Practice Questions for Test 3, CISC-203 2020W

Q1:
Find the set of all possible integer solutions to the following set of equations.

\[ x \equiv 4 \mod 14 \]
\[ x \equiv 6 \mod 9 \]

Q2:
Suppose \( a \oplus b = 0 \) in \( \mathbb{Z}_n \) with \( a > 0 \) and \( b > 0 \)

Prove there is no \( m \neq n \) such that \( a \oplus b = 0 \) in \( \mathbb{Z}_m \)

Q3:
Consider the statement "If \( a \otimes b = 0 \) in \( \mathbb{Z}_n \) then \( a = 0 \) or \( b = 0 \)"

Prove this is true when \( n \) is prime.

Prove this is false when \( n \) is composite.

Q4:
Suppose Eve finds Bob’s wallet, and inside she finds a scrap of paper with “\( p = 2017 \)” written on it.

How can she try to use this information to eavesdrop on messages Alice sends to Bob?
Q5

Find all solutions to \((x + 2) \times 4 \mod 7 = 5\)

Q6

Prove that if \(x\) has an inverse in \(\mathbb{Z}_n\), then \(x\) also has an inverse in \(\mathbb{Z}_{n^2}\)

Q7

Suppose \((a \otimes b)^{-1} = c\) in \(\mathbb{Z}_n\)

Prove that \((b \otimes c)^{-1} = a\) in \(\mathbb{Z}_n\)

Q8

Which is larger: \(5^{18} \mod 7\) or \(4^{8743} \mod 7\)