Quadratic congruences:

$f(x) = ax^2 + bx + c$

solve eqn: $x^2 \equiv n \mod p$ ↳ odd prime

n - non zero int $(n,p) = 1$

1 → $x^2 \equiv 1 \mod p$ has only 2 solns

$x \equiv 1 \mod p$ or $x \equiv -1 \mod p$.

2 → $x^2 \equiv -1 \mod 7$

$x \in \mathbb{Z} \longrightarrow \mathbb{Z}_7$

$x \mod 7 = r$

$x \equiv r \mod 7$

$-1 \equiv x^2 \equiv r^2 \mod 7$

$r^2 = 6 \mod 7$

$0 \to 0$
$1 \to 1$
$2 \to 4$
$3 \to 2$
$4 \to 2$
$5 \to 4$
$6 \to 1$

∴ no soln

3 → $x^2 \equiv -1 \mod 5$

has soln $x \equiv 2 \mod 5$

$x \equiv 3 \mod 5$

- FACT: $x^2 \equiv n \mod p$ will have atmost 2 solutions mod p.

4 → $x^2 \equiv 1 \mod 8$

$x \equiv \pm 1 \mod 8$
$x \equiv \pm 3 \mod 8$
$x \equiv \pm 5 \mod 8$
$x \equiv \pm 7 \mod 8$

} 4 solns

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

Here 1, 2, & 4 were squares of $\pm 1, \pm 3, \pm 2$.

- If quadratic congruence

$$x^2 \equiv n \bmod p \longrightarrow (1)$$

when $n \in \mathbb{Z}$, $n \neq 0$, & p odd prime, has a soln we call n as a quadratic residue modulo p. If (1) has no soln, then we say that n is a quadratic non residue modulo p.

Ex: $n = -1$ is a qr modulo 5 but qnr modulo 7.

nRp - qr modulo p

$n\bar{R}p$ - qnr modulo p.

$-1\ R\ 5$ & $-1\ \bar{R}\ 7$

Q) Find out QR modulo 11.

	QR	QNR
10, 1	1	2
9, 2	4	6
8, 3	9	7
7, 4	5	8
6, 5	3	10

- **Theorem:** Let p be an odd prime. Then every reduced residual system modulo p contains exactly $\frac{p-1}{2}$ quadratic residues & exactly $\frac{p-1}{2}$ quadratic non residue mod p.

~~$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2$~~

→ The qr belong to the residue classes containing the nos $1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2$

- **Theorem:** show that if $1 \leq k \leq \frac{p-1}{2}$ then

$$k^2 \equiv (p-k)^2 \bmod p$$

$$k^2 - (p-k)^2 \equiv (k+p-k)(k-p+k) = p(2k-p)$$

$$p \mid k^2 - (p-k)^2 \implies k^2 \equiv (p-k)^2 \bmod p$$

- **Legendre's Symbol:**

Let p be a odd prime., Let $n \neq 0$

we define symbol $\left(\frac{n}{p}\right)$ as follows:

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n R p \\ -1 & \text{if } n \bar{R} p \\ 0 & p \mid n \end{cases}$$

$\left(\frac{-1}{5}\right) = 1$; $\left(\frac{m^2}{p}\right) = 1$;

$\left(\frac{7}{11}\right) = -1$ as QR modulo 11 (are 1, 4, 9, 5, 3)

$\left(\frac{22}{11}\right) = 0$

$\left(\frac{18}{4}\right) = -1$

Properties of Legendre's symbol: $p \in$ $p \mid 223$ Then

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

② $\rightarrow \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

③ $n \equiv n \bmod p \rightarrow \left(\frac{m}{p}\right) = \left(\frac{n}{p}\right)$

$\rightarrow$ if a & b are congruent modulo p ie $a \equiv b \bmod p$

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

④ $\rightarrow$ If $(a, p) = 1$ then $\left(\frac{a^2}{p}\right) = 1$ &

$\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$

⑤ $\rightarrow \left(\frac{1}{p}\right) = 1$

$\rightarrow \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ ~~mod p~~

$\rightarrow \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$

Page No.
Date

Ex: $p=7,\ a=-1$

$\left(\frac{-1}{7}\right) = -1$ ∫ (1) (5) mod p

Ex:

$\rightarrow \left(\frac{20}{7}\right) = \left(\frac{-1}{7}\right) = \underline{-1}$

$\rightarrow \left(\frac{20}{7}\right) = \left(\frac{4\times5}{7}\right) = \left(\frac{2^2\times5}{7}\right) = \left(\frac{5}{7}\right) = \underline{-1}$

$\rightarrow x^2 \equiv 2\ (7)$

$\left(\frac{2}{7}\right) = -1^{49-1/8} = -1^6 = \underline{1}$

Q) $x^2 \equiv 219 \mod 383$

To show $\left(\frac{219}{383}\right) = 1$

- Quadratic reciprocity Law:

Let p & q be odd primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left[\frac{p-1}{2}\cdot\frac{q-1}{2}\right]}$$

$\rightarrow \frac{219}{383} = \left(\frac{73\times3}{383}\right) = \left(\frac{73}{383}\right)\left(\frac{3}{383}\right) = 1\times1 = \underline{1}$

$\therefore$ 219 is a square

$\left(\frac{73}{383}\right)\left(\frac{383}{73}\right) = -1^{72\times382/4} = \underline{1}$

$\Rightarrow \left(\frac{73}{383}\right) = \left(\frac{383}{73}\right) = \left(\frac{18}{73}\right) = \left(\frac{21}{73}\right) = \underline{1}$

$\left(\frac{3}{383}\right)\left(\frac{383}{3}\right) = -1^{2\times382/4} = \underline{-1}$ (div algo) $\left(\frac{a^2b}{p}\right)$ a^2/p

$\Rightarrow \left(\frac{3}{383}\right) = -\left(\frac{383}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = \underline{1}$

$\because 2 \not\equiv 3$

pr 1.) Given odd prime p, find all n that are quadratic residues modulo p.

pr 2) Given $n \neq 0$ find out all odd primes p for which n is a quadratic residue modulo p.

Ex 1: Determine those odd primes p for which 3 is a Q.R.

- Extension of Legendre symbol: Jacobi symbol

If p is a +ve odd int with

$$p = \prod_{i=1}^{r} p_i^{\alpha_i} \quad r \geq 1, \ \alpha_i \geq 1$$

we define Jacobi symbol as $\left(\frac{n}{p}\right) = \prod_{i=1}^{r} \left(\frac{n}{p_i}\right)^{\alpha_i}$

CM:

$f(mn) = f(m) f(n)$

$f(n) = n^q$

M:

if $(m,n) = 1$

then

$f(mn) = f(m) f(n)$

Ex: $f(n) = \phi(n)$

- Properties:

P, Q are odd & +ve then:

a) (Periodicity) If $m \equiv n \bmod p$ then

$$\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right)$$

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

c) $\left(\frac{n}{PQ}\right) = \left(\frac{n}{p}\right)\left(\frac{n}{Q}\right)$ (completely multiplicative in denominator)

d) $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$ if $(a,p) = 1$ or $(p \nmid a)$

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

f) $\left(\frac{2}{p}\right) = (-1)^{p^2-1/8} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 8 \\ -1 & \text{if } p \equiv \pm 3 \bmod 8 \end{cases}$

Page No.
Date

Restart:

$\left(\frac{a}{p}\right) = +1 \longrightarrow$ a is residue mod p. $\exists$ x such that $x^2 \equiv a \bmod p$.

- To find x: Find sq root of a mod p. (p - odd prime)

$p - 1 = 2^{\alpha} \cdot s$ ($s \to$ odd)

Select a non residue mod p, say n.

Let $b = n^s$

$r = a^{(s+1)/2}$

claim: $r^2 \cdot a^{-1}$ is $2^{\alpha-1}$ th root of unity.

Infact $(r^2 a^{-1})^{2^{\alpha-1}} = \left(\left(a^{\frac{(s+1)}{2}}\right)^2 a^{-1}\right)^{2^{\alpha-1}} = a^{s \cdot 2^{\alpha-1}} = a^{\frac{p-1}{2}} \bmod p$

$= \left(\frac{a}{p}\right) = 1$ ($\because$ a is residue)

claim: $b^{2^{\alpha}} = 1$

Infact $b^{2^{\alpha}} = n^{s 2^{\alpha}} = n^{p-1} \equiv 1 \bmod p$

To find $x = b^j r$ for some j such that $x^2 \equiv a \bmod p$

Write $j = j_0 + 2j_1 + 2^2 j_2 + \cdots + 2^{\alpha-2} j_{\alpha-2}$, where $j_0, j_1, \ldots j_{\alpha-2}$ are either 0 or 1. (binary rep of j)

To find j:

1. We find & have $(r^2 a^{-1})^{2^{\alpha-1}} = +1$

$\Rightarrow (r^2 a^{-1})^{2^{\alpha-2}} = \begin{cases} +1 \\ -1 \end{cases}$

Take $j_0 = 1$ if above is -1. Take $j_0 = 0$ if above is $+1$.

ie, we take j_0 such that

$$\left[\left(b^{j_0} r\right)^2 \cdot a^{-1}\right]^{2^{\alpha-2}} = +1$$

2. $\left[\left(b^j r\right)^2 a^{-1}\right]^{2^{\alpha-3}} = \begin{cases} +1 \\ -1 \end{cases}$

Take $j_1 = \begin{cases} 0 \\ 1 \end{cases}$, resply so that $\left[\left(b^{j_0 + 2j_1} r\right)^2 \cdot a^{-1}\right]^{2^{\alpha-3}} = +1$

3. Suppose we found $j_0, j_1, j_2 \cdots j_{k-1}$ such that

$$\left[\left(b^{j_0+2j_1+\cdots+2^{k-1}j_{k-1}} r\right)^2 a^{-1}\right]^{2^{\alpha-k-1}} = +1$$

$$\Rightarrow \left[\left(b^{j_0+2j_1+\cdots+2^{k}j_{k-1}} r\right)^2 a^{-1}\right]^{2^{\alpha-k-2}} = \begin{cases} +1 \\ -1 \end{cases}$$

Take $j_k = \begin{cases} 0 \\ 1 \end{cases}$ resply.

$$\left[\left(b^{j_0+2j_1+\cdots+2^{k}j_{k}} r\right)^2 a^{-1}\right]^{2^{\alpha-k-2}} = +1$$

when $k = \alpha-2$, we get

$$\left(b^j r\right)^2 a^{-1} = 1$$

$$(b^j r)^2 \equiv a \bmod p$$

$$\Rightarrow \boxed{x = b^j r}$$

Ex: Find sqrt of 302 mod 2081

$a = 302$, $p = 2081$

find $x = b^j r$ so that $x^2 \equiv a \bmod p$.

$b = n^r$, $p - 1 = 2^\alpha \cdot s$ $\quad n \to$ non residue.

$\left(\frac{2}{2081}\right) = +1 \Rightarrow 2$ is a remainder

$\left(\frac{3}{2081}\right) = \left(\frac{2081}{3}\right)\left(\frac{2}{3}\right) = -1$ $\quad \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ when $p \nmid q$ both $\equiv 3 \bmod 4$

$\Rightarrow 3$ is non residue.

we get; $s = 65$ & $\alpha = 5$

$\therefore b = 3 \bmod 2081$

$r = \frac{66}{a^{2^{i+1}}} = a^{33} = (302)^{33} \bmod 2081$

$p = 2081$, $a = 302$

$p - 1 = 2^s \cdot s$ (s odd)

$b = n^s$ (n - non residue)

$r = a^{(s+1)/2}$.

$(r^2 a^{-1})^{2^{\alpha-2}}$

$j = j_0 + 2 j_1 + \cdots + 2^{\alpha-2} j_{\alpha-2}$

$x = b^j r$.

$p - 1 = 2080 = 2^5 \cdot 65$

$s = 65$ & $\alpha = 5$

$n \neq 2$

$n = 3$ $\left(\because \left(\frac{3}{p}\right) = -1\right)$

$b = 3^{65} \bmod 2081 = 888 \bmod 2081$

$r = a^{33} = (302)^{33} = \underline{203}$

$302 \equiv 1 \bmod 2081$

To find j_0:

$[r^2 a^{-1}]^{2^3} = [(203)^2 \times 820]^8 = +1$

$2081 = 302 \times 6 + 269$

$302 = 269 + 33$

$269 = 33 \times 8 + 5$

$33 = 5 \times 6 + 3$

$5 = 3 \times 1 + 2$

$3 = 2 \times 1 + 1$

$1 = 3 - 2$

$= 3 - (5 - 3)$

$= 2 \cdot 3 - (33 - 5 \times 6)$

$= 2 \cdot 3 - 33 + 6 \cdot 5$

$= 2 \cdot 3 - 33 + 6 \cdot (269 - 33 \times 8)$

$= 2 \cdot 3 - 49 \cdot 33 + 6 \cdot 269$

$= 2 \cdot 3 - 49 (302 - 269) + 6 \cdot 269$

$= 2 \cdot 3 + 55 \cdot 269 - 49 \cdot 302$

$\therefore 302^{2080} \equiv 1 \bmod 2081$

$j_0 = 0$

$[r^2 a^{-1}]^4 = +1 \Rightarrow j_1 = 0$

$[r^2 a^{-1}]^2 = 2080 = -1$

$\Rightarrow j_2 = 1$

$\left(\left(b^{j_0 + 2j_1 + 2^2 j_2}\right)^2 a^{-1}\right)^{2^0}$

$= \underline{+1}$

$j = 4$

Soln $x = b^j r = 888^4 \times 203$

$a^{-1} = 820$

Ex. Find soln of $a = 186 \bmod p = 401$

$p - 1 = 400 = 2^4 \times 25$ $(\alpha = 4, s = 25)$

$\left(\frac{2}{p}\right) = \left(\frac{2}{401}\right) = 1$ $\left(\frac{3}{p}\right) = \left(\frac{3}{401}\right) = \left(\frac{401}{3}\right) = \left(\frac{2}{3}\right) = -1$

$\Rightarrow n = 3$

$b = n^s = 3^{25} = 268$ non squares

$r = a^{(s+1)/2} = 186^{13} = 103$

$a^{-1} = 186^{-1} = 235$

$j = j_0 + 2 j_1 + 2^2 j_2$ $\left(\because \alpha = 4,\ \alpha - 2 = 2\right)$

Find j_0:

$$\left[r^{\frac{2}{q}-1}\right]^2 = \left(103^2 \cdot 235\right)^4 = (98)^4 \bmod 401 \equiv -1.$$

$\rightarrow j_0 = 1$

$$\therefore \left(b^{j_0} \frac{g}{r}\right)^{\frac{2}{q}-1} = \left((208 \times 103)^2 \times 233\right) \equiv -1$$

$\vdots$

$j_1 = 0$

- **Binary quadratic forms:**

$x^2+y^2=n$

1) → A homogeneous polynomial of deg 2 is called a quadratic form.

Ex: $x^2+2y^2+3xy+5yz+12z^2$

2) A quadratic form in 2 variables is called binary quadratic form

Ex: $f(x,y)=x^2+y^2+3xy$

Non ex: $f(x)=x^2+2x+1$

In general a binary quadratic form $f(x,y)=ax^2+bxy+cy^2$ (+)

$a,b,c \Rightarrow$ constants. integers.

- **Discriminant of BQF:**

Let $f(x,y)$ be *, be an integral BQF. Define discriminant of f

$$d=b^2-4ac$$

If d is a perfect square, then f can be written as product of 2 linear forms.

ie $f(x,y)=(h_1x+k_1y)(h_2x+k_2y)$ (Ex 7-10, Niven)

- **Matrix representation of a BQF:**

$f(x,y)=ax^2+bxy+cy^2$ as

$$M_f=\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \qquad \text{Let } X=\begin{pmatrix} x \\ y \end{pmatrix}$$

$$X^T\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}X=\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

$$(x,y)$$

$$\Rightarrow \left[ax+\frac{by}{2}, \frac{bx}{2}+yc\right]\begin{pmatrix} x \\ y \end{pmatrix}$$

$$=ax^2+\frac{bxy}{2}+\frac{bxy}{2}+y^2c$$

$$\Rightarrow ax^2+bxy+cy^2=f(x,y)=f(X)$$

$$\boxed{X^T M_f X=f(x) \quad \forall\ X\in\mathbb{Z}^2}$$

- Eigen values of 2 quadratic forms:

Let f & g be 2 BQF forms. We say f is equivalent to g iff there $\exists A \in SL_2(\mathbb{Z})$ such that

$g(x) = f(Ax) \quad \forall \quad X = \begin{pmatrix} x \\ y \end{pmatrix} \quad x, y \in \mathbb{Z}$

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; ad - bc = 1 \quad a,b,c,d \in \mathbb{Z} \right\}$$

Alternate, we say $f \sim g$ iff

$\exists\ A \in SL_2(\mathbb{Z})$ st.

$$\boxed{M_g = A^t M_f A}$$

Q) Show that $f(x,y) = x^2 + y^2$

$g(x,y) = x^2 - 2xy + 2y^2$. $\Rightarrow f \sim g$

$M_f = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $M_g = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}$

Find $A \in SL_2(\mathbb{Z})$ st.

$M_g = A^T M_f A$

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow A^T A \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}^T \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$= \begin{pmatrix} a^2+c^2 & ab+cd \\ ba+dc & b^2+d^2 \end{pmatrix} = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}$

$\Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$

$a^2 + c^2 = 1 \Rightarrow a = 1$

$ab + cd = -1$, $b^2 + d^2 = 2$, $ad - bc = 1$

$\therefore f \sim g$

way 2: $f(x-y, y) = (x-y)^2 + y^2 = g(x,y)$

$\begin{pmatrix} x-y \\ y \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}$

$\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{bmatrix} x-y \\ y \end{bmatrix}$

$A \quad \Rightarrow \quad X$

Q) is $g \sim f$?

$f(x-y, y) = (x-y)^2 + y^2$

$= g(x,y)$

$M_g = A^T M_f A$

$(A^T)^{-1} M_g = M_f \cdot A$

$(A^{-1})^T M_g A^{-1} = M_f$

Q Show that $f \sim g$ is an equivalence relation.

1) $f \sim f$ (reflexive)

Since $A = Id$ satisfies $f(X) = f(AX)$

2) symmetric:

given $f \sim g$ st $g \sim f$.

ie ~~$M_g = A^T$~~ given that $\exists A \in SL_2(\mathbb{Z})$ st.

$M_g = A^T M_f A$ we need to find $B \in SL_2(\mathbb{Z})$ st.

$M_f = B^T M_g B$

(exercise)

3) Transitive:

$f \sim g$ & $g \sim h$ st $\Rightarrow f \sim h$

ie there exists A, B in $SL_2(\mathbb{Z})$ st.

$M_g = A^T M_f A$

& $M_h = B^T M_g B$

$M_h = B^T (A^T M_f A) B$

$= B^T A^T M_f A B$

$= (AB)^T M_f (AB)$

$\therefore f \sim h$.

- Discriminant: $b^2 - 4ac$ $\quad d \equiv b^2 \bmod 4$

$d \equiv 0, 1 \bmod 4$

~~(b+a)(b-d) mod 4 =~~

- **Applications of Cryptography:**

Cryptography
- Symetric key / pvt key cryptography
- asymetric key cryptography / Public key crypto system
  - Ex: RSA

- **RSA:**

A — Public: K, m — B

message: a

② $a^K \bmod m$

④ b

$(\log b = K \log a)$

it is difficult to rapture 'a' from b (encrypted message)

b released in public domain

difficult for public to find a from b as $\phi(m)$ is not easy to calculate.

① $m = pq$
$m \rightarrow$ very huge no.
$\phi(m) = (p-1)(q-1)$.

② $1 < K < \phi(m)$
generally choose $(K, \phi(m)) = 1$

K, m are publicly available

③ Find $k^{-1} \bmod \phi m$

⑤ $b^{k^{-1}} \bmod m$.
$=$
$a \bmod m$

- **Lemma:**

Suppose that m is a +ve int & let $a \in \mathbb{Z}$ such that $(a, m) = 1$. If k is a +ve int such that it is coprime to $\phi(m)$ then $a^{kk'} \equiv a \bmod m$.

Proof: Since $(k, \phi(m)) = 1 \; \exists \; k^{-1} \in \mathbb{Z}$ such that
$kk^{-1} \equiv 1 \bmod \phi(m) \Rightarrow \phi(m) \mid kk^{-1} - 1$.
$\Rightarrow kk^{-1} = 1 + t\phi(m)$ for some $t \in \mathbb{Z}$

residue
$a^{kk^{-1}} = a^{1 + \phi(m)t} = a(a^{\phi(m)})^t \equiv a \cdot 1^t \bmod m$

$(a, m) = 1 \Rightarrow a^{\phi(m)} \equiv 1 \bmod m$ (Euler's thm)

$a \bmod m$

Q1.) Suppose $b \equiv a^{67} \bmod 91$ & $(a, 91) = 1$. Find a +ve no h such that $b^h \equiv a \bmod 91$.

Ans: To find $k^{-1} \bmod \phi(m)$ $\quad k = 67$

$m = 91$, $\phi(m) = 12 \times 6 = 72$

$k^{-1} \equiv 43 \bmod 72$

Now, if $b = 53$ what is $a \bmod 91$

$a \equiv 53^{43} \bmod 91$

$53^{72} \equiv 1 \bmod 91$

$53^{36} \equiv \pm 1 \bmod 91$.

$43 = 32 + 8 + 2 + 1$

$53^{43} = (53)^{32} (53)^{8} (53)^{2} 53 \bmod 91$

$53^2 \equiv 79 \equiv -12 \bmod 91$

$53^4 \equiv 53 \bmod 91$

$53^8 \equiv 1 \bmod 91$

$53^{43} = 53^{8 \times 14 + 1} \equiv (53^8)^{14} \cdot 53 \bmod 91 \equiv 53 \bmod 91$

answer

$72 = 67 \times 1 + 5$

$67 = 13 \times 5 + 2$

$5 = 2 \times 2 + 1$

$1 = 5 - 2 \times 2$

$= 5 - 2(67 - 5 \times 13)$

$= 27 \cdot 5 - 2 \cdot 67$

$= 27 \cdot (72 - 67) - 2 \cdot 67$

$= 27 \cdot 72 - 29 \cdot 67$

$k^{-1} = 43$

Let $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ be a reduced class mod m.
Let $k \in \mathbb{N}$, $k > 1$
$\{r_1^k, r_2^k, \ldots, r_{\phi(m)}^k\}$

Theorem 2: Let k & m be natural numbers & let $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ be an RRS. Then
$\{r_1^k, r_2^k, \ldots, r_{\phi(m)}^k\}$ is an RRS mod m.
$\iff (k, \phi(m)) = 1$

proof of $\Leftarrow$ direction.

It is enough to show that $r_1^k, r_2^k, \ldots, r_{\phi(m)}^k$ are incongruent modulo m.

We prove by contradiction. Suppose $i \neq j$ be such that

$r_i^k \equiv r_j^k \bmod m$. $(r_i^k)^{k'} \equiv (r_j^k)^{k'} \bmod m \; \forall k'$

Since $(k, \phi(m))$ are coprimes $\exists$ k' an int such that

$kk' \equiv 1 \bmod \phi(m)$

$\Rightarrow (r_i^k)^{k'} = (r_j^k)^{k'}$ modulo m

$\Rightarrow r_i \equiv r_j$ modulo m. But this is not possible.

Hence proved

- Jacobi symbol:

Quadratic residue $x^2 \equiv n \bmod p$

p = odd prime & p is odd +ve.

If $p = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $\alpha_i \geq 1$

so factorization of p into primes powers then we had defined Jacobi symbol as:

$$\left(\frac{n}{p}\right) = \prod_{i=1}^{r} \left(\frac{n}{p_i}\right)^{\alpha_i}$$

1) $\left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = \left(\frac{mn}{p}\right)$ (multiplicative wrt numerator)

2) $\left(\frac{n}{P}\right)\left(\frac{n}{Q}\right) = \left(\frac{n}{PQ}\right)$ (" wrt denominator)

Note that $(n,p) > 1$, then $\left(\frac{n}{p}\right) = 0$

3) $\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right)$ if $m \equiv n \bmod p$

(periodicity)

4) $\left(\frac{a^2 n}{p}\right) = \left(\frac{n}{p}\right)$ if $(a,p) = 1$

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

6) $\left(\frac{2}{p}\right) = -1^{\frac{p^2-1}{8}}$ → 1 if $p \equiv \pm 1 \bmod 8$; -1 if $\pm 3 \bmod 8$

$\left(\frac{n}{p}\right) = 1 \Rightarrow x^2 \equiv n \bmod p$ has soln if p = prime

$\left(\frac{n}{p}\right) = 1 \not\Rightarrow x^2 \equiv n \bmod p$

Ex: $x^2 \equiv 2 \bmod 15$. has no soln but $\left(\frac{2}{15}\right) = 1$

Quadreciprocity

$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = -1^{\left[\left(\frac{P-1}{2}\right)\left(\frac{Q-1}{2}\right)\right]}$

1. Determine if 888 is quad. residue or not mod 1999.

if we show $\left(\frac{888}{1999}\right) = -1$ then no soln.

$= \left(\frac{8}{1999}\right)\left(\frac{111}{1999}\right) = \left(\frac{2^2 \times 2}{1999}\right)\left(\frac{3 \times 37}{1999}\right)$

$= \left(\frac{2}{1999}\right)$ ~~$\left(\frac{3}{1999}\right)\left(\frac{37}{1999}\right)$~~

$= \left(\frac{111}{1999}\right)$ $\left(\frac{1999}{111}\right)$

$\left(\frac{888}{1999}\right) = -\left(\frac{1999}{111}\right) = -\left(\frac{1999}{37}\right)\left(\frac{1999}{3}\right) = -1^{(999 \times 55)} = -1$

$\Rightarrow \left(\frac{888}{1999}\right) = -1 \Rightarrow$ no soln

---

Q) $x^2 \equiv 10 \bmod 127$

$\left(\frac{10}{127}\right) = \left(\frac{5 \times 2}{127}\right)$

3.6.9
4 8

If n sets contain n+1 or more distinct elements in total then atleast 1 of the sets contains 2 or more elements.

Combinatorial N.T:

→ Pigeon hole principle
→ Inclusion exclusion principle.

1. ~~a ≡ b mod m~~ Given any m+1 ints $n \in N$ prove that 2 can be selected out of those whose diff is a multiple of m.
Note that there are m distinct residue classes mod m & by PHP, 2 int must be in same residue class i.e
$i \neq j$ $a_j \equiv a_i \mod m$
$m \mid a_j - a_i$

2. Given any m ints $a_1, a_2 \ldots a_m$ pt a non empty subset of these can be selected whose sum is mult of m.

Given m+1 ints, ∃ b_i & b_j such that $m \mid b_i - b_j$.
$S = \{0, a_1, a_1 + a_2, \ldots a_1 + a_2 + \ldots + a_m\}$
let $b_i = a_1 + a_2 \ldots a_{i-1} + a_i$
$b_j = a_1 + a_2 \ldots + a_j$
i.e $m \mid a_{j+1} \ldots + a_i$
that is a subset of $\{a_1, a_2 \ldots a_m\}$ whose sum is a multiple of m is $\{a_{j+1} \ldots a_i\}$

Q) Find no of int in set $\{1, 2, 3 \ldots 6300\}$ that are divisible by neither 3 nor 4.
$n(S_3) = 2100$
$n(S_4) = 1575$
$n(S_{12}) = 525$
Total = 2100 + 1575 − 525 = 3150 ⟹ Multiples
⟹ 6300 − 3150 = 3150

Seen 06/11/24

4

Page No.
Date

Arithmetic func:

Ex: $\phi(n)$, $f(n) = n$
Any func f defined on set of rational nos is called an arithmetic functions.

Mobius func:
$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } p^2 \mid n \text{ for some } p \\ -1^k & \text{if } n = p_1 p_2 \ldots p_k \text{ for some } k \geq 1 \end{cases}$$

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

$\mu(n) = 0 \iff n$ has a square factor (greater than 1)

$$\mu_{36} = \sum_{\substack{1 \leq d \leq 36 \\ d \mid 36}} \mu(d)$$

1	−1	−1	0	1	0	0	0	0
1	2	3	4	6	9	12	18	36

• Theorem 1: If $n \geq 1$
$$\sum_{\substack{1 \leq d \leq n \\ d \mid n}} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$
$d \mid n = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$ $\quad 0 \leq \beta_i \leq \alpha_i$
Now consider $\mu(d) = 0$ if atleast
Now $\sum_{\substack{1 \leq d \leq n \\ d \mid n}} \mu(d) = \mu(1) + \mu(p_1) + \mu(p_2) \ldots + \mu(p_k)$
$+ \mu(p_1^2) + \mu(p_1 p_2) \ldots + \mu(p_{k-1})$
$\ldots + \mu(p_k^2)$
$+ \mu(p_1^2 p_2) + \ldots$
$\mu(p_1^{\alpha_1} \ldots p_k^{\alpha_k})$

$$\sum_{\substack{d \mid n}} \mu(d) = 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \binom{k}{3}(-1)^3 + \dots + \binom{k}{k}(-1)^k = (1-1)^k = 0$$

$$(1+x)^n = 1 + \binom{n}{1}x + \binom{n}{2}x^2 \dots \binom{n}{n}x^n$$

In case $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, k is no of dist prime divisors of n.

Divisor func:

$d(n)$ = no of divisors of n $= \sum_{\substack{d \mid n \\ 1 \le d \le n}} 1$

$\sigma(n)$ = sum of divisors of n $\sum_{\substack{1 \le d \le n \\ d \mid n}} d$

$\sigma(12) = 1+2+3+4+6+12 = 28$

$d(12) = \underline{6}$

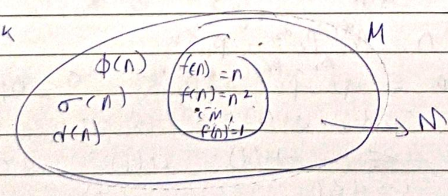
- **Multiplicative func:**

$f(mn) = f(m)f(n)$ if $(m,n) = 1$ $\qquad \phi$ is this

- **Completely multiplicative func:**

$f(mn) = f(m)f(n)$ whether m, n coprime or no

Ex: $f(n) = n^k$



$n = 12$

1, 5, 7, 11	2, 10	9, 3	4, 8	6	12
(gcd) $d = 1$	$d = 2$	$d = 3$	$d = 4$		

~~Suppose you consider~~ $\boxed{k}$

$d = 2$

$n = 12$

$2 \cdot 6$ $\qquad k = 2x$

$$\Rightarrow \phi(12) + \phi\left(\frac{12}{2}\right) + \phi\left(\frac{12}{4}\right) + \phi\left(\frac{12}{6}\right) + \phi\left(\frac{12}{12}\right)$$

Thm: For $n \in \mathbb{N}$ $\sum_{d \mid n} \phi(d) = n$

Soln: Let d be a divisor of n.

Let $A(d) = \{1 \le k \le n \mid (k,n) = d\}$

$= \{1 \le k \le n \mid (\frac{k}{d}, \frac{n}{d}) = 1\}$

$\# A(d) = \# \{1 \le k \le n \mid (\frac{k}{d}, \frac{n}{d}) = 1\}$

$\# \{1 \le \frac{k}{d} \le \frac{n}{d} \mid (\frac{k}{d}, \frac{n}{d}) = 1\}$

$= \phi(\frac{n}{d})$

$$\bigcup_{\substack{1 \le d \le n \\ d \mid n}} A(d) = \{1, 2, \dots n\}$$

$$\Rightarrow \sum_{\substack{1 \le d \le n \\ d \mid n}} \phi\left(\frac{n}{d}\right) = n$$

$$\sum_{\substack{1 \le d \le n \\ d \mid n}} \phi\left(\frac{n}{d}\right) = \sum_{d \mid n} \phi(d)$$