LOYOLA COLLEGE (AUTONOMOUS), CHENNAI – 600 034

M.Sc. DEGREE EXAMINATION – **MATHEMATICS**

SECOND SEMESTER – **APRIL 2022**

PMT 2602 – NUMBER THEORY AND CRYPTOGRAPHY

Date: 24-06-2022 Dept. No. Max. : 100 Marks

Time: 09:00 AM - 12:00 NOON

Answer all questions:

1. a) Find the g.c.d of 1547 and 560.

OR

b) If g.c.d (a, m) =1, then prove that $a^{\varphi(m)} \equiv 1 \bmod m$. (5)

c) i) Prove that the Euclidean algorithm always gives the greatest common divisor in a finite number of steps. In addition prove that for *a>b* the time of finding the G.C.D (a, b) by Euclidean algorithm is $O\left(\log^3(a)\right)$.

ii) Compute $2^{1000000} \bmod 77$. (9+6)

OR

d) i) State and prove Fermat's little theorem.

ii) State and prove Chinese Reminder theorem. (7+8)

2. a) Generate all the residues *mod*19 from 1 to 18 taking all the powers of 2.

OR

b) Prove that order of any $a \in F_q^*$ divides $q-1$. (5)

c) i) Define Quadratic residues and find the residues of F_{11}^*.

ii) Determine whether 7411 is a residue modulo to the prime 9283. (7+8)

OR

d) i) State and prove the law of quadratic reciprocity.

ii) Prove that every finite field has a generator. If *g* is a generator of F_q^*, then g^j is also a generator if and only if g.c.d$\left(j, q-1\right)=1$. In particular, there are a total of $\varphi(q-1)$ different generators of F_q^*. (8+7)

3. a) Define affine enciphering transformations of matrices.

OR

b) For $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in M_2(Z/26Z)$, encipher the plain text "NOANSWER". (5)

(P.T.O)

c) With the 26 alphabets and blank space as the 27th alphabet and with the digraph having numerical equivalence to $x + y$ and the most frequently occurring digraphs are in order ZA , IA and IW corresponding to the most frequent language " E " (E and space), "S " (S and space) and " T(space and T), use affine transformation of modulo 729 to find the deciphering key and read the message "NDXBHO".

(15)

OR

d) Suppose that we know that our adversary is using a 2x2 enciphering matrix with 29- letter alphabet, where A-Z have the usual numerical equivalents , blank=26, ?= 27, != 28. Encipher the text "GFPYJP X?UYXSTLADPLW" where we know that the last five letters of the plain text is "KARLA" Using only the last four letters of the plain text with digraphs DP and LW correspond to the plain text AR and LA encipher the text. (15)

4. a) Define Carmichael number with an example.

OR

b) Find the factor of 200819. (5)

c) i) Explain the Rho method for primality test.

ii) Factor 4087 using $f(x) = x^2 + x + 1$ and $x_0 = 2$. (8+7)

OR

d) Prove that if *n* is a strong pseudo prime to the base *b*, then it is an Euler pseudo prime to the base *b*. (15)

5. a) Find the order of P= (2,3) on $y^2 = x^3$.

OR

b) Define elliptic curve over field K with an example. (5)

c) State and prove Hasse's theorem and find the type of $y^2 = x^3 - x$ over F_{71}.

OR

d) Discuss the nature of elliptic curve over the field of reals. (15)

##########