Sunrise 6-01 AM

Unit III : (2.8 to 2.11)

Primitive Roots and Power Residues.

Definition 2.6: Let m denote a positive integer and 'a' any integer $\ni (a, m) = 1$. Let h be the smallest positive integer $\ni a^h \equiv 1 \pmod{m}$. Then we say that the order of 'a modulo m' is h or that 'a' belongs to the exponent 'h' modulo 'm' (or) the order of a modulo m is h

Lemma 2.31: If 'a' has order 'h' $\pmod{m}$, then the positive integers $k \ni a^k \equiv 1 \pmod{m}$ are precisely those for which $h | k$.

Proof:

Assume a has order $h \pmod{m}$

If k is a +ve multiple of h,

Then $k = qh$

$\Rightarrow a^k = a^{qh} = (a^h)^q \equiv 1 \pmod{m}$ ($\because$ by defn 2.6)

Conversely, if k is a positive integer $\ni$

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

By applying the division algorithm,

Sunset 6-22 PM

we have integers q and r s.t $k = qh + r$, $q \geq 0$ & $0 \leq r < h$.

$a^k \equiv 1 \pmod{m}$; $\quad a^r \equiv 1 \pmod{m}$ (by sym)

$\Rightarrow a^{qh+r} \equiv 1 \pmod{m}$; $\quad 1 \cdot a^r \equiv 1 \pmod{m}$

$\Rightarrow (a^h)^q \cdot a^r \equiv 1 \pmod{m}$; $\quad \Rightarrow r = 0$.

But $0 \leq r < h$ & h is the least positive power of 'a' that is congruent to 1 modulo m.

$\Rightarrow r = 0 \quad \Rightarrow k = qh$.

$\Rightarrow h \mid k$

* First prove the theorem in April 23 page. *

Corollary 2.32: If $(a, m) = 1$, Then the order of 'a' modulo 'm' divides $\phi(m)$.

Proof: Each reduced residue class 'a' modulo 'm' has finite order.

By Euler's Congruence $a^{\phi(m)} \equiv 1 \pmod{m}$ $\because (a, m) = 1$

Assume a has order h

Then take $k = \phi(m)$

By Lemma 2.31 $\quad h \mid k \Rightarrow h \mid \phi(m)$

$\Rightarrow$ order of 'a' modulo 'm' divides $\phi(m)$

Sunrise 5-59 AM

Theorem : Prove before Corollary 2.32

Sunset 6-23 PM

If 'a' belongs to the exponent 'h' modulo 'm' then $h \mid \phi(m)$, further $a^j \equiv a^k \pmod m$ iff h divides $j-k$.

Proof :

(i) Given $a \in e^h \pmod m$, $(a, m) = 1$

$\Rightarrow a^h \equiv 1 \pmod m$ ——— (1)

$\Rightarrow 1 \equiv a^h \pmod m$ ——— (2)

'h' is the least positive integer

By Euler theorem, $a^{\phi(m)} \equiv 1 \pmod m$ ——— (3)

from (1) & (3) $h \leq \phi(m)$

By division algorithm $\Rightarrow qh + r = \phi(m)$, $0 \leq r < h$ ——— (4)

Sub (4) in (3)

$\Rightarrow a^{qh+r} \equiv 1 \pmod m$

$a^{qh} \cdot a^r \equiv 1 \pmod m$

$(a^h)^q \cdot a^r \equiv 1 \pmod m$

$1 \cdot a^r \equiv 1 \pmod m$ [$\because$ by (1)]

$\Rightarrow r = 0$ $\because r < h$

(4) $\Rightarrow \phi(m) = qh$

$\Rightarrow h \mid \phi(m)$ ——— (5)

Sunrise 5:58 AM

(ii) Consider $a^j \equiv a^k \pmod m$

$\Rightarrow a^j \cdot a^{-k} \equiv 1 \pmod m$

$\Rightarrow a^{j-k} \equiv 1 \pmod m$

(5) $\Rightarrow h \mid j-k$

Conversely,

Assume $h \mid j-k$

$\Rightarrow j-k = mh$ ——— (6)

Add $a^h \equiv 1 \pmod m$

$\Rightarrow a^{mh} \equiv 1 \pmod m$

$\Rightarrow a^{j-k} \equiv 1 \pmod m$

$\Rightarrow a^{j-k} \cdot a^k \equiv a^k \pmod m$

$\Rightarrow a^j \equiv a^k \pmod m$

Thus $a^j \equiv a^k \pmod m$ if $h \mid j-k$.

(*) Proof of Lemma # 2.33

$a \in e^h \pmod m$

$\Rightarrow h$ is the least +ve integer $\ni$

$a^h \equiv 1 \pmod m$ ——— (1)

Suppose $a^k \in e^j \pmod m$

To prove: $j^\circ = \frac{h}{(h,k)}$

$a^k \equiv e^{j^\circ} \pmod m$

$\Rightarrow (a^k)^{j^\circ} \equiv 1 \pmod m$

j° is the smallest such integer

$\Rightarrow a^{kj^\circ} \equiv 1 \pmod m$ ——— (2)

From (1) and (2), as h is the smallest +ve integer, we have

$h \mid kj^\circ$ ——— (3)

Let $(h,k) = d \Rightarrow d \mid h,\ d \mid k$

Let $h = h_1 d$ & $k = k_1 d$, where $(h_1, k_1) = 1$ ——— (4)

(3) & (4) $\Rightarrow h \mid kj^\circ$

$\Rightarrow h_1 d \mid k_1 d j^\circ$

$\Rightarrow h_1 \mid k_1 j^\circ$

Since $(h_1, k_1) = 1$ we get $h_1 \mid j^\circ$ ——— (5)

Consider

$(a^k)^{h_1} = a^{kh_1} = a^{k_1 d h_1} = (a^{k_1})^{dh_1}$

$$= (a^{k_1})^h$$

$$= (a^h)^{k_1}$$

$$\equiv 1 \pmod m$$

Thus $(a^k)^{h_1} \equiv 1 \pmod m$

$\Rightarrow a^k$ belongs to the exponent $h_1 \pmod m$

$\therefore j \mid h_1$ ——— (6).

(5) & (6) $\Rightarrow j = h_1$

But $h_1 = \frac{h}{d}$

$\Rightarrow j = h_1 = \frac{h}{d}$

$\Rightarrow j = \frac{h}{(h,k)}$

Hence a^k belongs to the exponent $\frac{h}{(h,k)} \pmod m$

Lemma 2.34:

If a has order $h \pmod m$, b has order $k \pmod m$ and if $(h,k) = 1$, then ab has order $(hk) \pmod m$

Proof :

If a has order $h \pmod m$ then

$$a^h \equiv 1 \pmod m, \quad (a, m) = 1$$

If b has order $k \pmod m$ then

$$b^k \equiv 1 \pmod m, \quad (b, m) = 1$$

Consider $(ab)^{hk} = a^{hk} b^{hk}$

$$= (a^h)^k (b^k)^h$$

$$\equiv 1 \bmod m$$

$\Rightarrow$ ab has order $hk \pmod m$

Primitive Root :

Definition 2.7 : If $g \in$ to the exponent $\phi(m)$ modulo m, then g is called a primitive root modulo m.

Example :

Find the primitive roots of 5.

a	a^2	a^3	a^4
1	1	1	1
2	4	8	16
3	9	27	31
4	16	64	256

Sunrise 5-56 AM

Note: If $\phi(m)$ is the smallest positive integer, show that $a^{\phi(m)} \equiv 1 \pmod{m}$ Then 'a' is called a primitive root modulo m.

$2^4 \equiv 1 \pmod 5$; $3^4 \equiv 1 \pmod 5$

$\Rightarrow 16 - 1 \equiv 0 \pmod 5$; $81 - 1 \equiv 0 \pmod 5$

$\therefore$ 2 and 3 are primitive roots.

Theorem:

Suppose m has a primitive root, g, then $g^j \equiv g^k \pmod m$ iff $j \equiv k \pmod{\phi(m)}$.

In particular $g^j \equiv 1 \pmod m$ iff $\phi(m) \mid j$.

The set $\{g, g^2 \dots g^{\phi(m)}\}$ forms a reduced residue system modulo m, so that if a is any integer satisfying $(g, m) = 1$ Then there is one g^j in this set $\rightarrow g^j \equiv g \pmod m$.

Proof:

(i) Given g is a primitive root of m.

$\Rightarrow \phi(m)$ is the smallest positive integer s

Sunrise 5-56 AM Sunset 6-23 PM

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

Given $g^{j^\circ} \equiv g^k \pmod m$

To prove: $j^\circ \equiv k \pmod{\phi(m)}$

$g^{j^\circ} \equiv g^k \pmod m$

$g^{j^\circ - k} \equiv 1 \pmod m$ ——— (2)

$\Rightarrow \phi(m) \mid j^\circ - k$ [∵ from (1) & (2)]

$\phi(m)$ is the least positive integers

$\Rightarrow j^\circ - k \equiv 1 \pmod{\phi(m)}$

$j^\circ \equiv k \pmod{\phi(m)}$

Consider $j^\circ \equiv k \pmod{\phi(m)}$

To prove: $\phi(m) \mid j^\circ$.

$j^\circ \equiv k \pmod{\phi(m)}$

$\Rightarrow j^\circ \equiv k + \lambda(\phi(m))$ ——— (3)

$g^{j^\circ} \equiv g^{k + \lambda(\phi(m))} \pmod m$

$g^{j^\circ} \equiv g^k \cdot g^{\phi(m)} \pmod m$

$g^{j^\circ} \equiv g^k \pmod m$ [∵ $g^{\phi(m)} \equiv 1 \pmod m$]

In particular $g^j \equiv 1 \pmod{m}$

$\Rightarrow k = 0$.

$\therefore$ From (3) $j^\circ = 1\ \phi(m)$

$\Rightarrow \phi(m) \mid j^\circ$.

(ii°) Given g is a primitive root of m.

$\Rightarrow (g, m) = 1$

Each power of g is relatively prime to m.

$g, g^2 \cdots g^{\phi(m)}$ are all distinct residue mod m and all are relatively prime to m.

$g, g^2 \cdots g^{\phi(m)}$ forms a RRS modulo m

Here $(g, m) = 1$, There is only one g^{j° in this set $\Rightarrow g^{j^\circ} \equiv g \pmod{m}$

Theorem 2.37:

If p is a prime and $(a, p) = 1$, then the Congruence $x^n \equiv a \pmod{p}$ has $(n, p-1)$ Solutions or no solution according as

$$(p-1) \mid (n, p-1)$$

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

or not.

Proof :

Let $(n, p-1) = b$ and u be a solution of the congruence $x^n \equiv a \pmod{p}$ then

u is relatively prime to p.

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

Since u is a solution of $u^n \equiv a \pmod{p}$

$\Rightarrow a \equiv u^n \pmod{p}$ (by Symmetry)

$\therefore a^{\frac{p-1}{b}} \equiv u^{n\left(\frac{p-1}{b}\right)} \pmod{p}$

$\equiv \left(u^{p-1}\right)^{n/b} \pmod{p}$

$\equiv 1 \pmod{p}$ $\left[\because u^{p-1} \equiv 1 \pmod{p}\right]$

Thus if the congruence has a solution, then

$$a^{\frac{p-1}{(n,p-1)}} \equiv 1 \pmod{p}$$

If $a^{\frac{p-1}{(n,p-1)}} \not\equiv 1 \pmod{p}$, then the congruence has no solution.

To prove : There are $(n, p-1) = b$ solutions of

$$a^{\left(\frac{p-1}{n,p-1}\right)} \equiv 1 \pmod{p} \quad \text{——— (*)}$$

Since p is a prime there is a primitive root $g \bmod p$ $\Rightarrow$

$$g^{\phi(p)} \equiv 1 \pmod{p} \quad \text{——— (1)}$$

Since $(a, p) = 1$ there is an exponent j $\Rightarrow$ $g^{j} \equiv a \pmod{p}$ [$\because$ by previous theorem]

$$g^{j\left(\frac{p-1}{b}\right)} \equiv a^{\left(\frac{p-1}{b}\right)} \pmod{p}$$

$$g^{j\left(\frac{p-1}{b}\right)} \equiv 1 \pmod{p} \quad \text{——— (2)}$$

From (1) and (2)

$$\phi(p) \mid j\left(\frac{p-1}{b}\right)$$

$$\Rightarrow p-1 \mid j\left(\frac{p-1}{b}\right)$$

$$\Rightarrow b \mid j$$

Any solution of $x^{n} \equiv a \pmod{p}$ if exist can be taken as powers of g say $g^{j} \pmod{p}$

$\therefore$ The solution of $x^{n} \equiv a \pmod{p}$ corresponds to g^{y_n}

ie $g^{y_n} \equiv g^{j} \pmod{p}$

This Congruence has solution $\Leftrightarrow$ the Congruence $y^n \equiv j \pmod{\phi(p)}$ has solution.

$\Leftrightarrow$ The Congruence $y_n \equiv j \pmod{(p-1)}$ has solution.

Since $(n, p-1) = b$ and $b \mid j$

This Congruence has b solution.

[$\because ax \equiv b \pmod{m}$ & $(a,m) = d$ and $d \mid b$ Then The Congruence has a solution]

Hence the given Congruence has $b = (n, p-1)$ solution.

$\therefore a^{\frac{p-1}{(n,p-1)}} \not\equiv 1 \pmod{p}$, then the Congruence has no solutions.

Corollary : 2.38 Euler's Criterion.

If p is an odd prime and $(a,p)=1$, then $x^2 \equiv a \pmod{p}$ has two solutions or no solutions according as $a^{p-1/2} \equiv 1 \pmod{p}$ or $a^{p-1/2} \equiv -1 \pmod{p}$.

proof:

Since $(a,b)=1$ and p is a prime number

By Fermat's Theorem,

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

$$a^{p-1} - 1 \equiv 0 \pmod{p}$$

$$(a^{p-1/2} - 1)(a^{p-1/2} + 1) \equiv 0 \pmod{p}$$

$$\Rightarrow a^{p-1/2} + 1 \equiv 0 \pmod{p} \quad *$$

$$a^{p-1/2} - 1 \equiv 0 \pmod{p}$$

By the previous Theorem, the given Congruence has $(2, p-1) = 2$ solutions if

$$a^{p-1/2} - 1 \equiv 0 \pmod{p}$$

or $$a^{p-1/2} \equiv 1 \pmod{p}$$

and has no solutions if $a^{\frac{p-1}{2}} \neq 1 \pmod{p}$

ie $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Theorem 2.39 :

If p is a prime then $\exists\ \phi(\phi(p^2)) = (p-1)\phi(p-1)$ primitive roots modulo p^2

Sunrise 5-54 AM

Sunset 6-24 PM

Proof :

If g is a primitive root $(\text{mod } p)$, show that $g+tp$ is a primitive root $(\text{mod } p^2)$ for exactly $p-1$ values of $t \pmod p$.

Let h be the order of $g+tp \pmod{p^2}$

[Thus h may depend on t]

$$\Rightarrow (g+tp)^h \equiv 1 \pmod{p^2}$$

$$\Rightarrow (g+tp)^h \equiv 1 \pmod{p}$$

$$\Rightarrow g^h \equiv 1 \pmod{p}$$

$$\Rightarrow p-1 \mid h$$

By Corollary 2.32

"Order of a modulo m divides $\phi(m)$"

$$\therefore h \mid \phi(p^2)$$

$$\phi(p^2) = p(p-1)$$

$$\Rightarrow h \mid p(p-1)$$

$$\therefore h = p-1 \text{ or } h = p(p-1)$$

$h = p(p-1)$, $g+tp$ is a primitive root $(\text{mod } p^2)$

To prove : $h = p-1$ arises for only one of the p possible values of t

Let $f(x) = x^{p-1} - 1$

$\Rightarrow g+tp$ is a solution of the Congruence

This entire

Sunrise 5-54 AM

$f(x) \equiv 0 \pmod{p^2}$

Now $f(g) \equiv g^{p-1} - 1$

$f'(g) = (p-1)\, g^{p-2}$

$\not\equiv 0 \pmod{p}$ [∵ by Theorem 2.21 not in Syllabus]

Statement: Hensel's lemma

$\Rightarrow$ $g \pmod{p}$ lifts to a unique solution $g + tp \pmod{p^2}$

∴ For all other values of $t \pmod{p}$, the number $g + tp$ is a primitive root $\pmod{p^2}$

Now, Each $\phi(p-1)$ primitive roots $\pmod{p}$ gives exactly $p-1$ primitive roots $\pmod{p^2}$

We have shown that if at least
$(p-1)\phi(p-1)$ primitive roots (mod p^2)

To prove: There are no other primitive roots (mod p^2).

Let g be a primitive root (mod p^2)
$\Rightarrow g, g^2 \ldots g^{p(p-1)}$ forms reduced residue (mod p^2).

By Lemma 2.33
g^k is a primitive root iff
$\left(k, \frac{h}{(h,k)}\right) = 1$.

$h = p(p-1) \Rightarrow \frac{p(p-1)}{(p(p-1), k)}$

$\Rightarrow (p(p-1), k) = 1$

By defn of Euler ϕ function there are
$\phi(p(p-1))$ such values of k
among $1, 2, \ldots p(p-1)$.
We know $(p, p-1) = 1$

6 కృత్తిక ని.గం. ... ఉ.శే.వ.6-22 వ.

Sunrise 5-53 AM

Sunset 6-25

$p, p-1$ are relatively prime Then by CRT

Now Consider CRT

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

Theorem 2.40

If p is an odd prime and g is a primitive root modulo p^2, Then g is a primitive root modulo p^α for $\alpha = 3, 4, 5 \ldots$

Proof:

Suppose g is a primitive root $(\text{mod } p^2)$

$$[g^{\phi(p^2)} \equiv 1 \ (\text{mod } p^2)] \quad \text{——— ①}$$

Let h be the order of $g \ (\text{mod } p^\alpha)$, $\alpha > 2$.

$$\Rightarrow g^h \equiv 1 \ (\text{mod } p^\alpha)$$
$$\Rightarrow g^h \equiv 1 \ (\text{mod } p^2) \quad \text{——— ②}$$

from ① & ② we have

$$\phi(p^2) \mid h.$$

By Corollary 2.32

"If $(a, m) = 1$, then the order of a modulo m divides $\phi(m)$"

$\Rightarrow h \mid \phi(p^2)$

$\Rightarrow h = p^{\beta}(p-1)$

where $\beta = 1, 2, \ldots$ or $\alpha - 1$

To prove: $\beta = \alpha - 1$

ie To show that: $g^{p^{\alpha-2}(p-1)} \not\equiv 1 \pmod{p^\alpha}$ — (3)

Using induction, to show this holds for all $\alpha \geq 2$

The order of $g \pmod{p^2}$ is $\phi(p^2) = p(p-1)$

By (1) $g^{\phi(p^2)} \equiv 1 \pmod{p^2}$

$\Rightarrow g^{p(p-1)} \equiv 1 \pmod{p^2}$

$\Rightarrow g^{p-1} \not\equiv 1 \pmod{p^2}$

Sub $\alpha = 2$ in (3), we have

$g^{p-1} \not\equiv 1 \pmod{p^2}$

Sunrise 5-52 AM

By fermat's Congruence

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

$$\Rightarrow g^{p-1} = 1 + b_1 p, \quad p \nmid b_1$$

Now

$$g^{p(p-1)} = (1 + b_1 p)^p$$

$$= 1 + \binom{p}{1} b_1 p + \binom{p}{2} b_1^2 p^2 + \cdots$$

by binomial Theorem.

As $\boxed{p > 2}$, $\binom{p}{2} = \frac{p(p-1)}{2} \equiv 0 \pmod{p}$

$$\therefore g^{p(p-1)} \equiv 1 + b_1 p^2 \pmod{p^3}$$

Thus when $\alpha = 2$ in (3) we have

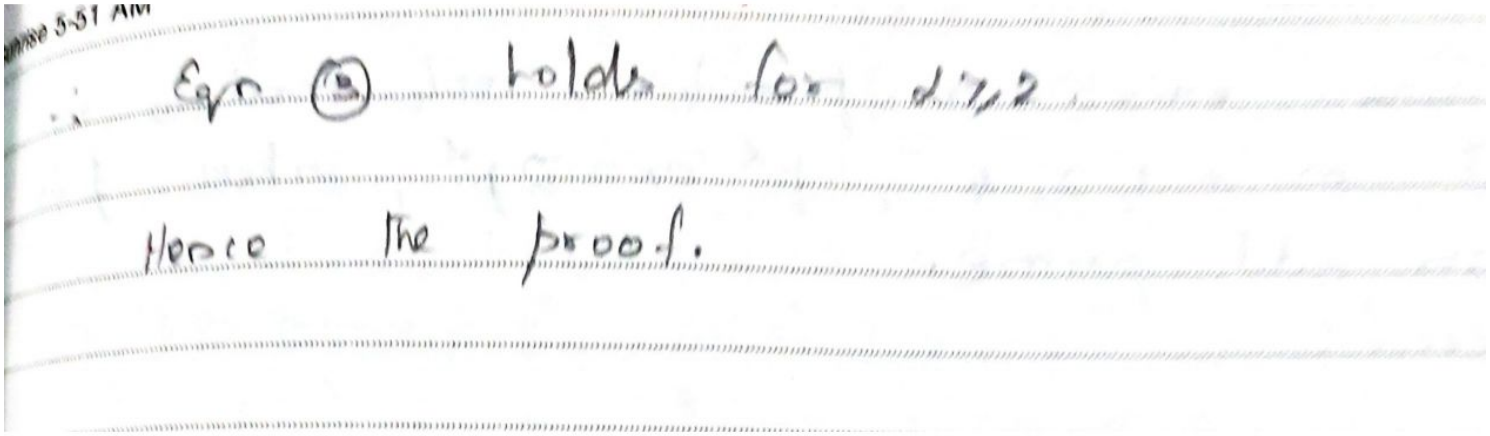
$$g^{p(p-1)} \not\equiv 1 \pmod{p^3}$$

$$\therefore g^{p(p-1)} = 1 + b_2 p^2 \quad \text{with } p \nmid b_2$$

Consider $g^{p(p-1)\cdot p} \equiv 1 + b_2 p^3 \pmod{p^4}$

[when $\alpha = 4$ in (3)]

I am the goal, support, master, witness, abode, refuge, friend, origin, dissolution, maintenance, storehouse, and imperishable seed – Bhag...


5:51 AM
∴ Eqn (2) holds for n = 2
Hence the proof.

Sunrise 5-51 AM

Theorem 2.41:

There exist a primitive root modulo m iff $m = 1, 2, 4, p^\alpha$ or $2p^\alpha$, where p is an odd prime.

proof: follows from Theorem 2.37

Corollary 2.42:

Suppose that $m = 1, 2, 4, p^\alpha$ or $2p^\alpha$, where p is an odd prime.

If $(a, m) = 1$ then the Congruence $x^n \equiv a \pmod m$ has $(n, \phi(m))$ solutions or no solution, according as $a^{\phi(m)/(n, \phi(m))} \equiv 1 \pmod m$

Problem:

Determine the number of solutions of the Congruence $x^4 \equiv 61 \pmod{117}$

Solution: $117 = 3^2 \cdot 13$

$\phi(9) \mid (4, \phi(9))$ $\quad \phi(9) = 6$

$\Rightarrow 6 \mid (4, 6) = 3.$

$61^3 \equiv (-2)^3 \equiv 1 \pmod 9$

$\therefore x^4 \equiv 61 \pmod 9$

has $(4, \phi(9)) = 2$ solutions

Now $\phi(13) \mid (4, \phi(13)) = 3$

& $61^3 \equiv (-4)^3 \equiv 1 \pmod{13}$

$\therefore x^4 \equiv 61 \pmod{13}$ has

$(4, \phi(13)) = 4$ solutions.

By CRT (2.20) The no of solutions modulo 117 is $2 \cdot 4 = 8$

Sunrise 5-51 AM

Sunset 6-26 P

Theorem 2.43

Suppose that $\alpha \geq 3$. The order of $5 \pmod{2^\alpha}$ is $2^{\alpha-2}$. The numbers $\pm 5, \pm 5^2, \pm 5^3 \ldots \pm 5^{2^{\alpha-2}}$ form a system of reduced residues $\pmod{2^\alpha}$. If a is odd, then $\exists$ i and j $\ni$ $a \equiv (-1)^i 5^j \pmod{2^\alpha}$. The values of i and j are uniquely determined $\pmod 2$ and $\pmod{2^{\alpha-2}}$, respectively.

Sunrise 5-50 AM

Corollary 2.44

Suppose that $\alpha \geq 3$ and that a is odd.
If n is odd, then the congruence $x^n \equiv a \pmod{2^\alpha}$ has exactly one solution.
If n is even, then choose β so that $(n, 2^{\alpha-2}) = 2^\beta$. The congruence $x^n \equiv a \pmod{2^\alpha}$ has $2^{\beta+1}$ solutions or no solution according as $a \equiv 1 \pmod{2^{\beta+2}}$ or not.

Sunrise 5-49 AM 2.9

Congruences of degree two, prime modulus.

The congruence of the form $ax^2+bx+c \equiv 0 \pmod{p}$ ... (1) where $p \nmid a$ is called the second degree congruence of prime modulus.

If $p>2$, p is odd then the problem of solving the congruence of degree 2 is reduced to that of solving of congruence of the form $x^2 \equiv a \pmod{p}$

Let $f(x) \equiv 0 \pmod{p}$, Then the degree is 2.

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

If p is odd;

$$4a\,f(x) = (2ax+b)^2 + 4ac - b^2$$

(1) is converted to the form $x^2 \equiv a \pmod{p}$ when $(2a, p) = 1$

Sunrise 5-49 AM Nrusimha Jayanthi Sunset 6-28 PM

Result:

The congruence $ax^2 + bx + c \equiv 0 \pmod{m}$ and $(2a, m) = 1$ can be reduced to the form $x^2 \equiv a \pmod{m}$

The congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ and $(a, p) = 1$ can always be reduced to the form $x^2 \equiv a \pmod{p}$

If the congruence $x^2 \equiv a \pmod{p}$ and $(a, p) = 1$ is solvable, then it has exactly 2 solution.

Problems.

1. Reduce $4x^2 + 2x + 1 \equiv 0 \pmod{5}$ to the form $x^2 \equiv a \pmod{p}$

Solution: $(a, p) = (4, 5) = 1 \rightarrow$ GCD $(4, 5)$ is 1

$4x^2 + 2x + 1 \equiv 0 \pmod{5}$ ——— (1)

Multiply (1) by $4a \Rightarrow 4 \times 4 = 16 \quad a = 4$

$\Rightarrow 64x^2 + 32x + 16 \equiv 0 \pmod{5}$

$\Rightarrow (8x)^2 + 2(8x)2 + 2^2 - 2^2 + 16 \equiv 0 \pmod{5}$

$\Rightarrow (8x + 2)^2 + 12 \equiv 0 \pmod{5}$

$\Rightarrow \underbrace{(2(4x+1))^2}_{x^2} \equiv \underbrace{-12}_{a} \pmod{\underbrace{5}_{p}}$

Sunrise 5-48 AM

Sunset 6-30 PM

Number Theory ~~from~~ ~~for~~ an algebraic viewpoint.

Group: 2.9:

A group Gr is a set of elements a, b, c.... together with a single valued binary operation ⊕ ∋

(1) The set is closed under the operation

(2) The associative law holds, namely

$a \oplus (b \oplus c) = (a \oplus b) \oplus c$ for all elements a, b, c in Gr.

(3) The set has a unique identity element e;

(4) each element in Gr has a unique inverse in Gr

i.e $a \oplus (-a) = (-a) \oplus a = e \quad \forall a \in Gr$

A group is called abelian (or) Commutative if

$a \oplus b = b \oplus a \quad \forall a, b \in Gr.$

A finite group is one with a finite no of elements otherwise it is called an infinite group.

If a group is finite, the number of elements is called the **order of the group.**

Example:

The set of all integers $0, \pm 1, \pm 2 \ldots$ is a group under addition, it is an abelian group.

Note: But this set is not a group under multiplication, because of the absence of inverses for all elements except ± 1.

Definition 2.10.

The groups $(G, \oplus)$ and $(G', \odot)$ are said to be isomorphic if there is a 1-1 correspondence b/w the element of G and those of G' s.t. if a in G corresponds to a' in G' and b in G corresponds to b' in G'

Then $a \oplus b$ in G corresponds to $a' \odot b'$ in G'

ie $G \approx G'$

A additive Group modulo 6.

Solution:

CRS of mod 6 is $\{0, 1, 2, 3, 4, 5\}$

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$3+4 \equiv 1 \pmod 6$; $5+5 \equiv 4 \pmod 6$

Another way of thinking of the additive group modulo 6 is in terms of the residue choosen.

Then residue classes will separate all the integers into the residue classes.

$C_0 = \{a \mid b \equiv 0 \pmod 6\}$

$= \{\ldots -18, -12, -6, 0, 6, 12, 18 \ldots\}$

element when divided by 6 Remainder is 0

$a \equiv b \pmod 6$

You alone know yourself through your own power, O best of persons, cause of the welfare of beings, Lord of beings,

Sunrise 5-48 AM

Sunset 6-30 PM

$C_1 = \{a \mid b \equiv 1 \pmod 6\}$ Elements when divided by 6 Remainder is 1

$= \{\ldots -17, -11, -5, 1, 13, 19 \ldots\}$

$C_2 = \{a \mid b \equiv 2 \pmod 6\}$

$= \{\ldots -16 -10 -4, 2, 8, 14, 20 \ldots\}$

$C_3 =$

$= \{\ldots -15, -9, -3, 3, 9, 15, 21 \ldots\}$

$C_4 =$

$= \{\ldots -14, -8, -2, 4, 10, 16, 22 \ldots\}$

$C_5 =$

$= \{\ldots -13, -7, -1, 5, 11, 17, 23 \ldots\}$

Note: If any element in C_2 is added to any element in C_3, the sum is an element in C_5.

ie $C_2 + C_3 = C_5$; $C_3 + C_4 = C_1$; $C_5 + C_3 = C_2$

+	C_0	C_1	C_2	C_3	C_4	C_5
C_0	C_0	C_1	C_2	C_3	C_4	C_5
C_1	C_1	C_2	C_3	C_4	C_5	C_0
C_2	C_2	C_3	C_4	C_5	C_0	C_1
C_3	C_3	C_4	C_5	C_0	C_1	C_2
C_4	C_4	C_5	C_0	C_1	C_2	C_3
C_5	C_5	C_0	C_1	C_2	C_3	C_4

5:48 AM

Thus $\{C_0, C_1, C_2, C_3, C_4, C_5\}$ form a group w.r.t $+^n$.

Further this group is isomorphic to the additive group modulo 6.

Theorem 24.6:

Any complete residue system modulo m forms a group under addition modulo m. Two complete residue system modulo m constitute isomorphic groups under addition, and so we speak of the additive group modulo m.

Proof:

Let the CRS modulus m; $G = \{0, 1, 2 \cdots m-1\}$

(i) clearly $a, b \in G \Rightarrow a+b \in G$ where $+$ is addition modulo m.

$\therefore$ G is closed w.r.t to addition mod m.

(ii) $(a +_m b) +_m c = a +_m (b +_m c)$

remainder when $a+b+c$ is divided by m.

$+_m$ is associative.

(iii) $a +_m 0 = 0 +_m a = a \quad \forall\, a \in G \;\&\; 0 \in G$

0 is the identity element and it is unique.

(iv) additive inverse of 0 is zero and the additive inverse of any number a is m-a these inverse are unique.

∴ $(C, +_m)$ is a group.

Passing from the system $0, 1, \ldots m-1$ to any CRS $r_0, r_1, \ldots r_{m-1}$,

⇒ All the above observations hold with a replaced by r_a, $a = 0, 1, \ldots m-1$

⇒ Same group with the new notation.

2.11 Groups, Rings and Fields.

Theorem 2.47:

Let $m > 1$ be a positive integer. Any reduced residue system modulo m is a group under multiplication modulo m. The group is of order $\phi(m)$. Any two such groups are isomorphic, so we speak of the multiplicative group modulo m, denoted by R_m.

Proof:

Consider and RRS $r_1, r_2 \dots r_n$ where $n = \phi(m$

By theorem 1.8

if $(r_i^\circ, m) = 1$, $(r_j^\circ, m) = 1$ Then $(r_i^\circ r_j^\circ, m) = 1$

Let $G = \{r_1, r_2 \dots r_m\}$

$r_1, r_2 \in G \Rightarrow r_1 \cdot r_2 \in G$

G is closed under multiplication mod m.

Since $a(bc) = (ab)c$ we have $a(bc) \equiv abc \pmod m$

G Contains one element say $r_j^\circ \ni r_j^\circ \equiv 1 \pmod m$.

This is the unique identity element of the group.

For each r_j° the congruence

$$x r_j^\circ \equiv r_j^\circ \pmod m$$

has unique solution since $(r_i^\circ, m) = 1$ by Theorem 2.17

$\Rightarrow$ Every r has a multiplicative inverse.

Hence G is a group under multiplication mod m.

Two different reduced residue systems modulo m are congruent, element by element, modulo m.

Hence we have an isomorphism b/w two groups.

Sunrise 5-48 AM

Sunset 6-32 PM

Theorem 2.48:

In any group G, $ab = ac \Rightarrow b = c$ and likewise $ba = ca \Rightarrow b = c$.

If a is any element of a finite group G with identity element e, then there is a unique smallest positive integer $r \rightarrow a^r = e$.

Proof:

(i) Let G be a group.

Let $a, b, c \in G$

Let a^{-1} be the inverse of a.

Assume $ab = ac$

Pre-multiply by a^{-1}

$\Rightarrow a^{-1}(ab) = a^{-1}(ac)$

$\Rightarrow (a^{-1}a)b = (a^{-1}a)c$ [$\because$ G is a group associativity]

$\Rightarrow eb = ec$

$\Rightarrow b = c$

(ii) Consider the series of elements obtained by repeated multiplication by a,

$[a^0 = e]$, $e, a, a^2, a^3 \ldots\ldots$

Since the group is finite and since the members of this series are elements of the group,

There must occur a repetition of the form

$a^s = a^t$ with $s < t$

Post multiply by a^{-s},

$a^s a^{-s} = a^t a^{-s}$

$a^0 = a^{t-s}$

$e = a^{t-s}$

Thus there is some +ve integer $t-s$ ∋ $a^{t-s} = e$

Let r be the smallest +ve exponent with the above property

ie $r = t-s$ ∋ $a^r = e$.

Definition 2.11 :

Let G be any group, finite or infinite and $a \in G$. If $a^s = e$ for some +ve integer s, then a is said to be of finite order. If a is a finite order, the order of a is the smallest positive integer r ∋ $a^r = e$. If there is no positive integer s ∋ $a^s = e$, then a is said to be of infinite order.

A group G is said to be cyclic if

it contains an element $a \neq$ the powers of a $\ldots, a^{-3}, a^{-2}, a^{-1}, a^0 = e, a, a^2, a^3, \ldots\ldots$ comprise the whole group. Such an element 'a' is said to generate the group and is called a generator.

Sunrise 5-48 AM

Sunset 6-32 PM

Theorem 2.49:

The order of an element of a finite group G is a divisor of the order of the group. If the order of the group is denoted by 'n', then $a^n = e$, for every element a in the group.

Proof:

Let $a \in G \rightarrow O(a) = r$

$\Rightarrow a^r = e$

And $G = \{ e, a, a^2 \dots a^{r-1} \}$ ——— (1)

$\Rightarrow O(G) = r$. and $a^{O(a)} = a^r = e = a^n$

If G contains more than these 'r' elements.

Let 'b_2' be another element of G.

Then: $b_2, b_2 a, b_2 a^2 \dots b_2 a^{r-1}$ ——— (2)

are 'r' distinct elements all different from the elements of (1)

First $b_2 a^s = b_2 a^t$

$\Rightarrow a^s = a^t$ by Theorem 2.48. } (*) ← exact explanation.

If $b_2 a^s = a^t$

$\Rightarrow b_2 = a^{t-s}$

$\Rightarrow$ b_2 would be among the powers of 'a'.

$\longrightarrow$

(*) $\therefore$ $b_2 a^s$ and $b_2 a^t$ are different element.

All elements of (2) are distinct.

Next to show that these elements are different from (1)

$\longrightarrow$ $b \in$ to (1) but $b_2 \in$ (2)

$\therefore$ b_2 would be among the powers of 'a'.

All the elements of (2) are different from the elements of (1)

If suppose there are still more elements

Let 'b_3' be another element $\neq$

$b_3, b_3a, b_3a^2 \ldots b_3a^{r-1} \in G$

clearly, they are distinct and different from (1) & (2) by a similar argument.

This process of obtaining new element $b_2, b_3 \ldots$ must terminate, since G_1 is finite.

If the last batch of new element is $b_k, b_k a, b_k a^2 \ldots b_k a^{r-1}$, then the order of the group G_1 is kr

$r \mid kr$ ie $O(a) \mid O(G_1)$.

Let $O(G_1) = n$ ie $n = kr$

$$a^n = a^{kr}$$

$$\Rightarrow = (a^r)^k$$

$$= e^k$$

$$= e$$

$$\Rightarrow a^n = e$$

Sunrise 5-48 AM

RING

Definition 2.12:

A ring is a set of at least two elements with two binary operations, $\oplus$ and $\odot$, if it is a commutative group under $\oplus$, is closed under $\odot$, and $\odot$ is associative and distributive w.r.t $\oplus$.

The identity element w.r.t $\oplus$ is called the zero of the ring. If all the elements of a ring, other than the zero, form a commutative group under $\odot$, then it is called a field.

Theorem 2.50:

The set Z_m of elements $0, 1, 2, \ldots m-1$ with addition and multiplication defined modulo m is a ring for any integer $m > 1$. Such a ring is a field iff m is a prime.

Proof:

$$Z_m = \{0, 1, 2 \ldots m-1\}$$

By Theorem 2.46, Z_m is a group under addition modulo 'm'.

Also this group is commutative under addition.

Sunrise 5-48 AM Sunset 6-34 PM

it is closed under ⊙.

Since, the ordinary multiplication is associative, further it is distributive w.r.t ⊕

∴ Z_m is a ring.

By Theorem 2.47, any reduced residue System modulo 'm' is a group under multiplication modulo 'm'.

If 'm' is a prime 'p' the RRS of Z_p is $\{1, 2 \cdots p-1\}$

(ie) all elements of Z_p other than zero.

Since '0' is the zero of the ring.

⇒ Z_p is a field.

Conversely, Assume Z_m is a field.

To prove: 'm' is prime.

Suppose, m is not prime.

Then 'm' is of the form ab, $1 < a \leq b < m$

Then the element of Z_m other than zero do not form a group under multiplication modulo 'm'.

Since there is no inverse for the element 'a', $ax \equiv 1 \pmod{m}$, $(a, m) = d$

$d \nmid 1$, $ax \equiv 1 \pmod{m}$ has no solution.

$\therefore$ Z_m is not a field.

$a \Rightarrow \Leftarrow$

$\therefore$ m is prime.

Problems:

1. Find the primitive roots of 3.

$\phi(m) = \phi(3) = 3 - 1 = 2$

	a	a^2
1	1	1
2	2	4

$2^2 \equiv 1 \pmod{3}$

2. Find the primitive roots of 7.