ITER, SOA (Deemed to be) University, Bhubaneswar

MCA I^{st} Semester
Assignment 4, December 2025
Subject: Discrete Mathematics (MA 3001)
Sections: 25C2A1, 25C2A2, 25C2B1, & 25C2B2

Answer all questions

4.1 Divisibility and Modular Arithmetic

1. Suppose that a and b are integers, $a \equiv 11(mod\ 19)$, and $b \equiv 3(mod\ 19)$. Find the integer c with $0 \leq c \leq 18$ such that
   (a) $c \equiv 13a\ (mod\ 19)$
   (b) $c \equiv a - b\ (mod\ 19)$
   (c) $c \equiv 7a + 3b\ (mod\ 19)$
   (d) $c \equiv 2a^2 + 3b^2\ (mod\ 19)$
   (e) $c \equiv a^3 + 4b^3\ (mod\ 19)$
2. Prove or disprove that if a, b and d are integers with $d > 0$, then $(a + b)\ div\ d = a\ div\ d + b\ div\ d$.
3. Let m be a positive integer. Show that $a \equiv b(mod\ m)$, if $a\ mod\ m = b\ mod\ m$.
4. Evaluate
   (a) $-17\ mod\ 2$
   (b) $-221\ mod\ 23$
   (c) $199\ mod\ 19$
   (d) $155\ mod\ 19$
5. Find each of these values.
   (a) $(177\ mod\ 31 + 270\ mod\ 31)\ mod\ 31$
   (b) $(457\ mod\ 23 \cdot 182\ mod\ 23)\ mod\ 23$

4.2 Interger Representation and Algorithm

6. Convert the decimal expansion of each of these integers to a binary expansion.
   (a) 231
   (b) 100632
7. Convert the binary expansion of each of these integers to a decimal expansion.

(a) $(1\ 1111)_2$

(b) $(111\ 1100\ 0001\ 1111)_2$

8. Convert the octall expansion of each of these integers to a binary expansion.

(a) $(572)_8$

(b) $(2417)_8$

9. Convert the binary expansion of each of these integers to an octal expansion.

(a) $(1111\ 0111)_2$

(b) $(101\ 0101\ 0101\ 0101)_2$

10. Convert the hexadecimal expansion of these integers to a binary expansion.

(a) $(80E)_{16}$

(b) $(DEFACED)_{16}$

11. Convert $(7345321)_8$ to its binary expansion and $(10\ 1011\ 1011)_2$ to its octal expansion.

4.3 Primes and GCD

12. What are the LCM and GCD of these pairs of integers?

(a) $2^2 \cdot 3^3 \cdot 5^5, 2^5 \cdot 3^3 \cdot 5^2$

(b) $2 \cdot 3 \cdot 5 \cdot 7, 2 \cdot 3 \cdot 5 \cdot 7$

(c) $3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^9$

(d) $1111, 0$

13. Find $gcd(1000, 625)$ and $lcm(1000, 625)$ and verify that $gcd(1000, 625) \cdot lcm(1000, 625) = 1000 \cdot 625$.

14. Using the method of extended Euclidean algorithm, express the gcd of each of these pairs of integers as a linear combination of these integers.

(a) $10, 11$

(b) $9999, 11111$

(c) $21, 55$

(d) $101, 203$

(e) $117, 213$

4.4 Solving Congruences

15. Find an inverse of 7 modulo 26.

16. Find an inverse of 13 modulo 2436

17. Find an inverse of 2 modulo 17.

18. Find an inverse of 55 modulo 89.

19. Find an inverse of 200 modulo 1001.

20. Solve the following congruence
    (a) $4x \equiv 5 \ (mod\ 9)$
    (b) $2x \equiv 7 \ (mod\ 17)$
    (c) $89x \equiv 2 \ (mod\ 232)$
    (d) $200x \equiv 13 \ (mod\ 1001)$
    (e) $34x \equiv 77 \ (mod\ 89)$

21. Solve the following system of congruences
    (a) $x \equiv 2 \ (mod\ 3)$
        $x \equiv 1 \ (mod\ 4)$
        $x \equiv 3 \ (mod\ 5)$.
    (b) $x \equiv 1 \ (mod\ 2)$
        $x \equiv 2 \ (mod\ 3)$
        $x \equiv 3 \ (mod\ 5)$
        $x \equiv 4 \ (mod\ 11)$.
    (c) $x \equiv 3 \ (mod\ 6)$
        $x \equiv 4 \ (mod\ 7)$.

4.6 Cryptography

22. Encrypt the message **DO NOT PASS GO** by traslating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.
    (a) $f(p) = (p + 13) \ mod\ 26$
    (b) $f(p) = (3p + 7) \ mod\ 26$

23. Encrypt the message **WATCH YOUR STEP** by traslating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters using the $f(p) = (-7p + 1) \ mod\ 26$.

24. Decrypt the message **WHVW WRGDB** that were encrypted using the Caesar cipher.

25. Decrypt the message **LO WI PBSOXN** encrypted using the shift cipher $f(p) = (p + 10) \ mod\ 26$.

26. What is the decryption function for an affine cipher if the encryption function is $c = (15p + 13) \ mod\ 26$?