CS681 - COMPUTATIONAL NUMBER THEORY & ALGEBRA
NITIN SAXENA

ASSIGNMENT 2

POINTS: 50

DATE GIVEN: 01-FEB-2025 DUE: 21-FEB-2025

Rules:

- You are strongly encouraged to work *independently*. That is the best way to understand the subject.
- Write the solutions on your own and honorably *acknowledge* the sources if any. `cse.iitk.ac.in/pages/AntiCheatingPolicy.html`
- Clearly express the fundamental *idea* of your proof/ algorithm before going into the other proof details. The distribution of partial marks is according to the proof steps.
- There will be a penalty if you write unnecessary or unrelated details in your solution. Also, do not repeat the proofs done in the class.
- Submit your solutions, before time, to your TA. Preferably, submit a printed/pdf copy of your LaTeXed or Word processed solution sheet.

  Your TA will help in grading and doubt resolution: `Tufan Singha Mahapatra <tufansm@cse.iitk.ac.in>`
- Problems marked '0 points' are for practice.

Question 1: (Interpolation) *[7 points]* Let f be a monic univariate polynomial in $\mathbb{F}[x]$ of degree d, and let $\alpha_1, \ldots, \alpha_d \in \mathbb{F}$ be distinct.

Given the values $f(\alpha_i)$, $i \in [d]$, show that $f(x)$ can be uniquely reconstructed. Estimate the time-complexity of your algorithm.

Question 2: (Inverse) *[8 points]* Let A be an $n \times n$ matrix over a field $\mathbb{F}$. Give an algorithm, as efficient as you can, to compute A^{-1} (if it exists). Estimate the time-complexity of your algorithm.

Question 3: *[7 points]* Recall the matrix multiplication tensor $T_{n,\mathbb{F}}$, for $n \geq 2$. Show that the rank of this tensor is at least n^2. That is, matrix multiplication requires at least n^2 "multiplications". (*The best lower bound known is* $2.5n^2 - 3n$.)

Question 4: *[7 points]* Show that the finite field $\mathbb{F}_{q^d}$ is a *sub*field of $\mathbb{F}_{q^{d'}}$ iff $d|d'$.

Question 5: *[12 points]* The Cantor-Zassenhaus algorithm done in the class was for *prime* fields $\mathbb{F}_p$ (after applying the Berlekamp reduction). Cantor-Zassenhaus idea could as well be applied directly to polynomials over *any* field $\mathbb{F}_q$.

Give the direct algorithm and the analysis.

Question 6: (Multivariate resultant) *[9 points]* Let $Z_{\mathbb{F}}(f_1, \ldots, f_m)$ denote the set of distinct *zeros* (or solutions) of the algebraic system $f_1 = \cdots = f_m = 0$ in the field $\mathbb{F}$ (which you could assume to be algebraically *closed*, if it helps).

Let $f, g \in \mathbb{F}[x_1, x_2, x_3]$, and let $h \in \mathbb{F}[x_1, x_2]$ be their resultant wrt x_3. How is $Z_{\mathbb{F}}(f, g)$ related to $Z_{\mathbb{F}}(h)$? Be precise.

Question 7: *[0 points]* Give an asymptotic solution for the recurrences, with $T(1) = O(1)$:

(1) $T(n) = \sqrt{n} \cdot T(\sqrt{n}) + O(n \log n)$,
(2) $T(n) = \sqrt{n} \cdot T(2\sqrt{n}) + O(n \log n)$, and
(3) $T(n) = \sqrt{n} \cdot T(3\sqrt{n}) + O(n \log n)$.

Question 8: *[0 points]* Is there a fast algorithm to multiply two degree $\leq n$ polynomials in $\mathbb{F}_q[x]$, that takes $O(n \log n)$ $\mathbb{F}_q$-operations?

Question 9: (Irreducibles) *[0 points]* Let $\mathbb{F}_q$ be a finite field. Show that, for every $d \geq 1$, there *exists* an irreducible polynomial of degree-d over $\mathbb{F}_q$.

Question 10: (Density) *[0 points]* Let $\mathbb{F}_q$ be a finite field. Show that the density of degree-d irreducible polynomials over $\mathbb{F}_q$ is around $1/d$. Use this to give a *fast* (poly$(d \log q)$-time) algorithm to construct the finite field $\mathbb{F}_{q^d}$.

Question 11: *[0 points]* Show that, for every $d \geq 1$, there *exists* an irreducible polynomial of degree-d over $\mathbb{Q}$ (resp. over $\mathbb{R}$).

What about $\mathbb{C}$? What are the field extensions of it?

Question 12: *[0 points]* Let p be a prime. Construct a field $\mathbb{F}$ of characteristic p and a polynomial $f \in \mathbb{F}[x]$ such that: $f'(x)$ vanishes but f is not a p-power.

Question 13: *[0 points]* A commutative ring R is a *domain* if it has no zerodivisor, i.e. $ab = 0$ in R implies that $a = 0$ or $b = 0$.

Show that if R is a domain then,

(1) R is contained in a field.
(2) $R[x]$ is a domain.

Question 14: *[0 points]* An ideal I of $\mathbb{F}[\mathbf{x}_n]$ is called *principal* if it has a single-generator, i.e. $I = \langle f \rangle$. Is there a non-principal ideal when $n = 1$? What about $n = 2$?

Does the *geometry* of $Z(I)$ relate to the number of generators of I?

Question 15: *[0 points]* Show that an $n \times n$ tensor could have rank n. What is the *largest* rank that an $n \times n \times n$ tensor could have?

□□□