KATHMANDU UNIVERSITY
End Semester Examination
February, 2025

Marks Scored:

Level : B.Sc.
Year : III

Course : MATH 327
Semester : II

Exam Roll No. :

Time: 30 mins.

F. M. : 10

Registration No.:

Date : 10 FEB 2025

SECTION "A"

[10Q. × 0.5 = 5 marks]

Fill in the blank space(s) by the most appropriate word(s) or symbol(s).

1. If p and q are distinct primes with $a^p \equiv a(mod q)$ and $a^q \equiv a(mod p)$, then_____.

2. For a positive integer n, defined τ by the rules $\tau(n) =$ _____ if $n = p_1 p_2 \dots p_r$, where p_i are distinct primes.

3. If f is multiplicative function and F is defined by $F(n) = \sum_{d|n} f(d)$. Then F_____.

4. $\phi(450) =$_____, where the symbol has its usual meaning.

5. $5^{38}\ (mod 11) =$_____where the symbol has its usual meaning.

6. $\tau(n) =$ _____for n = 59319, where the symbol has its usual meaning.

7. $\mu(150)=$ _____, where the symbol has its usual meaning.

8. There are exactly _____primitive roots of integer 9.

9. $\sum_{n=1}^{6} \left[\frac{6}{n}\right] =$ _____, where the symbol has its usual meaning.

10. The number of mutually incongruent solution of linear congruent $42x \equiv 90(mod 156)$ is _____.

SECTION "B"

[10 Q. × 0.5 = 5 marks]

Fill in the blank space(s) by selecting the most appropriate answer from among the given ones. (***DO NOT TICK THE ANSWER***)

11. If a and b are relatively prime positive integers, then the arithmetic progression $a, a + 2b, a + 3b, \ldots$ contain _____.
[finite number of prime — infinitely many prime
finite number of composites — infinitely many even number]

12. If a is a whole number and p is a prime number, then according to Fermat's theorem _____.
[$2^{p-1} - 2$ is not divisible by p — $2^{p-1} - 1$ is divisible by p
$2^p - 2$ is divisible by p — $2^p - 2$ is divisible by p]

13. If $a, b \in \mathbb{Z}$ and $b \neq 0$, then $\exists$ a unique pair of integers q and r such that $a = bq + r$ where, _____.
[$0 \leq r \leq |b|$ $0 \leq r < |b|$ $0 > r > |b|$ $0 \leq r \leq b$]

14. If $gcd(a, b) = 1$ for any two integers a and b, then a and b are _____.
[twin prime — relatively prime
multiples of each other — divisible]

15. Sieve of Eratosthenes is used for finding _____.
[all even numbers of given integers — all odd numbers of given integers
all composite numbers of given integers — all primes of given integers]

16. If $a|c, b|c$ and $(a, b) = 1$ then _____.
[$ab|c$ $bc|a$ $a|bc$ $c|ab$]

17. Which name matches statement if $a|bc$ and $(a, b) = 1$ then $a|c$ _____.
[Euclid's Lemma Fermat's Theorem Division Algorithm Euclidean Algorithm]

18. Every Integer n is a product of prime such that _____.
[$n > 1$ $n > 2$ $n < 1$ $n > 0$]

19. Which of the following Diophantine equations has no solution in integers _____.
[$3x + 7y = 10$ $8x - 12y = 5$ $6x + 12y = 96$ $5x + 10y = 25$]

20. The order of 5 modulo 19 is _____.
[8 16 9 5]

KATHMANDU UNIVERSITY
End Semester Examination
February, 2025

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

10 FEB 2025

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

SECTION "C"
[6Q. × 7 = 42 marks]

1. Define a divides b with an example. If a, b, c are integers, and if $a|bc$ with $gcd(a,b) = 1$, then $a|c$. A small clothing manufacturer produces two styles of sweaters: cardigan and pullover. She/He sells cardigans for \$31 each and pullovers for \$28 each. If her total revenue from a day's production is \$1460, how many of each type might she manufacture in a day? [1+2+4]

2. Define a system of linear congruence *modulo* m. When does a system of linear congruences have a unique solution? Obtain the eight incongruent solutions of the linear congruence. [1+1+5]

$$3x + 4y \equiv 5(mod 8)$$

OR

Define congruence modulo. State Chinese Remainder theorem. Determine whether the given system has a solution, and find them all, if any exist. [1+2+4]

$$x \equiv 5(mod 11)$$

$$x \equiv 14(mod 29)$$

$$x \equiv 15(mod 31)$$

3. Define reduced residue system modulo n. Prove that if $r_1, r_2, \ldots, r_{\phi(n)}$ is a reduced residue system modulo n, and a is a positive integer with $gcd(a,n) = 1$, then the set $ar_1, ar_2, \ldots, ar_{\phi(n)}$ is also a reduced residue system modulo n. Verify the example using an example. [1+4+2]

4. Define primitive root the order of integer modulo n. Show that 2 is not primitive root of modulo 7. Let the integer a has an order k modulo n, then $a^h \equiv 1(mod n)$ if and only if $k|h$; in particular $k|\phi(n)$. [1+2+4]

5. Define Indices. Make a table of indices for the prime 17 relative to the primitive root 3, solve the following congruence. [1+2+4]

$$x^{12} \equiv 13(mod 17)$$

6. Define symmetry and asymmetry key cryptography. Write RSA Algorithm. Write an example of how to encrypt and decrypt a message using the RSA algorithm. [1+3+3]

P.T.O.

SECTION "D"

[4Q. × 2 = 8 marks]

7. If $a \equiv b\ mod(n)$, then $a^k \equiv b^k(modn)$ for any positive integer k.

8. Show that 341 is a base 2 pseudoprime.

9. For any positive integer n, $\phi(n) = n\sum_{d|n}\frac{\mu(d)}{d}$, symbols have their usual meaning.

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