Lattices modulo N with long shortest distances

Elem. Math. 72 (2017) 111 – 121
0013-6018/17/030111-11
DOI 10.4171/EM/333

Elemente der Mathematik

Lattices modulo N with long shortest distances

Florian Pausinger

Florian Pausinger studied mathematics in Salzburg and Linz. He received a PhD from the Institute of Science and Technology Austria (IST Austria) and is currently a post doctoral researcher at Technical University Munich in the group of Geometry and Visualisation.

1 Introduction

A lattice Λ in $\mathbb{R}^2$ is a free $\mathbb{Z}$-module of rank 2, so $\Lambda = X\mathbb{Z}^2$ for some matrix $X = (\mathbf{x}_1, \mathbf{x}_2) \in \mathrm{GL}_2(\mathbb{R})$. Here, the column vectors $\mathbf{x}_1, \mathbf{x}_2$ form a basis for Λ and X is referred to as the corresponding matrix. The determinant of Λ, denoted by $\det(\Lambda)$, is defined to be $|\det(X)|$ and does not depend on the particular choice of a basis for Λ. We define $V(\Lambda)$ to be the closure of the set of all vectors in $\mathbb{R}^2$ which are closer to $\mathbf{0}$ than to any other vector of Λ; i.e., the Voronoi cell of $\mathbf{0}$ (see Figure 1). The area of the Voronoi cell is equal to $\det(\Lambda)$ and the real plane is tiled with translates $V(\Lambda)+\mathbf{y}$ for $\mathbf{y} \in \Lambda$. We inscribe a circle centered at a point of the lattice into each such translate and denote its largest possible radius with $r(\Lambda)$. Since all these circles are disjoint, we obtain a circle packing in $\mathbb{R}^2$, which is called

Im Jahre 1910 bewies Axel Thue, dass die dichteste Kreispackung in der Ebene durch die dichteste Kreisgitterpackung realisiert wird. Die dichteste Kreisgitterpackung wiederum liefert das hexagonale Bienenwabengitter, wie Lagrange schon 1773 nachwies. In der vorliegenden Arbeit geht es nun darum, eine Folge von ebenen Gittern zu konstruieren, deren Basisvektoren ganzzahlige Koordinaten haben und welche das hexagonale Gitter approximieren. Dabei kommen Methoden der elementaren Zahlentheorie zum Einsatz. Diese Gitter beantworten dann die folgende Frage: Für teilerfremde Zahlen N, a, b mit $0 < a, b < N$ definiere man die Menge

$$\{(na \pmod N, nb \pmod N) : 0 \leq n < N\}.$$

Wie gross ist die kürzeste Entfernung zwischen Punkten einer solchen Menge in Abhängigkeit von N? Welche Parameter N, a, b liefern die grösstmögliche kürzeste Distanz?

the *lattice packing* corresponding to Λ. The density of this packing is given by

$$\Delta(\Lambda) = \frac{\text{area of one circle}}{\text{area of the Voronoi cell}} = \frac{\pi r(\Lambda)^2}{\det(\Lambda)}$$

The classical lattice packing problem in $\mathbb{R}^2$ is to maximize this function on the space of all lattices and its answer goes back to works of Lagrange (1773), Gauss (1831) and Thue (1910, [11]): The density function Δ on lattices in $\mathbb{R}^2$ is maximized by the hexagonal lattice

$$\Lambda_h := \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{pmatrix} \mathbb{Z}^2.$$

The hexagonal lattice is also the solution to the general circle packing problem in $\mathbb{R}^2$ which was first proven by L. Fejes-Tóth in 1940; see [1, 2, 9].

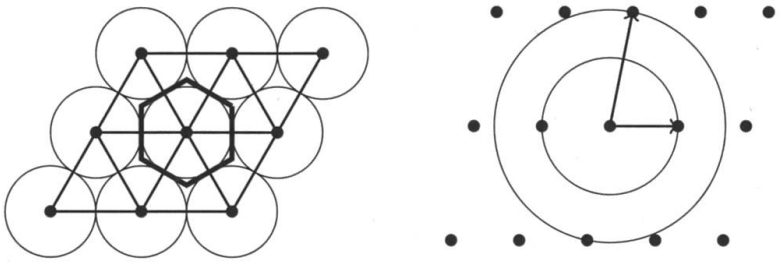

Figure 1 *Left:* The Voronoi cell $V(\Lambda_h)$ (thick) with 9 points of the lattice Λ_h and the corresponding circles and triangles. *Right:* A lattice and its successive minima.

In particular, it can be shown (see, e.g., [2] for a recent variant of the proof or [8] for a classical and elementary treatment) that if Λ is a lattice of rank 2 in $\mathbb{R}^2$, then

$$\Delta(\Lambda) \leq \Delta(\Lambda_h) = \frac{\pi}{2\sqrt{3}}$$

with equality if and only if Λ can be obtained from Λ_h by rotation and dilation; i.e., the two lattices are similar.

Finally, let B be the unit circle centered at the origin in $\mathbb{R}^2$. Given a lattice Λ, we define the *Minkowski successive minima* $\lambda_1 \leq \lambda_2$ of Λ to be

$$\lambda_i = \inf\{\lambda \in \mathbb{R}^+ : \Lambda \cap \lambda B \text{ contains } i \text{ linearly independent nonzero vectors}\},$$

in which $i = 1, 2$. We say that the vectors $\mathbf{x}_1, \mathbf{x}_2 \in \Lambda$ correspond to successive minima if they are linearly independent and

$$\|\mathbf{x}_1\| = \lambda_1, \quad \|\mathbf{x}_2\| = \lambda_2.$$

In other words, $\lambda_1 = \lambda_1(\Lambda)$ is the length of the shortest vector of the lattice Λ and as such it is equal to twice the in-radius of the largest circle inscribed in $V(\Lambda)$. Hence,

$$\Delta(\Lambda) = \frac{\pi \lambda_1^2}{4 \det(\Lambda)}.$$

In this note we are interested in approximations of Λ_h with good packing properties.

We ask:

> *How to approximate Λ_h with lattices $\Omega = X\mathbb{Z}^2$ where X is an integer matrix such that $\Delta(\Lambda_h) - \Delta(\Omega) < \varepsilon$ for a given $\varepsilon > 0$?*

We define a family of lattices Ω_s, $s \in \mathbb{N}$, as follows. Set $n = 2s + 1$ and let $b, N \in \mathbb{N}$ be such that their ratio has the particular continued fraction expansion

$$\frac{b}{N} = \frac{b_s}{N_s} = [0, b_1, b_2, \ldots, b_n] = [0, 2, 1, 2, 1, \ldots, 1, 2]; \tag{1.1}$$

see Section 3 for an explanation of this notation. With this we define

$$X_s = \begin{pmatrix} 0 & 1 \\ N_s & b_s \end{pmatrix}, \quad \Omega_s = X_s\mathbb{Z}^2, \quad \text{and prove:}$$

Theorem 1.1. *Let Ω_s and Λ_h be as defined above. If $s = 2m + 1$ is an odd integer, then*

$$\lim_{m\to\infty} \Delta(\Omega_{2m+1}) = \Delta(\Lambda_h).$$

Theorem 1.1 can be interpreted as follows: If we scale each lattice Ω_s so that its shortest vector has unit length, then this sequence of lattices converges to a limit lattice which is a rotated version of the hexagonal lattice; see Figure 2 for an illustration. We calculate the rotation angle $3\pi/4$ in Remark 4.2.

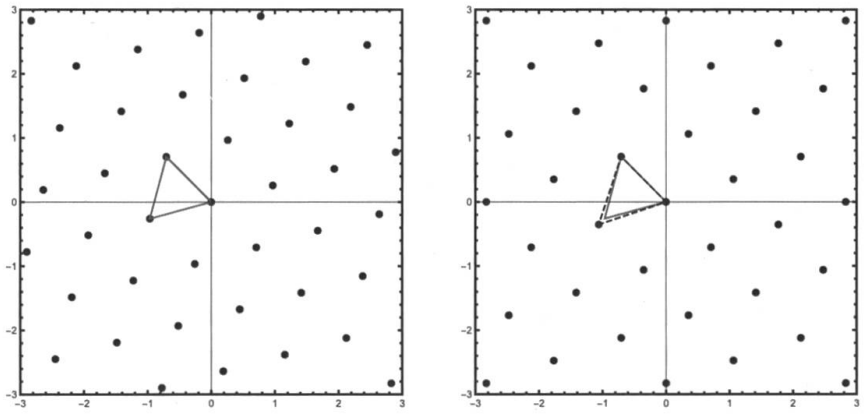

Figure 2 The rotated hexagonal lattice (*left*) and the lattice Ω_1 scaled by $1/(2\sqrt{2})$ which is the length of its shortest vector (*right*).

This result is closely related to an interesting question about lattices modulo N which was the original motivation for this note. For integers $0 < a, b < N$, with $\gcd(N, a, b) = 1$ we define the *lattice modulo N*, $\Pi_{N,a,b}$, generated by the pair (a, b) as

$$\Pi_{N,a,b} := \{(na \pmod N, nb \pmod N) : 0 \le n < N\}.$$

Thus, $\Pi_{N,a,b}$ is a subset of the square $[0, N-1]^2$. We are interested in the *shortest distance* between points of $\Pi_{N,a,b}$. This distance is exactly given by the length of the shortest vector

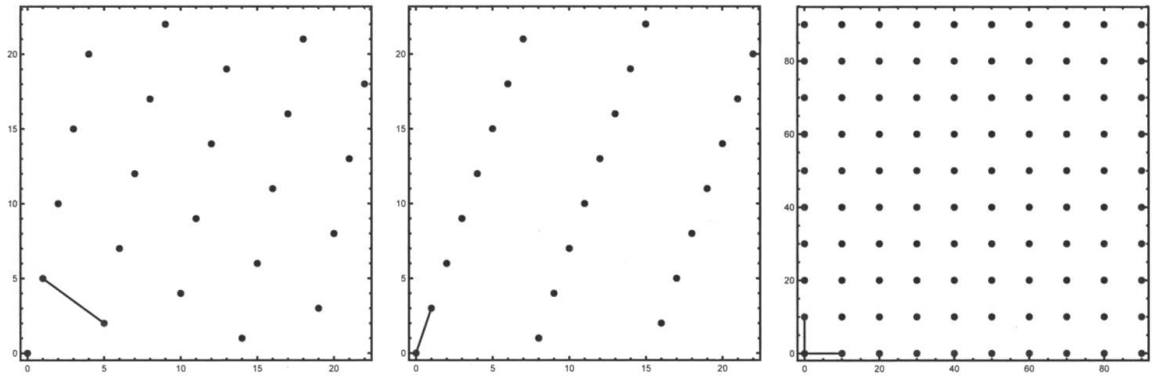

Figure 3 The *left* lattice modulo 23 does not contain the shortest vector of the corresponding lattice, whereas the lattice modulo 23 in the *middle* contains the shortest vector. On the *right* is the regular grid G_{100} with $f(G_{100}) = 1$.

of the lattice Π that is generated by the vectors (a, b), $(0, N)$, $(N, 0)$. Thus, whenever we work with lattices modulo N, we abuse notation and write $\lambda_1(\Pi_{N,a,b})$ for the shortest distance between points in $\Pi_{N,a,b}$; see Figure 3.

For every lattice $\Pi_{N,a,b}$ with $\gcd(N, a, b) = 1$ and arbitrary, distinct points $X = (na, nb)$, $Y = (ma, mb)$, we have that $\|(X - Y) \pmod N\| \geq \sqrt{2}$. Together with a simple area argument [6, Lemma 3.1], we obtain

$$\sqrt{2} \leq \lambda_1(\Pi_{N,a,b}) \leq 3/2\sqrt{N}.$$

Using this observation, we would like to compare the shortest vectors of different lattices. Thus, we define

$$f(\Pi_{N,a,b}) := \lambda_1(\Pi_{N,a,b})/\sqrt{N}.$$

Let $N = n^2$ and $G_N \subset [0, n^2 - n]^2$ be the regular grid generated by $(n, 0)$ and $(0, n)$; see Figure 3. It is easy to see that

$$\lambda_1(G_N)/\sqrt{N} = 1.$$

Naturally, we would like to know whether there is a systematic way to generate lattices modulo N with $f(\Pi_{N,a,b}) \approx 1$ for all N. This question was answered affirmatively in [6, Theorem 1.3]. Interestingly, one can show even more: namely that for infinitely many N there exists a pair of integers $(\tilde{a}, \tilde{b})$ such that $f(\Pi_{N,\tilde{a},\tilde{b}}) > 1$; [6, Theorem 1.4]. This result motivates to ask:

> *How large can $f(N, a, b)$ be? How do lattices with long shortest vectors look like?*

Since the densest circle packing in the plane is realized by the hexagonal lattice, we assume to have N points arranged on a scaled regular hexagonal lattice with edge length z contained in $[0, N - 1]^2$. How long can z be? Ignoring boundary effects, each point is contained in 6 equilateral triangles and, thus, we have roughly $6N/3 = 2N$ triangles in our lattice; see Figure 1. Since the area of an equilateral triangle of edge length z is $\sqrt{3}/4 \cdot z^2$,

we can roughly compute the maximal possible edge length $z = z(N)$ as

$$\max_{z\in\mathbb{R}} 2N \cdot \frac{\sqrt{3}}{4} z^2 \le (N-1)^2 \quad \Rightarrow \quad z \approx \sqrt{N}\sqrt{\frac{2}{\sqrt{3}}} \approx 1.07457\sqrt{N}.$$

Setting $f_{\max}(N) := \max_{1\le a,b\le N} f(\Pi_{N,a,b})$, we answer [6, Question 1.10] and prove in a constructive way that there exist lattices modulo N that come arbitrarily close to this value:

Theorem 1.2. *For every $\varepsilon > 0$, there exist infinitely many N such that*

$$f_{\max}(N) > \sqrt{\frac{2}{\sqrt{3}}} - \varepsilon.$$

Remark 1.3. It is possible to generalize (1.1) and consider integers b, N such that

$$\frac{b}{N} = \frac{b_{k,s}}{N_{k,s}} = [0, b_1, b_2, \ldots, b_n] = [0, k, 1, k, 1, \ldots, 1, k],$$

for arbitrary $k \in \mathbb{N}$, denoting the corresponding lattices $\Omega_{k,s}$. We can calculate the length of the shortest vectors of all lattices of the family $\Omega_{k,s}$ with our method and note that the lattices for small values of k have also long shortest vectors. However, it can be shown that

$$\max_k f(\Omega_{k,s}) = f(\Omega_{2,s}) \quad \text{and} \quad f(\Omega_{k,s}) \ge f(\Omega_{k+1,s}) \tag{1.2}$$

for all odd $s \ge 3$ and $k \ge 2$. We omit the proof of the general case in the following, since it is very technical, without adding any new insights.

2 Connection to other problems

We briefly describe two situations in which the answer to our problem is of interest. First, we consider the famous traveling salesman problem which asks for the length $\mathcal{L}(x_1, \ldots, x_N)$ of the shortest path through the points $\{x_1, \ldots, x_N\} \subset \mathbb{R}^d$. Setting $x_{\sigma(N+1)} := x_{\sigma(1)}$, we write

$$\mathcal{L}(x_1, \ldots, x_N) = \min_\sigma \sum_{n=1}^{N} \|x_{\sigma(n)} - x_{\sigma(n+1)}\|,$$

where the minimum is over all permutations σ of $\{1, 2, \ldots, N\}$. It can be shown that the length of the shortest path through all points of the lattice $\Pi_{N,a,b}$ (scaled to $[0,1]^2$) is essentially equal to $\lambda_1(\Pi_{N,a,b})$; see [6]. Thus, our results give an idea how long shortest paths through the points of a lattice modulo N can possibly be. This is especially interesting with respect to a result of Karloff [4], who obtained a general upper bound of $1.39159\sqrt{N} + 11$ for the length of the traveling salesman tour through any set of N points in $[0,1]^2$.

As a second appearance of our problem, we suppose to find ourselves on the two-dimensional torus $\mathbb{T}^2$ equipped with N candles and want to position the candles in such a way

that they heat up the space as efficiently as possible. In [7] a general construction of point sets was given that uses elementary number theory as the basic ingredient ensuring a fast heating of the space. Interestingly, for a given N the quantity

$$g(N) := \max_{1\le p\le N-1} \min_{\substack{(k,m)\in\mathbb{Z}^2\\(k,m)\neq(0,0)}} \left\{k^2+m^2 : m\cdot p+k\equiv 0 \mod N\right\},$$

plays a crucial role. Geometrically, $g(N)$ is determined by the largest shortest vector arising in the $N-1$ lattices spanned by $(1,-p)$ and $(0,-N)$ for $1\le p\le N-1$, since $m\cdot p+k\equiv 0$ if and only if (m,k) is of the form $t_1(1,-p)+t_2(0,-N)$ for $t_1,t_2\in\mathbb{Z}$.

3 Properties of the denominators of the convergents

In this section we study algebraic expressions of the form

$$b_0+\cfrac{1}{b_1+\cfrac{1}{b_2+\ldots+\frac{1}{b_n}}}, \tag{3.1}$$

for non-negative integers $b_0,\ldots,b_n$. We refer to the classical book of Khinchin [5] for a thorough introduction into this topic. Here, we just recall the most important notions and facts required to prove our results. An expression of the form (3.1) is called *finite continued fraction* and can be represented as the ratio of two polynomials, or, in case $b_0,\ldots,b_n$ have concrete numerical values, as an ordinary fraction p_n/q_n. Usually, an expression of the form (3.1) is written in a shorter way as $[b_0,b_1,\ldots,b_n]$. Truncating a given continued fraction after its first i, $1\le i\le n-1$, elements results in a fraction p_i/q_i which is called an ith order convergent of p_n/q_n. It can be shown that the fractions p_i/q_i become better and better approximations of p_n/q_n as i increases.

We are interested in the particular palindromic continued fraction of the form

$$\frac{b}{N}=[0,b_1,b_2,\ldots,b_n]=[0,2,1,2,1,\ldots,1,2]. \tag{3.2}$$

In the following we write q_i for the denominators of the convergents of the particular fraction b/N. First, we determine the general form of the q_i, before we obtain an important inequality for these numbers.

Lemma 3.1. *Let $n=2s+1$. If $N,b\in\mathbb{N}$ are as in (3.2), then*

$$q_i=\begin{cases}\frac{1}{2\sqrt{3}}\left((2-\sqrt{3})^m(\sqrt{3}-1)+(2+\sqrt{3})^m(\sqrt{3}+1)\right) & \text{if } i=2m \text{ is even,}\\ \frac{1}{\sqrt{3}}\left((2+\sqrt{3})^{m+1}-(2-\sqrt{3})^{m+1}\right) & \text{if } i=2m+1 \text{ is odd.}\end{cases}$$

Proof. According to [5, Theorem 1] we obtain the denominators of the convergents of b/N via the recurrence

$$q_i=b_i\cdot q_{i-1}+q_{i-2},$$

with $q_0 = 1$ and $q_1 = b_1$. Consequently we get two different equations in our case depending on the parity of i:

$$q_{2m} = q_{2m-1} + q_{2m-2} \tag{3.3}$$

$$q_{2m+1} = 2 \cdot q_{2m} + q_{2m-1}. \tag{3.4}$$

Setting $q_{2m} = A_m$ and $q_{2m+1} = B_m$ we can rewrite (3.3) and (3.4) as

$$A_m = 4A_{m-1} - A_{m-2}, \quad \text{and} \quad B_m = A_{m+1} - A_m.$$

We solve the first recurrence for A_m via the characteristic equation

$$r^2 - 4r + 1 = 0,$$

and obtain

$$r_1 = 2 - \sqrt{3} \quad \text{and} \quad r_2 = 2 + \sqrt{3}.$$

Setting

$$A_0 = 1 = \alpha_1 r_1^0 + \alpha_2 r_2^0, \quad \text{and} \quad A_1 = 1 + b_1 = 3 = \alpha_1 r_1^1 + \alpha_2 r_2^1,$$

we get

$$\alpha_1 = 1 - \frac{3 - r_1}{r_2 - r_1}, \quad \text{and} \quad \alpha_2 = \frac{3 - r_1}{r_2 - r_1}.$$

The general solution is then given by $A_m = \alpha_1 r_1^m + \alpha_2 r_2^m$, from which we obtain the stated closed form expressions for the q_i. □

To illustrate this lemma and to motivate the next, let us look at a concrete example. Set $n = 7 = 2 \cdot 3 + 1$ to obtain

$$[0, 2, 1, 2, 1, 2, 1, 2] = \frac{41}{112} = \frac{b_3}{N_3}.$$

It is an easy exercise to calculate the 6 convergents,

$$\frac{1}{2}, \frac{1}{3}, \frac{3}{8}, \frac{4}{11}, \frac{11}{30}, \frac{15}{41},$$

by hand and to verify the values of the denominators with our formula. Interestingly, we can observe even more from these values:

$$q_1^2 + q_5^2 = 4 + 900 > q_2^2 + q_4^2 = 9 + 121 > q_3^2 + q_3^2 = 64 + 64.$$

This is not a coincidence, but holds in general as the following lemma shows.

Lemma 3.2. *Let $n = 2s + 1$ with $s \geq 3$. If $N, b \in \mathbb{N}$ are as in (1.1) then, for $i = 1, \ldots, s - 1$,*

$$\left\| \begin{pmatrix} q_i \\ q_{n-i-1} \end{pmatrix} \right\| \geq \left\| \begin{pmatrix} q_{i+1} \\ q_{n-i-2} \end{pmatrix} \right\|.$$

Proof. We note that $0 < 2-\sqrt{3} < \sqrt{3}-1 < 1$. In the following we first prove the assertion for $i = 1, \dots, s-2$ and distinguish two cases depending on the parity of i. If $i = 2m$, then

$$\frac{1}{2\sqrt{3}}\left(1+(1+\sqrt{3})(2+\sqrt{3})^m\right) > q_{2m} > \frac{1}{2\sqrt{3}}\left((1+\sqrt{3})(2+\sqrt{3})^m\right).$$

On the other hand, if $i = 2m+1$, then

$$\frac{1}{\sqrt{3}}(2+\sqrt{3})^{m+1} > q_{2m+1} > \frac{1}{\sqrt{3}}\left((2+\sqrt{3})^{m+1}-1\right).$$

To prove the assertion we set $X = 2+\sqrt{3}$ and show that $q_i^2 + q_{n-i-1}^2 - q_{i+1}^2 - q_{n-i-2}^2$ is positive.

Case 1: If $i = 2m$ then

$$\begin{aligned} q_{2m}^2 - q_{2m+1}^2 &\geq \frac{1}{12}(1+\sqrt{3})^2 X^{2m} - \frac{1}{3}X^{2m+2} \\ &= -X^{2m+2}\left(\frac{(1+\sqrt{3})^2}{12X^2} - \frac{1}{3}\right). \end{aligned}$$

Moreover,

$$\begin{aligned} q_{2(s-m)}^2 - q_{2(s-m-1)+1}^2 &\geq \frac{1}{12}(1+\sqrt{3})^2(2+\sqrt{3})^{2(s-m)} - \frac{1}{3}X^{2(s-m)} \\ &= X^{2(s-m)}\left(\frac{(1+\sqrt{3})^2}{12} - \frac{1}{3}\right). \end{aligned}$$

By assumption $2 \leq i = 2m \leq s-2$ and $s \geq 3$, hence $2(s-m)-2(m+1) = 2s-4m-2 \geq 2$. We continue our calculation and multiply the above results by $X^{-2(m+1)}$ before we sum them to obtain

$$\begin{aligned} &X^{2(s-m)-2(m+1)}\left(\frac{(1+\sqrt{3})^2}{12} - \frac{1}{3}\right) - \frac{(1+\sqrt{3})^2}{12X^2} + \frac{1}{3} \\ &\qquad \geq 3^2\left(\frac{(1+\sqrt{3})^2}{12} - \frac{1}{3}\right) - \frac{(1+\sqrt{3})^2}{12\cdot 3^2} + \frac{1}{3} > 0, \end{aligned}$$

where we used that $X > 3$.

Case 2: If $i = 2m+1$ then

$$\begin{aligned} q_{2m+1}^2 - q_{2(m+1)}^2 &\geq \frac{1}{3}\left(X^{m+1}-1\right)^2 - \frac{1}{12}\left(1+(1+\sqrt{3})X^{m+1}\right)^2 \\ &= X^{2(m+1)}\left(\frac{1}{3} - \frac{(1+\sqrt{3})^2}{12} + \frac{1}{4X^{2(m+1)}} - \frac{5+\sqrt{3}}{6X^{m+1}}\right). \end{aligned}$$

Since $X > 3$ we see that the expression in brackets is for every non-negative m bounded by -1 and 0. Next,

$$\begin{aligned} q_{2(s-m-1)+1}^2 - q_{2(s-m-1)}^2 &\geq \frac{1}{3}\left(X^{s-m}-1\right)^2 - \frac{1}{12}\left(1+(1+\sqrt{3})X^{s-m-1}\right)^2 \\ &= \frac{X^{2(s-m)}}{3} - \frac{2X^{s-m}}{3} + \frac{1}{4} - \frac{(1+\sqrt{3})X^{s-m-1}}{6} - \frac{(1+\sqrt{3})^2 X^{2(s-m-1)}}{12} \\ &\geq X^{2(s-m)}\left(\frac{1}{3} - \frac{(1+\sqrt{3})^2}{12\cdot 3^2} + \frac{1}{4X^{2(s-m)}} - \frac{13+\sqrt{3}}{18X^{s-m}}\right), \end{aligned}$$

in which we used again that $X > 3$. Moreover, we observe that the expression in brackets is positive:

$$\begin{aligned} &\frac{1}{3} - \frac{(1+\sqrt{3})^2}{12\cdot 3^2} + \frac{1}{4X^{2(s-m)}} - \frac{13+\sqrt{3}}{18X^{s-m}} \\ &\qquad \geq \frac{1}{3} - \frac{(1+\sqrt{3})^2}{12\cdot 3^2} - \frac{13+\sqrt{3}}{18\cdot 9} > 0.17. \end{aligned}$$

Since $2s - 4m - 2 \geq 2$, and $X^2 > 3^2$ it follows that

$$q_{2m+1}^2 - q_{2(m+1)}^2 + q_{2(s-m-1)+1}^2 - q_{2(s-m-1)}^2 > 0.$$

Finally, a direct calculation verifies the assertion for $i = s-1$ as well. □

4 Shortest vectors

In this section we determine the shortest vectors of the lattices Ω_s. Already Gauss [3] invented an algorithm that finds a reduced basis of a 2-dimensional integral lattice. Therefore, arrange the given basis such that b_1 is shorter than b_2 and find $k \in \mathbb{Z}$ such that $b_2 - kb_1$ is of minimal Euclidean length. Then replace the vector b_2 by the vector $(b_2 - kb_1)$ and repeat this procedure until $k = 0$. If $k = 0$, return the pair (b_1, b_2). The shorter of the two basis vectors is then the desired shortest vector of the lattice.

Lemma 4.1. *Let $n = 2s+1$ and $s \geq 3$. If $N, b \in \mathbb{N}$ are as in (1.1) then the shortest vector of $\Pi_{N,1,b} = \Omega_s$ is $\left((-1)^s q_s, q_s\right)$.*

Proof. We start with the vectors $(1, b)$, $(N, 0)$, $(0, N)$ and use the method outlined in [10, Section 3] to compute a basis of this lattice. In particular, we obtain

$$(1, (1-N)b) \quad \text{and} \quad (0, N),$$

which we immediately reduce to $(1, b)$, $(0, N)$.

We can rewrite these two vectors as (q_0, q_{n-1}), (q_{-1}, q_n). In the next reduction step we replace the longer vector $(0, N)$ as follows:

$$\begin{pmatrix} 0 \\ N \end{pmatrix} - b_n \begin{pmatrix} 1 \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ q_n \end{pmatrix} - b_n \begin{pmatrix} q_0 \\ q_{n-1} \end{pmatrix} = \begin{pmatrix} -q_1 \\ q_{n-2} \end{pmatrix},$$

since $b_n = b_1$. In the second step we obtain

$$\begin{pmatrix} q_0 \\ q_{n-1} \end{pmatrix} - b_{n-1} \begin{pmatrix} -q_1 \\ q_{n-2} \end{pmatrix} = \begin{pmatrix} q_2 \\ q_{n-3} \end{pmatrix}.$$

Applying Lemma 3.2 we conclude again that (q_0, q_{n-1}) is longer than both $(-q_1, q_{n-2})$ and (q_2, q_{n-3}) and is thus replaced. To turn to the general step we assume that

$$\begin{pmatrix} (-1)^i q_i \\ q_{n-i-1} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} (-1)^{i+1} q_{i+1} \\ q_{n-i-2} \end{pmatrix}$$

is the reduced basis after the ith reduction step for $i = 1, \ldots, s-2$. Then, we can reduce this basis:

$$\begin{pmatrix} (-1)^i q_i \\ q_{n-i-1} \end{pmatrix} - b_{n-i-1} \begin{pmatrix} (-1)^{i+1} q_{i+1} \\ q_{n-i-2} \end{pmatrix} = \begin{pmatrix} (-1)^{i+2} q_{i+2} \\ q_{n-i-3} \end{pmatrix}.$$

By Lemma 3.2 we can repeat this procedure until we reach $((-1)^s q_s, q_s)$. Consequently this vector is the shortest vector of the lattice. □

Hence, we get if s is odd

$$\lim_{s\to\infty} \frac{\lambda_1(\Omega_s)}{\sqrt{N_s}} = \lim_{s\to\infty} \sqrt{\frac{2q_s^2}{q_{2s+1}}} = \sqrt{\frac{2}{\sqrt{3}}} = 1.0745\ldots,$$

which finishes the proof of Theorem 1.2. For completeness, if s is even, then

$$\lim_{s\to\infty} \frac{\lambda_1(\Omega_s)}{\sqrt{N_s}} = \lim_{s\to\infty} \sqrt{\frac{2q_s^2}{q_{2s+1}}} = \sqrt{\frac{1}{\sqrt{3}}} = 0.7598\ldots.$$

Lemma 4.1 also implies a proof of Theorem 1.1. Since the shortest vector of Ω_s is given by $((-1)^s q_s, q_s)$ we obtain for odd s,

$$\Delta(\Omega_s) = \frac{\pi\ 2q_s^2}{4\det(\Omega_s)} = \frac{\pi}{4}\frac{2q_s^2}{q_{2s+1}} \overset{s\to\infty}{\longrightarrow} \frac{\pi}{4}\frac{2}{\sqrt{3}} = \Delta(\Lambda_h).$$

Remark 4.2. Finally, we calculate the rotation angle for the hexagonal grid that we announced in the introduction. We know from Lemma 4.1 that $(-q_s, q_s)$ is the shortest vector of Ω_s for odd s. Dividing this vector by its length gives a vector of unit length that points in the same direction. We observe that

$$\lim_{m\to\infty} \frac{(-q_{2m+1}, q_{2m+1})}{\|(-q_{2m+1}, q_{2m+1})\|} = \left(-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right),$$

and the angle between $(1, 0)$ and $(-1/\sqrt{2}, 1/\sqrt{2})$ is just $\arccos(-1/\sqrt{2}) = 3\pi/4$.

References

[1] J.H. Conway, N.J.A. Sloane, Sphere Packings, Lattices and Groups. 3rd Edition, Springer, 1999.

[2] L. Fukshansky, Revisiting the hexagonal lattice: On optimal lattice circle packing. Elem. Math. **66** (2011), 1–9.

[3] C.F. Gauss, Disquisitiones arithmeticae. Gerh. Fleischer. Jun., 1801.

[4] H. Karloff, How long can a Euclidean traveling salesman tour be? SIAM J. Discrete Math. **2** (1989), no. 1, 91–99.

[5] A.Y. Khinchin, Continued Fractions. Dover, 1997.

[6] F. Pausinger, Bounds for the traveling salesman paths of two-dimensional modular lattices. To appear in: Journal of Combinatorial Optimization, doi: 10.1007/s10878-016-0043-7

[7] F. Pausinger, S. Steinerberger, Heating a room with number theory, submitted 2016.

[8] C.A. Rogers, The packing of equal spheres, Proc. London Math. Soc. **8** (1958), 447–465.

[9] C.A. Rogers, Packing and Covering. Cambridge University Press, 1964.

[10] G. Rote, Finding a shortest vector in a two-dimensional lattice modulo m. Theoret. Comput. Sci. **172** (1997), 303–308.

[11] A. Thue, Über die dichteste Zusammenstellung von kongruenten Kreisen in der Ebene, Norske Vid. Selsk. Skr. **1** (1910), 1–9.

Florian Pausinger
TU München
Zentrum Mathematik (M10)
D-85748 Garching, Germany
e-mail: florian.pausinger@gmx.at