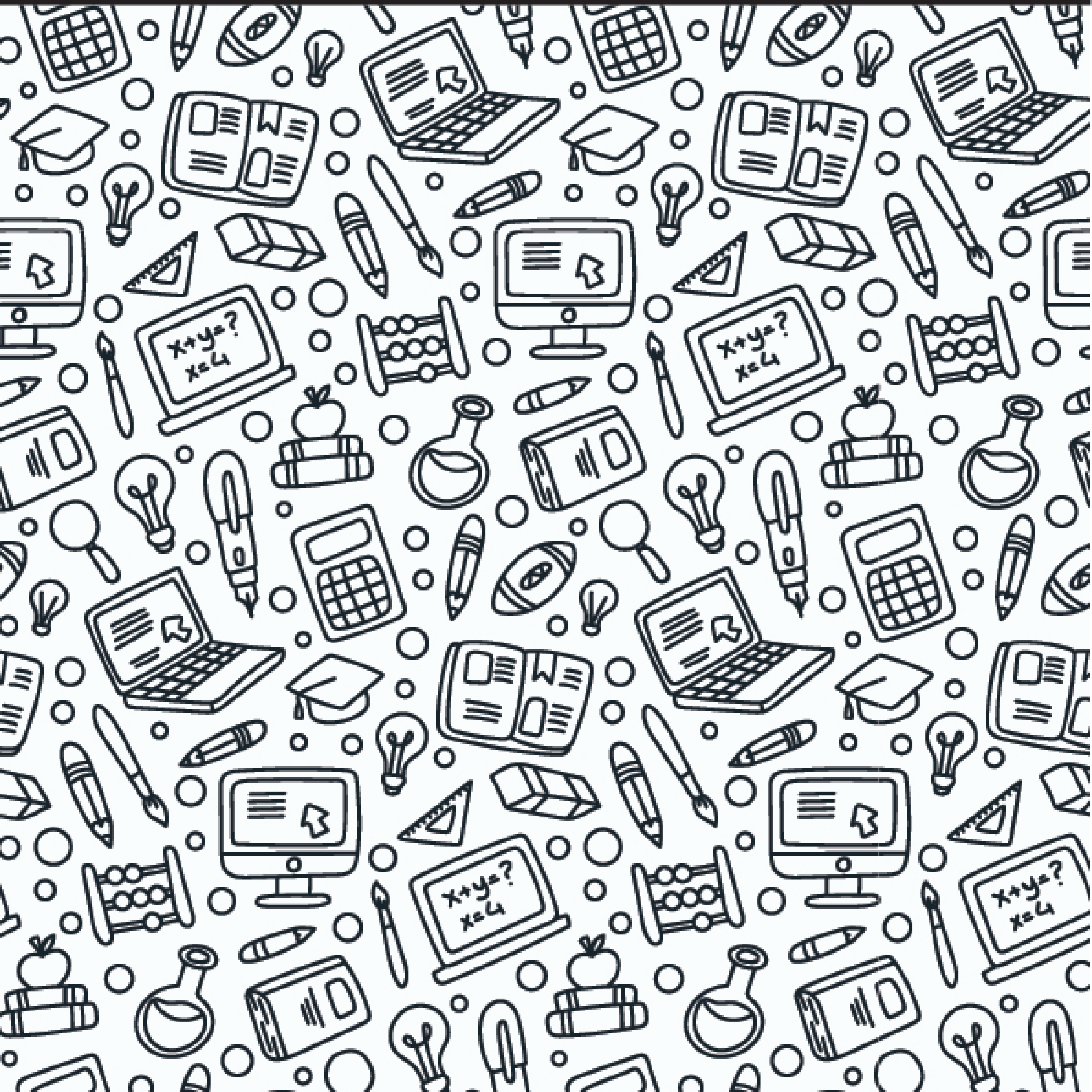
Number Theory



Ronak Sumbaly

classmate
Date
Page

3rd Sept.

Number Theory (Brief).

→ Types of Number Theory: 1. Elementary Number Theory. (Integers) *
2. Analytic Number Theory. (Complex analysis & calculus).
3. Algebraic Number Theory (rational roots of poly.).
4. Geometrical Number Theory.
5. Computational (Algorithm) Number Theory.
↳ e.g. Testing Prime Numbers. (Used in network security password - product of prime nos.) Cryptography.

→ Course Description:
1. Divisibility (Notation : | eg. 4|20)
2. GCD (For larger nos: Eucledian algo.).
3. Congruences. (Notation : ≡ eg. Used in clock arithmatic).
4. Arithmatic Functions
5. Prime Number.
6. Quadratic Residue
7. Continued Fraction.

4th Sept.

→ History of Number Theory:

Fermit's Law: $x^n+y^n=z^n$ ... NOT possible for $n \in I$ $n>2$. → Proved by Andrew Wiles.
Fermit and Pascal → Invention of Probability.
Octave based on numbers (Music).
Numbers used in rituals (havan) → Quadratic eq^n (Mahavira).

Pythagorean Triplet: $x=n$; $y=\frac{1}{2}(n^2-1)$; $z=\frac{1}{2}(n^2+1)$
↳ Odd number > 1. eg. 3, 4, 5 7, 24, 25
5, 12, 13

Even Triplet : 8, 15, 17   Formula $x = 4n$

12, 35, 37 $y = 4n^2 - 1$

16, 63, 65 $z = 4n^2 + 1 = y + 2$.

20, 99, 101

10^4 - Myraid - Geeks 10^3 - Roman - Millinieum.

10^{18} - Indian

Types of Equation :

1. Diophantine eqⁿs $\longrightarrow ax + by = c$ .. Indeterminate.
2. $x^n + y^n = z^n \longrightarrow$ Fermit's eq^n.
3. $x^2 - ny^2 = \pm 1 \longrightarrow$ Pells Eq^n (Astronomy)
4. $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} \longrightarrow$ Erdös - Straus eq^n.

   $\longrightarrow n > 2 \quad x, y, z \in +I$.

$k\ 3\overline{)10}(3\ q$
$\frac{9}{1\ (r)}$ $j = k\,q + r$

5th Sept.

Chapter 2. Divisibility.

(1.2.) – Basic Representation Theorem:

Let k be any integer > 1. Then $\forall$ positive integer n, $\exists$ a representation
$$n = a_0 k^s + a_1 k^{s-1} + \dots + a_s \quad \text{where} \quad a_0 \neq 0.$$
$a_0 \neq 0$ and where each a_i is non negative & less than k. Furthermore, this is a unique representation of n called representation of n to base k.

eg. Let $k = 10$ and $n = 126$.
$$126 = \underset{a_0}{1} \times 10^2 + \underset{a_1}{2} \times 10^1 + \underset{a_2}{6} \times 10^0$$

eg. $n = 23$ Binary = 10111 $k = 2$.
$$23 = \underset{a_0}{1} \times 2^4 + \underset{a_1}{0} \times 2^3 + \underset{a_2}{1} \times 2^2 + \underset{a_3}{1} \times 2^1 + \underset{a_4}{1} \times 2^0$$

Note: Each integer greater than 1 can serve as a base for representing +ve integers.

Euclids Division Lemma:

For any integer k $(k > 0)$ and j, $\exists$ unique integers q and r such that $0 \leq r < k$
$$j = q \cdot k + r$$
Unique representation

eg. $3\overline{)20}(6$
$\frac{18}{2}$

$20 = 3 \cdot 6 + 2$.
$j = q \cdot k + r$

Proof: Case 1 : $k = 1$
$$\underset{}{j} = j = j \cdot \underset{(k)}{1} + \underset{(r)}{0}$$

Case 2: Let $k > 1$ $(j > 0)$

Let j be represented as
$$j = a_s k^s + a_{s-1} k^{s-1} + \dots + a_1 k + a_0$$
... From Basic Representation Theorem

Taking k common
$$j = k(a_s k^{s-1} + a_{s-1} k^{s-2} + \dots + a_1) + a_0 \quad \text{— (1)}$$
Here $a_s k^{s-1} + a_{s-1} k^{s-2} + \dots + a_1$ is representation of some integer say 'q'.

Let $a_0 = r$.

Hence ① becomes; $j = q \cdot k + r$.

To prove uniqueness:

Let $\exists\ q'$ & r' such that j has another representation.

$$j = q' \cdot k + r' \quad — ②$$

As q' can be written as

$$q' = b_t k^t + b_{t-1} k^{t-1} + \ldots + b_1 k + b_0 \quad — ③$$

Putting ③ in ②

$$j = (b_t k^t + b_{t-1} k^{t-1} + \ldots + b_1 k + b_0) k + r'$$

$$j = b_t k^{t+1} + b_{t-1} k^t + \ldots + b_1 k^2 + b_0 k + r' \quad — ④$$

As ① and ④ are same, then powers of k must be same;

Comparing;

$$\cdot\ a_s k^s + a_{s-1} k^{s-1} + \ldots + a_1 k + a_0 = b_t k^{t+1} + b_{t-1} k^t + \ldots + b_1 k^2 + b_0 k + r'$$

10th Sept'13

On comparing;

$$a_0 = r'$$

$$b_i = a_{i+1}$$

$$s = t+1$$

$$q' = b_t k^t + b_{t-1} k^{t-1} + \ldots + b_1 k + b_0$$

↓ In Terms of a.

$$q' = a_s k^{s-1} + \cancel{b}\overset{a}{}_{s-1} k^{s-2} + \ldots + a_2 k + a_1 = q.$$

$\therefore$

$$q' = q.$$

Hence uniqueness proved.

Case 3: $j < 0$

$\therefore -j > 0.$

$\exists\ q'' \ \& \ r''$ such that.

$-j = q''k + r''$

$j = -q''k - r''$

Adding & subtracting k on RHS.

$= -k - q''k + k - r''$

$= k\underbrace{(-q''-1)}_{q} + \underbrace{(k - r'')}_{r}$

$j = kq + r$

Hence Proved.

Page 14.

Q7. Prove that if a is an odd integer than
$\{a^2 + (a+2)^2 + (a+4)^2 + 1\}$ is divisible by 12.

Proof: Let $a = 2m+1$.

Substituting in above eq^n.

$(2m+1)^2 + (2m+3)^2 + (2m+5)^2 + 1$

$4m^2 + 4m + 1 + 4m^2 + 12m + 9 + 4m^2 + 20m + 25 + 1$

$= 12m^2 + 36m + 36$

$12(m^2 + 3m + 3)$.

Hence Proved.

Q6. Prove that if a & b are an odd int. then
$a^2 - b^2$ is divisible by 8.

Proof. $a = 2m+1 \quad b = 2n+1$.

Substituting;

$4m^2 + 4m + 1 - 4n^2 - 4n - 1$

$\cancel{+2n^2}$

$\cancel{2}(\cancel{2m^2 + 2m + 2n + 1})$

Considering cases.

(1) $= 4m^2+4n^2+4m+4n+\cancel{2} = 4(m^2+n^2+m+n)$.

Cases: When both m & n are odd integers.

$m = 2p+1$ $\quad$ $n = 2r+1$.

Substituting;

$= 4((2p+1)^2+(2r+1)^2+2p+1+2r+1$

$= 4(4p^2+4r^2+6p+6r+4)$.

$= \underline{\underline{8}}(2p^2+2r^2+3p+3r+2)$.

↳ Divisible by 8.

(2) m & n even integers

$m = 2p$ $\quad$ $n = 2r$

Substituting;

$= 4(4p^2+4r^2+2p+2r)$

$= \underline{\underline{8}}(2p^2+2r^2+p+r)$.

↳ Divisible by 8.

(3) m → even $\quad$ n → odd.

$m = 2p$ $\quad$ $n = 2r+1$

Substituting.

$= 4((2p)^2+4r^2+2\cdot 2r+1+2r+1+2p)$

$= \underline{\underline{8}}(2p^2+2r^2+2r+p+1)$

↳ Divisible by 8.

(4) m → odd $\quad$ n → even

$2p+1$ $\quad$ $2r$

Substituting:

$= \underline{\underline{8}}(2p^2+2r^2+r+2p+1)$.

↳ Divisible by 8.

10th Sept.

22. Divisibility

Notation: Divides : $2|8$ $= 8/2$

Not divides : $3 \nmid 7$ $= 7/3 \longrightarrow$ Not a integer.

Results:

1. If a is any integer then $1|a = a/1 = a$. $-1|a$
2. " $a|a = 1$. $-a|a$
3. " $a|0 = 0$

Page 15.

Q24. Let a, b, c and d be integers & e divides both a and c then show that e divides $(ab+cd)$.

Proof: Given: e divides a and c. $e|a$ & $e|c$

$\therefore$ $a = eq_1 + r_1$ $r_1 = 0$ $= eq_1$ —① $q_1, q_2 \in I$

$c = eq_2 + r_2$ $r_2 = 0$ $= eq_2$. —②

Equation $= (ab+cd)$. —③

Substituting ① & ② in ③.

$(e.q_1.b + e.q_2.d)$.

Taking e common

$(ab+cd) = (e)(q_1b + q_2d)$.

Hence Proved.

$\frac{ab+cd}{e} = \underbrace{q_1b+q_2d}_{\in I} \Rightarrow e|ab+cd$.

- GCD:

Defⁿ: If a & b are integers both not zero then an integer d is called greatest common divisor of a & b if:

i) $d > 0$

ii) d is a common divisor of a & b.

iii) Each integer 'f' that is a common divisor of both a & b is also divisor of d.

Ex.2.5. Considering $a = 12$ $b = -8$

Divisors of 12 = 1, 2, 3, 4, 6, 12

Divisors of -8 = 1, 2, 4, 8

Greatest common divisor = d = 4.

Euclidean algorithm for finding the G.C.D.

Ex 2.7. Find G.C.D (341, 527)

Taking the largest number.

Dividing larger no. by small no ie.

$$341 \overline{)527}\,(1$$
$$\underline{-341}$$
$$186$$

By basic representation thⁿ.

$$\underbrace{527}_{\text{larger no.}} = 341 \times 1 + 186.$$

dividing by

$$186 \overline{)341}\,(1$$
$$\underline{-186}$$
$$155$$

$341 = 186 \times 1 + 155$

Dividing.

$186 = 155 \times 1 + 31$

Dividing.

$155 = 31 \times 5 + 0$

GCD. = 31.

Page 21.

Ex. (b). 361, 1178.

① $361 \overline{)1178}$ (3

1083

0095

$1178 = 361 \times 3 + 95$

② $95 \overline{)361}$ (3

−285

76

③ $361 = 95 \times 3 + 76$.

$76 \overline{)95}$ (1

−76

19.

$95 = 76 \times 1 + 19$.

④ $19 \overline{)76}$ (4

76

0.

GCD = 19

(c) 12321, 8658

① $8658 \overline{)12321}(1$
$$\begin{array}{r} 12321 \\ -8658 \\ \hline 3663 \end{array}$$

$12321 = 8658 \times 1 + 3663$

② $3663 \overline{)8658}(2$
$$\begin{array}{r} 8658 \\ -7326 \\ \hline 1332 \end{array}$$

$8658 = 3663 \times 2 + 1332$

③ $1332 \overline{)3663}(2$
$$\begin{array}{r} 3663 \\ -2664 \\ \hline 999 \end{array}$$

$3663 = 1332 \times 2 \times 999.$

④ $999 \overline{)1332}(31.$
$$\begin{array}{r} 1332 \\ -999 \\ \hline 333 \end{array}$$

⑤④ $333 \overline{)999}(3$
$$\begin{array}{r} 999 \\ 999 \\ \hline 0 \end{array}$$

GCD = 333.

15th Sept
Page 18.

Cor. 2-1. (Corollary)

If d is the g.c.d (a,b), then there exist integers x & y Show that.

$$ax+by=d.$$

(Proof skipped).

Q. Find integers x and y Such that (341, 527) GCD = 31.

$$341x + 527y = \underbrace{31}_{d}.$$

Basic Representation:

$$527 = 1 \times 341 + 186$$
$$341 = 1 \times 186 + 155$$
$$186 = 1 \times 155 + 31 \quad \text{Starting Point.}$$
$$155 = 5 \times 31. + 0$$

$$\downarrow$$

$$31 = 186 - 1 \times 155$$
$$= 186 - (1 \times 341 - 1 \times 186)$$
$$= 2 \times 186 - 1 \times 341$$

$$= 2(527 - 1 \times 341) - 1 \times 341$$
$$31 = 2 \times 527 - 3 \times 341$$

$\therefore$ $x = -3$ and $y = 2$.

$$-3 \times 341 + 2 \times 527 = 31.$$

Cor-2.2.

Page 19. In order that exists integers x and y satisfying

$ax+by = c$ ... Diophantine eq^n

it is necessary and sufficient (iff) that $d|c$ where

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

Proof Let $\exists\, x$ & y such that;

$$ax+by = c \quad -(1)$$

if d is $g.c.d(a,b)$. ie

$d|a$ and $d|b$

$\frac{a}{d} = e \longrightarrow a = de$ also $\frac{b}{d} = f \longrightarrow b = fd$.

Substituting a & b in (1).

$$de.x + df.y = c.$$

$$d(ex+fy) = c.$$

$$\underbrace{(ex+fy)}_{\exists \text{ Integer.}} = \frac{c}{d} \qquad \because e,x,f,y \ \exists\, I.$$

$\therefore d|c$ Proved. Necessary cond^n proved.

Case II: If $d|c \longrightarrow \frac{c}{d} = k \Rightarrow c = dk$.

from Corollary 2-1. $\exists\, x', y'$ such that

$$ax' + by' = d.$$

Multiply all sides by k

$$a(x'k) + b(y'k) = dk$$

$$\downarrow \qquad \downarrow \qquad \downarrow$$

$$x \qquad y \qquad c$$

$ax+by = c$ Hence Proved

Sufficient condition proved

Def^n 2.2. PRIME NO. A positive int. 'p' other than 1 is said to be a prime if its only (+) divisors are 1 and p.

Def^n 2.3 RELATIVE PRIME. We say a and b are relatively prime if g.c.d $(a,b)=1$.

Ex. If $d = g.c.d(a,b)$ then $\left(\frac{a}{d}\right)$ and $\left(\frac{b}{d}\right)$ are relatively prime

Proof. By Corollary 2.1 $\exists$ integer x & y such that

$$ax + by = d$$

Divide all by d

$$\left(\frac{a}{d}\right)x + \left(\frac{b}{d}\right)y = 1.$$

By def^n of G.C.D:

The G.C.D $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. ... Hence Relatively Prime.

Ex 2.11 If 'p' is a prime and 'a' is an integer. Such that $p \nmid a$ (p doesn't divide a), then p and a are relatively prime.

17th Sept.

Thm^r 2.3. If a, b, c are integers where a and c is relatively prime and if $c|ab$, then $c|b$.

Proof.

Since a & c relatively prime → g.c.d $(a,c)=1$.

there will be integers x & y such that

$$ax + cy = 1$$

$$abx + cby = b \quad \text{(multiply by 'b')} \quad \text{—①}$$

If $c|ab$

$$\frac{ab}{c} = k$$

$$ab = ck \quad \text{... Replacing ab in ①}$$

$$ckx + cby = b \quad -(2)$$

$$c(kx+by) = b$$

$\Rightarrow$ Integers.

$$\frac{b}{c} = \text{Integer} = kx+by$$

$$c \mid b$$

Hence 1 Proved.

Corollary 2.3. If a and b are integers p is a prime $p \mid ab$ & $p \nmid b$ then $p \mid b$

Relatively prime.

Ques.1. Use Euclidean algo & find G.C.D of 156, 1740.

Soln.

$$156 \overline{)1740}(11$$
$$\underline{1716}$$
$$24$$

$$1740 = 156 \times 11 + 24$$

$$24 \overline{)156}(6$$
$$\underline{144}$$
$$12$$

$$156 = 24 \times 6 + 12$$

$$12 \overline{)24}(2$$
$$\underline{24}$$
$$0$$

$$G.C.D = \underline{12}$$

Ques 2. G.C.D (299, 481). Find x & y such that $299x + 481y = d$.

Solution 1.

Step 1:

$$299 \overline{)\,481\,}(1$$
$$-299$$
$$182$$

$481 = 299 \times 1 + 182$.

Step 2:

$$182 \overline{)\,299\,}(1$$
$$-182$$
$$117$$

$299 = 117 + 182 \times 1$.

Step 3.

$$117 \overline{)\,182\,}(1$$
$$-117$$
$$65$$

$182 = 117 \times 1 + 65$.

Step 4.

$$65 \overline{)\,117\,}(1$$
$$65$$
$$52$$

$117 = 65 \times 1 + 52$

Step 5. $65 = 52 \times 1 + 13$

Step 6. $52 = 13 \times 4 + 0$

G.C.D = 13

Solution 2.

To find x & y.

$13 = 65 - 1 \times 52$

$13 = 65 - 1 \times (117 - 65 \times 1)$

$13 = 2 \times 65 - 1 \times 117$

$13 = 2 \times (182 - 117 \times 1) - 1 \times 117$

$13 = 2 \times 182 - 3 \times 117$

$13 = 2 \times 182 - 3 \times (299 - 182 \times 1)$

$13 = \overset{5}{\cancel{\ }} \times 182 - 3 \times 299$

$13 = \overset{5}{\cancel{\ }} \times (481 - 299 \times 1) - 3 \times 299$

$13 = \overset{5}{\cancel{\ }} \times 481 - \overset{8}{\cancel{\ }} \times 299$.

$\therefore x = \cancel{-6}\ {-8} \quad y = \cancel{8}\ 5$.

Soln: $299 \times (\cancel{-6}) - 481(\cancel{8}) = 13$
$(-8) \quad (5)$

$$\left.\begin{aligned} x &= -8 \\ y &= 5 \end{aligned}\right\}.$$

Lowest Common Multiple (L.C.M).

$$L.C.M = \frac{a\,b}{g.c.d(a,b)}.$$

eg. LCM(299,481)

$G.C.D(299,481) = 13$

By formula;

$$LCM(299,481) = \frac{299 \times 481}{13} = 11063$$

Ques 5. Find L.C.M of (n, n+1).

Consecutive number.

(One odd - One even).

For consecutive integers → No common factor expect → 1.

$\therefore G.C.D(n, n+1) = 1$ → Relatively prime

By Euclidean method:

$n+1 = n \times 1 \times 1$

$n = 1 \times n = 0$

$G.C.D = 1$

$$L.C.M(n, n+1) = \frac{n.(n+1)}{1} = n^2 + n.$$

Ques 7. Find LCM (2n-1, 2n+1).

$2n+1 = \overset{\times 1}{2n-1} + 2$

$2n-1 = n \times 2 - 1. = 2 \times (n-1) - 1$

$2n-1 = 1 \times (n-1) + 0.$

$G.C.D = 1.$

$$L.C.M = \frac{(2n-1)(2n+1)}{1} = 4n^2 - 1$$

Blankinships method to find G.C.D.

Ex. Find G.C.D (12, 30).

Step 1. Form a matrix $\begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix}$.

By elementary row transformation reduce to

$$\begin{pmatrix} d & x & y \\ 0 & x' & y' \end{pmatrix} \text{ or } \begin{pmatrix} 0 & x' & y' \\ d & x & y \end{pmatrix}$$

→ No fractional transformation

$$\begin{pmatrix} 30 & 1 & 0 \\ 12 & 0 & 1 \end{pmatrix}$$

$R_1 \rightarrow R_1 \times - {}^{2} \times R_2$.

$$\begin{pmatrix} 6 & 1 & -2 \\ 12 & 0 & 1 \end{pmatrix}$$

$R_2 \rightarrow R_2 - 2R_1$

$$\begin{pmatrix} 6 & 1 & -2 \\ 0 & -2 & 5 \end{pmatrix}$$

$d = 6 \quad x = 1$ and $y = -2$.

Ex. G.C.D (129, 301)

$$\begin{pmatrix} 301 & 1 & 0 \\ 129 & 0 & 1 \end{pmatrix}$$

$$\begin{array}{r} 301 \\ -258 \\ \hline 43 \end{array}$$

$R_1 \rightarrow R_1 - 2 \times R_2$

$$\begin{pmatrix} 43 & 1 & -2 \\ 129 & 0 & 1 \end{pmatrix}$$

$R_2 \rightarrow R_2 - 3R_1$

$$\begin{pmatrix} 43 & 1 & -2 \\ 0 & -3 & 7 \end{pmatrix}$$

$d = 43 \quad x = 1$ & $y = -2$

classmate
Date
Page

18th Sept '13.

Ex. Find G.C.D of (621, 414) by Blankinships method.

$$\begin{pmatrix} 621 & 1 & 0 \\ 414 & 0 & 1 \end{pmatrix}$$

$$R_1 \to R_1 - R_2$$

$$\begin{pmatrix} 207 & 1 & -1 \\ 414 & 0 & 1 \end{pmatrix}.$$

$$R_2 \to R_2 - 2R_1$$

$$\begin{pmatrix} 207 & 1 & -1 \\ 0 & -2 & +3 \end{pmatrix}$$

Solution. $d = 207$ $(x = 1 \quad y = -1)$

Ex. G.C.D (36, 24, 54, 27) by Euclidean algo.

Step 1. G.C.D(36, 24) : $36 = 24 \times 1 + 12$.

$24 = 12 \times 2 + 0$.

G.C.D = 12. —(1)

Step 2. G.C.D (12, 54, 27).

G.C.D(12, 27) . $27 = 12 \times 2 + 3$

$12 = 3 \times 4 + 0$

G.C.D = 3. —(2)

Step 3 G.C.D (54, 3) = $54 = 3 \times 18 + 0$

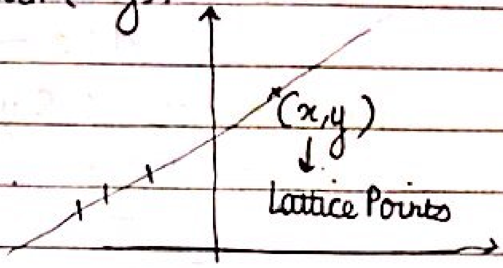
Solution G.C.D = 3 —(3)

classmate
Date
Page

Diophantine Equations:

$ax+by=c \longrightarrow$ Lattice Point soln (x,y).

- Linear equation with 2 unknowns. $x,y \in I$.
  $a,b,c \neq 0$
- Not all diophantine equations have a solution.



Theorem: The linear diophantine equation $ax+by=c$ has a solution if $d|c$ where $d = G.C.D(a,b)$
G.C.D (a,b).
Furthemore, if (x_0,y_0) is a solution of this equation then the set of soln. of the eq^n consists of all integers (x,y) where

If $ax+by=c$.
$$\begin{cases} x = x_0 + \dfrac{b}{d}t \\ y = y_0 - \dfrac{a}{d}t \end{cases} \qquad t = 0, \pm1, \pm2, \pm3 \ldots$$

If $ax-by=c$
$$\begin{cases} x = x_0 + b/d \cdot t \\ y = y_0 + a/d \cdot t \end{cases} \qquad t = 0, \pm1, \pm2 \ldots$$

Ex ① Does $15x+27y=1$ have a solution.

Answer. $G.C.D(15,27) = \quad 27 = 15 \times 1 + 12$

$15 = 12 \times 1 + 3$

$12 = 3 \times 4 + 0$

$G.C.D = d = 3$.

$c = 1$.

$\because d \nmid c \rightarrow 3 \nmid 1 \longrightarrow$ No integer solution

Ex. 2. $5x+6y=1$ solution ? $b=6$ $a=5$

$G.C.D=(5,6)=1.=d$

$\because d|c \rightarrow 1|1 \rightarrow$ Integer soln possible.

Direct soln $x_0=-1$ & $y_0=1$.

By Formula: $x=-1+\frac{6}{1}t = 6t-1$

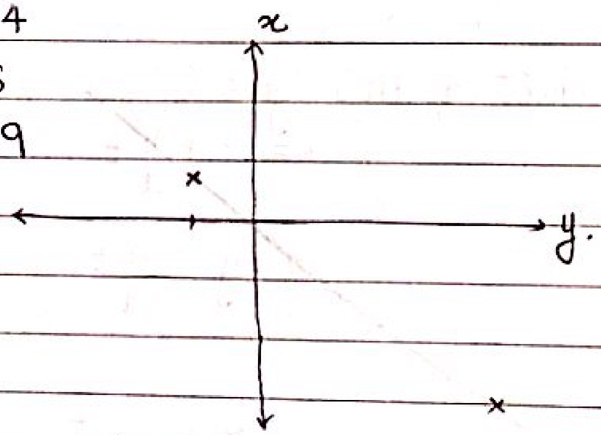
$t=0,\pm1,\pm2\ldots.$

$y = 1 \overset{(-)}{\ } \frac{5}{1}t \overset{(-)}{=} 5t+1$

Infinite pair of (x,y).

On axis.

Equidistant points
$t=0$ $x=-1$ $y=1$
$t=1$ $x=5$ $y=-4$
$t=-1$ $x=-7$ $y=+6$
$t=2$ $x=11$ $y=-9$



Ex. Pg25.

1. Find general soln if it exists.

a) $2x+3y=4$

b) $17x+19y=23$

c) $15x+51y=41$.

a) $2x+3y=4$ $(x_0=-1$ $y_0=2.)$

$G.C.D=(2,3)=1$

$1|4 \rightarrow$ Soln exists

$\left.\begin{array}{l} x=-1+3t \\ y=2+2t. \end{array}\right\}$ (x,y) pair

b) $17x+19y=23$ $(x_0=-2$ $y_0=3.)$

$GCD(17,19)=1$.

$1|23 \rightarrow$ Soln exists.

$\left.\begin{array}{l} x=-2+19t \\ y=3+17t \end{array}\right\}$ (x,y) pair

c) $15x+51y=41$ .. $51=15\times3+6$ G.C.D $=3$.

$15=6\times2+3$

$6=3\times2+0$

$3\nmid41 \rightarrow$ No soln exists

classmate
Date
Page

19th Sept '13.

(e) $10x - 8y = 42$

$G.C.D(10,8) = 10 = 8 \times 1 + 2$

$8 = 2 \times 4 + 0$ $\qquad 2 = 10 - 8 \times 1.$

$G.C.D = 2.$ $\qquad x = 1 \quad y = -1.$

$2 \mid 42$ ∴ Integer solution exists.

$10 \times 1 - 8 \times 1 = 2$ —①

→ $ax + by = d$. Multiply ① by 21.

$21\,(10 \times 1 + 8(-1) = 2 \times 21).$

$10 \times 21 + 8(-21) = 42.$ (Comparing with original eqⁿ).

$x_0 = 21 \qquad y_0 = +21.$

$$\left.\begin{aligned} x &= 21 + \frac{(+8)\,t}{2} = 21 + 4t \\ y &= +21 + 5t \end{aligned}\right\} \begin{array}{l} (x, y) \text{ pair.} \\ \infty \text{ Solution} \end{array}$$

For $t = 1$ $x = 25$ $y = 26$ $\qquad t = 0, \pm 1, \pm 2 \dots$

Ex. 2. A man pays \$1.43 for some apples & pears. If pears cost 17¢ & apple costs 15¢ each. How many of each did he buy.

Diaophanthine eqⁿ = $17x + 15y = 143.$

$G.C.D(17, 15) = 1.$ $\qquad 17 = 15 \times 1 + 2.$

$1 \mid 143.$ Integer soln exists.

Two methods: Hit and Try or Euclidean.

$17 = 15 \times 1 + 2$

$15 = 2 \times 7 + 1$

$7 = 2 \times 3 + 1.$

$3 = 2 \times 1 + 1$

$2 = 1 \times 2 + 0$

$G.C.D = \underline{1}.$

$1 = 15 - 2 \times 7.$

$\cancel{143 = 15 \times 14}$ $\quad 1 = 15 - 7 \times (17 - 15 \times 1).$

$1 = -7 \times 17 + \cancel{6} \times 15.$
8

$$1 = 8\times 15 - 7\times 17$$

Multiply by 143

$$143 = (8\times 143)15 - (7\times 143)17.$$

$$x = -(7\times \overset{2}{143}) = -1001$$

$$y = 8\times \overset{2}{143} = 1144$$

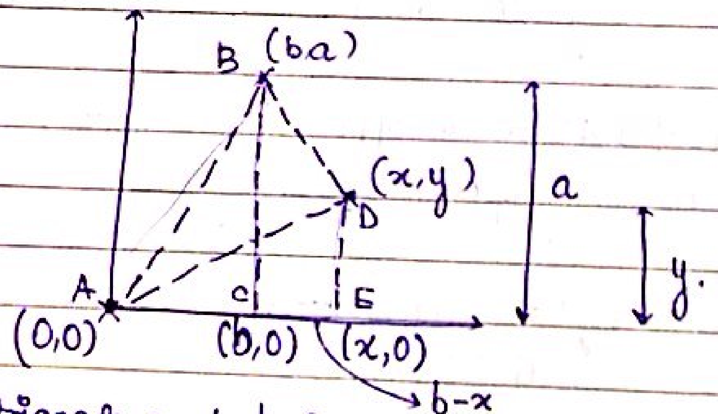
$x_0 = -1001$ $\qquad y_0 = 1144$

$$x = -1001 + 17t = -1001+17t. \quad \text{Only } \oplus \text{ answers.}$$

$$y = 1144 - 15t. = 1144-15t$$

$t = 67.$ $\underbrace{x = 4}_{\text{Pears}}$ $\underbrace{y = 5.}_{\text{Apples}}$ Solution.

4. Prove that area of the triangle whose vertices are $(0,0)$: (b,a) & (x,y) is $\dfrac{|by-ax|}{2}.$



Area of bigger triangle ABC $= \frac{1}{2} b.a.$

— " — $\triangle ADE = \frac{1}{2}xy.$

Trapezium BCDE $= \frac{1}{2}(bx-b)(a+y)$

$$\therefore \triangle ABD = \frac{1}{2}ba - \left(\frac{1}{2}xy + \frac{1}{2}(x-b)(a+y)\right)$$

$$= \frac{1}{2}(by-ax) = \frac{|by-ax|}{2}.$$

Area cannot be $\ominus$.

classmate

Date ____
Page ____

Q. Proof that if (x_0, y_0) is soln of $ax - by = 1$ then area of Δ whose vertices are $(0,0)$ (b,a) (x_0, y_0) is $1/2$.

Solution (x_0, y_0) satisfies $ax_0 - by_0 = 1$.

as we know area $= \frac{1}{2} |by - ax|$ if vertices are $(0,0); (b,a); (x,y)$.

If vertices are $(0,0)$ (b,a) (x_0, y_0)

$$\text{Area} = \frac{1}{2} |by_0 - ax_0|$$

$$by_0 - ax_0 = -1$$

$$= \frac{1}{2} |-1| = \frac{1}{2}.$$

Hence Proved.

22nd Sept.

Q7. What is the ⊥dicular dist to the origin $(0,0)$ from line $ax - by = 1$.

$$\text{Distance} = \frac{|ax - by - 1|}{\sqrt{a^2 + b^2}}$$

⊥dicular from origin $(x,y) = (0,0)$

$$= \frac{|-1|}{\sqrt{a^2 + b^2}}$$

$$= \frac{1}{\sqrt{a^2 + b^2}}$$

classmate

Date
Page

Article 2-4. Fundamentals of Arithmatic.

Any number n can be represented in the product of prime powers.

Fundamental Theorem of Arithmatic

Thm^r. For each integer $n>1$; there exists primes $p_1 \le p_2 \le p_3 \cdots \le p_r$ such that $n = p_1 \cdot p_2 \cdots p_r$ .. this representation is unique.

n	Factorization.
2	2
3	3
4	2^2
5	5
6	2×3
7	7

Ques. 3,4,5 → G.C.D & L CM from Fund^m Th^m of Arithmatic.

G.CD & L.C.M using Prime Factorization.

eg. (24, 65, 57)

$24 = 2^3 \times 3$

$65 = 5 \times 13$

$57 = 3 \times 19$

Express in Product of prime powers for all number

for. G.C.D.

① $24 = 2^3 \times 3 \times 5^0 \times 13^0 \times 19^0$

② $65 = 2^0 \times 3^0 \times 5 \times 13 \times 19^0$

③ $57 = 2^0 \times 3 \times 5^0 \times 13^0 \times 19$

Taking smallest power of all prime nos.

$GCD = 2^0 \times 3^0 \times 5^0 \times 13^0 \times 19^0$

$= 1$. G.CD.

FOR L.C.D Taking highest powers

$LCD = 2^3 \times 3 \times 5 \times 13 \times 19$

$= 120 \times 13 \times 19 = 120 \times 247 = \underline{34640}$

Ques 6. (1) Find g.c.d of (2187, 999) using prime factori

(2) g.c.d of (p^2q, pqr) where p q r are prime

(2). $p^2q = p^2 \times q \times r^0$

$pqr = p \times q \times r$

$G.C.D = p \times q \times r^0 = \underline{pq}$

$L.C.D = p^2 \times q \times r = \underline{\underline{p^2qr}}$

(1) $2187 = 3^7 \times 37^0$

$999 = 3^3 \times 37^1$.

$G.C.D = 3^3 \times 37^0 = 9 \times 3 = \underline{27}$

$L.C.M = 3^7 \times 37^1 = 2187 \times 37 = \underline{\underline{80919}}$.

Ques. 11. Find g.c.d (39, 102, 75)

$39 = 3 \times 13$

$102 = 3 \times 2 \times 17$

$75 = 3 \times 5^2$

$G.C.D = \underline{\underline{3}}$

$L.C.M = 3 \times 13 \times 5^2 \times 2 \times 17 = \underline{\underline{33{,}150}}$

Examples (1) If $a|b$ and $c|d$ then $ac|bd$

Let $a|b \longrightarrow \frac{b}{a} = k$ and $\frac{\cancel{c}}{\cancel{d}} = p$ $\frac{d}{c} = p$.

$b = ak$ $\cancel{c = dp}$. $d = cp$

To show $ac | bd$

$bd = ak \times \cancel{dp}\ cp$

$= ackp$.

$\frac{\cancel{ac}}{\cancel{bd}} = \frac{bd}{ac} = \frac{ackp}{ac} = kp \in \text{int}$

Hence Proved

classmate
Date
Page

Solve.

H.W
② If $a|b$ and $b|c$ then $a|c$
③ If $a|b$ & $a|c$ then $a|bx+cy$ $x, y \in$ Int.
④ If $a|b$ & $a|c$ then $a|b \pm c$.

Note: If $a|b$ and $c|d$ then $(a+c) + (b+d)$

Ques. Show g.c.d $(ab, ad) = a\,$g.c.d(b,d)

Proof: Let b and d be any intiger.

Let $b \geq d$

(A)
$$b = q_1 d + r_1.$$
$$d = q_2 r_1 + r_2 \qquad \text{(Divide by the remainder).}$$
$$r_1 = q_3 r_2 + r_3$$
$$\vdots$$

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

Multiply (A) by a on both sides.
$$ab = aq_1 d + ar_1$$
$$ad = aq_2 r_1 + ar_2$$
$$\vdots$$
$$ar_{n-1} = aq_{n+1} r_n + \underline{\underline{0}} \quad \leftarrow \text{Last eq}^n.$$

G.C.D $= \underline{ar_n}$

$$\text{G.C.D}(ab, ad) = a\underline{r_n} =$$
$$\text{G.C.D}(b,d)$$
$$= a\,\text{G.C.D}(b,d)$$

24th Sept.

Ex 22. Q. Prove $g.c.d(a+b, a-b) \geq g.c.d(a,b)$.

Proof. Let $g.c.d(a,b) = d$.

$d \mid a$ and $d \mid b$

Then d will divide $d \mid a+b$ & $d \mid a-b$

So g.c.d will $d \mid g.c.d(a+b, a-b)$ ... By defn of g.c.d.

as $g.c.d(a,b) = d$.

$\therefore g.c.d(a,b) \leq g.c.d(a+b, a-b)$.

Q. Show that for any integer n $\dfrac{21n+4}{14n+3}$ is irreducible.

To prove irreducible prog: $g.c.d(21n+4, 14n+3) = 1$.

or.

Find $ax + by = (d) \rightarrow g.c.d$

To find x & y such that. $(21n+4)x + (14n+3)y = 1$.

By hit and trial $x = -2$ $y = 3$

$(21n+4)(-2) + (14n+3)(3) = 1$.

Hence x & y exists. $\therefore g.c.d(21n+4, 14n+3) = 1$

Relatively prime.

Q. Show g.c.d of $(2a+1, 9a+4) = 1$.

$(2a+1)x + (9a+4)y = 1$

$x = +9$ $y = -2$.

$(2a+1)9 + (9a+4)(-2) = 1$

Hence x, y exists.

$\therefore g.c.d(2a+1, 9a+4) = 1$.

$2a+1 \overline{)9a+4}$ 4

$8a+4$

$+a$

$a \overline{)2a+1}$ 2

$2a$

1

24th Sept.

Chapter 4. Congruences.

Def^n. a is congruent to b(mod c) ⟶ $a \equiv b \pmod{c}$ if.

* $c \mid a-b$.

eg. $8 \equiv 4 \pmod{2}$ $\quad 2 \mid 8-4$ Congruent.

$5 \equiv 2 \pmod{3}$ Congruent

$4 \not\equiv 2 \pmod{3}$ Not congruent.

Real life eg. For a 24-hr time clock ⟶ eg. $17 \equiv ? \pmod{12}$

Used in cryptography. ↳ 5pm.

To find digits (last) of large nos ↳ 2^{1002}.

Fermat's Little Theorem:

If p is a prime number then $p \mid n^p - n$

in form of congruence

$$n^p \equiv n \pmod{p}$$

Wilson's Theorem:

If p is a prime number then $p \mid [(p-1)! + 1]$

$$(p-1)! \equiv -1 \pmod{p}$$

Note: 1. $a \equiv a \pmod{c}$ $\quad c \to$ non zero I.

2. If $c \neq 0$ and $a \equiv b \pmod{c}$ then $b \equiv a \pmod{c}$.

$$\frac{(a-b)}{c} = \text{int} = k.$$

$$-\frac{(b-a)}{c} = k.$$

Theorem 4-1. If a, b, c, d are integers $c \neq 0$, the following assertion hold.

1. $a \equiv a \pmod{c}$ .. Reflexive
2. If $a \equiv b \pmod{c}$ & $c \in I$ then $b \equiv a \pmod{c}$ .. Symmetric
3. If $a \equiv b \pmod{c}$ & $b \equiv d \pmod{c}$ then $a \equiv d \pmod{c}$ .. Transitive.

Proof. ①. $a \equiv a \pmod{c} \longrightarrow \frac{a-a}{c} = c|0$ .. True.

② $a \equiv b \pmod{c} \longrightarrow \frac{a-b}{c} = k \rightarrow -\frac{(b-a)}{c} = k \longrightarrow b \equiv a \pmod{c}$.

③ $a \equiv b \pmod{c} \longrightarrow \frac{a-b}{c} = k_1$

$b \equiv d \pmod{c} \longrightarrow \frac{b-d}{c} = k_2$ $\quad b = ck_2 + d$.

Substituting.

$$\frac{a - ck_2 - d}{c} = k_1$$

$$\frac{a-d}{c} - k_2 = k_1$$

$$\frac{a-d}{c} = \underbrace{k_1 + k_2}_{k \in I}$$

$$\therefore \frac{a-d}{c} = k \longrightarrow \text{congruent}$$

$$\Rightarrow a \equiv d \pmod{c}$$

26th Sept'13.

Thm 4-2. Suppose $a \equiv a' (\text{mod } c)$ and $b \equiv b' (\text{mod } c)$ then

$a \pm b \equiv (a' \pm b') \text{ mod } c$ and

$ab \equiv a'b' (\text{mod } c)$.

eg. $4 \equiv 2 (\text{mod } 2)$
$5 \equiv 3 (\text{mod } 2)$ $\Big\} \longrightarrow 9 \equiv \cancel{4}\,5 (\text{mod } c)$ also $20 \equiv 6 (\text{mod } 2)$

$5 \to a'+b'$; $a'b'$

$a+b$; True. ; 2 ; ab ; True.

Addition

Proof: $a \equiv a' (\text{mod } c) \longrightarrow \dfrac{a-a'}{c} = k$. — ①

$b \equiv b' (\text{mod } c) \longrightarrow \dfrac{b-b'}{c} = r$ — ②

Adding ① and ②.

$$\frac{a-a'}{c} + \frac{b-b'}{c} = k + r$$

$$\frac{(a+b) - (a'+b')}{c} = k + r$$

$\in$ Integer

In congurence.

$$(a+b) \equiv a'+b' (\text{mod } c).$$

Product.

(ii) $ab \equiv a'b' (\text{mod } c)$ (Reverse Proof).

$$\frac{ab - a'b'}{c}$$

adding & subtracting ab'

$$\frac{ab - ab' - a'b' + ab'}{c}$$

$$\frac{a(b-b') + b'(a-a')}{c}.$$

$$= \frac{a(b-b')}{c} + \frac{b'(a-a')}{c} = \text{integer}$$

From congruence rule for addn & subn.

Cancellation Law:

Thm^r 4.3. If $bd \equiv bd'(\mathrm{mod}\ c)$ and if $g.c.d(b,c)=1$ then $d \equiv d'(\mathrm{mod}\ c)$

eg. $6 \equiv 12 (\mathrm{mod}\ 2)$

$2 \times 3 \equiv 2^2 \times 3 (\mathrm{mod}\ 2)$.

① $3 \not\equiv 6 (\mathrm{mod}\ 2)$.

② $2 \equiv 2^2 (\mathrm{mod}\ 2)$ Cancellation of 3. (3,2) ... Relatively prime.

Proof: $\frac{bd - bd'}{c} = k$.

$\frac{b(d-d')}{c}$ as $\frac{b}{c} \to$ irreducible.

$g.c.d(b,c)=1$

$\therefore \frac{d-d'}{c} \to$ integer.

by congurence.

$d \equiv d'(\mathrm{mod}\ c)$.

$ax \equiv b(\mathrm{mod}\ c)$ ... Linear congruence.

Ex. Pg. 51. ① $5x \equiv 4 (\mathrm{mod}\ 3)$. By hit & trial.

$\frac{5x-4}{3} \to$ integer $\to x = 2, 8$

For congruence there will be ∞ no. of soln.

② $7x \equiv 6 (\mathrm{mod}\ 5)$

$\frac{7x-6}{5} \equiv\to$ integer $\to x = 3$

③ $9x \equiv 8 (\mathrm{mod}\ 7)$.

$\frac{9x-8}{7} \to$ integer $\to x = 4$

④ $6x \equiv 5 (\mathrm{mod}\ 4)$ G.C.D $(6,4) = 2 \nmid 5 \to$ No soln.

⑤ $10x \equiv 8 (\mathrm{mod}\ 6) \longrightarrow x = 2$.

$\rightarrow$ $\underbrace{ax \equiv b \pmod{c}}$

$\downarrow$

Find g.c.d $(a, c) = d$.

Iff $d \mid b \rightarrow$ Solution exists

$d \nmid b \rightarrow$ Solution doesn't exist.

1st Oct '13.

Page 52.

Ques. 3. Prove if $x \equiv y \pmod{m}$ and $a_0, a_1 \ldots a_r$ are integers then
$$a_0x^r + a_1x^{r-1} + \ldots a_r = a_0y^r + a_1y^{r-1} + \ldots a_r \pmod{m}.$$

Proof: To show: $a_0x^r + a_1x^{r-1} + \ldots a_r - (a_0y^r + a_1y^{r-1} + \ldots a_r) =$ is div by m.

Now,

$$a_0x^r + a_1x^{r-1} + \ldots - a_0y^r - a_1y^{r-1} - \ldots$$
$$a_0(x^r - y^r) + a_1(x^{r-1} - y^{r-1}) + \ldots a_1(x-y). \quad -①$$

Note:

$a^2 - b^2 = (a-b)(a+b)$

$a^3 - b^3 = (a-b)(a^2 + ba + b^2)$.

As we known in general.

$$x^r - y^r = (x-y)[x^{r-1} + x^{r-2}y + x^{r-3}y^2 + \ldots]$$

$\therefore$ ① becomes

$$= (x-y)[a_0x^{r-1} \ldots + a_1] \quad - Ⓐ$$

Given; $x \equiv y \pmod{m} \longrightarrow (x-y)$ is divisible by m.

$m \mid x-y. \quad -Ⓑ.$

Ⓑ implies A is divisible by m

Hence Proved.

Ques. 4. Prove if $bd \equiv bd' \pmod p$ where p is a prime & $p \nmid b$ then $d \equiv d' \pmod p$.

Proof: Given $bd \equiv bd' \pmod p$.

$$\frac{bd - bd'}{p} = \text{int} = k.$$

$$\frac{b(d-d')}{p} = k.$$

$\because p \nmid b. \quad \therefore p \mid d-d'.$

$$\therefore \frac{d-d'}{p} = k_2.$$

By terms of congruence:

$d \equiv d' \pmod p$.

Hence Proved.

Ques. 7. (c). $57 \equiv 208 \pmod 4$

$$\frac{57-208}{4} = \frac{-151}{4} \notin \text{Integer} \quad \therefore \text{does not hold}$$

$4 \nmid 151$

(d) $531 \equiv 1236 \pmod{7561}$

difference < mod $\therefore$ will not hold.

(e). $12321 \equiv 111 \pmod 3$

$$\frac{12321 - 111}{3} = \frac{12210}{3} = 4070 \quad \therefore \text{Holds}.$$

Ques. $12,345,678,987,654,321 \equiv (0 \pmod{12,345,678}))$

Prove for each number.

Using congruence rules: $a \equiv b \pmod c$

$a' \equiv b' \pmod c \longrightarrow (a-a') \equiv (b-b') \pmod c$

Article 4.2.

Residues:

Def^n 4-2. If h and j are two integers and $h \equiv j \pmod m$, then we say j is the residue of h mod m.

→ Complete Residue System:

Def^n 4-3 The set of integers $\{r_1, r_2 \dots r_s\}$ is a complete residue system mod m if (a) $r_i \not\equiv r_j$ whenever $i \neq j$

(b) for each integer n there corresponds an r_i such that

$$n \equiv r_i \pmod m.$$

Thm^r 4-4. If s different integers $r_1, r_2 \dots r_s$ form complete residue system mod m then $s = m$.

CRS: Complete Residue System.

Cor 4-1. Let m be a positive integer then $\{0, 1, 2 \dots m-1\}$ is a CRS mod m.

eg. For $m = 5$

CRS $= \{0, 1, 2, 3, 4\}$

$n = 7$.

$7 \equiv \boxed{r_i} \pmod 5$

$= 2$.

Ex. 4-6. The sets $\{1, 2, 3\}$, $\{0, 1, 2\}$, $\{-1, 0, 1\}$ and $\{1, 5, 9\}$ are all CRS mod 3.

I. $\{1, 2, 3\}$.

(a). $1 \not\equiv 2 \pmod 3$

$2 \not\equiv 3 \pmod 3$

$1 \not\equiv 3 \pmod 3$.

} Only combo.

$a \equiv b$

$b \equiv a$

} Same

(b) $5 \equiv \boxed{}$ mod 3 Hence CRS

II. $\{0, 1, 2\}$. → Direct from Corollary CRS.

$0 \not\equiv 1 \pmod 3$

$0 \not\equiv 2 \pmod 3$

$1 \not\equiv 2 \pmod 3$.

RRS.

III. $\{-1, 0, 1\}$

(a) $-1 \not\equiv 0 \pmod 3$

$-1 \not\equiv 1 \pmod 3$

$0 \not\equiv 1 \pmod 3$

(b) $67 \equiv \boxed{} \bmod 3$

$\downarrow$

1 Hence CRS.

IV $\{1, 5, 9\}$

(a) $1 \not\equiv 9 \pmod 3$

$5 \not\equiv 9 \pmod 3$

$1 \not\equiv 9 \pmod 3$

(b) $17 \equiv \boxed{} \bmod 3$

$\downarrow$

5 Hence CRS

2nd Oct'13.

Ex 4.7. Find an integer n that satisfies

$$325n \equiv 11 \pmod 3.$$

mod = 3.

C.R.S = $\{0, 1, 2\}$

↳ Complete residue system.

$325 \not\equiv 0 \pmod 3$

$325 \equiv 1 \pmod 3$.

$11 \equiv 2 \pmod 3$

present in C.R.S.

Replacing 325 and 11 by 1 & 2 respectively

$$1n \equiv 2 \pmod 3.$$

Smallest value $n = 2$.

$\therefore \quad 1 \times 2 \equiv 2 \pmod 3$.

$\therefore \boxed{n = 2}$ ...(Answer).

Reduced Residue System (RRS).

Defn 4.4. :- The set $\{r_1, r_2 \dots r_s\}$ is called a reduced residue system mod m.

(1). G.C.D $(r_i, m) = 1$. for each i

(2) $r_i \not\equiv r_j \pmod m$ whenever $i \neq j$

(3) for each integer n there corresponds an r_i such that

$$n \equiv r_i \pmod m.$$

Ex. mod = 12 mod 12

C.R.S = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11}

R.R.S = {1, 5, 7, 11}

All numbers relatively prime to 12 except 0

$\exists$ an n where suppose $n = 17$ gcd(17, 12) = 1.

$17 \equiv \boxed{} \bmod (12)$.

5

Note:- If modulus is prime number say 'p'. then {1, 2, 3 ...., p−1} forms the R.R.S.

Euler Function $\phi(m)$.

$\phi(m)$ denotes the no. of +ve integers less than or equal to m that are relatively prime to m.

Thm^r 4.5: If s integers $r_1, r_2 \ldots r_s$ form a RRS mod m then $\phi(m) = s$.

Ex. Ques. 1 Which of the following is are C.RS mod 11?

a) 0, 1, 2, 4, 8, 16, 32, 64, 128, 256, 512.

Step ①.

$0 \not\equiv 1 \pmod{11}$ $1 \not\equiv 2$ Repeat for r_i & r_j. $r_i \not\equiv r_j$

$0 \not\equiv 2$ —"— $1 \not\equiv 4$

$0 \not\equiv 4$ " $1 \not\equiv 8$

$0 \not\equiv 8$ " $1 \not\equiv 16$

$0 \not\equiv 16$ " $1 \not\equiv 32$

$0 \not\equiv 32$ " $1 \not\equiv 64$

$0 \not\equiv 64$ " $1 \not\equiv 128$

$0 \not\equiv 128$ " $1 \not\equiv 256$

$0 \not\equiv 256$ " $1 \not\equiv 512$

$0 \not\equiv (512)$ "

step ⑤. $n \equiv ? \pmod{11}$

Ques. 2.

(a). 1, 5, 25, 125, 625, 3125 mod 18. Check for R.R.S.

① ∵ All numbers end in 5 they are relatively prime to 18 and hence not congruent & are relatively prime.

② $1 \not\equiv 5 \pmod{18}$ $5 \not\equiv 25 \pmod{18}$ $25 \not\equiv 125 \pmod{18}$ $125 \not\equiv 625 \pmod{18}$

$1 \not\equiv 25$ " $5 \not\equiv 125$ $25 \not\equiv 625$ $\not\equiv 3125$

$\not\equiv 125$ " $5 \not\equiv 625$ $25 \not\equiv 3125$

$\not\equiv 625$ " $5 \not\equiv 3125$

$\not\equiv 3125$ " $625 \not\equiv 3125 \pmod{18}$

③. $n \equiv \underbrace{?}_{1} \pmod{18}$ ... True.

From RRS

3rd Oct '13.

Modified Farro Shuffle

Even number of cards.

Inshuffle - Left Hand Outshuffle - Right Hand.

Using Fermits Theorem.

Considering 6 cards being shuffled: 1st SHUFFLE 2ND SHUFFLE 3rd SHUFFLE.

1st SHUFFLE: L {1, 2, 3} {4, 5, 6} R

2ND SHUFFLE: L {4, 1, 5} {2, 6, 3} R

3rd SHUFFLE: L {2, 4, 6} {1, 3, 5} R

Original	After 1st shuffle	After 2nd shuffle	After 3rd shuffle
1	4	2	1
2	1	4	2
3	5	6	3
4	2	1	4
5	6	3	5
6	3	5	6

Modified Farro Shuffle.

Back to original in 3 Shuffle.

Fermits Thm^n: No. of shuffles reqd to get back pack to original position

$$\boxed{2^n \equiv 1 \pmod{m+1}} \quad \ldots \text{Thm}^n \text{ Eq}^n$$

Date
Page

Ex. How many shuffles are required to return a pack of cards of 52 to their original position

By Fermit's eqn: $2^n \equiv 1 \pmod{m+1}$

52.

$$2^n \equiv 1 \pmod{53}$$

$$2^{\phi(m)} \equiv 1 \pmod{\cancel{53}\ m}$$

If m is prime $\phi(m) = m-1$

$$2^{m-1} \equiv 1 \pmod{m}$$

$\because m = 53$

$\therefore n = m-1 = 52$ shuffles required ..(Ans).

$\Rightarrow \quad 2^{52} \equiv 1 \pmod{53}$

Ex. How many modified perfect faro shuffles needed to return in a deck of 6 cards, 8 cards & 12 cards.

1. $2^n \equiv 1 \pmod{7}$

$n = m-1 = 6$ shuffles. (3 shuffles).

2. $2^n \equiv 1 \pmod{9}$

$n = 6$ shuffles.

$2^6 \equiv 1 \pmod{9}$.

$\hookrightarrow 64$

3. $2^n \equiv 1 \pmod{13}$

$n = m-1 = 12$ shuffles

classmate
Date ____
Page ____

Solving Congruences.
Chapter 5.

$x \equiv 3 \pmod 2$
$x \equiv 5 \pmod 3$
$x \equiv 7 \pmod 2$

$ax \equiv c \pmod b$

Note : If n satisfies $an \equiv b \pmod c$ then $n+kc$ will also satisfy congruence.

Proof. Given n satisfies

$$an \equiv b \pmod c.$$

$$a(n+kc) \equiv an + akc \equiv \underbrace{an \pmod c}_{\text{Congruent}} \equiv b \pmod c.$$

Ques. $5n \equiv 3 \pmod 8$

For $n=-1$. Congruence holds.

$\equiv -17, -9, -1, 7, 15, \ldots$

$n = -1$

$-1 + k8 \rightarrow$ For diff^n values of k diff^n solutions.

Thm^n 5.1 If $d = g.c.d(a,c)$ then the congruence $an \equiv b \pmod c$ has no solution $d \nmid b$. if $d \mid b$ then it has 'd' mutually in congruent soln^n.

Ex $15x \equiv 9 \pmod{12}$.

$g.c.d(15,12) = 3 \mid 9 \longrightarrow$ Hence soln exist.

3 incongruent soln will exist.

$x_0 = 3$.. initial soln.

Rest of soln $x = x_0 + \frac{c}{d}t$ ... General Soln.

For incongruent soln start with $t = \underbrace{0, 1, 2}_{d}$.

$$x = 3 + \frac{12}{3}t = 3 + 4t =$$

$t=0$	3	
$t=1$	7	$\rightarrow$ Incongruent.
$t=2$	11	
$t=3$	15	
$t=4$	19	
$t=5$	23	

mutually incongruent

Solving: $ax \equiv b \pmod{c}$.

$$\frac{ax-b}{c} = k$$

$$ax-b = ck.$$

$$ax-ck = b \quad \text{... Diophantine eq}^n.$$

$$ax+by = c$$

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

Solving above eq^n:

$$x = x_0 + \frac{c}{d}t.$$

for behind eg: $15x \equiv 9 \pmod{12}$

$$\frac{15x-9}{12} = k.$$

$$15x-9 = 12k.$$

$$15x-12k = 9$$

Solve.

22nd Oct'13.

~~Q.2~~

(c). $\cancel{27x} \equiv \cancel{+} \pmod{\cancel{51}}$

~~g.c.d~~ $(\cancel{27,51})$

#. $d = g.c.d\,(a,c)$

$an \equiv b \pmod{c}$

if $g.c.d\,(a,c) = d$ & $d \mid b$ then there are d no. of incongruent soln.

if $d \nmid b \rightarrow$ no solution.

$ax \equiv b \pmod{c}$

$$\frac{ax-b}{c} = k \qquad k = k_0 + \frac{a}{d}t$$

$$ax - ck = b \qquad x = x_0 + \frac{c}{d}t$$

Q1. $7x \equiv 5 \pmod{11}$

$g.c.d(7,11) = 1 = d$

$b = 5 \quad d \mid b = 1 \mid 5 \quad \therefore$ Solution exist

$\frac{7x-5}{11} = y \rightarrow 7x - 11y = 5.$

$11 = 7 \times 1 + 4$

$7 = 4 \times 1 + 3$

$4 = 3 \times 1 + 1$

$3 = 1 \times 3 + 0$

$\hookrightarrow$ G.C.D

$\xrightarrow{\text{Reverse}}$

$1 = 4 - 3 \times 1$

$= 4 - 1(7 - 1 \times 4)$

$= 2 \times 4 - 1 \times 7$

$1 = 2 \times 11 - 3 \times 7 \rightarrow \times 5$

$x = -3 \quad y = -2$

$\downarrow \times 5$

$x = -15 \quad y = -10.$

$x = x_0 + \frac{c}{d} t = -15 + \frac{11}{1} t.$

$t = 2 \quad x = 7 \quad y = \frac{7 \times 7 - 5}{11} = 4.$ Positive one soln.

Q. $8x \equiv 10 \pmod{30}$

$g.c.d(8,30) = 2$

$b = 10 \quad d \mid b =$ 2 incongruent soln.

$\frac{8x-10}{30} = y \longrightarrow 8x - 30y = 10$

$30 = 8 \times 3 + 6$

$8 = 6 \times 1 + 2$

$6 = 2 \times 3 + 0$

$\xrightarrow{\text{Reverse}}$

$2 = 8 - 6 \times 1$

$= 8 - 1 \times (30 - 3 \times 8)$

$2 = 4 \times 8 - 1 \times 30 \ (\times 5)$

$10 = 20 \times 8 - 5 \times 30$

$x_0 = 20 \quad y_0 = 5$

$\therefore \quad x = 20 + 15t$

$t = 0 \quad x = 20$

$t = 1 \quad x = 35 \rightarrow y = 15$ & $15 + 30^{5}$ ... Incongruent soln.

Q.2. (c). $27x \equiv 1 \pmod{51}$

$g.c.d(27,51) = 3$ $b = 1$ $d \nmid b$ No solution

(f) $81x \equiv 57 \pmod{117}$

$g.c.d(81, 117) = 3$

$b = 57$ $d \nmid b$ No solution.

INVERSE.

-1 is additive inverse of 1 ... Additive inverse always 0

$1/2$ is multi. inverse of 2. ... Multiplicative —"— 1.

Defination of inverse.

A solution n of congruence

$$an \equiv b \pmod{c} \quad —①$$

is unique mod c if any solution n of ① is congruent to n mod c.

If $a\bar{a} \equiv 1 \bmod c$ we say $\bar{a}$ is inverse of a mod c.

Cor. 5.1. If $g.c.d(a,c) = 1$ then 'a' has an inverse and it is unique for mod c.

e.g. $25 \equiv 1 \pmod{8}$

$5 \times 5 \equiv 1 \pmod{8}$

$5 \equiv -3 \pmod{8}$

$5 \equiv -11 \pmod{8}$

All the nos which are congruent to the inverse are also congruent to your solution.

Q.3. Find $\bar{a}$, the inverse of a mod c

(a) $a = 2 \; ; c = 5$

$a\tilde{a} \equiv 1 \pmod 5$

$2\tilde{a} \equiv 1 \pmod 5$

$\downarrow$

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

$3 \equiv -2 \pmod 5$

$3 \equiv 8 \pmod 5$.

(b) $a = 7 \; ; c = 9$

$a\tilde{a} = 1 \pmod c$

$7\bar{a} \equiv 1 \pmod 9$

$\tilde{a} = 4$

$7 \times 4 \equiv 1 \pmod 9$

$4 \equiv -5 \pmod 9$

23rd Oct '13

Thm 5.2. Eulers Theorem.

If g.c.d $(a,m)=1$ then $a^{\phi(m)} \equiv 1 \pmod m$.

Proof: Let $\{r_1, r_2 \dots r_{\phi(m)}\}$ – be RRS (mod m).

If we multiply by 'a'

$\{ar_1, ar_2 \dots ar_{\phi(m)}\}$ ... Relatively prime to m by def^n of RRS.

$\downarrow$

Incongruent to each other.

$ar_i \not\equiv ar_j \pmod m$.

We can pair each ar_i with some r_j from RRS such that

$$ar_i \equiv r_j \pmod m$$

Then;

$$ar_1 ar_2 \dots ar_{\phi(m)} \equiv r_1 r_2 \dots r_j \, r_{\phi(m)} \pmod m.$$

$$a^{\phi(m)}(r_1 r_2 \dots r_{\phi(m)}) \equiv r_1 r_2 \dots r_{\phi(m)} \pmod m.$$

$\therefore$ By Cancellation Law:

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

Hence Proved.

Q.1. If $m = 13$ then a RRS(mod m) is $(1,2,3,4,5,6,7,8,9,\overset{10}{},11,12)$

Let $a = 3$. Exhibit the pairing of each of the preceding numbers with the numbers in the RRS as in Thm^n.

a.RR.S = $\{3,6,9,12,15,18,21,24,27,30,33,36\}$.

Pair 1. $3 \equiv 3 \pmod{13}$	5. $15 \equiv 2 \pmod{13}$	9. $27 \equiv 1 \pmod{13}$
2. $6 \equiv 6 \pmod{13}$	6. $18 \equiv 5 \pmod{13}$	10. $30 \equiv 4 \pmod{13}$
3. $9 \equiv 9 \pmod{13}$	7. $21 \equiv 8 \pmod{13}$	11. $33 \equiv 7 \pmod{13}$
4. $12 \equiv 12 \pmod{13}$	8. $24 \equiv 11 \pmod{13}$	12. $36 \equiv 10 \pmod{13}$

(None of it are repeating)

27th Oct'13.

Fermit's Little Theorem.

Cor. 5.2. If p is a prime then $n^p \equiv n \pmod p$.

Proof.

(i) Let $p \mid n$

$\rightarrow p \mid n^p$

$\rightarrow p \mid n^p - n$ (Also true).

$\Rightarrow \frac{n^p - n}{p} = k. \longrightarrow n^p \equiv n \pmod p$ .. Proved.

(ii) Let $p \nmid n$

$\rightarrow g.c.d(p, n) = 1$.

By ~~the~~ eulers thm^r: $a \rightarrow n$

$m \rightarrow p$.

$\phi(p) = p-1$ (Prime no)

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

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

mul by n.

$n^p \equiv n \pmod p$ ... Proved.

Wilson's Theorem:

Cor. 5.3. The congruence

$(m-1)! \equiv -1 \pmod m$ holds iff m is prime.

Note :- If $1, 2, 3 \ldots, m-1$ is a RRS

$1 \rightarrow 1$, $m-1 \rightarrow 1$, $\boxed{m-2}$

Then all elements from $2, 3 \ldots m-2$ can paired with their inverse.

classmate
Date
Page

Q.2. If $m=11$, exhibit the pairing for each of the nos in RRS with its inverse (mod m)

RRS = $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

$\downarrow$ L $\qquad\qquad$ $\downarrow$ L

(1) $2 \times (6) \equiv 1 \pmod{11}$

(2) $3 \times (4) \equiv 1 \pmod{11}$

(3) $5 \times (9) \equiv 1 \pmod{11}$

(4) $7 \times (8) \equiv 1 \pmod{11}$

All inverses exist.

Q.3. Prove that $1+a+a^2+\dots a^{\phi(m)-1} \equiv 0 \pmod m$
if $g.c.d(a,m) = g.c.d(a-1,m) = 1$.

If $(a-1)[1+a+a^2+\dots+a^{\phi(m)-1}]$

$a^{\phi(m)-1}$

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

$= a^{\phi(m)} - 1.$ —— (1)

From euler Thr^m.

$a^{\phi(m)} \equiv 1 \pmod m \quad \because g.c.d(a,m) = 1.$

$\therefore$ (1) $a^{\phi(m)} - 1$ is divisible by m.

$\Rightarrow$ L.H.S is also div. by m.

$\downarrow$.

$\because g.c.d(a-1,m) = 1 \quad a-1 \nmid m$

$\therefore$ m divisles $(1+a+a^2+\dots+a^{\phi(m)-1})$.

$\therefore$ By congruence def^n

$(1+a+a^2+\dots a^{\phi(m)-1}) \equiv 0 \pmod m$

Hence Proved.

classmate
Date
Page

Proof: If $r_1, r_2 \dots r_{\phi(m)}$ is a RRS mod m and m is odd then.
$r_1 + r_2 + \dots r_{\phi(m)} \equiv 0 \pmod m$.

Considering m to be odd prime. then
$1, 2 \dots m-1$ is RRS.

Adding all RRS values.

$$1+2+\dots(m-1) = \frac{m(m-1)}{2}$$

as $\frac{(m-1)m}{2}$ is divisible by m. congruent to

$\therefore r_1 + r_2 + \dots + r_{\phi(m)}$ is ~~RRS~~ mod m.

$r_1 + r_2 + \dots r_{\phi(m)} \equiv 0 \pmod m$

Hence Proved.

Q.5. What is the remainder when 41^{75} is divided by 3?

Soln. Representation of $75 = 37 \times 2 + 1$.

Basic

$$41^{(75)} = 41^{37 \times 2 + 1}$$
$$= 41^{37 \times 2} \times 41.$$

as $41^2 \equiv 1 \pmod 3$

$$= (41^2)^{37} \cdot 41.$$
$$\equiv (1)^{37} \cdot 41$$
$$\equiv 41 \equiv 2 \pmod 3$$

Remainder.

Q.6. Remainder when 473^{38} is divided by 5.

$$38 \equiv \cancel{12 \times 3}^{\,4\times 9} + 2.$$

$$(473)^{38} = (473)^{\cancel{12\times 3}\,4\times 9}(473)^{2}.$$

$$(473)^{\cancel{3}\,=4} \equiv \cancel{3}\,1 \bmod (5)$$

(4

$$= ((1)^4)^9 (473)^2$$

$$(473)^2 \equiv 4 \pmod 9.$$

remainder.

Q. (1) $3^8 \pmod{13}$

(2) $34 \times 17 \pmod{29}$

(1). $8 = 4 \times 2.$

$$(3)^{4\times 2}.$$

$$((3^4))^2.$$

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

$$(3)^2$$

$$= 9$$

Remainder

(2) $34 \times 17 \pmod{29}$.

$$34 \equiv 5 \pmod{29}$$

$$17 \equiv 17 \pmod{29}$$

$$17 \times 5 = 85 \equiv 26 \bmod 29$$

26

Remainder.

1. 29th Nov.

Q.7. Prove if $A = a_0 10^n + a_1 10^{n-1} + \ldots a_n$

$S = a_0 + \ldots + a_n$

Then $A \equiv S \pmod 9$

→ $A - S = a_0 10^n + a_1 10^{n-1} + \ldots + a_n - (a_0 + a_1 \ldots + a_n)$

$= a_0(10^n - 1) + a_1(10^{n-1} - 1)$

$\because 10 - 1 = 9 \rightarrow 10 \equiv 1 \pmod 9$

Using the result if $a \equiv b \pmod m$

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

$10^n \equiv 1^n \pmod 9$ also $10^{n-1} \equiv 1^{n-1} \pmod m$

So $A - S$ will be divisible by 9 as each term has $(10-1)$ as a multiple

Remainder.

Q. 16. 3^{56} is divided by 7.

As it is divided by prime, then Euler's thm^n can be applied.

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

$3^6 \equiv 1 \pmod 7$

$3^{56} = (3^6)^9 \cdot 3^2 = 1 \cdot 3^2 \equiv 2 \pmod 7$.

Remainder.

Chinese Remainder Thm^r

Q. $x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 3 \pmod 7$

Find initial solution $\qquad M = 3 \cdot 5 \cdot 7 = 105.$

$c_1 = 2 \;;\; c_2 = 3 \;;\; c_3 = 2.$

$n_1 = 35 \qquad n_2 = 21 \qquad n_3 = 15.$

$7 \times 5 \qquad 3 \times 7 \qquad 3 \times 5$

$\overline{n_1} = \qquad \overline{n_2} = \qquad \overline{n_3} =$

$n_1 \cdot \overline{n_1} \equiv 1 \pmod 3 \qquad n_2 \cdot \overline{n_2} \equiv 1 \pmod 5 \qquad n_3 \overline{n_3} \equiv 1 \pmod 7$

$85 \overline{n_1} \equiv 1 \pmod 3 \qquad 21 \cdot \overline{n_2} \equiv 1 \pmod 5 \qquad 15 \cdot \overline{n_3} \equiv 1 \pmod 7$

$\overline{n_1} = 2 \qquad \overline{n_2} = 1 \qquad \overline{n_3} = 1$

$x_0 = c_1 \cdot n_1 \cdot \overline{n_1} + c_2 n_2 \overline{n_2} + c_3 n_3 \overline{n_3}$

$= 2 \times 35 \times 2 + 21 \times 3 \times 1 + 2 \times 15$

$= 233$

$x_0 = 233$

$\equiv 233 \pmod M \qquad 105 \times 2 + 23$

$\equiv 233 \pmod{105} \longrightarrow \equiv \underline{23} \pmod{105}$

$\downarrow$

x

Q. $2x \equiv 5 \pmod{35}$

Composite number

System

$35 = 7 \times 5.$

$2x \equiv 5 \pmod 5$

$2x \equiv 5 \pmod 7$

$c_1 = 5 \qquad c_2 = 6.$

$n_1 = 7 \qquad n_2 = 5.$

$n_1 \cdot \overline{n_1} = 1 \pmod 5 \qquad 5 \cdot \overline{n_2} = 1 \pmod 7$

$7 \cdot \overline{n_1} \equiv 1 \pmod 5 \qquad \overline{n_2} = 3$

$\overline{n_1} = 8 \qquad x_0 = 5.7.8 + 6.5.3$

Chinese Remainder Theorem.

Thm 5.4: Suppose m_1, m_2, m_3 are integers all relatively prime to each other, let M be $M_1 \dots M_s$ and suppose $a_1 . a_2 \dots a_s$ are integers such that $g.c.d(a_i, m_i) = 1$ for each i then $a_1 x \equiv b_1 \pmod{m_1}$, $a_2 x \equiv b_2 \pmod{m_2} \dots$
$a_s x \equiv b_s \pmod{m_s}$ have a simultaneous solution that is unique (mod m).

Ques: Solve $3x \equiv 11 \pmod{2275}$

$2275 = 5^2 \times 7 \times 13$

$$\begin{cases} 3x \equiv 11 \pmod{25} \\ 3x \equiv 11 \pmod{7} \\ 3x \equiv 11 \pmod{13}. \end{cases}$$

Initial Soln.

$c_1 = 12$; $c_2 = 6$; $c_3 = 8$

$M = 2275$.

$n_1 = 7 \times 13 = 91$; $n_2 = 25 \times 13 = 325$; $n_3 = 25 \times 7 = 175$.

↓ Inverse ↓ Inverse ↓ Inverse

$91 \bar{n_1} \equiv 1 \pmod{25}$; $325 \bar{n_2} \equiv 1 \pmod{7}$; $175 \bar{n_3} \equiv 1 \pmod{13}$

$\bar{n_1} = 11$; $\bar{n_2} = 5$; $\bar{n_3} = 11$

$$x_0 = \underbrace{12}_{c_1} \times \underbrace{91}_{n_1} \times \underbrace{11}_{\bar{n_1}} + \underbrace{6}_{c_2} \times \underbrace{325}_{n_2} \times \underbrace{5}_{\bar{n_2}} + \underbrace{8}_{c_3} \times \underbrace{175}_{n_3} \times \underbrace{11}_{\bar{n_3}}$$

$= 37162 \pmod{2275}$

$\equiv \underline{762} \pmod{2275}$

x

30th Oct '13.

Application of Congruences

① Codes for days:

Sat	0
Sun	1
Mon	2
Tue	3
Wed	4
Thurs	5
Fri	6

② Codes for ~~years:~~ months.

1 4 4	0 2 5	0 3 6	1 4 6
J F M	A M J	J A S	O N D
12^2	5^2	6^2	$12^2 + 2^2$.

③ Code for years.

2000	Sub 1.
1900	nothing
1800	add 2
1700	add 4
1600	add 6
1500	if date is from Oct 15th 1582 to Dec 31st 1599 – Add 0 (nothing)
	~~else~~ – ~~Add 8~~

For dates before Oct 15th, 1582, the first two digits of the year is subtracted from 18 → Correction.

Geogrian Calendar.

Change from Eulian (Leap yr. was not considered).

Ⓕ For the year:

$$y + \left[\frac{y}{4}\right] \rightarrow \text{integer value.}$$

last 2 digits

classmate
Date
Page

Ex. 20th Aug 1993.

① $93 + \left[\frac{93}{4}\right] = 93 + 23 = 116 \equiv \underline{\underline{4}} \pmod 7$

year code = 4.

② $20 + 3 + 4 = 27 \equiv \underline{\underline{6}} \,(\text{mod}\,(7))$

(No correction)

Friday. (Born on).

Ex. 30th Oct 2013.

① $13 + \left[\frac{13}{4}\right] = 13 + 3 = 16 \equiv \underline{\underline{2}} \pmod 7$

yr code

② $30 + 1 + 2(-1) = 32 \equiv \underline{\underline{4}} \pmod 7$

Correction. A Wednesday.

Ex. Henry VIII th married Anne Bolian in secret ceremony on 25th Jan 1533 on what day of week..?

25th Jan 1533

① $33 + \left[\frac{33}{4}\right] = 33 + 8 = 41 \equiv 6 \pmod 7$

② $25 + 6 + 1 + 3 = \cancel{29}\ 35 \equiv \underline{\underline{\cancel{2}\ 0}} \pmod 7$

Correction = (18 - 15)

~~Sunday~~ Saturday

Ex. Battle of Hasting was fought on 14th Oct 1066. Day ?

(1). $66 + \left(\frac{66}{4}\right) = 66 + 16 = 82 \equiv 5 \pmod 7$

(2) $5 + 1 + 14 + (18-10) = 20+8 = 28 \equiv 0 \pmod 7$.

Saturday.

H.W Ex. Prove that any day in the 20^{th} century begⁿ with March 1^{st} 1900 falls on same day of the week 28yrs.

31st Oct'13.

Ex. Find the residue when 12! is divided by 13

R.R.S = {1, 2, 3 .... 12}

$a\tilde{a} \equiv 1 \pmod m$

$2 \times 7 \equiv 1 \pmod{13}$

$3 \times \overset{(9)}{4} \equiv 1 \pmod{13}$

$5 \times 8 \equiv 1 \pmod{13}$

$6 \times 11 \equiv 1 \pmod{13}$

$10 \times 4 \equiv 1 \pmod{13}$

Ex Show that 47 divides $5^{23}+1$

$5^4 \equiv 14 \pmod{47}$

$5^8 \equiv 14^2 \pmod{47}$

$14^2 \equiv 8 \pmod{47}$

$\therefore 5^8 \equiv 8 \pmod{47}$

$5^{16} \equiv 8^2 \pmod{47}$

$8^2 \equiv 17 \pmod{47}$

$\therefore 5^{16} \equiv 17 \pmod{47}$

classmate

Date

Page

$5^{24} = 5^{16+8} = 5^{16} \cdot 5^{8} = 17 \cdot 8 \equiv 42 \pmod{47}$

$42 \equiv -5 \pmod{47}$

Replace 42 by -5

to get in terms of 5

$5^{24} \equiv -5 \pmod{47}$

$5^{23} \equiv -1 \pmod{47}$

$5^{23} + 1 \equiv 0 \pmod{47}$

$\therefore$ $5^{23} + 1$ is divisible by 47.

H.W

Q. Find out whether $7 \times 30^{20} + 6$ is divisible by 41 or not.

Method of solving congruence.

→ Method 1.

Solve $42x \equiv 90 \pmod{156}$

$$\frac{42x - 90}{156}$$

divide Numr & Denr by 6

$$\frac{7x - 15}{26} \rightarrow 7x \equiv 15 \pmod{26}$$

Replace 7 by its residue 33 (mod 26)

$33x \equiv 15 \pmod{26}$

divide by 3 as G.C.D (3, 26) = 1

$11x \equiv 5 \pmod{26}$

As $11x \equiv -15 \pmod{26}$

By replacing.

$-15x \equiv 5 \pmod{26}$

$-3x \equiv 1 \pmod{26}$

$-3x \equiv 27 \pmod{26}$

$-x \equiv 9 \pmod{26}$

$x \equiv -9 \pmod{26}$

classmate

Date

Page

→ Method 2.

Using Multiple Technique.

$179x \equiv 283 \pmod{313}$

$\frac{313}{179}$ → Closet integer is 2

Multiply both sides by 2.

$358 - 313 = 45$

$358x \equiv 566 \pmod{313}$

$45x \equiv 253 \pmod{313}$

$\frac{313}{45}$ → Closet integer is 7.

Multiply both sides by 7.

$315x \equiv 1771 \pmod{313}$

$315 - 313 = 2$

$2x \equiv 206 \pmod{313}$ ∴ Cancellation Law.

$x \equiv 103 \pmod{313}$

6th Nov '13.

Chapter. 6. Arithmatic Function.

$\phi(n)$ ... Euler's fun^c
$d(n)$ ... All divisors of n (No. of divisor).
$\sigma(n)$ ... Sum of all divisors
$\mu(n)$ ... Mobuis func

1. $\phi(n)$ - Euler's fun^c

For prime number $n = p$ then ★ $\phi(p) = p - 1$.

★ $\phi(p^n) = p^n - p^{n-1} = p^n(1 - 1/p)$

n is some integer.

$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots$ (Multiplicative fun^c $\phi(n)$).

$\phi(n) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdots$

From formula. $p_1^{\alpha_1}(1 - 1/p_1)$

n	$\phi(n)$.		
1	1		
2	1	$\phi(2^1) = 2^1 - 2^{1-1} = 1$.	$(p-1)$
3	2	$\phi(3) = 3^1 - 3^0 = 2$.	$(p-1)$
4	2	$\phi(4) = \phi(2^2) = 2^2 - 2^{2-1} = 4 - 2 = 2$	
5	4	$\phi(5) = \phi(5^1) = 5^1 - 5^0 = 4$	$(p-1)$
6	2	$\phi(6) = \phi(2) \cdot \phi(3)$	(1
7	6		$(p-1)$
8	4	$\phi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$	
9	6	$\phi(3^2) = 3^2 - 3 = 9 - 3 = 6$	
10	4	$\phi(5)\phi(2)$	
11	10		
12	4	$\phi(2^2)\phi(3)$	
13	12		
14	6	$\phi(2)\phi(7)$	

n	$\phi(n)$	
15	8	$\phi(5)\phi(3)$
16	8	$\phi(2^4) = 2^4 - 2^3 = 16 - 8 = 8$
17	16	$p-1$
18	6	$\phi(3^2)\underset{1}{\phi(2)}$
19	18	
20	8	$\underset{2}{\phi(2^2)}\underset{4}{\phi(5)}$

Ques. Show that

$$1 + \phi(p) + \phi(p^2) + \dots \phi(p^n) = p^n$$

From L.H.S

$$\cancel{1} \cancel{+} (\cancel{p} \cancel{-1}) + (\cancel{p^2} - \cancel{p}) + (p^3 - \cancel{p^2}) \dots + p^n - p^{n-1}$$

All terms cancel out except

p^n = RHS

Hence Proved.

Thm^r 6-1. Show. Perfect number.

$$\sum_{d|n} \phi(d) = n$$

Let $n=6$

$d = 1, 2, 3, 6$

$$\sum \phi(d) = \phi(1) + \phi(2) + \phi(3) + \phi(6)$$
$$= 1 + 1 + 2 + 2 = 6 = n.$$

6th

Defn 6.1. Mobius Function ($\mu(n)$).

$$\mu(n) := \begin{cases} 1 & , \ n = 1 \\ 0 & . \ p^2 \mid n \\ (-1)^r & , \ \text{if } n = p_1 . p_2 \dots p_r \text{ where } p_i \text{ are distant prime.} \end{cases}$$

will only take
0, 1, −1

n	$\mu(n)$
1	1
2	−1
3	−1
4	0
5	−1
6	1
7	−1
8	0
9	0
10	1
11	−1
12	0

classmate

Date ______
Page ______

Thm^r 6.2. $\underset{A}{\phi(n)} = \underset{B}{\sum_{d|n} \mu(d) \frac{n}{d}} = \underset{C}{n \prod_{p|n} \left(1 - \frac{1}{p}\right)}$

A

$n = 10$ $\quad \phi(n) = 4$ (L.H.S).

B $\sum_{d|n} \mu(d) \frac{n}{d}$ $\qquad d = 1, 2, 5, 10.$

All divisors of n.

$= \mu(1) \cdot \frac{10}{1} + \mu(2) \cdot \frac{10}{2} + \mu(5) \frac{10}{5} + \mu(10) \cdot \frac{10}{10}$

$= 1 \cdot 10 + (-1) \cdot 5 + (-1) 2 + 1 \cdot 1$

$= 10 - 5 - 2 + 1$

$= 4.$

C

$n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)$ $\qquad p|n = 2, 5.$

$= n \left[1 - \frac{1}{2}\right] \cdot \left[1 - \frac{1}{5}\right]$

$= n \left[\frac{1}{2}\right] \left[\frac{4}{5}\right]$

$= 10 \cdot \frac{1}{2} \cdot \frac{4}{5}$

$= 4$

A = B = C

Q. $\phi(120)$.

$$\begin{array}{r|l} 2 & 120 \\ 2 & 60 \\ 2 & 30 \\ 3 & 15 \\ 5 & 5 \\ & 1 \end{array}$$

$\phi(2^3)(\phi(3)\phi(5)$

$= (2^3-2^2)(3^1-3^0)(5^1-5^0)$

$= 4 . 2 . 4$

$= \underline{\underline{32}}.$

10th Nov'13.

Ques. 6. Find all integers such that $\phi(n)=12$.

$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots$

$\phi(n) = \phi(p_1^{\alpha_1} p_2^{\alpha_2} \dots)$

$= \phi(p_1^{\alpha_1}) . \phi(p_2^{\alpha_2}) \dots$

RHS = $\underline{12}$.

↓

$\phi(p_1^{\alpha_1}) \dots$ factors of 12.

$12 = 1 \times 12$

$= 4 \times 3$

$4 = \phi(p_1^{\alpha_1})$

$3 = \phi(p_2^{\alpha_2}) \longrightarrow$ Not possible

ϕ values always even

Hence Assumption wrong.

$= 1 \times 12$

$\phi^{\alpha} \quad \phi^{\alpha}$.

↓ ↓

$1 . 13 = 13$ ... Answer

$\phi(13) = \underline{\underline{12}}$.

Page 81. Goldbach Conjecture:

Ques 7. Every even number greater than 2 is sum of 2 prime.

For any even number 2n such there exists integer prime q, r such that $\phi(q) + \phi(r) = 2n$

2nd Conjecture. Does Goldbach conjecture implies to 2nd.

Goldback Conjecture:

$$2n+2 = q + r \quad — ③ \quad q, r \text{ prime.}$$

As we know q, r prime,

$$\phi(q) = q-1$$
$$\phi(r) = r-1.$$
$$\rightarrow q = \phi(q) + 1 \quad —①$$
$$r = \phi(r) + 1 \quad —②$$

Putting ① & ② in ③.

$$2n + \cancel{2} = \phi(q) + \cancel{1} + \phi(r) + \cancel{1}$$
$$2n = \phi(q) + \phi(r)$$

Hence Proved.

Carmicheal's conjecture

Ques. 12. For each integer n ∃ a diffⁿ number/integer m such that

$$\phi(n) = \phi(m). \qquad n \neq m$$

each $\{\phi(1) = \phi(2)\}$

(a) Prove it for n congruent to 2 mod 4.

$$n \equiv 2 \pmod 4$$
$$\frac{n-2}{4} = r$$
$$n = 4r+2$$
$$\phi(n) = \phi(\underbrace{\cancel{4n+r}}_{4r+2}) = \phi(2.(2r+1))$$
$$= \phi(2) . \phi(2r+1)$$
$$\phi(n) = 1. \phi(2r+1)$$

Proves ϕ is same for n and 2r+1 is same

Ques. 13 Find ∞ly many integers n for which 10 divides $\phi(n) \rightarrow 10 \mid \phi(n)$

Solution Using $\phi(11) = 10$

Taking $\phi(11^n) = 11^n - 11^{n-1}$

$= 11^{n-1}(11-1)$

$= 11^{n-1}(10) \longrightarrow$ divisible by 10

$\checkmark$. $\longrightarrow$ Solution.

$n = 1 2 3 \dots \infty$.

Ques. 14. Prove that there are infinitely many integer n for which $\phi(n)$ is a perfect square.

Solution Let the number 2^{2n+1}

$\phi(2^{2n+1}) = \cancel{\phi 2}\ 2^{2n+1} - 2^{2n}$

$= 2^{2n}(2-1)$

$= 2^{2n}$

$= (2^n)^2 \longrightarrow$ Perfect square.

H.W. $\phi 19$, $\phi(49)$, $\phi(243)$, $\phi(1024)$.

classmate
Date
Page

Article 6.2.

$d(n)$ ... no. of divisors in n

$\sigma(n)$ ... Σ of divisors of n.

For $n=p$ $\quad d(n) = 2 \quad \ldots (1, p)$

$\sigma(p) = 1+p$

If $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_r^{\alpha_r}$

$d(n) = (\alpha_1+1)(\alpha_2+1)\ldots(\alpha_r+1)$

$$\sigma(n) = \underbrace{\frac{p_1^{\alpha_1+1}-1}{p_1-1}}_{\text{Sum of a G.P.}} \times \frac{p_2^{\alpha_2+1}-1}{p_2-1} \times \ldots \frac{p_r^{\alpha_r+1}-1}{p_r-1}$$

Direct method

$$\begin{array}{r|l} 2 & 210 \\ 3 & 105 \\ 5 & 35 \\ 7 & 7 \\ & 1 \end{array}$$

$3 \times 4 \times 6 \times 8 = 12 \times 48 = \underline{\underline{576}}$

Ques. 10. $\sigma(210) = \phi(2) \cdot \phi(3) \cdot \phi(5)\,\phi(7)$

$$= \frac{2^2-1}{2-1} \times \frac{3^2-1}{3-1} \times \frac{5^2-1}{5-1} \times \frac{7^2-1}{7-1}$$

$$= \frac{4-1}{1} \times \frac{9-1}{2} \times \frac{25-1}{4} \times \frac{49-1}{6}$$

$$= \frac{3 \times \cancel{8} \times \cancel{24}^{\,4} \times 48}{1 \times \cancel{2} \times \cancel{4} \times \cancel{6}} = 12 \times 48 = \underline{\underline{576}}$$

$$\sigma(999) = \sigma(3^3) \times \sigma(37) = \sigma(3^3 \times 37) \quad \frac{37^2-1}{37-1}$$

38.

$$= \frac{3^4-1}{3-1} \times \cancel{38}\; \frac{37^2-1}{37-1} \quad \underline{\underline{38}}$$

$$= \overset{3}{40} \times 38$$

$$= \underline{\underline{1520}}$$

$$\begin{array}{r|l} 7 & 63 \\ 3 & 9 \\ 3 & 3 \\ & 1 \end{array}$$

Q. $d(63) = \cancel{(3^2 \cdot 7)} = d(3^2 \times 7) = (2+1).2 = 6$

$d(6) = d(2)\, d(3)$

$\downarrow \quad = 2 \times 2 = 4.$

1, 2, 3, 6

12th Nov'13.

Q. Find $d(9!)$ and $\sigma(9!)$

$9! = 1 \times 2 \ldots 9$

$9! = 1 \cdot 2^7 \cdot 3^4 \cdot 5 \cdot 7$

$d(9!) = d(1)\, d(2^7)\, d(3^4)\, d(5)\, d(7)$

$= 1 \cdot 8 \cdot 5 \cdot 2 \cdot 2 = 160$

$\rightarrow p+1$

$\sigma(9!) = \sigma(1)\, \sigma(2^7)\, \sigma(3^2)\, \sigma(5)\, \sigma(7)$

$= 1 \cdot \dfrac{2^{7+1}-1}{2-1} \cdot \dfrac{3^3-1}{3-1} \cdot 6 \cdot 8$

$= 1 \cdot 255 \cdot 13 \cdot 6 \cdot 8$

Q. Find $d(n)$ & $\sigma(n)$ where n is product of 1st seven prime numbers.

$n = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$

$d(n) = 2 \cdot 2 \cdot 2 \ldots = 2^7 = 128$

$\sigma(n) = 3 \cdot 4 \cdot 6 \cdot 8 \cdot 12 \cdot 14 \cdot 18$

Pg 84

Q.1. Prove ~~d(n) is~~ $d(n)$ is odd iff n is a perfect square.

Proof

$n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$

$d(n) = (\alpha_1+1)(\alpha_2+1)\cdots(\alpha_r+1)$

For $d(n)$ to be odd each factor of (α_i+1) has to be odd

$\Rightarrow \alpha_i$'s should be even.

If $\alpha_i = 2m_i$, then $n = p_1^{2m_1} \cdot p_2^{2m_2} \ldots p_r^{2m_r}$

$n = (p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r})^2$

Hence Proved $\longrightarrow$ n is a perfect sq.

Q. for which value of n is $\sigma(n)$ .. odd :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

$$\sigma(n) = \sigma(p_1^{\alpha_1})\,\sigma(p_2^{\alpha_2}) \dots \sigma(p_r^{\alpha_r})$$

$$= \frac{p_1^{\alpha_1+1}+1}{p_1 \cancel{+} - 1} \times \frac{p_2^{\alpha_2+1}+1}{p_2-1} \times \dots$$

Let us write

$$p_i = \frac{p_i^{\alpha_i+1}-1}{p_i-1} = 1+p_i+p_i^2+\dots\ p_i^{\alpha_i}$$

If the no. of Terms is odd in the series, σ will alway be odd.

$\Rightarrow$ α_i's should be even.

Let $\alpha_i = 2^{m_i}$

$$n = p_1^{2m_1} p_2^{2m_2} \dots p_r^{2m_r}$$

$$= (p_1^{m_1} p_2^{m_2} \dots p_r^{m_r})^2 \quad \dots \text{ Perfect square.}$$

Q.1. Prove if there are 2 divisors of any no. it is prime ... Trivial

Q.2. —— " —— 3 divisors —— " —— square of a prime.

Soln.

d $\rightarrow$ no. of divisors. Let $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$

$$d(n) = (\alpha_1+1)(\alpha_2+1) \dots (\alpha_r+1)$$

$$3 = (\alpha_1+1)(\alpha_2+1) \dots$$

$$1 \times 3 = (\alpha_1+1)(\alpha_2+1) \longrightarrow \text{1 not included in } p_i^{\alpha}$$

$$\alpha_1+1 = 1 \quad ; \alpha_2+1 = 3$$

$$\alpha_1 = 0 \quad \alpha_2 = 2$$

$$n = p_1^0 p_2^2 = p_2^2 \text{ (Perfect sq).}$$

classmate
Date
Page

Q.3. 4 divisors $\longrightarrow$ cube of product of primes.

Soln $d(n) = 4 = (\alpha_1+1)(\alpha_2+1)(\alpha_3+1)$

(i) $4 = 1\times 4$ (ii) 2×2

(i) $\alpha_1 = 0$ $\alpha_2 = 3$; $n = p_2^{\,3}$

(ii) $\alpha_1 = 1$ $\alpha_2 = 1$ $n = p_1 \cdot p_2$.

Ques Prove n is a prime iff $\sigma(n) = n+1$

Proof. Let n, not be a prime, then $\sigma(n) = n+1$

To prove contradiction.

If n is not prime, then it has other divisor say d other than 1 & d.

Then $\sigma(n) \geq n+d+1 > n+1$.

Ques. Find an integer n S.T. $\sigma(n) = 36$

$36 = 1\times 36^{\times}$

$= 2\times 18$

$= 4\times 9$

$= 6\times 6 = 3\times 12$.

$p_1 = 5$ $\alpha_1 = 1$; $p_2 = 5$ $\alpha_2 = 1$.

$\times$ $n = 5^1 \times 5^1 = 25$

$p_1 = 2$; $\alpha_1 = 1$ $p_2 = 11$; $\alpha_2 = 2$.

$n = 2\times 11 = 22$.

classmate
Date
Page

13th Nov '13

Q3. Page 84. Prove if $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$

then $\sigma(n)\,\phi(n) = n^2(1-p_1^{-\alpha_2-1}) \ldots (1-p_r^{-\alpha_r-1})$

and

$$\phi(n)\cdot\sigma(n) > n^2\left(1-\frac{1}{p_1^2}\right)\left(1-\frac{1}{p_2^2}\right)\ldots\left(1-\frac{1}{p_r^2}\right).$$

$$\sigma(n)\cdot\phi(n) = \sigma(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r})\,\phi(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r})$$

$$= \sigma(p_1^{\alpha_1})\sigma(p_2^{\alpha_2})\ldots\sigma(p_r^{\alpha_r})\,\phi(p_1^{\alpha_1})\ldots\phi(p_r^{\alpha_r})$$

$$= \left(\frac{p_1^{\alpha+1}-1}{p_1-1}\right)\cdot\left(\frac{p_2^{\alpha_2+1}-1}{p_2-1}\right)\ldots\left(\frac{p_r^{\alpha_r+1}-1}{p_r-1}\right)\times(p_1^{\alpha_1}-p_1^{\alpha_1-1})\ldots(p_r^{\alpha_r}-p_r^{\alpha_r-1})$$

$$= \left(\frac{p_1^{\alpha_1+1}-1}{\cancel{p_1-1}}\right)\cdot\left(\frac{p_2^{\alpha_2+1}-1}{\cancel{p_2-1}}\right)\ldots p_1^{\alpha_1-1}(\cancel{p_1-1})\cdot p_2^{\alpha_2-1}(\cancel{p_2-1})\ldots$$

$$= (p_1^{\alpha_1+1}-1)(p_2^{\alpha_2+1}-1)\ldots p_1^{\alpha_1-1}\cdot p_2^{\alpha_2-1}$$

$$= p_1^{\alpha_1}(p_1-p_1^{-\alpha_1})\,p_2^{\alpha_2}(p_2-p_2^{-\alpha_2})\ldots\frac{p_1^{\alpha_1}}{p_1}\cdot\frac{p_2^{\alpha_2}}{p_2}\ldots$$

$$= (p_1^{\alpha_1})^2(p_2^{\alpha_2})^2\ldots\left(\frac{p_1-p_1^{-\alpha_1}}{p_1}\right)\left(\frac{p_2-p_2^{-\alpha_1}}{p_2}\right)\ldots$$

$$= n^2(1-p_1^{-\alpha_1-1})(1-p_2^{-\alpha_2-1})\ldots(1-p_r^{-\alpha_r-1}).$$

$(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r})^2$

n

If $\alpha_1=\alpha_2=1$ then.

$$= n^2\left(1-\frac{1}{p_1^2}\right)\left(1-\frac{1}{p_2^2}\right)\ldots\left(1-\frac{1}{p_r^2}\right)$$ 2nd case is proved.

Divisors add To given original number.

Q.9. If $\sigma(n)=2n$, n is a perfect number. Prove if n is a perfect no. then $\sum_{d|n}\frac{1}{d}=2$. (II)

$$2n = \sigma(n) = \sum_{d|n} d = \sum_{d|n}\frac{n}{d} = n\sum_{d|n}\frac{1}{d}$$

$$2\cancel{n} = \cancel{n}\sum_{d|n}\frac{1}{d}$$

$$2 = \sum_{d|n}\frac{1}{d}.$$

Thm^r.

Article. 6.3.

Show. $\sum_{d|n} d = \sum_{d|n}\frac{n}{d}$. To show

Suppose $n=6 \rightarrow$ Divisors $= d = 1, 2, 3, 6$.

$$\sum_{d|n} d = 1+2+3+6 = 12$$

$$\sum_{d|n}\frac{n}{d} = 6+3+2+1 = 12$$

LHS = RHS

Hence Proved

Proof. (1)

Q.12. Prove that $\frac{\phi(n)\sigma(n)+1}{n}$ is an integer if n is prime & not an integer if n is divisible by square of a prime.

(I). If $n=p$ (prime) $\qquad \phi(p)=p-1$.

$$\frac{\phi(p)\sigma(p)+1}{p}.$$

$$\frac{(p-1)(1+p)+1}{p}$$

$$\frac{p^2-1+1}{p} = p \in \text{Integer}$$

Hence Proved.

(II) n is divisible by sq. of prime.

$$n = \underline{p_1^2}\, p_2^{\alpha_2} \dots p_r^{\alpha_r}.$$

sq. of prime.

$$\phi(n) = \phi(p_1^2)\,\phi(p_2^{\alpha_2}) \dots \phi(p_r^{\alpha_r}).$$

$$\sigma(n) = \sigma(p_1^2)\cdot\sigma(p_2^{\alpha_2}) \dots \sigma(p_r^{\alpha_r})$$

$\dfrac{\phi(n)\sigma(n)+1}{n}$ = Expand above functions (1 will not get cancelled)

$\notin$ Integer.

Thm^r.
Article 6.3. $\phi(n), d(n), \sigma(d)$ and $\mu(n)$ are multiplicative arithmatic fun^n.

To show ① $\phi(m.n) = \phi(m).\phi(n)$

② $d(m.n) = d(m).d(n)$

③ $\sigma(dn.m) = \sigma(m).\sigma(n)$

④ $\mu(mn) = \mu(m).\mu(n)$. Symmetrical Proof.

Proof. ① Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$

$n = q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$

$$m.n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}$$

$$\begin{aligned}
\phi(m.n) &= \phi(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}) \\
&= [\phi(p_1^{\alpha_1}).\phi(p_2^{\alpha_2})] \dots [\phi(q_1^{\beta_1})\,\phi(q_2^{\beta_2})\,\phi(q_s^{\beta_s})] \\
&= \phi(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r})\,\phi(q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}) \\
&= \phi(m)\,\phi(n)
\end{aligned}$$

= Hence Proved (Same for ② ③).

④. $\mu(n) = \begin{cases} 1 & n=1 \\ 0 & p^2 \mid n \\ (-1)^r & n = p_1 p_2 \cdots p_r \end{cases}$

For $m=1\ n=1$ $\quad m.n = 1$

$$\mu(m.n) = 1$$

$$\mu(m) = \mu(n) = 1.$$

$$\therefore \mu(m.n) = \mu(m)\,\mu(n).$$

For $\mu(mn)=0$. Either m or n should have a square of prime no. as factor

Let $m = \underline{p_1^2}\, p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ $\qquad n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$.

Sq. of prime $\rightarrow \mu(m) = 0$ $\qquad \mu(n) = \mu(q_1^{\beta_1} \cdots q_s^{\beta_s})$

$$\mu(m).\mu(n) = 0$$

$\therefore$ LHS = RHS Hence Proved.

For $\mu(mn) = (-1)^n$ .. Solve urself.

In this case all $\mu_i = \beta_j = 1$.

$$\mu(mn) = \mu(p_1 p_2 .. p_r . q_1 q_2 \cdots q_s)$$

$$= (-1)^{r+s} = (-1)^r (-1)^s$$

$$= \mu(p_1 p_2 \cdots p_r)\,\mu(q_1 q_2 \cdots q_s)$$

$$= \mu(m) . \mu(n).$$

Q. Find last two decimal digits of 3^{1492}

Residue when u divide by 100

$$\begin{array}{r|l} 2 & 100 \\ 2 & 50 \\ 5 & 25 \\ 5 & 5 \\ & 1 \end{array}$$

$$3^{1492} \equiv ? \pmod{100}.$$

By Euler's Thm:

$a^{\phi(m)} \equiv 1 \pmod{m}$ a, m ... relatively prime.

$a = 3 \quad m = 100.$

$$3^{\phi(100)} \equiv 1 \pmod{100}$$

$$3^{\phi(2^2)\phi(5^2)}$$

$$3^{(4-2)(25-5)}$$

$$3^{2.20}$$

$$\phi(100) = \phi(2^2)\phi(5^2)$$
$$= (4-2)(25-5)$$
$$= 40$$

$$3^{40} \equiv 1 \pmod{100}$$

$$1492 \equiv 40 \times 37 + 12$$

$$3^{1492} = (3^{40})^{37} \cdot 3^{12}$$
$$= (1)^{37} \cdot 3^{12}$$
$$\equiv 531441 \ \% \ 100.$$

41 last two decimal digits.

Chapter 5, 6. Prime nos → Test 2.

G. K.

Prime below 10 million = 664579 Cooper Boone.

Largest Prime: $2^{32582657} - 1$.

9808358 digits

14th Nov '14.

Prime Numbers.

1. 2 is the only even prime
2. 2, 3 are only consecutive primes.
3. Odd consecutive primes (3, 5) (5, 7) (11, 13) (41, 43) → twin primes.

Seive of ~~Erathothenere~~

Method to find a no. is prime or not.

Q. Find all prime no. before 50.

$\sqrt{50} \approx 7$.

Go upto square root of a particular no.

1	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~

STOP

Total primes = 15.

Distribution of prime irregular Density – decreases

No n^{th} term formula.

Prime Triplets.

$(p, p+2, p+6) \longrightarrow (11, 13, 17) . (41, 43, 47)$

$(p, p+4, p+6) \longrightarrow (13, 17, 19)$

Q. To find whether a no. is prime.

eg. $\sqrt{50} \approx 7$

Note → Divide 50 by all primes ~~before~~ till 7.

(n). 2, 3, 5, 7

$\left.\frac{50}{2}, \frac{50}{5}\right\}$ → Divisible by one hence not prime.

eg. 2011

$\sqrt{2011} \approx 45$

Divide $\underset{\downarrow}{2011}$ by all primes till 45

Not divisible by any primes, hence **2011 is prime**.

Ex. For a larger number: before a number 'x'

Thm^r. The number of primes is denoted $\pi(x)$, it is

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

$\ln . x$.

eg. For 50 $\pi(50) \approx \frac{50}{\log_e 50} \approx 12.78 \rightarrow 13$ (Integer).

17th Nov'13.

Ex. $x = 10000 = 10^3$

168 primes before 10000

If we use;

$$\pi(x) = \frac{10^3}{\log_e 10^3} = 145$$

Chebychev

$\rightarrow$ $c_1 \frac{x}{\log_e x} \leq \pi(x) \leq c_2 \frac{x}{\log_e x}$

Thm^{r}. n^{th} prime satisfies

$$P_n \leq 2^{2^{n-1}} \text{ for all } n \geq 1.$$

e.g. 2, 3, 5, 7, 11 → 5^{th}

$$P_5 \leq 2^{2^{5-1}}$$
$$\leq 2^{2^4}$$
$$P_5 \leq 2^{16}$$

Thm^{r}: If $p \mid ab$ then $p \mid a$ or $p \mid b$

If $p \mid a_1 a_2 \dots a_n$ then p divides atleast one a_i

Thm^{r}: There are infinitely many primes.

Proof. Let there be finite number of prime.

and let them be $p_1, p_2 \dots p_k$.

Lets consider a number m. such that.

$$m = p_1 p_2 \dots p_k + 1 \qquad \text{— (a)}$$

If m is a prime or a composite number.

Case 1. m is prime,

We now have one more prime besides.

$p_1, p_2 \dots p_k \Rightarrow$ Number of primes not finite

$\therefore$ Contradiction

Hence ∞ no. of primes.

Case 2. m is composite, then it can be written as product of powers of primes,

$\Rightarrow$ m should be divisible by a prime ~~could~~ it will be from $p_1, p_2, \dots p_k$

Lets say it is 'p'

classmate
Date
Page

Note: Odd numbers are of the form $4n+1$ & $4n+3$.

$\Rightarrow p \mid m$. also $p \mid p_1 p_2 \dots p_k$.

$\Rightarrow p \mid \underbrace{m-(p_1 p_2 \dots p_k)}_{\text{From ⓐ } = 1} \longrightarrow p \mid 1 \rightarrow$ Contradiction

Hence Proved ∞ no. of prime numbers.

Lemma. Let a and b be integers of the form $4n+1$ then ab is of form $4n+1$

Proof. Let $a = 4r+1$

$b = 4s+1$.

$a.b = (4r+1)(4s+1)$

$= 16rs + 4r + 4s + 1$

$= 4\underbrace{(4rs+r+s)}_{K} + 1$.

$= 4K+1$

Hence Proved.

Thm^r: There are infinite number of primes of the form $4n+3$

Proof. Let the be finite number of primes $p_1, p_2 \dots p_k$.

Let us consider an integer.

$m = 4(p_1 p_2 \dots p_k) - 1$ — From ⓐ

If we take

$q = (p_1 p_2 \dots p_k) - 1$

$p_1 p_2 \dots p_k = q+1$.

$m = 4(q+1) - 1$

$= 4q+3$.

Can be prime OR Composite.

m is of the form $4q+3$.

Case (a) m is a prime → Gives us one more prime other than $p_1 \cdot p_2 \ldots p_k$.

$\therefore$ primes NOT finite   Contradiction.

Case (b). m is composite, it can be written as a product of prime powers

~~cannot be~~ all the factors of m cannot be of the form $4n+1$ (In that case the product will be of the form $4n+1$. But m is of the form $4n+3$.).

So atleast one factor will be of form $4n+3$ → say p.

→ $p \mid m$.

also, $p \mid 4p_1p_2 \ldots p_k$.

$p \mid \underbrace{4p_1p_2 \ldots p_k - m}_{ⓐ}$.

$p \mid 1$ → Contradiction.

Hence Proved.

∞ no. of primes.

Fermit's Number

Notation : F_n.

$$F_n = 2^{2^n}+1.$$ (Any no. of this form is Fermit number)

↓ If it is prime

Fermit's prime.

$n=0$ $F_0 = 3$ ... Fermit's prime
$=1$ $F_1 = 5$ ... —"—
$=2$ $F_2 = 17$ ... —"—
$=3$ $F_3 = 257$ ... —"—
$=4$ $F_4 = 65537$ ... —"—

For. $n=5$ $F_5 = 641 \times 6700417$ → NOT a prime Proved by Euler.

Mersenne Number

Notation : M_p → Only primes are considered.

$$M_p = 2^P - 1$$

$$\left.\begin{array}{ll} p=2 & M_2 = 3 \\ p=3 & M_3 = 7 \\ p=5 & M_5 = 31 \\ p=7 & M_7 = 127. \end{array}\right\} \text{Mersenne Prime}$$

$p=11$ $M_{11} = 2047 = 23 \times 89$ → Composite

19th Nov. '13.

Prime numbers can be of the form:

① $4n+1$
② $4n+3$
③ $6n+5$
\# ④ $8n+5$

$m = 4(p_1p_2\ldots p_r)-1$ $q = p_1p_2\ldots p_r - 1$.

$m = 6(p_1p_2\ldots p_r)-1$. $q = p_1p_2\ldots p_2-1$.

will be form either $6n+1$. $6n+5$ ③

For ∞ no. of prime.

For each form m & q are different.

will be odd number *

m — Can be → prime. Extra 'p' in $p_1p_2\ldots p_r$. Hence contradiction

m — composite → product of prime powers. Show multiple of prime & divisible by some prime (Using values of q & m) → $p \mid 1$ → Contradiction.

* They all can't be of form $6n+1$ so atleast one will be of the form $6n+5$ Let it be p

& $p \mid m \rightarrow p \mid 6p_1p_2\ldots -1$ So

$p \mid 6p_1p_2 - m \rightarrow p \mid 1$.

Contradiction.

Fermit's numbers : $2^{2^n}+1$

Mersenne numbers : 2^p-1

Exercise. 1. Find all positive integers 'n' for which $3n-4$, $4n-5$, $5n-3$ are all prime numbers

Soln. A. If we add the numbers

$3n-4+4n-5+5n-3$

$= 12n-12$ .. Even numbers.

- One or more one are even numbers
- Two have to be odd to give even number & one even

Even × n − Odd → Always odd.

Out of three either $3n-4$ is even or $5n-3$ is even } Both are prime. Only even prime $= 2$.

$3n-4=2 \rightarrow n=2$ ✓

or $5n-3=2$ or $n=1 \rightarrow 3n-4$ becomes neg. ✗.

$\therefore$ $n=2$ is a value

Primes → 2, 3, 7.

2. If p and q are primes and $x^2-px+q=0$ has distinct positive integral roots. Find p & q.

Solution. Quadratic eq^n : $x^2-px+q=0$.

$\downarrow$

Distinct + Roots $\longrightarrow x_1, x_2$.

$\downarrow$

$\Delta = 4ac = 4q$.

Sum of Roots $= \alpha+\beta = \frac{-b}{a}$ (x_1+x_2)

Sum of Roots $= p = x_1+x_2$

Product of roots $= q = x_1 \cdot x_2$ ↳ Product should be prime.

As q is prime either x_1 or $x_2 = 1$.

Suppose $x_1 = 1$.

$\rightarrow x_2 = q$.

$p = 1+q$.

$p-q=1$

Only Consecutive primes are $\underline{\underline{2, 3}}$.

$\left.\begin{aligned}\therefore p &= 3\\ q &= 2\end{aligned}\right\} \longrightarrow$ (Answer)

Skip these questions.

Q. Prove any + int of form ... has + integer...

Date
Page

Ques. 3. Find all prime numbers 'p' suchthat $17p+1$ is a square

Solution.

Let $17p+1 = x^2$.

as. 17 & p are prime

$17p = x^2 - 1$

$17 . p = (x-1)(x+1)$.

$x+1 = 17 \quad x = 16$
$x-1 = p \quad p = 15$ } Not True

OR.

$x-1 = 17 \quad x = 18$
$x+1 = p \quad p = 19$ } True.

$\therefore \quad p = 19$ for $17p+1$ to be a square

Revision. $\underbrace{2x \equiv 5 \pmod 6}$

$g.c.d(2,6) = 2$

$d \nmid 5 \rightarrow$ No solution

If it divides then d number of congruent solution.

12

$2x \equiv 4 \pmod 6$ $\quad \frac{2x-4}{6} = y$. Linear diophantine eq^n.

$\downarrow$.

$d = 2$.

$2 \mid 4$ $\quad 2x - 6y = 4$

2 incongruent soln. $\quad 6 = 2 \times 3 + 0$

1 24th Nov'13.

Primitive Roots.

$g, g^2, g^3 \ldots\ldots \pmod{m}$.

Ex. $\phi(m) = \{1, 3, 7, 9\}$. $m = 10$.

$3 \equiv 3 \pmod{10}$. $7 \equiv 7$ $9 \equiv 9$

$3^2 \equiv 9 \equiv 9 \pmod{10}$ $7^2 \equiv 9$ $9^2 \equiv 1$

$3^3 \equiv 7$ $7^3 \equiv 3$ $9^3 \equiv 9$.

Smallest. $3^4 \equiv 1$ $7^4 \equiv 1$

$3^5 \equiv 3$ $g.c.d(7, 10) = 1$.

$3^6 \equiv 9$

Def^n. 7.1. If h is the smallest positive integer such that

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

we say a belongs to exponent h mod m.

Thm^r. 7.1. In order that $a^b \equiv 1 \pmod{m}$ for some integer b, it is necessary & sufficient that $g.c.d\,(a, m) = 1$ (Relatively prime).

Thm^r 7.2 If a belongs to exponent h mod m & $a^r \equiv 1 \pmod{m}$ then $h \mid r$

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

QUADRATIC RESIDUES (Chapter 9).

Linear congruences: $2x \equiv 3 \pmod 5$

System of congruences: $\left.\begin{array}{l} x \equiv 3 \pmod 2 \\ x \equiv 5 \pmod 7 \\ \vdots \end{array}\right\}$

Quadratic congruence: $x^2 \equiv a \pmod m$.

Quadratic residue.

Condition for solution to exist.

If g.c.d $(a,p) = 1$ ie p doesn't divide 'a' then $p \nmid a$

$x^2 \equiv a \pmod m$ has a solution.

'a' is called quadratic solution

Can be 1, 4, 9 — All perfect squares need not be residues

eg. $x^2 \equiv 1 \pmod 7$

g.c.d $(1,7) = 1$ Hence soln exists.

$x^2 \Rightarrow$ soln $\rightarrow 1, -1$

a can 1, 4, 9 but cannot take 49.

$7 \mid 49$.

26th Nov '18.

$x^2 \equiv a \pmod{p}$.

$x^2 \equiv 1 \pmod{7}$

$\equiv 4$

$\equiv 9$

Note: All numbers congruent to 'a' are also quad. residue

$1 \equiv -6 \pmod{7}$

$4 \equiv -3 \pmod{7}$

$9 \equiv 2 \pmod{7}$

$-6, -3, 2$ ... quad residues.

Thm^n: The number 'a' is a quadratic residue mod p iff. (No Proof).

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad \text{... Euler Criteria.}$$

Exercise. Use Euler's criteria.

Pg 117.

(a) $a=2$; $p=5$

$$2^{\frac{5-1}{2}} \equiv 1 \pmod{5}$$

$$2^2 \not\equiv 1 \pmod{5}$$

2 is not a quad residue.

(b) $a=4$ $p=7$

$$4^{\frac{7-1}{2}} \equiv 1 \pmod{7}$$

$$4^3 \equiv 1 \pmod{7}$$

64 $\quad \frac{64-1}{7} \in I$

$\therefore$ 4 is a quadratic residue.

Art. 9-2. Legendre's Symbol.

Notation: $\left(\frac{a}{p}\right)$

Notdividing a = integer.
p = prime number.

Defn. If p is an odd prime then
$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quad residue} \\ 0 & \text{if } p \mid a \\ -1 & \text{otherwise.} \end{cases}$$

Thm. 9.2. If p is an odd prime & a, b are relatively prime to p, then

1. $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ if $a \equiv b \pmod p$

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

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

Proof 1. ~~Three~~ Two cases
Let $a \equiv b \pmod p$
Case 1: a is a quad. residue mod p
We know $\forall$ Integer congruent to 'a' are also quad. residues
$$\left(\frac{a}{p}\right) = 1 \quad \& \quad \left(\frac{b}{p}\right) = 1$$
$$\rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

1

Case 2: ~~Let~~ $p|a \rightarrow \left(\frac{a}{p}\right) = 0$

a is not a quad residue

$\left(\frac{a}{p}\right) = -1$ and $a \equiv b \rightarrow \left(\frac{b}{p}\right) = -1$

Proof 3. To show: $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (\text{mod } p)$

From euler's thm^r

criteria

$a^{\frac{p-1}{2}} \equiv 1 \ (\text{mod} p)$. $\longrightarrow$

if a is a quad residue.

$\left(\frac{a}{p}\right) = 1$

Replace 1 by $\left(\frac{a}{p}\right)$

$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \text{mod } p.$

If a is not a quad residue.

$\left(\frac{a}{p}\right) = -1$

and

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

classmate
Date
Page

Proof 2. To show: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

using Proof 3.

$$(ab)^{\frac{p-1}{2}} \equiv \left(ab \; a^{p-1/2} \cdot b^{p-1/2}\right) \equiv 1 \pmod p.$$

$$\equiv \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right) \pmod p.$$

*. Note: $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ if 'a' is a quad. residue
$\equiv -1 \pmod p$ if 'a' is not a quad. residue.

Jacobi's Symbol.

If $m = p_1 p_2 \ldots p_r$ then

$$\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right)\left(\frac{n}{p_2}\right)\cdots\left(\frac{n}{p_r}\right)$$

Exercise
Pg 118.

Q.1. Prove if c is odd then $\left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right)\cdot\left(\frac{b}{c}\right)$

Proof. Let $c = p_1 p_2 \ldots p_r$

$$\left(\frac{ab}{c}\right) = \left(\frac{ab}{p_1 p_2 \ldots p_r}\right) = \left(\frac{ab}{p_1}\right)\left(\frac{ab}{p_2}\right)\cdots\left(\frac{ab}{p_r}\right)$$ Using Jacobi's Symbol.

By Property 2.

$$= \left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)\left(\frac{a}{p_2}\right)\left(\frac{b}{p_2}\right)\cdots\left(\frac{a}{p_r}\right)\left(\frac{b}{p_r}\right)$$

Collecting all 'a' & 'b' terms $= \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right)\left(\frac{b}{p_1}\right)\left(\frac{b}{p_2}\right)\cdots\left(\frac{b}{p_r}\right)$

$$= \left(\frac{a}{c}\right)\left(\frac{b}{c}\right)$$ Hence Proved

classmate
Date
Page

Quadratic Reciprocity Law

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \quad \text{unless} \quad p \equiv q \equiv 3 \pmod 4$$

p.q :: primes

If $p \equiv q \equiv 3 \pmod 4$ then
$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$$

Formula list.

1. $\left(\frac{a^2}{p}\right) = 1$ if a and p are relatively prime

2. $\left(\frac{1}{p}\right) = 1$

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

4. $\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \pmod 4 \end{cases}$

5. $\left(\frac{2}{p}\right) = (-1)^{p^2-1/8}$

6. $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & p \equiv \pm 3 \pmod 8 \end{cases}$

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

8. $\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \equiv \pm 5 \pmod{12} \end{cases}$

27th Nov'13.

Thm 9.6 If p is an odd prime & g.c.d $(a,p)=1$ then

$$x^2 \equiv a \pmod{p^n}$$

has a solution if $\left(\frac{a}{p}\right)=1$ if $\left(\frac{a}{p}\right)=-1$ no solution

Ex Find whether $x^2 \equiv 15 \pmod{89}$ has a solution or not?

Soln. To find $\left(\frac{15}{89}\right)$

Note: Denominator must be a prime for Legendre's number.

$$\left(\frac{15}{89}\right) = \left(\frac{3.5}{89}\right)$$

$$= \left(\frac{3}{89}\right)\left(\frac{5}{89}\right)$$

To find $\left(\frac{3}{89}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & p \equiv \pm 5 \pmod{12} \end{cases}$ ✓

$89 \not\equiv \pm 1 \pmod{12}$ — ×.

$89 \equiv \pm 5 \pmod{12}$ — ✓

$\therefore \left(\frac{3}{89}\right) = -1$ — ①

To find $\left(\frac{5}{89}\right)$ $p=5$, $q=89$

By Repciprocity law

$5 = p \not\equiv 3 \pmod 4$

$89 = q \not\equiv 3 \pmod 4$

$$\therefore \left(\frac{p}{q}\right) = + \left(\frac{q}{p}\right)$$

$\therefore \left(\frac{5}{89}\right) = \left(\frac{89}{5}\right)$ By Quadratic Reciprocity Law.

89 is replaced by residue mod 5

$$\left(\frac{89}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) = 1. \quad -②$$

$\left(a^2/p\right)$ a, p relatively prime

Hence $\left(\frac{15}{89}\right) = \left(\frac{3}{89}\right)\left(\frac{5}{89}\right) = (-1)(1) = -1$

$\because \left(\frac{15}{89}\right) = -1$. there is no solutions .

Ex. Find the value of $\left(\frac{89}{103}\right)$.

$p = 89 \qquad q = 103$

$p \not\equiv 3 \pmod 4$

$q \not\equiv 3 \pmod 4$.

$\equiv$

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

$$\left(\frac{89}{103}\right) = \left(\frac{103}{89}\right)$$

$103 \equiv x \pmod{89}$

$\downarrow$

14

$$= \left(\frac{14}{89}\right) = \left(\frac{2}{89}\right)\left(\frac{7}{89}\right)$$

To find $\left(\frac{2}{89}\right)$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod 8 \\ -1 & p \equiv \pm 3 \pmod 8 \end{cases}$$

$89 \equiv -1 \pmod 8$

$\therefore \left(\frac{2}{89}\right) = 1$. — ①.

To find $\left(\frac{7}{89}\right)$

$p \equiv 3 \pmod 4$

$q \not\equiv 3 \pmod 4$

$\therefore \left(\frac{7}{89}\right) = \left(\frac{89}{7}\right)$

$89 \equiv x \pmod 7$

$\downarrow$

5

$$\left(\frac{89}{7}\right) = \left(\frac{5}{7}\right)$$

$\left(\frac{5}{7}\right) = \left(\frac{7}{5}\right)$ By Reciprocity Law $5 \not\equiv 3 \pmod 4$

$\downarrow$ mod 5

$= \left(\frac{2}{5}\right)$

To find $\left(\frac{2}{5}\right) = (-1)^{p^2-1/8}$

$= (-1)^{24/8} = (-1)$.

$\therefore \left(\frac{89}{103}\right) = \left(\frac{2}{89}\right)\left(\frac{7}{89}\right)$

$= 1 \cdot (-1)$

$= (-1)$ ... (Answer). No Solution exist.

Ex. $\left(\frac{2}{3}\right) = (-1)^{p^2-1/8} = -1$

Ex. Find whether $x^2 \equiv 5 \pmod{23}$ has a solution or not.

Solution exist if $\left(\frac{a}{p}\right) = 1$

and $\left(\frac{a}{p}\right) = 1$ when 'a' is a quadratic residue

By Euler's criteria: a is quad residue if

$a^{\frac{p-1}{2}} \equiv 1 \pmod p$.

$a = 5$ $p = 23$

$5^{23-1/2} \equiv 1 \pmod{23}$

$5^{22/2}$

$5^{11} \equiv 1 \pmod{23}$.

By Euler's thm^r $5^{\phi(23)} \equiv 1 \pmod{23}$

$5^{22} \equiv 1 \pmod{23}$

$(5^{11})^2 \equiv 1^2 \pmod{23}$.

x.

Ex. Find $\left(\frac{-2}{\cancel{15}\ 7}\right) = -\left(\frac{2}{7}\right)$

$= \left(\frac{-1}{7}\right)\left(\frac{2}{7}\right)$

$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \pmod 4 \end{cases}$.

$7 \equiv 3 \pmod 4$

$\therefore \left(\frac{-1}{7}\right) = -1.$

$\left(\frac{2}{7}\right) = (-1)^{p^2-1/8} = (-1)^{48/8} = (-1)^6 = 1.$

$\therefore \left(\frac{-2}{7}\right) = -1 . 1 = -1.$ ... Solution.

28th Nov'13.

Q. Find a '$\cancel{k}$ p' for which

$\cancel{k^2}\ x^2 \equiv -3 \pmod p.$

For solution to exist (Homework)

Find p such that $\left(\frac{-3}{p}\right) = 1.$

$\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$

Finding solution for quadratic residues.

Ex. Solve $x^2 \equiv 196 \pmod{1357}$ — ①

$\underline{1357} = 23 \times 59$
↳ Composite number.

$$\begin{cases} x^2 \equiv 196 \pmod{23} & \text{— (A)} \\ x^2 \equiv 196 \pmod{59} & \text{— (B)} \end{cases}$$

If (A) and (B) both have common soln then solve for ① exists.

Then $\left(\frac{196}{23}\right)$ and $\left(\frac{196}{59}\right)$ both should be 1.

$$\left(\frac{196}{23}\right) = \left(\frac{12}{23}\right) = \left(\frac{2^2 3}{23}\right) = \left(\frac{2^2}{23}\right)\left(\frac{3}{23}\right)$$

$\begin{array}{r} 23 \\ \times 8 \\ \hline 184 \end{array}$ 12

$p \not\equiv 3 \pmod 4$

$\therefore \left(\frac{12}{23}\right) = \left(\frac{23}{12}\right)$

$\left(\frac{a^2}{p}\right) = 1$

$\left(\frac{3}{23}\right) = 1.$

$23 \equiv +1 \pmod{12}$

$\therefore \left(\frac{196}{23}\right) = 1.$ .. (A)

$$\left(\frac{196}{59}\right) = \left(\frac{19}{59}\right) = -\left(\frac{59}{19}\right) = -\left(\frac{2}{19}\right) = (-1)^{19^2-1/8} = 1.$$

$\begin{array}{r} 59 \\ \times 3 \\ \hline 177 \\ \hline 19 \end{array}$ $\begin{array}{r} 19 \\ \times 3 \\ \hline 57 \end{array}$

By reciprocity law

$\begin{array}{r} 19 \\ \times 19 \\ \hline 171 \\ 19\times \\ \hline 261 \end{array}$

260

$19 \equiv 3 \pmod 8$

$= -1$

$= -(-1) = \underline{\underline{1}}$ ... (B)

(A). $x^2 \equiv 196 \pmod{23}$ ... one solution is 14.

$x = 14 \quad x^2 = 196.$

*.

Thm^r: If $x^2 \equiv a \pmod{p}$ has a solution say x_0 then the other solution is $(p - x_0.)$

$\therefore$ For (A)

One Solution $x_0 = \cancel{23}\ 14$

Other solution $p - x_0 = 23 - 14 = 9.$

(B) $x^2 \equiv 196 \pmod{59}$

1^{st} soln $= 14$

2^{nd} soln $= 59 - 14 = 45$

To find solution of (1)

Forming congruences,

$x \equiv 14 \pmod{23}, \quad x \equiv 14 \pmod{59}$ (2)

$x \equiv 14 \pmod{23}, \quad x \equiv 45 \pmod{59}$ (3)

$x \equiv 9 \pmod{23}, \quad x \equiv 14 \pmod{59}$ (4)

$x \equiv 9 \pmod{23}, \quad x \equiv 45 \pmod{59}$ (5)

14   9   mod 23

14   45   mod 59

Solve each of the above pair of congruences using Chinese Remainder Theorem.

classmate

Date ______
Page ______

(2) $x \equiv 14 \pmod{23}$ $\qquad$ $x \equiv 14 \pmod{59}$

$c_1 = 14$ $\qquad$ $c_2 = 14$

$n_1 = 59$ $\qquad$ $n_2 = 23$

$\overline{n_1} = 16$ $\qquad$ $\overline{n_2} = 18$

$59\overline{n_1} \equiv 1 \pmod{23}$

59
×16
354
59×
944
23

$x_0 = c_1 \cdot n_1 \cdot \overline{n_1} + c_2 n_2 \overline{n_2}$

$= 14 \cdot 59 \cdot 16 + 14 \cdot 23 \cdot 18$

$13216 + 5796$

$= 19012 \bmod 1357$

$x_0 = 14.$

Using CRT.

(3) $x_0 = 635$

(4) $x_0 = 722$

(5) $x_0 = 1343.$

all values solve eqⁿ (1) $x^2 \equiv 196 \pmod{1357}$.

Types of Quadratic Congruences.

(1) $x^2 \equiv 9 \pmod{2}$ → Prime $\qquad$ $x = 3$

→ Whole square

(2) $x^2 \equiv 9 \pmod{12}$ $\qquad$ Solve like before eg

→ Composite

(3) $x^2 \equiv 9 \pmod{2^3}$

or $\qquad$ Different method.

$x^2 \equiv 9 \pmod{7^2}$

①

3rd Dec '15

Q.2 $x^2 \equiv 23 \pmod{7^2}$

prime square.

Soln. exists or not ?

$\left(\frac{23}{49}\right)$

not prime

Make system:

$$\begin{cases} x^2 \equiv 23 \pmod 7 \\ x^2 \equiv 23 \pmod 7 \end{cases}$$

Soln exists if $\left(\frac{23}{7}\right) = 1$.

$\left(\frac{2}{7}\right) = 1$ $\left[\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}\right]$.

$\therefore$ Soln exists.

Step I. Find initial soln x_0

$x_0 = 3$

Formula to find b.

* $x_0^2 = a + bp^k$.

$a = 23$ $x_0 = 3$

For step 1 $k = 1$.

$p = 7$.

$3^2 = 23 + b7^1$

$b = -2$

Formula to find y_0

* $2x_0y_0 \equiv -b \pmod p$

$2 \cdot 3 \cdot y_0 \equiv 2 \pmod 7$

$6y_0 \equiv 2 \pmod 7$

$\gcd(2, 7) = 1$

Cancellation law divide by 2.

$3y_0 \equiv 1 \pmod 7$

$y_0 = 5$

$x_1 = x_0 + y_0p^k$

$x_1 = 3 + 5 \cdot 7 = 38$

-38 also a soln.

① $x_0^2 = a + bp^k$.

$k = 1$.

$b = -2$.

y_0.

$2x_0y_0 \equiv -b \pmod p$.

$y_0 = 5$

$x_1 = x_0 + y_0p^k$

$x_1^2 = a + bp^k$

$$\begin{array}{r} 62 \\ 38 \\ \times 38 \\ \hline 304 \\ 114\times \\ \hline 1444 \\ -49 \\ \hline 1395 \end{array}$$

Note:- If Ques is to solve

$$x^2 \equiv 23 \pmod{7^3}$$

we find $x_1 = 38$ then

Step 2:

To find b.

$$x_1^2 = a + b.7^2$$

$$38^2 = 23 + b.49.$$

$$b = 29.$$

To find y_1

$$2x_1.y_1 \equiv -b \pmod{p}$$

$$2.38\, y_1 \equiv -29 \pmod{7}$$

$$76\, y_1 \equiv -29 \pmod{7}$$

$$\cancel{y_1 = 5}. \quad y_1 = 1.$$

So, $x_2 = x_1 + y_1 p^k$.

$$x_2 = 38 + 1.7^2$$

$$= 38 + 49$$

$$x_2 = 87$$

-87 also a solution.

$x^2 \equiv 23 \pmod{7}$ $\qquad x_0 = 3$

$x^2 \equiv 23 \pmod{7^2}$. $\qquad x_1 = 38$

$x^2 \equiv 23 \pmod{7^3}$ $\qquad x_2 = 87$.

3 ques - 1 mark 2 ques - 2 marks → 7 marks total.

classmate Date Page

Thm^n. Let a be an odd integer and $p = 2$, then

a) $x^2 \equiv a \pmod 2$ always has a soln.

b) $x^2 \equiv a \pmod{2^2}$ has a solution if $a \equiv 1 \pmod 4$

c) $x^2 \equiv a \pmod{2^n}$, $n \geq 3$ has a solution if $a \equiv 1 \pmod 8$

Solution is;

$$x_0^2 = a + b2^n$$

$$x_0 y_0 \equiv -b \pmod 2$$

$$x_1 = x_0 + y_0 2^{n-1}$$

Thm^n. Let $n = 2^{k_0} \cdot p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$

be prime factorization of $n > 1$ & g.c.d $(a, n) = 1$

Then $x^2 \equiv a \pmod n$ is solvable if

a) $\left(\frac{a}{p_i}\right) = 1$ for $i = 1, 2 \dots r$

b) $a \equiv 1 \pmod 4$ if $4 | n$ but $a \equiv 1 \pmod 8$ if $8 | n$ → not sure.

Ques. Show, $x^2 \equiv 5 \pmod 8$ has no solution but $x^2 \equiv 5 \pmod 4$ has a solution.

$x^2 \equiv 5 \pmod 8$

$x^2 \equiv 5 \pmod{2^3}$.

$5 \not\equiv 1 \pmod 8$

Hence no solution.

$x^2 \equiv 5 \pmod 4$

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

By Thm^n. $a \equiv 1 \pmod 4$

$5 \equiv 1 \pmod 4$ ✓

Hence Solution exists.

Ques. Find whether soln. exists or not for:

ⓐ $x^2 \equiv 17 \pmod{16}$

$16 = 2^4$.

$17 \equiv 1 \pmod 8$ ✓

Hence solution exists.

ⓑ. $x^2 \equiv 17 \pmod{32}$.

$32 = 2^5$.

$17 \equiv 1 \pmod 8$.

Hence solution exists.

Q Solve:

$$x^2 \equiv 5 \pmod 4.$$

$a \equiv 1 \pmod 4$ $\therefore$ Solution exists.

Initial Solution

$$x_0 = 5.$$

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

Step 1. $\rightarrow$ $x_0^2 = a + b2^2$.

$25 = 5 + 4.b$

$b = 5$

$\rightarrow$ $x_0 \cdot y_0 \equiv -5 \pmod 2$

$5y_0 \equiv -5 \pmod 2$

$y_0 = 1$

$\rightarrow$ $x_1 = x_0 + y_0 2^{n-1}$

$= 5 + 1 \cdot 2^1$

$= 5 + 2 = \underline{\underline{7}}$

Solution exis

Other solution is -7

15th Dec '13. Type 3:

Ex. $x^2 + 5x \equiv 12 \pmod{31}$

Using:

* $(2ax+b)^2 \equiv (b^2-4ac) \pmod p$

$ax^2+bx+c \equiv 0 \pmod p$

$a = 1 \quad b = 5 \quad c = -12$

$\downarrow$

$(2.1.x+5)^2 \equiv (5^2 - 4.1.(-12)) \pmod{31}$

$(2x+5)^2 \equiv (25+48) \pmod{31}$

$(2x+5)^2 \equiv (73) \pmod{31}$

If $2x+5 = y$

$y^2 \equiv (73) \pmod{31}$

$\left(\frac{73}{31}\right) = \left(\frac{p}{q}\right) = \left(\frac{11}{31}\right) = -\left(\frac{31}{11}\right) = -\left(\frac{9}{11}\right)$

$p \equiv 3 \pmod 4$ ✓

$31 \equiv 3 \pmod 4$ ✓ } Both true $= -\left(\frac{a^2}{p}\right)$

$= -1$

$\downarrow$

No solution exists.

$9 \equiv -4 \pmod{13}$

Ex. $5x^2 - 6x + 2 \equiv 0 \pmod{13}$

$a = 5 \quad b = -6 \quad c = 2.$

$(2ax+b)^2 \equiv (b^2 - 4ac) \pmod{13}$

$(10x - 6)^2 \equiv (36 - 4.2.5) \pmod{13}$

$(10x-6)^2 \equiv (-4) \pmod{13}.$

$y = 10x - 6$

$\longrightarrow y^2 \equiv (-4) \pmod{13}$ or $y^2 \equiv 9 \pmod{13}$ ($9 \equiv -4 \pmod{13}$)

$\left(\frac{a}{c}\right) = \left(\frac{-4}{13}\right)$

$= \left(\frac{-1}{13}\right)\left(\frac{4}{13}\right)$

$(-1)^{p-1/2} \qquad \frac{a^2}{p} = 1$

$(-1)^{12/2} = (-1)^6$

$= 1 . 1$

$= \underline{\underline{1}}$ Solution exists.

$\left(\frac{9}{13}\right)$

$\left(\frac{a^2}{p}\right) = 1.$

One of the solution

$\boxed{y = 3.}$

Other solution

$\boxed{p - x_0 = 13 - 3 = 10.}$ (x_0 ↓ y_0)

*. Now solution is found from

$\boxed{2ax \equiv y - b \pmod{p}}$ (y → Initial Soln.)

$2.5.x \equiv 3 + 6 \pmod{p}$

$10x \equiv 9 \pmod{13}. \quad$ — (A)

Other Soln.

$10x \equiv 10 + 6 \pmod{13}$

$10x \equiv 16 \pmod{13} \quad$ — (B)

Initial soln for (A) $x = 10$ } Diophantine equation.
(B) $x = 13$

Formula Used :-

$$(2ax+b)^2 \equiv (b^2-4ac) \pmod{p}$$

Let $y = 2ax+b$

$$2ax \equiv (y-b) \pmod{p}$$

y is initial soln.

$\to y_0$

$p - y_0$

13th Dec.'13.

Continued Fractions.

Defn:- Continued Fraction $\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\cdots \cfrac{1}{a_n + \cfrac{1}{a_{n+1}}}}}}}$

$a_0 \to$ integer

All a_i's integer.

If it ends at 'n' $\to$ Finite Continued Fraction.

If all a_i's are integer the fraction is called Simple Continued Fraction.

$$\frac{111}{345} = \frac{1 + \frac{1 + 1/5}{4}}{3}.$$

Solving

$$= [a_0 ; a_1 ; a_2 \dots ; a_{n+1}]$$

Can be used to find square root of numbers & solve diophantine eq^{n}s.

eg $\sqrt{13} = 3 + \cfrac{4}{6 + \cfrac{4}{6 + \cfrac{4}{6 \dots}}}$

The value of any finite simple continued fraction will be a rational number.

Q. $\frac{23}{55}$

Basic Representation Thm^n $55 = 23 \times 2 + 9$ ① $\left(\frac{55}{23} = 2 + \frac{9}{23}\right)$ Ⓐ

Ⓐ $23 = 9 \times 2 + 5$ ② $\left(\frac{23}{9} = 2 + \frac{5}{9}\right)$ Ⓑ

Ⓑ $9 = 5 \times 1 + 4$

Ⓒ $5 = 4 \times 1 + 1$ ③ $\left(\frac{9}{5} = 1 + \frac{4}{5}\right)$ Ⓒ

④ $\left(\frac{5}{4} = 1 + \frac{1}{4} \right)$ → Stop.

Given: $\frac{23}{55} = \cfrac{1}{\frac{55}{23}}$ From ①

$= \cfrac{1}{2 + \frac{9}{23}}$

$= \cfrac{1}{2 + \cfrac{1}{\frac{23}{9}}}$ From ②

$= \cfrac{1}{2 + \cfrac{1}{2 + \frac{5}{9}}}$

$= \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{9/5}}}$ From ③

$= \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{1 + \frac{4}{5}}}}$

$= \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{5/4}}}}$ From ④

$$\frac{23}{55} = \cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{4}}}}}$$ ... Solution

$a_0 = 0$

Square Notation = $[0; 2; 2; 1; 1; 4]$

* When $Den^r > Num^r$ $a_0 = 0$

Q $\frac{2}{5}$

1. $5 = 2 \times 2 + 1$ $\quad \left(\frac{5}{2} = 2 + \frac{1}{2} \right)$

$$\frac{2}{5} = \frac{1}{\frac{5}{2}}$$

$$= \frac{1}{2 + 1/2}.$$

$[0; 2; 2]$

17th Dec, '13.

Q.2 $\frac{19}{51}$

1. $51 = 19 \times 2 + 13$ $\left(\frac{51}{19} = 2 + \frac{13}{19}\right)$

2. $19 = 13 \times 1 + 6$ $\left(\frac{19}{13} = 1 + \frac{6}{13}\right)$

3. $13 = 6 \times 2 + 1$ $\left(\frac{13}{6} = 2 + \frac{1}{6}\right)$

$$\frac{19}{51} = \cfrac{1}{\cfrac{51}{19}}$$

$$= \cfrac{1}{2 + \cfrac{13}{19}} = \cfrac{1}{2 + \cfrac{1}{\cfrac{19}{13}}}$$

$$= \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{6}{13}}}$$

$$= \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{\cfrac{13}{6}}}}$$

$$= \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{6}}}}$$

Square notation = [0 ; 2 ; 1 ; 2 ; 6]

Q3. $\frac{170}{53}$

159

1. ~~53~~ $170 = 53 \times 3 + 11$ $\quad \left(\frac{170}{53} = 3 + \frac{11}{53}\right)$

2. $53 = 11 \times 4 + 9$ $\quad \left(\frac{53}{11} = 4 + \frac{9}{11}\right)$

3. $11 = 9 \times 1 + 2$ $\quad \left(\frac{11}{9} = 1 + \frac{2}{9}\right)$

4. $9 = 2 \times 4 + 1$ $\quad \left(\frac{9}{2} = 4 + \frac{1}{2}\right)$

$$\frac{170}{53} = 3 + \frac{11}{53}$$

$$= 3 + \cfrac{1}{\frac{53}{11}} = 3 + \cfrac{1}{4 + \frac{9}{11}}$$

$$= 3 + \cfrac{1}{4 + \cfrac{1}{\frac{11}{9}}}$$

$$= 3 + \cfrac{1}{4 + \cfrac{1}{1 + \frac{2}{9}}} = 3 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{\frac{9}{2}}}}$$

$$= 3 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{4 + \frac{1}{2}}}}$$

Not Unique can be written as diff^n no.

$$= 3 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \frac{1}{1}}}}}$$

Soln: $[3; 4, 1, 4, 2]$

$= [3; 4, 1, 4, 1, 1]$

classmate
Date
Page

Simple continued fraction is not unique as if the last no. is a_n
It can be written as:

$$a_n = a_n - 1 + 1$$
$$= a_n - 1 + \frac{1}{1}$$

Not unique.

eg. $$\frac{19}{51} = \cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{6}}}} = \cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{5+\cfrac{1}{1}}}}}$$

$$[0; 2, 1, 2, 5, 1]$$

Note: If we take quotient of two successive fibonacci nos $\frac{U_{n+1}}{U_n}$ then it is represented by all 1s.

$$\frac{U_{n+1}}{U_n} = [1; 1, 1, \dots 1]$$

Ex. 1, 1, 2, 3, 5, 8, 13 ....

eg. $\frac{8}{5} =$

$8 = 5 \times 1 + 3$ $\quad (8/5 = 1 + 3/5)$

$5 = 3 \times 1 + 2$ $\quad (5/3 = 1 + 2/3)$

$3 = 2 \times 1 + 1$ $\quad (2/3 = 1 + 1/2)$.

$$= \cancel{\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+1/2}}}} \qquad 1 + \cfrac{1}{1+\cfrac{1}{1+1/2}}$$

$$= 1 + \cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1}}}}$$

$$= [1; 1, 1, 1, 1]$$

Solving diophantine equations using Continued Fraction.

Notations. C_K are continued fractions made of from cutting off the expansion after K^{th} partial denominator.

$$C_K = [a_0 ; a_1, a_2 \dots a_K]$$

where q_K is called K^{th} convergent

$$C_0 = a_0.$$

eg. $\frac{19}{51} = \cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{2+1/6}}}$ c_1, c_2, c_3

$C_0 = a_0 = 0$

$C_1 = 1/2$ $= \left(\frac{1}{2+1/1}\right)$ $(1/2)$

$C_2 = 1/3$ $= \left(\frac{1}{2+\frac{1}{1+1/2}}\right)$

$C_3 = 3/8$

$C_4 = 19/51$ Original fraction.

Thm^n.
$$\left.\begin{aligned} p_K &= a_K p_{K-1} + p_{K-2} \\ q_K &= a_K q_{K-1} + q_{K-2} \end{aligned}\right\} \text{ for } k = 2, 3 \dots n$$

where $p_0 = a_0$ $p_1 = a_1 a_0 + 1$

$q_0 = 1$ $q_1 = a_1$

and $C_K = \frac{p_K}{q_K}$ $0 \le K \le n$

For above eg. $\frac{19}{51}$. $a_0 = 0 \therefore p_0 = 0$

$p_1 = a_0 a_1 + 1 = 1$

$q_0 = 1$ $q_1 = 2$.

$C_0 = \frac{p_0}{q_0} = 0$ $C_1 = \frac{p_1}{q_1} = \frac{1}{2}$.

$p_2 = 1.1 + 0 = 1$ $C_2 = \frac{p_2}{q_2} = \frac{1}{3}$

$q_2 = 1.2 + 1 = 3$

$p_3 = 2.1 + 1 = 3$ $C_3 = \frac{3}{8}$.

$q_3 = 2.3 + 2 = 8$

$p_4 = 19 = 3.6 + 3$ $C_4 = \frac{19}{51}$

$q_4 = 51 = 6.8 + 3$

classmate

Date

Page

18th Dec '13

Method.

1. Given solve $ax+by=c$ write it as

$$ax+by=1$$

* We find continued fraction of $\frac{a}{b}$.

2. Find

$$C_{n-1} = \frac{p_{n-1}}{q_{n-1}} \text{ and } C_n = \frac{p_n}{q_n} = \frac{a}{b}$$

3. $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}$

$$a \underbrace{q_{n-1}}_{x} - b \underbrace{p_{n-1}}_{y} = (-1)^{n-1}$$

Ex Solve $43\overset{x}{\cancel{y}} + 5y = 250$.

Step 1. $43x + 5y = 1$.

Continued Fraction of $\frac{43}{5}$

$43 = 5 \times 8 + 3$ $\left(\frac{43}{5} = 8 + \frac{3}{5}\right)$

$5 = 3 \times 1 + 2$ $\left(\frac{5}{3} = 1 + \frac{2}{3}\right)$

$3 = 2 \times 1 + 1$ $\left(\frac{3}{2} = 1 + \frac{1}{2}\right)$

$$\frac{43}{5} = 8 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}}$$ [8; 1, 1, 2].

$C_0 = 8 = a_0$

$C_1 = 9$.

$C_2 = 17/2$

$C_3 = 43/5$

C_{n-2} $\quad$ C_{n-1}.

C_3 $\quad$ C_2

$\frac{43}{5}$ $\quad$ $\frac{17}{2}$ $\quad$ $n=3$

$43(2)-5(17)=(-1)^{3-1}$

$43(2)-5(17)=1$.

$(\times 250)$

$43(2\times250)-5(17\times250)=1\times250$

$\downarrow$ x $\quad$ $\downarrow$ y.

$x = 2\times250 = 500$

$y = -17\times250 = -4250$

General form:

$$\left.\begin{aligned} x &= 500+5t \\ y &= -4250-43t \end{aligned}\right\} \text{Solution.}$$

Ex. Solve. $158x-57y=1$.

Continued Fraction $\frac{158}{57}$.

$158 = 57\times2+44$ $\quad$ $\left(\frac{158}{57} = 2+\frac{44}{57}\right)$ $\frac{1}{57/44}$

$\cancel{44}$ $57 = 44\times1+13$ $\quad$ $\left(\frac{57}{44} = 1+\frac{13}{44}\right)$

$44 = 13\times3+5$ $\quad$ $\left(\frac{44}{13} = 3+\frac{5}{13}\right)$

$13 = 5\times2+3$ $\quad$ $\left(\frac{13}{5} = 2+\frac{3}{5}\right)$

$5 = 3\times1+2$ $\quad$ $\left(\frac{5}{3} = 1+\frac{2}{3}\right)$

$3 = 2\times1+1$ $\quad$ $\left(\frac{3}{2} = 1+\frac{1}{2}\right)$

38 48 $2 + \cfrac{1}{1+1/(3+1/2)}$

Continued Fraction

$$= 2 + \cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+1/2}}}}}$$

$C_0 = 2$

$C_1 = 3$

$C_2 = 11/4$

$C_3 = 25/9$.

$C_4 = \cancel{48/19}\ 36/13$

$C_5 = 61/22$

$C_6 = 158/57$

$\dfrac{61}{22} \quad \dfrac{158}{57} \qquad 6-1 \qquad (-1)^5 \quad \uparrow \times(-1)$

$-158\times(22) + 57(61) = 1$.

$x \qquad y$

$x = -22 \qquad y = -61$

General form

$$\left.\begin{aligned} x &= -22 + 57t \\ y &= -61 + 158t \end{aligned}\right\} \text{Solution}$$

Using Formula (For before eg).

$[2; 1, 3, 2, 2 1, 1, 2]$

$p_0 = a_0$ $\qquad q_0 = 1.$

$p_1 = a_1 a_0 + 1 = 1.2 + 1 = 3$

$q_1 = a_1 = 1$

$C_0 = \frac{p_0}{q_0} = 2.$

$p_2 = a_2 p_1 + p_0 = 3.3 + 2 = 11$

$q_2 = a_2 q_1 + q_0 = 3 + 1 = 4$

$C_2 = \frac{p_2}{q_2} = \frac{11}{4}.$

$p_3 = 25 \quad q_3 = 9$

$a_3 q_2 + q_1$

$a_3 p_2 + p_1$

$2.11 + 3$

$= 25$

$p_4 = a_4 p_3 + p_2$ $\qquad q_4 = 1.9 + 4$

$= 1.25 + 11$ $\qquad = 13$

$= 36$

$C_4 = \frac{36}{13}$