ON INTEGRAL WELL-ROUNDED LATTICES IN THE PLANE

LENNY FUKSHANSKY, GLENN HENSHAW, PHILIP LIAO, MATTHEW PRINCE, XUN SUN, AND SAMUEL WHITEHEAD

Abstract. We investigate distribution of integral well-rounded lattices in the plane, producing a complete parameterization of the set of their similarity classes by solutions of the family of Pell-type Diophantine equations of the form $x^2 + Dy^2 = z^2$ where $D > 0$ is squarefree. We then apply our results to the study of the greatest minimal norm and the highest signal-to-noise ratio on the set of such lattices with fixed determinant, also estimating cardinality of these sets (up to rotation and reflection) for each determinant value. This investigation extends previous work of the first author in the specific cases of integer and hexagonal lattices and is motivated by the importance of integral well-rounded lattices for discrete optimization problems. We separately study a special subclass of integral well-rounded lattices which come from ideals in quadratic number fields, generalizing some recent results of the first author with K. Petersen. In particular, we give a characterization of ideal well-rounded lattices in the plane and show that a positive proportion of real and imaginary quadratic number fields contains ideals giving rise to well-rounded lattices.

1. Introduction and statement of results

Let $N \geq 1$ be an integer, and let $\Lambda \subset \mathbb{R}^N$ be a lattice of full rank. Given a basis $\boldsymbol{a}_1, \dots, \boldsymbol{a}_N$ for Λ we can write $A = (\boldsymbol{a}_1 \dots \boldsymbol{a}_N)$ for the corresponding basis matrix, and then $\Lambda = A\mathbb{Z}^N$. The corresponding norm form is defined as

$$Q_A(\boldsymbol{x}) = \boldsymbol{x}^t A^t A \boldsymbol{x},$$

and we say that the lattice is *integral* if the coefficient matrix $A^t A$ of this quadratic form has integer entries; it is easy to see that this definition does not depend on the choice of a basis. Integral lattices are central objects in arithmetic theory of quadratic forms and in lattice theory. We define $\det(\Lambda)$ to be $|\det(A)|$, again independent of the basis choice, and (squared) *minimum* or *minimal norm*

$$|\Lambda| = \min\{\|\boldsymbol{x}\|^2 : \boldsymbol{x} \in \Lambda \setminus \{\boldsymbol{0}\}\} = \min\{Q_A(\boldsymbol{y}) : \boldsymbol{y} \in \mathbb{Z}^N \setminus \{\boldsymbol{0}\}\},$$

where $\| \ \|$ stands for the usual Euclidean norm. Then each $\boldsymbol{x} \in \Lambda$ such that $\|\boldsymbol{x}\|^2 = |\Lambda|$ is called a *minimal vector*, and the set of minimal vectors of Λ is denoted by $S(\Lambda)$. A lattice Λ is called *well-rounded* (abbreviated WR) if the set $S(\Lambda)$ contains N linearly independent vectors. These vectors do not necessarily form a basis for lattices in any dimension N, however they are known to form a

---

2010 *Mathematics Subject Classification.* 11H06, 11H55, 11D09, 11R11, 11E45.

Key words and phrases. integral lattices, well-rounded lattices, ideal lattices, binary and ternary quadratic forms, Epstein zeta function.

The authors were supported by a grant from the Fletcher Jones Foundation. The first author was also partially supported by a grant from the Simons Foundation (#208969 to Lenny Fukshansky).

basis for all $N \leq 4$; we will refer to such a basis as a *minimal basis* for Λ. WR lattices are important in discrete optimization, in particular in the investigation of sphere packing, sphere covering, and kissing number problems (see [14]), as well as in coding theory (see [1]). Properties of WR lattices have also been investigated in [15] in connection with Minkowski's conjecture and in [9] in connection with the linear Diophantine problem of Frobenius. A particularly interesting and important class of WR lattices are the integral well-rounded lattices (abbreviated IWR). The main objective of the current paper is to study the distribution properties of IWR lattices in the plane with a view toward discrete optimization problems. This extends the previous investigations of WR sublattices of $\mathbb{Z}^2$ [4], [5] and of the planar hexagonal lattice [7], as well as the study of WR lattices coming from ideals in quadratic number fields [8].

An important equivalence relation on lattices is geometric similarity: two lattices $\Lambda_1, \Lambda_2 \subset \mathbb{R}^N$ are called *similar*, denoted $\Lambda_1 \sim \Lambda_2$, if there exists a positive real number α and an $N \times N$ real orthogonal matrix U such that $\Lambda_2 = \alpha U \Lambda_1$. It is easy to see that similar lattices have the same algebraic structure, i.e., for every sublattice Γ_1 of a fixed index in Λ_1 there is a sublattice Γ_2 of the same index in Λ_2 so that $\Gamma_1 \sim \Gamma_2$. Most geometric and optimization properties of lattices (such as packing density, covering thickness, kissing number, signal-to-noise ratio, etc.) are invariant on similarity classes. Moreover, a WR lattice can only be similar to another WR lattice, so it makes sense to speak of WR similarity classes of lattices. If $\Lambda \subset \mathbb{R}^2$ is a full rank WR lattice, then its set of minimal vectors $S(\Lambda)$ contains 4 or 6 vectors, and this number is 6 if and only if Λ is similar to the hexagonal lattice

$$\mathcal{H} := \begin{pmatrix} 2 & 1 \\ 0 & \sqrt{3} \end{pmatrix} \mathbb{Z}^2$$

(see, for instance Lemma 2.1 of [8]). Any two linearly independent vectors $\boldsymbol{x}, \boldsymbol{y} \in S(\Lambda)$ form a minimal basis. While this choice is not unique, it is always possible to select $\boldsymbol{x}, \boldsymbol{y}$ so that the angle θ between these two vectors lies in the interval $[\pi/3, \pi/2]$, and any value of the angle in this interval is possible. From now on when we talk about a minimal basis for a WR lattice in the plane, we will always mean such a choice. Then the angle between minimal basis vectors is an invariant of the lattice, and we call it the *angle of the lattice* Λ, denoted $\theta(\Lambda)$; in other words, if $\boldsymbol{x}, \boldsymbol{y}$ is any minimal basis for Λ and θ is the angle between $\boldsymbol{x}$ and $\boldsymbol{y}$, then $\theta = \theta(\Lambda)$ (see [6] for details and proofs of the basic properties of WR lattices in $\mathbb{R}^2$). In fact, it is easy to notice that two WR lattices $\Lambda_1, \Lambda_2 \subset \mathbb{R}^2$ are similar if and only if $\theta(\Lambda_1) = \theta(\Lambda_2)$ (see [6] for a proof). Therefore the set of all similarity classes of WR lattices in $\mathbb{R}^2$ is bijectively parameterized by the set of all possible values of the angle, which is the interval $[\pi/3, \pi/2]$. On the other hand, this parameterization becomes less trivial if we talk about similarity classes of planar IWR lattices. In other words, one may wonder what are the possible values of $\theta(\Lambda)$ in the interval $[\pi/3, \pi/2]$ if Λ is IWR? Our first result answers this question in detail.

Theorem 1.1. *Let $\Lambda \subset \mathbb{R}^2$ be an IWR lattice, then*

$$\cos\theta(\Lambda) = \frac{p}{q}, \ \sin\theta(\Lambda) = \frac{r\sqrt{D}}{q} \tag{1}$$

for some $p, r, q, D \in \mathbb{Z}_{>0}$ such that

$$p^2 + Dr^2 = q^2, \ \gcd(p,q) = 1, \ \frac{p}{q} \leq \frac{1}{2}, \ \text{and } D \text{ squarefree}, \tag{2}$$

and so Λ is similar to

$$\Omega_D(p,q) := \begin{pmatrix} q & p \\ 0 & r\sqrt{D} \end{pmatrix} \mathbb{Z}^2. \tag{3}$$

Moreover, for every p,r,q,D satisfying (2), $\Omega_D(p,q)$ is an IWR lattice with the angle $\theta(\Omega_D(p,q))$ satisfying (1), and $\Omega_D(p,q) \sim \Omega_{D'}(p',q')$ if and only if $(p,r,q,D) = (p',r',q',D')$. In addition, if Λ is any IWR lattice similar to $\Omega_D(p,q)$, then

$$|\Lambda| \geq \left| \frac{1}{\sqrt{q}} \Omega_D(p,q) \right|, \tag{4}$$

where the lattice $\frac{1}{\sqrt{q}}\Omega_D(p,q)$ is also IWR. Due to this property, we call $\frac{1}{\sqrt{q}}\Omega_D(p,q)$ a minimal IWR lattice in its similarity class.

Remark 1.1. Notice in particular that the integer lattice $\mathbb{Z}^2 = \Omega_1(1,1)$ and the hexagonal lattice $\mathcal{H} = \Omega_3(1,2)$.

Hence we see that the set of similarity classes of planar IWR lattices is in bijective correspondence with the set of 4-tuples (p,r,q,D) satisfying (2). It is therefore natural to ask for an explicit parameterization of this set of 4-tuples.

Lemma 1.2. *Let D be a positive squarefree integer and $m,n \in \mathbb{Z}$ with $\gcd(m,n) = 1$ and $\sqrt{\frac{D}{3}} \leq \frac{m}{n} \leq \sqrt{3D}$. Now $p,r,q,D \in \mathbb{Z}_{>0}$ satisfies (2) if and only if*

$$p = \frac{|m^2 - Dn^2|}{2^e \gcd(m,D)},\ r = \frac{2mn}{2^e \gcd(m,D)},\ q = \frac{m^2 + Dn^2}{2^e \gcd(m,D)}, \tag{5}$$

where

$$e = \begin{cases} 0 & \text{if either } 2 \mid D, \text{ or } 2 \mid (D+1), mn \\ 1 & \text{otherwise.} \end{cases} \tag{6}$$

Our next result suggests an even closer connection between integral solutions to the equation $p^2 + r^2 D = q^2$ and IWR lattices, justifying the following definition: we say that an IWR planar lattice Λ is of *type D* for a squarefree $D \in \mathbb{Z}_{>0}$ if it is similar to some $\Omega_D(p,q)$ as in (3). Theorem 1.1 implies that the type is uniquely defined, i.e., Λ cannot be of two different types.

Theorem 1.3. *A planar IWR lattice Λ is of type D for some squarefree $D \in \mathbb{Z}_{>0}$ if and only if all of its IWR finite index sublattices are also of type D. If this is the case, Λ contains a sublattice similar to $\Omega_D(p,q)$ for every 4-tuple (p,r,q,D) as in (2).*

Remark 1.2. In fact, the set of similarity classes of IWR lattices of a fixed type can be endowed with a semigroup structure, coming from the geometric group law on rational points of a Pell conic. We include a brief discussion of this fact in Lemma 2.1 below.

Hence the set of planar IWR lattices is split into types which are indexed by positive squarefree integers with similarity classes inside of each type D being in bijective correspondence with solutions to the ternary Diophantine equation $p^2 + r^2 D = q^2$ as parameterized in Lemma 1.2. We prove the parameterization results of Theorems 1.1, 1.3, and Lemma 1.2 in Section 2.

In Section 3 we use these results to study certain optimization problems on the set of planar IWR lattices with fixed determinant, such as maximizing the minimal norm and signal-to-noise ratio. These problems are analogous to the questions considered in [2] on the set of fixed index sublattices of the hexagonal lattice and in [7] on the set of fixed index WR sublattices of the hexagonal lattice. Given a lattice $\Lambda \in \mathbb{R}^N$, we can regard its nonzero points as transmitters which interfere with the transmitter at the origin, and then a standard measure of the *total interference* of Λ is given by $E_\Lambda(2)$, where

$$E_\Lambda(s) = \sum_{\boldsymbol{x} \in \Lambda \setminus \{\boldsymbol{0}\}} \frac{1}{\|\boldsymbol{x}\|^{2s}} \tag{7}$$

is the Epstein zeta-function of Λ, and the signal-to-noise ratio of Λ is defined by

$$\mathrm{SNR}(\Lambda) = 10 \log_{10} \frac{1}{9E_\Lambda(2)}, \tag{8}$$

as in [2]. To maximize $\mathrm{SNR}(\Lambda)$ on the set of all planar IWR lattices of a fixed determinant Δ is the same as to minimize $E_\Lambda(2)$ on this set. In fact, $E_\Lambda(s)$ for each real $s \geq 3$ is maximized by the same planar WR lattice of fixed determinant Δ that maximizes $|\Lambda|$, and vice versa (this follows from an old result of S. S. Ryskov [18]; see Lemma 3.2 below). Moreover, Lemma 3.3 and Remark 3.1 below suggest that it may likely be so for $s = 2$ as well. This is not always so for non-WR lattices, as demonstrated in [2]. We discuss these optimization problems in further detail in Section 3, proving in particular the following result.

Theorem 1.4. *A positive real number Δ is a determinant value of IWR lattices if and only if $\Delta = M\sqrt{D}$ where $M, D \in \mathbb{Z}_{>0}$ with D squarefree so that the set*

$$\mathrm{mn}(M) = \left\{ (m,n) \in \mathbb{Z}^2_{>0} : \gcd(m,n) = 1, \sqrt{\frac{D}{3}} \leq \frac{m}{n} \leq \sqrt{3D}, \frac{2mn}{2^e \gcd(m,D)} \;\Big|\; M \right\} \tag{9}$$

where e is as in (6)*, is not empty. Fix such a Δ, and let $(m,n) \in \mathrm{mn}(M)$ be the pair that maximizes the expression*

$$\frac{m}{n} + D\frac{n}{m}$$

on $\mathrm{mn}(M)$*. Now define p, r, q as in* (5) *for this choice of m, n and let $k = M/r$. Then*

$$\Lambda = \sqrt{\frac{k}{q}}\; \Omega_D(p,q) \tag{10}$$

is an IWR lattice with $\det(\Lambda) = \Delta$ *and* $|\Lambda| = kq$ *which maximizes* $|\Lambda|$ *among all planar IWR lattices with determinant Δ. This lattice can be found in a finite number of steps for each fixed Δ.*

Remark 1.3. Some examples of such norm-maximizing lattices are presented in Table 1 below.

In fact, the set of all planar IWR lattices, up to rotation and reflection, with a fixed determinant is always finite, as we show in Lemma 3.1. Moreover, in Lemma 3.4 we present an estimate on cardinality of such a set depending on the value of the determinant.

Finally, in Section 4 we discuss IWR lattices coming from ideals in rings of integers of quadratic number fields, called *ideal lattices*. In particular, we exhibit infinite families of similarity classes of planar IWR lattices that contain such ideal lattices. These results build upon and extend the work on quadratic ideal lattices done in [7]. We call an ideal I in the ring of integers $\mathcal{O}_K$ of a quadratic number field $K = \mathbb{Q}(\sqrt{\pm D})$ well-rounded (WR) if the planar lattice $\sigma_K(I) \subseteq \mathbb{R}^2$ is IWR, where $\sigma_K : K \to \mathbb{R}^2$ is the standard embedding of K into the Euclidean space. We will say that D satisfies the *ν-nearsquare condition* if D is a positive odd squarefree integer which has a divisor d with $\sqrt{\frac{D}{\nu}} \leq d < \sqrt{D}$, where $\nu > 1$ is a real number. We prove the following theorem (all the notation is reviewed in Section 4).

Theorem 1.5. *If D satisfies the 3-nearsquare condition, then the rings of integers $\mathcal{O}_K$ of both quadratic number fields $K = \mathbb{Q}(\sqrt{\pm D})$ contain WR ideals; the statement becomes if and only if when $K = \mathbb{Q}(\sqrt{-D})$. This in particular implies that a positive proportion (more than $1/5$) of real and imaginary quadratic number fields contain WR ideals, more specifically*

$$\liminf_{N\to\infty} \frac{\left|\left\{K = \mathbb{Q}(\sqrt{\pm D}) : K \text{ contains a WR ideal}, 0 < D \leq N\right\}\right|}{\left|\left\{K = \mathbb{Q}(\sqrt{\pm D}) : 0 < D \leq N\right\}\right|} \geq \frac{\sqrt{3}-1}{2\sqrt{3}}. \tag{11}$$

Moreover, for every D satisfying the 3-nearsquare condition each imaginary quadratic number field $K = \mathbb{Q}(\sqrt{-D})$ contains only finitely many WR ideals, up to similarity of the corresponding lattices, and this number is

$$\ll \min\left\{2^{\omega(D)-1}, \frac{2^{\omega(D)}}{\sqrt{\omega(D)}}\right\}, \tag{12}$$

where $\omega(D)$ is the number of prime divisors of D and the constant in the Vinogradov notation $\ll$ does not depend on D.

In Section 4 below, we demonstrate explicit constructions of such ideals, in particular specifying infinite families of similarity classes of planar IWR lattices containing ideal lattices. In addition, we further discuss the case of real quadratic fields, as well as certain criteria for quadratic number fields to contain WR principal ideals at the end of Section 4.

We are now ready to proceed.

2. Parameterization of planar IWR similarity classes

In this section we prove Theorems 1.1, 1.3, and Lemma 1.2.

Proof of Theorem 1.1. Let $\Lambda = A\mathbb{Z}^2$ be a planar IWR lattice, where

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is a minimal basis matrix for Λ. Then the corresponding norm form has integral coefficient matrix

$$A^t A = \begin{pmatrix} a^2+c^2 & ab+cd \\ ab+cd & b^2+d^2 \end{pmatrix}.$$

Define

$$p = \frac{ab+cd}{\gcd(ab+cd, a^2+c^2)},\ q = \frac{a^2+c^2}{\gcd(ab+cd, a^2+c^2)},$$

then $\gcd(p,q)=1$ and $\cos\theta(\Lambda)=p/q\in\mathbb{Q}$, and so $p/q\le 1/2$. Hence

$$\sin\theta(\Lambda)=\frac{\sqrt{q^2-p^2}}{q}=\frac{r\sqrt{D}}{q},$$

where D is squarefree and $p^2+r^2D=q^2$. On the other hand, the lattice $\Omega_D(p,q)$ as defined in (3) also satisfies the equation $\cos\theta(\Omega_D(p,q))=p/q$, which means that $\Lambda\sim\Omega_D(p,q)$.

Now suppose (p,r,q,D) and (p',r',q',D') are two 4-tuples satisfying (2), and suppose that $\Omega_D(p,q)\sim\Omega_{D'}(p',q')$. It is easy to see that in this case $(p,r,q,D)=(p',r',q',D')$. Indeed, we must have

$$p/q=p'/q',\ r\sqrt{D}/q=r'\sqrt{D'}/q',$$

which implies right away that $D=D'$ and $(p,r,q)=(p',r',q')$, since

$$\gcd(p,q)=\gcd(r,q)=\gcd(p',q')=\gcd(r',q')=1.$$

Finally, we establish minimality of

$$\frac{1}{\sqrt{q}}\Omega_D(p,q)=\begin{pmatrix}\sqrt{q} & \frac{p}{\sqrt{q}}\\ 0 & \frac{r\sqrt{D}}{\sqrt{q}}\end{pmatrix}\mathbb{Z}^2 \tag{13}$$

among the IWR lattices in its similarity class. First of all notice that this lattice is itself integral, since the norm form corresponding to the minimal basis matrix as in (13) is $\begin{pmatrix}q & p\\ p & q\end{pmatrix}$, which has integer entries. Now suppose $\Lambda\sim\Omega_D(p,q)$ is an IWR lattice with minimal basis matrix A, then

$$A=\alpha U\begin{pmatrix}\sqrt{q} & \frac{p}{\sqrt{q}}\\ 0 & \frac{r\sqrt{D}}{\sqrt{q}}\end{pmatrix},$$

where $\alpha\in\mathbb{R}_{>0}$ and U is a 2×2 real orthogonal matrix. The corresponding norm form therefore has integral coefficient matrix

$$A^tA=\alpha^2\begin{pmatrix}q & p\\ p & q\end{pmatrix},$$

and so α^2 must be a rational number whose denominator must divide p and q, which are relatively prime, and hence $\alpha^2\in\mathbb{Z}$. This means that $\alpha^2\ge 1$, and so $\alpha\ge 1$. Therefore

$$|\Lambda|=\alpha^2q\ge q=\left|\frac{1}{\sqrt{q}}\Omega_D(p,q)\right|,$$

which completes the proof of the theorem. □

Proof of Lemma 1.2. We start by applying Lemma 2.1 of [7] to the equation $p^2+Dr^2=q^2$ for a fixed squarefree D: since $(p,r,q)=(1,0,1)$ is an integral solution of this equation with $q\neq 0$, the lemma guarantees that all positive integral solutions of this equation with $q\neq 0$ are rational multiples of

$$p_0=|m^2-Dn^2|,\ r_0=2mn,\ q_0=m^2+Dn^2, \tag{14}$$

where m,n range over all relatively prime non-negative integers, not both 0. In order for (p,r,q,D) to satisfy (2), we need two more conditions: $\gcd(p,q)=1$ and $p/q\le 1/2$. First consider p_0,r_0,q_0 as in (14) and notice that the fact that $p_0^2+Dr_0^2=q_0^2$ implies that $\gcd(p_0,q_0)=\gcd(r_0,q_0)=\gcd(p_0,r_0,q_0)$. Since $\gcd(m,n)=1$, it is easy to notice that $\gcd(p_0,q_0)=2^e\gcd(m,D)$, where e is as in (6). Hence if we define p, r, q as in (5), we ensure that they are relatively prime, and this covers all the relatively prime solutions of our equation for each fixed D. Finally, we need to select only the solutions with $p/q \leq 1/2$, which means that

$$-1/2 \leq \frac{m^2 - Dn^2}{m^2 + Dn^2} \leq 1/2,$$

and so we must have

$$\sqrt{\frac{D}{3}} \leq \frac{m}{n} \leq \sqrt{3D}. \tag{15}$$

This completes the proof of the theorem. □

Proof of Theorem 1.3. First suppose that Λ has type D, then it is similar to some $\Omega_D(p,q)$. It is therefore sufficient to show that every IWR finite index sublattice of $\Omega_D(p,q)$ has type D. Let $\Gamma \subseteq \Omega_D(p,q)$ be such a sublattice, then $\Gamma = A\mathbb{Z}^2$, where

$$A = \begin{pmatrix} q & p \\ 0 & r\sqrt{D} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is a minimal basis matrix for Γ and $a, b, c, d \in \mathbb{Z}$. It is then easy to see that

$$\cos\theta(\Gamma) = \frac{p'}{q'} \leq \frac{1}{2},\ \sin\theta(\Gamma) = \frac{r'\sqrt{D}}{q'}$$

where

$$p' = (ab + cd)q + (ad + bc)p,\ r' = (ad - bc)r,\ q' = (a^2 + c^2)q + 2acp.$$

Let $p_1 = p'/\gcd(p', r', q')$, $r_1 = r'/\gcd(p', r', q')$, $q_1 = q'/\gcd(p', r', q')$, then Γ is similar to $\Omega_D(p_1, q_1)$, and hence is of type D.

Now let $\Gamma \subseteq \Lambda$ be an IWR sublattice of finite index which is of type D. We want to show that Λ must also be of type D. It is a well-known fact that there exists a positive integer k such that $k\Lambda$ is a sublattice of Γ, and of course $\Lambda \sim k\Lambda$. By the argument above, all IWR sublattices of Γ must be of type D, which means that $k\Lambda$ (and hence Λ) is of type D.

Finally, suppose that Λ is of type D, then it is similar to some $\Omega_D(p,q)$. Let (p'', r'', q'', D) be a 4-tuple as in (2) different from (p, r, q, D), then $\Omega_D(p'', q'') \neq \Omega_D(p,q)$ is another lattice of type D. We want to show that Λ contains a sublattice similar to $\Omega_D(p'', q'')$. In fact, by similarity, it is sufficient to show that $\Omega_D(p,q)$ contains such a sublattice. Define

$$\Gamma_D(p, q, p'', q'') = \begin{pmatrix} q & p \\ 0 & r\sqrt{D} \end{pmatrix} \begin{pmatrix} rq'' & rp'' - r''p \\ 0 & r''q \end{pmatrix} \mathbb{Z}^2 = rq \begin{pmatrix} q'' & p'' \\ 0 & r''\sqrt{D} \end{pmatrix} \mathbb{Z}^2.$$

Then $\Gamma_D(p, q, p'', q'')$ is a sublattice of $\Omega_D(p,q)$ which is similar to $\Omega_D(p'', q'')$. This completes the proof. □

Lemma 2.1. *Let $D > 0$ be squarefree and let $\mathcal{C}(D)$ be the set of similarity classes of all IWR lattices of type D. Let us write $C_D(p,q)$ for each such class, i.e., for each (p,q) satisfying* (2),

$$C_D(p,q) = \{\Lambda : \Lambda \sim \Omega_D(p,q)\}, \tag{16}$$

and so

$$\mathcal{C}(D) = \{C_D(p,q) : (p,q) \text{ satisfy } (2)\}.$$

Then the set $\mathcal{C}(D)$ has the structure of an abelian semigroup, induced by the composition law on rational points of the Pell conic corresponding to D.

Proof. A Pell conic is a curve given by the equation $x^2 - Dy^2 = 1$. The following commutative composition law on the set of rational points on a Pell conic is defined in [13]:

$$(x_1, y_1) + (x_2, y_2) = (x_1x_2 + Dy_1y_2, x_1y_2 + x_2y_1). \tag{17}$$

In [13], this operation is also described geometrically by analogy with addition on an elliptic curve. Notice that a rational point $(x, y) = (q/p, r/p)$ is on this curve if and only if

$$p^2 + r^2D = q^2. \tag{18}$$

Then (17) induces the following commutative composition law on the set of solutions (p, r, q) of (18):

$$(p_1, r_1, q_1) + (p_2, r_2, q_2) = \frac{1}{g}(p_1p_2, r_1q_2 + r_2q_1, q_1q_2 + Dr_1r_2), \tag{19}$$

where $g = \gcd(p_1p_2, r_1q_2 + r_2q_1, q_1q_2 + Dr_1r_2)$. It is easy to check that the set of solutions of (18) is closed under this operation. Moreover, since $D > 0$,

$$\frac{q_1q_2 + Dr_1r_2}{p_1p_2} \geq \frac{q_1}{p_1} \times \frac{q_2}{p_2},$$

and so whenever $p_1/q_1, p_2/q_2 \leq 1/2$, we will have

$$\frac{p_1p_2}{q_1q_2 + Dr_1r_2} \leq \frac{1}{4}.$$

This ensures that $\mathcal{C}(D)$ is closed under this operation, and hence has a structure of an abelian semigroup, although not a monoid: the point $(1, 0, 1)$, which serves as identity, is not in $\mathcal{C}(D)$. □

3. Optimization properties and counting estimates

In this section we consider certain optimization problems on sets of planar IWR lattices with fixed determinants, prove Theorem 1.4, and give estimates on the size of such sets. First we observe that such sets are in fact finite up to rotation and reflection.

Lemma 3.1. *For $\Delta \in \mathbb{R}_{>0}$, define* $\mathrm{IWR}(\Delta)$ *to be the set of all planar IWR lattices, up to rotation and reflection, with determinant* $= \Delta$. *Then the set* $\mathrm{IWR}(\Delta)$ *is finite for any* Δ.

Proof. Let Λ be a planar IWR lattice, then Theorem 1.1 implies that

$$\Lambda = \alpha \frac{1}{\sqrt{q}} U \Omega_D(p, q) \tag{20}$$

for some (p, r, q, D) as in (2), $\alpha \geq 1$, and a 2×2 real orthogonal matrix U. If $\Lambda \in \mathrm{IWR}(\Delta)$, then

$$\det(\Lambda) = \alpha^2 r \sqrt{D} = \Delta,$$

which means that fixing Δ automatically implies fixing the type D, and hence also fixes $\Delta/\sqrt{D}$. Let

$$A = \frac{\alpha}{\sqrt{q}} U \begin{pmatrix} q & p \\ 0 & r\sqrt{D} \end{pmatrix} \tag{21}$$

be a basis matrix for Λ, then the corresponding norm form has coefficient matrix

$$A^tA = \alpha^2 \begin{pmatrix} q & p \\ p & q \end{pmatrix},$$

which must have integer entries. Since $\gcd(p,q) = 1$, this implies that $\alpha^2 \in \mathbb{Z}_{>0}$, write $k = \alpha^2$. Then $kr = \Delta/\sqrt{D}$ is fixed, meaning that there are only finitely many options for r. Also, since $p/q \leq 1/2$,

$$q^2 = p^2 + r^2 D \leq \frac{q^2}{4} + r^2 D, \tag{22}$$

and hence $q \leq 2r\sqrt{D}/\sqrt{3}$. Therefore for each fixed choice of r, there are only finitely many choices for q, and p is determined uniquely once r, q are fixed. Hence there are only finitely many different $\Omega_D(p,q)$ so that $\det(\Lambda) = \Delta$ for some Λ as in (20). Since each fixed choice of r determines k uniquely, this completes the proof. □

Now suppose that $\Delta = M\sqrt{D}$, $M \in \mathbb{Z}_{>0}$, is fixed and let $\Lambda \in \mathrm{IWR}(\Delta)$ be given as in (20) with $\alpha = \sqrt{k}$ for some $k \in \mathbb{Z}_{>0}$ so that $kr = M$. Then

$$|\Lambda| = kq = \frac{Mq}{r}, \tag{23}$$

and so to maximize $|\Lambda|$ on $\mathrm{IWR}(\Delta)$ we need to maximize q/r. A trivial upper bound for $|\Lambda|$ is given by $\frac{2\Delta}{\sqrt{3}}$: this is just a restatement of the fact that $\Delta = |\Lambda| \sin\theta(\Lambda)$ and $\theta \in [\pi/3, \pi/2]$.

We next discuss a connection between the the problems of maximizing $|\Lambda|$ and minimizing $E_\Lambda(s)$ on sets of WR lattices of fixed determinant in $\mathbb{R}^2$. This discussion is an adaptation and correction of Lemma 5.2 of [7].

Lemma 3.2. *Let Δ be a positive real number, and let $\mathrm{WR}_2(\Delta)$ be the set of all full rank WR lattices in $\mathbb{R}^2$ with determinant Δ. Then for any fixed real number $s \geq 3$, $E_\Lambda(s)$ is a decreasing function of $|\Lambda|$ on $\mathrm{WR}_2(\Delta)$.*

Proof. Let $Q_\Lambda(x,y)$ be the quadratic form of Λ corresponding to a minimal basis A as in (21), then

$$Q_\Lambda(x,y) = |\Lambda|(x^2 + y^2 + 2xy\cos\theta), \tag{24}$$

where $\theta = \theta(\Lambda) \in [\pi/3, \pi/2]$ and $|\Lambda|$ is as in (23). Now

$$\cos\theta = \frac{\sqrt{|\Lambda|^2 - \Delta^2}}{|\Lambda|} = \sqrt{1 - \frac{\Delta^2}{|\Lambda|^2}}, \tag{25}$$

and $0 \leq \cos\theta \leq 1/2$. Lemma 1 of [18] guarantees that $E_\Lambda(s)$ is a decreasing function of $\cos\theta$ for any real $s \geq 3$, and (25) implies that $\cos\theta$ is an increasing function of $|\Lambda|$. Hence $E_\Lambda(s)$ is a decreasing function of $|\Lambda|$ on $\mathrm{WR}_2(\Delta)$ for $s \geq 3$. □

In fact, it seems likely that the statement of Lemma 3.2 should hold for smaller real values of s as well. At the very least, we have the following bounds.

Lemma 3.3. *With notation as in Lemma 3.2, let $s > 1$ be real. Then there exist real constants $C_1(s)$ and $C_2(s)$, dependent only on s, such that*

$$\frac{C_1(s)}{|\Lambda|^s} \leq E_\Lambda(s) \leq \frac{C_2(s)}{|\Lambda|^s}, \tag{26}$$

for every $\Lambda \in \mathrm{WR}_2(\Delta)$.

Proof. Combining (24) and (25), we obtain

$$Q_\Lambda(x,y) = Tx^2 + Ty^2 + 2xy\sqrt{T^2-\Delta^2},$$

where $T = |\Lambda|$. The Epstein zeta-function of Λ is then given by

$$E_\Lambda(s) = \sum_{x,y\in\mathbb{Z}\setminus\{0\}} Q_\Lambda(x,y)^{-s} = \sum_{x,y\in\mathbb{Z}\setminus\{0\}} \frac{1}{\left(Tx^2+Ty^2+2xy\sqrt{T^2-\Delta^2}\right)^s}$$

$$= \sum_{x,y\in\mathbb{Z}_{>0}} \left(\frac{2}{\left(Tx^2+Ty^2+2xy\sqrt{T^2-\Delta^2}\right)^s} + \frac{2}{\left(Tx^2+Ty^2-2xy\sqrt{T^2-\Delta^2}\right)^s} \right).$$

Now recall that since $\theta \in [\pi/3, \pi/2]$, we must have $\frac{\sqrt{3}T}{2} \leq \Delta \leq T$, and so $0 \leq \sqrt{T^2-\Delta^2} \leq T/2$. Hence for each fixed real $s > 1$, we have

$$E_\Lambda(s) \leq \frac{2}{T^s} \sum_{x,y\in\mathbb{Z}_{>0}} \left(\frac{1}{(x^2+y^2)^s} + \frac{1}{(x^2+y^2-xy)^s} \right), \tag{27}$$

and

$$E_\Lambda(s) \geq \frac{2}{T^s} \sum_{x,y\in\mathbb{Z}_{>0}} \left(\frac{1}{(x^2+y^2)^s} + \frac{1}{(x^2+y^2+xy)^s} \right). \tag{28}$$

Since both series in the bounds of (27) and (28) converge, we have (26). □

Remark 3.1. Since WR lattice Λ with fixed $|\Lambda|$ and $\det(\Lambda)$ is unique up to multiplication by an orthogonal matrix U (which does not change the value of $E_\Lambda(s)$ for any s), Lemmas 3.2 and 3.3 make it natural to expect that the total interference of Λ is minimized on $\mathrm{WR}_2(\Delta)$ (and so $\mathrm{SNR}(\Lambda)$ is maximized) if and only if $|\Lambda|$ is maximized.

Proof of Theorem 1.4. We will now discuss a finite procedure to maximize q/r, and hence $|\Lambda|$, on the set $\mathrm{IWR}(\Delta)$ using finiteness of this set along with Lemma 1.2. First we notice that r has to be a divisor of $M = \Delta/\sqrt{D}$, hence we can start by going through the list of all possible divisors of M. For each such divisor r, consider all possible decompositions

$$r = \frac{2mn}{2^e \gcd(m,D)}$$

with relatively prime m,n so that $m/n \in \left[\sqrt{D/3}, \sqrt{3D}\right]$, as in (5). Out of all such decompositions, we want to pick one which maximizes the ratio

$$q/r = \frac{m^2+Dn^2}{2mn} = \frac{1}{2}\left(\frac{m}{n} + D\frac{n}{m}\right).$$

This can be done in a finite number of steps, since there are finitely many values for r, a divisor of M, and for each r there are finitely many such m,n. Hence we can choose Λ maximizing $|\Lambda|$ and $\mathrm{SNR}(\Lambda)$ on $\mathrm{IWR}(\Delta)$ to be as in (10). In particular, our argument confirms that Δ is a determinant value of an IWR lattice if and only if it is of the form $M\sqrt{D}$ with the set $\mathrm{mn}(M)$ as in (9) nonempty. This completes the proof. □

Remark 3.2. Let us write $m/n = \sqrt{D}x$ for appropriate $x \in \left[1/\sqrt{3}, \sqrt{3}\right]$. Then

$$q/r = \frac{\sqrt{D}}{2}(x + 1/x).$$

Now the function $f(x) = x + 1/x$ assumes its maximal values on the interval $\left[1/\sqrt{3}, \sqrt{3}\right]$ at the endpoints and has a minimum at $x = 1$. Hence, to maximize q/r one should consider m, n with m/n close to the endpoints of the interval $\left[\sqrt{D/3}, \sqrt{3D}\right]$. Keeping these considerations in mind can reduce the number of computational steps necessary to find maximizer for $|\Lambda|$ in $\mathrm{IWR}(\Delta)$ in each particular case.

We give some computational examples in Table 1 below.

Table 1. Examples of IWR lattices Λ with $\det(\Lambda) = \Delta$ that maximize $|\Lambda|$ on $\mathrm{IWR}(\Delta)$

Δ	$\|\Lambda\|$	Λ
$24\sqrt{5}$	61	$\sqrt{\frac{1}{61}}\Omega_5(29, 61)$
$24\sqrt{7}$	69	$\sqrt{\frac{3}{23}}\Omega_7(9, 23)$
$20\sqrt{11}$	75	$\sqrt{\frac{1}{3}}\Omega_{11}(7, 15)$
$24\sqrt{13}$	98	$\sqrt{\frac{2}{49}}\Omega_{13}(7, 15)$
$24\sqrt{17}$	104	$\sqrt{\frac{8}{13}}\Omega_{17}(4, 13)$
$105\sqrt{19}$	510	$\sqrt{\frac{15}{34}}\Omega_{19}(15, 34)$
$96\sqrt{23}$	522	$\sqrt{\frac{6}{87}}\Omega_{23}(41, 87)$

We will next discuss some estimates on the size of the set $\mathrm{IWR}(\Delta)$ for a fixed value of Δ. The first observation, which is an immediate consequence of Theorem 1.4, is that $\mathrm{IWR}(\Delta)$ is empty unless $\Delta = M\sqrt{D}$ with the set $\mathrm{mn}(M)$ as in (9) nonempty. For the purposes of the following lemma we assume that M satisfies this condition, so that $\mathrm{IWR}(\Delta)$ is nonempty.

Lemma 3.4. *The cardinality of the set* $\mathrm{IWR}(\Delta)$ *satisfies*

$$|\mathrm{IWR}(\Delta)| \leq \frac{1}{2} \sum_{r|M} 2^{\omega(rD)}. \tag{29}$$

Moreover,

$$|\mathrm{IWR}(\Delta)| \ll \sum_{r|M} \sum_{g|r} \mu\left(\frac{r}{g}\right) \frac{\tau(g^2 D)}{\sqrt{\omega(gD)}}, \tag{30}$$

where $\tau(u)$ is the number of divisors, $\omega(u)$ is the number of prime divisors, and $\mu(u)$ is the Möbius function of an integer u. The constant in the Vinogradov notation $\ll$ does not depend on Δ.

Proof. Let $\Delta = M\sqrt{D}$ as above so that $\mathrm{mn}(M)$ as in (9) is nonempty. Suppose $\Lambda \in \mathrm{IWR}(\Delta)$, then we can assume without loss of generality that

$$\Lambda = \sqrt{\frac{k}{q}}\ \Omega_D(p, q),$$

where $k = M/r$ and p, r, q are as in (5) for some $(m, n) \in \mathrm{mn}(M)$. Hence the choice of p, r, q determines Λ uniquely. For each $r \mid M$ define

$$f(r) = \left| \left\{ (p,q) \in \mathbb{Z}^2_{>0} : q^2 - p^2 = r^2 D,\ \gcd(p,q) = 1,\ 0 < \frac{p}{q} \leq \frac{1}{2} \right\} \right|, \tag{31}$$

then

$$|\mathrm{IWR}(\Delta)| = \sum_{r \mid M} f(r).$$

Hence we want to produce estimates on $f(r)$. Define

$$f_1(r) = \left| \left\{ (p,q) \in \mathbb{Z}^2_{>0} : q^2 - p^2 = r^2 D,\ \gcd(p,q) = 1 \right\} \right|,$$

and

$$f_2(r) = \left| \left\{ (p,q) \in \mathbb{Z}^2_{>0} : q^2 - p^2 = r^2 D,\ 0 < \frac{p}{q} \leq \frac{1}{2} \right\} \right|, \tag{32}$$

and notice that

$$f(r) \leq \min\{f_1(r), f_2(r)\}, \tag{33}$$

meaning that

$$|\mathrm{IWR}(\Delta)| \leq \sum_{r \mid M} \min\{f_1(r), f_2(r)\}. \tag{34}$$

The function $f_1(r)$ is well-studied; in particular, the following formula follows from Theorem 6.2.4 of [16]:

$$f_1(r) = \begin{cases} 2^{\omega(r^2 D) - 1} & \text{if } 2 \nmid r^2 D,\ r^2 D > 1 \\ 2^{\omega(r^2 D) - 1} & \text{if } 8 \mid r^2 D,\ r^2 D \text{ has odd prime divisors} \\ 1 & \text{if } r^2 D \text{ is a power of } 2 \\ 0 & \text{otherwise,} \end{cases} \tag{35}$$

hence $f_1(r) \leq 2^{\omega(r^2 D) - 1} = 2^{\omega(rD) - 1}$. Now (29) follows upon combining (34), (35).

Next we estimate $f_2(r)$. Let $c = r^2 D$, and let us write

$$a = q - p,\ b = q + p, \tag{36}$$

then $q = (a+b)/2$, $p = (b-a)/2$, and $ab = c$. Let $\alpha := p/q$, and assume that $0 < \alpha \leq 1/2$. Then let $\nu = \frac{1+\alpha}{1-\alpha}$, and observe that

$$1 < \nu = \frac{b}{a} \leq 3.$$

Since $ab = c$, we have $b = \sqrt{\nu c}$, and so

$$\sqrt{c} < b \leq \sqrt{3c}.$$

Therefore

$$f_2(r) = \left| \left\{ b \in \mathbb{Z}_{>0} : b \mid c,\ \sqrt{c} < b \leq \sqrt{3c} \right\} \right|. \tag{37}$$

For a positive integer t, Hooley's Δ-function of t (see [10] for detailed information) is defined as

$$\Delta(t) = \max_x \left| \left\{ b \in \mathbb{Z}_{>0} : b \mid t,\ e^x < b \leq e^{x+1} \right\} \right|.$$

Take $x = \log \sqrt{c}$, then

$$\left\{ b \in \mathbb{Z}_{>0} : b \mid c,\ \sqrt{c} < b \leq \sqrt{3c} \right\} \subseteq \left\{ b \in \mathbb{Z}_{>0} : b \mid c,\ e^x < b \leq e^{x+1} \right\},$$

since $\sqrt{3} < e$, and so $f_2(r) \leq \Delta(c)$. Therefore an estimate on $f_2(r)$ would follow from estimates on $\Delta(c)$, some of which can be found in Section 2 of [4]; in particular, equations (10)-(13) of [4] imply that the bound

$$f_2(r) \leq O\left(\frac{\tau(c)}{\sqrt{\omega(c)}}\right) \leq O\left(c^{\frac{(1+\varepsilon)\log 2}{\log\log c}}\right) \tag{38}$$

holds for any $\varepsilon > 0$, assuming c is greater than some $c_0(\varepsilon)$ for the second inequality; here the constant in O-notation is independent of c.

Next notice that if $q^2 - p^2 = r^2 D$ and $g \mid p, q$, then $g \mid r$, since D is squarefree. This implies that

$$f_2(r) = \sum_{g|r} f\left(\frac{r}{g}\right). \tag{39}$$

Recall that the Möbius function is defined by

$$\mu(u) = \begin{cases} (-1)^{\omega(u)} & \text{if } u \text{ is squarefree} \\ 0 & \text{otherwise,} \end{cases}$$

then applying the Möbius inversion formula to (39), we obtain

$$f(r) = \sum_{g|r} \mu\left(\frac{r}{g}\right) f_2(g) \ll \sum_{g|r} \mu\left(\frac{r}{g}\right) \frac{\tau(g^2 D)}{\sqrt{\omega(g^2 D)}}, \tag{40}$$

by (38). This establishes (30) upon the observation that $\omega(g^2 D) = \omega(gD)$. □

Remark 3.3. Theorems 431 and 432 of [11] state that normal orders of $\omega(u)$ and $\tau(u)$ are $\log\log u$ and $2^{\log\log u}$, respectively. This implies that one would normally expect

$$\frac{\tau(u)}{\sqrt{\omega(u)}} \leq 2^{\omega(u)}$$

for a randomly chosen integer u (in the appropriate sense).

We also record a corollary here, which will be useful to us in Section 4.

Corollary 3.5. *The equation $p^2 + D = q^2$ with squarefree positive integer D has an integral solution (p, q) satisfying $p/q \leq 1/2$ if and only if*

$$D = d_1 d_2 \text{ for some } d_1, d_2 \in \mathbb{Z}_{>0} \text{ with } d_1 < d_2,\ \sqrt{\frac{D}{3}} \leq d_1 < \sqrt{D}. \tag{41}$$

If this is the case, then $\gcd(d_1, d_2) = 1$*, and if (p, q) is such a solution, then* $\gcd(p, q) = 1$*. Moreover, if D is positive even squarefree integer, then there are no solutions to $p^2 + D = q^2$.*

Proof. Notice that $p^2 + D = q^2$ has an integral solution if and only if it has a positive integral solution. The number of positive integral solutions (p, q) with $p/q \leq 1/2$ is then given by $f_2(1)$ as in (32), and so the equation has solutions if and only if $f_2(1) \geq 1$. Hence (37) with $c = D$ implies that this happens if and only if

$$D = d_1 d_2 \text{ for some } d_1, d_2 \in \mathbb{Z}_{>0} \text{ with } d_1 < d_2,\ \sqrt{D} < d_2 \leq \sqrt{3D},$$

which is equivalent to (41). Now, if (41) holds, then $\gcd(d_1, d_2) = 1$ since D is squarefree. Similarly, suppose (p, q) is a solution with $\gcd(p, q) = g$, then $g^2 \mid D$, and so $g = 1$.

Finally, suppose $2 \mid D = q^2 - p^2$. Then $2 \mid q - p$ or $2 \mid q + p$, which means that 2 divides both, $q - p$ and $q + p$, and so $2^2 \mid D$, which contradicts D being squarefree. Hence $p^2 + D = q^2$ has no solutions. □

4. Ideal WR lattices in the plane

In this section we discuss ideal well-rounded lattices in the plane, proving Theorem 1.5. We start by setting some standard notation, following [8] (see also [3] for a detailed exposition). 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, as above. We have $\mathcal{O}_K = \mathbb{Z}[\delta]$, where

$$\delta = \begin{cases} -\sqrt{D} & \text{if } K = \mathbb{Q}(\sqrt{D}),\ D \not\equiv 1 (\operatorname{mod} 4) \\ \frac{1-\sqrt{D}}{2} & \text{if } K = \mathbb{Q}(\sqrt{D}),\ D \equiv 1 (\operatorname{mod} 4) \\ -\sqrt{-D} & \text{if } K = \mathbb{Q}(\sqrt{-D}),\ -D \not\equiv 1 (\operatorname{mod} 4) \\ \frac{1-\sqrt{-D}}{2} & \text{if } K = \mathbb{Q}(\sqrt{-D}),\ -D \equiv 1 (\operatorname{mod} 4). \end{cases} \tag{42}$$

Let $\sigma_1, \sigma_2 : K \to \mathbb{C}$ be the embeddings of K, given by

$$\sigma_1(x + y\sqrt{\pm D}) = x + y\sqrt{\pm D},\ \sigma_2(x + y\sqrt{\pm D}) = x - y\sqrt{\pm D}$$

for each $x + y\sqrt{\pm D} \in K$, where $\pm$ is determined by whether K is a real or an imaginary quadratic field, respectively. The number field norm on K is defined by

$$\mathbb{N}(x + y\sqrt{\pm D}) = \sigma_1(x + y\sqrt{\pm D})\sigma_2(x + y\sqrt{\pm D}) = \left(x + y\sqrt{\pm D}\right)\left(x - y\sqrt{\pm D}\right).$$

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

$$I = \{ax + (b + g\delta)y : x, y \in \mathbb{Z}\}, \tag{43}$$

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

$$b < a,\ g \mid a, b,\ \text{and } ag \mid \mathbb{N}(b + g\delta). \tag{44}$$

Such integral basis $a, b + g\delta$ is unique for each ideal I and is called the *canonical basis* for I.

We can now use the embeddings σ_1, σ_2 to define the standard 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 ideal $I \subseteq \mathcal{O}_K$ becomes a lattice of full rank in $\mathbb{R}^2$ under this embedding, which we will denote by $\Lambda_K(I) := \sigma_K(I)$. Such lattices are called planar *ideal lattices*; they play an important role in number theory and discrete geometry (see [8] for further details and an overview).

It is easy to check that ideal lattices are always integral. An investigation of well-rounded ideal lattices has been initiated in [8], devoting some special attention to the planar case. We will say that an ideal $I \subseteq \mathcal{O}_K$ is WR if the lattice $\Lambda_K(I)$ is WR. It has been established in [8] that $\mathcal{O}_K$ is WR if and only if $K = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$. On the other hand, infinite families of real and imaginary quadratic fields with WR ideals have been constructed in [8]. Here we extend and generalize these constructions, showing that many similarity classes of planar IWR lattices contain ideal lattices.

Let $K = \mathbb{Q}(\sqrt{\pm D})$ and $I \subseteq \mathcal{O}_K$ be an ideal with the canonical basis $a, b+g\delta$, as above. It is then easy to check that $\Lambda_K(I)$ has the following shape, which we record in a convenient form for the proof of our next lemmas:

If $K = \mathbb{Q}(\sqrt{D})$, $D \not\equiv 1(\operatorname{mod} 4)$, then

$$\Lambda_K(I) = \begin{pmatrix} a & b-g\sqrt{D} \\ a & b+g\sqrt{D} \end{pmatrix} \mathbb{Z}^2 = \begin{pmatrix} a-b+g\sqrt{D} & b-g\sqrt{D} \\ a-b-g\sqrt{D} & b+g\sqrt{D} \end{pmatrix} \mathbb{Z}^2. \tag{45}$$

If $K = \mathbb{Q}(\sqrt{D})$, $D \equiv 1(\operatorname{mod} 4)$, then

$$\Lambda_K(I) = \begin{pmatrix} a & \frac{2b+g}{2} - \frac{g\sqrt{D}}{2} \\ a & \frac{2b+g}{2} + \frac{g\sqrt{D}}{2} \end{pmatrix} \mathbb{Z}^2 = \begin{pmatrix} \frac{2a-2b-g}{2} + \frac{g\sqrt{D}}{2} & \frac{2b+g}{2} - \frac{g\sqrt{D}}{2} \\ \frac{2a-2b-g}{2} - \frac{g\sqrt{D}}{2} & \frac{2b+g}{2} + \frac{g\sqrt{D}}{2} \end{pmatrix} \mathbb{Z}^2. \tag{46}$$

If $K = \mathbb{Q}(\sqrt{-D})$, $-D \not\equiv 1(\operatorname{mod} 4)$, then

$$\Lambda_K(I) = \begin{pmatrix} a & b \\ 0 & -g\sqrt{D} \end{pmatrix} \mathbb{Z}^2 = \begin{pmatrix} a-b & b \\ g\sqrt{D} & -g\sqrt{D} \end{pmatrix} \mathbb{Z}^2. \tag{47}$$

If $K = \mathbb{Q}(\sqrt{-D})$, $-D \equiv 1(\operatorname{mod} 4)$, then

$$\Lambda_K(I) = \begin{pmatrix} a & \frac{2b+g}{2} \\ 0 & -\frac{g\sqrt{D}}{2} \end{pmatrix} \mathbb{Z}^2 = \begin{pmatrix} \frac{2a-2b-g}{2} & \frac{2b+g}{2} \\ \frac{g\sqrt{D}}{2} & -\frac{g\sqrt{D}}{2} \end{pmatrix} \mathbb{Z}^2. \tag{48}$$

Lemma 4.1. *Let D be a positive odd squarefree integer, satisfying* (41) *of Corollary 3.5, and let (p,q) be a solution to the equation $p^2 + D = q^2$ with $p/q \leq 1/2$. Let $C_D(p,q)$ be the similarity class of $\Omega_D(p,q)$ as in* (16)*. Then $C_D(p,q)$ contains ideal lattices. More specifically, let*

$$(a,b) = \begin{cases} \left(p+q, \frac{p+q-1}{2}\right) & \text{if } D \equiv 1(\operatorname{mod} 4) \\ (2(p+q), p+q) & \text{if } D \equiv 3(\operatorname{mod} 4), \end{cases} \tag{49}$$

and define

$$\begin{aligned} I = I(p,q) &:= \{ax + (b+\delta)y : x, y \in \mathbb{Z}\} \subset \mathcal{O}_{\mathbb{Q}(\sqrt{D})} \\ J = J(p,q) &:= \{ax + (b+\delta)y : x, y \in \mathbb{Z}\} \subset \mathcal{O}_{\mathbb{Q}(\sqrt{-D})} \end{aligned} \tag{50}$$

for this choice of (a,b), where δ is defined accordingly as in (42)*. Then I, J are WR ideals in their respective quadratic number rings, and the ideal lattices $\Lambda_{\mathbb{Q}(\sqrt{D})}(I)$, $\Lambda_{\mathbb{Q}(\sqrt{-D})}(J)$ belong to the similarity class $C_D(p,q)$.*

Proof. It is easy to verify that (a,b) as in (49) and $g = 1$ satisfy the conditions of (44) with δ chosen respectively as in (42). Therefore I and J defined in (50) are indeed ideals with the corresponding canonical basis $a, b+\delta$. Now a straight-forward calculation shows that the ideal lattices $\Lambda_{\mathbb{Q}(\sqrt{D})}(I), \Lambda_{\mathbb{Q}(\sqrt{-D})}(J)$ are WR with the corresponding minimal basis matrices being the second matrices in formulas (45)-(48), respectively, and cosine of the angle of each such lattice being p/q. This completes the proof. □

In fact, Lemma 4.1 combined with Theorem 1.3 allow for an additional observation on WR ideal lattices in the plane, which we record below.

Corollary 4.2. *Suppose that Γ is an IWR lattice of type D, where D is as in Lemma 4.1. Then Γ contains IWR sublattices similar to ideal lattices coming from ideals in $\mathbb{Q}(\sqrt{\pm D})$.*

Proof. Theorem 1.3 guarantees that Γ contains sublattices similar to $\Omega_D(p,q)$ for any p,r,q satisfying $p^2+r^2D=q^2$ with $\gcd(p,q)=1$ and $p/q \leq 1/2$. Since D is as in the statement of Lemma 4.1, there must exist such p,q with $r=1$. Then Γ must contain IWR sublattices similar to $\Lambda_{\mathbb{Q}(\sqrt{D})}(I)$ and to $\Lambda_{\mathbb{Q}(\sqrt{-D})}(J)$ for I,J as in (50) for each such choice of p,q. $\square$

Next we prove that the WR ideal lattices coming from imaginary quadratic fields constructed in Lemma 4.1 are all that there are, up to similarity.

Lemma 4.3. *Let $D \in \mathbb{Z}_{>0}$ be squarefree and let $K=\mathbb{Q}(\sqrt{-D})$ be such that there exists a WR ideal $I \subset \mathcal{O}_K$. Then D must satisfy* (41) *of Corollary 3.5 and $\Lambda_K(I) \sim \Omega_D(p,q)$ for some p,q so that $p^2+D=q^2$, $\gcd(p,q)=1$, $p/q \leq 1/2$.*

Proof. We start with a general remark that applies to any planar lattice Λ. Given a basis matrix A for Λ, there must exist a change of basis matrix

$$U=\begin{pmatrix} s_1 & s_2 \\ s_3 & s_4 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}) \tag{51}$$

so that $B=AU$ is a basis matrix for Λ corresponding to a Minkowski-reduced basis (in case Λ is WR, this is our minimal basis).

We are now ready to start the proof with notation as in the statement of the lemma. Assume that the canonical basis for the ideal I is $a, b+g\delta$, then $I=gI'$, 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 suppose that $-D \not\equiv 1 (\mathrm{mod}\, 4)$, $K=\mathbb{Q}(\sqrt{-D})$, then $\Lambda_K(I)$ is as in (47) with $g=1$. Let U as in (51) be the change of basis matrix from the first basis matrix in (47) to a minimal basis matrix. Then $\Lambda_K(I)$ is a WR lattice with minimal basis matrix

$$B=\begin{pmatrix} as_1+bs_3 & as_2+bs_4 \\ -s_3\sqrt{D} & -s_4\sqrt{D} \end{pmatrix}. \tag{52}$$

Since

$$\sin\theta(\Lambda_K(I))=\frac{\det \Lambda_K(I)}{|\Lambda_K(I)|}=\frac{r\sqrt{D}}{q}, \tag{53}$$

where $\gcd(r,q)=1$, we immediately deduce from (47) and (52) that

$$r=\frac{a}{\gcd(a,(as_1+bs_3)^2+Ds_3^2)},$$

where

$$(as_1+bs_3)^2+Ds_3^2=a(as_1^2+2bs_1s_3)+(b^2+D)s_3^2$$

is divisible by a, by (44), since $\mathbb{N}(b+g\delta)=b^2+D$ in this case. Therefore r must be equal to 1, and so $\Lambda_K(I) \sim \Omega_D(p,q)$ for some p,q so that $p^2+D=q^2$, $\gcd(p,q)=1$, $p/q \leq 1/2$.

Next suppose that $-D \equiv 1 (\mathrm{mod}\, 4)$, $K=\mathbb{Q}(\sqrt{-D})$, then $\Lambda_K(I)$ is as in (48) with $g=1$. Let U as in (51) be the change of basis matrix from the first basis matrix in (48) to a minimal basis matrix. Then $\Lambda_K(I)$ is a WR lattice with minimal basis matrix

$$B=\begin{pmatrix} as_1+(b+1/2)s_3 & as_2+(b+1/2)s_4 \\ -s_3\sqrt{D}/2 & -s_4\sqrt{D}/2 \end{pmatrix}. \tag{54}$$

Analogously to the argument above,

$$r = \frac{2a}{\gcd(2a, 4a^2 s_1^2 + 4a(2b+1)s_1 s_3 + ((2b+1)^2 + D)s_3^2} = 1,$$

since $(2b+1)^2 + D$ is divisible by $2a$, by (44), because $\mathbb{N}(b+g\delta) = \frac{1}{4}((2b+1)^2 + D)$ in this case. Hence again $\Lambda_K(I) \sim \Omega_D(p,q)$ for some p,q so that $p^2 + D = q^2$, $\gcd(p,q) = 1$, $p/q \leq 1/2$. This completes the proof of the lemma. □

In the case of a real quadratic field the situation appears to be more complicated. We propose the following question.

Question 1. *Do there exist real quadratic fields $K = \mathbb{Q}(\sqrt{D})$ with positive squarefree D not satisfying* (41) *of Corollary 3.5 so that $\mathcal{O}_K$ contains WR ideals?*

Computational evidence suggests that the answer to this question is no, however at the moment we only have the following partial result in this direction.

Lemma 4.4. *Let $D \in \mathbb{Z}_{>0}$ be squarefree and let $K = \mathbb{Q}(\sqrt{D})$ be such that there exists a WR ideal $I = \langle a, b + g\delta \rangle \subset \mathcal{O}_K$, where $a, b + g\delta$ is the canonical basis for I. Assume in addition that $a \mid 2D$, then D must satisfy* (41) *of Corollary 3.5 and $\Lambda_K(I) \sim \Omega_D(p,q)$ for some p,q so that $p^2 + D = q^2$, $\gcd(p,q) = 1$, $p/q \leq 1/2$. In particular, if*

(1) $D \not\equiv 1 (\operatorname{mod} 4)$ and $\min\{a^2, b^2 + D\} \geq 2ab$, or

(2) $D \equiv 1 (\operatorname{mod} 4)$ and $\min\left\{a^2, \frac{1}{4}((2b+1)^2 + D)\right\} \geq 2a(b+1)$,

then $a \mid 2D$.

Proof. First notice, as in the proof of Lemma 4.3, 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 $g = 1$.

It is easy to see that the condition $a \mid 2D$ is equivalent to $a \mid b^2 + D$ if $D \not\equiv 1 (\operatorname{mod} 4)$, and to $a \mid (2b+1)^2 + D$ if $D \equiv 1 (\operatorname{mod} 4)$. Indeed, if $D \not\equiv 1 (\operatorname{mod} 4)$, then (44) implies that

$$a \mid \mathbb{N}(b + g\delta) = b^2 - D, \tag{55}$$

and so $a \mid 2D$ if and only if $a \mid b^2 + D$; if $D \equiv 1 (\operatorname{mod} 4)$, then (44) implies that

$$a \mid \mathbb{N}(b + g\delta) = \frac{1}{4}((2b+1)^2 - D), \tag{56}$$

and so $a \mid 2D$ if and only if $a \mid (2b+1)^2 + D$.

Now suppose that $D \not\equiv 1 (\operatorname{mod} 4)$, $K = \mathbb{Q}(\sqrt{D})$, then $\Lambda_K(I)$ is as in (45) with $g = 1$. Let U as in (51) be the change of basis matrix from the first basis matrix in (45) to a minimal basis matrix. Then $\Lambda_K(I)$ is a WR lattice with minimal basis matrix

$$B = \begin{pmatrix} as_1 + (b - \sqrt{D})s_3 & as_2 + (b - \sqrt{D})s_4 \\ as_1 + (b + \sqrt{D})s_3 & as_2 + (b + \sqrt{D})s_4 \end{pmatrix}. \tag{57}$$

Then we must have:

$$a^2 s_1^2 + 2abs_1 s_3 + (b^2 + D)s_3^2 = a^2 s_2^2 + 2abs_2 s_4 + (b^2 + D)s_4^2, \tag{58}$$

and analogously to the arguments in the proof of Lemma 4.3 above in the imaginary case, we have

$$r = \frac{a}{\gcd(a, a^2 s_1^2 + 2abs_1 s_3 + (b^2 + D)s_3^2)}. \tag{59}$$

Hence if $a \mid 2D$, then $r = 1$, and so $\Lambda_K(I) \sim \Omega_D(p,q)$ for some p,q so that $p^2 + D = q^2$, $\gcd(p,q) = 1$, $p/q \leq 1/2$. We will now show that if (1) is satisfied, then $a \mid 2D$. Take U to be the identity matrix. The positive definite binary quadratic norm form corresponding to the basis matrix B in this case will be

$$Q_B(x,y) = 2a^2x^2 + 4abxy + 2(b^2 + D)y^2.$$

Since $\min\{a^2, b^2 + D\} \geq 2ab$, this form must be Minkowski reduced, which means that B must be a minimal basis matrix. Since $\Lambda_K(I)$ is WR, the form $Q_B(x,y)$ must be symmetric, i.e we must have $a^2 = b^2+D$, and hence $a \mid 2D$ by the argument above.

Next suppose that $D \equiv 1 (\bmod 4)$, $K = \mathbb{Q}(\sqrt{D})$, then $\Lambda_K(I)$ is as in (46) with $g = 1$. Let U as in (51) be the change of basis matrix from the first basis matrix in (46) to a minimal basis matrix. Then $\Lambda_K(I)$ is a WR lattice with minimal basis matrix

$$B = \begin{pmatrix} as_1 + \frac{(2b+1-\sqrt{D})s_3}{2} & as_2 + \frac{(2b+1-\sqrt{D})s_4}{2} \\ as_1 + \frac{(2b+1+\sqrt{D})s_3}{2} & as_2 + \frac{(2b+1+\sqrt{D})s_4}{2} \end{pmatrix}. \tag{60}$$

Then we must have:

$$\begin{aligned} & 4a^2s_1^2 + 8abs_1s_3 + 4as_1s_3 + ((2b+1)^2 + D)s_3^2 \\ = \; & 4a^2s_2^2 + 8abs_2s_4 + 4as_2s_4 + ((2b+1)^2 + D)s_4^2, \end{aligned} \tag{61}$$

and analogously to the arguments in the proof of Lemma 4.3 above in the imaginary case, we have

$$r = \frac{a}{\gcd(a, 4a^2s_1^2 + 8abs_1s_3 + 4as_1s_3 + ((2b+1)^2 + D)s_3^2)} = 1.$$

Hence if $a \mid 2D$, then $r = 1$, and so again $\Lambda_K(I) \sim \Omega_D(p,q)$ for some p,q so that $p^2 + D = q^2$, $\gcd(p,q) = 1$, $p/q \leq 1/2$. We will now show that if (2) is satisfied, then $a \mid 2D$. Again, take U to be the identity matrix. The positive definite binary quadratic norm form corresponding to the basis matrix B in this case will be

$$Q_B(x,y) = 2a^2x^2 + 4a(b+1)xy + \frac{1}{2}((2b+1)^2 + D)y^2.$$

Since $\min\left\{a^2, \frac{1}{4}((2b+1)^2 + D)\right\} \geq 2a(b+1)$, this form must be Minkowski reduced, which means that B must be a minimal basis matrix. Since $\Lambda_K(I)$ is WR, the form $Q_B(x,y)$ must be symmetric, i.e we must have $4a^2 = (2b+1)^2 + D$, and hence $a \mid 2D$ by the argument above. □

In addition, we have the following finiteness result for the number of WR ideals in a fixed imaginary quadratic number field.

Lemma 4.5. *Suppose that D satisfies* (41) *of Corollary 3.5 and $K = \mathbb{Q}(\sqrt{-D})$. Then K contains only finitely many WR ideals, up to similarity of the corresponding lattices, and this number is*

$$\ll \min\left\{2^{\omega(D)-1}, \frac{2^{\omega(D)}}{\sqrt{\omega(D)}}\right\}, \tag{62}$$

where the constant in the Vinogradov notation $\ll$ does not depend on D.

Proof. Corollary 3.5 guarantees that there exist integer pairs (p, q) such that

$$p^2 + D = q^2 \text{ for some } p, q \text{ with } \gcd(p, q) = 1, p/q \leq 1/2. \tag{63}$$

Now Lemma 4.1 guarantees that if $K = \mathbb{Q}(\sqrt{-D})$, then there exists a WR ideal $I \subseteq \mathcal{O}_K$ with $\Lambda_K(I) \in \Omega_D(p, q)$ for each p, q satisfying (63), and Lemma 4.3 implies that *all* WR ideals in $\mathcal{O}_K$ correspond to solutions of (63). Then the number of WR ideals in K, up to similarity of the lattices $\Lambda_K(I)$, is precisely the number of pairs p, q as in (63). This number is precisely $f(1)$ as defined in (31), which is estimated by (33). Now applying (35) and (38), and noticing that for a squarefree integer D

$$\frac{\tau(D)}{\sqrt{\omega(D)}} = \frac{2^{\omega(D)}}{\sqrt{\omega(D)}},$$

we obtain (62). □

Proof of Theorem 1.5. The first part of the theorem along with (12) follow from Lemmas 4.1, 4.3, and 4.5 above, so it is only left to establish (11). Define sets

$$\mathcal{A} = \left\{ D : D \in \mathbb{Z}_{>0} \text{ squarefree} \right\}, \tag{64}$$

and

$$\mathcal{B}_\nu = \left\{ D : D \in \mathbb{Z}_{>0} \text{ squarefree with a divisor } \frac{\sqrt{D}}{\nu} \leq d < \sqrt{D} \right\}, \tag{65}$$

where $\nu > 1$ is a real number. Define also

$$\mathcal{A}(N) = \left\{ D \in \mathcal{A} : D \leq N \right\}, \ \mathcal{B}_\nu(N) = \left\{ D \in \mathcal{B}_\nu : D \leq N \right\},$$

for any $N \in \mathbb{Z}_{>0}$. To prove (11) we simply need to show that

$$\liminf_{N \to \infty} \frac{\left| \mathcal{B}_{\sqrt{3}}(N) \right|}{|\mathcal{A}(N)|} \geq \frac{\sqrt{3} - 1}{2\sqrt{3}}. \tag{66}$$

An analogue of (66) for integers that are not necessarily squarefree has been established in Theorem 4.4 of [4]. We will now adapt the proof of Theorem 4.4 of [4] to account for the squarefree condition.

Theorem 333 of [11] implies that there exist absolute constants c_1, c_2 such that

$$\frac{6N}{\pi^2} + c_1\sqrt{N} \leq |\mathcal{A}(N)| \leq \frac{6N}{\pi^2} + c_2\sqrt{N}. \tag{67}$$

Now, following Section 4 of [4], we define

$$I_\nu(n) = \left\{ n^2, n(n-1), \dots, n\left(n - \left[\left(\frac{\nu - 1}{\nu} \right) n \right] \right) \right\},$$

for each $n \in \mathbb{Z}_{>0}$, and let

$$I'_\nu(n) = \left\{ m \in I_\nu(n) : m \text{ is squarefree} \right\}.$$

Suppose n is prime, then

$$I'_\nu(n) = \left\{ nm : \left(n - \left[\left(\frac{\nu - 1}{\nu} \right) n \right] \right) \leq m < n, \ m \text{ is squarefree} \right\},$$

and so, by (67)

$$\begin{aligned} |I'_\nu(n)| &= |\mathcal{A}(n)| - \left|\mathcal{A}\left(n - \left[\left(\frac{\nu-1}{\nu}\right)n\right]\right)\right| \\ &\geq \frac{6}{\pi^2}\left[\left(\frac{\nu-1}{\nu}\right)n\right] + (c_1-c_2)\sqrt{n}. \end{aligned} \tag{68}$$

Since each $I'_\nu(n) \subseteq I_\nu(n)$ and $I_\nu(n) \cap I_\nu(m) = \emptyset$ when $\gcd(n,m) = 1$, by part (ii) of Lemma 4.2 of [4], we conclude that $I'_\nu(n) \cap I'_\nu(m) = \emptyset$ when $\gcd(n,m) = 1$. Notice also that

$$\bigcup_{n=1}^{[\sqrt{N}]} I'_\nu(n) \subseteq \mathcal{B}_\nu(N).$$

Now we adapt the argument in the proof of Lemma 4.3 of [4]. Let $M = \pi(\sqrt{N})$, i.e. the number of primes up to $\sqrt{N}$. A result of Rosser and Schoenfeld (Corollary 1 on p. 69 of [17]) implies that for all $\sqrt{N} \geq 17$,

$$\frac{\sqrt{N}}{\log\sqrt{N}} < M < \frac{1.25506\,\sqrt{N}}{\log\sqrt{N}} \tag{69}$$

Hence suppose that $N \geq 289$, and let $p_1, \dots, p_M$ be all the primes up to $\sqrt{N}$ in ascending order. Then $I_\nu(p_i) \cap I_\nu(p_j) = \emptyset$ for all $1 \leq i \neq j \leq N$. Therefore, using (68), we obtain:

$$|\mathcal{B}_\nu(N)| \geq \sum_{i=1}^{M} |I'_\nu(p_i)| \geq \frac{6(\nu-1)}{\pi^2\nu}\sum_{i=1}^{M} p_i + (c_1-c_2)\sum_{i=1}^{M}\sqrt{p_i}. \tag{70}$$

A result of R. Jakimczuk [12] implies that

$$\sum_{i=1}^{M} p_i > \frac{M^2}{2}\ \log^2 M. \tag{71}$$

Notice also that

$$(c_1-c_2)\sum_{i=1}^{M}\sqrt{p_i} \geq -|c_1-c_2|M^{3/2},$$

and combining this observation with (69), (70), and (71), we obtain:

$$|\mathcal{B}_\nu(N)| > \frac{6(\nu-1)N}{2\pi^2\nu}\left(1 - \frac{\log\log\sqrt{N}}{\log\sqrt{N}}\right)^2 - |c_1-c_2|N^{3/4}\left(\frac{1.25506}{\log\sqrt{N}}\right)^{3/2}. \tag{72}$$

Notice also that as $N \to \infty$, (67) implies that $|\mathcal{A}(N)| \leq \frac{(6+\varepsilon)N}{\pi^2}$ for any $\varepsilon > 0$, and combining this observation with (72), we obtain:

$$\liminf_{N\to\infty} \frac{|\mathcal{B}_\nu(N)|}{|\mathcal{A}(N)|} > \frac{6(\nu-1)}{2(6+\varepsilon)\nu} \geq \frac{\nu-1}{2\nu}, \tag{73}$$

since the choice of ε is arbitrary. Now (66) follows by taking $\nu = \sqrt{3}$. □

Finally, we briefly discuss WR lattices coming from principal ideals. It is well known that every ideal in a ring of integers of a number field can be generated by at most two elements, and principal ideals play a very special role in algebraic number theory: they correspond to the identity element of the class group of a number field. It is therefore natural to ask whether principal ideals in a quadratic number ring can be WR? Corollary 2.4 of [8] implies that if $K = \mathbb{Q}\left(\sqrt{-D}\right)$, then $\mathcal{O}_K$ contains principal WR ideals if and only if $D = 1, 3$. In the real quadratic case, the situation is again more complicated. We propose the following question.

Question 2. *Do there exist real quadratic fields* $K = \mathbb{Q}(\sqrt{D})$ *with positive squarefree* $D \not\equiv 1 (\operatorname{mod} 4)$ *so that* $\mathcal{O}_K$ *contains principal WR ideals?*

Computational evidence suggests that the answer to this question is no. On the other hand, there do exist $D \equiv 1 (\operatorname{mod} 4)$ so that $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ contains a WR principal ideal I. In Table 2 below we present a few examples of number fields $K = \mathbb{Q}(\sqrt{D})$, $D \equiv 1 (\operatorname{mod} 4)$, so that the class number $h_K = 1$, which contain WR ideals. We present these ideals in terms of their canonical integral bases with δ as in (42).

Table 2. Examples of WR ideals in $K = \mathbb{Q}(\sqrt{D})$, $D \equiv 1 (\operatorname{mod} 4)$, $h_K = 1$

D	WR ideals	Their similarity classes p/q $(r = 1)$
21	$\langle 3, 1+\delta \rangle, \langle 7, 3+\delta \rangle$	$2/5, 2/5$
77	$\langle 7, 3+\delta \rangle, \langle 11, 5+\delta \rangle$	$2/9, 2/9$
133	$\langle 7, 3+\delta \rangle, \langle 19, 9+\delta \rangle$	$6/13, 6/13$
209	$\langle 11, 5+\delta \rangle, \langle 19, 9+\delta \rangle$	$4/15, 4/15$

Acknowledgment. We would like to thank the Fletcher Jones Foundation-supported Claremont Colleges research experience program, under the auspices of which this work was done during the Summer of 2011. We also thank Professor Wai Kiu Chan for his useful comments on the subject of this paper.

References

[1] A. H. Banihashemi and A. K. Khandani. On the complexity of decoding lattices using the Korkin-Zolotarev reduced basis. *IEEE Trans. Inform. Theory*, 44(1):162–171, 1998.
[2] M. Bernstein, N. J. A. Sloane, and P. E. Wright. On sublattices of the hexagonal lattice. *Discrete Math.*, 170(1-3):29–39, 1997.
[3] D. A. Buell. *Binary Quadratic Forms*. Springer-Verlag, 1989.
[4] L. Fukshansky. On distribution of well-rounded sublattices of $\mathbb{Z}^2$. *J. Number Theory*, 128(8):2359–2393, 2008.
[5] L. Fukshansky. On similarity classes of well-rounded sublattices of $\mathbb{Z}^2$. *J. Number Theory*, 129(10):2530–2556, 2009.
[6] L. Fukshansky. Revisiting the hexagonal lattice: on optimal lattice circle packing. *Elem. Math.*, 66(1):1–9, 2011.
[7] L. Fukshansky, D. Moore, R. A. Ohana, and W. Zeldow. On well-rounded sublattices of the hexagonal lattice. *Discrete Math.*, 310(23):3287–3302, 2010.
[8] L. Fukshansky and K. Petersen. On ideal well-rounded lattices. *Int. J. Number Theory, to appear; arXiv:1101.4442v3.*
[9] L. Fukshansky and S. Robins. Frobenius problem and the covering radius of a lattice. *Discrete Comput. Geom.*, 37(3):471–483, 2007.
[10] R. Hall and G. Tenenbaum. *Divisors*. Cambridge Univ. Press, 1988.
[11] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers. Fifth edition.* The Clarendon Press, Oxford University Press, New York, 1979.

[12] R. Jakimczuk. Inequalities and asymptotic formulas for sums of prime powers. *Bol. Soc. Mat. Mexicana (3)*, 11(1):5–10, 2005.
[13] F. Lemmermeyer. Conics - a poor man's elliptic curves. http://www.fen.bilkent.edu.tr/~franz/publ/conics.pdf.
[14] J. Martinet. *Perfect Lattices in Euclidean Spaces*. Springer-Verlag, 2003.
[15] C. McMullen. Minkowski's conjecture, well-rounded lattices and topological dimension. *J. Amer. Math. Soc.*, 18(3):711–734, 2005.
[16] R. A. Mollin. *Fundamental number theory with applications*. CRC Press, 1998.
[17] J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math*, 6:64–94, 1962.
[18] S. S. Ryskov. The two-dimensional ζ-function with real parameter. *Dokl. Akad. Nauk SSSR*, 184:288–291, 1969.

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

Department of Mathematics and Computer Science, Wesleyan University, Middletown, CT 06459
E-mail address: ghenshaw@wesleyan.edu

Department of Mathematics, Claremont McKenna College, Claremont, CA 91711
E-mail address: PLiao14@students.claremontmckenna.edu

Department of Mathematics, Harvey Mudd College, Claremont, CA 91711
E-mail address: mthwate@gmail.com

School of Mathematical Sciences, Claremont Graduate University, Claremont, CA 91711
E-mail address: foxfur_32@hotmail.com

Department of Mathematics, Pomona College, Claremont, CA 91711
E-mail address: scw22009@mymail.pomona.edu