KATHMANDU UNIVERSITY
End Semester Examination
May/June, 2022

Level : B.Sc.
Year : III
Time : 2 hrs.30 mins.

Course : MATH 327
Semester : II
F.M : 50

SECTION "C"
[6 Q. × 7 = 42 marks]

1. Prove that if d is a common divisor of a and b, then $d = \gcd(a, b)$ if and only if $\gcd(a|d, b|d) = 1$. There were 63 equal piles of plantain fruit put together and 7 single fruits. They were divided evenly among 23 travelers. What is the number of fruits in each pile? [3+4]

2. Define a linear congruence *modulo* m. Give an example to show that $a^2 \equiv b^2 (mod\ m)$ need not imply that $a \equiv b(modm)$. Find the solution of the given system of congruence. [1+2+4]

$$11x + 5y \equiv 7(mod20)$$

$$6x + 3y \equiv 8(mod20)$$

OR

Define congruence modulo. State Chinese Remainder theorem. Solve the following set of simultaneous congruence. [1+2+4]

$$x \equiv 5(mod6)$$

$$x \equiv 4(mod11)$$

$$x \equiv 3(mod17)$$

3. State and prove Fermat's Little Theorem. Clarify with a counterexample that the converse of Fermat's theorem is false. [1+3+3]

4. Define the order of integer modulo n. Show that the order of $3(mod9)$ is not defined. The following is a table of indices for the prime 17 relative to the primitive root 3. Solve the congruence $x^{12} \equiv 13(mod17)$ with the aid of the table. [1+2+4]

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$ind_3\ a$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

5. Define $Mobious\ \mu - function$. Find $\mu(n)$ if $n = 180$. Show that the function μ is multiplicative function. [1+2+4]

6. Explain RSA Algorithm. Write an example to encrypt and decrypt a message using RSA algorithm. [3+4]

SECTION "D"

[4 Q. × 2 = 8 marks]

7. Employing the Sieve of Eratosthenes, obtain all the prime between 100 and 200.

8. Verify that $4^{532} \equiv 5(mod 11)$.

9. Find $\tau(n)$ and $\sigma(n)$ for $n = 3655$, these symbols have its usual meaning.

10. Encrypt the plaintext "**Mathematics**" using Caesar Cipher ($Using\ key\ =\ 4$).