TORAL AUTOMORPHISMS AND APPLICATIONS TO NORM-EUCLIDEAN DOMAINS AND EUCLIDEAN MINIMA

JOHN C. MILLER

Abstract. A number field modulo its ring of integers is a torus, and the units act on this torus as hyperbolic toral automorphisms. We show sufficient control over the distribution of the rational orbits to give a new, non-computational proof that $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is a norm-Euclidean number field, and an improved upper bound for the Euclidean minima of real cyclotomic fields of power of 2 conductor.

1. Introduction

The orbits of rational points of the torus under hyperbolic toral automorphisms have periodic orbits. Is it possible to pick a "nice" representative of every rational orbit? Our motivation arises from applications to norm-Euclidean domains, i.e. number fields K whose rings of integers $\mathcal{O}$ are Euclidean domains with the usual number field norm playing the role of the Euclidean function. The *Euclidean minimum* M_K of K is defined to be

$$M_K = \sup_{x \in K} \inf_{y \in \mathcal{O}} |N_{K/\mathbb{Q}}(x-y)|.$$

A number field K is norm-Euclidean if and only if $M_K < 1$. It suffices to consider only those elements of K in some fundamental domain under the additive action by the ring of integers, in other words elements in the quotient space $K/\mathcal{O}$, which is isomorphic to the rational torus $(\mathbb{Q}/\mathbb{Z})^d$, where d is the degree of K.

If u is a unit, then $|N_{K/\mathbb{Q}}(ux-y)| = |N_{K/\mathbb{Q}}(x-u^{-1}y)|$. Thus, to determine M_K it suffices to consider the set of double cosets $\mathcal{O}^\times \backslash K/\mathcal{O}$, where the action of the group of units $\mathcal{O}^\times$ is by multiplication and $\mathcal{O}$ is by addition. The mixing of multiplication and addition can bring arithmetic into play. For example, the double cosets in $\mathcal{O}^\times \backslash K/\mathcal{O}$ can be used to define Hecke characters, and counting these double cosets leads to number theoretic considerations.

Given x in K, we may think of the double coset $\mathcal{O}^\times x + \mathcal{O}$ as the orbit of x in $K/\mathcal{O}$ under the action of $\mathcal{O}^\times$. Each u in $\mathcal{O}^\times$ acts on $K/\mathcal{O}$ by a toral automorphism, which is hyperbolic if u is not a root of unity. Our goal is to choose a "nice" representative of each orbit in order to get better control over the norms $N_{K/\mathbb{Q}}(ux-y)$.

This approach will give a new proof that $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is norm-Euclidean, a result that previously had only been proven using a computer to exhaustively check thousands of cases [4]. We also prove an upper bound on the Euclidean minima of the real cyclotomic fields of power of 2 conductor, improving earlier results of Bayer-Fluckiger and Nebe [1].

Theorem 1.1. *If K is the maximal real subfield of a cyclotomic field of conductor 2^k, and $\mathcal{O}$ is its ring of integers, then its Euclidean minimum has the upper bound*

$$M_K < \sqrt{\frac{2}{e}} \frac{\sqrt{D}}{2^n},$$

2010 *Mathematics Subject Classification.* Primary 13F07, 37P35; Secondary 11H50, 11R04.

where n is the degree of K and D is its discriminant.

2. Rational orbits of toral automorphisms

Let $A \in GL(d, \mathbb{Z})$ be a d-by-d matrix with integer entries and determinant ± 1. Then the action of A on $\mathbb{R}^d$ descends to an automorphism T of the torus $\mathbb{T}^d = \mathbb{R}^d/\mathbb{Z}^d$, which we can identify with $[0,1)^d$. The points in $\mathbb{Q}^d/\mathbb{Z}^d$ are the *rational points*. The Lebesgue measure of $\mathbb{R}^d$ can be pushed forward to give a measure μ on $\mathbb{T}^d$, with $\mu(\mathbb{T}^d) = 1$.

Definition 2.1. The automorphism $T : \mathbb{T}^d \to \mathbb{T}^d$ induced by a matrix $A \in GL(d, \mathbb{Z})$ is called a *hyperbolic toral automorphism* if none of the eigenvalues $\lambda \in \mathbb{C}$ of A have $|\lambda| = 1$.

One property of hyperbolic toral automorphisms is the following:

Proposition 2.2. *Let $T : \mathbb{T}^d \to \mathbb{T}^d$ be a hyperbolic toral automorphism. If U is a measurable subset of $\mathbb{T}^d$ such that $\mu(U) < 1$, then*

$$\lim_{N\to\infty} \bigcap_{n=0}^{N} T^n(U) = 0.$$

Our goal is to choose a "small" subset S of $\mathbb{T}^d$ such that, for all rational points x, the orbit $\{T^n(x) : n \in N\}$ intersects with S. In some cases, we can proceed quite directly. Let U be a subset of the torus such that

$$\bigcap_{n\geq 0}^{N} T^{-n}(U) = \emptyset$$

for some $N \geq 1$, and let S be the complement of U. Then S intersects with every orbit.

Example 2.3. Let A be the companion matrix of the Fibonacci recurrence relation $a_n = a_{n-1} + a_{n-2}$,

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix},$$

and let T be the corresponding toral automorphism. Let U be the subset of $\mathbb{T}^2$

$$U = \left(\frac{1}{5}, \frac{4}{5}\right) \times [0,1) \subseteq \mathbb{T}^2.$$

We can calculate that

$$\bigcap_{n=0}^{5} T^{-1}(U) = \emptyset,$$

so every orbit intersects the complement of U. We can interpret this in terms of recurrent sequences.

Theorem 2.4. *Let a_0, a_1 be integers and m be a positive integer. Let $(a_0, a_1, a_2, \dots)$ be the sequence of integers given by the Fibonacci recurrence relation $a_n = a_{n-1} + a_{n-2}$ for $n > 1$. Let $(b_0, b_1, b_2, \dots)$ be the sequence in $\{0, 1, \dots, m-1\}$ such that $a_n \equiv b_n \pmod m$. Note that $(b_0, b_1, b_2, \dots)$ is a periodic sequence. Then every subsequence $(b_k, b_{k+1}, b_{k+2}, b_{k+3}, b_{k+4}, b_{k+5})$ contains a term c such that $c \leq \frac{1}{5}m$ or $c \geq \frac{4}{5}m$.*

On the other hand, for some toral automorphisms, such a direct approach is not possible.

Example 2.5. Let A be the matrix,

$$A = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix},$$

and let T be the corresponding toral automorphism. Let U be the subset of $\mathbb{T}^2$

$$U = \left(\frac{1}{4}, \frac{3}{4}\right) \times [0, 1) \subseteq \mathbb{T}^2.$$

Clearly $\begin{bmatrix} 0 \\ 1/2 \end{bmatrix}$ is a fixed point under T. But aside from the fixed point, we would like to show that every other rational orbit intersects with the complement of U. However, since clearly

$$\bigcap_{n \geq 0}^{N} T^{-n}(U)$$

is contains the fixed point, hence is never empty, we must modify our approach.

3. Convex subsets of the torus

In order to better analyze the intersection of subsets, it is useful to have a notion of a convex subset of a torus.

Definition 3.1. We will call a subset U of the torus $\mathbb{T}^d$ *toral convex* if U is simply connected (in particular path-connected) and the pre-image of U in the universal cover $\mathbb{R}^d$ is a disjoint union of convex sets.

Lemma 3.2. *Suppose B is a simply connected subset of $\mathbb{T}^d$, and $A \subseteq B$. Let $\pi : \mathbb{R}^d \to \mathbb{T}^d$ be the universal covering map. If A is path-connected and $\pi^{-1}(A)$ is a disjoint union of convex sets, then A is simply connected and therefore toral convex.*

Proof. Since B is a simply connected, $\pi^{-1}(B)$ is a disjoint union of homeomorphic copies of B. Let C be one of these copies, so the restriction of $\pi|_C : C \to B$ is a homeomorphism. Then $\pi^{-1}(A) \cap C$ is path-connected, convex and hence simply connected. Moreover, $\pi^{-1}(A) \cap C$ is homeomorphic to A, so A is simply connected and therefore toral convex. □

Proposition 3.3. *Let A and B be toral convex subsets of $\mathbb{T}^d$. Then their intersection $A \cap B$ is a (possibly empty) disjoint union of path-connected components, each of which are toral convex. In particular, the intersection $A \cap B$ is toral convex if and only if $A \cap B$ is path-connected.*

Proof. The intersection $A \cap B$ is a disjoint union of path-connected components, and its preimage in the universal cover is a disjoint union of convex sets. Let U be a component. By Lemma 3.2, U is toral convex. □

Proposition 3.4. *Let A and B be toral convex subsets of $\mathbb{T}^d$, both of which are subsets of a simply connected subset C. Then their intersection $A \cap B$ is toral convex (or empty).*

Proof. Suppose $A \cap B$ is nonempty. Let $\pi : \mathbb{R}^d \to \mathbb{T}^d$ be the universal covering map, and let D be a homeomorphic copy of C in $\pi^{-1}(C)$. Then $\pi^{-1}(A) \cap D$ and $\pi^{-1}(B) \cap D$ are convex sets, whose intersection is convex, and moreover is homeomorphic to $A \cap B$. Therefore $A \cap B$ is path-connected, hence toral convex. □

Theorem 3.5. *Suppose that T is an automorphism of $\mathbb{T}^d$. If a subset U of $\mathbb{T}^d$ is toral convex, and if the intersection $U \cap T(U)$ is path-connected, then for each integer $N \geq 0$, the intersection*

$$\bigcap_{n=0}^{N} T^n(U)$$

is toral convex or the empty set.

Proof. Assume $U \cap T(U)$ is nonempty. By induction, it suffices to prove that $U \cap T(U)$ is toral convex, and $U \cap T(U \cap T(U)) = U \cap T(U) \cap T^2(U)$ is path-connected. By Proposition 3.3, $U \cap T(U)$ is toral convex. Since $U \cap T(U) \subseteq T(U)$ and $T(U \cap T(U)) \subseteq T(U)$, and $T(U)$ is simply connected, by Proposition 3.4 $(U \cap T(U)) \cap T(U \cap T(U)) = U \cap T(U) \cap T^2(U)$ is toral convex, and in particular is path-connected. □

Now we can return to Example 2.5.

Theorem 3.6. *Let A be the matrix,*

$$A = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix},$$

and let T be the corresponding toral automorphism. Let U be the subset of $\mathbb{T}^2$

$$U = \left(\frac{1}{4}, \frac{3}{4}\right) \times [0, 1) \subseteq \mathbb{T}^2.$$

Except for the fixed point $\begin{bmatrix} 0 \\ 1/2 \end{bmatrix}$, every rational orbit intersects with the complement of U.

Proof. The eigenvalues of A are $1 \pm \sqrt{2}$, so T and T^{-1} are hyperbolic toral automorphisms. By Proposition 2.2,

$$\lim_{N \to \infty} \mu \left(\bigcap_{n=0}^{N} T^{-n}(U) \right) = 0.$$

The subset U is not toral convex (since it is not simply connected), but $U \cap T^{-1}(U)$ is toral convex, and $U \cap T^{-1}(U) \cap T^{-2}(U)$ is path-connected. Thus by Theorem 3.5,

$$\bigcap_{n=0}^{N} T^{-n}(U)$$

is a polygon that is toral convex for all $N > 0$. This puts severe restrictions on the above intersection for large N. For example, given any three points that are not collinear, for sufficiently large N the intersection can not contain all three points, since the area of the intersection (which is a convex polygon) tends to zero as $N \to \infty$.

Let L be the subset of U given by the line segment of slope $-1/\sqrt{2}$ through the fixed point $\begin{bmatrix} 0 \\ 1/2 \end{bmatrix}$, i.e.

$$L = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \in U \,\middle|\, y - \frac{1}{2} = -\frac{x}{\sqrt{2}} \right\}.$$

Since $\begin{bmatrix} 0 \\ 1/2 \end{bmatrix}$ is a fixed point of T,

$$\begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \end{bmatrix} \in \bigcap_{n=0}^{\infty} T^{-n}(U).$$

Since $\begin{bmatrix} -\sqrt{2} \\ 1 \end{bmatrix}$ is an eigenvector of the matrix A^{-1}, with eigenvalue $-1-\sqrt{2}$, which has absolute value greater than 1, we have

$$L \subseteq T^{-1}(L),$$

and therefore

$$L = \bigcap_{n=0}^{\infty} T^{-n}(L) \subseteq \bigcap_{n=0}^{\infty} T^{-n}(U).$$

Suppose p is a point of U not in L. The finite intersection $\bigcap_{n=0}^{N} T^{-n}(U)$ is a toral convex polygon whose area approaches zero as $N \to \infty$, so for sufficiently large N,

$$p \notin \bigcap_{n=0}^{N} T^{-n}(U).$$

Thus we have the reverse inclusion,

$$\bigcap_{n=0}^{\infty} T^{-n}(U) \subseteq L.$$

Therefore, we conclude that

$$\bigcap_{n=0}^{\infty} T^{-n}(U) = L.$$

Since L has irrational slope,

$$L \cap (\mathbb{Q}/\mathbb{Z})^2 = \left\{ \begin{bmatrix} 0 \\ \frac{1}{2} \end{bmatrix} \right\}.$$

Thus every rational orbit, except for the fixed point $\begin{bmatrix} 0 \\ 1/2 \end{bmatrix}$, intersects the complement of U. □

Corollary 1. *Let x be an element of $\mathbb{Q}(\sqrt{2})$, such that $x - \sqrt{2}/2 \notin \mathbb{Z}[\sqrt{2}]$. Then there exists a unit ϵ in $\mathbb{Z}[\sqrt{2}]$ such that*

$$\epsilon x + \mathbb{Z}[\sqrt{2}] = a + b\sqrt{2} + \mathbb{Z}[\sqrt{2}]$$

with $0 \leq b \leq 1/4$.

Proof. The unit $1+\sqrt{2}$ acts on $\mathbb{Q}(\sqrt{2}) = \mathbb{Q} + \mathbb{Q}\sqrt{2} \cong \mathbb{Q}^2$ as the matrix A given in Theorem 3.6. Chose n such that

$$(1+\sqrt{2})^n x + \mathbb{Z}[\sqrt{2}] = a + b\sqrt{2} + \mathbb{Z}[\sqrt{2}]$$

with $|b| \leq 1/4$. If $b \geq 0$ then put $\epsilon = (1+\sqrt{2})^n$; otherwise put $\epsilon = -(1+\sqrt{2})^n$. □

4. An application to the norm-Euclideanity of $\mathbb{Q}(\sqrt{2+\sqrt{2}})$

Let K be a number field with ring of integers $\mathcal{O}_K$. Let $N_{K/\mathbb{Q}} : K \to \mathbb{Q}$ be the usual number field norm,

$$N_{K/\mathbb{Q}}(x) = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(x).$$

To show K is norm-Euclidean, it suffices to show that, for every $x \in K$, there exists $y \in \mathcal{O}_K$ such that

$$|N_{K/\mathbb{Q}}(x-y)| < 1.$$

One method to proceed is to choose a fundamental domain $\mathcal{F}$ of K with respect to the additive action by the ring integers $\mathcal{O}_K$. This fundamental domain can be divided into many small regions $\mathcal{F} = \bigcup \mathcal{F}_i$. It may be possible to check, for each $\mathcal{F}_i$, that there exists $y \in \mathcal{O}_K$ such that, for all $x \in \mathcal{F}_i$ we have that $|N_{K/\mathbb{Q}}(x-y)| < 1$. Often a computer is required to carry out such computations, and the reader is encouraged to consult the recent work of Cerri [2] for a detailed description of such methods.

Cohn and Deutsch used such a computer-based method to prove that $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is norm-Euclidean. We give here a new "manual" proof.

Theorem 4.1. *The number field $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is norm-Euclidean.*

Proof. Let $\omega = \sqrt{2+\sqrt{2}}$. The number field $K = \mathbb{Q}(\omega)$ has a ring of integers $\mathcal{O}_K = \mathbb{Z}[\omega]$. Let $\{1, \sqrt{2}, \omega, \omega\sqrt{2}\}$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$.

Let x be an element of K, which we can write as

$$x = a + b\sqrt{2} + \omega(c + d\sqrt{2})$$

with $a, b, c, d \in \mathbb{Q}$. The norm $N_{K/\mathbb{Q}}(x)$ is

$$N_{K/\mathbb{Q}}(x) = [(a+b\sqrt{2})^2 - (2+\sqrt{2})(c+d\sqrt{2})^2][(a-b\sqrt{2})^2 - (2-\sqrt{2})(c-d\sqrt{2})^2].$$

We use the Corollary 1 to choose a unit ϵ such that

$$\epsilon(c+d\sqrt{2}) + \mathbb{Z}[\sqrt{2}] = c_2 + d_2\sqrt{2} + \mathbb{Z}[\sqrt{2}]$$

with $0 \le d_2 \le \frac{1}{4}$.

We can choose an algebraic interger $\alpha \in \mathcal{O}_K$ such that $\epsilon x - \alpha$ can be written as

$$\epsilon x - \alpha = a_3 + b_3\sqrt{2} + \omega(c_3 + d_3\sqrt{2})$$

such that:

(1) $0 \le d_3 \le \frac{1}{4}$,
(2) $|b_3| \le \frac{1}{2}$,
(3) $|a_3 - b_3\sqrt{2}| \le \frac{1}{2}$, and
(4) $-\frac{1}{2}\frac{1}{\sqrt{2-\sqrt{2}}} \le c_3 - d_3\sqrt{2} \le 1 - \frac{1}{2}\frac{1}{\sqrt{2-\sqrt{2}}}$.

Noting that $\frac{1}{2}\frac{1}{\sqrt{2-\sqrt{2}}} \approx 0.6533$, we have

$$|c_3 - d_3\sqrt{2}|^2 \le \frac{1}{4}\frac{1}{2-\sqrt{2}},$$

and so

$$|(a_3 - b_3\sqrt{2})^2 - (2-\sqrt{2})(c_3 - d_3\sqrt{2})^2| \le \frac{1}{4}.$$

Since $c_3 + d_3\sqrt{2} = c_3 - d_3\sqrt{2} + 2d_3\sqrt{2}$, we have

$$-\frac{1}{2}\frac{1}{\sqrt{2-\sqrt{2}}} \leq c_3 + d_3\sqrt{2} \leq 1 - \frac{1}{2}\frac{1}{\sqrt{2-\sqrt{2}}} + \frac{1}{2}\sqrt{2},$$

so that $|c_3 + d_3\sqrt{2}| \leq 1.0539$. Then we have

$$(2+\sqrt{2})(c_3 + d_3\sqrt{2})^2 \leq 3.7922.$$

Since also

$$|a_3 + b_3\sqrt{2}|^2 \leq (|a_3 - b_3\sqrt{2}| + |2b_3\sqrt{2}|)^2 \leq \left(\frac{1}{2} + \sqrt{2}\right)^2 \leq 3.6643,$$

we have

$$|(a_3 + b_3\sqrt{2})^2 - (2+\sqrt{2})(c_3 + d_3\sqrt{2})^2| \leq 3.7922.$$

Therefore,

$$|N(x - \epsilon^{-1}\alpha)| = |N(\epsilon x - \alpha)| \leq 3.7922\left(\frac{1}{4}\right) < 0.95,$$

proving that $K = \mathbb{Q}(\sqrt{2+\sqrt{2}})$ is a norm-Euclidean number field.

□

5. Euclidean minima of fields of real cyclotomic fields of power of 2 conductor

Let K be a totally real number field and $\mathcal{O}$ its ring of integers. Minkowski conjectured that its Euclidean minimum has the upper bound,

$$M_K \leq \frac{\sqrt{D}}{2^n}$$

where D is the discriminant and n is the degree of K. Minkowski's conjecture has been proven for totally real fields of degree $n \leq 8$ [5] and for real cyclotomic fields of prime power conductor [1].

In particular, Bayer-Fluckiger and Nebe proved the conjecture for real cyclotomic fields of power of 2 conductor, i.e. $K = \mathbb{Q}(\zeta_{2^k} + \zeta_{2^k}^{-1})$, $k \geq 0$. The discriminant of K is $2^{n-1}n^n$, so we can express their result as

$$M_K \leq \frac{1}{\sqrt{2}}\left(\frac{n}{2}\right)^{n/2}.$$

We can improve upon this result by using Corollary 1, but it is convenient to first work out the trivial upper bound for M_K.

We will need some basic results concerning K. Its degree n is 2^{k-2} and its ring of integers is $\mathcal{O} = \mathbb{Z}[\zeta_{2^k} + \zeta_{2^k}^{-1}]$. We define b_j to be

$$b_j = \zeta_{2^k}^j + \zeta_{2^k}^{-j} = 2\cos(2\pi j/2^k).$$

Then $\{1, b_1, \ldots, b_{n-1}\}$ is an integral basis for K. A fundamental domain $\mathcal{F}$ for K under the additive action of $\mathcal{O}$ is

$$\mathcal{F} = \left\{\sum_{j=0}^{n-1} a_j b_j \in K : a_j \in [0,1) \cap \mathbb{Q}\right\} \cong ([0,1) \cap \mathbb{Q})^n.$$

Let $\Phi : K \to \mathbb{R}^n$ be the usual map defined by the Galois embeddings of K

$$\Phi(x) = (\sigma_1(x), \sigma_2(x), \ldots, \sigma_n(x)).$$

Under Φ the image of our fundamental domain $\mathcal{F}$, which isomorphic to the unit cube, is *almost* a cube. In fact,

Proposition 5.1. *The image of $\mathcal{F}$ under the embedding map Φ is an n-dimensional box, with every side of length $\sqrt{2n}$, except for one side which has length $\sqrt{n}$.*

Proof. The integral basis element $1 \in K$ maps under Φ to the vector $(1, 1, \ldots, 1)$, which has length $\sqrt{n}$. The other basis elements b_j with $1 \leq j \leq n-1$ map to $(\sigma_1(x), \sigma_2(x), \ldots, \sigma_n(x))$, which has squared length

$$\sum_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(b_j)^2 = \sum_{\sigma} \sigma(b_j^2) = \sum_{\sigma} \sigma(2 + b_{2j}) = \mathrm{Tr}_{K/\mathbb{Q}}(2 + b_{2j}) = 2n.$$

It remains to show that the images of the integral basis elements $\{1, b_1, \ldots, b_{n-1}\}$, under the map Φ, are orthogonal. Indeed, for $1 \leq j \leq n-1$,

$$\sum_{\sigma} \sigma(1)\sigma(b_j) = \sum_{\sigma} \sigma(b_j) = \mathrm{Tr}_{K/\mathbb{Q}}(b_j) = 0$$

and for $1 \leq j < k \leq n-1$,

$$\sum_{\sigma} \sigma(b_j)\sigma(b_k) = \sum_{\sigma} \sigma(b_k b_j) = \sum_{\sigma} \sigma(b_{k+j} + b_{k-j}) = \mathrm{Tr}_{K/\mathbb{Q}}(b_{k+j}) + \mathrm{Tr}_{K/\mathbb{Q}}(b_{k-j}) = 0.$$

□

We can now determine a trivial upper bound for the Euclidean minimum of K. Choose x in $\mathcal{F}$. Then there exists a vertex y of $\mathcal{F}$ (so $y \in \mathcal{O}$) such that the Euclidean distance from $\Phi(x)$ to $\Phi(y)$ is less than or equal to

$$\frac{1}{2}\sqrt{n + 2n + 2n + \cdots + 2n} = \frac{\sqrt{2n^2 - n}}{2}.$$

By the arithmetic-geometric inequality,

$$|N_{K/\mathbb{Q}}(x-y)| = \prod_{\sigma} \sigma(x-y) \leq \left(\sum_{\sigma} \frac{\sigma(x-y)^2}{n} \right)^{n/2} \leq \left(\frac{2n^2 - n}{4n} \right)^{n/2} = \left(\frac{n}{2} - \frac{1}{4} \right)^{n/2}.$$

Therefore, we have the trivial bound for the Euclidean minimum

$$M_K \leq \left(\frac{n}{2} - \frac{1}{4} \right)^{n/2} < e^{-1/4} \left(\frac{n}{2} \right)^{n/2} = \frac{\sqrt{2}}{e^{1/4}} \frac{\sqrt{D}}{2^n},$$

which does not yet improve upon the results in [1]. However, we can get a better bound by using Corollary 1. Let π be the projection map,

$$\pi : K \to \mathbb{Q}(\sqrt{2}), \quad \pi\left(\sum_{j=0}^{n-1} a_j b_j \right) = a_0 b_0 + a_{n/2} b_{n/2} = a_0 + a_{n/2}\sqrt{2}$$

where $a_j \in \mathbb{Q}$.

Lemma 5.2. *If $x \in \mathbb{Q}(\sqrt{2})$ and $y \in K$, then $\pi(xy) = x\pi(y)$.*

Proof. It suffices to prove that $\pi(\sqrt{2} b_j) = 0$ for $j \neq 0, n/2$. Indeed, we have

$$\pi(\sqrt{2} b_j) = \pi(b_{n/2} b_j) = \pi(b_{n/2+j}) + \pi(b_{n/2-j}) = 0 + 0 = 0.$$

□

We can now show the improved upper bound

$$M_K < \sqrt{\frac{2}{e}}\frac{\sqrt{d(K)}}{2^n}.$$

Proof of Theorem 1.1. Let x be an element of K. Use Corollary 1 and Lemma 5.2 to choose a unit ϵ of $\mathbb{Q}(\sqrt{2})$ such that

$$\pi(\epsilon x) = \epsilon\pi(x) = a + b\sqrt{2}$$

and such that the distance of b to the nearest integer is less than or equal to $1/4$. Now choose $w \in \mathcal{O}$ such that $\epsilon x - w \in \mathcal{F}$. Then we can choose $y \in \mathcal{O}$, corresponding to a vertex of $\mathcal{F}$ such that the Euclidean distance from $\Phi(\epsilon x - w)$ to $\Phi(y)$ is less than or equal to

$$\frac{1}{2}\sqrt{n + \frac{2n}{2} + 2n + \cdots + 2n} = \frac{\sqrt{2n^2 - 2n}}{2},$$

where the factor $1/2$ savings comes from our choice of b above. By the arithmetic-geometric inequality, we have

$$M_K \leq \left(\frac{2n^2 - 2n}{4n}\right)^{n/2} \leq \left(\frac{n}{2} - \frac{1}{2}\right)^{n/2} < e^{-1/2}\left(\frac{n}{2}\right)^{n/2} = \sqrt{\frac{2}{e}}\frac{\sqrt{D}}{2^n},$$

improving upon the bound conjectured by Minkowski and proven by Bayer-Fluckiger and Nebe [1]. □

6. Concluding remarks

The *Weber class number problem* is the conjecture that all real cyclotomic fields of conductor 2^k have class number 1. One may further speculate that all these fields are norm-Euclidean. However, our only knowledge in this direction is Cerri's result [2] that $\mathbb{Q}(\zeta_{32} + \zeta_{32}^{-1})$ is norm-Euclidean. Unfortunately, the computational methods used by Cohn and Deutsche and later by Cerri run into difficulties as the degree of the field increases. It is probably within reach to prove $\mathbb{Q}(\zeta_{64} + \zeta_{64}^{-1})$ is norm-Euclidean, but $\mathbb{Q}(\zeta_{128} + \zeta_{128}^{-1})$ would pose substantial computational difficulties. This highlights the necessity of developing further theoretical resources to apply to this problem.

7. Acknowledgments

I would like to thank my advisor, Henryk Iwaniec, for introducing me to Weber's class number problem and his steadfast encouragement. I would also like to thank Doron Zeilberger; this paper originally began as a class project in his experimental mathematics course.

References

[1] E. Bayer-Fluckiger and G. Nebe, *On the Euclidean minimum of some real number fields.* J. Théor. Nombres de Bordeaux 17.2 (2005), 437–454. http://dx.doi.org/10.5802/jtnb.500

[2] J-P. Cerri, *Euclidean minima of totally real number fields: Algorithmic determination*, Math. Comp. 76, no. 259 (2007), 1547–1575. http://dx.doi.org/10.1090/S0025-5718-07-01932-1

[3] J. P. Cerri, *De l'euclidianité de* $\mathbb{Q}(\sqrt{2+\sqrt{2+\sqrt{2}}})$ *et* $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ *pour la norme*, J. Théor. Nombres Bordeaux 12 (2000), 103–126. http://dx.doi.org/10.5802/jtnb.269

[4] H. Cohn and J. Deutsch, *Use of a computer scan to prove* $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ *and* $\mathbb{Q}(\sqrt{3+\sqrt{2}})$ *are Euclidean*, Math. Comp. 46, no. 173 (1986), 295–299. http://dx.doi.org/10.1090/S0025-5718-1986-0815850-8

[5] R. J. Hans-Gill, M. Raka and R. Sehmi, *On conjectures of Minkowski and Woods for* $n = 8$, Acta Arith. 147, no. 4 (2011), 337–385. http://dx.doi.org/10.4064/aa147-4-3

Department of Mathematics, Rutgers University, Hill Center for the Mathematical Sciences, 110 Frelinghuysen Road Piscataway, NJ 08854-8019
E-mail address: jcmiller@math.rutgers.edu