SECTION C — $(3 \times 10 = 30)$

Answer any THREE Questions.

16. Show that for every real number $y \geq 2, \sum_{p \leq y} \frac{1}{p} > \log\log y - 1$.

17. Show that the congruence $f(x) \equiv 0 (\bmod p)$ of degree n has atmost n..

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

19. Suppose that $n > 0$, and let $N(n)$ denote the number of solutions of the congruence $S^2 \equiv -1 (mod\, n)$. Show that $r(n) = 4N(n)$, and $R(n) = \sum r\left(n/d^2\right)$ where the sum is extended over all those positive d for which d^2/x.

20. Find all solutions of $999x - 49y = 5000$.

(For candidates admitted from 2016–2017 onwards)

M.Sc. DEGREE EXAMINATION, NOVEMBER 2022.

Mathematics – Elective

ALGEBRAIC NUMBER THEORY

Time : Three hours Maximum : 75 marks

SECTION A — $(10 \times 2 = 20)$

Answer ALL questions.

1. Define divisible.

2. Define least common multiple.

3. Determine the value of $999^{179} (\bmod 1763)$.

4. Solve $x^2 + x + 7 \equiv 0 (\bmod 81)$.

5. Define Group.

6. Define Legendre symbol.

7. Define quadratic forms.

8. Define modular group.

9. Find all integer's x and y such that $147x + 258y = 369$.

10. Define unimodular.

SECTION B — ($5 \times 5 = 25$)

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

11. (a) State and prove the division algorithm.

Or

(b) Show that for any integer x, $(a,b) = (b,a) = (a,-b) = (a, b+ax)$.

12. (a) Show that 1387 is composite.

Or

(b) Suppose that m is a positive integer and that $(a,m) = 1$. Show that if k and $\bar{k}$ are positive integers such that $k\bar{k} \equiv 1(mod\, \phi(m))$, then $a^{k\bar{k}} \equiv a(\text{mod}\, m)$.

13. (a) The set Z_m of elements 0, 1, 2, …. , $m-1$, with addition and multiplication defined modulo m, is a ring for any integer $m > 1$. Show that such a ring is a field if and only if m is a prime.

Or

(b) Let P be an odd prime. Prove that

(i) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} (\text{mod p})$

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

14. (a) Let $f(x,y) = ax^2 + bxy + cy^2$ be a binary quadratic form with integral coefficients and discriminant d. Show that if $d \neq 0$ and d is not a perfect square, then $a \neq 0$, $c \neq 0$ and the only solution of the equation $f(x, y = 0)$ in integers is given by $x = y = 0$.

Or

(b) Let f and g be binary quadratic forms. Prove that

(i) $f \sim f$

(ii) if $f \sim g$, then $g \sim f$. ,

15. (a) Let S be a set of k integers. If $m > 1$ and $2^k > m+1$, prove that there are two distinct non empty subsets of S, the sums of whose elements are congruent modulo m.

Or

(b) Show that if u and v are relatively prime positive integers whose product uv is a perfect square, then u and v are both perfect squares.