Progress

week 7

Counting

NPTEL » Randomized Algorithms

Unit 9 - Week 7: Number Theoretic Algorithms

Course outline Assignment 7 How does an NPTEL online The due date for submitting this assignment has passed. course work? As per our records you have not submitted this assignment. Week 0:Prerequisite Assume P ≠ NP. Which of the following statements are true? Week 1: Introduction to There is a polynomial time algorithm to check if a graph contains a Hamiltonian cycle. Randomized Algorithms There is a polynomial time algorithm to check if a given assignment satisfies a given Boolean formula. Week 2: Probability Review There is a polynomial time algorithm to check if a graph has an Eulerian cycle Week3: Moments and No, the answer is incorrect. Deviations Score: 0 Accepted Answers: Week4: Probabilistic Method 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 Week 5: Markov Chains Let p ≥ 5 be a prime number. Which of the following statements are true? Week 6: Markov Chains-II There is no number a such that $a^{p-1} \equiv 1 \mod p$ Week 7: Number Theoretic Algorithms There exists exactly one number a such that $a^{p-1} \equiv 1 \mod p$ Introduction to Computational Complexity There exists infinitely many numbers a such that $a^{p-1} \equiv 1 \mod p$ Pratt's Certificate There exist a number a between 2 and p-1 (both inclusive) such that $a^{p-1}\equiv 1\mod p$ Primality Testing No, the answer is incorrect. Miller Rabin Algorithm Score: 0 Accepted Answers: Quiz : Assignment 7 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 $a^{p-1} \equiv 1 \mod p$ Weekly feedback form for 3) Let n ≥ 5 be a composite number. Which of the following statements are true? Week 8: Graph Theoretic Algorithms There is no number a such that $a^{n-1} \equiv 1 \mod n$ Week 9 : Approximate There exists exactly one number a such that $a^{n-1} \equiv 1 \mod n$ Week 10 : Randomization and There exists infinitely many numbers a such that $a^{n-1} \equiv 1 \mod n$ Data Structures Week 11: Computational For every number $2 \le a \le n-1$, there exist an x < n-1 such that $a^x \equiv 1 \mod n$. Complexity No, the answer is incorrect. Score: 0 Week 12 : Summary Accepted Answers: There exists infinitely many numbers a such that $a^{n-1} \equiv 1 \mod n$ Download Videos Let p ≥ 5 be a prime number. Which of the following statements are true? 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.

```
Due on 2020-03-18, 23:59 IST.
                                                                                                                                                               1 point
 There is a polynomial time algorithm to check if a given assignment is the only assignment which satisfies a given Boolean formula.
                                                                                                                                                               1 point
                                                                                                                                                               1 point
                                                                                                                                                               1 point
  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 ≥ 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 \le 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 \le 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 \le a < n we have a^{\frac{n-1}{2}} \not\equiv 1 \mod n, a^{\frac{n-1}{2}} \not\equiv 1 \mod n, a^{\frac{n-1}{2}} \not\equiv 1 \mod n and
a^{n-1} \equiv 1 \mod n, then n is prime.
7) Let p \ge 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 ≥ 5 be a composite number. Which of the following statements are true?
                                                                                                                                                               1 point
 The numbers among \{1, 2, \dots, n-1\} which are relatively prime to n do not form a group.
 The numbers \{1, 2, \dots, n-1\} do not form a field under \mod n multiplication.
 The numbers \{1, 2, \dots, n-1\} form a field under mod n multiplication.
 The numbers among \{1, 2, \dots, n-1\} which are relatively prime to n form a group.
No, the answer is incorrect.
Score: 0
Accepted Answers:
The numbers \{1, 2, \dots, n-1\} do not form a field under \mod n multiplication.
The numbers among \{1, 2, \dots, n-1\} which are relatively prime to n form a group.
```