Assignment 6

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

Due on 2020-10-28, 23:59 IST.

1) Which of the following is true for \( f, g \in \mathbb{F}_p[x] \)?
   - \( \gcd(f, g) \neq 1 \) if there exists \( x, t \in \mathbb{F}_p[x] \setminus \{0\} \) such that \( xt + ty = 0 \) with degree of \( x \) less than degree of \( g \) and degree of \( t \) less than degree of \( f \)
   - \( \text{res}(f, g) = 0 \) if \( \gcd(f, g) \neq 1 \)
   - \( \text{res}(f, g) = 0 \) if there exist \( x, t \in \mathbb{F}_p[x] \setminus \{0\} \) such that \( xt + ty = 0 \) where degree of \( x \) is less than degree of \( g \) and degree of \( t \) is less than degree of \( f \) then \( \text{res}(f, g) = 0 \)
   - All of the above.

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

2) Let \( f \) be a quadratic polynomial over \( \mathbb{F}_p[x] \), \( f = ax^2 + bx + c \), where \( a \neq 0 \). Let \( f' \) denote the derivative of \( f \). Then, which of the following is true?
   - \( \text{res}(f, f') = 0 \) if \( f \) has equal roots.
   - \( \text{res}(f, f') = 0 \) if \( f \) is square free.
   - \( \text{res}(f, f') = 0 \) if \( f \) has equal roots.
   - All of these.

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

3) Let \( p \) be a prime and \( q \) be a prime power, \( q = p^k \), where \( k \geq 1 \). Let \( d \) be the degree of input polynomial given over finite field \( \mathbb{F}_p \) or its finite extension \( \mathbb{F}_{q^m} \). Then, which of the following is true?
   - If we have a deterministic \( \mathbb{F}_{q^m} \) factorization algorithm over \( \mathbb{F}_p \), then we have a deterministic \( \mathbb{F}_q \) factorization algorithm over \( \mathbb{F}_{q^m} \).
   - If we have a deterministic \( \mathbb{F}_{q^m} \) factorization algorithm over \( \mathbb{F}_p \), then we have a deterministic \( \mathbb{F}_q \) factorization algorithm over \( \mathbb{F}_{q^m} \).
   - Both of these.
   - Factoring over \( \mathbb{F}_p \) is unrelated to factoring over \( \mathbb{F}_{q^m} \).

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

4) Let \( f \) be an irreducible polynomial of degree \( d \) in \( \mathbb{F}_p[x] \) with \( p \) being the characteristic of \( \mathbb{F}_p \). Recall that \( F := \mathbb{F}_p(\xi) \) is also a finite field. Which of the following is true about \( F \)?
   - \( F \) is a finite field of order \( p^d \).
   - \( F \) is a finite field of characteristic \( p \).
   - Only 1.
   - Only 2.
   - Only 3.
   - Only 2 and 3.

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

5) Let \( \mathbb{F}_p \) be a finite field of the characteristic \( p > 2 \). Which of the following is true about the polynomial \( f := x^{p^k - 1} + 1 \) in \( \mathbb{F}_p[x] \)?
   - Only the quadratic non-residues in \( \mathbb{F}_p \) can be the roots of \( f \).
   - All the quadratic non-residues in \( \mathbb{F}_p \) are the roots of \( f \).
   - Some quadratic residue in \( \mathbb{F}_p \) might be the root of \( f \).
   - Only 1.
   - Only 1 and 2.
   - Only 3.
   - Only 2 and 3.

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

6) Let \( f, g \in \mathbb{F}_p[x] \) be two univariate polynomials, where \( p \) is a field, such that their resultant vanishes identically. Which of the following is necessarily true?
   - \( f \) and \( g \) share a common factor in \( \mathbb{F}_p[x] \).
   - \( f \) and \( g \) share a common root in \( \mathbb{F}_p[x] \).
   - Only 1.
   - Only 2.
   - Both 1 and 2.
   - Neither 1 nor 2.

No, the answer is incorrect.
Score: 0
Accepted Answers: Only 1.