Assignment 12

Due on 2020-12-09, 22:59 IST.

1) Which of the following is false?

- Integer Factoring has a deterministic poly time algorithm since integral polynomial factoring has a deterministic poly time algorithm.
- AKS primality algorithm which decides whether an integer is factorizable in deterministic poly time can be modified to output a factor also in deterministic poly time.
- Integer factoring has a known randomized poly time factoring algorithm for all integers.
- All of these.

No, the answer is incorrect
Score: 0
Accepted Answers:
All of these.

2) Recall Agrawal-Biswas' randomized primality test which outputs n to be PRIME if 
\((a + 1)^n \equiv a^n \equiv 1 \mod (n, Q(a))\) and COMPOSITE otherwise. Where Q(x) is chosen to be a random polynomial of low degree. Let us use this test for n=4 by running it two times. In the first run, suppose the algorithm chooses the random polynomial Q(x) to be x+1 and in the second run, suppose it chooses Q(x) to be x^2. What will be the output of the algorithm in the two runs respectively, for the integer n=4?

- PRIME, PRIME
- PRIME, COMPOSITE
- COMPOSITE, PRIME
- COMPOSITE, COMPOSITE

No, the answer is incorrect
Score: 0
Accepted Answers:
COMPOSITE, PRIME.

3) Recall Fermat Method covered in lectures to factorize special types of integers efficiently. Which of the following factorization will be output of the Fermat Method when it is given n = 60 as input.

- 2 * 30
- 3 * 20
- 4 * 15
- 6 * 10

No, the answer is incorrect
Score: 0
Accepted Answers:
2 * 15.

4) We used the term \(I_{n}(x, c)\) in lectures which is a standard way denote the time complexity of many modern integer factoring methods. What is \(I_{n}(1/4, 2)\)?

- \(e^{\frac{2 \log n}{\log \log n}}\)
- \(e^{\frac{2 \log \log n}{\log n}}\)
- \(e^{\frac{2 \log n}{\log \log n}}\)
- \(e^{\frac{2 \log \log \log n}{\log n}}\)

No, the answer is incorrect
Score: 0
Accepted Answers:
\(e^{\frac{2 \log n}{\log \log n}}\).

5) Which of the following is true?

- The probability of choosing a \(I_{n}(x, c)\)-smooth number in \([1, \ldots, n]\) is around \(\frac{n}{x} \cdot \frac{\zeta(x)}{x^x}\).

2) Eratosthenes sieve algorithm takes time \(I_{n}(1, \frac{1}{2})\) to factor an integer n.

- Only 1.
- Only 2.
- Both 1 and 2.
- Neither 1 nor 2.

No, the answer is incorrect
Score: 0
Accepted Answers:
Both 1 and 2.

5) Which of the following is true?

- Pollard's rho method takes time \(\tilde{O}(\sqrt{n} \log n)\) to factor an integer n where prime \(p\) divides n.

2) Pollard's p-1 method is used to eliminate composite numbers in search of big Mersenne primes.

- Only 1.
- Only 2.
- Both 1 and 2.
- Neither 1 nor 2.

No, the answer is incorrect
Score: 0
Accepted Answers:
Both 1 and 2.