Algebra and Computation

Problem Set 3

Due date: May 12th, 2019

Instructions

1. The problem set has **7 questions** with a total score of **80 points**.
2. The due date is **Sunday, May 12$^{\text{th}}$, 2019**.
3. You are welcome to discuss with other classmates **as long as these discussion are reasonable**; these are not meant for one to solve the problem for the other. You are eventually expected to find and write your own solutions and code.

   If you do discuss, you are expected to explicitly mention who you discussed with and which parts of your solution came from these discussions.
4. Solutions are expected as a LaTeX documents.

Questions

Question 1. [10 points] Use Hensel lifting to factorise the following polynomial modulo 256:

$$f(x) = x^2 + 95x + 146 \bmod 256.$$

(Show the intermediate factorisations that you obtained)

Question 2. [10 points] Suppose you are given a polynomial $f \in \mathbb{F}[x]$ of degree at most n, and distinct points $a_1, \ldots, a_n \in \mathbb{F}$ (don't worry about what the field is; you are told that field operations are constant time). The goal is to compute $f(a_1), \ldots, f(a_n)$.

Show, *formally**, that we can compute $f(a_1), \ldots, f(a_n)$ deterministically with $O(n \log^3 n)$ field operations.

**: I know; it is there in the notes but several details are missing. Write down the full proof of correctness.*

Question 3 (Gauss' Lemma)**. [10 points]**

In class when we were studying factorisation of bivariate polynomials, we often interpret an $f(x,y) \in \mathbb{F}[x,y]$ as an element of $(\mathbb{F}(y))[x]$. In other words, as a univariate polynomials whose coefficients are *rational* functions in y. Fortunately, there is a very useful lemma called Gauss' Lemma to help us.

> **Lemma.** *Suppose $f(x,y) \in \mathbb{F}[x,y]$ and there are polynomials $g(x,y), h(x,y) \in (\mathbb{F}(y))[x]$ whose degree in x is non-zero, then there are also polynomials $\tilde{g}, \tilde{h} \in \mathbb{F}[x,y]$ such that $f(x,y) = \tilde{g} \cdot \tilde{h}$.*

The notes has a proof of this for a slightly different situation. Modify that proof to prove the above lemma.

Question 4. [15 points] Say we are given polynomials $f(x,y), g(x,y) \in \mathbb{F}_q[x,y]$ and assume that $q \gg (\deg f)(\deg g)$ and $f(x,y), g(x,y)$ are monic with respect to x. Make the following sketch a formal algorithm for bivariate GCD computation.

> For elements $\{a_1, a_2, \ldots, a_r\}$ from $\mathbb{F}_q$ and compute the gcd of the partial evaluations — $h_{a_i}(x) = \gcd(f(x,a_i), g(x,a_i))$. Find a polynomial $h(x,y)$ of the right degree such that $h(x,a_i) = h_{a_i}(x)$ for all $i \in \{1,\ldots,r\}$ and show that this must indeed be $\gcd(f,g)$.

This r must be decided by you.

Question 5. Consider the following map

$$\begin{aligned} \mathrm{Tr} &: \mathbb{F}_{q^r} \to \mathbb{F}_{q^r} \\ \mathrm{Tr} &: a \mapsto a + a^q + a^{q^2} + \cdots + a^{q^{r-1}}. \end{aligned}$$

- **[10 points]** Show that for any $a \in \mathbb{F}_{q^r}$, show that $\mathrm{Tr}(a) \in \mathbb{F}_q$. Hence, the map Tr is really a map from $\mathbb{F}_{q^r} \to \mathbb{F}_q$.
- **[5 points]** Show that if a is chosen at random from $\mathbb{F}_{q^r}$, then $\mathrm{Tr}(a)$ is a uniformly random element of $\mathbb{F}_q$.
- **[10 points]** Use this map to give an alternate randomized polynomial time algorithm for factorising polynomials in $\mathbb{F}_q[x]$.

Question 6. [10 points] Show that any lattice in $\mathbb{Z}^n$ of rank r has a generating set of at most r vectors.

That is, if say $\mathbf{b}_1, \ldots, \mathbf{b}_m \in \mathbb{Z}^n$ such that $\mathrm{rank}_{\mathbb{Q}}(B) = r$, where B is the matrix consisting of the $\mathbf{b}_i$s are rows. Show that there you can find vectors $\mathbf{b}'_1, \ldots, \mathbf{b}'_r \in \mathbb{Z}^n$ such that

$$\langle \mathbf{b}_1, \ldots, \mathbf{b}_m \rangle_{\mathbb{Z}} = \langle \mathbf{b}'_1, \ldots, \mathbf{b}'_r \rangle_{\mathbb{Z}}.$$

Question 7 (Bonus! No points for this.)**.** Prove or disprove the following:

> For any monic polynomial $f(x) \in \mathbb{Z}[x]$ that is irreducible, there is some prime p such that $f(x)$ is irreducible $\bmod p$.