2021
B.A./B.Sc.
Fifth Semester
DSE – 1
MATHEMATICS
Course Code: MAD 5.11
(Number Theory)

Total Mark: 70 *Pass Mark: 28*
Time: 3 hours

Answer five *questions, taking* one *from each unit.*

UNIT–I

1. (a) A customer bought a dozen pieces of fruit, apples and oranges for Rs. 132.00. If an apple costs Rs. 3.00 more than an orange and more apples than oranges were purchased, how many pieces of each kind were bought? 7
   (b) State and prove Fermat's theorem. 7
2. (a) Solve the linear congruence $17x \equiv 9 (\mathrm{mod}\, 276)$. 7
   (b) Prove that the quadratic congruence $x^2 + 1 \equiv 0 (\mathrm{mod}\, p)$, where p is an odd prime, has a solution if and only if $p \equiv 1 (\mathrm{mod}\, 4)$. 7

UNIT–II

3. (a) Prove that $\sigma(n)$ is an odd integer if and only if n is a perfect square or twice a perfect square. 7
   (b) State and prove the Möbius inversion formula. 7
4. (a) If F is a multiplicative function and the $F(n) = \sum_{d|n} f(d)$, then prove that f is also multiplicative. 7
   (b) The Mangoldt function Λ is defined by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k, \text{ where } p \text{ is a prime and } k \geq 1 \\ 0 & \text{otherwise} \end{cases}$$

Prove that $\Lambda(n) = \sum_{d|n} \mu(n/d)\log d = -\sum_{d|n} \mu(d)\log d$. 7

UNIT–III

5. (a) Find the highest power of 7 dividing 2000!. 3
   (b) For any real numbers x, y show that
   $[x]+[y] \le [x+y] \le [x]+[y]+1$ 4
   (c) State and prove the Euler's theorem. 7
6. (a) Show that $\phi(3n) = 3\phi(n)$ if and only if $3|n$. 4
   (b) Show that $[[x]/m] = [x/m]$ for any real number x and positive integer m. 3
   (c) Prove that the Euler's phi function ϕ is a multiplicative function. 7

UNIT–IV

7. (a) If the integer a has order k modulo n, prove that $a^h \equiv 1 (\mathrm{mod}\, n)$ if and only if $k|h$. 6
   (b) If r is a primitive root of p, then prove that $r^{(p-1)/2} \equiv -1 (\mathrm{mod}\, p)$. 4
   (c) Determine if the congruence $x^2 \equiv 219 (\mathrm{mod}\, 419)$ is solvable. 4
8. (a) State and prove Gauss's lemma. 7
   (b) Evaluate the Legendre symbol $\left(\frac{1234}{4567}\right)$. 3
   (c) Solve the quadratc congruence $x^2 \equiv 2 (\mathrm{mod}\, 7^3)$. 4

UNIT–V

9. (a) Decipher the message BBOT XWBZ AWUVGK, which was produced by the autokey cipher with seed RX. 4
   (b) Prove that the area of a pythagorean triangle can never be equal to a perfect (integral) square. 5
   (c) If x, y, z is a primitive Pythagorean triple, then prove that one of the integers x or y is even, while the other is odd. 5
10. (a) Show that the equation $x^2 + y^2 = z^3$ has infinitely many solutions for x, y, z positive integers. 5

(b) Suppose that the following ciphertext is received by a person having ElGamal public key (71, 7, 32) and private key $k = 30$:

(56,45) (56,38) (56,29) (56,03) (56,67)
(56,05) (56,27) (56,31) (56,38) (56,29)

Obtain the plaintext message. 5

(c) Find two different Pythagorean triplets, not necessarily primitive, of the form 16, y, z. 4
