CS681 - COMPUTATIONAL NUMBER THEORY & ALGEBRA
NITIN SAXENA

ASSIGNMENT 4

POINTS: 50

DATE GIVEN: 31-MAR-2025 DUE: 22-APR-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: (Hensel) *[3 points]* Let $f(x,y)$ be a polynomial over a field $\mathbb{F}$ s.t. both $(0,0)$ and $(1,0)$ are its roots. Prove that $f(x,y) \bmod y^k$ factors nontrivially, for every $k \geq 1$.

Question 2: *[4 points]* Let $f(x,y_1,\ldots,y_n)$ be a polynomial, that is monic in x, and is over a large enough field $\mathbb{F}$. Could you prove a variant of Hilbert's irreducibility theorem by projecting to *uni*variate (instead of bivariate as done in the class)?

Question 3: (Gauss & Lagrange) *[12 points]* Show that a variant of the LLL algorithm gives an *exact* shortest vector in the case of *two* dimensional lattices, in deterministic poly-time.

Question 4: (Korselt 1899) *[11 points]* Prove the following characterization of Carmichael numbers:

$\forall a \in (\mathbb{Z}/n\mathbb{Z})^*$, $a^n \equiv a \pmod n \iff n$ is square-free and for each prime factor p, $(p-1)|(n-1)$.

Question 5: (Quadratic reciprocity) *[3+4+10 points]* Give the proofs of the classical properties of the Jacobi symbol used in the class. I.e. for odd and coprime $a, n \in \mathbb{N}$:

(1) $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.
(2) $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.
(3) $\left(\frac{a}{n}\right) \cdot \left(\frac{n}{a}\right) = (-1)^{(a-1)(n-1)/4}$.

Question 6: (Frobenius) *[3 points]* Let $a(x)$ be an integral polynomial and n be a prime. Show that $a(x)^n \equiv a(x^n) \bmod n$.

Question 7: *[0 points]* What is the difference between *coprime* and the concept of *pseudo*-coprime used in Hensel lifting?

Question 8: *[0 points]* Show that, in Hensel lifting, if we start with $g_0(x) \equiv g(x, 0)$ for an *actual* monic factor $g|f$, then we end up with $g_k = g(x, y)$.

Question 9: *[0 points]* Identify the step in Kaltofen's blackbox factoring algorithm that requires projecting $f(x, \mathbf{y})$ to *tri*variate and fails with bivariate.

Question 10: *[0 points]* Prove the correctness of Solovay-Strassen randomized poly-time primality test.

Question 11: *[0 points]* Let $\alpha_i, i \in [n], \epsilon$ be given reals. Devise an algorithm that finds integers $p_i, i \in [n], q$ such that $|p_i - \alpha_i q| \le \epsilon$. The time-complexity should be poly$(n, \log \frac{1}{\epsilon})$.

Question 12: *[0 points]* Show that a variant of the LLL algorithm gives an *exact* shortest vector in the case of n dimensional lattices, in deterministic poly(n^n, B)-time, where B is the input bitsize.

Question 13: *[0 points]* Consider the $\mathbb{F}$-roots E of the cubic equation $y^2 = x^3 + ax + b$ for $a, b \in \mathbb{F}$. Show that the set E has an abelian *group* structure.

Question 14: *[0 points]* Given integers a, n as input, could you give a fast algorithm to compute the integer $\sqrt{a} \bmod n$ (or decide its nonexistence)?

Question 15: *[0 points]* Read about the Quadratic Number Field Sieve and its generalization (NFS) to factor integers.

□□□