INDEX

NAME ______ STD ______ SEC ______ ROLL NO ______

S.No.	Date	Title	Page No.	Teacher's Sign/ Remarks

$\tau(n)$ = The no. of the divisions of n.
$\sigma(n)$ = The sum of the division of n.
$\phi(n)$ = No. of integer less than n relatively prime to n.

Kalika
Number Theory

$\tau(1) = 1$
$\sigma(1) = 1$
$\mu(1) = 1$
$\phi(1) = 1$

$$n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_r^{k_r}$$

$$\tau(n) = (k_1+1)(k_2+1)\cdots(k_r+1)$$

$$\sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1}$$

$$\phi(n) = n\left(1-\tfrac{1}{p_1}\right)\left(1-\tfrac{1}{p_2}\right)\cdots\left(1-\tfrac{1}{p_r}\right)$$

$$\sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1} \times \frac{p_2^{k_2+1}-1}{p_2-1} \times \cdots \times \frac{p_r^{k_r+1}-1}{p_r-1}$$

$$\phi(p) = p-1.$$

Ch-2 — 5-17 (10-17)
Ch-3 - 18 — 21 (21-22)
Ch-4 — 22 — 59
Lin. Cong - 35, Chinese - 42, Decimal - 56
Ch-5 — 60 — 69
Ch-6 — 70 —

5 5.2 - 200
5.3 - 192
6. 6.1 - 206
6.2 - 188
6.3 - 203
7 7.2 - 185
7.3
7.4
8 8.1
8.2
8.3

Slect 1Tut

I Linear Diophantine Eqn, Prime Counting function Statement of prime no. thm, Goldbach conjecture, Linear congruences, complete set of Residues, Chinese Remainder theorem, Fermat's little thm, Wilson theorem.

Ref:
[1] Ch-2 (2.5), Ch-3 (3.3), Ch-4 (4.2, 4.4), Ch-5 (sec-5, excluding pseudoprimes, 5.3)
[2] Ch-3 (3.2)

II Number theoretic functions, Sum & no. of divisors, totally multiplicative functions, Def^n & Properties of the Dirichlet product, the Möbius inversion formula, the greatest integer function, Euler's phi-function, Euler's thm. Reduced set of Residues, Some properties of Euler's phi-function.

Ref: [1] Ch-6 (6.1-6.3), Ch-7
[2] Ch-5 (5.2 (Def^n 5.5- Thm 5.10), 5.3 (Thm - 5.15-5.17, 5.19))

III Order of an integer modulo n, primitive roots for primes, composite nos having primitive roots, Euler's Criterion, the Legendre symbol and its properties, Quadratic reciprocity, Quadratic congruences with composite moduli. Public key encryption, RSA encryption & decryption, the eq^n $x^2+y^2=z^2$, Fermat's little theorem.

Ref [1] Ch-8 (8.1-8.3), Ch-9, Ch-10 (10.1), Ch-12

[1] David M. Burton (Elementary NT 6Ed) TMH
[2] Neville Robinns. (Beginning NT, 2Ed) Narosa Pub.

Guidelines

Ch-2, 2.5, Q 1,2,3, 6,7

Ch-3, 3.3, Q 6,10

Ch-4, 4.2, Q 2,4, 6, 10, 5, 11, 12

4.4 → 4.7, 4.8, 4.9 with pfs

Q 1,2,4,5,6,7,11,12,17,18

Ch-5, 5.2, Fermat's little thm, lemma on p89

Delete thm 5.2, 5.3,

Q. 1,2,3,4,5,6,7,10,11,12,13,14

5.3, Wilson's thm, 5.2, 5.3, 5.4 thm

Q. 1,2,3,4,5,6,7,9,10(a)

Ch-6. 6.1 All thms

Q. 7,8, 9,16

6.2, Q. 1,3,4,6

6.3, thm 6.11 statement only.

Q 1, 2(i), 3, 5(a)

Ch-7, 7.2 thm 7.2 statement only.

Q - 1,3,4,6, 8, 13, 14, 16

7.3, Q 1,4,5,7, 10, 12, 13

7.4, Q 2,3,4,5,8, 16

Ch-8, 8.1 - 1,3,11

8.2, 8,9,10,11,12

8.3, Statement of lemma 1,2, Q

thm 8.9, 8.10

8.4

Ch 9 9.1 Q, 1,4, 12 (1,4, 12)

9.2 Statement of lemma on p 193, thm 9.7, 9.8

Q. 1,2,5

9.3 Q, 1.4.5, 9.11, 1,2

Ch-10, Q - 1,2, 3, 7,8, 12, 13

Ch-12, 12.1 pf of only thm 12.1, Rest Results without Pfs, Q = 1,2,4

Ch - 12.2, statement of thm, 12.3, 12.4 Q 12.5

Q. 1

Ref [2]: Ch-5 Defn 5.5, 5.6. Prop. of Dirichlet thm 5.3, 5.4

Prime counting fn without pfs & Prime Num thm

:- let a and b be two integer

$$a = qb + r$$

where $q \le r \le b$

where q, r are called constant and Remainder.

$a|b$ (a divides b)

b is divisible by a.

for example

$4|12$, $3|6$, $2|8$

Theorem: let 'a', 'b', 'c' and 'd' be integers, then —

(i) $a|1 \iff a = \pm 1$

(ii) $a|b \iff b|c \implies a|c$

(iii) $a|c \iff$ and $b|d \implies ab|cd$

(iv) $a|b$ and $b|a \iff a = \pm b$

(v) $a|b$ with $b \ne 0$

then $|a| \le |b|$

(vi) $a|b$ and $a|c$

$\implies a | bx + cy \quad \forall\ x, y \in \mathbb{Z}$

* G.C.D :- let 'a' & 'b' be two integer then the gretest common divisior is the integer 'd' if it satisfy the following two property —

(i) $d|a$ and $d|b$

(ii) if $c|a$ and $c|b$

$\implies c \le d$

for any given integer a and b.

$\exists$ integers x & y s.t.

$$\boxed{\gcd(a,b) = ax+by}$$

* PRIME NUMBER

Any No. $p>1$ is called a prime no. if it have two positive division.

* COMPOSITE NUMBER

Any number $n>1$, which is not a prime is called composite number

RELATIVELY PRIME

Two numbers a & b are called relatively prime.

$$\boxed{\gcd(a,b) = 1}$$

Corollary: let a and b be reletively prime then $\exists$ integer x and y s.t

$$ax+by=1$$

Result: (i) If $\gcd(a,b) = 1$, then

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

(ii) If $a|bc$ with $\gcd(a,b)=1$ then $a \nmid c$

(iii) If $ab \nmid c$ with $\gcd(a,c)=1$ then $b \nmid c$

* **LCM:-** let a and b be two integer then the least common multiple of a & b is the integer 'm'.

If it satisfy following two property:—

(i) if a/m and b/m

(ii) if a/n and b/n

Result: for any two following integer a and b

$$\boxed{\operatorname{lcm}(a,b) * \gcd(a,b) = ab}$$

Theorem: DIOPHANTINE EQUATION

The simplest type of Diophantine Equation that we shall consider is the linear Diphantine in two unknowns.

$$ax+by=c$$

has a sol^n iff $d|c$

where $d = \gcd(a,b)$

If x_0 & y_0 is an particular sol^n of this eq^n then all other solution are given by

$$\boxed{x = x_0 + \left(\frac{b}{d}\right)t}$$

&

$$\boxed{y = y_0 - \left(\frac{a}{d}\right)t}$$

where d is an arbitrary.

Proof: let us suppose that x_0 & y_0 is an known sol^n of the given equation and let x' and y' be any other sol^n of the given eq^n then —

$$ax_0 + by_0 = c = ax' + by'$$

$$\Rightarrow a(x_0 - x') = b(y' - y_0) \quad \text{—(i)}$$

As $\gcd(a,b) = d$, $\exists\ r, s \in \mathbb{Z}$ s.t $\gcd(r,s) = 1$ & $a = dr$, $b = ds$

putting this in (1) we get –

$$dr(x_0 - x') = ds(y' - y_0)$$

$$\Rightarrow r(x_0 - x') = s(y' - y_0) \quad \text{—— (2)}$$

$$\Rightarrow r \mid s(y' - y_0) \Rightarrow r \mid (y_0 - y')$$

[$\because \gcd(r, s) = 1$]

$\Rightarrow (y_0 - y') = rt$ for $t \in \mathbb{Z}$

$$\Rightarrow y' = y_0 - rt$$

$$\Rightarrow y' = y_0 - \frac{a}{d}t \quad \text{—— (3)}$$

Also from (2) & (3) –

$$\Rightarrow r(x' - x_0) = rst$$

$$\Rightarrow x' = x_0 + st$$

$$x' = x_0 + \frac{b}{d}t$$

thus

$$\boxed{\begin{aligned} x' &= x_0 + \frac{b}{d}t \\ y' &= y_0 - \frac{a}{d}t \end{aligned}} \quad , t \in \mathbb{Z}$$

Exercise

1, 2(c), 3(c), 6, 7

Conversely $\Leftarrow$

$d|c \Rightarrow c = dt$ for any $t \in \mathbb{Z}$ — (2)

$gcd(a,b) = ax_0 + by_0$

$\Rightarrow d = ax_0 + by_0$

for eqn (2) —

$c = dt = (ax_0 + by_0)t$

$\Rightarrow a(tx_0) + b(ty_0) = c$

$\Rightarrow$ the diophantine eqn $ax + by = c$ has a soln $x = tx_0, y = ty_0$

Problem 2.5 (p-387)

1 (a) $6x + 51y = 22$

$gcd(a,b) = 3$

$\Rightarrow 3 \nmid 22$

$\Rightarrow$ this eqn can't be solved

2 (c) $221x + 35y = 11$

$gcd(221, 35) = 1$ & $1 | 11$

$\Rightarrow$ this eqn has solution.

$221 = 6 \times 35 + 11$

$35 = 3 \times 11 + 2$

$11 = 5 \times 2 + 1$

$\Rightarrow 1 = 11 - 5 \times 2$

$= 11 - 5(35 - 3 \times 11)$

$= 16.11 - 5.35$

$= 16(221 - 6 \times 35) - 5(35)$

$= 16.221 - 101.35$

$\Rightarrow 11 = 11.16.221 - 11.101.35$

$= 176.221 + (-1111)35$

$\therefore x_0 = 176$ & $y_0 = -1111$

$\therefore y = y_0 - \left(\frac{a}{d}\right)t$, $x = x_0 + \left(\frac{b}{d}\right)t$

$y = -1111 - \left(\frac{221}{1}\right)t$

Result: If any diophantine eqn has a soln then it has infinitely many soln

$x = 176 + 35t$

$y = -1111 - 221t$ where $t \in \mathbb{Z}$

Q.3(c) $123x + 360y = 99$

find all solns in the positive integers

given condition $x > 0, y > 0$

$gcd(123, 360) = 3$ & $3 | 99$

$\Rightarrow$ this eqn has soln

$360 = 2 \times 123 + 114$

$123 = 1.114 + 9$

$114 = 12 \times 9 + 6$

$9 = 1.6 + 3$

$\Rightarrow 3 = 9 - 6$

$= -(114 - 12 \times 9) + 9$

$= 13.9 - 114$

$123)\,360\,(2$
246
$114)\,123\,(1$
114
$9)\,114$

$= 13 \cdot (123 - 114) - 114$

$= 13 \cdot 123 - 14 \cdot 114$

$= 13 \cdot 123 - 14(360 - 2 \cdot 123)$

$3 = 41 \cdot 123 - 14 \cdot 360$

$\Rightarrow 99 = 3 \cdot 33 = \underline{41 \cdot 33} \cdot 123 - \underline{14 \cdot 33} \cdot 360$

$= 1353 \cdot 123 - 462 \cdot 360$

Here $x_0 = 1353$ & $y_0 = -462$

$\therefore x = 1353 + \left(\frac{360}{3}\right)t$

$= 1353 + 120t$

& $y = -462 - \left(\frac{123}{3}\right)t$ $\quad \forall t \in \mathbb{Z}$

$= -462 - 41t$

for positive solⁿ $x > 0$ & $y > 0$

$1353 + 120t > 0$ & $-462 - 41t > 0$

$\Rightarrow -1353 < 120t$ & $-462 > 41t$

$\Rightarrow t > \frac{-1353}{120}$ & $\frac{-462}{41} > t$

$\Rightarrow t > -11.27$ & $t < -11.268$

$-11.275 < t < -11.268$

& $t \in \mathbb{Z}$

$\Rightarrow$ t has no value

$\Rightarrow$ the given diophantine eqⁿ has no positive solⁿ.

(P 37)

(3)(d) $158x - 57y = 7$

Results (i) The diaphantine eqⁿ $ax + by = c$ has a solⁿ $\Leftrightarrow$ the diophanthe eqⁿ $ax - by = c$ has a solⁿ.

Suppose $ax + by = c \rightarrow (x_0, y_0)$

$\therefore ax - by = c \rightarrow (x_0, -y_0)$

(ii) The diophantine eqⁿ $ax - by = c$ has a solⁿ iff $\gcd(a,b) \mid c$

(iii) If the Diophantine eqⁿ $ax + by = c$ has a solⁿ (x_0, y_0) the all solⁿ of the Diophantine eqⁿ $ax - by = c$ are given by

$$x = x_0 + \left(\frac{b}{d}\right)t$$

$$-y = -\left[y_0 - \left(\frac{a}{d}\right)t\right]$$

where $d = \gcd(a,b)$ & $t \in \mathbb{Z}$

verify for $ax - by = c$

$= ax_0 + by_0 = c$

for eg $a = 158$, $b = 57$, $c = 7$ | $\gcd(158, 57) = 1$ & $1 \mid 7$

first we will solve

$158 + 57y = c$

so $158 = 57 \cdot 2 + 44$

$57 = 1 \cdot 44 + 13$

$57 \overline{)158}(2$
114
$44)57$

Page No. 14 Date 16/1/15

$44 = 3\cdot 13 + 5$

$13 = 2\cdot 5 + 3$

$5 = 1\cdot 3 + 2$

$3 = 1\cdot 2 + 1$

$\Rightarrow 1 = 3 - 1\cdot 2$

$= 3 - 1\cdot(5 - 1\cdot 3)$

$= 2\cdot 3 - 1\cdot 5$

$= 2\cdot(13 - 2\cdot 5) - 1\cdot 5$

$= 2\cdot 13 - 5\cdot 5$

$= 2\cdot 13 - 5(44 - 3\cdot 13)$

$= 17\cdot 13 - 5\cdot 44$

$= 17\cdot(57 - 44) - 5\cdot 44$

$= 17\cdot 57 - 22\cdot 44$

$= 17\cdot 57 - 22(158 - 57\cdot 2)$

$= 61\cdot 57 - 22\cdot 158$

$\Rightarrow 1\cdot 7 = 7\cdot 61\cdot 57 - 22\cdot 7\cdot 158$

$= 427\cdot 57 - 154\cdot 158$

$\Rightarrow 7 = (-154)\cdot 158 + (427)\cdot 57$

$\therefore$ The Diophantine eqn has a soln

$x_0 = -154$

& $y_0 = 427$

$\rightarrow$ All soln of given Diophantine eqn are given by

$\therefore x = x_0 + \left(\frac{b}{d}\right)t = -154 + 57t$

$y = -\left(y_0 - \left(\frac{a}{d}\right)t\right) = -427 + 158t$

$t \in \mathbb{Z}$.

$\therefore$ for positive soln —

$-154 + 57t > 0$ & $-427 + 158t > 0$

$t > \frac{154}{57} = 2.702$ & $t > \frac{+427}{158}$

$t < 2.702$

$t \in \mathbb{Z}$

Page No. 15

$\Rightarrow t \geq 3$

$\therefore$ All positive soln of Diophantine eqn $158x - 57y = 7$ are given by

$x = -154 + 57t = -154 + 171 = 17$

$y = -427 + 158t = -427 + 474 = 47$

Q.6 A farmer purchased 100 head of livestock for a total cost of \$4000. Prices were as follow: calves \$120 each; lambs \$50 each; piglets \$25 each. If the farmer obtained at least one animal of each type, how many of each did he buy?

Soln: Let the farmer buy x calves, y lambs & z piglets

then $120x + 50y + 25z = 4000$ —(1)

$x + y + z = 100$ —(2)

$x > 0, y > 0, z > 0$

$\gcd(120, 50, 25) = 5$

from eqn (2) $z = 100 - x - y$

using it in eqn (1), we have —

$120x + 50y + 25(100 - x - y) = 4000$

$\Rightarrow 95x + 25y = 4000 - 2500 = 1500$

$\Rightarrow 19x + 5y = 300$

$x, y > 0$

$\gcd(19,5)=1$,

$19 = 3\cdot 5 + 4$

$5 = 1\cdot 4 + 1$

$\Rightarrow 1 = 5 - 1\cdot 4$

$= 5 - 1\cdot(19 - 3\cdot 5)$

$= 4\cdot 5 - 1\cdot 19$

$300\cdot 1 = 300\cdot 4\cdot 5 - 300\cdot 1\cdot 19$

$\Rightarrow$ The Diophantine eqn $19x + 5y = 300$ has a soln

$x_0 = -300$ & $y_0 = 1200$

$\therefore$ All soln of the given Diophantine eqn is given by

$\Rightarrow x = x_0 + \left(\frac{b}{d}\right)t$

$= -300 + 5t$

& $y = y_0 - \left(\frac{a}{d}\right)t = 1200 - 19t$

$\therefore$ for positive soln $(x>0, y>0)$

$-300 + 5t > 0$ & $1200 - 19t > 0$

$\Rightarrow 5t > \frac{300}{5} = 60$ & $t < \frac{1200}{19} = 63.157$

$60 < t < 63.157$

$\Rightarrow t = 61, 62, 63$

$\therefore$ for $t = 61$ | $t = 62$ | $t = 63$

$x = -300 + 305 = 5$

$y = 1200 - 1159 = 41$

$\Rightarrow x = 5$, $y = 41$, $z = 54$

$x = 10$, $y = 22$, $z = 68$

(7) When Mr. Smith cashed a cheek at his bank, the teller mistook the no. of cents for the no of dollars and vice versa. Unaware of this Mr. Smith spent 68 cents and then noticed to his surprise that he had twice the amount of the original check. Determine the smallest value for which the check could have been written.

Soln Let x denotes the no. of dollars & y denotes the no of cents, then

$1\$ = 100$ cent

$x\$$ & y cent | $y\$$ & x cent

$100x + y$, | $100y + x$

then $2(100x + y) = 100y + x - 68$

$\Rightarrow 199x - 98y = -68$

$\gcd(199, -98) = 1$

given condition $y > 0$ & $y < 100$

Ans $x\$$ & y cent

for this solve the eqn $199x + 98y = +68$

$\therefore 1 = \cancel{199 - 98}$ $3-2$

$199 = 98\times 2 + 3$

$98 = 3\times 32 + 2$

$32 = 16\times 2 + 0$

$98)\,199\,(2$ 196

$3)\,98\,(32$ 96

$2)\,3\,(1$

(only 3.3) Chapter - 3

The Theory of congruence

$a \equiv b \pmod{n} \Rightarrow n \mid a-b$

$\Rightarrow a-b = kn$ for some $k \in \mathbb{Z}$

Theorem let a & b be two integer than and p be prime number

(i) if $p \mid ab \Rightarrow p \mid a$ or $p \mid b$

(ii) if $p \mid a+b \Rightarrow p \mid a$ & $p \mid b$

(iii) If $p \mid a_1 a_2 \cdots a_k \Rightarrow p \mid a_i$ for some $1 \le i \le k$

(iv) If $p_1, p_2, \ldots p_k$ are primes and $p \mid p_1 p_2 \cdots p_k \Rightarrow p = p_i$ for some $1 \le i \le k$

Fundamental theorem of Arithematic

Every integer $n > 1$ is either prime or a product of prime thus we representation is unique upto to the order in which the factors occurs.

Canonical form of positive integer

Any positive integer $n > 1$ can be written as uniqually in canonical form.

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

where $k_1, k_2, \ldots k_r$ ~~are integer~~ $\in \mathbb{Z}$

$p_1, p_2, p_3 \ldots p_r$ are primes s.t

$p_1 < p_2 < p_3 < \cdots < p_r$

for example:

$72 = 2^3 \times 3^2$

$= 2 \times 2 \times 2 \times 3 \times 3$

$= 2 \times 3 \times 3 \times 2 \times 2$

Example:

$9216 = 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 3 \times 3$

$= 2^{10} \cdot 3^2$

Theorem $\sqrt{2}$ is an irrational number.

Proof: let $\sqrt{2}$ be an irrational no.

$\sqrt{2} = \frac{a}{b}$, where $b \neq 0$ and $\gcd(a,b) = 1$.

$\Rightarrow \exists$ integer x and y s.t

$ax + by = 1$

$\Rightarrow \sqrt{2} = \sqrt{2}(ax + by)$

$= (\sqrt{2}a)x + (\sqrt{2}b)y$

$= 2bx + ay \in \mathbb{Z}$

$\sqrt{2} = \frac{a}{b}$

$\Rightarrow 2 = \frac{\sqrt{2}a}{b}$

$\sqrt{2}a = 2b$

$\Rightarrow \sqrt{2}$ is an integer

which is a contradiction.

Prime Counting function

: let x be Any positive integer, then the prime counting function defined by 'πx' Counts the no. of primes less than equal to x.

$$\boxed{\pi(x) = \text{no. of primes} \le x}$$

Example: $\pi(10) = 4$ $(2, 3, 5, 7, \le 10)$

$\pi(30) = 10$ $(2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \le 30)$

Asymptetically Equivallent functions

let $f(x)$ and $g(x)$ be two f^ns defined for $x > 0$. then $f(x)$ is said to Asymptetically equivalent to $g(x)$

or (Any $f(x)$ is asymptotic to $g(x)$)

if $\boxed{\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1}$

or $f(x) \sim g(x)$

for example

$\lim_{x\to\infty} \frac{\sin(1/x)}{1/x}$, $\sin 1/x \sim 1/x$

Example $\lim_{x\to\infty} \frac{1+1/x}{1-1/x}$, $1+1/x \sim 1-1/x$

or $\boxed{\cancel{\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1}}$

Prime Number Theorem:

The prime counting function is assympt-otetic to the function to $x/\log x$.

i.e $\boxed{\pi(x) \sim \frac{x}{\log x}}$

$\boxed{\lim_{x\to\infty} \frac{\pi(x)}{x/\log(x)} = 1}$

Euclid Theorem:

There are infinity many primes:

Proof: let $P_1, P_2, \ldots P_n$ be any prime no s.
Now, consider the number
$N = P_1 P_2 \ldots P_n + 1$
Since $P_1 P_2 \ldots P_n$ are the only primes no.
so, N must be composite number
let p be a prime no. s.t $p \mid N$

$\Rightarrow p \mid (P_1 P_2 P_3 \ldots P_n + 1)$ — (1)

$\because P_1, P_2, \ldots P_n$ are only primes

$\Rightarrow P = P_i$ for some $1 \le i \le n$

$\Rightarrow P \mid P_1 P_2 \ldots P_n$ — (2)

from (1) & (2) —

$P \mid n$ (contradiction)

So, there are infinitely many prime number

The Goldbach conjecture

The Goldbach Conjecture says that an even no. $n \geq 2$ can be written as sum of two primes.

or Any even no. $n > 4$ can be written as sum of two odd prime

Example
$4 = 2+2$
$6 = 3+3$
$14 = 7+7 = 3+11$
$16 = 3+13$ or $5+11$

Twin Prime

A pair of primes are called to twin prime.

Q 6 PT the Goldbach conjecture that every even integer ≥ 2 is the sum of two primes is equivalent to the statement that every integer > 5 is the sum of three primes.

Sol: for $n > 2$ consider

8, 6, 10

Ex - 3.3

Page No. 21 Date 19|01|15

$2n-2 = P_1 + P_2$

$\Rightarrow 2n = P_1 + P_2 + 2$ —— (1)

$\Rightarrow$ every even integer (>5) can be written as sum of three primes

from eq^n (1)

$2n+1 = P_1 + P_2 + 3$

$\Rightarrow$ every odd integer (>5) can be written as sum of three primes.

$\Leftarrow$ Suppose every integer >5 is the sum of three primes $\forall\ n > 3$.

$2n = P_1 + P_2 + P_3$ —— (1)

$\because$ L.H.S the even no.

~~Since the~~ So, on the the R.H.S, at least one of P_i must be even prime & 2 is the only even prime.

So let $P_3 = 2$

from (1), $2n = P_1 + P_2 + 2$

$\Rightarrow 2(n-1) = P_1 + P_2$

$\Rightarrow$

This shows that every integer >5 ~~can~~ ~~can~~ is the sum of three primes

Post

(10)

$n > 2 \Rightarrow (n+1) > 3$ $\qquad (n+1)! - (n+1)$

So $(n+1)! = (n+1)n(n-1)\ldots 3.2.1$

$\Rightarrow 2 \mid \{(n+1)! - 2\}$

$3 \mid \{(n+1)! - 3\}$

$\vdots$

$n \mid \{(n+1)! - n\}$

$(n+1) \mid \{(n+1)! - (n+1)\}$

Produces n consecutive composite integer for $n > 2$.

This shows that $(n+1)! - 2$, $(n+1)! - 3$, ——

CHAPTER - 4

Page No. 22 Date 21|01|15

$\pi(x) =$ no. of primes $\leq x$

Read

$\pi(x) \sim \dfrac{x}{\log x}$

as $x \to \infty$, $\pi(x) = \dfrac{x}{\log x}$

$\pi(10), \pi(100), \pi(1000)$

$\pi(10^{10}), \quad \pi(10^{12})$

$10^{10}, 10^{12}, \ldots \to \infty$

$\pi(10^{10}) = \dfrac{10^{10}}{\log_e 10^{10}}$

$= \dfrac{10^{10}}{10 \cdot 2.303}$

Chapter - 4 (only 4.2 & 4.4)

The Theory of Congruence

$a \equiv b \pmod n$

$\Rightarrow n \mid a-b \Rightarrow a-b = kn$ for some $k \in \mathbb{Z}$

Theorem 4.2

Let $n > 1$ be fixed. And a, b, c, d be arbitrary integers. then following property holds.

(a) $a \equiv a \pmod n$

$n \mid 0$ ($=0$) $\Rightarrow n \mid a-a \Rightarrow a \equiv a \pmod n$

(b) If $a \equiv b \pmod n$, then $b \equiv a \pmod n$

$a-b = kn$ $\quad (n \mid (a-b))$

Page No. 23
Date 21 01 15

$n \mid (a-b) \Rightarrow n \mid -(a-b)$

$\Rightarrow n \mid b-a$ $\quad \left[\because n>1 \text{ so } n \nmid -1\right]$

$\Rightarrow b \equiv a \pmod n$

(iii) If $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$

$\left.\begin{array}{l} n \mid a-b \\ \& \; n \mid b-c \end{array}\right\} \Rightarrow n \mid (a-b)+(b-c) = a-c$

$\Rightarrow n \mid a-c$

$\Rightarrow a \equiv c \pmod n$

(iv) If $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then $a+c \equiv b+d \pmod n$ and $ac \equiv bd \pmod n$.

$n \mid a-b$ and $n \mid c-d$

$\Rightarrow \cancel{n \mid a+c+c-b}$

$\Rightarrow n \mid a-b+c-d$

$\Rightarrow n \mid (a+c)-(b+d)$

$\Rightarrow a+c \equiv b+d \pmod n$

And $n \mid a-b$ & $n \mid c-d$

$\Rightarrow n \mid c(a-b) \Rightarrow n \mid b(c-d)$

$\Rightarrow n \mid c(a-b)+b(c-d) = ac-bd$

Page No. 24
Date 21 01 15

$\Rightarrow n \mid ac-bd$

$\Rightarrow ac \equiv bd \pmod n$

Or $n \mid (a-b) \Rightarrow a-b = k_1 n$

$\Rightarrow a = b+k_1 n$

$n \mid (c-d) \Rightarrow c-d = k_2 n$

$\Rightarrow c = d+k_2 n$

$(ac - bd) = (k_1 d + k_2 b) n + k_1 k_2 n^2$

$(ac-bd) = (k_1 d+k_2 b)n + k_1 k_2 n^2$

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

$\Rightarrow ac \equiv bd \pmod n$.

(v) If $a \equiv b \pmod n$, then $a+c \equiv b+c \pmod n$ & $ac \equiv bc \pmod n$.

$n \mid (a-b) \Rightarrow n \mid (a-c+c-b)$

$\Rightarrow n \mid (a+c)-(b+c)$

$\Rightarrow a+c \equiv b+c \pmod n$

||rly $n \mid (a-b)$

$\Rightarrow n \mid c(a-b) = ac-bc$

$\Rightarrow n \mid ac-bc$

$\Rightarrow ac \equiv bc \pmod n$

(vi) If $a \equiv b \pmod n$, then $a^k \equiv b^k \pmod n$
for any positive integer k.

$n \mid a-b$ —— (i)

$\because k > 0$, so $a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \cdots + b^{k-1})$

$\Rightarrow (a-b) \mid (a^k - b^k)$ —— (ii)

from (i) & (ii) $\Rightarrow$

$n \mid a^k - b^k \Rightarrow a^k \equiv b^k \pmod n$

Example: Show that $41 \mid (2^{20} - 1)$.
4.2 | 8-64

$2^{20} = x \pmod n$, $x = ?$

$2 \equiv 2 \pmod{41}$

$\Rightarrow 2^5 = 32 \pmod{41}$

$\equiv -9 \pmod{41}$

$\Rightarrow (2^5)^2 = (-9)^2 \pmod{41}$

$\Rightarrow 2^{10} \equiv 81 \mod 41$

$\Rightarrow 2^{10} \equiv -1 \pmod{41}$

$\Rightarrow (2^{10})^2 \equiv (-1)^2 \pmod{41}$

$\Rightarrow 2^{20} \equiv 1 \pmod{41}$

$\Rightarrow 41 \mid 2^{20} - 1$

Example: (H.W)
(4.3)

Theorem (4.3) If $ca \equiv cb \pmod n$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$.

$n \mid (ca - cb) \Rightarrow n \mid c(a-b)$

$\Rightarrow n/c \mid a-b$

also

$c(a-b) = ca - cb = kn$ for some $k \in \mathbb{Z}$ —— (1)

and

$\gcd(c, n) = d$

$\Rightarrow d \mid c$ & $d \mid n$

$\Rightarrow \exists$ integers r & s such that

$c = dr$ & $n = ds$

& $\gcd(r, s) = 1$

Using in eq^n (1), we have ——

$dr(a-b) = kds$

$\Rightarrow r(a-b) = ks \Rightarrow s \mid r(a-b)$

$\Rightarrow s \mid (a-b) \Rightarrow a \equiv b \pmod s$

$\Rightarrow a \equiv b \pmod{n/d}$ $\{\because n = ds\}$

Cor. 1 If $ca \equiv cb \pmod n$, and $\gcd(c, n) = 1$
then $a \equiv b \pmod n$

In thm 4.3 $d = 1$

If $ca \equiv cb \pmod n$

then $a \equiv b \pmod{n/d}$

putting $n = 1$

we have $a \equiv b \pmod n$

Proved

Cor. II If $ca \equiv cb \pmod p$ and $p \nmid c$ where p is a prime no. then $a \equiv b \pmod p$.

$\because$ p is prime no.

$\Rightarrow$ ~~$p \mid (a-b)$~~

$\Rightarrow p \mid ca - cb$

$\Rightarrow p \mid c(a-b)$

$\because p \nmid c$

$\Rightarrow p \mid a-b$

$\Rightarrow a \equiv b \pmod p$.

Ex-4.2 (4 a)

~~Example~~ (a) find the remainder when 41^{65} is divided by 7.

Sol:

~~$7 \mid (41^{65} + c)$~~

~~$\Rightarrow 41^{65} + c = 7k$ for some $k \in Z$~~

$\Rightarrow 41 \equiv -1 \pmod 7$

$\Rightarrow 41^{65} \equiv (-1)^{65} \pmod 7$

$\Rightarrow 41^{65} \equiv -1 \pmod 7$

$\Rightarrow 41^{65} \equiv 6 \pmod 7$

$\therefore$ Remainder $= 6$

Complete (System) Set of Residues modulo n

A collection of an integer $a_1, a_2, a_3 \dots a_n$ is said to form a

Complete set of Residues modulo n if

~~A compset set of residue modulo n~~

If every integer is congruent modulo n to one and only one of the a_k $(1 \le k < n)$

In other words, $a_1, a_2, \dots a_n$ are congruent modulo n to $0, 1, 2, \dots n-1$ in some order.

(based Q-11)

(11) verify that $0, 1, 2, 2^2, 2^3, \dots 2^9$ form a complete set of Residues modulo 11, but $0, 1^2, 2^2, 3^2 \dots 10^2$ do not.

2022

Sol:

$0 \equiv 0 \pmod{11}$	$0 \equiv 0$
$1 \equiv 1 \pmod{11}$	$1 \equiv 1$
$2 \equiv 2 \pmod{11}$	$2^2 \equiv 4$
$2^2 \equiv 4$	$3^2 \equiv 9$
$2^3 \equiv 8$	$4^2 \equiv 5$
$2^4 \equiv 5$	$5^2 \equiv 3$
$2^5 \equiv 10$	$6^2 \equiv 3$
$2^6 \equiv 9$	$7^2 \equiv 5$
$2^7 \equiv 7$	$8^2 \equiv 9$
$2^8 \equiv 3$	$9^2 \equiv 4$
$2^9 \equiv 6$	$10^2 \equiv 1$
In congruent	2, 6, 7, 8, 10.

$5^2 \equiv 6^2 \pmod{11}$

$\Rightarrow$

Ex- 4.2

Page No. 29
Date 22/01/15

Ex- 4.2

4(b) What is the Remainder when the following sums is divided by by 4 ?

2013

$$1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5$$

Solⁿ:- The integers between 1 & 100 are congruent to ~~0, 1, 2, 3, (mod 4)~~
0, 1, 2, 3 (mod 4)

⇒ the integers b/w 1 & 100 of the type $4k$, $4k+1$, $4k+2$, $4k+3$, where $k \in \mathbb{Z}$

⇒ ~~$(4k)^5$~~ $4 \mid (4k)^5$

⇒ $(4k)^5 \equiv 0 \pmod 4$

$(4k+2)^5 \equiv 2^5 \pmod 4$
$\equiv 0 \pmod 4$

$(4k+1)^5 \equiv 1^5 \pmod 4$
$\equiv 1 \pmod 4$
$\{ \because 4k+1 \equiv 1 \pmod 4$

$(4k+3)^5 \equiv (3)^5 \pmod 4$
$\equiv 3 \pmod 4$

Since there are 25 integers of the type $4k+1$ between 1 & 100 & 25 integers of the type $4k+3$ b/w 1 & 100

$$\equiv \underbrace{(1+1+\cdots+1)}_{25 \text{ times}} + \underbrace{(-1+(-1)+(-1)+\cdots+(-1))}_{25 \text{ times}} \pmod 4$$

Ex- 4.2

Page No. 30
Date

$\equiv 25 + (-25) \pmod 4$
$\equiv 0 \pmod 4$
∴ Remainder $= 0$

(5) PT the integer $53^{103} + 103^{53}$ is divisible by 39 and that $111^{333} + 333^{111}$ is divisible by 7

$39 \equiv 0 \pmod{39}$
⇒ $(39+14=) 53 \equiv 14 \pmod{39}$
⇒ $53^2 \equiv (14)^2 \equiv 1 \pmod{39}$
⇒ $53^{102} \equiv (53^2)^{51} \equiv 1 \pmod{39}$
⇒ $53^{103} \equiv 14 \pmod{39}$ ——— (i)

Now,
$103 \equiv -14 \pmod{39}$
⇒ $103^2 \equiv (-14)^2 \pmod{39}$
$\equiv 1 \pmod{39}$
⇒ ~~$(103)^{52} \equiv (1)^{52} \equiv 1 \pmod{39}$~~
⇒ ~~$((103)^2)^{26} \equiv$~~
⇒ $(103)^{52} \equiv (103^2)^{26} \equiv (1)^{26} \pmod{39}$
⇒ $103^{52} \equiv 1 \pmod{39}$
⇒ $103^{53} \equiv (-14) \pmod{39}$ ——— (ii)

∴ from (i) + (ii), we get —
$53^{103} + 103^{53} \equiv (14 - 14) \bmod (39)$
$\equiv 0 \bmod (39)$
So $53^{103} + 103^{53}$ is divisible by 39.

Next for $111^{333} + 333^{111}$
$111 \equiv -1 \pmod 7$
⇒ $(111)^{333} \equiv (-1)^{333} \pmod 7$

Ex- 4.2

$\Rightarrow (111)^{333} \equiv -1 \pmod 7$

Also $333 \equiv -3 \pmod 7$

$\Rightarrow (333)^3 \equiv (-3)^3 \pmod 7$

$\equiv 1 \pmod 7$

$\Rightarrow (333)^{111} \equiv (333^3)^{37} \equiv 1^{37} \pmod 7$

$\equiv 1 \bmod 7$

Thus, $111^{333} + 333^{111} \equiv (-1+1) \pmod 7$

$\equiv 0 \pmod 7$

So $111^{333} + 333^{111}$ is divisible by 7.

[6] for $n \geq 1$, use congruence theory to establish each of the following divisibility statements

P-68

(a) $7 \mid 5^{2n} + 3 \cdot 2^{5n-2}$

$\because 5^{2n} + 3 \cdot 2^{5n-2}$

$\because 7 \equiv 0 \pmod 7$

$5 \equiv -2 \pmod 7$

$5^2 \equiv (-2)^2 \equiv -3 \pmod 7$

~~$2^5 \equiv 5 \bmod 7$~~

~~$\Rightarrow 2^{5n} \equiv 5^{2n} \bmod 7$~~

~~$2^{5n} + 3 \cdot 2^{5n-2} \equiv (5^{2n} + 3 \cdot 2^{5n-2}) \bmod 7$~~

$\equiv 2^{2n}(1+3 \cdot$

(b) $13 \mid 3^{n+2} + 4^{2n+1}$

$\because 4^2 \equiv 3 \bmod (13)$

$\Rightarrow 4^{2n} \equiv 3^n \bmod (13)$

$\Rightarrow 4^{2n+1} \equiv 3^n \cdot 4 \pmod{13}$

$3^2 \equiv -4 \pmod{13}$

or $4 \equiv -3^2 \pmod{13}$

$\because 4^{2n+1} \equiv 3^n \cdot (-3^2) \pmod{13}$

$\Rightarrow 4^{2n+1} + 3^{n+2} \equiv 0 \bmod 13$

(c) $27 \mid 2^{5n+1} + 5^{n+2}$

$2^5 \equiv 5 \pmod{27}$

$2^{5n} \equiv 5^n \pmod{27}$

$\Rightarrow 2^{5n+1} \equiv 5^n \cdot 2 \pmod{27}$

~~$\Rightarrow 2^{5n+1} - 5^n(2) \equiv 0 \pmod{27}$~~

Now

$5^2 \equiv -2 \bmod (27)$

or $-2 \equiv 5^2 \pmod{27}$

i.e $-2 \equiv 25$

$\Rightarrow 2^{5n+1} + 5^{n+2} \equiv (5^n \cdot 2 + 5^{n+2}) \pmod{27}$

$\Rightarrow 2^{5n+1} + 5^{n+2} \equiv 5^n(2+5^2) \bmod 27$

$\equiv 0 \pmod{27}$

$\Rightarrow 27 \mid 2^{5n+1} + 5^{n+2} \quad \forall n \in \mathbb{N}$

(d) $43 \mid 6^{n+2} + 7^{2n+1}$

$6^2 \equiv -7 \pmod{43}$

or $7^2 \equiv 6 \pmod{43}$

$\Rightarrow 7^{2n} \equiv 6^n \pmod{43}$

$\Rightarrow 7^{2n+1} \equiv 6^n \cdot 7 \pmod{43}$

$\because 7^{2n+1} + 6^{n+2} \equiv (6^n \cdot 7 + 6^{n+2}) \pmod{43}$

$\equiv 6^n(7+6^2) \pmod{43}$

$\equiv 6^n(7+36) \bmod 43$

$\equiv 0 \bmod 43$

So $43 \mid 7^{2n+1} + 6^{n+2}$

Ex - 4.2

Page No. 33

(9) $7 \mid 5^{2n} + 3 \cdot 2^{5n-2}$

$2^5 \equiv 2^2 \pmod 7$

$2^{5n} \equiv 2^{2n} \pmod 7$

$2^{5n-2} \equiv 2^{2n-2} \pmod 7$

$5^2 \equiv 2^2 \pmod 7$

$5^{2n} \equiv 2^{2n} \pmod 7$

$\therefore (5^{2n} + 3 \cdot 2^{5n-2}) \equiv (2^{2n} + 3 \cdot 2^{5n-2}) \bmod 7$

$\equiv 2^{2n}(1 + 3 \cdot 2^{3n-2}) \bmod 7$

$\equiv 2^{2n-2}(4 + 3 \cdot 2^{3n})$

$\equiv 2^{2n-2}(4+3 \cdot 1) \bmod 7$

$\equiv 2^{2n-2} \cdot 7 \bmod 7$

$\equiv 0 \bmod 7$

$\because 2^3 \equiv 1 \bmod 7$

$\therefore (2^3)^n \equiv 1^n \bmod 7$

$2^{3n} \equiv 1 \bmod 7$

(10) If $a_1, a_2, \dots a_n$ is a complete set of Residues modulo n and $\gcd(a,n) = 1$, P.T $aa_1, aa_2, \dots aa_n$ is also a complete set of Residues modulo n.

~~$a_1, a_2, a_3 \dots a_n$ are n integers~~

~~$a_1, a_2, \dots, a_n$ are incongruent~~

$a_1, a_2, \dots a_n$ congruent to $0, 1, 2, \dots n$ modulo n in some order.

$\Rightarrow \{a_1, a_2, \dots a_n\}$ ~~are congruent to 0, 1.~~ form a complete set of Resi. mod n

Result: If $a_1, a_2, a_3 \dots a_n$ are n incongruent modulo n then they form a ~~set~~ complete set of Residues modulo n

Page No. 34 Date 23 01 15

(10) Sol^n We will show that $aa_1, aa_2, \dots aa_n$ are in congruent modulo n.

$\gcd(a,n) = 1$

Suppose any two are congruent modulo n $(aa_i \,\&\, aa_j)$

$aa_i \equiv aa_j \pmod n \qquad 1 \le i, j \le n$

$\Rightarrow a_i \equiv a_j \pmod n$

$[\because \gcd(a,n) = 1]$

$\Rightarrow a_1, a_2, \dots a_n$ is not a complete set of Residues modulo n.

$\longrightarrow \quad \longleftarrow$

(12) Prove that —

(a) If $\gcd(a,n) = 1$, then the integers $c, c+a, c+2a, c+3a, \dots c+(n-1)a$ form a complete set of Residues modulo n for any c.

Sol^n $c + ia \equiv c + ja \pmod n \qquad 0 \le i, j \le n-1$

$\Rightarrow ia \equiv ja \pmod n$

$\Rightarrow i \equiv j \pmod n \qquad 0 \le i, j \le n-1$

$\Rightarrow n \mid j - i \qquad [|j-i| < n]$

$\Rightarrow j - i = 0$

$\Rightarrow i = j$

$\Rightarrow c, c+a, c+2a, \dots c+(n-1)a$ are incongruent.

(b) Any n consecutive integers form a complete set of residues modulo n.

take $a=1$, (from part a)

$c, c+1, c+2, \ldots, c+n-1$

$\because \gcd(n,1)=1$

from part (a), $c, c+1, c+2, \ldots, c+(n-1)$ form a complete set of residues modulo n

(c) The product of any set of n consecutive integers is divisible by n.

sol^n

In Exam, if only part (c) or (b) coming then take

let $c+i \equiv c+j \pmod n$

Suppose $c, c+1, c+2, \ldots, c+(n-1)$ form a complete set of residues modulo n

then they form $0, 1, 2, \ldots, (n-1)$ in same order

$\Rightarrow c(c+1)(c+2)\ldots(c+n-1) \equiv 0\cdot 1\cdot 2 \ldots (n-1) \pmod n$

$\Rightarrow n \mid c(c+1)(c+2)\ldots(c+n-1)$

[4.4] LINEAR CONGRUENCE AND THE CHINESE REMAINDER THEOREM

Theorem 4.7 (p. 78)

The linear congruence $ax \equiv b \pmod n$ has a sol^n iff $d \mid b$ where $d=\gcd(a,n)$. If $d \mid b$ then it has d mutually incongruent sol^{n}s modulo n.

Proof:

$ax \equiv b \pmod n$

$\Rightarrow n \mid ax-b \Rightarrow ax-b = ny$ for some $y \in \mathbb{Z}$

$\Rightarrow ax-ny=b$

this equation has a sol^n iff $d \mid b$

where $d=\gcd(a,n)$

$\Rightarrow$ The linear congruence $ax \equiv b \pmod n$ has a sol^n iff $d \mid b$ where $d=\gcd(a,n)$

II - Part

If $d \mid b$ then $ax \equiv b \pmod n$ has a sol^n

$\Rightarrow ax-ny=b$ has a sol^n.

let (x_0, y_0) be a sol^n of $ax-ny=b$

then the other solutions of this equation are given by —

$x = x_0 + \frac{n}{d}t$

$y = y_0 + \frac{n}{d}t$ for some $t \in \mathbb{Z}$

Consider the case when t takes successive values $t=0,1,2,\ldots,d-1$

$x = x_0, x_0+\frac{n}{d}, x_0+\frac{2n}{d}, \ldots, x_0+\frac{(d-1)n}{d}$

Now we will show that these integers are incongruent modulo n

Suppose any two are congruent modulo n

$x_0+\frac{n}{d}t_1 \equiv x_0+\frac{n}{d}t_2 \pmod n$, $0 \le t_1, t_2 \le d-1$

$\Rightarrow \frac{n}{d}t_1 \equiv \frac{n}{d}t_2 \pmod n$

$$\boxed{\begin{array}{l} ca \equiv cb \pmod n \\ a \equiv b \pmod{n/d} \\ \text{when } d=\gcd(c,n) \end{array}}$$

$\Rightarrow t_1 \equiv t_2 \pmod{n/(n/d)}$

$\Rightarrow t_1 \equiv t_2 \pmod d$ $\left[\gcd\left(\frac{n}{d}, n\right) = n/d \quad \because n/d < n \;\&\; n/d \mid n\right]$

$\Rightarrow t_1 \equiv t_2 \pmod d$

$\Rightarrow d \mid t_1 - t_2$

$\Rightarrow t_1 - t_2 = 0 \Rightarrow t_1 = t_2$

let $x = x_0 + \frac{n}{d} t$ (where $t \geq d$) be a soln of $ax \equiv b \pmod n$

by division Algorithm $\exists$ integers q, r such that $t = qd + r$, where $0 \leq r < d$

$$x_0 + \frac{n}{d} t = x_0 + \left(\frac{n}{d}\right)(qd + r)$$
$$= x_0 + nq + \left(\frac{n}{d}\right) r$$
$$= nq + x_0 + \left(\frac{n}{d}\right) r$$

$$\Rightarrow \left\{x_0 + \left(\frac{n}{d}\right)t\right\} - \left\{x_0 + \left(\frac{n}{d}\right) r\right\} = nq.$$

$$\Rightarrow n \mid \left[\left\{x_0 + \frac{n}{d} t\right\} - \left\{x_0 + \frac{n}{d} r\right\}\right]$$

$$\Rightarrow x_0 + \left(\frac{n}{d}\right) t \equiv x_0 + \frac{n}{d} r \pmod n$$

where $0 \leq r \leq d-1$

Result: If x_0 is any soln of linear congruence $ax \equiv b \pmod n$ and $\gcd(a, n) = d$. Then the d incongruent soln are given by

$$x_0,\ x_0 + \frac{n}{d},\ x_0 + 2\left(\frac{n}{d}\right),\ \ldots\ x_0 + \frac{(d-1)}{d} n.$$

i.e $x_0,\ x_0 + \frac{n}{d},\ x_0 + 2\left(\frac{n}{d}\right),\ \ldots\ x_0 + (d-1)\frac{n}{d}$

Soln (1) (e) $34x \equiv 60 \pmod{98}$

$\gcd(a, n) = \gcd(34, 98) = 2$

$2 \mid 60$

Then it has $d = 2$ incongruent soln.

$34x - 98y = 60$

$98 = 2 \cdot 34 + 30$

$34 = 1 \cdot 30 + 4$

$30 = 7 \cdot 4 + 2$

$2 = 30 - 7 \cdot 4$

$= 30 - 7(34 - 30)$

$= 8 \cdot 30 - 7 \cdot 34$

$= 8(98 - 2 \cdot 34) - 7 \cdot 34$

$2 = 8 \cdot 98 - 23 \cdot 34$

$30 \cdot 2 = 30 \cdot 8 \cdot 98 - 30 \cdot 23 \cdot 34$

$= 240 \cdot 98 + (-690) \cdot 34$

$\therefore x_0 = -690$

$\therefore$ Incongruent soln are —

(i) $x_0 = -690$

(ii) $x_0 + \frac{n}{d} = -690 + \frac{98}{2}$ ($\frac{98}{2} = 49$)

$x \equiv -690, -641 \pmod{98}$

$x \equiv (98 \times 8 - 690), (98 \times 7 - 641) \pmod{98}$

$x \equiv 94, 45 \pmod{98}$

H.W (f) $140x \equiv 133 \pmod{301}$ — (1)

$\gcd(140, 301) = 7$

Now,

$7 = 21 - 14$

$= 21 - (140 - 6 \times 21)$

$= 7 \times 21 - 140$

$= 7(301 - 2 \times 140) - 140$

$140 \overline{)301} (2$, 280, $21 \overline{)140} (6$, 126, $14 \overline{)21} (1$, 14, 7

$= (7)(301) + (-15)(140)$

$\Rightarrow 140(-15) \equiv 7 \pmod{301}$

$\Rightarrow 140(-19 \times 15) \equiv (19)(7) \pmod{301}$

$\Rightarrow 140(-301+16) \equiv 133 \pmod{301}$

$\Rightarrow (140)(16) \equiv 133 \pmod{301}$

$\Rightarrow$ Thus, $x_0 = 16$ is a sol^n (1)

By the thm,

7 non-congruent modulo are—

$x = 16 + \left(\frac{301}{7}\right)t \quad , t = 0, 1, 2, 4, 5, 6$

$= 16 + 43t \quad , t = 0, 1, 2, \ldots 6$

$\Rightarrow x = 16, 59, 102, 145, 188, 231 \pmod 7$

H.W

(d) $36x \equiv 8 \pmod{102}$

$\gcd(36, 102) = 6$

$$\begin{array}{r} 36)\,102\,(2 \\ 72 \\ \hline 30)\,36\,(1 \\ 30 \\ \hline 6)\,30 \\ 30 \\ \hline \times \end{array}$$

As $6 \nmid 8$, (1) has no sol^n.

(e) $25x \equiv 15 \pmod{29}$

$$\begin{array}{r} 25)\,29\,(1 \\ 25 \\ \hline 4)\,25\,(6 \\ 24 \\ \hline 1 \end{array}$$

$\gcd(25, 29) = 1$

$1 = 25 - 4 \times 6$

$= 25 - (29 - 25) \times 6$

$= 7 \times 25 + (-6) \times 29$

$\Rightarrow 25(7) \equiv 1 \pmod{29}$

$\Rightarrow 25(105) \equiv 15 \pmod{29}$

$\Rightarrow 25(29 \times 3 + 18) \equiv 15 \pmod{29}$

$\Rightarrow 25(18) \equiv 15 \bmod 29$

$\therefore x_0 = 18$ is a sol^n of

$25x \equiv 15 \bmod 29$

As $\gcd(25, 29) = 1$ the linear congruence

$25x \equiv 15 \pmod{29}$ has a unique sol^n

$x_0 = 18 \bmod 29$.

(P-79) Thm 4.8

CHINESE REMAINDER THEOREM

let $n_1, n_2, \ldots n_r$ be the integer s.t. $\gcd(n_i, n_j) = 1 \ \forall\ i \neq j$, the the system of L. Cong. is —

$x \equiv a_1 \pmod{n_1}$

$x \equiv a_2 \pmod{n_2}$

$\vdots$

$x \equiv a_r \pmod{n_r}$

has a simultaneously sol^n which is unique modulo $n_1 n_2 \cdots n_r$

Proof: let $n = n_1 n_2 \cdots n_r$

& $N_i = \frac{n}{n_i} \quad \forall\ 1 \leq i \leq r$

$\Rightarrow \gcd(N_i, n_i) = 1 \quad \forall\ i \quad$ —(i)

& $N_j \equiv 0 \pmod{n_i} \quad \forall\ i \neq j$

from (i), the linear congruence

$N_i x_i \equiv 1 \pmod{n_i}$ has a unique sol^n.

Claim: $\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$

is simultaneous sol^n of the given system.

$\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$

$\equiv a_i N_i x_i \pmod{n_i} \ \forall\ i$

$\equiv a_i \cdot 1 \pmod{n_i}$

$\equiv a_i \pmod{n_i} \quad \forall\ i$

$\Rightarrow \bar{x} \equiv a_i \pmod{n_i} \quad \forall\ i$

let $\bar{x}$ & x^* be two ~~simul~~ sol^n of the given system —

$\bar{x} \equiv a_i \pmod{n_i} \quad \forall\ 1 \leq i \leq r$

$x^* \equiv a_i \pmod{n_i} \quad \forall\ \text{''}$

$\Rightarrow n_i \mid (\bar{x} - a_i)$ & $n_i \mid (x^* - a_i)$

$\Rightarrow n_i \mid \{(\bar{x} - a_i) - (x^* - a_i)\}$

$\Rightarrow n_i \mid \bar{x} - x^* \quad \forall\ 1 \leq i \leq r$

$\gcd(n_i, n_j) = 1 \quad \forall\ i \neq j$

$\Rightarrow n_1 n_2 \cdots n_r \mid (\bar{x} - x^*)$

$\Rightarrow \bar{x} \equiv x^* \pmod{n_1 n_2 \cdots n_r}$

Q.(4) (c). Solve the sets of simultaneous Cong.

(d) $x \equiv 5 \pmod 6$, $x \equiv 4 \pmod{11}$, $x \equiv 3 \pmod{17}$

$n_1 = 6,\ n_2 = 11,\ n_3 = 17$

here $\gcd(6, 11) = \gcd(11, 17)$
$= \gcd(6, 17)$
$= 1$

$n = 6 \cdot 11 \cdot 17 = 1122$

$N_1 = \frac{n}{n_1} = \frac{1122}{6} = 11 \times 17 = 187$

$N_2 = \frac{n}{n_2} = \frac{6 \times 11 \times 17}{11} = 102$

$N_3 = \frac{n}{n_3} = \frac{6 \times 11 \times \cancel{17}}{\cancel{17}} = 66$

$N_1 x_1 \equiv 1 \pmod 6$

$\Rightarrow 187 x_1 \equiv 1 \pmod 6$

$\Rightarrow 1 \cdot x_1 \equiv 1 \pmod 6$

$\Rightarrow x_1 = 1$

$6 \overline{)187}\ 31$, 18, 7, 6, 1

$N_2 x_2 \equiv 1 \pmod{11}$

$\Rightarrow 102 x_2 \equiv 1 \pmod{11}$

$\Rightarrow 3 x_2 \equiv 1 \pmod{11}$

$x_2 = 4$

Now $N_3 x_3 \equiv 1 \pmod{17}$

$\Rightarrow 66 x_3 \equiv 1 \pmod{17}$

$\Rightarrow 15 x_3 \equiv 1 \pmod{17}$
$\equiv 1+119$

$x_3 = 8$

we have
$a_1 = 5$
$a_2 = 4$
$a_3 = 3$

Sol^n of given ~~simultaneous~~ system is

$x \equiv a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 \pmod{n_1 n_2 n_3}$

$\equiv (5)(187)(1) + 4(102)(4) + 3(66)(8) \pmod{1122}$

$\equiv (935 + 1632 + 1584) \pmod{1122}$

$\equiv (4151) \pmod{1122}$

$x \equiv 785 \pmod{1122}$

66
24

264
132

1584

(4) (d) $2x \equiv 1 \pmod 5$ $\Rightarrow 6x \equiv 3 \pmod 5$ $\Rightarrow x \equiv 3 \pmod 5$

$3x \equiv 9 \pmod 6$ $\rightarrow x \equiv 3 \pmod 6$

$4x \equiv 1 \pmod 7$ $\rightarrow x \equiv 2 \pmod 7$

$5x \equiv 9 \pmod{11}$ $\rightarrow 10x \equiv 18 \pmod{11}$

Sol^n $\Rightarrow$

$\Rightarrow -x \equiv 7 \pmod{11}$

$\Rightarrow x \equiv -7 \pmod{11}$

$\Rightarrow x \equiv 4 \pmod{11}$

Theorem 4.9

The system of linear congruences

$ax + by \equiv r \pmod n$ —— (i)

$cx + dy \equiv s \pmod n$ —— (ii)

has a unique sol^n modulo n whenever $\gcd(ad-bc, n) = 1$

(1) $\times d$ − (2) $\times b$ $\Rightarrow$

$(ad - bc)\, x \equiv (rd - sb) \pmod n$ (3)

$\Rightarrow$ ∵ $\gcd(ad-bc, n) = 1$

So, this linear congruence
$(ad-bc)x \equiv 1 \pmod n$
has a unique sol^n t (say)

$(ad-bc)t \equiv 1 \pmod n$

Now multiply eq^n (3) by t —

$(ad-bc)tx \equiv (rd-sb) \pmod n$

$\Rightarrow x \equiv (rd-sb)t \pmod n$

(2) $\times a$ − (1) $\times c$ $\Rightarrow$

$(\cancel{ac} + ad - \cancel{ac} - bc)\, x \equiv (sa - rc) \pmod n$

$\Rightarrow (ad - bc)y \equiv (sa-rc) \bmod (n)$ (4)

∵ $\gcd(ad-bc, n) = 1$

So the linear congruence (4) has a unique sol^n t

(17) Find the sol^{n}s of the system of congruences

$3x + 4y \equiv 5 \pmod{13}$

$2x + 5y \equiv 7 \pmod{13}$

$a=3,\ b=4,\ c=2,\ d=5$

$r=5,\ s=7,\ n=13$

$ad-bc = 15-8 = 7$

$\therefore gcd(ad-bc, n) = (7, 13) = 1$

so, it is solveable

Now

$(ad-bc)t \equiv 1 \pmod n$

$\Rightarrow 7t \equiv 1 \pmod{13}$

$\Rightarrow t = 2$

$\therefore x \equiv (rd-sb)t \pmod{13}$

$x \equiv (25-28)(2) \pmod{13}$

$x \equiv (-6) \pmod{13}$

$x \equiv 7 \pmod{13}$

llly

$y = (as-cr)t \pmod n$

$\equiv (21-10)2 \pmod{13}$

$\equiv (22) \pmod{13}$

$\equiv (9) \pmod{13}$

(11) PT, the congruences $x \equiv a \pmod n$ & $x \equiv b \pmod m$ admits a simultaneous solⁿ $\Leftrightarrow gcd(n,m) \mid a-b$, if a solⁿ exists, Confirm that it is unique.

let x_0 be a simultaneous solⁿ of a given congruences.

let $gcd(m,n)=d$

$x_0 \equiv a \pmod n \Rightarrow n \mid x_0 - a$

$x_0 \equiv b \pmod m \Rightarrow m \mid x_0 - b$

let $gcd(m,n)=d$

$\Rightarrow d \mid m$ & $d \mid n$

$\Rightarrow d \mid x_0 - b$ & $d \mid x_0 - a$

$\Rightarrow d \mid \{(x_0-b)-(x_0-a)\}$

$\Rightarrow d \mid a-b$

$\Rightarrow a \equiv b \pmod n$

$\Rightarrow a \equiv b \pmod{gcd(m,n)}$

$\Rightarrow gcd(m,n) \mid a-b$

($\Leftarrow$) Let $gcd(m,n) \mid a-d$

$\Rightarrow d \mid a-b$ — (I)

$\because gcd(m,n) = d$

$\Rightarrow gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$

$\Rightarrow \exists$ integers r & s such that

$\frac{mr}{d} + \frac{ns}{d} = 1$ when $gcd(r,s)=1$ — (II)

$x = \frac{bns}{d} + \frac{amr}{d}$

$= \frac{bns}{d} + \frac{amr}{d} + \frac{bmr}{d} - \frac{bmr}{d}$

$= b\left(\frac{ns}{d} + \frac{mr}{d}\right) + \frac{(a-b)}{d} mr$

$= b + \left(\frac{a-b}{d}\right) rm$ by (ii)

$\Rightarrow \cancel{\frac{bns}{d}} \mid \left(\frac{bns}{d} + \frac{amr}{d}\right) - b = \left(\frac{a-b}{d}\right) rm$

Page No. 48
Date 30 | 1 | 15

$\Rightarrow m \left| \left(\frac{bns}{d} + \frac{amr}{d} \right) - b \right.$

$\Rightarrow \frac{bns}{d} + \frac{amr}{d} \equiv b \pmod m$ ——— (2)

Now,

$\frac{bns}{d} + \frac{amr}{d} =$

$= \frac{bns}{d} + \frac{amr}{d} + \frac{ans}{d} - \frac{ans}{d}$

$= a\left(\frac{mr}{d} + \frac{ns}{d}\right) + (b-a)\frac{ns}{d}$

$= a + (b-a)sn$

$\Rightarrow \left(\frac{bns}{d} + \frac{amr}{d}\right) - a \equiv \left(\frac{b-a}{d}\right) sn$

$\Rightarrow n \left| \left(\frac{bns}{d} + \frac{amr}{d} \right) - a \right.$

$\Rightarrow \frac{bns}{d} + \frac{amr}{d} \equiv a \pmod n$ ——— (3)

from (2) & (3) ——

given congruences has a simultaneous sol^n

$$\boxed{x = \frac{bns}{d} + \frac{amr}{d}}$$

Rest Proof

~~my method~~

Suppose $x \equiv a \pmod n$
and $x \equiv b \pmod m$ } — (1)
admits a simultaneous sol^n, say x_0
then $n \mid (x_0 - a)$ & $m \mid (x_0 - b)$

Page No. 49
Date 30 | 1 | 15

let $d = \gcd(m,n)$, then

$d \mid (x_0 - a)$ and $d \mid (x_0 - b)$

$\Rightarrow d \mid [(x_0 - b) - (x_0 - a)]$

$\Rightarrow d \mid (a - b)$

$\Rightarrow \gcd(m,n) \mid (a-b)$

$\Leftarrow$ Assume that $d = \gcd(m,n) \mid (a-b)$

$x \equiv a \pmod n \Rightarrow x - a = k_1 n$
$\Rightarrow x = a + k_1 n$

So Putting this value in
$x \equiv b \pmod m$, we get —

$\Rightarrow a + k_1 n \equiv b \pmod m$

$\Rightarrow k_1 n \equiv (b-a) \pmod m$ ——— (ii)

Since $d = \gcd(m,n) \mid (a-b)$ or $(b-a)$

Now, $\exists\ k_2 \in \mathbb{Z}$, that satisfies (ii)

Now, $k_2 \in \mathbb{Z}$ be such that —

$k_2 n \equiv (b-a) \pmod m$

$\Rightarrow a + k_2 n \equiv b \pmod m$

Let $x_0 = a + k_2 n$, then

$x_0 \equiv b \pmod m$

So, we get $x_0 \equiv a \pmod n$

||ly $x_0 \equiv b \pmod m$

Uniqueness: Let x_0 & y_0 be two sol^{n}s of (1),

then ~~x_0~~ ——

Ex 4.4

Page No. 50 Date 1 | 2 | 15

$x_0 \equiv a \pmod n \Rightarrow (x_0 + 0y) \equiv a \pmod n$

$y_0 \equiv a \pmod n \Rightarrow (0x_0 + y_0) \equiv a \pmod n$

$\therefore gcd(ad-bc, n) = gcd(1, n) = 1$

Since gcd is 1, so it has uniqueness (By thm)

Let x_0 & y_0 be two solns of (1)

then,

$x_0 \equiv y_0 \equiv a \pmod n$ and $x_0 \equiv y_0 \equiv b \pmod m$

$\Rightarrow n \mid (x_0 - y_0)$ | $m \mid (x_0 - y_0)$

$\Rightarrow lcm(n, m) \mid (x_0 - y_0)$

$\Rightarrow x_0 \equiv y_0 \pmod{lcm(m,n)}$

(12) Use Problem (11) to show that the given system doesn't posses a soln —

$x \equiv 5 \pmod 6$ and

$x \equiv 7 \pmod{15}$

Soln Here $a = 5$ and $b = 7$, $m = 6$, $n = 15$

Now, $gcd(m, n) = gcd(6, 15) = 3$

so by problem (11), $gcd(m,n) \mid (a-b)$

$\therefore 3 \mid (5-7) = 2$ which is not possible.

So the above system of eqn has no solns.

Solve the linear Congruence

Page No. 51 Date 1 | 2 | 15

(5) $17x \equiv 3 \pmod{3 \cdot 2 \cdot 5 \cdot 7}$ by solving

Soln

$17x \equiv 3 \pmod 2 \Rightarrow x \equiv 1 \pmod 2$

$17x \equiv 3 \pmod 3 \Rightarrow 2x \equiv 0 \pmod 3$

$17x \equiv 3 \pmod 5 \Rightarrow x \equiv 4 \pmod 5$

$17x \equiv 3 \pmod 7 \Rightarrow 3x \equiv 3 \pmod 7$

$\Rightarrow 6x \equiv 6 \pmod 7$

$\Rightarrow -x \equiv -1 \pmod 7$

$\Rightarrow x \equiv 1 \pmod 7$

let $n = 2 \cdot 3 \cdot 5 \cdot 7 = 210$

$\therefore N_1 = \frac{n}{n_1} = 3 \cdot 5 \cdot 7 = 105$

$N_2 = \frac{n}{n_2} = 2 \cdot 5 \cdot 7 = 70$

$N_3 = \frac{n}{n_3} = 2 \cdot 3 \cdot 7 = 42$

$N_4 = \frac{n}{n_4} = 2 \cdot 3 \cdot 5 = 30$

$gcd(N_1, n_1) = gcd(105, 2) = 1$

$= gcd(70, 3) = 1$

$= gcd(42, 5) = 1$

$= gcd(30, 7) = 1$

$\boxed{\therefore N_i x_i \equiv 1 \pmod{n_i}}$

$\rightarrow 105 x_1 \equiv 1 \pmod 2$

$x_1 \equiv 1 \pmod 2$

$\Rightarrow 2 \mid x_1 - 1 \Rightarrow x_1 = 1$

$\rightarrow 70 x_2 \equiv 1 \pmod 3$

$x_2 \equiv 1 \pmod 3$ or

$3 \mid x_2 - 1 \Rightarrow x_2 = 1$

$\rightarrow 42 x_3 \equiv 1 \pmod 5$

$\Rightarrow 3 \times 2 x_3 \equiv 1 \times 3 \pmod 5$

$x_3 \equiv 3 \pmod 5 \Rightarrow x_3 = 3$

Ex- 4.4

$30x_4 \equiv 1 \pmod 7$

$\Rightarrow 2x_4 \equiv 1 \pmod 7$

$\Rightarrow x_4 \equiv 4 \pmod 7 \quad \Rightarrow x_4 \equiv 4$

So, the sol^n of the given set is —

$\bar{x} \equiv x^* \pmod n$

$\bar{x} \equiv a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 + a_4N_4x_4$

$\equiv (1)(105)(1) + 0 + (4)(42)(3) + (1)(30)(4)$

$\equiv (105 + 504 + 120) \pmod n$

$\equiv (729) \pmod{210}$

$\equiv (99) \pmod{210}$

⑥ find the smallest integer $a > 2$, s.t
$2|a,\ 3|a+1,\ 4|a+2,\ 5|a+3,\ 6|a+4$

sol $a \equiv 0 \pmod 2 \quad \Rightarrow a \equiv 2 \pmod 2$ — i

$a+1 \equiv 0 \pmod 3 \quad \Rightarrow a \equiv 2 \pmod 3$ — ii

$(a \equiv -1 \bmod 3 \Rightarrow a \equiv 2 \bmod 3)$

$a+2 \equiv 0 \pmod 4 \Rightarrow a \equiv 2 \pmod 4$ — iii

$a+3 \equiv 0 \pmod 5 \Rightarrow a \equiv 2 \pmod 5$ — iv

$a+4 \equiv 0 \pmod 6 \Rightarrow a \equiv 2 \pmod 6$ — v

Consider (iii) ⇒ (i) and
(v) ⇒ (ii).(i) so
we can leave (iii) & (v), and thus we
solve,

$a \equiv 2 \pmod 4$ — (vi)

$a \equiv 2 \pmod 5$ — (vii)

$a \equiv 2 \pmod 3$ — (viii)

Now, gcd(2,3) = 1,
gcd(3,5)
= gcd(5,3) } = 1

$n = 2 \cdot 3 \cdot 5 = 30$

$\therefore N_1 = \frac{30}{2} = 15$

$N_2 = \frac{30}{3} = 10$

$N_3 = \frac{30}{5} = 6$

$\boxed{N_i x_i \equiv 1 \pmod{n_i}}$ solve it

→ $15x_1 \equiv 1 \pmod 2$

$\Rightarrow x_1 \equiv 1 \pmod 2 \quad \Rightarrow x_1 = 1$

→ $10x_2 \equiv 1 \pmod 3$

$x_2 \equiv 1 \pmod 3 \quad \Rightarrow x_2 = 1$

→ $6x_3 \equiv 1 \pmod 5$

$x_3 \equiv 1 \pmod 5 \quad \Rightarrow x_3 = 1$

$\therefore \bar{x} \equiv (a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3) \pmod n$

$\equiv (2\cdot15\cdot1 + 2\cdot10\cdot1 + 2\cdot6\cdot1) \pmod{30}$

$\equiv (30 + 20 + 12) \pmod{30}$

$\equiv (62) \pmod{30}$ or $2 \bmod 30$

since $a > 2$ so $a = 62$

∴ smallest positive integer a is 62.

⑱ ~~Suppose every~~ obtain the two incongruent sol^n modulo 210 of the system
$2x \equiv 3 \pmod 5$
$4x \equiv 2 \pmod 6$
$3x \equiv 2 \pmod 7$

Page No. 54 Date 2/2/15

$2x \equiv 3 \pmod 5 \Rightarrow x \equiv 4 \pmod 5$

$4x \equiv 2 \pmod 6 \Rightarrow 2x \equiv 4 \pmod 6$

$x \equiv 5 \pmod 6$ $\Rightarrow x \equiv 2 \pmod 6$

$3x \equiv 2 \pmod 7 \Rightarrow 2x \equiv 6 \pmod 7$

$\Rightarrow x \equiv 3 \pmod 7$

$\gcd(5,6) = 1 = \gcd(6,7)$

$= \gcd(5,7)$

$\therefore N_1 = \frac{n}{n_1} = \frac{5\times6\times7}{5} = 42$ 21

$N_2 = \frac{5\times6\times7}{6} = 35$

$N_3 = \frac{5\times6\times7}{7} = 35$

Now, solving $\boxed{N_i x_i \equiv d \pmod{n_i}}$

→ $42x_1 \equiv 1 \pmod 5 \Rightarrow 2x \equiv 1 \pmod 5$

$\Rightarrow x_1 = 3$

→ $35x_2 \equiv 1 \pmod 6 \Rightarrow 5x \equiv 1 \pmod 6$

$\Rightarrow x \equiv -1 \pmod 6$

$x_2 = 5$

→ $30x_3 \equiv 1 \pmod 7 \Rightarrow 2x_3 \equiv 1 \pmod 7$

$x_3 = 4$

$\therefore x \equiv (4.42.3 + 2.35.5 + 3.30.4) \bmod (210)$

$\equiv (504 + 350 + 360) \bmod (210)$

$\equiv (1214) \bmod (210)$

$\equiv (5\times242 + 4) \bmod 210$

$\equiv (1210 + 4) \bmod 210$

Page No. 55

VB

$2x \equiv 3 \pmod 5$

$4x \equiv 2 \pmod 6$

$3x \equiv 2 \pmod 7$

2 sol^n

$x \equiv 4 \pmod 5$ | $n_1 = 5,\ n_2 = 6,\ n_3 = 7$

$x \equiv 2, 5 \pmod 6$

$x \equiv 3 \pmod 7$

$n = 5\times6\times7 = 210$

$N_1 = \frac{n}{n_1} = \frac{210}{5} = 42$

$N_2 = \frac{n}{n_2} = \frac{210}{6} = 35$

$N_3 = \frac{n}{n_3} = \frac{210}{7} = 30$

Now solving $\boxed{N_i x_i \equiv 1 \pmod{n_i}}$

→ $42x_1 \equiv 1 \pmod 5$

$2x_1 \equiv 6 \pmod 5 \Rightarrow x_1 \equiv 3 \pmod 5$

$\Rightarrow x_1 = 3$

→ $35x_2 \equiv 1 \pmod 6$

$5x_2 \equiv 1 + (24) \pmod 6$

$\Rightarrow 5x_2 \equiv 25 \pmod 6$ $\Rightarrow x_2 = 5$

→ $30x_3 \equiv 1 \pmod 7$

$2x_3 \equiv 8 \pmod 7$ $\Rightarrow x_3 = 4$

$\therefore$ Sol^n is given by

$x_1 \equiv [(4)(42)(3) + (2)(35)(5) + 3(30)(4)] \pmod{210}$

$\equiv (504) + 350 + 360) \bmod (210)$

$x \equiv 1214 \equiv 164 \pmod{210}$

And $x_2 \equiv [4(42)(3) + (5)(35)(5) + 3(30)(4)] \pmod{210}$

$\equiv (504 + 875 + 360) \pmod{210}$

$\equiv 1739 \equiv 59 \pmod{210}$

$\Rightarrow x \equiv 164, 59 \pmod{210}$

(Not in syllabus)

DECIMAL REPRESENTATION OF INTEGER

$a_n a_{n-1} a_{n-2} \cdots a_2 a_1 a_0$
$= a_n \times 10^n + a_{n-1} \times 10^{n-1} + a_{n-2} \times 10^{n-2} + \cdots$
$\cdots a_2 \times 10^2 + a_1 \times 10 + a_0$

$123479 = 1\times 10^5 + 2\times 10^4 + 3\times 10^3 + 7\times 10^2 + 7\times 10 + 9$

Thm: let $p(x) = \sum_{k=0}^{m} c_k x^k$ be a poly. fn of x with integral co-efficients c_k. If $a \equiv b \pmod n$ then $p(a) \equiv p(b) \pmod n$

Soln:

$p(a) = \sum_{k=0}^{m} c_k a^k$

$p(b) = \sum_{k=0}^{m} c_k b^k$

$\because$ given $a \equiv b \pmod n$

$\Rightarrow a^k \equiv b^k \pmod n \quad \forall\ k \geq 0$

$\Rightarrow c_k a^k \equiv c_k b^k \pmod n \quad \forall\ k \geq 0$

Now, Add $m+1$ congruences.

$\sum_{k=0}^{m} c_k a^k = \sum_{k=0}^{m} c_k b^k$

$a_m \times 10^m + a_{m-1} \times 10^{m-1} + \cdots + a_1 \times 10 + a_0$

RESULT: let $N = a_m a_{m-1} \cdots a_1 a_0$ be an integer. Then $3 \mid N \Leftrightarrow 3 \mid (a_m + a_{m-1} + \cdots + a_1 + a_0)$

Proof:

let $p(x) = \sum_{k=0}^{m} a_k x^k$

Now,

$10 \equiv 1 \pmod 3$

$4\times 7+1$
29×1

$\Rightarrow p(10) \equiv p(1) \pmod 3$

$\because p(10) = N$ & $p(1) = a_m + a_{m-1} + \cdots a_1 + a_0$

$\Rightarrow N \equiv (a_m + a_{m-1} + \cdots a_1 + a_0) \pmod 3$ —— (1)

Suppose $3 \mid N$

$\Rightarrow N \equiv 0 \pmod 3$

from eqn (1)

$a_m + a_{m-1} + \cdots + a_1 + a_0 \equiv 0 \pmod 3$

$\Rightarrow 3 \mid (a_m + a_{m-1} + \cdots + a_1 + a_0)$

$\Leftarrow$ let $3 \mid (a_m + a_{m-1} + \cdots + a_1 + a_0)$

$\Rightarrow (a_m + a_{m-1} + \cdots + a_1 + a_0) \equiv 0 \pmod 3$

$\Rightarrow N \equiv 0 \pmod 3$ [from eqn (1)]

H.W
1. $9 \mid N \Leftrightarrow 9 \mid (a_m + a_{m-1} + \cdots + a_1 + a_0)$
2. $11 \mid N \Leftrightarrow 11 \mid (a_0 - a_1 + a_2 - \cdots + (-1)^m a_m)$

Pf:

let $p(x) = \sum_{k=0}^{m} a_k x^k$

Now, $10 \equiv -1 \pmod{11}$

$\Rightarrow p(10) \equiv p(-1) \pmod{11}$

$\because p(10) = N$

& $p(-1) = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m$

$\Rightarrow N \equiv (a_0 - a_1 + a_2 + \cdots + (-1)^m a_m) \pmod{11}$ —— (1)

Suppose $11 \mid N$

$\Rightarrow N \equiv 0 \pmod{11}$

from eqn (1) —

$a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^m a_m$

$\Rightarrow 11 \mid (a_0 - a_1 + a_2 - \cdots + (-1)^m a_m)$

$\Leftarrow$ Let $11 \mid (a_0 - a_1 + a_2 - \cdots + (-1)^m a_m)$

$\Rightarrow (a_0 - a_1 + a_2 - \cdots + (-1)^m) \equiv 0 \pmod{11}$

$\Rightarrow N \equiv 0 \pmod{11}$ [from (1)]

$\Rightarrow 11 \mid N$

(3) $5 \mid N \iff 5 \mid a_0$

Pf let $P(x) = \sum_{k=0}^{m} a_k x^k$

Now,

$10 \equiv 0 \pmod 5$

$\Rightarrow P(10) \equiv P(0) \pmod 5$

$\because P(10) = N$ & $P(0) = a_0$

$\Rightarrow N \equiv a_0 \pmod 5$

Suppose $5 \mid N \Rightarrow N \equiv 0 \pmod 5$

$\Rightarrow a_0 \equiv 0 \pmod 5$

$\Rightarrow 5 \mid a_0$

$\Leftarrow$ let $5 \mid a_0$

$a_0 \equiv 0 \pmod 5$

$\Rightarrow N \equiv 0 \pmod 5$

$\Rightarrow 5 \mid N$

Check Eg

LAST DIGIT OF ANY NUMBER

$3^{41} = ?$

$3^{41} \equiv x \pmod{10}$

$\Rightarrow x = ?$ $x = 3$

$3^2 \equiv 9 \equiv x \pmod{10}$

$3^2 \equiv (-1)^4 \pmod{10}$

$(3^2)^{20} \equiv 1 \pmod{10}$

$3^{41} \equiv 3 \pmod{10}$

$x = 3$

Last two digit of any no.

$3^{41} \equiv x \pmod{100}$

$x = ?$ $\Rightarrow x = 03$

$3^4 \equiv 19 \pmod{100}$

$(3^4)^5 \equiv (19)^5 \equiv (99)^4$

$\equiv (-1) \pmod{100}$

$(3^{20})^2 \equiv (-1)^2 \pmod{100}$

$3^{40} \cdot 3 \equiv -3 \pmod{100}$

$3^{41} \equiv 03 \pmod{100}$

for three digit of any no.

$3^{41} \equiv x \pmod{10^3 = 1000}$

$x = ?$

$3 \equiv 3 \pmod{100}$

$3^2 \equiv 9 \pmod{100}$

$\Rightarrow 3^4 \equiv 81 \pmod{100}$

$\Rightarrow 3^8 \equiv (81)^2 \equiv 6561 \equiv (61) \pmod{100}$

$\Rightarrow 3^{16} \equiv (61)^2 \equiv (3721) \equiv 21 \pmod{100}$

$\Rightarrow 3^{32} \equiv (21)^2 \equiv 441 \equiv 41 \pmod{100}$

$\Rightarrow 3^{32} \cdot 3^8 \equiv 41 \cdot 61 \pmod{100}$

$\Rightarrow 3^{40} \equiv 2501 \pmod{100}$

$\equiv 01 \pmod{100}$

$\Rightarrow 3^{41} \equiv 03 \pmod{100}$

$\therefore x = 03$

FERMAT'S THEOREM

FERMAT'S LITTLE THEOREM

Theorem [5.7] P.88: Let p be a prime and suppose that $p \nmid a$. then—

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

Proof: Now consider $p-1$ positive multiple of a.

$$a, 2a, 3a, \ldots (p-1)a$$

We will show these no.s are in congruent modulo p.

Suppose these are not congruent modulo p.

~~Suppose these~~ are for $i \neq j$

$$ia \equiv ja \pmod p \quad \text{where } 1 \le i, j \le p-1$$

$$\Rightarrow p \mid (ia - ja) \Rightarrow p \mid (i-j)a$$

$$\Rightarrow p \mid (i-j)$$

but $|i-j| < p$ & $p \mid i-j$

$$\Rightarrow i-j = 0$$

$$\Rightarrow i = j$$

Which is contradiction.

These numbers $a, 2a, 3a, \ldots (p-1)a$ are congruent to $1, 2, 3 \ldots, p-1$ in some order

$$a \cdot 2a \cdot 3a \ldots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod p$$

$$\Rightarrow a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod p$$

but $\gcd(p, (p-1)!) = 1$

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

Q.(1) $17 \mid (11^{104} + 1)$ (verify using Fermat's thm)

$17 \nmid 11$

$$\Rightarrow 11^{17-1} \equiv 1 \pmod{17} \quad \text{(from Fermat's theorem)}$$

$$\Rightarrow 11^{16} \equiv 1 \pmod{17}$$

$$\Rightarrow (11^{16})^6 \equiv 1^6 \pmod{17}$$

$$\Rightarrow 11^{96} \equiv 1 \pmod{17}$$

$$\Rightarrow 11 \equiv 11 \pmod{17}$$

$$\Rightarrow 11^2 = 121 \equiv 2 \pmod{17}$$

$$\Rightarrow (11^2)^4 \equiv 2^4 \pmod{17}$$

$$\Rightarrow 11^8 \equiv 16 \pmod{17}$$

$$11^{104} = 11^{96} \cdot 11^8 \equiv$$

$$\equiv (1)(16) \pmod{17}$$

$$\Rightarrow 11^{104} \equiv 16 \pmod{17}$$

$$\equiv -1 \pmod{17} \Rightarrow 11^{104} + 1 \equiv -1+1 \equiv 0 \pmod{17}$$

Corollary (P.88) If p is a prime then $a^p \equiv a \pmod p$ $\forall a \in \mathbb{Z}$

Proof:

Case-I	Case-II
when $p \nmid a$	when $p \mid a$
$a^{p-1} \equiv 1 \pmod p$	$p \mid a \Rightarrow p \mid a^p$
$\Rightarrow a^p \equiv a \pmod p$	$p \mid a$ & $p \mid a^p$
	$\Rightarrow p \mid a^p - a$
	$\Rightarrow a^p \equiv a \pmod p$

Lemma (P.89) If p & q are distinct primes with $a^p \equiv a \pmod q$ and $a^q \equiv a \pmod p$ then $a^{pq} \equiv a \pmod{pq}$

$\Rightarrow a^p \equiv a \pmod q$

$\Rightarrow (a^p)^q \equiv a^q \pmod q$

$\Rightarrow a^{pq} \equiv a^q \pmod q$

$\Rightarrow a^{pq} \equiv a \pmod q$

$\Rightarrow q \mid a^{pq} - a$ —— (i)

$a^q \equiv a \pmod p$

$\Rightarrow (a^q)^p \equiv a^p \pmod p$

$\Rightarrow a^{qp} \equiv a \pmod p$

$\Rightarrow p \mid a^{qp} - a$ —— (2)

$\because$ p & q are distinct primes

$\Rightarrow \gcd(p, q) = 1$

from eq^n (1) & (2)

$pq \mid (a^{pq} - a)$

$\Rightarrow a^{pq} \equiv a \pmod{pq}$

Q.2(c) $\gcd(a, 133) = 1$, $\gcd(b, 133) = 1$

To show $133 \mid a^{18} - b^{18}$

Sol^n. $133 = 19 \cdot 7$

$\Rightarrow \gcd(a, 19) = 1$ & $\gcd(a, 7) = 1$

$\Rightarrow a^{18} \equiv 1 \pmod{19}$ & $a^6 \equiv 1 \pmod 7$

$\Rightarrow a^{18} \equiv 1 \pmod 7$

$\Rightarrow a^{18} \equiv 1 \pmod{133}$

Similarly $b^{18} \equiv 1 \pmod{133}$

So, $133 \mid a^{18} - b^{18}$

WILSON'S THEOREM

Thm (5.4) An integer $p > 1$ is prime iff $(p-1)! \equiv -1 \pmod p$

Suppose p is prime.

To Show $(p-1)! \equiv -1 \pmod p$.

for $p = 2$ $(2-1)! \equiv 1 \equiv -1 \pmod 2$

for $p = 3$, $(3-1)! \equiv 2 \equiv -1 \pmod 3$

Now, consider $p > 3$.

let a be any +ive integer with $\gcd(a, p) = 1$ & $a < p$

Now, consider the linear congruence

$ax \equiv 1 \pmod p$

This congruences has a unique sol^n a' with $1 \le a' \le p-1$

So,

$aa' \equiv 1 \pmod p$ for $1 \le a' \le p-1$ & $1 \le a \le p-1$

Suppose $a = a'$ then

$a^2 \equiv 1 \pmod p$

$\Rightarrow p \mid (a^2 - 1) \Rightarrow p \mid (a-1)(a+1)$

$\Rightarrow p \mid (a-1)$ or $p \mid (a+1)$

$\Rightarrow a \equiv 1 \pmod p$ or $a \equiv -1 \pmod p$

$a = 1$ or $a = p-1$

If we will have $b = p$ integer 1 & $p-1$ and proof p integer $2, 3, 4, \ldots p-2$ in pair.

a, a' $(a \ne a')$

s.t

$aa' \equiv 1 \pmod p$

$2 \cdot 3 \cdot 4 \ldots p-1 \equiv 1 \pmod p$

$\Rightarrow 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1) \equiv (p-1) \pmod p$

$\Rightarrow (p-1)! \equiv -1 \pmod p$.

Now use $\boxed{aa' \equiv 1 \pmod{13}}$

if $p = 13$ | if $p = 12$

$a = 2, a' = 7$ | $a' = 1, \ a' = 12$

$2 \cdot 7 \equiv 1 \pmod{13}$ | $a = 3, \ a' = 9$

$3 \cdot 9 \equiv 1 \pmod{13}$ | $a = 4, \ a' = 10$

$4 \cdot 10 \equiv 1 \pmod{13}$ | $a = 5, \ a' = 8$

$5 \cdot 8 \equiv 1 \pmod{13}$ | $a = 6, \ a' = 11$

$6 \cdot 11 \equiv 1 \pmod{13}$

$2 \cdot 7 \cdot 3 \cdot 9 \cdot 4 \cdot 10 \cdot 5 \cdot 8 \cdot 6 \cdot 11 \equiv 11^5 \pmod{13}$

$\Rightarrow 12! = 12 \pmod{13}$

$\Rightarrow (13-1)! \equiv -1 \pmod{13}$

$\Leftarrow$ Assume that

$(p-1)! \equiv -1 \pmod p$

T.S. p is prime.

$p \mid (p-1)! + 1$ —— (1)

Suppose p is not a prime, thus $\Rightarrow$ p has factor d s.t —

$1 < d < p$

$\Rightarrow 1 < d \leq p-1$

$\Rightarrow d \mid (p-1)!$ —— (2)

$\because d \mid p$

from eqn (1) $d \mid \{(p-1)! + 1\}$ —— (3)

from (2) & (3) ——

$d \mid 1$

which is contradiction

$\Rightarrow p$ is prime.

Que. 5.3 (p-96)

1 (a) Find the remainder when $15!$ is divided by 17.

(a) 17 is prime (Apply wilson's thm)

$16! \equiv -1 \pmod{17}$

$\Rightarrow 16 \cdot 15! \equiv -1 \pmod{17}$

$\Rightarrow (-1)\, 15! \equiv -1 \pmod{17}$

$\Rightarrow 15! \equiv 1 \pmod{17}$

→ Find the remainder when $2(26)!$ is divided by 29.

(b) 29 is prime.

$\therefore$ by wilson's theorem —

$28! \equiv -1 \pmod{29}$

$28 \cdot 27 \cdot 26! \equiv -1 \pmod{29}$

$(-2)(-1)\, 26! \equiv -1 \pmod{29}$

$2\,(26!) \equiv -1 \pmod{29}$

$\Rightarrow 2(26!) \equiv 28 \pmod{29}$

General form of quadratic Congruences

$$ax^2 + bx + c \equiv 0 \pmod n$$

with $a \not\equiv 0 \pmod n$

Theorem [5.5] (p-96) The ~~quadrict~~ quadratic Congruences $x^2 + 1 \equiv 0 \pmod p$ where p is an odd prime has a sol^n $\Leftrightarrow p \equiv 1 \pmod 4$

Proof: Suppose the quadratic congruences ~~$x^2+1=0$~~ $x^2 + 1 \equiv 0 \pmod p$ has a solution.

To show —

$p \equiv 1 \pmod 4$

p is of the form $(4k+1)$

Let a be the sol^n of quadratic Congruence $x^2 + 1 \equiv 0 \pmod p$ —— (1)

If $p \mid a$ then $p \mid a^2$

$\Rightarrow a^2 \equiv 0 \pmod p$

~~which~~ $a^2+1 \equiv 1 \pmod p$

which is contradiction

$\Rightarrow p \nmid a$

$\therefore$ from fermat's theorem —

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

$\Rightarrow (a^2)^{\frac{p-1}{2}} \equiv 1 \pmod p$

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

p is an odd prime.

p can be of the form $4k+1$ or $4k+3$

Suppose p is not of the form $4k+1$

$\Rightarrow p$ is of the form $4k+3$.

from eq^n (2) $\Rightarrow$

$(-1)^{\frac{4k+3-1}{2}} \equiv 1 \pmod p$

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

$-1 \equiv 1 \pmod p$

$\Rightarrow p \mid (-1-1)$

$\Rightarrow p \mid -2$

$\Rightarrow p = 2$

$\Rightarrow p$ is not an odd prime which is a contradiction.

If show that p is of the form $4k+1$ or

$p \equiv 1 \pmod 4$

$\Leftarrow$ Assume that $p \equiv 1 \pmod 4$

To show $x^2+1 \equiv 0 \pmod p$ has a sol^n.

p is prime.

from wilson's theorem —

$(p-1)! \equiv -1 \pmod p$

$\Rightarrow 1.2.3 \ldots \left(\frac{p-1}{2}\right)\left(\frac{p+2}{2}\right) \ldots (p-2)(p-1) \equiv -1 \pmod p$

$(p-1) \equiv -1 \pmod p$

$(p-2) \equiv -2 \pmod p$

$(p-3) \equiv -3 \pmod p$

$\vdots$

$\left(\frac{p+1}{2}\right) \equiv -\left(\frac{p-1}{2}\right) \pmod p$

Now, using these in eq^n (1), we have —

$1.2.3 \ldots \left(\frac{p-1}{2}\right)\left\{-\left(\frac{p-1}{2}\right)\right\} \ldots (-3)(-2)(-1) \equiv -1 \pmod p$

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

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

$\because p \equiv 1 \pmod 4$

$\Rightarrow p = 4k+1$

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

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

$\Rightarrow \left\{\left(\frac{p-1}{2}\right)!\right\}^2 + 1 \equiv 0 \pmod p$

$\Rightarrow x^2+1 \equiv 0 \pmod p$ has a sol^n

$x = \left(\frac{p-1}{2}\right)!$

* * *

(2) Determine whether 17 is a prime by deciding whether $16! \equiv -1 \pmod{17}$

Sol^n. Since we have —

$16! = (16)(15)(14) \cdots (2)(1)$

$= (17-1)(17-2) \cdots (17-8)(8)(7) \cdots 2.1$

$\equiv (-1)(-2) \cdots (-8)(8)(7) \cdots 2.1 \pmod{17}$

$\equiv (-1)^8 (8!)^2 \pmod{17}$

$\equiv [(8)(2)(7)(5)(6)(3)(4)]^2 \pmod{17}$

$\equiv 16 \cdot 35 \cdot 18 \cdot 4$

$\equiv (17-1)^2 (2\times17+1)^2 (17+1)^2 (17-1) \bmod 17$

$\equiv (-1)^2 (1)^2 (1)^2 (-1) \bmod 17$

$\equiv -1 \bmod 17$

$\Rightarrow$ 17 is prime no.

(3) Arrange the integers 2, 3, 4 … 21 in pairs a & b that satisfy $ab \equiv 1 \pmod{23}$

(2,12), (3,8), (4,6), (5,14), (7,10),
(9,18), (11,21), (13,16), (15,20), (17,19)

(4) Show that $18! \equiv -1 \pmod{437}$

2014

$437 = 19 \cdot 23$

By Wilson's theorem, we have —

$(19-1)! \equiv -1 \pmod{19}$

$\Rightarrow 18! \equiv -1 \pmod{19}$ — (1)

Also

$(23-1)! \equiv -1 \pmod{23}$

$\Rightarrow 22! \equiv -1 \pmod{23}$

We have $22! \equiv (23-1)(23-2)(23-3)(23-4)(18!)$

$\equiv (-1)(-2)(-3)(-4)(18!) \pmod{23}$

$\equiv (23+1)(18!) \pmod{23}$

$\equiv 1 \cdot 18! \pmod{23}$

$\Rightarrow (-1) \equiv 18! \pmod{23}$ — (2)

$\therefore$ from (1) & (2), we have —

$19 \mid (18!+1)$ & $23 \mid (18!+1)$

& $\gcd(19,23) = 1$, we get —

$(19)(23) \mid (18!+1) \Rightarrow 437 \mid (18!+1)$

$\Rightarrow 18! \equiv -1 \pmod{437}$

(5) (a) PT an integer $n>1$ is prime $\Leftrightarrow (n-2)! \equiv 1 \pmod{n}$

n is prime.

$\Leftrightarrow (n-1)!+1 \equiv 0 \pmod{n}$

$\Leftrightarrow (n-1)(n-2)!+1 \equiv 0 \pmod{n}$

$\Leftrightarrow (0-1)(n-2)!+1 \equiv 0 \pmod{n}$

$\Leftrightarrow (n-2)! \equiv 1 \pmod{n}$

(b) If n is a composite integer, show that $(n-1)! \equiv 0 \pmod{n}$, except when $n=4$.

for $n=4$, $(n-1)! = 3! = 6 \equiv 0 \pmod{4}$

Suppose $n>4$ & n is perfect sq. of a prime p, $p \geq 3$.

$\therefore$ both $p, 2p$, occurs in the product.

$(1)(2) \cdots (n-1) \Rightarrow p^2 \mid (n-1)! \Rightarrow (n-1)! \equiv 0 \pmod{n}$

→ let n be composite no., s.t $n \geq 6$ & $n = pq$ where p, q are distinct & $2 \leq p, q \leq n-1$, then —

we write $(n-1)!$ as —

$(2)(3) \cdots (n-1)$, then both p, q occurs at some places in product, therefore

$pq \mid (2)(3) \cdots (n-1) \Rightarrow n \mid (n-1)!$

$\Rightarrow (n-1)! \equiv 0 \pmod{n}$

[for $n=4$, $(n-1)! \equiv 6 \equiv 2 \not\equiv 0 \pmod{4}$]

Chapter-6

NUMBER-THEORETIC FUNCTIONS or (ARITHMETIC FUNCTIONS)

Def^n: for any positive ~~no.~~ integer n. $\tau(n)$ denotes the no. of positive divisors of n & $\sigma(n)$ denotes the sum of positive divisors of n.

$$\tau(n) = \sum_{d|n} 1$$

$$\sigma(n) = \sum_{d|n} d$$

$n = 200 \quad = 1, 2, 4, 5, 8, 10, 200, 100, 50, 40, 25, 20$

$\tau(200) = 12$

$\sigma(200) = 465$

$n = 12 \quad | \; 12 = 1, 2, 3, 4, 6, 12$

$\tau(12) = 6$

$\sigma(12) = 1+2+3+4+6+12$
$= 28$

Special Cases

\# If n is any prime no. then

$\tau(n) = 2$

$\sigma(n) = n+1$

Canonical form (or Prime factorization)

$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ & $p_1 < p_2 < \dots < p_r$

for eg $12 = 2^2 \times 3^1$ (order preserve)

$3^1 \times 2^2$ ✗

$n = 2^k p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$

$p_1 < p_2 < \dots < p_r$

Here p_i's an odd prime

Thm. 6.1 If $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ is the prime factorization of any no. $n > 1$ then the positive divisors of n are of the form

$$d = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$$

where $0 \le a_i \le k_i$
$\forall \; 1 \le i \le r$

factors $12 = \cancel{2^2 \times 3^1} \rightarrow 2^0 \times 3^0, 2^1 \times 3^0, 2^2 \times 3^0, 2^1 \times 3^1, 2^0 \times 3^1, 2^2 \times 3^1$

Theorem 6.2 If $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ is the prime factorization of any no. $n > 1$, then

$$\tau(n) = (k_1+1)(k_2+1) \dots (k_r+1)$$

$$\& \quad \sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \times \frac{p_2^{k_2+1} - 1}{p_2 - 1} \times \dots \frac{p_r^{k_r+1} - 1}{p_r - 1}$$

Proof The positive divisors d of n are of the form

$d = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ when $0 \le a_i \le k_i \quad \forall \; 1 \le i \le r$

$a_1 = 0, 1, 2, \dots k_1 \rightarrow (k_1+1)$ choices

& $a_2 = 0 \rightarrow (k_2+1)$ choices

$a_i = 0, 1, 2, \dots k_i$

here each a_i has (k_i+1) choices $\forall \; 1 \le i \le r$

Here the no. of positive divisors of n is given by —

$$\tau(n) = (k_1+1)(k_2+1) \dots (k_r+1)$$

$\sigma(n) = ?$

Page No. 72 Date 9/2/15

Consider the no. $p_1^{a_1}$ —

Its positive divisors are $1, p_1, p_1^2, \ldots$

$\ldots p_1^{k_1-1}, p_1^{a_1}$.

Sum of all positive divisors of $p_1^{a_1}$ is given by —

$$1 + p_1 + p_1^2 + \cdots + p_1^{k_1-1} + p_1^{k_1}$$

||ly

Sum of all positive divisors of $p_2^{a_2}$ is given by —

$$p_2^{a_2} = 1 + p_2 + p_2^2 + \cdots + p_2^{k_2-1} + p_2^{k_2}$$

In general, sum of all divisors of $p_i^{a_i}$ ($\forall\ 1 \le i \le r$) is given by —

$$1 + p_i + p_i^2 + \cdots + p_i^{k_i-1} + p_i^{k_i}$$

Here these p_i's are distinct primes so, the sum of all positive divisors of n is given by —

$$\tau(n) = (1 + p_1 + p_1^2 + \cdots + p_1^{k_1-1} + p_1^{k_1})(1 + p_2 + p_2^2 + \cdots + p_2^{k_2-1} + p_2^{k_2}) \cdots (1 + p_r + p_r^2 + \cdots + p_r^{k_r-1} + p_r^{k_r})$$

we know that —

$$1 + p_i + p_i^2 + \cdots + p_i^{k_i-1} + p_i^{k_i} = \frac{p_i^{k_i+1} - 1}{p_i - 1}$$

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}$$

Page No. 73 Date 9/2/15

Ex (1) $\tau(200) = (3+1)(2+1) = 12$

$\sigma(200) = 465$

$200 = 2^3 \times 5^2$

$$\sigma(200) = \frac{2^{3+1} - 1}{2 - 1} \times \frac{5^{2+1} - 1}{5 - 1}$$

$$= 15 \times \frac{124}{4} = 15 \times 31 = 465$$

if $n_1 < n_2$

then $\not\Rightarrow$ $\tau(n_1) < \tau(n_2)$

also $\not\Rightarrow$ $\sigma(n_1) < \sigma(n_2)$

(2)

$180 = 2^2 \times 3^2 \times 5$

$\tau(180) = (2+1)(2+1)(1+1)$

$= 3 \times 3 \times 2 = 18$

$$\sigma(180) = \frac{2^3 - 1}{2 - 1} \times \frac{3^3 - 1}{3 - 1} \times \frac{5^2 - 1}{5 - 1}$$

$$= 7 \times 13 \times \frac{24}{4} = 7 \times 13 \times 6$$

$= 42 \times 13 = 546$

Defn (6.2) MULTIPLICATIVE FUNCTION

A number theoretic f^n is called multiplicative if

$$f(mn) = f(m) f(n)$$

whenever $\gcd(m, n) = 1$

$$\left(\begin{array}{l} \tau(1) = 1 \\ \sigma(1) = 1 \end{array} \right)$$

Theorem (6.3) (p. 107) τ & σ are both multiplicative f^ns

If

$$\tau(mn) = \tau(m)\,\tau(n)$$

& $$\sigma(mn) = \sigma(m)\,\sigma(n)$$

Case-I when $m=1,\ n>1$

$$\tau(mn) = \tau(n) = 1\cdot\tau(n) = \tau(1)\,\tau(n)$$
$$= \tau(m)\tau(n)$$

Ilmly $$\sigma(mn) = \sigma(n) = 1\cdot\sigma(n) = \sigma(1)\cdot\sigma(n)$$
$$= \sigma(m)\,\sigma(n)$$

Case-II when $m>1,\ n=1$

$$\tau(mn) = \tau(m) = \tau(m)\cdot 1 = \tau(m)\,\tau(1)$$
$$= \tau(m)\,\tau(n)$$
$$\sigma(mn) = \sigma(m)\cdot 1 = \sigma(m)\,\sigma(1)$$
$$= \sigma(m)\,\sigma(n).$$

Case-III when $m>1,\ n>1$ with $\gcd(m,n)=1$

$\tau(mn)$

Suppose the prime factorization of m is given by —

$$m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

& the prime factors of n is given by

$$n = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$$

Since $\gcd(m,n) = 1$

$\Rightarrow \gcd(m,n) = 1$

$\Rightarrow p_i \neq q_j \quad \forall\ 1 \le j \le r$

$$mn = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}\, q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$$
$1 \le j \le s$

$$\therefore \tau(mn) = (a_1+1)(a_2+1)\cdots(a_r+1)(b_1+1)(b_2+1)\cdots(b_s+1)$$
$$= [(a_1+1)\cdots(a_r+1)][(b_1+1)\cdots(b_s+1)]$$
$$= \tau(m)\cdot\tau(n)$$

Now

$$\sigma(mn) = \frac{p_1^{a_1+1}-1}{p_1-1}\cdot\frac{p_2^{a_2+1}-1}{p_2-1}\cdots\frac{p_r^{a_r+1}-1}{p_r-1}\times$$
$$\frac{q_1^{b_1+1}-1}{q_1-1}\cdot\frac{q_2^{b_2+1}-1}{q_2-1}\cdots\frac{q_r^{b_r+1}-1}{q_r-1}$$
$$= \sigma(m)\,\sigma(n)$$

Thus τ and σ both are multiplicative functions.

Lemma (P. 108) If $\gcd(m,n)=1$ then the set of positive divisors of mn consists of all products d_1d_2, where $d_1|m$ & $d_2|n$ & $\gcd(d_1,d_2)=1$ moreover, these products are all distinct.

Proof: Assume that $m>1,\ n>1$

Suppose the prime factor of m is given by

$$m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

& the prime factorization of n is given by —

$$n = q_1^{b_1} q_2^{b_2} \cdots q_r^{b_r}$$

$\gcd(m,n)=1 \Rightarrow p_i \neq q_j \quad \forall\ 1 \le j \le r$

$mn = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}, \quad 1 \le j \le s$

Hence any positive divisor d of mn is of the form

$$d = p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r} q_1^{e_1} q_2^{e_2} \cdots q_s^{e_s}$$

where $0 \le c_i \le a_i$ & $0 \le e_i \le b_i$

$$\Rightarrow d = (p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r})(q_1^{e_1} q_2^{e_2} \cdots q_s^{e_s})$$
$$= d_1 d_2$$

where $d_1 = p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}$ $(1 \le c_i \le a_i)$

& $d_2 = q_1^{e_1} q_2^{e_2} \cdots q_s^{e_s}$ $(1 \le e_i \le b_i)$

is positive divisors of n.

Since $p_i \ne q_j \Rightarrow \gcd(d_1, d_2) = 1$

Theorem 6.4 (P-109) 2014

If f is a multiplicative function and F is defined by

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

then F is also multiplicative.

Proof. let $\gcd(m,n) = 1$

If $F(mn) = F(m)F(n)$

$$F(mn) = \sum_{d \mid mn} f(d)$$

$$= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1 d_2) \quad \text{where } \gcd(d_1, d_2) = 1$$

$$\Rightarrow F(mn) = \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1) f(d_2) \quad [\because f \text{ is multiplicative}]$$

$$= \left(\sum_{d_1 \mid m} f(d_1)\right)\left(\sum_{d_2 \mid n} f(d_2)\right)$$

$$= F(m) F(n)$$

$\Rightarrow F$ is multiplicative

11-02-15 * * *

(6.2) Mobius Inversion formula :-

Def^n (6.3) Mobius μ function:- For a +ve integer n, mobius μ-function is defined as

$$\mu n = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{if } p^2 \mid n \text{ for some prime } p \\ (-1)^r, & \text{if } n = p_1 p_2 p_3 \cdots p_r \end{cases}$$

where p_i's are primes.

Thm (6.5) Theorem:- The function μ is a multiplicative functions.

Prf:-

Case-I when $m = 1$ or $n = 1$

$\mu(mn) = \mu(m)\,\mu(n)$

trivially, $\mu(mn) = \mu(m)\,\mu(n)$ $[\because \mu(1) = 1]$

Case-II when $p^2 \mid m$ or $p^2 \mid n$ for some prime p.

If $p^2 \mid m$ or $p^2 \mid n$

then $p^2 \mid mn$

$\Rightarrow \mu(mn) = 0$

$p^2 \mid m$ or $p^2 \mid n$

$\Rightarrow \mu(m) = 0$ or $\mu(n) = 0$

$\Rightarrow \mu(m)\mu(n) = 0$

In this case, we have

$\mu(mn) = \mu(m)\mu(n)$

Case-III

when both m & n are squre free integers with

$\gcd(m,n) = 1$

$m = p_1 p_2 p_3 \ldots p_r$, $n = q_1 q_2 q_3 \ldots q_s$

Here $p_i \neq q_j \ \forall \ 1 \le i \le r, 1 \le j \le s$

$mn = p_1 p_2 \ldots p_r q_1 q_2 \ldots q_s$

$\mu(mn) = (-1)^{r+s} = (-1)^r (-1)^s = \mu(m)\mu(n)$

It shows that μ is a multiplicative function

Theorem:- (6.6) for each positive integers $n \ge 1$

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{if } n > 1 \end{cases}$$

Prf:- for $n = 1$,

$$\sum_{d \mid 1} \mu(d) = \mu(1) = 1$$

Assume that $n > 1$

for $n > 1$, define $F(n) = \sum_{d \mid n} \mu(d)$ — (1)

$F(p^k) = \sum_{d \mid p^k} \mu(d)$ $[p^k \rightarrow 1, p, p^2, \ldots p^{k-1}, p^k]$

$= \mu(1) + \mu(p) + \mu(p^2) + \ldots + \mu(p^k)$

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

$= +1 - 1 = 0$

Now assume that the prime ~~functions~~ Factorization of n is

$n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$

$F(n) = F(p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r})$

$= F(p_1^{k_1}) F(p_2^{k_2}) \ldots F(p_r^{k_r})$

[$\because$ μ is multiplicative from eqn (1), F is also multiplicative]

$= 0 \cdot 0 \cdot 0 \ldots 0$

$= 0$

$F(n) = 0$

$\Rightarrow \sum_{d \mid n} \mu(d) = 0 \quad \forall \ n > 1$

Result :- $n = d \cdot \frac{n}{d}$

$d \mid n \Leftrightarrow \frac{n}{d} \mid n$

Prf:- $\sum_{d \mid n} f(d) = \sum_{d \mid n} f\left(\frac{n}{d}\right) = \sum_{\frac{n}{d} \mid n} f(d)$

$= \sum_{\frac{n}{d} \mid n} f\left(\frac{n}{d}\right)$

6.3 Question (8). Show that

$$\sum_{d|n} \frac{1}{d} = \frac{\sigma(n)}{n} \quad \forall n \in \mathbb{Z}^+$$

SOL^n

$$n\sum_{d|n}\frac{1}{d} = \sum_{d|n}\frac{n}{d} = \sum_{d|n} d = \sigma(n)$$

$$\Rightarrow \sum_{d|n}\frac{1}{d} = \frac{\sigma(n)}{n}$$

Q. (9) If n is a square free integer then $\tau(n) = 2^r$, where r is the number of prime divisors of n.

Sol^n

$n = p_1 p_2 \cdots p_r$

$$\tau(n) = (1+1)(1+1)\cdots(1+1)(r \text{ times})$$
$$= 2\cdot 2 \cdots 2 \,(r \text{ times})$$
$$= 2^r$$

See [6.4]

Mobius Inversion Formula

:→ Let F and f be two number-theoretic functions related by the formula.

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

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

$$= \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$$

Prf:- If $d|n \Leftrightarrow \frac{n}{d}|n$

So, trivially

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

Now,

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

$$= \sum_{d|n} \sum_{c|\frac{n}{d}} \mu(d) f(c) \quad \text{---} \quad (1)$$

Claim, $d|n$ & $c|\frac{n}{d} \Leftrightarrow c|n$ & $d|\frac{n}{c}$

Let $d|n$ & $c|\frac{n}{d}$

$\Rightarrow n = dk_1$ & $\frac{n}{d} = ck_2$

$\therefore n = dck_2 \Rightarrow c|n$

$\Rightarrow \frac{n}{c} = dk_2$

$\Rightarrow d|n/c$

Conversly ($\Leftarrow$)

Let $c|n$ & $d|\frac{n}{c}$

~~$\Rightarrow n = ck_1$ & $\frac{n}{c} = dk_2$~~ $d = \frac{n}{c} k_2$

~~$\Rightarrow n = cdk_2 \Rightarrow d|n$~~

$\Rightarrow n = ck_1$ & $\frac{n}{c} = dk_2$

$\Rightarrow n = cdk_2$

$d \mid n$

$\frac{n}{d} = ck_2 \Rightarrow c \mid \frac{n}{d}$

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

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

$$= \sum_{c=n} f(c) \cdot 1 = f$$

$$\left\{ \begin{array}{l} \because \sum_{d|n} \mu(d) = \begin{cases} 1, & n=1 \\ 0, & n>1 \end{cases} \\ \sum_{d|\frac{n}{c}} \mu(d) = \begin{cases} 1, & c=n \\ 0 & c \neq n \end{cases} \end{array} \right\}$$

$$= f(n)$$

from eqn (1)

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = F(n)$$

(6.8) Theorem :- If F is a multiplicative Function and $F(n) = \sum_{d|n} f(d)$

then f is also multiplicative

Prf :- Let $m, n \in \mathbb{Z}^+$ such that $\gcd(m,n) = 1$

To show,

$f(mn) = f(m) f(n)$

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

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

$$f(mn) = \sum_{d|mn} \mu(d) F\left(\frac{mn}{d}\right)$$

[If $d \mid mn$ & $\gcd(m,n) = 1$ then $d = d_1 d_2$ where $d_1 \mid m$ & $d_2 \mid n$ with $\gcd(d_1, d_2) = 1$

$$= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1 d_2) F\left(\frac{mn}{d_1 d_2}\right)$$

$$= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1) \mu(d_2) F\left(\frac{m}{d_1}\right) F\left(\frac{n}{d_2}\right)$$

$$= \sum_{d_1|m} \mu(d_1) F\left(\frac{m}{d_1}\right) \sum_{d_2|n} \mu(d_2) F\left(\frac{n}{d_2}\right)$$

$$= f(m) f(n)$$

$\Rightarrow$ f is multiplicative

Question (1) (a) for all $n \in \mathbb{Z}^+$

$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$

(b) $\forall\, n \geq 3$,

show that $\sum_{k=1}^{n} \mu(k!) = 1$

Solⁿ :- (b) $\forall\, n \geq 3$

To show $\sum_{k=1}^{n} \mu(k!) = 1$

$\mu(1) + \mu(1.2) + \mu(1.2.3) + 0 + 0 + 0 \cdots 0$

$\Rightarrow 1 + (-1) + 1$

$= 1.$

Solⁿ (a) $n \equiv 0$ or 1 or 2 or 3 (mod 4)

$\Rightarrow n \equiv 0 \pmod 4$ or $(n+3) \equiv 0 \pmod 4$

or $(n+2) \equiv 0 \pmod 4$
or $(n+3) \equiv 0 \pmod 4$

$\Rightarrow 2^2 | n$ or $2^2 | (n+3)$ or $2^2 | (n+2)$ or $2^2 | (n+1)$

$\Rightarrow \mu(n) = 0$ or $\mu(n+3) = 0$ or $\mu(n+2) = 0$ or $\mu(n+1) = 0$

$\Rightarrow \mu(n)\,\mu(n+1)\,\mu(n+2)\,\mu(n+3) = 0$

$\Rightarrow f(m)\, f(n)$

$\Rightarrow f$ is multiplicative

* * *

13/02/15

6.3 Greatest Integer function ($[x]$)

for any arbitrary real no. x, the greatest integer function denoted by $[x]$ is the largest integer $\le x$

i.e $[x]$ is the unique integer satisfying
$$x-1 < [x] \le x.$$

$[\sqrt{3}] = 1$, $[\pi/2] = 1$, $[-e] = -3$

$[\pi] = 3$, $[-\pi] = -4$

Theorem 6.9 If n is a positive integer and p is a prime, then the exponent of the highest power of p that divides $n!$ is
$$\sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$$
where the series is finite, bcz $\left[\frac{n}{p^k}\right] = 0$ for $p^k > n$.

Proof:- Among the first ~~[illegible]~~ n positive integers,

those divisible by p are $p, 2p, 3p, \dots tp$

where $tp \le n$ {t is the largest integer s.t $tp < n$}

i.e t is largest integer s.t $t = \frac{n}{p}$

$\Rightarrow \left[\frac{n}{p}\right] = t$

therefore there are exactly $\left[\frac{n}{p}\right]$ multiples of p that occuring in the product of $n!$

Among the first n positive integer those are divisible by p^2 are

$p^2, 2p^2, 3p^2, \dots t_1p^2, \dots t_1p^2 \le n$

where t_1 is the largest integer s.t

$t_1 = \frac{n}{p^2} \Rightarrow \left[\frac{n}{p^2}\right] = t_1$

therefore there are exactly $\left[\frac{n}{p^3}\right]$ multiples of p^2. that occuring in the product of $n!$

Illy there are exactly $\left[\frac{n}{p^3}\right]$ multiples of p^3 that occuring in the product of $n!$

After a finite no. of representation of this process, we obtain that the exponent of highest power of p that divides $n!$ is
$$\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right] = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots$$
$$= \sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$$

Theorem

Q 6.10 If n and r are positive integers with $1 \le r \le n$, then the binomial co-efficient

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$ is also an integer

Pf:- we know that for any two +ve real number a & b.

$$[a+b] \ge [a] + [b]$$

and $n = r + (n-r)$

$\Rightarrow \frac{n}{p^k} = \frac{r}{p^k} + \frac{(n-r)}{p^k}$ where p is any prime

$$\Rightarrow \left[\frac{n}{p^k}\right] = \left[\frac{r}{p^k} + \frac{(n-r)}{p^k}\right] \ge \left[\frac{r}{p^k}\right] + \left[\frac{n-r}{p^k}\right]$$

$$\Rightarrow \left[\frac{n}{p^k}\right] \ge \left[\frac{r}{p^k}\right] + \left[\frac{n-r}{p^k}\right]$$

$$\Rightarrow \sum_{K=1}^{\infty}\left[\frac{n}{p^k}\right] \ge \sum_{K=1}^{\infty}\left[\frac{r}{p^k}\right] + \sum_{K=1}^{\infty}\left[\frac{n-r}{p^k}\right] \quad (1)$$

in eqn (1) —

the L.H.S is the highest power p that divides $n!$ and

the RHS is the highest power of p that divides $r!(n-r)!$.

So, p appears in the numerator of $\frac{n!}{r!(n-r)!}$ at least as many times as it occurs in the denominator.

It is true for every prime divisor p

$\Rightarrow$ $r!(n-r)!$ divides $n!$

$\Rightarrow \binom{n}{r} = \frac{n!}{r!(n-r)!}$ is an integer.

Corollary: for a positive integer r, ~~the product~~ the product of any r consecutive positive integers is divisible by $r!$

Pf: ~~The~~ let r consecutive integers are $n, n-1, n-2, \dots n-(r-1)$

we have

$$n(n-1)(n-2)\dots(n-(r-1))$$

$$= \frac{n(n-1)(n-2)\dots(n-(r-1))(n-r)\cdot(n-(r+1))\cdots 3.2.1}{(n-r)(n-(r+1))\dots 3.2.1}$$

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

we know that $\binom{n}{r}$ is an integer

$\Rightarrow$ $r!$ divides $n(n-1)(n-2)\dots(n-(r-1))$

Thm (6.11) let f & F be number-theoretic functions such that $F(n) = \sum_{d|n} f(d)$.

(statement only) Then, for any positive integer N.

$$\sum_{n=1}^{N} F(n) = \sum_{K=1}^{N} f(k)\left[\frac{N}{K}\right]$$

Corollary: 8(2) If N is a positive integer, then

$$\sum_{n=1}^{N} \tau(n) = \sum_{n=1}^{N} \left[\frac{N}{n}\right]$$

and

$$\sum_{k=1}^{N} \sigma(n) = \sum_{k=1}^{N} k\left[\frac{N}{k}\right]$$

And verify these result for $N = 6$

$\tau(n) = \sum_{d|n} 1$ (if $F(n) = \sum_{d|n} f(d)$)

$$\Rightarrow \sum_{n=1}^{N} \tau(n) = \sum_{k=1}^{N} 1 \cdot \left[\frac{N}{k}\right] = \sum_{k=1}^{N} \left[\frac{N}{k}\right]$$

$\sigma(n) = \sum_{d|n} d$

$$\Rightarrow \sum_{k=1}^{N} \sigma(n) = \sum_{k=1}^{N} k\left[\frac{N}{k}\right]$$

for $N = 6$

$$\sum_{n=1}^{6} \tau(n) = \tau(1)+\tau(2)+\tau(3)+\tau(4)+\tau(5)+\tau(6)$$
$$= 1+2+2+3+2+4$$
$$= 14$$

Example: Verify that 50! terminates in 12 zeros.

Sol: Highest power of 2 that divides 50! is —

$$\sum_{k=1}^{\infty} \left[\frac{50!}{2^k}\right]$$
$$= [25] + [12.5] + [6.25] + [3.125] + [1.56] + [0.756] + \dots$$
$$= 25+12+6+3+1+0 = 47$$

Highest power of 5 that divides 50! is

$$\sum_{k=1}^{\infty} \left[\frac{50!}{5^k}\right] = [10] + [2] + [0.4] + \dots$$
$$= 10+2$$
$$= 12$$

$\Rightarrow$ 50! terminates in 12 zeros.

(Problems of 6.3 on back side) — p-203

* * *

6/02/15

CHAPTER - 7

Euler's Phi function ($\phi(n)$)

Def^n [7.1] for $n \geq 1$, $\phi(n)$ is the no. of integers less than n that are relatively prime to n.

$$S = \{m : 1 \leq m < n, \gcd(m,n) = 1\}$$

then $\phi(n) = o(S)$

$\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$ (1, 2)

$\phi(4) = 2$ $(1, \cancel{2}, 3 = 2)$ $\phi(5) = 4$ (1, 2, 3, 4)

$\phi(6) = 2$ $(1, \cancel{2}, \cancel{3}, \cancel{4}, 5)$

If p is a prime then

$\phi(p) = p-1$ $(1, 2, 3 \dots p-1)$

Result: ϕ is a multiplicative function i.e if $\gcd(m,n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$

Theorem 7.1 If the integer $n>1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ then

$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1})$$

$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$$

then $\phi(n) = O(s)$

Proof: let p be the prime.
then $\gcd(p^k, n) = 1 \Leftrightarrow p \nmid n$.

Now consider the integers betn 1 & p^k, that are divisible by p.
$p, 2p, 3p, 4p, 5p, \dots (p^{k-1})p$

These are p^{k-1} integers.
$\Rightarrow$ The set $\{1, 2, 3, \dots p^k\}$ has $p^k - p^{k-1}$

$$\boxed{\phi(p^k) = \mathrm{Card}\{m : 1 \le m < p^k : \gcd(m, p^k) = 1\}}$$

elements that are relatively prime to p^k.

$$\Rightarrow \phi(p^k) = p^k - p^{k-1} \quad \text{--- (1)}$$

Since, the ~~prime factorization~~ integer $n>1$ has the prime factorization
$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ then

$$\phi(n) = \phi(p_1^{k_1})\,\phi(p_2^{k_2}) \cdots \phi(p_r^{k_r})$$

$\{\because p_1, p_2, \dots p_r$ are distinct primes and ϕ is ~~___~~ multiplicative fn.$\}$

$$= (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1})$$

$$= p_1^{k_1}\left(1-\frac{1}{p_1}\right) p_2^{k_2}\left(1-\frac{1}{p_2}\right)\cdots p_r^{k_r}\left(1-\frac{1}{p_r}\right)$$

$$= p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$$

$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$$

Eg $\phi(360) = 96$
$\phi(16) = 8$
$(1, 3, 5, 7, 9, 11, 13, 15)$

$\phi(360) = 96$

$360 = 2^3 \times 3^2 \times 5$

$\therefore \phi(n) = 360\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$

$= \overset{12}{\cancel{360}} \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5}$

$= 24 \times 4 = 96$

Lemma:

(7.1) Given integers a, b, c, $\gcd(a, bc) = 1$
$\Leftrightarrow \gcd(a, b) = 1$ & $\gcd(a, c) = 1$

Proof: Let $\gcd(a, bc) = 1$
Suppose $\gcd(a, b) = d \ne 1$

$\Rightarrow d \mid a$ & $d \mid b$

$\Rightarrow d \mid a$ & $d \mid bc \Rightarrow$ ~~gcd(a, bc) = 1~~

$\Rightarrow \gcd(a, bc) \ge d$

Now $\gcd(a, c) = d \ne 1$
$d \mid a$ & $d \mid c \Rightarrow d \mid a$ & $d \mid bc$
$\Rightarrow \gcd(a, bc) \ge d$

$\Rightarrow \gcd(a,b)=1$ & $\gcd(a,c)=1$

$\Leftarrow$ Assume that $\gcd(a,b)=1$ & $\gcd(a,c)=1$

T.S $\gcd(a,bc)=1$

Suppose $\gcd(a,bc)=d\neq 1$

$\Rightarrow d>1$

~~then $d|a$ & $d|bc$~~

$\Rightarrow$ d has a prime factor p.

$\because \gcd(a,bc)=d \Rightarrow d|a$ & $d|bc$

$\Rightarrow p|a$ & $p|bc$

$\Rightarrow p|a$ & $p|b$ or $p|c$

$\Rightarrow \underbrace{p|a \,\&\, p|b}$ or $\underbrace{p|a \,\&\, p|c}$

$\Rightarrow \gcd(a,b)\geq p$ or $\gcd(a,c)\geq p$

$\Rightarrow \gcd(a,b)\neq 1$ or $\gcd(a,c)\neq 1$

$\longrightarrow \longleftarrow$

$\Rightarrow \gcd(a,bc)=1$

lemma (p-137) let $n>1$ and $\gcd(a,n)=1$. If $a_1, a_2 \dots a_{\phi(n)}$ are positive integers less than n and relatively prime to n. then $aa_1, aa_2, \dots aa_{\phi(n)}$ are congruent modulo n to $a_1, a_2 \dots a_{\phi(n)}$ in some order.

Pf:- First we will show that $aa_1, aa_2, \dots aa_{\phi(n)}$ are incongruent modulo n.

suppose for $i\neq j$

$aa_i \equiv aa_j \pmod n$

$\Rightarrow a_i \equiv a_j \pmod n$ $[\gcd(a,n)=1]$

$\longrightarrow \longleftarrow$

for any ~~integer~~ $1\leq i\leq \phi(n)$

$\gcd(aa_i, n)=1$ $[\because \gcd(a,n)=1$ & $\gcd(a_i,n)=1 \;\forall\; 1\leq i\leq\phi(n)]$

$\Rightarrow aa_1, aa_2, \dots aa_{\phi(n)}$ are incongruent modulo n & relatively prime to n.

$[a=n,\ b=a,\ c=a_i]$

for any i ($1\leq i\leq \phi(n)$)

let $aa_i \equiv b \pmod n$, where $0\leq b<n$

$\Rightarrow \gcd(aa_i, n)=1$

$\Rightarrow \gcd(b,n)=1$ & $1\leq b<n$

$\Rightarrow b\in\{a_1, a_2, \dots a_{\phi(n)}\}$

$\Rightarrow$ b must be one of the integers $a_1, a_2, \dots a_{\phi(n)}$

$\Rightarrow aa_1, aa_2 \dots aa_{\phi(n)}$ are congruent to $a_1, a_2, \dots a_{\phi(n)}$ modulo n in some order

Euler's Theorem
(Generalization of fermat's theorem)

Theorem 7.5 (p-137) If $n\geq 1$, and $\gcd(a,n)=1$ then
$$a^{\phi(n)}\equiv 1 \pmod n$$

pf: for $n=1$

$\phi(1)=1$ & $1 \mid (a-1)$

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

Now assume that $n > 1$ & let $a_1, a_2, \dots a_{\phi(n)}$ be positive integers less than n and relatively prime to n.

given that $\gcd(a, n) = 1$

$\Rightarrow aa_1, aa_2, \dots aa_{\phi(n)}$ are congruent modulo n to $a_1, a_2 \dots a_{\phi(n)}$ in some order

$(aa_1)(aa_2)\dots(aa_{\phi(n)}) \equiv a_1 a_2 \dots a_{\phi(n)} \pmod n$

$\Rightarrow a^{\phi(n)}(a_1 a_2 \dots a_{\phi(n)}) \equiv a_1 a_2 \dots a_{\phi(n)} \pmod n$ — (1)

$\because \gcd(a_i, n) = 1 \ \forall\ 1 \le i < \phi(n)$

$\Rightarrow \gcd(a_1 a_2 \dots a_{\phi(n)}, n) = 1$

from eq^n (1) $a^{\phi(n)} \equiv 1 \pmod n$

[7.4] SOME PROPERTIES OF THE PHI FUNCTION

Theorem [7.6] (p-141) Gauss

for each positive integer $n \ge 1$

$$n = \sum_{d \mid n} \phi(d)$$

for $n = 1$

$$\sum_{d \mid 1} \phi(d) = \phi(1) = 1$$

Now Assume for $n > 1$

Suppose prime factorization of n is

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$$

let $F(n) = \sum_{d \mid n} \phi(d)$ — (1)

$\because \phi(n)$ is multiplicative $\Rightarrow F$ is multiplicative.

$\because F(n) = \sum_{d \mid n} f(d)$ if f is multiplicative $\Rightarrow F$ is multiplicative

for any prime p

$$F(p^k) = \sum_{d \mid p^k} \phi(d)$$

$\because$ the divisors of p^k are $1, p, p^2 \dots p^{k-1}, p^k$

$\therefore F(p^k) = \phi(1) + \phi(p) + \phi(p^2) + \dots + \phi(p^{k-1}) + \phi(p^k)$

$= 1 + (p-1) + (p^2 - p) + (p^3 - p^2) + \dots + (p^{k-1} - p^{k-2}) + (p^k - p^{k-1})$

$= p^k$

$\because n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$

$\Rightarrow F(n) = F(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r})$

$= F(p_1^{k_1}) F(p_2^{k_2}) \dots F(p_r^{k_r})$

($\because F$ is multiplicative & p_i are distinct primes)

$= p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$

$= n$

$\Rightarrow \sum_{d \mid n} \phi(d) = n$ (from eq^n (1))

Theorem For $n > 2$, $\phi(n)$ is an even integer.

Proof: Case-I, when n is a power of 2.

$n = 2^k$ for some $k \in \mathbb{Z}^+$ & $k \neq 1$.

$$\phi(n) = \phi(2^k) = 2^k\left(1 - \tfrac{1}{2}\right)$$
$$= 2^{k-1} = \text{even integer}$$

Case-II, when n is not a power of 2.

In this case, n is divisible by some odd prime p.

We can write $n = p^k m$ where $p \nmid m$

$$\phi(n) = \phi(p^k) \cdot \phi(m)$$
$$= p^{k-1}(p-1)\,\phi(m)$$
$$= \text{even integer}$$

$\because p$ odd prime $\Rightarrow (p-1) \rightarrow$ even no.

Theorem For $n > 1$, the sum of the positive integers less than n and relatively prime to n is $\frac{n\,\phi(n)}{2}$.

Proof: let $a_1, a_2, a_3, \ldots, a_{\phi(n)}$ be the '$\phi(n)$' integers, which are less than n and relatively prime to n.

We know that

$$\gcd(a, n) = 1 \Leftrightarrow \gcd(n-a, n) = 1$$

the integers are -

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

suppose $\gcd(n-a, n) = d \Rightarrow d \mid (n-a)$ & $d \mid n$

$\Rightarrow d \mid n - (n-a)$

$\Rightarrow d \mid a$

$\Rightarrow \gcd(a, n) \geq d$

IIly $\Leftarrow$ can be done

the integers are

$\Rightarrow (n-a_1), (n-a_2), \ldots, (n-a_{\phi(n)})$ are equal to $a_1, a_2, \ldots, a_{\phi(n)}$ in some order.

$$\Rightarrow (n-a_1) + (n-a_2) + \cdots + (n-a_{\phi(n)}) = a_1 + a_2 + \cdots + a_{\phi(n)}$$

$$\Rightarrow 2(a_1 + a_2 + \cdots + a_{\phi(n)}) = n\,\phi(n)$$

$$\Rightarrow a_1 + a_2 + a_3 + \cdots + a_{\phi(n)} = \frac{n\,\phi(n)}{2}$$

so $\frac{n\,\phi(n)}{2}$ is an integer $\forall n$

Theorem For any positive integer n

$$\phi(n) = n \sum_{d \mid n} \frac{\mu(d)}{d}$$

Pf:— let $F(n) = n = \sum_{d \mid n} \phi(d)$

$$\Rightarrow F(n) = \sum_{d \mid n} \phi(d)$$

[mobius inversion formula]

$$\Rightarrow \phi(n) = \sum_{d \mid n} \mu(d)\, F\left(\frac{n}{d}\right)$$

$$= \sum_{d \mid n} \mu(d)\frac{n}{d} = n \sum_{d \mid n} \frac{\mu(d)}{d}$$

7.2 (16) Show that the Goldbach Conjecture implies that for each even integer $2n$, there exists integers n_1 & n_2 with $\phi(n_1) + \phi(n_2) = 2n$

Sol^n:-

$2 = \phi(1) + \phi(1)$

$4 = \phi(3) + \phi(3)$

for every $n > 1$

$2(n+1) = p_1 + p_2$

$\Rightarrow 2n = (p_1 - 1) + (p_2 - 1)$

$\Rightarrow 2n = \phi(p_1) + \phi(p_2)$

$f(m) = f(m \cdot 1)$
$\Rightarrow f(m) f(1)$
$\Rightarrow f(m)(1 - f(1)) = 0$

Reduced set of Residues modulo n

for given $n > 1$, the set of $\phi(n)$ integers that are relatively prime to n & that are incongruent modulo n, is called a Reduced set of Residues modulo n.

Ques (12) (b) $3, 3^2, 3^3, 3^4, 3^5, 3^6$ form a RSR modulo 14

7.4 (3) Show that $\sum_{d|n} \frac{\mu^2(d)}{\phi(d)} = \frac{n}{\phi(n)}$

Sol^n

for $n = 1$

for $n > 1$, $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$

Let $F(n) = \sum_{d|n} \frac{\mu^2(d)}{\phi(d)}$

$\Rightarrow$ Since $\mu(d)$ is multiplicative, so $\mu^2(d)$ ________

Also $\phi(d)$ ________

So $\frac{\mu^2(d)}{\phi(d)}$ ________

$\Rightarrow F$ is multiplicative,

for any prime p.

$F(p^k) = \sum_{d|p^k} \frac{\mu^2(d)}{\phi(d)}$

$= \frac{\mu^2(1)}{\phi(1)} + \frac{\mu^2(p)}{\phi(p)} + \cdots + \frac{\mu^2(p^k)}{\phi(p^k)}$

$= 1 + \frac{(-1)^2}{p-1} + 0 + 0 + \cdots + 0$

$= 1 + \frac{1}{p-1} = \frac{p-1+1}{p-1}$

$= \frac{p}{p-1}$

$F(n) = F(p_1^{k_1}) F(p_2^{k_2}) \cdots F(p_r^{k_r})$

$= \frac{p_1}{p_1 - 1} \frac{p_2}{p_2 - 1} \cdots \frac{p_r}{p_r - 1}$

$$= \frac{p_1^{k_1}}{p_1^{k_1-1}(p_1-1)} \frac{p_2^{k_2}}{p_2^{k_2-1}(p_2-1)} \cdots \frac{p_r^{k_r}}{p_r^{k_r-1}(p_r-1)}$$

$$= \frac{p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}}{p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}(1-1/p_1)(1-1/p_2)\cdots(1-1/p_r)}$$

$$= \frac{n}{\phi(n)}$$

CHAPTER - 8

PRIMITIVE ROOTS

The order of an integer mod n

Def^n (8.1) Let $n>1$ and $\gcd(a,n)=1$. The order of a modulo n is the smallest positive integer k s.t $a^k \equiv 1 \pmod n$.

Notation: $O_n(a)$ or $O(a) \pmod n$ or $O(a)$

Eg. (a) find order of 2 modulo 17

$2 \equiv 2 \pmod{17}$

$2^2 \equiv 4 \pmod{17}$

$2^3 \equiv 8 \pmod{17}$

$2^4 \equiv 16 \equiv -1 \pmod{17}$

$2^5 \equiv -2 \equiv 15 \pmod{17}$

$2^6 \equiv -4 \equiv 13 \pmod{17}$

$2^7 \equiv -8 \equiv 9 \pmod{17}$

$2^8 \equiv -(-16) \equiv 1 \pmod{17}$

2 - 1
4 - 2
8 - 3
16 - 4

$\therefore O_{17}(2) = 8$

(b) 2 modulo 19

$2 \equiv 2 \pmod{19}$

$2^2 \equiv 4$

$2^3 \equiv 8$

$2^4 \equiv 16 \equiv -3$

$2^5 \equiv 32 \equiv -6$

$2^6 \equiv 64 \equiv -12$

$2^7 \equiv 128 \equiv -24 \equiv -5$

$2^8 \equiv 256 \equiv -48 \equiv -10$

$2^9 \equiv 512 \equiv -96 \equiv -20 \equiv -1$

$(2^9)^2 \equiv (-1)^2 = 1$

$O_{19}(2) = 18$

Theorem (8.1) p-139: Let the integer a have order k modulo n. Then $a^h \equiv 1 \pmod n \Leftrightarrow k \mid h$

Pf: $\Rightarrow$ Suppose $k \mid h$

$\Rightarrow h = kh_1$ where $h_1 \in \mathbb{Z}$

$a^h = a^{kh_1} = (a^k)^{h_1} \equiv (1)^{h_1} \equiv 1 \pmod n$

$\Rightarrow a^h \equiv 1 \pmod n$

$\Leftarrow$ (Conversely)

Suppose $a^h \equiv 1 \pmod n$

TP $k \mid h$ — ??

Since, the integer a have order k modulo n. so k is the smallest positive integer s.t

$a^k \equiv 1 \pmod n$.

& it is given that $a^h \equiv 1 \pmod n$

$\Rightarrow h \geq k$

by division algorithm, $\exists$ integers q & r s.t —

$h = qk + r$, where $0 \leq r < k$

$a^h \equiv 1 \pmod n$

$\Rightarrow a^{qk+r} \equiv 1 \pmod n$

$\Rightarrow a^{qk} \cdot a^r \equiv 1 \pmod n$

$\Rightarrow (a^k)^q \cdot a^r \equiv 1 \pmod n$

$\Rightarrow 1 \cdot a^r \equiv 1 \pmod n$

$\Rightarrow a^r \equiv 1 \pmod n$

$\Rightarrow r = 0$

We have $h = qk \Rightarrow k \mid h$

Result: let $n > 1$ & $\gcd(a, n) = 1$, if the integer a have order k mod n then $k \mid \phi(n)$

Ex 8.1 (3) P.T $\phi(2^n - 1)$ is a multiple of n for any $n > 1$.

Sol^n Since n is the smallest +ve integer s.t

$(2^n - 1) \mid (2^n - 1)$

$\Rightarrow 2^n \equiv 1 \bmod (2^n - 1)$

$\Rightarrow$ order of 2 modulo $(2^n - 1) = n$

$\Rightarrow n \mid \phi(2^n - 1)$

Theorem (8.2) P-143: If the integer a have order k modulo n, then $a^i \equiv a^j \pmod n \Leftrightarrow i \equiv j \pmod k$

first suppose that —

$a^i \equiv a^j \pmod n$

$\Rightarrow a^{i-j} \equiv a^0 \pmod n$

$\Rightarrow a^{i-j} \equiv 1 \pmod n$

$\Rightarrow k \mid (i-j) \Rightarrow i \equiv j \pmod k$

$\Leftarrow$ Assume that $i \equiv j \pmod k$

$\Rightarrow k \mid (i-j)$

$\Rightarrow i - j = kq$ for some $q \in \mathbb{Z}$

$\Rightarrow i = j + kq$

$a^i = a^{j+kq} = a^j (a^{kq})$

$\equiv a^j (1)^a \pmod n$

$\equiv a^j \pmod n$

$\Rightarrow a^i \equiv a^j \pmod n$

Corollary: If the integer a have order k modulo n, then the integers $a, a^2, \ldots a^k$ are incongruent modulo n.

Suppose $a^i \equiv a^j \pmod n$ where $1 \le i, j \le k$

$\Rightarrow i \equiv j \pmod k$ $\quad [\because |i-j| < k]$

$\Rightarrow k \mid (i-j)$

$\Rightarrow i-j=0$

$\Rightarrow i=j$

Theorem (8.3) If the integer a has order k modulo n and $h>0$, then a^h has order ~~$k/\gcd(h,k)$~~ ~~modulo n.~~ $\dfrac{k}{\gcd(h,k)}$ modulo n.

Proof: let $\gcd(h,k)=d$, then $\exists$ integers h_1 & k_1 s.t $h=h_1 d$ & $k=k_1 d$ where $\gcd(h_1,k_1)=1$

let the integer a^h have order r.

Now, Consider

$(a^h)^{k_1} = (a^{h_1 d})^{k/d} = a^{h_1 k}$

$\Rightarrow (a^k)^{h_1} \equiv 1^h \pmod n$

$\equiv 1 \pmod n$

$(a^h)^{k_1} \equiv 1 \pmod n$

$\Rightarrow r \mid k_1 \longrightarrow (1)$

$\Rightarrow (a^h)^r \equiv 1 \pmod n$

$\Rightarrow a^{hr} \equiv 1 \pmod n$

$O(a)=k \Rightarrow k \mid hr$

$\Rightarrow k_1 d \mid h_1 d r$

from (1) & (2) $\Rightarrow k_1 \mid h_1 r \Rightarrow k_1 \mid r \longrightarrow (2)$

$r_1 = k_1 = \dfrac{k}{d} = \dfrac{k}{\gcd(h,k)}$

Corollary: ~~let a have~~ If the integers a have order k modulo n and $h>0$. Then a^h have also order $k \Leftrightarrow \gcd(h,k)=1$.

PRIMITIVE ROOT

Defn (8.2) If $\gcd(a,n)=1$ and a is of order $\phi(n)$ mod n then a is a primitive Root of the integer n.

Q. find primitive Root of 10.

$\phi(10) = 4 \qquad (1, 3, 7, 9)$

so primitive root of $10 = 3, 7$

$1^4 \equiv 1 \pmod{10}$ ✗

$3^4 \equiv 81 \equiv 1 \pmod{10}$ ✓

Theorem (8.4) (P-150) Let $\gcd(a,n)=1$, and let $a_1, a_2, a_3 \ldots a_{\phi(n)}$ be the positive integer less than n and Relatively prime to n. If a is a primitive root of n, then —

$a, a^2, \ldots a^{\phi(n)}$

are congruent modulo n to $a_1, a_2 \ldots a_{\phi(n)}$ in some order.

Proof:- Since $\gcd(a,n)=1$

$\Rightarrow \gcd(a^h, n)=1$ for all $h \in \mathbb{Z}$

Page No. 106 Date 24 2 15

$\Rightarrow$ Any power of a is congruent to some a_i, when $1 < i < n$

Since, a is a primitive root of n

so $a, a^2, \ldots a^{\phi(n)}$ are incongruent modulo n.

Thus, these integers $a, a^2, a^3 \ldots a^{\phi(n)}$ are congruent modulo n to $a_1, a_2 \ldots a_{\phi(n)}$ in some order.

Corollary: If n has a primitive, then it has exactly $\phi(\phi(n))$ of them.

Proof:- ~~Since a~~ let a be a primitive root of n.

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

order of $a = \phi(n)$ $\quad (O(a) = \phi(n))$

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

$\Rightarrow \gcd(a^h, n) = 1 \quad \forall\ h \in \mathbb{Z}$

Any other primitive root of n is found from the set $\{a, a^2, \ldots a^{\phi(n)}\}$

The no. of powers a^k $(1 \le k \le \phi(n))$ have order $\phi(n)$ if $\gcd(k, \phi(n)) = 1$

$\Rightarrow$ There are $\phi(\phi(n))$ such integers. Thus, If n has a primitive root, it has exactly $\phi(\phi(n))$ of them.

Ex-12(b). Use the information that 3 is a primitive root of 17. find other Primitive Root.

(P-152)

Page No. 107 Date 24 2 15

$3^1, 3^2, \ldots 3^{16}$

Consider the set $\{3^k : 1 \le k \le 16\}$

$\gcd(k, 16) = 1$, 1

~~Consider the set~~

$\gcd(1,16) = 1$ $\quad$ primitive Root $= 3$

$\gcd(3,16) = 1$ $\quad$ $3^3 \equiv 10 \pmod{17}$

$\Rightarrow$ Primitive Root $= 10$?

* * *

Friday 27/02/15

Section [8.2]

(8) Let r be a primitive root of the odd prime p. Prove the following:-

(a) If $p \equiv 1 \pmod 4$, then $-r$ is also a primitive root of p.

(b) If $p \equiv 3 \pmod 4$, then $-r$ has order $\frac{(p-1)}{2}$ modulo p.

Sol^n:-

$O(r) = \phi(p) \Rightarrow p-1$

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

(a) $p \equiv 1 \pmod 4 \Rightarrow p = 4k+1$

$(-r)^{p-1} = (-1)^{p-1} \cdot r^{p-1} = (-1)^{4k} \cdot r^{p-1}$

$= r^{p-1} \equiv 1 \pmod p$

$\Rightarrow O(-r) \mid (p-1)$

Suppose $O(-r) = k < (p-1)$

$(-r)^k \equiv 1 \pmod p$

$\Rightarrow (-1)^k (r)^k \equiv 1 \pmod p$

$\Rightarrow (-1)^k \equiv 1 \pmod p$ & $r^k \equiv 1 \pmod p$

or $(-1)^k \equiv -1 \pmod p$ & $r^k \equiv -1 \pmod p$

$\Rightarrow (-1)^k \equiv 1 \pmod p$ & $r^k \equiv -1 \pmod p$

$\Rightarrow k = \frac{p-1}{2}$

$\rightarrow \leftarrow$

$\Rightarrow o(-r) = p-1$

$\Rightarrow (-r)$ is also a primitive Root of p.

Result: For $n > 2$, If a is a primitive Root of n then $a^{\frac{\phi(n)}{2}} = -1 \pmod n$

Pf: $o(a) = \phi(n)$

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

$\Rightarrow \left\{a^{\frac{\phi(n)}{2}}\right\}^2 - 1 \equiv 0 \pmod n$

$\Rightarrow \left(a^{\frac{\phi(n)}{2}} - 1\right)\left(a^{\frac{\phi(n)}{2}} + 1\right) \equiv 0 \pmod n$

$\Rightarrow \left\{a^{\frac{\phi(n)}{2}} - 1\right\} \equiv 0 \pmod n$ or

$a^{\frac{\phi(n)}{2}} + 1 \equiv 0 \pmod n$

If $a^{\frac{\phi(n)}{2}} - 1 = 0 \pmod n$

$\Rightarrow a^{\frac{\phi(n)}{2}} \equiv 1 \pmod n$

$\Rightarrow o(a) \leq \frac{\phi(n)}{2} < \phi(n)$

$\rightarrow \leftarrow$

So, we have

$a^{\frac{\phi(n)}{2}} + 1 \equiv 0 \pmod n$

$\Rightarrow a^{\frac{\phi(n)}{2}} \equiv -1 \pmod n$

(10) Use the fact that each prime p has a primitive root to give a different proof of Wilson's theorem.

Proof: Case-I $p = 2$, $(2-1)! \equiv 1 \equiv -1 \pmod 2$

Case-II $p > 2$ (odd prime)

Let r be the primitive root of p.

$\Rightarrow r, r^2, \ldots, r^{p-1}$ are congruent $a_1\ a_2$ to $1, 2, 3 \ldots p-1$ in some order

$\Rightarrow r \cdot r^2 \ldots r^{p-1} \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \pmod p$

$\Rightarrow r^{\frac{p(p-1)}{2}} \equiv (p-1)! \pmod p$ — (1)

Since r is a primitive root of p

$\Rightarrow o(r) = p-1$

$\Rightarrow r^{\frac{p-1}{2}} \equiv -1 \pmod p$

$\Rightarrow$ Using it in eqn (1), we have

$(-1)^p \equiv (p-1)! \pmod p$

$\Rightarrow -1 \equiv (p-1)! \pmod p$

$\Rightarrow (p-1)! \equiv -1 \pmod p$

Thm (8.5) **Lagrange's theorem**

If p is a prime and $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $a_n \not\equiv 0 \pmod p$ is a polynomial of degree $n \geq 1$ with integeral co-efficients, then the congruence $f(x) \equiv 0 \pmod p$ has at most n incongruent sol^n modulo p.

Proof: We proceed by induction on n.

$a_n \not\equiv 0 \pmod p$

$\Rightarrow p \nmid a_n$

$\Rightarrow \gcd(p, a_n) = 1 \quad \forall n$

$\deg(f(x)) = 1$

$\Rightarrow f(x) = a_1 x + a_0$

$f(x) \equiv 0 \pmod p \Rightarrow a_1 x + a_0 \equiv 0 \pmod p$

$\Rightarrow a_1 x \equiv -a_0 \pmod p$ —— (1)

$\because \gcd(a_1, p) = 1 \Rightarrow$ Congruence (1) have unique sol^n

Now, Assume that theorem is true for k polynomial of degree k.

Let $f(x)$ be a polynomial of degree $(k+1)$. If $f(x) \equiv 0 \pmod p$ has no sol^n then we ~~have~~ are done.

If $f(x) \equiv 0 \pmod p$ has at least one solution α.

If $f(x)$ is divided by $(x-\alpha)$ then

$f(x) = (x-\alpha)q(x) + r(x)$ where $r(x) = 0$ or $\deg(r(x)) < \deg(x-\alpha) = 1$

$\Rightarrow \deg r(x) = 0 \Rightarrow r(x) = r$ (constant)

$f(x) = (x-\alpha)q(x) + r$

$\because f(\alpha) \equiv 0 \pmod p$

$f(\alpha) = (\alpha - \alpha)q(x) + r \equiv 0 \pmod p$

$\Rightarrow r \equiv 0 \pmod p$

from eq^n (1) $f(x) \equiv (x-\alpha)q(x) \pmod p$

—— (2)

If $f(x) \equiv 0 \pmod p$ has no sol^n other than α then we are done.

If β is a sol^n of $f(x) \equiv 0 \pmod p$ other than α

$f(\beta) \equiv 0 \pmod p$

$\Rightarrow (\beta - \alpha)q(\beta) \equiv 0 \pmod p$ (from eq^n (2))

$\Rightarrow q(\beta) \equiv 0 \pmod p$

$\Rightarrow \beta$ is a sol^n of $q(x) \equiv 0 \pmod p$

is a sol^n of $q(x) \equiv 0 \pmod p$

$\because \deg q(x) = k$

And we have assume that theorem is true for poly. of deg. k

$\Rightarrow q(x) \equiv 0 \pmod p$ has at most k incongruent sol^n and therefore $f(x) \equiv 0 \pmod p$ has at most $k+1$ incongruent sol^n.

This completes the proof.

Corollary: If p is a prime number and $d \mid p-1$, then the congruence $x^d - 1 \equiv 0 \pmod p$ has exactly d sol^{n}s.

$\because d \mid (p-1) \Rightarrow p-1 = dk$ for some $k \in \mathbb{Z}$

$x^{p-1} - 1 = x^{dk} - 1 = (x^d - 1) f(x)$

where $f(x) = x^{d(k-1)} + x^{d(k-2)} + \cdots + x^d + x^d + 1$

where $d(k-1) = dk - d = p-1-d$

By Lagrange's theorem
$f(x) \equiv 0 \pmod p$ has at most
$p-1-d$ incongruent sol.s.

And by fermat's theorem —
$x^{p-1} - 1 \equiv 0 \pmod p$
has exactly $p-1$ sol^{n}s $1, 2, \ldots p-1$.

Suppose a is a sol^n of $x^{p-1}-1 \equiv 0 \pmod p$
which is not a sol^n of
$f(x) \equiv 0 \pmod p$

then $a^{p-1} - 1 \equiv 0 \pmod p$

$\Rightarrow (a^d - 1) f(a) \equiv 0 \pmod p$

$\Rightarrow a^d - 1 \equiv 0 \pmod p$ $[\because f(a) \not\equiv 0 \pmod p]$

$\Rightarrow a$ is a sol^n of $x^d - 1 \equiv 0 \pmod p$

$\Rightarrow$ Every sol^n of $x^{p-1} - 1 \equiv 0 \pmod p$
which is not a sol^n of $f(x) = 0 \pmod p$
if a sol^n of $x^d - 1 \equiv 0 \pmod p$

$\Rightarrow$ The congruence $x^d - 1 \equiv 0 \pmod p$
have at least.
$(p-1) - (p-1-d) = d$ sol^{n}s

$\because$ deg. $(x^d - 1) = d$

By Lagrange's theorem $x^d - 1 \equiv 0 \pmod p$
has at most d sol^{n}s.

Thus $x^d - 1 \equiv 0 \pmod p$ has exactly
d sol^{n}s.

Result: If p is a prime and $d \mid (p-1)$ then
there are exactly $\phi(d)$ incongruent
integers having order d modulo p.

the Q. 6)
p. 154

Theorem: If $p \equiv 1 \pmod 4$ then the congruence
$x^2 + 1 \equiv 0 \pmod p$ is solvable.

$p \equiv 1 \pmod 4 \Rightarrow 4 \mid p-1$

$\Rightarrow$ There are exactly $\phi(4) = 2$ incongruent
integral having order 4 modulo p.

let a be any integers of order 4.

$\therefore a^4 \equiv 1 \pmod p \Rightarrow a^4 - 1 \equiv 0 \pmod p$

$\Rightarrow (a^2 - 1)(a^2 + 1) \equiv 0 \pmod p$

$\Rightarrow a^2 - 1 \equiv 0 \pmod p$ or $a^2 + 1 \equiv 0 \pmod p$

If $a^2 - 1 \equiv 0 \pmod p$

$\Rightarrow a^2 \equiv 1 \pmod p$

$\Rightarrow o(a) \leq 2$

(11) Show that the product of the $\phi(p-1)$
primitive roots of p is congruent
modulo p. to $(-1)^{\phi(p-1)}$

sol^n:- If r is a primitive root of p
then r^k is a primitive root of
p if $\gcd(k, p-1) = 1$.

~~Product of primitive roots of p~~

Suppose $a_1, a_2 \ldots a_{\phi(p-1)}$ are integers
s.t $\gcd(k, a_i) = 1$ $\forall\ 1 \leq i \leq \phi(p-1)$

Product of primitive roots of p

$= r^{a_1} r^{a_2} \ldots r^{a_{\phi(p-1)}}$

$= r^{a_1 + a_2 + \ldots a_{\phi(p-1)}}$

$= r^{\frac{(p-1)\phi(p-1)}{2}} = \left\{ r^{\left(\frac{p-1}{2}\right)} \right\}^{(p-1)}$

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

* * *

30/03/15

Theorem

If p is an odd prime & $\gcd(a, p) = 1$, then the congruence $x^2 \equiv a \pmod{p^n}$, $n \geq 1$, has a sol^n $\Leftrightarrow \left(\frac{a}{p}\right) = 1$.

CHAPTER-9

THE QUADRATIC RECIPROCITY LAWS

Quadratic Congruence

$x^2+1 \equiv 0 \pmod{n}$

In general —

$ax^2+bx+c \equiv 0 \pmod{p}$

we will consider $ax^2+bx+c \equiv 0 \pmod{p}$

where $\gcd(a,p)=1$

if $\gcd(a,p) \neq 1$

$\Rightarrow \gcd(a,p)=p$

$ax^2+bx+c \equiv 0 \pmod{p}$ —— (1)

where p is an odd prime.

$\gcd(a,p)=1$

$\Rightarrow \gcd(4a,p)=1$

Now, multiply (1) by ~~2a~~ $4a$, —

$4a(ax^2+bx+c) \equiv 0 \pmod{p}$

$\Rightarrow (4a^2x^2+4abx+4ac) \equiv 0 \pmod{p}$

$\Rightarrow (2ax+b)^2 \equiv b^2-4ac \pmod{p}$

$\Rightarrow y^2 \equiv d \pmod{p}$

$y = ax^2+bx+c$

$\Rightarrow y' = 2ax+b$

$y^2 \equiv d \pmod{p}$

where $y = 2ax+b$ &

$d = b^2-4ac$

Q(1)(b) $3x^2+9x+7 \equiv 0 \pmod{13}$ —— (1)

multiplying (1) by $4a$ where $a=3$

$12(3x^2+9x+7) \equiv 0 \pmod{13}$

$\Rightarrow (6x+9)^2 \equiv 9^2 - 12(7) \pmod{13}$

$\Rightarrow (6x+9)^2 \equiv -3 \equiv 10 \pmod{13}$

$\Rightarrow y^2 \equiv 10 \pmod{13}$ where $y = 6x+9$

$y \equiv \pm 6 \pmod{13}$

$\Rightarrow y \equiv 6, 7 \pmod{13}$

$6x+9 \equiv 6 \pmod{13}$	$6x+9 \equiv 7 \pmod{13}$
$\Rightarrow 2x+3 \equiv 2 \pmod{13}$	$\Rightarrow 6x \equiv -2 \pmod{13}$
$\Rightarrow 2x \equiv -1 \pmod{13}$	$\Rightarrow 3x \equiv -1 \pmod{13}$
$\Rightarrow 14x \equiv -7 \pmod{13}$	$\Rightarrow 12x \equiv -4 \pmod{13}$
$\Rightarrow x \equiv 6 \pmod{13}$	$\Rightarrow x \equiv -9 \pmod{13}$
	$\Rightarrow x \equiv 4 \pmod{13}$

Quadratic Residue of p

Let p be a odd prime and gcd (a, p) = 1. If the quadratic congruency $x^2 \equiv a \pmod{p}$ is solvable then 'a' is called Quadratic Residue of p. otherwise 'a' is called a Quadratic non-Residue of p.

Legendre Symbol

Let p be a odd prime & gcd (a, p) = 1 then the Legendre symbol $\left(\frac{a}{p}\right)$ is defined as —

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a Quadratic R of } p. \\ -1 & \text{if } a \text{ is a Q. non. R of } p \end{cases}$$

Euler's Criterion

Thm 9.1 Let p be an odd prime & gcd (a, p) = 1. Then a is a Q.R of p iff $a^{\left(\frac{p-1}{2}\right)} \equiv 1 \pmod{p}$

or

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

Pf:—

$a_1, a_2, \ldots a_{\phi(n)}$ gcd $(a_i, p) = 1$

r is primitive Root of p.

$\Rightarrow r, r^2, \ldots r^{\phi(n)} \equiv a_1, a_2, \ldots a_{\phi(n)}$ in some order

Let $\left(\frac{a}{p}\right) = 1$

$\Rightarrow a$ is a Q. R of p.

$\Rightarrow x^2 \equiv a \pmod{p}$ is solvable.

Let x be a soln of congruence

$x^2 \equiv a \pmod{p}$

$\Rightarrow x_1^2 \equiv a \pmod{p}$

$\because$ gcd $(a, p) = 1 \Rightarrow$ gcd $(x_1^2, p) = 1$

$\Rightarrow$ gcd $(x_1, p) = 1$

By Fermat's theorem

$x_1^{p-1} \equiv 1 \pmod{p}$

$\Rightarrow (x_1^2)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

$\Rightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

$\Leftarrow$ Conversely

Let $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

$\gcd(a, p) = 1$ &

let r be a primitive Root of p

$\Rightarrow r^k \equiv a \pmod{p}$ for some $1 \le k \le p-1$

Given that

$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

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

$\Rightarrow O_p(r) \mid \frac{k(p-1)}{2}$

$\Rightarrow (p-1) \mid \frac{k(p-1)}{2}$

$\Rightarrow 2 \mid k \Rightarrow k = 2j + r$ for some $j \in \mathbb{R}$

from eq (1)

$r^{2j} \equiv a \pmod{p}$

$\Rightarrow (r^j)^2 \equiv a \pmod{p}$

$\Rightarrow r^j$ is a soln of $x^2 \equiv a \pmod{p}$

Thus If $\gcd(a, p) = 1$, p odd prime

then $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

or

$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

Proof $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

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

$\Rightarrow \left(a^{\frac{p-1}{2}} + 1\right)\left(a^{\frac{p-1}{2}} - 1\right) \equiv 0 \pmod{p}$

Corollary Let p be an odd prime and $\gcd(a, p) = 1$. Then a is Quadratic Residue or Q. non-Residue of p a/c to whether

$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

or $a^{p-1/2} \equiv -1 \pmod{p}$

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

Theorem 9.2 Let p be an odd prime & $\gcd(a, p) = 1$ & $\gcd(b, p) = 1$

p-176

(a) If $a \equiv b \pmod{p}$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(b) $\left(\frac{a^2}{p}\right) = 1$

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

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

(e) $\left(\frac{1}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

or $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$

(f) $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}$

$x^2 + 1 \equiv 0 \pmod{p}$ is solvable iff $p \equiv 1 \pmod{4}$

Pf: If $p \equiv 1 \pmod 4$

$\Rightarrow x^2 + 1 \equiv 0 \pmod p$ has a soln

$\Rightarrow x^2 \equiv -1 \pmod p$ has a soln.

$\Rightarrow \left(\frac{-1}{p}\right) = 1$

If $p \equiv 3 \pmod 4$ is solvable

$\Rightarrow p \not\equiv 1 \pmod 4$

$\Rightarrow x^2+1 \equiv 0 \pmod p$ has a soln

$\Rightarrow x^2 \equiv -1 \pmod p$ has a soln.

$\Rightarrow \left(\frac{-1}{p}\right) = -1$

1 (a) $\left(\frac{19}{23}\right) = ?$

$= \left(\frac{-4}{23}\right) = \left(\frac{-1}{23}\right)\left(\frac{4}{23}\right) = \left(\frac{-1}{23}\right)\left(\frac{2^2}{23}\right)$

$= \left(\frac{-1}{23}\right) = -1$

(b) $\left(\frac{23}{59}\right) = \left(\frac{36}{59}\right) = \left(\frac{1}{59}\right)\left(\frac{6^2}{59}\right)$

$= \left(\frac{1}{59}\right) = 1$

25|03|15

GAUSS LEMMA

Theorem 9.5 (P-179) let p be an odd prime & $\gcd(a,p) = 1$ if n denotes the no. of integer in S

$$S = \left\{a, 2a, 3a, \ldots \left(\frac{p-1}{2}\right)a\right\}$$

whose Remainder ~~division~~ p exceeds $p/2$ then

then

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

Ex. 9.2 (P. 184)

2 (a) Use gauss lemma Compute $\left(\frac{8}{11}\right)$

$a = 8, \; p = 11, \; \frac{p-1}{2} = 5$

$S = \{8, 16, 24, 32, 40\}$

Remainder set after division by 11

$R = \{8, 5, 2, 10, 7\}$ $\quad \left(\frac{p}{2} = 5.5\right)$

we can see that $n = 3$

$\gcd(a,p) = 1$

$\left(\frac{a}{p}\right) = (-1)^3 = -1$

(b) $\left(\frac{7}{13}\right)$ $\quad a = 7, \; p = 13, \; \frac{p-1}{2} = 6$

$S = \{7, 14, 21, 28, 35, 42\}$

Remainder set after division by 13

$R = \{7, 1, 8, 2, 9, 3\}$ $\quad \left(\frac{p}{2} = 6.5\right)$

we can see that $n = 3$

$\gcd(a,p) = 1$

$\left(\frac{a}{p}\right) = (-1)^n = (-1)^3 = -1$

Theorem 9.6 (P-180) If p is an odd prime, then

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

or $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

or

or $\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 7 \pmod 8 \\ -1, & \text{if } p \equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8 \end{cases}$

Theorem: If p and $2p+1$ are both odd primes then the integer $2\cdot(-1)^{\left(\frac{p-1}{2}\right)}$ is a primitive root of $2p+1$.

Q.7 (p-181)

Pf: Let $q = 2p+1$

Case-I

$p \equiv 1 \pmod 4 \Rightarrow p = 4k+1$

$2\cdot(-1)^{\frac{p-1}{2}} = 2$

T.S. 2 is a primitive root of 2.

Clearly $\gcd(2, q) = 1$

Here $\phi(q) = q-1 = 2p+1-1 = 2p$

$\because O_q(2) \mid \phi(q)$

$\Rightarrow O_q(2) = 1$ or 2 or p or $2p$

If $O_q(2) = 1 \Rightarrow 2 \equiv 1 \pmod q$ $\rightarrow\leftarrow$

If $O_q(2) = 2 \Rightarrow 2^2 \equiv 1 \pmod q$

$\Rightarrow q \mid 3 \Rightarrow q = 3 \Rightarrow 2p+1 = 3$

$\Rightarrow p = 1$ $\rightarrow\leftarrow$

$p \equiv 1 \pmod 4 \Rightarrow 4 \mid p-1$

$\Rightarrow 8 \mid 2p-2 \Rightarrow 8 \mid q-3$

$\Rightarrow q \equiv 3 \pmod 8$

$\Rightarrow \left(\frac{2}{q}\right) = -1$

$\Rightarrow \left(\frac{2}{q}\right) \equiv -1 \pmod q$

$\Rightarrow 2^{\left(\frac{q-1}{2}\right)} \equiv -1 \pmod q$

$\Rightarrow 2^{p} \equiv -1 \pmod q$

$\Rightarrow O_q(2) \neq p$

$\Rightarrow O_q(2) = 2p = \phi(q)$

$\Rightarrow 2$ is a primitive root of $2p+1$

Case-II $p \equiv 3 \pmod 4 \Rightarrow p = 4k+3$

$2\cdot(-1)^{\frac{p-1}{2}} = -2$

T.S. -2 is primitive root of q.

$\because \phi(q) = 2p$

$O_q(-2) \mid \phi(q)$

$\Rightarrow O_q(-2) = 1$ or 2 or p or $2p$

If $O_q(-2) = 1 \Rightarrow -2 \equiv 1 \pmod q$

$\Rightarrow q \mid -3 \Rightarrow q = 3 \Rightarrow p = 1$ $\rightarrow\leftarrow$

If $O_q(-2) = 2 \Rightarrow (-2)^2 \equiv 1 \pmod q$

$\Rightarrow q = 3 \Rightarrow p = 1$ $\rightarrow\leftarrow$

$p \equiv 3 \pmod 4 \Rightarrow 4 \mid p-3 \Rightarrow 8 \mid 2p-6$

$\Rightarrow 8 \mid q-7$

$\Rightarrow q \equiv 7 \pmod 8$

$\left(\frac{-2}{p}\right) = \left(\frac{-1}{q}\right)\left(\frac{2}{q}\right)$ $\quad \because q \equiv 7 \pmod 8$, $q \equiv 3 \pmod 4$

$= (-1)(+1)$

$= -1$

$\Rightarrow \left(\frac{2}{q}\right) \equiv -1 \pmod q$

$\Rightarrow (-2)^{\frac{q-1}{2}} \equiv -1 \pmod q$

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

$\Rightarrow O_q(-2) \neq p \Rightarrow O_q(-2) = 2p = \phi(q)$

$\Rightarrow -2$ is a primitive root of $2p+1$

Theorem 9.8 (P-182): There are infinitely many primes of the form $8k-1$

Proof: Suppose that there are finite no.s of prime $p_1, p_2, \dots, p_r$

Consider the integer

$N = (4p_1p_2\dots p_r)^2 - 2$

$= 2(8p_1^2p_2^2\dots p_r^2 - 1) = 2M$

There exists at least one prime factor p of N

$\Rightarrow p \mid \{(4p_1p_2\dots p_r)^2 - 2\}$

$\Rightarrow (4p_1p_2\dots p_r)^2 \equiv 2 \pmod p$

$\Rightarrow \left(\frac{2}{p}\right) = 1$

$\Rightarrow p \equiv \pm 1 \pmod 8$

Case-I Suppose $p \equiv 1 \pmod 8$

$\Rightarrow p$ is of the form $8k+1$

If all the odd prime divisors of N are of the form $8k+1$ then $(8p_1^2p_2^2\dots p_r^2 - 1) = M$ must be of the form $8k+1$ and therefore N must be of the form $16k+2$

This is impossible because N is of the form $16k-2$

Case-II Suppose $p \equiv -1 \pmod 8$

$\Rightarrow p$ is of the form $8k-1$

$\Rightarrow p \mid N$ and $p \mid (4p_1p_2\dots p_r)^2$

$\Rightarrow p \mid N+2 \Rightarrow p \mid 2$

$\rightarrow\leftarrow$

Therefore, infinitely many primes of the form $8k-1$.

Lemma If p is an odd prime and a an odd integer with $\gcd(a,p)=1$, then

$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right]}$

greatest integer fn.

[9.3] QUADRATIC RECIPROCITY

Theorem (9.9) (P-186) Quadratic Reciprocity Law

If p and q are distinct odd primes, then

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

(lattice points are points whose coordinates are integer)

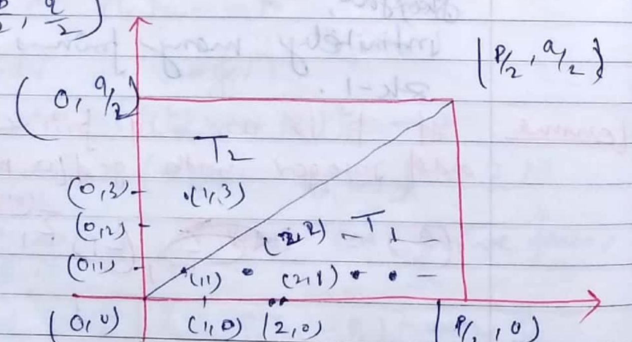
We know that

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{k=1}^{\frac{q-1}{2}} \left[\frac{kp}{q}\right]}$$

& $$\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kq}{p}\right]}$$

$$\Rightarrow \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{\frac{q-1}{2}} \left[\frac{kp}{q}\right] + \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kq}{p}\right]} \quad \text{---} (1)$$

Consider the Rectangle in xy-plane whose vertices are $(0,0)$, $(0, q/2)$, $(p/2, 0)$ & $(p/2, q/2)$



Let R denotes the Region within this Rectangle

No. of lattice pts in R = No. of lattice pts in the set

$$S = \left\{(m,n) : 0 \le m < \frac{p}{2},\ 0 \le n < \frac{q}{2}\right\}$$

= no. of lattice pts in the set.

$$S = \left\{(m,n) : 1 \le m \le \frac{p-1}{2},\ 1 \le n \le \frac{q-1}{2}\right\}$$

$$= \frac{p-1}{2} \cdot \frac{q-1}{2}$$

Now the eqn of the Diagonal D joining $(0,0)$ & $(p/2, q/2)$

$$y - 0 = \frac{q/2 - 0}{p/2 - 0}(x - 0)$$

$$\Rightarrow y = \frac{q}{p}x \Rightarrow py = qx$$

Suppose only lattice pt (m,n) exists on diagonal, then $pn = qm$

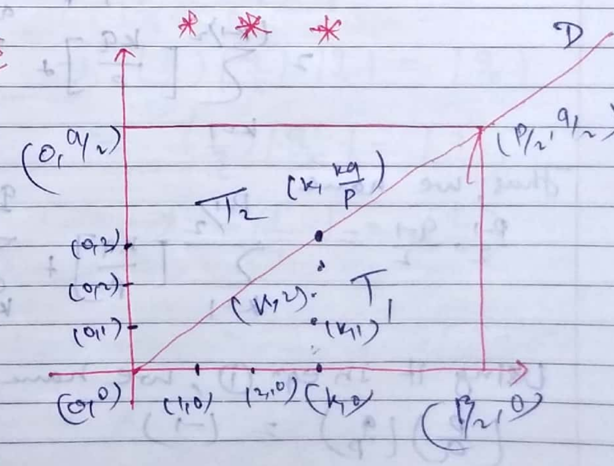
$\Rightarrow q \mid pn \Rightarrow q \mid n$

because $1 \le n \le \frac{q-1}{2}$

$\Rightarrow$ None of the lattice pts inside R lie on the diagonal.

27/03/15

* * *



The no. of integers $0 < y < \frac{kq}{p}$

is equal to $\left[\frac{kq}{p}\right]$

Thus for $1 \le k \le \frac{p-1}{2}$.

The no. of lattice points in T_1.

$$T_1 = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{kq}{p}\right]$$

Ilrly, No. of lattice pts in

$$T_2 = \sum_{k=1}^{\frac{q-1}{2}} \left[\frac{kp}{q}\right]$$

Since non of lattice pt. in R will be on diagonal. D.

∴ The total no. of lattice pts inside R = Total no. of lattice pts in T_1 & T_2

$$= \sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right] + \sum_{k=1}^{q-1/2} \left[\frac{kp}{q}\right]$$

Thus, we have

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{k=1}^{p-1/2} \left[\frac{kq}{p}\right] + \sum_{k=1}^{\frac{q-1}{2}} \left[\frac{kp}{q}\right]$$

Using it in eqn ①, we have

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)$$

Corollary (1) If p & q are distinct odd primes then —

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 ; \text{ if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -1 \text{ if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Proof: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$

$\Rightarrow \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$ if $\frac{p-1}{2}$ or $\frac{q-1}{2}$ is an even integer if $\frac{p-1}{2}$ is even or $\frac{q-1}{2}$ is even.

if $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$

Corollary (2) If p & q are distinct odd primes, then —

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) \text{ if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) \text{ if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

If $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$

then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$

$\Rightarrow \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)\left(\frac{q}{p}\right) = \left(\frac{q}{p}\right)$

$\Rightarrow \left(\frac{p}{q}\right)\left(\frac{q^2}{p}\right) = \left(\frac{q}{p}\right)$

$\Rightarrow \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$

Second part: —

Theorem 9.10 (P-189) If $P \neq 3$ is an odd prime, then

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } P \equiv \pm 1 \pmod{12} \\ -1 & \text{if } P \equiv \pm 5 \pmod{12} \end{cases}$$

Proof: We know that —

$$\left(\frac{3}{P}\right) = \begin{cases} \left(\frac{P}{3}\right) & \text{if } P \equiv 1 \pmod 4 \\ -\left(\frac{P}{3}\right) & \text{if } P \equiv 3 \pmod 4 \end{cases} \quad \text{—— (1)}$$

$$\frac{P}{3} = \begin{cases} 1 & \text{if } P \equiv 1 \pmod 3 \\ -1 & \text{if } P \equiv 2 \pmod 3 \end{cases} \quad \text{—— (2)}$$

$\left(\frac{3}{P}\right)$ = from eqⁿ (1) & (2)

$\left(\frac{3}{P}\right) = 1$ if $P \equiv 1 \pmod 4$ & $P \equiv 1 \pmod 3$

or $P \equiv 3 \pmod 4$ & $P \equiv 2 \pmod 3$

$\Rightarrow \left(\frac{3}{P}\right) = 1$ if $P \equiv 1 \pmod{12}$

or ~~4 | P & 3 | P~~

$P \equiv -1 \pmod 4$ & $P \equiv -1 \pmod 3$

$\Rightarrow \left(\frac{3}{P}\right) = 1$ if $P \equiv 1 \pmod{12}$ or

$P \equiv -1 \pmod{12}$

Again from (1) & (2), we have

$\left(\frac{3}{P}\right) = -1$ if $P \equiv 1 \pmod 4$ &

$P \equiv 2 \pmod 3$

or $P \equiv 3 \pmod 4$ & $P \equiv 1 \pmod 3$

$\Rightarrow \left(\frac{3}{P}\right) = -1$ if $P \equiv 5 \pmod 3$

or $P \equiv -5 \pmod 4$ & $P \equiv -5 \pmod 3$

30/3/15

$\Rightarrow \left(\frac{3}{P}\right) = -1$; if $P \equiv \pm 5 \pmod{12}$

* * *

Theorem (9.11) If p is an odd prime & $\gcd(a,p) = 1$. Then the congruence $x^2 \equiv a \pmod{p^n}$, $n \geq 1$, has a solⁿ $\Leftrightarrow$ $\left(\frac{a}{p}\right) = 1$.

Pf: Suppose the congruence $x^2 \equiv a \pmod{p^n}$ has a solⁿ x_1 (say)

$\Rightarrow x_1^2 \equiv a \pmod{p^n}$

$\Rightarrow p^n \mid (x_1^2 - a)$

$\Rightarrow p \mid (x_1^2 - a)$

$\Rightarrow x_1^2 \equiv a \pmod p$

$\Rightarrow x^2 \equiv a \pmod p$ has a solⁿ

$\Rightarrow \left(\frac{a}{p}\right) = 1$.

$\Leftarrow$ Conversely,
Assume that $\left(\frac{a}{p}\right) = 1$

T.S $x^2 \equiv a \pmod{p^n}$ has a solⁿ $\forall n \geq 1$.

We will use induction on n.

For $n = 1$

$\Rightarrow x^2 \equiv a \pmod p$ has a solⁿ.

$\Rightarrow$ Thm is true for $n = 1$.

Assume that theorem is true for $n = k$

T.S Theorem is true for $n = k+1$.

$\because x^2 \equiv a \pmod{p^k}$ has a solⁿ x_0 (say)

$\Rightarrow x_0^2 \equiv a \pmod{p^k}$

$\Rightarrow p^k \mid (x_0^2 - a)$ $\Rightarrow x_0^2 - a = bp^k$ where $b \in \mathbb{Z}$.

$\Rightarrow x_0^2 = a + bp^k$ —— (1)

Now consider the linear congruence

$2x_0 y \equiv -b \pmod p$

$\because \gcd(2x_0, p) = 1$

therefore this congruence has a unique sol^n y_0 (say)

i.e $2x_0y \equiv -b \pmod p$ —— (2)

we need to show that

$x^2 \equiv a \pmod{p^{k+1}}$

has a sol^n.

Consider $x_1 = x_0 + y_0 p^k$.

Claim: x_1 is a sol^n of $x^2 \equiv a \pmod{p^{k+1}}$

$x_1^2 = x_0^2 + y_0^2p^{2k} + 2x_0y_0p^k = (x_0+y_0p^k)^2$

$= (\cancel{a+bp^k) + bp^k + y_0^2p^{2k} \pmod p})$

$= a + bp^k + 2x_0y_0p^k + y_0^2p^{2k}$ (using (1))

$\equiv a + (2x_0y_0+b)p^k + y_0^2p^{2k}$

$\equiv a+0+0 \pmod{p^{k+1}}$ [By eq^n (2)]

$\equiv a \pmod{p^{k+1}}$

$\Rightarrow x^2 \equiv a \pmod{p^{k+1}}$ has a sol^n.

Q(2)(i) Solve $x^2 \equiv 2 \pmod{7^3}$

$\left(\frac{2}{7}\right) = 1$, $\because 7 \equiv 7 \pmod 8$

$\Rightarrow x^2 \equiv 2 \pmod{7^3}$ has a sol^n.

first we will solve —

$x^2 \equiv 2 \pmod 7$

$x_0 = 3$ is a sol^n of this congruence.

$9 = x_0^2 = a + bp = 2 + 7 \cdot b$

Consider the linear congruence

$2x_0y \equiv -b \pmod 7$

$\Rightarrow 6y \equiv -1 \pmod 7$

$y_0 = 1$ is a sol^n of this congruence

$x_1 = x_0 + y_0p$

$= 3 + (1)7 = 10$

$x_1 = 10$ is a sol^n of $x^2 \equiv 2 \pmod{7^2}$

$\Rightarrow x_1^2 = a + bp^2$,

$10^2 = 2 + b(7)^2 \Rightarrow b = 2$

Consider the congruence

$2x_1y_1 \equiv -b \pmod p$

$\Rightarrow 20y_1 \equiv -2 \pmod 7$

$\Rightarrow y_1 = 2$.

$x_2 = x_1 + y_1p^2$ is a sol^n of $x^2 \equiv 2 \pmod{7^3}$.

~~Theorem~~

Theorem 9.12 (P-194) let a be an odd integer, then we have the following —

(i) $x^2 \equiv a \pmod 2$ always has a sol^n

(ii) $x^2 \equiv a \pmod 4$ has a sol^n $\Leftrightarrow a \equiv 1 \pmod 4$

(iii) $x^2 \equiv a \pmod{2^n}$, for $n \geq 3$ has a sol^n $\Leftrightarrow$ $a \equiv 1 \pmod 8$.

Pf: (i) $\because a$ is odd $\Rightarrow a-1$ is even.

$\Rightarrow 2 \mid a(a-1)$

$\Rightarrow x = a$ is a sol^n of $x^2 \equiv a \pmod 2$.

(ii) $x \equiv 0, 1, 2, 3 \pmod 4$

$\Rightarrow x^2 \equiv 0, 1 \pmod 4$

$\because a$ is an odd integer

$\Rightarrow a \not\equiv 0 \pmod 4$

$\therefore x^2 \equiv a \pmod 4$ has a sol^n iff a is of the form $4k+1$

namely $x=1$, & $x=3$

(iii) $x^2 \equiv a \pmod{2^n}$ has a sol^n for $n \geq 3$.

Suppose x_1 is a sol^n.

$2^n \mid (x_1^2 - a) \Rightarrow 2^3 \mid x_1^2 - a$.

$\Rightarrow x_1^2 \equiv a \pmod 8$

$\because$ Square of every odd no. is always congruent to 1 modulo 8.

$\therefore a \equiv 1 \pmod 8$

$\Leftarrow$ Conversely

Assume that $a \equiv 1 \pmod 8$

we will use induction on n.

for $n = 3$.

$x^2 \equiv a \pmod 8$

$\because a \equiv 1 \pmod 8$

$\Rightarrow x^2 \equiv 1 \pmod 8$

$\Rightarrow x = 1, 3, 5, 7$

Thus, theorem is true for $n = k$.

Now, Assume that this is true for $n = k$.

T.S Theorem is true for $n = k+1$,

$\because x^2 \equiv a \pmod{2^k}$ has a sol^n x_0 (say)

$\Rightarrow x_0^2 = a + b2^k$ where $b \in \mathbb{Z}$ —— (1)

Now, Consider the linear Congruence

$x_0 y \equiv -b \pmod 2$

$\because \gcd(2, x_0) = 1$.

$\therefore$ This congruence has a unique sol^n y_0 (say)

$\Rightarrow x_0 y_0 \equiv -b \pmod 2$ —— (2)

Consider $x_1 = x_0 + y_0 2^{k-1}$.

Claim: x_1 is a sol^n of $x^2 \equiv a \pmod{2^{k+1}}$

$x_1^2 = x_0^2 + y_0^2 2^{2k-2} + 2x_0 y_0 2^{k-1}$.

$\Rightarrow x_1^2 = a + b2^k + x_0 y_0 2^k + y_0^2 2^{2k-2}$

$\Rightarrow x_1^2 = a + (b + x_0 y_0) 2^k + y_0^2 2^{2k-2}$

$\equiv a + 0 + 0 \pmod 2$ [using eq (2)]

$\equiv a \pmod 2$

$\Rightarrow x_1$ is a sol^n of

$x^2 \equiv a \pmod{2^{k+1}}$

$\Rightarrow$ theorem is true for $n = k+1$

by ~~fundamental~~ induction,

this is true for all n $(n \geq 3)$

* * *

CHAPTER - 10

Introduction to Cryptography

In the language of Cryptography, where codes are called ciphers and the information is called 'plaintext'. After transformation to a secret form, the msg. is called 'cipher text'. The process of converting from plaint text to ciper text is called "encrypting", where as the reverse process of converting from cipertext to plain text is called "decrypting".

The word Cryptography comes from the greek word 'kryptos' meaning hidden and 'grapheir' meaning to write.

(1) Caesar Cipher

$$C \equiv P + 3 \pmod{26}$$

SHIVAJI COLLEGE

P: 18 07 08 21 00 09 08 | 02 14 11 11 04 07 04

C: 21 10 11 24 03 12 11 | 05 17 14 14 07 10 07

Coded message is —

~~KKL~~ VKLYDML FROOHKH

S	= 18
H	= 07
I	= 08
V	= 21
A	= 01
J	= 09
C	= 03
O	= 14
L	= 11
E	= 04
G	= 06

A	B	C	D	E	F	G	H	I	J	K
00	01	02	03	04	05	06	07	08	09	10

L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
11	12	13	14	15	16	17	18	19	20	21				

for decoding the msg

$$P \equiv C - 3 \pmod{26}$$

The Caesar Ciper is very simple and hence, extremly insecure.

Ex-10.1 (2) (P-206) If the Ceasar Cipher produced KDSSB ELUWKGDB, what is the plaintext message?

$$P \equiv C - 3 \pmod{26}$$

C: 10 03 18 18 01 | 04 11 20 22 10 06 03

P: 07 00 15 15 24 | 01 08 17 19 07 03 24

Plain text message is —

HAPPY BIRTHDAY

(3)(a) A Linear cipher is defined by the congruence $C \equiv aP + b \pmod{26}$, where a & b are integers with $\gcd(a, 26) = 1$. ST the corresponding decrypting congruence is $P \equiv a'(C - b) \pmod{26}$. Where the integer a' satisfies $aa' \equiv 1 \pmod{26}$.

Soln.

$$C \equiv aP + b \pmod{26}$$

$$\Rightarrow aP \equiv C - b \pmod{26} \quad \text{--- (1)}$$

Consider the linear congruence

$$ax \equiv 1 \pmod{26}$$

$\because \gcd(a, 26) = 1$, therefore this congruence has a unique soln a' (say)

Page No. 152
Date 01 4 15

$\therefore aa' \equiv 1 \pmod{26}$ —— (ii)

multiply eq^n (i) by a', we have

$apa' = a'(c-b) \pmod{26}$

$\Rightarrow aa'p \equiv a(c-b) \pmod{26}$

$\Rightarrow p \equiv a'(c-b) \pmod{26}$

(using eq^n (ii))

Proved

10.1 (3)(b) Using the linear cipher $C \equiv 5P + 11 \pmod{26}$ encrypt the message "NUMBER THEORY IS EASY".

$C \equiv 5P + 11 \pmod{26}$

N U
13 20

Page No. 153
Date 01 04 15

10.1 (3)(c) Decrypt the message RXQTGU HOZT-KGH FLKTMMTG, which was produced using the linear cipher
$C \equiv 3P + 7 \pmod{26}$

Sol^n

$\Rightarrow C \equiv 3P + 7 \pmod{26}$

$3P \equiv C - 7 \pmod{26}$

$\Rightarrow 9(3P) \equiv 9(C-7) \pmod{26}$

$P \equiv 9C - 63 \pmod{26}$

$P \equiv 9C + 15 \pmod{26}$

17 23 16 19 06 20

$P \equiv 9(17) + 15 \equiv 168 \equiv 12 \pmod{26} \rightarrow M$

$P \equiv 9(23) + 15 \equiv 222 \equiv 14 \pmod{26} \rightarrow O$

$P \equiv 9(16) + 15 \equiv 159 \equiv 3 \pmod{26} \rightarrow D$

$P \equiv 9(19) + 15 \equiv 186 \equiv 4 \pmod{26} \rightarrow E$

$P \equiv 9(06) + 15 \equiv 69 \equiv 17 \pmod{26} \rightarrow R$

$P \equiv 9(20) + 15 \equiv 195 \equiv 13 \pmod{26} \rightarrow N$

Hill's Cipher

In the Hill's cipher take 2 successive letters and transform there numerical equivalent $P_1 P_2$ into a block $C_1 C_2$ of cipher text no.s using the pair of congruency.

The four co-eff a, b, c, d are

$C_1 = aP_1 + bP_2 \pmod{26}$

$C_2 = cP_1 + dP_2 \pmod{26}$

Page No. 154
Date 01-04-015

selected s.t —

$\gcd(ad - bc, 26) = 1$

10.1
Q.7
(P-207)

(a) Use the Hill cipher

$C_1 \equiv 5P_1 + 2P_2 \pmod{26}$

$C_2 \equiv 3P_1 + 4P_2 \pmod{26}$

to encrypt the message GIVE THEM TIME.

Sol^n

In this message first two successive letters are GI are numerically equivalent to 06 08

Here $P_1 = 06$, $P_2 = 08$

Replace these values in given congruence.

$\Rightarrow$ ~~C~~

$C_1 \equiv 5(6) + 2(8) \pmod{26}$

$\equiv 30 + 16 \equiv 46 \equiv 20 \pmod{26}$

$\Rightarrow C_1 \to U$

$C_2 \equiv 3(6) + 4(8)$

$\equiv 18 + 32 \equiv 50 \equiv 24 \pmod{26}$

$C_2 \to Y$

~~GI 0608 2104 | 1907 0412 | 19 0812 04~~

UYJB

Now VE are Numerically Equivalent to 21 04

Here $P_1 = 21$, $P_2 = 04$

$\Rightarrow C_1 \equiv 5(21) + 2(04) \equiv 105 + 08 \equiv 113 \equiv 9 \pmod{26}$

$\Rightarrow C_1 \to J$

$C_2 \equiv 3(21) + 4(04) \equiv 63 + 16 \equiv 79 \equiv 1 \pmod{26}$

$\to B$

Page No. 155
Date

Que (10.1)
(Q7)(b)

To ciphertext ALXWU VADCOJO has been enciphered with the cipher.

$8\times \quad C_1 \equiv 4P_1 + 11P_2 \pmod{26}$ —(i) $\quad 3\times$

$11\times \quad C_2 \equiv 3P_1 + 8P_2 \pmod{26}$ —(ii) $\quad 4\times$

Derive the plaintext.

$\gcd(32 - 33, 26) = \gcd(-1, 26) = 1$

multiply eq^n (1) by 8 & (2) by 11 & then substracts (2) from (1) —

$8C_1 - 11C_2 \equiv -P_1 \pmod{26}$

$\Rightarrow P_1 \equiv -8C_1 + 11C_2 \pmod{26}$ —(3)

$(1) \times 3 - (2) \times 4 \Rightarrow$

$3C_1 - 4C_2 \equiv P_2 \pmod{26}$

$\Rightarrow P_2 \equiv 3C_1 - 4C_2 \pmod{26}$

RIGHT

ALXWU VADCOJO

00 11 23, 22 20

Now for the block 00, 11 —

$P_1 \equiv -8(00) + 11(11) \equiv 121 \equiv 17 \pmod{26}$

$\to R$

$P_2 \equiv 3(00) - 4(11) \equiv -44 \equiv 8 \pmod{26}$

$\to I$

for the Block 23, 22 — $P_1 \equiv -8(23) + 11(22)$

$\equiv 24 + \ldots \equiv 6 = G$

$P_2 \equiv 3(23) - 4(22) \ldots = H$

2PS| Monday

Page No. 156 Date 06|04|15

RSA Algorithm or RSA Encryption

Step-I take two distinct primes p & q.

Step-II $n = pq$

Step-III Calculate $\phi(n) = (p-1)(q-1)$

Step-IV Choose k s.t $\gcd(k, \phi(n)) = 1$

Step-V $M^k \equiv r \pmod n$

where M is the numerical value of letters in plaintext.

Step-VI find j such that

$kj \equiv 1 \pmod{\phi(n)}$

Step-VII $r^j \equiv M \pmod n$

Que. (10.3) (P-205) $p = 29$, $q = 53$, $k = 47$

Encrypt the message using RSA Algorithm.

NO WAY

Sol^n.

$n = 29 \cdot 53 = 1537$

$\phi(n) = 28 \cdot 52 = 1456$

$\gcd(k, \phi(n)) = \gcd(47, 1456) = 1$

N-13
O-14
W-22
A-00
Y=24

Numerical value of given Plaintext is-

13 14 22 00 24

$(13)^{47} \equiv 354 \pmod{1537}$

$(14)^{47} \equiv 416 \pmod{1537}$

$(22)^{47} \equiv$

$(00)^{47} \equiv 0 \pmod{1537}$

$(24)^{47} \equiv$

Page No. 157 Date 6|4|15

$13^{3}, 13$

$2\ (660)^{15} \cdot 13^2$

find j s.t

$kj \equiv 1 \pmod{\phi(n)}$

$\Rightarrow 47j \equiv 1 \pmod{1456}$

If $p = 29$, $q = 53$, $k = 47$

Using RSA Algorithm

Encrypt the message

NO WAY.

Sol^n

$1456 \mid (47j - 1)$

$\Rightarrow 47j - 1456y = +1$

$\Rightarrow$ ~~1456 - 47j = 1~~

$1456 = 47 \cdot 30 + 46$

$47 = 1 \cdot 46 + 1$

$\Rightarrow 1 = 47 - 46$

$= 47 - (1456 - 47 \cdot 30)$

$= 31 \cdot 47 - 1456$

$\Rightarrow y = +1$ & $j = +31$.

Calculate

$354^{31} \equiv 13 \pmod{n = 1537}$

$416^{31} \equiv 14 \pmod{1537}$

Q. 8 (P-207) A long string of ciphertext resulting from a Hill cipher

$C_1 \equiv aP_1 + bP_2 \pmod{26}$ — (I)

$C_2 \equiv cP_1 + dP_2 \pmod{26}$ — (II)

revealed that the most frequently occurring two-letter blocks were HO & PP, in that order.

(a) Find the values of a, b, c & d.

Sol^n The most common two letter blocks in the English language are TH & followed by HE in that order

⇒ TH transforms in HO &
HE transforms in PP

∵ TH transforms into HO
⇒ the block 1907 transform into 0714 using it in eq^n (1), we have

$$19a + 7b \equiv 7 \pmod{26} \quad \text{—(3)}$$
$$19c + 7d \equiv 14 \pmod{26} \quad \text{—(4)}$$

∵ HE transforms into PP
⇒ the block 0714 transforms 1515 using it in eq^n (1) & (2), we have

$$7a + 4b \equiv 15 \pmod{26} \quad \text{—(5)}$$
$$7c + 4d \equiv 15 \pmod{26} \quad \text{—(6)}$$

∴ by (3) (5) —

$$(49b - 76b) \equiv (49 - 60) \pmod{26}$$
$$\Rightarrow -27b \equiv -11 \pmod{26}$$
$$\Rightarrow 27b \equiv 11 \pmod{26}$$
$$\Rightarrow 1b \equiv 11 \pmod{11}$$

$$0a + 11b \equiv 22 \pmod{26}$$

$$11b \equiv 22 \pmod{26} \Rightarrow b = 2$$

Using it in eq^n (3), we have

$$19a + 14 \equiv 7 \pmod{26}$$
$$\Rightarrow 19a \equiv 19 \pmod{26}$$
$$\Rightarrow a = 1$$

Now for (4) & (5) we have c & d.

CERTAIN NON-LINEAR DIO-PHANTINE EQUATIONS

(12.1) Pythagorean triple

A Pythagorean triple is a set of three integers x, y & z s.t $x^2+y^2=z^2$. This Pythagorean triple is called Primitive if $\gcd(x,y,z)=1$

Suppose (x,y,z) is a pythagorean triple and $\gcd(x,y,z)=1$ and

$$\gcd(x,y) = \gcd(y,z) = \gcd(x,z) = 1$$

~~TS~~ $x^2+y^2=z^2$
given $\gcd(x,y,z)=1$

T.S $\gcd(x,y) = \gcd(y,z) = \gcd(x,z) = 1$

Suppose $\gcd(x,y) \neq 1$
$\Rightarrow \gcd(x,y) = d > 1$
$\Rightarrow d|x$ & $d|y$
$\Rightarrow d^2|x^2$ & $d^2|y^2$
$\Rightarrow d^2|(x^2+y^2) \Rightarrow d^2|z^2$
$\Rightarrow d|z$
$\Rightarrow \gcd(x,y,z) \geq d > 1$
$\Rightarrow \gcd(x,y,z) \neq 1$
$\rightarrow \leftarrow$
Contradiction

~~Solve ...~~

Lemma 1: If (x,y,z) is a Primitive Pythagorean (P-242) triple, then one of the integers x & y is even while other is odd.

Pf: Case-I. when both x & y are even then $2|x$ & $2|y$
$\Rightarrow 4|x^2$ & $4|y^2$
$\Rightarrow 4|(x^2+y^2) \Rightarrow 4|z^2$
$\Rightarrow 2|z$
$\Rightarrow \gcd(x,y,z) \geq 2$
$\Rightarrow (x,y,z)$ is not Primitive.

Case-II Suppose both x & y are odd
$\Rightarrow x^2 \equiv 1 \pmod 4$
& $y^2 \equiv 1 \pmod 4$

$\Rightarrow z^2 = x^2+y^2 \equiv 1+1 \pmod 4$
$\Rightarrow z^2 \equiv 2 \pmod 4$
$\rightarrow \leftarrow$

Lemma: 2 If $ab=c^n$ with $\gcd(a,b)=1$ then there exists Positive integers a_1, b_1 for which $a=a_1^n$, $b=b_1^n$

(No Proof Req.)

Page No. 162 Date 06 04 15

Theorem 12.1 All the solutions of the Pythagorean eqⁿ $x^2+y^2=z^2$ satisfying the conditions

$\gcd(x,y,z)=1$, $2|x$, $x>0, y>0$, $z>0$

are given by the formulas —

$x=2st$, $y=s^2-t^2$, $z=s^2+t^2$

for integers $s>t>0$ such that $\gcd(s,t)=1$ and $s\not\equiv t \pmod 2$

(Proof on page — 163)

— x —

Q.① (P-251) find three different Pythagorean triples of the form 16, y, z

$x^2+y^2=z^2$

$\Rightarrow z^2-y^2=x^2=16^2$

$\Rightarrow (z-y)(z+y)=256$ — ①

we know that $(z+y)>(z-y)$

from eqⁿ ① —

$z+y=32$ and $z-y=8$

$\Rightarrow y=12, z=20, x=16$

the other possibilities is

$z+y=64$ & $z-y=4$

$\Rightarrow y=30, z=34, x=16$

the other possibility is —

$z+y=128$ & $z-y=2$

$\Rightarrow z=63, z=65, x=16$

Page No. 163 Date 06 04 15

$z+y=256$, $z-y=1$

— x —

10-04-15 No class due to test

13/04/15 Test Ques discussion

$a^{4n+1}\equiv a \pmod{10}$

$a^{4n+1}\equiv a \pmod{10}$

use induction on n.

5 is prime, $a^5\equiv a \pmod 5$

$a^2\equiv a \pmod 2$

$\Rightarrow a^5\equiv a \pmod 2$

$\gcd(2,5)=1$

$a^5\equiv a \pmod{10}$

— x —

* * *

15-04-15

pf! Thm: (x,y,z) is primitive Pythagorean triple $\Leftrightarrow$ $x=2st$, $y=s^2-t^2$, $z=s^2+t^2$, $s,t>0$, $s\not\equiv t \pmod 2$

pf: ∵ (x,y,z) is a primitive Pythagorean triple;

∴ $x^2+y^2=z^2$

$\Rightarrow z^2-y^2=x^2$

$\Rightarrow \left(\frac{x}{2}\right)^2=\frac{z^2-y^2}{4}$

$\Rightarrow \left(\frac{x}{2}\right)^2=\left(\frac{z-y}{2}\right)\left(\frac{z+y}{2}\right)=uv$

where $u = \frac{z-y}{2}$, $v = \frac{z+y}{2}$

Claim: $\because \gcd(u,v) = 1$

$\because \gcd(x,y,z) = 1$ & (x,y,z) is pythogoream triple.

$\Rightarrow \gcd(y,z) = \gcd(x,z) = \gcd(x,y) = 1$

let $\gcd(u,v) = d > 1$

$\Rightarrow d|u$ & $d|v$

$\Rightarrow d \mid \frac{z-y}{2}$ & $d \mid \frac{z+y}{2}$

$\Rightarrow d \mid \left(\frac{z-y}{2} + \frac{z+y}{2}\right)$ & $d \mid \left(\frac{z+y}{2} - \frac{z-y}{2}\right)$

$\Rightarrow d \mid z$ & $d|y$

$\Rightarrow \gcd(y,z) \geq d > 1$

$\longrightarrow \longleftarrow$

$\therefore \gcd(u,v) = 1$

from eq^n (1), $\exists$ s & t with $\gcd(s,t) = 1$, such that $u = s^2$, & $v = t^2$

$\therefore u = \frac{z+y}{2}$, & $v = \frac{z-y}{2}$

$\Rightarrow z = u+v = s^2+t^2$

$y = u-v = s^2-t^2$

from eq^n (1), $\left(\frac{x}{2}\right)^2 = uv = s^2t^2$

$\Rightarrow x = 2st$

T.S $s \not\equiv t \pmod 2$

Suppose $2 \mid (s-t)$ — (1)

$\Rightarrow 2 \mid (s-t+2t)$

$\Rightarrow 2 \mid (s+t)$ — (2)

from (1) & (2) —

$2 \mid (s-t)(s+t)$

$\Rightarrow 2 \mid s^2-t^2 \Rightarrow 2 \mid y$

$\Rightarrow x$ & y both are even

$\longrightarrow \longleftarrow$

$\Leftarrow$ (converse part)

let $x = 2st$

$y = s^2-t^2$

$z = s^2+t^2$

with $\gcd(s,t) = 1$, $s \not\equiv t \pmod 2$

$x^2+y^2 = 4s^2t^2 + (s^2-t^2)^2$

$= s^4+t^4+2s^2t^2$

$= (s^2+t^2)^2 = z^2$.

Suppose $\gcd(x,y,z) = d > 1$.

$\Rightarrow d|x$, $d|y$ & $d|z$

$d > 1 \Rightarrow \exists$ a prime p s.t. $p \mid d$

$\Rightarrow p|y$ & $p|z$

$\Rightarrow p|(s^2-t^2)$ & $p \mid (s^2+t^2)$

$\Rightarrow p \mid 2s^2$ & $p \mid 2t^2$

$\Rightarrow p = 2$ or $p \mid s^2$ & $p \mid t^2$. — (3)

~~If $p|2$, then $2|x$ & $2|y$~~

~~$\Rightarrow x$ & y both are even.~~

$\because s \not\equiv t \pmod 2$

$\Rightarrow 2 \nmid (s-t)$ & $2 \nmid (s+t)$

$2 \nmid (s^2 - t^2)$

$\Rightarrow p \neq 2$

from eqn (3)

$p \mid s^2$ & $p \mid t^2$

$\Rightarrow p \mid s$ & $p \mid t$

$\Rightarrow \gcd(s,t) \geq p$

$\longrightarrow \longleftarrow$

Ex-12.1 (P-251)

Q.4 Prove that in a primitive Pythagorean triple x, y, z the product xy is divisible by 12, hence $60 \mid xyz$.

Pf: T.S $12 \mid xy$

$\because x, y, z$ is a primitive Pythagorean triple.

$\therefore x = 2st$

$y = s^2 - t^2$; $z = s^2 + t^2$ with $\gcd(s,t) = 1$ & $s \not\equiv t \pmod 2$.

Suppose $3 \mid s$ or $3 \mid t$

$\Rightarrow 3 \mid st \Rightarrow 3 \mid x \Rightarrow 3 \mid xy$.

If $3 \nmid s$, & $3 \nmid t$,

$\Rightarrow \gcd(3,s) = 1$ & $\gcd(3,t) = 1$

$\Rightarrow s^2 \equiv 1 \pmod 3$ & $t^2 \equiv 1 \pmod 3$ (using fermat's theorem)

$\Rightarrow (s^2 - t^2) \equiv 1 - 1 \equiv 0 \pmod 3$

$\Rightarrow 3 \mid (s^2 - t^2) \Rightarrow 3 \mid y \Rightarrow 3 \mid xy$

$\because s^2 \equiv 0$ or $1 \pmod 4$

$t^2 \equiv 0$ or $1 \pmod 4$

If $s^2 \equiv 0 \pmod 4$ or

$t^2 \equiv 0 \pmod 4$

then $4 \mid s^2$ or $4 \mid t^2$

$\Rightarrow 2 \mid s$ or $2 \mid t$

$\Rightarrow 2 \mid st \Rightarrow 4 \mid 2st \Rightarrow 4 \mid x$

If $s^2 \equiv 1 \pmod 4$ & $t^2 \equiv 1 \pmod 4$

$\Rightarrow s^2 - t^2 \equiv 0 \pmod 4$.

$\Rightarrow 4 \mid (s^2 - t^2) \Rightarrow 4 \mid y$

$\Rightarrow y$ is even.

$\Rightarrow x$ & y both are even

$\longrightarrow \longleftarrow$

$\because 3 \mid xy$, $4 \mid xy$

& $\gcd(3,4) = 1$

$\Rightarrow 12 \mid xy$ — (1)

T.S $60 \mid xyz$

$\because 12 \mid xy \Rightarrow 12 \mid xyz$ — (2)

Suppose $5 \mid s$ or $5 \mid t$

$\Rightarrow 5 \mid st \Rightarrow 5 \mid x \Rightarrow 5 \mid xyz$ — (3)

$\because \gcd(5, 12) = 1 \Rightarrow 60 \mid xyz$

If $5 \nmid s$ and $5 \nmid t$

$\Rightarrow \gcd(s, 5) = 1$ & $\gcd(t, 5) = 1$

$\Rightarrow$ ~~gcd~~ $s^4 \equiv 1 \pmod 5$ &

$t^4 \equiv 1 \pmod 5$.

Exercise - 12.1

$\Rightarrow s^4 - t^4 \equiv 1-1 \equiv 0 \pmod 5$

$\Rightarrow 5 \mid s^4 - t^4$

$\Rightarrow 5 \mid (s^2-t^2)(s^2+t^2)$

$\Rightarrow 5 \mid yz \Rightarrow 5 \mid xyz$

$\because \gcd(5,12) = 1$

$\Rightarrow 60 \mid xyz$

Q(1)(5) Obtain all primitive Pythagorean triple x, y, z in which $x = 40$

Sol^n $x = 2st$, $y = s^2-t^2$, $z = s^2+t^2$

$\Rightarrow 40 = 2st \Rightarrow st = 20$ (20×1, 10×2, 5×4)

$s = 20$, $t = 1$ $\Rightarrow y = 399$, $z = 401$, $x = 40$

$s = 5$, $t = 4$ $\Rightarrow y = 9$, $z = 41$, $x = 40$

$\because \gcd(s,t) = 1$ & $s \not\equiv t \pmod 2$

So, we have the following choices for s & t

$s = 20$, $t = 1$

$s = 5$, $t = 4$

If $s = 20$, $t = 1$, then

$x = 40$, $y = 399$, $z = 401$.

If $s = 5$, $t = 4$, then

$x = 40$, $y = 9$, $z = 41$

[12.2] FERMAT'S LAST THEOREM

Theorem (12.3): The Diophantine $x^4+y^4 = z^4$ has no sol^n in positive integers x, y, z

(only statement)

Corollary (P-253): The Diophantine eq^n $x^4+y^4 = z^4$ has no sol^n in the positive integers.

Proof: Suppose x_0, y_0, z_0 is a positive sol^n of $x^4+y^4 = z^4$. $\Rightarrow x_0^4+y_0^4 = z_0^4 = (z_0^2)^2$

then x_0, y_0, z_0^2 is a positive sol^n of $x^4+y^4 = z^2$ $\rightarrow \leftarrow$

Fermat's last theorem

For $n > 2$, the Diophantine eq^n $x^n+y^n = z^n$ has no sol^n in positive integers.

Ex 12.2

Q(1) Show that the eq^n $x^2+y^2 = z^3$ has infinitely many sol^{n}s for x, y, z positive integers.

Sol^n For $n \geq 1$, $x = 2n^3$, $y = 11n^3$, $z = 5n^2$ is sol^n for this diophantine eq^n

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

$(2n^3)^2 + (11n^3)^2 = 4n^6 + 121n^6$

$= 125n^6$

$= (5n^2)^3$.

* *

Page No. 170
Date 15 4 15

Ex-12.1
Q.2

(2014)

If x, y, z is a Primitive Pythagorean triple. Prove that $x+y$ and $x-y$ are congruent modulo 8 to either 1 or 7.

Sol^n

We will show $(x+y)^2 \equiv 1 \pmod 8$

$\because x, y, z$ is a Primitive Pythagorean triple.

$\Rightarrow x = 2st$

$y = s^2 - t^2$ $\quad \gcd(s,t) = 1$

$z = s^2 + t^2$ $\quad s > t > 0$

$s \not\equiv t \pmod 2$.

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

$= 4s^2t^2 + s^4 + t^4 - 2s^2t^2 + 4st(s^2 - t^2)$.

$= (s^2+t^2)^2 + 4st(s-t)(s+t)$

$\equiv (\text{odd integers})^2 + 0 \pmod 8$

$\because s \not\equiv t \pmod 2$

$\Rightarrow$ ~~$2 \nmid (s-t)$~~

$\Rightarrow 2 \mid s$ or $2 \mid t$

$\Rightarrow 2 \mid st$

$\Rightarrow s^2 + t^2$ is an odd integer

$\equiv 1 \pmod 8$

$\Rightarrow (x+y) \equiv 1 \pmod 8$

or $(x+y) \equiv -1 \pmod 8$

$\Rightarrow (x+y) \equiv 1 \pmod 8$ or

$(x+y) \equiv 7 \pmod 8$

* * *

Page No. 171
Date 17 04 15

~~17/04/15~~

Sol^n

Q.3 (5) Prove that if $p > 3$, is an odd Prime then

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 6 \\ -1 & \text{if } p \equiv 5 \pmod 6 \end{cases}$$

P. Kalika
BSc Classroom Notes