

Roll No.

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Total No. of Pages : 02

Total No. of Questions : 07

M.Sc Mathematics (2017 Batch) (Sem.-3)
NUMBER THEORY AND CRYPTOGRAPHY
Subject Code : MSM-302
Paper ID : [75382]

Time : 3 Hrs.

Max. Marks : 80

INSTRUCTION TO CANDIDATES :

1. **SECTION-A** is **COMPULSORY** consisting of **EIGHT** questions carrying **TWO** marks each.
2. **SECTION - B & C.** have **THREE** questions in each section carrying **SIXTEEN** marks each.
3. **Select atleast TWO** questions from **SECTION - B & C EACH.**

SECTION-A

1. Answer briefly :

- (a) If $p \neq 5$ is an odd prime, prove that either $p^2 - 1$ or $p^2 + 1$ is divisible by 10.
- (b) Find order of 3, modulo 23. <http://www.punjabpapers.com>
- (c) Find the index of 5 relative to each of the primitive roots of 13.
- (d) Show that μ is a multiplicative function.
- (e) Find the remainder when $2(26!)$ is divided by 29.
- (f) Show that $\sqrt{2}$ is irrational.
- (g) Evaluate Legendre Symbol $(7/13)$.
- (h) Show that $\phi(2n) = \phi(n)$, if n is odd integer.

SECTION-B

2. (a) If $p \neq 5$ is an odd prime, prove that either $p^2 - 1$ or $p^2 + 1$ is divisible by 10.

- (b) State and prove Chinese Remainder Theorem.
3. (a) For what value of $n \geq 1$, $1! + 2! + 3! + \dots + n!$ is a perfect square.
- (b) State and prove Wilson's Theorem and its converse.
4. (a) Determine whether the 1-56947-303-10 is a correct ISBN (International Standard Book Number) or not. Justify your answer.
- (b) Let r be a primitive root of the odd prime p . Prove the following:
- If $p \equiv 1 \pmod{4}$, then $-r$ is also a primitive root of p .
 - If $p \equiv 3 \pmod{4}$, then $-r$ has order $(p-1)/2$ modulo p .

<http://www.punjabpapers.com>

SECTION-C

5. (a) Use indices to solve the congruences: $7x^3 \equiv 3 \pmod{11}$
- (b) Evaluate Legendre Symbol: $(19/23)$
6. (a) If n is a positive integer, show that
- $$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0.$$
- (b) If p and q are distinct primes, prove that for any integer a .
- $$pq \mid a^{pq} - a^p - a^q + a.$$
7. (a) In RSA, given $N=187$ and the encryption key (E) as 17, find out the corresponding private key (D).
- (b) Use the Hill cipher

$$C_1 \equiv 5P_1 + 2P_2 \pmod{26}$$

$$C_2 \equiv 3P_1 + 4P_2 \pmod{26}$$

to encipher the message "GIVE THEM TIME".