Math 288X: Algorithms in Algebra and Number Theory

Fall 2021

Problem set #7

Problem 1. We call a basis $(v_1, \dots, v_n)$ of $\mathbb{R}^n$ *Gauß reduced* if we have $|v_1| \leqslant \dots \leqslant |v_n|$ and the Gram-Schmidt coefficients satisfy $|\mu_{ij}| \leqslant \frac{1}{2}$ for all $i < j$.

a) Show that every lattice Λ in $\mathbb{R}^n$ has a Gauß reduced basis.

b) For $n \leqslant 4$, show that there is a constant $\delta_n > 0$ such that if $(v_1, \dots, v_n)$ is a Gauß reduced basis, then any nonzero vector in $\Lambda = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_n$ has length at least $\delta \cdot |v_1|$.

c) For $n \geqslant 5$, show that there is no constant $\delta_n > 0$ as in b).

Problem 2. Show that Algorithm 13.6 from class (computing an LLL-reduced lattice basis) terminates for any basis $v_1, \dots, v_n$ of $\mathbb{R}^n$. (We only showed this for $v_1, \dots, v_n \in \mathbb{Z}^n$.)

Problem 3. Show that for fixed n, given a basis $v_1, \dots, v_n \in \mathbb{Z}^n$ satisfying $|v_1|, \dots, |v_n| \leqslant B$ of a lattice Λ, you can find a shortest vector in Λ in time $\widetilde{\mathcal{O}}_n((\log B)^2)$.

Problem 4. Let $n \geqslant 1$ and consider the cyclotomic field $K = \mathbb{Q}(\zeta_n)$. Its Galois group is $\mathrm{Gal}(K|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, where an element $t \in (\mathbb{Z}/n\mathbb{Z})^\times$ corresponds to the automorphism σ_t sending ζ_n to ζ_n^t. Denote the n-th cyclotomic polynomial by ϕ_n. Let p be any prime number not dividing n.

a) Show that for any prime $\mathfrak{p}$ of K dividing p, the Frobenius automorphism for $\mathfrak{p}|p$ is $\sigma_{p \bmod n}$.

b) Show that $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ with distinct primes $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ of K, where $f = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{F}_p]$ is the multiplicative order of p modulo n.

c) Show that $\phi_n(X) \equiv g_1(X) \cdots g_k(X) \mod p$ with distinct irreducible polynomials $g_1, \dots, g_k \in \mathbb{F}_p[X]$ of degree f. Can you show this directly without using b)?

Problem 5 (Experimental Chebotarev, bonus)**.** Consider the following two polynomials:

$$f(X) = X^3 - 2, \qquad g(X) = X^3 - 3X + 1.$$

a) For each of the two polynomials, which splitting behavior modulo p occurs for which fraction of primes $p < 10000$?

b) What are the Galois groups of the Galois closures of $\mathbb{Q}[X]/(f)$ and $\mathbb{Q}[X]/(g)$ over $\mathbb{Q}$?

c) How to determine the splitting behavior of f, g modulo an unramified prime p from the corresponding Frobenius conjugacy class?

d) Which Frobenius conjugacy class occurs for which fraction of primes $p < 10000$?