# Algebraic Number Theory - P16MAE5C

## Unit - I

1. State Division Algorithm

Given any integer $a$ and $b$ with $a > 0$, there exist unique integer $q$ and $r$ such that $b = qa + r$, $0 \leq r < a$

If $a \times b$ then $r$ satisfies the stranger inequalities $0 < r < a$

2. Let $f(x) = x^2 + x + 7$ find all roots of the congruence $f(x) \equiv 0 \pmod{15}$

Let $x = 0$

$f(x) = 7 \not\equiv 0 \pmod{15}$

$x = 1 = 9 \not\equiv 0 \pmod{15}$

$x = -1 = 7 \not\equiv 0 \pmod{15}$

$x = 2 \Rightarrow 12 \not\equiv 0 \pmod{15}$

$x = -2 \Rightarrow 9 \not\equiv 0 \pmod{15}$

$a = 0, \pm 1, \pm 2$ has no soln

$\therefore 5/15$ it follow that there is no soln $\pmod{15}$

3. State Fermats theorem:

Let $P$ denote a prime If $P \times a$ then $a^{P-1} \equiv 1 \pmod{p}$ for every integer $a$ [or] $a^P \equiv a \pmod{P}$

4. Define: Linear congruence

An equation is of the form $ax \equiv b \pmod{m}$ is called a linear congruence.

5. P.T $2^{340} \equiv 1 \pmod{341}$

$a^p \equiv a \pmod{q}$

$a^q \equiv a \pmod{p}$

$a^{pq} \equiv a \pmod{pq}$

$341 = 11 \times 31$

$p = 11,\ q = 31,\ a = 2$

$a^p \equiv a \pmod{q}$

$2^{11} \equiv 2 \pmod{31}$

$a^q \equiv a \pmod{p}$

$2^{31} \equiv 2 \pmod{11}$

$a^{pq} \equiv a \pmod{pq}$

$2^{11 \cdot 31} \equiv 2 \pmod{341}$

$2^{341} \equiv 2 \pmod{341}$

$\div 2$

$2^{340} \equiv 1 \pmod{341}$

Unit - II

**6. State Hensel's lemma:**

Suppose that $f(x)$ is a polynomial with integral co-eff it $f(a) \equiv 0 \pmod{p^j}$ and $f'(a) \not\equiv 0 \pmod{p}$ then there is a unique $t \pmod{p}$

$$f'(a + tp^j) \equiv 0 \pmod{p^{j+1}}$$

**7. Order of modulo m:**

Let $m$ denote a +ve integer and $a$ any integer such that

$$(a, m) = 1$$

Then the order of $a$ modulo $m$ is the smallest +ve integer $h$ ∋

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

Ex:

The order of $2 \pmod{7}$ is 3 Because,

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

$$2^2 \equiv 4 \pmod{7}$$

$$2^3 \equiv 1 \pmod{7}$$

8. State Euler's Criterian

If $P$ is a odd Prime and $(a,p)=1$ then $x^2 \equiv a \pmod{p}$ has solution or no solution according as

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

9. Solve the conguvence $x^5 \equiv 6 \pmod{101}$

Soln:

Define suffices to verify that

$$6^{20} \equiv 1 \pmod{101}$$

To find. $I$ such that

$$9^i \equiv 6 \pmod{101}$$

To fact that

$$6^{20} \equiv 1 \pmod{101}$$

Assume us that $5|i$

[ with more wark done may R.T $9=2$ is a primitive root $\pmod{101}$ ]

$$2^{70} \equiv 6 \pmod{101}$$

Hence the five solution are

$$x \equiv 2^{14+20j} \pmod{101}$$

where $j = 0, 1, 2, 3, 4$

ie] $x = 22, 70, 85, 96, 30 \pmod{101}$

hence the proved.

10. Define primitive root

Let 'a' be any integer ∋ a has order $\phi(m)$ [m is +ve integer] and $(a,m) = 1$

Then 'a' is a primitive roots of m ie] An integer m has a primitive root 'a' if

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

$$a^{K} \not\equiv 1 \pmod{m} \; \forall \; K \leq \phi(m)$$

Unit - III

11 Define - Quadratic non residue modulo 'm'

For all a such that $(a,m) = 1$, a is a quadratic residue modulo m if the congruence $x^2 \equiv a \pmod{m}$ has a soln

If it has no solution, then a is called a quadratic non residue modulo m

Ex:

The Quadratic residuces mod 5 are 1 & 4 2 & 3 non Residuces

ie] $x^2 \equiv 1 \pmod{5}$

$x^2 \equiv 4 \pmod{5}$

12. Define - Legendre symbol $[a/p]$

If $p$ denotes an odd prime then the legendre symbol $(a/p)$ is defined to be 1 if $a$ is a quadratic residue $-1$ if $a$ is a quadratic non residue modulo $p$ and 0 if $p/a$

ie $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is quadratic residue} \\ -1 & \text{if } a \text{ is quadratic not residue} \\ 0 & \text{if } p/a \text{ is} \end{cases}$

13. State - The Gaussion reciprocity law

If $p$ & $q$ are distinct odd primes then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\{(p-1)/2\}\{(q-1)/2\}}$

[or]

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

14. Evaluate $\left[\frac{-42}{61}\right]$

Soln

$$\frac{-42}{61} = \left(\frac{-1}{61}\right)\left(\frac{2}{61}\right)\left(\frac{3}{61}\right)\left(\frac{7}{61}\right)$$

$$\left(\frac{-1}{61}\right) = (-1)^{60/2} = 1$$

$$\frac{2}{61} = (-1)^{(61^2-1)/8}$$

$= (-1)^{3720/8}$

$= (-1)^{465}$

$\frac{2}{61} = -1$

$\left(\frac{3}{61}\right) = \left(\frac{61}{3}\right)(-1)^{(2/2)(60/2)}$

$= (-1)^{60/2 \cdot 61/3}$

$= 1 \cdot 61/3$

$= 1/3$

$(3/61) = 1$

$\frac{7}{61} = \left(\frac{61}{7}\right)(-1)^{(6/2)(60/2)}$

$= \frac{61}{7}(-1)^{3(30)}$

$= \frac{61}{7}(-1)^{90}$

$= \frac{61}{7}(+1)$

$= \frac{5}{7}$

$\frac{5}{7} = 7/5\,(-1)^{6/2 \cdot 4/2}$

$= 7/5\,(-1)^{3 \cdot 2}$

$= 7/5\,(-1)^{6} \Rightarrow 7/5(1)$

$= 7/5$

$= 2/5$

$= (-1)^{2418}$

$= (-1)^{3}$

$$\frac{7}{61} = -1$$

$$-\frac{42}{61} = \left(\frac{-1}{61}\right)\left(\frac{2}{61}\right)\left(\frac{3}{61}\right)\left(\frac{7}{61}\right)$$

$$= (1)(-1)(1)(-1)$$

$$-\frac{42}{61} = 1$$

**15.** solve the congruence $x^2 \equiv 5 \pmod{29}$

$$x^2 \equiv 5 \pmod{29}$$
$$\equiv 5 + 29 \pmod{29}$$
$$\equiv 34 \pmod{29}$$
$$\equiv 34 + 29 \pmod{29}$$
$$\equiv 63 \pmod{29}$$
$$\equiv 63 + 29 \pmod{29}$$
$$= 92 \pmod{29}$$
$$= 92 + 29 \pmod{29}$$
$$= 121 \pmod{29}$$
$$x^2 = 11^2 \pmod{29}$$

The soln of given congruence are $x_0 \& (P - x_0)$

$$x_0 = 11, \quad P = 29$$
$$x^2 = 11, (29 - 11)$$
$$x^2 = 11, 18$$

## Unit - IV

16. Define. Class number of $d$

If $d$ is not a perfect square then the number of equivalence clases of binary quadratic forms of discriminant $d$ is called the class number of $d$ denoted by $H(d)$

17. State Mobiaus inversion formula

Let $F$ and $f$ be two number theortic function if $F(n) = \sum_{d/n} f(d)$ Then

$$f(n) = \sum_{d/n} \mu(d) F(n/d) = \sum_{d/n} \mu(n/d) F(d)$$

18. Find the higher power of 7 that divisdes by 1000!

Soln:

$$\left[\frac{1000}{7}\right] = 142$$

$$\left[\frac{142}{7}\right] = 20$$

$$\left[\frac{20}{7}\right] = 2$$

Adding then we have $142 + 20 + 2 = 164$

Hence proved.

19. Define : Greatest integer function

For any arbitary real number $x$ we denote by $[x]$ the largest integer less then or equal to $x$

ie] $[x]$ is the unique integer satisfying

$$[x] \leq x \leq [x]+1$$

20. Let $f, g$ and $h$ be binary quadratic forms then $f \sim f$

Proof:

we have seen that $f \sim g$ iff there is an $M \in \Gamma$ such that

$$M^t F M = G$$

$\therefore$ Take $M = I$ the identity Matrix

since $I \in \Gamma$ and $I^t F I = F$

we conclude that $f \sim f$

Unit - V

21. The equation $15x^2 - 7y^2 = 9$ has no soln in integers

Proof:

Since the first and third member are divisible by 3 It follows that

$$3 / 7y^2 \text{ and}$$

hence $3 | y$

Thus the second and third member are divisible by 9

so that $9 | 15x^2$

Hence $3 | x$

Put $x_1 = x/3$, $y_1 = y/3$

so that $9 | 15x^2$

Put $x_1 = x/3$, $y_1 = y/3$

So that $15x_1^2 - 15y_1^2 = 1$

This has no soln as a congruence (mod 3)

Hence proved.

Q2 **Diophantine equation:**

The equation $ax + by = c$ any equation in one (or) more unknowns which to be solved in integers is called the 'diophantine'

A linear diophantine equated in two variables having integral co-efs can be written in the form $ax + by = c$ where $a, b, c$ are given integers and $ab$ not both zero

23. Simultaneous linear equation:

Let $a_1, a_2 \ldots a_n$ be integers and not all zero and suppose we wish to find all solutions in integer of the equation

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$$

we may show that such a solution exist iff gcd $(a_1, a_2 \ldots a_n)$ divides $c$

The numerical technique express the preceeding section also existen to the value of $n$

24. Solve: $2x + 3y + 4z = 5$

Soln:

| $C_1$ | $C_2$ | $C_3$ | |
|---|---|---|---|
| 2 | 3 | 4 | 5 |
| 1 | 0 | 0 | |
| 0 | 1 | 0 | |
| 0 | 0 | 1 | |

| $C_1$ | $C_2 - C_1$ | $C_3 - 2C_1$ | |
|---|---|---|---|
| 2 | 1 | 0 | 5 |
| 1 | -1 | -2 | |
| 0 | 1 | 0 | |
| 0 | 0 | 1 | |

| $C_1 - 2C_2$ | $C_2$ | $C_3$ | |
|---|---|---|---|
| 0 | 1 | 0 | 5 |
| 3 | -1 | -2 | |
| -2 | 1 | 0 | |
| 0 | 0 | 1 | |

The simultaneous equation involving 3 new variables say $t, u, v$

$$u = 5$$
$$x = 3t - u - 2v$$
$$x = 3t - 2v - 5$$
$$y = -2t + u$$
$$y = -2t + 5$$
$$z = v$$

25. Define: unimodular matrix

A square matrix $U$ with integral element is called unimodular if $\det(U) = \pm 1$