1-1-2015

Stability of Ideal Lattices from Quadratic Number Fields

Lenny Fukshansky
Claremont McKenna College

STABILITY OF IDEAL LATTICES FROM QUADRATIC NUMBER FIELDS

LENNY FUKSHANSKY

Abstract. We study semi-stable ideal lattices coming from real quadratic number fields. Specifically, we demonstrate infinite families of semi-stable and unstable ideal lattices of trace type, establishing explicit conditions on the canonical basis of an ideal that ensure stability; in particular, our result implies that an ideal lattice of trace type coming from a real quadratic field is semi-stable with positive probability. We also briefly discuss the connection between stability and well-roundedness of Euclidean lattices.

1. Introduction and statement of results

Let $\Lambda \subset \mathbb{R}^n$ be a lattice of rank $n \geq 2$. For each $1 \leq i \leq n$, the i-th successive minimum of Λ is defined as

$$\lambda_i = \min\left\{\lambda \in \mathbb{R}_{>0} : \dim\left(\mathrm{span}_{\mathbb{R}}\left\{\Lambda \cap B_n(\lambda)\right\}\right) \geq i\right\},$$

where $B_n(\lambda)$ is a closed ball of radius λ centered at the origin in $\mathbb{R}^n$. Then clearly

$$\lambda_1 \leq \cdots \leq \lambda_n, \tag{1}$$

and we say that Λ is well-rounded (abbreviated WR) if there is equality throughout in (1). Two lattices Λ and Ω are said to be similar, written $\Lambda \sim \Omega$, if there exists a positive real number γ and an $n \times n$ real orthogonal matrix U such that $\Lambda = \gamma U \Omega$. It is easy to see that ratios of successive minima, and hence well-roundedness, are preserved under similarity.

On the other hand, the lattice Λ is called semi-stable if for each sublattice $\Omega \subseteq \Lambda$,

$$\det(\Lambda)^{1/\operatorname{rk}(\Lambda)} \leq \det(\Omega)^{1/\operatorname{rk}(\Omega)}. \tag{2}$$

For instance, when $\operatorname{rk}(\Lambda) = 2$ the defining inequality (2) can be restated as

$$\lambda_1 \geq \det(\Lambda)^{1/2}, \tag{3}$$

since for each sublattice $\Omega = \mathrm{span}_{\mathbb{Z}}\{\boldsymbol{z}\} \subset \Lambda$ of rank 1, $\det(\Omega) = \|\boldsymbol{z}\| \geq \lambda_1$. Semi-stability, the same as well-roundedness, is preserved under similarity. If a lattice is not semi-stable, we will say that it is unstable.

The notion of semi-stability was originally introduced by Stuhler [14] in the context of reduction theory and later used by Grayson [10] in the study of arithmetic subgroups of semi-simple algebraic groups (see also [7] for an excellent survey of Stuhler's and Grayson's work). As indicated in [1], semi-stability heuristically means that the successive minima are not far from each other (see [5] for a detailed investigation of this connection), i.e., inequality (1) is not far from equality. As a

2010 *Mathematics Subject Classification.* 11H06, 11R11, 11E16, 11H55.

Key words and phrases. semi-stable lattices, ideal lattices, quadratic number fields.

The author was partially supported by the NSA Young Investigator Grant #1210223 and a collaboration grant from the Simons Foundation (#208969 to Lenny Fukshansky).

first observation, however, we note that the converse is not true; in other words, successive minima being close to each other does not necessarily imply stability. Specifically, we prove the following lemma.

Lemma 1.1. *All WR full-rank lattices in $\mathbb{R}^2$ are semi-stable. On the other hand, for each $n \geq 3$ there exist infinitely many similarity classes of unstable WR lattices of rank n in $\mathbb{R}^n$.*

Proof. First suppose that $\Lambda \subset \mathbb{R}^2$ is WR. Then there exists a basis $\boldsymbol{x}_1, \boldsymbol{x}_2$ for Λ consisting of vectors corresponding to successive minima, i.e.

$$\lambda_1 = \|\boldsymbol{x}_1\| = \|\boldsymbol{x}_2\| = \lambda_2.$$

Let θ be the angle between these vectors, then

$$\det(\Lambda) = \|\boldsymbol{x}_1\|\|\boldsymbol{x}_2\| \sin\theta = \lambda_1^2 \sin\theta \leq \lambda_1^2.$$

and so Λ is semi-stable by (3). This shows that all WR lattices in $\mathbb{R}^2$ are semi-stable.

Next suppose $n \geq 3$ and let $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ be the standard basis vectors in $\mathbb{R}^n$. We construct a family of examples of WR lattices of rank n in $\mathbb{R}^n$, which are unstable. From our simple construction, it becomes immediately clear that many other such examples are possible. Let $\theta \in [\pi/3, \pi/2)$, and let

$$\boldsymbol{x}_\theta = \cos\theta \boldsymbol{e}_1 + \sin\theta \boldsymbol{e}_2,$$

and define

$$\Lambda_\theta = \mathrm{span}_{\mathbb{Z}} \left\{ \boldsymbol{e}_1, \boldsymbol{x}_\theta, \boldsymbol{e}_3, \dots, \boldsymbol{e}_n \right\}.$$

It is easy to see that Λ_θ is WR with

$$\lambda_1 = \cdots = \lambda_n = 1,$$

where $\boldsymbol{e}_1, \boldsymbol{x}_\theta, \boldsymbol{e}_3, \dots, \boldsymbol{e}_n$ are the vectors corresponding to successive minima. Consider a sublattice $\Omega_\theta = \mathrm{span}_{\mathbb{Z}} \{\boldsymbol{e}_1, \boldsymbol{x}_\theta\} \subset \Lambda$ of rank 2, and notice that

$$\det(\Lambda_\theta)^{1/n} = (\sin\theta)^{1/n} > (\sin\theta)^{1/2} = \det(\Omega_\theta)^{1/2},$$

since $\sqrt{3}/2 \leq \sin\theta < 1$. Hence Λ_θ is unstable, and two such lattices Λ_{θ_1} and Λ_{θ_2} are similar if and only if $\theta_1 = \theta_2$. □

Remark 1.1. A particularly important subclass of WR lattices are perfect lattices, which figure prominently as potential candidates for extremum points of the sphere packing density function on the space of lattices, as well as in other related optimization problems. Y. Kim recently showed [12] that, while all perfect lattices in dimensions ≤ 7 are semi-stable, there exists one 8-dimensional perfect lattice which is not semi-stable.

In [1], the author remarks that, while semi-stable lattices have been investigated in several arithmetic and geometric contexts, they have not yet been seriously studied in the scope of classical lattice theory. A goal of this note is to partially remedy this situation. One important construction widely used in lattice theory is that of ideal lattices coming from number fields. Ideal lattices have been extensively studied in a series of papers by Eva Bayer-Fluckiger and her co-authors in the 1990's and 2000's (see, for instance, [2], [3], [4]). Here we consider a restricted notion of ideal lattices coming from quadratic number fields, called ideal lattices of trace type. Let K be a quadratic number field, and let us write $\mathcal{O}_K$ for its ring of integers. Then $K = \mathbb{Q}(\sqrt{D})$ (real quadratic) or $K = \mathbb{Q}(\sqrt{-D})$ (imaginary quadratic), where D is a positive squarefree integer. The embeddings $\sigma_1, \sigma_2 : K \to \mathbb{C}$ can be used

to define the standard Minkowski embedding σ_K of K into $\mathbb{R}^2$: if $K = \mathbb{Q}(\sqrt{D})$, then $\sigma_K : K \to \mathbb{R}^2$ is given by $\sigma_K = (\sigma_1, \sigma_2)$; if $K = \mathbb{Q}(\sqrt{-D})$, then $\sigma_2 = \overline{\sigma_1}$, and $\sigma_K = (\Re(\sigma_1), \Im(\sigma_1))$, where $\Re$ and $\Im$ stand for real and imaginary parts, respectively. Each nonzero ideal $I \subseteq \mathcal{O}_K$ becomes a lattice of full rank in $\mathbb{R}^2$ under this embedding, which we will denote by $\Lambda_K(I) := \sigma_K(I)$. These are the ideal lattices we consider.

WR ideal lattices were studied in [9] and [8], where in particular it was shown that a positive proportion of quadratic number fields contain ideals giving rise to WR lattices. In view of Lemma 1.1, it is interesting to understand which ideal lattices coming from quadratic number fields are semi-stable. An inequality connecting successive minima of an ideal lattice and the norm of its corresponding ideal I in the ring of integers of a fixed number field K follows from Lemma 3.2 of [9]:

$$\lambda_1(\Lambda_K(I))^2 \geq (r_1 + r_2)\mathbb{N}(I)^{\frac{1}{r_1+r_2}}. \tag{4}$$

Here r_1 is the number of real embeddings and r_2 is the number of pairs of complex conjugate embeddings of K; $\mathbb{N}(I)$ stands for the norm of the ideal I in $\mathcal{O}_K$. A direct adaptation of Lemma 2 on p.115 of [13] implies that

$$\det(\Lambda_K(I)) = 2^{-r_2}|\Delta_K|^{\frac{1}{2}}\mathbb{N}(I), \tag{5}$$

where Δ_K is the discriminant of K.

In this note, we discuss the case of real quadratic fields. When K is a real quadratic number field, $r_1 = 2$ and $r_2 = 0$, and so combining (4) with (5), we only obtain

$$\lambda_1(\Lambda_K(I)) \geq \frac{\sqrt{2}}{|\Delta_K|^{1/8}} \det(\Lambda_K(I))^{1/4}.$$

Hence the situation is more complicated and requires more detailed analysis and additional notation. Let $D > 1$ be a squarefree integer and let $K = \mathbb{Q}(\sqrt{D})$. We have $\mathcal{O}_K = \mathbb{Z}[\delta]$, where

$$\delta = \begin{cases} -\sqrt{D} & \text{if } K = \mathbb{Q}(\sqrt{D}),\ D \not\equiv 1 (\mathrm{mod}\, 4) \\ \frac{1-\sqrt{D}}{2} & \text{if } K = \mathbb{Q}(\sqrt{D}),\ D \equiv 1 (\mathrm{mod}\, 4). \end{cases} \tag{6}$$

Now $I \subseteq \mathcal{O}_K$ is an ideal if and only if

$$I = I(a, b, g) := \{ax + (b + g\delta)y : x, y \in \mathbb{Z}\}, \tag{7}$$

for some $a, b, g \in \mathbb{Z}_{\geq 0}$ such that

$$b < a,\ g \mid a, b,\ \text{and } ag \mid \mathbb{N}(b + g\delta). \tag{8}$$

Such integral basis $a, b + g\delta$ is unique for each ideal I and is called the canonical basis for I (see Section 6.3 of [6] for details). In Section 4 we prove the following result.

Theorem 1.2. *Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic number field. Then there exist infinitely many ideals $I \subseteq \mathcal{O}_K$ for which the corresponding ideal lattice $\Lambda_K(I)$ is semi-stable, as well as infinitely many such ideals with the corresponding lattice unstable. Specifically, let $\gamma \in \mathbb{R}_{>0}$ and define the functions*

$$u_\gamma(b) = \begin{cases} \frac{\gamma(2b+1)}{2} & \text{if } D \equiv 1 (\mathrm{mod}\, 4) \\ \gamma b & \text{if } D \not\equiv 1 (\mathrm{mod}\, 4), \end{cases}$$

$$v(b) = \begin{cases} \frac{(2b+1)^2+D}{2\sqrt{D}} & \text{if } D \equiv 1 (\mathrm{mod}\, 4) \\ \frac{b^2+D}{\sqrt{D}} & \text{if } D \not\equiv 1 (\mathrm{mod}\, 4), \end{cases}$$

$$h(b) = \begin{cases} \frac{(2b+1)^2-D}{2} & \text{if } D \equiv 1 (\mathrm{mod}\, 4) \\ b^2 - D & \text{if } D \not\equiv 1 (\mathrm{mod}\, 4). \end{cases}$$

Then there exists an absolute constant $\gamma > 1$ such that if

$$u_\gamma(b) \leq a \leq v(b), \tag{9}$$

then the lattice $\Lambda_K(I(a,b,g))$ is semi-stable for every triple a, b, g satisfying (8). *On the other hand, if*

$$v(b) < a \leq h(b), \tag{10}$$

then the lattice $\Lambda_K(I(a,b,g))$ is unstable for every triple a, b, g satisfying (8).

In fact, Remark 4.1 below shows that the probability of an arbitrary ideal lattice $\Lambda_{\mathbb{Q}(\sqrt{D})}(I(a,b,g))$ being semi-stable is positive (specifically, the probability is at least $1/\gamma$ as $b \to \infty$).

In Section 2 we prove a technical lemma on distribution of divisors of integers of the form $x^2 - D$, which is useful to us later in our main argument. In Section 3 we establish Proposition 3.1, which is the core of our argument. Finally, we use this proposition in Section 4 to prove Theorem 1.2. We are now ready to proceed.

2. A divisor lemma

In this section we make an observation on the finiteness of the set of integers of the form $x^2 \pm D$ which have divisors in small intervals around their square root. This result is later used in the proof of Theorem 1.2. The proof of this lemma was suggested to me by Florian Luca.

Lemma 2.1. *Let $|D| > 1$ be a squarefree integer and $0 < \varepsilon < 1/2$ a real number. Then the set*

$$\left\{ x \in \mathbb{Z}_{>0} : \exists\ b \mid x^2 - D \text{ such that } x < b \leq x + x^{1/2-\varepsilon} \right\}$$

is finite.

Proof. Since there are only finitely many positive integers less than any fixed constant, we can assume without loss of generality that

$$x > \max\left\{ |D|, 2^{1/\varepsilon} \right\}.$$

Let us write $x^2 - D = bd$, where $b \in (x, x + x^{1/2-\varepsilon}]$, then $d \in [x - x^{1/2-\varepsilon}, x)$. Notice that $b = d + a$, where $a \in [0, 2x^{1/2-\varepsilon}]$. Therefore

$$x^2 - D = d(d+a) = d^2 + 2d\frac{a}{2} + \left(\frac{a}{2}\right)^2 - \left(\frac{a}{2}\right)^2 = \left(d + \frac{a}{2}\right)^2 - \left(\frac{a}{2}\right)^2,$$

and therefore

$$(2x)^2 = (2d+a)^2 + (4D - a^2),$$

meaning that

$$(2x - (2d+a))(2x + (2d+a)) = 4D - a^2.$$

Taking absolute values, we see that the left hand side cannot be equal to zero; since $|D| > 1$, the assumption that $4D - a^2 = 0$ would imply that $D = (a/2)^2 > 1$,

which would contradict D being squarefree. Since $2x-(2d+a)$ is an integer, $|2x-(2d+a)|\geq 1$, which means that

$$|(2x-(2d+a))(2x+(2d+a))|\geq 2x+(2d+a)>2x.$$

On the other hand,

$$|4D-a^2|\leq 4|D|+a^2<4|D|+4x^{1-2\varepsilon},$$

and so we have

$$2x<4x^{1-2\varepsilon}+4|D|.$$

Therefore, since $x>2^{1/\varepsilon}$,

$$x<2x(1-2x^{-2\varepsilon})<4|D|,$$

meaning that there are at most $4|D|$ such integers x. □

3. Lemmas on stability of some planar lattices

Our goal here is to develop a collection of lemmas that will allow us to treat ideal lattices coming from any real quadratic number field simultaneously. Throughout this section, let $D>1$ be fixed a squarefree integer. For each pair of integers (a,b) such that

$$0<b<a,\ a\mid b^2-D, \tag{11}$$

define the lattice

$$\Lambda(a,b)=\begin{pmatrix} a & b-\sqrt{D}\\ a & b+\sqrt{D}\end{pmatrix}\mathbb{Z}^2. \tag{12}$$

We want to understand for which pairs (a,b) satisfying (11) the corresponding lattice $\Lambda(a,b)$ is semi-stable. Let

$$S(D)=\left\{(a,b)\in\mathbb{Z}^2:(a,b)\text{ satisfies (11)}\right\}.$$

We prove the following result.

Proposition 3.1. *For infinitely many pairs $(a,b)\in S(D)$, the corresponding lattice $\Lambda(a,b)$ is semi-stable, and for infinitely many pairs it is unstable. Specifically, there exists an absolute constant $\gamma>1$ such that if*

$$\gamma b\leq a\leq\frac{b^2+D}{\sqrt{D}}, \tag{13}$$

then the lattice $\Lambda(a,b)$ is semi-stable. On the other hand, if

$$\frac{b^2+D}{\sqrt{D}}<a\leq b^2-D, \tag{14}$$

then the lattice $\Lambda(a,b)$ is unstable.

To establish Proposition 3.1, notice that for each $(a,b)\in S(D)$, $\det(\Lambda(a,b))=2a\sqrt{D}$, and so $\Lambda(a,b)$ is semi-stable if and only if

$$\lambda_1(\Lambda(a,b))^2\geq 2a\sqrt{D}.$$

The norm form of $\Lambda(a,b)$ corresponding to the choice of basis as in (12) is

$$Q(x,y)=Q_{(a,b)}(x,y):=2(xa+yb)^2+2y^2D,$$

then

$$\lambda_1^2 = \min\left\{Q(x,y) : (x,y) \in \mathbb{Z}^2 \setminus \{(0,0)\}\right\}.$$

Let $(\alpha,\beta) \in \mathbb{Z}^2$ be a point at which this minimum is achieved, i.e.,

$$Q(\alpha,\beta) = 2\min\left\{(xa+yb)^2 + y^2 D : (x,y) \in \mathbb{Z}^2 \setminus \{(0,0)\}\right\},$$

then $\gcd(\alpha,\beta) = 1$, and semi-stability is equivalent to the inequality

$$Q(\alpha,\beta) \geq 2a\sqrt{D}. \tag{15}$$

Lemma 3.2. *(α,β), the minimum of $Q(x,y)$ falls into one of the following three categories:*

(I) $(\alpha,\beta) = (1,0)$,
(II) $(\alpha,\beta) = (0,1)$,
(III) $0 < \alpha \leq b,\ \alpha \leq |\beta| \leq a,\ \beta < 0$.

Proof. Assume (I) and (II) do not hold, which means that $\alpha\beta \neq 0$. Then $\alpha\beta < 0$, since otherwise

$$Q(\alpha,\beta) \geq 2(a+b)^2 + 2D > 2(b^2+D) = Q(0,1).$$

Hence we can assume without loss of generality that $\beta < 0$, since $Q(\alpha,\beta) = Q(-\alpha,-\beta)$. If $|\beta| > a$, then

$$Q(\alpha,\beta) > 2a^2 D > 2a^2 = Q(1,0).$$

Now consider

$$f(\alpha) = Q(\alpha,\beta) = 2(\alpha a - |\beta| b)^2 + 2\beta^2 D$$

as a function of α. Notice that it is increasing when $\alpha > |\beta| b/a$. Since $|\beta| \leq a$, $\alpha > |\beta| b/a$ when $\alpha > b$, meaning that $Q(\alpha,\beta)$ cannot achieve its minimum for such values of α. Finally, assume that $\alpha > |\beta|$ and recall that $a > b$. Then

$$Q(\alpha,\beta) = 2(\alpha a - |\beta| b)^2 + 2\beta^2 D \geq 2(2a-b)^2 + 2D = 8(a^2 - ab) + 2(b^2+D) > Q(0,1).$$

Hence we established that the inequalities (III) hold, which proves the lemma. □

Let us define three sets of pairs $(a,b) \in S(D)$, corresponding to each of the three cases above:

$$S_1 = S_1(D) := \{(a,b) \in S(D) : (\alpha,\beta) \text{ is as in (I)}\},$$

$$S_2 = S_2(D) := \{(a,b) \in S(D) : (\alpha,\beta) \text{ is as in (II)}\},$$

$$S_3 = S_3(D) := \{(a,b) \in S(D) : (\alpha,\beta) \text{ is as in (III)}\}.$$

We can write $a = C(b^2 - D)$ for some $C \in \mathbb{R}_{>0}$, $b/(b^2-D) < C \leq 1$. Then $\Lambda(a,b)$ is semi-stable if and only if $Q(\alpha,\beta) \geq 2C(b^2-D)\sqrt{D}$, which is equivalent to

$$C\left(\alpha^2 C(b^2-D) + 2\alpha\beta b - \sqrt{D}\right) \geq -\frac{\beta^2(b^2+D)}{b^2-D}. \tag{16}$$

The right hand side of (16) is always non-positive and $C > 0$.

Lemma 3.3. *The set S_1 is finite, and the lattice $\Lambda(a,b)$ is semi-stable for every pair $(a,b) \in S_1$ with $b > \sqrt{D}$.*

Proof. Let $(a,b) \in S_1$ with $b > \sqrt{D}$, then $\beta = 0$, $\alpha = 1$ and (16) holds for all values of C. Hence the lattice $\Lambda(a,b)$ is semi-stable.

Now we show that S_1 is finite. Notice that for each $(a,b) \in S_1$,

$$\frac{1}{2}Q(1,0) = C^2(b^2-D)^2 \leq \frac{1}{2}Q(0,1) = b^2 + D,$$

and so $C \leq \frac{\sqrt{b^2+D}}{b^2-D}$, which means that

$$b < a \leq \sqrt{b^2+D} < b + \sqrt{D}.$$

Therefore b is an integer such that $b^2 - D$ has a divisor $a \in (b, b+\sqrt{D})$, and clearly $\sqrt{D} < b^{1/2-\varepsilon}$ for any $\varepsilon > 0$ for all but finitely many b. There are only finitely many such integers b by Lemma 2.1, and so the set of such pairs (a,b) is finite, since a is bounded by $\sqrt{b^2+D}$. □

Lemma 3.4. *Let $(a,b) \in S_2$ and $a = C(b^2-D)$ as above. Then $\Lambda(a,b)$ is semi-stable if and only if $C \leq \frac{b^2+D}{(b^2-D)\sqrt{D}}$.*

Proof. Suppose $\alpha = 0$, then $\beta = 1$, then (16) holds if and only if

$$C \leq \frac{b^2+D}{(b^2-D)\sqrt{D}}. \tag{17}$$

□

Lemma 3.5. *Let $(a,b) \in S_3$ and $a = C(b^2-D)$ as above. There exists an absolute real constant $\gamma > 1$ such that if $C \geq \frac{\gamma b}{b^2-D}$, then $\Lambda(a,b)$ is semi-stable.*

Proof. If the set S_3 is finite, there is nothing to prove, so assume it is infinite. Let

$$S_3' = \{b \in \mathbb{Z}_{>0} : \exists\ a \in \mathbb{Z}_{>0} \text{ such that } (a,b) \in S_3\}.$$

In the asymptotic argument below, when we consider b getting large or tending to infinity, we always mean that b stays in S_3' and $a = C(b^2-D)$ is such that $(a,b) \in S_3$.

For each $(a,b) \in S_3$, the corresponding $\alpha, \beta \neq 0$ are such that $\beta < 0 < \alpha \leq |\beta|$. The inequality (16) certainly holds when

$$\alpha^2 C(b^2-D) + 2\alpha\beta b - \sqrt{D} \geq 0, \tag{18}$$

which is true whenever

$$C \geq \frac{2\alpha|\beta|b + \sqrt{D}}{\alpha^2(b^2-D)} = \left(\frac{|\beta|}{\alpha}\right)\left(\frac{2b}{b^2-D}\right) + \frac{\sqrt{D}}{\alpha^2(b^2-D)}. \tag{19}$$

Claim 1. *There exists an absolute constant ρ so that $1 \leq \frac{|\beta|}{\alpha} \leq \rho$ for all $(a,b) \in S_3$.*

Proof. Suppose not, then there exists some monotone increasing unbounded real-valued function $f(b)$ such that

$$\liminf_{b\to\infty} \frac{|\beta|}{\alpha f(b)} = 1. \tag{20}$$

Hence we can assume that there exists an infinite subsequence of positive integers b for which $\beta \sim -\alpha f(b)$ as $b \to \infty$. Then for all sufficiently large b,

$$\begin{aligned} & \frac{1}{2}\min\left\{Q(x,y) : (x,y) \in \mathbb{Z}^2 \setminus (0,0)\right\} \\ = \ & \frac{1}{2}Q(\alpha,\beta) \sim \left(\alpha C(b^2-D) - \alpha b f(b)\right)^2 + \alpha^2 f(b)^2 D \\ = \ & \alpha^2 f(b)^2 \left(b^2 \left(\frac{C(b^2-D)}{bf(b)} - 1 \right)^2 + D \right) > b^2 + D = \frac{1}{2}Q(0,1), \end{aligned} \tag{21}$$

unless $\frac{C(b^2-D)}{bf(b)} \to 1$ as $b \to \infty$. Suppose this is the case, then

$$\frac{C(b^2-D)}{bf(b)} = \left(\frac{|\beta|}{\alpha f(b)}\right)\frac{\alpha C(b^2-D)}{|\beta| b} \to 1,$$

and since $|\beta|/\alpha f(b) \to 1$ and $a = C(b^2-D)$, we have $\frac{a}{b} \times \frac{\alpha}{|\beta|} \to 1$ as $b \to \infty$. Since a, b, α, β are integers, we must have

$$\frac{a}{b} = \frac{|\beta|}{\alpha} \tag{22}$$

for all sufficiently large b. Since α and β are relatively prime, we must have $\alpha = b/d$, $\beta = -a/d$, where $d = \gcd(a,b) \mid D$ by (11). Then

$$\frac{1}{2}Q(\alpha,\beta) = \frac{a^2 D}{d^2} \leq b^2 + D = \frac{1}{2}Q(0,1),$$

and so

$$\frac{a}{b} \leq d\sqrt{\frac{1}{D} + \frac{1}{b^2}} < d\sqrt{2} \leq D\sqrt{2}. \tag{23}$$

Now (23) combined with (22) implies that $|\beta|/\alpha \leq D\sqrt{2}$. This completes the proof. □

Thus we conclude that $|\beta|/\alpha \leq \rho$ for all $b \in S_3'$. Then (19) implies that for all $b \in S_3'$, if

$$C \geq \frac{2\rho b}{b^2 - D} + \frac{\sqrt{D}}{\alpha^2(b^2-D)}, \tag{24}$$

then the lattice $\Lambda(a,b)$ is semi-stable. In other words, there exists some real constant $\gamma > \rho \geq 1$ such that whenever $a = C(b^2-D)$ for $C \in [\gamma b/(b^2-D), 1]$ so that $(a,b) \in S_3$, the lattice $\Lambda(a,b)$ is semi-stable. □

Proof of Proposition 3.1. Let γ be the constant as in the statement of Lemma 3.5. First, let $(a,b) \in S(D)$ as above with $b > \sqrt{D}$, and assume that (13) is satisfied. Notice that (a,b) is either in S_1, S_2, or S_3. Then the result follows by combining Lemmas 3.3, 3.4, and 3.5.

Next, assume that (14) holds, then

$$\det(\Lambda(a,b)) = 2a\sqrt{D} > 2(b^2+D) = Q(0,1) \geq \lambda_1(\Lambda(a,b))^2,$$

and so $\Lambda(a,b)$ is unstable.

To construct an infinite family of pairs $(a,b) \in S(D)$ giving rise to unstable lattices, simply take $a = b^2 - D$ for each integer $b > \sqrt{\frac{D+D\sqrt{D}}{\sqrt{D}-1}}$; the resulting lattice is unstable since (14) is satisfied.

On the other hand, for each $m \in \mathbb{Z}_{>0}$ let $b = mD$ and take $a = \frac{b^2-D}{D} = m^2D - 1$. Let γ be the constant as in the statement of Lemma 3.5. For each $m \geq \frac{\gamma D+\sqrt{\gamma^2D^2+4D}}{2D}$, the inequality (13) is satisfied, and hence the resulting lattice is semi-stable by the argument above. □

Remark 3.1. In the argument above, we constructed a family of unstable lattices $\Lambda(a,b)$ with a large comparing to b. On the other hand, there also exist unstable lattices $\Lambda(a,b)$ with a close to b. For instance, let $D = 13$ and consider the pair $(a,b) = (276, 259) \in S(D)$. Then

$$\lambda_1^2 \leq Q_{(a,b)}(1,-1) = 604 < 2a\sqrt{D} = 552\sqrt{13} = \det(\Lambda(a,b)),$$

and so the lattice $\Lambda(276, 259)$ is unstable.

4. The case of real quadratic number fields

In this section we prove Theorem 1.2. Let $D > 1$ be a squarefree integer, $K = \mathbb{Q}(\sqrt{D})$, integers $a, b, g \geq 0$ satisfying (8), and the ideal $I = I(a,b,g) \subseteq \mathcal{O}_K$ as in (7). Then

$$\Lambda_K(I) = \begin{pmatrix} a & b - g\sqrt{D} \\ a & b + g\sqrt{D} \end{pmatrix} \mathbb{Z}^2, \tag{25}$$

if $D \not\equiv 1 (\mathrm{mod}\, 4)$, and

$$\Lambda_K(I) = \begin{pmatrix} a & \frac{2b+g}{2} - \frac{g\sqrt{D}}{2} \\ a & \frac{2b+g}{2} + \frac{g\sqrt{D}}{2} \end{pmatrix} \mathbb{Z}^2, \tag{26}$$

if $D \equiv 1 (\mathrm{mod}\, 4)$. Notice that $I = gI'$, where I' has canonical basis $\frac{a}{g}, \frac{b}{g} + \delta$ and $\Lambda_K(I) \sim \Lambda_K(I')$. Hence we can assume without loss of generality that $g = 1$.

First assume that $D \not\equiv 1 (\mathrm{mod}\, 4)$, then

$$I = \{ax + (b - \sqrt{D})y : x, y \in \mathbb{Z}\} \subseteq \mathcal{O}_K.$$

Here the pair (a,b) satisfies the conditions of (11) and $\Lambda_K(I) = \Lambda(a,b)$. The statement of Theorem 1.2 in this case readily follows from Proposition 3.1.

Now assume that $D \equiv 1 (\mathrm{mod}\, 4)$, then

$$I = \left\{ ax + \left(\frac{2b + 1 - \sqrt{D}}{2} \right) y : x, y \in \mathbb{Z} \right\} \subseteq \mathcal{O}_K,$$

where

$$b < a,\ a \mid \frac{1}{4}\left((2b+1)^2 - D\right), \tag{27}$$

and

$$\Lambda_K(I) = \begin{pmatrix} a & \frac{2b+1}{2} - \frac{\sqrt{D}}{2} \\ a & \frac{2b+1}{2} + \frac{\sqrt{D}}{2} \end{pmatrix} \mathbb{Z}^2. \tag{28}$$

Let $a_1 = 2a$, $b_1 = 2b+1$, and notice that the pair (a_1, b_1) satisfies the conditions of (11) and $\Lambda_K(I) = \frac{1}{2}\Lambda(a_1, b_1)$. Observe that $\Lambda_K(I)$ is semi-stable if and only if $\Lambda(a_1, b_1)$ is semi-stable, and hence the statement of Theorem 1.2 in this case again follows from Proposition 3.1.

Remark 4.1. In fact, Theorem 1.2 implies that an arbitrary ideal lattice $\Lambda_{\mathbb{Q}(\sqrt{D})}(I)$ is semi-stable with positive probability.

Indeed, for $x > 0$ let

$$M(D,x) = \{q \in \mathbb{Z}_{>0} : q < x, D \text{ is a quadratic residue} \bmod q\}, \tag{29}$$

then $q < x$ is in $M(D,x)$ if and only if D is a quadratic residue modulo every prime dividing q. Professor Gang Yu pointed out to me that an argument essentially identical to the proof of the main result of [11] shows that there exists a positive real constant $C(D)$ such that

$$|M(D,x)| \sim C(D)\left(\frac{x}{\sqrt{\log x}}\right) \tag{30}$$

as $x \to \infty$ (the set $M(D,x)$ can also be compared to the set $S(x) = M(-1,x)$ in the definition of Landau-Ramanujan constant [15], where the same classical asymptotic emerges). Then (30) implies that for $0 < k_1 < k_2 < 1$,

$$|M(D,x) \cap [k_1 x, k_2 x]| \sim C(D)(k_2 - k_1)\left(\frac{x}{\sqrt{\log x}}\right),$$

and so

$$\lim_{x\to\infty} \frac{|M(D,x) \cap [k_1 x, k_2 x]|}{|M(D,x)|} = k_2 - k_1,$$

which means that elements of $M(D,x)$ are equidistributed in subintervals of $[1,x]$. In other words, as $x \to \infty$, every subinterval $[k_1 x, k_2 x]$ with $0 < k_1 < k_2 < 1$ will contain a $(k_2 - k_1)$-proportion of integers q such that D is quadratic residue modulo q. This implies that probability of such a modulus q to be in the interval $[k_1 x, k_2 x]$ tends to $k_2 - k_1$ as $x \to \infty$.

Now let $K = \mathbb{Q}(\sqrt{D})$, let $I = I(a,b,1) \subseteq \mathcal{O}_K$ be an ideal, and let

$$a_1 = \begin{cases} a & \text{if } D \not\equiv 1 (\bmod 4) \\ 2a & \text{if } D \equiv 1 (\bmod 4), \end{cases}$$

and

$$b_1 = \begin{cases} b & \text{if } D \not\equiv 1 (\bmod 4) \\ 2b+1 & \text{if } D \equiv 1 (\bmod 4). \end{cases}$$

Then $a_1 \mid b_1^2 - D$ and $b_1 < a_1 \leq b_1^2 - D$. Let $d_1 = (b_1^2 - D)/a_1$, so $d_1 \mid b_1^2 - D$ and $1 \leq d_1 < b_1$. Theorem 1.2 implies that if

$$\sqrt{D}\left(\frac{b_1^2 - D}{b_1^2 + D}\right) \leq d_1 \leq \frac{1}{\gamma} b_1 - \frac{D}{\gamma b_1}, \tag{31}$$

then the lattice $\Lambda_K(I)$ is semi-stable. In other words, (31) implies that for each $\varepsilon > 0$ there exists $B \in \mathbb{R}_{>0}$ such that for all $b_1 > B$, if

$$d_1 \in \left[\frac{\sqrt{D}}{b_1} b_1, \frac{1}{\gamma} b_1 - \varepsilon\right], \tag{32}$$

then $\Lambda_K(I)$ is semi-stable. Since $d_1 \in M(D, b_1)$, our argument above suggests that the probability of (32) holding tends to $\frac{1}{\gamma}$ as $b_1 \to \infty$.

Acknowledgment. I would like to thank Professor Florian Luca for suggesting the proof of Lemma 2.1, as indicated above. I also thank Professors Gang Yu and David Speyer, whose comments were instrumental to the formulation of Remark 4.1. Finally, I thank the referee for many useful suggestions which improved the quality of the paper.

References

[1] Y. André. On nef and semistable hermitian lattices, and their behaviour under tensor product. *Tohoku Math. J. (2)*, 63(4):629–649, 2011.
[2] E. Bayer-Fluckiger. Lattices and number fields. Contemp. Math. 241, pages 69–84, 1999.
[3] E. Bayer-Fluckiger. Ideal lattices. In *A panorama of number theory or the view from Baker's garden (Zurich, 1999)*, pages 168–184. Cambridge Univ. Press, Cambridge, 2002.
[4] E. Bayer-Fluckiger and G. Nebe. On the Euclidean minimum of some real number fields. *J. Théor. Nombres Bordeaux*, 17(2):437454, 2005.
[5] T. Borek. Successive minima and slopes of Hermitian vector bundles over number fields. *J. Number Theory*, 113(2):380–388, 2005.
[6] D. A. Buell. *Binary Quadratic Forms*. Springer-Verlag, 1989.
[7] B. Casselman. Stability of lattices and the partition of arithmetic quotients. *Asian J. Math.*, 8(4):607–637, 2004.
[8] L. Fukshansky, G. Henshaw, P. Liao, M. Prince, X. Sun, and S. Whitehead. On well-rounded ideal lattices, II. *Int. J. Number Theory*, 9(1):139–154, 2013.
[9] L. Fukshansky and K. Petersen. On ideal well-rounded lattices. *Int. J. Number Theory*, 8(1):189–206, 2012.
[10] D. R. Grayson. Reduction theory using semistability. *Comment. Math. Helv.*, 59(4):600–634, 1984.
[11] R. D. James. The distribution of integers represented by quadratic forms. *Amer. J. Math.*, 60(3):737–744, 1938.
[12] Y. Kim. On semistability of root lattices and perfect lattices. *preprint, Univ. Illinois*, 2009.
[13] S. Lang. *Algebraic Number Theory*. Springer-Verlag, 1994.
[14] U. Stuhler. Eine Bemerkung zur Reduktionstheorie quadratischer Formen. *Arch. Math. (Basel)*, 27(6):604–610, 1976.
[15] E. W. Weisstein. Landau-Ramanujan constant. From MathWorld – a Wolfram web resource. `http://mathworld.wolfram.com/Landau-RamanujanConstant.html`.

Department of Mathematics, 850 Columbia Avenue, Claremont McKenna College, Claremont, CA 91711
E-mail address: `lenny@cmc.edu`