5. (a) Prove that the quadratic congruence $6x^2+5x+1 \equiv 0 \pmod{p}$ has a solution for every prime p, even though the equation $6x^2+5x+1 \equiv 0 \pmod{p}$ has no solution in the integers. 7.5

(b) (i) Prove that there are infinitely many primes of the form 4k + 1. 4

(ii) Show that 3 is quadratic residue of 23 but quadratic non residue of 31. 3.5

(c) The cipher text VKYAQ VAKEC has been enciphered with the Linear Cipher $C \equiv 17P+10 \pmod{26}$

Derive the plaintext. 7.5

6. (a) Prove that 2 is not a primitive root of any prime of the form $p = 3.2^n + 1$ except when p = 13. 7.5

(b) Find the value of Legendre symbols (461/773) and (– 219/383). 7.5

(c) Use the Hill's cipher $C1 \equiv 5P1 + 2P2 \pmod{26}$ $C2 \equiv 3P1 + 4P2 \pmod{26}$ to encrypt the message GIVE THEM TIME. 7.5

***

[This question paper contains 4 printed pages].

Your Roll No. : ....

Sl. No. of Q. Paper : 1232 I

Unique Paper Code : 2353012003

Name of the Paper : Number Theory DSE-1

Name of the Course : **B.Sc.(Hons.) Mathematics**

Semester : V

Time : 3 Hours ***Maximum Marks : 90***

Instructions for Candidates :

(a) Write your Roll No. on the top immediately on receipt of this question paper.

(b) Attempt **all** questions by selecting **two** parts from each question.

(c) **All** questions carry equal marks.

(d) Use of Calculator not allowed.

1. (a) (i) Use the Euclidean Algorithm to find integers x and y satisfying

$\gcd(1769, 2378) = 1769x + 2378y$ 4

(ii) Determine all solutions in the integers of the Diophantine equation

$221x + 35y = 11$ 3.5

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

(c) Obtain the **two** incongruent solutions modulo 210 of the system 7.5

$$2x \equiv 3 \pmod 5$$

$$4x \equiv 2 \pmod 6$$

$$3x \equiv 2 \pmod 7$$

2. (a) (i) Make use of Fermat's theorem to prove that, if p is an odd prime, then

$$1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots + (p-1)^{p-1} \equiv -1 \pmod p$$ 4

(ii) For any integer a, verify that a^5, and 'a' have the same units digit. 3.5

(b) If p is a prime, prove that for any integer a, 7.5

$$p \mid a^p + (p-1)!a \text{ and } p \mid (p-1)!a^p + a$$

(c) Prove that if $n = p_1^{k_1}.p_2^{k_2}.......p_r^{k_r}$. is a prime factorization of n > 1, then 7.5

$$\sigma(n) = \left(\frac{p_1^{k_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{k_2+1}-1}{p_2-1}\right)\cdots\cdots\left(\frac{p_r^{k_r+1}-1}{p_r-1}\right)$$

3. (a) If F is a multiplicative function and $F(n) = \sum_{d/n} f(d)$.

Then show that f is also multiplicative. 7.5

(b) (i) For n > 2, Show that $\phi(n)$ is an even integer. 3.5

(ii) Determine the day of the week January 10, 2020. 4

(c) If $F_n = 2^{2^n} + 1, n > 1$ is a prime then show that 2 is not a primitive root of F_n. 7.5

4. (a) If the integer a has order k modulo n, then $a^i \equiv a^j$ (mod n) if and only if $i \equiv j$ (mod n). 7.5

(b) (i) Determine all primitive roots of 11. 3.5

(ii) Use Euler Theorem to show that for any integer a,

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

(c) 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=7.5