6. (a) State Gauss Lemma and prove that :

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

(b) Define Jacobi symbol evaluate the following :

(i) $\left(\frac{-35}{97}\right)$

(ii) $\left(\frac{51}{71}\right)$

(iii) $\left(\frac{10}{127}\right)$

Unit IV

7. (a) Define monoalphabetic and polyalphabetic cipher systems by taking suitable examples and explain the encryption and decryption method of Hill Cipher.

(b) Encipher the message HAVE A NICE TRIP using a Vigenere cipher with the keyword MATH.

No. of Printed Pages : 5 **Roll No. ....**

II344

M.Sc. Mathematics (5 Year Integrated) EXAMINATION, May 2019

(Ninth Semester)

(B. Scheme) (Re-appear)

B.Sc. (Hons.) M.Sc. (Mathematics)

MAT617H

ANALYTICAL NUMBER THEORY AND CRYPTOGRAPHY

Time : 3 *Hours*] [*Maximum Marks :* 75

Before answering the question-paper candidates should ensure that they have been supplied to correct and complete question-paper. No complaint, in this regard, will be entertained after the examination.

Note : Attempt *Five* questions in all, selecting at least *one* question from each Unit.

Unit I

1. (a) Prove that primes one infinite in number. **5**

(b) Prove that $gcd\ (F_m, F_n) = 1$, where $m > n \geq 0$ and F_m and F_n are Fermat numbers. **5**

(c) If $\frac{a}{b}$ and $\frac{a'}{b'}$ are consecutive fractions in the 4th row, then prove that $a'b - ab' = 1$. **5**

2. (a) Let θ be a rational multiple of π. Then prove that cos θ, sin θ, tan θ are irrational numbers apart from the cases where tan θ is undefined and – ve exceptions

$\cos\theta = 0, \ \pm\frac{1}{2}, \pm 1;\ \sin\theta = 0, \ \pm\frac{1}{2}, \pm 1;$

$\tan\theta = 0, \ \pm 1.$ **10**

(b) State Hurwitz theorem and prove that $\sqrt{5}$ appearing in Hurwitz theorem is the best possible. **5**

Unit II

3. (a) Prove that energy prime of the form $4\ k + 1$ can be written as a sum of two squares. **10**

(b) Find all solutions in positive integers of $15x + 7y = 111$. **5**

4. (a) Define $G(k)$ and prove that $G(2^\theta) \geq 2^{\theta+2}$. **7½**

(b) Find all integers that give the remainders 1, 2, 3 when divided by 3, 4, 5 respectively. **7½**

Unit III

5. (a) If p is a prime, then the group U_p has $\phi\ (d)$ elements of order d for each d dividing $p - 1$ and hence prove that U_p is cyclic.

(b) If $e \geq 3$, then prove that :

$$U_{2^e} = \{\pm\ 3^i \mid 0 \leq i < 2^{e-2}\}$$

8\. (a) Construct a multiplex sequence in a binary field F_2 using the sequences $s_0, s_1, s_2,$ .... and $t_0, t_1, t_2,$ .... in F_2 with $s_{n+3}, = s_{n+1} + s_n$ for $n = 0, 1, 2,$ .... $t_{n+4}, = t_{n+3} + t_n$ for $n = 0, 1, 2,$ .... and initial state vectors (1, 0, 0) and (1, 0, 0, 0) respectively.

(b) The message NOT NOW is to be sent to a user of the Elgamal system who has public key (37, 2, 18) and private key $k = 17$. If the integer j used to construct the cipher text is changed over successive four digit blocks from $j = 13$ to $j = 28$ to $j = 11$. What is the encrypted message produced ?

8\. (a) Construct a multiplex sequence in a binary field F_2 using the sequences $s_0, s_1, s_2,$ .... and $t_0, t_1, t_2,$ .... in F_2 with $s_{n+3}, = s_{n+1} + s_n$ for $n = 0, 1, 2,$ .... $t_{n+4}, = t_{n+3} + t_n$ for $n = 0, 1, 2,$ .... and initial state vectors (1, 0, 0) and (1, 0, 0, 0) respectively.

(b) The message NOT NOW is to be sent to a user of the Elgamal system who has public key (37, 2, 18) and private key $k = 17$. If the integer j used to construct the cipher text is changed over successive four digit blocks from $j = 13$ to $j = 28$ to $j = 11$. What is the encrypted message produced ?