(8 pages) Reg. No. : ....

Code No. : 5381 **Sub. Code : ZMAE 31**

M.Sc. (CBCS) DEGREE EXAMINATION, APRIL 2023.

Third Semester

Mathematics

Elective – ALGEBRAIC NUMBER THEORY

(For those who joined in July 2021 onwards)

Time : Three hours Maximum : 75 marks

PART A — ($10 \times 1 = 10$ marks)

Answer ALL questions.

Choose the correct answer :

1. The linear Diophantine equation $ax+by=c$ has a solution if and only if ________.
   (a) $\gcd(a, c) \mid b$
   (b) $\gcd(a, b) \mid c$
   (c) $\gcd(c, b) \mid a$
   (d) $c \mid \gcd(a, b)$

2. Which of the following Diophantine equation cannot be solved?
   (a) $6x+51y=22$ (b) $33x+14y=115$
   (c) $14x+35y=93$ (d) $11x+13y=21$

3. Let a and b be integers, not both zero. Then a and b are relatively prime iff there exists integers x and y such that
   (a) $1+ax+by$ (b) $2=ax+by$
   (c) $ab=ax+by$ (d) $a-b=ax+by$

4. The Euclidean algorithm is used for finding the
   (a) 1 cm of two integers
   (b) gcd of two integers
   (c) prime numbers
   (d) composite numbers

5. Two integers a and b, not both of which are zero, are said to be relatively prime if
   (a) $\gcd(a, b)=a$ (b) $a \mid b$
   (c) $\gcd(a, b)=1$ (d) $b \mid a$

6. If p is prime, then P^{*} is the
   (a) sum of all primes that are less than or equal to p
   (b) product of all primes that are less than or equal to p
   (c) sum of squares of all primes that are less than or equal to p
   (d) product of all primes that are greater than or equal to p

7. The Sieve of Eratosthenes is used for finding
   (a) all primes below a given integer
   (b) all even numbers below a given integer
   (c) all odd numbers below a given integer
   (d) all composite numbers below a given integer

8. If n is an odd pseudo prime, then $2^{n}-1$ is
   (a) pseudo prime (b) prime
   (c) irrational (d) not pseudo prime

9. If p is a prime and a is any integer then $a^{p}-a$ is
   (a) a multiple of p^2 (b) a multiple of $p-1$
   (c) a multiple of $2p$ (d) a multiple of p

10. If m and n are relatively prime integers then $\varphi(mn)=$ ________.
    (a) $\varphi(m)+\varphi(n)$ (b) $\varphi(m)/\varphi(n)$
    (c) $\varphi(m)-\varphi(n)$ (d) $\varphi(m)\varphi(n)$

PART B — ($5 \times 5 = 25$ marks)

Answer ALL questions by choosing either (a) or (b).

11. (a) Find all solutions in integers of $2x+3y+4z=5$.

    Or

    (b) Find all solutions in positive integer $15x+7y=111$.

12. (a) Prove that 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.

    Or

    (b) Determine whether the Diophantic equation $x^2-5y^2-91z^2=0$ has a nontrivial integral solution.

13. (a) If we define $r_n = \langle a_0, a_1, \ldots, a_n \rangle$ for all integers $n \geq 0$, then prove that $r_n = h_n/k_n$.

Or

(b) Prove that the two distinct simple continued fractions converge to different values.

14. (a) Let ξ denote any irrational number. If there is a rational number $\frac{a}{b}$ with $b \geq 1$ such that $\left|\xi - \frac{a}{b}\right| < \frac{1}{2b^2}$ then prove that $\frac{a}{b}$ equals one of the convergents of the simple continued fraction expansion of ξ.

Or

(b) Prove that the product of two primitive polynomial is primitive.

15. (a) The norm of a product equal the product of the norms, $N(\alpha\beta) = N(\alpha)N(\beta) \cdot N(\alpha) = 0$ iff $\alpha = 0$. The norm of an integers in $Q(\sqrt{m})$, then prove that $N(\gamma) = \pm 1$ iff γ is a unit.

Or

(b) Prove that the reciprocal of a unit is a unit. The units of an algebraic number field from a multiplicative group.

PART C — (5 × 8 = 40 marks)

Answer ALL questions by choosing either (a) or (b).

16. (a) Let U be an $m \times m$ matrix with integral elements. Then prove that the following are equivalent :

(i) U is unimodular ;

(ii) The inverse matrix U^{-1} exists and has integral elements ;

(iii) U may be expressed as a product of elementary row matrices. $U = R_g R_{g-1} \ldots R_2 R_1$;

(iv) U may be expressed as a product of elementary column matrices, $U = C_1 C_2 \ldots C_{h-1} C_h$.

Or

(b) Find all solutions of the simultaneous congruences $3x + 3z \equiv 1 \pmod 5$, $4x - y + 5z \equiv 3 \pmod 5$.

17. (a) Suppose that $ax^2 + by^2 + cz^2$ factors into linear factors modulo m and also modulo n; that is $ax^2 + by^2 + cz^2 \equiv (\alpha_1 x + \beta_1 y + \gamma_1 z)(\alpha_2 x + \beta_2 y + \gamma_2 z) \pmod m$

$$ax^2 + by^2 + cz^2 \equiv (\alpha_3 x + \beta_3 x + \gamma_3 z)(\alpha_4 x + \beta_4 y + \gamma_4 z) \pmod n.$$

If $(m, n) = 1$ then prove that $ax^2 + by^2 + cz^2$ factors into linear factors modulo mn.

Or

(b) Determine whether the equation $x^2 + 3y^2 + 5z^2 + 2xy + 4yz + 6zx = 0$ has a nontrivial solution.

18. (a) Prove that the values r_n defined in $r_n = \langle a_0, a_1, \ldots, a_n \rangle$ satisfy the infinite chain of inequalities

$$r_0 < r_2 < r_4 < r_6 < \ldots < r_7 < r_5 < r_3 < r_1.$$

Or

(b) If $\langle a_0, a_1, \ldots, a_j \rangle = \langle b_0, b_1, \ldots, b_n \rangle$ where these finite continuous fractions are simple, and if $a_j > 1$ and $b_{n>1}$, then prove that $j = n$ and $a_i = b_1$ for $i = 0, 1, \ldots, n$.

19. (a) Prove that the convergents h_n/k_n are successively closer to ξ, that is $\xi - \left|\frac{h_n}{k_n}\right| < \xi - \left|\frac{h_{n-1}}{k_{n-1}}\right|$.

Or

(b) Prove that the continued fraction expansion of the real quadratic irrational number ξ is purely periodic iff $\xi > 1$ and $-1 < \xi' < 0$, where ξ' denotes the conjugate of ξ.

20. (a) Prove that every Euclidean quadratic field has the unique factorization property.

Or

(b) Prove that the fields $Q(\sqrt{m})$ for $m = -1, -2, -3, -7, 2, 3$ are Euclidean and so have the unique factorization property.

———