Math 288X: Algorithms in Algebra and Number Theory

Fall 2021

Problem set #5

Assume that we can do arithmetic in $\mathbb{F}_q$ and choose an element uniformly at random in $\mathcal{O}(1)$.

Problem 1. Verify Lemma 8.3: $X^q - X = u_q(X)v_q(X)$, where

$$u_q(X) = X^{(q+1)/2} - X, \quad v_q(X) = X^{(q-1)/2} - 1 \qquad \text{if } q \text{ is odd}$$

$$u_q(X) = \sum_{i=0}^{r-1} X^{2^i}, \quad v_q(X) = u_q(X) + 1 \qquad \text{if } q = 2^r.$$

Problem 2 (Berlekamp's algorithm)**.** Let $f \in \mathbb{F}_q[X]$ be a squarefree polynomial.

a) Show that the number of irreducible factors of f is the dimension of the $\mathbb{F}_q$-vector space $\{t \in \mathbb{F}_q[X]/(f) : t^q = t\}$.

b) Show that we can find the number of irreducible factors in time $\widetilde{\mathcal{O}}(n^\omega + n \log q)$, where $\omega > 2$ is a matrix multiplication exponent.

c) Let $P = \lceil \frac{q}{2} \rceil / q$. Show that there is a randomized algorithm that finds a splitting $f = gh$ in time $\widetilde{\mathcal{O}}(n^\omega + n \log q)$, where $\deg(g) = k$ with probability $\binom{n}{k} P^k (1-P)^{n-k}$.

d) Show that there is a randomized algorithm that factors f in expected time $\widetilde{\mathcal{O}}(n^\omega + n \log q)$.

Problem 3. Assume that we can do arithmetic in the field K in $\mathcal{O}(1)$. Let $f \in K[X]$ be a polynomial of degree n and let $g_1, \ldots, g_k \in K[X]$ be polynomials of degrees $m_1, \ldots, m_k \geqslant 1$. Show that we can compute the largest numbers $e_1, \ldots, e_k \geqslant 0$ such that $g_i^{e_i} \mid f$ for all $1 \leqslant i \leqslant n$ in time $\widetilde{\mathcal{O}}(n + m_1 + \cdots + m_k)$.
Hint: First, find the smallest power of two greater than e_i. Then, use a binary search.

Problem 4. Let $f \in \mathbb{F}_q[X]$ be a polynomial of degree n with n distinct roots in $\mathbb{F}_q$. Let $P = \lceil \frac{q}{2} \rceil / q$ and let $u_q(X)$ and $v_q(X)$ as in Lemma 8.3. Pick $(a, b) \in \mathbb{F}_q^2$ uniformly at random. Write $f = gh$ with

$$g = \gcd(f, u_q(a + bX)), \qquad h = \gcd(f, v_q(a + bX)).$$

Show that $\mathbb{E}(\deg(g)) = nP$ and $\operatorname{Var}(\deg(g)) = nP(1-P)$. (Hence, we could have used random linear polynomials $a+bX$ instead of random polynomials $a_0 + \cdots + a_{n-1}X^{n-1}$ in the algorithm for Lemma 8.3 and this would still suffice for Theorem 8.4. That's what Cohen does in Algorithm 3.4.6.)

Problem 5 (bonus)**.** Let $f \in \mathbb{F}_q[X]$ be a squarefree polynomial of degree n with k irreducible factors.

a) Show that $\operatorname{disc}(f) \in \mathbb{F}_q^\times$ is a square if and only if $k \equiv n \mod 2$.
Hint: Let $r_1, \ldots, r_n \in \overline{\mathbb{F}_q}$ be the roots of f. Consider the action of the Frobenius automorphism $\varphi_q : \overline{\mathbb{F}_q} \to \overline{\mathbb{F}_q}$ on $\prod_{i<j}(r_i - r_j)$.

b) Show that we can compute $k \bmod 2$ in $\widetilde{\mathcal{O}}(n + \log q)$. (I don't know how to compute k this quickly, even if f splits into linear factors!)