CS681 - COMPUTATIONAL NUMBER THEORY & ALGEBRA
NITIN SAXENA

ASSIGNMENT 3

POINTS: 50

DATE GIVEN: 07-MAR-2025 DUE: 30-MAR-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: (RS distance) *[3 points]* Let m, m' be two distinct $N = bk$-bit messages, viewed as elements in $(\mathbb{F}_{2^b})^k$. Encode them to codewords $\phi(m), \phi(m') \in (\mathbb{F}_{2^b})^n$ using the Reed-Solomon encoding.

Give the least number of *bits* in which the two codewords differ. Does this imply error-tolerance close to 50%?

Question 2: *[6+6 points]* Prove that the encoding and decoding of Reed-Solomon is doable in $\tilde{O}(nb)$ time.

Question 3: (Roots) *[4+4+3 points]* Let f be a degree d nonzero polynomial in $\mathbb{F}[x]$.

(1) Show that f has at most d roots if $\mathbb{F}$ is a field.
(2) What if $\mathbb{F}$ is *not* a field?
(3) What if f is a bivariate over a field $\mathbb{F}$?

Question 4: (Cyclic) *[7+7 points]* You have proved earlier that the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic, for any prime p.

Lifting this property, show that the multiplicative group $(\mathbb{Z}/p^e\mathbb{Z})^*$ is *cyclic*, except in the case when $e > 2 = p$.

- Characterize the integers $n > 1$ for which $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic.

Question 5: (Cyclotomic) *[10 points]* You know about the cyclotomic factors of $X^r - 1$ over $\mathbb{Q}$. Building on that, prove the following factorization pattern over finite fields:

The irreducible factors of $\varphi_r(X)$, over $\mathbb{F}_q$, are equidegree ($= \mathrm{ord}_r(q)$, i.e. multiplicative *order* of q mod r).

Question 6: (2-powers) *[0 points]* Show that the multiplicative group $(\mathbb{Z}/2^e\mathbb{Z})^*, e \geq 3$, is *almost*-cyclic: It has a generating set of size two (e.g. $\{-1, 3\}$?).

Question 7: *[0 points]* The list-decoding algorithm that we did in the class could handle $n - 2\sqrt{nk}$ errors. What can you say about list-decoding beyond these many errors?

Question 8: *[0 points]* How do you construct the finite field $\mathbb{F}_{p^n}$ in deterministic poly(p^n)-time? ... in deterministic polylog(p^n)-time?

Question 9: (Density) *[0 points]* Let f be a degree d nonzero polynomial in $\mathbb{F}[x_1, \ldots, x_n]$ and $S \subseteq \mathbb{F}$ be a finite subset of the field. Prove that

$$\mathrm{Pr}_{\mathbf{a} \in S^n}\left[f(\mathbf{a}) = 0\right] \;\leq\; \frac{d}{|S|}\,.$$

Is this bound optimal?

Question 10: *[0 points]* Let $f(x,y)$ be a bivariate polynomial s.t. $x^2 | f(x,0)$ but $f(x,y)$ is square-free. What can you say about '$x^2 | f(x,a)$' for a *random* a?

Question 11: *[0 points]* *Unit*, in a ring R, is an element that has a multiplicative inverse. They form a group that is denoted by R^*. Describe the elements of the group $(\mathbb{F}[x,y]/\langle y^k \rangle)^*$.

Question 12: (Inseparable) *[0 points]* Suppose input $f(x,y) \in \mathbb{F}_p[x,y]$ has a factor g with *multiplicity* p. Could you find g efficiently?

Now take a multivariate input $f(x_1, \ldots, x_n) \in \mathbb{F}_p[\mathbf{x}]$. Suppose it has a factor $g(\mathbf{x})$ with multiplicity p. Could you find g efficiently?

Question 13: *[0 points]* We would like to factor an integral polynomial $f(x)$ efficiently. Suppose we first factor it modulo $\langle 2 \rangle$ and then use Hensel lifting modulo $\langle 4 \rangle$, $\langle 8 \rangle$, $\langle 16 \rangle$, etc. Would this yield an integral factor of f?

What problems do you envisage?

Question 14: (Chebotarev) *[0 points]* Let input $f(x) \in \mathbb{Z}[x]$ be an *ir*reducible integral polynomial of degree d. Are there primes p s.t. f mod p is reducible?

Could you find p efficiently?

Question 15: (Cramer) *[0 points]* Let $A \in \mathbb{F}^{n\times n}$ and $b \in \mathbb{F}^{n\times 1}$. Assuming A nonsingular we want to solve the linear system $Ax = b$. Express x_i, $i \in [n]$, as a *ratio* of two determinants.

□□□