Indian Institute of Technology Kharagpur
Department of Computer Science and Engineering

CS60094 Computational Number Theory **Spring 2026**

Quiz 2 **7th of April 2026, 9:35 AM – 9:55 AM** **Marks: 10 × 1.5 = 15**

Please write your answers in the space provided. Do not mark in the question itself.

---

1. Which of the following polynomials is irreducible in $\mathbb{F}_2[x]$?
   - A. $x^4 + x^3 + x + 1$
   - B. $x^4 + x^2 + x + 1$
   - C. $x^4 + x^2 + 1$
   - **D.** $x^4 + x^3 + 1$

2. The gcd of a polynomial $f(x) \in \mathbb{F}_q[x]$ with $x^{q^2} - x \in \mathbb{F}_q[x]$ tells us whether $f(x)$
   - **A. has quadratic and linear factors**
   - B. completely factors into linear factors over $\mathbb{F}_q$.
   - C. has any roots in $\mathbb{F}_q$
   - D. has linear factors

3. Let $\mathbb{F}_{16} = \mathbb{F}_{2^4} = \mathbb{F}_2(\theta)$ where θ is a root of the polynomial $x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x]$. The element $\theta^2 + 1$ is
   - A. primitive but not normal
   - B. primitive normal
   - **C. normal but not primitive**
   - D. neither primitive nor normal.

4. p-th power exponentiations in $\mathbb{F}_{p^n}$ is most efficient in which of the following representations
   - A. polynomial basis
   - B. discrete log representation
   - **C. normal basis**
   - D. arbitrary basis

5. Running time of the algorithm for testing irreducibility of $f(x) \in \mathbb{F}_q[x]$ with $\deg f = d$ is
   - A. $O(d^2 \log^3 q)$
   - B. $O(d^3 \log^2 q)$
   - **C.** $O(d^3 \log^3 q)$
   - D. $O(d^2 \log^2 q)$

6. Which of the following statements is incorrect?
   - A. Every Euler pseudoprime to base a is a strong pseudoprime to base a.
   - **B. Every Euler pseudoprime to base a is a Fermat pseudoprime to base a.**

C. Every Fermat pseudoprime to base a is a strong/Miller-Rabin pseudoprime to base a.

D. Every Fermat pseudoprime to base a is an Euler pseudoprime to base a.

7. Let n be an odd composite integer. Which of the following is correct?

   A. n is not an Euler pseudoprime to atleast half the bases in $\mathbb{Z}_n^*$.

   B. n is a Fermat pseudoprime to all bases in $\mathbb{Z}_n^*$.

   C. n is not an Fermat pseudoprime to atleast half the bases in $\mathbb{Z}_n^*$.

   D. There is atleast one base in $\mathbb{Z}_n^*$ to which n is not a Fermat pseudoprime.

8. Let $\{F_m\}_{m\geq 0}$ denote the Fibonacci sequence. Which of the following statements about the Fibonacci test is incorrect?

   A. It is a determinitic test

   B. The test is based on the fact that n is prime iff $F_{n-(\frac{3}{n})} \equiv 0 \bmod n$

   C. The test is based on the fact that n is prime iff $F_{n-(\frac{5}{n})} \equiv 0 \bmod n$

   D. Failure depends on distribution of Fibonacci pseudoprimes

9. Which of the following is incorrect?

   A. $F_{2k+2} = F_{k+1}(F_{k+1} + 2F_k)$

   B. $F_{2k+1} = F_{k+1}^2 + F_k^2$

   C. $F_{2k} = F_k(2F_{k+1} - F_k)$

   D. $F_{2k} = F_{k+1}^2 + F_k^2$

10. Running time of Miller-Rabin primality test (on input n) is

    A. $O(\log^3 n)$

    B. $O(n \log n)$

    C. $O(n)$

    D. $O(\log^4 n)$