

(Solution generated by ChatGPT and verified by the instructor)

1. Answer the following MCQ-type questions:

- (a) (1 point) Suppose the jug capacities are 6 liters and 10 liters. Which target amount B is **not** possible?

(A) 2 (B) 4 (C) 5 (D) 8

Solution: The possible amounts must be multiples of

$$\gcd(6, 10) = 2.$$

The amounts 2, 4, and 8 are possible, but 5 is not divisible by 2. Therefore the correct answer is

(C) 5.

- (b) (1 point) What is $\mathbb{Z}_{10}^*$?

(A) $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ (B) $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ (C) $\{1, 3, 7, 9\}$ (D) $\{2, 4, 6, 8\}$

Solution: The set $\mathbb{Z}_{10}^*$ consists of the residues modulo 10 that are relatively prime to 10. These are

$$1, 3, 7, 9.$$

Thus

$$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}.$$

The correct answer is

(C).

- (c) (1 point) If $p = 5$, $q = 11$, and $e = 3$, then $\phi(N) = 40$. Which value of d satisfies $3d \equiv 1 \pmod{40}$?

(A) 7 (B) 13 (C) 27 (D) 40

Solution: We need to solve

$$3d \equiv 1 \pmod{40}.$$

Checking the options,

$$3 \cdot 27 = 81 \equiv 1 \pmod{40}.$$

Therefore

$$\boxed{d = 27},$$

and the correct answer is

(C).

- (d) (1 point) If $p = 5$, $q = 11$, and $e = 3$, then $\phi(N) = 40$. What is the encryption of $M = 10$?

Solution: Here

$$N = pq = 5 \cdot 11 = 55.$$

In RSA encryption, the ciphertext is

$$C \equiv M^e \pmod{N}.$$

Thus

$$C \equiv 10^3 \pmod{55}.$$

Since

$$10^3 = 1000$$

and

$$1000 = 55 \cdot 18 + 10,$$

we get

$$1000 \equiv 10 \pmod{55}.$$

Therefore the encryption of $M = 10$ is

$$\boxed{10}.$$

(e) (1 point) Which one is a generator for $\mathbb{Z}_7^*$?

(A) 1 (B) 2 (C) 3 (D) 6

Solution: We have

$$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}.$$

The powers of 3 modulo 7 are

$$3^1 \equiv 3,$$

$$3^2 \equiv 9 \equiv 2,$$

$$3^3 \equiv 6,$$

$$3^4 \equiv 18 \equiv 4,$$

$$3^5 \equiv 12 \equiv 5,$$

$$3^6 \equiv 15 \equiv 1 \pmod{7}.$$

Thus the powers of 3 generate all elements of $\mathbb{Z}_7^*$. Therefore the correct answer is

$$\boxed{(C) \ 3}.$$

2. Let S be the subset of the set of ordered pairs of integers defined recursively by:

Basis step: $(0, 0) \in S$.

Recursive step: If $(a, b) \in S$, then $(a + 3, b + 2) \in S$ and $(a + 2, b + 3) \in S$.

Answer the questions that follow:

(a) (1 point) State True or False: $(12, 13)$ is in the set S .

Solution: True.

Starting from $(0, 0)$, apply the two recursive rules in the following way:

$$(0, 0) \rightarrow (3, 2) \rightarrow (6, 4) \rightarrow (8, 7) \rightarrow (10, 10) \rightarrow (12, 13).$$

Therefore

$$\boxed{(12, 13) \in S}.$$

(b) (1 point) State True or False: $(12, 12)$ is in the set S .

Solution: False.

Each recursive step increases the sum $a + b$ by

$$(3 + 2) = 5$$

or by

$$(2 + 3) = 5.$$

Since the basis element $(0, 0)$ has sum 0, every element $(a, b) \in S$ must satisfy that $a + b$ is a multiple of 5.

But for $(12, 12)$,

$$12 + 12 = 24,$$

which is not a multiple of 5. Therefore

$$(12, 12) \notin S.$$

- (c) (1 point) State True or False: For every $(a, b) \in S$, $a + b$ is a multiple of 5.

Solution: True.

We prove this using structural induction.

Basis step: For $(0, 0)$,

$$0 + 0 = 0,$$

which is a multiple of 5.

Recursive step: Suppose $(a, b) \in S$ and $a + b$ is a multiple of 5. Then

$$(a + 3) + (b + 2) = a + b + 5,$$

which is also a multiple of 5. Similarly,

$$(a + 2) + (b + 3) = a + b + 5,$$

which is also a multiple of 5.

Therefore every $(a, b) \in S$ satisfies that $a + b$ is a multiple of 5.

True

- (d) (1 point) State True or False: For every (a, b) where $a + b$ is a positive multiple of 5, $(a, b) \in S$.

Solution: False.

For example, take

$$(a, b) = (4, 1).$$

Then

$$4 + 1 = 5,$$

which is a positive multiple of 5. However, $(4, 1)$ cannot be generated from $(0, 0)$ using the recursive rules.

After one recursive step, the only elements with sum 5 are

$$(3, 2) \quad \text{and} \quad (2, 3).$$

Thus

$$(4, 1) \notin S.$$

So the statement is false.

(e) (1 point) Give a reason for your answer to part (d).