Mathematische Annalen

Upper bounds for the Euclidean minima of abelian fields of odd prime power conductor

Eva Bayer-Fluckiger · Piotr Maciak

Abstract The aim of this paper is to give upper bounds for the Euclidean minima of abelian fields of odd prime power conductor. In particular, these bounds imply Minkowski's conjecture for totally real number fields of conductor p^r, where p is an odd prime number and $r \geq 2$.

1 Introduction

Let K be an algebraic number field, and let $\mathcal{O}_K$ be its ring of integers. Let $\mathrm{N} : K \to \mathbb{Q}$ be the absolute value of the norm map. The number field K is said to be *Euclidean* (with respect to the norm) if for every $a, b \in \mathcal{O}_K$ with $b \neq 0$ there exist $c, d \in \mathcal{O}_K$ such that $a = bc + d$ and $\mathrm{N}(d) < \mathrm{N}(b)$. It is easy to check that K is Euclidean if and only if for every $x \in K$ there exists $c \in \mathcal{O}_K$ such that $\mathrm{N}(x - c) < 1$. This suggests to look at

$$M(K) = \sup_{x \in K} \inf_{c \in \mathcal{O}_K} \mathrm{N}(x - c),$$

called the *Euclidean minimum* of K.

The study of Euclidean number fields and Euclidean minima is a classical one, see for instance [9] for a survey. The present paper is concerned with *upper bounds* for $M(K)$ in the case where K is an abelian field of odd prime power conductor. Let us recall some previous results. Let n be the degree of K and D_K the absolute value of its

E. Bayer-Fluckiger (✉) · P. Maciak
École Polytechnique Fédérale de Lausanne, EPFL–FSB–MATHGEOM–CSAG,
1015 Lausanne, Switzerland
e-mail: eva.bayer@epfl.ch

P. Maciak
e-mail: piotr.maciak@epfl.ch

discriminant. It is shown in [2] that for any number field K, we have $M(K) \leq 2^{-n} D_K$. The case of *totally real* fields is especially interesting, and has been the subject matter of several papers. In particular, a conjecture attributed to Minkowski states that if K is totally real, then

$$M(K) \leq 2^{-n} \sqrt{D_K}.$$

This conjecture is proved for $n \leq 8$, cf. [6,7,13]; see also McMullen's paper [13] for a proof of the case $n \leq 6$ and a survey of the topic.

The point of view taken in the present paper is to study this conjecture for totally real abelian fields, and more generally give upper bounds for Euclidean minima of abelian fields. A starting point of this investigation is [2] where it is proved that we have $M(K) \leq 2^{-n} \sqrt{D_K}$ if K is a cyclotomic field of prime power conductor or the maximal totally real subfield of such a field. The present paper contains some results concerning abelian fields of odd prime power conductor. In particular, we show that if K is such a field, then there exist constants $C = C(K) \leq \frac{1}{3}$ and $\varepsilon = \varepsilon(K) \leq 2$ such that

$$M(K) \leq C^n (\sqrt{D_K})^\varepsilon.$$

If $[K : \mathbb{Q}] > 2$, then one may choose $\varepsilon(K) < 2$. Moreover, we show that ε is asymptotically equal to 1 and that under certain assumptions C is asymptotically equal to $\frac{1}{2\sqrt{3}}$; see Theorem 1 for the precise statement. In Theorem 2 we obtain the bound

$$M(K) \leq \omega^n \sqrt{D_K},$$

where $\omega = \omega(K)$ is a constant which under certain assumptions is asymptotically equal to $\frac{1}{2\sqrt{3}}$. In particular, using these bounds we show

Theorem *Suppose that K is a totally real field of conductor p^r, where p is an odd prime and $r \geq 2$. Let n be the degree of K and let D_K be its discriminant. Then*

$$M(K) \leq 2^{-n} \sqrt{D_K}.$$

In other words, Minkowski's conjecture holds for this family of fields.

The strategy of the proofs is the following. If K is an algebraic number field, we consider lattices defined on the ring of integers $\mathcal{O}_K$ in the sense of [1], Sect. 1. This leads to a Hermite–like invariant of $\mathcal{O}_K$, denoted by $\tau_{\min}(\mathcal{O}_K)$, cf. [1], Definition 9, and Sect. 4 of the present paper. By [2], Corollary 5.2, we have

$$M(K) \leq \left(\frac{\tau_{\min}(\mathcal{O}_K)}{n} \right)^{n/2} \sqrt{D_K},$$

where n is the degree of K and D_K the absolute value of its discriminant. In order to apply this result, we have to estimate $\tau_{\min}(\mathcal{O}_K)$. The main technical task of this paper is to do this in the case of abelian fields of odd prime power conductor.

The paper is structured as follows. After a brief section containing the notation used throughout the paper, Sect. 3 describes the main results (Theorems 1, 2). The rest of the paper is devoted to their proofs, starting in Sect. 4 with a summary of some notions and results concerning lattices and number fields, and their relation to Euclidean minima. Suppose now that K is an abelian field of prime power conductor. In Sect. 5, we construct integral bases of $\mathcal{O}_K$. In Sect. 6, these bases are used to describe the lattice obtained by the canonical embedding of $\mathcal{O}_K$ (equivalently, the lattice given by the trace form). It turns out that this lattice is isomorphic to the orthogonal sum of lattices similar to the dual of a root lattice of type A and of a lattice invariant by a symmetric group which already appears in [2]. Using this information, we obtain an estimate of the Hermite–like thickness of the lattice $\mathcal{O}_K$, leading to an upper bound of $\tau_{\min}(\mathcal{O}_K)$ that we apply in Sect. 7 to prove Theorems 1 and 2. Finally, Sect. 8 contains some partial results and open questions concerning abelian fields of odd prime conductor.

2 Notation and a definition

The following notation will be used throughout this paper. The set of all abelian extensions of $\mathbb{Q}$ of odd prime power conductor will be denoted by $\mathcal{A}$. For $K \in \mathcal{A}$ we set:

$$n - \text{ the degree of } K/\mathbb{Q},$$
$$D - \text{ the absolute value of the discriminant of } K,$$
$$p - \text{ the unique prime dividing the conductor of } K,$$
$$r - \text{ the } p\text{-adic additive valuation of the conductor of } K,$$
$$\zeta - \text{ a primitive root of unity of order } p^r,$$
$$e - \text{ the degree } [\mathbb{Q}(\zeta) : K].$$

If the dependence on the field K needs to be emphasized, we shall add the index K to the above symbols. For example, we shall write n_K instead of n.

We also need the following definition

Definition 1 Let $\psi : \mathcal{D} \to \mathbb{R}$ be a function, where $\mathcal{D} \subset \mathcal{A}$. We shall say that $\psi_o \in \mathbb{R}$ is the limit of ψ as n_K goes to infinity and write

$$\lim_{n_K \to \infty} \psi(K) = \psi_0$$

if for every $\epsilon > 0$ there exists $N > 0$ such that for every field $K \in \mathcal{D}$

$$n_K > N \implies |\psi(K) - \psi_0| < \epsilon.$$

We shall also write

$$\lim_{p_K \to \infty} \psi(K) = \psi_0$$

if for every $\epsilon > 0$ there exists $N > 0$ such that for every field $K \in \mathcal{D}$

$$p_K > N \implies |\psi(K) - \psi_0| < \epsilon.$$

3 Euclidean minima—statement of the main results

In this section we present the main results of the paper; the proofs will be given in Sect. 7. We keep the notation and definitions of the previous sections.

Theorem 1 *Let $K \in \mathcal{A}$. Then there exist constants $\varepsilon = \varepsilon(K) \leq 2$ and $C = C(K) \leq \frac{1}{3}$ such that*

$$M(K) \leq C^n \, (\sqrt{D_K})^\varepsilon.$$

If $[K : \mathbb{Q}] > 2$, then one may choose $\varepsilon(K) < 2$. Moreover,

$$\lim_{n_K \to \infty} \varepsilon(K) = 1.$$

If $r_K \geq 2$, or $r_K = 1$ and $[\mathbb{Q}(\zeta) : K]$ is constant, then we also have

$$\lim_{p_K \to \infty} C(K) = \frac{1}{2\sqrt{3}}.$$

Theorem 2 *Let $K \in \mathcal{A}$. Then there is a constant $\omega = \omega(K)$ such that*

$$M(K) \leq \omega^n \sqrt{D_K}.$$

If $r_K \geq 2$, or $r_K = 1$ and $[\mathbb{Q}(\zeta) : K]$ is constant, then

$$\lim_{p_K \to \infty} \omega(K) = \frac{1}{2\sqrt{3}}.$$

Moreover, if $r_K \geq 2$, then $\omega(K) \leq 3^{-2/3}$.

Note that this implies that Minkowski's conjecture holds for all totally real fields $K \in \mathcal{A}$ with composite conductor

Corollary 1 *Let $K \in \mathcal{A}$, and suppose that the conductor of K is of the form p^r with $r > 1$. Then*

$$M(K) \leq 2^{-n} \sqrt{D_K}.$$

This follows from Theorem 2, since $3^{-2/3} < 1/2$, and for K totally real this is precisely Minkowski's conjecture.

4 Lattices and number fields

We start by recalling some standard notion concerning Euclidean lattices (see for instance [4] and [12]). A *lattice* is a pair (L, q), where L is a free $\mathbb{Z}$–module of finite rank, and $q : L_{\mathbb{R}} \times L_{\mathbb{R}} \to \mathbb{R}$ is a positive definite symmetric bilinear form, where $L_{\mathbb{R}} = L \otimes_{\mathbb{Z}} \mathbb{R}$. If (L, q) is a lattice and $a \in \mathbb{R}$, then we denote by $a(L, q)$ the lattice (L, aq). Two lattices (L, q) and (L', q') are said to be *similar* if and only if there exists $a \in \mathbb{R}$ such that (L', q') and $a(L, q)$ are isomorphic, in other words if there exists an isomorphism of $\mathbb{Z}$-modules $f : L \to L'$ such that $q'(f(x), f(y)) = aq(x, y)$.

Let (L, q) be a lattice, and set $q(x) = q(x, x)$. The *maximum* of (L, q) is defined by

$$\max(L, q) = \sup_{x \in L_{\mathbb{R}}} \inf_{c \in L} q(x - c).$$

Note that $\max(L, q)$ is the square of the covering radius of the associated sphere covering. The *determinant* of (L, q) is denoted by $\det(L, q)$. It is by definition the determinant of the matrix of q in a $\mathbb{Z}$–basis of L. The *Hermite–like thickness* of (L, q) is

$$\tau(L, q) = \frac{\max(L, q)}{\det(L, q)^{1/m}},$$

where m is the rank of L. Note that $\tau(L, q)$ only depends on the similarity class of the lattice (L, q).

A family of lattices

Let $m \in \mathbb{N}$, and $b \in \mathbb{R}$ with $b > m$. Let $L = L_{b,m}$ be a lattice in $\mathbb{R}^m$ with Gram matrix

$$bI_m - J_m = \begin{pmatrix} b-1 & -1 & \dots & -1 \\ -1 & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & -1 \\ -1 & \dots & -1 & b-1 \end{pmatrix},$$

where I_m is the $m \times m$-identity matrix and $J_m \in \{1\}^{m \times m}$ is the all-ones matrix. Then L is a lattice of determinant $(b - m)b^{m-1}$. Moreover, the automorphism group of L contains $\langle -I_m \rangle \times S_m$, where the symmetric group S_m acts by permuting the coordinates. These lattices were defined in [3], (4.1). Note that the lattice $L_{m+1,m}$ is similar to the dual lattice $A_m^{\#}$ of the root lattice A_m (see for instance [4], Chapter 4, Sect. 6, or [12] for the definition of the root lattice A_m).

Lattices defined over number fields

In the sequel, we will be concerned with lattices defined on rings of integers of abelian number fields. Let K be a number field of degree n, and suppose that K is either totally real or totally complex. Let us denote by $^- : K \to K$ the identity in the first case

and the complex conjugation in the second one, and let P be the set of totally positive elements of the fixed field of this involution. Let us denote by $\text{Tr} : K \to \mathbb{Q}$ the trace map. For any $\alpha \in P$, set $q_\alpha(x, y) = \text{Tr}(\alpha x \overline{y})$ for all $x, y \in K$. Then $(\mathcal{O}_K, q_\alpha)$ is a lattice. Set

$$\tau_{\min}(\mathcal{O}_K) = \inf\{\tau(\mathcal{O}_K, q_\alpha) \mid \alpha \in P\}.$$

If D_K is the absolute value of the discriminant of K, then, by [2], Corollary 5.2, we have

$$M(K) \leq \left(\frac{\tau_{\min}(\mathcal{O}_K)}{n}\right)^{\frac{n}{2}} \sqrt{D_K}, \tag{1}$$

This upper bound will be used in Sect. 7 to prove Theorems 1 and 2.

5 Gaussian periods and integral bases

Let $K \in \mathcal{A}$. In order to exploit the upper bound of Sect. 4, we need some information concerning the lattices defined on the ring of integers $\mathcal{O}_K$, and these will be described using integral bases of $\mathcal{O}_K$. The aim of this section is to find such bases. This will be done in the spirit of the work of Leopold [10], see also Lettl [11].

Recall that the p^r is the conductor of K and that $e = [\mathbb{Q}(\zeta) : K]$. Then e divides $p - 1$. This implies that the extension $\mathbb{Q}(\zeta)/K$ is tamely ramified, and hence the trace map $\text{Tr} : \mathbb{Z}[\zeta] \to \mathcal{O}_K$ is surjective.

Set $R = \mathbb{Z}/p^r\mathbb{Z}$ and let us denote by H the unique subgroup of order e of R^*. Then H acts on R by left multiplication. The orbit $H0$ will be denoted by $\mathbf{0}$ and called the zero orbit.

Definition 2 For $\mathbf{x} \in R/H \setminus \{\mathbf{0}\}$, we define a Gaussian period

$$f_\mathbf{x} = \sum_{x \in \mathbf{x}} \zeta^x.$$

In addition, we set $f_\mathbf{0} = e$.

If $\mathbf{x} = Hx$, then $f_\mathbf{x} = \text{Tr}_{\mathbb{Q}(\zeta)/K}(\zeta^x)$. As the trace map $\text{Tr} : \mathbb{Z}[\zeta] \to \mathcal{O}_K$ is surjective., Gaussian periods are generators of $\mathcal{O}_K$ over $\mathbb{Z}$. The next proposition will be used to show that $\mathcal{O}_K$ has actually an integral basis consisting of Gaussian periods.

Set $S = \mathbb{Z}/p^{r-1}\mathbb{Z}$, and let $\pi : R \to S$ be the canonical projection. The group H acts on S by $h \cdot s = \pi(h)s$. Clearly, π is a morphism of H-sets and hence it induces the unique map between the orbit sets $\rho : R/H \to S/H$ such that $\rho(Hx) = H\pi(x)$ for all $x \in R$. In other words, if $\mu_R : R \to R/H$ and $\mu_S : S \to S/H$ are the canonical projections, then $\rho\mu_R = \mu_S\pi$. In particular, ρ is surjective. For any subset A of R, set $\zeta^A = \{\zeta^a \mid a \in A\}$, and let us denote by A^c the complement of A in R. For a finite set X, we denote by $|X|$ the number of elements of X.

We thank H.W. Lenstra, Jr, for sending us the part (1) $\Leftrightarrow$ (2) of the following proposition.

Proposition 1 *Let $A \subset R \setminus \{0\}$ be an H-invariant set. The following conditions are equivalent:*

1. *ζ^A is a basis of $\mathbb{Z}[\zeta]$.*
2. *The restriction $\pi : A^c \to S$ is a bijection.*
3. *The restriction $\rho : A^c/H \to S/H$ is a bijection.*
4. *For every $\mathbf{y} \in S/H$ we have*

$$|\rho^{-1}(\mathbf{y}) \cap A/H| = |\rho^{-1}(\mathbf{y})| - 1.$$

5. *$Tr_{\mathbb{Q}(\zeta)/K}(\zeta^A) = \{ f_{\mathbf{x}} \mid \mathbf{x} \in A/H \}$ is a basis of $\mathcal{O}_K$.*

Proof $(1) \Leftrightarrow (2)$ Note that the sum of powers of ζ over any coset of $\ker \pi$ in R equals zero. Thus, if ζ^A is a $\mathbb{Z}$-basis, then A must miss at least one element of each coset. It cannot miss more than one since then the cardinality of A would be too small. Conversely, if A misses exactly one element from each coset, then the sum relation mentioned shows that the $\mathbb{Z}$-span of ζ^A contains all roots of unity of order p^r. Hence ζ^A forms an integral basis.

$(2) \Rightarrow (3)$ This follows immediately from the fact that π is a morphism of H-sets and A^c is H-invariant.

$(3) \Rightarrow (2)$ First, we shall show that $\pi_{|A^c}$ is onto. Suppose that this is not true. Then π must miss at least one full orbit since it is an H-map but in such a case the restriction of $\rho : A^c/H \to S/H$ would not be surjective. Thus $\pi_{|A^c}$ is onto. We claim that $|A^c| = |S|$, which implies that $\pi_{|A^c}$ is a bijection. Indeed, the set A^c/H maps bijectively onto S/H, which implies that they have the same cardinality. Since both A^c/H and S/H contain the respective zero orbits, it is easy to check that

$$\left|A^c/H\right| = 1 + \frac{|A^c| - 1}{e} \quad \text{and} \quad |S/H| = 1 + \frac{|S| - 1}{e},$$

which readily implies $|A^c| = |S|$.

$(3) \Leftrightarrow (4)$ Since A is H-invariant, it follows that the sets A/H, A^c/H form a partition of the orbit space R/H. Consequently, for every $\mathbf{y} \in S/H$ we have

$$|\rho^{-1}(\mathbf{y}) \cap A/H| = |\rho^{-1}(\mathbf{y})| - |\rho^{-1}(\mathbf{y}) \cap A^c/H|.$$

The restriction $\rho : A^c/H \to S/H$ is a bijection if and only if $|\rho^{-1}(\mathbf{y}) \cap A^c/H| = 1$ for every $\mathbf{y} \in S/H$.

$(1) \Rightarrow (5)$ Assume now that ζ^A is a basis of $\mathbb{Z}[\zeta]$. We shall show that $Tr_{\mathbb{Q}(\zeta)/K}(\zeta^A)$ is an integral basis of K. Since $0 \notin A$, it follows that A is a union of n orbits, each of cardinality e. Consequently,

$$|Tr_{\mathbb{Q}(\zeta)/K}(\zeta^A)| \leq n = \operatorname{rank} \mathcal{O}_K.$$

Since $\mathbb{Q}(\zeta)/K$ is tamely ramified, $Tr_{\mathbb{Q}(\zeta)/K}(\zeta^A)$ generates $\mathcal{O}_K$, which in turn implies that we have in fact $|Tr_{\mathbb{Q}(\zeta)/K}(\zeta^A)| = n$ and that $Tr_{\mathbb{Q}(\zeta)/K}(\zeta^A)$ is an integral basis of K.

$(5) \Rightarrow (1)$ Since $\mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(\zeta^A)$ is a basis, we have $|\mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(\zeta^A)| = n$. It follows that $|A| \geq ne = p^{r-1}(p-1)$. Suppose by contradiction that ζ^A is not a basis. Then $\pi : A^c \to S$ is not a bijection. Since

$$|A^c| = |R| - |A| \leq p^r - p^{r-1}(p-1) = p^{r-1} = |S|,$$

it follows that $\pi : A^c \to S$ is not a surjection. Consequently, there exists $x_0 \notin \ker \pi$ such that the coset $C = x_0 + \ker \pi$ is contained in A. Note that the intersection of C with any H-orbit is either empty or a singleton. Indeed, if $x_0 + z_1 = h(x_0 + z_2)$ for some $z_1, z_2 \in \ker \pi$ and $h \in H \setminus \{1\}$, then $(1 - h)x_0 \in \ker \pi$. Note that $1 - h$ is invertible. Hence $x_0 \in \ker \pi$, which is a contradiction. Therefore the set $HC = \{hc \mid h \in H, c \in C\}$ is contained in A and it has $|H| \cdot |C|$ elements. Furthermore, HC/H is contained in A/H and

$$\sum_{\mathbf{x} \in HC/H} f_{\mathbf{x}} = \sum_{hc \in HC} \zeta^{hc} = \sum_{h \in H} \sum_{c \in C} \zeta^{hc} = 0,$$

which contradicts the linear independence of elements of $\mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(\zeta^A)$. Thus ζ^A is a basis of $\mathbb{Z}[\zeta]$.   □

This proposition implies that $\mathcal{O}_K$ has an integral basis consisting of Gaussian periods. Indeed, we have

Corollary 2 *There exists an H–invariant set $A \subset R \setminus \{0\}$ such that*

$$Tr_{\mathbb{Q}(\zeta)/K}(\zeta^A) = \{f_{\mathbf{x}} \mid \mathbf{x} \in A/H\}$$

is a basis of $\mathcal{O}_K$.

Proof For all $\mathbf{y} \in S/H$ with $\mathbf{y} \neq \mathbf{0}$, let us choose $\mathbf{x_y} \in R/H$ such that $\rho(\mathbf{x_y}) = \mathbf{y}$. Set $\mathbf{x_0} = \mathbf{0}$, and let $B = \cup_{\mathbf{y} \in S/H} \mathbf{x_y}$. Then B is an H–invariant subset of R containing 0, and the restriction $\rho : B/H \to S/H$ is a bijection. Set $A = B^c$; then A is an H–invariant subset of $R \setminus \{0\}$, and the restriction $\rho : A^c/H \to S/H$ is a bijection. By Proposition 1, this implies that $\mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(\zeta^A) = \{f_{\mathbf{x}} \mid \mathbf{x} \in A/H\}$ is a basis of $\mathcal{O}_K$.   □

6 Geometry of the ring of integers

We keep the notation of the previous section; in particular, $K \in \mathcal{A}$ and $p = p_K$. Recall that $\mathcal{O}_K$ is the ring of integers of K, and let us consider the lattice $(\mathcal{O}_K, q)$, where q is defined by $q(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}(x\overline{y})$. As we have seen in Sect. 4, the Hermite–like thickness of this lattice can be used to give an upper bound of the Euclidean minimum of K. The purpose of this section is to describe the lattice $(\mathcal{O}_K, q)$ using the results of Sect. 5, so that we can compute its Hermite–like thickness.

We will see that $(\mathcal{O}_K, q)$ decomposes in a natural way into the orthogonal sum of a lattice Γ_K, which is similar to the orthogonal sum of copies of the dual lattice of

the root lattice A_{p-1}, and of a lattice Λ_K, which is similar to a certain lattice of type $L_{b,m}$ defined in Sect. 4. The Hermite–like thickness of these lattices can be estimated, cf. [3], Theorem 4.1. This allows us to give good upper bounds for the Euclidean minima of fields $K \in \mathcal{A}$, following the strategy outlined in the introduction and in Sect. 4.

Let Γ_K be the orthogonal sum of $\frac{p^{r-1}-1}{e}$ copies of the lattice $p^{r-1}A_{p-1}^{\#}$. Set $d = \frac{p-1}{e}$, and let $\Lambda_K = ep^{r-1}L_{\frac{p}{e},d}$ (note that the scaling is taken in the sense of Sect. 4, that is it refers to multiplying the quadratic form by the scaling factor).

Theorem 3 *The lattice $(\mathcal{O}_K, q)$ is isometric to the orthogonal sum of Γ_K and of Λ_K.*

Before proving this theorem, we need a few lemmas. Recall that R denotes the ring $\mathbb{Z}/p^r\mathbb{Z}$, and let $\mathfrak{m} = p\mathbb{Z}/p^r\mathbb{Z}$ be the maximal ideal of R. Note that if $r = 1$, then $\mathfrak{m}$ is the zero ideal. For $\mathbf{x} \in R/H$ we set $\mathrm{ord}_p(\mathbf{x}) = \max\{k \in \mathbf{N} \mid \mathbf{x} \subset \mathfrak{m}^k\}$. Let us denote by μ the Möbius function.

Lemma 1 *Let $\mathbf{x} \in R/H$. Then,*

$$Tr_{K/\mathbb{Q}}(f_{\mathbf{x}}) = \frac{\phi(p^r)}{\phi(p^{r-s})} \cdot \mu(p^{r-s}),$$

where $s = \mathrm{ord}_p(\mathbf{x})$

Proof Let $x_0 \in \mathbf{x}$. We have

$$\mathrm{Tr}_{K/\mathbb{Q}}(f_{\mathbf{x}}) = \mathrm{Tr}_{K/\mathbb{Q}}(\mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(\zeta^{x_0})) = \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta^{x_0})$$

Assume first that $s = 0$. Then, $\mathbf{x} \subset R^*$ and hence $x_0 \in R^*$. Consequently,

$$\mathrm{Tr}_{K/\mathbb{Q}}(f_{\mathbf{x}}) = \sum_{x \in R^*} \zeta^{x_0 x} = \sum_{x \in R^*} \zeta^x = \mu(p^r) = \frac{\phi(p^r)}{\phi(p^{r-s})} \cdot \mu(p^{r-s}).$$

Now, assume that $1 \le s < r$. Then, $x_0 = p^s x_1$ with $x_1 \in R^*$. Set $\xi = \zeta^{p^s}$ and $T = \mathbb{Z}/p^{r-s}\mathbb{Z}$. Then ξ is a primitive root of unity of order p^{r-s}. If $\tau : R^* \to T^*$ is the natural map with kernel G, and the set $Y \subset R^*$ is mapped by τ bijectively onto $(\mathbb{Z}/p^{r-s}\mathbb{Z})^*$, then

$$\mathrm{Tr}_{K/\mathbb{Q}}(f_{\mathbf{x}}) = \sum_{x \in R^*} \xi^{x_1 x} = \sum_{x \in R^*} \xi^x = \sum_{g \in G}\sum_{y \in Y} \xi^{gy} = \sum_{g \in G}\sum_{y \in Y} \xi^y$$

$$= |G| \cdot \sum_{t \in T^*} \xi^t = \frac{\phi(p^r)}{\phi(p^{r-s})} \cdot \mu(p^{r-s}).$$

Finally, if $s = r$, then $\mathbf{x} = \mathbf{0}$ and $x_0 = 0$ and hence

$$\mathrm{Tr}_{K/\mathbb{Q}}(f_{\mathbf{x}}) = \mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1) = \phi(p^r) = \frac{\phi(p^r)}{\phi(p^{r-s})} \cdot \mu(p^{r-s}).$$

$\square$

Proposition 2 *Let* $\mathbf{x_1}, \mathbf{x_2} \in R/H \setminus \{\mathbf{0}\}$. *Then,*

$$Tr_{K/\mathbb{Q}}(f_{\mathbf{x_1}} \overline{f_{\mathbf{x_2}}}) = \begin{cases} p^r - p^{r-1} & \text{if } \mathbf{x_1} = \mathbf{x_2} \text{ and } \rho(\mathbf{x_1}) = \rho(\mathbf{x_2}) \neq \mathbf{0}, \\ p^r - ep^{r-1} & \text{if } \mathbf{x_1} = \mathbf{x_2} \text{ and } \rho(\mathbf{x_1}) = \rho(\mathbf{x_2}) = \mathbf{0}, \\ -p^{r-1} & \text{if } \mathbf{x_1} \neq \mathbf{x_2} \text{ and } \rho(\mathbf{x_1}) = \rho(\mathbf{x_2}) \neq \mathbf{0}, \\ -ep^{r-1} & \text{if } \mathbf{x_1} \neq \mathbf{x_2} \text{ and } \rho(\mathbf{x_1}) = \rho(\mathbf{x_2}) = \mathbf{0}, \\ 0 & \text{if } \mathbf{x_1} \neq \mathbf{x_2} \text{ and } \rho(\mathbf{x_1}) \neq \rho(\mathbf{x_2}). \end{cases}$$

Proof Let $x_1 \in \mathbf{x_1}$ and $x_2 \in \mathbf{x_2}$. For $h \in H$ we set $\mathbf{x}(h) = H(x_1 - x_2 h)$ and $s(h) = \text{ord}_p \mathbf{x}(h)$. Then,

$$\begin{aligned} f_{\mathbf{x_1}} \overline{f_{\mathbf{x_2}}} &= \left(\sum_{h_1 \in \hbar} \zeta^{x_1 h_1} \right) \left(\sum_{h_2 \in \hbar} \zeta^{-x_2 h_2} \right) = \sum_{h_1 \in \hbar} \sum_{h_2 \in \hbar} \zeta^{x_1 h_1 - x_2 h_2} \\ &= \sum_{h_1 \in \hbar} \sum_{h \in \hbar} \zeta^{x_1 h_1 - x_2 h h_1} = \sum_{h_1 \in \hbar} \sum_{h \in \hbar} \zeta^{(x_1 - x_2 h) h_1} \\ &= \sum_{h \in \hbar} \sum_{h_1 \in \hbar} \zeta^{(x_1 - x_2 h) h_1} = \sum_{h \in \hbar} f_{\mathbf{x}(h)}. \end{aligned}$$

By Lemma 1, we have

$$\text{Tr}_{K/\mathbb{Q}}(f_{\mathbf{x_1}} \overline{f_{\mathbf{x_2}}}) = \sum_{h \in H} \text{Tr}_{K/\mathbb{Q}}(f_{\mathbf{x}(h)}) = \sum_{h \in H} \frac{\phi(p^r)}{\phi(p^{r-s(h)})} \cdot \mu(p^{r-s(h)}). \qquad (2)$$

If $\mathbf{x_1} = \mathbf{x_2}$, we can take $x_1 = x_2$ and then $\mathbf{x}(h) = Hx_1(1-h)$. Clearly, $s(1) = r$. If $h \neq 1$, then we have $s(h) = \text{ord}_p \mathbf{x_1}$. Thus, if $\text{ord}_p \mathbf{x_1} < r - 1$, then $\rho(\mathbf{x_1}) \neq \mathbf{0}$ and the only non-zero term of the sum (2) is the one corresponding to $h = 1$. Thus, we have

$$\text{Tr}_{K/\mathbb{Q}}(f_{\mathbf{x_1}} \overline{f_{\mathbf{x_2}}}) = \frac{\phi(p^r)}{\phi(p^{r-s(1)})} \cdot \mu(p^{r-s(1)}) = \phi(p^r) = p^r - p^{r-1}.$$

If $\text{ord}_p(\mathbf{x_1}) = r - 1$, then $\rho(\mathbf{x_1}) = \mathbf{0}$ and the sum (2) becomes

$$\begin{aligned} \text{Tr}_{K/\mathbb{Q}}(f_{\mathbf{x_1}} \overline{f_{\mathbf{x_2}}}) &= \sum_{h \in H} \frac{\phi(p^r)}{\phi(p^{r-s(h)})} \cdot \mu(p^{r-s(h)}) \\ &= \phi(p^r) + (e-1) \cdot \frac{\phi(p^r)}{\phi(p^{r-1})} \cdot \mu(p) \\ &= p^r - ep^{r-1}. \end{aligned}$$

Suppose now that $\mathbf{x_1} \neq \mathbf{x_2}$. Observe that $\rho(\mathbf{x_1}) = \rho(\mathbf{x_2})$ if and only if there is an $h \in H$ such that $s(h) = r - 1$. Moreover, in such a case an element h with this property is unique unless $\rho(\mathbf{x_1}) = \mathbf{0}$, in which case we have $s(h) = r - 1$ for all $h \in H$. Thus, assuming that $\rho(\mathbf{x_1}) = \rho(\mathbf{x_2})$ and $\rho(\mathbf{x_1}) \neq \mathbf{0}$, we have

$$\mathrm{Tr}_{K/\mathbb{Q}}(f_{\mathbf{x_1}}\overline{f_{\mathbf{x_2}}}) = \sum_{h \in H} \frac{\phi(p^r)}{\phi(p^{r-s(h)})} \cdot \mu(p^{r-s(h)})$$

$$= \frac{\phi(p^r)}{\phi(p)} \cdot \mu(p) = -p^{r-1}.$$

If $\rho(\mathbf{x_1}) = \mathbf{0}$, then

$$\mathrm{Tr}_{K/\mathbb{Q}}(f_{\mathbf{x_1}}\overline{f_{\mathbf{x_2}}}) = \sum_{h \in H} \frac{\phi(p^r)}{\phi(p^{r-s(h)})} \cdot \mu(p^{r-s(h)})$$

$$= \sum_{h \in H} \frac{\phi(p^r)}{\phi(p)} \cdot \mu(p) = -ep^{r-1}.$$

Finally, if $\rho(\mathbf{x_1}) \neq \rho(\mathbf{x_2})$, then $s(h) \leq r - 2$ for all $h \in H$, which gives

$$\mathrm{Tr}_{K/\mathbb{Q}}(f_{\mathbf{x_1}}\overline{f_{\mathbf{x_2}}}) = 0.$$

$\square$

Lemma 2 *Let* $\mathbf{y} \in S/H$. *Then,*

$$|\rho^{-1}(\mathbf{y})| = \begin{cases} 1 + \frac{p-1}{e} & \text{if } \mathbf{y} = \mathbf{0}, \\ p & \text{if } \mathbf{y} \neq \mathbf{0}. \end{cases}$$

Proof Let $X = \rho^{-1}(\mathbf{y})$. Note that $\mathbf{0} \in X$ if and only if $\mathbf{y} = \mathbf{0}$, hence

$$|\mu_R^{-1}(X)| = \begin{cases} 1 + e \cdot (|X| - 1) & \text{if } \mathbf{y} = \mathbf{0}, \\ |X| \cdot e & \text{if } \mathbf{y} \neq \mathbf{0}. \end{cases}$$

On the other hand, $\mu_R^{-1}(X) = \mu_R^{-1}(\rho^{-1}(\mathbf{y})) = (\rho\mu_R)^{-1}(\mathbf{y}) = (\mu_S\pi)^{-1}(\mathbf{y})$.
    If $\mathbf{y} = \mathbf{0}$, then

$$\mu_R^{-1}(X) = (\mu_S\pi)^{-1}(\mathbf{0}) = \{x \in R \mid H\pi(x) = \mathbf{0}\} = \mathfrak{m}^{r-1}$$

and hence $|(\mu_S\pi)^{-1}(\mathbf{0})| = p$, which implies that $|X| = 1 + \frac{p-1}{e}$.
    If $\mathbf{y} \neq \mathbf{0}$, then there is an element $x_0 \in R \setminus \mathfrak{m}^{r-1}$ such that $\mathbf{y} = H\pi(x_0)$. Consequently,

$$\mu_R^{-1}(X) = (\mu_S\pi)^{-1}(\mathbf{y}) = \{x \in R \mid H\pi(x) = H\pi(x_0)\}$$

$$= \{x \in R \mid x = k + hx_0 \text{ for some } k \in \mathfrak{m}^{r-1} \text{ and } h \in H\}.$$

Let $k_1, k_2 \in \mathfrak{m}^{r-1}$ and $h_1, h_2 \in H$. If $k_1 + h_1 x_0 = k_2 + h_2 x_0$, then $h_1(1 - h_1^{-1}h_2)x_0 \in \mathfrak{m}^{r-1}$. Since $x_0 \notin \mathfrak{m}^{r-1}$, it follows that $1 - h_1^{-1}h_2$ is not invertible. Hence $h_1 = h_2$, which in turn implies that $k_1 = k_2$. Therefore $|(\mu_S\pi)^{-1}(\mathbf{y})| = |\mathfrak{m}^{r-1}| \cdot |H| = pe$, which gives $|X| = p$. $\square$

Proof of Theorem 3 Let $A \subset R \setminus \{0\}$ be an H-invariant set such that $\mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(\zeta^A)$ is a basis of $\mathcal{O}_K$. For $\mathbf{y} \in S/H$ we set

$$B_{\mathbf{y}} = \{ f_{\mathbf{x}} \in \mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(\zeta^A) \mid \rho(\mathbf{x}) = \mathbf{y} \} \quad \text{and} \quad L_{\mathbf{y}} = \mathrm{span}_{\mathbb{Z}} B_{\mathbf{y}}.$$

By Proposition 2, we have

$$\mathcal{O}_K = \perp_{\mathbf{y} \in S/H} L_{\mathbf{y}}, \tag{3}$$

in other words the lattice $(\mathcal{O}_K, q)$ is the orthogonal sum of the lattices obtained by the restriction of q to $L_{\mathbf{y}}$ for $\mathbf{y} \in S/H$. Combining Lemma 2 and the condition (4) of Proposition 1, we obtain that

$$|B_{\mathbf{y}}| = \begin{cases} \frac{p-1}{e} & \text{if } \mathbf{y} = \mathbf{0}, \\ p-1 & \text{if } \mathbf{y} \neq \mathbf{0}. \end{cases}$$

Furthermore, using Proposition 2 again, we conclude that the Gram matrix of the lattice $L_{\mathbf{y}}$ with respect to $B_{\mathbf{y}}$ is $p^{r-1}(pI_{p-1} - J_{p-1})$ unless $\mathbf{y} = \mathbf{0}$ in which case it equals $ep^{r-1}(\frac{p}{e}I_d - J_d)$, where $d = \frac{p-1}{e}$. Consequently, we have $L_{\mathbf{0}} = \Lambda_K$. Moreover, S/H has $\frac{p^{r-1}-1}{e}$ nonzero orbits. As a result,

$$\perp_{\mathbf{y} \neq \mathbf{0}} L_{\mathbf{y}} \simeq \Gamma_K.$$

Thus the equality (3) implies that $(\mathcal{O}_K, q)$ is isometric to the orthogonal sum of Γ_K and Λ_K.

We now apply Theorem 3 to give an upper bound of the Hermite–like thickness of the lattice $(\mathcal{O}_K, q)$. The following is well–known

Lemma 3 *We have*

$$\det(\mathcal{O}_K, q) = p^{\upsilon},$$

where

$$\upsilon = rn - \frac{(p^{r-1} - 1)}{e} - 1.$$

Proof Note that $\det(\mathcal{O}_K, q)$ is the absolute value of the discriminant of K. The result follows from Theorem 4.1 in [14]. Alternatively, one can compute $\det(\mathcal{O}_K, q)$ directly using Theorem 3. □

Lemma 4 *We have*

$$\max(\mathcal{O}_K, q) \leq n \cdot \frac{p^{r+1} + p^r + 1 - e^2}{12p}.$$

Proof By Theorem 4.1 in [3], we have

$$\max(L_{\frac{p}{e},d}) \leq \frac{d(p^2 + p + 1 - e^2)}{12ep}.$$

Furthermore, $\max(L_{p,p-1}) = \frac{p^2-1}{12}$. Consequently,

$$
\begin{aligned}
\max(\mathcal{O}_K, q) &= \sum_{\mathbf{y} \in S/H} \max(L_{\mathbf{y}}) \\
&\leq \frac{p^{r-1} - 1}{e} \cdot p^{r-1} \cdot \frac{p^2 - 1}{12} + p^{r-1} \cdot \frac{d(p^2 + p + 1 - e^2)}{12p} \\
&= dp^{r-1} \left[\left(\frac{p^{r-1} - 1}{p - 1} \right) \cdot \left(\frac{p^2 - 1}{12} \right) + \frac{p^2 + p + 1 - e^2}{12p} \right] \\
&= n \cdot \frac{(p^{r-1} - 1)(p + 1)p + (p^2 + p + 1 - e^2)}{12p} \\
&= n \cdot \frac{p^{r+1} + p^r + 1 - e^2}{12p}.
\end{aligned}
$$

$\square$

As a direct consequence of the above lemmas, we obtain the following upper bound of $\tau_{\min}(\mathcal{O}_K)$

Corollary 3 *We have*

$$\tau_{\min}(\mathcal{O}_K) \leq \tau(\mathcal{O}_K, q) \leq n \cdot p^{r - \frac{v}{n}} \cdot \frac{p^{r+1} + p^r + 1 - e^2}{12p^{r+1}}.$$

This bound will be used in the next section to prove Theorems 1 and 2.

7 Euclidean minima—proof of the main results

In this section we prove the main results of the paper, namely the upper bounds for Euclidean minima stated in Sect. 3. Recall that for any number field K of degree n, we have

$$M(K) \leq \left(\frac{\tau_{\min}(\mathcal{O}_K)}{n} \right)^{\frac{n}{2}} \sqrt{D_K},$$

where D_K is the absolute value of the discriminant of K. For $K \in \mathcal{A}$, we now have an upper bound (see Corollary 3) and this will be used in the proofs.

Proof of Theorem 1 Set

$$f = \frac{p^{r+1} + p^r + 1 - e^2}{12p^{r+1}}, \quad C = \sqrt{f}, \quad \varepsilon = \frac{rn}{v}.$$

Then, by the inequality (1) and Corollary 3, we get

$$M(K) \leq \left(\frac{\tau(\mathcal{O}_K)}{n}\right)^{\frac{n}{2}} \sqrt{D_K} \leq C^n \cdot (\sqrt{D_K})^{\varepsilon}.$$

First we shall prove that $\varepsilon(K)$ has the stated properties. If $r = 1$, then $\upsilon = n - 1$ and $\varepsilon = \frac{n}{n-1}$, which implies that $\varepsilon \leq 2$ with the equality only for $n = 2$. It is also clear that $\varepsilon \to 1$ if $n \to \infty$. Assume that $r \geq 2$. A simple calculation shows that

$$2\upsilon - rn = rdp^{r-1} - 2d\left(\frac{p^{r-1} - 1}{p - 1}\right) - 2.$$

Clearly,

$$\frac{p^{r-1} - 1}{p - 1} \leq (r - 1)p^{r-2},$$

which gives

$$2\upsilon - rn \geq rdp^{r-1} - 2d(r - 1)p^{r-2} - 2 = rdp^{r-2}(p - 1) + p^{r-2}d - 2 > 0,$$

which implies that $\varepsilon < 2$. Another simple calculation shows that

$$\varepsilon = \frac{r\left(1 + \frac{1}{\upsilon}\right)}{(r - \delta)}, \tag{4}$$

where

$$\delta = \frac{p^{r-1} - 1}{p^{r-1}(p - 1)}.$$

Observe that

$$\ln n < r \ln p < r(p - 1) \leq rp - 1.$$

Since $0 \leq \delta < \frac{1}{p}$, it follows that for $n \geq 3$ we have

$$0 \leq \frac{r}{r - \delta} - 1 < \frac{1}{rp - 1} < \frac{1}{\ln n}.$$

Thus we get

$$\lim_{n \to \infty} \frac{r}{r - \delta} = 1. \tag{5}$$

Finally, it follows from (4) that $\upsilon + 1 = (r - \delta)n$. Since $r - \delta > r - 1 \geq 1$, we get $\upsilon > n - 1$. Consequently

$$\lim_{n \to \infty} \left(1 + \frac{1}{\upsilon}\right) = 1. \tag{6}$$

Combining the equalities (5), (6), we obtain

$$\lim_{n_K \to \infty} \varepsilon(K) = 1.$$

Now we prove the properties of $C(K)$. We have

$$f = \frac{p^{r+1} + p^r + 1 - e^2}{12 p^{r+1}} \leq \frac{p^{r+1} + p^r}{12 p^{r+1}} = \frac{p+1}{12p} \leq \frac{1}{9}$$

and hence $C \leq \frac{1}{3}$. We can also write

$$f = \frac{p^{r+1} + p^r + 1 - e^2}{12 p^{r+1}} = \frac{1}{12}\left(1 + \frac{1}{p} + \frac{1}{p^{r+1}} - \frac{e^2}{p^{r+1}}\right).$$

If $r = 1$ and e is constant, then f clearly approaches $\frac{1}{12}$ as $p \to \infty$ and hence $C(K) \to \frac{1}{2\sqrt{3}}$. Assume now that $r \geq 2$. Since $1 \leq e \leq p - 1$, it follows that

$$0 < f - \frac{1}{12} \leq \frac{1}{12p}$$

and thus

$$0 < C(K) - \frac{1}{2\sqrt{3}} \leq \frac{\sqrt{3}}{12p}.$$

Consequently,

$$\lim_{p_K \to \infty} C(K) = \frac{1}{2\sqrt{3}}$$

and this concludes the proof of the theorem.

Proof of Theorem 2 We shall use the same notation as in the proof of Theorem 1. In addition, we set

$$\omega(K) = C(K) \cdot (\sqrt{p})^{\delta + \frac{1}{n}}.$$

A simple calculation using Corollary 3 and formulas derived in the proof of Theorem 1 gives

$$\left(\frac{\tau(\mathcal{O}_K)}{n}\right)^{\frac{1}{2}} \leq \omega(K)$$

Then, by the inequality (1), we have

$$M(K) \leq \omega^n \sqrt{D_K}.$$

If $r \geq 2$, then $\delta + \frac{1}{n} \leq \frac{2}{p}$ and hence

$$1 < (\sqrt{p})^{\delta + \frac{1}{n}} \leq \sqrt[p]{p}.$$

Consequently, using Theorem 1, we obtain

$$\lim_{p \to \infty} \omega(K) = \lim_{p \to \infty} C(K) \cdot \lim_{p \to \infty} (\sqrt{p})^{\delta + \frac{1}{n}} = \frac{1}{2\sqrt{3}}. \tag{7}$$

Moreover, using Theorem 1 and the fact that the sequence $\{\sqrt[p]{p}\}_{p \geq 3}$ is decreasing, we also get

$$\omega(K) \leq C(K) \cdot \sqrt[p]{p} \leq \frac{1}{3}\sqrt[3]{3} = 3^{-2/3}.$$

If $r = 1$, then $\delta = 0$ and

$$(\sqrt{p})^{\delta + \frac{1}{n}} = (\sqrt{p^e})^{\frac{1}{p-1}}.$$

Thus assuming that e is constant, we see that (7) holds as well. This concludes the proof of the theorem.

8 Abelian fields of prime conductor

If K is an abelian field of conductor p^r with $r \geq 2$, then we have seen that $M(K) \leq 2^{-n}\sqrt{D_K}$, cf. Corollary 1. In particular, if K is totally real, then Minkowski's conjecture holds for K. If $r = 1$, that is if the conductor of K is prime, then our results are less complete. The aim of this section is to have a closer look at this case. As we will see, one can prove Minkowski's conjecture in a number of special cases when K is totally real.

8.1 Totally real fields

Let us consider the set $\mathcal{S}_e$ of all totally real abelian fields of prime conductor such that $[\mathbb{Q}(\zeta) : K] = e$, where e is an even positive integer. The Dirichlet prime number theorem implies that the set $\mathcal{S}_e$ is infinite. By Theorem 2, we have

$$\lim_{p_K \to \infty} \omega(K) = \frac{1}{2\sqrt{3}}.$$

In particular, for each e there exists $N = N(e)$ such that for every field $K \in \mathcal{S}_e$ with $p_K > N$ we have

$$\omega(K) \leq \frac{1}{2}.$$

and hence Minkowski's conjecture holds for these fields. The next result shows that we can take $N(e) = 2e^2$.

Proposition 3 *Let e be an even positive integer and $K \in \mathcal{S}_e$. If $p_K > 2e^2$, then*

$$M(K) \leq 2^{-n} \sqrt{D_K}$$

Proof We shall use the same notation as in the proofs of Theorems 1 and 2. Additionally, let

$$T = \{ (x, y) \in \mathbb{R}^2 \mid x \geq 2 \text{ and } y \geq 2x + 1 \}$$

and $h : T \to \mathbb{R}$ be a function given by

$$h(x, y) = \frac{y^2 + y + 1 - x^2}{3y^2} \cdot y^{\frac{x}{y-1}}.$$

Then we have

$$\omega(K) = C(K) \cdot p^{1/2n} = \frac{1}{2} \cdot \sqrt{h(e, p)}.$$

Thus it is enough to show that $h(e, p) \leq 1$ for $p > 2e^2$. We set

$$h_1(x, y) = \frac{y^2 + y + 1 - x^2}{3y^2}$$

$$h_2(x, y) = y^{\frac{x}{y-1}}.$$

For every $x \geq 2$ and every $y > 2(x^2 - 1)$ we have

$$\frac{\partial h_1}{\partial y}(x, y) = \frac{1}{3} \left(\frac{2(x^2 - 1)}{y^3} - \frac{1}{y^2} \right) < 0.$$

Furthermore, for every $x \geq 2$ and every $y \geq 2x + 1$ we have

$$\frac{\partial h_2}{\partial y}(x, y) = \frac{x h_2(x, y)}{(y - 1)^2} \left(\frac{y - 1}{y} - \ln y \right) < 0.$$

Consequently, for every $x \geq 2$ and every $i = 1, 2$ the function $y \mapsto h_i(x, y)$ is positive and decreasing on the interval $[2x^2, \infty)$. Hence the function $y \mapsto h(x, y)$ is decreasing on the interval $[2x^2, \infty)$. Moreover,

$$h(x, 2x^2) = (2x^2)^{\frac{x}{2x^2-1}} \cdot \frac{4x^4 + x^2 + 1}{12x^4} < (2x^2)^{\frac{1}{2x-1}} \frac{1}{2} \leq 1.$$

Consequently, $h(x, y) < 1$ for all $x \geq 2$ and $y \geq 2x^2$. The result follows. □

We can have $h(e, p) \leq 1$ even if $p < 2e^2$, which in many cases allows us to show that Minkowski's conjecture holds for every $K \in \mathcal{S}_e$.

Example 1 If $e \leq 1202$ is an even integer, then Minkowski's conjecture holds for every $K \in \mathcal{S}_e$.

Proof If $p > 2e^2$, then the result follows from Proposition 3. For $p < 2e^2$, it has been verified using Magma Computational Algebra System [5] that either $h(e, p) \leq 1$ or $n_K \leq 8$. In the first case, the result follows from the proof of Proposition 3. In the second case, it follows from the fact that Minkowski's conjecture is known to hold for fields of degree not exceeding 8.

The previous results are based on upper bounds of $\tau_{\min}(\mathcal{O}_K)$ obtained through the lattice $(\mathcal{O}_K, q)$. Another approach is to estimate $\tau_{\min}(\mathcal{O}_K)$ using a scaling factor α, giving rise to the lattice $(\mathcal{O}_K, q_\alpha)$, see Sect. 4. A computation shows that if $p < 400$, then for an appropriate $\alpha \in \mathcal{P}$ the lattice $(\mathcal{O}_K, q_\alpha)$ is isomorphic to the unit lattice. Then [2], Corollary (5.5) implies that Minkowski's conjecture holds.   □

8.2 Totally imaginary fields

If $p \equiv 3 \pmod 4$, then $K = \mathbb{Q}(\sqrt{-p}) \in \mathcal{A}$. Using formulas derived in the proof of Theorem 1, we get

$$M(K) \leq \frac{(p+1)^2}{16p}.$$

Note that this bound is known to be the exact value of the Euclidean minimum of K (see for instance Proposition 4.2 in [9]). In particular, the inequality

$$M(K) \leq 2^{-n}\sqrt{D_K}$$

does not hold in general for number fields that are not totally real. Just as in the totally real case, we have

$$M(K) \leq 3^{-2n/3}\sqrt{D_K} < 2^{-n}\sqrt{D_K} \tag{8}$$

for all totally imaginary fields $K \in \mathcal{A}$ with composite conductors. If the conductor of K is prime and $n_K > 2$, then by Theorem 1 we have

$$M(K) \leq 3^{-n}(\sqrt{D_K})^\varepsilon \tag{9}$$

with $\varepsilon < 2$. Note that given the asymptotic behavior of the expressions $\varepsilon(K)$, $C(K)$, $\omega(K)$, using the formulas derived in the proofs of Theorems 1 and 2 directly will often lead to better bounds.

References

1. Bayer-Fluckiger, E.: Ideal Lattices, proceedings of the conference Number Theory and Diophantine Geometry, (Zurich: 1999) Cambridge University Press 168–184 (2002)
2. Bayer-Fluckiger, E.: Upper bounds for Euclidean minima of algebraic number fields. J. Number Theory **121**(2), 305–323 (2006)
3. Bayer-Fluckinger, E., Nebe, G.: On the euclidean minimum of some real number fields. J. Theory Nombres Bordeaux **17**, 437–454 (2005)
4. Conway, J.H., Sloane, N.J.A.: Sphere Packings, Lattices and Groups, 3rd edn. Springer, New York (1999)
5. Bosma, W., Cannon, J.: Playoust Catherine The Magma algebra system I. The user language. J. Symbolic Comput. **24**(3–4), 235–265 (1997)
6. Hans-Gill, R.J., Raka, M., Sehmi, R.: On Conjectures of Minkowski and Woods for $n = 7$. J. Number Theory **129**, 1011–1033 (2009)
7. Hans-Gill, R.J., Raka, M., Sehmi, R.: On Conjectures of Minkowski and Woods for $n = 8$. Acta Arith. **147**, 337–385 (2011)
8. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers, 5th edn. Oxford Univ. Press, London (1979)
9. Lemmermeyer, F.: The Euclidean algorithm in algebraic number fields. Expo. Math. **13**, 385–416 (1995)
10. Leopoldt, H.-W.: Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers. J. Reine Angew. Math. **201**, 119–149 (1959)
11. Lettl, G.: The ring of integers of an abelian number field. J. Reine Angew. Math. **404**, 162–170 (1990)
12. Martinet, J.: Réseaux parfaits des espaces euclidiens, Masson (1996) English translation: Perfect lattices of Euclidean spaces, Springer-Verlag, Grundlehren der math. Wiss **327**(2003)
13. McMullen, C.T.: Minkowski's conjecture, well-rounded lattices and topological dimension. J. Am. Math. Soc. **18**, 711–734 (2005)
14. da Nóbrega Neto, T.P., Interlando, J.C., Lopes, J.O.D.: On computing discriminants of subfields of $\mathbb{Q}(\zeta_p^r)$. J. Number Theory **96**(2), 319–325 (2002)