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 $v = v_0 + w$.

Solution. First we show existence. Let $\{v_1, \dots, v_n\}$ be a $\mathbf{Z}$-basis of L. Write $v = \sum_i \alpha_i v_i$. For each i, write $\alpha_i = t_i + a_i$ with $0 \leqslant t_i < 1$ and $a_i \in \mathbf{Z}$. Setting $v_0 = \sum_i t_i v_i$ and $w = \sum_i a_i v_i$ gives the desired decomposition $v = v_0 + w$.

For uniqueness, suppose we had two such descriptions $v = v_0 + w = v_0' + w'$. Then since the v_i are linearly independent, we have $t_i + a_i = t_i' + a_i'$, and so

$$t_i - t_i' = a_i' - a_i \in \mathbf{Z}.$$

The only way $t_i - t_i'$ can be an integer is if $t_i = t_i'$. This also forces $a_i = a_i'$. Hence $v_0 = v_0'$ and $w = w'$. □

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.]

Solution. Let $w \in \mathbf{R}^n \setminus L$ and write $w = \sum_{i=1}^n a_i v_i$. Since B is an orthogonal basis we have for any $v = \sum_{i=1}^n \alpha_i v_i$:

$$\|w - v\|^2 = \left\| \sum_{i=1}^n (a_i - \alpha_i) v_i \right\|^2 = \sum_{i=1}^n (a_i - \alpha_i)^2 \|v_i\|^2.$$

We want to minimise this quantity with $v \in L$. Since each term in the sum is non-negative, this can be achieved by minimising $|a_i - \alpha_i|$ for all i. Set α_i to be a_i rounded to the nearest integer. Then $v_i = \sum_{i=1}^n \alpha_i v_i \in L$ is the closest vector to w. □

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 $\|v_1\| \, \|v_2\|$?

Solution.

(a) The formula follows by computing $\det L$ as the volume of the fundamental domain defined by v_1 and v_2. From linear algebra this is given by

$$\det L = \|v_1\| \, \|v_2\| \, |\sin\theta|.$$

(b) Since

$$\|v_1\| \, \|v_2\| = \frac{\det L}{|\sin\theta|},$$

we want to maximise $|\sin\theta|$, in other words we want θ to be as close as possible to $\pi/2$. □

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 $\det L \leqslant 1$.

Solution.

(a) Scaling any of the basis vectors multiplies the determinant by that scalar. If $\hat{v_i} = \frac{v_i}{\|v_i\|}$ and $\hat{L}$ is the lattice spanned by the $\hat{v_i}$ then

$$\det L = \|v_1\| \cdots \|v_n\| \det \hat{L} \leqslant \|v_1\| \cdots \|v_n\|.$$

(b) Recall from linear algebra that an orthogonal matrix Q has inverse given by its transpose, or equivalently its rows form an orthonormal basis with respect to the standard inner product. Let $U = \mathsf{Span}_{\mathbf{R}}\{v_2, \dots, v_n\}$ and pick a vector orthogonal to all of U. Any finite set of linearly independent vectors in a finite dimensional vector space can be extended to form a basis, and then we can apply Gram–Schmidt to get an orthonormal basis. Call this orthonormal basis $\{u_1, \dots, u_n\}$ where u_1 is orthogonal to U (i.e. $\langle u_1, v_i \rangle = 0$ for $i = 2, \dots, n$). Let Q be the matrix with i-th row given by u_i. Then the first coordinate of Qv_i is given by $\langle u_1, v_i \rangle = 0$ for $i = 2, \dots, n$. Hence $Qv_i \in W$.

(c) Let M be the basis matrix of L with basis $\{v_1, \dots, v_n\}$. Then the matrix with columns Qv_i has determinant $\det(QM) = \det(Q)\det(M)$. Since Q is orthogonal, $\det Q = \pm 1$. Hence the determinant of the lattice with basis $\{Qv_1, \dots, Qv_n\}$ is the same as $\det L$.

(d) The base case is one-dimensional and so $\det L = \|e_1\| = 1$. For general n, by the previous part, we can compute $\det L$ by computing the determinant of the matrix with columns Qv_i. Since $Qv_i \in W$ for $i = 2, \dots, n$, the first row of QM has zero in all entries except the first (which is $\langle u_1, v_1 \rangle$). Doing cofactor expansion along the first row we then get

$$\det(QM) = \langle u_1, v_1 \rangle \cdot \det M',$$

where M' is the $(n-1) \times (n-1)$ lower right block of QM. The matrix M' has columns given by the 2-nd to n-th coordinates of $Qv_2, \dots, Qv_n$, and since Q preserves lengths, these are all unit vectors (since the first coordinate of these are all zero). Hence by the inductive hypothesis $|\det N| \leqslant 1$. Similarly, using Cauchy–Schwarz we can get $|\langle u_1, v_1 \rangle| \leqslant \|u_1\| \|v_1\| = 1$. Hence the result follows. □

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 $\chi(p) = \left(\frac{-1}{p}\right)$ for odd primes p and $\chi(2) = 0$. This was done by simply noticing that $L(\chi, 1) = \arctan(1) = \frac{\pi}{4} > 0$.

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 $\dfrac{\pi}{2\sqrt{2}}$.

Solution.

(a) By Quadratic Reciprocity we know that for an odd prime p

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

and

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8, \\ -1 & \text{if } p \equiv 3, 5 \pmod 8. \end{cases}$$

By multiplicativity then

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 3 \pmod 8, \\ -1 & \text{if } p \equiv 5, 7 \pmod 8. \end{cases}$$

(b) Part (a) gives us $\chi(p)$ for odd primes, and $\chi(2) = 0$. Then χ gets extended multiplicatively. Therefore $\chi(2m) = 0$ for all $m \in \mathbf{Z}_{\geqslant 1}$. For odd n, the value $\chi(n)$ depends only on the squarefree part of n. Also, any pair of primes p, p' that are congruent modulo 8 contribute $\chi(pp') = 1$. So for the purpose of determining $\chi(n)$, it suffices to consider numbers of the form

$$n = p_1^{a_1} p_3^{a_3} p_5^{a_5} p_7^{a_7},$$

where $p_i \equiv i \pmod 8$ and $a_i = 0, 1$, giving 16 overall cases, one of which is trivial ($a_i = 0$ for all i, where $\chi(n) = 1$).

Looking now at all possibilities for $n \pmod 8$, these cases split into

$$\begin{aligned} 8m+1 &= p_1, p_3p_5p_7, p_1p_3p_5p_7 \\ 8m+3 &= p_3, p_1p_3, p_5p_7, p_1p_5p_7 \\ 8m+5 &= p_5, p_1p_5, p_3p_7, p_1p_3p_7 \\ 8m+7 &= p_7, p_1p_7, p_3p_5, p_1p_3p_5. \end{aligned}$$

Putting this together with $\chi(p_1) = \chi(p_3) = 1$, $\chi(p_5) = \chi(p_7) = -1$, we get

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

(c) Using part (b), we break the sum into even indices (where χ is 0) and odd indices modulo 8:

$$\begin{aligned} \sum_{n=1}^{\infty} \chi(n)\, x^{n-1} &= \sum_{m=0}^{\infty} \chi(8m+1)\, x^{8m} + \sum_{m=0}^{\infty} \chi(8m+3)\, x^{8m+2} \\ &\quad + \sum_{m=0}^{\infty} \chi(8m+5)\, x^{8m+4} + \sum_{m=0}^{\infty} \chi(8m+7)\, x^{8m+6} \\ &= \sum_{m=0}^{\infty} x^{8m} + x^2 \sum_{m=0}^{\infty} x^{8m} - x^4 \sum_{m=0}^{\infty} x^{8m} - x^6 \sum_{m=0}^{\infty} x^{8m}, \end{aligned}$$

which leads to the desired expression for $L(\chi, 1)$.

(d) In the first place, for $0 < x < 1$ we have

$$\sum_{m=0}^{\infty} x^{8m} = \frac{1}{1-x^8},$$

so

$$L(\chi, 1) = \int_0^1 \frac{1 + x^2 - x^4 - x^6}{1 - x^8}\, dx = \int_0^1 \frac{(1-x^4)(1+x^2)}{(1-x^4)(x+x^4)}\, dx = \int_0^1 \frac{1+x^2}{1+x^4}\, dx.$$

(e) Now let $u = x - \dfrac{1}{x}$, then $u^2 = x^2 + \dfrac{1}{x^2} - 2$, so $u^2 - 2 = x^2 + \dfrac{1}{x^2} = \dfrac{1+x^4}{x^2}$. Moreover

$$du = \left(1 + \frac{1}{x^2}\right) dx = \frac{1+x^2}{x^2} dx = \frac{1+x^4}{x^2} \frac{1+x^2}{1+x^4} dx = (u^2+2) \frac{1+x^2}{1+x^4} dx.$$

So after the substitution the integral becomes

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

Substitute $v = u/\sqrt{2}$, then $u^2 + 2 = 2(v^2+1)$ and $dv = du/\sqrt{2}$ so

$$L(\chi, 1) = \frac{1}{\sqrt{2}} \int_{-\infty}^{0} \frac{dv}{v^2+1} = \frac{1}{\sqrt{2}} \Big[\arctan(v) \Big]_{-\infty}^{0} = \frac{1}{\sqrt{2}} \left(0 + \frac{\pi}{2}\right) = \frac{\pi}{2\sqrt{2}}. \qquad \square$$

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.]

Solution. Recall that the Riemann zeta function satisfies

$$-\zeta(2) \leqslant \log \zeta(s) - \sum_p \frac{1}{p^s} \leqslant \zeta(2) \quad \text{for all real } s \geqslant 1, \tag{1}$$

and the Dirichlet L-function attached to χ satisfies

$$-\zeta(2) \leqslant \log L(\chi, s) - \sum_p \frac{\chi(p)}{p^s} \leqslant \zeta(2) \quad \text{for all real } s \geqslant 1. \tag{2}$$

Adding (1) and (2):

$$-2\zeta(2) \leqslant \log \zeta(s) + \log L(\chi, s) - \sum_p \frac{1}{p^s} - \sum_p \frac{\chi(p)}{p^s} \leqslant 2\zeta(2).$$

We have

$$-\sum_p \frac{1}{p^s} - \sum_p \frac{\chi(p)}{p^s} = -\frac{1}{2^s} - 2 \sum_{p \equiv 1,3 \pmod 8} \frac{1}{p^s},$$

and $L(\chi, 1) > 0$ by Tutorial Question 11.5, so by taking the limit as $s \longrightarrow 1$ we conclude that there are infinitely many primes $p \equiv 1, 3 \pmod 8$.

Similarly, if we subtract (2) from (1) we end up with

$$-2\zeta(2) + \log L(\chi, s) + \frac{1}{2^s} \leqslant \log \zeta(s) - 2 \sum_{p \equiv 5,7 \pmod 8} \frac{1}{p^s} \leqslant 2\zeta(2) + \log L(\chi, s) + \frac{1}{2^s} \quad \text{for all real } s \geqslant 1,$$

which shows that there are infinitely many primes $p \equiv 5, 7 \pmod 8$. $\square$