On sparse geometry of numbers

Lenny Fukshansky
Claremont McKenna College
(joint work with Pavel Guerzhoy and Stefan Kühnlein)

Diophantine Analysis and Related Topics
Online conference at Moscow State University
May 31 - June 5, 2021

Norms

Let $n \geq 2$, then for every $\boldsymbol{x} \in \mathbb{R}^n$ define

$$\textbf{Euclidean norm: } \|\boldsymbol{x}\| = \left(\sum_{i=1}^{n} x_i^2\right)^{1/2},$$

$$\textbf{Sup-norm: } |\boldsymbol{x}| = \max_{1 \leq i \leq n} |x_i|,$$

$$\textbf{0-norm: } \|\boldsymbol{x}\|_0 = \sum_{i=1}^{n} x_i^0, \ (\text{convention: } 0^0 = 0)$$

and for every $A = (a_{ij}) \in \mathrm{GL}_n(\mathbb{R})$, define $|A| = \max_{1 \leq i,j \leq n} |a_{ij}|$.

Norms

Let $n \geq 2$, then for every $\boldsymbol{x} \in \mathbb{R}^n$ define

$$\textbf{Euclidean norm:}\ \|\boldsymbol{x}\| = \left(\sum_{i=1}^{n} x_i^2\right)^{1/2},$$

$$\textbf{Sup-norm:}\ |\boldsymbol{x}| = \max_{1 \leq i \leq n} |x_i|,$$

$$\textbf{0-norm:}\ \|\boldsymbol{x}\|_0 = \sum_{i=1}^{n} x_i^0,\ (\text{convention: } 0^0 = 0)$$

and for every $A = (a_{ij}) \in \mathrm{GL}_n(\mathbb{R})$, define $|A| = \max_{1 \leq i,j \leq n} |a_{ij}|$.

Let $L = A\mathbb{Z}^n$ be a lattice of full rank with basis matrix A, and define

$$\textbf{Minimal norm of the lattice:}\ |L| = \min\left\{\|\boldsymbol{x}\| : \boldsymbol{x} \in L \setminus \{\boldsymbol{0}\}\right\}.$$

Sparsity levels

A vector $\boldsymbol{x}$ is called k-**sparse** if $\|\boldsymbol{x}\|_0 \leq k$. Sparsity is extensively studied in *compressive sensing*, a signal processing paradigm.

Sparsity levels

A vector $\boldsymbol{x}$ is called k-**sparse** if $\|\boldsymbol{x}\|_0 \leq k$. Sparsity is extensively studied in *compressive sensing*, a signal processing paradigm.

Recent work by *Aliev et al.* focused on sparsity of integer representations of lattice vectors, i.e. on representing a vector $\boldsymbol{x} \in B\mathbb{Z}^n$ as $\boldsymbol{x} = B\boldsymbol{y}$ with $\boldsymbol{y} \in \mathbb{Z}^n$ being as sparse as possible, where B is an $m \times n$ integer matrix, $m \leq n$.

Sparsity levels

A vector $\boldsymbol{x}$ is called k-**sparse** if $\|\boldsymbol{x}\|_0 \leq k$. Sparsity is extensively studied in *compressive sensing*, a signal processing paradigm.

Recent work by *Aliev et al.* focused on sparsity of integer representations of lattice vectors, i.e. on representing a vector $\boldsymbol{x} \in B\mathbb{Z}^n$ as $\boldsymbol{x} = B\boldsymbol{y}$ with $\boldsymbol{y} \in \mathbb{Z}^n$ being as sparse as possible, where B is an $m \times n$ integer matrix, $m \leq n$.

We study sparsity of the lattice vectors themselves, defining the **successive sparsity levels** $1 \leq s_1 \leq \cdots \leq s_n \leq n$ of the lattice L

$$s_i(L) := \min\left\{s : \exists\ i \text{ linearly independent vectors } \boldsymbol{x}_1, \ldots, \boldsymbol{x}_i \in L \text{ with } \|\boldsymbol{x}_1\|_0, \ldots, \|\boldsymbol{x}_i\|_0 \leq s\right\}.$$

Sparsity levels

A vector $\boldsymbol{x}$ is called k-**sparse** if $\|\boldsymbol{x}\|_0 \leq k$. Sparsity is extensively studied in *compressive sensing*, a signal processing paradigm.

Recent work by *Aliev et al.* focused on sparsity of integer representations of lattice vectors, i.e. on representing a vector $\boldsymbol{x} \in B\mathbb{Z}^n$ as $\boldsymbol{x} = B\boldsymbol{y}$ with $\boldsymbol{y} \in \mathbb{Z}^n$ being as sparse as possible, where B is an $m \times n$ integer matrix, $m \leq n$.

We study sparsity of the lattice vectors themselves, defining the **successive sparsity levels** $1 \leq s_1 \leq \cdots \leq s_n \leq n$ of the lattice L

$$s_i(L) := \min\left\{s : \exists\ i \text{ linearly independent vectors } \boldsymbol{x}_1, \dots, \boldsymbol{x}_i \in L \text{ with } \|\boldsymbol{x}_1\|_0, \dots, \|\boldsymbol{x}_i\|_0 \leq s\right\}.$$

Question 1

What can be said about successive sparsity levels of L? Assuming that some $s_\ell \leq k$, can we find ℓ such k-sparse vectors in L?

Rational dimension

For every nonzero vector $\boldsymbol{x} \in L$ define its **rational dimension**

$$d(\boldsymbol{x}) := \dim_{\mathbb{Q}} \operatorname{span}_{\mathbb{Q}} \{x_1, \ldots, x_n\}.$$

Rational dimension

For every nonzero vector $\boldsymbol{x} \in L$ define its **rational dimension**

$$d(\boldsymbol{x}) := \dim_{\mathbb{Q}} \operatorname{span}_{\mathbb{Q}} \{x_1, \ldots, x_n\}.$$

If A is an $n \times n$ real matrix with row vectors $\boldsymbol{a}_i$ for $1 \leq i \leq n$, then for each subset

$$I \subseteq [n] := \{1, \ldots, n\}, \text{ define } d_I(A) := \sum_{i \in I} d(\boldsymbol{a}_i).$$

Rational dimension

For every nonzero vector $\boldsymbol{x} \in L$ define its **rational dimension**

$$d(\boldsymbol{x}) := \dim_{\mathbb{Q}} \operatorname{span}_{\mathbb{Q}} \{x_1, \dots, x_n\}.$$

If A is an $n \times n$ real matrix with row vectors $\boldsymbol{a}_i$ for $1 \leq i \leq n$, then for each subset

$$I \subseteq [n] := \{1, \dots, n\}, \text{ define } d_I(A) := \sum_{i \in I} d(\boldsymbol{a}_i).$$

Also write

$$d(A) := d_{[n]}(A) \text{ and } d(L) := d(A),$$

where A is any basis matrix for L (this definition does not depend on the choice of a basis). Then $d(L) \geq n$, we call it the rational dimension of L.

Rational dimension

For every nonzero vector $\boldsymbol{x} \in L$ define its **rational dimension**

$$d(\boldsymbol{x}) := \dim_{\mathbb{Q}} \operatorname{span}_{\mathbb{Q}} \{x_1, \ldots, x_n\}.$$

If A is an $n \times n$ real matrix with row vectors $\boldsymbol{a}_i$ for $1 \leq i \leq n$, then for each subset

$$I \subseteq [n] := \{1, \ldots, n\}, \text{ define } d_I(A) := \sum_{i \in I} d(\boldsymbol{a}_i).$$

Also write

$$d(A) := d_{[n]}(A) \text{ and } d(L) := d(A),$$

where A is any basis matrix for L (this definition does not depend on the choice of a basis). Then $d(L) \geq n$, we call it the rational dimension of L. Certainly $d(L) = n$ for all rational lattices, but there also exist non-rational lattices for which $d(L) = n$, for instance

$$L = \begin{pmatrix} \sqrt{2} & 2\sqrt{2} \\ \sqrt{3} & 3\sqrt{3} \end{pmatrix} \mathbb{Z}^2.$$

Irrationality measures

We also define two "**measures of irrationality**" of vectors in a lattice L and of L itself. First, if $\boldsymbol{x} \in L$ has $d(\boldsymbol{x}) = k$, then it can be written as

$$\boldsymbol{x} = \sum_{i=1}^{k} \alpha_i \boldsymbol{f}_i, \tag{1}$$

where $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_k$ are integer vectors with relatively prime coordinates.

Irrationality measures

We also define two "**measures of irrationality**" of vectors in a lattice L and of L itself. First, if $\boldsymbol{x} \in L$ has $d(\boldsymbol{x}) = k$, then it can be written as

$$\boldsymbol{x} = \sum_{i=1}^{k} \alpha_i \boldsymbol{f}_i, \tag{1}$$

where $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_k$ are integer vectors with relatively prime coordinates. This decomposition is unique only if $k = 1$, for example

$$\begin{aligned} \left(1, \sqrt{2}, -2\sqrt{3}\right) &= 1 \cdot (1,0,0) + \sqrt{2} \cdot (0,1,0) - 2\sqrt{3} \cdot (0,0,1) \\ &= 1 \cdot (1,0,0) + \left(\frac{\sqrt{2}}{2} - \sqrt{3}\right) \cdot (0,1,1) \\ &\quad + \left(\frac{\sqrt{2}}{2} + \sqrt{3}\right) \cdot (0,1,-1). \end{aligned}$$

Irrationality measures

Define

$$\nu(\boldsymbol{x}) := \begin{cases} |\alpha_1| & \text{if } k = 1, \\ 0 & \text{if } k > 1. \end{cases}$$

Irrationality measures

Define

$$\nu(\boldsymbol{x}) := \begin{cases} |\alpha_1| & \text{if } k = 1, \\ 0 & \text{if } k > 1. \end{cases}$$

For our basis matrix A, we define

$$\nu(A) := \prod_{i=1}^{n} \nu(\boldsymbol{a}_i),$$

and for the lattice $L = A\mathbb{Z}^n$, we let $\nu(L) = \nu(A)$. This definition does not depend on the choice of the basis matrix A. Clearly, there are many lattices for which $\nu(L) = 0$: in fact

$$\nu(L) > 0 \Longleftrightarrow d(L) = n.$$

Irrationality measures

Next, let $\langle L \rangle$ be the additive abelian group generated by the entries of vectors of L, and suppose that $\langle L \rangle$ has rank $k \geq 1$. Let

$$\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_k)$$

be a basis for $\langle L \rangle$ over $\mathbb{Z}$, then for every $\boldsymbol{x} \in L$

$$\boldsymbol{x} = \sum_{i=1}^{k} \alpha_i \boldsymbol{f}_i,$$

where $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_k \in \mathbb{Z}^n$.

Irrationality measures

Next, let $\langle L \rangle$ be the additive abelian group generated by the entries of vectors of L, and suppose that $\langle L \rangle$ has rank $k \geq 1$. Let

$$\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_k)$$

be a basis for $\langle L \rangle$ over $\mathbb{Z}$, then for every $\boldsymbol{x} \in L$

$$\boldsymbol{x} = \sum_{i=1}^{k} \alpha_i \boldsymbol{f}_i,$$

where $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_k \in \mathbb{Z}^n$. Define a map $\Phi_{\boldsymbol{\alpha}} : L \to \mathbb{R}^{nk}$ by

$$\Phi_{\boldsymbol{\alpha}} \left(\sum_{i=1}^{k} \alpha_i \boldsymbol{f}_i \right) = \begin{pmatrix} \boldsymbol{f}_1 \\ \vdots \\ \boldsymbol{f}_k \end{pmatrix}. \tag{2}$$

The map $\Phi_{\boldsymbol{\alpha}}$ is additive, and hence extends to a map

$$\Phi_{\boldsymbol{\alpha}} : \mathbb{R} \otimes L = \mathbb{R}^n \to \mathbb{R}^{nk}.$$

Irrationality measures

Now, pull back the sup-norm $|\cdot|$ on $\mathbb{R}^{nk}$ to $\mathbb{R}^n$ under $\Phi_{\boldsymbol{\alpha}}$ by defining

$$|\boldsymbol{x}|_{\Phi_{\boldsymbol{\alpha}}} := |\Phi_{\boldsymbol{\alpha}}(\boldsymbol{x})|,$$

this way obtaining a norm $|\cdot|_{\Phi_{\boldsymbol{\alpha}}}$ on $\mathbb{R}^n$, which can then be compared to the sup-norm on $\mathbb{R}^n$. Specifically, we can define

$$\mu(\boldsymbol{\alpha}) := \sup\left\{ \frac{|\boldsymbol{x}|_{\Phi_{\boldsymbol{\alpha}}}}{|\boldsymbol{x}|} : \boldsymbol{x} \in \mathbb{R}^n \setminus \{\mathbf{0}\} \right\}. \tag{3}$$

We can now state our first result.

Minkowski-style theorem

Theorem 1 (F., Guerzhoy, Kühnlein (2020))

Let $A \in \mathrm{GL}_n(\mathbb{R})$ and let $L = A\mathbb{Z}^n$. Fix a basis $\boldsymbol{\alpha}$ for $\langle L \rangle$ as above and let $\mu(\boldsymbol{\alpha})$ be as given in (3). Let $1 \leq k < n$ and suppose that there exists a subset $I \subset [n]$ of $n-k$ distinct indices such that $d_I(A) < n$. Let $\ell = n - d_I(A)$. Then $s_\ell(L) \leq k$, and there exist ℓ linearly independent vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_\ell \in L$ with $\|\boldsymbol{x}_i\|_0 \leq k$ and

$$\prod_{i=1}^{\ell} |\boldsymbol{x}_i| \leq n^{n-d_I(A)/2} |A|^n \mu(\boldsymbol{\alpha})^{d_I(A)}. \qquad (4)$$

Minkowski-style theorem

Theorem 1 (F., Guerzhoy, Kühnlein (2020))

Let $A \in \mathrm{GL}_n(\mathbb{R})$ and let $L = A\mathbb{Z}^n$. Fix a basis $\boldsymbol{\alpha}$ for $\langle L \rangle$ as above and let $\mu(\boldsymbol{\alpha})$ be as given in (3). Let $1 \le k < n$ and suppose that there exists a subset $I \subset [n]$ of $n-k$ distinct indices such that $d_I(A) < n$. Let $\ell = n - d_I(A)$. Then $s_\ell(L) \le k$, and there exist ℓ linearly independent vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_\ell \in L$ with $\|\boldsymbol{x}_i\|_0 \le k$ and

$$\prod_{i=1}^{\ell} |\boldsymbol{x}_i| \le n^{n-d_I(A)/2} |A|^n \mu(\boldsymbol{\alpha})^{d_I(A)}. \tag{4}$$

From our method of proof, it follows that the dependence of the bound (4) on $|A|$ and $\mu(\boldsymbol{\alpha})$ has correct order of magnitude.

Minkowski-style theorem

This theorem is a “sparse” partial analogue of Minkowski's successive minima theorem. Indeed, if we know that $s_\ell(L) \leq k$, we can define the k-**sparse successive minima**

$$\lambda_1(L,k) \leq \cdots \leq \lambda_\ell(L,k)$$

with respect to sup-norm to be

$$\lambda_i(L,k) = \min\Big\{ t \in \mathbb{R}_{>0} \ : \ \exists \text{ lin. ind. } \boldsymbol{x}_1,\dots,\boldsymbol{x}_i \in L \text{ with } \|\boldsymbol{x}_j\|_0 \leq k, |\boldsymbol{x}_j| \leq t \Big\},$$

so the usual successive minima are $\lambda_i(L) = \lambda_i(L,n)$. Then (4) is an upper bound on the product of these k-sparse successive minima.

Sketch of proof of Theorem 1

For each row vector $\boldsymbol{a}_i$ of A let $d_i = d(\boldsymbol{a}_i)$. Then there exist $\mathbb{Q}$-linearly independent real numbers $\alpha_{i1}, \ldots, \alpha_{id_i}$ such that

$$\boldsymbol{a}_i = \sum_{j=1}^{d_i} \alpha_{ij} \boldsymbol{f}_{ij},$$

where $\boldsymbol{f}_{ij}$ are integer vectors with relatively prime coefficients for all $1 \leq i \leq n$, $1 \leq j \leq d_i$. Let $d = \sum_{i=1}^{n} d_i$ and let $F(A)$ be the $d \times n$ matrix with rows $\boldsymbol{f}_{ij}$.

Sketch of proof of Theorem 1

For each row vector $\boldsymbol{a}_i$ of A let $d_i = d(\boldsymbol{a}_i)$. Then there exist $\mathbb{Q}$-linearly independent real numbers $\alpha_{i1}, \ldots, \alpha_{id_i}$ such that

$$\boldsymbol{a}_i = \sum_{j=1}^{d_i} \alpha_{ij} \boldsymbol{f}_{ij},$$

where $\boldsymbol{f}_{ij}$ are integer vectors with relatively prime coefficients for all $1 \leq i \leq n$, $1 \leq j \leq d_i$. Let $d = \sum_{i=1}^{n} d_i$ and let $F(A)$ be the $d \times n$ matrix with rows $\boldsymbol{f}_{ij}$.

Then

$$|F(A)| := \max_{1 \leq i \leq n} \max_{1 \leq j \leq d_i} |\boldsymbol{f}_{ij}| \leq \mu(\boldsymbol{\alpha})|A|. \tag{5}$$

Sketch of proof of Theorem 1

Let $I \subset [n]$ be a subset of $n-k$ distinct indices such that $d_I(A) < n$. Let A_I be the $(n-k) \times n$ submatrix of A consisting of the rows indexed by I. Let $F(A)_I$ be the $d_I(A) \times n$ submatrix of $F(A)$ consisting of rows with $\boldsymbol{f}_{i_l j}$ for $i_l \in I$ and $1 \leq j \leq d_{i_l}$.

Sketch of proof of Theorem 1

Let $I \subset [n]$ be a subset of $n-k$ distinct indices such that $d_I(A) < n$. Let A_I be the $(n-k) \times n$ submatrix of A consisting of the rows indexed by I. Let $F(A)_I$ be the $d_I(A) \times n$ submatrix of $F(A)$ consisting of rows with $\boldsymbol{f}_{i_l j}$ for $i_l \in I$ and $1 \leq j \leq d_{i_l}$.

Then

$$V := \{\boldsymbol{y} \in \mathbb{Q}^n : A_I \boldsymbol{y} = \boldsymbol{0}\} = \{\boldsymbol{y} \in \mathbb{Q}^n : F(A)_I \boldsymbol{y} = \boldsymbol{0}\}$$

is an ℓ-dimensional subspace of $\mathbb{Q}^n$, $\ell = n - d_I(A)$.

Sketch of proof of Theorem 1

Let $I \subset [n]$ be a subset of $n-k$ distinct indices such that $d_I(A) < n$. Let A_I be the $(n-k) \times n$ submatrix of A consisting of the rows indexed by I. Let $F(A)_I$ be the $d_I(A) \times n$ submatrix of $F(A)$ consisting of rows with $\boldsymbol{f}_{i_l j}$ for $i_l \in I$ and $1 \leq j \leq d_{i_l}$.

Then

$$V := \{\boldsymbol{y} \in \mathbb{Q}^n : A_I \boldsymbol{y} = \boldsymbol{0}\} = \{\boldsymbol{y} \in \mathbb{Q}^n : F(A)_I \boldsymbol{y} = \boldsymbol{0}\}$$

is an ℓ-dimensional subspace of $\mathbb{Q}^n$, $\ell = n - d_I(A)$.

By a version of Siegel's lemma, there exist ℓ linearly independent vectors $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_\ell \in V \cap \mathbb{Z}^n$ such that

$$\prod_{j=1}^{\ell} |\boldsymbol{y}_j| \leq \left(\sqrt{n}|F(A)|\right)^{d_I(A)}. \tag{6}$$

The theorem follows from this observation.

Virtually rectangular lattices

Unfortunately, the upper bound of Theorem 1 depends on the choice of the basis for L and for $\langle L \rangle$. We can alleviate this dependence for lattices L with rational dimension $d(L) = n$.

Virtually rectangular lattices

Unfortunately, the upper bound of Theorem 1 depends on the choice of the basis for L and for $\langle L \rangle$. We can alleviate this dependence for lattices L with rational dimension $d(L) = n$.

A lattice L is **rectangular** if it has an orthogonal basis; L is **virtually rectangular** if it contains a rectangular sublattice of finite index.

Virtually rectangular lattices

Unfortunately, the upper bound of Theorem 1 depends on the choice of the basis for L and for $\langle L \rangle$. We can alleviate this dependence for lattices L with rational dimension $d(L) = n$.

A lattice L is **rectangular** if it has an orthogonal basis; L is **virtually rectangular** if it contains a rectangular sublattice of finite index.

Theorem 2 (F., Guerzhoy, Kühnlein (2020))

Let $L \subset \mathbb{R}^n$ be a lattice of full rank. The following three statements are equivalent:

1. $d(L) = n$,
2. $\nu(L) > 0$,
3. $s_1(L) = \cdots = s_n(L) = 1$.

Further, a full-rank lattice $L' \subset \mathbb{R}^n$ is virtually rectangular if and only if it is isometric to some lattice L satisfying the three equivalent conditions above.

Virtually rectangular lattices

Theorem 3 (F., Guerzhoy, Kühnlein (2020))

Let $A \in \mathrm{GL}_n(\mathbb{R})$ be such that the lattice $L = A\mathbb{Z}^n$ satisfies the equivalent conditions of Theorem 2. Then L contains a rectangular sublattice M with a basis of 1-sparse vectors $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ so that

$$\prod_{i=1}^{n} |\boldsymbol{x}_i| = [L : M] = \left(\frac{\det(L)}{\nu(L)} \right)^{n-1}. \tag{7}$$

More generally, if $L' \subset \mathbb{R}^n$ is a virtually rectangular lattice, then there exists a rectangular sublattice M' of L' such that

$$[L' : M'] = \left(\frac{\det(L)}{\nu(L)} \right)^{n-1},$$

where L is a lattice isometric to L' satisfying Theorem 2.

Sketch of proof of Theorem 3

Since $d(L) = n$, we must have $d(\boldsymbol{a}_i) = 1$ for each row vector $\boldsymbol{a}_i$ of A. Then there exist nonzero real numbers $\alpha_1, \dots, \alpha_n$ and primitive integer row vectors $\boldsymbol{f}_1, \dots, \boldsymbol{f}_n$ so that $\boldsymbol{a}_i = \alpha_i \boldsymbol{f}_i$ for each $1 \leq i \leq n$.

Sketch of proof of Theorem 3

Since $d(L) = n$, we must have $d(\boldsymbol{a}_i) = 1$ for each row vector $\boldsymbol{a}_i$ of A. Then there exist nonzero real numbers $\alpha_1, \dots, \alpha_n$ and primitive integer row vectors $\boldsymbol{f}_1, \dots, \boldsymbol{f}_n$ so that $\boldsymbol{a}_i = \alpha_i \boldsymbol{f}_i$ for each $1 \leq i \leq n$.

This implies that

$$B := A \operatorname{adj}(F(A)) = \mathcal{A} F(A) \operatorname{adj}(F(A)) = \det(F(A)) \mathcal{A},$$

where $\mathcal{A}$ is the diagonal matrix with diagonal entries $\alpha_1, \dots, \alpha_n$ and $\operatorname{adj}(F(A))$ be the adjugate of $F(A)$ (transpose of the cofactor matrix).

Sketch of proof of Theorem 3

Since $d(L) = n$, we must have $d(\boldsymbol{a}_i) = 1$ for each row vector $\boldsymbol{a}_i$ of A. Then there exist nonzero real numbers $\alpha_1, \dots, \alpha_n$ and primitive integer row vectors $\boldsymbol{f}_1, \dots, \boldsymbol{f}_n$ so that $\boldsymbol{a}_i = \alpha_i \boldsymbol{f}_i$ for each $1 \leq i \leq n$.

This implies that

$$B := A \operatorname{adj}(F(A)) = \mathcal{A} F(A) \operatorname{adj}(F(A)) = \det(F(A)) \mathcal{A},$$

where $\mathcal{A}$ is the diagonal matrix with diagonal entries $\alpha_1, \dots, \alpha_n$ and $\operatorname{adj}(F(A))$ be the adjugate of $F(A)$ (transpose of the cofactor matrix).

Then take $M = B\mathbb{Z}^n$, and so

$$[L : M] = |\det(\operatorname{adj}(F(A))| = \left| \frac{\det(A)}{\det(\mathcal{A})} \right|^{n-1} = \left(\frac{\det(L)}{\nu(L)} \right)^{n-1}.$$

Elliptic curves

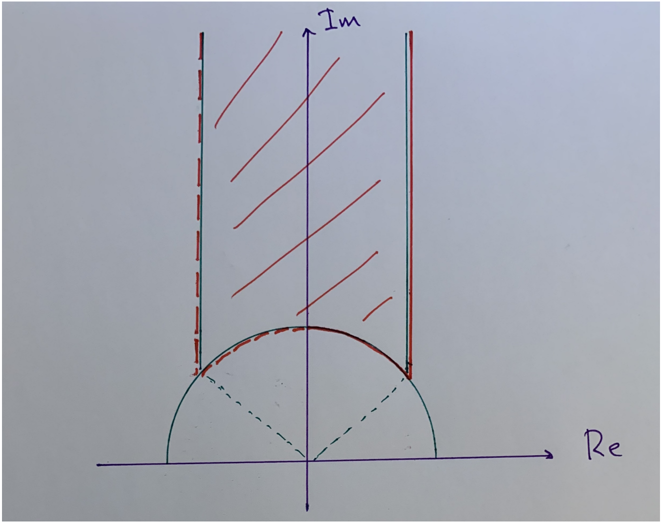
In the 2-dimensional case, our results have interesting implications for elliptic curves. Up to isomorphism, an elliptic curve E can be realized as a complex torus $\mathbb{C}/\Gamma_\tau$ for a planar lattice

$$\Gamma_\tau = \mathbb{Z} + \mathbb{Z}\tau = \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \mathbb{Z}^2,$$

where $\tau = a + bi$ belongs to the set $\mathcal{D} =$

$$\{\tau \in \mathbb{C} : -\frac{1}{2} < \Re(\tau) \leq \frac{1}{2}, \Im(\tau) \geq 0, |\tau| \geq 1\} \setminus \left\{ e^{i\theta} : \frac{\pi}{2} < \theta < \frac{2\pi}{3} \right\}.$$

Domain $\mathcal{D}$



Elliptic curves

Let $j : \mathcal{D} \to \mathbb{C}$ be the Klein modular invariant, which gives the j-invariant $j(\tau)$ for each isomorphism class E_τ of elliptic curves. Then $j(\tau) \in \mathbb{R}$ if and only if τ belongs to one of the sets

$$\left\{ \frac{1}{2} + it : t \in \mathbb{R}, t \geq \frac{\sqrt{3}}{2} \right\},$$

$$\left\{ e^{i\theta} : \theta \in [\pi/3, \pi/2] \right\},$$

$$\{ it : t \in \mathbb{R}, t \geq 1 \},$$

and j maps the first of these three subsets bijectively onto the interval $(-\infty, 0]$, the second onto $[0, 1]$, and the third onto $[1, \infty)$.

Virtually rectangular elliptic curves

Theorem 4 (F., Guerzhoy, Kühnlein (2020))

Let $\tau = a + bi \in \mathcal{D}$ and let E_τ be the corresponding elliptic curve with the period lattice Γ_τ. The following are equivalent:

Virtually rectangular elliptic curves

Theorem 4 (F., Guerzhoy, Kühnlein (2020))

Let $\tau = a + bi \in \mathcal{D}$ *and let* E_τ *be the corresponding elliptic curve with the period lattice* Γ_τ. *The following are equivalent:*

1. *Either* $a \in \mathbb{Q}$ *or there exists some* $t \in \mathbb{R}$ *such that* $\frac{v'}{v} := a - bt$, $\frac{w'}{w} := a + b/t \in \mathbb{Q}$,

Virtually rectangular elliptic curves

Theorem 4 (F., Guerzhoy, Kühnlein (2020))

Let $\tau = a + bi \in \mathcal{D}$ and let E_τ be the corresponding elliptic curve with the period lattice Γ_τ. The following are equivalent:

1. *Either $a \in \mathbb{Q}$ or there exists some $t \in \mathbb{R}$ such that $\frac{v'}{v} := a - bt, \frac{w'}{w} := a + b/t \in \mathbb{Q}$,*
2. *Γ_τ is virtually rectangular,*

Virtually rectangular elliptic curves

Theorem 4 (F., Guerzhoy, Kühnlein (2020))

Let $\tau = a + bi \in \mathcal{D}$ and let E_τ be the corresponding elliptic curve with the period lattice Γ_τ. The following are equivalent:

1. *Either $a \in \mathbb{Q}$ or there exists some $t \in \mathbb{R}$ such that $\frac{v'}{v} := a - bt, \frac{w'}{w} := a + b/t \in \mathbb{Q}$,*
2. *Γ_τ is virtually rectangular,*
3. *E_τ is isogenous to E' with real j-invariant ≥ 1,*

Virtually rectangular elliptic curves

Theorem 4 (F., Guerzhoy, Kühnlein (2020))

Let $\tau = a + bi \in \mathcal{D}$ and let E_τ be the corresponding elliptic curve with the period lattice Γ_τ. The following are equivalent:

1. *Either $a \in \mathbb{Q}$ or there exists some $t \in \mathbb{R}$ such that $\frac{v'}{v} := a - bt, \frac{w'}{w} := a + b/t \in \mathbb{Q}$,*
2. *Γ_τ is virtually rectangular,*
3. *E_τ is isogenous to E' with real j-invariant ≥ 1,*
4. *E_τ is isogenous to E' with real j-invariant in $[0, 1]$.*

Virtually rectangular elliptic curves

Theorem 4 (F., Guerzhoy, Kühnlein (2020))

Let $\tau = a + bi \in \mathcal{D}$ and let E_τ be the corresponding elliptic curve with the period lattice Γ_τ. The following are equivalent:

1. *Either $a \in \mathbb{Q}$ or there exists some $t \in \mathbb{R}$ such that $\frac{v'}{v} := a - bt$, $\frac{w'}{w} := a + b/t \in \mathbb{Q}$,*
2. *Γ_τ is virtually rectangular,*
3. *E_τ is isogenous to E' with real j-invariant ≥ 1,*
4. *E_τ is isogenous to E' with real j-invariant in $[0, 1]$.*

If (1) - (4) hold with $a = p/q \in \mathbb{Q}$, then exists an isogeny $E' \to E_\tau$ with degree $\delta(E'/E_\tau) = q$. If If (1) - (4) hold with $a \notin \mathbb{Q}$ and $t \in \mathbb{R}$ satisfies (1), then exists an isogeny $E' \to E_\tau$ with

$$\delta(E'/E_\tau) = \frac{|b||vw|(t^2 + 1)}{|t|}.$$

Remarks

- CM elliptic curves (those for which τ is a quadratic irrationality) are the only ones whose period lattice contains non-parallel rectangular sublattices: in the CM case, there are infinitely many t satisfying condition (1) of Theorem 4 (each corresponding to a different rectangular sublattice), whereas for all other virtually rectangular elliptic curves such t is essentially unique.

Remarks

- CM elliptic curves (those for which τ is a quadratic irrationality) are the only ones whose period lattice contains non-parallel rectangular sublattices: in the CM case, there are infinitely many t satisfying condition (1) of Theorem 4 (each corresponding to a different rectangular sublattice), whereas for all other virtually rectangular elliptic curves such t is essentially unique.
- Virtually rectangular lattices in the plane have intrinsic geometric meaning in terms of the corresponding points on the modular curve: they correspond precisely to the points that lie on geodesics closed at infinity.

Reference

L. Fukshansky, P. Guerzhoy, S. Kühnlein, *On sparse geometry of numbers*, Research in the Mathematical Sciences, vol. 8 no. 1 (2021), Article #2

Preprint is available at:

`http://math.cmc.edu/lenny/research.html`

Reference

L. Fukshansky, P. Guerzhoy, S. Kühnlein, *On sparse geometry of numbers*, Research in the Mathematical Sciences, vol. 8 no. 1 (2021), Article #2

Preprint is available at:

`http://math.cmc.edu/lenny/research.html`

Thank you!