5-1-2007

On Distribution of Integral Well-Rounded Lattices in Dimension Two

Lenny Fukshansky
Claremont McKenna College

On distribution of integral well-rounded lattices in dimension two

Lenny Fukshansky
Texas A&M University

Illinois Number Theory Fest
May 2007

Introduction

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

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

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

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

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 connection with sphere packing, covering, and kissing number problems, coding theory, and the linear Diophantine problem of Frobenius, just to name a few of the contexts.

Still, the WR condition is special enough so that one would expect WR lattices to be rather sparce among all lattices.

McMullen's theorem

In 2005 C. McMullen 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 (McMullen, 2005)**.** *Let A be a subgroup of $SL_N(\mathbb{R})$ consisting 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.*

Arithmetic problem

We consider an arithmetic problem: study the WR sublattices of $\mathbb{Z}^N$ and understand their distribution among all sublattices of $\mathbb{Z}^N$.

In this talk we describe our results for the case $N = 2$.

Question 1: Which full-rank sublattices of $\mathbb{Z}^2$ are WR?

Examples: WR sublattices of $\mathbb{Z}^2$:

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mathbb{Z}^2, \quad \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mathbb{Z}^2$$

for any $a, b \in \mathbb{Z}$ - these come from ideals in $\mathbb{Z}[i]$ and have orthogonal bases.

No orthogonal basis:

$$\begin{pmatrix} 4 & 4 \\ 3 & -3 \end{pmatrix} \mathbb{Z}^2, \quad \begin{pmatrix} 7 & 7 \\ 5 & -5 \end{pmatrix} \mathbb{Z}^2, \quad \begin{pmatrix} 7 & -1 \\ 4 & 8 \end{pmatrix} \mathbb{Z}^2$$

Gauss's criterion

Lemma 2 (Gauss)**.** *Let Λ be a full-rank sublattice of $\mathbb{Z}^2$, let $\boldsymbol{x}, \boldsymbol{y}$ be a basis for Λ, and let θ be the angle between $\boldsymbol{x}$ and $\boldsymbol{y}$. If*

$$\frac{\pi}{3} \leq \theta \leq \frac{2\pi}{3},$$

then the basis $\boldsymbol{x}, \boldsymbol{y}$ contains a minimal vector of Λ.

This leads to the following characterization of full-rank WR sublattices of $\mathbb{Z}^2$.

Lemma 3. *A sublattice $\Lambda \subseteq \mathbb{Z}^2$ of rank 2 is WR if and only if it has a basis $\boldsymbol{x}, \boldsymbol{y}$ with*

$$\|\boldsymbol{x}\| = \|\boldsymbol{y}\|, \ |\cos\theta| = \frac{|\boldsymbol{x}^t \boldsymbol{y}|}{\|\boldsymbol{x}\|\|\boldsymbol{y}\|} \leq \frac{1}{2}, \qquad (1)$$

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.

Parametrization of WR lattices

Let

$$\mathrm{WR}(\mathbb{Z}^2) = \left\{ \Lambda \subseteq \mathbb{Z}^2 \ : \ \mathrm{rk}(\Lambda) = 2,\ \Lambda \text{ is WR} \right\}.$$

Lemma 4. *Let $a, b, c, d \in \mathbb{Z}$ be such that*

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

Then

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

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

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

Lemma 5. *Let $a, b, c, d \in \mathbb{Z}$ be such that*

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

Then

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

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

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

Proposition 6. *Suppose* $\Lambda \in \mathrm{WR}(\mathbb{Z}^2)$. *Then* Λ *is either of the form as described in Lemma 4 or as in Lemma 5.*

In other words, we are able to completely describe all WR sublattices of $\mathbb{Z}^2$. Next we want to understand how they are distributed among all sublattices of $\mathbb{Z}^2$. For this, we first define and study the **minima** and **determinant** sets of elements $\mathrm{WR}(\mathbb{Z}^2)$.

Let

$$\begin{aligned}\mathfrak{M} &= \left\{ \min_{0 \neq \boldsymbol{x} \in \Lambda} \|\boldsymbol{x}\|^2 : \Lambda \in \mathrm{WR}(\mathbb{Z}^2) \right\} \\ &= \{a^2 + b^2 : a, b \in \mathbb{Z}\}.\end{aligned}$$

Let

$$\begin{aligned}\mathcal{D} &= \{\det(\Lambda) : \Lambda \in \mathrm{WR}(\mathbb{Z}^2)\} \\ &= \Big\{(a^2+b^2)cd \ : \ a, b \in \mathbb{Z}_{\geq 0},\ \max\{a,b\} > 0, \\ &\qquad\qquad c, d \in \mathbb{Z}_{>0},\ 1 \leq \frac{c}{d} \leq \sqrt{3} \Big\}.\end{aligned}$$

Determinant and minima sets

Question 2: Is the determinant of a lattice in $\mathrm{WR}(\mathbb{Z}^2)$ related to its minimum?

Not difficult to show:

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

for every $\Lambda \in \mathrm{WR}(\mathbb{Z}^2)$.

A classical result of E. Landau (1908) implies that $\mathfrak{M}$ has asymptotic density 0 in $\mathbb{Z}$, i.e.

$$\lim_{M\to\infty} \frac{|\{m \in \mathfrak{M} : m \leq M\}|}{M} = 0.$$

Theorem 7. *The set $\mathcal{D}$ has positive lower density. More precisely*

$$\liminf_{M\to\infty} \frac{|\{u \in \mathcal{D} : u \leq M\}|}{M} \geq \frac{3^{\frac{1}{4}} - 1}{2 \cdot 3^{\frac{1}{4}}} \approx 0.12008216\ldots$$

Number of WR sublattices with fixed determinant

Question 3: For a fixed $u \in \mathcal{D}$, how many lattices in $\mathrm{WR}(\mathbb{Z}^2)$ have determinant equal to u?

For each $u \in \mathbb{Z}_{>0}$, let

$$\mathcal{N}(u) = |\{\Lambda \in \mathrm{WR}(\mathbb{Z}^2) : \det(\Lambda) = u\}|,$$

so $\mathcal{N}(u) \neq 0$ if and only if $u \in \mathcal{D}$.

We will give an explicit formula for $\mathcal{N}(u)$ and investigate its rate of growth, normal order, and extremal properties. This information provides information about the distribution of elements of $\mathrm{WR}(\mathbb{Z}^2)$ among all sublattices of $\mathbb{Z}^2$.

To state an explicit formula for $\mathcal{N}(u)$, we need to introduce more notation.

Arithmetic functions

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

$$\alpha(u) = \left|\left\{(a,b) \in \mathbb{Z}^2_{\geq 0} \ : \ a^2 + b^2 = u,\ a \leq b,\ \gcd(a,b) = 1\right\}\right|,$$

if $u > 2$, and $\alpha(1) = \alpha(2) = \frac{1}{2}$.

Let

$$\beta(u) = \left|\left\{d \in \mathbb{Z}_{>0} : d \mid u \text{ and } \sqrt{\frac{u}{\sqrt{3}}} \leq d \leq \sqrt{u}\right\}\right|.$$

Also let

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

and

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

Theorem 8. *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*

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

Then:

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

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

Corollaries

Corollary 9. *If $u \in \mathbb{Z}_{>0}$ is odd, then $\mathcal{N}(u) = \mathcal{N}(2u)$.*

Corollary 10. *Let p be a prime, $k \in \mathbb{Z}_{>0}$. Let $u = p^k$ or $2p^k$. Then*

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

Corollary 11. *If $u = p_1 p_2$, where $p_1 < p_2$ are odd primes, then*

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

Hence when u is as in Corollaries 10 and 11, all full-rank WR sublattices of $\mathbb{Z}^2$ come from ideals in $\mathbb{Z}[i]$, and so have orthogonal bases.

Asymptotics

Corollary 12. *For each $u \in \mathbb{Z}_{>0}$,*

$$\mathcal{N}(u) \leq O\left(\left(\frac{\sqrt{2}\log u}{\omega(u)}\right)^{2\omega(u)}\right),$$

where $\omega(u)$ is the number of distinct prime divisors of u. Moreover,

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

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 $k \geq 1$

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

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

Example of an extremal determinant sequence

Let $v_n = \prod_{i=1}^{n} p_i^2$, where $p_1, p_2, \ldots$ are primes congruent to 1 mod 4; by Dirichlet's theorem, there are infinitely many of them: 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	6001613673020239098038402 5	14324372	12413026.85

Let $\mathcal{N}_I(v_n)$ be the number elements of WR($\mathbb{Z}^2$) with determinant v_n coming from ideals of $\mathbb{Z}[i]$. For comparison with the table above,

$$\mathcal{N}_I(v_n) = 3^n.$$

Zeta function

Define **zeta-function of WR sublattices** of $\mathbb{Z}^2$ to be

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

where $s \in \mathbb{C}$ is a complex variable. This is an example of a *Dirichlet series*.

Studying the properties of $\zeta_{\mathrm{WR}(\mathbb{Z}^2)}(s)$ yields important arithmetic information about the distribution of elements of $\mathrm{WR}(\mathbb{Z}^2)$ among all full-rank sublattices of $\mathbb{Z}^2$.

First of all, we will compare $\zeta_{\mathrm{WR}(\mathbb{Z}^2)}(s)$ to two well-known zeta functions in number theory. This will allow us to see that although WR lattices are sparce, there are more of them than one may expect.

Let

$$\begin{aligned}\zeta_{\mathbb{Z}[i]}(s) &= \sum_{I \subseteq \mathbb{Z}[i]} (\mathbb{N}(I))^{-s} \\ &= \sum_{u=1}^{\infty} \mathcal{N}_I(u) u^{-s},\end{aligned}$$

where $\mathcal{N}_I(u)$ is the number of ideals of norm u in $\mathbb{Z}[i]$. Ideals in $\mathbb{Z}[i]$ are in bijective correspondence with lattices in $\mathsf{WR}(\mathbb{Z}^2)$ that have an orthogonal basis.

Also, let

$$\begin{aligned}\zeta_{\mathbb{Z}^2}(s) &= \sum_{\Lambda \subseteq \mathbb{Z}^2} (\det(\Lambda))^{-s} \\ &= \sum_{u=1}^{\infty} F_2(u) u^{-s},\end{aligned}$$

where $F_2(u) = O(u)$ is the number of all full-rank sublattices of $\mathbb{Z}^2$ with determinant u.

Therefore

$$\mathcal{N}_I(u) \leq \mathcal{N}(u) \leq F_2(u)$$

for all $u \in \mathbb{Z}_{>0}$. Therefore $\zeta_{\mathsf{WR}(\mathbb{Z}^2)}(s)$ is "squeezed" between $\zeta_{\mathbb{Z}[i]}(s)$ and $\zeta_{\mathbb{Z}^2}(s)$.

$\zeta_{\mathbb{Z}[i]}(s)$ is analytic for all $s \in \mathbb{C}$ with $\Re(s) > 1$, and has a simple pole at $s = 1$.

$\zeta_{\mathbb{Z}^2}(s)$ is analytic for all $s \in \mathbb{C}$ with $\Re(s) > 2$, and has a simple pole at $s = 2$; u-th coefficient of $\zeta_{\mathbb{Z}^2}(s)$ is $O(u)$.

Theorem 13. *Let the notation be as above, then $\zeta_{\mathsf{WR}(\mathbb{Z}^2)}(s)$ is analytic for all $s \in \mathbb{C}$ with $\Re(s) > 1$, and has a pole of order 2 at $s = 1$, meaning that*

$$0 < \lim_{s \to 1+} |s-1|^2 \sum_{u=1}^{\infty} |\mathcal{N}(u) u^{-s}| < \infty.$$

It should be noted that in Theorem 13 we are not using the notion of a pole in a sense that would imply the existence of an analytic continuation, but only to reflect on the growth of the coefficients. In fact, $\zeta_{\mathsf{WR}(\mathbb{Z}^2)}(s)$ is unlikely to have an analytic continuation to the left of $s = 1$, however it can be expressed as a product / sum of Dirichlet series (generating functions of certain known arithmetic functions), one of which has an analytic continuation and an Euler product.