Deep hole lattices and isogenies of elliptic curves

Lenny Fukshansky
Claremont McKenna College

(*joint work with Pavel Guerzhoy and Tanis Nielsen*)

SIU Mathematics Conference
May 16-17, 2024

My co-authors

P. Guerzhoy (Honolulu, HI) T. Nielsen (Chicago, IL)

Similarity classes of planar lattices

Every $A \in \mathrm{GL}_2(\mathbb{R})$ is a basis matrix for some planar lattice

$$\Omega := A\mathbb{Z}^2 = AB\mathbb{Z}^2,$$

for any $B \in \mathrm{GL}_2(\mathbb{Z})$.

Similarity classes of planar lattices

Every $A \in \mathrm{GL}_2(\mathbb{R})$ is a basis matrix for some planar lattice

$$\Omega := A\mathbb{Z}^2 = AB\mathbb{Z}^2,$$

for any $B \in \mathrm{GL}_2(\mathbb{Z})$. Hence the space of planar lattices $\mathcal{L}_2$ can be identified with $\mathrm{GL}_2(\mathbb{R})/\,\mathrm{GL}_2(\mathbb{Z})$.

Similarity classes of planar lattices

Every $A \in \mathrm{GL}_2(\mathbb{R})$ is a basis matrix for some planar lattice

$$\Omega := A\mathbb{Z}^2 = AB\mathbb{Z}^2,$$

for any $B \in \mathrm{GL}_2(\mathbb{Z})$. Hence the space of planar lattices $\mathcal{L}_2$ can be identified with $\mathrm{GL}_2(\mathbb{R})/\,\mathrm{GL}_2(\mathbb{Z})$.

Two lattices Ω and Γ are said to be **similar**, denoted $\Omega \sim \Gamma$, if $\Omega = \alpha U \Gamma$ for some positive real constant α and orthogonal matrix U.

Similarity classes of planar lattices

Every $A \in \mathrm{GL}_2(\mathbb{R})$ is a basis matrix for some planar lattice

$$\Omega := A\mathbb{Z}^2 = AB\mathbb{Z}^2,$$

for any $B \in \mathrm{GL}_2(\mathbb{Z})$. Hence the space of planar lattices $\mathcal{L}_2$ can be identified with $\mathrm{GL}_2(\mathbb{R}) / \mathrm{GL}_2(\mathbb{Z})$.

Two lattices Ω and Γ are said to be **similar**, denoted $\Omega \sim \Gamma$, if $\Omega = \alpha U \Gamma$ for some positive real constant α and orthogonal matrix U.

Every lattice $\Omega \in \mathcal{L}_2$ is similar to a unique lattice of the form

$$\Gamma_\tau := \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \mathbb{Z}^2 \text{ for some } \tau := a + bi \text{ in}$$

$$\mathcal{F} := \{\tau = a + bi \in \mathbb{C} : 0 \leq a \leq 1/2, b \geq 0, |\tau| \geq 1\}.$$

We refer to $\mathcal{F}$ as the **set of similarity classes** of lattices in $\mathcal{L}_2$.

Elliptic curves and isogenies

Given lattices $\Lambda, \Lambda' \subset \mathbb{C}$ a nonzero morphism $\mathcal{E} \to \mathcal{E}'$ between the corresponding elliptic curves $\mathcal{E} = \mathbb{C}/\Lambda$ and $\mathcal{E}' = \mathbb{C}/\Lambda'$ which takes 0 to 0 is called an **isogeny**.

Elliptic curves and isogenies

Given lattices $\Lambda, \Lambda' \subset \mathbb{C}$ a nonzero morphism $\mathcal{E} \to \mathcal{E}'$ between the corresponding elliptic curves $\mathcal{E} = \mathbb{C}/\Lambda$ and $\mathcal{E}' = \mathbb{C}/\Lambda'$ which takes 0 to 0 is called an **isogeny**. An isogeny is always surjective and has a finite kernel. For instance, if $\beta \in \mathbb{C}^*$ is such that $\beta\Lambda \subseteq \Lambda'$, then multiplication by β function $z \mapsto \beta z$ maps $\mathbb{C} \to \mathbb{C}$ modulo the lattices, hence maps $\mathcal{E} \to \mathcal{E}'$.

Elliptic curves and isogenies

Given lattices $\Lambda, \Lambda' \subset \mathbb{C}$ a nonzero morphism $\mathcal{E} \to \mathcal{E}'$ between the corresponding elliptic curves $\mathcal{E} = \mathbb{C}/\Lambda$ and $\mathcal{E}' = \mathbb{C}/\Lambda'$ which takes 0 to 0 is called an **isogeny**. An isogeny is always surjective and has a finite kernel. For instance, if $\beta \in \mathbb{C}^*$ is such that $\beta\Lambda \subseteq \Lambda'$, then multiplication by β function $z \mapsto \beta z$ maps $\mathbb{C} \to \mathbb{C}$ modulo the lattices, hence maps $\mathcal{E} \to \mathcal{E}'$. In fact, every isogeny is of this form. The **degree** of this isogeny is the degree of the morphism, which is equal to the index of the sublattice $\beta\Lambda$ in Λ', i.e.

$$\deg(\beta) = [\Lambda' : \beta\Lambda].$$

Elliptic curves and isogenies

Given lattices $\Lambda, \Lambda' \subset \mathbb{C}$ a nonzero morphism $\mathcal{E} \to \mathcal{E}'$ between the corresponding elliptic curves $\mathcal{E} = \mathbb{C}/\Lambda$ and $\mathcal{E}' = \mathbb{C}/\Lambda'$ which takes 0 to 0 is called an **isogeny**. An isogeny is always surjective and has a finite kernel. For instance, if $\beta \in \mathbb{C}^*$ is such that $\beta\Lambda \subseteq \Lambda'$, then multiplication by β function $z \mapsto \beta z$ maps $\mathbb{C} \to \mathbb{C}$ modulo the lattices, hence maps $\mathcal{E} \to \mathcal{E}'$. In fact, every isogeny is of this form. The **degree** of this isogeny is the degree of the morphism, which is equal to the index of the sublattice $\beta\Lambda$ in Λ', i.e.

$$\deg(\beta) = [\Lambda' : \beta\Lambda].$$

This is precisely the size of its kernel. If an isogeny $\mathcal{E} \to \mathcal{E}'$ exists, then there also exists the dual isogeny $\mathcal{E}' \to \mathcal{E}$ of the same degree such that their composition is the multiplication-by-degree map, and hence the curves are called **isogenous**: this is an equivalence relation. There may exist multiple isogenies between two elliptic curves, but since degree of an isogeny is a positive integer, we can ask for an isogeny of minimal degree.

Isomorphism classes of elliptic curves

An **isomorphism** of elliptic curves is an injective isogeny, i.e. of degree one. Each elliptic curve is isomorphic to an elliptic curve $\mathcal{E}_\tau$ with period lattice

$$\Gamma_\tau = \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \mathbb{Z}^2 \text{ for some } \tau := a + bi \text{ in}$$

$$\mathcal{D} := \{\tau = a + bi \in \mathbb{C} : -1/2 < a \leq 1/2, b \geq 0, |\tau| \geq 1\}.$$

Further, $\mathcal{D}' := \mathcal{D} \setminus \{e^{i\theta} : \pi/2 < \theta < 2\pi/3\}$ is precisely the **set of isomorphism classes** of elliptic curves.

Isomorphism classes of elliptic curves

An **isomorphism** of elliptic curves is an injective isogeny, i.e. of degree one. Each elliptic curve is isomorphic to an elliptic curve $\mathcal{E}_\tau$ with period lattice

$$\Gamma_\tau = \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \mathbb{Z}^2 \text{ for some } \tau := a + bi \text{ in}$$

$$\mathcal{D} := \{\tau = a + bi \in \mathbb{C} : -1/2 < a \leq 1/2, b \geq 0, |\tau| \geq 1\}.$$

Further, $\mathcal{D}' := \mathcal{D} \setminus \{e^{i\theta} : \pi/2 < \theta < 2\pi/3\}$ is precisely the **set of isomorphism classes** of elliptic curves.

This set $\mathcal{D}$ can also be viewed as a fundamental domain for the action of the group $\mathrm{SL}_2(\mathbb{Z})$ on the set of lattices Γ_τ by right matrix multiplication by g^{-1} for each $g \in SL_2(\mathbb{Z})$:

$$\Gamma_\tau = \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \mathbb{Z}^2 \mapsto g \cdot \Gamma_\tau := \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} g^{-1} \mathbb{Z}^2.$$

Arithmetic, well-rounded, semi-stable lattices

A lattice $\Gamma = A\mathbb{Z}^2$ is called **arithmetic** if the matrix A^tA is a scalar multiple of an integral matrix: this property is independent of the choice of the basis matrix A.

Arithmetic, well-rounded, semi-stable lattices

A lattice $\Gamma = A\mathbb{Z}^2$ is called **arithmetic** if the matrix $A^t A$ is a scalar multiple of an integral matrix: this property is independent of the choice of the basis matrix A.

Successive minima of Γ are real numbers $0 < \lambda_1(\Gamma) \leq \lambda_2(\Gamma)$:

$$\lambda_i(\Gamma) := \min\left\{r \in \mathbb{R}_{>0} : \dim_{\mathbb{R}} \operatorname{span}_{\mathbb{R}}\left(\mathbb{B}(r) \cap L\right) \geq i\right\},$$

where $\mathbb{B}(r)$ is the disk of radius r centered at the origin in $\mathbb{R}^2$. Γ is called **well-rounded (WR)** if $\lambda_1(\Gamma) = \lambda_2(\Gamma)$. WR lattices are central to discrete optimization and connected areas.

Arithmetic, well-rounded, semi-stable lattices

A lattice $\Gamma = A\mathbb{Z}^2$ is called **arithmetic** if the matrix $A^t A$ is a scalar multiple of an integral matrix: this property is independent of the choice of the basis matrix A.

Successive minima of Γ are real numbers $0 < \lambda_1(\Gamma) \leq \lambda_2(\Gamma)$:

$$\lambda_i(\Gamma) := \min \left\{ r \in \mathbb{R}_{>0} : \dim_{\mathbb{R}} \operatorname{span}_{\mathbb{R}} \left(\mathbb{B}(r) \cap L \right) \geq i \right\},$$

where $\mathbb{B}(r)$ is the disk of radius r centered at the origin in $\mathbb{R}^2$. Γ is called **well-rounded (WR)** if $\lambda_1(\Gamma) = \lambda_2(\Gamma)$. WR lattices are central to discrete optimization and connected areas.

Γ is called **semi-stable** if

$$\lambda_1(L)^2 \geq \det(\Gamma) := |\det(A)|.$$

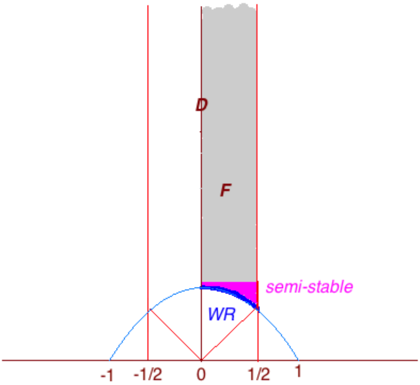
Semi-stable lattices are important in reduction theory of algebraic groups.

Geometrically speaking...

These properties of lattices are constant on similarity classes, hence we speak of arithmetic, WR, semi-stable similarity classes in $\mathcal{L}_2$, and therefore in $\mathcal{F}$.

Geometrically speaking...

These properties of lattices are constant on similarity classes, hence we speak of arithmetic, WR, semi-stable similarity classes in $\mathcal{L}_2$, and therefore in $\mathcal{F}$.



Algebraically speaking...

Γ_τ is arithmetic iff $\tau \in \mathcal{F}$ is of the form

$$\tau = \tau(a, b, c, d) := \frac{a}{b} + i\sqrt{\frac{c}{d}}$$

for some integers a, b, c, d such that

$$\gcd(a, b) = \gcd(c, d) = 1,\ 0 \leq a \leq b/2,\ c/d \geq 1 - a^2/b^2.$$

Algebraically speaking...

Γ_τ is arithmetic iff $\tau \in \mathcal{F}$ is of the form

$$\tau = \tau(a, b, c, d) := \frac{a}{b} + i\sqrt{\frac{c}{d}}$$

for some integers a, b, c, d such that

$$\gcd(a, b) = \gcd(c, d) = 1,\ 0 \leq a \leq b/2,\ c/d \geq 1 - a^2/b^2.$$

This condition is equivalent to the elliptic curve $\mathcal{E}_\tau$ with period lattice Γ_τ having **complex multiplication** (CM) by the imaginary quadratic field $\mathbb{Q}(\tau)$, i.e. the endomorphism ring of $\mathcal{E}_\tau$ is an order in $\mathbb{Q}(\tau)$ properly containing $\mathbb{Z}$.

The j-invariant

The **Klein j-function** is a bijective holomorphic map

$$j : \mathcal{D}' := \mathcal{D} \setminus \{e^{i\theta} : \pi/2 < \theta < 2\pi/3\} \to \mathbb{C}.$$

The j-invariant

The **Klein j-function** is a bijective holomorphic map

$$j : \mathcal{D}' := \mathcal{D} \setminus \{e^{i\theta} : \pi/2 < \theta < 2\pi/3\} \to \mathbb{C}.$$

If $\mathcal{E}$ is an elliptic curve, then it is isomorphic to an elliptic curve $\mathcal{E}_\tau$ for precisely one $\tau \in \mathcal{D}'$, and hence the value $j(\tau)$ is an invariant of this elliptic curve, called its **j-invariant**.

The j-invariant

The **Klein j-function** is a bijective holomorphic map

$$j : \mathcal{D}' := \mathcal{D} \setminus \{e^{i\theta} : \pi/2 < \theta < 2\pi/3\} \to \mathbb{C}.$$

If $\mathcal{E}$ is an elliptic curve, then it is isomorphic to an elliptic curve $\mathcal{E}_\tau$ for precisely one $\tau \in \mathcal{D}'$, and hence the value $j(\tau)$ is an invariant of this elliptic curve, called its j-**invariant**. Here are some properties of the j-invariant in terms of the corresponding lattices:

The j-invariant

The **Klein j-function** is a bijective holomorphic map

$$j : \mathcal{D}' := \mathcal{D} \setminus \{e^{i\theta} : \pi/2 < \theta < 2\pi/3\} \to \mathbb{C}.$$

If $\mathcal{E}$ is an elliptic curve, then it is isomorphic to an elliptic curve $\mathcal{E}_\tau$ for precisely one $\tau \in \mathcal{D}'$, and hence the value $j(\tau)$ is an invariant of this elliptic curve, called its j-**invariant**. Here are some properties of the j-invariant in terms of the corresponding lattices:

- For $\tau \in \mathcal{D}$, $j(\tau) \in \mathbb{R}$ iff τ belongs to the boundary of $\mathcal{F}$, and Γ_τ is WR iff $j(\tau) \in [0, 1]$.

The j-invariant

The **Klein j-function** is a bijective holomorphic map

$$j : \mathcal{D}' := \mathcal{D} \setminus \{e^{i\theta} : \pi/2 < \theta < 2\pi/3\} \to \mathbb{C}.$$

If $\mathcal{E}$ is an elliptic curve, then it is isomorphic to an elliptic curve $\mathcal{E}_\tau$ for precisely one $\tau \in \mathcal{D}'$, and hence the value $j(\tau)$ is an invariant of this elliptic curve, called its j-**invariant**. Here are some properties of the j-invariant in terms of the corresponding lattices:

- For $\tau \in \mathcal{D}$, $j(\tau) \in \mathbb{R}$ iff τ belongs to the boundary of $\mathcal{F}$, and Γ_τ is WR iff $j(\tau) \in [0, 1]$.
- Suppose $\tau \in \mathcal{F}$ is algebraic. Then

  $$\Gamma_\tau \text{ is arithmetic } \iff \deg_{\mathbb{Q}}(\tau) = 2 \iff j(\tau) \in \overline{\mathbb{Q}}.$$

  In this case, the degree of the algebraic number $j(\tau)$ is the class number of the quadratic imaginary number field $\mathbb{Q}(\tau)$.

Deep holes

Let $L \subset \mathbb{R}^2$ be a lattice with successive minima $\lambda_1 \leq \lambda_2$ and the corresponding minimal basis vectors $\boldsymbol{x}_1, \boldsymbol{x}_2$. It is well known that, choosing $\pm\boldsymbol{x}_1, \pm\boldsymbol{x}_2$ if necessary, we can ensure that the angle θ between these vectors is in the interval $[\pi/3, \pi/2]$: this angle is an invariant of the lattice, we call it **angle** of L.

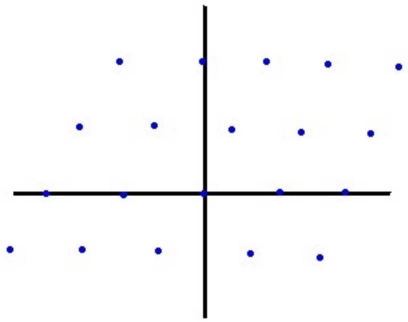
Deep holes

Let $L \subset \mathbb{R}^2$ be a lattice with successive minima $\lambda_1 \leq \lambda_2$ and the corresponding minimal basis vectors $\boldsymbol{x}_1, \boldsymbol{x}_2$. It is well known that, choosing $\pm\boldsymbol{x}_1, \pm\boldsymbol{x}_2$ if necessary, we can ensure that the angle θ between these vectors is in the interval $[\pi/3, \pi/2]$: this angle is an invariant of the lattice, we call it **angle** of L.

A **deep hole** of L is a point in $\mathbb{R}^2$ which is farthest away from the lattice. The distance from the origin to the nearest deep hole is the *covering radius* μ of L. There is a unique deep hole $\boldsymbol{z}$ of L contained in the triangle T with vertices $\boldsymbol{0}$ and the endpoints of $\boldsymbol{x}_1, \boldsymbol{x}_2$: we call it the *fundamental deep hole* of L. Define the **deep hole lattice** of L to be

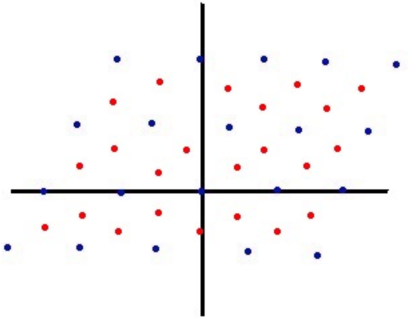
$$H(L) := \operatorname{span}_{\mathbb{Z}}\{\boldsymbol{x}_1, \boldsymbol{z}\}.$$

Deep holes



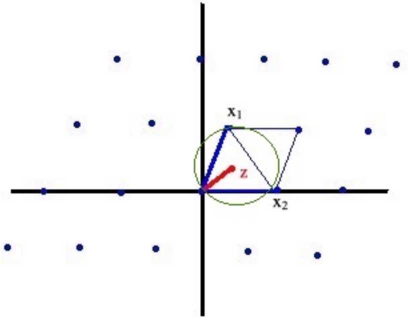
Lattice points in blue

Deep holes



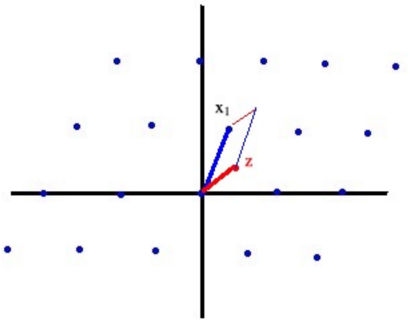
Deep holes in red

Deep holes



Fundamental deep hole

Deep holes



Deep hole lattice: $H(L) = \text{span}_{\mathbb{Z}}\{\boldsymbol{x}_1, \boldsymbol{z}\}$.

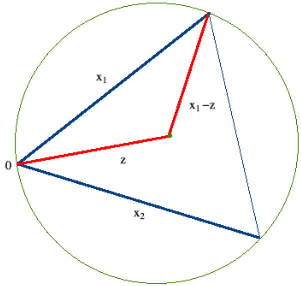
Properties of deep hole lattices

Theorem 1 (F., Guerzhoy, Nielsen (2023))

Let L be a lattice in the plane with the angle $\theta \in [\pi/3, \pi/2]$ and successive minima λ_1 and $\lambda_2 = \alpha\lambda_1$ for some $\alpha \geq 1$. Let $H(L)$ be the deep hole lattice of L. The following statements hold:

1. *If $\alpha \leq 2\sin(\theta + \pi/6)$, then $H(L)$ is WR.*
2. *If L is semi-stable, then $H(L)$ is WR.*
3. *If L is WR, then $H(L) \sim L$.*
4. *If $L \subset K^2$ for some subfield K of $\mathbb{R}$, then $H(L) \subset K^2$.*

Idea of proof



$$\|\boldsymbol{z}\| = \|\boldsymbol{x}_1 - \boldsymbol{z}\| = \frac{\sqrt{\lambda_1^2 + \lambda_2^2 - 2\lambda_1\lambda_2\cos\theta}}{2\sin\theta}$$

is the covering radius of L, where $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$ are vectors corresponding to successive minima of L so that θ is the angle between them. If the angle between $\boldsymbol{z}$ and $\boldsymbol{x}_1 - \boldsymbol{z}$ is in $[\pi/3, \pi/2]$, then $H(L)$ is WR.

Deep hole lattices in the fundamental strip

Next we turn our attention specifically to the lattices of the form Γ_τ for $\tau \in \mathcal{F}$ parameterizing all the similarity classes in the plane. Given a subfield K of $\mathbb{R}$, we say that a similarity class represented by τ **lies over** K if $\tau = a + bi$ with real numbers $a, b \in K$. This is equivalent to saying that some lattice in this similarity class is contained in $K(i) \subseteq \mathbb{C}$, which is identified with $K^2 \subseteq \mathbb{R}^2$.

Deep hole lattices in the fundamental strip

Next we turn our attention specifically to the lattices of the form Γ_τ for $\tau \in \mathcal{F}$ parameterizing all the similarity classes in the plane. Given a subfield K of $\mathbb{R}$, we say that a similarity class represented by τ **lies over** K if $\tau = a + bi$ with real numbers $a, b \in K$. This is equivalent to saying that some lattice in this similarity class is contained in $K(i) \subseteq \mathbb{C}$, which is identified with $K^2 \subseteq \mathbb{R}^2$.

Theorem 2 (F., Guerzhoy, Nielsen (2023))

Let $\tau_0 = a_0 + b_0 i \in \mathcal{F}$ with $a_0, b_0 \in K$ for some subfield $K \subseteq \mathbb{R}$. There exists a finite sequence of numbers $\tau_1, \dots, \tau_n$ given by $\tau_k = a_k + b_k i$ for all $1 \leq k \leq n$, so that

$$a_k = \frac{1}{2}, \; b_k = \frac{a_{k-1}^2 + b_{k-1}^2 - a_{k-1}}{2b_{k-1}} \in K \; \forall \, 1 \leq k \leq n, \qquad (1)$$

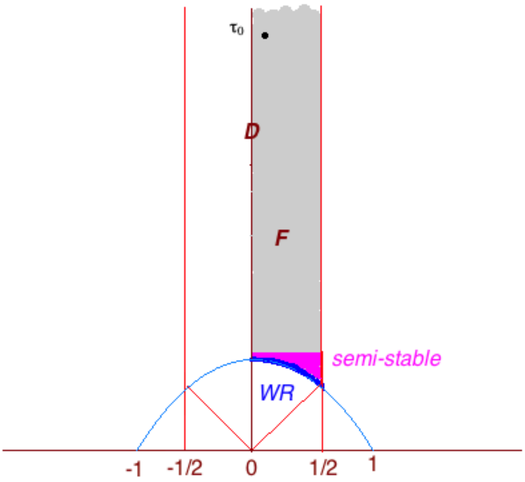
with $\Gamma_{\tau_k} = H(\Gamma_{\tau_{k-1}})$ and Γ_{τ_n} WR, hence $H(\Gamma_{\tau_n}) \sim \Gamma_{\tau_n}$. Also, $\tau_1, \dots, \tau_{n-1} \in \mathcal{F}$, $|\tau_n| \leq 1$ and $n \leq \log_2\left(2b_0/\sqrt{3}\right)$.

Deep hole sequence

We call $\tau_k = a_k + b_k i,\ 1 \leq k \leq n$ the **deep hole sequence** for $\tau_0 = a_0 + b_0 i \in \mathcal{F}$.

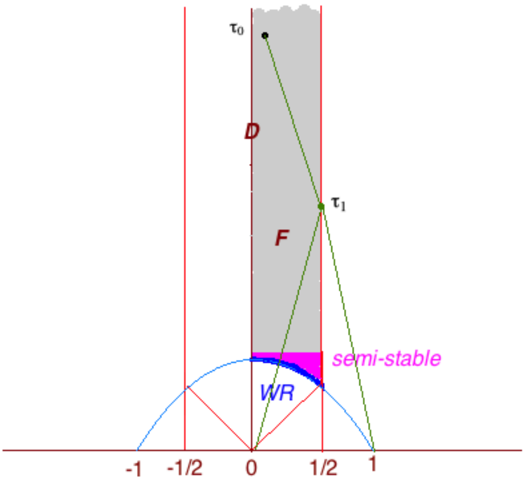
Deep hole sequence

We call $\tau_k = a_k + b_k i,\ 1 \leq k \leq n$ the **deep hole sequence** for $\tau_0 = a_0 + b_0 i \in \mathcal{F}$.



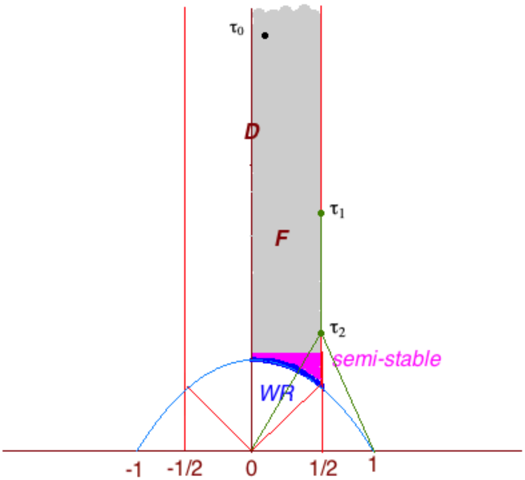
Deep hole sequence

We call $\tau_k = a_k + b_k i,\ 1 \leq k \leq n$ the **deep hole sequence** for $\tau_0 = a_0 + b_0 i \in \mathcal{F}$.



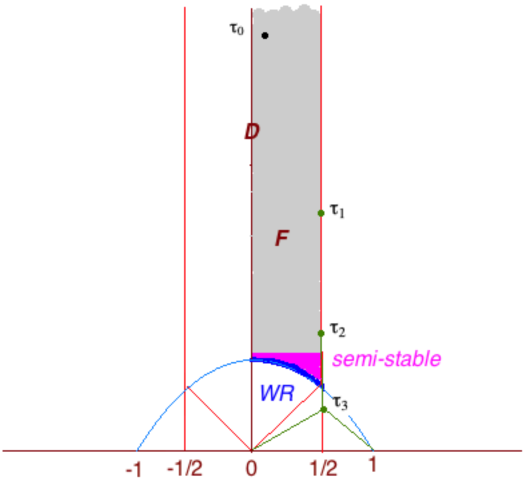
Deep hole sequence

We call $\tau_k = a_k + b_k i,\ 1 \leq k \leq n$ the **deep hole sequence** for $\tau_0 = a_0 + b_0 i \in \mathcal{F}$.



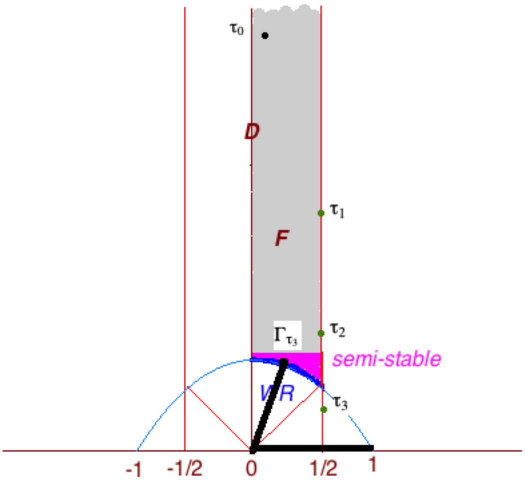
Deep hole sequence

We call $\tau_k = a_k + b_k i,\ 1 \leq k \leq n$ the **deep hole sequence** for $\tau_0 = a_0 + b_0 i \in \mathcal{F}$.

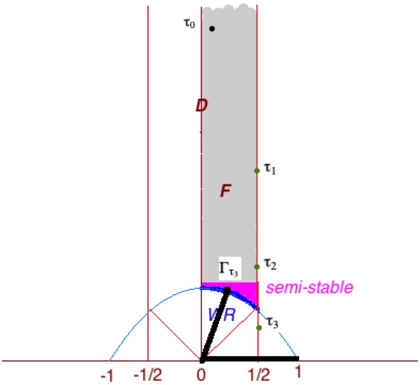


Deep hole sequence

We call $\tau_k = a_k + b_k i,\ 1 \leq k \leq n$ the **deep hole sequence** for $\tau_0 = a_0 + b_0 i \in \mathcal{F}$.



Deep hole sequence



Thus, the map $\tau_i \to \tau_{i+1}$ defines a dynamical system, in which every point is (pre-)periodic with orbit size n as in Theorem 2.

CM case

This orbit is especially interesting in the arithmetic/CM case.

CM case

This orbit is especially interesting in the arithmetic/CM case.

Theorem 3 (F., Guerzhoy, Nielsen (2023))

Let $\tau_0 = a_0 + b_0 i \in \mathcal{F}$ be a quadratic irrationality and

$$\{\tau_k = a_k + b_k i\}_{k=1}^{n}$$

its corresponding deep hole sequence. For each $0 \leq k \leq n$, let $\mathcal{E}_{\tau_k}$ be the corresponding CM elliptic curve with the arithmetic period lattice Γ_{τ_k}. Then all of these elliptic curves are isogenous. Furthermore, for any $0 \leq k \leq n-1$, there exists an isogeny between $\mathcal{E}_{\tau_k}$ and $\mathcal{E}_{\tau_{k+1}}$ with degree

$$\delta_k \leq \frac{12\sqrt{3}\ b_{k+1}\ d_k^4\ (a_k^2 + b_k^2)^2}{b_k},$$

where $d_k = \min\{d \in \mathbb{Z}_{>0} : da_k, d^2 b_k^2 \in \mathbb{Z}\}$.

Proof idea

The proof is based on our previous work with **Max Forst**. Consider the deep hole τ_{k+1} as an element of the quotient group $\mathbb{R}^2/\Gamma_{\tau_k}$. In the arithmetic/CM case, since all the τ_j's are quadratic irrationalities, τ_{k+1} has finite order ℓ in this group, meaning that $\ell\tau_{k+1} \in \Gamma_{\tau_k}$.

Proof idea

The proof is based on our previous work with **Max Forst**. Consider the deep hole τ_{k+1} as an element of the quotient group $\mathbb{R}^2/\Gamma_{\tau_k}$. In the arithmetic/CM case, since all the τ_j's are quadratic irrationalities, τ_{k+1} has finite order ℓ in this group, meaning that $\ell\tau_{k+1} \in \Gamma_{\tau_k}$.

This implies that Γ_{τ_k} contains a similar copy of $\Gamma_{\tau_{k+1}}$ as a sublattice. Hence, the corresponding elliptic curves $\mathcal{E}_{\tau_k}$ and $\mathcal{E}_{\tau_{k+1}}$ are isogenous. Since isogeny is an equivalence relation, we have that the entire sequence of elliptic curves $\{\mathcal{E}_{\tau_k}\}_{k=0}^{n}$ is isogenous.

Proof idea

The proof is based on our previous work with **Max Forst**. Consider the deep hole τ_{k+1} as an element of the quotient group $\mathbb{R}^2/\Gamma_{\tau_k}$. In the arithmetic/CM case, since all the τ_j's are quadratic irrationalities, τ_{k+1} has finite order ℓ in this group, meaning that $\ell\tau_{k+1} \in \Gamma_{\tau_k}$.

This implies that Γ_{τ_k} contains a similar copy of $\Gamma_{\tau_{k+1}}$ as a sublattice. Hence, the corresponding elliptic curves $\mathcal{E}_{\tau_k}$ and $\mathcal{E}_{\tau_{k+1}}$ are isogenous. Since isogeny is an equivalence relation, we have that the entire sequence of elliptic curves $\{\mathcal{E}_{\tau_k}\}_{k=0}^n$ is isogenous.

A bound on the smallest degree of an isogeny follows by an application of Siegel's lemma, guaranteeing a "small" solution to a certain 2×3 homogeneous linear system over $\mathbb{Z}$.

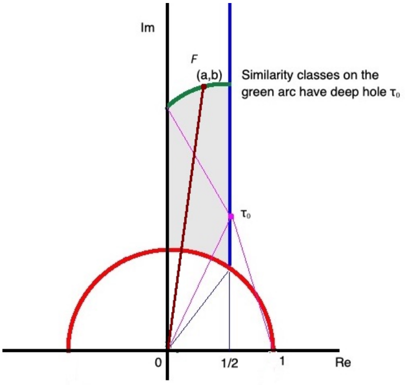
The counting problem

Now, we consider a certain inverse problem. Let K be a number field of degree n and suppose that the similarity class represented by $\tau_0 = \frac{1}{2} + it \in \mathcal{F}$ lies over K. Consider the set

$$S_{K,\tau_0} = \{\tau \in \mathcal{F} : \tau \text{ is defined over } K \text{ and } H(\Gamma_\tau) = \Gamma_{\tau_0}\}. \qquad (2)$$

i.e., the set of similarity classes defined over K whose deep hole lattice is Γ_{τ_0}. While this is an infinite set, we can count these similarity classes bounding the so-called primitive height $\mathcal{H}^p$ of τ.

The counting problem



Similarity classes with a prescribed deep hole. Pink lines are radii of the circle centered at τ_0. The brown line $y = \frac{b}{a}x$ intersects the green arc at a point $\tau = a + bi$ defined over K.

The primitive height

- $\Delta_K =$ be the discriminant of K
- $\mathcal{O}_K =$ ring of integers of K
- $r_1 =$ number of real embeddings, $r_2 =$ number of conjugate pairs of complex embeddings, so $n = r_1 + 2r_2$
- $M(K) =$ set of place of K

The primitive height

- $\Delta_K =$ be the discriminant of K
- $\mathcal{O}_K =$ ring of integers of K
- $r_1 =$ number of real embeddings, $r_2 =$ number of conjugate pairs of complex embeddings, so $n = r_1 + 2r_2$
- $M(K) =$ set of place of K

For a point $\boldsymbol{x} \in K^m$, define its **denominator** to be

$$d(\boldsymbol{x}) = \min\{c \in \mathbb{Q}_{>0} : c\boldsymbol{x} \in \mathcal{O}_K^m\}, \tag{3}$$

and let the **(rationally) primitive point** corresponding to $\boldsymbol{x}$ be $\boldsymbol{x}_p = d(\boldsymbol{x})\boldsymbol{x}$.

The primitive height

- $\Delta_K =$ be the discriminant of K
- $\mathcal{O}_K =$ ring of integers of K
- $r_1 =$ number of real embeddings, $r_2 =$ number of conjugate pairs of complex embeddings, so $n = r_1 + 2r_2$
- $M(K) =$ set of place of K

For a point $\boldsymbol{x} \in K^m$, define its **denominator** to be

$$d(\boldsymbol{x}) = \min\{c \in \mathbb{Q}_{>0} : c\boldsymbol{x} \in \mathcal{O}_K^m\}, \tag{3}$$

and let the **(rationally) primitive point** corresponding to $\boldsymbol{x}$ be $\boldsymbol{x}_p = d(\boldsymbol{x})\boldsymbol{x}$.
We define the **primitive height** of $\boldsymbol{x} \in K^m$ to be

$$\mathcal{H}^p(\boldsymbol{x}) := \max_{v|\infty} |\boldsymbol{x}_p|_v.$$

The counting estimate

Theorem 4 (F., Guerzhoy, Nielsen (2023))

For a real number $T \geq 1$, define

$$S_{K,\tau_0}(T) = \{\tau \in S_{K,\tau_0} : \mathcal{H}^p(\tau) \leq T\},$$

where $\tau_0 = \frac{1}{2} + it \in \mathcal{F}$ lies over K. Then, as $T \to \infty$,

$$|S_{K,\tau_0}(T)| \leq \left(\frac{4^{r_1}\pi^{2r_2}}{8\zeta(2n)\left(2t + \sqrt{4t^2+1}\right)|\Delta_K|} \right) T^{2n} + O(T^{2n-1}),$$

where ζ stands for the Riemann zeta-function and $n = [K : \mathbb{Q}]$.

Proof idea

- Use Minkowski embedding of the number field K to turn $\mathcal{O}_K$ into a full-rank lattice in $\mathbb{R}^n$.

Proof idea

- Use Minkowski embedding of the number field K to turn $\mathcal{O}_K$ into a full-rank lattice in $\mathbb{R}^n$.
- Use some standard lattice-point counting methods to count *all* the points satisfying the appropriate “size” restrictions.

Proof idea

- Use Minkowski embedding of the number field K to turn $\mathcal{O}_K$ into a full-rank lattice in $\mathbb{R}^n$.
- Use some standard lattice-point counting methods to count *all* the points satisfying the appropriate "size" restrictions.
- Use a theorem of Nyman (a version of Cesàro's theorem) on the density of primitive points to specialize the counting estimate to the primitive points we need.

Reference

L. Fukshansky, P. Guerzhoy, T. Nielsen. *Deep hole lattices and isogenies of elliptic curves*, Research in Number Theory, vol. 10 no. 2 (2024), Article#33, 12 pp.

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

Reference

L. Fukshansky, P. Guerzhoy, T. Nielsen. *Deep hole lattices and isogenies of elliptic curves*, Research in Number Theory, vol. 10 no. 2 (2024), Article#33, 12 pp.

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

Thank you!