ALGEBRAIC NUMBER THEORY(P16MAE5C)

INCHARGE : Ms. A. HELEN SHOBANA

**CLASS : ** II M.Sc., MATHEMATICS

UNIT - I

DIVISIBLE:

An integer b is divisible by an integer a, not zero, if there is an integer x such that b = ax and write a\b.

DIVISION ALGORITM:

Given any integers a and b, with a > 0, there exists unique integers q and r such that $b = qa + r, 0 \le r < a.$

GREASTEST COMMON DIVISOR:

The integer a is a common divisor of b and c in case a\b and a\c. Since there is only a finite number of divisors of any nonzero integer, there is only a finite of common divisors of b and c, except in the case b= c= 0. If at least one of b and c is not 0, the greatest among their common divisors is called the greatest common divisor of b and c and is denoted by (b, c).

PRIME NUMBER:

An integer p > 1 is called a prime number, or a prime, in case there is no divisor d of p satisfying 1 < d < p. If an integer a > 1 is not a prime, it is called a composite number.

FUNDAMENTAL THEOREM OF ARITHMETIC:

The factoring of any integer n > 1 into primes is unique apart from the order of the prime factors.

EUCLID THEOREM:

The number of primes is infinite.

BINOMIAL THEOREM:

Let α be any real number, and let k be a non- negative integer. Then the binomial coefficient $\binom{\alpha}{k}$ is given by the formula

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)\ldots\ (\alpha-k-1)}{k!}$$

CONGRUENT:

If an integer m, not zero, divides the difference a – b , then a is congruent to b modulo m and write $a \equiv b(\text{mod } m)$. If a – b is not divisible by m, then a is not congruent to b modulo m and write $a \neq b(\text{mod } m)$.

RESIDUE:

If $x \equiv y(\text{mod } m)$, then y is called a residue of x modulo m. A set $x_1, x_2, ..., x_m$ is called a complete residue system modulo m if for every integer y there is one and only x_j such that $y \equiv x_j(\text{mod } m)$

REDUCED RESIDUE SYSTEM:

A reduced residue system modulo m is a set of integers r_i *such that* $(r_i, m) = 1$ *if* $i \neq j$, and such that every x prime to m is congruent modulo m to some member r_i of the set.

FERMAT'S THEOREM:

Let p denote a prime. If p does not divide a, then $a^{p-1} \equiv 1(\text{mod } p)$. For every integer a, $a^p \equiv a(\text{mod } p)$.

EULER'S GENERALIZATION OF FERMAT'S THEOREM:

If $(a, m) = 1$, then $a^{\phi(m)} \equiv 1(\text{mod } p)$.

WILSON'S THEOREM:

If p is a prime, then (p-1)! ≡ -1(mod p).

CHINESE REMAINDER THEOREM:

Let $m_1, m_2, \ldots\ldots m_r$ denote r positive integers that are relatively prime in pairs and let $a_1, a_2, \ldots\ldots a_r$ denote only r integers. Then the congruences

$x \equiv a_1(\text{mod } m_1)$

$x \equiv a_2(\text{mod } m_2)$

………………

$x \equiv a_r(\text{mod } m_r)$

have common solutions. If x_0 is one such solution, then an integer x satisfies the above congruences iff x is the form, $x = x_0 + km$ for some integer k.

UNIT - II

HENSEL'S LEMMA:

Suppose that f(x) is a polynomial with integral coefficients. If $f(a) \equiv 0 (\bmod p^j)$ *and* $f'(a) \not\equiv 0 (\bmod p)$, then there is a unique t(mod p) such that $f(a + tp^j) \equiv 0 (\bmod p^{j+1})$.

ORDER OF A MODULO:

Let m denote a positive integer and a any integer such that $(a, m) = 1$. Let h be the smallest positive integer such that $a^h \equiv 1 (\bmod m)$. Then the order of a modulo m is h, or that a belongs to the exponent h modulo m.

PRIMITIVE ROOT MODULO m:

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

n^{th} POWER RESIDUE MODULO p:

If $(a, p) = 1$ *and* $x^n \equiv a (\bmod p)$ has a solution, then a is called an n^{th} power residue modulo p.

EULER'S CRITERION:

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

VALUE OF $\mathbf{999^{179} (\textit{mod } 1763)}$.

Solution:

We know that,

$$179 = 1+2+2^4 + 2^5 + 2^7,$$

$$999^2 = 143 (mod\ 1763)$$

$$999^4 \equiv 143^2 \equiv 1056 (mod\ 1763)$$

$$999^8 \equiv 1056^2 \equiv 920 (mod\ 1763)$$

$$999^{16} \equiv 920^2 \equiv 160 (mod\ 1763)$$

$$999^{32} \equiv 160^2 \equiv 918 (mod\ 1763)$$

$$999^{64} \equiv 918^2 \equiv 10 (mod\ 1763)$$

so that $999^{128} \equiv 10^2 \equiv 100 \equiv (mod\ 1763).$

Hence,

$$999^{179} \equiv 999 \cdot 143 \cdot 160 \cdot 918 \cdot 100 \equiv 54 \cdot 160 \cdot 918 \cdot 100 \equiv 1588 \cdot 918 \cdot 100$$
$$\equiv 1546 \cdot 100 \equiv 1219 (mod\ 1763).$$

UNIT - III

GROUP:

A Group G is a set of elements a, b, c..... together with a single-valued binary operation $\oplus$ such that

- The set is closed under the operation
- The associate law holds namely a$\oplus$ $(b \oplus c) = (a \oplus b) \oplus c$ where a, b, c in G
- The set has a unique identity element e;
- Each element in G has a unique inverse in G

ABELIAN GROUP:

A group G is called abelian or commutative group if $a \oplus b = b \oplus a$ for every pair of elements a, b in G.

INFINITE GROUP:

A finite group is one with a finite number of elements; otherwise it is an infinite group.

ORDER OF THE GROUP:

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

ISOMORPHIC:

Two groups, G with operation $\oplus$ *and* G' with the operation Θ are said to be isomorphic if there is one – one correspondence between the elements of G and those of G' such that 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 $a' \Theta b'$ *in* G'. That is $G \cong G'$

FINITE ORDER:

Let G be any group, finite or infinite and a an element of G. If a^s = e for some positive integer s , then a is said to be finite order. If a is of finite order, the order of a is the smallest positive integer r such that $a^r = e$

INFINITE ORDER:

If there is no positive integer s such that $a^s = e$, then a is said to be infinit order

CYCLIC:

A group G is said to be cyclic if it contains an element a such that the powers of a

$$....,a^{-3},a^{-2},a^{-1},a^{0}=e,a,a^{2},a^{3},......$$

comprise the whole group. An element a is said to generate the group and is called a generator.

RING:

A Ring is a set of at least two elements with two binary operations , $\oplus$ and Θ , such that it is a commutative group under $\oplus$, is closed under Θ is associative and distributive with respect to $\oplus$. The identity element with respect to $\oplus$ is called zero of the ring.

FIELD:

If all the elements of a ring, other than the zero, form a commutative group under Θ, then it is called a field.

QUADRATIC RESIDUE MODULO:

For all a such that (a, m) = 1 , a is called a quadratic residue modulo m if the congruence $x^2 \equiv a(mod\ m)$has a solution. If it has no solution, then a is called a quadratic non-residue modulo m.

LEGENDRE SYMBOL:

If p denotes an odd prime , then the legendre symbol $\left(\frac{a}{p}\right)$ is defined to be 1 if a is a quadrqtic residue , -1 if a is a quadratic nonresidue modulo p, and 0 if p/a.

GAUSSIAN RECIPROCITY LAW:

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

JACOBI SYMBOL:

Let Q be positive and odd , so that Q = $q_1q_2 \ldots \ldots \ldots q_s$ where the q_i are odd primes , not necessarily distinct. Then the Jacobi symbol $\left(\frac{P}{Q}\right)$ is defined by

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s}\left(\frac{P}{q_j}\right)$$

where $\left(\frac{P}{q_j}\right)$ *is the Legendre symbol.*

UNIT - IV

QUADRATIC FORM:

A polynomial in several variables is called a form, or is said to be homogeneous if all its monomial terms have the same degree. A form of degree 2 is called a quadratic form. Thus the quadratic form is a sum of the shape

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}\, x_i\, x_j \cdot$$

BINARY QUADRATIC FORMS:

A form in two variables is called binary. Generally, we can write as

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

INDEFINITE AND SEMIDEFINITE:

A form f(x, y) is called indefinite if it takes on both positive and negative values. The form is called positive semi definite if f(x, y) ≥ 0 for all integers x , y. A semi definite form is called definite if in addition the only integers x , y for which f(x, y) = 0 are x = 0, y = 0.

REDUCED:

Let f be a binary quadratic form whose discriminant d is not a perfect square. We call f reduced if $-|a| < b \leq |a| < |c|$ or if $0 \leq b \leq |a| = |c|$.

CLASS NUMBER OF d:

If d is not a perfect square, then the number of equivalence classes of binary quadratic forms of discriminant d is called the class number of d, denoted H(d).

TOTALLY MULTIPLICATIVE (OR) COMPLETELY MULTIPLICATIVE:

If f(n) is an arithmetic function not identically zero such that f(mn) = f(m)f(n) for every pair of positive integers m ,n satisfying (m , n) = 1, then f(n) is said to be multiplicative. If f(mn) =f(m)f(n) whether m and n are relatively prime or not, then f(n) is said to be totally multiplicative or completely multiplicative.

7) MÖBIUS MU FUNCTION:

For positive integers n, put $\mu(n) = (-1)^{w(n)}$ if n is square free, and set $\mu(n) = 0$ otherwise. The $\mu(n)$ is the mÖbius mu function.

8) MODULAR GROUP:

The group of 2×2 matrices with integral elements and determinant 1 is denoted by Γ **,** and is called the modular group. The modular group is non-commutative.

UNIT -V

UNIMODULAR MATRIX:

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

PYTHAGOREAN TRIANGLES:

The two solutions 3,4,5 and 5,12,13 is a triple of positive integers as a Pythagorean triple or a Pythagorean triangle, since in geometric terms x and y are the legs of a right triangle with hypotenuse in view of algebraic identity

$$(r^2 - s^2)^2 + (2rs)^2 = (r^2+s^2)^2$$

TERNARY QUADRATIC FORMS:

A triple (x, y, z) of numbers for which f(x,y,z) = 0 is called a zero of the form. The solution (0,0,0) is the trivial zero.

If we have a solution in rational numbers, not all zero, then we can construct a primitive solution in integers by multiplying each coordinate by the least common denominator of the three.

THE EQUATION $x^3 + 2y^3 + 4z^3 = 9w^3$ HAS NO NONTRIVIAL SOLUTION :

Proof:

We show that the congruence $x^3 + 2y^3 + 4z^3 = 9w^3$ (mod 27) has no solution for which g.c.d (x,y,z,w,3)= 1.

We note that for any integers a, $a^3 \equiv o$r $\pm$ (mod 9).

Thus $x^3 + 2y^3 + 4z^3 \equiv 0$(mod 9) implies that x ≡ y ≡ z ≡0. (mod 3)

but $x^3 + 2y^3 + 4z^3 \equiv 0$(mod 27), so that $3/w^3$.

Hence 3/w.

This contradicts the assumption that g.c.d (x, y, z, w, 3) =1 .

The Diophantine equation $x^4+x^3+x^2+x+1= y^2$ has the integral solutions $(-1,1)$, (0,1),(3,11) and no others:

Proof:

Put f(x) = $4x^4 + 4x^3 + 4x^2 + 4x + 4$.

Since $f(x) = (2x^2 + x)^2 + 3(x + 2/3)^2 + 8/3$,

it follows that $f(x) > (2x^2 + x)^2$ for real x.

On the other hand, $f(x) = (2x^2 + x + 1)^2 - (x + 1)(x-3)$.

Here the last term is positive except for those real numbers x in the interval $I = [-1,3]$.

That is ,$f(x) < (2x^2 + x + 1)^2$ provided that $x \notin I$.

Thus if x is an integer, $x \notin I$, then $f(x)$ lies between two consecutive perfect squares, namely $(2x^2 + x)^2$ and $(2x^2 + x + 1)^2$.

Hence $f(x)$ cannot be a perfect square, except possibly for those integers $x \in I$, which we examine individually.