Rosen and Shnidman *Res. Number Theory*☒
DOI 10.1007/s40993-017-0073-y

Research in Number Theory

RESEARCH

Open Access

Extensions of CM elliptic curves and orbit counting on the projective line

Julian Rosen[1] and Ariel Shnidman[2*]

[*]Correspondence:
shnidman@bc.edu
[2]Department of Mathematics, Boston College, Chestnut Hill, MA 02647, USA
Full list of author information is available at the end of the article

Abstract

There are several formulas for the number of orbits of the projective line under the action of subgroups of GL_2. We give an interpretation of two such formulas in terms of the geometry of elliptic curves, and prove a more general formula for a large class of congruence subgroups of Bianchi groups. Our formula involves the number of walks on a certain graph called an isogeny volcano. Underlying our results is a complete description of the group of extensions of a pair of CM elliptic curves, as well as the group of extensions of a pair of lattices in a quadratic field.

Keywords: Kleinian groups, Elliptic curves, Complex multiplication

1 Introduction

We begin with some motivation from two well-known and elegant formulas. The first formula is for the number of orbits of $\mathbb{P}^1(\mathbb{Q})$ under the action of the congruence subgroup $\Gamma_0(N) \subset \mathrm{GL}_2(\mathbb{Z})$,[1] acting by fractional-linear transformation [3, §II.1]:

$$\#\Gamma_0(N)\backslash\mathbb{P}^1(\mathbb{Q}) = \sum_{d|N} \phi_u\left(\gcd(d, N/d)\right). \tag{1.1}$$

Here ϕ_u is the *reduced totient function*

$$\phi_u(n) = \#\left(\frac{(\mathbb{Z}/n\mathbb{Z})^\times}{\{\pm 1\}}\right) = \begin{cases} \frac{\phi(n)}{2} & \text{if } n \geq 3, \\ 1 & \text{if } n = 1, 2. \end{cases}$$

If we replace ϕ_u by ϕ, then the right hand side of (1.1) also counts the number of cusps on the modular curve $X_0(N)$.

The second formula is for the number of orbits of $\mathbb{P}^1(K)$ under the action of $\mathrm{GL}_2(\mathcal{O}_K)$, where K is a number field and $\mathcal{O}_K$ is its ring of integers:

$$\#\mathrm{GL}_2(\mathcal{O}_K)\backslash\mathbb{P}^1(K) = h. \tag{1.2}$$

Here, $h = h(K)$ is the size of the class group $\mathrm{Pic}(\mathcal{O}_K)$. When K is an imaginary quadratic field, (1.2) counts the number of cusps on the corresponding Bianchi orbifold and is due to Bianchi himself. A formula counting the number of orbits of $\mathbb{P}^1(K)$ under the action of congruence subgroups analogous to $\Gamma_0(N)$ is given in [2].

[1] Our definition of $\Gamma_0(N)$ is not the traditional one, as we allow elements of determinant -1.

Springer Open

We can connect these two formulas using the theory of elliptic curves. For this, we let E and E' be elliptic curves over $\mathbb{C}$, and we consider the number $N(E, E')$ of elliptic curves on the abelian surface $A = E \times E'$ up to the action of $\mathrm{Aut}(A)$. This number is finite by [5], and in fact $N(E, E') = 2$ unless there exists an isogeny $\lambda \colon E \to E'$. This raises the question: how do we compute $N(E, E')$ if E and E' are isogenous?

If $\mathrm{End}(E) = \mathbb{Z}$, then $\mathrm{Hom}(E, E') = \mathbb{Z}\lambda$, for a certain minimal isogeny λ, whose degree we will denote by N. Then $\mathrm{Aut}(A) \simeq \Gamma_0(N)$ and we have $N(E, E') = \#\Gamma_0(N)\backslash\mathbb{P}^1(\mathbb{Q})$ [9, Prop. 3.7]. So the number $N(E, E')$ is given by (1.1). On the other hand, if E has complex multiplication (CM) by an imaginary quadratic field K, we may think of $\mathrm{Aut}(A)$ as a subgroup of $\mathrm{GL}_2(K)$. As before, we have $N(E, E') = \#\mathrm{Aut}(A)\backslash\mathbb{P}^1(K)$; see Lemma 3.1. In the special case where $E = E'$ and $\mathrm{End}(E) = \mathcal{O}_K$, we have $\mathrm{Aut}(A) \simeq \mathrm{GL}_2(\mathcal{O}_K)$ and Bianchi's formula (1.2) gives $N(E, E) = h$.

Our main result is a formula for $N(E, E')$ for any two elliptic curves E, E' with CM by K. Equivalently, we compute $\#\mathrm{Aut}(M)\backslash\mathbb{P}^1(K)$ for any lattice $M \subset K^2$. To state the result, we follow Kani [4] and define the *e-conductor* of an elliptic curve E with CM by K to be the index $[\mathcal{O}_K \colon \mathrm{End}(E)]$. Thus, if E has e-conductor c, then $\mathrm{End}(E)$ is isomorphic to $\mathcal{O}_c$, the unique subring of index c inside $\mathcal{O}_K$. Concretely, if $E \simeq \mathbb{C}/\mathfrak{a}$, for some lattice $\mathfrak{a}$ in K, then c is the index of the ring of multipliers $\{\alpha \in K \colon \alpha\mathfrak{a} \subset \mathfrak{a}\}$ in $\mathcal{O}_K$.

Theorem 1.1 *Let K be an imaginary quadratic field whose only roots of unity are ± 1.*[2] *Suppose E and E' are elliptic curves with complex multiplication by K and with e-conductors c and c', respectively. Define $f = \mathrm{lcm}(c, c')$ and $f' = \gcd(c, c')$. Then*

$$N(E, E') = \sum_{d \mid f} h_d \cdot \phi_u(f/d) \sum_{k \mid d} 2^{\omega(d/k)} r_K\left(f', k, f/d\right).$$

Here,

- $h_d = \#\mathrm{Pic}(\mathcal{O}_d) = \#\mathrm{Pic}(\mathcal{O}_K) \cdot d \prod_{p \mid d} (1 - \chi_K(p)/p)$,
- *χ_K is the quadratic Dirichlet character associated to K,*
- *$\omega(n)$ is the number of distinct prime factors of n, and*
- *$r_K(a, b, N)$ is the number of cyclic subgroups of order N of a fixed elliptic curve of e-conductor a such that the quotient has e-conductor b.*

The mysterious quantity in our formula is the function $r_K(a, b, N)$. This is a 3-variable multiplicative function which is made completely explicit in Corollary 4.3. For each prime p, the values of r_K on powers of p depend only on how p splits in K, so the number $N(E, E')$ depends only on the two integers c and c' and the values of χ_K on primes dividing cc'. The explicit formulas for $r_K(a, b, N)$ are derived by interpreting these numbers as counting certain walks on graphs called *p-isogeny volcanoes*. The structure of the p-isogeny volcano then allows one to compute $r_K(a, b, N)$ simply by looking at the graph (see Theorem 4.2). We also provide a Sage script for computing the numbers $N(E, E')$ [10].

As a corollary of Theorem 1.1, we obtain orbit counting formulas for a large class of subgroups of $\mathrm{GL}_2(K)$ which are commensurable with the Bianchi group $\mathrm{GL}_2(\mathcal{O}_K)$.

[2] There are analogous formulas for the two imaginary quadratic fields with more roots of unity, but we omit these cases for simplicity.

Explicitly, if $E = \mathbb{C}/\mathfrak{a}$ and $E' = \mathbb{C}/\mathfrak{a}'$, for lattices $\mathfrak{a}$ and $\mathfrak{a}'$ in K, then $\mathrm{Aut}(E \times E')$ is isomorphic to the group:

$$\Gamma(\mathfrak{a}, \mathfrak{a}') := \left\{ \gamma \in \begin{pmatrix} \mathcal{O}_c & c\mathfrak{a}(f'\mathfrak{a}')^{-1} \\ c'\mathfrak{a}'(f'\mathfrak{a})^{-1} & \mathcal{O}_{c'} \end{pmatrix} : \det\gamma = \pm 1 \right\}.$$

We then have the following orbit counting formula:

Corollary 1.2

$$\#\Gamma(\mathfrak{a}, \mathfrak{a}')\backslash\mathbb{P}^1(K) = \sum_{d|f} h_d \cdot \phi_u(f/d) \sum_{k|d} 2^{\omega(d/k)} r_K\left(f', k, f/d\right).$$

In favorable cases, the formula in Corollary 1.2 simplifies. For example, if $\mathfrak{a} = \mathfrak{a}' = \mathcal{O}_f$ for some $f \geq 1$, then $\Gamma(\mathfrak{a}, \mathfrak{a}') = \mathrm{GL}_2(\mathcal{O}_f)$ and the right hand side becomes a simple Dirichlet convolution:

Corollary 1.3 *For any $f \geq 1$,*

$$\#\mathrm{GL}_2(\mathcal{O}_f)\backslash\mathbb{P}^1(K) = \sum_{d|f} h_d \cdot \phi_u(f/d).$$

Proof See Sect. 4. □

These results have application to other counting problems in geometry. For example, $\#\Gamma(\mathfrak{a}, \mathfrak{a}')\backslash\mathbb{P}^1(K)$ is the number of cusps on the hyperbolic 3-manifold $\Gamma(\mathfrak{a}, \mathfrak{a}')\backslash\mathbb{H}^3$. It is also the number of equivalence classes of contractions of the abelian surface $A = E \times E'$, in the sense of the minimal model program. Our formula can be used to study the asymptotics of these quantities as A varies, and should be helpful in individual computations as well.

The proof of Theorem 1.1 involves a careful study of Ext-groups in the category of products of elliptic curves with complex multiplication by K, or equivalently, in the category of lattices in imaginary quadratic fields. These results, found in Sect. 2, are interesting in their own right and should find other applications.

2 Extensions of CM elliptic curves

Fix an imaginary quadratic number field $K \subset \mathbb{C}$. A *K-lattice of rank n* is a free abelian subgroup $L \subset K^n$ of rank $2n$. The quotient $\mathbb{C}^n/L$ is a complex torus, which is known to be algebraic.

2.1 Singular abelian surfaces

For context, we recall a basic fact about the abelian surfaces we are considering.

Proposition 2.1 [6] *Let A be a complex be an abelian surface over $\mathbb{C}$. Then the following are equivalent:*

1. *$A \simeq \mathbb{C}^2/\Lambda$, with Λ a K-lattice of rank 2.*
2. *A is isomorphic to a product of two elliptic curves, both having CM by K.*
3. *A is isogenous to a product of two elliptic curves, both having CM by K.*

If these equivalent conditions hold, we say that A is *singular* and that A has *CM by K*.

2.2 Rank 1 K-lattices

Recall that an *order* in K is a subring $R \subset \mathcal{O}_K$ such that $\mathrm{Frac}(R) = K$. Every order has the form $R = \mathbb{Z} + f\mathcal{O}_K$ for a unique positive integer f, called the *conductor* of R. For each lattice $L \subset K^n$, the *ring of multipliers* $R(L)$ is the order $\{\alpha \in K : \alpha L \subset L\}$. The conductor of L is defined to be the conductor of $R(L)$.

If $\mathfrak{a}$ is a rank 1 K-lattice, then $\mathfrak{a}$ is projective as an $R(\mathfrak{a})$-module. Two rank 1 K-lattices $\mathfrak{a}$ and $\mathfrak{a}'$ are *homothetic* if $\mathfrak{a} = \gamma\mathfrak{a}'$ for some $\gamma \in K^\times$. The set of homothety classes of lattices of conductor f forms a group under multiplication of lattices, which is denoted $\mathrm{Pic}(\mathcal{O}_f)$. The set of homothety classes of lattices in K is therefore in bijection with $\coprod_{f\geq 1} \mathrm{Pic}(\mathcal{O}_f)$. If $E = \mathbb{C}/\mathfrak{a}$, then we define the e-conductor of E to be the conductor of $\mathfrak{a}$.

Proposition 2.2 *Let A be a singular abelian surface with CM by K. Then there is a positive integer f and a lattice $\mathfrak{a} \subset K$ of conductor f' dividing f such that*

$$A \cong \mathbb{C}/\mathcal{O}_f \oplus \mathbb{C}/\mathfrak{a}.$$

Moreover, the integers f, f' and the class $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}_{f'})$ are uniquely determined by these conditions. In particular,

$$A \mapsto (f/f', [\mathfrak{a}])$$

is a bijection between the set of isomorphism classes of singular abelian surfaces with CM by K and pairs $(g, [\mathfrak{a}])$, where $g \geq 1$ and $[\mathfrak{a}]$ is a homothety class of lattices in K.

Proof Since A is singular with CM by K, we may write $A = E \times E'$ with $E = \mathbb{C}/\mathfrak{a}$ and $E' = \mathbb{C}/\mathfrak{a}'$ for rank 1 K-lattices $\mathfrak{a}$ and $\mathfrak{a}'$. Let c and c' be the e-conductors of these elliptic curves. Then $E \times E' \simeq \mathbb{C}/\mathcal{O}_f \times \mathbb{C}/\mathfrak{a}\mathfrak{a}'$, where $f = \mathrm{lcm}(c_1, c_2)$. Moreover, if two lattices $\mathfrak{a}, \mathfrak{b} \subset K$ have multiplication by $\mathcal{O}_f$, then $\mathbb{C}^2/(\mathcal{O}_f \oplus \mathfrak{a}) \simeq \mathbb{C}^2/(\mathcal{O}_f \oplus \mathfrak{b})$ if and only if $\mathfrak{a}$ and $\mathfrak{b}$ are homothetic (see [6] or [4]). □

2.3 Extensions of rank 1 lattices

Let $L_1, L_2 \subset K$ be K-lattices of conductors f_1 and f_2, and let $E_i = \mathbb{C}/L_i$ (for $i = 1, 2$) be the corresponding elliptic curves. Suppose also that $L_1 = \mathbb{Z} + \mathbb{Z}\tau_1$ and $L_2 = \mathbb{Z} + \mathbb{Z}\tau_2$ for elements τ_1 and τ_2 of K; up to homothety, we may always choose such a basis.

We wish to classify the *extensions* of E_1 by E_2, i.e. the short exact sequences

$$0 \to E_2 \to S \to E_1 \to 0,$$

where S is a complex torus. Another extension

$$0 \to E_2 \to S' \to E_1 \to 0,$$

is said to be equivalent to the first if there is an isomorphism $S \to S'$ which induces the identity on E_2 and E_1. There is a natural group operation on the set of equivalences classes of extensions, and this group is denoted $\mathrm{Ext}^1_{\mathrm{an}}(E_1, E_2)$. The subgroup of extensions with S an abelian surface, i.e. an algebraic complex torus, is denoted $\mathrm{Ext}^1_{\mathrm{alg}}(E_1, E_2)$. We refer to [1, §I] for more details regarding extensions of complex tori.

The following result shows that the extensions of E_1 by E_2 are controlled by a third elliptic curve $\tilde{E} := \mathbb{C}/L_1L_2$.

Proposition 2.3 [1, I.5.7 and I.6.2] *The association*

$$z \longmapsto \frac{\mathbb{C}^2}{\begin{pmatrix} \tau_2 & 1 & z & 0 \\ 0 & 0 & \tau_1 & 1 \end{pmatrix}}$$

induces an isomorphism between the group $\tilde{E} = \mathbb{C}/L_1L_2$ *and the group* $\mathrm{Ext}^1_{\mathrm{an}}(E_1, E_2)$*. Under this bijection, the torsion points in* $\tilde{E}$ *corresponds to the subgroup* $\mathrm{Ext}^1_{\mathrm{alg}}(E_1, E_2)$ *of algebraic extensions.*

Remark There is a similar result in [8, Thm. 6.1], attributed to Lichtenbaum, but the result is not stated correctly there.

Proposition 2.3 shows that $\mathrm{Ext}^1_{\mathrm{alg}}(E_1, E_2) \simeq (\mathbb{Q}/\mathbb{Z})^2$ as a group. But it is not clear which (or how many) extension classes correspond to some fixed abelian surface S. The following theorem gives this extra information.

Theorem 2.4 *Let* $P \in \tilde{E}$ *be a torsion point of order n, and let*

$$0 \to E_2 \to S \to E_1 \to 0$$

be the corresponding extension given by Proposition 2.3. Then

$$S \simeq \mathbb{C}/\mathcal{O}_{nf} \times \tilde{E}/\langle P\rangle,$$

where $f = \mathrm{lcm}(f_1, f_2)$*.*

In the proof, we consider several different notions of extension.

- For any integer c divisible by f, the lattices L_1 and L_2 can be considered as $\mathcal{O}_c$-modules, and we have the group $\mathrm{Ext}^1_{\mathcal{O}_c}(L_1, L_2)$ of extensions of $\mathcal{O}_c$-modules;
- The group $\mathrm{Ext}^1(L_1, L_2)$ of extensions of K-lattices;
- The group $\mathrm{Ext}^1_{\mathrm{alg}}(\mathbb{C}/L_1, \mathbb{C}/L_2)$ of extensions of abelian varieties;
- The group $\mathrm{Ext}^1_{\mathrm{an}}(\mathbb{C}/L_1, \mathbb{C}/L_2)$ of extensions of complex tori.

An extension of modules determines an extension of K-lattices, which determines an extension of abelian varieties, which determines an extension of complex tori, so there is a sequence of group homomorphisms

$$\begin{aligned} \mathrm{Ext}^1_{\mathcal{O}_c}(L_1, L_2) &\xrightarrow{\gamma_1} \mathrm{Ext}^1(L_1, L_2) \xrightarrow{\gamma_2} \mathrm{Ext}^1_{\mathrm{alg}}(\mathbb{C}/L_1, \mathbb{C}/L_2) \\ &\xrightarrow{\gamma_3} \mathrm{Ext}^1_{\mathrm{an}}(\mathbb{C}/L_1, \mathbb{C}/L_2). \end{aligned} \tag{2.1}$$

It is not hard to see that γ_1, γ_2, and γ_3 are injective. Moreover, γ_2 is an isomorphism, as there is an equivalence of categories between the category of K-lattices and the category of abelian varieties isogenous to a product of elliptic curves with CM by K. The latter equivalence of categories can be deduced from the main results of [4] or [7]. Finally, Proposition 2.3 implies the image of γ_3 is the torsion subgroup of $\mathrm{Ext}^1_{\mathrm{an}}(\mathbb{C}/L_1, \mathbb{C}/L_2)$.

Proposition 2.5 *For any c divisible by* $f = \mathrm{lcm}(f_1, f_2)$*, there is an isomorphism of* $\mathcal{O}_c$*-modules*

$$\mathrm{Ext}^1_{\mathcal{O}_c}(L_1, L_2) \cong \frac{\mathrm{Hom}_{\mathcal{O}_c}(L_1, L_2)}{\frac{c}{f}\mathrm{Hom}_{\mathcal{O}_c}(L_1, L_2)}.$$

Proof Choose an algebraic integer ω with $\mathcal{O}_K = \mathbb{Z} + \omega\mathbb{Z}$; then $\mathcal{O}_c = \mathbb{Z} + c\omega\mathbb{Z}$. Tensoring with $\mathcal{O}_{f_1}$ induces a surjection $\mathrm{Pic}(\mathcal{O}_c) \to \mathrm{Pic}(\mathcal{O}_{f_1})$, so we can find a sublattice $\widetilde{L}_1 \subset L_1$ with ring of multipliers $\mathcal{O}_c$ such that $\mathcal{O}_{f_1} \cdot \widetilde{L}_1 = L_1$. Consider the following resolution of L_1 by projective $\mathcal{O}_c$-modules:

$$0 \longleftarrow L_1 \xleftarrow{\varphi_0} \widetilde{L}_1^2 \xleftarrow{\varphi_1} \widetilde{L}_1^2 \xleftarrow{\varphi_2} \dots,$$

with

$$\varphi_0 = [1, -k\omega] \quad \text{and} \quad \varphi_1 = \varphi_2 = \dots = \begin{bmatrix} c\omega & -f_1 c\omega^2 \\ \frac{c}{f_1} & -c\omega \end{bmatrix}.$$

We apply the functor $\mathrm{Hom}(-, L_2)$ and examine the first coordinate to obtain

$$\begin{aligned} \mathrm{Ext}^1_{\mathcal{O}_c}(L_1, L_2) &= \frac{\left\{\alpha \in \mathrm{Hom}_{\mathcal{O}_c}(\widetilde{L}_1, L_2) : \mathcal{O}_{f_1}\alpha \subset \mathrm{Hom}_f(\widetilde{L}_1, L_2)\right\}}{\left\{\frac{c}{f_1}\mathcal{O}_{f_1} \cdot \mathrm{Hom}_{\mathcal{O}_c}(\widetilde{L}_1, L_2)\right\}} \\ &= \frac{\mathrm{Hom}_{\mathcal{O}_c}(L_1, L_2)}{\frac{c}{f}\mathrm{Hom}_{\mathcal{O}_c}(L_1, L_2)}, \end{aligned}$$

where the second line follows from [4, Lem. 15]. □

Remark Proposition 2.5 holds if K is a *real* quadratic field as well.

Corollary 2.6 *The map* γ_1 *of* (2.1) *takes* $\mathrm{Ext}^1_{\mathcal{O}_c}(L_1, L_2)$ *isomorphically onto the* (c/f)*-torsion in* $\mathrm{Ext}^1(L_1, L_2)$.

Proof Note that as an abelian group, $\mathrm{Hom}_{\mathcal{O}_c}(L_1, L_2)$ is free of rank 2. Hence, by Proposition 2.5, $\mathrm{Ext}^1_{\mathcal{O}_c}(L_1, L_2)$ is an (c/f)-torsion group of size $(c/f)^2$ and γ_1 maps into the (c/f)-torsion in $\mathrm{Ext}^1(L_1, L_2)$. Proposition 2.3 implies that the (c/f)-torsion in $\mathrm{Ext}^1_{\mathrm{alg}}(\mathbb{C}/L_1, \mathbb{C}/L_2)$ has cardinality $(c/f)^2$, hence the (c/f)-torsion in $\mathrm{Ext}^1(L_1, L_2)$ also has cardinality $(c/f)^2$ because γ_2 is an isomorphism. As γ_1 induces an injective map between two sets of the same cardinality, it must be an isomorphism onto the (c/f)-torsion of $\mathrm{Ext}^1(L_1, L_2)$. □

Lemma 2.7 *Suppose*

$$0 \to L_2 \to L \to L_1 \to 0$$

is an extension of K*-lattices, where* L_i *has conductor* f_i *(for* $i = 1, 2$*). If the corresponding element of* $\mathrm{Ext}^1(L_1, L_2)$ *has order* n*, then* L *has conductor* nf.

Proof The conductor of L is the minimal c such that the class in $\mathrm{Ext}^1(L_1, L_2)$ representing L is in the image of $\mathrm{Ext}^1_{\mathcal{O}_c}(L_1, L_2)$. Corollary 2.6 implies that this value is nf. □

Proof of Theorem 2.4 By Proposition 2.2, the abelian surface S is isomorphic to $\mathbb{C}/\mathcal{O}_N \times \mathbb{C}/\mathfrak{a}$ for some integer N and some lattice $\mathfrak{a} \subset K$ with $\mathcal{O}_N \subset R(\mathfrak{a})$. Since the conductor of $\mathcal{O}_N \oplus \mathfrak{a}$ is N, we must have $N = nf$ by the previous lemma. Thus, it remains to show that $\mathbb{C}/\mathfrak{a} \simeq \tilde{E}/\langle P \rangle$. We do this by computing the exterior power of the lattice corresponding to S in two different ways.

On the one hand, we can recover $\mathfrak{a}$ as the quotient of the group

$$\bigwedge\nolimits^2_{\mathcal{O}_N}(\mathcal{O}_N \oplus \mathfrak{a}) \cong \bigwedge\nolimits^2_{\mathcal{O}_N} \mathfrak{a} \oplus \bigwedge\nolimits^2_{\mathcal{O}_N} \mathcal{O}_N \oplus (\mathcal{O}_N \otimes_{\mathcal{O}_N} \mathfrak{a}) \cong \left(\bigwedge\nolimits^2_{\mathcal{O}_N} \mathfrak{a}\right) \oplus \mathfrak{a}$$

modulo its torsion. On the other hand, we have $S \simeq \mathbb{C}^2/L$, where L is the $\mathbb{Z}$-span of the period matrix in Proposition 2.3, with $z \in \mathbb{C}$ any lift of the order n torsion point $P \in \tilde{E} = \mathbb{C}/L_1L_2$. The torsion-free part of $\bigwedge^2_{\mathcal{O}_N} L$ is spanned by the 2×2-minors of the period matrix. Thus, $\mathfrak{a}$ is the lattice in K generated by these minors, i.e. the lattice generated by L_1L_2 and the element z. This is precisely the lattice corresponding to the elliptic curve $\tilde{E}/\langle P\rangle$. □

3 Proof of Theorem 1.1 and Corollary 1.2

Let $A = E \times E'$ be a product of two elliptic curves with CM by the same imaginary quadratic field K. Then we may think of $\mathrm{Aut}(A)$ as a subgroup of $\mathrm{GL}_2(K)$. Explicitly, choose an isogeny $\lambda \colon E \to E'$, and identify $\mathrm{Hom}(E, A) \otimes_{\mathbb{Z}} \mathbb{Q}$ with K^2 via the basis $(1, 0)$ and $(0, \lambda)$. Then $\mathrm{Aut}(A)$ acts faithfully on this 2-dimensional K-vector space by post-composition. On the other hand, $\mathrm{GL}_2(K)$ acts on $\mathbb{P}^1(K)$ by fractional linear transformation.

Lemma 3.1 *The orbits of* $\mathbb{P}^1(K)$ *under the action of* $\mathrm{Aut}(A) \subset \mathrm{GL}_2(K)$ *are in bijection with the* $\mathrm{Aut}(A)$*-orbits of elliptic curves contained in* A*.*

Proof Every elliptic curve on $A = E \times E'$ is isogenous to E, so is the image of some non-zero map $E \to A$. Two maps $a, b : E \to A$ have the same image if and only if there are non-zero $x, y \in \mathrm{End}(E)$ with $ax = by$. In other words, a and b have the same image if and only if they determine the same class in the K-projectivization $\mathbb{P}_K(\mathrm{Hom}(E, A) \otimes_{\mathbb{Z}} \mathbb{Q}) = \mathbb{P}^1(K)$. So we have constructed an injective map from the set of elliptic curves on A to $\mathbb{P}^1(K)$, which is also surjective since every non-zero element of $\mathrm{Hom}(E, A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a K-multiple of an element of $\mathrm{Hom}(E, A)$. This bijection is evidently compatible with the pushforward action of $\mathrm{Aut}(A)$ on elliptic curves and the action of $\mathrm{Aut}(A)$ on $\mathbb{P}^1(K)$ defined above, so the lemma follows. □

Corollary 1.2 follows from Lemma 3.1 and Theorem 1.1, so we focus for the rest of this section on the proof of Theorem 1.1. In other words, we will count the number $N(E, E')$ of $\mathrm{Aut}(A)$-equivalence classes of elliptic curves on the abelian surface $A = E \times E'$. By Proposition 2.2, we may assume $E = \mathbb{C}/\mathcal{O}_f$ and $E' = \mathbb{C}/\mathfrak{a}$, where $\mathfrak{a}$ has conductor f' dividing f. If $E_0 \subset A$ is an elliptic curve contained in A, then both E_0 and the quotient A/E_0 are elliptic curves with CM by K, and one has a short exact sequence of abelian varieties:

$$0 \to E_0 \to A \to A/E_0 \to 0. \tag{3.1}$$

If $E_1 \subset A$ is another elliptic curve with corresponding sequence

$$0 \to E_1 \to A \to A/E_1 \to 0, \tag{3.2}$$

then $E_0 \subset A$ and $E_1 \subset A$ are $\mathrm{Aut}(A)$-equivalent if and only if (3.1) and (3.2) are isomorphic as short exact sequences.

Lemma 3.2 *If* $E_1 \subset A$ *is an elliptic curve, then the e-conductor of* E_1 *divides* f*.*

Proof Choose a map $\iota : E \to A$ such that $E_1 = \iota(E)$. Write $\iota = (\iota_1, \iota_2)$ for maps $\iota_1 : E \to E$ and $\iota_2 : E \to \mathbb{C}/\mathfrak{a}$. Since $\mathcal{O}_f$ acts on both E and $\mathbb{C}/\mathfrak{a}$, we have $\ker \iota_1 = E[I_1]$ and

$\ker \iota_2 = E[I_2]$ for certain ideals I_1 and I_2 of $\mathcal{O}_f$, by a result of Kani [4, Thm. 20(b)]. Here, $E[I]$ is the subgroup of points that lie in the kernel of $\alpha : E \to E$, for every $\alpha \in I$. Thus,

$$\ker \iota = \ker \iota_1 \cap \ker \iota_2 = E[I_1] \cap E[I_2] = E[I_1 + I_2].$$

It follows that $E_1 \simeq E/\ker \iota \simeq E/E[I_1 + I_2]$, and so E_1 has complex multiplication by $\mathcal{O}_f$. □

Proposition 3.3 *$N(E, E')$ is equal to the number of isomorphism classes of short exact sequences*

$$0 \to E_1 \to A \to E_2 \to 0,$$

with E_1 and E_2 elliptic curves of e-conductor dividing f.

Proof The previous lemma shows that any elliptic curve $E_1 \subset A$ has e-conductor dividing f. Dualizing, we see that $E_2 = A/E_1$ is also an elliptic curve in $\hat{A} \simeq A$, so has e-conductor dividing f as well. □

We continue the proof of Theorem 1.1. Suppose that E_1 and E_2 are elliptic curves with e-conductor dividing f. Observe that if $\gamma_1, \gamma_2 \in \mathrm{Ext}^1(E_2, E_1)$ correspond to extensions

$$0 \to E_1 \to A_1 \to E_2 \to 0, \tag{3.3}$$

$$0 \to E_1 \to A_2 \to E_2 \to 0, \tag{3.4}$$

then (3.3) and (3.4) are isomorphic as short exact sequences if and only if γ_1 and γ_2 are in the same orbit of $\mathrm{Aut}(E_1) \times \mathrm{Aut}(E_2)$ on $\mathrm{Ext}^1(E_2, E_1)$. By assumption, K contains no non-trivial roots of unity, so $\mathrm{Aut}(E_1) = \mathrm{Aut}(E_2) = \{\pm 1\}$. Combining this observation with Proposition 3.3, we obtain

$$N(E, E') = \#\mathrm{Aut}(A)\,\mathbb{P}^1(K) = \sum_{f_1, f_2 | f} \sum_{\substack{[L_1] \in \mathrm{Pic}(\mathcal{O}_{f_1}) \\ [L_2] \in \mathrm{Pic}(\mathcal{O}_{f_2})}} \#\mathrm{Ext}^1_{\mathcal{O}_f}(L_2, L_1)_A / \{\pm 1\},$$

where $\mathrm{Ext}^1_{\mathcal{O}_f}(L_2, L_1)_A$ is the set of extensions classes $0 \to L_1 \to L \to L_2 \to 0$ in $\mathrm{Ext}^1_{\mathcal{O}_f}(L_2, L_1)$ such that $A \simeq \mathbb{C}^2/L$.

Now fix integers f_1 and f_2 dividing f, and set $k = \gcd(f_1, f_2)$, $d = \mathrm{lcm}(f_1, f_2)$. Recall that an isogeny of elliptic curves is *cyclic* if its kernel is a cyclic group. We call a cyclic isogeny *based* if the kernel is equipped with a distinguished generator. By Theorem 2.4, classes in $\mathrm{Ext}^1_{\mathcal{O}_f}(L_2, L_1)_A$ correspond to based cyclic isogenies $\mathbb{C}/L_1L_2 \to \mathbb{C}/\mathfrak{a}$ of degree f/d. Dualizing, we find that these are equinumerous to based cyclic (f/d)-isogenies $\mathbb{C}/\mathfrak{a} \to \mathbb{C}/L_1L_2$.

Recall that $r_K(a, b, N)$ is the number of cyclic subgroups of order N of a fixed elliptic curve of e-conductor a such that the quotient has e-conductor b. Thus, there are $r_K(f', k, f/d)$ cyclic subgroups $G \subset \mathbb{C}/\mathfrak{a}$ of order f/d such that the quotient has e-conductor k. For each such subgroup, there are $h_{f_1}h_{f_2}/h_k = h_d$ pairs $[L_1] \in \mathrm{Pic}(\mathcal{O}_{f_1})$, $[L_2] \in \mathrm{Pic}(\mathcal{O}_{f_2})$ with $(\mathbb{C}/\mathfrak{a})/G \cong \mathbb{C}/L_1L_2$. Given such G, L_1, and L_2, there are $\phi_u(f/d)$ based cyclic (f/d)-isogenies $\mathbb{C}/\mathfrak{a} \to \mathbb{C}/L_1L_2$ with kernel G, up to the action of $\{\pm 1\}$. So we conclude that

$$
\begin{aligned}
\#\mathrm{Aut}(A)\backslash\mathbb{P}^1(K) &= \sum_{\substack{f_1,f_2\,|f\\ k:=\gcd(f_1,f_2)\\ d:=\mathrm{lcm}(f_1,f_2)}} h_d\cdot\phi_u\left(f/d\right)\cdot r_K\left(f',k,f/d\right)\\
&= \sum_{k\,|\,d\,|f} 2^{\omega(d/k)}\cdot h_d\cdot\phi_u\left(f/d\right)\cdot r_K\left(f',k,f/d\right),
\end{aligned}
$$

completing the proof of Theorem 1.1.

4 Computation of $r_K(a,b,c)$

To make Theorem 1.1 explicit, we need to compute the number $r_K(a,b,c)$ of cyclic subgroups C of order c of a fixed CM elliptic curve E of e-conductor a such that E/C has e-conductor b. We will see that this does not depend on the choice of the elliptic curve E of e-conductor a. First we reduce to the case where a, b, and c are powers of a prime p:

Lemma 4.1 *The function $r_K(a,b,c)$ is multiplicative: if we factor a, b, and c into prime powers $a=\prod_p p^{a_p}$, $b=\prod_p p^{b_p}$, and $c=\prod_p p^{c_p}$, then*

$$
r_K(a,b,c)=\prod_p r_K\left(p^{a_p},p^{b_p},p^{c_p}\right).
$$

Proof If E is an elliptic curve, then giving a cyclic subgroup of order c is the same as giving a cyclic subgroup of order p^{c_p} for every prime p. Furthermore, if $E\to E'$ is an isogeny of CM elliptic curves of p-power degree, the ratio of the e-conductors of E and E' is a power of p. To see this, it suffices to show that if $\mathfrak{a}\subset\mathfrak{b}$ is an inclusion of rank 1 K-lattices of index p^a, then the conductors of $\mathfrak{a}$ and $\mathfrak{b}$ are off by a power of p. And indeed, if ℓ is any prime, then the ℓ-part of the conductor of a lattice can be computed locally at ℓ. In particular, if $\ell\neq p$, then $\mathfrak{a}\hookrightarrow\mathfrak{b}$ induces an isomorphism $\mathfrak{a}\otimes\mathbb{Z}_\ell\simeq\mathfrak{b}\otimes\mathbb{Z}_\ell$. It follows then that

$$
r_K(a,b,c)=\prod_p r_K\left(a,p^{b_p}\prod_{\ell\neq p}\ell^{a_\ell},p^{c_p}\right).
$$

To prove the lemma it now suffices to show that

$$
r_K\left(a,p^{b_p}\prod_{\ell\neq p}\ell^{a_\ell},p^{c_p}\right)=r_K(p^{a_p},p^{b_p},p^{c_p}),
$$

or, equivalently, that $r_K\left(p^am,p^bm,p^c\right)=r_K\left(p^a,p^b,p^c\right)$, for any integer m, prime to p.

First note that if E has e-conductor p^am, then there exists an elliptic curve E' of e-conductor p^a and an isogeny $\phi\colon E\to E'$ of degree prime to p. Indeed, it is enough to show that E admits an isogeny to $\mathbb{C}/\mathcal{O}_{p^am}$ of degree prime to p. For this, write $E=\mathbb{C}/\mathfrak{a}$ and choose an ideal λ of $\mathcal{O}_{p^am}$ in the class of $\mathfrak{a}^{-1}$ in $\mathrm{Pic}(\mathcal{O}_{p^am})$, and whose norm is prime to p. Then the map

$$
E\to E/E[\lambda]\simeq\mathbb{C}/\mathfrak{a}\lambda^{-1}\simeq\mathbb{C}/\mathcal{O}_{p^am}
$$

is such an isogeny. The equality $r_K(p^am,p^bm,p^c)=r_K(p^a,p^b,p^c)$ now follows since cyclic subgroups of E size p^c are in bijection with cyclic subgroups of E' of size p^c, via $C\mapsto\phi(C)$. Moreover, if E/C has e-conductor p^bm, then $E'/\phi(C)$ has e-conductor p^b, by the argument in the first paragraph of this proof. □

Next, we fix a prime p and show how to compute $r_K(p^a, p^b, p^c)$. We will use p-isogeny volcanoes [11], a tool typically used in the study of elliptic curves over finite fields. We define a graph G_p, whose vertex set is the set of isomorphism classes of elliptic curves $E/\mathbb{C}$ with CM by K (we omit the dependence on K from the notation). The edge set of G_p is the set of isomorphism classes of p-isogenies between two such elliptic curves. For each isogeny $\phi\colon E \to E'$ there is a dual isogeny $\hat{\phi}\colon E' \to E$, so we identify these two edges and consider G_p as an undirected graph.

For our purposes we need only consider connected components of G_p containing a vertex representing a curve of e-conductor 1. If H_p is such a component, then the vertices of H are partitioned into *levels* $H_{p,0}, H_{p,1}, \ldots, H_{p,k}, \ldots$, one for each $k \geq 0$, where $H_{p,k}$ consists of the curves in H_p with e-conductor p^k. We call the subgraph on $H_{p,0}$ the *surface*. The key fact is that all such connected components are isomorphic, and each is a *volcano*. In particular, if H_p is the connected component of a curve of e-conductor 1, then H_p has the following properties [11, §2]:

- H_p is $(p+1)$-regular.
- The surface $H_{p,0}$ is a $(1+\chi_K(p))$-regular graph on t vertices, where t is the order of the class $[\mathfrak{p}]$ in $\mathrm{Pic}(\mathcal{O}_K)$, for any prime ideal $\mathfrak{p}$ above p.
- For $k \geq 1$, each vertex in $H_{p,k}$ has a unique edge leading to $H_{p,k-1}$, and this accounts for every edge not in the surface.

We note that for this description of H_p to be accurate, we must require that K contain no roots of unity other than $\{\pm 1\}$.

Figures 1, 2 and 3 depict examples of H_p in the case $p = 3$, for each of the three splitting types. In p is inert in K then every H_p is of the form in the Fig. 1. If p is ramified, each $H_{p,0}$ either has two surface vertices with a unique edge connecting them (as in the Fig. 2), or a single vertex with a self-loop. If p is split, each component either has an n-cycle at the surface with $n \geq 2$ (the case drawn in Fig. 3 is $n = 3$), or there is a unique vertex with two self loops.

Recall that if $G = (V, E)$ is a graph, and $v, v' \in V$ are vertices, then a *walk from v to v' of length c* is a sequence

$$v = v_0, e_1, v_1, e_2, \ldots, v_{c-1}, e_c, v_c = v',$$

where each $e_i \in E$ is an edge connecting v_{i-1} and v_i.

Definition A walk is called *non-backtracking* if $e_i \neq e_{i+1}$ for all i.

Theorem 4.2 *Let a, b, c be non-negative integers. Then $r_K(p^a, p^b, p^c)$ is the number of non-backtracking walks of length c in H_p starting at a fixed vertex of level a and ending at a vertex of level b.*

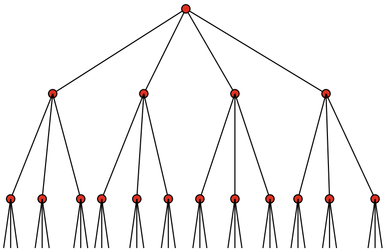

Fig. 1 Connected component of H_3, inert case

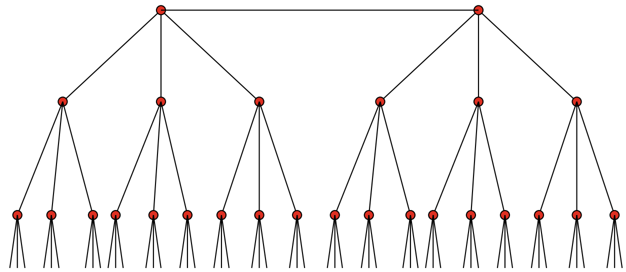

Fig. 2 Connected component of H_3, ramified case

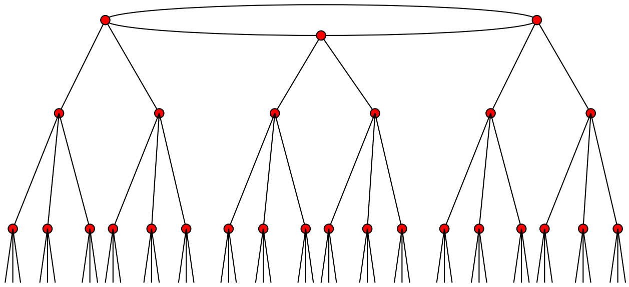

Fig. 3 Connected component of H_3, split case

Proof Suppose E is an elliptic curve with CM by K of e-conductor p^a. Then isomorphism classes of p-isogenies out of E are in bijection with subgroups of E of order p, since we work in characteristic 0, and since $\mathrm{Disc}(K) < -4$. It follows that subgroups of E of order p are in bijection with length 1 walks on H_p starting at E. An isogeny of degree p^c is a composition of p-isogenies, and thus corresponds to a walk along H_p of length c. Backtracking amounts to composing with the dual of the previous p-isogeny, which would make the the composite isogeny divisible by p and hence not cyclic. The theorem follows. □

Theorem 4.2 allows us to compute $r_K(p^a, p^b, p^c)$ explicitly:

Corollary 4.3 *Let $\chi_K(p)$ equal -1, 0 , or 1, depending on whether p is inert, ramified, or split in K. Then*

$$r_K(p^a,p^b,p^c) = \begin{cases} 1 & \text{if } a=b=c=0 \\ 1+\chi_K(p) & \text{if } a=b=0 \text{ and } c>0 \\ 0 & \text{if } a<b \text{ and } c<b-a \\ p^c & \text{if } 0<a\le b \text{ and } c=b-a \\ (p-\chi_K(p))\,p^{c-1} & \text{if } 0=a<b \text{ and } c=b \\ (p-1)p^{(b-a+c)/2-1} & \text{if } a\le b \text{ and } b-a<c<b+a \\ (p-\chi_K(p)-1)p^{b-1} & \text{if } a\le b \text{ and } c=b+a>0 \\ (1+\chi_K(p))\,(p-\chi_K(p))\,p^{b-1} & \text{if } a\le b \text{ and } c=b+a+1>1 \\ (\chi_K(p)+|\chi_K(p)|)\,(p-1)p^{b-1} & \text{if } a\le b \text{ and } c>b+a+1>1 \\ r_K(p^b,p^b,p^{c-a+b}) & \text{if } a>b. \end{cases}$$

Here, we use the convention that $p^s = 0$ *if* s *is not an integer. Note that the formula in the last case reduces to one of the earlier cases.*

Proof The key point is that non-backtracking walks on H_p are very constrained: once a non-backtracking walk begins to descend down the volcano, it cannot reascend. Moreover, the only 'horizontal' edges on H_p are at the surface. It follows that a non-backtracking walk on H_p consists of (at most) three stages in the following order: ascend up the volcano, move horizontally at the surface, and then descend down the volcano.

We give the proof of the corollary in the case $a \leq b$ and $c > b + a + 1$, and leave the proofs of the other cases to the reader, as they are similar. We must choose a vertex in level a and count the number of non-backtracking walks of length c to a vertex of level b. Note that $b \geq 1$ in this case. Since $c > a + b$, any non-backtracking walk from level a to level b of length c on H_p must begin by ascending via the unique path to the surface. Then the walk must take $c - b - a \geq 2$ horizontal steps along the surface before descending down to level b. This is only possible, without backtracking, if p splits in K, and in that case there are exactly two ways to traverse across the n-cycle at the surface. There are then $(p-1)p^{b-1}$ ways to descend to level b. Thus, in the split case there are a total of $2(p-1)p^{b-1}$ non-backtracking walks, whereas in the non-split cases there are $0 = \chi_K(p) + |\chi_K(p)|$ such walks, as claimed. □

As an example of how to compute these numbers "by eye", we now give the proof of Corollary 1.3. This is the special case where $A = \mathbb{C}^2/\mathcal{O}_f^2$, and hence $\mathrm{Aut}(A) = \mathrm{GL}_2(\mathcal{O}_f)$.

Proof of Corollary 1.3 We need to show that if $k \mid d \mid f$, then

$$r_K(f, k, f/d) = \begin{cases} 1 & \text{if } k = d \\ 0 & \text{otherwise.} \end{cases}$$

By Lemma 4.1, we may assume $f = p^a$, $k = p^b$, and $d = p^c$, with $a \geq c \geq b$. Then if $b < c$, a vertex in level a cannot walk to level b in $a - c$ steps. But if $b = c$, there is a unique (ascending) walk from a vertex of level a to a vertex of level b of length $a - b$, as claimed. □

In the general case, the formula for $N(E, E')$ obtained by combining Theorem 1.1 and Corollary 4.3 does not seem to simplify much further.

Author details

[1]Department of Mathematics, University of Michigan, 530 Church St., Ann Arbor, MI 48109, USA, [2]Department of Mathematics, Boston College, Chestnut Hill, MA 02647, USA.

Acknowledgements

AS thanks Andrew Snowden for a helpful conversation and Andrew Sutherland for help with the figures. AS was partially supported by NSF Grant DMS-0943832.

Received: 19 August 2016 Accepted: 17 January 2017
Published online: 01 May 2017

References

1. Birkenhake, C., Lange, H.: Complex Tori. Springer, Berlin (1999)
2. Cremona, J. E., Aranés, M. T.: Congruence subgroups, cusps and manin symbols over number fields. In: Boeckle, G., Wiese, G. (eds.) Computations with Modular Forms. Contributions in Mathematical and Computational Sciences, vol. 6, pp. 109–127. Springer International Publishing (2014)
3. Gross, B.H., Zagier, D.: Heegner points and derivatives of *L*-series. Invent. Math. **84**, 225–320 (1986)
4. Kani, E.: Products of CM elliptic curves. Collect. Math. **62**(3), 297–339 (2011)
5. Lenstra Jr., H., Oort, F., Zarhin, Y.: Abelian subvarieties. J. Algebra **180**(2), 513–516 (1996)

6. Mitani, T., Shioda, T.: Singular abelian surfaces and binary quadratic forms. In: Classification of Algebraic Varieties and Compact Complex Manifolds. Lecture Notes Mathematics, vol. 412, pp. 259–287 (1974)
7. Oort, F., Zarhin, Y.: Complex tori. Indag. Math. **7**, 473–487 (1996)
8. Papanikolas, M., Ramachandran, N.: A Weil–Barsotti formula for Drinfeld modules. J. Number Theory **98**(2), 407–431 (2003)
9. Rosen, J., Shnidman, A.: Néron-Severi groups of product abelian surfaces. arXiv: 1402.2233 (2014)
10. Sage script for computing orbit counts. arXiv:1608.01390v1
11. Sutherland, A.: Isogeny volcanoes. Open Book Ser. **1**(1), 507–530 (2013)