Unit 9 - Week 7: Number Theoretic Algorithms

Assignment 7

The due date for submitting this assignment has passed.
As per our records you have not submitted this assignment.

Due on 2020-03-18, 23:59 IST.

1) Assume $P \neq NP$. Which of the following statements are true?   *1 point*

☐ There is a polynomial time algorithm to check if a graph contains a Hamiltonian cycle.

☐ There is a polynomial time algorithm to check if a given assignment is the only assignment which satisfies a given Boolean formula.

☐ There is a polynomial time algorithm to check if a given assignment satisfies a given Boolean formula.

☐ There is a polynomial time algorithm to check if a graph has an Eulerian cycle

No, the answer is incorrect.
Score: 0

Accepted Answers:
There is a polynomial time algorithm to check if a given assignment satisfies a given Boolean formula.
There is a polynomial time algorithm to check if a graph has an Eulerian cycle

2) Let $p \geq 5$ be a prime number. Which of the following statements are true?   *1 point*

☐

There is no number a such that $a^{p-1} \equiv 1 \mod p$

☐

There exists exactly one number a such that $a^{p-1} \equiv 1 \mod p$

☐

There exists infinitely many numbers a such that $a^{p-1} \equiv 1 \mod p$

☐

There exist a number a between 2 and $p-1$ (both inclusive) such that $a^{p-1} \equiv 1 \mod p$

No, the answer is incorrect.
Score: 0

Accepted Answers:
There exists infinitely many numbers a such that $a^{p-1} \equiv 1 \mod p$
There exist a number a between 2 and $p-1$ (both inclusive) such that $a^{p-1} \equiv 1 \mod p$

3) Let $n \geq 5$ be a composite number. Which of the following statements are true?   *1 point*

○

There is no number a such that $a^{n-1} \equiv 1 \mod n$

○

There exists exactly one number a such that $a^{n-1} \equiv 1 \mod n$

○

There exists infinitely many numbers a such that $a^{n-1} \equiv 1 \mod n$

○

For every number $2 \leq a \leq n-1$, there exist an $x < n-1$ such that $a^x \equiv 1 \mod n$.

No, the answer is incorrect.
Score: 0

Accepted Answers:
There exists infinitely many numbers a such that $a^{n-1} \equiv 1 \mod n$

4) Let $p \geq 5$ be a prime number. Which of the following statements are true?   *1 point*

☐

On input p, the Miller-Rabin algorithm says that p is prime with probability at most 0.5.

☐

On input p, the Miller-Rabin algorithm says that p is prime with probability 1.

☐

On input p, the Miller-Rabin algorithm says that p is prime with probability at least 0.5.

☐

On input p, the time taken for Miller-Rabin algorithm could be exponential in the size of p.

No, the answer is incorrect.
Score: 0

Accepted Answers:
On input p, the Miller-Rabin algorithm says that p is prime with probability 1.
On input p, the Miller-Rabin algorithm says that p is prime with probability at least 0.5.

5) Let $n \geq 5$ be a composite number. Which of the following statements are true?   *1 point*

○

On input n, the Miller-Rabin algorithm says that n is prime with probability at most 0.5.

○

On input n, the Miller-Rabin algorithm says that n is composite with probability 1

○

On input n, the Miller-Rabin algorithm says that n is prime with probability at least 0.5

○

On input n, the time taken for Miller-Rabin algorithm could be exponential in the size of n

No, the answer is incorrect.
Score: 0

Accepted Answers:
On input n, the Miller-Rabin algorithm says that n is prime with probability at most 0.5.

6) Let $n = 1 + 11^{n_1} \times 7^{n_2} \times 2^{n_3}$ where $n_1, n_2, n_3 \in \mathbb{N}$. Which of the following statements are true?   *1 point*

○

n is prime.

○

n is composite.

○

If for $2 \leq a < n$ we have $a^{\frac{n-1}{2}} \not\equiv 1 \mod n$, $a^{\frac{n-1}{7}} \not\equiv 1 \mod n$, $a^{\frac{n-1}{11}} \not\equiv 1 \mod n$ and $a^{n-1} \equiv 1 \mod n$, then n is prime.

○

If for $2 \leq a < n$ we have $a^{n-1} \equiv 1 \mod n$, then n is composite.

No, the answer is incorrect.
Score: 0

Accepted Answers:
If for $2 \leq a < n$ we have $a^{\frac{n-1}{2}} \not\equiv 1 \mod n$, $a^{\frac{n-1}{7}} \not\equiv 1 \mod n$, $a^{\frac{n-1}{11}} \not\equiv 1 \mod n$ and $a^{n-1} \equiv 1 \mod n$, then n is prime.

7) Let $p \geq 5$ be a prime number and a be a number between 1 and $p-1$ (including both). Which of the following statements are true?   *1 point*

○

There is no a satisfying the equation $a^2 \equiv 1 \mod p$.

○

There is exactly two numbers satisfying the equation $a^2 \equiv 1 \mod p$

○

There is exactly one a satisfying the equation $a^2 \equiv 1 \mod p$.

○

There are more than two a satisfying the equation $a^2 \equiv 1 \mod p$.

No, the answer is incorrect.
Score: 0

Accepted Answers:
There is exactly two numbers satisfying the equation $a^2 \equiv 1 \mod p$

8) Let $n \geq 5$ be a composite number. Which of the following statements are true?   *1 point*

☐

The numbers among $\{1, 2, \cdots, n-1\}$ which are relatively prime to n do not form a group.

☐

The numbers $\{1, 2, \cdots, n-1\}$ do not form a field under $\mod n$ multiplication.

☐

The numbers $\{1, 2, \cdots, n-1\}$ form a field under $\mod n$ multiplication.

☐

The numbers among $\{1, 2, \cdots, n-1\}$ which are relatively prime to n form a group.

No, the answer is incorrect.
Score: 0

Accepted Answers:
The numbers $\{1, 2, \cdots, n-1\}$ do not form a field under $\mod n$ multiplication.
The numbers among $\{1, 2, \cdots, n-1\}$ which are relatively prime to n form a group.