 LOYOLA COLLEGE (AUTONOMOUS), CHENNAI – 600 034

**M.Sc.** DEGREE EXAMINATION - **MATHEMATICS**

THIRD SEMESTER – **NOVEMBER 2012**

# MT 3960 - NUMBER THEORY AND CRYPTOGRAPHY

Date : 08/11/2012 Dept. No. Max. : 100 Marks

Time : 9:00 - 12:00

ANSWER ALL QUESTIONS

I a ) Describe subtraction bit operations.

[OR]

b) Prove that . (5)

c) i) If eggs are removed from a basket 3, 5 and 7 at a time there remain respectively

1, 2 and 3 eggs . Using Chinese Remainder Theorem, find the least number of

eggs that could have been in the basket.

ii) If 

[OR]

d) i) Find the upper bound for the number of bit operations required to compute 

ii) Prove that the Euclidean algorithm always gives the greatest common divisor in

a finite number of steps. (8 + 7)

II a) State and prove any two properties of Legendre’s symbols.

[OR]

b) Find the value of the Legendre’s symbol . (5)

c) Prove that  where is a prime number. (15)

[OR]

d) (i) Prove that the order of any  .

(ii) Find the Gaussian sum  (8 + 7)

III a) Decipher the message DWWDF NDWGD ZQ, which was enciphered

using Ceasar cipher.

[OR]

b)Decipher FWMDIQ , which has been enciphered using the matrix

 (5)

c) i) Discuss about Knapsack ciphers.

ii) Solve the Knapsack problem . (8 + 7)

[OR]

1. A person is using 2 x 2 enciphering matrix with a 29 letter alphabet, where A – Z

have the usual numerical equivalents , blank = 26, ? = 27, ! = 28. He receives the message “GFPYJP X?UYXSTLADPLW”. He knows that the last five letters of the plaintext are KARLA . Find the deciphering matrix and read the message. (15)

IV a) Find all bases for which 21 is a pseudo prime.

[OR]

b) If *n* is an Euler pseudo prime to the base *b* , then prove that it is a pseudo prime

to the base *b* .Also discuss about the converse. (5)

c) Let *n* be an odd composite integer. Then prove that

(i) *n* is a pseudoprime to the base *b*, where g.c.d*.(b, n)* = 1, then *n* is a pseudoprime

to the base 

(ii) *n* is a pseudoprime to the base *b*, where g.c.d*.(b, n)* = 1, if and only if the order

of *b* in *( Z/nZ )\** divides *n -*1

(iii) *n* is a pseudoprime to the bases , then *n* is a pseudoprime to the base

and also to the base  .

(iv) If *n* is not a pseudoprime to a single base *b**( Z/nZ )\**, then *n* is not a

pseudoprime to atleast half of the possible bases *b**( Z/nZ )\**

[OR]

d) Discuss about any two primality tests (15)

V a) Check whether 141467 is a prime number.

[OR]

b) Write a note on Fermat factorization method (5)

c) Let E be the elliptic curve  defined over . Then

i) List the points on E

ii) Compute P + Q if P = (2, 3) and Q = (4, 0)

iii) Compute 2P if P = (2, 3) (7 + 4 + 4)

[OR]

d) Write about elliptic curve discrete log problem. (15)