Q1 Extended Euclid

2 Points

Consider positive integers x, m, where $\gcd(x, m) = 1$. Assume $a, b \in \mathbb{N}$ satisfies $ax + bm = \gcd(x, m)$.

Q1.1 Multiplicative inverse

1 Point

What is the multiplicative inverse of x modulo m?

- (●) a
- ( ) b
- ( ) x
- ( ) m

Explanation

Since $ax + bm \equiv 1 \pmod{m}$, we have $ax \equiv 1 - bm \equiv 1 \pmod{m}$.

Q1.2 Another multiplicative inverse

1 Point

What is the multiplicative inverse of m modulo x?

- ( ) a
- (●) b
- ( ) x
- ( ) m

Explanation

Since $ax + bm \equiv 1 \pmod{m}$, we have $bm \equiv 1 - ax \equiv 1 \pmod{m}$.

Q2 Chinese Remainder Theorem

2 Points

Let n, m be positive integers with $\gcd(n, m) = 1$. Assume $u \equiv n^{-1} \pmod{m}$.

Q2.1

1 Point

What is $u \cdot n \pmod{m}$?

- ○ 0
- ◉ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5

Explanation

u is the multiplicative inverse of n modulo m.

Q2.2

1 Point

What is $u \cdot n \pmod{n}$?

- ◉ 0
- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5

Explanation

Any multiple of n is 0 modulo n.

Q3 What is True

3 Points

Let x, m be positive integers and define $d = \gcd(x, m)$. Check if the following statements are true.

Q3.1

1 Point

x/d is an integer.

- (●) True
- ( ) False

Explanation

Since d is a divisor of x.

Q3.2

1 Point

$\gcd(\frac{x}{d}, m)$ is always 1.

- ( ) True
- (●) False

Explanation

If $x = 8$ and $m = 4$, then $d = 4$ and $\gcd(\frac{x}{d}, m) = \gcd(2, 4) = 2 \neq 1$.

Q3.3
1 Point

$\gcd(\frac{x}{d}, \frac{m}{d})$ is always 1.

- (●) True
- ( ) False

Explanation

Since d is the *greatest* common divider.