(b) State quadratic law of reciprocity and using this find all primes p such that $\left(\frac{3}{5}\right) = \pm 1$. **15**

Unit IV

7. (a) Define the notion of Discrete logarithm. Find a primitive root modulo 17 and hence determine the discrete logarithm of 5, 7 and 10 for the prime 17 with base as above obtain primitive root.

(b) Define multiplexed sequence $u_0, u_1, \ldots\ldots$ in a finite field F_p, having prime no. of elements p. If $s_0, s_1, s_2, \ldots\ldots$ be a kth order and $t_0, t_1, t_2, \ldots\ldots$ an m-th order maximal period sequence in F_p. Then prove that sequence $u_0, u_1, u_2, \ldots\ldots$ is periodic and its least period divides $\lim(p^k-1, p^n-1)$. **15**

8. (a) Ram uses the RSA cryptosystem to receive message from Sita. He chooses

No. of Printed Pages : 05 Roll No. ....

II-344

Dual Degree/B.Sc. (Hons.)

M.Sc. (Mathematics) EXAMINATION, Dec. 2018

(Ninth Semester)

(Main & Re-appear)

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 the primes of the form $4k+1$ are infinite in number.

   (b) In p_n is the n the prime then prove that $p_n \le 2^{2^{n-1}}$.

   (c) Prove that the number of Farey fractions $\frac{a}{b}$ of order n satisfying the inequalities $0 \le \frac{a}{b} \le 1$ is $1+\sum_{j=1}^{n}\phi(j)$ and that their sum is exactly half this value. **15**

2. (a) Prove that π is irrational.

   (b) State and prove Hurwitz theorem. **15**

Unit II

3. (a) Prove that all the solutions of $x^2+y^2=z^2$ is integers x, y, z such that $x>0$, $y>0$, $z>0$, gcd$(x, y)=1$ and x is even are given by $x = 2ab$, $y = a^2 - b^2$, $z = a^2 + b^2$, where a and b satisfy the conditions that $a > b > 0$, gcd $(a, b) = 1$ and a and b have opposite parity. **10**

   (b) Prove that $g(2) = 4$. **5**

4. (a) Prove that $G(k) \ge k + 1$, $k \ge 2$.

   (b) Find the general solution of the simultaneous congruences : $x \equiv 11 \pmod{36}$, $x \equiv 7 \pmod{40}$ and $x \equiv 32 \pmod{75}$ **15**

Unit III

5. (a) State and prove Gauss-Lemma on quadratic residues. **7**

   (b) Define Z_n and prove that for each integer $x \ge 1$ the set U_n forms an abelian group under multiplication modulo n. **4**

   (c) Prove that the group U_2e is cyclic if and only if $e = 1$ or $e = 2$. **4**

6. (a) Let p be an odd prime and $a \in Z$. Then prove that $a \in Q_pe$ if and only if $a \in Q_p$ where $e \ge 1$ and Q_pe denotes the set of quadratic residues modulo p^e.

primes p = 11, q = 17 and the public key K = 23. Check whether K = 23 is a valid public key (exponent). Find the recovery (private) key of Ram. Sita wants to send Ram the plaintext U, that is, '20'. Verify Ram can decrypt this message.

(b) The message SELL NOW is to be encrypted in the Elgamal cryptosystem and forwarded to a user with public key (43, 3, 22) and private key = 15. If the random integer chosen for encryption is j = 25, determine the ciphertext. **15**

primes p = 11, q = 17 and the public key K = 23. Check whether K = 23 is a valid public key (exponent). Find the recovery (private) key of Ram. Sita wants to send Ram the plaintext U, that is, '20'. Verify Ram can decrypt this message.

(b) The message SELL NOW is to be encrypted in the Elgamal cryptosystem and forwarded to a user with public key (43, 3, 22) and private key = 15. If the random integer chosen for encryption is j = 25, determine the ciphertext. **15**