Unit IV

7. (a) If $r \geq 3$, then show that :

$$U_{2^r} = \left\{\pm 3^i : 0 \leq i \leq 2^{r-2}\right\}$$

(b) Prove that the group U_n is cyclic for every $n = 1, 2, 4, p^r$ or $2p^r$, where p is a prime and r is a positive integer.

8. (a) Let x be any primitive roots modulo p^2, then prove that x is a primitve root modulo p^e for all $e \geq 2$.

(b) Show that the cubic polynomial $x^3 - 1$ has nine roots in $\mathbf{Z}_{63}$.

CC-314

M.Sc. EXAMINATION, May 2017

(Third Semester)

(Re-appear Only)

(MATH)

MAT-609-B

Analytical Number Theory-I

Time : 3 *Hours*] [*Maximum Marks :* 100

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. All questions carry equal marks.

Unit I

1. (a) Suppose that $gcd\ (a,\ m) = 1$, then prove that $a^{\phi(m)} \equiv 1 \pmod{m}$. Deduce that $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ is an integer for every integer n.

(b) Prove that if n is composite, then $2^n - 1$ is also composite. Is the converse true ?

2. (a) Show that there are infinitely many primes of the form $4k + 1$.

(b) State and prove Wilson's theorem.

Unit II

3. (a) Find all integers that give remainder 1, 2, 3 when divided by 3, 4, 5 respectivley.

(b) State Hurwitz theorem and prove that the constant in Hurwitz is the least possible.

4. (a) If $gcd(a,\ m) = 1$, then prove that $ax \equiv b (\text{mod } m)$ has exactly one solution. Using this solve linear Diophantine equation $9x + 16y = 35$.

(b) Prove that π is irrational.

Unit III

5. (a) Prove that every prime of the form $4n + 1$ can be written as a sum of two squares.

(b) Let p be an odd prime and $gcd\ (a,\ p) = 1$. Then prove that a is a quadratic residue or non-residue of p accordingly as : $a^{(p-1)/2} \equiv 1 \ (\text{mod } p)$, $a^{(p-1)/2} \equiv -1 \ (\text{mod } p)$ Find all quadratic resiude and non-residue for $p = 13$.

6. (a) Prove that $G(2) = 4$.

(b) Define Jacobi Symbol. Suppose that P and Q is odd and P, Q > 0, then prove that :

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{(P-1)(Q-1)/4}$$