

CS 235: Algebraic Algorithms

Final Exam

Each of the following problems is worth twenty points. Complete any six of them, for a total of 120 points. Do not complete more than six! We will only grade the first six. If you change your mind about which problem you want to hand in, make sure you clearly cross out the old one.

Good luck!

1 Modular roots

Let p be prime, and suppose $p \equiv 1 \pmod{5}$. Let g be a generator modulo p . In terms of g and p , find a nontrivial fifth root of 1 mod p , that is, a value $r \neq 1$ such that $r^5 = 1 \pmod{p}$. Explain your answer.

2 Solving Polynomials

When working with nonzero polynomials modulo a prime, the number of zeroes is always at most the degree of the polynomial. Modulo composites, this is no longer true. Here you will demonstrate this with a linear polynomial.

Let $f(x) = 5x$. Find an $n > 5$ such that, if f is taken modulo n , it has exactly five zeroes.

3 Repeated squaring

Given a nonzero input $a \in \mathbb{Z}_p$ (p prime), and using only multiplication, addition, and division, what is the smallest number of arithmetic operations needed to compute:

- (1) a^{256} ?
- (2) a^{255} ?

You can assume all operations are in \mathbb{Z}_p (don't include computation of the remainders in your total). Explain your answer. Be careful, this is slightly different than on the practice sheet.

4 Subgroups

How many subgroups of size 3 are there in \mathbb{Z}_9 ? In $\mathbb{Z}_3 \times \mathbb{Z}_3$? Explain.

5 Commutativity

Let G be the (noncommutative) group D_4 , all rigid motions of a square. Remember that $|D_4| = 8$. Find:

- (1) An element $x \in D_4$ such that x commutes with every other element, that is, for all $g \in D_4$, $gx = xg$.
- (2) An element $x \in D_4$ such that x does not commute, that is, there exists some $g \in D_4$ such that $gx \neq xg$.

6 Group Decomposition

List all commutative groups of size 100. Only list each group once: for full credit, if there are two ways of writing down the same (isomorphic) group, only use one of them.

7 Irreducible polynomials

List all irreducible polynomials modulo 3 of the form $x^2 + ax + 1$, where $a \in \mathbb{Z}_3$. Prove your answer.

8 Finite Fields

Consider the finite field of size 4, $\mathbb{Z}_2[x]/(x^2 + x + 1)$. Compute:

- (1) $01 \cdot 10$
- (2) $10 \cdot 10$
- (3) $10 \cdot 11$
- (3) $11 \cdot 11$

9 Error-correcting codes

It is possible to do this problem without completing the previous one. We will now compute Reed-Solomon codes with the finite field from the previous problem. We will send messages of length 2 (meaning 2 field elements, or four bits), encoded as four field elements.

- (1) What is the codeword corresponding to the message $(01, 11)$?
- (2) Suppose you decode a message, and obtain the polynomial $01X^3 + 11X^2 + \dots$. Assume there is only one error in the message. Which output of the polynomial contains that error?