D-MATH
Prof. Richard Pink

Algebraic Number Theory

FS 2018

Solutions 3

Lattices and Minkowski Theory

*1. Show *Minkowski's second theorem about successive minima*: Let Γ be a complete lattice in a euclidean vector space $(V, \langle\ ,\ \rangle)$ of finite dimension n. The *successive minima* $\lambda_1, \ldots, \lambda_n$ *of* Γ are defined iteratively by choosing for any $1 \leqslant i \leqslant n$ an element $\gamma_i \in \Gamma \smallsetminus \bigoplus_{j=1}^{i-1} \mathbb{R}\gamma_j$ of minimal length $\lambda_i := \|\gamma\|$. Then

$$\frac{2^n}{n!}\operatorname{vol}(\mathbb{R}^n/\Gamma) \ \leqslant\ \lambda_1 \cdots \lambda_n \cdot \operatorname{vol}(B) \ \leqslant\ 2^n \operatorname{vol}(\mathbb{R}^n/\Gamma),$$

where B is the closed ball of radius 1.

Solution: See Theorem 6.3.3 in
`https://www.math.leidenuniv.nl/~evertse/Minkowski.pdf`.

2. Show *Lagrange's four square theorem*: Every nonnegative integer n can be written as the sum of four squares.

(a) Show that if m and n are sums of four squares, then so is mn.
Hint: Use the reduced norm on the ring of quaternions $\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$.

(b) Reduce the theorem to the case that n is a prime number p.

(c) Find integers α, β such that $\alpha^2 + \beta^2 \equiv -1 \bmod p$.
Hint: Consider the intersection of the sets

$$S := \Big\{\alpha^2 \bmod p \ \Big|\ 0 \leqslant \alpha < \frac{p}{2}\Big\} \quad \text{and} \quad S' := \Big\{-1-\beta^2 \bmod p \ \Big|\ 0 \leqslant \beta < \frac{p}{2}\Big\}.$$

(d) For any such α, β show that

$$\Gamma := \big\{a = (a_1, \ldots, a_4) \in \mathbb{Z}^4 \ \big|\ a_1 \equiv \alpha a_3 + \beta a_4 \operatorname{mod}(p) \text{ and } a_2 \equiv \beta a_3 - \alpha a_4 \operatorname{mod}(p)\big\}$$

contains a nonzero point a in the open ball of radius $\sqrt{2p}$ in $\mathbb{R}^4$.

(e) Show that $\|a\|^2 = p$ and conclude.

Solution: See
`https://concretenonsense.wordpress.com/2009/02/10/lagranges-four-square-theorem/`.

3. (a) Show that the number fields $\mathbb{Q}(\sqrt{11})$ and $\mathbb{Q}(\sqrt{-11})$ have class number 1.

(b) Show that the class group of $\mathbb{Q}(\sqrt{-14}))$ is cyclic of order 4.

(c) Show that $f := X^3 + X + 1 \in \mathbb{Q}[X]$ is irreducible and that the cubic number field $\mathbb{Q}(\theta)$ with $f(\theta) = 0$ has class number 1.

Solution: See also Chapter 12.6 in Alaca, Williams [1] to compute the class group.

(a) **Case** $K := \mathbb{Q}(\sqrt{11})$**:** Since $11 \equiv 3 \bmod 4$, we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{11}] \cong \mathbb{Z}[X]/(X^2 - 11)$ and $\operatorname{disc}(\mathcal{O}_K) = 4 \cdot 11 = 44$. Since $11 > 0$, the field is real quadratic with $r = 2$ and $s = 0$. By a proposition from the lecture, every ideal class in $\mathrm{Cl}(\mathcal{O}_K)$ contains an ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ with

$$\mathrm{Nm}(\mathfrak{a}) \leqslant \left(\frac{2}{\pi}\right)^s \sqrt{|\operatorname{disc}(\mathcal{O}_K)|} = \sqrt{44} = 6.6332...$$

Therefore, it suffices to show that all ideals $\mathfrak{a}$ of $\mathcal{O}_K$ of norm $\leqslant 6$ are principal.
Recall that for any non-zero ideal $\mathfrak{a} \subset \mathcal{O}_K$ we have $\mathrm{Nm}(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}]$. In particular $\mathrm{Nm}(\mathfrak{a}) = 1$ if and only if $\mathfrak{a} = (1)$, which is principal. Moreover, any prime divisor $\mathfrak{p}|\mathfrak{a}$ satisfies $\mathrm{Nm}(\mathfrak{p})|\,\mathrm{Nm}(\mathfrak{a})$. As any non-zero ideal is a product of prime ideals, it thus suffices to show that every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ of norm $\leqslant 6$ is principal. For any such $\mathfrak{p}$, the norm is the order of the residue field and therefore a prime power.
If $\mathrm{Nm}(\mathfrak{p}) = 2$, then $(2) \subseteq \mathfrak{p}$, and $\mathfrak{p}/(2)$ is an ideal of index 2 of the factor ring $\mathcal{O}_K/(2) \cong \mathbb{F}_2[X]/(X^2 + 1) = \mathbb{F}_2[X]/(1 + X)^2$. Thus $\mathfrak{p}/(2)$ corresponds to the unique maximal ideal $(1 + X)$, and so $\mathfrak{p} = (2, 1 + \sqrt{11})$. It remains to show that $\mathfrak{p} = (\alpha)$ for some $\alpha = a + b\sqrt{11} \in \mathcal{O}_K$. Any such α must satisfy $|a^2 - 11b^2| = |\,\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)| = \mathrm{Nm}((\alpha)) = 2$. A little experimentation shows that the equality $|a^2 - 11b^2| = 2$ holds for $\alpha := 3 + \sqrt{11}$. For this we then in fact have $\mathrm{Nm}((\alpha)) = 2$ and hence $(\alpha) = \mathfrak{p}$. Thus the only ideal of $\mathcal{O}_K$ of norm 2 is principal.
If $\mathrm{Nm}(\mathfrak{p}) = 3$, then likewise $\mathfrak{p}/(3)$ is an ideal of index 3 of $\mathcal{O}_K/(3) \cong \mathbb{F}_3[X]/(X^2+1)$. But since $X^2 + 1$ is irreducible in $\mathbb{F}_3[X]$, this factor ring is a field of order 9 and does not possess an ideal of index 3. Thus there exists no ideal of $\mathcal{O}_K$ of norm 3.
If $\mathrm{Nm}(\mathfrak{p}) = 4$, then $(4) \subseteq \mathfrak{p}$. For $\mathfrak{p}$ prime this implies that $(2) \subset \mathfrak{p}$, which by comparing indices implies that $(2) = \mathfrak{p}$. But we have seen above that $\mathcal{O}_K/(2)$ is not a field; hence (2) is not a prime ideal. Thus there is no prime ideal of norm 4.
If $\mathrm{Nm}(\mathfrak{p}) = 5$, then likewise $\mathfrak{p}/(5)$ is an ideal of index 5 of $\mathcal{O}_K/(5) \cong \mathbb{F}_5[X]/(X^2 - 1)$ $= \mathbb{F}_5[X]/((1 + X)(1 - X))$. Thus $\mathfrak{p}/(5)$ corresponds to the maximal ideal $(1 \pm X)$ and so $\mathfrak{p} = (5, 1 \pm \sqrt{11})$ for some choice of sign. It remains to show that $\mathfrak{p} = (\alpha)$ for some $\alpha = a + b\sqrt{11} \in \mathcal{O}_K$. Any such α must satisfy $|a^2 - 11b^2| = |\,\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)| = \mathrm{Nm}((\alpha)) = 5$. A little experimentation shows that the equality $|a^2 - 11b^2| = 2$ holds for $\alpha := 4 \mp \sqrt{11} = 5 - (1 \pm \sqrt{11}) \in \mathfrak{p}$. For this we then have $\mathrm{Nm}((\alpha)) = 5$, and comparing indices shows that $(\alpha) = \mathfrak{p}$. Thus every ideal of $\mathcal{O}_K$ of norm 5 is principal.
Finally, there is no prime ideal with $\mathrm{Nm}(\mathfrak{p}) = 6$, because 6 is not a prime power.
Case $K := \mathbb{Q}(\sqrt{-11})$**:** Since $-11 \equiv 1 \bmod 4$, we have $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-11}}{2}] \cong \mathbb{Z}[X]/(X^2 - X + 3)$ and $\operatorname{disc}(\mathcal{O}_K) = -11$. Since $\mathbb{Q}(\sqrt{-11})$ does not have any embeddings into $\mathbb{R}$, we have $r = 0$ and $s = 1$. By a proposition from the lecture, every ideal class in $\mathrm{Cl}(\mathcal{O}_K)$ contains an ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ with

$$\mathrm{Nm}(\mathfrak{a}) \leqslant \left(\frac{2}{\pi}\right)^s \sqrt{|\operatorname{disc}(\mathcal{O}_K)|} = \frac{2}{\pi} \cdot \sqrt{11} = 2.1114...$$

Therefore, it suffices to show that all ideals $\mathfrak{a}$ of $\mathcal{O}_K$ of norm $\leqslant 2$ are principal.

Again $\mathrm{Nm}(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}] = 1$ if and only if $\mathfrak{a} = (1)$, which is principal.

If $\mathrm{Nm}(\mathfrak{a}) = 2$, then $(2) \subseteq \mathfrak{a}$, and $\mathfrak{a}/(2)$ is an ideal of index 2 of the factor ring $\mathcal{O}_K/(2) \cong \mathbb{F}_2[X]/(X^2 - X + 3)$. Since $X^2 - X + 3 = X^2 + X + 1$ in $\mathbb{F}_2[X]$ is irreducible, this factor ring is a field of order 4 and does not possess an ideal of index 2. Thus there exists no ideal of $\mathcal{O}_K$ of norm 2, and we are done.

(b) See Example 12.6.4 in [1]. To factor (2) and (3), instead of using the Legendre symbol, one can do the following: We have $\mathcal{O}_K/(2) \cong \mathbb{F}_2[X]/(X^2)$ with (X) the only prime ideal and hence $(2) = (2, \sqrt{-14})^2$. Similarly, we have $\mathcal{O}_K/(3) \cong \mathbb{F}_3[X]/(X^2 + 2)$ which has the prime ideals $(1 - X)$ and $(1 + X)$. Hence $(3) = (3, 1 + \sqrt{-14}) \cdot (3, 1 - \sqrt{-14})$.

(c) See Example 12.6.8 in [1]. To factor (3), instead of using the theorem from the reference, we calculate it manually: We have $\mathcal{O}_K/(3) \cong \mathbb{F}_3[X]/(X^3+X+1)$, where $(X - 1)(X^2 + X - 1) \equiv X^3 + X + 1 \bmod 3$ is the factorization in $\mathbb{F}_3[X]$. Then $\bar{\mathfrak{p}}_1 := (X - 1)$ and $\bar{\mathfrak{p}}_2 := (X^2 + X - 1)$ are prime and their product is 0. Hence $(3) = (3, \theta - 1) \cdot (3, \theta^2 + \theta - 1)$ is the prime factorization.

4. (a) Let K be a number field. Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$ and $m \geqslant 1$ an integer such that $\mathfrak{a}^m = (\alpha)$. Let L/K be a finite extension containing an element $\sqrt[m]{\alpha}$ such that $\sqrt[m]{\alpha}^{\,m} = \alpha$. Show that $\mathfrak{a}\mathcal{O}_L = \sqrt[m]{\alpha}\,\mathcal{O}_L$.

   (b) Show that there is a finite field extension L/K such that for every fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ the ideal $\mathfrak{a}\mathcal{O}_L$ is principal.

Solution:

(a) Since $\mathfrak{a}^m = \alpha\mathcal{O}_K$, it follows that $(\mathfrak{a}\mathcal{O}_L)^m = \mathfrak{a}^m\mathcal{O}_L = \alpha\mathcal{O}_L = \sqrt[m]{\alpha}^{\,m}\mathcal{O}_L = (\sqrt[m]{\alpha}\,\mathcal{O}_L)^m$. Unique factorization of fractional ideals in L now implies that $\mathfrak{a}\mathcal{O}_L = \sqrt[m]{\alpha}\,\mathcal{O}_L$.

(b) Let h be the class number of K and let $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ denote a system of representatives of the elements of the class group. For each i choose $\alpha_i \in K^\times$ such that $\mathfrak{a}_i^h = (\alpha_i)$ and an element $\sqrt[h]{\alpha_i}^{\,h} \in \bar{K}$ such that $\sqrt[h]{\alpha_i}^{\,h} = \alpha_i$. Set $L := K(\sqrt[h]{\alpha_1}, \ldots, \sqrt[h]{\alpha_h}) \subset \bar{K}$. Then for any fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ we have $\mathfrak{a} = \alpha\mathfrak{a}_j$ for some $\alpha \in K^\times$ and some j; hence by (a) we have $\mathfrak{a}\mathcal{O}_L = \alpha\mathfrak{a}_j\mathcal{O}_L = \alpha\sqrt[h]{\alpha_i}\,\mathcal{O}_L$, which is a principal ideal.

5. Let p be a prime with $p \equiv 3 \bmod 4$. It is known that the class number of $K := \mathbb{Q}(\sqrt{p})$ is odd. Use this fact to prove that there exist $a, b \in \mathbb{Z}$ such that

$$|a^2 - pb^2| = 2.$$

Hint: Show that $(2, 1 + \sqrt{p}) = (2, 1 + \sqrt{p})^{|\mathrm{Cl}(\mathcal{O}_K)|} \cdot \mathfrak{a}$ for a principal ideal $\mathfrak{a}$.

Solution: See
`http://people.math.carleton.ca/~williams/ant/ch12-solns/ch12-qu28.pdf`.

For the fact that the class number of K is odd, see Brown [2].

References

[1] S. Alaca, K. S. Williams, *Introductory to Algebraic Number Theory.* Cambridge University Press. 2004.

[2] E. Brown. Class numbers of real quadratic number fields. *Trans. Amer. Math. Soc.*, 190:99–107, 1974.