(Pages : 3) **4148**

Reg. No. : ....

Name : ....

M.Sc. Final Degree Examination, July 2009
(I.D.E.)
Branch : MATHEMATICS
MM 1212 : Elective – II – Analytic Number Theory
(Common for 2006 Admn. and Prior to 2006 Admission)

Time : 3 Hours Max. Marks : 85

Instructions : *i) Answer either Part* ***A*** *or Part* ***B*** *of* ***each*** *question.*
ii) ***All*** *questions carry* ***equal*** *marks.*

I. A) i) Show that every integer $n > 1$ can be represented as a product of prime factors in only one way apart from the order of the factors. **6**

ii) Given integers a and b show that there is one and only one number d with the following properties.

i) $d \geq 0$

ii) d divides a and d divides b

iii) If e divides a and e divides b then e divides d. **7**

iii) If $(a, b) = 1$ then show that $(a + b, a – b)$ is either 1 or 2. **4**

I. B) i) State and prove Euclidean algorithm. **7**

ii) Show that $\sum_{n=1}^{\infty} \frac{1}{p_n}$ diverges. **6**

iii) Given x and y, let $m = ax + by$, $n = cx + dy$ where $ad – bc = \pm 1$. Prove that $(m, n) = (x, y)$. **4**

P.T.O.

II. A) i) Define the Möbius function. Show that $\sum_{d/n} \mu(d) = \left[\frac{1}{n}\right]$ **5**

ii) Define multiplicative and completely multiplicative functions. Show that a multiplicative function f is completely multiplicative if and only if $f^{-1}(n) = \mu(n) f(n)$ for all $n \geq 1$. **7**

iii) Find the Bell series for Euler's totient ϕ. **5**

II. B) i) Show that $\sum_{d/n} \phi(d) = n$ **5**

ii) Show that the set of all arithmetical functions form a group under Dirichlet multiplication. **8**

iii) Show that $\sum_{d/n} \lambda(d) = 1$ if n is a square and zero otherwise. **4**

III. A) i) State and prove Lagrange's theorem. **8**

ii) State and prove Chinese remainder theorem. Deduce that the set of all lattice points in the plane visible from the origin has arbitrarily large square gaps. **(5+4)**

III. B) i) Let $n \geq 2$. Let r be a solution of the congruence $f(x) \equiv 0 \bmod (p^{\alpha - 1})$ lying in the interval $0 \leq r < p^{\alpha - 1}$, show that if $f'(r) \not\equiv 0 \pmod p$ then r can be lifted in a unique way from $p^{\alpha - 1}$ to p^{α}. **6**

ii) Let r, d and k be positive integers with d/k and (r, d) = 1. Show that the number of elements in the set s = {r + td : t = 1, 2, ... k/d} which are relatively prime to k is $\phi(k)/\phi(d)$. **7**

iii) Let (a, m) = 1 show that $ax \equiv b \pmod m$ has exactly one solution. **4**

IV. A) i) State and prove the quadratic reciprocity law. **6**

ii) State and prove Gauss Lemma. **7**

iii) Show that $(2|p) = (-1)^{(p^2 - 1)/8}$. **4**

IV. B) i) Find (219|383). **4**

ii) Show that the Diophantins equation $y^2 = x^3 + k$ has no solution if k has the form $(4n - 1)^3 - 4m^2$ where m and n are integers such that no prime $p \equiv -1 \pmod 4$ divides m. **7**

iii) State and prove Euler's criterion. **6**

V. A) i) If p is an odd prime and $\alpha \geq 1$, show that there exist odd primitive roots of modulo p^{α} and each such g is also a primitive root mod $2p^{\alpha}$. **6**

ii) Let p be an odd prime. Show that there are exactly $\phi(p - 1)$ primitive roots mod p. **7**

iii) Let g be a primitive root mod p, where p is an odd prime. Show that $g^2, g^4, ..., g^{p-1}$ are quadratic residues mod p. **4**

V. B) i) Let $m \neq 1, 2, 4, p^{\alpha}, 2p^{\alpha}$ where p is an odd prime. Show that there are no primitive roots mod m. **8**

ii) Show that there are no primitive roots mod 2^{α}. **5**

iii) Let g be a primitive root mod p such that $g^{(p-1)} \not\equiv 1 \pmod{p^2}$. Show that $g^{\phi(p\alpha - 1)} \not\equiv 1 \pmod{p^{\alpha}}$ for every $\alpha \geq 2$. **4**
