Math 288X: Algorithms in Algebra and Number Theory

Fall 2021

Problem set #6

Assume that we can do arithmetic in $\mathbb{F}_q$ and choose an element uniformly at random in $\mathcal{O}(1)$. Also assume that we can multiply $n \times n$-matrices in time $\mathcal{O}(n^\omega)$, with $2 < \omega \leqslant 3$.

Problem 1 (bonus)**.** Show that (for large n), the average smallest degree of an irreducible factor of a (uniformly) random nonzero polynomial $f \in \mathbb{F}_q[X]$ is $\mathcal{O}(\log n)$, where the constant doesn't depend on q.

Problem 2. Show that there is a randomized algorithm that finds an irreducible polynomial $f \in \mathbb{F}_q[X]$ of degree n in average time $\widetilde{\mathcal{O}}(n^2 \log q)$.

Problem 3. Let $f \in \mathbb{F}_q[X]$ be a polynomial of degree n.

a) For polynomials $g, h \in \mathbb{F}_q[X]$ of degree at most n, show that you can compute $g(h(X)) \bmod f(X)$ in time $\widetilde{\mathcal{O}}(n^{(\omega+1)/2})$.
Hint: Let $m = \lceil n^{1/2} \rceil$. Write $g(X) = \sum_i g_i(X) X^{im}$ with polynomials g_i of degree less than m.

b) Given the polynomial $X^q \bmod f$, show that for $k \geqslant 1$, you can compute $X^{q^k} \bmod f$ in time $\widetilde{\mathcal{O}}(n^{(\omega+1)/2} \log k)$.

c) Show that you can determine whether the polynomial f is irreducible in time $\widetilde{\mathcal{O}}(n^{(\omega+1)/2} + n \log q)$.

d) Show that there is a randomized algorithm that finds an irreducible polynomial $f \in \mathbb{F}_q[X]$ of degree n in average time $\widetilde{\mathcal{O}}(n^{(\omega+3)/2} + n \log q)$.

Remark 4. In fact, there is a randomized algorithm that finds an irreducible polynomial $f \in \mathbb{F}_q[X]$ of degree n in average time $\widetilde{\mathcal{O}}(n^2 + n \log q)$. See [Sho94].

Problem 5. Prove Theorem 11.2: Let K be a nonarchimedean local field as in class. Given monic polynomials $f, g_1, \ldots, g_r \in \mathcal{O}[X]$ such that $f \equiv g_1 \cdots g_r \mod \mathfrak{p}$ with $g_1, \ldots, g_r$ pairwise coprime modulo $\mathfrak{p}$, we can compute the monic polynomials $\widetilde{g}_1, \ldots, \widetilde{g}_r \mod \mathfrak{p}^k$ such that $f \equiv g_1 \cdots g_r \mod \mathfrak{p}^k$ and $\widetilde{g}_i \equiv g_i \mod p$ for $i = 1, \ldots, r$ in time $\widetilde{\mathcal{O}}(nk)$. (As a special case, you should prove Theorem 11.1.)

Problem 6 (More general form of Hensel's lemma). a) Let R be an integral domain with field of fractions K. Let $f, g \in R[X]$ be monic polynomials. Show that their resultant $\mathrm{Res}(f, g)$ can be written as $\mathrm{Res}(f, g) = af + bg$ with polynomials $a, b \in R[X]$.
Hint: If this is unclear, use an adjugate matrix.

b) Let K be a nonarchimedean local field as in class. Let $f, g, h \in \mathcal{O}[X]$ be monic polynomials. Assume that g, h are coprime in K, so that $\mathrm{Res}(g, h) \neq 0$. Let $l = v(\mathrm{Res}(g, h))$. Assume that $f \equiv gh \mod \mathfrak{p}^{k+l}$ for some $k \geqslant l+1$. Show that there are monic polynomials $g, h \in \mathcal{O}[X]$ such that $f = \widetilde{g}\widetilde{h}$ and $\widetilde{g} \equiv g \mod \mathfrak{p}^k$ and $\widetilde{h} \equiv h \mod \mathfrak{p}^k$.

References

[Sho94] Victor Shoup. "Fast construction of irreducible polynomials over finite fields". In: *J. Symbolic Comput.* 17.5 (1994), pp. 371–391. ISSN: 0747-7171. DOI: 10.1006/jsco.1994.1025. URL: https://doi-org.ezp-prod1.hul.harvard.edu/10.1006/jsco.1994.1025.