KATHMANDU UNIVERSITY
End Semester Examination
July/August, 2024

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

26 JUL 2024

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

SECTION "C"
[6 Q. × 7 = 42 marks]

1. Define a divides b with an example. If a, b, m and n are integers, and if $c|a$ and $c|b$ then prove $c|(ma + nb)$. Aayush buys large shirts for \$18 each and small shirts for \$11 each. The shirts cost a total of \$1188. What is the smallest total number of shirts he could have bought? [1+2+4]

2. Define a system of linear congruence *modulo* m. When does a system of linear congruences have a unique solution? Find the solution of the given system of unity. [1+1+5]

$$7x + 3y \equiv 6(mod 11)$$
$$4x + 2y \equiv 9(mod 11)$$

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]

$$x \equiv 5(mod\ 6)$$
$$x \equiv 4(mod 11)$$
$$x \equiv 3(mod 17)$$

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. Let the integer a has an order k modulo n, then $a^h \equiv 1(mod\ n)$ if and only if $k|h$. Make a table of indices for the prime 13 relatives to the primitive root 2 and solve congruence $4x^9 \equiv 7(mod 13)$ with the aid of the table. [1+3+3]

5. Define $Euler - \phi$ function. Verify that the equality $\phi(n) = \phi(n+1) = \phi(n+2)$ holds when $n = 5186$. Show that the Mobius function μ is a multiplicative function. [1+2+4]

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

SECTION "D"
[4 Q. × 2 = 8 marks]

7. If p is a prime and $p|ab$, then show that $p|a$ or $p|b$.

8. Show that $561|\ 2^{561} - 2$.

9. Define the Primitive root. Show that 2 is a primitive root of 5.

10. Encrypt the plaintext "Computational" using Caesar Cipher ($Using\ key\ =\ 3$).

KATHMANDU UNIVERSITY
End Semester Examination
July/August, 2024

Marks Scored:

Level : B.E.
Year : III

26 JUL 2024

Course : MATH 327
Semester : II

Exam Roll No. :

Time: 30 mins.

F. M. : 10

Registration No.:

Date :

SECTION "A"

[10 Q. × 0.5 = 5 marks]

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

1. $2^{50} mod(17) =$ _____ .
2. If p and q are distinct primes with $a^p \equiv a(mod\ q)$ and $a^q \equiv a(mod\ p)$, then _____ _____.
3. Let m be a positive integer, two integers a and b are congruence modulo m if and only if _____.
4. A composite integer n is called pseudoprime whenever _____.
5. Euler phi- function of a number p is $\varphi(p) =$ _____.
6. For a positive integer n, define μ by the rules $\mu(n) =$ _____ if $n = p_1 p_2 \dots p_r$, where p_i are distinct primes.
7. If f is multiplicative function and F is defined by$F(n) = \sum_{d|n} f(d)$. Then F _____ _____.
8. $\phi(360) =$ _____, where the symbol has its usual meaning.
9. There are exactly _____ primitive roots of integer 9, these being the integers 2 and 5.
10. The set _____ has reduced residue system modulo 8.

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. The linear Diophantine equation $ax + by = c$ has a solution if and only if _____.
[$gcd(a, c)|b$ gcd(a, b)|c gcd(c, b)|a c|gcd(a, b)]
12. The number of primes is_____.
[finite uncountable
infinite Neither finite nor infinite]

13. The 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]

14. The integers 1949 and 1951 are _____.
[Prime and composite Composites Twin primes Pseudoprimes]

15. The solution of $25x \equiv 15 mod(29)$ is _____.
[$x \equiv 18(\text{mod}29)$ $x \equiv 29(\text{mod}29)$ $x \equiv 18(mod19)$ $x \equiv 17(mod19)$]

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

17. The composite numbers n that are pseudoprime to every base a are called _____.
[Pseudoprime Prime
Pseudoprime to the base a Absolute pseudoprimes]

18. The number of Pseudoprimes is infinitely many. The smallest one Pseudoprime being _____ to base2.
[91 217 341 245]

19. Which theorem states that if p is a prime, then $(p-1)! \equiv -1(mod\ p)$ _____
[Euler's Theorem Wilson's Theorem
Fermat's Little Theorem Dirichlet's Theorem]

20. The order of 2 modulo 17 is _____.
[8 16 11 5]