Z}$

proof:-

$$n / a_1 - b_1 \Rightarrow n / (a_1 + c) - (b_1 + c)$$

$$\Rightarrow (a_1 + c) \equiv (b_1 + c) \pmod{n}$$

(v) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

proof:-

$$a_1 \equiv b_1 \pmod{n}$$

$$\Rightarrow a_1 a_2 \equiv b_1 a_2 \pmod{n} \quad -(i) \quad (\text{by (iii)})$$

also $a_2 \equiv b_2 \pmod{n}$

$$\Rightarrow b_1 a_2 \equiv b_1 b_2 \pmod{n} \quad -(ii)$$

By (i) & (ii)

$$a_1 a_2 \equiv b_1 b_2 \pmod{n}.$$

(vi) $a_1^m \equiv b_1^m \pmod{n}$, $\forall m \in N$.

proof:-

$$a_1 \equiv b_1 \pmod{n} \;\&\; a_1 \equiv b_1 \pmod{n}$$

$$\Rightarrow a_1 a_1 \equiv b_1 b_1 \pmod{n}$$

$$\Rightarrow a_1^2 \equiv b_1^2 \pmod{n}$$

$$\Rightarrow a_1^2 \cdot a_1 \equiv b_1^2 \cdot b_1 \pmod{n}$$

Date: 1~, 1

continuing this process finally we ge

$a_1^m \equiv b_1^m \pmod n$, $\forall m \in N$.

(4) p.T. $a \equiv b \pmod n$
$\Rightarrow a^m \equiv b^m \pmod n$, $\forall m \in N$.
by using mathematical induction method

Sol:

for $m=1$ we have
$a \equiv b \pmod n$
$\therefore$ result is proved for $m=1$

suppose result is true for m
i.e $a^m \equiv b^m \pmod n$
Then we have to p.t. result is true for $m+1$
i.e. $a^{m+1} \equiv b^{m+1} \pmod n$

Now, $a^m \equiv b^m \pmod n$ &
$a \equiv b \pmod n$
$\therefore a^m \cdot a \equiv b^m \cdot b \pmod n$
$\therefore a^{m+1} \equiv b^{m+1} \pmod n$
$\therefore$ By mathematical induction,
we say that,
$a^m \equiv b^m \pmod n$.

(5) If $ca \equiv cb \pmod n$ & $(c,n)=1$. then p.t. $a \equiv b \pmod n$.

Sol: Here
$ca \equiv cb \pmod n$

Date: / /

$\Rightarrow a \equiv b \pmod{n}$.

(6) If $a \equiv b \pmod{n}$ then p.t $ca \equiv cb \pmod{n}$ for $c \in \mathbb{Z}$.

Does the converse hold? verify.
If not then under which condition converse true

Sol: prove prop. (iii)

converse need not be true because

$3 / 9-6 \Rightarrow 9 \equiv 6 \pmod{3}$

$\Rightarrow 3 \cdot 3 \equiv 3 \cdot 2 \pmod{3}$

but $3 \not\equiv 2 \pmod{3}$

$(\because 3 \nmid 3-2)$

If $(c, n) = 1$ then

$ca \equiv cb \pmod{n}$

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

prove it.

(7) P.T. any integer x satisfies atleast one of the following congruences

$x \equiv 0 \pmod{2}$, $x \equiv 0 \pmod{3}$,
$x \equiv 1 \pmod{4}$, $x \equiv 5 \pmod{6}$,
$x \equiv 7 \pmod{12}$.

Sol^n:

Let x be any integer
If x is even then $2 / x \Rightarrow 2 / x-0$

Date: 7 / 8

If x is odd integer. Then it must be of the form
$12k+1,\ 12k+3,\ 12k+5,\ 12k+7,\ 12k+9\ \&\ 12k+11.$

If $x = 12k+3$ or $x = 12k+9$ then
$3 / x$
$\Rightarrow x \equiv 0 \pmod 3$.

If $x = 12k+1$ or $12k+5$
then $4 / x-1$
$\Rightarrow x \equiv 1 \pmod 4$.

If $x = 12k+11$ then
$6 / x-5$
$\Rightarrow x \equiv 5 \pmod 6$

If $x = 12k+7$ then
$12 / x-7$
$\Rightarrow x \equiv 7 \pmod{12}$

(8) P.T. $x^2+y^2=z^2$ has no sol^n. ~~consti~~ consisting of only primes.

OR

P.T. $x^2+y^2=z^2$ has no prime sol^n.

OR

P.T. Pythagoras eq^n. has no prime sol^n.

Date : / /

Sol^n: Let $x^2+y^2=z^2$

suppose $x=a$, $y=b$, $z=c$

(where a, b, c all are primes)

are prime sol^{ns} of $x^2+y^2=z^2$.

If a is even prime i.e. $a=2$ then

$a^2+b^2=c^2$

$\Rightarrow c^2-b^2=4$

$\Rightarrow (c-b)(c+b)=4=1\cdot 4$

$\Rightarrow c-b=1$ & $c+b=4$

$\Rightarrow 2c=5 \Rightarrow c=5/2$ $\times$

($\because c$ is prime)

If a & b both are odd prime then clearly

$4/a^2-1$ & $4/b^2-1$

$\Rightarrow 4/(a^2+b^2)-2$

$\Rightarrow 4/c^2-2$ — (*)

Since a & b are odd prime, $a^2+b^2=c^2$ is even no.

$\therefore 2/c^2$

$\Rightarrow 2/c$.

$\Rightarrow c=2$ ($\because c$ prime)

by (*)

$4/2^2-2$

$\Rightarrow 4/2$ $\times$

Hence our supposition is wrong

Date: 1/ N /08

(9) Prove that, the necessary and sufficient condition for a +ve integer n can be divisible by 3 is that the sum of its digits is divisible by 3.

proof:

Let n be any +ve integer.

we know that, every integer n can be written in the form,

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_k 10^k.$$

i.e. $n = a_k a_{k-1} \cdots a_1 a_0$.

Clearly, $3 / 10-1$

$$\Rightarrow 10 \equiv 1 \pmod 3$$
$$\Rightarrow 10^2 \equiv 1 \pmod 3$$
$$\Rightarrow 10^3 \equiv 1 \pmod 3$$
$$\vdots$$
$$\Rightarrow 10^k \equiv 1 \pmod 3$$

Now,

$3 / a_0 - a_0$

$\Rightarrow a_0 \equiv a_0 \pmod 3$

also, $\Leftrightarrow a_1 \cdot 10 \equiv a_1 \pmod 3$

$\Leftrightarrow a_2 \cdot 10^2 \equiv a_2 \pmod 3$

$\vdots$

$a_k \cdot 10^k \equiv a_k \pmod 3$

By adding we get.

$$(a_0 + a_1 \cdot 10 + \dots + a_k 10^k) \equiv (a_0 + a_1 + a_2 + \dots + a_k) \pmod 3$$

$$\Rightarrow n \equiv (a_0 + a_1 + \dots + a_k) \pmod 3 \quad -(*)$$

Now,

$3/n \Leftrightarrow n \equiv 0 \pmod 3$

$\Leftrightarrow (a_0 + a_1 + \dots + a_k) \equiv 0 \pmod 3$

Date : / /

* Remark :- Same condition can be proved for 9.

(10) Find a necessary & sufficient condition that a +ve integer (which is) is divisible by 11 or

Sol^n:- Let n be any +ve integer
we can write,
$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_k 10^k .$$
we know that,
$$11 / 10-(-1)$$
i.e. $10 \equiv (-1) \pmod{11}$
$$\Rightarrow 10^2 \equiv 1 \pmod{11}$$
$$\Rightarrow 10^3 \equiv (-1) \pmod{11}$$
$$\vdots$$
$$\Rightarrow 10^k \equiv (-1)^k \pmod{11}$$
Now,
$$11 / a_0 - a_0$$
$$\Rightarrow a_0 \equiv a_0 \pmod{11}$$
also,
$$a_1 \cdot 10 \equiv (-a_1) \pmod{11}$$
$$a_2\, 10^2 \equiv a_2 (\cancel{\pm a_2} -1)^2 \pmod{11}$$
$$\vdots$$
$$a_k\, 10^k \equiv (-1)^k a_k \pmod{11}$$
By adding, we get
$$(a_0 + a_1 10 + \dots\ a_k 10^k) \equiv (a_0 - a_1 + a_2 - \dots \pm a_k) \pmod{11}$$
$$\Rightarrow n \equiv (a_0 - a_1 + a_2 - \dots \pm a_k) \pmod{11} \quad -(*)$$
#>

Date: 10

Now,

$11/n \Leftrightarrow n \equiv 0 \pmod{11}$

$\Leftrightarrow (a_0 - a_1 + a_2 - \cdots \pm a_k) \equiv 0 \pmod{11}$ (by *)

$\Leftrightarrow 11 / (a_0 - a_1 + \cdots \pm a_k)$

which is req^rd necessary & sufficient condition

P.T.

(11) Every no. containing more than two digits can be divided by 4 iff the no. formed by its last two digits can be divided by 4.

proof:-

let $n = a_k a_{k-1} \cdots a_2 a_1 a_0$ be any +ve integer containing more than two digits we can write

$n = a_1 a_0 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + \cdots + a_k 10^k$

we know that,

$4/10^2$

$\Rightarrow 10^2 \equiv 0 \pmod 4$

$\Rightarrow 10^3 \equiv 0 \pmod 4$

$\vdots$

$\Rightarrow 10^k \equiv 0 \pmod 4$

also,

$a_1 a_0 \equiv a_1 a_0 \pmod 4$

$a_2 \cdot 10^2 \equiv 0 \pmod 4$

$a_3 \cdot 10^3 \equiv 0 \pmod 4$

$\vdots$

$a_k \cdot 10^k \equiv 0 \pmod 4$

By adding we get

$a_1 a_0 + a_2 \cdot 10^2 + \cdots + a_k 10^k \equiv$

$\Rightarrow n \equiv a_1 a_0 \pmod 4$ — (*)

Now,

$4/n \Leftrightarrow n \equiv 0 \pmod 4$

$\Leftrightarrow a_1 a_0 \equiv 0 \pmod 4$

$\Leftrightarrow 4/a_1 a_0$.

(12) Find a necessary & sufficient conditi[on] that a +ve integer can be divided by 7.

Sol^n:- Let n be any +ve integer then we can write

$n = a_0 + a_1 * 1000 + a_2 \cdot 1000^2 + \cdots + a_k (10[00]^k)$

we know that, $0 \le a_i \le 999$

$7/1001$

i.e $7/1000-(-1)$

$\left.\begin{array}{l} \Rightarrow 1000 \equiv (-1) \pmod 7 \\ \Rightarrow 1000^2 \equiv (1) \pmod 7 \\ \Rightarrow 1000^3 \equiv (-1) \pmod 7 \\ \quad \vdots \\ (1000)^k \equiv (-1)^k \pmod 7 \end{array}\right\}$ — (*)

$\therefore n = a_0 + a_1 \cdot 1000 + a_2 \cdot 1000^2 + \cdots + a_k (1000)^k$

$\Rightarrow n \equiv (a_0 - a_1 + a_2 - \cdots \pm a_k) \pmod 7$ — (**)

(by (*))

Now $7/n$

$\Leftrightarrow n \equiv 0 \pmod 7$

$\Leftrightarrow (a_0 - a_1 + a_2 - \cdots \pm a_k) \equiv 0 \pmod 7$

$\Leftrightarrow 7/(a_0 - a_1 + a_2 \ldots$

Date: 1/4

Remark: Same condition can be proved for 13.

(13) Check which of the following integer are divided by 3, 9, 4, 7, 11, 13.

(i) 7654321. (1) 765432 = q

Sol^n:-

$7+6+5+4+3+2 = 27$ | Here, $7+6+5+4+3+2+1 = 28$

(1) $3/27$ | and $3 \nmid 28$.

$\therefore 3/q$ | $\therefore 3 \nmid 7654321$.

(2) $9/q$ | similarly $9 \nmid 7654321$

(3) last two digit 32 | also, no. formed by last two digit

$4/32$ | is 21 & $4 \nmid 21$

$\therefore 4/q$ | $\therefore 4 \nmid 7654321$.

(4) 765432

$= 432 + 765 \times 1000$ | we can write,

$432 - 765$ | $\underline{7654321} = \underset{a_0}{321} + \underset{a_1}{654} \times 1000 + \underset{a_2}{7} \times 1000^2$.

$= -333$ | also, $321 - 654 + 7 = -326$

$7 \nmid -333$ | but $7 \nmid (-326)$

$13 \nmid -333$ | $\therefore 7 \nmid 7654321$

$\therefore 7 \nmid q$ & $13 \nmid q$ | also $13 \nmid 7654321$

(5) $2-3+4-5+6-7$ | also, $1-2+3-4+5-6+7$

$= -3$ | $= 4$

& $11 \nmid -3$ | and $11 \nmid 4$

$\therefore 11 \nmid q$. | $\therefore 11 \nmid 7654321$

(ii) 15643278

Sol:-

$1+5+6+4+3+2+7+8 = 36$

and $3 \mid 3$ $3 \mid 36$

$\therefore 3 \mid 15643278$ & $9 \mid 15643278$

$4 \nmid 78$ $\therefore 4 \nmid 15643278$

Here

$278 - 643 + 15 = -350$

also $7 \mid (-350)$

$\therefore 7 \mid 15643278$

but $13 \nmid (-350)$

$\therefore 13 \nmid 15643278$

also $8-7+2-3+4-6+5-1$

$= 2$

but $11 \nmid 2$ $\therefore 11 \nmid 15643278$

U-4 (start) — UNIT-4

* Complete residue system modulo m (CRS):-

Let m be a fix +ve integer then the complete residue system modulo m is the set of m-integers such that every integer is congruent to exactly one integer of the set $\{0, 1, 2, \ldots, m-1\}$ with modulo m

Date: / /

* Remark :-

(1) $\{26, 37, 48, 59, 10\}$ is CRS mod 5.
$\{6, 7, 8, 9, 20\}$ is CRS mod 5.
$\{16, 17, 18, 19, 40\}$ is CRS mod 5.

(2) All integers which are congruent to 0 with modulo m, forms a class.
All int^s which are congruent to 1 forms another class and so on.
clearly any int must be in one & only one class and any two int^s of the same class are congruent to each other. also any two int^s from different classes are not congruent (incongruent) to each other.

(14) P.T. A set of k int^s $a_1, a_2, \ldots a_k$ is a complete residue system modulo m iff (i) $k=m$ & (ii) $a_i \not\equiv a_j \pmod m$, $\forall i \neq j$.

proof:-

If $\{a_1, a_2, \ldots, a_k\}$ is CRS modulo m then by def^n. it is set of m integers such that every integer is congruent to the exactly one element of the set $\{0, 1, 2, \ldots, m-1\}$ with modulo m
$\therefore k=m$
and every element a_i are in different classes
i.e. $a_i \not\equiv a_j \pmod m$, $\forall i \neq j$

Date : / /

* converse part :-

If conditions (i) & (ii) are satisfied then we say that $a_1, a_2, \dots, a_m$ is the set of m integer such that $a_i \not\equiv a_j \pmod m$, $\forall i \neq j$.
i.e all a_i are in different classe
i.e each a_i congruent to exactly one integer of the set $\{0, 1, 2, \dots, m-1\}$ with modulo m.
Hence by defⁿ we say that $a_1, a_2, \dots, a_k$ forms a CRS of mod m.

(15) True or false:

(i) $\{6, 8, 10, 12, 14, 16, 17\}$ is CRS modulo 8.

It is false because it contains 7 elements only.

(ii) $\{6, 8, 10, 12, 14, 16, 17\}$ is CRS modulo 7
false
because $7 \mid 17-10$ i.e $17 \equiv 10 \pmod 7$

(iii) $\{6, 8, 10, 12, 14, 16, 18\}$ is CRS modulo 7
True.
because $k = 7$ &

$6 \equiv 6 \pmod 7$ $\quad 14 \equiv 0 \pmod 7$
$8 \equiv 1 \pmod 7$ $\quad 16 \equiv 2 \pmod 7$
$10 \equiv 3 \pmod 7$ $\quad 18 \equiv 4 \pmod 7$
$12 \equiv 5 \pmod 7$

one element of set $\{0,1,2,3,4,5,6\}$ modulo 7.

(16) If $a_1, a_2, \dots, a_m$ is CRS modulo m and $(a, m) = 1$ then p.t.

$aa_1+b,\ aa_2+b, \dots, aa_m+b$ forms a CRS mod m, where b is any in

proof:- (i) P.T. $a_1+b, \dots, a_m+b$ is CRS (ii) $aa_1, \dots, aa_m$ is CRS mod m if $(a$

It is sufficient to p.t.

$(aa_i+b) \not\equiv (aa_j+b) \pmod m,\ \forall i \neq j$

suppose,

$(aa_i+b) \equiv (aa_j+b) \pmod m$, for some $i \neq j$

$\Rightarrow aa_i \equiv aa_j \pmod m$

$\Rightarrow a_i \equiv a_j \pmod m$ $(\because (a, m) = 1$

$\times$

because $a_1, a_2, \dots, a_m$ is CRS modulo m

$\therefore (aa_i+b) \not\equiv (aa_j+b) \pmod m$

(17) If $m \equiv 0 \pmod 2$; $a_1, a_2, \dots, a_m$ & $b_1, b_2, \dots, b_m$ are CRS modulo m then p.t. $a_1+b_1, a_2+b_2, \dots, a_m+b_m$ is not CRS modulo m

proof:-

Here $a_1, a_2, \dots a_m$ is CRS mod m then by def^n we say that

$\sum^{m} a_i \equiv \sum^{m} i \pmod m$

$$\Rightarrow \sum_{i=1}^{m} a_i \equiv \frac{m(m+1)}{2} \pmod m$$

$$\Rightarrow \sum_{i=1}^{m} a_i \equiv \frac{m}{2} \pmod m \quad (\because m+1 \equiv 1 \pmod m) \quad \text{— } (*)$$

Similarly, we can p.t.

$$\sum_{i=1}^{m} b_i \equiv \frac{m}{2} \pmod m \quad \text{-- } (**)$$

Suppose ~~Since~~ $a_1+b_1, a_2+b_2, \ldots, a_m+b_m$ is CRS modulo m then

by above argument we say that

$$\sum_{i=1}^{m} (a_i+b_i) \equiv \frac{m}{2} \pmod m \quad \text{--- } (***)$$

By adding $(*)$ & $(**)$,

$$\sum_{i=1}^{m} (a_i+b_i) \equiv m \pmod m$$

$$\Rightarrow \sum_{i=1}^{m} (a_i+b_i) \equiv 0 \pmod m \quad \text{— } (****)$$

By $(***)$ & $(****)$ we say that,

$$\frac{m}{2} \equiv 0 \pmod m$$

$$\Rightarrow m \mid \frac{m}{2} \Rightarrow 2 \mid 1 \quad \times$$

our supposition is wrong

i.e $a_1+b_1, a_2+b_2, \ldots, a_n+b_n$ is not CRS modulo m

* Reduced residue system modulo m (R…

In a CRS modulo m the set of all integers which are relatively prime to m is called a reduced residue system m.

→ Find RRS modulo 7 of $\{6, 8, 10, 12, 14, 16, 18\}$.

Ans:- $\{6, 8, 10, 12, 16, 18\}$.

→ Remark:-

We know that,

$\phi(m)$ = Total no. of +ve integers less than m & which are relatively prime to m

m	2	3	4	5	6
$\phi(m)$	1	2	2	4	2

Clearly $\phi(m) \le m-1$, $\forall m > 1$

If m is prime then $\phi(m) = m-1$.

If m is not prime, then $\phi(m) < m-1$.

RRS mod m contains $\phi(m)$ elements.

(18) P.T. a set of k integers $a_1, a_2, \dots, a_k$ is reduced residue system modulo m iff (i) $k = \phi(m)$.

(ii) $(a_i, m) = 1$, $\forall i$

(iii) $a_i \not\equiv a_j \pmod{m}$, $\forall i \ne j$.

proof:-

If $a_1, a_2, \dots, a_k$ is RRS mod m

It satisfies all three conditions.

→ converse part:-

If given three conditions are satisfied then by condition (iii), we say that,

$a_1, a_2, \ldots, a_k$ are in CRS mod m

also by condition (ii) we say that, every element a_i is relatively prime to m.

Hence we say that,

$a_1, a_2, \ldots, a_k$ is RRS modulo m.

(19) If $a_1, a_2, \ldots, a_{\phi(m)}$ is RRS modulo m and $(a,m)=1$ then prove the following:

(i) $aa_1, aa_2, \ldots, aa_{\phi(m)}$ is RRS mod m

(ii) $a_1+b, a_2+b, \ldots, a_{\phi(m)}+b$ is not RRS [illegible]

~~(ii) $aa_1+b, aa_2+b, \ldots, aa_{\phi(m)}+b$ is RRS not mod m~~

where b is any integer.

proof:- First we prove that,

$aa_i \not\equiv aa_j \pmod{m}, \forall i \neq j$.

suppose $aa_i \equiv aa_j \pmod{m}$, for some $i \neq j$

$\Rightarrow a_i \equiv a_j \pmod{m}$ $(\because (a,m)=1$

but $\{6+1, 7+1, 8+1, 9+1\}$ is not

$\therefore\ aa_i \not\equiv aa_j \pmod m,\ \forall i \neq j$.

Now we p.t. $(aa_i, m) = 1$.

Clearly.

$$(aa_i, m) = (a_i, m) \quad (\because (a,m)=1$$
$$= 1 \quad (\because a_1, \ldots, a_{\phi(m)} \text{ is RR}$$

Hence, $aa_1, aa_2, \ldots, aa_{\phi(m)}$ is RRS mod

(1) $\{6, 7, 8, 9, 10\}$ is CRS modulo 5
$\{6, 7, 8, 9\}$ is RRS modulo 5
but $\{6+1, 7+1, 8+1, 9+1\}$ is not RRS mo

First we p.t.

$$aa_i + b \not\equiv aa_j + b \pmod m,\ \forall i \neq j.$$

If possible,

suppose,

$(aa_i + b) \equiv (aa_j + b) \pmod m$, for some $i \neq j$.

$\Rightarrow\ aa_i \equiv aa_j \pmod m$

$\Rightarrow\ a_i \equiv a_j \pmod m \quad (\because (a,m) = 1$

$\times$

$(\because a_1, \ldots, a_{\phi(m)}$ is RRS mod

$\therefore\ aa_i + b \not\equiv aa_j + b \pmod m,\ \forall i \neq j$

Now we p.t.

$$(aa_i + b, m) = 1.$$

Clearly, $(aa_i + b, m) = (aa_i, m)$
$= (a_i, m)$
$= 1$.

Hence,

$aa_1 + b,\ aa_2 + b, \ldots, aa_{\phi(m)} + b$ is RRS

(20) State & prove Euler's theorem

→ If $(a, m) = 1$ then $a^{\phi(m)} \equiv 1 \pmod{m}$.

proof:-

Let $x_1, x_2, \ldots, x_{\phi(m)}$ be a RRS mod m

then by above theorem, we say that

$ax_1, ax_2, \ldots, ax_{\phi(m)}$ is also RRS mod m

$(\because (a, m) = 1.$

Hence by multiplying the congruent relation, we get

$$ax_1 \cdot ax_2 \cdots ax_{\phi(m)} \equiv x_1 \cdot x_2 \cdots x_{\phi(m)} \pmod{m}$$

$$\Rightarrow a^{\phi(m)} x_1 \cdot x_2 \cdots x_{\phi(m)} \equiv x_1 \cdot x_2 \cdots x_{\phi(m)} \pmod{m}$$

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

$\left(\begin{array}{l} \because (x_i, m) = 1, \forall i \\ \therefore (x_1 x_2 \cdots x_{\phi(m)}, m) = 1 \end{array}\right.$

Hence, Euler's thm is proved.

(21) Fermat's theorem (or Fermat's little thm)

→ For any integer a, if p is prime then p.t $a^p \equiv a \pmod{p}$.

~~(i.e. $a^{p-1} \equiv 1 \pmod{p}$)~~.

×

case-1

proof:- If p / a then p / a^p.

$$\Rightarrow p / a^p - a$$

$$\Rightarrow a^p \equiv a \pmod{p}$$

Case-2 If $p \nmid a$ then $(p,a)=1$.

then by Euler's thm,

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

$$\Rightarrow a^{p-1} \equiv 1 \pmod{p} \quad (\because p \text{ prime})$$

$$\Rightarrow a^{p} \equiv a \pmod{p}.$$

Definition:-

If $(a,m)=1$ & λ is the smallest +ve integer such that, $a^{\lambda} \equiv 1 \pmod{m}$ then λ is called order of a modulo m

(22) If $a^{n} \equiv 1 \pmod{m}$ & d is order of a modulo m then p.t. d/n

proof:- Here d is order of a mod m

$\therefore$ d is the least +ve int $\ni$

$$a^{d} \equiv 1 \pmod{m} \quad \text{---} (*)$$

By divison algorithm property on d & n we can write,

$$n = qd + r, \quad \text{where } 0 \le r < d$$

If $0 < r < d$ then by (*)

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

$$\Rightarrow (a^{d})^{q} \equiv 1^{q} \pmod{m}$$

$$\Rightarrow a^{qd} \cdot a^{r} \equiv a^{r} \pmod{m}.$$

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

$$\Rightarrow a^{r} \equiv 1 \pmod{m}. \quad (\because a^{n} \equiv 1 \pmod{m}$$

$\times$ where $0 < r < d$)

~~($\because$ d is the least +ve int $\ni$~~

Date: / /

$\therefore r = 0.$

$\therefore n = qd$

$\therefore d / n$

(23) If $(a, m) = 1$, $a^{m-1} \equiv 1 \pmod{m}$ & $a^n \not\equiv 1 \pmod{m}$ for any proper divisor n of $m-1$, then p.t. m is prime

proof:-

If d is order of a modulo m then $d / m-1$ (by above thm)

If d is proper divisor of $m-1$ then $a^d \not\equiv 1 \pmod{m}$ X

($\because d$ is order of a $\therefore a^d \equiv 1 \pmod{m}$)

$\therefore d$ is not a proper divisor of $m-1$

$\therefore d = m-1$

Thus order of a mod m is $m-1$.

Since $(a, m) = 1$, by Euler's thm

$a^{\phi(m)} \equiv 1 \pmod{m}$ and order of a is $m-1$

$\therefore$ by above thm, we say that,

$m-1 / \phi(m)$.

$\Rightarrow m-1 \leq \phi(m)$.

also we know that, $\phi(m) \leq m-1$

$\therefore \phi(m) = m-1$

Hence, m is prime

$\Rightarrow q \,/\, (F_{n-1})^{2^{n+1}} + 1$, also q is prime & odd

then by last thm, we say that

$q = 2^{n+2}t + 1$, for some $t \in \mathbb{Z}$.

Hence the thm is proved

(See-12 ...)

(29) Prove that, $\phi(p^k) = p^k\left(1 - \frac{1}{p}\right) \left(= p^k - p^{k-1}\right)$
(U-4) where p is prime.

proof:-

Here p is prime $\therefore \phi(p) = p-1$.
In a CRS modulo p^k, the only multipliers of p are, $p, 2p, 3p, \ldots, p^{k-1}.p$.
These numbers are not relatively prime to p. Thus there are total p^{k-1} elements which are not relatively prime to p.
Hence, the remaining $p^k - p^{k-1}$ elements are relatively prime to p^k.
Hence, by def^n

$$\phi(p^k) = p^k - p^{k-1}$$

$$= p^k\left[1 - \frac{1}{p}\right].$$

(30) Find $\phi(128)$, $\phi(625)$, $\phi(81)$.

sol^n: $\phi(128) = \phi(2^7) = 2^7 - 2^6 = 128 - 64 = 64$

Date: / /

$\phi(625) = \phi(5^4) = 5^4 - 5^3 = 625 - 125$
$= 500.$

$\phi(81) = \phi(3^4) = 3^4 - 3^3 = 81 - 27 = 54$

V-4

(31) $\sum_{i=0}^{k} \phi(p^i) = p^k$, where p is prime

Sol: $\sum_{i=0}^{k} \phi(p^i) = \underbrace{\phi(p^0)}_{\phi(1)} + \sum_{i=1}^{k} (p^i - p^{i-1})$

$= 1 + \sum_{i=1}^{k} p^i - \sum_{i=1}^{k} p^{i-1}$

$= 1 + p^k - 1 = p^k$

V-4

(32) Find $\phi(32) + \phi(16) + \phi(8) + \phi(4) + \phi(2) + \phi(1)$ or $\sum_{i=0}^{5} \phi(2^i)$.

Sol:- by above ex. $\sum_{i=0}^{5} \phi(2^i) = 2^5 = 32$.

V-4

imp (33) If $(a,b) = 1$ then p.t. $\phi(ab) = \phi(a)\phi(b)$.

OR

V-4

p.T. Euler's function is multiplicative function

proof:

Let $x_1, x_2, \dots x_{\phi(a)}$ and $y_1, y_2, \dots, y_{\phi(b)}$ be RRS modulo a & modulo b respectively.

consider the set

$S = \{ bx_i + ay_j \mid i = 1, 2, \dots, \phi(a), \; j = 1, 2, \dots, \phi(b) \}$

which contains $\phi(a)\cdot\phi(b)$ elements.

we have to p.t. $\phi(ab) = \phi(a)\phi(b)$.

$\therefore$ It is sufficient to p.t S is RRS mod (ab)

first we p.t.

$$(bx_i + ay_j) \not\equiv (bx_k + ay_l) \pmod{ab}$$
$$(\forall i \neq k, j \neq l)$$

suppose,

$$bx_i + ay_j \equiv (bx_k + ay_l) \pmod{(ab)}$$
for some $i \neq k, j \neq l$

$$\Rightarrow ab / [b(x_i - x_k) + a(y_j - y_l)]$$

$$\Rightarrow a / [b(x_i - x_k) + a(y_j - y_l)]$$
$$(\because a/ab \ \& \ ab/z \Rightarrow a/z)$$

$$\Rightarrow a / b(x_i - x_k) \quad (\because a / a(y_j - y_l))$$

$$\Rightarrow a / x_i - x_k \quad [\because (a, b) = 1]$$

$$\Rightarrow x_i \equiv x_k \pmod{a} \quad \times$$

$$(\because x_1, x_2, \ldots, x_{\phi(a)} \text{ is RRS mod } m)$$

$\therefore$ our supposition is wrong.

$$\therefore (bx_i + ay_j) \not\equiv (bx_k + ay_l) \pmod{ab}$$
$$(\forall i \neq k, j \neq l).$$

Now we p.t.

$$(bx_i + ay_j, ab) = 1 \quad \forall i, j.$$

we know that

$(x_i, a) = 1, \quad \forall i = 1, 2, \ldots, \phi(a).$

& $(a, b) = 1$

$\therefore (\ldots$

Date: / /

$\Rightarrow (a, bx_i + ay_j) = 1, \forall i, j.$

Similarly we can p.t.

$(b, bx_i + ay_j) = 1, \forall i, j.$

$\Rightarrow (bx_i + ay_j, ab) = 1, \forall i, j.$

Now we p.t. every element relatively prime to ab belongs to S.

Suppose $(z, ab) = 1$, we know that

$(a, b) = 1$

$\Rightarrow ax_0 + by_0 = 1$, for $x_0, y_0 \in \mathbb{Z}$

$\Rightarrow zax_0 + zby_0 = z$, for $x_0, y_0 \in \mathbb{Z}$ & $z \in \mathbb{Z}$.

$\Rightarrow ay + bx = z$, for $y = zx_0, x = zy_0$

also we know that

$(z, ab) = 1.$

$\Rightarrow (z, a) = 1$

$\Rightarrow (ay + bx, a) = 1$

$\Rightarrow (bx, a) = 1$

$\Rightarrow (x, a) = 1 \quad (\because (a, b) = 1$

$\Rightarrow x \equiv x_i \pmod a$, for some $i = 1, 2, \ldots, \phi(a)$.

Similarly

we can p.t

$y \equiv y_j \pmod b$, for some $j = 1, 2, \ldots, \phi(b)$.

Hence we get

$bx \equiv bx_i \pmod{ab}$ &

$ay \equiv ay_j \pmod{ab}$.

$\Rightarrow bx + ay \equiv bx_i + ay_j \pmod{ab}$,

$\Rightarrow z \equiv bx_i + ay_j \pmod{ab} \Rightarrow z \in S$

Hence S is RRS modulo ab.

$\therefore \phi(ab) = \phi(a)\,\phi(b)$.

$\therefore$ Euler's f^n is multi. f^n

(34) If $m = p_1^{m_1} \cdot p_2^{m_2} \cdots p_k^{m_k}$, where all p_i are primes then p.t. $\phi(m) = m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \cdots \left(1-\frac{1}{p_k}\right)$

proof :-

$$L.H.S. = \phi(m) = \phi\left(p_1^{m_1} \cdot p_2^{m_2} \cdots p_k^{m_k}\right)$$

$$= \phi(p_1^{m_1}) \cdot \phi(p_2^{m_2}) \cdots \phi(p_k^{m_k})$$

$$= p_1^{m_1}\left(1-\frac{1}{p_1}\right) \cdot p_2^{m_2}\left(1-\frac{1}{p_2}\right) \cdots p_k^{m_k}\left(1-\frac{1}{p_k}\right)$$

$$= m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \cdots \left(1-\frac{1}{p_k}\right)$$

$= RHS$.

(35) Find $\phi(300)$, $\phi(301)$, $\phi(1234)$.

$300 = 3 \times 5 \times 5 \times 2 \times 2 = 2^2 \times 3 \times 5^2$

~~301 =~~

$$\therefore \phi(300) = 300\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$

$$= 300\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)$$

$$= 80$$

$301 = 7 \times 43$

$$\therefore \phi(301) = 301\left(1-\frac{1}{7}\right)\left(1-\frac{1}{43}\right) = 301\left(\frac{6}{7}\right)\left(\frac{42}{43}\right)$$

$= 252$

$1234 = 2 \times 617$

$$\therefore \phi(1234) = 1234\left(1-\frac{1}{2}\right)\left(1-\frac{1}{617}\right)$$
$$= 1234\left(\frac{1}{2}\right)\left(\frac{616}{617}\right)$$
$$= \underline{616}$$

V-2

(36) P.T. $\phi(ab) = \dfrac{\phi(a)\phi(b)d}{\phi(d)}$, where $d = (a,b)$

<u>Sol^n</u>: We know that,

$$\phi(ab) = ab \cdot \prod_{p/ab}\left(1-\frac{1}{p}\right) \quad -(*)$$

where p is prime

$$\Rightarrow \frac{\phi(ab)}{ab} = \prod_{p/ab}\left(1-\frac{1}{p}\right)$$

$p=1,2,$

$p/4.8$

$$= \frac{\prod_{p/a}\left(1-\frac{1}{p}\right)\prod_{p/b}\left(1-\frac{1}{p}\right)}{\prod_{p/(a,b)}\left(1-\frac{1}{p}\right)}.$$

1,2   1,2

$p/4$ $p/8$

$p/4$

5,3   5,2   1,2

$p/15.10$

$p/(15,10)$

$$= \frac{\frac{\phi(a)}{a} \cdot \frac{\phi(b)}{b}}{\frac{\phi(d)}{d}}, \text{ where } d = (a,b)$$

(by (*))

$$\text{Thus, } \frac{\phi(ab)}{ab} = \frac{\phi(a)\phi(b)d}{ab\,\phi(d)}$$

$$\Rightarrow \phi(ab) = \phi(a)\phi(b)d$$

(37) P.T the sum of $\phi(m)$ +ve integers less than m $(m>1)$ and relatively prim to m is $\frac{m}{2}\phi(m)$.

proof:

Let $x_1, x_2, ---, x_{\phi(m)}$ be any $\phi(m)$ +ve integers less than m and also $(x_i, m) = 1, \forall i$

Clearly $x_1, x_2, ---, x_{\phi(m)}$ is RRS modulo m

Now we p.t. $m-x_1, m-x_2, ---, m-x_{\phi(m)}$ is also RRS modulo m

If $m-x_i \equiv m-x_j \pmod m$

$\Rightarrow m / (m-x_i)-(m-x_j)$

$\Rightarrow m / x_j - x_i$

$\Rightarrow x_i \equiv x_j \pmod n$ $\times$

$\therefore m-x_i \not\equiv m-x_j \pmod m$.

Also, $(m-x_i, m) = (-x_i, m) = (x_i, m) = 1$

Thus, $m-x_1, m-x_2, ---, m-x_{\phi(m)}$ is RRS modulo m.

Hence, $x_1+x_2+---+x_{\phi(m)} = (m-x_1)+(m-x_2)+ \dots +(m-x_{\phi(m)})$

$= m\phi(m) - (x_1+x_2+---+x_{\phi(m)})$

$\Rightarrow 2(x_1+x_2+---+x_{\phi(m)}) = m\phi(m)$

(38) Find all +ve integers m & n such that $\phi(mn) = \phi(m) + \phi(n)$.

Sol^n:-

We know that,

$$\phi(mn) = \frac{\phi(m)\,\phi(n)\,d}{\phi(d)},$$

where $d = (m, n)$

$$\Rightarrow \phi(m) + \phi(n) = \frac{\phi(m)\,\phi(n)\,d}{\phi(d)}$$

$$\Rightarrow \frac{\phi(m)\,\phi(d) + \phi(n)\,\phi(d)}{\phi(m)\,\phi(n)} = d$$

$$\Rightarrow \frac{\phi(d)}{\phi(n)} + \frac{\phi(d)}{\phi(m)} = d$$

$$\Rightarrow \frac{1}{a} + \frac{1}{b} = d, \text{ where } a = \frac{\phi(n)}{\phi(d)},\ b = \frac{\phi(m)}{\phi(d)} \in N$$

under-standing

Now $(m, n) = d$

$\Rightarrow d/m,\ d/n$

$\Rightarrow \phi(d)/\phi(m)$ & $\phi(d)/\phi(n)$

$$\Rightarrow \frac{\phi(m)}{\phi(d)},\ \frac{\phi(n)}{\phi(d)} \in Z$$

$\Rightarrow a, b \in Z$

Thus we have

$\frac{1}{a} + \frac{1}{b} = d$, where $d = 2$ when $a = 1 = b$

& $d = 1$ when, $a = 2 = b$.

Now, $\phi(m) = b\,\phi(d)$ &

$\phi(n) = a\,\phi(d)$.

$a = 1 = b$, $d = 2$

$\Rightarrow \phi(m) = 1 \cdot 1 = 1$ & $\phi(n) = 1$

also, $a = 2 = b$, $d = 1$

$\Rightarrow \phi(m) = 2 \cdot 1 = 2$. & $\phi(n) = 2 \cdot 1 = 2$

Thus, $\phi(m) = 1 = \phi(n) \Rightarrow m, n = 2,$ $m=n=2$,

$\phi(m) = 2 = \phi(n) \Rightarrow m, n = \{3, 4, 6\}$.

$\Rightarrow (m,n) = (2,2), (3,4)\ \cancel{(3,6)},$

$(4,3), \cancel{(4,6)}, \cancel{(6,4)}, \cancel{(6,3)}$

$\cancel{(3,3)}, \cancel{(4,4)}, \cancel{(6,6)}$.

$= (2,2), (3,4)\ (4,3)$

If $(m,n) = (2,2)$ then

$\phi(mn) = \phi(4) = 2$

$\phi(m) = \phi(2) = 1$

$\phi(n) = \phi(2) = 1$

$\therefore \phi(mn) = \phi(m) + \phi(n)$

If $(m,n) = (3,4)$ then

$\phi(mn) = \phi(12) = 4$

$\phi(3) = 2$, $\phi(4) = 2$

$\therefore (m,n) = (3,4)$ satisfies given eq^n

Similarly, $(m,n) = (4,3)$ " " "

If $(m,n) = (3,6)$ then
$\phi(mn) = \phi(18) = 6$

& $\phi(m) + \phi(n) = 2 + 2 = 4$

$\therefore (m,n) = (3,6)$ does not satisfy given eq^n.

Similarly we can check that,

all remaining (m,n) do not satisfy the given condition

Hence, $(2,2)$, $(3,4)$ & $(4,3)$ satisfy the given equation.

U-4 (conti) — (conti pg. 146)

** Congruence in one unknown:-
Let $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$.
The congruence in one unknown,
$f(x) \equiv 0 \pmod m$ is said to be of order 'n'
if $m \nmid a_n$.

If $f(a) \equiv 0 \pmod m$ then $x \equiv a \pmod m$ is sol^n of $f(x) \equiv 0 \pmod m$.

(39) (i) Prove that, the linear congruence in one unknown $ax + b \equiv 0 \pmod m$, where $(a,m) = 1$ has exactly one sol^n $x \equiv -a^{\phi(m)-1} \cdot b \pmod m$.

(ii) When $(a,m) = d\ (>1)$ then prove that $ax + b \equiv 0 \pmod m$ has sol^n iff $d \mid$

By (2) we say that,

$$F(a) = \sum_{d/a} \mu(d) = 0.$$

~~Since, d takes all factors of 'a',~~

$\frac{a}{d}$ also takes all the factors of 'a'

$\left(\because \; a=12, \; d = 1,2,3,4,6,12 \quad \frac{a}{d} = 12,6,4,3,2,1 \right.$

$\therefore$ We can write, $\sum_{d/a} \mu\left(\frac{a}{d}\right) = 0.$

U-4

~~UNIT-4~~ (continued)

(25) If m is +ve integer then p.t

$$\phi(m) = m \sum_{d/m} \frac{\mu(d)}{d} = \sum_{d/m} \mu\left(\frac{m}{d}\right) \cdot d.$$

$$\left[\because m \sum_{d/m} \frac{\mu\left(\frac{m}{d}\right)}{\frac{m}{d}} \right]$$

proof

Let $m = p_1^{m_1} p_2^{m_2} \ldots p_k^{a_k}$.

where all p_i's are primes

Now, define a function,

$$F(m) = \sum_{d/m} \frac{\mu(d)}{d}.$$

first we prove that,

$F(bc) = F(b)F(c)$, if $(b,c) = 1$.

L.H.S $= F(bc) = \sum \frac{\mu(d)}{}$

$$= 1 + \frac{\mu(b)}{b} + \frac{\mu(c)}{c} + \frac{\mu(bc)}{bc}.$$

$$= 1 + \frac{\mu(b)}{b} + \frac{\mu(c)}{c} + \frac{\mu(b)\mu(c)}{bc}.$$

$$= \left[\frac{\mu(1)}{1} + \frac{\mu(b)}{b}\right]\left[\frac{\mu(1)}{1} + \frac{\mu(c)}{c}\right].$$

$$= F(b)F(c)$$

$$= R.H.S.$$

Since, $m = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$,

$$F(m) = F(p_1^{m_1}) \cdots F(p_k^{m_k}) \quad -(2)$$

$$F(p_i^{m_i}) = \sum_{d / p_i^{m_i}} \frac{\mu(d)}{d}.$$

$$= \mu(1) + \frac{\mu(p_i)}{p_i} + \frac{\mu(p_i^2)}{p_i^2} + \cdots$$

$$= 1 + \frac{(-1)}{p_i} + 0 \cdots$$

$$= 1 - \frac{1}{p_i}.$$

By (2)

$$F(m) = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

$$\Rightarrow mF(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

$$= \phi(m).$$

Date: / /

$$\Rightarrow m \sum_{d/m} \frac{\mu(d)}{d} = \phi(m) \quad -(3)$$

Since d takes all factors of m, $\frac{m}{d}$ also takes all factors of m

$\therefore$ By (3), we can write,

$$m \sum_{d/m} \frac{\mu\left(\frac{m}{d}\right)}{\frac{m}{d}} = \phi(m).$$

$$\Rightarrow \phi(m) = \sum_{d/m} \mu\left(\frac{m}{d}\right) d.$$

Hence theorem is proved

(26) P.T. $\sum_{d/m} \phi(d)\mu(d) = 0$. iff m is even

oof:

Let $m = p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k}$

Define, F by

$$F(m) = \sum_{d/m} \phi(d)\mu(d).$$

first we p.t.,

$$F(bc) = F(b)F(c), \text{ if } (b,c) = 1.$$

$$L.H.S. = F(bc) = \sum_{d/bc} \phi(d)\mu(d)$$

$$= \phi(1)\mu(1) + \phi(b)\mu(b) + \phi(c)\mu(c) + \phi(bc)\mu(bc).$$

$$= 1 + \phi(b)\mu(b) + \phi(c)\mu(c) + \phi(b)\phi(c) + \mu(b)\mu(c).$$

$$= [1 + \phi(b)\mu(b)][1 + \phi(c)\mu(c)].$$

$$= [\phi(1)\mu(1) + \phi(b)\mu(b)][\phi(1)\mu(1) + \phi(c)\mu(c)]$$

$$= \left(\sum_{d/b} \phi(d)\mu(d)\right)\left(\sum_{d/c} \phi(d)\mu(d)\right).$$

$$= F(b)F(c) = RHS.$$

Now,

$$m = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}.$$

$$\Rightarrow F(m) = F(p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k})$$

$$= F(p_1^{m_1})F(p_2^{m_2}) \cdots F(p_k^{m_k}). \quad -(1)$$

Here,

$$F(p_i^{m_i})$$

$$= \sum_{d/p_i^{m_i}} \phi(d)\mu(d)$$

$$= \phi(1)\mu(1) + \phi(p_i)\mu(p_i) + \phi(p_i^2)\mu(p_i^2) + \cdots + \phi(p_i^{m})\mu(p_i^{m}).$$

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

$$= 1 - (p_i - 1)$$

$$= 2 - p_i, \forall i.$$

$\therefore$ By (1),

$$F(m) = (2-p_1)(2-p_2)\cdots(2-p_k).$$

$$\Rightarrow F(m) = \Pi$$

Date: / /

Now, $\sum \phi(d)\mu(d) = 0$

$\Leftrightarrow F(m) = 0$

$\Leftrightarrow \prod_{p_i/m} (2 - p_i) = 0$

$\Leftrightarrow 2/m$ $\quad (\because 2 - p_i = 0 \Rightarrow p_i = 2$ & $p_i/m \Rightarrow 2/m$

$\Leftrightarrow$ m is even

(27) P.T. the necessary and sufficient condition for m is prime is,

$\phi(m) + s(m) = m \times T(m)$.

OR

P.T. m is prime, iff

$\phi(m) + s(m) = m \times T(m)$.

roof:

If m is prime then

$\phi(m) = m - 1$.

$s(m) = m + 1$.

$T(m) = 2$.

$\Rightarrow \phi(m) + s(m) = m - 1 + m + 1$

$= 2m$

$= m \times T(m)$

Hence,

$\phi(m) + s(m) = m \times T(m)$.

Converse part :-

If $\phi(m) + s(m) = m \times T(m)$, then we have to prove that,

m is prime

$< 2^{k+1} = 2^k \cdot 2 \Rightarrow \sigma(p^k) < 2p^k$.

Suppose m is not prime.

Case-1 :- If $m = 1$ then,

$L.H.S. = \phi(1) + \sigma(1) = 2$ &

$R.H.S. = 1 \cdot T(1) = 1$

$\therefore LHS \neq RHS$. ✗

Case-2 :- If $m = p^k$, $k \geq 2$, p is prime.
(* m is not prime)

We know that,

$$\left.\begin{aligned} &\sigma(p^k) < 2p^k \text{ if } p = 2 \ \& \\ &\sigma(p^k) < \tfrac{3}{2}p^k \text{ if } p \geq 3 \\ &\text{i.e. } \sigma(p^k) < 2p^k \text{ if } p \geq 3. \end{aligned}\right\} \quad \text{--- (1)}$$

$$\begin{aligned} L.H.S. &= \phi(m) + \sigma(m) \\ &= \phi(p^k) + \sigma(p^k) \\ &< p^k + 2p^k \quad (\because \phi(m) < m \ \& \text{ by (1)}) \\ &= 3p^k \\ &= 3m. \\ &\leq T(p^k)\, m \\ &= m\,T(p^k) \\ &= R.H.S. \end{aligned}$$

$\left(\because m = p^3 \Rightarrow T(m) = 3+1 = 4\right.$ p is prime
$\Rightarrow \cancel{T(m)}$
$T(p^k) = k+1 \geq 3 \ (\because k \geq 2)$
i.e. $\left. 3 \leq T(p^k) \right)$

Thus.

$\phi(m) + \sigma(m) < m\,T(m)$ ✗

Case-3 :- If $m = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$.
where all p_i's are primes.
& $p_1 < p_2 < \cdots < p_k$ & $k \geq 2$.

↓

Date: / /

$$\text{L.H.S.} = \phi(m) + \sigma(m)$$
$$< m + \sigma(p_1^{m_1})\,\sigma(p_2^{m_2}) \cdots \sigma(p_k^{m_k})$$
$$< m + 2p_1^{m_1}\left(\frac{3}{2}p_2^{m_2}\right)\cdots\left(\frac{3}{2}p_k^{m_k}\right).$$

(by (1))

$$= m + m\cdot 2\left(\frac{3}{2}\right)^{k-1}$$
$$= m + m\cdot 3\cdot\left(\frac{2}{3}\right)\left(\frac{3}{2}\right)^{k-1}$$
$$= m + m\cdot 3\left(\frac{3}{2}\right)^{k-2}.$$
$$< m + 3m\,2^{k-2}\left(\because \frac{3}{2} < 2\right).$$
$$= m\left(1 + 3\cdot 2^{k-2}\right)$$
$$\leq m\left[2^{k-2} + 3\cdot 2^{k-2}\right] \quad (\because k \geq 2).$$
$$= m\left[4\cdot 2^{k-2}\right]$$
$$= m(2^k)$$
$$\leq m\cdot T(m).$$

Thus,

$$\phi(m) + \sigma(m) < mT(m) \quad \times$$

$$\left(\because T(m) = T(p_1^{m_1})\,T(p_2^{m_2}) * \cdots * T(p_k^{m_k})\right.$$
$$= (m_1+1)(m_2+1)\cdots(m_k+1)$$
$$\geq 2\cdot 2\cdots 2 \quad (\because m_i \geq 1, \forall i)$$
$$= 2^k \quad \therefore T(m) \geq 2^k.$$

Hence by case-(1), (2) & (3), we say that our supposition is wrong
Hence m is prime.

If $(m,n) = (3,6)$ then
$\phi(mn) = \phi(18) = 6$

& $\phi(m) + \phi(n) = 2 + 2 = 4$

$\therefore (m,n) = (3,6)$ does not satisfy given eq^n.

Similarly we can check that,

all remaining (m,n) do not satisfy the given condition.

Hence, $(2,2)$, $(3,4)$ & $(4,3)$ satisfy the given equation.

U-4 (cont.) (Kouth p. 146)

* Congruence in one unknown:-

Let $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$.

The congruence in one unknown, $f(x) \equiv 0 \pmod{m}$ is said to be of order 'n' if $m \nmid a_n$.

If $f(a) \equiv 0 \pmod{m}$ then $x \equiv a \pmod{m}$ is sol^n of $f(x) \equiv 0 \pmod{m}$.

(39) (i) Prove that, the linear congruence in one unknown $ax+b \equiv 0 \pmod{m}$, where $(a,m)=1$ has exactly one sol^n $x \equiv -a^{\phi(m)-1} b \pmod{m}$

(ii) When $(a,m) = d\ (>1)$ then prove that $ax+b \equiv 0 \pmod{m}$ has sol^n iff d

In this case it has 'd' sol^{ns}.

$x_i \equiv a + i\frac{m}{d} \pmod m$, $i = 0, 1, 2, \ldots, d-1$.

of which $x \equiv a \pmod{\frac{m}{d}}$ is unique sol^n of $\frac{a}{d}x + \frac{b}{d} \equiv 0 \pmod{\frac{m}{d}}$.

proof :- (i) If $(a, m) = 1$.

Let $x_1, x_2, \ldots, x_m$ be CRS modulo m

then $ax_1, ax_2, \ldots, ax_m$ is also CRS modulo m.

$\therefore ax_1 + b, ax_2 + b, \ldots, ax_m + b$ is also CRS modulo m

$\therefore$ Among them exactly one element say ↑ $\leftarrow ax_k + b$ is cong. 0 mod m

i.e. $ax_k + b \equiv 0 \pmod m$)

Thus we say that,

$ax + b \equiv 0 \pmod m$ has exactly one sol^n.

Now, $ax + b \equiv 0 \pmod m$

$\Rightarrow ax \equiv -b \pmod m$

$\Rightarrow a^{\phi(m)-1} \cdot ax = -b \cdot a^{\phi(m)-1} \pmod m$

$\Rightarrow a^{\phi(m)} \cdot x \equiv -a^{\phi(m)-1} \cdot b \pmod m$.

but $(a, m) = 1 \Rightarrow a^{\phi(m)} \equiv 1 \pmod m$

($\because$ by Euler thm)

$\therefore x \equiv -a^{\phi(m)-1} \cdot b \pmod m$

(ii) $(a, m) = d$ $(d > 1)$

If $ax + b \equiv 0 \pmod m$ has sol^n —(*)

then $m / ax+b$ also $(a, m) = d$

$\therefore d/m$ & d/a

$\Rightarrow d / ax+b$ & d/a

$\Rightarrow d / ax+b$ & d / ax

$\Rightarrow d$ ...

→ converse part :-

If d / b then $\frac{b}{d} \in Z$.

Now $(a, m) = d \Rightarrow \left(\frac{a}{d}, \frac{m}{d}\right) = 1$.

then by case (i), we say that,

$\frac{a}{d}x + \frac{b}{d} \equiv 0 \pmod{\frac{m}{d}}$ has solⁿ. (**)

i.e $ax + b \equiv 0 \pmod{m}$ has solⁿ.

If unique solⁿ of (**) is, $x \equiv a \pmod{\frac{m}{d}}$

then all integers of the form

* $a + t\cdot\frac{m}{d}$ $(t \in Z)$ are also solⁿˢ of eqⁿ (**)

Hence from above integers, all incongruent integers modulo m are solⁿˢ of (*)

we know that,

$$a + t_1\frac{m}{d} \equiv a + t_2\frac{m}{d} \pmod{m}$$
$$\Leftrightarrow (t_1 - t_2)\frac{m}{d} \equiv 0 \pmod{m}$$
$$\Leftrightarrow m / (t_1 - t_2)\frac{m}{d}$$
$$\Leftrightarrow d / t_1 - t_2$$
$$\Leftrightarrow t_1 \equiv t_2 \pmod{d}$$

Thus we say that all incongruent solⁿˢ can be obtained for $t = 0, 1, \dots, d-1$

Hence $a, a + \frac{m}{d}, \dots, a + (d-1)\frac{m}{d}$ are all incongruent solⁿˢ of (*)

* $\frac{m}{d} / x - a$ & $\frac{m}{d} / t\cdot\frac{m}{d}$ ⇒ $\frac{m}{d} / x - a - t\frac{m}{d}$ ⇒ $x \equiv \left(a + t\frac{m}{d}\right) \bmod \left(\frac{m}{d}\right)$.

(40) Provethat, the necessary and sufficient condition for,

$ax+by+c \equiv 0 \pmod m$ has sol^n is d/c

where $d = (a, b, m)$ also provethat, it has 'md' sol^{ns}.

proof:-

If $ax+by+c \equiv 0 \pmod m$ has sol^n (1)

let $d = (a, b, m)$ then

d/a, d/b, d/m also $m / ax+by+c$ (by (1))

$\Rightarrow d/ax$, d/by & $d/ax+by+c$

$\Rightarrow d/c$

If d/c, where $d = (a, b, m)$

let $(a, m) = d_1$ then $(d_1, b) = d$

Thus d/c & $d = (b, d_1)$

$\therefore$ By above thm,

$by + c \equiv 0 \pmod{d_1}$ has sol^n. —(2)

clearly it has 'd' sol^{ns}.

also by (2) we say that,

$d_1 / by+c \Rightarrow by+c = q d_1$. for $q \in Z$

$\therefore d_1 / q d_1$ & $(a, m) = d_1$.

$\therefore$ By above thm,

$ax + q d_1 \equiv 0 \pmod m$ has sol^n —(3)

clearly it has d_1 sol^{ns}.

Thus $ax+by+c \equiv 0 \pmod m$ has sol^n.

Now we p.t eq^n (1) has md sol^{ns}
from eq^n (2), we say that,

$by + c \equiv 0 \pmod{d_1}$ has d sol^{ns}
with modulo d_1.

$$\therefore \frac{m}{d_1} by + \frac{m}{d_1} c \equiv 0 \left(\bmod \frac{m}{d_1} d_1\right) \text{ has sol}^n$$

clearly, it has $\left(\frac{m}{d_1} b, \frac{m}{d_1} d_1\right) = \frac{m}{d_1} d$ sol^{ns}
with modulo m —(4)

also by (3), we say that,

$ax + q d_1 \equiv 0 \pmod{m}$ has d_1 sol^{ns}
with modulo m

Hence eq^n (1) has total $\frac{m}{d_1} d \cdot d_1$ sol^{ns}
i.e eq^n (1) has 'md' sol^{ns} with modulo m

* Remark:-

In general we can easily prove that $(a_1x_1 + a_2x_2 + \cdots + a_nx_n + b) \equiv 0 \pmod{m}$ has sol^{ns} iff $d \mid b$ where $d = (a_1, a_2, \ldots, a_n, m)$ also it has total $m^{n-1} \cdot d$ sol^{ns} with r.t. modulo m

(* pair of sol^{ns},

$x_0, x_1, \ldots, x_{d_1 - 1}$

$\downarrow$

$y_0, y_1, \ldots, y_{\left(\frac{m}{d_1} d - 1\right)}$

$d_1 \left(\frac{m}{d_1} d - 1\right)$.

(41) Prove that, the system of congruences, $x \equiv a \pmod m$, $x \equiv b \pmod n$ has solⁿ iff $a \equiv b \pmod{(m,n)}$. If this condition satisfied then prove that system has unique solⁿ w.r.to modulo $[m,n]$.

proof:-

Suppose $x = c$ is solⁿ of given system then $c \equiv a \pmod m$ & $c \equiv b \pmod n$

$\Rightarrow m / c-a$, $n / c-b$

$\Rightarrow d / c-a$, $d / c-b$, where $d = (m,n)$

$\Rightarrow d / a-b$

$\Rightarrow a \equiv b \pmod d$

$\Rightarrow a \equiv b \pmod{(m,n)}$

* converse part:-

If $a \equiv b \pmod{(m,n)}$ then

$a \equiv b \pmod d$ where $d = (m,n)$.

Thus we have

$d / a-b$ and $(m,n) = d$ then by theorem (39), we say that

$my + (a-b) \equiv 0 \pmod n$ has solⁿ.

say $y = y_1$

$\therefore my_1 + (a-b) \equiv 0 \pmod n$

$\Rightarrow a + my_1 \equiv b \pmod n$ — (1)

We know that,

m / my_1 $\therefore$ $m / (a+my_1)-a$

$\Rightarrow a + my_1 \equiv a \pmod m$ — (2)

Date: / /

By (1) and (2) we say that,
$x = a + my_1$ is sol^n of given system

Now, we p.t. it has unique sol^n
suppose, x_1 & y_1 are sol^{ns} of given system then,

$$x_1 \equiv a \pmod m, \quad y_1 \equiv b \pmod n$$
$$\Rightarrow \quad x_1 \equiv b \pmod n, \quad y_1 \equiv a \pmod m.$$

$$\Rightarrow x_1 \equiv y_1 \pmod m \;\&$$
$$x_1 \equiv y_1 \pmod n$$

$$\Rightarrow m / x_1 - y_1, \quad n / x_1 - y_1$$

$$\Rightarrow [m, n] / x_1 - y_1.$$

$$\Rightarrow x_1 \equiv y_1 \pmod{[m, n]}$$

Thus, the system has unique sol^n w.r. to modulo $[m, n]$.

* Solve the following equations :-

(42) $12x + 15 \equiv 0 \pmod{45}$.

sol^n:- comparing given eq^n with
$ax + b \equiv 0 \pmod m$, we get
$a = 12, \; b = 15, \; m = 45.$

Now, $(a, m) = (12, 45) = 3.$
and $3 / 15$

$\therefore$ given eq^n has sol^n
and it has 3 sol^{ns}.

Here $12x+15 \equiv 0 \pmod{45}$

$\Rightarrow 45 / 12x+15$

$\Rightarrow 12x+15 = 45y$, for some $y \in \mathbb{Z}$

$\Rightarrow 12x-45y+15=0$.

$\Rightarrow 4x-15y+5=0$.

$\therefore x=10,\ y=3$.

Hence, reqrd. sol^{ns} are,

$x \equiv 10 + i\left(\frac{45}{3}\right) \pmod{45}$, $i=0,1,2$.

Hence reqrd sol^{ns} are,

$x \equiv 10 + i \cdot 15 \pmod{45}$, $i=0,1,2$

$\Rightarrow x \equiv 10 \pmod{45}$

$x \equiv 25 \pmod{45}$

$x \equiv 40 \pmod{45}$

i.e $x \equiv 10, 25, 40 \pmod{45}$ are reqrd sol^{ns}.

(43) $18x \equiv 30 \pmod{42}$. i.e $18x-30 \equiv 0 \pmod{42}$.

sol^n: Here $(18, 42) = 6$ and $6/30$.

$\therefore$ given system has sol^n. & it has 6 sol^{ns}

Now, $42 / 18x-30$

$\Rightarrow 18x-30-42y=0$

$\Rightarrow 3x-7y-5=0$

$\Rightarrow x=4,\ y=1$

Hence reqrd sol^{ns} are

$x \equiv 4 + i\left(\frac{42}{6}\right) \pmod{42}$, $i=0,1,2,\ldots,5$

i.e

$x \equiv 4 + i \cdot 7 \pmod{42}$, $i=0,1,2,\ldots,5$

$\Rightarrow x \equiv 4, 11, 18, 25, 32, 39 \pmod{42}$ are reqrd sol^{ns}.

(44) $9x \equiv 21 \pmod{30}$.

sol^n:-

Here, $(9,30) = 3$ and $3/21$,

$\therefore$ given eq^n has sol^n & it has 3 sol^{ns}.

Now, $30 / 9x - 21$

$\Rightarrow 9x - 30y - 21 = 0$, $y \in \mathbb{Z}$

$\Rightarrow 3x - 10y - 7 = 0$

$\Rightarrow x = 9$, $y = 2$

Here, reqrd sol^{ns} are

$x = 9 + i \cdot \left(\frac{30}{3}\right) \pmod{30}$, $i = 0, 1, 2$.

i.e. $x \equiv 9 + i \cdot 10 \pmod{30}$, $i = 0, 1, 2$

i.e. $x \equiv 9 \pmod{30}$,

$x \equiv 19 \pmod{30}$,

$x \equiv 29 \pmod{30}$ are reqrd sol^{ns}.

(45) $103x \equiv 57 \pmod{211}$.

sol^n:- Here $(103, 211) = 1$.

$\therefore$ given eq^n has one sol^n

Now, $211 / 103x - 57$

103 —

$\Rightarrow 103x - 211y - 57 = 0$, $y \in \mathbb{Z}$

$\Rightarrow 103[x - 2y] - 5y - 57 = 0$

$\Rightarrow 103u - 5y - 57 = 0$, where $u = x - 2y$ —(1)

$\Rightarrow 5(20u - y - 11) + 3u - 2 = 0$

$\Rightarrow 5v + 3u - 2 = 0$, where $v = 20u - y - 11$ —(2)

$\therefore v = 1$, $u = -1$.

by eq^n (2), $1 = -20 - y - 11$

$\Rightarrow y = -32$

also by eq^n (1) $x = u + 2y$

$\Rightarrow x = -1 + 2(-32) = -65$

Hence reqrd sol^n is,

$x \equiv -65 \pmod{211}$

i.e. $x \equiv 146 \pmod{211}$

(46) $111x \equiv 75 \pmod{321}$.

sol^n: Here $(111, 321) = 3$ and $3/75$.

$\therefore$ given eq^n has three sol^{ns}.

Now, $321 / 111x - 75$

$\Rightarrow 111x - 321y - 75 = 0$

$\Rightarrow 37x - 107y - 25 = 0$

$\Rightarrow 37(x - 2y) - 33y - 25 = 0$

$\Rightarrow 37u - 33y - 25 = 0$, where $u = x - 2y$ — (1)

$\Rightarrow 33(u - y) + 4u - 25 = 0$

$\Rightarrow 33v + 4u - 25 = 0$, where $v = u - y$ — (2)

$37[x-3y+1]+4y+12=0$

$37u+4y+12=0$

$[9u+y+3]+u=0$

$+v+u=0$

$\boxed{u=-4, v=1}$

$-36+y+3=0$

$y=33$

$x=-4+102+1$

$\boxed{x=99}$

$\therefore v = 1$, $u = -2$

from (2) $1 = -2 - y \Rightarrow y = -3$

from (1) $-2 = x - 2(-3) \Rightarrow x = -8$

Hence reqrd sol^{ns} are,

$x \equiv -8 + \frac{321}{3} i \pmod{321}$, $i = 0, 1, 2$

i.e. $x \equiv -8 + 107 i \pmod{321}$, $i = 0, 1, 2$

$\Rightarrow x \equiv -8 \pmod{321}$ i.e. $x \equiv 313 \pmod{321}$

$x \equiv 99 \pmod{321}$

Date: / /

(47) $863x \equiv 880 \pmod{2151}$

Sol^n:-

Here $(863, 2151) = 1$ and $1/880$.

$\therefore$ given eq^n has one sol^n

Now, $2151 / 863x - 880$

$\Rightarrow 863x - 2151y - 880 = 0, \; y \in \mathbb{Z}$

$\Rightarrow 863(x - 2y - 1) - 425y - 17 = 0$

$\Rightarrow 863u - 425y - 17 = 0, \; u = x - 2y - 1 \quad \text{---(1)}$

$\Rightarrow 425(2u - y) + 13u - 17 = 0$

$\Rightarrow 425v + 13u - 17 = 0, \; v = 2u - y \quad \text{---(2)}$

$\Rightarrow 13(32v + u - 1) + 9v - 4 = 0$

$\Rightarrow 13w + 9v - 4 = 0, \; w = 32v + u - 1 \quad \text{---(3)}$

$\therefore w = 1, \; v = -1$

from (3)

$1 = -32 + u - 1 \Rightarrow u = +34$

from (2) $-1 = 68 - y \Rightarrow y = 69$

from (1) $34 = x - 138 - 1$

$\Rightarrow x = 173$

Hence, reqrd sol^n is, $x \equiv 173 \pmod{2151}$

(48) $2x + 7y \equiv 5 \pmod{12}$

i.e $2x + 7y - 5 \equiv 0 \pmod{12}$.

Sol^n:-

Here $(2, 7, 12) = 1$ & $1/(-5)$

$\therefore$ given eq^n has $md = 12 \times 1 = 12$ sol^{ns}.

Now, $12 / 2x+7y-5$

$\Rightarrow 2x+7y-5-12z=0 \quad , z \in \mathbb{Z}$

$\Rightarrow 2(x+3y-6z)+y-5=0$

$\Rightarrow 2u+y-5=0 , \quad u=x+3y-6z \quad -(1)$

$\Rightarrow y = 5-2u \quad -(2)$

By (1) $u = x+3(5-2u)-6z$

$\Rightarrow x = 7u+6z-15$

Hence, reqrd sol^{ns} are,

$x \equiv (7u+6z-15) \pmod{12}$

$y \equiv (5-2u) \pmod{12}$

where $u = 0,1,2,\dots,5$ and

$z = 0,1$

(* by thm (90), we say that

$by+c \equiv 0 \pmod m$ has md_1 sol^{ns}. d_1

& $ax+c_1d_1 \equiv 0 \pmod m$ has d_1 sol^{ns}.

Here $m=12$, $(a,m)=d_1$

$\Rightarrow (2,12)=2$

$\therefore d_1=2$ also $d=1$

(99) $6x+15y \equiv 9 \pmod{18}$

sol^n :-

Here $(6,15,18)=3$ & $3/(-9)$

$\therefore$ given eq^n. has $md = 18\times3=54$ sol^{ns}.

Now, $18 / 6x+15y-9$

$\Rightarrow 6x+15y-18z-9=0 , \quad z \in \mathbb{Z}.$

$\Rightarrow 2x+5y-\cancel{18}6z-3=0$

$\Rightarrow 2(x+2y-3z-1)+y-1=0$

Date: / /

$\Rightarrow 2u+y-1=0, \quad u = x+2y-3z-1$

$\Rightarrow y = 1-2u \quad -(1)$

$\Rightarrow u = x+2(1-2u)-3z-1$

$\Rightarrow x = 5u+3z-1 \quad -(2)$

Hence reqrd sol^{ns} are

$x \equiv (5u+3z-1) \pmod{18}$

$y \equiv (1-2u) \pmod{18}$

where $u = 0,1,2,\dots,8$ $\left(\because \frac{m}{d_1}\cdot d = \frac{18}{6}\cdot 3 = 9\right.$

$z = 0,1,2,\dots 5.$ $\quad d_1 = 6$

(50) State and prove Chinese remainder theorem. OR

State & prove Sun-Tsu theorem.

* Statement:-

Let $m_1, m_2, \dots, m_k$ be pairwise relatively prime +ve integers. then the system of congruences $x \equiv a_i \pmod{m_i}$, $\forall i = 1,2,\dots,k$ has a unique sol^n.

$$x \equiv \sum_{i=1}^{k} \frac{m}{m_i} x_i a_i \pmod{m}$$

where $m = m_1 \cdot m_2 \cdot \dots \cdot m_k$ and $\frac{m}{m_i} x_i \equiv 1 \pmod{m_i}$, $\forall i$.

Pf:- Let $m = m_1 \cdot m_2 \cdot \dots m_k$.

$\Rightarrow \frac{m}{m_i} = m_1 \cdot m_2 \cdots m_{i-1} \cdot m_{i+1} \cdots m_k \quad -(1)$

also, clearly $\left(\frac{m}{m_i}, m_i\right) = 1$

By thm. (39), we say that,

$\frac{m}{m_i} x \equiv 1 \pmod{m_i}$ has sol^n say x_i.

Thus. $\frac{m}{m_i} x_i \equiv 1 \pmod{m_i}$, $\forall i = 1, 2, \ldots, k$ —(2)

also by eq^n (1) we say that

$$m_j \Big/ \left(\frac{m}{m_i}\right), \ \forall j \neq i$$

$$\Rightarrow \frac{m}{m_i} \equiv 0 \pmod{m_j}, \ \forall j \neq i.$$

$$\Rightarrow \frac{m}{m_i} a_i x_i \equiv 0 \pmod{m_j}, \ \forall j \neq i.$$

$$\Rightarrow \sum_{\substack{i=1 \\ (i \neq j)}}^{k} \frac{m}{m_i} a_i x_i \equiv 0 \pmod{m_j}$$

$m_j \nmid \frac{m}{m_j}$

$m_j \Big/ \sum_{\substack{i=1 \\ (i\neq j)}}^{k} \frac{m}{m_i} a_i x_i$

$$\Rightarrow \sum_{i=1}^{k} \frac{m}{m_i} a_i x_i \equiv \frac{m}{m_j} a_j x_j \pmod{m_j}$$

$$\Rightarrow \sum_{i=1}^{k} \frac{m}{m_i} a_i x_i \equiv a_j \pmod{m_j}, \ \forall j = 1, 2, \ldots k$$

(by (2))

$g \Big/ \sum_{i=1}^{k} \frac{m}{m_i} a_i x_i - \frac{m}{m_j} a_j x_j$

Thus, $\sum_{i=1}^{k} \frac{m}{m_i} a_i x_i$ is a sol^n of given system

Hence,

$$x \equiv \sum_{i=1}^{k} \frac{m}{m_i} a_i x_i \pmod{m_j}, \ \forall j = 1, 2, \ldots k$$

Hence, $x \equiv \sum_{i=1}^{k} \frac{m}{m_i} a_i x_i \pmod{m}$ is reqrd sol^n

$\left(\because \ m_1 / x-p, \ m_2 / x-p, \ \ldots, \ m_k / x-p\right.$

$\Rightarrow m_1 \cdot m_2 \cdots m_k / \ldots \Rightarrow m / x-p$

p.t.o.

Now, we prove uniqueness.

If x and y are two sol^{ns} of given system then, $x \equiv a_i \pmod{m_i}$

$y \equiv a_i \pmod{m_i}$, $\forall i = 1, 2, \ldots k$

$\Rightarrow x \equiv y \pmod{m_i}$, $\forall i = 1, 2, \ldots, k$

$\Rightarrow x \equiv y \pmod{m}$.

Hence given system has unique sol^n.

* Solve the following system of congruences.

(51) $x \equiv 2 \pmod 3$; $x \equiv 3 \pmod 5$; $x \equiv 2 \pmod 7$.

Sol^n:-

Here, $a_1 = 2$, $a_2 = 3$, $a_3 = 2$

$m_1 = 3$, $m_2 = 5$, $m_3 = 7$.

$\therefore$ All m_i $(i = 1, 2, 3)$ are pairwise relatively prime

Now $m = m_1 \cdot m_2 \cdot m_3$

$= 3 \cdot 5 \cdot 7 = 105$.

also, $\frac{m}{m_1} = \frac{105}{3} = 35$,

$\frac{m}{m_2} = \frac{105}{5} = 21$

$\frac{m}{m_3} = \frac{105}{7} = 15$.

Since $\frac{m}{m_i} x_i \equiv 1 \pmod{m_i}$, $\forall i = 1, 2, 3$.

$\Rightarrow 35x \equiv 1 \pmod 3$.

$21x \equiv 1 \pmod 5$

$15x \equiv 1 \pmod 7$

Date: 1/7/

Thus $3 / 35x-1$

which is satisfied by $x_1 = 2$

$5 / 21x-1$

which is satisfied by $x_2 = 1$

& $7 / 15x-1$

which is satisfied by $x_3 = 1$.

Hence by Chinese remainder theorem we say that,

required solⁿ is,

$$x \equiv \sum_{i=1}^{3} \frac{m}{m_i} x_i a_i \pmod m$$

$$\Rightarrow x \equiv [(35 \times 2 \times 2) + (21 \times 1 \times 3) + (15 \times 1 \times 2)] \pmod{105}$$

$$\Rightarrow x \equiv 233 \pmod{105}$$

$$\Rightarrow x \equiv 23 \pmod{105}.$$

(52) $2x \equiv 1 \pmod 5$

$3x \equiv 1 \pmod 7$.

Sol^n:-

Here $5 / 2x-1$ & $7 / 3x-1$

which are satisfied by $x = 3$ & $x = 5$ respect.

$\therefore$ given system is equivalent to,

$$x \equiv 3 \pmod 5$$

$$x \equiv 5 \pmod 7$$

Date: / /

$a_1 = 3$, $a_2 = 5$, $m_1 = 5$, $m_2 = 7$, which pairwise relatively prime

$\therefore m = 35$.

also, $\frac{m}{m_1} = 7$, $\frac{m}{m_2} = 5$.

since,

$$\frac{m}{m_i} x_i \equiv 1 \pmod{m_i}, \quad i = 1, 2$$

$\Rightarrow 7x \equiv 1 \pmod 5$

$5x \equiv 1 \pmod 7$.

Now, $5 / 7x - 1$ & $7 / 5x - 1$

which are satisfied by $x_1 = 3$ & $x_2 = 3$ respectively

Hence by Chinese theorem,

reqrd sol^n is,

$$x \equiv \sum_{i=1}^{2} \frac{m}{m_i} x_i a_i \pmod m \ldots\ldots$$

$\Rightarrow x \equiv [(7 \times 3 \times 3) + (5 \times 3 \times 5)] \pmod{35}$

$\Rightarrow x \equiv 138 \pmod{35}$

x $[\Rightarrow x \equiv 68 \pmod{35}]$. x

$\Rightarrow x \equiv 33 \pmod{35}$.

(53) $x \equiv 1 \pmod 4$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

Sol :- $a_1 = 1,\ a_2 = 3,\ a_3 = 2$

$m_1 = 4,\ m_2 = 5,\ m_3 = 7$

which are pairwise relatively prime

Now, $m = 140$

$\therefore \frac{m}{m_1} = 35,\ \frac{m}{m_2} = 28,\ \frac{m}{m_3} = 20$

Since,

$$\frac{m}{m_i} x_i \equiv 1 \pmod{m_i},\ i = 1, 2, 3$$

$$\Rightarrow 35x \equiv 1 \pmod 4$$

$$28x \equiv 1 \pmod 5$$

$$20x \equiv 1 \pmod 7$$

Now,

$$4 \,/\, 35x-1,\quad 5 \,/\, 28x-1,\quad 7 \,/\, 20x-1$$

which are satisfied by $x_1 = \cancel{4}\,3$, $x_2 = 2$, $x_3 = 6$ resp.

$\therefore$ By Chinese thm, reqrd soln is,

$$x \equiv \sum_{i=1}^{3} \frac{m}{m_i} x_i a_i \pmod m$$

$$\Rightarrow x \equiv [(35 \times \cancel{4\times1}\,3) + (28 \times 2 \times 3) + (20 \times 6 \times 2)] \pmod{140}$$

$$\Rightarrow x \equiv \cancel{548}\,513 \pmod{140}$$

$$\Rightarrow x \equiv 93 \pmod{140}$$

Page No.:
Date: / /

(54) $x \equiv -2 \pmod{12}$
$x \equiv 6 \pmod{10}$
$x \equiv 1 \pmod{15}$.

Sol^n:-

Here, $(m_i, m_j) \neq 1$, $\forall i,j$.
we can write given system as,

$x \equiv -2 \pmod 4$
$x \equiv -2 \pmod 3$.

$x \equiv 6 \pmod 5$
$x \equiv 6 \pmod 2$

$x \equiv 1 \pmod 5$
$x \equiv 1 \pmod 3$.

Thus given system is equivalent to,

$x \equiv 2 \pmod 4$
$x \equiv 1 \pmod 3$
$x \equiv 1 \pmod 5$
$x \equiv 0 \pmod 2$

Since, $x \equiv 2 \pmod 4$ & $x \equiv 0 \pmod 2$ are satisfied by $x = 2$.

$\therefore x \equiv 2 \pmod{[4,2]}$

$\therefore x \equiv 2 \pmod 4$.

Thus given system is equivalent to

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

$a_1 = 2, \quad a_2 = 1, \quad a_3 = 1$

$m_1 = 4, \quad m_2 = 3, \quad m_3 = 5. \quad \therefore m = 60$

also, $\frac{m}{m_1} = 15, \quad \frac{m}{m_2} = 20, \quad \frac{m}{m_3} = 12.$

Since,

$$\frac{m}{m_i} x_i \equiv 1 \pmod{m_i}, \ \forall i = 1, 2, 3$$

$$\Rightarrow 15x \equiv 1 \pmod{4}$$
$$20x \equiv 1 \pmod{3}$$
$$12x \equiv 1 \pmod{5}$$

$$4 / 15x - 1, \quad 3 / 20x - 1, \quad 5 / 12x - 1$$

$$\Rightarrow x_1 = 3, \quad x_2 = 2, \quad x_3 = 3.$$

Hence by Chinese thm,

$$x \equiv \sum_{i=1}^{3} \frac{m}{m_i} x_i a_i \pmod{m}$$

$$\Rightarrow x \equiv [(15 \times 3 \times 2) + (20 \times 2 \times 1) + (12 \times 3 \times 1)] \pmod{60}$$

$$\Rightarrow x \equiv 166 \pmod{60}$$

$$\Rightarrow x \equiv 46 \pmod{60}$$

Date: / /

(55) State and prove Wilson's theorem.

→ Statement:-

The integer 'p' is prime iff
$(p-1)! + 1 \equiv 0 \pmod{p}$.

Proof:- If p is prime then by Euler's theorem,

we say that,

every integer x which is relatively prime to p is sol^n of $x^{p-1} \equiv 1 \pmod{p}$.

clearly it has total $p-1$ different sol^{ns} $1, 2, \ldots, p-1$.

p is prime $\phi(p) = p-1$

Hence,

$x \equiv 1, 2, \ldots, p-1 \pmod{p}$

are sol^{ns} of $x^{p-1} \equiv 1 \pmod{p}$

also, we can write,

$x^{p-1} - 1 \equiv 0 \pmod{p}$

$\therefore x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-(p-1)) \pmod{p}$

for ~~putting~~ $x = 0$, we get

$-1 \equiv (-1)(-2)\cdots(-(p-1)) \pmod{p}$.

$\Rightarrow -1 \equiv (-1)^{p-1} (p-1)! \pmod{p}$ — (1)

If p is even prime

i.e. $p = 2$ then

$1 + 1 \equiv 0 \pmod{2}$

i.e. $(p-1)! + 1 \equiv 0 \pmod{p}$, if $p = 2$

If p is odd prime then $p-1$ is even no.

$\therefore$ by eq^n (1) we get

$-1 \equiv (p-1)! \pmod p$

$\Rightarrow (p-1)! \equiv -1 \pmod p$

$\Rightarrow (p-1)!+1 \equiv 0 \pmod p$, if p is odd prime

* Converse part:-

If $(p-1)!+1 \equiv 0 \pmod p$ then we have to p.t. p is prime integer

Suppose p is not prime. then we can write,

$p = q \cdot q_1$ for $1 < q, q_1 < p$.

Now, $(p-1)! = 1 \cdot 2 \cdot 3 \cdots q(q+1) \cdots (p$

$(q<p)$

$\Rightarrow q / (p-1)!$

$\Rightarrow (p-1)! \equiv 0 \pmod q$

$\Rightarrow (p-1)!+1 \equiv 1 \pmod q$ —(1)

Similarly we can prove,

$(p-1)!+1 \equiv 1 \pmod{q_1}$ —(2)

By (1) & (2)

$(p-1)!+1 \equiv 1 \pmod p$ $(\because p = qq_1)$ $(q,q_1)=$

$\times$

$(\because (p-1)!+1 \equiv 0 \pmod p)$

Hence p must be prime.

— x —

Conversly if,

$$(p-1)!+1 \equiv 0 \pmod{p} \quad \text{---} (*)$$

then we have to p.t. p is prime

Suppose p is not prime.

Let q be a proper factor of p

Since $1 < q < p$ i.e. $q \leq p-1$,

q occurs as one of the factor in $(p-1)!$

i.e $q / (p-1)!$

$\Rightarrow (p-1)! \equiv 0 \pmod{q}$

which contradicts (*)

$\because$ by (*) $p / [(p-1)!+1]$

$\Rightarrow q / [(p-1)!+1]$

$\Rightarrow (p-1)!+1 \equiv 0 \pmod{q}$

$\therefore$ Our supposition is wrong

Hence p must be prime.