[This question paper contains 4 printed pages.]

Your Roll No.....

Sr. No. of Question Paper : 1696 **G**

Unique Paper Code : 2353012003

Name of the Paper : Number Theory

Name of the Course : **B.Sc. (H) Mathematics – DSE**

Semester : III

Duration : 3 Hours Maximum Marks : 90

Instructions for Candidates

1. Write your Roll No. on the top immediately on receipt of this question paper.
2. Attempt **all** questions by selecting **two** parts from each question.
3. Both parts of a question to be attempted together.
4. **All** questions carry equal marks.
5. Use of Calculator not allowed.

1. (a) When Mr. Smith cashed a check at his bank, the teller mistook the number of cents for the number of dollars and vice versa. Unaware of this, Mr. Smith spent 68 cents and then noticed to his

P.T.O.

surprise that he had twice the amount of the original check. Determine the smallest value for which the check could have been written. (7.5)

(b) Solve the linear congruence $17x \equiv 3 (\text{mod } 2 \cdot 3 \cdot 5 \cdot 7)$. (7.5)

(c) Verify that $0, 1, 2, 2^2, 2^3, \ldots, 2^9$ form a complete set of residues modulo 11, but that $0, 1^2, 2^2, 3^2, \ldots, 10^2$ do not. (7.5)

2. (a) State and prove Wilson's Theorem. (7.5)

(b) (i) If $\gcd(a, 30) = 1$, show that 60 divides $a^4 + 59$. (4.5)

(ii) Use Fermat's theorem to verify that 17 divides $11^{104} + 1$. (3)

(c) If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then derive the formulae for $\tau(n)$ and $\sigma(n)$, where $\tau(n)$ denotes the number of positive divisors of n and $\sigma(n)$ denotes the sum of these divisors. Also, show that the product of positive divisors of n is $n^{\frac{\tau(n)}{2}}$. (7.5)

3. (a) State and prove Euler's theorem. Find the last two digits of 3^{256}. (4+3.5)

(b) For each positive integer n, show that $\mu(n)\,\mu(n+1)\,\mu(n+2)\,\mu(n+3) = 0$ Also, show that for any integer $n \geq 3$, $\sum_{k=1}^{n} \mu(k!) = 1$. (4+3.5)

(c) (i) Find the highest power of 9 dividing 901!. (4.5)

(ii) Determine all primitive roots of 3^2. (3)

4. (a) (i) Show that if the integer n has r distinct odd prime factors, then 2^r divides $\emptyset(n)$, where $\emptyset$ is the Euler Phi function. (3.5)

(ii) Use Euler's theorem to show that for any integer a,

$$a^{37} \equiv a \pmod{1729}.$$ (4)

(b) Prove that for any integer a, a and a^{4n+1} have same last digit. (7.5)

(c) (i) Show that if $F_n = 2^{2n} + 1$, $n > 1$, is a prime, then 2 is not a primitive root of F_n. (3.5)

(ii) Let r be a primitive root of the odd prime p. Show that if $p \equiv 1 \pmod 4$, then $-r$ is also a primitive root of the odd prime p. (4)

5. (a) Define a quadratic residue of an odd prime p.

Let p be an odd prime and gcd(a, p) = 1. Then

prove a is a quadratic residue of p if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Hence show that 3 is a quadratic residue of 23, but a quadratic nonresidue of 31. (1+4+2.5)

(b) (i) Let p be an odd prime and let a and b be integers relatively prime to p. Then prove $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Hence calculate $\left(\frac{1234}{4567}\right)$. (2+3)

(ii) Is $x^2 \equiv -46 \pmod{17}$ solvable ? (2.5)

(c) (i) Show that there are infinitely many primes of the form $6k + 1$. (3)

(ii) Solve the quadratic congruence $x^2 \equiv 7 \pmod{3^2}$. (4.5)

6. (a) Encrypt the message HAPPIEST MINDS using the linear cipher

$$C \equiv 5P + 11 \pmod{26}.$$ (7.5)

(b) Use the Hill Cipher

$$C_1 \equiv 4P_1 + 2P_2 \pmod{26}$$
$$C_2 \equiv 3P_1 + 8P_2 \pmod{26}$$

to encipher the message ACT NOW. (7.5)

(c) Encrypt the plaintext message PAINTS using RSA algorithm, with key (2701,7). (7.5)