B. Sc. Mathematics (Hons.) Examination, 2023

(3rd Year, 2nd Semester)

Number Theory

Paper – DSE-3A

Time : Two hours | Full Marks : 40

The figures in the margin indicate full marks.

Special credit will be given for precise answer.

(Unexplained Symbols/Notations have their usual meanings.)

Use separate answer scripts for each Part.

Part – I (20 Marks)

Answer ***any four*** questions. 4×5=20

1. The linear congruence $ax \equiv b \pmod{n}$ if and only if $d \mid b$, where $d = \gcd(a,n)$. If $d \mid b$, then it has d mutually incongruent solutions modulo n. 5

2. State Chinese Remainder Theorem. Find the unique solution of following the system of linear congruence
$$7x+3y \equiv 10 \pmod{16}$$
$$2x+5y \equiv 9 \pmod{16}.$$ 5

3. Define pseudoprime. If n is an odd pseudoprime, then show that $M_n = 2^n - 1$ is a larger one. 5

4. If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then show that

   a) $\tau(n) = (k_1+1)(k_2+1)\cdots(k_r+1)$ and

[Turn over

b) $\sigma(n)=\frac{p_1^{k_1+1}}{p_1-1}\frac{p_2^{k_1+1}}{p_2-1}\cdots\frac{p_r^{k_r+1}}{p_1-1}$. 2+3=5

5. Define multiplicative function. If f is a multiplicative function and F is defined by $F(n)=\sum_{d|n} f(d)$, then F is also multiplicative. Hence, show that $F(8\cdot 3)=F(8)F(3)$. 1+3+1=5

6. Define Möbius μ-function. If F and f are number-theoretic functions related by the formula $F(n)=\sum_{d|n} f(d)$, then show that

$$f(n)=\sum_{d|n}\mu(d)F\left(\frac{n}{d}\right)=\sum_{d|n}\mu\left(\frac{n}{d}\right)F(d).$$ 5

Part – II (20 Marks)

Answer ***any four*** questions. 5×4=20

1. a) For a positive integer n, define a primitive root modulo n. 1

   b) Using the result "an element $a\in U_n$ is a primitive root modulo n if and only if $a^{\phi(n)/q}\neq 1$ in U_n for each prime q dividing $\phi(n)$". 3

   i) check if 3 is a primitive root modulo 7.

   ii) find a primitive root modulo 9.

   c) State for which integers n, there exists primitive root modulo n. 1

2. Let n be a positive integer and Q_n denote the set of elements $a\in U_n$ which are quadratic residues modulo n.

Prove that $1, ab, a^{-1}\in Q_n \forall a, b\in Q_n$. If $n>2$ and g is a primitive root modulo n then prove that Q_n has $\frac{\phi(n)}{2}$ elements which are even powers of g. 2+3

3. a) Let p be an odd prime and $\left(\frac{a}{p}\right)$ denotes the *Legendre symbol*. Prove that $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\forall a,b$. 2

   b) Find the number of solutions to the congruence $x^{39}\equiv 1(\text{mod } 79)$.

   State the relevant result that might have been used to solve the above problem. 3

4. a) Determine $\left(\frac{2}{59}\right)$ and hence determine if the congruence $x^2\equiv 2(\text{mod } 59)$ has solution. 3

   b) Using Quadratic reciprocity law determine $\left(\frac{3}{61}\right)$. 2

5. Find all prime p such that $\left(\frac{10}{p}\right)=1$. 5

6. a) Determine the number of solutions of the congruence $x^4\equiv 61(\text{mod } 117)$. 2

   b) State the results used in solving the problem in (a). 3