Claremont Colleges
Scholarship @ Claremont

CMC Faculty Publications and Research | CMC Faculty Scholarship

8-1-2008

On Distribution of Well-Rounded Sublattices of Z^2

Lenny Fukshansky
Claremont McKenna College

Recommended Citation
Fukshansky, Lenny. "On distribution of well-rounded sublattices of Z^2." Journal of Number Theory 128.8 (2008): 2359-2393.

This Article is brought to you for free and open access by the CMC Faculty Scholarship at Scholarship @ Claremont. It has been accepted for inclusion in CMC Faculty Publications and Research by an authorized administrator of Scholarship @ Claremont. For more information, please contact scholarship@cuc.claremont.edu.

ON DISTRIBUTION OF WELL-ROUNDED SUBLATTICES OF $\mathbb{Z}^2$

LENNY FUKSHANSKY

Abstract. A lattice is called well-rounded if its minimal vectors span the corresponding Euclidean space. In this paper we completely describe well-rounded full-rank sublattices of $\mathbb{Z}^2$, as well as their determinant and minima sets. We show that the determinant set has positive density, deriving an explicit lower bound for it, while the minima set has density 0. We also produce formulas for the number of such lattices with a fixed determinant and with a fixed minimum. These formulas are related to the number of divisors of an integer in short intervals and to the number of its representations as a sum of two squares. We investigate the growth of the number of such lattices with a fixed determinant as the determinant grows, exhibiting some determinant sequences on which it is particularly large. To this end, we also study the behavior of the associated zeta function, comparing it to the Dedekind zeta function of Gaussian integers and to the Solomon zeta function of $\mathbb{Z}^2$. Our results extend automatically to well-rounded sublattices of any lattice $A\mathbb{Z}^2$, where A is an element of the real orthogonal group $O_2(\mathbb{R})$.

Contents

1. Introduction and statement of results 1
2. A special divisor function 5
3. Parametrization of well-rounded lattices 7
4. Proof of Theorem 1.2 12
5. Proof of Theorem 1.3 16
6. Corollaries 19
7. Counting well-rounded lattices with fixed minimum 23
8. Zeta function of well-rounded lattices 25
References 29

1. Introduction and statement of results

Let $N \geq 2$ be an integer, and let $\Lambda \subseteq \mathbb{R}^N$ be a lattice of full rank. Define the *minimum* of Λ to be

$$|\Lambda| = \min_{\boldsymbol{x} \in \Lambda \setminus \{\mathbf{0}\}} \|\boldsymbol{x}\|,$$

where $\| \ \|$ stands for the usual Euclidean norm on $\mathbb{R}^N$. Let

$$S(\Lambda) = \{\boldsymbol{x} \in \Lambda : \|\boldsymbol{x}\| = |\Lambda|\}$$

1991 *Mathematics Subject Classification.* Primary: 11H06, 11M41, 11N56; Secondary: 11N25, 11R42.

Key words and phrases. well-rounded lattices, zeta functions, sums of two squares, divisors.

be the set of *minimal vectors* of Λ. We say that Λ is a *well-rounded* lattice (abbreviated WR) if $S(\Lambda)$ spans $\mathbb{R}^N$. WR lattices come up in a wide variety of different contexts, including sphere packing, covering, and kissing number problems, coding theory, and the linear Diophantine problem of Frobenius, just to name a few. Still, the WR condition is special enough so that one would expect WR lattices to be relatively sparse. However, in 2005 C. McMullen [15] showed that in a certain sense *unimodular* WR lattices are "well distributed" among all *unimodular* lattices in $\mathbb{R}^N$, where a unimodular lattice is a lattice with determinant equal to 1. More specifically, he proved the following theorem, from which he derived the 6-dimensional case of the famous Minkowski's conjecture for unimodular lattices.

Theorem 1.1 ([15])**.** *Let $A \subseteq SL_N(\mathbb{R})$ be the subgroup of diagonal matrices with positive diagonal entries, and let Λ be a full-rank unimodular lattice in $\mathbb{R}^N$. If the closure of the orbit $A\Lambda$ is compact in the space of all full-rank unimodular lattices in $\mathbb{R}^N$, then it contains a WR lattice.*

Notice that in a certain sense this is a statement about distribution of WR lattices in the space of all unimodular lattices in a fixed dimension. Motivated by this beautiful theorem, we want to investigate the distribution of WR sublattices of $\mathbb{Z}^N$, which is a natural arithmetic problem. For instance, for a fixed positive integer t, does there necessarily exist a WR subllatice $\Lambda \subseteq \mathbb{Z}^N$ so that $\det(\Lambda) = t$? If so, how many different such sublattices are there? The first trivial observation is that if $t = d^N$ for some $d \in \mathbb{Z}_{>0}$ and I_N is the $N \times N$ identity matrix, then the lattice $\Lambda = (dI_N)\mathbb{Z}^N$ is WR with $\det(\Lambda) = t$ and $|\Lambda| = d$. It seems however quite difficult to describe *all* WR sublattices of $\mathbb{Z}^N$ in an arbitrary dimension N. This paper is concerned with providing such a description in dimension two.

From now on we will write $\mathrm{WR}(\Omega)$ for the set of all full-rank WR sublattices of a lattice Ω; in this paper we will concentrate on $\mathrm{WR}(\mathbb{Z}^2)$. In section 3 we develop a certain parametrization of lattices in $\mathrm{WR}(\mathbb{Z}^2)$, which we then use to investigate the determinant set $\mathcal{D}$ of such lattices and to count the number of them for a fixed value of determinant. Specifically, let $\mathcal{D}$ be the set of all possible determinant values of lattices in $\mathrm{WR}(\mathbb{Z}^2)$, and let $\mathfrak{M}$ be the set of all possible values of squared minima of these lattices, i.e. $\mathfrak{M} = \{|\Lambda|^2 : \Lambda \in \mathrm{WR}(\mathbb{Z}^2)\}$. It is easy to see that $\mathfrak{M}$ is precisely the set of all positive integers, which are representable as a sum of two squares. Then it is interesting to understand how dense are these sets in $\mathbb{Z}_{>0}$.

For any subset $\mathcal{P}$ of $\mathbb{Z}$ and $M \in \mathbb{Z}_{>0}$, we write

$$\mathcal{P}(M) = \{n \in \mathcal{P} : n \leq M\}.$$

Define *lower density* of $\mathcal{P}$ in $\mathbb{Z}$ to be

$$\underline{\Delta}_{\mathcal{P}} = \liminf_{M\to\infty} \frac{|\mathcal{P}(M)|}{M},$$

and its *upper density* in $\mathbb{Z}$ to be

$$\overline{\Delta}_{\mathcal{P}} = \limsup_{M\to\infty} \frac{|\mathcal{P}(M)|}{M}.$$

Clearly, $0 \leq \underline{\Delta}_{\mathcal{P}} \leq \overline{\Delta}_{\mathcal{P}} \leq 1$. If $0 < \underline{\Delta}_{\mathcal{P}}$, we say that $\mathcal{P}$ *has density*, and if $\underline{\Delta}_{\mathcal{P}} = \overline{\Delta}_{\mathcal{P}}$, i.e. if $\lim_{M\to\infty} \frac{|\mathcal{P}(M)|}{M}$ exists, we say that $\mathcal{P}$ *has asymptotic density* equal to the value of this limit, which could be 0.

With this notation, we will show that $\mathcal{D}$ has density. More specifically, we prove the following.

Theorem 1.2. *The determinant set $\mathcal{D}$ of lattices in $\mathrm{WR}(\mathbb{Z}^2)$ has representation*

$$\mathcal{D} = \left\{ (a^2+b^2)cd \ : \ a,b \in \mathbb{Z}_{\geq 0},\ \max\{a,b\} > 0,\ c,d \in \mathbb{Z}_{>0},\ 1 \leq \frac{c}{d} \leq \sqrt{3} \right\},$$

and lower density

$$\underline{\Delta}_{\mathcal{D}} \geq \frac{3^{\frac{1}{4}}-1}{2\cdot 3^{\frac{1}{4}}} \approx 0.12008216\ldots \tag{1}$$

The minima set $\mathfrak{M}$ has asymptotic density 0.

We prove Theorem 1.2 in section 4. Now, if $\Lambda \in \mathrm{WR}(\mathbb{Z}^2)$, let $\boldsymbol{x}, \boldsymbol{y}$ be a minimal basis for Λ, and let θ be the angle between the vectors $\boldsymbol{x}$ and $\boldsymbol{y}$; it is a well known fact that in dimensions ≤ 4 a lattice is always generated by vectors corresponding to its successive minima, so such a basis certainly exists (see, for instance, [18]). Then there is a simple connection between the minimum and the determinant of Λ:

$$\det(\Lambda) = \|\boldsymbol{x}\|\|\boldsymbol{y}\|\sin\theta = |\Lambda|^2\sqrt{1-\frac{(\boldsymbol{x}^t\boldsymbol{y})^2}{|\Lambda|^4}} = \sqrt{|\Lambda|^4-(\boldsymbol{x}^t\boldsymbol{y})^2}.$$

Lemma 3.2 below implies that $0 \leq |\boldsymbol{x}^t\boldsymbol{y}| \leq \frac{|\Lambda|^2}{2}$. Therefore we have

$$\frac{\sqrt{3}\,|\Lambda|^2}{2} \leq \det(\Lambda) \leq |\Lambda|^2.$$

In view of this relation, it is especially interesting that the determinant set has positive density while the minima set has density 0.

Next, for each $u \in \mathcal{D}$ we want to count the number of $\Lambda \in \mathrm{WR}(\mathbb{Z}^2)$ such that $\det(\Lambda) = u$. We need some additional notation. Suppose $t \in \mathbb{Z}_{>0}$ has prime factorization of the form

$$t = 2^w p_1^{2k_1}\ldots p_s^{2k_s} q_1^{m_1}\ldots q_r^{m_r}, \tag{2}$$

where $p_i \equiv 3 \pmod 4$, $q_j \equiv 1 \pmod 4$, $w \in \mathbb{Z}_{\geq 0}$, $k_i \in \frac{1}{2}\mathbb{Z}_{>0}$, and $m_j \in \mathbb{Z}_{>0}$ for all $1 \leq i \leq s$, $1 \leq j \leq r$. Let $\alpha(t)$ be the number of representations of t as a sum of two squares ignoring order and signs, that is

$$\alpha(t) = \left|\left\{(a,b) \in \mathbb{Z}^2_{\geq 0} : a^2+b^2 = t,\ a \leq b\right\}\right|. \tag{3}$$

Also define

$$\alpha_*(t) = \left|\left\{(a,b) \in \mathbb{Z}^2_{\geq 0} : a^2+b^2 = t,\ a \leq b,\ \gcd(a,b) = 1\right\}\right|, \tag{4}$$

for all $t > 2$, and define $\alpha_*(1) = \alpha_*(2) = \frac{1}{2}$. It is a well-known fact that $\alpha(t)$ is given by

$$\alpha(t) = \begin{cases} 0 & \text{if any } k_i \text{ is a half-integer} \\ \frac{1}{2}B & \text{if each } k_i \text{ is an integer and } B \text{ is even} \\ \frac{1}{2}\left(B-(-1)^w\right) & \text{if each } k_i \text{ is an integer and } B \text{ is odd,} \end{cases}$$

where $B = (m_1+1)\ldots(m_r+1)$ (see, for instance [19], [22]). Clearly, when t is squarefree, $\alpha_*(t) = \alpha(t)$. It is also a well-known fact that for t as in (2)

$$\alpha_*(t) = \begin{cases} 0 & \text{if } s \neq 0 \text{ or } w > 1 \\ 2^{r-1} & \text{if } s = 0 \text{ and } w = 0 \text{ or } 1. \end{cases}$$

We also define the function

$$\beta_\nu(t) = \left|\left\{d \in \mathbb{Z}_{>0} : d \mid t \text{ and } \frac{\sqrt{t}}{\nu} \leq d \leq \sqrt{t}\right\}\right|, \tag{5}$$

for every $1 < \nu \leq 3^{1/4}$. The value of ν which will be particularly important to us is $\nu = 3^{1/4}$, therefore we define

$$\beta(t) = \beta_{3^{1/4}}(t).$$

We discuss the function $\beta_\nu(t)$ in more detail in section 2; at least it is clear that for each given t, $\beta_\nu(t)$ is effectively computable for every ν. Finally, for any $t \in \mathbb{Z}_{>0}$ define

$$\delta_1(t) = \begin{cases} 1 & \text{if } t \text{ is a square} \\ 2 & \text{if } t \text{ is not a square,} \end{cases}$$

and

$$\delta_2(t) = \begin{cases} 0 & \text{if } t \text{ is odd} \\ 1 & \text{if } t \text{ is even, } \frac{t}{2} \text{ is a square} \\ 2 & \text{if } t \text{ is even, } \frac{t}{2} \text{ is not a square.} \end{cases}$$

With this notation, we can state our second main theorem.

Theorem 1.3. *Let $u \in \mathbb{Z}_{>0}$, and let $\mathcal{N}(u)$ be the number of lattices in $\mathrm{WR}(\mathbb{Z}^2)$ with determinant equal to u. If $u = 1$ or 2, then $\mathcal{N}(u) = 1$, the corresponding lattice being either $\mathbb{Z}^2$ or $\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\mathbb{Z}^2$, respectively. Let $u > 2$, and define*

$$t = t(u) = \begin{cases} u & \textit{if } u \textit{ is odd} \\ \frac{u}{2} & \textit{if } u \textit{ is even.} \end{cases}$$

Then:

$$\begin{aligned} \mathcal{N}(u) &= \delta_1(t)\beta(t) + \delta_2(t)\beta\left(\frac{t}{2}\right) + 4 \sum_{\substack{n \mid t, 1 < n < t/2 \\ n \textit{ not a square}}} \alpha_*\left(\frac{t}{n}\right)\beta(n) \\ &+ 2 \sum_{\substack{n \mid t, 1 \leq n < t/2 \\ n \textit{ a square}}} \alpha_*\left(\frac{t}{n}\right)(2\beta(n) - 1). \end{aligned} \tag{6}$$

In particular, if $u \notin \mathcal{D}$, then the right hand side of (6) is equal to zero.

Theorem 1.3 can also be easily extended to a more general class of lattices. Namely, write $O_2(\mathbb{R})$ for the real orthogonal group, then for every $A \in O_2(\mathbb{R})$ and every $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^2$ we have $(A\boldsymbol{x})^t(A\boldsymbol{y}) = \boldsymbol{x}^t\boldsymbol{y}$, i.e. $O_2(\mathbb{R})$ is the isometry group of $\mathbb{R}^2$ with respect to the Euclidean norm. Therefore, if $A \in O_2(\mathbb{R})$ then $\Lambda \in \mathrm{WR}(A\mathbb{Z}^2)$ if and only if $A^t\Lambda \in \mathrm{WR}(\mathbb{Z}^2)$. This immediately implies the following result.

Corollary 1.4. *Let $A \in O_2(\mathbb{R})$. Then the determinant set and the minima set of lattices in $\mathrm{WR}(A\mathbb{Z}^2)$ are $\mathcal{D}$ and $\mathfrak{M}$ respectively, as defined above. Moreover, for each $u \in \mathcal{D}$ the number of lattices in $\mathrm{WR}(A\mathbb{Z}^2)$ with determinant equal to u is given by $\mathcal{N}(u)$ as in Theorem 1.3.*

We prove Theorem 1.3 in section 5. In section 6 we use Theorem 1.3 to work out simple examples of our formula in the case of prime power and product of two primes determinants. We also describe the "orthogonal" elements of $\mathrm{WR}(\mathbb{Z}^2)$, which come from ideals in Gaussian integers; these are quite sparse among all lattices in

$\mathrm{WR}(\mathbb{Z}^2)$. We then derive easy to use bounds on $\mathcal{N}(u)$ and on the normal order of $\mathcal{N}(u)$. We also demonstrate examples of "extremal" sequences of determinant values, for which $\mathcal{N}(u)$ is especially large; see Corollary 6.5. In section 7 we derive a formula for the number of lattices in $\mathrm{WR}(\mathbb{Z}^2)$ of fixed minimum.

In section 8 we study some basic properties of a zeta function, corresponding to the well-rounded sublattices of $\mathbb{Z}^2$. Namely, for $s \in \mathbb{C}$ define

$$\zeta_{\mathrm{WR}(\mathbb{Z}^2)}(s) = \sum_{\Lambda \in \mathrm{WR}(\mathbb{Z}^2)} (\det(\Lambda))^{-s} = \sum_{u=1}^{\infty} \mathcal{N}(u) u^{-s}, \tag{7}$$

where $\mathcal{N}(u)$ is as above. In particular, $\mathcal{N}(u) \neq 0$ if and only if $u \in \mathcal{D}$. For a Dirichlet series $\sum_{n=1}^{\infty} c_n n^{-s}$, we say that it has a *pole of order* μ at $s = s_0$, where μ and s_0 are positive real numbers, if

$$0 < \lim_{s \to s_0^+} |s - s_0|^{\mu} \sum_{n=1}^{\infty} |c_n n^{-s}| < \infty. \tag{8}$$

We will also say that such a Dirichlet series is *bounded from above (or below)* by a Dirichlet series $\sum_{n=1}^{\infty} b_n n^{-s}$, if $\sum_{n=1}^{\infty} |c_n n^{-s}| \leq \sum_{n=1}^{\infty} |b_n n^{-s}|$ (respectively, $\geq \sum_{n=1}^{\infty} |b_n n^{-s}|$). In section 8 we prove the following result.

Theorem 1.5. *Let the notation be as above, then $\zeta_{\mathrm{WR}(\mathbb{Z}^2)}(s)$ is analytic for all $s \in \mathbb{C}$ with $\Re(s) > 1$, and is bounded from below by a Dirichlet series that has a pole of order 2 at $s = 1$. Moreover, for every real $\varepsilon > 0$ there exists a Dirichlet series with a pole of order $2 + \varepsilon$ at $s = 1$, which bounds $\zeta_{\mathrm{WR}(\mathbb{Z}^2)}(s)$ from above.*

Notice that Theorem 1.5 provides additional information about the growth of $\mathcal{N}(u)$. In section 8 we prove Theorem 1.5 by means of considering the behavior of some related Dirichlet series, namely the generating functions of α_* and β_ν. We should remark that we are not using the notion of a pole here in a sense that would imply the existence of an analytic continuation, but only to reflect on the growth of the coefficients; in fact, the arithmetic function $\mathcal{N}(u)$ behaves sufficiently erraticaly that one would doubt $\zeta_{\mathrm{WR}(\mathbb{Z}^2)}(s)$ having an analytic continuation to the left of $s = 1$. We are now ready to proceed.

2. A special divisor function

As above, let $1 < \nu \leq 3^{1/4}$. In this section we briefly discuss bounds on the divisor function $\beta_\nu(t)$. Let

$$\mathcal{M}_\nu(t) = \left\{ d \in \mathbb{Z}_{>0} : d \mid t \text{ and } \frac{\sqrt{t}}{\nu} \leq d \leq \sqrt{t} \right\}.$$

Lemma 2.1. *If $d_1, d_2 \in \mathcal{M}_\nu(t)$, then $\gcd(d_1, d_2) > 1$.*

Proof. Suppose $d_1, d_2 \in \mathcal{M}_\nu(t)$, and $\gcd(d_1, d_2) = 1$. Then $d_1 d_2 | t$, but

$$\frac{t}{\nu^2} < d_1 d_2 \leq t.$$

Notice that $d_1 d_2 \neq t$, since this would imply $d_1 = d_2 = \sqrt{t}$. Then

$$1 < \frac{t}{d_1 d_2} < \nu^2 \leq \sqrt{3},$$

but $\frac{t}{d_1 d_2} \in \mathbb{Z}$, which is a contradiction. $\square$

Lemma 2.1 implies in particular that $\mathcal{M}_\nu(t)$ can contain at most one prime q, and in this case every $d \in \mathcal{M}_\nu(t)$ must be divisible by q. Write $p(t)$ for the smallest prime divisor of t. Another immediate consequence of Lemma 2.1 is that gaps between two consecutive elements of $\mathcal{M}_\nu(t)$ must be greater or equal than $p(t)$. Therefore, since $\beta_\nu(t) = |\mathcal{M}_\nu(t)|$, we obtain

$$\beta_\nu(t) \leq \left[\left(\frac{\nu-1}{\nu p(t)}\right)\sqrt{t}\right] + 1, \tag{9}$$

where $p(t) \geq 2$ for each $t \in \mathbb{Z}$, however for most t better bounds are known.

Let us write $\tau(t)$ for the number of distinct divisors of t and $\omega(t)$ for the number of distinct prime divisors of t (see [7] for detailed information on $\tau(t)$ and $\omega(t)$). Hooley's Δ-function of t is defined by

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

If we take $x = \log \frac{\sqrt{t}}{\nu}$, then it is easy to see that

$$\mathcal{M}_\nu(t) \subseteq \left\{d \in \mathbb{Z}_{>0} : d|t,\ e^x < d \leq e^{x+1}\right\},$$

and hence $\beta_\nu(t) \leq \Delta(t)$. Now, as stated in [13] (see also [7]) a consequence of Sperner's theorem is that

$$\beta_\nu(t) \leq \Delta(t) \leq O\left(\frac{\tau(t)}{\sqrt{\omega(t)}}\right), \tag{10}$$

and if t is squarefree the constant in O-notation is equal to 2. By Theorem 317 of [8], for any $\varepsilon > 0$ there exists an integer $t_0(\varepsilon)$ such that for all $t > t_0(\varepsilon)$,

$$\tau(t) < 2^{(1+\varepsilon)\frac{\log t}{\log\log t}}. \tag{11}$$

Then combining (10) with (11), we see that for any $\varepsilon > 0$ there exists an integer $t_0(\varepsilon)$ such that for all $t > t_0(\varepsilon)$,

$$\beta_\nu(t) \leq O\left(t^{\frac{(1+\varepsilon)\log 2}{\log\log t}}\right), \tag{12}$$

which is much better than $O(\sqrt{t})$, the bound of (9), when t is sufficiently large. In fact, for most t we expect $\beta_\nu(t)$ to be even much smaller. A result of [13] states that if $\psi(t)$ is any function such that $\psi(t) \to \infty$, as slowly as we wish, as $t \to \infty$, then

$$\beta_\nu(t) \leq \Delta(t) < \psi(t)\log\log t \tag{13}$$

for all positive integers t in a sequence of asymptotic density 1.

The function $\beta_\nu(t)$ also has a geometric interpretation. Write the prime decomposition for t as

$$t = p_1^{e_1} \dots p_{\omega(t)}^{e_{\omega(t)}}$$

for corresponding distinct primes $p_1, \dots, p_{\omega(t)}$ and positive integers $e_1, \dots, e_{\omega(t)}$. If d is a divisor of t, then

$$d = p_1^{x_1} \dots p_{\omega(t)}^{x_{\omega(t)}}$$

for some integers $0 \leq x_i \leq e_i$ for each $1 \leq i \leq \omega(t)$. Then $\frac{\sqrt{t}}{\nu} \leq d \leq \sqrt{t}$ if and only if

$$\log\frac{\sqrt{t}}{\nu} \leq \sum_{i=1}^{\omega(t)} x_i \log p_i \leq \log\sqrt{t}.$$

In other words, $\beta_\nu(t)$ is precisely the number of integer lattice points in the polytope $P_\nu(t)$ in $\mathbb{R}^{\omega(t)}$ bounded by the hyperplanes

$$x_i = 0,\ x_i = e_i\ \forall\ 1 \le i \le \omega(t),\ \sum_{i=1}^{\omega(t)} x_i = \log\frac{\sqrt{t}}{\nu},\ \sum_{i=1}^{\omega(t)} x_i = \log\sqrt{t}. \tag{14}$$

In other words, $\beta_\nu(t) = \left|P_\nu(t) \cap \mathbb{Z}^{\omega(t)}\right|$, and $P_\nu(t)$ may be an irrational polytope. Counting integer lattice points in irrational polytopes is a very hard problem; a generating function for this problem is defined in [3], but almost nothing seems to be known about it.

3. Parametrization of well-rounded lattices

In this section we present an explicit description and a convenient parametrization of lattices in $\mathrm{WR}(\mathbb{Z}^2)$, which we later use to prove the main results of this paper.

First we introduce some additional notation, following [17]. An ordered collection of linearly independent vectors $\{\boldsymbol{x}_1, \dots, \boldsymbol{x}_k\} \subset \mathbb{R}^N$, $2 \le k \le N$, is called *nearly orthogonal* if for each $1 < i \le k$ the angle between $\boldsymbol{x}_i$ and the subspace of $\mathbb{R}^N$ spanned by $\boldsymbol{x}_1, \dots, \boldsymbol{x}_{i-1}$ is in the interval $\left[\frac{\pi}{3}, \frac{2\pi}{3}\right]$. In other words, this condition means that for each $1 < i \le k$

$$\frac{|\boldsymbol{x}_i^t \boldsymbol{y}|}{\|\boldsymbol{x}_i\|\|\boldsymbol{y}\|} \le \frac{1}{2}, \tag{15}$$

for all non-zero vectors $\boldsymbol{y} \in \mathrm{span}_{\mathbb{R}}\{\boldsymbol{x}_1, \dots, \boldsymbol{x}_{i-1}\}$. The following result is Theorem 1 of [17]; in case $N = 2$ this was proved by Gauss.

Theorem 3.1 ([17])**.** *Suppose that an ordered basis $\{\boldsymbol{x}_1, \dots, \boldsymbol{x}_k\}$ for a lattice Λ in $\mathbb{R}^N$ of rank $1 < k \le N$ is nearly orthogonal. Then it contains a minimal vector of Λ.*

In particular, if all vectors $\boldsymbol{x}_1, \dots, \boldsymbol{x}_k$ of Theorem 3.1 have the same norm, then Λ is a WR lattice; we will call such a basis $\boldsymbol{x}_1, \dots, \boldsymbol{x}_k$ minimal.

For the rest of this paper we will restrict to the case $N = 2$. Here is a first characterization of WR sublattices of $\mathbb{Z}^2$.

Lemma 3.2. *A sublattice $\Lambda \subseteq \mathbb{Z}^2$ of rank 2 is in $\mathrm{WR}(\mathbb{Z}^2)$ if and only if it has a basis $\boldsymbol{x}, \boldsymbol{y}$ with*

$$\|\boldsymbol{x}\| = \|\boldsymbol{y}\|,\ |\cos\theta| = \frac{|\boldsymbol{x}^t\boldsymbol{y}|}{\|\boldsymbol{x}\|\|\boldsymbol{y}\|} \le \frac{1}{2}, \tag{16}$$

where θ is the angle between $\boldsymbol{x}$ and $\boldsymbol{y}$. Moreover, if this is the case, then the set of minimal vectors $S(\Lambda) = \{\pm\boldsymbol{x}, \pm\boldsymbol{y}\}$. In particular, a minimal basis for Λ is unique up to $\pm$ signs and reordering.

Proof. Suppose first that Λ contains a basis $\boldsymbol{x}, \boldsymbol{y}$ satisfying (16). By Theorem 3.1 this must be a minimal basis, meaning that Λ is WR.

Next assume that Λ is WR, and let $\boldsymbol{x}, \boldsymbol{y} \in S(\Lambda)$ be linearly independent vectors. It is a well known fact that for lattices of rank ≤ 4 linearly independent minimal vectors form a basis, hence $\boldsymbol{x}, \boldsymbol{y}$ is a basis for Λ, and $|\Lambda| = \|\boldsymbol{x}\| = \|\boldsymbol{y}\|$. Let θ be the

angle between $\boldsymbol{x}$ and $\boldsymbol{y}$. We can assume without loss of generality that $\cos\theta > 0$: if not, replace $\boldsymbol{x}$ with $-\boldsymbol{x}$ or $\boldsymbol{y}$ with $-\boldsymbol{y}$. Notice that $\mathbf{0} \neq \boldsymbol{x} - \boldsymbol{y} \in \Lambda$, and

$$\|\boldsymbol{x} - \boldsymbol{y}\| = \sqrt{\|\boldsymbol{x}\|^2 + \|\boldsymbol{y}\|^2 - 2\boldsymbol{x}^t\boldsymbol{y}} = |\Lambda|\sqrt{2(1-\cos\theta)}.$$

If $\cos\theta > \frac{1}{2}$, then $\|\boldsymbol{x} - \boldsymbol{y}\| < |\Lambda|$, which is a contradiction. This proves (16), and also implies that the angle between two minimal linearly independent vectors in Λ must lie in the interval $\left[\frac{\pi}{3}, \frac{2\pi}{3}\right]$.

Now assume that $\Lambda \in \mathrm{WR}(\mathbb{Z}^2)$, and let $\boldsymbol{x}, \boldsymbol{y}$ be a minimal basis for Λ, so $|\Lambda| = \|\boldsymbol{x}\| = \|\boldsymbol{y}\|$. Let

$$\theta_1, \theta_2, \theta_3, \theta_4$$

be angles between pairs of vectors $\{\boldsymbol{x}, \boldsymbol{y}\}$, $\{\boldsymbol{y}, -\boldsymbol{x}\}$, $\{-\boldsymbol{x}, -\boldsymbol{y}\}$, and $\{-\boldsymbol{y}, \boldsymbol{x}\}$ respectively. Since all of these vectors are in Λ and have length $|\Lambda|$, it must be true that

$$\theta_1, \theta_2, \theta_3, \theta_4 \in \left[\frac{\pi}{3}, \frac{2\pi}{3}\right].$$

On the other hand,

$$\theta_2 = \theta_4 = \pi - \theta_1, \ \theta_3 = \theta_1.$$

Assume there exists a vector $\boldsymbol{z} \in \Lambda$ of length $|\Lambda|$ which is not equal to $\pm\boldsymbol{x}, \pm\boldsymbol{y}$. Then all the angles it makes with the vectors $\pm\boldsymbol{x}, \pm\boldsymbol{y}$ must lie in the interval $\left[\frac{\pi}{3}, \frac{2\pi}{3}\right]$. This means that at least one of these angles must be equal to $\frac{\pi}{3}$, assume without loss of generality that this is the angle $\boldsymbol{z}$ makes with $\boldsymbol{x}$. Then

$$\boldsymbol{z} = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{\pi}{3}\right) & -\sin\left(\frac{\pi}{3}\right) \\ \sin\left(\frac{\pi}{3}\right) & \cos\left(\frac{\pi}{3}\right) \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \frac{x_1}{2} - \frac{x_2\sqrt{3}}{2} \\ \frac{x_1\sqrt{3}}{2} + \frac{x_2}{2} \end{pmatrix},$$

where $x_1, x_2 \in \mathbb{Z}$ are coordinates of $\boldsymbol{x}$. Since $\boldsymbol{z} \in \Lambda$, it must be true that $z_1, z_2 \in \mathbb{Z}$, but this is not possible. Hence a vector $\boldsymbol{z}$ like this cannot exist, and this completes the proof. □

Next we develop a certain convenient explicit parametrization of lattices in $\mathrm{WR}(\mathbb{Z}^2)$. We start with lemmas describing two different families of such lattices.

Lemma 3.3. *Let $a, b, c, d \in \mathbb{Z}$ be such that*

$$0 < |d| \leq |c| \leq \sqrt{3}|d|, \ \max\{|a|, |b|\} > 0. \tag{17}$$

Then

$$\Lambda = \begin{pmatrix} ac + bd & ac - bd \\ bc - ad & bc + ad \end{pmatrix} \mathbb{Z}^2 \tag{18}$$

is in $\mathrm{WR}(\mathbb{Z}^2)$ *with*

$$\det(\Lambda) = 2(a^2 + b^2)|cd|. \tag{19}$$

Proof. Suppose $a, b, c, d \in \mathbb{Z}$ satisfy (17). Let $\boldsymbol{x} = \begin{pmatrix} ac + bd \\ bc - ad \end{pmatrix}$ and $\boldsymbol{y} = \begin{pmatrix} ac - bd \\ bc + ad \end{pmatrix}$, then

$$\begin{aligned} \|\boldsymbol{x}\|^2 &= (ac + bd)^2 + (bc - ad)^2 \\ &= (a^2 + b^2)(c^2 + d^2) \\ &= (ac - bd)^2 + (bc + ad)^2 = \|\boldsymbol{y}\|^2. \end{aligned} \tag{20}$$

Let $\Lambda = \operatorname{span}_{\mathbb{Z}}\{\boldsymbol{x}, \boldsymbol{y}\}$, then $\operatorname{rk}\Lambda = 2$. Let θ be the angle between $\boldsymbol{x}$ and $\boldsymbol{y}$, and let $c = \gamma d$, where by (17), $1 \le |\gamma| \le \sqrt{3}$. Then, by (20) and (17)

$$\begin{aligned} |\cos(\theta)| &= \frac{|\boldsymbol{x}^t\boldsymbol{y}|}{\|\boldsymbol{x}\|\|\boldsymbol{y}\|} = \frac{|(a^2+b^2)(c^2-d^2)|}{(a^2+b^2)(c^2+d^2)} \\ &= \frac{c^2-d^2}{c^2+d^2} = \frac{\gamma^2-1}{\gamma^2+1} \le \frac{1}{2}. \end{aligned}$$

Therefore $\theta \in \left[\frac{\pi}{3}, \frac{2\pi}{3}\right]$, and so, by Lemma 3.2, Λ is WR; (19) follows. This completes the proof. □

Lemma 3.4. *Let $a, b, c, d \in \mathbb{Z}$ be such that*

$$c^2 + d^2 \ge 4|cd|, \ \max\{|a|, |b|\} > 0. \tag{21}$$

Then

$$\Lambda = \begin{pmatrix} ac-bd & ad-bc \\ ad+bc & ac+bd \end{pmatrix} \mathbb{Z}^2 \tag{22}$$

is in $\mathrm{WR}(\mathbb{Z}^2)$ *with*

$$\det(\Lambda) = (a^2+b^2)|c^2-d^2|. \tag{23}$$

Proof. Suppose $a, b, c, d \in \mathbb{Z}$ satisfy (21). Let $\boldsymbol{x} = \begin{pmatrix} ac-bd \\ ad+bc \end{pmatrix}$ and $\boldsymbol{y} = \begin{pmatrix} ad-bc \\ ac+bd \end{pmatrix}$, and define $\Lambda = \operatorname{span}_{\mathbb{Z}}\{\boldsymbol{x}, \boldsymbol{y}\}$. Then $\operatorname{rk}\Lambda = 2$, and $\|\boldsymbol{x}\|, \|\boldsymbol{y}\|$ are the same as in (20). Let θ be the angle between $\boldsymbol{x}$ and $\boldsymbol{y}$. Then, by (20) and (21)

$$\begin{aligned} |\cos(\theta)| &= \frac{|\boldsymbol{x}^t\boldsymbol{y}|}{\|\boldsymbol{x}\|\|\boldsymbol{y}\|} = \frac{2|cd|(a^2+b^2)}{(a^2+b^2)(c^2+d^2)} \\ &= \frac{2|cd|}{c^2+d^2} \le \frac{1}{2}. \end{aligned}$$

Therefore $\theta \in \left[\frac{\pi}{3}, \frac{2\pi}{3}\right]$, and so, by Lemma 3.2, Λ is WR; (23) follows. This completes the proof. □

Proposition 3.5. *Suppose $\Lambda \in \mathrm{WR}(\mathbb{Z}^2)$. Then Λ is either of the form as described in Lemma 3.3 or as in Lemma 3.4.*

Proof. Suppose $\Lambda \in \mathrm{WR}(\mathbb{Z}^2)$, and let $\boldsymbol{x}, \boldsymbol{y} \in \Lambda$ be a minimal basis

$$\|\boldsymbol{x}\|^2 = x_1^2 + x_2^2 = |\Lambda|^2 = y_1^2 + y_2^2 = \|\boldsymbol{y}\|^2. \tag{24}$$

Notice that due to (24) it must be true that either the pairs x_1, y_1 and x_2, y_2, or the pairs x_1, y_2 and x_2, y_1 are of the same parity. Indeed, suppose this is not true, then we can assume without loss of generality that x_1, x_2 are even and y_1, y_2 are odd. But then

$$x_1^2 + x_2^2 \equiv 0 \pmod 4, \ y_1^2 + y_2^2 \equiv 2 \pmod 4,$$

which contradicts (24). Therefore, either

$$\frac{x_1-y_1}{2}, \ \frac{x_1+y_1}{2}, \ \frac{y_2-x_2}{2}, \ \frac{x_2+y_2}{2} \in \mathbb{Z}, \tag{25}$$

or

$$\frac{x_1-y_2}{2}, \ \frac{x_1+y_2}{2}, \ \frac{y_1-x_2}{2}, \ \frac{x_2+y_1}{2} \in \mathbb{Z}. \tag{26}$$

First assume (25) is true. Then let

$$c = \gcd\left(\frac{x_1+y_1}{2}, \frac{x_2+y_2}{2}\right), \ a = \frac{x_1+y_1}{2c}, \ b = \frac{x_2+y_2}{2c}, \ d = \frac{(y_2-x_2)c}{x_1+y_1}. \tag{27}$$

Clearly $a, b, c \in \mathbb{Z}$. We will now show that $d \in \mathbb{Z}$. Indeed,

$$d = \frac{(y_2-x_2)c}{x_1+y_1} = \frac{y_2^2-x_2^2}{(x_2+y_2)\left(\frac{x_1+y_1}{c}\right)},$$

and of course $(x_2+y_2) \mid (y_2^2-x_2^2)$. Also, by (24)

$$\left(\frac{x_1+y_1}{c}\right) \mid (x_1+y_1) \mid (x_1^2-y_1^2) = (y_2^2-x_2^2),$$

and by definition of c in (27),

$$\gcd\left(x_2+y_2, \ \frac{x_1+y_1}{c}\right) = 1,$$

which implies that

$$(x_2+y_2)\left(\frac{x_1+y_1}{c}\right) \mid (y_2^2-x_2^2),$$

and hence $d \in \mathbb{Z}$. With these definitions of a, b, c, d, it is easy to see that

$$x_1 = ac+bd, \ x_2 = bc-ad, \ y_1 = ac-bd, \ y_2 = bc+ad,$$

and hence Λ is precisely of the form (18). Moreover, since it is WR, Lemma 3.2 implies that it must satisfy condition (16), which implies (17). This finishes the proof in case (25) is true. The proof in case (26) is true is completely analogous, in which case Λ is of type (22), and then (21) is satisfied.

□

Suppose now that a lattice

$$\Lambda = \begin{pmatrix} ac-bd & ad-bc \\ ad+bc & ac+bd \end{pmatrix} \mathbb{Z}^2$$

with

$$c^2+d^2 \geq 4|cd|, \ \max\{|a|,|b|\} > 0$$

as in Lemma 3.4, and

$$\det(\Lambda) = (a^2+b^2)|c^2-d^2|$$

is even. We will show that in this case Λ can be represented in the form as in Lemma 3.3. First assume that a^2+b^2 is even, then a^2, b^2, and hence a, b, must be of the same parity, meaning that $a+b$ and $a-b$ are even. Define

$$a_1 = \frac{a-b}{2}, \ b_1 = \frac{a+b}{2},$$

then $a^2+b^2 = 2(a_1^2+b_1^2)$. Let c_1, d_1 be such that $c_1d_1 = c^2-d^2$, and

$$|c_1| = \max\{|c-d|, |c+d|\}, \ |d_1| = \min\{|c-d|, |c+d|\}.$$

Suppose for instance that $c_1 = c+d$ and $d_1 = c-d$ (the argument is completely analogous in case $c_1 = c-d$ and $d_1 = c+d$). Then

$$c = \frac{c_1+d_1}{2}, \ d = \frac{c_1-d_1}{2},$$

and so $4cd = c_1^2 - d_1^2$. On the other hand $c^2+d^2 = \frac{c_1^2+d_1^2}{2}$. The fact that $c^2+d^2 \geq 4|cd|$ implies that

$$\frac{c_1^2+d_1^2}{2} \geq |c_1^2 - d_1^2| = c_1^2 - d_1^2,$$

since $|c_1| \geq |d_1|$, and so

$$|c_1| \leq \sqrt{3}\ |d_1|.$$

This choice of a_1, b_1, c_1, d_1 satisfies the conditions of (17), and it is easy to see that

$$\Lambda = \begin{pmatrix} ac-bd & ad-bc \\ ad+bc & ac+bd \end{pmatrix} \mathbb{Z}^2 = \begin{pmatrix} a_1c_1+b_1d_1 & a_1c_1-b_1d_1 \\ b_1c_1-a_1d_1 & b_1c_1+a_1d_1 \end{pmatrix} \mathbb{Z}^2, \tag{28}$$

and $\det(\Lambda) = 2(a_1^2+b_1^2)|c_1d_1|$.

Next assume that c^2-d^2 is even. Then $(c+d)(c-d)$ is even and $(c+d)+(c-d) = 2c$ is even, which implies that $(c+d)$ and $(c-d)$ must both be even, in particular c^2-d^2 is divisible by 4. Let c_1, d_1 be such that $4c_1d_1 = c^2-d^2$, and

$$|c_1| = \frac{1}{2}\max\{|c-d|, |c+d|\},\ |d_1| = \frac{1}{2}\min\{|c-d|, |c+d|\}.$$

By an argument as above, we can easily deduce again that

$$|d_1| \leq |c_1| \leq \sqrt{3}\ |d_1|.$$

Let

$$a_1 = a-b,\ b_1 = a+b,$$

then $2(a^2+b^2) = a_1^2+b_1^2$, and so

$$\det(\Lambda) = (a^2+b^2)|c^2-d^2| = 4(a^2+b^2)|c_1d_1| = 2(a_1^2+b_1^2)|c_1d_1|.$$

Once again, it is easy to check that with a_1, b_1, c_1, d_1 defined this way (28) holds.

Let

$$\mathcal{E}' = \left\{(a,b,c,d) \in \mathbb{Z}^4\ :\ 0 < |d| \leq |c| \leq \sqrt{3}|d|,\ \max\{|a|,|b|\} > 0\right\}, \tag{29}$$

and

$$\begin{aligned} \mathcal{O}' = \{(a,b,c,d) \in \mathbb{Z}^4\ :\ & 0 < |d| \leq |c| \leq \sqrt{3}|d|,\ \max\{|a|,|b|\} > 0, \\ & \text{so that } 2 \nmid (a^2+b^2)|cd|\}. \end{aligned} \tag{30}$$

Define two classes of integral lattices

$$\mathcal{E} = \left\{\Lambda(a,b,c,d) = \begin{pmatrix} ac+bd & ac-bd \\ bc-ad & bc+ad \end{pmatrix} \mathbb{Z}^2 : (a,b,c,d) \in \mathcal{E}'\right\}, \tag{31}$$

and

$$\mathcal{O} = \left\{\Lambda(a,b,c,d) = \begin{pmatrix} \frac{ac+ad+bd-bc}{2} & \frac{ac-ad-bc-bd}{2} \\ \frac{ac+bc+bd-ad}{2} & \frac{ac+ad+bc-bd}{2} \end{pmatrix} \mathbb{Z}^2 : (a,b,c,d) \in \mathcal{O}'\right\}. \tag{32}$$

Then for every $\Lambda = \Lambda(a,b,c,d) \in \mathcal{E}$,

$$\det(\Lambda) = 2(a^2+b^2)|cd|,$$

is even, and for every $\Lambda = \Lambda(a,b,c,d) \in \mathcal{O}$,

$$\det(\Lambda) = (a^2+b^2)|cd|$$

is odd. We proved the following theorem.

Theorem 3.6. *The set* $\mathrm{WR}(\mathbb{Z}^2)$ *can be represented as the disjoint union of* $\mathcal{E}$ *and* $\mathcal{O}$*. Moreover, the set of all possible determinants of lattices in* $\mathrm{WR}(\mathbb{Z}^2) = \mathcal{E} \cup \mathcal{O}$ *is*

$$\mathcal{D} = \{(a^2+b^2)|cd| : a,b,c,d \in \mathbb{Z},\ 0 < \max\{|a|,|b|\},\ 0 < |d| \le |c| \le \sqrt{3}|d|\}. \tag{33}$$

Remark 3.1. Notice also that

$$|\Lambda|^2 = \begin{cases} (a^2+b^2)(c^2+d^2) & \text{if } \Lambda \in \mathcal{E} \\ \frac{1}{2}(a^2+b^2)(c^2+d^2) & \text{if } \Lambda \in \mathcal{O}. \end{cases}$$

Therefore the set of squared minima $\mathfrak{M}(\mathcal{E})$ of the lattices from $\mathcal{E}$ can be represented as

$$\begin{aligned} \mathfrak{M}(\mathcal{E}) = \{(a^2+b^2)(c^2+d^2) \quad : \quad & a,b,c,d \in \mathbb{Z},\ 0 < \max\{|a|,|b|\}, \\ & 0 < |d| \le |c| \le \sqrt{3}|d},\ 2|(a^2+b^2)cd\}, \end{aligned} \tag{34}$$

and the set of squared minima $\mathfrak{M}(\mathcal{O})$ of the lattices from $\mathcal{O}$ can be represented as

$$\begin{aligned} \mathfrak{M}(\mathcal{O}) = \left\{\frac{1}{2}(a^2+b^2)(c^2+d^2) \quad : \quad & a,b,c,d \in \mathbb{Z},\ 0 < \max\{|a|,|b|\}, \\ & 0 < |d| \le |c| \le \sqrt{3}|d},\ 2 \nmid (a^2+b^2)cd\right\}. \end{aligned} \tag{35}$$

Then the set of squared minima $\mathfrak{M}$ can be represented as $\mathfrak{M} = \mathfrak{M}(\mathcal{E}) \cup \mathfrak{M}(\mathcal{O})$.

Corollary 3.7. *The determinant set* $\mathcal{D}$ *in (33) and the squared minima set* $\mathfrak{M}$ *are commutative monoids under multiplication.*

Proof. If $t_1 = (a_1^2+b_1^2)c_1d_1$ and $t_2 = (a_2^2+b_2^2)c_2d_2$ are in $\mathcal{D}$, then $t_1t_2 = (a_3^2+b_3^2)c_3d_3 \in \mathcal{D}$, where $a_3 = a_1a_2+b_1b_2$, $b_3 = b_1a_2 - a_1b_2$, $c_3 = \pm\max\{|c_1d_2|,|d_1c_2|\}$, and $d_3 = \pm\min\{|c_1d_2|,|d_1c_2|\}$. It is also obvious that a product of two integers which are representable as sums of two squares is also representable as a sum of two squares. □

Next we will use Theorem 3.6 to investigate the structure of the set $\mathcal{D}$ and to count the number of lattices in $\mathrm{WR}(\mathbb{Z}^2)$ of a fixed determinant.

4. Proof of Theorem 1.2

The description of the set $\mathcal{D}$ in the statement of Theorem 1.2 follows immediately from (33). In this section we will mostly be concerned with deriving the estimate (1) for the lower density of $\mathcal{D}$.

For each real number $1 < \nu \le 3^{1/4}$, define the set

$$\mathcal{B}_\nu = \left\{n \in \mathbb{Z}_{>0} : \exists\ d \in \mathbb{Z}_{>0} \text{ such that } d \mid n \text{ and } \frac{\sqrt{n}}{\nu} \le d \le \sqrt{n}\right\}. \tag{36}$$

Then notice that another description of the set $\mathcal{D}$ in (33) is

$$\mathcal{D} = \mathfrak{M}\mathcal{B}_{3^{1/4}} = \{mn : m \in \mathfrak{M},\ n \in \mathcal{B}_{3^{1/4}}\},$$

where $\mathfrak{M}$ is the set of squared minima of lattices in $\mathrm{WR}(\mathbb{Z}^2)$, as before, so

$$\mathfrak{M} = \{m \in \mathbb{Z}_{>0} : m = k^2+l^2 \text{ for some } k,l \in \mathbb{Z}\}. \tag{37}$$

By a well known theorem of Fermat, the set $\mathfrak{M}$ consists precisely of those positive integers m in whose prime factorization every prime of the form $(4k+3)$ occurs an even number of times. Since $1 \in \mathfrak{M} \cap \mathcal{B}_{3^{1/4}}$, we have $\mathfrak{M}, \mathcal{B}_{3^{1/4}} \subset \mathcal{D}$; on the other

hand, $6 \in \mathcal{B}_{3^{1/4}} \setminus \mathfrak{M}$ and $2 \in \mathfrak{M} \setminus \mathcal{B}_{3^{1/4}}$, hence $\mathfrak{M} \subsetneq \mathcal{D}$ and $\mathcal{B}_{3^{1/4}} \subsetneq \mathcal{D}$. Moreover, $\mathcal{D} \subsetneq \mathbb{Z}_{>0}$, since for instance $3 \notin \mathcal{D}$.

It is a well-known result of Landau (see, for instance [16]) that $\mathfrak{M}$ has asymptotic density equal to 0, specifically

$$\lim_{M\to\infty} \frac{1}{M} \left|\{n \in \mathfrak{M} : n \le M\}\right| = \lim_{M\to\infty} \frac{1}{\sqrt{\log M}} = 0.$$

Let us investigate the density of the sets $\mathcal{B}_\nu$ for a fixed $\nu \in (1, 3^{1/4}]$. As before, for each $M \in \mathbb{Z}_{>0}$ we write

$$\mathcal{B}_\nu(M) = \{n \in \mathcal{B}_\nu : n \le M\}.$$

For each $n \in \mathbb{Z}_{>0}$ define

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

Notice that every $k \in \mathcal{B}_\nu(M)$ is of the form $k = n(n-i)$ for some n and $i \le \left[\left(\frac{\nu-1}{\nu}\right) n\right]$, and so if $n \le [\sqrt{M}]$, then $k \in \bigcup_{n=1}^{[\sqrt{M}]} I_\nu(n)$. For each $n \in \mathbb{Z}_{>0}$,

$$|I_\nu(n)| = \left[\left(\frac{\nu-1}{\nu}\right) n\right] + 1. \tag{38}$$

There may also be some $k = n(n-i) \in \mathcal{B}_\nu(M)$ with $n > [\sqrt{M}]$ for some $i \le \left(\frac{\nu-1}{\nu}\right) n$. Then $k = n^2 - ni \le M$, and so $i \ge n - \frac{M}{n}$. It is easy to see that this is only possible if $n \le \left[\sqrt{\nu M}\right]$, and so for each $[\sqrt{M}] < n \le \left[\sqrt{\nu M}\right]$ define

$$J_{\nu,M}(n) = \left\{n(n-i) : \left[n - \frac{M}{n}\right] + 1 \le i \le \left[\left(\frac{\nu-1}{\nu}\right) n\right]\right\}.$$

Clearly, $J_{\nu,M}(n) \subseteq I_\nu(n)$ for each such n, and

$$\mathcal{B}_\nu(M) = \left(\bigcup_{n=1}^{[\sqrt{M}]} I_\nu(n)\right) \cup \left(\bigcup_{n=[\sqrt{M}]+1}^{[\sqrt{\nu M}]} J_{\nu,M}(n)\right). \tag{39}$$

For simplicity of approximation notice that

$$\bigcup_{n=1}^{[\sqrt{M}]} I_\nu(n) \subseteq \mathcal{B}_\nu(M) \subseteq \bigcup_{n=1}^{[\sqrt{\nu M}]} I_\nu(n). \tag{40}$$

We immediately obtain an upper bound on $|\mathcal{B}_\nu(M)|$.

Lemma 4.1. *For all $M \in \mathbb{Z}_{>0}$,*

$$|\mathcal{B}_\nu(M)| \le \frac{\nu-1}{2}\, M + \frac{\nu-1}{2\sqrt{\nu}}\, \sqrt{M}. \tag{41}$$

Proof. Combining (40) and (38), we obtain:

$$|\mathcal{B}_\nu(M)| \le \sum_{n=1}^{[\sqrt{\nu M}]} |I_\nu(n)| \le \frac{\nu-1}{\nu} \sum_{n=1}^{[\sqrt{\nu M}]} n \le \frac{\nu-1}{2\nu}\sqrt{\nu M}\left(\sqrt{\nu M} + 1\right).$$

The bound of (41) follows. □

Next we want to produce a lower bound on $|\mathcal{B}_\nu(M)|$. For this we first consider the pairwise intersections of the sets $I_\nu(n)$.

Lemma 4.2. *Let $m < n \leq [\sqrt{M}]$.*

(1) If $n > m\sqrt{\nu}$, or if $n \geq m\sqrt{\nu}$ and $\sqrt{\nu}$ is irrational, then $I_\nu(n) \cap I_\nu(m) = \emptyset$.
(2) If $\gcd(m,n) = 1$, then $I_\nu(n) \cap I_\nu(m) = \emptyset$.
(3) If $m < n < m\sqrt{\nu}$, then

$$|I_\nu(n) \cap I_\nu(m)| \leq \left[\frac{\nu - 1}{\nu} \ \gcd(m,n)\right] + 1.$$

Proof. Define $Q = \frac{\nu-1}{\nu}$. Let $m < n \leq [\sqrt{M}]$, and suppose that $k \in I_\nu(n) \cap I_\nu(m)$. Then

$$k = n(n-x) = m(m-y),$$

for some integers $0 \leq x \leq Qn$ and $0 \leq y \leq Qm$. Define a line

$$L(n,m) = \{(x,y) \in \mathbb{R}^2 : nx - my = n^2 - m^2\},$$

and a rectangular box

$$R(n,m) = \{(x,y) \in \mathbb{R}^2 : 0 \leq x \leq Qn, \ 0 \leq y \leq Qm\}.$$

It follows immediately that

$$|I_\nu(n) \cap I_\nu(m)| = |L(n,m) \cap R(n,m) \cap \mathbb{Z}^2|.$$

The line $L(m,n)$ passes through the points $\left(\frac{n^2-m^2}{n}, 0\right)$ and $\left(0, -\frac{n^2-m^2}{n}\right)$, so in particular $L(n,m) \cap R(n,m) = \emptyset$ if $\frac{n^2-m^2}{n} > Qn$, i.e. if $n > m\sqrt{\nu}$. Also if $\sqrt{\nu}$ is irrational, then $m\sqrt{\nu}$ is never an integer, and so $I_\nu(n) \cap I_\nu(m) = \emptyset$ if $n \geq m\sqrt{\nu}$, proving (1).

Now suppose $m < n < m\sqrt{\nu}$, and let $(x,y) \in L(n,m) \cap R(n,m) \cap \mathbb{Z}^2$. Then

$$y = -\frac{n(n-x)}{m} + m \in \mathbb{Z}_{>0},$$

hence $m \mid n(n-x)$. Clearly, $m \nmid n$, and so we must have

$$\operatorname{lcm}(m,n) = \frac{mn}{\gcd(m,n)} \mid n(n-x),$$

meaning that

$$\frac{m}{\gcd(m,n)} \mid n - x. \tag{42}$$

In particular, if $\gcd(m,n) = 1$, we must have $m \mid n - x$, but $n - x \leq n < 2m$, meaning that in order for $n - x$ to be divisible by m, it must be equal to m. This would imply that $x = n - m < \frac{n^2-m^2}{n}$, hence $y < 0$, meaning that $(x,y) \notin R(n,m)$, which is a contradiction. This proves (2).

Now assume that $(x_1, y_1), (x_1+t, y_2) \in L(n,m) \cap R(n,m) \cap \mathbb{Z}^2$, where t is as small as possible. By (42), $\frac{m}{\gcd(m,n)} \mid n - x_1$ and $\frac{m}{\gcd(m,n)} \mid n - x_1 - t$, so $\frac{m}{\gcd(m,n)} \mid t$, and by minimality of t we must have $t = \frac{m}{\gcd(m,n)}$. Therefore x-coordinates of points in $L(n,m) \cap R(n,m) \cap \mathbb{Z}^2$ must satisfy

$$\frac{n^2 - m^2}{n} \leq x < Qn,$$

and the distance between x-coordinates of any two such points must be at least $\frac{m}{\gcd(m,n)}$. Hence,

$$\begin{aligned} |I_\nu(n) \cap I_\nu(m)| &= |L(n,m) \cap R(n,m) \cap \mathbb{Z}^2| \leq \left[\frac{Qn - \frac{n^2-m^2}{n}}{\frac{m}{\gcd(m,n)}} \right] + 1 \\ &= \left[\frac{(\nu m^2 - n^2)\gcd(m,n)}{\nu m n} \right] + 1 \leq \left[\frac{\nu-1}{\nu} \ \gcd(m,n) \right] + 1. \end{aligned}$$

This proves (3). □

Lemma 4.3. *For all $M \in \mathbb{Z}_{>0}$,*

$$|\mathcal{B}_\nu(M)| > \frac{\nu-1}{2\nu} \ M \left(1 - \frac{\log\log\sqrt{M}}{\log\sqrt{M}} \right)^2. \tag{43}$$

Proof. Let $N = \pi(\sqrt{M})$, i.e. the number of primes up to $\sqrt{M}$. It is a well-known fact that for all $\sqrt{M} \geq 11$,

$$N \geq \frac{\sqrt{M}}{\log\sqrt{M}}. \tag{44}$$

Hence suppose that $M \geq 121$, and let $p_1, \ldots, p_N$ be all the primes up to $\sqrt{M}$ in ascending order. By part (2) of Lemma 4.2,

$$I_\nu(p_i) \cap I_\nu(p_j) = \emptyset,$$

for all $1 \leq i \neq j \leq N$. As above, we let $Q = \frac{\nu-1}{\nu}$. Therefore, using (38) we obtain:

$$|\mathcal{B}_\nu(M)| \geq \sum_{i=1}^{N} |I_\nu(p_i)| \geq Q \sum_{i=1}^{N} p_i. \tag{45}$$

A result of R. Jakimczuk [9] implies that

$$\sum_{i=1}^{N} p_i > \frac{N^2}{2} \ \log^2 N. \tag{46}$$

The bound (43) follows upon combining (45) with (46) and (44).

Now assume that $M < 121$, so $\sqrt{M} < 11$. A direct verification shows that in this case $I_\nu(n) \cap I_\nu(m) = \emptyset$ for all $1 \leq n \neq m \leq [\sqrt{M}]$, and so

$$|\mathcal{B}_\nu(M)| \geq \sum_{n=1}^{[\sqrt{M}]} |I_\nu(n)| \geq Q \sum_{n=1}^{[\sqrt{M}]} n \geq \frac{\nu-1}{2\nu} \ M.$$

This completes the proof. □

Combining Lemmas 4.1 and 4.3, we obtain the following result.

Theorem 4.4.

$$\frac{\nu-1}{2\nu} \leq \underline{\Delta}_{\mathcal{B}_\nu} \leq \overline{\Delta}_{\mathcal{B}_\nu} \leq \frac{\nu-1}{2}.$$

Proof. Using (43), we see that

$$\underline{\Delta}_{\mathcal{B}_\nu} = \liminf_{M\to\infty} \frac{|\mathcal{B}_\nu(M)|}{M} \geq \frac{\nu-1}{2\nu} \lim_{M\to\infty} \left(1 - \frac{\log\log\sqrt{M}}{\log\sqrt{M}} \right)^2 = \frac{\nu-1}{2\nu},$$

and using (41), we see that

$$\overline{\Delta}_{\mathcal{B}_\nu} = \limsup_{M\to\infty} \frac{|\mathcal{B}_\nu(M)|}{M} \leq \frac{\nu-1}{2} + \frac{\nu-1}{2\sqrt{\nu}} \lim_{M\to\infty} \frac{1}{\sqrt{M}} = \frac{\nu-1}{2}.$$

This completes the proof. □

Remark 4.1. It is also possible to produce bounds on $|\mathcal{B}_\nu(M)|$ using decomposition (39) instead of (40), and employing the fact that

$$|J_{\nu,M}(n)| = \left[\left(\frac{\nu-1}{\nu}\right)n\right] - \left[n - \frac{M}{n}\right].$$

It is also possible to employ the full power of Lemma 4.2, in particular part (3), to further refine the lower bound on $|\mathcal{B}_\nu(M)|$. These estimates however produce only marginally better constants, but much messier bounds in general.

We could also lift the restriction that $\nu \leq 3^{1/4}$ with essentially no changes to the arguments, but in any case the important situation is that with ν being close to 1, and we want to emphasize that the case of utmost importance to us is that with $\nu = 3^{1/4}$.

Now (1) of Theorem 1.2 follows immediately by recalling that $\mathcal{B}_{3^{1/4}} \subseteq \mathcal{D}$, and applying Theorem 4.4 with $\nu = 3^{1/4}$. The bounds on density of $\mathcal{B}_\nu$ are of independent interest, and will also be used in section 8 below to determine the order of the pole of the zeta function of well-rounded lattices.

5. Proof of Theorem 1.3

We start with a lemma which identifies all the 4-tuples from $\mathcal{E}' \cup \mathcal{O}'$ which parametrize the same lattices.

Lemma 5.1. *Let $(a_1,b_1,c_1,d_1),(a_2,b_2,c_2,d_2) \in \mathcal{E}' \cup \mathcal{O}'$. Then*

$$\Lambda(a_1,b_1,c_1,d_1) = \Lambda(a_2,b_2,c_2,d_2) \tag{47}$$

if and only if there exists $0 \neq \gamma \in \mathbb{Q}$ such that (a_1,b_1,c_1,d_1) is equal to one of the following:

$$\begin{gathered}\left(\frac{a_2}{\gamma},\frac{b_2}{\gamma},\gamma c_2,\gamma d_2\right),\ \left(\frac{b_2}{\gamma},-\frac{a_2}{\gamma},-\gamma d_2,\gamma c_2\right),\ \left(-\frac{b_2}{\gamma},\frac{a_2}{\gamma},-\gamma d_2,\gamma c_2\right),\\ \left(-\frac{a_2}{\gamma},-\frac{b_2}{\gamma},\gamma c_2,\gamma d_2\right),\ \left(-\frac{a_2}{\gamma},-\frac{b_2}{\gamma},-\gamma c_2,\gamma d_2\right),\ \left(\frac{b_2}{\gamma},-\frac{a_2}{\gamma},\gamma d_2,\gamma c_2\right),\\ \left(-\frac{b_2}{\gamma},\frac{a_2}{\gamma},\gamma d_2,\gamma c_2\right),\left(\frac{a_2}{\gamma},\frac{b_2}{\gamma},-\gamma c_2,\gamma d_2\right).\end{gathered} \tag{48}$$

Proof. If (a_1,b_1,c_1,d_1) is equal to one of the 4-tuples as in (48), then a direct verification shows that (47) is true. Suppose, on the other hand, that (47) is true. Let

$$\boldsymbol{x}_1 = \begin{pmatrix} a_1c_1+b_1d_1 \\ b_1c_1-a_1d_1\end{pmatrix},\ \boldsymbol{y}_1 = \begin{pmatrix} a_1c_1-b_1d_1 \\ b_1c_1+a_1d_1\end{pmatrix},$$

and

$$\boldsymbol{x}_2 = \begin{pmatrix} a_2c_2+b_2d_2 \\ b_2c_2-a_2d_2\end{pmatrix},\ \boldsymbol{y}_2 = \begin{pmatrix} a_2c_2-b_2d_2 \\ b_2c_2+a_2d_2\end{pmatrix},$$

if $(a_1,b_1,c_1,d_1),(a_2,b_2,c_2,d_2)\in\mathcal{E}'$, or

$$\boldsymbol{x}_1=\begin{pmatrix}\frac{a_1c_1+a_1d_1+b_1d_1-b_1c_1}{2}\\ \frac{a_1c_1+b_1c_1+b_1d_1-a_1d_1}{2}\end{pmatrix},\ \boldsymbol{y}_1=\begin{pmatrix}\frac{a_1c_1-a_1d_1-b_1c_1-b_1d_1}{2}\\ \frac{a_1c_1+a_1d_1+b_1c_1-b_1d_1}{2}\end{pmatrix},$$

and

$$\boldsymbol{x}_2=\begin{pmatrix}\frac{a_2c_2+a_2d_2+b_2d_2-b_2c_2}{2}\\ \frac{a_2c_2+b_2c_2+b_2d_2-a_2d_2}{2}\end{pmatrix},\ \boldsymbol{y}_2=\begin{pmatrix}\frac{a_2c_2-a_2d_2-b_2c_2-b_2d_2}{2}\\ \frac{a_2c_2+a_2d_2+b_2c_2-b_2d_2}{2}\end{pmatrix},$$

if $(a_1,b_1,c_1,d_1),(a_2,b_2,c_2,d_2)\in\mathcal{O}'$. By Lemma 3.2, this means that the basis matrix $(\boldsymbol{x}_1\ \boldsymbol{y}_1)$ for $\Lambda(a_1,b_1,c_1,d_1)$ must be equal to one of the following basis matrices for $\Lambda(a_2,b_2,c_2,d_2)$:

$$(\boldsymbol{x}_2\ \boldsymbol{y}_2),\ (-\boldsymbol{x}_2\ \boldsymbol{y}_2),\ (\boldsymbol{x}_2\ -\boldsymbol{y}_2),\ (-\boldsymbol{x}_2\ -\boldsymbol{y}_2),$$
$$(\boldsymbol{y}_2\ \boldsymbol{x}_2),\ (-\boldsymbol{y}_2\ \boldsymbol{x}_2),\ (\boldsymbol{y}_2\ -\boldsymbol{x}_2),\ (-\boldsymbol{y}_2\ -\boldsymbol{x}_2).$$

A direct verification shows that in each of these cases (a_1,b_1,c_1,d_1) is equal to one of the 4-tuples as in (48), in the same order. This completes the proof. □

Remark 5.1. Notice that in Lemma 5.1 (a_1,b_1,c_1,d_1) can be equal to the second, third, sixth, or seventh 4-tuple in (48) only if

$$|c_1|=|\gamma||d_2|,\ |d_1|=|\gamma||c_2|,$$

but on the other hand we know that $(a_1,b_1,c_1,d_1),(a_2,b_2,c_2,d_2)\in\mathcal{E}'\cup\mathcal{O}'$. Combining these facts we obtain

$$|c_1|=|\gamma||d_2|\le|\gamma||c_2|=|d_1|\le|c_1|, \tag{49}$$

which implies that there must be equality everywhere in (49). In this case the determinant of the corresponding lattice Λ is equal to $(a_1^2+b_1^2)c_1^2$ if $\Lambda\in\mathcal{O}$ or to $2(a_1^2+b_1^2)c_1^2$ if $\Lambda\in\mathcal{E}$.

Proof of Theorem 1.3. Let $u\in\mathcal{D}$. If $u=1,2$, the proof is by direct verification. Assume from here on that $u>2$, and let

$$t=t(u)=\begin{cases}u & \text{if } u \text{ is odd}\\ \frac{u}{2} & \text{if } u \text{ is even.}\end{cases}$$

Define

$$D(t)=\{n\in\mathbb{Z}_{>0}:n|t\},$$

i.e. $D(t)$ is the set of positive divisors of t. Define

$$D_1(t)=\{(c,d)\in D(t)\times D(t):d\le c\le\sqrt{3}d,\ cd|t\}.$$

For each $(c,d)\in D_1(t)$, define

$$S_t(c,d)=\left\{(a,b)\in\mathbb{Z}_{\ge0}^2:a^2+b^2=\frac{t}{cd},\ a\le b\right\}.$$

Also let

$$T(t)=\{(a,b,c,d)\in\mathbb{Z}_{\ge0}^4:(c,d)\in D_1(t),\ (a,b)\in S_t(c,d)\}.$$

Define an equivalence relation on $T(t)$ by writing

$$(a_1,b_1,c_1,d_1)\sim(a_2,b_2,c_2,d_2)$$

if $(a_1,b_1,c_1,d_1)=\left(\frac{a_2}{\gamma},\frac{b_2}{\gamma},\gamma c_2,\gamma d_2\right)$ for some $\gamma\in\mathbb{Q}_{>0}$. Then let $T_1(t)$ be the set of all equivalence classes of elements of $T(t)$ under $\sim$, i.e. $T_1(t)=T(t)/\sim$. By

abuse of notation, we will write (a,b,c,d) for an element of $T_1(t)$. We first have the following lemma.

Lemma 5.2. *For each equivalence class in $T_1(t)$ it is possible to select a unique representative (a,b,c,d) with $\gcd(a,b)=1$.*

Proof. Let $(a,b,c,d)\in T_1(t)$, and let $q=\gcd(a,b)$, then it is easy to see that

$$(a,b,c,d)\sim\left(\frac{a}{q},\frac{b}{q},qc,qd\right).$$

Moreover, suppose that $(a_1,b_1,c_1,d_1),(a_2,b_2,c_2,d_2)\in T_1(t)$ are such that

$$\gcd(a_1,b_1)=\gcd(a_2,b_2)=1,$$

and

$$(a_1,b_1,c_1,d_1)\sim(a_2,b_2,c_2,d_2).$$

Then there exists $\gamma=\frac{s}{q}\in\mathbb{Q}_{>0}$ with $\gcd(s,q)=1$ such that

$$a_1=\frac{q}{s}a_2,\ b_1=\frac{q}{s}b_2,\ c_1=\frac{s}{q}c_2,\ d_1=\frac{s}{q}d_2.$$

Then $s|a_2$, $s|b_2$, and so $s|\gcd(a_2,b_2)=1$, hence $s=1$. Also $q|qa_2=a_1$, $q|qb_2=b_1$, and so $q|\gcd(a_1,b_1)=1$, hence $q=1$. Therefore

$$(a_1,b_1,c_1,d_1)=(a_2,b_2,c_2,d_2).$$

This completes the proof. □

Therefore, for each t we only need to count the lattices produced by the 4-tuples $(a,b,c,d)\in T_1(t)$ with $\gcd(a,b)=1$. Let (a,b,c,d) be such a 4-tuple, then either $(a,b)=(0,1)$ or $a,b,c,d\neq 0$, since $\gcd(0,b)=b$. Moreover, $a\neq b$ unless $a=b=1$.

First assume $c\neq d$. If $(a,b)\neq(0,1),(1,1)$. By Lemma 5.1 and Remark 5.1 only the following 4-tuples produce the same lattice $\Lambda(a,b,c,d)$:

$$(a,b,c,d),\ (-a,-b,-c,-d),\ (-a,-b,c,d),\ (a,b,-c,-d),$$
$$(a,b,-c,d),\ (a,b,c,-d),\ (-a,-b,-c,d),\ (-a,-b,c,-d).$$

Then each $(a,b,c,d)\in T_1(t)$ gives rise to the four distinct lattices:

$$\Lambda(a,b,c,d),\ \Lambda(-a,b,c,d),\ \Lambda(b,a,c,d),\ \Lambda(-b,a,c,d), \tag{50}$$

since $\Lambda(a,b,d,c)=\Lambda(-b,a,c,d)$. Also, each of $(0,1,c,d),(1,1,c,d),(a,b,1,1)\in T_1(t)$ gives rise to the following pairs of distinct lattices, respectively:

$$\Lambda(0,1,c,d),\ \Lambda(1,0,c,d);$$
$$\Lambda(1,1,c,d),\ \Lambda(-1,1,c,d);$$
$$\Lambda(a,b,1,1),\ \Lambda(-a,b,1,1). \tag{51}$$

Now suppose that $c=d$. Then

$$\Lambda(a,b,c,c)=\Lambda(-b,a,c,c),\ \Lambda(-a,b,c,c)=\Lambda(b,a,c,c).$$

Hence, if $(a,b)\neq(0,1),(1,1)$, then each $(a,b,c,c)\in T_1(t)$ gives rise to two distinct lattices, $\Lambda(a,b,c,c)$ and $\Lambda(b,a,c,c)$. Notice also that

$$\Lambda(0,1,c,c)=\Lambda(1,0,c,c),\ \Lambda(1,1,c,c)=\Lambda(-1,1,c,c).$$

Hence 4-tuples $(0,1,c,c),(1,1,c,c)\in T_1(t)$ give rise to only one lattice each.
The formula for $\mathcal{N}(u)$, $u\in\mathcal{D}$, of Theorem 1.3 follows. Also notice that if $u\in\mathbb{Z}_{>0}\setminus\mathcal{D}$, then for every divisor n of u, either $\alpha_*(t/n)$ or $\beta(n)$ is equal to zero, and

so the right hand side of (6) is equal to zero by construction. This completes the proof of the theorem. □

Remark 5.2. Our problem can be interpreted in terms of counting integral points on certain varieties. Let us say that two points

$$\boldsymbol{x} = (x_1, x_2, x_3, x_4)^t, \ \boldsymbol{y} = (y_1, y_2, y_3, y_4)^t \in \mathbb{R}^4$$

are equivalent if there exists $U \in GL_2(\mathbb{Z})$ such that

$$U \begin{pmatrix} x_1 & x_3 \\ x_2 & x_4 \end{pmatrix} = \begin{pmatrix} y_1 & y_3 \\ y_2 & y_4 \end{pmatrix}.$$

Notice that the number of *all* full-rank sublattices of $\mathbb{Z}^2$ with determinant equal to u is precisely the number of integral points on the hypersurface

$$x_1x_4 - x_2x_3 = u,$$

modulo this equivalence. This number is well known: one formula, for instance, is given by (52) below. On the other hand, by Lemma 3.2, the number of *well-rounded* full-rank sublattices of $\mathbb{Z}^2$ with determinant equal to u is the number of integral points on the subset of the variety

$$x_1x_4 - x_2x_3 = u, \ x_1^2 + x_2^2 - x_3^2 - x_4^2 = 0,$$

defined by the inequality

$$2|x_1x_3 + x_2x_4| \leq x_1^2 + x_2^2,$$

modulo the same equivalence. This makes direct counting much harder, and so our parametrization is quite useful.

6. Corollaries

The first immediate consequence of Theorem 1.3 is the following.

Corollary 6.1. *If $u \in \mathbb{Z}_{>0}$ is odd, then $\mathcal{N}(u) = \mathcal{N}(2u)$.*

To demonstrate some examples of our formulas at work, we derive the following simpler looking expressions for the case of prime-power determinants.

Corollary 6.2. *Let p be a prime, $k \in \mathbb{Z}_{>0}$. Let $u = p^k$ or $2p^k$. Then*

$$\mathcal{N}(u) = \begin{cases} 0 & \text{if } p \equiv 3 \pmod 4 \text{ and } k \text{ is odd} \\ 1 & \text{if } p \equiv 3 \pmod 4 \text{ and } k \text{ is even} \\ 1 & \text{if } p = 2 \\ k+1 & \text{if } p \equiv 1 \pmod 4 \end{cases}$$

Proof. First assume that $p \neq 2$. Define t as in the statement of Theorem 1.3, then $t = p^k$. If k is even, then by Theorem 1.3

$$\begin{aligned} \mathcal{N}(u) &= \beta(p^k) + 4\sum_{j=1}^{\frac{k}{2}} \alpha_*(p^{k+1-2j})\beta(p^{2j-1}) + 2\sum_{j=0}^{\frac{k}{2}-1} \alpha_*(p^{k-2j})(2\beta(p^{2j}) - 1) \\ &= 1 + 2\sum_{j=0}^{\frac{k}{2}-1} \alpha_*(p^{k-2j}), \end{aligned}$$

since $\beta(p^{2j-1}) = 0$, and $\beta(p^{2j}) = 1$ for all j. If $p \equiv 3 \pmod 4$, then $\alpha_*(p^{k-2j}) = 0$ for all j. If $p \equiv 1 \pmod 4$, then $\alpha_*(p^{k-2j}) = 1$ for all j, in which case

$$\mathcal{N}(u) = 1 + 2\sum_{j=0}^{\frac{k}{2}-1} 1 = k+1.$$

Next assume $k > 1$ is odd. Then, in the same manner as above,

$$\begin{aligned}\mathcal{N}(u) &= 2\beta(p^k) + 4\sum_{j=1}^{\frac{k-1}{2}} \alpha_*(p^{k+1-2j})\beta(p^{2j-1}) + 2\sum_{j=0}^{\frac{k-1}{2}} \alpha_*(p^{k-2j})(2\beta(p^{2j})-1) \\ &= 2\sum_{j=0}^{\frac{k-1}{2}} \alpha_*(p^{k-2j}),\end{aligned}$$

which is equal to 0 if $p \equiv 3 \pmod 4$. If $p \equiv 1 \pmod 4$, then

$$\mathcal{N}(u) = 2\sum_{j=0}^{\frac{k-1}{2}} 1 = k+1.$$

If $k = 1$, then by Theorem 1.3

$$\mathcal{N}(u) = 2\alpha_*(p) = \begin{cases} 0 & \text{if } p \equiv 3 \pmod 4 \\ 2 & \text{if } p \equiv 1 \pmod 4. \end{cases}$$

Now assume that $p = 2$, $u = p^k$, and $k > 1$: the case $k = 1$, i.e. $u = 2$ is considered separately in the statement of Theorem 1.3. If k is even, then

$$\begin{aligned}\mathcal{N}(u) &= 2\beta(2^{k-1}) + \beta(2^{k-2}) + 4\sum_{j=1}^{\frac{k-2}{2}} \alpha_*(2^{k-2j})\beta(2^{2j-1}) \\ &+ 2\sum_{j=0}^{\frac{k-4}{2}} \alpha_*(2^{k-1-2j})(2\beta(2^{2j})-1) = 1,\end{aligned}$$

since $\alpha_*(2^i) = 0$ for all $i > 1$, and $\beta(2^i) = 0$ for all odd i. Now let k be odd. Then

$$\begin{aligned}\mathcal{N}(u) &= \beta(2^{k-1}) + 2\beta(2^{k-2}) + 4\sum_{j=1}^{\frac{k-3}{2}} \alpha_*(2^{k-2j})\beta(2^{2j-1}) \\ &+ 2\sum_{j=0}^{\frac{k-3}{2}} \alpha_*(2^{k-1-2j})(2\beta(2^{2j})-1) = 1.\end{aligned}$$

This completes the proof. □

In precisely the same manner, we obtain the following formulas for the case when determinant is a product of two odd primes.

Corollary 6.3. *If $u = p_1p_2$, where $p_1 < p_2$ are odd primes, then*

$$\mathcal{N}(u) = \begin{cases} 0 & \textit{if } p_1 \textit{ or } p_2 \equiv 3 \pmod 4 \textit{ and } p_2 > \sqrt{3}p_1 \\ 2 & \textit{if } p_1 \textit{ or } p_2 \equiv 3 \pmod 4 \textit{ and } p_2 \leq \sqrt{3}p_1 \\ 4 & \textit{if } p_1 \textit{ and } p_2 \equiv 1 \pmod 4 \textit{ and } p_2 > \sqrt{3}p_1 \\ 6 & \textit{if } p_1 \textit{ and } p_2 \equiv 1 \pmod 4 \textit{ and } p_2 \leq \sqrt{3}p_1. \end{cases}$$

Proof. Direct verification. □

The same way one can apply the formulas of Theorem 1.3 to obtain explicit expressions for $\mathcal{N}(u)$ for many other instances of u as well.

Notice that some of the lattices in $\mathrm{WR}(\mathbb{Z}^2)$ come from ideals in $\mathbb{Z}[i]$. Namely, let $u = a^2 + b^2 \in \mathcal{D}$ and consider the lattices $\Lambda_1(a,b) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mathbb{Z}^2$ and $\Lambda_2(a,b) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mathbb{Z}^2$ with $\det(\Lambda_1) = \det(\Lambda_2) = u$. Let $I_1(a,b)$ and $I_2(a,b)$ be the ideals in $\mathbb{Z}[i]$ generated by $a+bi$ and $a-bi$ respectively, then $-b+ai = i(a+bi) \in I_1(a,b)$ and $b+ai = i(a-bi) \in I_2(a,b)$. Hence $I_1(a,b)$ and $I_2(a,b)$ map bijectively onto $\Lambda_1(a,b)$ and $\Lambda_2(a,b)$ respectively under the canonical mapping $x+iy \to \begin{pmatrix} x \\ y \end{pmatrix}$, and $\Lambda_1(a,b) = \Lambda_2(a,b)$ if and only if $b = 0$, which can only happen when u is a square. Notice that such representation is only possible for the determinant values u which are also in the minima set $\mathfrak{M}$; in other words, a full-rank WR sublattice of $\mathbb{Z}^2$ comes from an ideal in $\mathbb{Z}[i]$ if and only if it has an orthogonal basis. It is easy to see that the number of such lattices of determinant $u \in \mathfrak{M}$, which is precisely the number of ideals of norm u in $\mathbb{Z}[i]$, is equal to $2\alpha(u)$ if u is not a square, and $2\alpha(u)+1$ if u is a square. With this in mind, we can now state the following immediate consequence of Corollaries 6.2 and 6.3.

Corollary 6.4. *If $u \in \mathcal{D}$ is of the form $u = p^k, 2p^k$, where p is a prime, or $u = p_1p_2$ where $\sqrt{3}p_1 < p_2$ are odd primes, then all lattices in $\mathrm{WR}(\mathbb{Z}^2)$ of determinant u come from ideals of norm u in $\mathbb{Z}[i]$.*

This of course is not true in general, in fact the class of such lattices coming from ideals in $\mathbb{Z}[i]$ is quite thin. Notice in particular that in order for a lattice $\Lambda \in \mathrm{WR}(\mathbb{Z}^2)$ to come from an ideal of $\mathbb{Z}[i]$ it must first of all be true that $\det \Lambda \in \mathfrak{M}$, which has density 0 versus the entire determinant set $\mathcal{D}$, which has positive density.

Remark 6.1. Let $\mathfrak{P} = \{p_1, p_2, \dots\}$ be the collection of all primes in the arithmetic progression $4n+1$. By Dirichlet's theorem on primes in arithmetic progressions, $\mathfrak{P}$ is infinite. For each $p_i \in \mathfrak{P}$ define $\mathcal{P}_i = \{p_i^k, 2p_i^k\}_{k=1}^{\infty}$. Then $\bigcup_{i=1}^{\infty} \mathcal{P}_i \subset \mathcal{D}$, and Corollary 6.2 implies that for each i,

$$\mathcal{N}(u) = \frac{\log u}{\log p_i} + 1,$$

for each $u \in \mathcal{P}_i$. In other words, there are infinite sequences in $\mathcal{D}$ on which $\mathcal{N}(u)$ grows at least logarithmically in u. For comparison, it is a well known fact (see for instance [6]) that for any positive integer u with prime factorization $u = q_1^{c_1} \dots q_m^{c_m}$ the number of *all* full-rank sublattices of $\mathbb{Z}^2$ with determinant u is

$$F(2,u) = \prod_{j=1}^{m} \frac{q_j^{c_j+1} - 1}{q_j - 1}, \tag{52}$$

which grows linearly in u. It is therefore interesting to exhibit sequences of determinant values u for which $\mathcal{N}(u)$ is especially large.

Recall that for an integer u, $\tau(u)$ and $\omega(u)$ are numbers of divisors and of prime divisors of u, respectively. We can report the following consequence of Theorem 1.3.

Corollary 6.5. *For each $u \in \mathbb{Z}_{>0}$,*

$$\mathcal{N}(u) \leq O\left(\tau(u)^2 2^{\omega(u)}\right) \leq O\left(\left(\frac{\sqrt{2}\log u}{\omega(u)}\right)^{2\omega(u)}\right). \tag{53}$$

Moreover,

$$\mathcal{N}(u) < O\left((\log u)^{\log 8}\right), \tag{54}$$

for all $u \in \mathcal{D}$ outside of a subset of asymptotic density 0. However, there exist infinite sequences $\{u_k\}_{k=1}^{\infty} \subset \mathcal{D}$ such that for every $k \geq 1$

$$\mathcal{N}(u_k) \geq (\log u_k)^k. \tag{55}$$

For instance, there exists such a sequence with $u_k \leq \exp\left(O(k(\log k)^2)\right)$ and $\omega(u_k) = O(k\log k)$.

Proof. Notice that the right hand side of (6) is the sum of at most $\tau(u)$ nonzero terms. Combining (10) with the formula for α_* in section 1, it follows that each of these terms is at most $O\left(\tau(u)2^{\omega(u)}\right)$. Let u have a prime decomposition of the form $u = p_1^{e_1}\dots p_n^{e_n}$, so $\omega(u) = n$, then:

$$\frac{\log u}{n} = \frac{1}{n}\sum_{i=1}^{n} e_i \log p_i \geq \left(\prod_{i=1}^{n} e_i \log p_i\right)^{\frac{1}{n}} \geq \left(O\left(\prod_{i=1}^{n}(e_i+1)\right)\right)^{\frac{1}{n}} = (O(\tau(u)))^{\frac{1}{n}}.$$

This proves (53), and (54) follows from (53) combined with Theorems 431 and 432 of [8], which state that the normal orders of $\omega(u)$ and $\tau(u)$ are $\log\log u$ and $2^{\log\log u}$, respectively.

Next, write p_n for the n-th prime congruent to 1 mod 4. It is a well known fact that

$$p_n = O(n\log n). \tag{56}$$

For each $n \geq 1$, define $v_n = \prod_{i=1}^{n} p_i^2$. Write $\mathcal{N}_I(v_n)$ for the number of lattices in $\mathrm{WR}(\mathbb{Z}^2)$ with determinant v_n that come from ideals in $\mathbb{Z}[i]$, then

$$\mathcal{N}(v_n) \geq \mathcal{N}_I(v_n) = 2\alpha(v_n) + 1 = 3^n. \tag{57}$$

Let k be a positive integer. We want to choose n such that

$$\mathcal{N}(v_n) \geq 3^n \geq \left(\log\left(\prod_{i=1}^{n} p_i^2\right)\right)^k = 2^k\left(\sum_{i=1}^{n}\log p_i\right)^k. \tag{58}$$

By (56),

$$\sum_{i=1}^{n}\log p_i = \sum_{i=1}^{n}\log\left(O(i\log i)\right) = \sum_{i=1}^{n} O\left(\log(i\log i)\right) = \sum_{i=1}^{n} O\left(\log i\right) \leq O(n\log n). \tag{59}$$

Combining (58) with (59) and taking logarithms, we see that it is sufficient to choose n such that

$$\frac{n}{\log n} \geq O(k),$$

hence we can take $n = O(k\log k)$. Then, by (59), for this choice of n we have

$$v_n = \exp\left(2\sum_{i=1}^{n}\log p_i\right) \leq \exp\left(O(n\log n)\right) = \exp\left(O(k(\log k)^2)\right).$$

Let $u_k = v_n$ for this choice of n, and so $n = \omega(u_k)$. This completes the proof. $\square$

Remark 6.2. Let v_n be as in the proof of Corollary 6.5 above, i.e. $v_n = \prod_{i=1}^{n} p_i^2$, where $p_1, p_2, \dots$ are primes congruent to 1 mod 4; for instance, the first 9 such primes are 5, 13, 17, 29, 37, 43, 47, 53, 61. For each k choose the smallest n so that $v_n > (\log v_n)^k$, and let $u_k = v_n$ for this choice of n. Here is the actual data table for the first few values of the sequence $\{u_k\}$ computed with Maple.

k	n	$u_k = v_n$	$\mathcal{N}(u_k)$	$(\log u_k)^k$
1	2	4225	9	8.34877454
2	4	1026882025	518	430.5539044
3	7	5741913252704971225	215002	80589.79464
4	9	600161367302023909803840 25	14324372	12413026.85

Notice that the choice of $n = O(k \log k)$ as in Corollary 6.5 insures that not just $\mathcal{N}(u_k)$, but even the much smaller $\mathcal{N}_I(u_k)$ (compare for instance the values of $\mathcal{N}(u_k)$ in the table above to $\mathcal{N}_I(u_k) = 3^n$) is greater than $(\log u_k)^k$, and even with this stronger restriction u_k and $\omega(u_k)$ grow relatively slow as functions of k.

7. Counting well-rounded lattices with fixed minimum

Let $m \in \mathbb{Z}_{>0}$, then, as stated in [14], there exist $\left[\frac{m+1}{2}\right]$ WR lattices Λ, not necessarily integral, of rank 2 in $\mathbb{R}^2$ with $|\Lambda| = \sqrt{m}$, generated by a minimal basis $\boldsymbol{x}, \boldsymbol{y}$ with $0 < \boldsymbol{x}^t \boldsymbol{y} \leq \left[\frac{m-1}{2}\right]$. This information, however, does not lead to an explicit formula for the number of WR sublattices of $\mathbb{Z}^2$ of prescribed minimum. We derive such a formula here.

Let $m \in \mathbb{Z}_{>0}$. Suppose that $\Lambda \in \mathrm{WR}(\mathbb{Z}^2)$ and $|\Lambda|^2 = m$, then by Lemma 3.2 there exists a representation $\Lambda = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} \mathbb{Z}^2$ with

$$\boldsymbol{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \ \boldsymbol{y} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \in \mathbb{Z}^2, \ \|\boldsymbol{x}\| = \|\boldsymbol{y}\| = m, \ \theta(\boldsymbol{x}, \boldsymbol{y}) \in \left[\frac{\pi}{3}, \frac{\pi}{2}\right], \tag{60}$$

where $\theta(\boldsymbol{x}, \boldsymbol{y})$ is the angle between vectors $\boldsymbol{x}$ and $\boldsymbol{y}$, since if $\theta(\boldsymbol{x}, \boldsymbol{y}) \in \left(\frac{\pi}{2}, \frac{2\pi}{3}\right]$ we can always replace $\boldsymbol{x}$ with $-\boldsymbol{x}$ or $\boldsymbol{y}$ with $-\boldsymbol{y}$ to ensure that $\theta(\boldsymbol{x}, \boldsymbol{y}) \in \left[\frac{\pi}{3}, \frac{\pi}{2}\right]$. Then define

$$\mathcal{C}_m = \{\boldsymbol{x} \in \mathbb{Z}^2 : x_2 > 0, \ \|\boldsymbol{x}\| = m\}.$$

For each $\boldsymbol{x} \in \mathcal{C}_m$ let

$$E_m(\boldsymbol{x}) = \left\{\boldsymbol{y} \in \mathbb{Z}^2 : y_2 \geq 0, \ \|\boldsymbol{y}\| = m, \ \theta(\boldsymbol{x}, \boldsymbol{y}) \in \left[\frac{\pi}{3}, \frac{\pi}{2}\right]\right\},$$

and define $\eta_m(\boldsymbol{x}) = |E_m(\boldsymbol{x})|$. The following result follows immediately.

Theorem 7.1. *Let $m \in \mathfrak{M}$. Let $\mathcal{N}'(m)$ be the number of lattices in $\mathrm{WR}(\mathbb{Z}^2)$ with minimum equal to m. Then*

$$\mathcal{N}'(m) = \sum_{\boldsymbol{x} \in \mathcal{C}_m} \eta_m(\boldsymbol{x}).$$

Notice that for each $\boldsymbol{x} \in \mathcal{C}_m$, $\eta_m(\boldsymbol{x})$ is precisely the number of integer lattice points on the arc of the circle of radius $\sqrt{m}$, bounded by the points $\begin{pmatrix} \frac{x_1}{2} - \frac{x_2\sqrt{3}}{2} \\ \frac{x_1\sqrt{3}}{2} + \frac{x_2}{2} \end{pmatrix}$ and $\begin{pmatrix} -x_2 \\ x_1 \end{pmatrix}$. The angle corresponding to this arc is $\frac{\pi}{6}$. On the other hand, $\alpha(m)$ as defined by (3) is the number of integer lattice points on the quarter-circle of radius $\sqrt{m}$ centered at the origin and bounded by the points $(\sqrt{m}, 0)$, $(0, \sqrt{m})$. It is not difficult to see that for every $\boldsymbol{x} \in \mathcal{C}_m$,

$$\eta_m(\boldsymbol{x}) \leq \begin{cases} \alpha(m) & \text{if } m \text{ is not a square} \\ \alpha(m) + 1 & \text{if } m \text{ is a square.} \end{cases}$$

Indeed, for each $\begin{pmatrix} 0 \\ \sqrt{m} \end{pmatrix} \neq \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \in E_m(\boldsymbol{x})$, either $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ or $\begin{pmatrix} -y_2 \\ y_1 \end{pmatrix}$ is contained in the first quadrant and so is counted by $\alpha(m)$; if m is a square, we add one to account for the point $\begin{pmatrix} 0 \\ \sqrt{m} \end{pmatrix}$, which is not counted by $\alpha(m)$. In general, these bounds are sharp, for instance $\alpha(13) = \eta_{13}\begin{pmatrix} 2 \\ 3 \end{pmatrix} = 1$. However, if $\alpha(m)$ is large and the integral points $\boldsymbol{x}$ are well distributed on the quarter-circle, it is possible to do better. For this m needs to satisfy certain special conditions. More precisely, write prime decomposition of m as

$$m = 2^w p_1^{2l_1} \dots p_s^{2l_s} q_1^{k_1} \dots q_r^{k_r},$$

where $p_i \equiv 3 \pmod 4$, $q_j \equiv 1 \pmod 4$, $w \in \mathbb{Z}_{\geq 0}$, $l_i \in \frac{1}{2}\mathbb{Z}_{>0}$, and $k_j \in \mathbb{Z}_{>0}$ for all $1 \leq i \leq s$, $1 \leq j \leq r$. If $l_i \notin \mathbb{Z}$ for any $1 \leq i \leq s$, then $\alpha(m) = 0$, so let us assume that $l_i \in \mathbb{Z}$ for all $1 \leq i \leq s$. Then

$$\alpha(m) = \alpha\left(\frac{m}{2^w p_1^{2l_1} \dots p_s^{2l_s}}\right),$$

hence we can assume that

$$m = q_1^{k_1} \dots q_r^{k_r}, \tag{61}$$

where $q_j \equiv 1 \pmod 4$ and $k_j \in \mathbb{Z}_{>0}$ for all $1 \leq j \leq r$. Define

$$L(m) = \sqrt{\frac{\log(q_1 \dots q_r)}{\log \alpha(m)}},$$

and let

$$\mathfrak{M}_1 = \{m \in \mathfrak{M} : m \text{ as in (61) and } L(m) \to 0 \text{ as } m \to \infty\}.$$

A result of Babaev [2] implies that for $m \in \mathfrak{M}_1$

$$\eta_m(\boldsymbol{x}) = \frac{\alpha(m)}{3} + O(L(m)\alpha(m)), \tag{62}$$

for each $\boldsymbol{x} \in \mathcal{C}_m$. For $m \in \mathfrak{M} \setminus \mathfrak{M}_1$ I am not aware of upper bounds on $\eta_m(\boldsymbol{x})$ better than $\alpha(m)$; a classical result of Jarnik on the number of integral lattice points on convex curves [10] as well as more modern results, for instance of Bombieri and Pila [4], imply a general bound on $\eta_m(\boldsymbol{x})$ which is at best $O\left(m^{\frac{1}{4}+\varepsilon}\right)$ for each $\boldsymbol{x} \in \mathcal{C}_m$.

In precisely the same manner as Corollary 1.4 follows from Theorem 1.3, the following is an immediate consequence of Theorem 7.1.

Corollary 7.2. *Let $A \in O_2(\mathbb{R})$. Then for each $m \in \mathfrak{M}$ the number of full-rank WR sublattices of $A\mathbb{Z}^2$ with squared minimum equal to m is given by $\mathcal{N}'(m)$ as in Theorem 7.1.*

Remark 7.1. Notice that even fixing both, the minimum and the determinant, does not identify an element of $\mathrm{WR}(\mathbb{Z}^2)$ uniquely. For instance, if u is representable as a sum of two squares, then the number of lattices $\Lambda \in \mathrm{WR}(\mathbb{Z}^2)$ with $|\Lambda|^2 = \det(\Lambda) = u$ is

$$\mathcal{N}_I(u) = \begin{cases} 2\alpha(u) & \text{if } u \text{ is not a square} \\ 2\alpha(u)+1 & \text{if } u \text{ is a square,} \end{cases}$$

i.e. precisely the number of lattices in $\mathrm{WR}(\mathbb{Z}^2)$ of determinant u coming from ideals in $\mathbb{Z}[i]$, as defined in section 6. Hence even this number can tend to infinity with u.

8. Zeta function of well-rounded lattices

Given any finitely generated group G, it is possible to associate a zeta function $\zeta_G(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ to it, where the coefficients a_n count the number of its subgroups of index n and $s \in \mathbb{C}$ (see [12], Chapter 15 for details). Such zeta functions are extensively studied objects, since they encode important arithmetic information about the group in question and often have interesting properties. For example, by Theorem 15.1 of [12] (see also (5) of [5])

$$\zeta_{\mathbb{Z}^2}(s) = \sum_{\Lambda \subseteq \mathbb{Z}^2} (\det(\Lambda))^{-s} = \sum_{u=1}^{\infty} F(2,u)u^{-s} = \zeta(s)\zeta(s-1), \tag{63}$$

where the sum is taken over all sublattices Λ of $\mathbb{Z}^2$ of finite index, $F(2,u)$ is given by (52), and $\zeta(s)$ is the Riemann zeta function. This $\zeta_{\mathbb{Z}^2}(s)$ is an example of Solomon's zeta function (see [5], [20]). The identity (63) holds in the half-plane $\Re(s) > 2$, where this series is absolutely convergent, and so the function $\zeta_{\mathbb{Z}^2}(s)$ is analytic (Proposition 1 of [5]). Moreover, in this half-plane $\zeta_{\mathbb{Z}^2}(s) = \sum_{u=1}^{\infty} \sigma(u)u^{-s}$, where $\sigma(u) = \sum_{d|u} d$ (see Theorem 290 of [8]); $\zeta_{\mathbb{Z}^2}(s)$ has a pole at $s = 2$.

In this section we study the properties of the partial zeta function corresponding not to all, but only to the *well-rounded* sublattices of $\mathbb{Z}^2$ as defined by (7). We also define the Dedekind zeta function of Gaussian integers $\mathbb{Z}[i]$

$$\zeta_{\mathbb{Z}[i]}(s) = \sum_{\mathfrak{A} \subseteq \mathbb{Z}[i]} \mathbb{N}(\mathfrak{A})^{-s} = \sum_{\substack{\Lambda \in \mathrm{WR}(\mathbb{Z}^2) \\ |\Lambda|^2 = \det(\Lambda)}} (\det(\Lambda))^{-s} = \sum_{m=1}^{\infty} \mathcal{N}_I(m)m^{-s}, \tag{64}$$

where $\mathcal{N}_I(m)$ is as above, and the first sum is taken over all the ideals $\mathfrak{A} = (a+bi)\mathbb{Z}[i]$ for some $a, b \in \mathbb{Z}$, and $\mathbb{N}(\mathfrak{A}) = a^2 + b^2$ is the norm of such ideal. In other words, coefficients of $\zeta_{\mathbb{Z}[i]}(s)$ count the elements of $\mathrm{WR}(\mathbb{Z}^2)$ that come from ideals in $\mathbb{Z}[i]$ while coefficients of $\zeta_{\mathrm{WR}(\mathbb{Z}^2)}(s)$ count all elements of $\mathrm{WR}(\mathbb{Z}^2)$. We also note that $\zeta_{\mathbb{Z}[i]}(s)$ is analytic on $\Re(s) > 1/2$ except for a simple pole at $s = 1$ (see Theorem 5 on p. 161 of [11]). It is clear that for all $u \in \mathbb{Z}_{>0}$

$$\mathcal{N}_I(u) \leq \mathcal{N}(u) \leq F(2,u), \tag{65}$$

in other words $\zeta_{\mathrm{WR}(\mathbb{Z}^2)}(s)$ is "squeezed" between $\zeta_{\mathbb{Z}[i]}(s)$ and $\zeta_{\mathbb{Z}^2}(s)$. Moreover, our estimates on coefficients in the previous sections suggest that $\zeta_{\mathrm{WR}(\mathbb{Z}^2)}(s)$ should be "closer" to $\zeta_{\mathbb{Z}[i]}(s)$ than to $\zeta_{\mathbb{Z}^2}(s)$. Theorem 1.5, which we will now prove, makes this statement more precise. We start by studying some related Dirichlet series.

Lemma 8.1. *Let $t = t(u)$ be as in Theorem 1.3. The Dirichlet series $\sum_{u=1}^{\infty} \frac{2\alpha_*(t)}{u^s}$ is absolutely convergent at least in the half-plane $\Re(s) > 1$ with a simple pole at $s = 1$. Moreover, when $\Re(s) > 1$ it has an Euler product expansion:*

$$\sum_{u=1}^{\infty} \frac{2\alpha_*(t)}{u^s} = \left(1 + \frac{1}{2^s} + \frac{1}{4^s}\right) \prod_{p \equiv 1 (\mathrm{mod}\, 4)} \frac{p^s + 1}{p^s - 1}. \tag{66}$$

Proof. First of all, notice that for every $u \in \mathbb{Z}_{>0}$,

$$2\alpha_*(t) \leq 2\alpha(t) \leq 2\alpha(u) + 1 \leq \mathcal{N}_I(u) + 1,$$

therefore $\sum_{u=1}^{\infty} 2\alpha_*(t)u^{-s}$ is absolutely convergent at least on the half-plane $\Re(s) > 1$ with at most a simple pole at $s = 1$, since $\sum_{u=1}^{\infty} (\mathcal{N}_I(u) + 1)u^{-s} = \zeta_{\mathbb{Z}[i]}(s) + \zeta(s)$ is. Next, let

$$\alpha'_*(n) = \begin{cases} \alpha_*(n) & \text{if } n \text{ is odd} \\ 0 & \text{if } n \text{ is even.} \end{cases}$$

Notice that $2\alpha'_*$ is a multiplicative arithmetic function, specifically $2\alpha'_*(1) = 1$ and $2\alpha'_*(mn) = 2\alpha'_*(m)2\alpha'_*(n)$ for all $m, n \in \mathbb{Z}_{>0}$ with $\gcd(m, n) = 1$. Therefore, by Theorem 286 of [8] the series $\sum_{u=1}^{\infty} 2\alpha'_*(u)u^{-s}$ has the following Euler-type product representation, where p is always a prime:

$$\begin{aligned} \sum_{u=1}^{\infty} 2\alpha'_*(u)u^{-s} &= \prod_p \left(\sum_{k=0}^{\infty} 2\alpha'_*(p^k)p^{-ks}\right) = \prod_{p \equiv 1 (\mathrm{mod}\, 4)} \left(1 + 2\sum_{k=1}^{\infty} p^{-ks}\right) \\ &= \prod_{p \equiv 1 (\mathrm{mod}\, 4)} \left(\frac{2}{1 - p^{-s}} - 1\right) = \prod_{p \equiv 1 (\mathrm{mod}\, 4)} \frac{p^s + 1}{p^s - 1}, \end{aligned}$$

whenever this product is convergent. Also notice that since $\alpha_*(2u) = 0$ if $2|u$ and $\alpha_*(2u) = \alpha_*(u)$ if $2 \nmid u$, we have

$$\begin{aligned} \sum_{u=1}^{\infty} \frac{2\alpha_*(t)}{u^s} &= \sum_{u=1}^{\infty} \frac{2\alpha'_*(u)}{u^s} + \sum_{u=1}^{\infty} \frac{2\alpha_*(u)}{(2u)^s} \\ &= \sum_{u=1}^{\infty} \frac{2\alpha'_*(u)}{u^s} + \frac{1}{2^s}\left(\sum_{u=1}^{\infty} \frac{2\alpha'_*(u)}{u^s} + \frac{1}{2^s}\sum_{u=1}^{\infty} \frac{2\alpha'_*(u)}{u^s}\right) \\ &= \left(1 + \frac{1}{2^s} + \frac{1}{4^s}\right) \sum_{u=1}^{\infty} \frac{2\alpha'_*(u)}{u^s}, \end{aligned}$$

which proves (66) when $\prod_{p \equiv 1 (\mathrm{mod}\, 4)} \frac{p^s+1}{p^s-1}$ is convergent. It is easy to notice that this happens when $\Re(s) > 1$, but $\prod_{p \equiv 1 (\mathrm{mod}\, 4)} \frac{p+1}{p-1}$ diverges, meaning that $\sum_{u=1}^{\infty} \frac{2\alpha_*(t)}{u^s}$ must have a pole at $s = 1$, and by our argument above we know that it must be a simple pole. This completes the proof. □

For the next lemma, let $\mathcal{B}_\nu$ be as in (36) in section 4.

Lemma 8.2. *For each $1 < \nu \leq 3^{1/4}$, the Dirichlet series $\sum_{u \in \mathcal{B}_\nu} \frac{1}{u^s}$ is absolutely convergent in the half-plane $\Re(s) > 1$ with a simple pole at $s = 1$ in the sense of (8).*

Proof. First notice that

$$\sum_{u\in\mathcal{B}_\nu}\left|\frac{1}{u^s}\right|\leq\sum_{n=1}^{\infty}\left|\frac{1}{n^s}\right|,$$

and so must be analytic when $\Re(s)>1$ with at most a simple pole at $s=1$.

On the other hand, let the Dirichlet lower density of the set $\mathcal{B}_\nu$ be defined as

$$\liminf_{s\to1^+}\frac{\sum_{u\in\mathcal{B}_\nu}u^{-s}}{\sum_{u\in\mathbb{Z}_{>0}}u^{-s}}=\liminf_{s\to1^+}\frac{1}{\zeta(s)}\sum_{u\in\mathcal{B}_\nu}u^{-s}.$$

It is a well known fact (see for instance equation (1.6) of [1]) that the Dirichlet lower density of a set is greater or equal than its lower density. Hence, by Theorem 4.4

$$0<\frac{\nu-1}{2\nu}\leq\underline{\Delta}_{\mathcal{B}_\nu}\leq\liminf_{s\to1^+}\frac{1}{\zeta(s)}\sum_{u\in\mathcal{B}_\nu}u^{-s},$$

which implies that $\sum_{u\in\mathcal{B}_\nu}u^{-s}$ must have a pole of the same order as $\zeta(s)$ at $s=1$. This completes the proof. □

Lemma 8.3. *For each $1<\nu\leq3^{1/4}$, Dirichlet series $\sum_{u=1}^{\infty}\frac{\beta_\nu(u)}{u^s}$ is absolutely convergent in the half-plane $\Re(s)>1$, and is bounded below by a Dirichlet series with a pole of order 1 at $s=1$. Moreover, for every real $\varepsilon>0$ there exists a Dirichlet series with a pole of order $1+\varepsilon$ at $s=1$, which bounds $\sum_{u=1}^{\infty}\frac{\beta_\nu(u)}{u^s}$ from above.*

Proof. For each $1<\nu\leq3^{1/4}$, define χ_ν to be the characteristic function of the set $\mathcal{B}_\nu$, i.e. for each $u\in\mathbb{Z}_{>0}$,

$$\chi_\nu(u)=\begin{cases}1 & \text{if } u\in\mathcal{B}_\nu\\ 0 & \text{if } u\notin\mathcal{B}_\nu.\end{cases}$$

Clearly, $\beta_\nu(u)\geq\chi_\nu(u)$, therefore

$$\sum_{u=1}^{\infty}\left|\frac{\beta_\nu(u)}{u^s}\right|\geq\sum_{u=1}^{\infty}\left|\frac{\chi_\nu(u)}{u^s}\right|=\sum_{u\in\mathcal{B}_\nu}\left|\frac{1}{u^s}\right|,$$

which, combined with Lemma 8.2, proves the lower bound of the lemma.

On the other hand, recall that $\beta_\nu(u)\leq\Delta(u)$ for all $u\in\mathbb{Z}_{>0}$, where $\Delta(u)$ is Hooley's Δ-function, as defined in section 2, hence $\sum_{u=1}^{\infty}|\beta_\nu(u)u^{-s}|\leq\sum_{u=1}^{\infty}|\Delta(u)u^{-s}|$. Hooley's Δ-function is known to satisfy

$$\sum_{u=1}^{\infty}\left|\frac{\Delta(u)}{u^s}\right|\ll_\varepsilon\sum_{u=1}^{\infty}\left|\frac{(\log u)^\varepsilon}{u^s}\right|,\tag{67}$$

for every $\varepsilon>0$, which is a consequence of Tenenbaum's bound on the average order of $\Delta(u)$ (see [21], also [7]), and so the upper bound of the lemma follows by observing that $\sum_{u=1}^{\infty}(\log u)^\varepsilon u^{-s}$ has a pole of order $1+\varepsilon$ at $s=1$. Since $\sum_{u=1}^{\infty}(\log u)^\varepsilon u^{-s}$ is absolutely convergent in the half-plane $\Re(s)>1$, (67) also proves that so is $\sum_{u=1}^{\infty}\frac{\beta_\nu(u)}{u^s}$. □

We are now ready to prove Theorem 1.5.

Proof of Theorem 1.5. First of all notice that (65) combined with comparison test for series imply that $\sum_{u=1}^{\infty}\mathcal{N}(u)u^{-s}$ has a pole at $s=1$, since $\zeta_{\mathbb{Z}[i]}(s)$ has a pole at

$s=1$, and is absolutely convergent, i.e. $\zeta_{\mathrm{WR}(\mathbb{Z}^2)}(s)$ is analytic, for $\Re(s)>2$, since $\zeta_{\mathbb{Z}^2}(s)$ is analytic when $\Re(s)>2$. In fact, we can do better. Let

$$\beta'(n)=\begin{cases} 2\beta(n)-1 & \text{if } n \text{ is a square} \\ 2\beta(n) & \text{if } n \text{ is not a square,}\end{cases}$$

for every $n\in\mathbb{Z}_{>0}$. Notice that for every $u\in\mathbb{Z}_{>0}$, $\mathcal{N}(u)$ can be expressed in terms of the Dirichlet convolution of arithmetic functions $2\alpha_*$ and β':

$$\mathcal{N}(u)=(2\alpha_*\ast\beta')(t)+\left(\delta_1(t)\beta(t)+\delta_2(t)\beta\left(\frac{t}{2}\right)-2\beta'(t)-\frac{1+(-1)^t}{2}\beta'\left(\frac{t}{2}\right)\right),$$

where $t=t(u)$, $\delta_1(t)$, and $\delta_2(t)$ are as in Theorem 1.3. Therefore, by Theorem 284 of [8]

$$\begin{aligned}\zeta_{\mathrm{WR}(\mathbb{Z}^2)}(s) &= \sum_{u=1}^{\infty}(2\alpha_*\ast\beta')(t)u^{-s} \\ &+ \sum_{u=1}^{\infty}\left(\delta_1(t)\beta(t)+\delta_2(t)\beta\left(\frac{t}{2}\right)-2\beta'(t)-\frac{1+(-1)^t}{2}\beta'\left(\frac{t}{2}\right)\right)u^{-s} \\ &= \left(\sum_{u=1}^{\infty}2\alpha_*(t)u^{-s}-2\right)\left(\sum_{u=1}^{\infty}\beta'(t)u^{-s}\right) \\ &+ \sum_{u=1}^{\infty}\left(\delta_1(t)\beta(t)+\delta_2(t)\beta\left(\frac{t}{2}\right)\right)u^{-s}-\sum_{u=1}^{\infty}\frac{1+(-1)^t}{2}\beta'\left(\frac{t}{2}\right)u^{-s}, \qquad (68)\end{aligned}$$

whenever these three series are absolutely convergent. Now notice that

$$\frac{1}{|2^s|}\sum_{u=1}^{\infty}\frac{\beta(u)}{|u^s|}\le\sum_{u=1}^{\infty}\frac{\delta_1(t)\beta(t)}{|u^s|}\le 2\sum_{u=1}^{\infty}\frac{\beta(u)}{|u^s|},$$

and

$$\frac{1}{|4^s|}\sum_{u=1}^{\infty}\frac{\beta(u)}{|u^s|}\le\sum_{u=1}^{\infty}\frac{\delta_2(t)\beta\left(\frac{t}{2}\right)}{|u^s|}=\frac{1}{|4^s|}\sum_{u=1}^{\infty}\frac{\delta_1(u)\beta(u)}{|u^s|}\le\frac{2}{|4^s|}\sum_{u=1}^{\infty}\frac{\beta(u)}{|u^s|},$$

as well as

$$\frac{1}{|2^s|}O\left(\sum_{u=1}^{\infty}\frac{\beta(u)}{|u^s|}\right)=\frac{1}{|2^s|}\sum_{u=1}^{\infty}\frac{\beta'(u)}{|u^s|}\le\sum_{u=1}^{\infty}\frac{\beta'(t)}{|u^s|}\le\sum_{u=1}^{\infty}\frac{\beta'(u)}{|u^s|}=O\left(\sum_{u=1}^{\infty}\frac{\beta(u)}{|u^s|}\right),$$

whenever $\Re(s)>0$. Also

$$\sum_{u=1}^{\infty}\frac{1+(-1)^t}{2}\beta'\left(\frac{t}{2}\right)u^{-s}=4^{-s}\sum_{u=1}^{\infty}\beta'(u)u^{-s}.$$

Now the conclusion of Theorem 1.5 follows by applying these observations along with Lemmas 8.1, 8.3 to (68). □

Remark 8.1. Notice that one implication of Theorem 1.5 is that $\mathcal{N}(u)$, the coefficient of $\zeta_{\mathrm{WR}(\mathbb{Z}^2)}(s)$, grows, roughly speaking, like the coefficient of $\zeta_{\mathbb{Z}[i]}(s)^2$, which is

$$\sum_{mn=u}\mathcal{N}_I(m)\mathcal{N}_I(n).$$

Finally, we mention that in the same manner one can define zeta functions of well-rounded sublattices of any lattice Ω in $\mathbb{R}^N$ for any N. Studying the properties of these functions may yield interesting arithmetic information about the distribution of such sublattices.

Acknowledgment. I would like to thank Kevin Ford, Preda Mihailescu, Baruch Moroz, Gabriele Nebe, Bogdan Petrenko, Sinai Robins, Eugenia Soboleva, Paula Tretkoff, Jeff Vaaler and Victor Vuletescu for their helpful comments on the subject of this paper. I would also like to acknowledge the wonderful hospitality of Max-Planck-Institut für Mathematik in Bonn, Germany, where a large part of this work has been done.

References

[1] R. Ahlswede and L. H. Khachatrian. Number-theoretic correlation inequalities for Dirichlet densities. *J. Number Theory*, 63(1):34–46, 1997.
[2] G. Babaev. Distribution of integral points on certain surfaces defined by norms. *Soviet Math. Dokl.*, 1:992–995, 1960.
[3] A. Barvinok. Computing the volume, counting integral points, and exponential sums. *Discrete Comput. Geom.*, 10(2):123–141, 1993.
[4] E. Bombieri and J. Pila. The number of integral points on arcs and ovals. *Duke Math. J.*, 59(2):337–357, 1989.
[5] C. Bushnell and I. Reiner. Zeta functions of arithmetic orders and Solomon's conjectures. *Math. Z.*, 173(2):135–161, 1980.
[6] B. Gruber. Alternative formulae for the number of sublattices. *Acta Cryst. Sect. A*, 53(6):807–808, 1997.
[7] R. Hall and G. Tenenbaum. *Divisors*. Cambridge Univ. Press, 1988.
[8] 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.
[9] R. Jakimczuk. Inequalities and asymptotic formulas for sums of prime powers. *Bol. Soc. Mat. Mexicana (3)*, 11(1):5–10, 2005.
[10] V. Jarnik. Uber die Gitterpunkte auf konvexen Curven. *Math. Z.*, 24:500–518, 1926.
[11] S. Lang. *Algebraic Number Theory*. Springer-Verlag, 1994.
[12] A. Lubotzky and D. Segal. *Subgroup Growth*. Progress in Mathematics, 212. Birkhauser Verlag, Basel, 2003.
[13] H. Maier and G. Tenenbaum. On the normal concentration of divisors. *J. London Math. Soc. (2)*, 31(3):393–400, 1985.
[14] J. Martinet and B. Venkov. On integral lattices having an odd minimum. *St. Petersburg Math. J.*, 16(3):507–539, 2005.
[15] C. McMullen. Minkowski's conjecture, well-rounded lattices and topological dimension. *J. Amer. Math. Soc.*, 18(3):711–734, 2005.
[16] Y. Motohashi. On the number of integers which are sums of two squares. *Acta Arith.*, 23:401–412, 1973.
[17] R. Neelamani, S. Dash, and R. Baraniuk. On nearly orthogonal lattice bases and random lattices. *SIAM J. Discrete Math.*, 21(1):199–219, 2007.
[18] M. Pohst. On the computation of lattice vectors of minimal length, successive minima and reduced bases with applications. *ACM SIGSAM Bulletin*, 15(1):37–44, 1981.
[19] J. H. Silverman. *A Friendly Introduction to Number Theory*. Prentice Hall, 2006.
[20] L. Solomon. Zeta functions and integral representation theory. *Advances in Math.*, 26(3):306–326, 1977.
[21] G. Tenenbaum. Sur la concentration moyenne des diviseurs. *Comment. Math. Helv.*, 60(3):411–428, 1985.
[22] E. W. Weisstein. Sum of squares function. *From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/SumofSquaresFunction.html*.

Department of Mathematics, Claremont McKenna College, 850 Columbia Avenue, Claremont, CA 91711-6420

E-mail address: lenny@cmc.edu