Topics: Lattices, Dirichlet L-functions.

11.1. Prove Proposition 4.7: Let L be a full lattice in $\mathbf{R}^n$ and let $\mathcal{F}$ be a fundamental domain for L. Then for every $v \in \mathbf{R}^n$ there exist unique vectors $v_0 \in \mathcal{F}$ and $w \in L$ such that $v = v_0 + w$.

11.2 (CVP in orthogonal case)**.** Let L be a lattice in $\mathbf{R}^n$ with basis $B = \{v_1, \dots, v_n\}$.

Solve the Closest Vector Problem for L under the assumption that B is an orthogonal basis.

[**Hint**: See the solution to SVP in Example 4.12.]

11.3. Let $L \subset \mathbf{R}^2$ be a full lattice.

(a) Prove that the Hadamard ratio of a basis $B = \{v_1, v_2\}$ is

$$\mathcal{H}(B) = \sqrt{|\sin\theta|},$$

where θ is the angle between the vectors v_1 and v_2.

(b) Fixing L and letting B vary, what θ minimises the product $\|v_1\|\,\|v_2\|$?

11.4. Let $L \subset \mathbf{R}^n$ be a full lattice with basis $\{v_1, \dots, v_n\}$. We will prove Hadamard's Inequality:

$$\det L \leqslant \|v_1\|\,\|v_2\|\,\dots\,\|v_n\|.$$

(a) Show that if the inequality holds whenever the vectors v_i are unit vectors, then it holds in general.

So from now on we may assume that $\|v_i\| = 1$ for all i.

(b) Let $W = \mathsf{Span}_{\mathbf{R}}\{e_2, \dots, e_n\}$. Prove that there exists an orthogonal matrix Q such that $Qv_2, \dots, Qv_n \in W$.

(c) Write down the matrix with columns $Qv_1, \dots, Qv_n$ and think about its determinant.

(d) Give a proof (by induction on n) that $\det L \leqslant 1$.

11.5. A crucial piece of the proof that there are infinitely many primes $p \equiv 1 \pmod 4$ that we sketched in the lectures was showing that $L(\chi, 1) > 0$, where $\chi(p) = \left(\dfrac{-1}{p}\right)$ for odd primes p and $\chi(2) = 0$. This was done by simply noticing that $L(\chi, 1) = \arctan(1) = \dfrac{\pi}{4} > 0$.

We now consider the same question for $\chi(p) = \left(\dfrac{-2}{p}\right)$ for odd primes p and $\chi(2) = 0$. We start by expressing

$$\frac{1}{n} = \int_0^1 x^{n-1}\,dx,$$

so that

$$L(\chi, 1) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} = \sum_{n=1}^{\infty} \int_0^1 \chi(n)\,x^{n-1}\,dx.$$

We will assume (without worrying about how to prove it) that it is valid to interchange the summation and the integral, so that

$$L(\chi, 1) = \int_0^1 \left(\sum_{n=1}^{\infty} \chi(n)\,x^{n-1}\right) dx.$$

(a) Show that, for p an odd prime, we have

$$\chi(p) = \begin{cases} 1 & \text{if } p \equiv 1, 3 \pmod 8, \\ -1 & \text{if } p \equiv 5, 7 \pmod 8. \end{cases}$$

(b) Use part (a) to show that, for $m \in \mathbf{Z}_{\geqslant 0}$, we have

$$\begin{aligned} \chi(8m+1) = \chi(8m+3) &= 1, \\ \chi(8m+5) = \chi(8m+7) &= -1, \\ \chi(2m) &= 0. \end{aligned}$$

(c) Use part (b) to obtain

$$L(\chi, 1) = \int_0^1 \left((1 + x^2 - x^4 - x^6) \sum_{m=0}^{\infty} x^{8m} \right) dx.$$

(d) Simplify the integrand to $\dfrac{1+x^2}{1+x^4}$. Note that at this point we can already conclude that $L(\chi, 1) > 0$.

(e) Let's actually evaluate $L(\chi, 1)$ fully. Summon enough calculus powers to substitute $u = x - \dfrac{1}{x}$, get

$$L(\chi, 1) = \int_{-\infty}^{0} \frac{du}{u^2 + 2},$$

then evaluate this last integral to $\dfrac{\pi}{2\sqrt{2}}$.

11.6. Prove that there are:

(a) infinitely many primes $p \equiv 1$ or $3 \pmod 8$;

(b) infinitely many primes $p \equiv 5$ or $7 \pmod 8$.

[**Hint**: Mimic the proof given in the lectures for $p \equiv 1 \pmod 4$, letting $\chi(p) = \left(\dfrac{-2}{p}\right)$ and using Tutorial Question 11.5.]