Course is completed. The course result can no longer be changed.

Modular Arithmetics

PREVIOUS NEXT

Quiz

Bookmark this page

Now, it's time for a short quiz to recap what you've learned. The quiz is **graded**, so you can take it only once. Each question will be followed by feedback explaining why your answer is right or wrong. If your answer is incorrect, you will see a suggestion of what you might need to refresh your memory.

Good luck!

Read the question below and enter an answer. Then, click "Submit."

What is $70 \ mod \ 10$?

0

0

Correct: Nice job!

Submit You have used 1 of 1 attempt

Read the question below and select the correct answer. Then, click "Submit."

Which of the following statements is correct?

- If $a, b \in Z$ and $m \in Z^+$, then $m \mid a-b$ iff $a \equiv b \pmod{m}$.
- If $a, b \in Z^+$ and $m \in Z$, then $m \mid a-b$ iff $a \equiv b \pmod{m}$.
- If $a, b \in Z$ and $m \in Z^+$, then $a-b \mid m$ if $a \equiv b \pmod{m}$.
- If $a, b \in Z^+$ and $m \in Z$, then $a-b \mid m$ iff $a \equiv b \pmod{m}$.

Correct: Great job!

Submit You have used 1 of 1 attempt

Read the question below and select the correct answer. Then, click "Submit."

Which of the following statements is correct?

- $(ab) \ mod \ m = (a \ mod \ m) * (b \ mod \ m)$
- $(ab) \ mod \ m = ((a \ mod \ m) * (b \ mod \ m)) \ mod \ m$
- $(ab) \ mod \ m = ((a \ mod \ m) + (b \ mod \ m)) \ mod \ m$
- $(ab) \ mod \ m = (a \ mod \ m) + (b \ mod \ m)$

Correct: Nice job!

Submit You have used 1 of 1 attempt

Read the question below and select the correct answer. Then, click "Submit."

Suppose a, b, and m are integers and $m > 0$. Which of the following is the correct formulation of a modular linear equation?

- Find all values of x such that $ax \equiv b \,(mod\, m)$.
- Find all values of x from the set $\{0, 1, \ldots, m-1\}$ such that $ax = b$.
- Find all values of x from the set $\{0, 1, \ldots, m-1\}$ such that $ax \; mod \; m = b$.
- (selected) Find all values of x from the set $\{0, 1, \ldots, m-1\}$ such that $ax \equiv b \,(mod\, m)$.

✔

Correct: Great job!

Submit You have used 1 of 1 attempt

*Read the question below and select **all** the answers that are correct. Then, click "Submit."*

Suppose the equation $ax \equiv b \,(mod\, m)$ is solvable. Which TWO of the following statements are correct?

- [ ] $d \mid a$, where $d = gcd\,(b, m)$.
- [x] $d \mid b$, where $d = gcd\,(a, m)$.
- [x] The equation has d solutions, where $d = gcd\,(a, m)$.
- [ ] The equation has $(d-1)$ solutions, where $d = gcd\,(a, m)$.

✔

Correct: Nice job!

Submit You have used 1 of 1 attempt

Read the question below and select the correct answer. Then, click "Submit."

Which of the following statements is correct?

- Let $a \in Z$ and $m \in Z^+$. The modular inverse of a by modulo m is an integer x such that $ax \equiv 0 \,(mod\, m)$, where $0 < x < m$.
- Let $a \in Z$ and $m \in Z^+$. The modular inverse of a by modulo m is an integer x such that $a \equiv x \,(mod\, m)$, where $0 < x < m$.
- (selected) Let $a \in Z$ and $m \in Z^+$. The modular inverse of a by modulo m is an integer x such that $ax \equiv 1 \,(mod\, m)$, where $0 < x < m$.
- Let $a \in Z$ and $m \in Z^+$. The modular inverse of a by modulo m is an integer x such that $ax \equiv m - 1 \,(mod\, m)$, where $0 < x < m$.

✔

Correct: Great job!

Submit You have used 1 of 1 attempt

Read the question below and enter an answer. Then, click "Submit."

What is the modular inverse of 159403863864233720 3 by modulo 5?

2 ✔

2

Correct: Nice job!

Submit You have used 1 of 1 attempt

Read the question below and select the correct answer. Then, click "Submit."

What is the modular inverse of 2 by modulo 4?

- 0
- 1

- 2
- 3
- It does not exist.

Correct: Right! The modular inverse of 2 by modulo 4 does not exist.

Submit You have used 1 of 1 attempt

*Read the question below and select **all** the answers that are correct. Then, click "Submit."*

Which TWO of the following statements are correct?

- [x] The modular inverse of a by modulo m is unique if $gcd\,(a, m) = 1$.
- [ ] The modular inverse of a by modulo m is $gcd\,(a, m)$.
- [ ] The modular inverse of a by modulo m is $gcd\,(a, m) + i * m$, where $i \in \{0, 1, \ldots, m-1\}$.
- [x] The modular inverse of a by modulo m does not exist if $gcd\,(a, m) > 1$.
- [ ] The modular inverse of a by modulo m does not exist if $gcd\,(a, m) = 1$.
- [ ] The modular inverse of a by modulo m always exists.

Correct: Great job!

Submit You have used 1 of 1 attempt

PREVIOUS NEXT