LONG SHORTEST VECTORS IN THREE DIMENSIONAL LATTICES

FLORIAN PAUSINGER

Abstract. For coprime integers \( N, a, b, c \), with \( 0 < a < b < c < N \), we define the set
\[
\{(na \pmod{N}, nb \pmod{N}, nc \pmod{N}) : 0 \leq n < N\}.
\]
We study which parameters \( N, a, b, c \) generate point sets with long shortest distances between
the points of the set in dependence of \( N \). As a main result, we present an infinite family of
lattices whose appropriately normalised shortest vectors converge to a heuristic upper bound
based on the optimal lattice packing in \( \mathbb{R}^3 \).

1. Introduction
We are interested in point sets
\[
\Pi_{N, \mathbf{v}} := \{(na \pmod{N}, nb \pmod{N}, nc \pmod{N}) : 0 \leq n < N\},
\]
in which \( \mathbf{v} = (a, b, c) \) such that \( a \neq b \neq c \) and \( \gcd(N, a) = 1 \), which ensures that we have \( N \)
different points in the cube \([0, N - 1]^3\). Defining the shortest distance between points in \( \Pi_{N, \mathbf{v}} \)
as
\[
\lambda_3(\Pi_{N, \mathbf{v}}) := \min_{x, y \in \Pi_{N, \mathbf{v}}} \|x - y\|,
\]
we ask:
(Q1) How long can the shortest distance between points of such sets be in dependence of \( N \)?
(Q2) How to explicitly construct sets with long shortest distances?

We start with simple bounds on \( \lambda = \lambda_3(\Pi_{N, \mathbf{v}}) \). By the definition of our sets, the shortest
possible distance between two points is \( \sqrt{6} \) for a difference vector containing \( 1, -1, \pm 2 \). On the
other hand, assume that \( \lambda \) is a shortest distance. Our point sets always contain \((0, 0, 0)\) and are
always contained in the cube \([0, N - 1]^3\). Therefore, a ball of radius \( \lambda \) centered at \((0, 0, 0)\) (resp.
its intersection with the cube \([0, N - 1]^3\) which is \(1/8\) of the ball) will never contain any other
point of the set. In particular, we can attach such a fraction of a ball of radius \( \lambda \) to any point
in the set. This yields a simple upper bound on \( \lambda \) since we know that our point set is contained
in a cube of volume \((N - 1)^3\) and we can attach a fraction of an empty ball of radius \( \lambda \) to every
point. Therefore,
\[
\sqrt{6} \leq \lambda_3(\Pi_{N, \mathbf{v}}) \leq C \cdot N^{2/3},
\]
for a constant \( C > 0 \).

The main aim of this note is to answer (Q1) and (Q2). We derive a heuristic upper bound
for the maximal, normalised shortest distance between two points in sets of the form \( \Pi_{N, \mathbf{v}} \)
based on optimal lattice packing; i.e. we determine the constant \( C \) heuristically. Furthermore,
in Theorem 3 we present a parametrised family of lattices whose normalised shortest distance
converges (from below) to the upper bound as the parameter goes to infinity.

In the following we recall some basic notions and relate our point sets to lattices in \( \mathbb{R}^3 \) before
we state our main results and discuss previous work in Section 2. Section 3 contains a detailed
discussion of numerical results as well as of a remarkable lattice while Section 4 contains the
proofs our main results.

2010 Mathematics Subject Classification. Primary (11P21, 52C07); Secondary (11H31, 11B50).
Key words and phrases. shortest vector; shortest distance; lattice; sequences (mod \( m \)).
1.1. Lattices and reduced basis. Let $X = \{v_1, \ldots, v_d\}$ be linearly independent vectors in $\mathbb{R}^d$. The lattice generated by $X$ is the set
\[ \Lambda(X) = \left\{ \sum_{i=1}^d x_i \cdot v_i : x_i \in \mathbb{Z} \right\} = \{X \cdot x : x \in \mathbb{Z}^d\} \]
of all integer linear combinations of the vectors in $X$, and the set $X$ is called a basis for the lattice. Two bases $X, X'$ generate the same lattice, i.e. $\Lambda(X) = \Lambda(X')$, if and only if there exists a unimodular matrix $U$ such that $X = X'U$; see [1].

Now we restrict to three-dimensional lattices.

**Definition 1.** A basis $X = \{v_1, v_2, v_3\}$ of a three dimensional lattice in $\mathbb{R}^3$ is reduced if its vectors satisfy:

1. $\|v_1\| \leq \|v_2\| \leq \|v_3\|$;
2. $\|v_2 + x_1 v_1\| \geq \|v_2\|$ and $\|v_3 + x_2 v_2 + x_1 v_1\| \geq \|v_3\|$ for all integers $x_1, x_2$.

We refer to $\Pi$ for a three-dimensional lattice reduction algorithm. Importantly, the shortest vector in a reduced basis is always the shortest vector of the lattice.

A basic, but important observation is that our point sets can be obtained as intersections of the cube $[0, N - 1]^3$ with three-dimensional integer lattices and the shortest distance in our point sets is given by the shortest vector of the underlying lattices. (Note however that the shortest vector of the underlying lattice need not be an element of our sets!) A second basic, but important observation is that the shortest distance of a point set does not change when we change the order of the generating vector; i.e. $\lambda_3(\Pi_{N,v}) = \lambda_3(\Pi_{N,v'})$ if $v = (a, b, c)$ and $v' = (c, a, b)$ or any other permutation of $a, b, c$. Hence, we can assume $a < b < c$. In particular, our assumptions on $N, a, b, c$ allow us to restrict to generating vectors of the form $(1, b, c)$, since we can always solve the congruence
\[ a \cdot n' \equiv 1 \pmod{N}. \]
Therefore, we can replace the generating vector $(a, b, c)$ with $(n'a, n'b, n'c) = (1, b', c')$ in which $n'$ is such that $n'a \equiv 1 \pmod{N}$, $n'b \equiv b' \pmod{N}$ and $n'c \equiv c' \pmod{N}$ generate the same set of points. Restricting to generating vectors of the form $(1, b, c)$ gives a particularly simple generating matrix for the underlying lattices.

**Lemma 1.** Let $v = (1, b, c)$ with $b < c$. Then
\[ \Pi_{N,v} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & N & b \\ N & 0 & c \end{pmatrix} \mathbb{Z}^3 \cap [0, N - 1]^3 \]

**Proof.** Note that we can always find unique integers $x, y$ such that $0 < Nx + nb < N$ and $0 < Ny + nc < N$ for $1 \leq n \leq N - 1$. Every point in $\Pi_{N,v}$ can thus be obtained by multiplying the matrix with $(y, x, n)$. On the other hand it is easy to see that these are the only vectors in $\mathbb{Z}^3$ that yield points in $[0, N - 1]^3$. □

2. Main results

2.1. A heuristic for the three-dimensional case. We use the connection to lattices and their shortest vectors to refine the upper bound on the longest shortest distance. It is well known and was first shown by Gauss in 1831 that the face-centered cubic (FCC) lattice
\[ \Omega := \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \mathbb{Z}^3 \]
gives the densest (sphere) lattice packing in $\mathbb{R}^3$. In fact, the FCC lattice gives the densest packing among all lattices according to the famous Kepler Conjecture which was finally settled by Hales and Ferguson [4, 6] utilising an approach of Fejes Tóth [2] as well as state-of-the-art
formal proof techniques [5]; see also [12]. Importantly, the shortest vector in the FCC lattice is exactly twice the radius of the spheres which are centered at the nodes of the lattice. We can refine the volume argument of the previous section to get an accurate value for the constant in the upper bound.

We recall that the the FCC lattice can be built out of the basic cube in Figure 1. Ignoring boundary effects, each of the $N$ points is contained in 8 basic cubes and each basic cube contains 4 lattice points. Thus, we can build $2N$ basic cubes with edge length $\ell$. We are looking for the maximal edge length $\ell$ such that all $2N$ basic cubes fit into $[0,N-1]^3$:

$$\max_{\ell \in \mathbb{R}} 2N\ell^3 \leq (N-1)^3 \Rightarrow \ell \approx \frac{N^{2/3}}{\sqrt[3]{2}}.$$

The shortest distances between the nodes of this lattice are the face diagonals. Thus, we get an accurate idea of the constant $C$ in (1):

$$C \approx \frac{1}{\sqrt[3]{2}} \sqrt{2} = 2^{1/6} \approx 1.122.$$

![Figure 1. Basic building block of FCC lattice.](image)

2.2. The two-dimensional case. In [8] the two-dimensional variant of the problem was studied. It is well known that the hexagonal lattice

$$\Lambda_h = \left( \begin{array}{cc} 1 & 1/2 \\ 0 & \sqrt{3}/2 \end{array} \right) \mathbb{Z}^2$$

maximises the packing density in $\mathbb{R}^2$; see [3, 9, 10]. We define

$$\Pi_{N,(a,b)} := \{(na \mod N, nb \mod N) : 0 \leq n < N\}$$

and $\lambda_2(\Pi_{N,(a,b)}) := \min_{x,y \in \Pi_{N,(a,b)}} \|x - y\|$. It turns out that the shortest distance in any two-dimensional set $\Pi_{N,(a,b)}$ satisfies

$$\sqrt{2} \leq \lambda_2(\Pi_{N,(a,b)}) \leq \sqrt{N} \sqrt{2/\sqrt{3}},$$

in which the upper bound follows from the assumption that the $N$ points are arranged on a scaled regular hexagonal lattice in $[0,N-1]^2$, while the lower bound follows from the definition. Set $n = 2s + 1$ and define

$$\frac{b_s}{N_s} = [0, b_1, b_2, \ldots, b_n] = [0, 2, 1, 2, 1, \ldots, 1, 2]$$

via this particular continued fraction expansion. It was then shown that the particular family of integer lattices

$$X_s = \left( \begin{array}{cc} 0 & 1 \\ N_s & b_s \end{array} \right) \mathbb{Z}^2$$

converges to (a rotated and scaled version of) the hexagonal lattice as the parameter $s$ approaches infinity; i.e. the lattice packing density and therefore the normalised length, $\lambda_2(\Pi_{N_s,(1,b_s)})/\sqrt{N}$, of the shortest vector converge to the respective values of the hexagonal lattice.
2.3. Main result and numerical observations. Having the heuristic upper bound and knowing that the problem can be fully resolved in two dimensions motivates to look for optimal lattices in three dimensions. As a main result we show how to construct lattices, $\Pi_{N,v}$, whose normalised shortest distance is arbitrarily close to $2^{1/6}$.

**Theorem 1.** For every $\varepsilon > 0$ there exist infinitely many pairs $(N,v)$ such that
\[
\frac{\lambda_3(\Pi_{N,v})}{N^{2/3}} > 2^{1/6} - \varepsilon.
\]

See Theorem 3 in Section 4 for an explicit construction of such lattices. This construction is based on our extensive numerical analysis of all lattices, $\Pi_{N,v}$, up to $N = 310$; see Figure 2 (left). From these observations it appears at first as if it is not possible to obtain lattices with the longest possible shortest distances. The best lattice we can find up to $N = 310$ is for the parameters $N = 244$ with $v = (1,13,169)$. We will study this remarkable lattice which led to our explicit constructions in the next section.

Furthermore, we present a similar construction in Theorem 2 of lattices such that the normalised shortest distance converges to 1. While the first family of lattices can be interpreted as an approximation of the FCC lattice, the second family approximates a cubic lattice. To see this, set $N = n^3$ and look at the set
\[
G_n = \begin{pmatrix} n^2 & 0 & 0 \\ 0 & n^2 & 0 \\ 0 & 0 & n^2 \end{pmatrix} \mathbb{Z}^3 \cap [0,N-1]^3.
\]
Then
\[
\frac{\lambda_3(G_n)}{n^{2/3}} = \frac{n^2}{n^2} = 1.
\]
We close this section with an open problem for which we expect an affirmative answer.

**Problem 1.** Prove that there exists an absolute $\varepsilon > 0$ such that for every $N > N_0$ there is a generating vector $v = (1,b,c)$ with $1 < b < c < N$ and
\[
\frac{\lambda_3(\Pi_{N,v})}{N^{2/3}} > 1 + \varepsilon.
\]

**Remark 1.** If we relax the condition on the generating vector to $\gcd(N,a,b,c) = 1$, then we can also get very good lattices for small $N$ as the examples $N = 20$, $v = (6,15,18)$ for which we get $\lambda_3(\Pi_{N,v})/N^{2/3} = 1.0942 \ldots$ or $N = 78$, $v = (15,65,75)$ with $\lambda_3(\Pi_{N,v})/N^{2/3} = 1.09965 \ldots$ show. However, in general it seems that there is no systematic improvement as shown in Figure 2 (right) at least for $10 \leq N \leq 80$. 

![Figure 2](image-url)
3. A remarkable lattice

The lattice for $N = 244$ and $v = (1, 13, 169)$ has several remarkable properties which helped to find the family of lattices presented in Theorem 2 and Theorem 3 and which gives an idea why lattices with long short vectors seem so rare and hard to find. First, we notice that $b^2 = c$, i.e. $13^2 = 169$, and that $b \cdot c = b^3 = 2197 \equiv 1 \pmod{244}$. This property has important implications. If we look at the three two-dimensional orthogonal projections of the lattice, i.e. the lattices generated by

$$
\begin{pmatrix}
0 & 1 \\
244 & 13
\end{pmatrix}
,\begin{pmatrix}
0 & 1 \\
244 & 169
\end{pmatrix}
,\begin{pmatrix}
0 & 13 \\
244 & 169
\end{pmatrix}
,$$

we see that they are all copies of the same two-dimensional lattice modulo 244; see Figure 3.

The second lattice can be obtained from the first via a rotation by $\pi/2$ and a reflection on the $x$-axis:

$$(1, b) \cdot \begin{pmatrix}
0 & -1 \\
1 & 0
\end{pmatrix} \cdot \begin{pmatrix}
1 & 0 \\
1 & -1
\end{pmatrix} = (b, 1) = (b \cdot 1, b \cdot c).$$

Thus, there is a bijection between the two lattices; the point $(n, bn)$ in the first lattice is obtained as point $(k, kc)$ for $k = bn$ in the second lattice. Similarly, we see that there is also a bijection between the first and third lattice using both conditions on the parameters; i.e. $bc = 1$ and $b^2 = c$ modulo 244. We have that

$$(1, b) = (b^2 \cdot b, b^2 \cdot c),$$

and hence the point $(n, bn)$ in the first lattice is obtained as point $(kb, kc)$ in the third lattice for $k = b^2 n$. An easy calculation shows that the first of the three two-dimensional lattices has a reduced basis of the form $(1, 13), (19, 3)$; this corresponds to the points with indices $n = 1$ and $n = 19$. Using the bijections of the indices of the points that we have just established, we can translate these two vectors and see that we obtain these vectors for indices $k = 13$ and $k = 19b = 3$ in the second lattice as well as $k' = b^2 = c = 169$ and $k' = 19b^2 = -39$ in the third lattice. Interestingly, the three three-dimensional vectors for $n = 1$, $k = b$, $k' = c$ give three variations of the vector $(1, b, c)$ thanks to our assumptions, whereas the vectors for $n = 19$, $k = 3$ and $k' = -39$ are

$$
\begin{align*}
\mathbf{v}_1 &= \begin{pmatrix} 19 \\ 3 \\ 39 \end{pmatrix}, \\
\mathbf{v}_2 &= \begin{pmatrix} 3 \\ 39 \\ 19 \end{pmatrix}, \\
\mathbf{v}_3 &= \begin{pmatrix} -39 \\ -19 \\ -3 \end{pmatrix}
\end{align*}
$$

and as such a reduced basis of the lattice. Hence, we obtain

$$
\frac{\lambda(\Pi_{244, (1, 13, 169)})}{244^{2/3}} = \frac{\sqrt{1891}}{244^{2/3}} = 1.11366\ldots
$$
This lattice is a rhombohedral lattice whose fundamental domain is an almost perfect approximation of the FCC lattice. The angle $\alpha$ between the edges of the rhomboid is given as

$$\alpha = \arccos \left( \frac{\mathbf{v}_1 \cdot \mathbf{v}_2}{\|\mathbf{v}_1\| \|\mathbf{v}_2\|} \right) = \arccos \left( \frac{\mathbf{v}_1 \cdot \mathbf{v}_3}{\|\mathbf{v}_1\| \|\mathbf{v}_3\|} \right) = \arccos \left( \frac{\mathbf{v}_2 \cdot \mathbf{v}_3}{\|\mathbf{v}_2\| \|\mathbf{v}_3\|} \right) = 1.06572 \ldots$$

which is almost the angle $\pi/3 = 1.0472 \ldots$ obtained for the FCC lattice via

$$\arccos \left( \frac{(1, 1, 0) \cdot (1, 0, 1)}{\|\mathbf{v}_1\| \|\mathbf{v}_2\|} \right) = \pi/3.$$

3.1. A general procedure? The calculations in the previous section suggest the following general procedure: Assume $N, b, c$ are such that $bc \equiv 1 \pmod{N}$ and $b^2 \equiv c \pmod{N}$ (or $bc \equiv -1 \pmod{N}$ and $b \equiv c^2 \pmod{N}$). Then it is easy to see, using the same index bijections as before, that the three two-dimensional projections of the lattice are indeed always variants of the same lattice. And it is tempting to hope that the resulting lattice is again rhombohedral such that the vectors of the reduced basis are permutations of $(\pm x, \pm xb, \pm xb^2)$ as in the example for $N = 244$ for $x$ being the non-trivial index of the shortest vector in the two-dimensional lattice. The length of the shortest vector should then be given as $\| (x, xb, xb^2) \|$. In turns out, that the shortest vector is in general indeed of this form. Unfortunately, it also seems that in general only two of the three vectors of the reduced basis are of this form, while the third vector is (very) different. Thus, in general we do not obtain a rhombohedral lattice approximating the FCC lattice. Even worse, the third basis vector turns out to have a much larger norm in general, generating a lattice that is far from being rhombohedral.

As an example we look at $N = 366$ and $\mathbf{v} = (1, 13, 169)$. We have that $b \cdot c = b^2 = 2197 \equiv 1 \pmod{366}$ and $b^2 = c$. The three two-dimensional projections are variants of the lattice spanned by $(0, 366)$ and $(1, 13)$ with reduced basis $(1, 13)$ and $(-28, 2)$. Hence, in the above notation $x = -28$, $xb = -28 \cdot 13 \equiv 2 \pmod{366}$ and $xb^2 = -28 \cdot 169 \equiv 26 \pmod{366}$. However, we observe that

$$x + xb + xb^2 = x(1 + b + b^2) \equiv 0 \pmod{366}$$

– a property which makes it impossible to get a reduced basis as in the case of $N = 244$. This seems to be the generic case for examples of this kind. Indeed, the reduced basis of the three dimensional lattice $\Pi_{366, \mathbf{v}}$ is

$$\mathbf{v}_1 = \begin{pmatrix} -28 \\ 2 \\ 26 \end{pmatrix}, \mathbf{v}_2 = \begin{pmatrix} -2 \\ -26 \\ 28 \end{pmatrix}, \mathbf{v}_3 = \begin{pmatrix} 61 \\ 61 \\ 61 \end{pmatrix}.$$

Hence,

$$\frac{\lambda(\Pi_{366, \mathbf{v}})}{366^{2/3}} = \frac{2\sqrt{366}}{366^{2/3}} = 0.7477 \ldots,$$

and similarly for other lattices of this form and generated by $(1, 13, 169)$; see Table I

4. Two infinite sets of lattices

The results in Table I and for similar sets of examples suggest that while the case of $N = 244$ seems highly exceptional and mysterious there may be two general patterns for bases of the form $N = b^3 - 1$ and $N = (b^3 - 1)/2$ for integers $b > 0$. We explore these examples in the following and note that Theorem II implies Theorem I.

**Theorem 2.** For an integer $m > 2$ let $N = m^3 - 1$ and $\mathbf{v} = (a, b, c) = (1, m, m^2)$. Then

$$\lambda_3(\Pi_{N, \mathbf{v}}) = \sqrt{1 + m^2 + m^4}$$

such that

$$\lim_{m \to \infty} \frac{\lambda_3(\Pi_{N, \mathbf{v}})}{N^{2/3}} = 1.$$
Table 1. Lattices satisfying the conditions $bc \equiv 1 \pmod N$ and $b^2 \equiv c \pmod N$ for $\mathbf{v} = (1, 13, 169)$. *The shortest vector for $N = 2196$ is given by $(1, 13, 169)$; see Theorem 2.

| $N$ | $x$ | $bx$ | $bx^2$ | $\lambda(\Pi_{N\mathbf{v}})/N^{2/3}$ |
|-----|-----|-----|-------|----------------------------------|
| 61  | -4  | 9   | -5    | 0.7127                           |
| 122 | 10  | 8   | -18   | 0.7830                           |
| 183 | -14 | 1   | 13    | 0.5935                           |
| 244 | 19  | 3   | 39    | 1.11366                          |
| 366 | -28 | 2   | 26    | 0.7477                           |
| 549 | -42 | 3   | 39    | 0.8560                           |
| 732 | -56 | 4   | 52    | 0.9421                           |
| 1098| -84 | 6   | 78    | 1.0785                           |
| 2196| -168| 12  | 156   | 1.0032                           |

Proof. We prove the theorem by showing that

$$\mathbf{v}_1 = \begin{pmatrix} 1 \\ m \\ m^2 \end{pmatrix}, \mathbf{v}_2 = \begin{pmatrix} -m \\ -m^2 \\ -1 \end{pmatrix}, \mathbf{v}_3 = \begin{pmatrix} -m^2 \\ -1 \\ -m \end{pmatrix}$$

is a reduced lattice basis for the lattice

$$\mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$ 

First, we recall that two lattices with bases $\mathbf{B}$ and $\mathbf{B}'$ are equivalent if there exists a unimodular matrix $\mathbf{U}$ such that $\mathbf{B} \cdot \mathbf{U} = \mathbf{B}'$. We observe that

$$\begin{pmatrix} 1 & -m & -m^2 \\ m & -m^2 & -1 \\ m^2 & -1 & -m \end{pmatrix} \begin{pmatrix} m \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ m \end{pmatrix}.$$ 

And the determinant of the second matrix is indeed 1. Next, we show that $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ form a reduced basis. The first condition in Definition 1 is obviously satisfied since all three vectors have the same set of entries. The second condition

$$\left\| \begin{pmatrix} 1 \\ m \\ m^2 \end{pmatrix} + \mathbf{v}_1 \begin{pmatrix} -m \\ -m^2 \\ -1 \end{pmatrix} \right\| = \left\| \begin{pmatrix} 1 - x_1 m \\ m - x_1 m^2 \\ m^2 - x_1 \end{pmatrix} \right\| \geq \left\| \begin{pmatrix} 1 \\ m \\ m^2 \end{pmatrix} \right\|$$

follows from the observation that

$$1 + m^2 + m^4 + x_1^2(m^4 + m^2 + 1) - 2x_1(m^3 + m^2 + m) \geq 1 + m^2 + m^4,$$

for all $x_1 \in \mathbb{Z}$ and $m > 2$. This is obviously true for all $x_1 \geq 2$ and all $x_1 \leq 0$. For $x_1 = 1$, we need that

$$m^4 + m^2 + 1 - 2m^3 - 2m^2 - 2m \geq 0,$$

which holds for all integers $m > 2$. In a similar way, we can also verify that $\|\mathbf{v}_3 + x_2 \mathbf{v}_2 + x_1 \mathbf{v}_1\| \geq \|\mathbf{v}_3\|$. In this case the inequality reduces to

$$(m^4 + m^2 + 1)(1 + x_1^2 + x_2^2) + (m^4 + m^2 + m)(2x_1 - 2x_2 - 2x_1x_2) \geq m^4 + m^2 + 1.$$ 

Since $(x_1 - x_2)^2 + 2(x_1 - x_2) \geq 0$ unless $x_1 - x_2 = -1$, it is easy to see that the inequality holds for $m \geq 1$ and $x_1, x_2$ with $x_1 + 1 \neq x_2$. Now, assume $x_1 + 1 = x_2$; in this case,

$$-1 = x_1^2 + (x_1 + 1)^2 - 2x_1 - 2x_2 - 2x_1x_2,$$

and the inequality can be reduced to the above (12). Hence, the basis is indeed reduced and the length of the shortest vector in the lattice is $\sqrt{1 + m^2 + m^4}$. \square
We prove the theorem by showing that

\[ \text{Proof.} \]

which is true for \( k \). Next we have to check that

\[ (14) \begin{pmatrix} v_1 \mid v_2 \mid v_3 \end{pmatrix} \]

is a reduced lattice basis for the lattice

\[ \lambda_3 \left( \frac{\Pi_{N,v}}{N^{2/3}} \right) = 2^{1/6} \]

First, we observe that

\[ (13) \]

\[ \begin{pmatrix} v_1 \mid v_2 \mid v_3 \end{pmatrix} \begin{pmatrix} -k & 1+k & 1 \\ k & 1 & 1 \\ k + k(2k+1) & k + k(2k+1) & k + k(2k+1) + 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ b^{3-1} & 0 & b \\ 0 & b^{3-1} & b^2 \end{pmatrix} \]

And the determinant of the second matrix is indeed -1. Next we have to check that \( \|v_2 + x_1v_1\| \geq \|v_2\| \). We have that \( \|v_2\| = 2k^2(3 + 6k + 4k^2) \) and the above inequality reduces to

\[ 2k^2(3 + 6k + 4k^2)(1 - x_1 + x_1^2) \geq 2k^2(3 + 6k + 4k^2), \]

which is true for \( k \geq 1 \) and all integers \( x_1 \). Finally, we have to show that

\[ \|v_3 + x_2v_2 + x_1v_1\| \geq \|v_3\| \]

for all integers \( x_1, x_2 \). We have that \( \|v_3\| = (1 + 2k + 2k^2)(3 + 6k + 4k^2) \). Setting \( \alpha = 3 + 6k + 4k^2 \), the inequality can be simplified to

\[ (1 + 2k + 2k^2)\alpha + 2k^2 \alpha(x_1^2 + x_2^2 + x_1 - x_2 - x_1 x_2) \geq (1 + 2k + 2k^2)\alpha, \]

and hence to

\[ x_1^2 + x_2^2 + x_1 - x_2 - x_1 x_2 \geq 0. \]

Depending on the signs of \( x_1 \) and \( x_2 \) we either write \( x_1 - x_2(1 - x_1) \) or \( x_1(1 - x_2) - x_2 \) to see that this inequality holds in each case and for all pairs of integers \( x_1, x_2 \). Thus, we get that

\[ \lim_{k \to \infty} \frac{\Pi_{N,v}}{N^{2/3}} = \lim_{k \to \infty} \frac{\sqrt{2} \sqrt{k^2(3 + 6k + 4k^2)}}{k(3 + 6k + 4k^2))^{2/3}} = 2^{1/6}. \]

\[ \Box \]

**Theorem 3.** Let \( b = 2k + 1 \) be odd and set \( N = \frac{b^3 - 1}{2} \), \( v = (1, b, b^2) \). Then we have

\[ \lim_{k \to \infty} \frac{\lambda_3(\Pi_{N,v})}{N^{2/3}} = 2^{1/6} \]
Remark 2. We can calculate the value of $k$ needed to get a lattice whose normalised shortest vector is longer than for the exceptional lattice $\Pi = \Pi_{244,(1,13,169)}$. In [7] we calculated that $\lambda_3(\Pi)/244^{2/3} = \sqrt{1891}/244^{2/3} \approx 1.1136$, which is only improved for $k > 31$ or $N \geq 137312$; see Figure 4.

References

[1] J.H. Conway, N.J.A. Sloane, Sphere Packings, Lattices and Groups. 3rd Edition, Springer, 1999.
[2] L. Fejes Tóth, Lagerungen in der Ebene auf der Kugel und im Raum, Springer-Verlag, Berlin 1953.
[3] L. Fukshansky, Revisiting the hexagonal lattice: On optimal lattice circle packing. Elem. Math. 66 (2011), 1–9.
[4] T. Hales, A proof of the Kepler conjecture, Ann. Math. 162 (2005), 1065–1185.
[5] T. Hales, Dense sphere packings. A blueprint for formal proofs. Cambridge University Press, 2012.
[6] J. Lagarias (ed.), The Kepler Conjecture. The Hales-Ferguson proof. Springer/Verlag, Berlin, 2011.
[7] F. Pausinger, Bounds for the traveling salesman paths of two-dimensional modular lattices, J Comb Optim 33 (2017), 1378–1394.
[8] F. Pausinger, Lattices modulo $N$ with long shortest distances, Elem. Math. 72 (2017), 1–11.
[9] C. A. Rogers, The packing of equal spheres, Proc. London Math. Soc. 8 (1958), 447–465.
[10] C. A. Rogers, Packing and Covering. Cambridge University Press, 1964.
[11] I. Semaev, A 3-Dimensional Lattice Reduction Algorithm, J.H. Silverman (Ed.): CaLC 2001, LNCS 2146, 181–193, Springer, 2001.
[12] G. G. Szpiro, Kepler’s conjecture. How some of the greatest minds in history helped solve one of the oldest math problems in the world. John Wiley & Sons, 2003.

School of Mathematics & Physics, Queen’s University Belfast, BT7 1NN, Belfast, United Kingdom.
E-mail address: f.pausinger@qub.ac.uk