CS681 - COMPUTATIONAL NUMBER THEORY & ALGEBRA

NITIN SAXENA

MID-SEMESTER EXAMINATION

POINTS: 50

GIVEN: 24-FEB-2025 DUE: 28-FEB-2025 (1PM)

Rules:

- Solve it independently. You are *not* allowed to discuss.
- 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 or the assignments.
- Submit your solutions, before time, to your TA (CC: Instructor). Preferably, submit a printed/pdf copy of your LaTeXed or Word processed solution sheet.

  Your TA will help in the doubt resolution: `Tufan Singha Mahapatra <tufansm@cse.iitk.ac.in>`

Question 1: *[16 points]* Recall that integral polynomials $f, g \in \mathbb{Z}[x]$ of bitsize ℓ can be multiplied in $\tilde{O}(\ell)$ time. Use this to sketch an $\tilde{O}(\ell)$-time algorithm that can do *polynomial division*, i.e. compute polynomials q, r such that $f = q \cdot g + r$, where $\deg(r) < \deg(g)$.

Question 2: *[9 points]* Let $f(x)$ be an integral polynomial and $p \neq q$ be prime numbers. Consider p, q, f as the input, given in binary. Design a randomized poly-time algorithm to compute *all* the roots of $f(x)$ modulo pq, or output "none exists".

Question 3: *[4+4+5 points]* Let $\mathbb{F}$ be a field and consider bivariate polynomials $a, b \in \mathbb{F}[x_1, x_2] =: R$. Show that there is a *uni*variate polynomial $r(x_1)$ such that

$$\langle a, b \rangle_R \cap \mathbb{F}[x_1] = \langle r \rangle_{\mathbb{F}[x_1]}.$$

Show that r divides the resultant $\mathrm{Res}_{x_2}(a, b)$.

Prove or disprove whether the resultant $\mathrm{Res}_{x_2}(a, b)$ divides r.

Question 4: *[12 points]* Let $\mathbb{F}_q$ be a finite field of characteristic p. Design a fast/practical algorithm to decide: if for a given polynomial $f(x, y) \in \mathbb{F}_q[x, y]$ there exists an $\alpha \in \mathbb{F}_q$ such that $f(x, \alpha)$ has a *repeated* root in $\mathbb{F}_p$?

□□□