MCA.II/05.14.0473

B

M.C.A. DEGREE II SEMESTER EXAMINATION MAY 2014

CAS 2205/2202 NUMBER THEORY

(New Scheme – Supplementary)

Time: 3 Hours Maximum Marks : 50

PART A

(Answer ***ALL*** questions)

(15 x 2 = 30)

I. (a) Prove that there are infinitely many primes.
(b) Find the gcd of 595 and 252.
(c) If P is prime and P/ab, then prove that P/a or P/b.

II. (a) State and prove Wilson's theorem.
(b) Solve the congruence $6x \equiv 15 \pmod{21}$,
(c) Prove that equation $y^2 = x^3 - 2$ has only the integer solutions $(3, \pm 5)$.

III. (a) Show that Legendre's symbol (n/p) is a complete multiplicative function of n.
(b) Find the quadratic residue modulo II.
(c) Define Jacobi symbol.

IV. (a) Apply Rho method to factor 4087 with $f(x) = x^2 + x + 1$ and $x_o = 2$.
(b) What are pseudoprimes?
(c) Define simple continued fraction.

V. (a) Define zero-knowledge protocol.
(b) How do you send a signature in RSA?
(c) What are the basic requirements for a digital signature?

PART B

(5 x 4 = 20)

VI. State and prove Chinese Remainder theorem.

OR

VII. State and prove Fermat's theorem.

VIII If P is prime and $P \equiv 1 \pmod{4}$ then show that there exist integers a and b such that $a^2 + b^2 = p$.

OR

IX. Solve $x \equiv 12 \pmod{31}$

$x \equiv 87 \pmod{127}$

$x \equiv 91 \pmod{255}$

X. State the law of quadratic reciprocity. Determine the odd primes P for which 3 is a quadratic residue and those for which it is a non-residue.

OR

XI. Prove that $(2/p) \equiv (-1)^{(p^2-1)/8}$ where P is an odd positive integer.

XII. Explain Fermat's factorization method.

OR

XIII. Describe the elliptic curve factorization.

XIV. Explain the RSA cryptosystem.

OR

XV. Explain the requirements for message authentification codes.

***