On arithmetic lattices in the plane

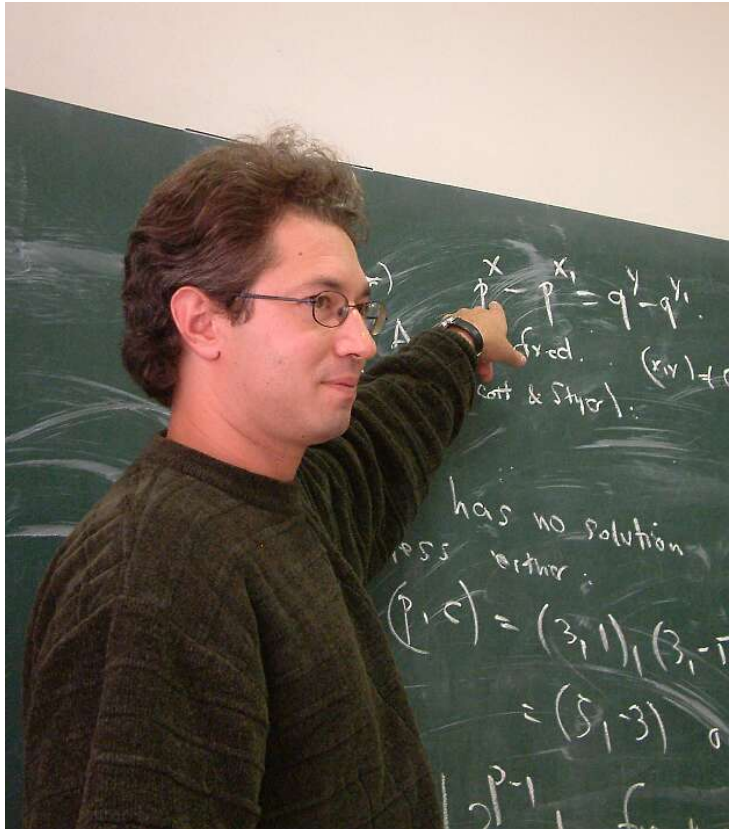
Lenny Fukshansky
Claremont McKenna College

(*joint work with Pavel Guerzhoy and Florian Luca*)

SIU Mathematics Conference
May 16-17, 2016

My co-authors

P. Guerzhoy (Hawaii, USA)



F. Luca (Wits, South Africa)

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** 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** 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 $\mathcal{L}_2$.

Isomorphism classes of elliptic curves

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

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^tA 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^tA 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

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

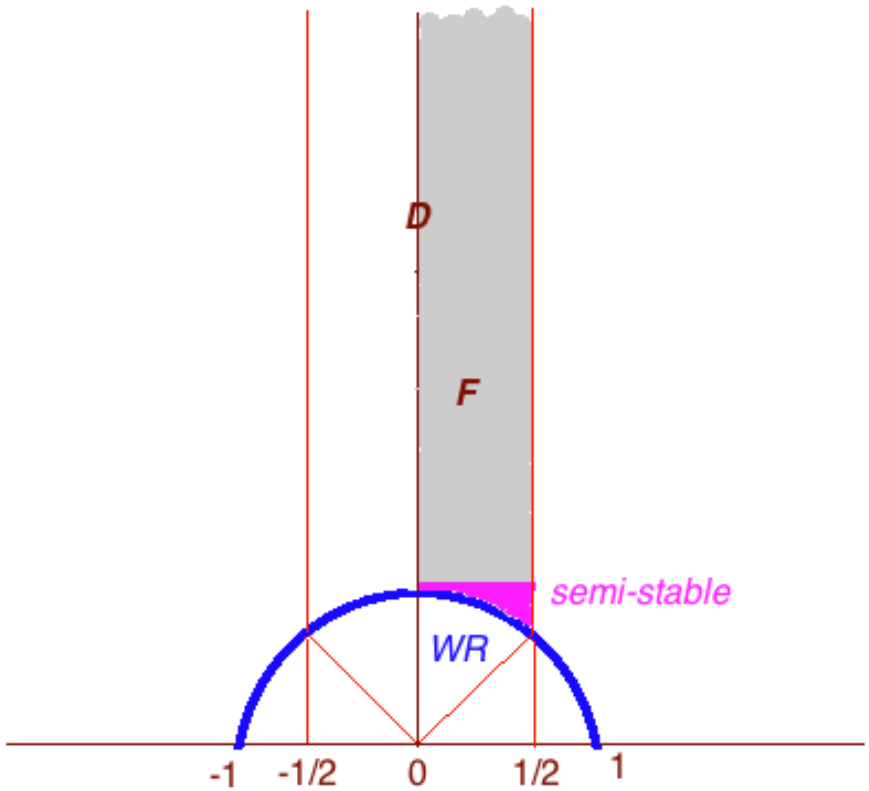
Semi-stable lattices are important in reduction theory of algebraic groups.

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

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

In addition, arithmetic Γ_τ is semi-stable iff

$$1 = \lambda_1(\Lambda_\tau)^2 \ge \det(\Lambda_\tau) = \sqrt{c/d},$$

that is $c \le d$.

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

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

In addition, arithmetic Γ_τ is semi-stable iff

$$1 = \lambda_1(\Lambda_\tau)^2 \ge \det(\Lambda_\tau) = \sqrt{c/d},$$

that is $c \le d$.
Finally, arithmetic Γ_τ is WR iff

$$1 = |\tau|^2 = \frac{a^2}{b^2} + \frac{c}{d},$$

that is $d = b^2$ and $c = b^2 - a^2$.

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 $\mathbb{Q}(\tau)$.

A height function on lattices

Height functions are tools to measure arithmetic complexity of objects. We define the **maximum height** of an arithmetic similarity class $\Gamma_{\tau(a,b,c,d)}$ to be

$$\mathfrak{m}(\Gamma_{\tau(a,b,c,d)}) = \mathfrak{m}(\tau(a,b,c,d)) := \max\{|a|,|b|,|c|,|d|\}.$$

This naive height function satisfies the Northcott's finiteness property; i.e., the number of arithmetic similarity classes with $\mathfrak{m}(\Gamma_{\tau(a,b,c,d)}) \leq T$ is finite for every real number T.

A height function on lattices

Height functions are tools to measure arithmetic complexity of objects. We define the **maximum height** of an arithmetic similarity class $\Gamma_{\tau(a,b,c,d)}$ to be

$$\mathfrak{m}(\Gamma_{\tau(a,b,c,d)}) = \mathfrak{m}(\tau(a,b,c,d)) := \max\{|a|,|b|,|c|,|d|\}.$$

This naive height function satisfies the Northcott's finiteness property; i.e., the number of arithmetic similarity classes with $\mathfrak{m}(\Gamma_{\tau(a,b,c,d)}) \leq T$ is finite for every real number T.

Our main result is a counting estimate on the number of such similarity classes. Let $T \in \mathbb{Z}_{>0}$, and let

$$N_1(T) = |\{\Lambda_\tau : \Lambda_\tau \text{ is arithmetic and } \mathfrak{m}(\Lambda_\tau) \leq T\}|,$$
$$N_2(T) = |\{\Lambda_\tau : \Lambda_\tau \text{ is arithmetic semi-stable and } \mathfrak{m}(\Lambda_\tau) \leq T\}|,$$
$$N_3(T) = |\{\Lambda_\tau : \Lambda_\tau \text{ is arithmetic WR and } \mathfrak{m}(\Lambda_\tau) \leq T\}|.$$

Main result

Theorem 1 (F., Guerzhoy, Luca (2015))

With notation as above, $N_1(T) > N_2(T) > N_3(T)$, *and as* $T \to \infty$,

$$N_1(T) = \frac{39T^4}{8\pi^4} + O(T^3 \log T),$$

and

$$N_2(T) = \frac{3T^4}{8\pi^4} + O(T^3 \log T),$$

while

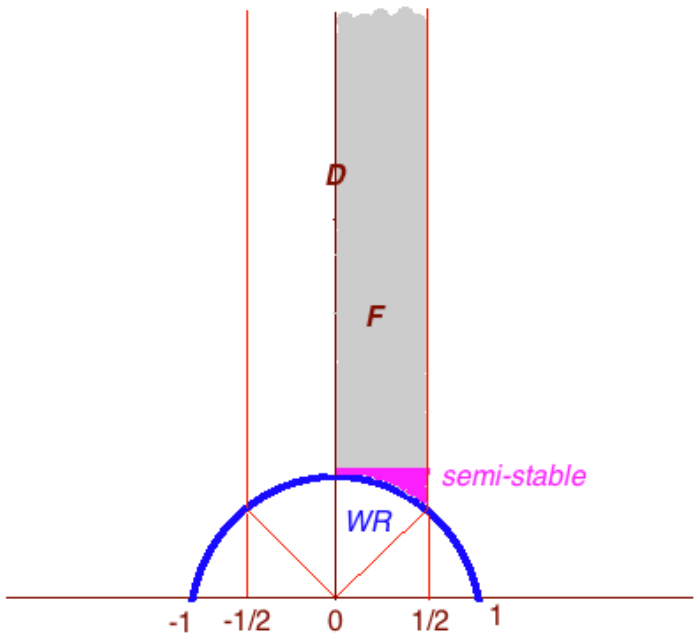
$$N_3(T) = \frac{3T^2}{2\pi^2} + O(T \log T).$$

Consequence

It follows from Theorem 1 that about 7.7% of arithmetic similarity classes in the plane are semi-stable, when counted with respect to the maximum height.

Consequence

It follows from Theorem 1 that about 7.7% of arithmetic similarity classes in the plane are semi-stable, when counted with respect to the maximum height.



On the other hand, only about 4.5% (with respect to Poincare measure) of all similarity classes in the plane are semi-stable.

Method of proof

Asymptotic for $N_3(T)$ follows from a simple estimate on $\sum_{b=1}^{T} \varphi(b)$ for the Euler φ-function, which is well known.

Method of proof

Asymptotic for $N_3(T)$ follows from a simple estimate on $\sum_{b=1}^{T} \varphi(b)$ for the Euler φ-function, which is well known. Then we show that, as $T \to \infty$,

$$N_1(T) \sim N_2(T) + \frac{3T^2}{\pi^2} \sum_{b=1}^{T} \varphi(b).$$

Method of proof

Asymptotic for $N_3(T)$ follows from a simple estimate on $\sum_{b=1}^{T} \varphi(b)$ for the Euler φ-function, which is well known. Then we show that, as $T \to \infty$,

$$N_1(T) \sim N_2(T) + \frac{3T^2}{\pi^2} \sum_{b=1}^{T} \varphi(b).$$

Estimating $N_2(T)$ comes down to proving that for $b \in \mathbb{Z}_{>0}$,

$$\sum_{\substack{a=0 \\ \gcd(a,b)=1}}^{[b/2]} \frac{a^2}{b^2} = \frac{\varphi(b)}{24} + O\left(2^{\omega(b)}\right)$$

where $\omega(b)$ is the number of prime divisors of b. Our main tools are Abel's summation formula and estimates on average order of some arithmetic functions.

Thank you!