Assignment 3

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

1) Let $f(x)$ be a polynomial of degree $n$ over $\mathbb{C}[x]$, where $n$ is a power of 2. Let $\omega$ be an $n$-th primitive root of unity. Given $\omega^0, \omega^1, \ldots, \omega^{n-1}$, what is the minimum time complexity of $O(n \log n)$, $O(n)$, $O(n^2 \log n)$, $O(n^2)$, $O(n)$ operations in which you can compute $f(\omega^0), f(\omega^1), \ldots, f(\omega^{n-1})$?

- $O(n \log n)$
- $O(n)$
- $O(n^2 \log n)$
- $O(n^2)$
- $O(n)$

No, the answer is incorrect.
Score: 0
Accepted Answer: $O(n \log n)$

2) Which of the following can be false for some $n$-th root of unity, $\omega$?

- $\omega^0$ is an $n$-th root of unity, for even $n$.
- $\omega^{n/2} = \omega^2$, for every integer $k$.
- $\omega^{n/3} = \omega^k$, for every integer $k$ and even $n$.
- The $n$-th roots of unity form a cyclic group under multiplication.

No, the answer is incorrect.
Score: 0
Accepted Answer: None of these

3) Which of the following is false for polynomial multiplication of two degree $n$ polynomials over $\mathbb{R}[x]$?

- If $R$ has a $n$-th primitive root of unity and $n$ is a power of 2, polynomial multiplication can be done in $O(n \log n)$ $R$ operations.
- If $R$ does not have a $n$-th primitive root of unity, polynomial multiplication can be done in $O(n)$ $R$ operations.
- Polynomial multiplication can be done in $O(n)$ $R$ operations for any $R$.

None of these
Score: 0
Accepted Answer: None of these

4) Let $f(x) = g(x)$ be two polynomials, over a field $F$, of degree at most $\ell$. You learned in lectures about Schonhage-Strassen's algorithm for fast multiplying $f \times g$ where $\ell$ was assumed to be a power of 2. In which of the following scenarios the algorithm does not work?

- When the characteristic of $F$ is 0.
- When the characteristic of $F$ is 2.
- When the characteristic of $F$ is odd.
- None of the above options.

No, the answer is incorrect.
Score: 0
Accepted Answer: None of these

5) In lectures, you saw the discrete fourier transform matrix $DFT[\omega]$, where $\omega$ is the primitive $n$th root of unity with $\ell$, a power of 2. What is $DFT[\omega^0] \cdot DFT[\omega]$, $I_{\ell \times \ell}$ be the $\ell \times \ell$ identity matrix?

- $\ell \cdot I_{\ell}$
- $I_{\ell}$
- $\omega^0 \cdot I_{\ell}$
- $\omega^{n/2} \cdot I_{\ell}$

No, the answer is incorrect.
Score: 0
Accepted Answer: $\ell \cdot I_{\ell}$

6) Let $\mathbb{Z}$ be the ring of integers and $\ell$ be a positive integer. In which of the following ring extensions of $\mathbb{Z}$, the identity $1 + y + y^2 + \cdots + y^\ell - 1 = 0$ holds?

- $\mathbb{Z}/(y^\ell)$
- $\mathbb{Z}/(y^\ell - 1)$
- $\mathbb{Z}/(y^\ell + 1)$
- $\mathbb{Z}/(y)$

No, the answer is incorrect.
Score: 0
Accepted Answer: $\mathbb{Z}/(y^\ell + 1)$