**CS688 - COMPUTATIONAL ARITHMETIC-GEOMETRY & APPLICATIONS**

**NITIN SAXENA**

# ASSIGNMENT 1

**POINTS: 50**

DATE GIVEN: 13-JAN-2023 DUE: 03-FEB-2023 (6PM)

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.
  TA: Diptajit Roy `diptajit@cse.iitk.ac.in`
- Problems marked '0 points' are for practice.

**Question 1:** *[2+2 points]* Recall the definition of a ring and its *characteristic*. Which integers can be the characteristic of a ring? Of a *field*?

**Question 2:** *[6+6+6 points]* Let $p$ be a prime number. Give a construction of the algebraically closed field $\overline{\mathbb{F}}_p$.

- Show that any finite subgroup of $\overline{\mathbb{F}}_p^* := \overline{\mathbb{F}}_p \setminus \{0\}$ is cyclic.

- What can you say about the Galois group of $\overline{\mathbb{F}}_p$ over $\mathbb{F}_p$?

For Qns. 3-4, let $k$ be a finite field of characteristic $p$.

**Question 3:** *[4 point]* Given $n \in \mathbb{Z}_{\geq 0}$ and $x \in k$, we want to compute $x^n$. Estimate the *time complexity* in bit operations.

**Question 4:** (Frobenius morphism) *[4+5+5 points]* Let $\varphi : k[\mathbf{x}] \to k[\mathbf{x}]$ be the map $u \mapsto u^p$. Show that $\varphi$ is a (ring) *homomorphism*.

- Show that, in fact, $\varphi$ is an *automorphism* of $k$. When is it *nontrivial*?
- What are the other endomorphisms of $k$?

**Question 5:** (FLT instance) *[2+3+5 points]* Consider the equation $x^3 + y^3 = z^3$. We consider its *nontrivial* solutions only, i.e. $xyz \neq 0$ and $(x, y, z)$ considered the same as $(\alpha x, \alpha y, \alpha z)$ for any nonzero $\alpha$.

- How many solutions are there in the field $\mathbb{Z}/5\mathbb{Z}$?
- How many solutions do you "expect" in the field $\mathbb{Z}/p\mathbb{Z}$? Justify.
- How many *integral* solutions are there?

**Question 6:** (Hilberts Nullstellensatz) *[0 points]* Recall *prime* and *maximal* ideals of the polynomial ring $A := k[x_1, \ldots, x_n]$. Suppose $k$ is an *algebraically closed* field.

- Let $\mathcal{M}$ be a maximal ideal of $A$. Show that $A/\mathcal{M}$ is a field.
- Show that $A/\mathcal{M} \cong k$.
- Deduce that a set of polynomials $f_1, \ldots, f_m$ have a common solution in $k$ iff $1 \notin \langle f_1, \ldots, f_m \rangle$.

**Question 7:** *[0 points]* Let $k$ be a field and $S$ be its finite subset. Prove that $\overline{k} \setminus S$ is not a closed set.

**Question 8:** *[0 points]* Show that $\mathbb{A}^2_{\overline{k}}$ is an affine variety.

**Question 9:** (Noetherian) *[0 points]* Show that every ideal of $k[\mathbf{x}]$ is *finitely* generated.

How do you interpret this geometrically?

**Question 10:** *[0 points]* Is there a fast algorithm to find a *generator* of $k^*$, where $k$ is a finite field?

□□□