Master of Science Examination, 2024

(Second Year, Third Semester)

Mathematics

Unit : DSE - 04

(Number Theory)

Time : 2 *Hours* *Full Marks* : 40

Symbols have usual meanings, if not mentioned otherwise

Answer question **No. 1** and ***any three*** from the rest.

1. *(a)* If a, b and c are integers, show that $ax+by=c$ has a solution in integer if and only if $(a,b)\mid c$.

(b) Show that $\alpha \in \mathbb{Z}[i]$ is a unit if and only if $\lambda(\alpha)=1$. Deduce that $1, -1, i$ and $-i$ are the only units in $\mathbb{Z}[i]$.

(c) Show that $\nu(n)$ is odd if and only if n is a square.

(d) If n is not a prime, show that $(n-1)! \equiv 0(n)$, except when $n = 4$. 2+2+3+3=10

2. *(a)* Solve the system of congruences $x \equiv 1(7)$, $x \equiv 4(9)$, $x \equiv 3(5)$ with the help of Chinese Remainder Theorem.

(b) Let p be an odd prime. Show that a is a primitive root modulo p if and only if $a^{(p-1)/q} \not\equiv 1(p)$ for all prime divisors q of $p-1$. 4+6=10

3. *(a)* Prove that product of two primitive polynomials in $\mathbb{Z}[x]$ is a primitive polynomial.

(b) Let α be an algebraic integer and $f(x) \in \mathbb{Q}[x]$ be the monic polynomial of least degree where $f(\alpha) = 0$. Show that $f(x) \in \mathbb{Z}[x]$. 6+4=10

4. *(a)* Let $f(x) \in \mathbb{Z}[x]$. We say that a prime p divides $f(x)$ if there is an integer n such that $p \mid f(n)$. Describe the prime divisors of $x^2 + 1$ and $x^2 - 2$.

(b) Use the Jacobi symbol to determine $\left(\frac{215}{761}\right)$, $\left(\frac{514}{1093}\right)$, and $\left(\frac{401}{757}\right)$. 5+5=10

5. *(a)* Suppose that p is a prime with $p \equiv 1(3)$. Prove that there are integers A and B such that $4p = A^2 + 27B^2$. If $A \equiv 1(3)$, then prove that A is uniquely determined, and $N(x^3 + y^3 = 1) = p - 2 + A$.

(b) Find the number of solutions to the equation $x^3 + y^3 = 1$ in F_p for $p = 19$, 37, and 97. 5+5=10

6. *(a)* If π is a prime in D, prove that $x^3 \equiv 2(\pi)$ is solvable if and only if $\pi \equiv 1(2)$.

(b) Suppose p is a rational prime such that $p \equiv 1(3)$. Prove that $x^3 \equiv 2(p)$ is solvable if and only if there are integers C and D such that $p = C^2 + 27D^2$.

(c) Show that 1) $x^3 \equiv 2(7)$ is not solvable, and 2) $x^3 \equiv 2(31)$ is solvable. 3+4+3=10

★ ★ ★