DEEP HOLE LATTICES AND ISOGENIES OF ELLIPTIC CURVES

LENNY FUKSHANSKY, PAVEL GUERZHOY, AND TANIS NIELSEN

ABSTRACT. Given a lattice L in the plane, we define the affiliated deep hole lattice $H(L)$ to be spanned by a shortest vector of L and a deep hole of L contained in the triangle with sides corresponding to the shortest basis vectors. We study the geometric and arithmetic properties of deep hole lattices. In particular we investigate conditions on L under which $H(L)$ is well-rounded and prove that $H(L)$ is defined over the same field as L. For the period lattice corresponding to an isomorphism class of elliptic curves, we produce a finite sequence of deep hole lattices ending with a well-rounded lattice which corresponds to a point on the boundary arc of the fundamental strip under the action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper halfplane. In the case of CM elliptic curves, we prove that all elliptic curves generated by this sequence are isogenous to each other and produce bounds on the degree of isogeny. Finally, we produce a counting estimate for the planar lattices with a prescribed deep hole lattice.

1. INTRODUCTION

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. The lattice L is called *well-rounded* (WR) if $\lambda_1 = \lambda_2$; it is called *semi-stable* if $\lambda_1 \geq \det(L)^{1/2}$. For planar lattices, WR property implies semi-stability (this is not true in higher dimensions). Two lattices L_1 and L_2 are said to be *similar*, denoted $L_1 \sim L_2$, if there exists $\alpha \in \mathbb{R}_{>0}$ and $U \in \mathcal{O}_2(\mathbb{R})$ such that $L_2 = \alpha U L_1$. This is an equivalence relation which preserves WR and semi-stability properties, hence we will speak of WR and semi-stable similarity classes. WR and semi-stable lattices play an important role in lattice theory and are objects of substantial study; see [2], [5], [6] and references within for some details.

Similarity classes of planar lattices can be parameterized as follows. Let $\mathbb{H} = \{\tau = a + bi : b \geq 0\} \subset \mathbb{C}$ be the upper half-plane, and let

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

Let

$$\mathcal{F} := \{\tau = a + bi \in \mathbb{H} : 0 \leq a \leq 1/2, |\tau| \geq 1\},$$
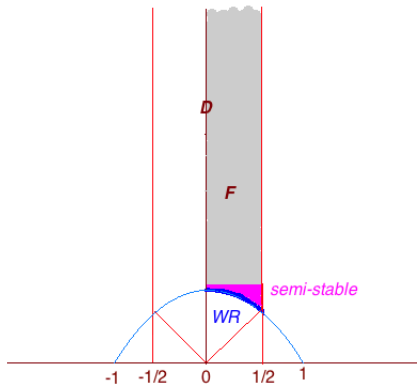
FIGURE 1. Space of lattices in $\mathbb{R}^2$ with WR and semi-stable sub-regions marked by colors.

so, loosely speaking, $\mathcal{F}$ is "half" of $\mathcal{D}$. Every point $\tau = a + bi \in \mathcal{F}$ can be identified with a lattice

$$(1) \qquad\qquad \Lambda_\tau := \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \mathbb{Z}^2$$

in $\mathbb{R}^2$. Then the lattice L with successive minima $\lambda_1 \leq \lambda_2$ and the corresponding minimal basis vectors $\boldsymbol{x}_1, \boldsymbol{x}_2$ is similar to $L' = \frac{1}{\lambda_1} L$. Rotating if necessary, we can ensure that the image of $\boldsymbol{x}_1$ under this similarity coincides with $\boldsymbol{e}_1 := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Then the image $\boldsymbol{x}_2'$ of $\boldsymbol{x}_2$ must have its first coordinate between 0 and $1/2$, since otherwise one of $\boldsymbol{x}_2' \pm \boldsymbol{e}_1 \in L$ would be a shorter vector than $\boldsymbol{x}_2'$ and still linearly independent with $\boldsymbol{e}_1$. Furthermore, reflecting over $\boldsymbol{e}_1$, if necessary, we can assume that $\boldsymbol{x}_2'$ has a positive second coordinate. In other words, every planar lattice L is similar to a lattice of the form Λ_τ for some $\tau \in \mathcal{F}$, and it is a well-known fact that it is similar to *precisely one* such lattice; we will say that this similarity class is *represented* by τ. Hence, $\mathcal{F}$ can be thought of as the space of similarity classes of lattices in $\mathbb{R}^2$ (see Figure 1). WR similarity classes correspond to the circular arc $\{\tau \in \mathcal{F} : |\tau| = 1\}$ and semi-stable similarity classes correspond to the set $\{\tau = a + bi \in \mathcal{F} : b \leq 1\}$.

On the other hand, the full domain $\mathcal{D}$ can be viewed as the space of isomorphism classes of elliptic curves: a point τ corresponds to the isomorphism class of the elliptic curve given by the complex torus $\mathbb{C}/\Lambda_\tau$, where we are identifying $\mathbb{C}$ with $\mathbb{R}^2$ and thinking of Λ_τ as $\mathrm{span}_{\mathbb{Z}}\{1, \tau\} \subset \mathbb{C}$. This being said, while the lattices Λ_τ and $\Lambda_{-\bar\tau}$ are similar the corresponding elliptic curves are not isomorphic: instead, the two elliptic curves have conjugate j-invariants, since $j(-\bar\tau) = \overline{j(\tau)}$ (here j is Klein's modular j-function; see [9] for details).

A *deep hole* of a lattice 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

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

The main goal of this paper is to investigate the properties of this new family of deep hole lattices and connect them to the properties of the associated elliptic curves. We start with some observations about the geometry and arithmetic of $H(L)$, proving the following theorem in Section 2.

Theorem 1.1. *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 $H(L) \subset K^2$.*

Next we turn our attention specifically to the lattices of the form Λ_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 $K^2 \subseteq \mathbb{R}^2$.

A similarity class represented by τ lying over K contains infinitely many lattices $L \subset K^2$. It is not difficult to observe that the similarity class of the deep hole lattice lies over the same field as the similarity class of the original lattice (Lemma 3.1). In fact, the deep hole construction allows us to describe an interesting family of similarity classes defined over the same field.

Theorem 1.2. *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 $\tau_1, \ldots, \tau_n$ given by $\tau_k = a_k + b_k i$ for all $1 \leq k \leq n$, so that*

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

with $\Lambda_{\tau_k} = H(\Lambda_{\tau_{k-1}})$ and Λ_{τ_n} well-rounded, hence $H(\Lambda_{\tau_n}) \sim \Lambda_{\tau_n}$. Furthermore, $\tau_1, \ldots, \tau_{n-1} \in \mathcal{F}$, $|\tau_n| \leq 1$ and $n \leq \log_2\left(\frac{2b_0}{\sqrt{3}}\right)$.

We prove Theorem 1.2 in Section 3. For a given $\tau_0 = a_0 + b_0 i \in \mathcal{F}$, we will refer to the sequence of complex numbers

$$\tau_k = a_k + b_k i, \ 1 \leq k \leq n,$$

defined as in (2), as the *deep hole sequence* for τ_0 and call the corresponding sequence of lattices Λ_{τ_k} as defined in Corollary 1.2 the *deep hole lattice sequence* for Λ_{τ_0}.

We focus on a particular situation in which this deep hole lattice sequence is especially interesting. A lattice $L = A\mathbb{Z}^2 \subset \mathbb{R}^2$ is called *arithmetic* if the corresponding Gram matrix $A^\top A$ is a scalar multiple of an integer matrix, i.e. L is similar to an integral lattice. A lattice Λ_τ is arithmetic if and only if

$$\tau = \frac{p}{q} + i\sqrt{\frac{s}{t}} \in \mathcal{F}$$

for some $p, q, s, t \in \mathbb{Z}$, i.e. τ is a quadratic irrationality. This condition is equivalent to the elliptic curve E_τ with period lattice Λ_τ having complex multiplication by the imaginary quadratic field $\mathbb{Q}(\tau)$, i.e. the endomorphism ring of E_τ is an order in $\mathbb{Q}(\tau)$ properly containing $\mathbb{Z}$. Thus, if τ_0 in Theorem 1.2 is a quadratic irrationality, then Λ_{τ_0} and the entire sequence of deep hole lattices $\Lambda_{\tau_1}, \ldots, \Lambda_{\tau_n}$ are arithmetic with the

corresponding CM elliptic curves E_{τ_k} having their endomorphism rings in the same imaginary quadratic field $\mathbb{Q}(\tau_0)$. Furthermore, each curve E_{τ_k} for $1 \leq k \leq n-1$ has a real negative j-invariant, whereas the curve E_{τ_n} corresponds to a well-rounded lattice Λ_{τ_n}, and hence has real j-invariant in the interval $[0,1]$ (see [5] for details). We review the necessary notation and prove the following result in Section 3.

Theorem 1.3. *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 E_{τ_k} be the corresponding CM elliptic curve with the arithmetic period lattice Λ_{τ_k}. Then all of these elliptic curves are isogenous. Furthermore, for any $0 \leq k \leq n-1$, there exists an isogeny between E_{τ_k} and $E_{\tau_{k+1}}$ 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 $d_k = \min\{d \in \mathbb{Z}_{>0} : da_k, d^2 b_k^2 \in \mathbb{Z}\}$.

Finally, we consider a certain inverse problem. From here on, let K be an arbitrary 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

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

i.e., the set of similarity classes defined over K whose deep hole lattice is Λ_{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 which is defined in Section 4.

Theorem 1.4. *For a real number $T \geq 1$, define*

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

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 $n = [K : \mathbb{Q}]$.

We recall necessary notation and prove Theorem 1.4 in Section 4. We are now ready to proceed.

2. Geometry of deep hole lattices

The main goal of this section is to prove Theorem 1.1. We do it via a lemma and three corollaries, each proving one of the four parts of the theorem. As in the statement of the theorem, let us write α for the quotient $\lambda_2/\lambda_1 \geq 1$.

Lemma 2.1. *If $\alpha \leq 2\sin(\theta + \pi/6)$, then $H(L)$ is WR.*

Proof. Let ν be the angle between the vectors $\boldsymbol{z}, \boldsymbol{x}_1 - \boldsymbol{z}$. Since $\boldsymbol{z}$ is the center of the circle circumscribed about the triangle T, we have $\|\boldsymbol{z}\| = \|\boldsymbol{x}_1 - \boldsymbol{z}\|$ as both of these line segments are radii of this circle. This common value is μ, the covering radius of the lattice L, which is given by the formula

$$\mu = \frac{\sqrt{\lambda_1^2 + \lambda_2^2 - 2\lambda_1\lambda_2\cos\theta}}{2\sin\theta},$$

see Lemma 5.2 of [3].

Then the triangle with sides

$$\boldsymbol{x}_1, \boldsymbol{z}, \boldsymbol{x}_1 - \boldsymbol{z}$$

is isosceles, and so the bisector of the angle ν is perpendicular to $\boldsymbol{x}_1$ and is the median of that side. Therefore we have

$$(4) \qquad \sin(\nu/2) = \frac{\lambda_1/2}{\mu} = \frac{\lambda_1 \sin\theta}{\sqrt{\lambda_1^2 + \lambda_2^2 - 2\lambda_1\lambda_2 \cos\theta}} = \frac{\sin\theta}{\sqrt{1 + \alpha^2 - 2\alpha \cos\theta}}.$$

If $\nu \in [\pi/3, \pi/2]$, then the lattice $H(L)$ is well-rounded: since $\|\boldsymbol{z}\| = \|\boldsymbol{x}_1 - \boldsymbol{z}\|$,

$$\|a\boldsymbol{z} + b(\boldsymbol{x}_1 - \boldsymbol{z})\|^2 = (a^2 + b^2)\|\boldsymbol{z}\|^2 + 2ab\|\boldsymbol{z}\|^2 \cos\nu \geq \|\boldsymbol{z}\|^2,$$

for any $a, b \in \mathbb{Z}$, and hence $\boldsymbol{z}, \boldsymbol{x}_1 - \boldsymbol{z}$ is a minimal basis for $H(L)$. Thus the sufficient condition is $\sin(\nu/2) \geq \sin(\pi/6) = 1/2$, and so we have the condition:

$$4\sin^2\theta \geq 1 + \alpha^2 - 2\alpha \cos\theta.$$

Using the identity $\sin^2\theta = 1 - \cos^2\theta$ and rearranging, we obtain

$$3 - 3\cos^2\theta = 3\sin^2\theta \geq \alpha^2 - 2\alpha \cos\theta + \cos^2\theta = (\alpha - \cos\theta)^2,$$

which leads to

$$\alpha \leq \sqrt{3}\sin\theta + \cos\theta = 2\sin(\theta + \pi/6).$$

$\square$

Now suppose that $L \sim \Lambda_\tau$ for some

$$(5) \qquad \tau = \alpha e^{i\theta} = \alpha \cos\theta + \alpha i \sin\theta \in \mathcal{F},$$

where $\alpha = |\tau|$ and θ is the angle of L.

Corollary 2.2. *If L is semi-stable, then $H(L)$ is WR.*

Proof. If L is semi-stable, then

$$\alpha = |\tau| \leq \sqrt{5}/2 < \sqrt{3} = \min\left\{2\sin(\theta + \pi/6) : \theta \in [\pi/3, \pi/2]\right\},$$

and so the condition of Lemma 2.1 is satisfied. $\square$

Corollary 2.3. *If L is WR, then $H(L) \sim L$.*

Proof. Notice that two WR lattices are similar if and only if they have the same angle. Using notation and setup of Lemma 2.1 and applying (4) with $\alpha = 1$ (since L is WR), we obtain:

$$\sin(\nu/2) = \frac{\sin\theta}{\sqrt{2 - 2\cos\theta}}, \quad \cos(\nu/2) = \frac{\sqrt{2 - 2\cos\theta - \sin^2\theta}}{\sqrt{2 - 2\cos\theta}}.$$

Therefore

$$\begin{aligned}\cos\nu &= \cos^2(\nu/2) - \sin^2(\nu/2) = \frac{2 - 2\cos\theta - 2\sin^2\theta}{2 - 2\cos\theta} \\ &= \frac{-\cos\theta(1 - \cos\theta)}{1 - \cos\theta} = -\cos\theta = \cos(\pi - \theta).\end{aligned}$$

Hence the angle between $\boldsymbol{z}$ and $-(\boldsymbol{z} - \boldsymbol{x}_1) = \boldsymbol{x}_1 - \boldsymbol{z}$ is $\theta \in [\pi/3, \pi/2]$. Then $\boldsymbol{z}, \boldsymbol{x}_1 - \boldsymbol{z}$ is a minimal basis for $H(L)$, so the angle of $H(L)$ is θ. $\square$

Corollary 2.4. *If $L \subset K^2$ for some subfield K of $\mathbb{R}$, then $H(L) \subset K^2$, and hence the similarity class of $H(L)$ lies over K.*

Proof. Since $L \subset K^2$, we have $\lambda_j^2 = \|\boldsymbol{x}_j\|^2 \in K$ for $j = 1, 2$, and so $\alpha^2 \in K$. Let $A = (\boldsymbol{x}_1 \ \boldsymbol{x}_2) \in \mathrm{GL}_2(K)$ be the corresponding basis matrix. By Lemma 4.1 of [3], the fundamental deep hole of L is

$$(6) \qquad \boldsymbol{z} = \frac{1}{2}(A^\top)^{-1} \begin{pmatrix} \lambda_1^2 \\ \lambda_2^2 \end{pmatrix},$$

and hence $H(L) = \mathrm{span}_{\mathbb{Z}} \{\boldsymbol{x}_1, \boldsymbol{z}\} \subset K^2$. As we detailed in Section 1, this implies that the similarity class of $H(L)$ lies over K. $\qquad \square$

3. Deep hole lattices in the fundamental strip

We start with a simple observation about the similarity class of a deep hole lattice.

Lemma 3.1. *Let $\tau = a + bi \in \mathcal{F}$, Λ_τ the corresponding lattice as in (1) and suppose that Λ_τ lies over a field $K \subseteq \mathbb{C}$. Then $\gamma \in \mathcal{F}$ representing the similarity class of $H(\Lambda_\tau)$ also lies over K.*

Proof. Let us write

$$\boldsymbol{e}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \ \boldsymbol{\tau} = \begin{pmatrix} a \\ b \end{pmatrix}$$

for the minimal basis of Λ_τ and $\theta \in [\pi/3, \pi/2]$ for the angle between these two vectors, hence

$$\cos\theta = \frac{a}{\sqrt{a^2 + b^2}}, \ \sin\theta = \frac{b}{\sqrt{a^2 + b^2}}.$$

Then (6) guarantees that the fundamental deep hole of Λ_τ is

$$(7) \qquad \boldsymbol{\tau}_1 = \begin{pmatrix} 1/2 \\ (a^2 + b^2 - a)/2b \end{pmatrix},$$

which certainly lies over K and $H(\Lambda_\tau) = \Lambda_{\tau_1}$ for $\tau_1 = \frac{1}{2} + \frac{a^2 + b^2 - a}{2b}i$. If $\tau_1 \in \mathcal{F}$, then $\gamma = \tau_1$ and we are done.

Suppose $\tau_1 \notin \mathcal{F}$. This means that $|\tau_1| < 1$, then the vectors $\boldsymbol{\tau}_1, \boldsymbol{e}_1 - \boldsymbol{\tau}_1 \in \Lambda_{\tau_1}$ have equal length and the angle between them is in the interval $(\pi/3, 2\pi/3]$: the largest value $2\pi/3$ is attained when $\tau = \frac{1}{2} + \frac{\sqrt{3}}{2}i$. On the other hand, $|\tau_1| < 1$ implies that $(a^2 + b^2 - a)/2b < \sqrt{3}/2$, hence

$$\frac{\|\boldsymbol{\tau}\|}{\|\boldsymbol{e}_1\|} = \sqrt{a^2 + b^2} < \frac{\sqrt{3}b + a}{\sqrt{a^2 + b^2}} = \sqrt{3}\sin\theta + \cos\theta,$$

which means that Λ_τ satisfies the condition of Lemma 2.1. Therefore $H(\Lambda_\tau)$ is WR and its similarity class γ lies over K by Corollary 2.4. This completes the proof. $\quad \square$

We can use this lemma to give a quick proof of Theorem 1.2.

Proof of Theorem 1.2. Existence of the sequence τ_k with the claimed properties follows by iterative application of (7). Further, $a_k \leq 1/2$ for each k, so

$$b_k = \frac{b_{k-1}}{2} - \frac{a_{k-1}(1 - a_{k-1})}{2b_{k-1}} \leq \frac{b_{k-1}}{2} - \frac{1}{8b_{k-1}} < \frac{b_{k-1}}{2},$$

hence $b_k < \frac{b_0}{2^k}$. If $n \geq \log_2\left(\frac{2b_0}{\sqrt{3}}\right)$, then $b_n < \sqrt{3}/2$, which means that $|\tau_n| < 1$ (i.e., $\tau_n \notin \mathcal{F}$) and hence Λ_{τ_n} is well-rounded. Then Corollary 2.3 implies that $H(\Lambda_{\tau_n})$ is similar to Λ_{τ_n} and hence the sequence of deep holes has stabilized. $\square$

Next we turn to the proof of Theorem 1.3. First, let us recall the definition of an isogeny. Given lattices $\Lambda, \Lambda' \subset \mathbb{C}$ a nonzero morphism $E \to E'$ between the corresponding elliptic curves $E = \mathbb{C}/\Lambda$ and $E' = \mathbb{C}/\Lambda'$ 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, and hence maps $E \to E'$. In fact, every isogeny is of this form. The *degree* of this isogeny is then 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 $E \to E'$ exists, then there also exists the dual isogeny $E' \to E$ of the same degree such that their composition is simply 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. See [9] for more details on elliptic curves and their isogenies.

Proof of Theorem 1.3. To prove the first statement, pick any $0 \leq k \leq n-1$, then $\boldsymbol{\tau}_{k+1} = \begin{pmatrix} a_{k+1} \\ b_{k+1} \end{pmatrix}$ is the fundamental deep hole of Λ_{τ_k}. Notice that the successive minima of Λ_{τ_k} are $\lambda_{k1} = 1$, $\lambda_{k2} = |\tau_k|$ with the corresponding minimal basis vectors $\boldsymbol{e}_1, \boldsymbol{\tau}_k$, and hence

$$\boldsymbol{e}_1 \cdot \boldsymbol{\tau}_k = a_k \lambda_{k1}^2 = \frac{a_k}{a_k^2 + b_k^2} \lambda_{k2}^2,$$

where $a_k, \frac{a_k}{a_k^2 + b_k^2} \in \mathbb{Q}$. Then Theorem 4.3 of [3] implies that the deep hole $\boldsymbol{\tau}_{k+1}$ has finite order ℓ in the quotient group $\mathbb{R}^2/\Lambda_{\tau_k}$, meaning that $\ell\boldsymbol{\tau}_{k+1} \in \Lambda_{\tau_k}$. Since $\ell\boldsymbol{e}_1 \in \Lambda_{\tau_k}$, we have that

$$\ell\Lambda_{\tau_{k+1}} = \ell\operatorname{span}_{\mathbb{Z}}\{\boldsymbol{e}_1, \boldsymbol{\tau}_{k+1}\} \subseteq \Lambda_{\tau_k} = \operatorname{span}_{\mathbb{Z}}\{\boldsymbol{e}_1, \boldsymbol{\tau}_k\},$$

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

Next, we prove a bound on the smallest degree of an isogeny. Recall that $d_k = \min\{d \in \mathbb{Z}_{>0} : da_k, d^2 b_k^2 \in \mathbb{Z}\}$, and notice that the fundamental deep hole of the lattice $d_k\Lambda_{\tau_k} = \operatorname{span}_{\mathbb{Z}}\{d_k\boldsymbol{e}_1, d_k\boldsymbol{\tau}_k\}$ is $d_k\boldsymbol{\tau}_{k+1}$. Successive minima of this new lattice are $d_k\lambda_{k1}, d_k\lambda_{k2}$; furthermore,

$$(d_k\lambda_{k1})^2, \ (d_k\lambda_{k2})^2, \ d_k\boldsymbol{e}_1 \cdot d_k\boldsymbol{\tau}_k \in \mathbb{Z}.$$

Then Theorem 4.3 of [3] implies that the deep hole $d_k\boldsymbol{\tau}_{k+1}$ has order

$$\ell \leq 12\sqrt{3} \, (d_k\lambda_{k2})^4 = 12\sqrt{3} \, d_k^4 \, |\tau_k|^4$$

in $\mathbb{R}^2/\Lambda_{d_k\tau_k}$, which is the same as the order of $\boldsymbol{\tau}_{k+1}$ in $\mathbb{R}^2/\Lambda_{\tau_k}$. Then

$$[\Lambda_{\tau_k} : \ell\Lambda_{\tau_{k+1}}] = \frac{\ell^2 \det \Lambda_{\tau_{k+1}}}{\det \Lambda_{\tau_k}} = \frac{\ell^2 b_{k+1}}{b_k} \leq \frac{12\sqrt{3}\, b_{k+1}\, d_k^4\, (a_k^2 + b_k^2)^2}{b_k}.$$

There exists an isogeny between E_{τ_k} and $E_{\tau_{k+1}}$ whose degree is $\delta_k = [\Lambda_{\tau_k} : \ell\Lambda_{\tau_{k+1}}]$.

$\square$

4. COUNTING SIMILARITY CLASSES WITH A PRESCRIBED DEEP HOLE

In this section we will prove Theorem 1.4, starting with some notation. Throughout this section, let K be a number field of degree n over $\mathbb{Q}$ with at least one real embedding, let Δ_K be the discriminant of K, and let $\mathcal{O}_K$ be its ring of integers. Write $\sigma_1, \ldots, \sigma_{r_1}$ for the real embeddings of K. Specifically, we fix the real embedding σ_1 and identify every element $c \in K$ with the corresponding real number $\sigma_1(c)$. Let also $\tau_1, \bar{\tau}_1, \ldots, \tau_{r_2}, \bar{\tau}_{r_2}$ be the complex embeddings of K, then

$$n = r_1 + 2r_2.$$

The space $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ can be viewed as a subspace of

$$\left\{ (\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} : y_{r_2+j} = \bar{y}_j \ \forall\ 1 \leq j \leq r_2 \right\} \subset \mathbb{C}^n.$$

Then for any $m \geq 1$, $K_{\mathbb{R}}^m$ is a mn-dimensional Euclidean space under the bilinear form induced by the trace form on K:

$$\langle \alpha, \beta \rangle := \mathrm{Tr}_K(\alpha\bar{\beta}) \in \mathbb{Q},$$

for every $\alpha, \beta \in K$, where Tr_K is the absolute number field trace on K. We also define the sup-norm on $K_{\mathbb{R}}^m$ by

$$|\boldsymbol{x}| := \max\{|x_1|, \ldots, |x_{mn}|\},$$

for any $\boldsymbol{x} \in K_{\mathbb{R}}^m$, where $|x_j|$ stands for the usual absolute value of x_j on $\mathbb{C}$. Let

$$\Sigma_K = (\sigma_1, \ldots, \sigma_{r_1}, \tau_1, \bar{\tau}_1, \ldots, \tau_{r_2}, \bar{\tau}_{r_2}) : K \hookrightarrow K_{\mathbb{R}}$$

be the Minkowski embedding. We also write Σ_K for the induced map $K^m \hookrightarrow K_{\mathbb{R}}^m$. Then $\Lambda_K^m := \Sigma_K(\mathcal{O}_K^m)$ is a lattice of full rank in $K_{\mathbb{R}}^m$. We define the determinant of a full-rank lattice to be the absolute value of the determinant of any basis matrix for the lattice, then

$$(8) \qquad\qquad \det(\Lambda_K^m) = |\Delta_K|^{m/2},$$

as follows, for instance, from Corollary 2.4 of [1] (see also Theorem 2 of [10]).

Let $M(K)$ be the set of places of K and let $n_v = [K_v : \mathbb{Q}_v]$ be the local degree of K at each place $v \in M(K)$. Select absolute values so that $|\ |_v$ extends the usual absolute value on $\mathbb{Q}$ if v is archimedean and $|\ |_v$ extends the usual p-adic absolute value on $\mathbb{Q}$ if v is non-archimedean. With this choice, the product formula reads

$$\prod_{v \in M(K)} |c|_v^{n_v} = 1,$$

for each $0 \neq c \in K$. For each archimedean place v, $|c|_v = |\sigma_j(c)|$ or $|\tau_j(c)|$ for an appropriate $1 \leq j \leq r_1$ or $1 \leq j \leq r_2$, depending on whether v is real (i.e., $n_v = 1$) or complex (i.e, $n_v = 2$); here $|\ |$ stands for the usual absolute value on $\mathbb{C}$. For each $v \in M(K)$, define the local sup-norm of a vector $\boldsymbol{x} \in K^m$ as

$$|\boldsymbol{x}|_v = \max\{|x_1|_v, \ldots, |x_m|_v\}.$$

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

$$(9) \qquad d(\boldsymbol{x}) = \min\{c \in \mathbb{Q}_{>0} : c\boldsymbol{x} \in \mathcal{O}_K^m\},$$

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

Lemma 4.1. *The denominator $d(\boldsymbol{x})$ (and hence the primitive point $\boldsymbol{x}_p$) is well-defined.*

Proof. We need to show that the minimum in the definition (9) exists. Let

$$\boldsymbol{x} = (x_1, \ldots, x_m) \in K^m.$$

There exists a rational number c such that $c\boldsymbol{x} \in \mathcal{O}_K^m$, and write $c = \frac{c_1}{c_2} \in \mathbb{Q}$ with $\gcd(c_1, c_2) = 1$. Then

$$\frac{c_1}{c_2} x_j \in \mathcal{O}_K, \ \forall \ 1 \leq j \leq m,$$

and hence the number field norm

$$\mathbb{N}_K\left(\frac{c_1}{c_2} x_j\right) = \frac{c_1^n}{c_2^n} \mathbb{N}_K(x_j) \in \mathbb{Z},$$

while $\mathbb{N}_K(x_j) = x_{j1}/x_{j2} \in \mathbb{Q}$ with $\gcd(x_{j1}, x_{j2}) = 1$. This means that $c_2 \mid x_{j1}$ for all $1 \leq j \leq m$, which means that the set of possible denominators for c is finite, and hence the minimum of c exists. $\square$

Notice that for any $\boldsymbol{x} \in K^m$ and non-archimedean $v \in M(K)$, $|\boldsymbol{x}_p|_v \leq 1$, since $\boldsymbol{x}_p \in \mathcal{O}_K^m$. We define the *primitive height* of $\boldsymbol{x} \in K^m$ to be

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

While it is clear that when $\boldsymbol{x}_p = \boldsymbol{y}_p$, then $\boldsymbol{x}$ and $\boldsymbol{y}$ represent the same projective point over K, it may happen that $\boldsymbol{x}_p \neq \boldsymbol{y}_p$ while $\boldsymbol{x} = \alpha\boldsymbol{y}$ for some $\alpha \in K$ (e.g., $\boldsymbol{x} = -\boldsymbol{y}$).

Now, let τ_0 be the fundamental deep hole lying over K for some lattice Λ_τ, $\tau = a + bi \in \mathcal{F}$. Then $\Re(\tau_0) = 1/2$ and (2) implies that

$$t := \Im(\tau_0) = \frac{a^2 + b^2 - a}{2b} \in K, \ b > t.$$

The set of $\tau \in \mathcal{F}$ so that τ_0 is the deep hole for Λ_τ can then be described as

$$(10) \qquad S_{\tau_0} := \left\{a + bi : 0 \leq a \leq \frac{1}{2}, \ b > t, \ \left(a - \frac{1}{2}\right)^2 + (b - t)^2 = \frac{1}{4} + t^2\right\},$$

which is precisely the green arc in Figure 2. Notice that each line $y = sx$ through the origin with slope

$$(11) \qquad s \geq 2t + \sqrt{4t^2 + 1}$$

intersects S_{τ_0} in precisely one point. Conversely, every point on S_{τ_0} is the intersection point with a unique such line. Hence, S_{τ_0} is in bijective correspondence with the set of slopes $[2t + \sqrt{4t^2 + 1}, \infty)$. Further, notice that $\boldsymbol{0}$ is a point on the circle of which S_{τ_0} is an arc. Let K be a number field, and notice the line $y = sx$ through $\boldsymbol{0}$ intersects S_{τ_0} in a point $(a, b) \in K^2$ if and only if $s \in K$. This means that the set S_{K,τ_0} as defined in (3) is given by $\{a + bi \in S_{\tau_0} : a, b \in K\}$, and hence is in bijective correspondence with the set of slopes

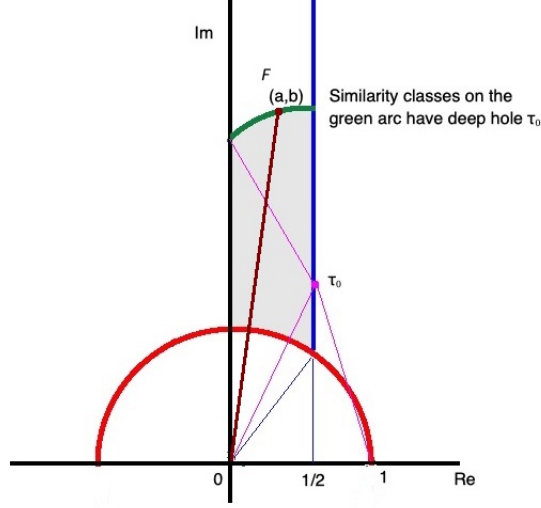$$\mathcal{M}_{K,\tau_0} := \left\{s \in K : s \geq 2t + \sqrt{4t^2 + 1}\right\}.$$

FIGURE 2. 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.

For each $s \in \mathcal{M}_{K,\tau_0}$ there exists a unique $a + bi \in S_{\tau_0}$ such that $s = b/a$, and for each such pair (a,b) there is a primitive point $(\alpha, \beta) \in \mathcal{O}_K^2$ such that $b/a = \beta/\alpha$, i.e. (α, β) is the unique primitive point on the line $y = sx$. Define

$$P_{K,\tau_0} = \left\{ (\alpha, \beta) \in \mathcal{O}_K^2 : (\alpha, \beta) \text{ is primitive}, \beta/\alpha \geq 2t + \sqrt{4t^2 + 1} \right\},$$

then we have a bijective correspondence:

$$\tau = a + bi \in S_{K,\tau_0} \longleftrightarrow (\alpha, \beta) \in P_{K,\tau_0} \text{ such that } \beta/\alpha = b/a.$$

Let us write $\mathcal{H}^p(\tau)$ for the primitive height $\mathcal{H}^p(a,b)$, then for any $T \geq 1$,

$$(12) \qquad |\{\tau \in S_{K,\tau_0} : \mathcal{H}^p(\tau) \leq T\}| = |\{(\alpha, \beta) \in P_{K,\tau_0} : |\Sigma_K(\alpha, \beta)| \leq T\}|,$$

which is finite.

Lemma 4.2. *Let $T \geq 1$ and let*

$$P_{K,\tau_0}(T) = \left\{ (\alpha, \beta) \in P_{K,\tau_0} : |\Sigma_K(\alpha, \beta)| \leq T \right\}.$$

Then, as $T \to \infty$,

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

where ζ stands for the Riemann zeta-function.

Proof. Consider the lattice $\Lambda_K^2 \subset K_{\mathbb{R}}^2$ and write $(\Lambda_K^2)_{\mathrm{pr}}$ for the set of primitive points in Λ_K^2, i.e. points that are not integer multiples of any other points in Λ_K^2. Notice that if $(\alpha, \beta) \in P_{K,\tau_0}$, then $\Sigma_K(\alpha, \beta) \in (\Lambda_K^2)_{\mathrm{pr}}$. Let us write points in $K_{\mathbb{R}}^2$ as $(\boldsymbol{x}_1, \boldsymbol{y}_1, \boldsymbol{x}_2, \boldsymbol{y}_2)$, where $(\boldsymbol{x}_1, \boldsymbol{y}_1), (\boldsymbol{x}_2, \boldsymbol{y}_2) \in K_{\mathbb{R}}$. Write x_{11} and x_{21} for the first coordinates of $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$, respectively, and define

$$C_{K,t}(T) = \left\{ \boldsymbol{z} := (\boldsymbol{x}_1, \boldsymbol{y}_1, \boldsymbol{x}_2, \boldsymbol{y}_2) \in K_{\mathbb{R}}^2 : |\boldsymbol{z}| \leq T, x_{21} \geq \left(2t + \sqrt{4t^2 + 1}\right) x_{11} \geq 0 \right\},$$

then $\Sigma_K(P_{K,\tau_0}(T)) \subseteq C_{K,t}(T) \cap (\Lambda_K^2)_{\mathrm{pr}}$. Write $q := \left(2t + \sqrt{4t^2 + 1}\right)$ and observe that $C_{K,t}(T)$ is a direct product of $2r_2$ circular discs of radius T, given by

$$|y_{jk}| \leq T, \ \forall \ j = 1, 2 \text{ and } k = 1, \ldots, r_2,$$

$2r_1 - 2$ intervals given by

$$|x_{jk}| \leq T, \ \forall \ j = 1, 2 \text{ and } k = 2, \ldots, r_1,$$

and the set $\{(x_{11}, x_{21}) : 0 \leq x_{11} \leq x_{21}/q\}$. Then

$$\mathrm{Vol}_{2n} C_{K,t}(T) = \left(\pi T^2\right)^{2r_2} (2T)^{2r_1 - 2} \left(\frac{T^2}{2q}\right) = \left(\frac{4^{r_1} \pi^{2r_2}}{8q}\right) T^{2n}.$$

Since $C_{K,t}(T) = TC_{K,t}(1)$, Theorem 2 on p.128 of [7] combined with (8) asserts that

$$\left|C_{K,t}(T) \cap \Lambda_K^2\right| \quad \leq \quad \left(\frac{\mathrm{Vol}_{2n} C_{K,t}(1)}{\det \Lambda_K^2}\right) T^{2n} + O(T^{2n-1})$$

(13)
$$= \quad \left(\frac{4^{r_1} \pi^{2r_2}}{8\left(2t + \sqrt{4t^2 + 1}\right)|\Delta_K|}\right) T^{2n} + O(T^{2n-1}),$$

as $T \to \infty$.

Now, let $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{2n}$ be a basis for Λ_K^2, in particular $\Lambda_K^2 = \mathrm{span}_{\mathbb{Z}}\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{2n}\}$. Let $\varphi : \Lambda_K^2 \to \mathbb{Z}^{2n}$ be given by

$$\boldsymbol{y} = \sum_{j=1}^{2n} a_j \boldsymbol{x}_j \mapsto \boldsymbol{a} = (a_1, \ldots, a_{2n})^\top,$$

then $\boldsymbol{y} \in \Lambda_K^2$ is primitive if and only if $\varphi(\boldsymbol{y}) \in \mathbb{Z}^{2n}$ is primitive. Further, φ extends to a linear map $\varphi : K_{\mathbb{R}}^2 \to \mathbb{R}^{2n}$ and the set $\varphi(C_{K,t}(T))$ is a convex polyhedron with $\boldsymbol{0}$ on its boundary. In particular, if a lattice point $\boldsymbol{a} \in \mathbb{Z}^{2n}$ is contained in $\varphi(C_{K,t}(T))$ then there is a corresponding primitive point $\boldsymbol{a}' \in \mathbb{Z}^{2n}$ contained in $\varphi(C_{K,t}(T))$ such that $\boldsymbol{a} = c\boldsymbol{a}'$ for some $c \in \mathbb{Z}$. Hence, if $T' = \max\{|\boldsymbol{a}| : \boldsymbol{a} \in \varphi(C_{K,t}(T))\}$, then for a randomly chosen point in $\varphi(C_{K,t}(T))$ the probability that it is primitive is the same as for a randomly chosen point in $\{\boldsymbol{a} \in \mathbb{Z}^{2n} : |\boldsymbol{a}| \leq T'\}$. By Theorem 1 of [8], this probability tends to $1/\zeta(2n)$ as $T' \to \infty$. Since $T' \to \infty$ as $T \to \infty$, this implies that the proportion of primitive points among all lattice points in $C_{K,t}(T) \cap \Lambda_K^2$ tends to $1/\zeta(2n)$ as $T \to \infty$. Combining this observation with (13) completes the proof of the lemma. $\qquad\square$

Proof of Theorem 1.4. The theorem follows by combining (12) with Lemma 4.2. $\quad\square$

References

[1] E. Bayer Fluckiger. Upper bounds for Euclidean minima of algebraic number fields. *J. Number Theory*, 121 (2006), no. 2, pp. 305–323.

[2] B. Casselman. Stability of lattices and the partition of arithmetic quotients. *Asian J. Math.*, vol. 8 (2004) no. 4, pp. 607–637.

[3] M. Forst and L. Fukshansky. On lattice extensions. *Monatsh. Math.*, to appear (2024).

[4] L. Fukshansky. Stability of ideal lattices from quadratic number fields. *Ramanujan J.*, vol. 37 (2015) no. 2, pp. 243–256.

[5] L. Fukshansky, P. Guerzhoy and F. Luca. On arithmetic lattices in the plane. *Proc. Amer. Math. Soc.*, vol. 145 (2017) no. 4, pp. 1453–1465.

[6] L. Fukshansky, D. Kogan. Cyclic and well-rounded lattices. *Mosc. J. Comb. Number Theory*, vol. 11 (2022) no. 1, pp. 79–96.

[7] S. Lang. Algebraic Number Theory. Springer-Verlag, 1986.

[8] J. E. Nymann. On the probability that k positive integers are relatively Prime. *J. Number Theory*, vol. 4 (1972), pp. 469–473.

[9] J. Silverman. The Arithmetic of Elliptic Curves. *Second edition. Graduate Texts in Mathematics, 106*, Springer, Dordrecht, 2009.

[10] J. Thunder. An asymptotic estimate for heights of algebraic subspaces. *Trans. Amer. Math. Soc.*, vol. 331 (1992) no. 1, pp. 395–424.

Department of Mathematics, Claremont McKenna College, 850 Columbia Avenue, Claremont, CA 91711

Email address: `lenny@cmc.edu`

Department of Mathematics, University of Hawaii, 2565 McCarthy Mall, Honolulu, HI, 96822-2273

Email address: `pavel@math.hawaii.edu`

Department of Mathematics, Harvey Mudd College, 320 E. Foothill Blvd., Claremont CA 91711

Email address: `tnielsen@g.hmc.edu`