CSD2258 Homework 3

Due: Mar 10, 2024

The following problem set is used for the on-line homework 3 set up on Moodle. Please key in your answers on Moodle by the due date.
Highly appreciate if you could let me know typos and errors.

Questions 1-2. Let a, b be positive integers with $ab = 2^7 3^8 5^2 7^{11}$ and $\gcd(a, b) = 2^3 3^4 57^3$.

Question 1. What is $\text{lcm}(a, b)$? (Hint. $\text{lcm}(a, b) = \dfrac{ab}{\gcd(a, b)}$)

(A) $2^4 3^4 57^8$ (B) 7^{11} (C) $2^3 3^4 5$ (D) $2^7 3^8 5^2 7^{11}$ (E) None of these

Question 2. Assume $a \leq b$. Which number among $2^3 3^4 57^4$, $2^4 3^4 57^5$, $2^3 3^4 57^3$ could be a?

(A) None of them (B) All of them (C) $2^3 3^4 57^4$ (D) $2^4 3^4 57^5$ (E) $2^3 3^4 57^3$

Questions 3-7 (Bezout coefficients, extended Euclidean algorithm, modular inverse)

Question 3. Let a, b be integers. Let s and t be Bezout coefficients of a and b, respectively. Which of the following equations is true?

(A) $as + bt = 1$ (B) $as + bt = \gcd(a, b)$ (C) $as + bt \equiv \gcd(a, b)$
(D) $as + bt = \gcd(s, t)$ (E) None of these

Question 4. Let s and t be Bezout coefficients of 99 and 88, respectively. What is t?

(A) $t = -1$ (B) $t = -100$ (C) $t = 98$ (D) Any A,B,C (E) None of A,B,C

gcd(a,m) > 1, a ^-1 mod m doesnt exist

Question 5. Which number among -1, -100, 98 could be $88^{-1} \mod 99$?

(A) Only -1 (B) Only -100 (C) Only 98 (D) Both A and B
(E) Both (A) and (C) (F) Both (A) and (C) (G) All of them (H) None of them

Question 6. Let s and t be Bezout coefficients of 323 and 124, respectively. What is s?

(A) $s = 323$ (B) $s = 124$ (C) $s = 43$ (D) $s = -112$ (E) It doesn't exit

Question 7. Which number among $43, 167, -81$ could be $323^{-1} \pmod{124}$?

(A) Only 43 (B) Only 167 (C) Only -81 (D) (A) and (B)
(E) (A) and (C) (F) (B) and (C) (G) All of them (H) None of them

Question 8. Let a, b, m be integers such that $a \equiv b \pmod{m}$. Which equation among

(a) $a - b \equiv 0 \pmod{m}$ (b) $a = b + km$ for some $k \in \mathbb{Z}$

is correct?

(A) Only (a) (B) Only (b) (C) Both (a) and (b) (D) None of them

Question 9. Let a, b, m be integers. When solving $ax \equiv b \pmod{m}$, the solution in x needs to be expressed in which form among the following? (Tick all that apply)
(A) $x = x_0$ for some $x_0 \in \mathbb{Z}$
(B) $x = x_0$ for some $x_0 \in \{0, 1, \ldots, m-1\}$
(C) $x \equiv x_0 \pmod{n}$ for some $k, n \in \mathbb{Z}$
(D) $x = x_0 + kn$ for some $x_0, k, n \in \mathbb{Z}$
(E) None of these

Questions 10-14. Consider integers $a = 252$ and $m = 356$.

Question 10. Let s, t be Bezout coefficients of a and m. What is s?

(A) $s = -24$ (B) $s = 332$ (C) $s = -380$ (D) Any A,B,C (E) None of A,B,C

Question 11. For what integer b does the equation $252x \equiv b \pmod{356}$ have solution?

(A) Any integer (B) $b \equiv 0 \pmod{4}$ (C) $b \equiv 1 \pmod{4}$
(D) $b \equiv 2 \pmod{4}$ (E) None of these

Question 12. What is the solution to $252x \equiv 12 \pmod{356}$?

(A) $x = 17$ (B) $x = 106$ (C) $x \equiv 17 \pmod{89}$ (D) $x \equiv 17 \pmod{356}$ (E) None of these

Question 13. How many solutions x are there to $252x \equiv 12 \pmod{356}$ in the set $\{0, 1, \ldots, 355\}$?

(A) 0 (B) 4 (C) 12 (D) Infinite (E) None of these

Question 14. How many solutions x are there to $252x \equiv 12 \pmod{356}$ in the set $\{0, 1, \ldots, 1000\}$?

(A) 1 (B) 4 (C) 12 (D) Infinite (E) None of these

Question 15. Decrypt the message HDW GLP VXP using Caesar cipher with the key $k = 3$.

(A) EAT DIM SUM (B) EAT AND RUN (C) RUN AND EAT
(D) NOT EAT ABLE (E) None of these

Questions 16-17. The affine cipher with the key $k = (a, b)$ encrypts a plaintext P to ciphertext $C = aP + b$ and decrypts C to $P = a^{-1}(C - b) \pmod{26}$.

Question 16. Encrypt the message PROBLEM using affine cipher with the key $k = (3, 2)$

(A) PROBLEM (B) NOODLES (C) VBSFJOM (D) CSDJKAT (E) None of these

Question 17. Decrypt the message TPJJNDP using an affine cipher with the key $k = (7, 13)$.

(A) MESSAGE (B) PROBLEM (C) MEANING (D) SOLUTION (E) None of these