Algebra & Number Theory

Volume 2

2008

No. 2

mathematical sciences publishers

Algebra & Number Theory
www.jant.org

PRODUCTION

ant@mathscipub.org
Paulo Ney de Souza, Production Manager
Silvio Levy, Senior Production Editor

See inside back cover or www.jant.org for submission instructions.

Regular subscription rate for 2008: $180.00 a year ($120.00 electronic only).
Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA.

Algebra & Number Theory, ISSN 1937-0652, at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

PUBLISHED BY
mathematical sciences publishers
http://www.mathscipub.org
A NON-PROFIT CORPORATION
Typeset in LaTeX

A topological property of quasireductive group schemes

Najmuddin Fakhruddin and Vasudevan Srinivas

In a recent paper, Gopal Prasad and Jiu-Kang Yu introduced the notion of a quasireductive group scheme $\mathscr{G}$ over a discrete valuation ring R, in the context of Langlands duality. They showed that such a group scheme $\mathscr{G}$ is necessarily of finite type over R, with geometrically connected fibres, and its geometric generic fibre is a reductive algebraic group; however, they found examples where the special fibre is nonreduced, and the corresponding reduced subscheme is a reductive group of a different type. In this paper, the formalism of vanishing cycles in étale cohomology is used to show that the generic fibre of a quasireductive group scheme cannot be a restriction of scalars of a group scheme in a nontrivial way; this answers a question of Prasad, and implies that nonreductive quasireductive group schemes are essentially those found by Prasad and Yu.

Gopal Prasad and Jiu-Kang Yu [2006] introduced the notion of a *quasireductive group scheme* over a discrete valuation ring R in a recent paper: this is an affine, flat group scheme $\pi : \mathscr{G} \to \operatorname{Spec} R$, such that

(i) the generic fibre $\mathscr{G}_K$ is a smooth, connected group scheme over the quotient field K of R;

(ii) the reduced geometric special fibre $(\mathscr{G}_{\bar{k}})_{\text{red}}$ is of finite type over the algebraic closure of the residue field k of R, and its identity component is a reductive affine algebraic group;

(iii) $\dim \mathscr{G}_K = \dim \mathscr{G}_k$.

They showed that $\mathscr{G}$ is necessarily of finite type over R, with geometrically connected fibres, and its geometric generic fibre is a reductive algebraic group. Further, $\mathscr{G}$ is a reductive group scheme over $\operatorname{Spec} R$, except possibly when R has residue characteristic 2 and the geometric generic fibre $\mathscr{G}_{\overline{K}}$ has a nontrivial normal subgroup of type SO_{2n+1}, for some $n \geq 1$. They gave examples to show that in case $\mathscr{G}_{\overline{K}} = \mathrm{SO}_{2n+1}$, reductivity can fail to hold, with a nonreduced geometric special fibre, and they gave a classification of such $\mathscr{G}$. Their work arose in response to

MSC2000: primary 14L15; secondary 20G35.

Keywords: group scheme, quasireductive, nearby cycle.

a question of Vilonen to Prasad, in connection with a Tannakian construction of Langlands dual groups; see [Mirković and Vilonen 2004].

In this context, it is natural to ask if there are any other possibilities for nonreductive, quasireductive group schemes $\mathscr{G}$, except the examples found by Prasad and Yu, and the others obtained from these by simple modifications (like products and so forth). From their results, this boils down to the following specific question:

> Does there exist a quasireductive group scheme $\pi : \mathscr{G} \to \operatorname{Spec} R$, where R is a complete DVR with algebraically closed residue field, such that for some finite, separable (totally ramified) extension field L of K, of degree > 1, the generic fibre $\mathscr{G}_K$ is isomorphic to $R_{L/K}(\mathrm{SO}_{2n+1})_L$, the Weil restriction of scalars of $(\mathrm{SO}_{2n+1})_L$?

One aim of this paper is to show that *there do not exist any such quasireductive group schemes*; see Corollary 2 below. Gopal Prasad has obtained a stronger conclusion, combining Corollary 2 with the arguments based on [Prasad and Yu 2006]; at his urging, this is included below (Theorem 11).

The nonexistence proof is based on a topological result, Theorem 1, on the ℓ-adic cohomology of a quasireductive group scheme; it says roughly that, though a quasireductive group scheme may not be smooth over the base, it is almost so from the point of view of ℓ-adic cohomology. This property of quasireductive group schemes (including the nonsmooth ones) may also be of interest in potential applications of such group schemes. This topological result was motivated by the well known Serre–Tate criterion [1968] for good reduction of abelian varieties, which relies ultimately on the theory of Néron models. In a sense, [Prasad and Yu 2006] also relies on some aspects of this theory.

Theorem 1. *Let R be a complete DVR with quotient field K and algebraically closed residue field k. Let*

$$\pi : \mathscr{G} \to \operatorname{Spec} R$$

be a quasireductive group scheme. Let $G \to \operatorname{Spec} K$ be the generic fibre. Let ℓ be a prime number, invertible in R. Then the action of the inertia group $\operatorname{Gal}(\overline{K}/K)$ on the étale cohomology group $H^i_{\mathrm{et}}(G_{\overline{K}}, \mathbb{Z}/\ell^n\mathbb{Z})$ is trivial, for any $i, n \geq 0$. Thus, the inertia action on the ℓ-adic cohomology $H^i_{\mathrm{et}}(G_{\overline{K}}, \mathbb{Q}_\ell)$ is trivial, for all $i \geq 0$.

For a more technical assertion, which implies the above result, and may be viewed as the key new observation in this paper, see Proposition 8 in Section 2 below.

Corollary 2. *Let R be a complete DVR with quotient field K, and algebraically closed residue field k. Let L be a finite extension field of K, and let*

$$\pi : \mathscr{G} \to \operatorname{Spec} R$$

be a quasireductive group scheme, whose generic fibre $\mathcal{G}_K$ is isomorphic to the restriction of scalars of a positive dimensional reductive affine algebraic group G over L. Then we must have $L = K$.

Proof. We first note that since $G_{\overline{K}}$ is a positive dimensional reductive algebraic group over an algebraically closed field, it has a nonzero ℓ-adic Betti number in some positive degree; for example, this is a simple consequence of the classification of reductive groups over algebraically closed fields. Let $i > 0$ be the smallest such degree.

Next, since the generic fibre of $\mathcal{G} \to \operatorname{Spec} R$ is a reductive group and is obtained by the restriction of scalars from L to K, the extension field L/K is necessarily separable. (If L/K is a purely inseparable finite extension and G is an algebraic group over L, then the kernel of the natural homomorphism $R_{L/K}(G)_L \to G$ is unipotent; see [Oesterlé 1984, A.3.5], for example.)

Now, if L/K is a separable extension of degree $n > 1$, then the geometric generic fibre $\mathcal{G}_{\overline{K}}$ is isomorphic to a product of n copies of $G_{\overline{K}}$, and the inertia group $\operatorname{Gal}(\overline{K}/K)$ permutes the n factors transitively. From the Kunneth formula, it follows that for the chosen $i > 0$, the étale cohomlogy group $H^i_{\text{et}}(\mathcal{G}_{\overline{K}}, \mathbb{Q}_\ell)$ is a direct sum of (a positive number of) copies of a nontrivial permutation Galois module. This contradicts Theorem 1. □

1. Some preliminaries

Before proving Theorem 1, we discuss some preliminaries.

Recall that, if k is an algebraically closed field, a *unipotent isogeny* between connected reductive algebraic k-groups is a homomorphism, which is a finite surjective morphism, whose kernel does not contain any nontrivial subgroup scheme of multiplicative type (that is, isomorphic to a subgroup scheme of $\mathbb{G}_m^e$ for some $e \geq 1$).

The following lemma sheds more light on unipotent isogenies (see Corollary 4). We thank Conrad for explaining this argument to us; the reader might compare this with [Prasad and Yu 2006, Lemma 2.2].

Lemma 3. *Let H be a reduced group scheme over a perfect field k, let G be a closed normal subgroup scheme of H and let G^{red} be the reduced subscheme of G. Then G^{red} is also a normal subgroup scheme of H. If H is connected and G is finite then G^{red} is in the center of H.*

Proof. We first recall that since k is perfect, the product of reduced k-schemes is reduced, so the morphism $G^{\text{red}} \times G^{\text{red}} \to G$ induced by the product morphism of G factors through G^{red} and similarly for the inverse morphism. Hence G^{red} is a subgroup scheme of G. Since H is reduced, so is $H \times G^{\text{red}}$, and hence $(H \times G)^{\text{red}} = H \times G^{\text{red}}$.

Let $c : H \times G \to G$ be the morphism giving the conjugation action of H on G and let $i : G^{\mathrm{red}} \to G$ be the inclusion. Then there is a unique morphism $c^{\mathrm{red}} : H \times G^{\mathrm{red}} \to G^{\mathrm{red}}$ making the diagram below commute,

$$\begin{tikzcd} H \times G^{\mathrm{red}} \arrow[r, "c^{\mathrm{red}}"] \arrow[d, "\mathrm{Id}\times i"'] & G^{\mathrm{red}} \arrow[d, "i"] \\ H \times G \arrow[r, "c"] & G. \end{tikzcd}$$

Thus G^{red} is normal.

Now suppose G is finite and H is connected. Since $H(k)$ is nonempty, H is geometrically connected over k [EGA 6, 4.5.13]. We may assume that k is algebraically closed and so G^{red} is a disjoint union of copies of $\operatorname{Spec} k$. Then the inclusion $e\colon \operatorname{Spec} k \to H$ given by the identity induces a bijection of connected components of G^{red} with those of $H \times G^{\mathrm{red}}$. Since c^{red} is continuous, it follows that

$$c^{\mathrm{red}} = p_{G^{\mathrm{red}}},$$

the projection onto G^{red}. Thus G^{red} is central. □

Corollary 4. *The kernel of a unipotent isogeny between connected reductive algebraic groups over an algebraically closed field k is infinitesimal, so that such an isogeny must be purely inseparable.*

Proof. If H is a connected reductive algebraic group over k, and G is the kernel of a unipotent isogeny with domain H, then G is a finite, normal subgroup scheme of H. By Lemma 3, G^{red} is a central subgroup scheme, hence contained in a maximal torus. Since G, and hence G^{red}, has no nontrivial subgroup scheme of multiplicative type, this means G^{red} is trivial, that is, G is infinitesimal. □

Lemma 5. *Let k be an algebraically closed field of characteristic $p > 0$, and ℓ a prime distinct from p. Let $f : G_1 \to G_2$ be either*

(i) *a unipotent isogeny between connected reductive algebraic groups over k, or*

(ii) *a closed immersion of k-schemes of finite type, which induces an isomorphism on the underlying reduced schemes.*

Then

$$\mathcal{F} \mapsto f_*\mathcal{F}, \quad \mathcal{F}' \mapsto f^*\mathcal{F}'$$

determine an equivalence of categories between étale sheaves on G_1 and G_2, and there are natural isomorphisms $H^i_{\mathrm{et}}(G_2, f_*\mathcal{F}) \cong H^i_{\mathrm{et}}(G_1, \mathcal{F})$ for all i.

Proof. A finite, surjective, radicial morphism induces an equivalence of categories on étale sheaves, and hence isomorphisms on étale cohomology — see [SGA 4 II, Exposé VIII, Théorème 1.1, Cor. 1.2]. □

The main input in the proof of Theorem 1 is the formalism of vanishing cycles, and in particular, the notion of the *complex of nearby cycles*, as explained in [SGA 7 II, Exposé XIII]. We briefly review what we need.

Suppose given a morphism of schemes $\pi : X \to T$, where T is the spectrum of a complete discrete valuation ring with algebraically closed residue field. Denote the generic point of T by η, and fix an algebraic closure of the quotient field of the DVR, giving a geometric generic point $\overline{\eta}$ of T. Let X_0 be the closed fibre, and let $X_{\overline{\eta}}$ be the geometric generic fibre.

If $\mathcal{F}$ is any étale sheaf of $\mathbb{Z}/\ell^n\mathbb{Z}$-modules on X, then one defines the complex of nearby cycles $R\psi_T(\mathcal{F})$ on the closed fibre X_0 as follows: if $i : X_0 \to X$ is the inclusion, and $j : X_{\overline{\eta}} \to X$ the evident morphism, then

$$R\psi_T(\mathcal{F}) = i^* Rj_* j^* \mathcal{F}.$$

The adjunction map $\mathrm{id} \to i_* i^*$ gives a map $Rj_* j* \to i_* i^* Rj_* j*$ and the adjunction map $\mathrm{id} \to Rj_* j^*$ gives a map $i^* \to i^* Rj_* j^*$. These give rise to maps on cohomology:

$$\begin{aligned} H^i_{\mathrm{et}}(X_{\overline{\eta}}, j^*\mathcal{F}) &\to H^i_{\mathrm{et}}(X_0, R\psi_T(\mathcal{F})),\\ H^i_{\mathrm{et}}(X_0, \mathcal{F}_0) &\to H^i_{\mathrm{et}}(X_0, R\psi_T(\mathcal{F})). \end{aligned} \tag{1-1}$$

Further, $H^i_{\mathrm{et}}(X_0, R\psi_T(\mathcal{F}))$ carries an action of the inertia group $\mathrm{Gal}(k(\overline{\eta})/k(\eta))$, such that the above two maps on cohomology are equivariant (where the inertia action on $H^i_{\mathrm{et}}(X_0, \mathcal{F}_0)$ is taken to be trivial). We may of course replace the closed fibre X_0 by its reduced subscheme in the above, since the categories of étale sheaves on X_0 and $(X_0)_{\mathrm{red}}$ are equivalent. If $T = \mathrm{Spec}\, R$, we may write ψ_R instead of ψ_T.

The adjunctions above fit into a square

$$\begin{tikzcd} \mathrm{id} \arrow[r] \arrow[d] & Rj_* j^* \arrow[d] \\ i_* i^* \arrow[r] & i_* i^* Rj_* j^* \end{tikzcd}$$

which gives a commutative diagram

$$\begin{tikzcd} H^i_{\mathrm{et}}(X, \mathcal{F}) \arrow[r] \arrow[d] & H^i_{\mathrm{et}}(X_{\overline{\eta}}, j^*\mathcal{F}) \arrow[d] \\ H^i_{\mathrm{et}}(X_0, \mathcal{F}_0) \arrow[r] & H^i_{\mathrm{et}}(X_0, R\psi_T(\mathcal{F})). \end{tikzcd} \tag{1-2}$$

Here the left vertical arrow is an isomorphism if f is proper [SGA 5, proper base change theorem, Exposé XII].

Lemma 6. *If in the above situation, $f : X \to T$ is smooth, and $\mathcal{F}$ is a locally constant constructible sheaf of $\mathbb{Z}/\ell^n\mathbb{Z}$-modules, with ℓ invertible in $\mathcal{O}_T$, then the natural map*

$$\mathcal{F}_0 \to R\psi_T(\mathcal{F})$$

is an isomorphism, and so induces isomorphisms on étale cohomology.

Proof. This follows from the definition of $R\psi_T$, and the smooth base change theorem [SGA 7 II, Exposé XIII, Reformulation 2.1.5 and above]. □

Lemma 7. *Let X be a noetherian scheme, $i : Y \to X$ a closed embedding, $\beta : X' \to X$ a finite morphism, $Y' = X' \times_X Y$ with induced embedding $i' : Y' \to X'$ and finite morphism $\alpha : Y' \to Y$. For all $\mathcal{I} \in D^+(X_{\mathrm{et}})$ and $r \in \mathbb{Z}$ the restriction map*

$$H^r_{\mathrm{et}}(X', \mathcal{I}) \to H^r_{\mathrm{et}}(Y', i'^*\mathcal{I})$$

is equal to the composite

$$H^r_{\mathrm{et}}(X', \mathcal{I}) \to H^r_{\mathrm{et}}(X, R\beta_*\mathcal{I}) \to H^r_{\mathrm{et}}(Y, i^*R\beta_*\mathcal{I}) \to H^r_{\mathrm{et}}(Y, R\alpha_*i'^*\mathcal{I}) \to H^r_{\mathrm{et}}(Y', i'^*\mathcal{I})$$

where the first and the last map are the natural isomorphisms, the second is the restriction map and the third is induced by the base change map.

Proof. If $\mathcal{I}$ is represented by a single sheaf $\mathcal{F}$ (in degree 0) and $r = 0$ then the equality follows from the very definition of the base change map [SGA 5, Exposé XII, §4].

We now assume that $\mathcal{I}$ is (represented by) a bounded below complex of injective sheaves

$$\dots \mathcal{I}^{j-1} \to \mathcal{I}^j \to \mathcal{I}^{j+1} \to \cdots .$$

Then $i'^*\mathcal{I}$ is (represented by) the complex

$$\cdots i'^*\mathcal{I}^{j-1} \to i'^*\mathcal{I}^j \to i'^*\mathcal{I}^{j+1} \to \cdots .$$

Let $\mathcal{J}$ be a complex of injective sheaves on Y' with a quasiisomorphism $q' : i'^*\mathcal{I} \to \mathcal{J}$. Then the map $H^r_{\mathrm{et}}(X', \mathcal{I}) \to H^r_{\mathrm{et}}(Y', i'^*\mathcal{I})$ is induced by the map of complexes of abelian groups which in cohomological degree r is the composite

$$\Gamma(X', \mathcal{I}^r) \to \Gamma(Y', i'^*\mathcal{I}^r) \to \Gamma(Y', \mathcal{J}^r) .$$

Since the pushforward by a finite morphism is exact on the category of étale sheaves,

$$\alpha_*(q) : \alpha_*i'^*\mathcal{I} \to \alpha_*\mathcal{J}$$

is a quasiisomorphism and $\alpha_*\mathcal{J}$ is also a complex of injective sheaves on Y. Using the base change isomorphism we may view $q' := \alpha_*(q)$ as a quasiisomorphism

$i^*\beta_*\mathcal{I} \to \alpha_*\mathcal{J}$, and hence we may use it to compute the second map in the sequence of the lemma. Since the diagram

$$\begin{tikzcd}
\Gamma(Y', i'^*\mathcal{J}^j) \arrow[r, "q"] \arrow[d] & \Gamma(Y', \mathcal{J}^j) \arrow[d] \\
\Gamma(Y, \alpha_* i'^*\mathcal{J}^j) \arrow[r, "q'"] & \Gamma(Y, \alpha_*\mathcal{J}^j),
\end{tikzcd}$$

where the vertical maps are the canonical isomorphisms, commutes for all j, the lemma then follows from the first step of the proof. □

2. Proof of the theorem

We now give the proof of Theorem 1.

If we apply the formalism of nearby cycles to our quasireductive group scheme

$$\pi : \mathcal{G} \to \operatorname{Spec} R$$

(which is of course not proper), with geometric generic fibre $\mathcal{G}_{\overline{K}}$, special fibre $\mathcal{G}_0$, and

$$\mathcal{F} = (\mathbb{Z}/\ell^n\mathbb{Z})_{\mathcal{G}},$$

where ℓ is invertible in R, then from (1-1) we obtain homomorphisms

$$H^i_{\text{et}}(\mathcal{G}_{\overline{K}}, \mathbb{Z}/\ell^n\mathbb{Z}) \to H^i_{\text{et}}(\mathcal{G}_0, R\psi_R(\mathbb{Z}/\ell^n\mathbb{Z})), \tag{2-1}$$

$$H^i_{\text{et}}(\mathcal{G}_0, \mathbb{Z}/\ell^n\mathbb{Z}) \to H^i_{\text{et}}(\mathcal{G}_0, R\psi_R(\mathbb{Z}/\ell^n\mathbb{Z})). \tag{2-2}$$

These are equivariant for the action of the inertia $\operatorname{Gal}(\overline{K}/K)$, where the action on $H^i_{\text{et}}(\mathcal{G}_0, Z/\ell^n\mathbb{Z})$ is trivial.

Thus, Theorem 1 follows from:

Proposition 8. *With the above notation, the maps in* (2-1), (2-2) *are* isomorphisms, *for any n.*

We first consider the situation of a smooth reductive group scheme.

Lemma 9. *Let R be a complete DVR with algebraically closed residue field. Let*

$$\varphi : \mathcal{H} \to \operatorname{Spec} R$$

be a smooth, reductive group scheme. Let H_0 be the closed fibre of φ, and $H_{\overline{\eta}}$ the geometric generic fibre. Then for any prime ℓ which is invertible in R, we have the following.

(i) *The canonical map*

$$(\mathbb{Z}/\ell^n\mathbb{Z})_{H_0} \to R\psi_R(\mathbb{Z}/\ell^n\mathbb{Z})_{\mathcal{H}}$$

is an isomorphism.

(ii) *The canonical maps*

$$H^i_{\text{et}}(H_{\bar\eta}, \mathbb{Z}/\ell^n Z) \to H^i_{\text{et}}(H_0, R\psi_R(\mathbb{Z}/\ell^n\mathbb{Z})),$$
$$H^i_{\text{et}}(H_0, \mathbb{Z}/\ell^n\mathbb{Z}) \to H^i_{\text{et}}(H_0, R\psi_R(\mathbb{Z}/\ell^n\mathbb{Z}))$$

are isomorphisms.

Proof. Since φ is a smooth morphism, the isomorphism in (i) holds by Lemma 6.

To get the isomorphisms in (ii), consider (1-2) constructed with $X = \mathscr{H}$, $f = \varphi$, $\mathscr{F} = \mathbb{Z}/\ell^n\mathbb{Z}$:

$$\begin{tikzcd}
H^i_{\text{et}}(\mathscr{H}, \mathbb{Z}/\ell^n\mathbb{Z}) \arrow[r] \arrow[d] & H^i_{\text{et}}(H_{\bar\eta}, \mathbb{Z}/\ell^n\mathbb{Z}) \arrow[d] \\
H^i_{\text{et}}(H_0, \mathbb{Z}/\ell^n\mathbb{Z}) \arrow[r] & H^i_{\text{et}}(H_0, R\psi_R(\mathbb{Z}/\ell^n\mathbb{Z})).
\end{tikzcd}$$

We claim that the left vertical and top horizontal arrows are isomorphisms; this follow at once from [Raynaud 1968, Théorème 3.7] or [SGA 5, Exposé VII, Proposition 6.2, p. 315]. From (i), the bottom horizontal arrow is also an isomorphism, and so the right vertical arrow must be one as well. □

We now return to the case of a "general" quasireductive group scheme.

Lemma 10. *Let* $\pi : \mathscr{G} \to \operatorname{Spec} R$ *be a quasireductive group scheme, where R is a complete DVR with algebraically closed residue field, and ℓ a prime invertible in R. Let $\mathscr{G}_0$ be the closed fibre of π. Then the canonical map*

$$(\mathbb{Z}/\ell^n\mathbb{Z})_{\mathscr{G}_0} \to R\psi_R(\mathbb{Z}/\ell^n\mathbb{Z})_{\mathscr{G}}$$

is an isomorphism.

Proof. Combining Propositions 3.4 and 4.3 of [Prasad and Yu 2006], we see that there is a finite extension field K' of K (contained in our chosen algebraic closure $\bar{K}$) with the following property. Let R' be the integral closure of R in K', and set

$$\widetilde{\mathscr{G}} = \text{ normalization of } \mathscr{G} \times_{\operatorname{Spec} R} \operatorname{Spec} R'.$$

Then

(i) R' is a complete DVR (with the same residue field as R),

(ii) $\widetilde{\mathscr{G}} \to \operatorname{Spec} R'$ is a smooth, reductive group scheme with connected fibres, and

(iii) the induced morphism on reduced, geometric special fibres $\widetilde{\mathscr{G}}_0 \to (\mathscr{G}_0)_{\text{red}}$ is a unipotent isogeny between connected, reductive groups of the same dimension.

The propositions cited rely on a result due independently to Raynaud and Faltings, whose proof is given in [Conrad 2006].

We note that there is a commutative diagram

$$\begin{tikzcd}
\widetilde{\mathscr{G}} \arrow[r] \arrow[d, "\pi'"'] & \mathscr{G} \arrow[d, "\pi"] \\
\operatorname{Spec} R' \arrow[r] & \operatorname{Spec} R.
\end{tikzcd}$$

By choice, the geometric point $\overline{\eta}$ of Spec R is also a geometric point of Spec R'.

Let $\widetilde{\mathscr{G}}_1 = \widetilde{\mathscr{G}} \times_{\mathscr{G}} \mathscr{G}_0$. We may regard the special fibre $\widetilde{\mathscr{G}}_0$ of $\pi' : \widetilde{\mathscr{G}} \to \operatorname{Spec} R'$ as a closed subscheme of $\widetilde{\mathscr{G}}_1$, and in fact it is just the underlying reduced subscheme. Thus the inclusion

$$i_0 : \widetilde{\mathscr{G}}_0 \hookrightarrow \widetilde{\mathscr{G}}_1$$

induces an equivalence of categories between étale sheaves on the two schemes; under this equivalence, the constant sheaves $\mathbb{Z}/\ell^n\mathbb{Z}$ on the two schemes correspond. There is a commutative diagram

$$\begin{tikzcd}
 & & \mathscr{G}_{\overline{K}} \arrow[d, "j'"] \\
\widetilde{\mathscr{G}}_0 \arrow[r, "i_0"] \arrow[dr] & \widetilde{\mathscr{G}}_1 \arrow[r, "i_1"] \arrow[d, "\alpha"'] & \widetilde{\mathscr{G}} \arrow[d, "\beta"] \\
 & \mathscr{G}_0 \arrow[r, "i"] & \mathscr{G}
\end{tikzcd}$$

where the square is a pullback, and the inclusion $i' : \widetilde{\mathscr{G}}_0 \to \widetilde{\mathscr{G}}$ is the composition $i' = i_1 \circ i_0$.

From the definitions, we have that

$$R\psi_{R'}(\mathbb{Z}/\ell^n\mathbb{Z})_{\widetilde{\mathscr{G}}} = i'^* Rj'_*(\mathbb{Z}/\ell^n\mathbb{Z})_{\mathscr{G}_{\overline{K}}} \ .$$

From Lemma 9, this is isomorphic to the constant sheaf $\mathbb{Z}/\ell^n\mathbb{Z}$ on $\widetilde{\mathscr{G}}_0$. Hence we obtain isomorphisms

$$(\mathbb{Z}/\ell^n\mathbb{Z})_{\widetilde{\mathscr{G}}_0} \cong i'^* Rj'_*(\mathbb{Z}/\ell^n\mathbb{Z})_{\mathscr{G}_{\overline{K}}} \cong i_0^* i_1^* Rj'_*(\mathbb{Z}/\ell^n\mathbb{Z})_{\mathscr{G}_{\overline{K}}} \ .$$

This implies that

$$(\mathbb{Z}/\ell^n\mathbb{Z})_{\widetilde{\mathscr{G}}_1} \cong i_1^* Rj'_*(\mathbb{Z}/\ell^n\mathbb{Z})_{\mathscr{G}_{\overline{K}}} \ .$$

Applying $R\beta_* = \beta_*$ (since β is a finite morphism), and using the proper base-change theorem, we get isomorphisms

$$\alpha_*(\mathbb{Z}/\ell^n\mathbb{Z})_{\widetilde{\mathscr{G}}_1} \cong i^* R(\beta \circ j')_*(\mathbb{Z}/\ell^n\mathbb{Z})_{\mathscr{G}_{\overline{K}}} = R\psi_R(\mathbb{Z}/\ell^n\mathbb{Z})_{\mathscr{G}} \ .$$

Now the three arrows

$$i_0 : \widetilde{\mathscr{G}}_0 \to \widetilde{\mathscr{G}}_1, \quad \widetilde{\mathscr{G}}_0 \to (\mathscr{G}_0)_{\mathrm{red}}, \quad (\mathscr{G}_0)_{\mathrm{red}} \hookrightarrow \mathscr{G}_0$$

induce equivalences of categories between the respective categories of étale sheaves (the middle arrow is a unipotent isogeny, the other two are inclusions of underlying reduced schemes). Hence α_* also induces such an equivalence of categories, so $R\psi_R(\mathbb{Z}/\ell^n\mathbb{Z})_{\mathscr{G}}$ is isomorphic to $(\mathbb{Z}/\ell^n\mathbb{Z})_{\mathscr{G}_0}$. It follows from the description of the stalks of $R^i\psi_R(\mathbb{Z}/\ell^n\mathbb{Z})_{\mathscr{G}}$ [SGA 7 II, Exposé 12, Proposition 2.1.4] that the canonical map $(\mathbb{Z}/\ell^n\mathbb{Z})_{\mathscr{G}_0} \to R^0\psi_R(\mathbb{Z}/\ell^n\mathbb{Z})_{\mathscr{G}}$ is an injection of sheaves. Since any injection from $(\mathbb{Z}/\ell^n\mathbb{Z})_{\mathscr{G}_0}$ to itself must be an isomorphism, the lemma follows. □

In particular, we see that the map (2-2) is an isomorphism. It remains to consider the map (2-1)

$$H^i_{\mathrm{et}}(\mathscr{G}_{\overline{K}}, \mathbb{Z}/\ell^n\mathbb{Z}) \to H^i_{\mathrm{et}}(\mathscr{G}_0, R\psi_R\mathbb{Z}/\ell^n\mathbb{Z}).$$

This map is constructed as the composition

$$H^i_{\mathrm{et}}(\mathscr{G}_{\overline{K}}, \mathbb{Z}/\ell^n\mathbb{Z}) \cong H^i_{\mathrm{et}}(\mathscr{G}, Rj_*\mathbb{Z}/\ell^n\mathbb{Z}) \to H^i_{\mathrm{et}}(\mathscr{G}_0, i^*Rj_*\mathbb{Z}/\ell^n\mathbb{Z}) = H^i_{\mathrm{et}}(\mathscr{G}_0, R\psi_R\mathbb{Z}/\ell^n\mathbb{Z}).$$

Thus it suffices to show that the restriction map

$$H^i_{\mathrm{et}}(\mathscr{G}, Rj_*\mathbb{Z}/\ell^n\mathbb{Z}) \to H^i_{\mathrm{et}}(\mathscr{G}_0, i^*Rj_*\mathbb{Z}/\ell^n\mathbb{Z}) \tag{2-3}$$

is an isomorphism.

The analogous map for the group scheme $\pi' : \widetilde{\mathscr{G}} \to \operatorname{Spec} R'$ is similarly expressed as a composition

$$H^i_{\mathrm{et}}(\mathscr{G}_{\overline{K}}, \mathbb{Z}/\ell^n\mathbb{Z}) \cong H^i_{\mathrm{et}}(\widetilde{\mathscr{G}}, Rj'_*\mathbb{Z}/\ell^n\mathbb{Z}) \to H^i_{\mathrm{et}}(\widetilde{\mathscr{G}}_0, i'^*Rj'_*\mathbb{Z}/\ell^n\mathbb{Z}) = H^i_{\mathrm{et}}(\widetilde{\mathscr{G}}_0, R\psi_{R'}\mathbb{Z}/\ell^n\mathbb{Z}).$$

As seen in Lemma 9, this composition is an isomorphism.

Since $i' = i_0 \circ i_1$, where i_0 is finite, surjective and radicial, we see that the restriction map

$$H^i_{\mathrm{et}}(\widetilde{\mathscr{G}}, Rj'_*\mathbb{Z}/\ell^n\mathbb{Z}) \to H^i_{\mathrm{et}}(\widetilde{\mathscr{G}}_1, i_1^*Rj'_*\mathbb{Z}/\ell^n\mathbb{Z}) \tag{2-4}$$

is also an isomorphism. The formula $j = \beta \circ j'$, Lemma 7, the proper base change theorem and (2-4) imply that the map in (2-3) is indeed an isomorphism, thus completing the proof of the theorem.

3. An application

Gopal Prasad has given the following application of Corollary 2; we include his proof here.

Theorem 11. *Let R be a strictly Henselian DVR with algebraically closed residue field, and K be its field of fractions. Then the generic fibre $G = \mathscr{G}_K$ of any quasireductive R-scheme $\mathscr{G}$ splits over K.*

Proof. In view of [Prasad and Yu 2006, Proposition 4.4 (i)], we can assume that G is either a torus or a semisimple K-simple group. Now if G is a torus, then it follows from [SGA 3 II, Exposé X, Théorème 8.8], that $\mathscr{G}$ is a R-torus, which implies that it splits over R [SGA 3 III, Exposé XXII, Proposition 2.1], and hence the generic fibre G is a K-split torus. We assume now that G is a semisimple K-simple group. If G does not contain a normal subgroup, defined and isomorphic over the algebraic closure $\overline{K}$ of K, to SO_{2n+1} for some $n \geqslant 1$, then according to [Prasad and Yu 2006, Theorem 1.2], $\mathscr{G}$ is smooth and reductive, so again by [SGA 3 III, Exposé XXII, Proposition 2.1], $\mathscr{G}$ is split, and so its generic fibre G is K-split. On the other hand, if G contains a normal subgroup defined and isomorphic over $\overline{K}$ to SO_{2n+1} for some $n \geqslant 1$, then as SO_{2n+1} is a group of adjoint type, and G is K-simple, there exists a finite separable extension $L \subset \overline{K}$ of K, and an absolutely simple L-group H such that

(i) H is $\overline{K}$-isomorphic to SO_{2n+1}, and

(ii) $G \cong R_{L/K}(H)$; see [Borel and Tits 1965, 6.21(ii) and 6.17].

Now Corollary 2 implies that since $\mathscr{G}$ is quasireductive, $L = K$. Thus G is a K-group which is isomorphic to SO_{2n+1} over $\overline{K}$. But as K is a field of cohomological dimension $\leqslant 1$, according to a well known theorem of Steinberg [1965] (if K is imperfect, see also [Borel and Springer 1968, 8.6]), G is quasisplit over K. But as G is an absolutely simple K-group of type B_n, if it is quasisplit over K, then it is K-split. This completes the proof of the above theorem. □

Remark 12. Let R and K be as in the theorem above. According to [Prasad and Yu 2006, 8.2], a quasireductive group scheme $\mathscr{G}$ is by definition a *good* quasireductive model of its generic fibre G if $\mathscr{G}(R)$ is a hyperspecial parahoric subgroup of $G(K) = \mathscr{G}(K)$. If G admits a good quasireductive model, then it is K-split, by Lemma 8.1 of the same references. Theorems 9.3–9.5 of Prasad and Yu classify all good quasireductive models of G. It is an interesting problem to determine all quasireductive models of a connected K-split reductive group G. For $G = \mathrm{SO}_{2n+1}$, all such models have been determined in Section 10 of the same article.

4. Further remarks

We briefly discuss an analogue of quasireductive group schemes wherein we replace reductive algebraic groups by abelian varieties.

Definition 13. For a scheme S, we call a group scheme $\pi : \mathscr{A} \to S$ *quasiabelian* if it is proper and flat over S and if it is an abelian scheme when restricted to an open dense subset of S.

If all residue fields of S are of characteristic zero then a quasiabelian scheme is necessarily an abelian scheme by Cartier's theorem [SGA 3 I, Exposé VI_{B}, Corollaire 1.6.1].

Now suppose S is the spectrum of a DVR R with residue characteristic $p > 0$ and $\pi : \mathscr{A} \to S$ a quasiabelian scheme. The following statements are in contrast with the quasireductive case.

1. If $\mathscr{A}$ is normal then it is an abelian scheme. This follows from (i) the existence of Néron models and (ii) the fact that for any commutative group scheme $\mathscr{G}$, flat and of finite type over S, the morphism

$$[n] : \mathscr{G} \to \mathscr{G}$$

of multiplication by n, where $n \in \mathbb{Z}$ and $(n, p) = 1$, is étale. (One can use [SGA 3 I, Exposé VI_{A}, p. 316, Proposition] to prove that $[n]$ is flat; it is unramified because n is a unit in R).

Since $\mathscr{A}$ is proper and its geometric special fibre contains no rational curves, it follows that the rational map from $\mathscr{A}'$, the Néron model of $\mathscr{A}$, to $\mathscr{A}$ extending the identity morphism on the generic fibres, is actually a morphism. By examining prime to p torsion (using (ii)) we deduce that the induced morphism on special fibres is dominant, which implies that $\mathscr{A}'$ is an abelian scheme. We then use Zariski's main theorem to conclude.

2. For any prime number p there exists S as above and a quasiabelian scheme over S which is *not* an abelian scheme. Such schemes can be constructed as follows: Let $\mathscr{B}'$, $\mathscr{B}$ be abelian schemes over S and $\phi : \mathscr{B}' \to \mathscr{B}$ a flat isogeny with kernel $\mathscr{K}'$. Suppose there is an abelian subscheme $\mathscr{A}'$ of $\mathscr{B}'$ such that $\mathscr{K}' \cap \mathscr{A}'$ is *not* flat over S. Then $\mathscr{A} := \phi(\mathscr{A}')$ is quasiabelian but not abelian. For any p one may easily find such data with $\mathscr{B}'$ the product of a one dimensional abelian scheme with itself.

One could generalize the definition of quasiabelian schemes by considering group schemes $\pi : \mathscr{A} \to S$ which are flat and of finite type over S, abelian over a dense open subset and such that all reduced geometric fibres are semiabelian. In this generality, we do not know if the analogue of item 1 above continues to hold (though it does if the relative dimension is one since there exist canonical regular compacifications in this case).

Acknowledgement

The second author wishes to thank Gopal Prasad for mentioning the above existence problem, along with a guess that such a group scheme does not exist, and also for explaining the context in which this problem arises. He also thanks Brian Conrad for pointing out a mistake in an earlier version of this paper, and thanks the first author for collaborating with him to correct it. The final topological statement obtained is a bit weaker than what was claimed in the earlier manuscript, but suffices for the application.

Part of the preparation of this paper was done during a visit of the second author to the ETH, Zürich sponsored by FIM; he wishes to thank R. Pink and G. Mislin for some useful discussions, and FIM for supporting his visit.

References

[Borel and Springer 1968] A. Borel and T. A. Springer, "Rationality properties of linear algebraic groups, II", *Tôhoku Math. J.* (2) **20** (1968), 443–497. MR 39 #5576 Zbl 0211.53302

[Borel and Tits 1965] A. Borel and J. Tits, "Groupes réductifs", *Inst. Hautes Études Sci. Publ. Math.* 27 (1965), 55–150. MR 34 #7527 Zbl 0395.20024

[Conrad 2006] B. Conrad, "Appendix to [Prasad and Yu 2006]", 2006.

[EGA 6] A. Grothendieck, "Éléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, II", *Inst. Hautes Études Sci. Publ. Math.* 24 (1965), 1–231. MR 33 #7330 Zbl 0135.39701

[Mirković and Vilonen 2004] I. Mirković and K. Vilonen, "Geometric Langlands duality and representations of algebraic groups over commutative rings", preprint, 2004. arXiv math/0410222

[Oesterlé 1984] J. Oesterlé, "Nombres de Tamagawa et groupes unipotents en caractéristique p", *Invent. Math.* **78**:1 (1984), 13–88. MR 86i:11016 Zbl 0542.20024

[Prasad and Yu 2006] G. Prasad and J.-K. Yu, "On quasireductive group schemes", *J. Algebraic Geom.* **15**:3 (2006), 507–549. MR 2007c:14047 Zbl 1112.14053

[Raynaud 1968] M. Raynaud, "Modules projectifs universels", *Invent. Math.* **6** (1968), 1–26. MR 38 #4462 Zbl 0216.32601

[Serre and Tate 1968] J.-P. Serre and J. Tate, "Good reduction of abelian varieties", *Ann. of Math.* (2) **88** (1968), 492–517. MR 38 #4488 Zbl 0172.46101

[SGA 3 I] M. Demazure and A. Grothendieck (editors), *Schémas en groupes, I: Propriétés générales des schémas en groupes* (Séminaire de Géométrie Algébrique du Bois Marie 1962/64 = SGA 3 I), Lecture Notes in Math. **151**, Springer, Berlin, 1970. MR 43 #223a Zbl 0207.51401

[SGA 3 II] M. Demazure and A. Grothendieck (editors), *Schémas en groupes, II: Groupes de type multiplicatif, et structure des schémas en groupes généraux* (Séminaire de Géométrie Algébrique du Bois Marie 1962/64 = SGA 3 II), Lecture Notes in Math. **152**, Springer, Berlin, 1970. MR 43 #223b Zbl 0209.24201

[SGA 3 III] M. Demazure and A. Grothendieck (editors), *Schémas en groupes. III: Structure des schémas en groupes réductifs* (Séminaire de Géométrie Algébrique du Bois Marie 1962/64 = SGA 3 III), Lecture Notes in Math. **153**, Springer, Berlin, 1970. MR 43 #223c Zbl 0212.52810

[SGA 4 II] M. Artin, A. Grothendieck, and J. L. Verdier (editors), *Théorie des topos et cohomologie étale des schémas. Tome 2. Exposes V à VIII.* (Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4)), Lecture Notes in Math. **270**, Springer, Berlin, 1972. MR 50 #7131 Zbl 0237.00012

[SGA 5] P. Deligne, *Cohomologie l-adique et fonctions L* (Séminaire de Géométrie Algébrique du Bois-Marie = SGA 5), Lecture Notes in Math. **589**, Springer, Berlin, 1977. MR 57 #3132 Zbl 0349.14008

[SGA 7 II] P. Deligne and N. Katz (editors), *Groupes de monodromie en géométrie algébrique, II* (Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 = SGA 7 II), Lecture Notes in Math. **340**, Springer, Berlin, 1973. MR 50 #7135 Zbl 0258.00005

[Steinberg 1965] R. Steinberg, "Regular elements of semisimple algebraic groups", *Inst. Hautes Études Sci. Publ. Math.* 25 (1965), 49–80. MR 31 #4788 Zbl 0136.30002

Communicated by Brian D. Conrad
Received 2007-03-12 Revised 2007-07-25 Accepted 2007-08-25

naf@math.tifr.res.in *School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Colaba, Mumbai-400005, India*

srinivas@math.tifr.res.in *School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Colaba, Mumbai-400005, India*

Piecewise polynomials, Minkowski weights, and localization on toric varieties

Eric Katz and Sam Payne

We use localization to describe the restriction map from equivariant Chow cohomology to ordinary Chow cohomology for complete toric varieties in terms of piecewise polynomial functions and Minkowski weights. We compute examples showing that this map is not surjective in general, and that its kernel is not always generated in degree one. We prove a localization formula for mixed volumes of lattice polytopes and, more generally, a Bott residue formula for toric vector bundles.

1. Introduction

Let Δ be a complete fan in $N_{\mathbb{R}}$, where N is a lattice of rank n, and let $X = X(\Delta)$ be the corresponding complete n-dimensional toric variety. See [Fulton 1993] for standard notation and general background on toric varieties. The equivariant operational Chow cohomology ring with integer coefficients $A_T^*(X)$ is naturally isomorphic to the ring of integral piecewise polynomial functions on Δ [Payne 2006a], and there is a canonical map to ordinary Chow cohomology with integer coefficients

$$\iota^* : A_T^*(X) \to A^*(X)$$

induced by inclusions of X in the finite dimensional approximations of the Borel mixed space [Edidin and Graham 1998a]. Now $A^*(X)$ is naturally isomorphic to the ring of Minkowski weights on Δ [Fulton and Sturmfels 1997], and ι^* has a natural interpretation in terms of localization and equivariant multiplicities, as follows.

Let $M = \operatorname{Hom}(N, \mathbb{Z})$, which is naturally identified with the character lattice of T, and let $\operatorname{Sym}^{\pm}(M)$ be the $\mathbb{Z}$-graded ring obtained by inverting all of the homogeneous elements in the ring $\operatorname{Sym}^*(M)$ of polynomials with integer coefficients. We refer to elements of $\operatorname{Sym}^{\pm}(M)$ as rational functions, and elements of

MSC2000: primary 14M25; secondary 14C17, 52B20.

Keywords: toric variety, localization, tropical geometry, piecewise polynomial, Minkowski weight.

Payne was supported by the Clay Mathematics Institute. Part of this research was done during his visit to the Institut Mittag-Leffler (Djursholm, Sweden).

the subring $\mathrm{Sym}^*(M)$ as polynomials. Each maximal cone $\sigma \in \Delta$ corresponds to a nondegenerate torus fixed point $x_\sigma \in X$, which has an "equivariant multiplicity" $e_{x_\sigma}[X] \in \mathrm{Sym}^{\pm}(M)$, which is a homogeneous rational function of degree $-n$. Since every rational polyhedral cone admits a unimodular subdivision, these equivariant multiplicities are determined by the following two properties.

(1) If $\sigma_1, \ldots, \sigma_r$ are the maximal cones of a rational polyhedral subdivision of a cone σ, then
$$e_{x_\sigma}[X] = e_{x_{\sigma_1}}[X] + \cdots + e_{x_{\sigma_r}}[X].$$

(2) If σ is a unimodular cone, spanned by a basis $e_1, \ldots, e_n$ for N, then
$$e_{x_\sigma}[X] = \frac{1}{e_1^* \cdots e_n^*}\ .$$

The fact that the sum of rational functions determined by (1) and (2) is independent of the choice of unimodular subdivision is not obvious from elementary considerations, though it follows directly from the theory of localization at torus fixed points in algebraic geometry [Edidin and Graham 1998b] and the theory of equivariant multiplicities developed by Rossmann [1989] and Brion [1997, Theorem 4.2 and Proposition 4.3, in particular]. Here we give a combinatorial proof of this independence; the techniques of this proof may be of independent interest. We view the multigraded Hilbert function $\mathrm{Hilb}(\sigma)$ of the affine toric variety U_σ, given by
$$\mathrm{Hilb}(\sigma) = \sum_{u \in (\sigma^* \cap M)} x^u\ ,$$
as a rational function on the dense torus $T \subset X$. We define e_σ to be $(-1)^n$ times the quotient of the leading forms when $\mathrm{Hilb}(\sigma)$ is written as a quotient of two polynomials in local coordinates at the identity 1_T. We then show that e_σ satisfies properties analogous to (1) and (2) and therefore is equal to $e_{x_\sigma}[X]$. See Section 2 for details. Our approach is inspired by the presentation of multidegrees of multigraded modules over polynomial rings in [Knutson and Miller 2005, Sections 1.2 and 1.7] and [Miller and Sturmfels 2005, Chapter 8].

Recall that the ring of integral piecewise polynomial functions $PP^*(\Delta)$ is the ring of continuous functions $f : |\Delta| \to \mathbb{R}$ such that the restriction f_σ of f to each maximal cone $\sigma \in \Delta$ is a polynomial in $\mathrm{Sym}^*(M)$.

Proposition 1.1. *Let Δ be a complete n-dimensional fan, and let $f \in PP^k(\Delta)$ be a piecewise polynomial function. Then*
$$\sum_\sigma e_\sigma f_\sigma$$
is a homogeneous polynomial in $\mathrm{Sym}^*(M)$ *of degree $k - n$.*

In particular, if the degree of f is less than n then $\sum e_\sigma f_\sigma$ vanishes. If $\deg f = n$, then $\sum e_\sigma f_\sigma = d$ is an integer, which may be identified with the codimension n Minkowski weight $c(0) = d$ on Δ.

Minkowski weights of codimension less than n may be constructed similarly from piecewise polynomials using equivariant multiplicities, as follows. For any cone $\tau \in \Delta$, let Δ_τ be the fan in $(N/(N \cap \operatorname{span}\tau))_{\mathbb{R}}$ whose cones are the projections of the cones in Δ that contain τ. If σ is a maximal such cone, we define $e_{\sigma,\tau}$ to be $e_{\bar{\sigma}}$, where $\bar{\sigma}$ is the image of σ in Δ_τ. So $e_{\sigma,\tau}$ is a homogeneous rational function of degree $(\dim\tau - n)$ in the graded subring $\operatorname{Sym}^{\pm}(\tau^{\perp} \cap M)$ of $\operatorname{Sym}^{\pm}(M)$.

Proposition 1.2. *Let Δ be a complete fan, and let $f \in PP^k(\Delta)$ be a piecewise polynomial function. Then, for any $\tau \in \Delta$,*

$$c(\tau) = \sum_{\sigma \succeq \tau} e_{\sigma,\tau} f_\sigma$$

is a homogeneous polynomial in $\operatorname{Sym}^*(M)$ *of degree* $k + \dim\tau - n$.

If $k \leq n$ then $c(\tau)$ is an integer for every codimension k cone in Δ, and these integers are a Minkowski weight of codimension k. Propositions 1.1 and 1.2 are proved in Section 3 using elementary properties of generating functions for lattice points in polyhedral cones.

Remark 1.3. Proposition 1.1 is the special case of Proposition 1.2 where $\tau = 0$. The essential content of Propositions 1.1 and 1.2 is that the denominator of the sum must divide the numerator. In some special cases, this divisibility may be seen as a consequence of Brion's Formula, and its generalizations, in the theory of generating functions for lattice points in polyhedra. See Section 5 below. Other special cases of these cancellations appeared earlier in [Brion 1996]; in particular, Brion showed that $\sum e_{\sigma,\tau} f_\sigma$ is in $\operatorname{Sym}^*(M_{\mathbb{Q}})$ when Δ is simplicial.

Theorem 1.4. *The natural map $\iota^* : A_T^k(X) \to A^k(X)$ takes the equivariant Chow cohomology class corresponding to a piecewise polynomial function f to the ordinary Chow cohomology class corresponding to the Minkowski weight c given by*

$$c(\tau) = \sum_{\sigma \succeq \tau} e_{\sigma,\tau} f_\sigma,$$

for all codimension k cones $\tau \in \Delta$.

We prove Theorem 1.4 in Section 3 by interpreting Propositions 1.1 and 1.2 in terms of general localization formulas in equivariant Chow cohomology [Edidin and Graham 1998b].

We apply Theorem 1.4 to study the map $\iota^* : A^*_T(X) \to A^*(X)$. Recall that if X is smooth then capping with the fundamental class of X gives isomorphisms

$$A^*(X) \cong A_{n-*}(X) \text{ and } A^*_T(X) \cong A^T_{n-*}(X).$$

Furthermore, the globally linear functions $u \in M$, identified with the equivariant first Chern classes of the toric line bundles $\mathbb{O}(\operatorname{div} \chi^u)$, act on $A^T_*(X)$ as homogeneous operators of degree -1, and there is a natural isomorphism to ordinary Chow homology [Brion 1997, Section 2.3],

$$A^T_*(X)/MA^T_*(X) \cong A_*(X).$$

It follows that if X is a smooth toric variety then ι^* is surjective and its kernel is generated by M in degree one. Similar arguments show that if X is simplicial, then ι^* becomes surjective after tensoring with $\mathbb{Q}$, with kernel generated by $M_{\mathbb{Q}}$ in degree one.

Theorem 1.5. *There exist projective toric surfaces X such that $\iota^* : A^2_T(X) \to A^2(X)$ is not surjective.*

In particular, even when the natural map $PP^*(\Delta)/(M) \to A^*(X)$ becomes an isomorphism after tensoring with $\mathbb{Q}$, it need not be an isomorphism over $\mathbb{Z}$.

Theorem 1.6. *There exist projective toric threefolds X such that $\iota^* : A^*_T(X)_{\mathbb{Q}} \to A^*(X)_{\mathbb{Q}}$ is not surjective and its kernel is not generated in degree one.*

It follows that the natural map from piecewise polynomials modulo linear functions to Minkowski weights is neither injective nor surjective in general. We prove Theorems 1.5 and 1.6 in Section 4 by computing the maps $A^*_T(X) \to A^*(X)$ for several examples of singular toric varieties using Theorem 1.4.

Remark 1.7. Minkowski weights on Δ, and classes in $A^*(X)$, correspond to tropical varieties supported on the cones of Δ, and are of significant interest in tropical geometry [Katz 2007, Section 9; Mikhalkin 2006, p. 10]. The desire to use piecewise polynomials to produce interesting examples of Minkowski weights was one of the main motivations for this research. We hope and expect that the combinatorial localization techniques developed here will be useful in tropical geometry.

2. Combinatorics of equivariant multiplicities

Let N be a lattice of rank n, and let $M = \operatorname{Hom}(N, \mathbb{Z})$ be its dual lattice. Let $\operatorname{Poly}(N)$ denote the rational polytope algebra on $N_{\mathbb{R}}$, the subring of real-valued functions on $N_{\mathbb{R}}$ generated by the characteristic functions of closed rational polyhedra. We write $[Q] \in \operatorname{Poly}(N)$ for the characteristic function of a closed polyhedron Q. Recall that Q has a polar dual Q^*, which is a closed polyhedron in $M_{\mathbb{R}}$, defined by

$$Q^* = \{\, u \in M_{\mathbb{R}} \mid \langle u, v\rangle \geq -1 \text{ for all } v \in Q \,\},$$

and there is a linear map from $\mathrm{Poly}(N)$ to $\mathrm{Poly}(M)$ given by $[Q] \mapsto [Q^*]$ [Lawrence 1988]. Furthermore, there is a linear map

$$\nu : \mathrm{Poly}(M) \to \mathbb{Q}(M),$$

to the quotient field $\mathbb{Q}(M)$ of the multivariate Laurent polynomial ring $\mathbb{Z}[M]$, that takes the class of a closed, pointed polyhedron P to the generating function $\sum_{u \in (P \cap M)} x^u$, expressed as a rational function, and takes the class of a polyhedron containing a line to 0 [Barvinok 2002, Theorem VIII.3.3]. In particular, for any closed polyhedral cone σ in $N_{\mathbb{R}}$, $\nu(\sigma^*) = \mathrm{Hilb}(\sigma)$, where

$$\mathrm{Hilb}(\sigma) = \sum_{u \in (\sigma^* \cap M)} x^u$$

is the multigraded Hilbert series of the affine toric variety U_σ. Composing polar duality with the valuation ν then gives a linear map

$$\nu^* : \mathrm{Poly}(N) \to \mathbb{Q}(M)$$

that takes $[\sigma]$ to $\mathrm{Hilb}(\sigma)$.

Lemma 2.1. *If $\sigma_1, \dots, \sigma_r$ are the maximal cones in a rational polyhedral subdivision of an n-dimensional cone σ, then*

$$\mathrm{Hilb}(\sigma) = \mathrm{Hilb}(\sigma_1) + \cdots + \mathrm{Hilb}(\sigma_r).$$

Proof. In the polytope algebra $\mathrm{Poly}(N)$,

$$[\sigma] = [\sigma_1] + \cdots + [\sigma_r] \pm \text{ classes of lower dimensional cones.}$$

Since the duals of lower dimensional cones contain lines, these terms are all in the kernel of ν^*. Therefore, $\nu^*([\sigma]) = \nu^*([\sigma_1]) + \cdots + \nu^*([\sigma_r])$, and the lemma follows. □

The generating function $\mathrm{Hilb}(\sigma)$, being an element of $\mathbb{Q}(M)$, is naturally interpreted as a rational function on the torus $T = \mathrm{Spec}\, \mathbb{Q}[M]$. Therefore, $\mathrm{Hilb}(\sigma)$ may be expanded as a quotient of two power series in local parameters at the identity 1_T. The principal part of this expansion, the quotient of the leading forms, which we denote by

$$\mathrm{Hilb}(\sigma)_\circ \in \mathrm{Sym}^{\pm}(M_{\mathbb{Q}}),$$

is a rational function on the tangent space of T at 1_T, which cuts out the tangent cone of zeros of $\mathrm{Hilb}(\sigma)$ minus the tangent cone of its poles. See the Appendix for details on principal parts of rational functions.

Definition 2.2. If σ is an n-dimensional rational polyhedral cone in $N_{\mathbb{R}}$ then

$$e_\sigma = (-1)^n \cdot \mathrm{Hilb}(\sigma)_\circ.$$

Lemma 2.3. *If σ is an n-dimensional rational polyhedral cone in $N_{\mathbb{R}}$, then e_σ is homogeneous of degree $-n$.*

Proof. The lemma follows directly from closed formulas for polyhedral generating functions, such as those given in [Payne 2007], as follows. Suppose Σ is a unimodular subdivision of σ^*, and $u_1, \dots, u_s$ are the primitive generators of the rays of Σ. Then every lattice point in σ^* lies in the relative interior of a unique cone $\tau \in \Sigma$, and the generating function for those in the relative interior of τ is $\prod_{u_i \in \tau} x^{u_i}/(1-x^{u_i})$. Therefore,

$$(1-x^{u_1})\cdots(1-x^{u_s})\cdot \operatorname{Hilb}(\sigma) = \sum_{\tau\in\Sigma}\Bigl(\prod_{u_i\in\tau} x^{u_i} \prod_{u_j\notin\tau}(1-x^{u_j})\Bigr).$$

If $\tau_1, \dots, \tau_r$ are the maximal cones of Σ, then taking leading forms at 1_T on both sides gives

$$u_1\cdots u_s \cdot (-1)^n \cdot \operatorname{Hilb}(\sigma)_\circ = \sum_{i=1}^{r} \prod_{u_j\notin\tau_i} u_j,$$

provided that the right hand side is nonvanishing. Since all of the u_j lie in σ^*, the right hand side is strictly positive on the interior of σ. In particular, it does not vanish, so the degree of $\operatorname{Hilb}(\sigma)_\circ$ is $-n$. □

Lemma 2.3 can also be seen as a special case of more general results on multigraded Hilbert series of modules. See [Miller and Sturmfels 2005, Definition 8.45 and Claim 8.54].

Lemma 2.4. *Let σ be a unimodular cone, spanned by a basis $e_1, \dots, e_n$ for N. Then the principal part of* $\operatorname{Hilb}(\sigma)$ *at 1_T is*

$$\operatorname{Hilb}(\sigma)_\circ = \frac{(-1)^n}{e_1^*\cdots e_n^*},$$

where $e_1^*, \dots, e_n^*$ is the dual basis for M.

Proof. The generating function $\operatorname{Hilb}(\sigma)$ is given by

$$\operatorname{Hilb}(\sigma) = \frac{1}{(1-x^{e_1^*})\cdots(1-x^{e_n^*})}.$$

Now, $(1-x^{e_i^*})$ is a local parameter at 1_T, with principal part $(1-x^{e_i^*})_\circ = -e_i^*$. Since principal parts are multiplicative, it follows that the principal part of $1/(1-x^{e_i^*})$ is $-1/e_i^*$, and the lemma follows. □

Proposition 2.5. *Let σ be an n-dimensional rational polyhedral cone in $N_{\mathbb{R}}$.*

(1) *If $\sigma_1, \dots, \sigma_r$ are the maximal cones in a rational polyhedral subdivision of σ, then*

$$e_\sigma = e_{\sigma_1} + \cdots + e_{\sigma_r}.$$

(2) *If σ is unimodular, spanned by a basis $e_1, \ldots, e_n$ for N, then*

$$e_\sigma = \frac{1}{e_1^* \cdots e_n^*} .$$

In particular, the sum determined by (1) and (2) is independent of the choice of unimodular subdivision.

Proof. Part (1) follows from the additivity of $\mathrm{Hilb}(\sigma_i)$ (Lemma 2.1) and the fact that $\mathrm{Hilb}(\sigma)$ and the $\mathrm{Hilb}(\sigma_i)$ all have principal parts in degree $-n$ (Lemma 2.3). See Proposition A.1, in the Appendix. Part (2) is an immediate consequence of Lemma 2.4. □

Recall that for any cone $\tau \in \Delta$, Δ_τ is the fan in $(N/(N \cap \operatorname{span} \tau))_{\mathbb{R}}$ whose cones are the projections of the cones in Δ that contain τ. If σ is a maximal cone containing τ, we define $e_{\sigma,\tau}$ to be $e_{\overline{\sigma}}$, where $\overline{\sigma}$ is the image of σ in Δ_τ. So $e_{\sigma,\tau}$ is a homogeneous rational function of degree $(\dim \tau - n)$ in the graded subring $\mathrm{Sym}^{\pm}(\tau^{\perp} \cap M)$ of $\mathrm{Sym}^{\pm}(M)$. We write $V(\tau)$ for the T-invariant subvariety of X corresponding to τ.

Corollary 2.6. *If σ is an n-dimensional rational polyhedral cone in $N_{\mathbb{R}}$ and τ is a face of σ, then*

$$e_\sigma = e_{x_\sigma}[X] \ \text{ and } \ e_{\sigma,\tau} = e_{x_\sigma}[V(\tau)].$$

Lemma 2.7. *If σ is a unimodular cone spanned by a basis $e_1, \ldots, e_n$ for N and $\tau \preceq \sigma$ then*

$$e_{\sigma,\tau} = \prod_{e_i \notin \tau} \frac{1}{e_i^*}.$$

Proof. Apply part (2) of Proposition 2.5 to the fan Δ_τ. □

3. Localization and Minkowski weights

Here we use equivariant multiplicities to describe the natural map from piecewise polynomials on a complete fan to Minkowski weights. We then use localization to show that this map agrees with $\iota^* : A_T^*(X) \to A^*(X)$.

Lemma 3.1. *Let Δ be a complete n-dimensional fan. Then the sum of the rational functions e_σ for all maximal cones $\sigma \in \Delta$ is given by*

$$\sum_\sigma e_\sigma = \begin{cases} 0 & \text{for } n \geq 1, \\ 1 & \text{for } n = 0. \end{cases}$$

Proof. If $n = 0$, then Δ contains only one cone 0, and $e_0 = 1$. Suppose $n \geq 1$. In the polytope algebra ,

$$\sum_{\sigma} [\sigma] = [N_{\mathbb{R}}] \pm \text{ classes of smaller dimensional cones.}$$

Applying the linear transformation ν^* gives

$$\sum_{\sigma} \mathrm{Hilb}(\sigma) = 1.$$

Since each of the principal parts $\mathrm{Hilb}(\sigma)_\circ = (-1)^n \cdot e_\sigma$ is homogeneous of degree $-n$, it follows that the sum of these principal parts must vanish by Proposition A.1 in the Appendix, and the lemma follows. □

Lemma 3.2. *Let τ be a cone in a complete n-dimensional fan Δ. Then*

$$\sum_{\sigma \succeq \tau} e_{\sigma,\tau} = \begin{cases} 0 & \textit{for } \dim \tau < n, \\ 1 & \textit{for } \dim \tau = n. \end{cases}$$

Proof. Apply Lemma 3.1 to the fan Δ_τ. □

Piecewise polynomials are especially well-behaved on unimodular fans, that is, fans in which each maximal cone is spanned by a basis for the lattice. Suppose Δ is a unimodular fan, and $\rho_1, \ldots, \rho_s$ are the rays of Δ. Let v_i be the primitive generator of ρ_i. Then there is a unique piecewise linear function $\Psi_i \in PP^1(\Delta)$ whose values at the primitive generators of the rays are given by the Kronecker delta function

$$\Psi_i(v_j) = \delta_{ij},$$

and whose values elsewhere are given by extending linearly on each cone.

Then, for any k-dimensional cone $\tau \in \Delta$, we have a piecewise polynomial $\Psi_\tau \in PP^k(\Delta)$ that vanishes away from $\mathrm{Star}(\tau)$, the union of the cones in Δ that contain τ, defined by

$$\Psi_\tau = \prod_{v_i \in \tau} \Psi_i,$$

and $PP^*(\Delta)$ is generated by $\{\Psi_\tau\}_{\tau \in \Delta}$ as a $\mathrm{Sym}^*(M)$-module.

Proof of Proposition 1.1. Since equivariant multiplicities are additive with respect to subdivisions, we may assume that Δ is unimodular. Say $\rho_1, \ldots, \rho_s$ are the rays of Δ and v_i is the primitive generator of ρ_i. Since $PP^*(\Delta)$ is generated as a $\mathrm{Sym}^*(M)$-module by the piecewise polynomials Ψ_τ, it suffices to prove that

$$\sum e_\sigma \cdot (\Psi_\tau)_\sigma$$

is in $\mathrm{Sym}^*(M)$ for all τ. Now, if σ is spanned by a basis $e_1, \dots, e_n$ for N and $\tau \preceq \sigma$, then $(\Psi_\tau)_\sigma = \prod_{v_i \in \tau} e_i^*$. It then follows from Lemma 2.7 that

$$e_\sigma \cdot (\Psi_\tau)_\sigma = \begin{cases} e_{\sigma,\tau} & \text{for } \sigma \succeq \tau, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, by Lemma 3.2, $\sum e_\sigma \cdot (\Psi_\tau)_\sigma$ vanishes unless τ is a maximal cone, in which case the sum is equal to one. In particular, $\sum e_\sigma \cdot (\Psi_\tau)_\sigma$ is in $\mathrm{Sym}^*(M)$, as required. □

Proof of Proposition 1.2. The sum in Proposition 1.2 is over the maximal cones in $\mathrm{Star}(\tau)$. Then the proof of Proposition 1.2 is similar to the proof of Proposition 1.1, since $PP^*(\mathrm{Star}(\tau))$ is generated as a $\mathrm{Sym}^*(M)$-module by the restrictions of the piecewise polynomial functions Ψ_γ, for $\gamma \in \mathrm{Star}(\tau)$. □

It remains to show that if f is a homogeneous piecewise polynomial of degree k, then the integer-valued function c on codimension k cones of Δ given by

$$c(\tau) = \sum_{\sigma \succeq \tau} e_{\sigma,\tau} f_\sigma$$

is a Minkowski weight of codimension k, and that $f \mapsto c$ agrees with the natural map $\iota^* : A_T^*(X) \to A^*(X)$. Although the entire statement can be proved using the general machinery of localization, the fact that the integers $c(\tau)$ give a Minkowski weight is purely combinatorial, and we include an elementary proof.

We recall the definition of Minkowski weights from [Fulton and Sturmfels 1997]. If γ is a codimension $k+1$ cone in Δ contained in a codimension k cone τ, we write $v_{\tau/\gamma} \in N/(N \cap \mathrm{span}\, \gamma)$ for the primitive generator of the image of τ in Δ_γ.

Definition 3.3. An integer valued function c on codimension k cones $\tau \in \Delta$ is a Minkowski weight if, for every codimension $k+1$ cone $\gamma \in \Delta$,

$$\sum_{\tau \succeq \gamma} c(\tau) \cdot v_{\tau/\gamma} = 0.$$

We will use the following basic property of equivariant multiplicities to show that the integer-valued function c coming from a piecewise polynomial function is a Minkowski weight. Let v_ρ denote the primitive generator of a ray ρ.

Proposition 3.4. *If σ is an n-dimensional rational polyhedral cone in $N_\mathbb{R}$ and u is in M then*

$$\sum_{\rho \preceq \sigma} \langle u, v_\rho \rangle \cdot e_{\sigma,\rho} = u \cdot e_\sigma.$$

We will prove the proposition by subdividing σ and reducing to the case where σ is unimodular.

Lemma 3.5. *If σ is an n-dimensional unimodular cone in $N_{\mathbb{R}}$ and u is in M then*

$$\sum_{\rho \preceq \sigma} \langle u, v_\rho \rangle \cdot e_{\sigma,\rho} = u \cdot e_\sigma .$$

Proof. Say σ is spanned by a basis $e_1, \dots, e_n$ for N, and $u = u_1 e_1^* + \cdots u_n e_n^*$. Then

$$\sum \langle u, v_\rho \rangle \cdot e_{\sigma,\rho} = \sum_{i=1}^{n} \frac{u_i}{e_1^* \cdots \widehat{e_i^*} \cdots e_n^*},$$

which is equal to $u \cdot e_\sigma$. □

Lemma 3.6. *If $\sigma_1, \dots, \sigma_s$ are the maximal cones in a subdivision of σ, and if ρ is a ray in this subdivision then*

$$\sum_{\sigma_i \succeq \rho} e_{\sigma_i,\rho} = \begin{cases} e_{\sigma,\rho} & \textit{if } \rho \preceq \sigma, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. Suppose ρ lies in the relative interior of a k-dimensional face $\tau \preceq \sigma$. Consider the fan Δ_ρ, whose maximal cones are the images of the $\sigma_i \succeq \rho$. The support $|\Delta_\rho|$ is a closed polyhedral cone in an $(n-1)$-dimensional vector space whose minimal face is $(k-1)$-dimensional, so the polar dual $|\Delta_\rho|^*$ has dimension $n-k$. It follows that the principal part of $\nu^*(|\Delta_\rho|)$ has degree $k-n$. Since each $e_{\sigma,\rho}$ has degree $1-n$, and $\sum e_{\sigma_i,\rho}$ is the principal part of $\pm\nu^*(|\Delta_\rho|)$ unless this sum vanishes (Appendix, Proposition A.1), the lemma follows. □

Proof of Proposition 3.4. Let $\sigma_1, \dots, \sigma_r$ be the maximal cones of a unimodular subdivision of σ. Then $u \cdot e_\sigma = u \cdot e_{\sigma_1} + \cdots + u \cdot e_{\sigma_r}$. Since σ_i is unimodular,

$$u \cdot e_{\sigma_i} = \sum_{\rho \preceq \sigma_i} \langle u, v_\rho \rangle e_{\sigma_i,\rho} .$$

Therefore, by rearranging terms in the summation, we have

$$u \cdot e_\sigma = \sum_{\rho} \Big(\sum_{\sigma_i \succeq \rho} \langle u, v_\rho \rangle \cdot e_{\sigma_i,\rho} \Big).$$

By Lemma 3.6, the right hand side is equal to $\sum_{\rho \preceq \sigma} e_{\sigma,\rho}$, as required. □

Proposition 3.7. *Let $f \in PP^k(\Delta)$ be a homogeneous piecewise polynomial of degree k. Then the integers*

$$c(\tau) = \sum_{\sigma \succeq \tau} e_{\sigma,\tau} f_\sigma$$

are a Minkowski weight of codimension k on Δ.

Proof. Let γ be a codimension $k+1$ cone in Δ. It will suffice to show that $\sum\langle u, v_{\tau/\gamma}\rangle c(\tau)=0$ for any $u\in(M\cap\gamma^{\perp})$, where the sum is over all codimension k cones τ containing γ. To prove this, we will show that $\sum\langle u, v_{\tau/\gamma}\rangle c(\tau)$, which is an integer by Proposition 1.2, is divisible by the linear function u in $\mathrm{Sym}^*(M)$. Now,

$$\sum_{\tau}\langle u, v_{\tau/\gamma}\rangle\, c(\tau)=\sum_{\tau}\Big(\sum_{\sigma\succeq\tau}\langle u, v_{\tau/\gamma}\rangle\, e_{\sigma,\tau}\, f_{\sigma}\Big),$$

and the sum on the right hand side may be rearranged as

$$\sum_{\sigma}\Big(f_{\sigma}\cdot\sum_{\tau\preceq\sigma}\langle u, v_{\tau/\gamma}\rangle\, e_{\sigma,\tau}\Big).$$

Applying Proposition 3.4 to Δ_{γ} then gives

$$\sum_{\tau\preceq\sigma}\langle u, v_{\tau/\gamma}\rangle\, e_{\sigma,\tau}=u\cdot e_{\sigma,\gamma}.$$

It follows that the integer $\sum\langle u, v_{\tau/\gamma}\rangle c(\tau)$ is divisible by u in $\mathrm{Sym}^*(M)$, as claimed, and hence must vanish. □

Proof of Theorem 1.4. To show that $f\mapsto c$ agrees with the natural map $\iota^*: A_T^*(X)\to A^*(X)$, we must prove that

$$\int_{V(\tau)}\iota^* c_f=c(\tau),$$

where c_f denotes the equivariant Chow cohomology class whose restriction to a torus fixed point is $f_{\sigma}\in\mathrm{Sym}^*(M)\cong A_T^*(x_{\sigma})$. By Corollary 2.6, $e_{\sigma,\tau}$ is equal to the equivariant multiplicity $e_{x_{\sigma}}[V(\tau)]$ of the nondegenerate T-fixed point x_{σ} in $V(\tau)$. Therefore, by localization [Edidin and Graham 1998b], in equivariant Chow homology tensored with $\mathrm{Sym}^{\pm}(M)$, we have

$$\int_{V(\tau)}c_f=\sum_{\sigma}e_{\sigma}f_{\sigma}.$$

Since $\sum_{\sigma}e_{\sigma}f_{\sigma}$ is an integer, projecting to $A_*(X)$ gives $\int_{V(\tau)}\iota^*c_f=c(\tau)$. □

4. Applications to Chow cohomology of toric varieties

Here we use combinatorial computations with piecewise polynomials to study the map $\iota^*: A_T^*(X)\to A^*(X)$ for some specific complete toric varieties X. As discussed in the introduction, this map is known to be surjective with kernel generated by M in degree one if X is smooth, and similar statements hold over $\mathbb{Q}$ if X is simplicial. We give the first examples showing that ι^* is not surjective in general, and that its kernel is not always generated in degree one.

Example 4.1 (Mirror dual of $\mathbb{P}^1 \times \mathbb{P}^1$). Let $N = \mathbb{Z}^2$, and let Δ be the complete fan in $\mathbb{R}^2$ whose rays are generated by

$$v_1 = (1, 1), \;\; v_2 = (1, -1), \;\; v_3 = (-1, -1), \;\; v_4 = (-1, 1),$$

and whose maximal cones are

$$\sigma_1 = \langle v_1, v_2\rangle, \;\; \sigma_2 = \langle v_2, v_3\rangle, \;\; \sigma_3 = \langle v_3, v_4\rangle, \;\; \sigma_4 = \langle v_1, v_4\rangle.$$

Then $X = X(\Delta)$ is isomorphic to $(\mathbb{P}^1 \times \mathbb{P}^1)/\mathbb{Z}_2$, which is the Fano surface that is "mirror dual" to $\mathbb{P}^1 \times \mathbb{P}^1$.

We claim that the image of $PP^2(X)$ under the map $f \mapsto \sum_{i=1}^4 e_{\sigma_i} f_{\sigma_i}$ is exactly $2\mathbb{Z}$. We compute $e(\sigma_1)$ using the unimodular subdivision of σ_1 along $v = (1, 0)$,

$$\sigma_1 = \langle v_1, v\rangle \cup \langle v, v_2\rangle.$$

Then, writing $a = e_1^*$ and $b = e_2^*$, the dual cones of $\langle v_1, v\rangle$ and $\langle v, v_2\rangle$ are $\langle b, a - b\rangle$ and $\langle b, a + b\rangle$, respectively, so

$$e(x_1) = \frac{1}{b(a-b)} - \frac{1}{b(a+b)} = \frac{2}{a^2 - b^2}.$$

Similarly, we compute $e(\sigma_3) = 2/(a^2 - b^2)$ and

$$e(\sigma_2) = e(\sigma_4) = \frac{-2}{a^2 - b^2}.$$

Therefore, since two divides every term in $\sum_{i=1}^4 e_{\sigma_i} f_{\sigma_i}$, the sum must be divisible by two. Also, the piecewise polynomial function f that vanishes on $\sigma_2 \cup \sigma_3 \cup \sigma_4$ and whose restriction to σ_1 is $a^2 - b^2$ maps to two. So the image of $PP^2(\Delta)$ is $2\mathbb{Z}$, as required.

Proof of Theorem 1.5. Applying Theorem 1.4 to Example 4.1 shows that the image of $\iota^* : A_T^2(X) \to A^2(X)$ is $2A^2(X)$, which is a proper subgroup of $A^2(X) \cong \mathbb{Z}$. □

In the following examples, we consider fans in $\mathbb{R}^3$ with respect to the lattice $N = \mathbb{Z}^3$.

Example 4.2 (Mirror dual of $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$). Consider the toric variety $X = X(\Delta)$, where Δ is the fan whose nonzero cones are the cones over the faces of the cube with vertices $(\pm 1, \pm 1, \pm 1)$. Then X is the Fano toric threefold that is "mirror dual" to $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$. Recall that, since X is complete, the rank of $A^i(X)$ is equal to the rank of $A_i(X)$ [Fulton and Sturmfels 1997, Proposition 2.4], so $\operatorname{rk} A^0(X) = \operatorname{rk} A^3(X) = 1$. Furthermore, since $A_2(X)$ is the Weil divisor class group of X, we also have $\operatorname{rk} A^2(X) = 5$. The remainder of the following table can be filled in by straightforward linear algebra computations with piecewise polynomial functions.

From these computations, it is clear that $A_T^2(X)$ does not surject onto $A^2(X)$, since its image has rank at most two.

	$\operatorname{rk} A_T^i(X)$	$\operatorname{rk} M \cdot A_T^{i-1}(X)$	$\operatorname{rk} A^i(X)$
$i=0$	1	0	1
$i=1$	4	3	1
$i=2$	11	9	5
$i=3$	23	22	1

Example 4.3 (Fulton's threefold). Consider the toric variety $X' = X(\Delta')$, where Δ' is the fan combinatorially equivalent to the fan over the cube as in the preceding example, but with the ray through $(1,1,1)$ replaced by the ray through $(1,2,3)$. Then X' is complete and, as in the previous example, $\operatorname{rk} A^0(X') = \operatorname{rk} A^3(X') = 1$, and $\operatorname{rk} A^2(X') = 5$, but Fulton showed that X' has no nontrivial line bundles [Fulton 1993, pp. 25–26], so $A^1(X') = 0$. The remainder of the following table is filled in by linear algebra computations with piecewise polynomial functions.

	$\operatorname{rk} A_T^i(X')$	$\operatorname{rk} M \cdot A_T^{i-1}(X')$	$\operatorname{rk} A^i(X')$
$i=0$	1	0	1
$i=1$	3	3	0
$i=2$	8	6	5
$i=3$	20	16	1

Here, again, we see that $\iota^* : A_T^2(X') \to A^2(X')$ is not surjective, since its image has rank at most two. Furthermore, the kernel of ι^* is not generated in degree one, since the degree one part of the kernel is M, and $A_T^3(X')/M \cdot A_T^2(X')$ has rank four, and hence cannot map injectively into $A^3(X')$. However, X' is not projective, so to prove Theorem 1.6, it remains to give a projective example with similar properties.

Example 4.4. Consider the toric variety $X'' = X(\Delta'')$, where Δ'' is the fan combinatorially equivalent to the fan over the cube as in Example 4.2, but with the ray through $(1,1,1)$ replaced by the ray through $(1,1,2)$ and with the ray through $(1,-1,1)$ replaced by the ray through $(1,-1,2)$. It is straightforward to check that $-3K_{X''}$ is Cartier and ample, so X'' is $\mathbb{Q}$-Fano and projective. We compute the following table as in the preceding examples.

	$\operatorname{rk} A_T^i(X'')$	$\operatorname{rk} M \cdot A_T^{i-1}(X'')$	$\operatorname{rk} A^i(X'')$
$i=0$	1	0	1
$i=1$	4	3	1
$i=2$	10	9	5
$i=3$	22	19	1

Proof of Theorem 1.6. From the computations in Example 4.4, we conclude that $\iota^* : A^*_T(X)_{\mathbb{Q}} \to A^*(X)_{\mathbb{Q}}$ is not surjective in degree two, and its kernel in degree three is not in the ideal generated by its kernel in degree one. □

To balance these negative results, we conclude by proving a positive statement: $\iota^* : A^*_T(X) \to A^*(X)$ is always surjective in degree one.

Theorem 4.5. *For any toric variety $X = X(\Delta)$, $\iota^* : A^1_T(X) \to A^1(X)$ is surjective, giving a natural isomorphism $A^1(X) \cong PP^1(\Delta)/M$.*

Proof. If X is smooth, then the statement is clear. Suppose X is singular, and let

$$X_r \to \cdots \to X_1 \xrightarrow{\pi} X_0 = X$$

be a resolution of singularities, where each $X_i = X(\Delta_i)$ is a toric variety and $X_{i+1} \to X_i$ is the blowup along a smooth T-invariant center. Say X_1 is the blowup of X along $V(\tau)$ and $V(\rho) \subset X_1$ is the exceptional divisor. By induction on r, we may assume $A^1(X_1) \cong PP^1(\Delta_1)/M$. Also, we may assume $A^1(V(\rho)) = PP^1(\mathrm{Star}(\rho))/M$ and $A^1(V(\tau)) = PP^1(\mathrm{Star}(\tau))/M$, by induction on dimension. Then $\pi^* : A^1(X) \to A^1(X_1)$ is injective, and $c \in A^1(X_1)$ is in the image of π^* if and only if $c|_{V(\rho)}$ is in the image of $A^1(V(\tau))$ [Kimura 1992, Theorem 3.1]. The theorem then follows, since $\mathrm{Star}(\rho)$ is a subdivision of $\mathrm{Star}(\tau)$, Δ_1 and Δ coincide everywhere else, and the class of a piecewise linear function $[\Psi] \in PP^1(\mathrm{Star}(\rho))/M$ is pulled back from $\mathrm{Star}(\tau)$ if and only if Ψ is given by a single linear function on each cone of $\mathrm{Star}(\tau)$. □

Corollary 4.6. *For any toric variety X, the canonical map* $\mathrm{Pic}(X) \to A^1(X)$ *is an isomorphism.*

Proof. The corollary follows from the canonical identification of $PP^1(X)/M$ with $\mathrm{Pic}(X)$ [Fulton 1993, pp. 65–66]. □

Corollary 4.6 was known previously in the case where X is complete [Brion 1989]. See also [Fulton and Sturmfels 1997, Corollary 3.4].

Remark 4.7. One can use Kimura's inductive method, as in the proof of Corollary 4.6 and [Payne 2006a, Theorem 1], to compute the Chow cohomology of an arbitrary toric variety in all degrees. However, the resulting induction is more subtle, as Theorems 1.5 and 1.6 suggest.

5. Localization formula for mixed volumes of lattice polytopes

Let $P_1, \dots, P_n$ be lattice polytopes in $M_{\mathbb{R}}$. For nonnegative real numbers a_i, the euclidean volume of $a_1 P_1 + \cdots + a_n P_n$ is a homogeneous polynomial function of $(a_1, \dots, a_n)$. The *mixed volume* $V(P_1, \dots, P_n)$ is defined to be the coefficient of $a_1 \cdots a_n$ in this polynomial. Let Δ be the inner normal fan to $P_1 + \cdots + P_n$, and let $u_i(\sigma) \in M$ be the vertex of P_i that is minimal on σ, for each maximal cone $\sigma \in \Delta$.

Theorem 5.1. *The mixed volume of the polytopes P_i is given by*

$$n! \cdot V(P_1, \dots, P_n) = (-1)^n \sum_{\sigma \in \Delta} e_\sigma \cdot u_1(\sigma) \cdots u_n(\sigma).$$

Theorem 5.1 follows from Theorem 1.4 and the fact that $V(P_1, \dots, P_n)$ is the degree of $D_1 \cdots D_n$, where D_i is the T-Cartier divisor on $X(\Delta)$ corresponding to P_i [Fulton 1993, p. 116]. However, the statement of the theorem is purely combinatorial, and we give a combinatorial proof based on Brion's formula for generating functions for lattice points in polyhedra. The methods used in this proof may be of independent interest.

Let P be a lattice polytope in $M_{\mathbb{R}}$. Let Δ be the normal fan to P, and let $u(\sigma) \in M$ be the vertex of P that is minimal on σ, for each maximal cone $\sigma \in \Delta$.

Brion's Formula. The generating function for lattice points in P is

$$\sum_{u \in (P \cap M)} x^u = \sum_{\sigma} x^{u(\sigma)} \cdot \text{Hilb}(\sigma).$$

In addition to Brion's Formula, we will use the following formula for mixed volumes, which is a lattice point counting analogue of the alternating sum of volumes in formula (3) of [Fulton 1993, p. 116].

Proposition 5.2. *Let $P_1, \dots, P_n$ be lattice polytopes in $M_{\mathbb{R}}$. Then*

$$n! \cdot V(P_1, \dots, P_n) = \sum_{1 \le i_1 < \cdots < i_k \le n} (-1)^{n-k} \#((P_{i_1} + \cdots + P_{i_k}) \cap M).$$

Proof. The number of lattice points in $a_1 P_1 + \cdots + a_n P_n$ is a polynomial in the a_i of degree at most n, and the degree n part of this polynomial is $n!$ times the volume of $a_1 P_1 + \cdots + a_n P_n$ [McMullen 1978/79, Theorem 7]. Therefore, $n! \cdot V(P_1, \dots, P_n)$ is the coefficient of $a_1 \cdots a_n$ in this polynomial, and the proposition is an immediate consequence of the following lemma. □

Lemma 5.3. *Let $f \in \mathbb{R}[t_1, \dots, t_n]$ be a polynomial function on $\mathbb{R}^n$ of degree at most n. The coefficient of $t_1 \cdots t_n$ in f is*

$$\sum_{1 \le i_1 < \cdots < i_k \le n} (-1)^{n-k} f(e_{i_1} + \cdots + e_{i_k})$$

where $\{e_1, \dots, e_n\}$ is the standard basis for $\mathbb{R}^n$.

Proof. The function taking a polynomial g to $\sum (-1)^{n-k} g(e_{i_1} + \cdots + e_{i_k})$ vanishes on any monomial that does not contain all n variables, and its value on $t_1 \cdots t_n$ is 1. □

Proof of Theorem 5.1. For each σ, $(-1)^n \cdot e_\sigma \cdot u_1(\sigma) \cdots u_n(\sigma)$ is the principal part of

$$(x^{u_1(\sigma)} - 1) \cdots (x^{u_n(\sigma)} - 1) \cdot \mathrm{Hilb}(\sigma).$$

Expanding the product of the binomials, taking the sum over all σ, and applying Brion's Formula then gives

$$\sum_{1 \le i_1 < \cdots < i_k \le n} (-1)^{n-k} \cdot \sum_{u \in (P_{i_1} + \cdots + P_{i_k} \cap M)} x^u.$$

The theorem then follows from Proposition 5.2 by taking principal parts, since the leading form of x^u at 1_T is equal to one. □

6. Bott residue formula for toric vector bundles

The mixed volume $V(P_1, \dots, P_n)$ is the degree of the top Chern class of the toric vector bundle $\mathcal{O}(D_1) \oplus \cdots \oplus \mathcal{O}(D_n)$, where D_i is the T-Cartier divisor corresponding to P_i. Therefore, mixed volumes are a special case of Chern numbers of toric vector bundles, and Theorem 5.1 may be generalized as follows. Given a multiset of linear functions $\mathbf{u} \subset M$ let $\varepsilon_i(\mathbf{u}) \in \mathrm{Sym}^i(M)$ be the i-th elementary symmetric function in the elements of $\mathbf{u}$. For instance, if $\mathbf{u} = \{u_1, \dots, u_r\}$, then $\varepsilon_1(\mathbf{u}) = u_1 + \cdots + u_r$ and $\varepsilon_r(\mathbf{u}) = u_1 \cdots u_r$. For a partition $\lambda = (\lambda_1, \dots, \lambda_s)$ of n, let $\varepsilon_\lambda(\mathbf{u}) \in \mathrm{Sym}^n(M)$ be the product

$$\varepsilon_\lambda(\mathbf{u}) = \varepsilon_{\lambda_1}(\mathbf{u}) \cdots \varepsilon_{\lambda_s}(\mathbf{u}).$$

Recall that, for any toric vector bundle $\mathcal{E}$ on an arbitrary toric variety $X = X(\Delta)$ and any maximal cone $\sigma \in \Delta$, there is a unique multiset $\mathbf{u}(\sigma) \subset M$ such that the restriction of $\mathcal{E}$ to U_σ splits equivariantly as

$$\mathcal{E}|_{U_\sigma} \cong \bigoplus_{u \in \mathbf{u}(\sigma)} \mathcal{O}(\operatorname{div} \chi^u).$$

See [Klyachko 1989] or [Payne 2006b, Section 2] for this and other basic facts about toric vector bundles.

Theorem 6.1. *Let $\mathcal{E}$ be a toric vector bundle on a complete toric variety X, and let λ be a partition of n. Then the Chern number $c_\lambda(\mathcal{E})$ is given by*

$$c_\lambda(\mathcal{E}) = \sum_\sigma e_\sigma \cdot \varepsilon_\lambda(\mathbf{u}(\sigma)).$$

Proof. The Chern number $c_\lambda(\mathcal{E})$ is equal to the integral over $[X]$ of the equivariant Chow cohomology class corresponding to the piecewise polynomial whose restriction to σ is $\varepsilon_\lambda(\mathbf{u}(\sigma))$. Therefore, the theorem follows from Theorem 1.4. □

Theorem 6.1 has a straightforward generalization to top degree polynomials in the Chern classes of several toric vector bundles (we omit the details), and may be seen as a Bott residue formula for vector bundles on toric varieties with arbitrary singularities. This solves the toric case of the problem of proving residue formulas on singular varieties posed in [Edidin and Graham 1998b, Section 5]. Edidin and Graham handled the case of toric subvarieties of smooth toric varieties, but the extension to arbitrary toric varieties is nontrivial; there are singular toric varieties, such as Fulton's threefold (Example 4.3) that have no nontrivial line bundles, and hence admit no nonconstant morphisms to smooth varieties.

Example 6.2. We apply Theorem 6.1 to compute the Chern numbers of a specific nonsplit rank two toric vector bundle on the singular toric variety $X = X(\Delta)$ mirror dual to $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$ (see Example 4.2). For this example, we assume that the base field has at least three elements. The primitive generators of the rays of Δ are

$$\begin{array}{llll} v_1 = (1, 1, 1), & v_2 = (1, 1, -1), & v_3 = (1, -1, 1), & v_4 = (1, -1, -1), \\ v_5 = (-1, 1, 1), & v_6 = (-1, 1, -1), & v_7 = (-1, -1, 1), & v_8 = (-1, -1, -1), \end{array}$$

and the maximal cones of Δ are

$$\begin{array}{lll} \sigma_1 = \langle v_1, v_2, v_3, v_4 \rangle, & \sigma_2 = \langle v_1, v_2, v_5, v_6 \rangle, & \sigma_3 = \langle v_1, v_3, v_5, v_7 \rangle, \\ \sigma_4 = \langle v_2, v_4, v_7, v_8 \rangle, & \sigma_5 = \langle v_3, v_4, v_7, v_8 \rangle, & \sigma_6 = \langle v_5, v_6, v_7, v_8 \rangle. \end{array}$$

Let ρ_i be the ray of Δ spanned by v_i, let $E = k^2$, fix four distinct lines L_1, L_2, L_3, and L_4 in E, and let $\mathscr{E}$ be the toric vector bundle determined by the filtrations

$$E^{\rho_1}(i) = \begin{cases} E & \text{for } i \le -1, \\ L_1 & \text{for } 0 \le i \le 3, \\ 0 & \text{for } i > 3, \end{cases} \qquad E^{\rho_4}(i) = \begin{cases} E & \text{for } i \le -1, \\ L_2 & \text{for } 0 \le i \le 3, \\ 0 & \text{for } i > 3, \end{cases}$$

$$E^{\rho_6}(i) = \begin{cases} E & \text{for } i \le -1, \\ L_3 & \text{for } 0 \le i \le 3, \\ 0 & \text{for } i > 3, \end{cases} \qquad E^{\rho_7}(i) = \begin{cases} E & \text{for } i \le -1, \\ L_4 & \text{for } 0 \le i \le 3, \\ 0 & \text{for } i > 3, \end{cases}$$

and

$$E^{\rho_j}(i) = \begin{cases} E & \text{for } i \le 1, \\ 0 & \text{for } i > 1, \end{cases}$$

for $j \in \{2, 3, 5, 8\}$. Since the lines L_i are distinct, the vector bundle $\mathscr{E}$ does not split as a sum of line bundles. It is straightforward to check that the multisets of linear functions $\mathbf{u}(\sigma_i)$ determined by $\mathscr{E}$ are as follows. For simplicity, we write a, b, and c, for e_1^*, e_2^* and e_3^*, respectively.

$$\begin{array}{ll} \mathbf{u}(\sigma_1) = \{(a+b+c), (a-b-c)\}, & \mathbf{u}(\sigma_2) = \{(a+b+c), (-a+b-c)\}, \\ \mathbf{u}(\sigma_3) = \{(a+b+c), (-a-b+c)\}, & \mathbf{u}(\sigma_4) = \{(a-b-c), (-a+b-c)\}, \\ \mathbf{u}(\sigma_5) = \{(a-b-c), (-a-b+c)\}, & \mathbf{u}(\sigma_6) = \{(-a+b-c), (-a-b+c)\}. \end{array}$$

To compute the Chern numbers of $\mathscr{E}$, we now need only to compute the equivariant multiplicities e_{σ_i}. First, σ_1^* is spanned by $u_1 = (1, 1, 0)$, $u_2 = (1, 0, 1)$, $u_3 = (1, 0, -1)$, and $u_4 = (1, -1, 0)$. Let $u = (1, 0, 0)$. We compute, as in [Payne 2007, Example 1.8],

$$\mathrm{Hilb}(\sigma_1) = \frac{(1+x^u)(1-x^{2u})}{(1-x^{u_1})(1-x^{u_2})(1-x^{u_3})(1-x^{u_4})}.$$

Since the principal parts of $1+x^u$, $1-x^{2u}$ and $1-x^{u_i}$ at 1_T are 2, $-2u$, and $-u_i$ respectively, it is then straightforward to compute $e_{\sigma_1} = -\mathrm{Hilb}(\sigma)_\circ$. Then

$$e_{\sigma_1} = \frac{4a}{(b^2-a^2)(c^2-a^2)}.$$

By symmetry, $e_{\sigma_6} = -e_{\sigma_1}$, and similarly

$$e_{\sigma_2} = \frac{4b}{(a^2-b^2)(c^2-b^2)} = -e_{\sigma_5},$$

and

$$e_{\sigma_3} = \frac{4c}{(a^2-c^2)(b^2-c^2)} = -e_{\sigma_4}.$$

Then, using Theorem 6.1 and combining the summands coming from σ_i and σ_{7-i}, we obtain

$$c_{111}(\mathscr{E}) = \frac{2\cdot(2a)^3\cdot 4a}{(b^2-a^2)(c^2-a^2)} + \frac{2\cdot(2b)^3\cdot 4b}{(a^2-b^2)(c^2-b^2)} + \frac{2\cdot(2c)^3\cdot 4c}{(a^2-c^2)(b^2-c^2)},$$

which simplifies to $c_{111}(\mathscr{E}) = 64$. Similarly,

$$c_{21}(\mathscr{E}) = \frac{16a^2(a^2-b^2-c^2)}{(b^2-a^2)(c^2-a^2)} + \frac{16b^2(-a^2+b^2-c^2)}{(a^2-b^2)(c^2-b^2)} + \frac{16c^2(-a^2-b^2+c^2)}{(a^2-c^2)(b^2-c^2)},$$

which simplifies to $c_{21}(\mathscr{E}) = 32$.

Appendix: Principal parts of rational functions

Associated graded rings and leading forms have been standard tools for about as long as commutative algebra has been applied to local algebraic geometry [Samuel 1953; 1955]. The generalization from leading forms of regular functions to principal parts of rational functions is straightforward but, since we have been unable to locate a reference, we include a brief account.

Let X be an algebraic variety over a field k, and let $x \in X(k)$ be a smooth point. Let $\mathfrak{m}$ be the maximal ideal in the local ring $\mathscr{O}_{X,x}$. Since x is smooth,

$$(\mathfrak{m}^d/\mathfrak{m}^{d+1}) \cong \mathrm{Sym}^d(\mathfrak{m}/\mathfrak{m}^2),$$

for all nonnegative integers d [Atiyah and Macdonald 1969, Theorem 11.22]. Suppose $g \in \mathcal{O}_{X,x}$ is a regular function whose order of vanishing at x is d. Then the *leading form* of g is its image

$$g_\circ \in \mathrm{Sym}^d(\mathfrak{m}/\mathfrak{m}^2).$$

In other words, if $x_1, \dots, x_n$ is a local system of parameters, then g can be expanded uniquely as a power series in $k[[x_1, \dots, x_n]]$, and the sum of the lowest degree terms in this power series is the homogeneous degree d polynomial in $x_1, \dots, x_n$ that maps to $g_\circ$ under the canonical isomorphism

$$k[x_1, \dots, x_n]_d \cong \mathrm{Sym}^d(\mathfrak{m}/\mathfrak{m}^2).$$

Now $\mathfrak{m}/\mathfrak{m}^2$ is the cotangent space of X at x, so $g_\circ$ is naturally a regular function on the tangent space $T_{X,x}$, and the zero locus of $g_\circ$ is the tangent cone of the divisor of zeros of g at x [Harris 1992, Lecture 20]. Note that leading forms are multiplicative; if $g, h \in \mathcal{O}_{X,x}$, then $(gh)_\circ = g_\circ h_\circ$ in $\mathrm{Sym}^*(\mathfrak{m}/\mathfrak{m}^2)$. For convenience, we define the leading form of zero to be $0 \in \mathrm{Sym}^*(\mathfrak{m}/\mathfrak{m}^2)$.

Suppose f is a rational function on X. Then f can be written as a fraction $f = g/h$, with $g, h \in \mathcal{O}_{X,x}$. We define the *principal part* of f to be

$$f_\circ = g_\circ / h_\circ,$$

which is a homogeneous element of $\mathrm{Sym}^\pm(\mathfrak{m}/\mathfrak{m}^2)$, the $\mathbb{Z}$-graded ring obtained by inverting all homogeneous elements in $\mathrm{Sym}^*(\mathfrak{m}/\mathfrak{m}^2)$. Note that $f_\circ$ is well-defined; if $g/h = g'/h'$, then $gh' = g'h$ (since $\mathcal{O}_{X,x}$ is a domain), and therefore

$$g_\circ h'_\circ = g'_\circ h_\circ,$$

since leading forms are multiplicative, so $g_\circ / h_\circ = g'_\circ / h'_\circ$. Also, $f_\circ$ is naturally a rational function on $T_{X,x}$, and its divisors of zeros and poles are the tangent cones of the zeros and poles of f, respectively.

Proposition A.1. *Suppose $f_1, \dots, f_s$ are rational functions on X with principal parts in degree d, and let $f = f_1 + \cdots + f_s$. Then either*

$$f_\circ = (f_1)_\circ + \cdots + (f_s)_\circ,$$

or $(f_1)_\circ + \cdots + (f_s)_\circ = 0$ and the principal part of f is in degree strictly greater than d.

Proof. If $f = 0$ then the proposition is clear. Suppose f is nonzero, and express each f_i as a fraction $f_i = g_i/h_i$, with $g_i, h_i \in \mathcal{O}_{X,x}$. Then we can write f as a fraction over a common denominator

$$f = \sum_{i=1}^{s} \frac{g_i \cdot h_1 \cdots \widehat{h_i} \cdots h_s}{h_1 \cdots h_s}.$$

Say h_i vanishes to order d_i at x. Then each summand in the numerator above vanishes to order exactly $d_1+\cdots+d_s+d$. Therefore, either the numerator vanishes to order exactly $d_1+\cdots+d_s+d$ and $f_\circ = (f_1)_\circ + \cdots + (f_s)_\circ$, or the numerator vanishes to some larger order and $f_\circ$ has degree greater than d. □

Corollary A.2. *Suppose $f_1, \dots, f_s$ are rational functions on X with principal parts in degree d, and suppose $f = f_1 + \cdots + f_s$ is regular at x. Then $(f_1)_\circ + \cdots + (f_s)_\circ \in \mathrm{Sym}^*(\mathfrak{m}/\mathfrak{m}^2)$ is regular on $T_{X,x}$.*

Proof. By Proposition A.1, if $(f_1)_\circ + \cdots + (f_s)_\circ$ does not vanish then it is equal to $f_\circ$, which is the principal part of a regular function. □

Acknowledgments

We thank B. Sturmfels for illuminating the connection between Minkowski weights and tropical geometry, D. Speyer for enlightening discussions on Brion's Formula, E. Miller for helping us understand multidegrees, and T. Ekedahl for useful conversations related to principal parts of rational functions.

References

[Atiyah and Macdonald 1969] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, Reading, MA, 1969. MR 39 #4129 Zbl 0175.03601

[Barvinok 2002] A. Barvinok, *A course in convexity*, Graduate Studies in Mathematics **54**, American Mathematical Society, Providence, RI, 2002. MR 2003j:52001 Zbl 1014.52001

[Brion 1989] M. Brion, "Groupe de Picard et nombres caractéristiques des variétés sphériques", *Duke Math. J.* **58**:2 (1989), 397–424. MR 90i:14048 Zbl 0701.14052

[Brion 1996] M. Brion, "Piecewise polynomial functions, convex polytopes and enumerative geometry", pp. 25–44 in *Parameter spaces* (Warsaw, 1994), edited by P. Pragacz, Banach Center Publ. **36**, Polish Acad. Sci., Warsaw, 1996. MR 99h:14052 Zbl 0878.14035

[Brion 1997] M. Brion, "Equivariant Chow groups for torus actions", *Transform. Groups* **2**:3 (1997), 225–267. MR 99c:14005 Zbl 0916.14003

[Edidin and Graham 1998a] D. Edidin and W. Graham, "Equivariant intersection theory", *Invent. Math.* **131**:3 (1998), 595–634. MR 99j:14003a Zbl 0940.14003

[Edidin and Graham 1998b] D. Edidin and W. Graham, "Localization in equivariant intersection theory and the Bott residue formula", *Amer. J. Math.* **120**:3 (1998), 619–636. MR 99g:14005 Zbl 0980.14004

[Fulton 1993] W. Fulton, *Introduction to toric varieties*, Annals of Mathematics Studies **131**, Princeton University Press, Princeton, NJ, 1993. MR 94g:14028 Zbl 0813.14039

[Fulton and Sturmfels 1997] W. Fulton and B. Sturmfels, "Intersection theory on toric varieties", *Topology* **36**:2 (1997), 335–353. MR 97h:14070 Zbl 0885.14025

[Harris 1992] J. Harris, *Algebraic geometry. A first course*, Graduate Texts in Mathematics **133**, Springer, New York, 1992. MR 93j:14001 Zbl 0779.14001

[Katz 2007] E. Katz, "A tropical toolkit", preprint, 2007. arXiv math.AG/0610878v2

[Kimura 1992] S. Kimura, "Fractional intersection and bivariant theory", *Comm. Algebra* **20**:1 (1992), 285–302. MR 93d:14010 Zbl 0774.14004

[Klyachko 1989] A. A. Klyachko, "Equivariant bundles over toric varieties", *Izv. Akad. Nauk SSSR Ser. Mat.* **53**:5 (1989), 1001–1039, 1135. MR 91c:14064 Zbl 0706.14010

[Knutson and Miller 2005] A. Knutson and E. Miller, "Gröbner geometry of Schubert polynomials", *Ann. of Math.* (2) **161**:3 (2005), 1245–1318. MR 2006i:05177 Zbl 1089.14007

[Lawrence 1988] J. Lawrence, "Valuations and polarity", *Discrete Comput. Geom.* **3**:4 (1988), 307–324. MR 90b:52001 Zbl 0646.52003

[McMullen 1978/79] P. McMullen, "Lattice invariant valuations on rational polytopes", *Arch. Math.* (*Basel*) **31**:5 (1978/79), 509–516. MR 80d:52011 Zbl 0387.52007

[Mikhalkin 2006] G. Mikhalkin, "Tropical geometry and its applications", pp. 827–852 in *International Congress of Mathematicians* (Madrid, Spain, August 22–30, 2006), vol. II, edited by M. Sanz-Solé et al., Eur. Math. Soc., Zürich, 2006. MR 2275625 Zbl 1103.14034

[Miller and Sturmfels 2005] E. Miller and B. Sturmfels, *Combinatorial commutative algebra*, Graduate Texts in Mathematics **227**, Springer, New York, 2005. MR 2006d:13001 Zbl 1066.13001

[Payne 2006a] S. Payne, "Equivariant Chow cohomology of toric varieties", *Math. Res. Lett.* **13**:1 (2006), 29–41. MR 2007f:14052 Zbl 1094.14036

[Payne 2006b] S. Payne, "Toric vector bundles, branched covers of fans, and the resolution property", preprint, 2006. To appear in *J. Alg. Geom.* arXiv math.AG/0605537

[Payne 2007] S. Payne, "Ehrhart series and lattice triangulations", preprint, 2007. To appear in Discr. Comput. Geom. arXiv math.CO/0702052

[Rossmann 1989] W. Rossmann, "Equivariant multiplicities on complex varieties", *Astérisque* 173-174 (1989), 11, 313–330. MR 91g:32042 Zbl 0691.32004

[Samuel 1953] P. Samuel, *Algèbre locale*, Mémor. Sci. Math. **123**, Gauthier-Villars, Paris, 1953. MR 14,1012c Zbl 0053.01901

[Samuel 1955] P. Samuel, *Méthodes d'algèbre abstraite en géométrie algébrique*, Ergebnisse der Mathematik (N.F.) **4**, Springer, Berlin, 1955. MR 17,300b Zbl 0067.38904

Communicated by Andrei Zelevinsky
Received 2007-04-02 Revised 2007-10-22 Accepted 2007-11-20

eekatz@math.utexas.edu *Department of Mathematics, University of Texas,*
Austin, TX 78712, United States

spayne@stanford.edu *Department of Mathematics, Bldg 380, Stanford University,*
Stanford, CA 94305, United States

ALGEBRA AND NUMBER THEORY 2:2(2008)

The nef cone volume of generalized Del Pezzo surfaces

Ulrich Derenthal, Michael Joyce and Zachariah Teitler

We compute a naturally defined measure of the size of the nef cone of a Del Pezzo surface. The resulting number appears in a conjecture of Manin on the asymptotic behavior of the number of rational points of bounded height on the surface. The nef cone volume of a Del Pezzo surface Y with (-2)-curves defined over an algebraically closed field is equal to the nef cone volume of a smooth Del Pezzo surface of the same degree divided by the order of the Weyl group of a simply-laced root system associated to the configuration of (-2)-curves on Y. When Y is defined over an arbitrary perfect field, a similar result holds, except that the associated root system is no longer necessarily simply-laced.

1. Introduction

An *ordinary Del Pezzo surface* is a smooth projective rational surface X on which the anticanonical class $-K_X$ is ample. If X is defined over an algebraically closed field, then X is one of the following: $\mathbb{P}^2$, $\mathbb{P}^1 \times \mathbb{P}^1$, or the blowup of $\mathbb{P}^2$ at up to 8 points in general position. Points are in general position if no three are collinear, no six lie on a conic, and no eight lie on a cubic with one of them a singular point of the cubic. Then X may contain (-1)-curves, but no (-2)-curves, where for $n \in \{1, 2\}$, a *$(-n)$-curve* is a smooth rational curve on X having self-intersection number $-n$.

A *generalized Del Pezzo surface* is a smooth projective rational surface Y on which $-K_Y$ is big and nef. If Y is defined over an algebraically closed field, then Y is one of the following: $\mathbb{P}^2$, $\mathbb{P}^1 \times \mathbb{P}^1$, the Hirzebruch surface $\mathbb{F}_2$, or a surface obtained from $\mathbb{P}^2$ by a sequence of blowings-up at up to 8 points, possibly infinitely near, each not lying on any (-2)-curve. Over an algebraically closed field, a generalized Del Pezzo surface is ordinary if and only if it contains no (-2)-curves. See Section 3 for more details.

MSC2000: primary 14J26; secondary 14C20, 14G05.

Keywords: Del Pezzo surface, Manin's conjecture, nef cone, root system.

The first author was partially supported by a Feodor Lynen Research Fellowship of the Alexander von Humboldt Foundation.

The nef cone volume of a generalized Del Pezzo surface Y is equal to the volume of the cross-section of the nef cone of Y obtained by intersecting with the hyperplane consisting of those divisor classes whose intersection with the anticanonical class $-K_Y$ is equal to 1. The resulting cross-section is a polytope. Its volume is a rational number, denoted by $\alpha(Y)$. We give details of this definition in Section 2.

In this paper we compute $\alpha(Y)$ for generalized Del Pezzo surfaces Y.

The *degree* of Y is the self-intersection number

$$d = \langle -K_Y, -K_Y \rangle.$$

It satisfies $1 \le d \le 9$, and when Y is the blowup of $\mathbb{P}^2$ at r points in almost general position, $d = 9 - r$.

A generalized Del Pezzo surface Y defined over a field $\mathbb{K}$ is *split* if it is either $\mathbb{P}^2$, $\mathbb{P}^1 \times \mathbb{P}^1$, $\mathbb{F}_2$, or the blowup of $\mathbb{P}^2$ at $1 \le r \le 8$ $\mathbb{K}$-rational points in almost general position. See Definition 3.2. Otherwise, Y is said to be nonsplit (for example, the blowup of $\mathbb{P}^2$ at two conjugate points). We consider only split Y until Section 6, and so the reader may assume that $\mathbb{K}$ is algebraically closed until that point.

An investigation of $\alpha(Y)$ for split ordinary Del Pezzo surfaces was undertaken by the first author. He proved the following result.

Theorem 1.1 [Derenthal 2007, Theorem 4]. *Let X_d denote a split ordinary Del Pezzo surface of degree d obtained by blowing up $9-d$ points in general position on $\mathbb{P}^2$ and let N_d denote the number of (-1)-curves on X_d. For $d \le 6$,*

$$\alpha(X_d) = \frac{N_d}{d(9-d)} \alpha(X_{d+1}).$$

Combining this with simple calculations that show that

$$\alpha(\mathbb{P}^2) = \tfrac{1}{3}, \quad \alpha(\mathbb{P}^1 \times \mathbb{P}^1) = \tfrac{1}{4}, \quad \alpha(X_8) = \tfrac{1}{6}, \quad \alpha(X_7) = \tfrac{1}{24},$$

this theorem allows for an inductive calculation of $\alpha(X)$ for any split ordinary Del Pezzo surface X. This calculation is summarized in Table 1.

We extend this result in two directions. First, we study split generalized Del Pezzo surfaces. In Section 4, we prove the following theorem by analyzing the nef cone of such a surface Y. It allows us to compute $\alpha(Y)$ by induction on the rank of the Néron–Severi group of Y.

d	8	7	6	5	4	3	2	1
N_d	1	3	6	10	16	27	56	240
$\alpha(X_d)$	$\frac{1}{6}$	$\frac{1}{24}$	$\frac{1}{72}$	$\frac{1}{144}$	$\frac{1}{180}$	$\frac{1}{120}$	$\frac{1}{30}$	1

Table 1. Values of $\alpha(X_d)$ for ordinary Del Pezzo surfaces X_d.

Theorem 1.2. *Let Y be a split generalized Del Pezzo surface of degree $d \leq 7$. For each E in the set $\mathscr{C}$ of (-1)-curves on Y, let Y_E denote the split generalized Del Pezzo surface of degree $d+1$ obtained by contracting E. Then*

$$\alpha(Y) = \sum_{E \in \mathscr{C}} \frac{1}{d(9-d)} \alpha(Y_E).$$

As with Theorem 1.1, using the additional calculation that $\alpha(\mathbb{F}_2) = \frac{1}{8}$, this theorem allows us to compute $\alpha(Y)$ for any split generalized Del Pezzo surface Y.

The first author computed $\alpha(Y)$ for split generalized Del Pezzo surfaces Y of degree $d \geq 3$ directly, using computer programs to find a triangulation of the nef cone case by case [Derenthal 2007, Section 3]. This numerical data led us to formulate the following theorem; see Section 5C for its proof.

Theorem 1.3. *Let Y be a split generalized Del Pezzo surface of degree $d \leq 7$ and let X be a split ordinary Del Pezzo surface of the same degree. Then*

$$\alpha(Y) = \frac{1}{\#W(R_Y)} \alpha(X),$$

where $W(R_Y)$ is the Weyl group of the root system R_Y whose simple roots are the (-2)-curves on Y.

When combined with Theorem 1.1 the computation of $\alpha(Y)$ for an arbitrary split generalized Del Pezzo surface Y of any degree is reduced to a determination of the (-2)-curves on the surface. See Section 5 for more information on the root system R_Y and its Weyl group.

We also consider the case of nonsplit surfaces. Suppose that Y is a generalized Del Pezzo surface and X is an ordinary Del Pezzo surface, both of the same degree and defined over the same perfect field $\mathbb{K}$. Then the Néron–Severi groups of X and Y coincide (Proposition 6.2) and the absolute Galois group of $\mathbb{K}$ acts as a finite group G of automorphisms of this group (Proposition 6.1). Assume that the Galois actions associated to X and Y coincide. The Galois action on the root system R_Y allows us to associate to Y an orbit root system $\mathbb{O}(R_Y, G)$ (Definition 6.5). Our third main result is that under these assumptions

$$\alpha(Y) = \frac{\alpha(X)}{\#W(\mathbb{O}(R_Y, G))}.$$

See Corollary 7.5. The integer appearing in the denominator is the order of a Weyl group and is straightforward to compute. Thus all that is left is to compute $\alpha(X)$. There are a finite number of cases in each degree d, one for each conjugacy class of subgroups of the Weyl group of a canonically defined root system R_d (Section 5B). We perform the computations for $d \geq 5$ in Section 7B.

Manin's conjecture. The primary motivation for our study of the nef cone volume α is its appearance in Manin's conjecture on the number of rational points of bounded height on Fano varieties defined over number fields, as described below. Although the conjecture is now known not to hold for all Fano varieties [Batyrev and Tschinkel 1996, Theorems 3.1–3.3], it has been verified in a large number of cases, including some varieties for which the anticanonical class is big but not ample.

Let X be a smooth projective variety defined over a number field $\mathbb{K}$ for which $-K_X$ is big and assume that the set $X(\mathbb{K})$ of rational points is Zariski dense. Equip $X(\mathbb{K})$ with an anticanonical height function H (consult [Hindry and Silverman 2000, Part B] for information on height functions) and for any constructible set $U \subset X$ let

$$\mathcal{N}_U(B) := \#\{P \in U(\mathbb{K}) : H(P) \leq B\}.$$

The original formulation of the Manin conjecture [Batyrev and Manin 1990, Conjecture B] posits the existence of a Zariski open set $U \subset X$ such that for any open set $V \subset U$

$$\mathcal{N}_V(B) \sim c(X)B(\log B)^{\rho-1} \quad \text{asymptotically as } B \to \infty,$$

where ρ is the Néron–Severi rank of X. The conjecture was initially made for Fano varieties, but a more ambitious version of the conjecture relaxes the condition on $-K_X$ to merely being big. The leading constant was given a conjectural interpretation by Peyre [1995, Definition 2.4] and Batyrev and Tschinkel [1995, Theorem 4.4.4]. They predict that $c(X) = \alpha(X)\beta(X)\tau(X)$, where $\alpha(X) \in \mathbb{Q}$ is the constant of interest in this paper, $\beta(X) \in \mathbb{N}$ is a cohomological invariant of the Galois action on the Néron–Severi group of X, and $\tau(X) \in \mathbb{R}$ is a volume of adelic points on X.

2. Definition of the nef cone volume

We recall the definition of $\alpha(X)$, first introduced by Peyre [1995, Definition 2.4].

Let X be a smooth complete variety for which $-K_X$ is big. We denote the intersection form on X by $\langle \cdot , \cdot \rangle$. Recall that a divisor class D on X is *numerically trivial* if $\langle D, C\rangle = 0$ for all curves (equivalently, all 1-cycles) C on X, and two divisor classes are *numerically equivalent* if their difference is numerically trivial. One similarly defines numerical equivalence of curves. Numerical equivalence classes of divisors on X form a finitely-generated torsion-free abelian group $N^1(X)$ whose dual group $N_1(X)$ consists of numerical equivalence classes of 1-cycles on X. Let $N^1(X)_{\mathbb{R}} = N^1(X) \otimes_{\mathbb{Z}} \mathbb{R}$ and $N_1(X)_{\mathbb{R}} = N_1(X) \otimes_{\mathbb{Z}} \mathbb{R}$ be the associated Euclidean spaces. Inside $N^1(X)_{\mathbb{R}}$ lies the *effective cone* $\mathrm{Eff}^1(X)$, the closed convex cone spanned by the classes of effective divisors.

Recall that for a finite-dimensional real inner product space V and a convex cone $\Gamma \subset V$, the dual convex cone $\Gamma^\vee \subset V$ is defined by

$$\Gamma^\vee = \{\, v \in V : \langle v, c\rangle \geq 0 \text{ for all } c \in \Gamma \,\}.$$

The cone $\Gamma^\vee$ is closed as a subspace of the Euclidean space V. The dual $\mathrm{Eff}^1(X)^\vee$ of the effective cone of X in $N^1(X)_\mathbb{R}$ is the movable cone of X (see [Boucksom et al. 2004, Theorem 2.2], [Lazarsfeld 2004, Section 11.4.C]). Note that when X is a surface, $N_1(X) = N^1(X)$ and $\mathrm{Eff}^1(X)^\vee$ is the *nef cone* of X, denoted by $\mathrm{Nef}(X)$.

Since the cone $\mathrm{Eff}^1(X)^\vee$ has infinite volume in $N_1(X)_\mathbb{R}$, a natural means of measuring its "size" is to truncate the cone in an (anti)canonical manner. To do this, consider the hyperplane

$$\mathcal{H}_X := \{C \in N_1(X)_\mathbb{R} : \langle -K_X, C\rangle = 1\}.$$

Note that since $-K_X$ is big by hypothesis, $\mathcal{H}_X$ intersects each ray of $\mathrm{Eff}^1(X)^\vee$. We endow $N_1(X)_\mathbb{R}$ with Lebesgue measure ds normalized so that $N_1(X)$ has covolume 1, and we endow $\mathcal{H}_X$ with the induced Leray measure $d\mu$ with respect to the linear form $\langle -K_X, \cdot\rangle$. That is, letting l be the linear form $l(v) = \langle -K_X, v\rangle$, we have $ds = d\mu \wedge dl$. We construct the polytope

$$\mathcal{P}_X := \mathrm{Eff}^1(X)^\vee \cap \mathcal{H}_X$$

and define

$$\alpha(X) := \mathrm{Vol}(\mathcal{P}_X) = \int_{\mathcal{P}_X} d\mu.$$

There are variants of this definition differing only by a dimensional factor. Let $\rho = \dim N_1(X)_\mathbb{R}$ and

$$\mathcal{C}_X := \{C \in \mathrm{Eff}^1(X)^\vee : \langle -K_X, C\rangle \leq 1\}$$

be the convex hull of $\mathcal{P}_X$ and the origin. Then a simple slicing argument shows that $\alpha(X) = \rho \cdot \mathrm{Vol}(\mathcal{C}_X)$. Additionally,

$$\alpha(X) = \frac{1}{(\rho-1)!} \int \cdots \int_{\mathrm{Eff}^1(X)^\vee} \exp\left(-\langle -K_X, s\rangle\right) ds,$$

with the bigness of $-K_X$ ensuring the convergence of the integral.

Example 2.1. Let us compute $\alpha(\mathbb{P}^2)$. We have $N^1(\mathbb{P}^2)_\mathbb{R} \cong \mathbb{R}^1$, with the real number $x \in \mathbb{R}$ corresponding to the (real) divisor class xL, where L is the class of a line in $\mathbb{P}^2$. Then the nef cone $\mathrm{Nef}(\mathbb{P}^2) = \{x \in \mathbb{R} : x \geq 0\}$ and the anticanonical class corresponds the real number 3. The hyperplane $\mathcal{H}_{\mathbb{P}^2}$ is just $\{\frac{1}{3}\}$. The polytope $\mathcal{P}_{\mathbb{P}^2}$ is also $\{\frac{1}{3}\}$ and the convex hull $\mathcal{C}_{\mathbb{P}^2} = [0, \frac{1}{3}]$. Thus $\mathcal{C}_{\mathbb{P}^2}$ has volume $\frac{1}{3}$ and so $\alpha(\mathbb{P}^2) = 1 \cdot \mathrm{Vol}(\mathcal{C}_{\mathbb{P}^2}) = \frac{1}{3}$.

Example 2.2. Let X_8 be the blowup of $\mathbb{P}^2$ at a single point. Let L be the class of the pullback of a line to X_8 and let E be the class of the exceptional divisor. Then $N^1(X_8)$ is generated by L and E. In $N^1(X_8)_\mathbb{R} \cong \mathbb{R}^2$, with (a, b) corresponding to $aL + bE$, the nef cone $\mathrm{Nef}(X_8)$ is equal to

$$\{(a, b) : a \geq 0, a + b \geq 0\},$$

that is, the cone with extremal rays spanned by L and $L - E$. The anticanonical class corresponds to the point $(3, -1)$. The hyperplane $\mathcal{H}_{X_8}$ is the line $3a + b = 1$. One checks that $\mathcal{P}_{X_8}$ is the segment joining the points $(\frac{1}{3}, 0)$ and $(\frac{1}{2}, -\frac{1}{2})$. Then $\mathcal{C}_{X_8}$ is the triangle with vertices the above two points together with the origin. The area of this triangle is $\frac{1}{12}$, and so $\alpha(X_8) = 2 \operatorname{Vol} \mathcal{C}_{X_8} = \frac{1}{6}$.

Terminology. Peyre [1995] introduced the notation $\alpha(X)$, but did not give a name to this quantity. We will refer $\alpha(X)$ as the "nef cone volume of X" whenever X is a surface.

3. Generalized Del Pezzo surfaces

As stated in the introduction, a *generalized Del Pezzo surface* is a smooth projective rational surface Y on which $-K_Y$ is big and nef. If Y is defined over an algebraically closed field, Y is one of $\mathbb{P}^2$, $\mathbb{P}^1 \times \mathbb{P}^1$, the Hirzebruch surface $\mathbb{F}_2$, or $\mathbb{P}^2$ blown up at $1 \leq r \leq 8$ points in almost general position [Demazure 1980, Definition III.2.1]. To blow up r points on $\mathbb{P}^2$ in almost general position is to construct a sequence of morphisms

$$Y = Y_r \to Y_{r-1} \to \cdots \to Y_1 \to Y_0 = \mathbb{P}^2,$$

where each map $Y_i \to Y_{i-1}$ is the blowup of Y_{i-1} at a point $p_i \in Y_{i-1}$ not lying on any irreducible curves of self-intersection number -2 on Y_i.

For $n \in \{1, 2\}$, a $(-n)$-*class* on Y is a divisor class D such that $\langle D, D\rangle = -n$ and $\langle D, -K_Y\rangle = 2 - n$. If such a class is effective, then there is necessarily a unique curve in that class. If this curve is irreducible, we use the term $(-n)$-*curve* both for this curve and its class. It follows from the genus formula that a $(-n)$-curve is a smooth rational curve. A simple calculation [Demazure 1980, Tables 2 and 3] shows that the sets of (-1)- and (-2)-classes on a generalized Del Pezzo surface are finite.

Let Y be a generalized Del Pezzo surface defined over a field $\mathbb{K}$. We denote $Y \times_\mathbb{K} \overline{\mathbb{K}}$ by $\overline{Y}$. Recall that a generalized Del Pezzo surface Y is an ordinary Del Pezzo surface if and only if the anticanonical class $-K_Y$ is ample. Equivalently, there are no (-2)-curves on $\overline{Y}$.

Convention 3.1. Throughout the paper, we will use X to refer to an ordinary Del Pezzo surface and Y to refer to a generalized (possibly ordinary) Del Pezzo surface.

The absolute Galois group $G_{\mathbb{K}} = \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ acts on $N^1(\overline{Y})$.

Definition 3.2. A generalized Del Pezzo surface Y is *split* if $Y(\mathbb{K}) \neq \varnothing$ and the action of $G_{\mathbb{K}}$ on $N^1(\overline{Y})$ is trivial.

Apart from the exceptional cases where $\overline{Y}$ is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$ or $\mathbb{F}_2$, the existence of a rational point assures that Y is a blowup of $\mathbb{P}^2$ and the triviality of the Galois action assures that each exceptional divisor is defined over $\mathbb{K}$, and thus the sequence of blown-up points must themselves be defined over $\mathbb{K}$.

In the remainder of this section, we prove that for a split Y, the effective cone $\mathrm{Eff}^1(Y)$ is generated by the set of (-1)- and (-2)-curves on Y, collecting a number of useful facts along the way.

By the following lemma, the group $N^1(Y)$ depends only on the degree of Y. We will make frequent use of this well-known result.

Lemma 3.3. *Let X be a split ordinary Del Pezzo surface and let Y be a split generalized Del Pezzo surface of the same degree $d \leq 7$. There is an isomorphism of $N^1(X)$ and $N^1(Y)$ which identifies the intersection forms and takes $-K_X$ to $-K_Y$.*

Proof. Say X is the blowup of $\mathbb{P}^2$ at points $p_1, \dots, p_r \in \mathbb{P}^2$, $r = 9 - d$, with blowdown $\pi_X : X \to \mathbb{P}^2$, and say Y is obtained by blowing up $\mathbb{P}^2$ at points $q_1, \dots, q_r$:

$$\pi_Y : Y = Y_r \to Y_{r-1} \to \cdots \to Y_1 \to Y_0 = \mathbb{P}^2$$

where $Y_j = \mathrm{Bl}_{q_j}(Y_{j-1})$, $q_j \in Y_{j-1}$. Let $E_{X,j}$ be the exceptional divisor over p_j, and let $E_{Y,j}$ be the total transform in Y of the exceptional divisor over q_j. (That is, if $f_j : Y \to Y_{j-1}$, then $E_{Y,j} = f_j^{-1}(q_j)$, scheme-theoretically.)

Then $N^1(X)$ is the free abelian group on $L_X = \pi_X^* \mathcal{O}_{\mathbb{P}^2}(1)$, $E_{X,1}, \dots, E_{X,r}$. Similarly, $N^1(Y)$ is the free abelian group on $L_Y = \pi_Y^* \mathcal{O}_{\mathbb{P}^2}(1)$, $E_{Y,1}, \dots, E_{Y,r}$. The intersection form on $N^1(X)$ is given in this basis by the diagonal matrix with entries $(1, -1, \dots, -1)$; the intersection form on $N^1(Y)$ is given in this basis by the same matrix. We have $-K_X = 3L_X - \sum E_{X,j}$ and $-K_Y = 3L_Y - \sum E_{Y,j}$. □

Remark 3.4. Note that the identification made in the proof of Lemma 3.3 is not necessarily unique; see [Harbourne 1985, Theorem 0.1].

The next lemma is a modest generalization of [Hassett and Tschinkel 2004, Proposition 4.5].

Lemma 3.5. *Let S be a surface and let $D_1, \dots, D_k$ be irreducible effective divisors on S. Let Γ denote the cone generated by $D_1, \dots, D_k$. Then the effective cone of S is equal to Γ if and only if $\Gamma^\vee \subset \Gamma$.*

Proof. If the effective cone of S is equal to Γ then it is a closed cone. The nef cone $\mathrm{Nef}(S) = \Gamma^\vee$ is contained in the closure of the effective cone, which is just Γ.

For the converse, it is clear that Γ is contained in the effective cone of S. Let D be an effective divisor. Then we can write $D = D' + a_1D_1 + \cdots + a_kD_k$ with $a_i \geq 0$ and D' having none of the D_i as an irreducible component. It is clear that D' is contained in $\Gamma^\vee$, and by hypothesis, D' is consequently contained in Γ. Hence the same is true of D. □

Proposition 3.6. *If Y is a split generalized Del Pezzo surface, every (-1)-class in $N^1(Y)$ is effective. Indeed, if E is any (-1)-class, then either*

(1) *E is a (-1)-curve, or*

(2) *E can be written as the sum of a (-1)-curve and one or more (-2)-curves, or*

(3) *$d = 1$ and E can be written as the sum of $-K_Y$ and one or more (-2)-curves.*

Proof. See [Demazure 1980, Theorem III.2.c]. □

For a split generalized Del Pezzo surface Y of degree $d \geq 2$, this shows that every (-1)-class is a nonnegative integral linear combination of (-1)- and (-2)-curves. By the following lemma, this holds also in degree $d = 1$ if we allow rational instead of integral coefficients.

Lemma 3.7. *For a split generalized Del Pezzo surface Y of degree 1, the anticanonical class $-K_Y$ is a linear combination of (-1)- and (-2)-curves with nonnegative rational coefficients.*

Proof. Let X be an ordinary Del Pezzo surface of degree 1. It is easy to check that the sum of all (-1)-classes on X is $-240K_X$.

Using the identification of Lemma 3.3, the sum of all (-1)-classes on Y is $-240K_Y$. Using Proposition 3.6, we can write n of the (-1)-classes as the sum of a (-1)-curve and possibly some (-2)-curves, and the remaining $240 - n$ of the (-1)-classes as the sum of $-K_Y$ and some (-2)-classes. Note that $E_{Y,8}$ in the proof of Lemma 3.3 is a (-1)-curve on Y, so we have $n > 0$.

This gives us $-240K_Y$ as the sum of n (-1)-curves, $-(240-n)K_Y$, and some (-2)-curves. We transform this equation to write $-nK_Y$ as a sum of (-1)- and (-2)-curves. □

Lemma 3.8. *Let Y be a split generalized Del Pezzo surface and let E be a (-1)-class in $N^1(Y)$. Then E is irreducible if and only if $\langle E, C\rangle$ is nonnegative for every (-2)-curve C.*

Proof. See [Demazure 1980, Corollary on page 46]. □

In the case of ordinary Del Pezzo surfaces, the following result is well-known.

Proposition 3.9. *Let X be a split ordinary Del Pezzo surface of degree $d \leq 7$. Then the effective cone of X is minimally generated by the (-1)-classes on X, all of which are (-1)-curves.*

Proof. This can be proved directly (see [Hartshorne 1977, Theorem V.4.11] for a proof when $d = 3$) or can be taken as an immediate consequence of the calculation of generators for the Cox ring given in [Batyrev and Popov 2004, Theorem 3.2], making use of Lemma 3.7 in the case $d = 1$. □

We now reach our main goal for this section.

Theorem 3.10. *If Y is a split generalized Del Pezzo surface and has degree $d \leq 7$, the effective cone of Y is finitely generated by the set of (-1)- and (-2)-curves.*

Proof. Let Γ be the cone generated by the (-1)- and (-2)-curves on Y. To prove the theorem, it suffices by Lemma 3.5 to show that $\Gamma^\vee \subset \Gamma$. Let X be a split ordinary Del Pezzo surface of the same degree as Y. Identify $N^1(X)$ and $N^1(Y)$ as in Lemma 3.3. Note that this identification takes (-1)-classes to (-1)-classes. By Proposition 3.9, $\mathrm{Eff}^1(X)$ is generated by (-1)-classes. Each (-1)-class lies in Γ by Proposition 3.6 and Lemma 3.7. Therefore $\mathrm{Eff}^1(X) \subset \Gamma$. It follows immediately that $\Gamma^\vee \subset \mathrm{Eff}^1(X)^\vee$. From Lemma 3.5 we have $\mathrm{Eff}^1(X)^\vee \subset \mathrm{Eff}^1(X)$. Thus $\Gamma^\vee \subset \Gamma$ and hence $\Gamma = \mathrm{Eff}^1(Y)$, again by Lemma 3.5. □

Remark 3.11. A generalization of Theorem 3.10 has already been proved by Lahyane and Harbourne [2005, Lemma 4.1]. We include our presentation both as a summary of results that we will use later and also because the approach here seems to have interest in its own right.

Corollary 3.12. *Let X be a split ordinary Del Pezzo surface and Y a split generalized Del Pezzo surface with $\deg(X) = \deg(Y) \leq 7$. Identifying $N^1(X)$ and $N^1(Y)$ as in Lemma 3.3, we have $\mathrm{Eff}^1(X) \subset \mathrm{Eff}^1(Y)$ and $\mathrm{Nef}(X) \supset \mathrm{Nef}(Y)$.*

Let $\Gamma \subset N^1(Y)_{\mathbb{R}}$ be the cone spanned by the set of (-2)-curves on Y. Then $\mathrm{Eff}^1(Y)$ is the sum of $\mathrm{Eff}^1(X)$ and Γ, and $\mathrm{Nef}(Y) = \mathrm{Nef}(X) \cap \Gamma^\vee$. □

4. Inductive method

With these preliminaries in place, we now turn to proving Theorem 1.2. For a generalized Del Pezzo surface Y and any class $D \in N^1(Y)_{\mathbb{R}}$, we denote by $D^\perp$ the hyperplane

$$D^\perp := \{C \in N_1(Y)_{\mathbb{R}} : \langle D, C\rangle = 0\}.$$

Lemma 4.1. *Let Y be a split generalized Del Pezzo surface and E a (-1)-curve on Y. Let $\pi_E : Y \to Y_E$ be the contraction of E. Then*

$$\pi_E^* : N^1(Y_E) \longrightarrow E^\perp \cap N^1(Y)$$

is an isomorphism and induces an isomorphism of convex cones,

$$\pi_E^*(\mathrm{Nef}(Y_E)) = \mathrm{Nef}(Y) \cap E^\perp.$$

Proof. We have $N^1(Y) = \pi_E^*(N^1(Y_E)) \oplus \mathbb{Z}E$. We may identify $\mathrm{Nef}(Y_E)$ with $\pi_E^*(\mathrm{Nef}(Y_E)) \subset E^\perp$. The inclusion $\pi_E^*(\mathrm{Nef}(Y_E)) \subset \mathrm{Nef}(Y)$ follows immediately from the projection formula. This proves $\pi_E^*(\mathrm{Nef}(Y_E)) \subset \mathrm{Nef}(Y) \cap E^\perp$.

For the reverse inclusion, let $D \in \mathrm{Nef}(Y) \cap E^\perp$. Since $E^\perp = \pi_E^*(N^1(Y_E))$, we have $D = \pi_E^* \pi_{E*} D$. Again by the projection formula, for any curve $C \subset Y_E$,

$$\langle \pi_{E*} D, C\rangle_{Y_E} = \langle D, \pi_E^* C\rangle \geq 0,$$

since $D \in \mathrm{Nef}(Y)$. □

We now prove the first of our main theorems. We repeat it here for convenience.

Theorem 1.2. *Let Y be a split generalized Del Pezzo surface of degree $d \leq 7$. For each E in the set $\mathscr{C}$ of (-1)-curves on Y, let Y_E denote the split generalized Del Pezzo surface of degree $d+1$ obtained by contracting E. Then*

$$\alpha(Y) = \sum_{E \in \mathscr{C}} \frac{1}{d(9-d)} \alpha(Y_E).$$

Proof. We follow the argument used in [Derenthal 2007, Theorem 4]. Let $\mathscr{E}$ be the set of (-1)- and (-2)-curves on Y. Then $\mathscr{E}$ is exactly the set of generators for $\mathrm{Eff}^1(Y)$ described in Theorem 3.10. Recall that the hyperplane $\mathscr{H}_Y$ is defined as

$$\mathscr{H}_Y = \{C \in N_1(Y)_\mathbb{R} : \langle -K_Y, C\rangle = 1\}.$$

The intersection $\mathscr{P}_Y = \mathrm{Nef}(Y) \cap \mathscr{H}_Y$ is a polytope with faces corresponding to $E \in \mathscr{E}$. For $E \in \mathscr{E}$, let $\mathscr{P}_E \subset \mathscr{H}_Y$ be the convex hull of the vector $\frac{1}{d}(-K_Y)$ and the face $\mathscr{P}_Y \cap E^\perp$. (Note that $-K_Y$ is nef by the definition of generalized Del Pezzo surface and $\frac{1}{d}(-K_Y)$ is in $\mathscr{P}_Y$ since $\langle -K_Y, -K_Y\rangle = d$.) Then

$$\mathscr{P}_Y = \mathrm{Nef}(Y) \cap \mathscr{H}_Y = \bigcup_{E \in \mathscr{E}} \mathscr{P}_E.$$

The intersection of any two of the $\mathscr{P}_E$ has volume zero in $\mathscr{H}_Y$ because the intersection lies in a subspace of dimension strictly less than that of $\mathscr{H}_Y$. Therefore,

$$\alpha(Y) = \mathrm{Vol}\,\mathscr{P}_Y = \sum_{E \in \mathscr{E}} \mathrm{Vol}\,\mathscr{P}_E.$$

For each (-2)-curve E, $\langle K_Y, E\rangle = 0$ and hence $\frac{1}{d}(-K_Y) \in E^\perp$. Thus $\mathscr{P}_E$ lies in the hyperplane $\mathscr{H}_Y \cap E^\perp$ of dimension $\dim(\mathscr{H}_Y) - 1$, and so $\mathscr{P}_E$ has volume zero. We thus reduce to $\mathrm{Vol}\,\mathscr{P}_Y = \sum_{E \in \mathscr{C}} \mathrm{Vol}\,\mathscr{P}_E$.

For $E\in\mathscr{C}$, let $\pi_E : Y\to Y_E$ be the contraction. By Lemma 4.1 we have $\pi_E^*\mathscr{H}_{Y_E} = \mathscr{H}_Y \cap E^\perp$. This identifies the base of the cone $\mathscr{P}_E$ as $\mathscr{P}_Y\cap E^\perp = \pi_E^*\mathscr{P}_{Y_E}$. Thus $\mathscr{P}_E$ is a cone of dimension $9-d$ with height $1/d$ and base volume $\operatorname{Vol}(\pi_E^*\mathscr{P}_{Y_E})$. By Lemma 4.1, the sublattices $N^1(Y_E)\subset N^1(Y_E)_{\mathbb{R}}$ and $\pi_E^*(N^1(Y_E)) = E^\perp \cap N^1(Y)\subset E^\perp$ are isomorphic, so π_E^* is volume-preserving and $\operatorname{Vol}(\pi_E^*\mathscr{P}_{Y_E}) = \operatorname{Vol}\mathscr{P}_{Y_E} = \alpha(Y_E)$. Consequently,

$$\operatorname{Vol}\mathscr{P}_E = \frac{1}{d(9-d)}\operatorname{Vol}\mathscr{P}_{Y_E} = \frac{1}{d(9-d)}\alpha(Y_E).$$

Summing over $E\in\mathscr{C}$ gives the desired result. □

Remark 4.2. This generalization explains why Theorem 1.1 does not hold for $d=7$. When one blows down a (-1)-curve on an ordinary Del Pezzo surface of degree d for $d\le 7$ the result is an ordinary Del Pezzo surface of degree $d+1$. For $d\le 6$, the resulting ordinary Del Pezzo surfaces all have the same nef cone volume. This is no longer true when $d=7$. Let X_d denote an ordinary Del Pezzo surface of degree d obtained by blowing up $9-d$ points in general position on $\mathbb{P}^2$. Recall that $X_7=\operatorname{Bl}_{p,q}(\mathbb{P}^2)$ contains three (-1)-curves: the exceptional divisors E_p and E_q, and the proper transform L_{pq} of the line through p and q. Contracting E_p or E_q results in an X_8, while contracting L_{pq} results in $\mathbb{P}^1\times\mathbb{P}^1$. We have

$$\alpha(X_7) = \frac{1}{14}(2\alpha(X_8)+\alpha(\mathbb{P}^1\times\mathbb{P}^1)) = \frac{1}{24}$$

since $\alpha(X_8)=\frac{1}{6}$ and $\alpha(\mathbb{P}^1\times\mathbb{P}^1)=\frac{1}{4}$.

5. Root systems and Weyl groups

In this section, we recall some of the basic facts about the root system of (-2)-classes on a Del Pezzo surface and its associated Weyl group. We use this structure in our second main result which relates the nef cone volumes of split generalized and ordinary Del Pezzo surfaces of the same degree.

5A. *Root systems.*

Definition 5.1. A *root system* R is a finite collection of nonzero vectors in a finite-dimensional real vector space V with a nondegenerate definite inner product $\langle\cdot,\cdot\rangle$ satisfying the following conditions.

(1) The set R spans V, namely R is essential.

(2) For each $x\in R$, let $s_x : V\to V$ be the reflection through the hyperplane orthogonal to x:

$$s_x(v) = v - 2\frac{\langle x,v\rangle}{\langle x,x\rangle}x.$$

For each $x\in R$, it is required that s_x takes R to R.

(3) For every $x_1, x_2 \in R$,
$$2\frac{\langle x_1, x_2\rangle}{\langle x_2, x_2\rangle}$$
is an integer, that is, R is crystallographic.

(4) If $x \in R$ and $cx \in R$, then $c \in \{1, -1\}$, that is, R is reduced.

Definition 5.2. A morphism of root systems from $R \subset V$ to $R' \subset V'$ is a linear map $\Phi : V \to V'$ such that (1) $\Phi(R) \subset R'$, and (2) Φ preserves inner products up to a scalar multiple, that is, there is a $c \in \mathbb{R}$ such that $\langle \Phi(x), \Phi(y)\rangle = c \cdot \langle x, y\rangle$. Equivalently, the integers $2\langle x_1, x_2\rangle/\langle x_2, x_2\rangle$ are preserved for all $x_1, x_2 \in R$.

Remark 5.3. We will sometimes refer to a root system R in a vector space V even when R does not span V. Strictly speaking, R is only a root system in the subspace it spans, but this minor abuse of language should not cause any confusion.

We recall some standard notions; for details, see [Humphreys 1990, Section 1.3], [Bourbaki 2002, Section VI.1.2], [Hall 2003, Chapter 8]. Any hyperplane in V not containing any root of R divides R into two subsets, with *positive roots* on one side (and negative roots on the other side). Those positive roots which cannot be written as a sum of other positive roots with positive coefficients form a set of *simple roots*. Each set of simple roots (for each choice of a set of positive roots) is a linearly independent set such that every root in R is either a sum of simple roots with nonnegative coefficients or a sum of simple roots with nonpositive coefficients.

A decomposition of R is a disjoint union $R = R_1 \cup \cdots \cup R_k$ such that the span of R is the direct sum of the spans of the R_j, each R_j is a root system in its span, and the spans of the R_j are orthogonal to each other. If R admits no nontrivial decomposition, then R is an *irreducible root system*. If R is reducible, it has a unique (up to order) decomposition into irreducible root systems, called the *irreducible components* of R.

Recall the classification of root systems by *Dynkin diagrams*. For a root system R and a choice of a set R_0 of simple roots in R, the Dynkin diagram of R is the graph with vertex set R_0 and an edge joining two vertices if and only the corresponding roots are not perpendicular. One labels the edges of the graph according to the angle between the roots and their relative length; for details, see [Bourbaki 2002]. The Dynkin diagram is independent of the choice of a set of simple roots. The irreducible root systems correspond to connected graphs. The irreducible components of a reducible root system R correspond exactly to the connected components of the Dynkin diagram of R. One has the well-known classification of irreducible root systems corresponding to Dynkin diagrams of types $\mathbf{A}_n$ for $n \geq 1$, $\mathbf{B}_n$ for $n \geq 2$, $\mathbf{C}_n$ for $n \geq 3$, $\mathbf{D}_n$ for $n \geq 4$, $\mathbf{E}_n$ for $6 \leq n \leq 8$, $\mathbf{F}_4$ and $\mathbf{G}_2$.

The group of orthogonal transformations generated by all $s_x, x \in R$, is finite and is called the *Weyl group* $W(R)$. A *wall* in V is a hyperplane orthogonal to an

root system R	$\mathbf{A}_n$	$\mathbf{D}_n$	$\mathbf{E}_6$	$\mathbf{E}_7$	$\mathbf{E}_8$
$\#W(R)$	$(n+1)!$	$2^{n-1}\cdot n!$	$2^7\cdot 3^4\cdot 5$	$2^{10}\cdot 3^4\cdot 5\cdot 7$	$2^{14}\cdot 3^5\cdot 5^2\cdot 7$

Table 2. The orders of simply laced Weyl groups.

root system R	$\mathbf{B}_n$	$\mathbf{C}_n$	$\mathbf{F}_4$	$\mathbf{G}_2$
$\#W(R)$	$2^n\cdot n!$	$2^n\cdot n!$	$2^7\cdot 3^2$	$2^2\cdot 3$

Table 3. The orders of nonsimply laced Weyl groups.

$x \in R$. Removing the walls from V leaves a finite set of open convex cones called *chambers*. The action of $W(R)$ permutes these chambers simply transitively.

Table 2 lists all of the *simply laced* root systems (those in which all roots have the same self-intersection) and the orders of their Weyl groups. Table 3 gives the same data for the nonsimply laced root systems.

5B. ***Root systems on Del Pezzo surfaces.*** Let Y be a split generalized Del Pezzo surface of degree $d \leq 7$. By [Manin 1986, Sections 23–25], the finite set R_d of (-2)-classes on Y is a root system in $N^1(Y)_{\mathbb{R}}$ and of course depends only on the degree d. For $d \leq 6$, the roots span the hyperplane $(-K_Y)^{\perp}$. The classification of this root system is shown in Table 4.

Not only is R_d a root system, but in fact the subset of (-2)-classes that are effective on Y gives rise to a root system [Demazure 1980, Theorem III.2.b].

Theorem 5.4 (Demazure). *Let Y be a split generalized Del Pezzo surface of degree $d \leq 6$ and let R_Y^+ be the set of effective (-2)-classes on Y. Then $R_Y := R_Y^+ \cup -R_Y^+$ is a root system in $N^1(Y)$ whose simple roots are the (-2)-curves of Y and whose positive roots are R_Y^+. It is contained in R_d.* □

Remark 5.5. Urabe [1983, Main Theorem] has shown that every root system contained in R_d occurs as the root system R_Y of a generalized Del Pezzo surface Y of degree d as in Theorem 5.4, with four exceptions: the subsystem of type $7\mathbf{A}_1$ in R_2 and the subsystems of type $7\mathbf{A}_1$, $8\mathbf{A}_1$, and $\mathbf{D}_4+4\mathbf{A}_1$ in R_1.

Remark 5.6. The root system R_Y can have irreducible components of the following types: $\mathbf{A}_1, \dots, \mathbf{A}_8$, $\mathbf{D}_4, \dots, \mathbf{D}_8$, $\mathbf{E}_6$, $\mathbf{E}_7$, $\mathbf{E}_8$.

For Y of degree $d \geq 3$, consider the anticanonical morphism ϕ defined by the linear series $|-K_Y|$ which maps Y to a projective space of dimension d. For $d = 2$

d	7	6	5	4	3	2	1
R_d	$\mathbf{A}_1$	$\mathbf{A}_1\times\mathbf{A}_2$	$\mathbf{A}_4$	$\mathbf{D}_5$	$\mathbf{E}_6$	$\mathbf{E}_7$	$\mathbf{E}_8$

Table 4. Classification of root systems R_d.

(respectively, $d = 1$), let ϕ be the morphism defined by the linear series $|-2K_Y|$ (respectively, $|-3K_Y|$). Let Y' be the image of Y under ϕ. The map ϕ sends the union of (-2)-curves corresponding to any connected component of the Dynkin diagram to a singularity of Y', while it is an isomorphism between the complement of the (-2)-curves on Y and the complement of the singularities on Y'. Each singularity on Y' is a rational double point. Its type in the **ADE**-classification is given by the type of the corresponding irreducible Dynkin diagram. The surface Y' is a singular Del Pezzo surface, whose minimal desingularization is the generalized Del Pezzo surface Y.

5C. ***Weyl groups and nef cone volume.*** We proceed with the proof of our second main result, which we repeat here for the convenience of the reader.

Theorem 1.3. *Let Y be a split generalized Del Pezzo surface of degree $d \le 7$ and let X be a split ordinary Del Pezzo surface of the same degree. Then*

$$\alpha(Y) = \frac{1}{\#W(R_Y)}\alpha(X),$$

where $W(R_Y)$ is the Weyl group of the root system R_Y whose simple roots are the (-2)-curves on Y.

Proof. Identify $N^1(X)$ and $N^1(Y)$ as in Lemma 3.3.

With notation as in the statement of Theorem 5.4, let C be the open convex cone in $N_1(Y)_{\mathbb{R}}$ dual to the cone spanned by the (-2)-curves of Y. That is,

$$C = \{\, v \in N_1(Y)_{\mathbb{R}} : \langle v, x\rangle > 0 \text{ for all } (-2)\text{-curves } x \text{ on } Y\}.$$

Since the (-2)-curves are a system of simple roots of R_Y, C is a single chamber for the Weyl group $W(R_Y)$. Recall that by Corollary 3.12, $\mathrm{Nef}(Y) = \mathrm{Nef}(X) \cap \overline{C}$. Intersecting with the hyperplane $\mathcal{H}_X$ gives $\mathcal{P}_Y = \overline{C} \cap \mathcal{P}_X$. We have

$$N^1(X)_{\mathbb{R}} = \bigcup_{w\in W(R_Y)} \overline{wC},$$

so

$$\mathcal{P}_X = \bigcup_{w\in W(R_Y)} \left(\overline{wC} \cap \mathcal{P}_X\right).$$

The sets $\overline{wC} \cap \mathcal{P}_X$, $w \in W(R_Y)$, are pairwise disjoint except along boundaries, which have zero volume. The action of $W(R_Y)$ preserves volume and fixes $\mathrm{Nef}(X)$ and $-K_X$. Therefore it fixes $\mathcal{P}_X$, and we have

$$\begin{aligned}\alpha(X) = \mathrm{Vol}\,\mathcal{P}_X = \sum_{w\in W(R_Y)} \mathrm{Vol}(\overline{wC}\cap\mathcal{P}_X) &= \#(W(R_Y))\ \mathrm{Vol}(\overline{C}\cap\mathcal{P}_X)\\ &= \#(W(R_Y))\ \mathrm{Vol}\,\mathcal{P}_Y = \#(W(R_Y))\cdot\alpha(Y).\end{aligned}$$ □

Remark 5.7. As in Remark 5.6, let Y' be the singular Del Pezzo surface whose minimal desingularization is Y. The number $\#W(R_Y)$, and therefore $\alpha(Y)$, can be determined directly from the types of singularities on Y' as follows. The types R of the singularities of Y' coincide with the types of the irreducible components of R_Y. The orders of their Weyl groups $W(R)$ can be found in Table 2. Their product is $\#W(R_Y)$.

6. Nonsplit generalized Del Pezzo surfaces

We recall some facts about the geometry of generalized Del Pezzo surfaces that are not split and then introduce the notion of orbit root systems. The results collected here will be used in Section 7 to relate the nef cone volume of nonsplit generalized Del Pezzo surfaces to the nef cone volume of ordinary Del Pezzo surfaces.

6A. ***The Galois action.*** Throughout this section, we let Y be a generalized Del Pezzo surface of degree $d \leq 7$ defined over a perfect field $\mathbb{K}$ and we assume that Y contains a $\mathbb{K}$-rational point; we let $\overline{Y} = Y \times_{\mathbb{K}} \overline{\mathbb{K}}$. The Galois group $G_{\mathbb{K}} = \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ acts on $N^1(\overline{Y})$, and each automorphism of $N^1(\overline{Y})$ induced by an element of $G_{\mathbb{K}}$ preserves both the intersection form and the anticanonical class.

Proposition 6.1. *The group of automorphisms of $N^1(\overline{Y})$ which preserve the intersection form $\langle \cdot, \cdot \rangle$ and the anticanonical class $-K_Y$ is canonically isomorphic to $W(R_d)$.*

Proof. The result for ordinary Del Pezzo surfaces can be found in [Manin 1986, Theorem 23.9]. (The statement there is given only for $d \leq 6$, but the $d = 7$ case is an easy calculation.) The result holds for generalized Del Pezzo surfaces via the identification described in Lemma 3.3. □

Thus the action of $G_{\mathbb{K}}$ factors through (a subgroup of) the finite group $W(R_d)$.

Proposition 6.2. *Let Y be a generalized Del Pezzo surface defined over the field $\mathbb{K}$ containing a $\mathbb{K}$-rational point. Then $N^1(Y) = N^1(\overline{Y})^{G_{\mathbb{K}}}$.*

Recall that if S is a set on which the group G acts, the standard notation

$$S^G = \{s : gs = s \text{ for all } g \in G\}$$

denotes the set of fixed points of the action.

Proof. A result of Colliot-Thélène and Sansuc [1987, Theorem 2.1.2, Claim (iii)] assures that under the hypotheses of the proposition, $\mathrm{Pic}(Y) = \mathrm{Pic}(\overline{Y})^{G_{\mathbb{K}}}$. Since the intersection form on $\mathrm{Pic}(\overline{Y})$ is nondegenerate, we have $\mathrm{Pic}(\overline{Y}) = N^1(\overline{Y})$. Finally, to show $N^1(Y) = \mathrm{Pic}(Y)$ it suffices to prove that a divisor is numerically trivial on $\mathrm{Pic}(\overline{Y})$ if it is numerically trivial on $\mathrm{Pic}(Y)$.

Suppose $D \in \operatorname{Pic} Y$ is numerically trivial in $\operatorname{Pic} Y$. Let E be any divisor class on $\overline{Y}$. Recall that the action of $G_{\mathbb{K}}$ on $N^1(\overline{Y})$ factors through the finite Weyl group $W(R_d)$, so the $G_{\mathbb{K}}$-orbit of E is finite. Say this orbit is $\{E_1, \dots, E_s\}$. Since $G_{\mathbb{K}}$ preserves the intersection form on $\overline{Y}$ and D is $G_{\mathbb{K}}$-invariant,

$$\langle D, E\rangle = \frac{1}{s}\sum_i \langle D, E_i\rangle = \Big\langle D, \frac{1}{s}\sum_i E_i\Big\rangle = 0$$

because $(1/s)\sum E_i$ lies in $(\operatorname{Pic} \overline{Y})^{G_{\mathbb{K}}} = \operatorname{Pic} Y$.

With the above results put together, $N^1(Y) = \operatorname{Pic}(Y) = \operatorname{Pic}(\overline{Y})^{G_{\mathbb{K}}} = N^1(\overline{Y})^{G_{\mathbb{K}}}$, which proves the proposition. □

We now explain the relation between the effective cone of Y and that of $\overline{Y}$.

Proposition 6.3. *The effective cone of Y is equal to the cone of $G_{\mathbb{K}}$-invariant effective classes of $\overline{Y}$, that is,*

$$\operatorname{Eff}^1(Y) = \operatorname{Eff}^1(\overline{Y})^{G_{\mathbb{K}}}.$$

Proof. By Proposition 6.2, we have $N^1(Y) = N^1(\overline{Y})^{G_{\mathbb{K}}}$. It is clear that

$$\operatorname{Eff}^1(Y) \subseteq \operatorname{Eff}^1(\overline{Y})^{G_{\mathbb{K}}}.$$

To show the reverse inclusion, first note that if D is any effective divisor on $\operatorname{Eff}^1(\overline{Y})$, with $\mathbb{L}$ being a finite Galois extension of $\mathbb{K}$ over which D is defined, then $\sum_{\sigma \in \operatorname{Gal}(\mathbb{L}/\mathbb{K})} \sigma(D) \in \operatorname{Eff}^1(Y)$. For any $D \in \operatorname{Eff}^1(\overline{Y})^{G_{\mathbb{K}}}$ that is defined over a finite Galois extension $\mathbb{L}/\mathbb{K}$, we have

$$D = \frac{1}{\#\operatorname{Gal}(\mathbb{L}/\mathbb{K})} \sum_{\sigma \in \operatorname{Gal}(\mathbb{L}/\mathbb{K})} \sigma(D).$$

This completes the proof. □

The action of $G_{\mathbb{K}}$ on $N^1(\overline{Y})$ induces an action both on the set of (-1)-curves and on the set of (-2)-curves.

Corollary 6.4. *A set of generators for the effective cone of Y consists of, for each orbit of $G_{\mathbb{K}}$ on the sets of (-1)-curves and (-2)-curves, the sum of the classes in that orbit.* □

Note that this set of generators may fail to be minimal. (See rows 3, 6 and 9 of Table 8 for examples.)

6B. ***Orbit root systems.*** We will use the following construction in Section 7A in the case of $G_{\mathbb{K}}$ acting on the root system $R_{\overline{Y}} \subset N^1(\overline{Y})$ (as in Theorem 5.4) of $\overline{Y}$, in order to obtain a root system in $N^1(Y)$.

Definition 6.5. Let $R \subset V$ be a possibly reducible root system with a chosen set Π of positive roots. Suppose a group G acts linearly on V in such a way that it permutes the elements of R, preserves the inner product between elements of R and preserves positivity. In this case, we say that G acts on R. The set

$$\mathbb{O}(R, G) := \Big\{ \sum_{x \in \mathbb{O}} x : \mathbb{O} \text{ is a } G\text{-orbit of an element of } R \Big\}$$

is called the *orbit root system* of R with respect to G. (We show below that $\mathbb{O}(R, G)$ is indeed a root system.)

Proposition 6.6. *Let $R \subset V$ be an irreducible root system with a chosen positive system Π. Suppose G acts on R. Then $\mathbb{O}(R, G)$ is an irreducible root system as in Table 5. The simple* (*respectively*, *positive*) *roots of* $\mathbb{O}(R, G)$ *are the sums of elements of orbits of simple* (*respectively*, *positive*) *roots of R.*

Proof. Any group action which preserves inner products and positivity must necessarily act as an automorphism of the Dynkin diagram. Indeed, the group takes nonsimple roots to nonsimple roots, and thus takes simple roots to simple roots. Thus the group acts on the vertices of the Dynkin diagram; since the edges (and edge labelings) are determined by the inner product, they are preserved by the group. We check case by case that all nontrivial admissible group actions on irreducible Dynkin diagrams are listed in Table 5. In each case, a direct calculation shows that $\mathbb{O}(R, G)$ is indeed a root system of the listed type. □

A list similar to Table 5 has been compiled by Kac [1990, Propositions 7.9 and 7.10]. The main difference between our list and Kac's is that we use the sum of roots in an orbit, while he uses the average; because of this difference Kac's approach sometimes gives the dual root system to ours.

Lemma 6.7. *Let $R \subset V$ be a possibly reducible root system with a chosen positive system Π. Suppose G acts on R. Then G acts on the irreducible components of R in the following sense. If $R = \bigcup_{i=1}^{n} R_i$ is a decomposition of R into irreducible components and $g \in G$, the image $g(R_i)$ for any i is one of the irreducible components R_j.*

R	G	$\mathbb{O}(R, G)$
$\mathbf{A}_{2n}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbf{B}_n$
$\mathbf{A}_{2n+1}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbf{B}_{n+1}$
$\mathbf{D}_n$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbf{C}_{n-1}$
$\mathbf{D}_4$	$\mathbb{Z}/3\mathbb{Z}$ or $\mathfrak{S}_3$	$\mathbf{G}_2$
$\mathbf{E}_6$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbf{F}_4$

Table 5. Nontrivial irreducible orbit root systems.

Proof. One way to see this is by considering the Dynkin diagram D of R. Each component R_i corresponds to a connected component of the graph D. As noted above, the group G acts as a graph automorphism of D. Then each element of G must take connected components of D to connected components. □

To avoid confusion between the actions of G on R and on the set of irreducible components of R, we refer to orbits in the latter set as "component orbits".

Proposition 6.8. *Let $R \subset V$ be a possibly reducible root system with a chosen positive system Π. Suppose G acts on R. Let $R_1, \dots, R_k$ be irreducible components of R which form a set of component orbit representatives, that is, each component orbit contains exactly one of the R_i. For each i, let $G_i \subset G$ be the subgroup fixing R_i. Then $\mathbb{O}(R, G)$ is a root system and*

$$\mathbb{O}(R, G) \cong \bigcup_{i=1}^{k} \mathbb{O}(R_i, G_i). \tag{$*$}$$

Proof. First, note the right-hand side is indeed a root system. For by Proposition 6.6, each $\mathbb{O}(R_i, G_i)$ is a root system contained in the subspace spanned by R_i (since each element of $\mathbb{O}(R_i, G_i)$ is a sum of one or more elements of R_i). Then if $i \neq j$, by assumption R_i and R_j are distinct irreducible components of R, so they span perpendicular subspaces of V. Therefore $\mathbb{O}(R_i, G_i)$ and $\mathbb{O}(R_j, G_j)$ are perpendicular. Hence the union on the right-hand side of $(*)$ is a perpendicular union of root systems.

Now, the spans of the component orbits are pairwise perpendicular, so we may treat them separately. We consider the orbit $i = 1$, the others being similar. Let the component orbit of R_1 consist of the components $R_{1,1} = R_1, R_{1,2}, \dots, R_{1,p}$. Choosing elements $g_1 = \mathrm{id}_G, g_2, \dots, g_p \in G$ such that $g_i R_1 = R_{1,i}$ for each i, we get isomorphisms

$$(\operatorname{span} R_1, R_1) \cong (\operatorname{span} R_{1,2}, R_{1,2}) \cong \cdots \cong (\operatorname{span} R_{1,p}, R_{1,p}).$$

Under this identification we have an isomorphism of the diagonal

$$\Delta \subset (\operatorname{span} R_1)^p \cong (\operatorname{span} R_{1,1}) \oplus \cdots \oplus (\operatorname{span} R_{1,p})$$

with $\operatorname{span}(R_1)$ by projection onto the first factor. Note that this projection preserves angles and ratios of lengths, but divides all lengths by a factor of $\sqrt{p}$. One can check that the projection takes $\mathbb{O}(R_{1,1} \cup \cdots \cup R_{1,p}, G)$ to $\mathbb{O}(R_1, G_1)$, as desired.

More precisely, if $\mathbb{O}$ is the orbit of $r \in R_1$ under G_1, then $\mathbb{O} \cup g_2\mathbb{O} \cup \cdots \cup g_p\mathbb{O}$ is the orbit of r under G. Then $g_i \sum_{x \in \mathbb{O}} x = \sum_{x \in g_i\mathbb{O}} x$ is an element of $\mathbb{O}(R_{1,i}, g_i G_1 g_i^{-1})$ where $g_i G_1 g_i^{-1}$ is the subgroup of G fixing $R_{1,i}$, while $\sum_{i=1}^{p} g_i \sum_{x \in \mathbb{O}} x$ is an element of $\mathbb{O}(R_{1,1} \cup \cdots \cup R_{1,p}, G)$, which lies in Δ. It is projected to the element $\sum_{x \in \mathbb{O}} x$ of $\mathbb{O}(R_1, G_1)$. □

Corollary 6.9. *In the setting of Proposition 6.8*,

$$W(\mathbb{O}(R,G)) \cong \prod_{i=1}^{k} W(\mathbb{O}(R_i,G_i)). \qquad \square$$

7. Nef cone volume of nonsplit generalized Del Pezzo surfaces

Let Y be a nonsplit generalized Del Pezzo surface of degree at most 7, defined over a perfect field $\mathbb{K}$. As in Section 6 we continue to assume that Y contains a $\mathbb{K}$-rational point. Then $G_{\mathbb{K}} = \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ acts on the set of (-2)-curves on $\overline{Y}$ and on the associated root system. In this situation, we can construct an orbit root system as in Definition 6.5. As in the split case (Theorem 1.3), this allows us to relate the nef cone volume of Y to a volume associated to an ordinary Del Pezzo surface of the same degree. In Section 7B, we compute this volume for all nonsplit Del Pezzo surfaces of degree at least 5.

7A. ***Nef cone volume of pairs.*** Using Proposition 6.1, we can associate to a generalized Del Pezzo surface Y of degree $d \le 7$ the pair $(\overline{Y}, H_Y)$, where $H_Y \subset W(R_d)$ is the image of $G_{\mathbb{K}}$ under the homomorphism

$$G_{\mathbb{K}} \to \mathrm{Aut}\big(N^1(\overline{Y}), \langle\cdot\,,\cdot\rangle, -K_Y\big) \cong W(R_d).$$

Note that $G_{\mathbb{K}}$ and therefore also H_Y acts on the set of (-2)-curves on $\overline{Y}$ and also on the set of its (-1)-curves.

Remark 7.1. To every generalized Del Pezzo surface Y over $\mathbb{K}$ there is the associated pair $(\overline{Y}, H_Y)$, as described above. The "realization problem for pairs" is to describe which pairs $(\overline{Y}, H)$ are obtained in this manner. That is, for which pairs $(\overline{Y}, H)$, consisting of a split generalized Del Pezzo surface $\overline{Y}$ over $\overline{\mathbb{K}}$ of degree d and a subgroup $H \subset W(R_d)$ acting on the set of (-2)-curves, is there a Y defined over $\mathbb{K}$ such that $\overline{Y} = Y \times_{\mathbb{K}} \overline{\mathbb{K}}$ and $H = H_Y$ is the image of $G_{\mathbb{K}}$ in $W(R_d)$?

Corn has shown that every pair $(\overline{X}, H)$, with $\overline{X}$ a split *ordinary* Del Pezzo surface of degree 6 and $H \subset W(R_6)$ arbitrary, is realizable in the above sense [Corn 2005, Theorem 5.1].

We use pairs to circumvent this realization problem. This allows us to prove comparison theorems without having to address realization (see Corollary 7.5).

We now define the nef cone volume $\alpha(Y, H)$ of a pair (Y, H) where Y is any *split* generalized Del Pezzo surface of degree $d \le 7$ and H is any subgroup of $W(R_d)$ that acts on the set of (-2)-curves on Y. It follows from Lemma 3.8 that H also acts on the set of (-1)-curves. Note that there is no restriction on H if Y is ordinary.

For such a pair (Y, H), define $N^1(Y, H)$ to be $N^1(Y)^H$. Motivated by Corollary 6.4, we define $\mathrm{Eff}^1(Y, H)$ to be the cone in $N^1(Y, H)_{\mathbb{R}}$ generated by the sum of the classes in each orbit of H acting on the sets of (-1)-curves and (-2)-curves of Y. We naturally get a dual cone

$$\mathrm{Nef}(Y, H) := \{C \in N^1(Y, H)_{\mathbb{R}} : \langle D, C\rangle \geq 0 \text{ for all } D \in \mathrm{Eff}^1(Y, H)\}.$$

We then have the hyperplane

$$\mathcal{H}_{Y,H} := \{C \in N^1(Y, H)_{\mathbb{R}} : \langle C, -K_Y\rangle = 1\}$$

and the polytope

$$\mathcal{P}_{Y,H} := \mathrm{Nef}(Y, H) \cap \mathcal{H}_{Y,H}.$$

And so we define $\alpha(Y, H) := \mathrm{Vol}(\mathcal{P}_{Y,H})$, with respect to the Leray measure $d\mu$ defined in the analogous manner to the way it was defined in Section 2.

It is immediate from Proposition 6.2 and Corollary 6.4 that if Y is any generalized Del Pezzo surface (not necessarily split), then $\alpha(Y) = \alpha(\overline{Y}, H_Y)$.

Lemma 7.2. *Assume that Y is split and let H_1, H_2 be two conjugate subgroups in $W(R_d)$. Then $\alpha(Y, H_1) = \alpha(Y, H_2)$.*

Proof. Let $w \in W(R_d)$ be such that $H_2 = wH_1w^{-1}$. Let $\mathbb{O}_i$, $i \in I$, denote the orbits of the (-1)- and (-2)-classes under H_1. By definition, $\mathrm{Eff}^1(Y, H_1)$ is generated by the sums $\sum_{D\in\mathbb{O}_i} D$, $i \in I$. A simple calculation shows that the orbits of these classes under H_2 are given by $w\mathbb{O}_i$, $i \in I$. We have

$$\alpha(Y, H_1) = \mathrm{Vol}\big(\{C \in N^1(Y, H_1)_{\mathbb{R}} : \langle -K_Y, C\rangle = 1, \langle C, \sum_{D\in\mathbb{O}_i} D\rangle \geq 0 \text{ for all } i \in I\}\big).$$

Making use of the fact that elements of $W(R_d)$ preserve the intersection form and anticanonical class and noting that elements of $W(R_d)$ are orthogonal transformations and thus preserve volumes, we compute

$$\begin{aligned}\alpha(Y, H_2) &= \mathrm{Vol}\big(\{C \in N^1(Y, H_2)_{\mathbb{R}} : \langle -K_Y, C\rangle = 1, \langle C, \sum_{D\in\mathbb{O}_i} wD\rangle \geq 0\ \forall i \in I\}\big)\\ &= \mathrm{Vol}\big(\{C \in N^1(Y, H_2)_{\mathbb{R}} : \langle -K_Y, w^{-1}C\rangle = 1, \langle w^{-1}C, \sum_{D\in\mathbb{O}_i} D\rangle \geq 0\ \forall i \in I\}\big)\\ &= \mathrm{Vol}\big(w\{C \in N^1(Y, H_1)_{\mathbb{R}} : \langle -K_Y, C\rangle = 1, \langle C, \sum_{D\in\mathbb{O}_i} D\rangle \geq 0\ \forall i \in I\}\big)\\ &= \alpha(Y, H_1). \qquad \square\end{aligned}$$

Corollary 7.3. *Let Y_1 and Y_2 be generalized Del Pezzo surfaces of degree $d \leq 7$, defined over a perfect field $\mathbb{K}$, which are geometrically isomorphic, that is, $\overline{Y_1} \cong \overline{Y_2}$. Let H_1 and H_2 denote the images of $G_{\mathbb{K}}$ under the respective homomorphisms $G_{\mathbb{K}} \to W(R_d)$. If H_1 and H_2 are conjugate in $W(R_d)$, then $\alpha(Y_1) = \alpha(Y_2)$.* □

We arrive at the following analogue of Theorem 1.3. That theorem provided a comparison between the nef cone volumes of a split generalized Del Pezzo surface and of a split ordinary Del Pezzo surface of the same degree. The following theorem generalizes this to the nef cone volumes of pairs.

Theorem 7.4. *Let Y be a split generalized Del Pezzo surface of degree $d \leq 7$, X a split ordinary Del Pezzo surface of the same degree, and H a subgroup of $W(R_d)$ acting on the set of (-2)-curves on Y. Let R_Y be the root system whose simple roots are the (-2)-curves on Y, and let $\mathbb{O}(R_Y, H)$ be the orbit root system associated to the action of H on R_Y as in Definition 6.5. Then*

$$\alpha(Y, H) = \frac{\alpha(X, H)}{\#W(\mathbb{O}(R_Y, H))}.$$

Proof. The proof of this theorem is a generalization of the argument that proves Theorem 1.3. Using Lemma 3.3, we identify $N^1(X)$ and $N^1(Y)$. This gives an identification of $N^1(X, H)$ and $N^1(Y, H)$. As before, $\mathrm{Nef}(Y, H)$ is the intersection of $\mathrm{Nef}(X, H)$ with the closure of a chamber defined by the simple roots of $\mathbb{O}(R_Y, H)$. As in the proof of Theorem 1.3, the chambers of the Weyl group $W(\mathbb{O}(R_Y, H))$ intersect only along boundaries, which have zero volume. They fill $N^1(Y)$. There are $\#W(\mathbb{O}(R_Y, H))$ of the chambers. From here, the proof is completed by the same steps as in the proof of Theorem 1.3. □

We arrive at our third main result, the computation of the nef cone volume of a generalized Del Pezzo surface over an arbitrary perfect field.

Corollary 7.5. *Let Y be a generalized Del Pezzo surface of degree $d \leq 7$ over the perfect field $\mathbb{K}$ and X a split ordinary Del Pezzo surface of the same degree. Let $\overline{Y} = Y \times_{\mathbb{K}} \overline{\mathbb{K}}$, and identify $N^1(\overline{Y})$ with $N^1(X)$ as in Lemma 3.3. Let $H_Y \subset W(R_d)$ be the image of $G_{\mathbb{K}}$. Let $R_{\overline{Y}} \subset R_d$ be the root system whose simple roots are (-2)-curves on $\overline{Y}$. Then*

$$\alpha(Y) = \alpha(\overline{Y}, H_Y) = \frac{\alpha(X, H_Y)}{\#W(\mathbb{O}(R_{\overline{Y}}, H_Y))}. \qquad \square$$

Using Proposition 6.6 and Corollary 6.9, the integer appearing in the denominator is straightforward to compute. This reduces the computation of the nef cone volume of an arbitrary generalized Del Pezzo surface over a nonclosed field to the computation of the nef cone volume of a pair involving a split ordinary Del Pezzo surface.

7B. ***Pairs involving ordinary Del Pezzo surfaces of high degree.*** As examples, let us compute $\alpha(X)$ for the various possible nonsplit ordinary Del Pezzo surfaces X of degree $d \geq 5$.

For $d \geq 7$ there are very few possible nontrivial Galois actions on $\overline{X}$, and we list these cases briefly.

(1) There are no nontrivial possibilities with $d = 9$: we must have $\overline{X} \cong \mathbb{P}^2$, the Galois action is trivial, and $\alpha(X) = \frac{1}{3}$.

(2) For $d = 8$, the only nontrivial form occurs when X is a twist of $\mathbb{P}^1 \times \mathbb{P}^1$ in which the Galois action permutes the two generating rulings. In this case $\alpha(X) = \frac{1}{2}$.

(3) For $d = 7$, the only possible nontrivial form occurs when X is the blowup of two conjugate rational points on $\mathbb{P}^2$, so the Galois action interchanges the points. In this case $\alpha(X) = \frac{1}{6}$.

For $d = 5, 6$ there are many more cases. For the remainder of this section, let X be a possibly nonsplit ordinary Del Pezzo surface of degree 5 or 6 defined over a nonclosed perfect field $\mathbb{K}$. Let $\overline{X} = X \times_{\mathbb{K}} \overline{\mathbb{K}}$. As above, we have $\alpha(X) = \alpha(\overline{X}, H_X)$ where H_X is the image of the Galois group in $W(R_d)$. We compute $\alpha(X)$ by finding the values of $\alpha(\overline{X}, H)$ for all subgroups H of $W(R_d)$. (As noted in Remark 7.1, it is not obvious which subgroups H of $W(R_d)$ arise as images of Galois groups, so a priori some values $\alpha(\overline{X}, H)$ might not correspond to any $\alpha(X)$.)

For the case $d = 6$, recall that $\overline{X}$ is obtained by blowing up three noncollinear points in $\mathbb{P}^2$ and the cone $\mathrm{Eff}^1(\overline{X})$ is minimally generated by the (-1)-curves on $\overline{X}$. Let E_1, E_2, E_3 denote the exceptional curves and L denote the pullback of a line. The set of (-1)-curves is shown schematically in Figure 1: the vertices correspond to the generating classes for $\mathrm{Eff}^1(\overline{X})$, with the convenient shorthand $L_{ij} = L - E_i - E_j$. Two classes intersect if and only if the corresponding vertices in the graph are connected by an edge.

Table 6 lists the subgroups of $W(R_6) = W(\mathbf{A}_1) \times W(\mathbf{A}_2) \cong \mathbb{Z}/2\mathbb{Z} \times \mathfrak{S}_3 \cong D_6$. By Lemma 7.2, it suffices to consider subgroups up to conjugacy. For each conjugacy class, we choose a representative subgroup H and give the order $\#H$ of H, the orbit structure of H on the generators of $\mathrm{Eff}^1(\overline{X})$, the rank ρ of $N^1(\overline{X}, H)$, the number m of generators in the minimal generating set of $\mathrm{Eff}^1(\overline{X}, H)$, and finally the nef cone volume $\alpha(\overline{X}, H)$. We describe H in terms of generators, using the generator

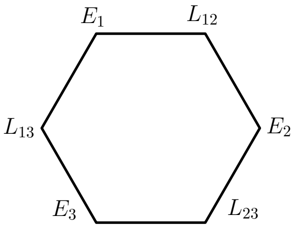

Figure 1. Configuration of (-1)-curves on an ordinary Del Pezzo surface of degree 6.

H	$\#H$	Orbit structure	ρ	m	$\alpha(\overline{X},H)$
$\langle s_{123}, s_{12}, s_{23}\rangle$	12	$\{E_1, E_2, E_3, L_{12}, L_{13}, L_{23}\}$	1	1	1
$\langle s_{23}s_{123}, s_{23}s_{12}\rangle$	6				
$\langle s_{123}s_{12}s_{23}\rangle$	6				
$\langle s_{12}, s_{23}\rangle$	6	$\{E_1, E_2, E_3\}, \{L_{12}, L_{13}, L_{23}\}$	2	2	$\frac{1}{3}$
$\langle s_{12}s_{23}\rangle$	3				
$\langle s_{123}, s_{23}\rangle$	4	$\{E_1, L_{23}\}, \{E_2, E_3, L_{12}, L_{13}\}$	2	2	$\frac{1}{2}$
$\langle s_{123}s_{12}\rangle$	2	$\{E_1, L_{12}\}, \{E_2, L_{13}\}, \{E_3, L_{23}\}$	2	2	$\frac{1}{2}$
$\langle s_{123}\rangle$	2	$\{E_1, L_{23}\}, \{E_2, L_{13}\}, \{E_3, L_{12}\}$	3	3	$\frac{1}{8}$
$\langle s_{12}\rangle$	2	$\{E_1, E_2\}, \{E_3\}, \{L_{12}\}, \{L_{13}, L_{23}\}$	3	4	$\frac{1}{12}$
$\langle e\rangle$	1	$\{E_1\}, \{E_2\}, \{E_3\}, \{L_{12}\}, \{L_{13}\}, \{L_{23}\}$	4	6	$\frac{1}{72}$

Table 6. Values of $\alpha(\overline{X}, H)$ for a split ordinary Del Pezzo surface $\overline{X}$ of degree 6.

$s_{123} := s_{L-E_1-E_2-E_3}$ (180° rotation) of $W(\mathbf{A}_1)$ and the generators $s_{12} := s_{E_1-E_2}$ (flip swapping E_1 and E_2) and $s_{23} := s_{E_2-E_3}$ (flip swapping E_2 and E_3) of $W(\mathbf{A}_2)$.

Given H, we may compute $\alpha(\overline{X}, H)$ as follows. We explicitly compute the sums of elements in each orbit of the action of H on the generators of $\mathrm{Eff}^1(\overline{X})$, obtaining a set of generators of the cone $\mathrm{Eff}^1(\overline{X}, H)$. We compute the dual cone in $N^1(\overline{X}, H)$, obtaining $\mathrm{Nef}(\overline{X}, H)$. Intersecting with the hyperplane $\mathcal{H}_{\overline{X},H}$ gives the polytope $\mathcal{P}_{\overline{X},H}$, whose volume is $\alpha(\overline{X}, H)$. For the case when $d = 5$, recall that $\overline{X}$ is the blowup of $\mathbb{P}^2$ at 4 points in general position. Similarly to the case $d = 6$, the cone $\mathrm{Eff}^1(\overline{X})$ is generated by the (-1)-curves E_i for $1 \leq i \leq 4$ and $L_{ij} = L - E_i - E_j$ for $1 \leq i < j \leq 4$.

Figure 2 uses a different diagram to exhibit the full symmetry of the configuration of these 10 curves with respect to $W(R_5) = \mathfrak{S}_5$. (It seems impossible to make visible all of the symmetries in a diagram analogous to Figure 1). Here the minimal

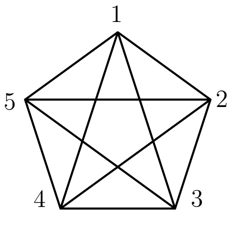

Figure 2. Configuration of (-1)-curves on an ordinary Del Pezzo surface of degree 5.

generators of $\mathrm{Eff}^1(\overline{X})$ correspond to *edges* of the graph, and two generating classes intersect if and only if the corresponding edges do *not* share a common vertex. The action of $W(R_5) = \mathfrak{S}_5$ corresponds to permuting the 5 vertices. Table 7 shows the

[12]	[13]	[14]	[15]	[23]	[24]	[25]	[34]	[35]	[45]
E_1	E_2	E_3	E_4	L_{34}	L_{24}	L_{23}	L_{14}	L_{13}	L_{12}

Table 7. Correspondence of edges in Figure 2 to generators of the effective cone of an ordinary Del Pezzo surface of degree 5.

H	$\#H$	Orbit structure	ρ	m	$\alpha(\overline{X}, H)$
$\langle(12), (12345)\rangle$ $\langle(12)(34), (253)\rangle$ $\langle(1234), (13)(24), (12543)\rangle$ $\langle(12)(34), (13542)\rangle$	120 60 20 10	$\{E_1, E_2, E_3, E_4, L_{12},$ $L_{13}, L_{14}, L_{23}, L_{24}, L_{34}\}$	1	1	1
$\langle(12), (1234)\rangle$ $\langle(123), (12)(34), (14)(23)\rangle$	24 12	$\{E_1, E_2, E_3, L_{14}, L_{24}, L_{34}\},$ $\{E_4, L_{12}, L_{13}, L_{23}\}$	2	2	$\frac{2}{3}$
$\langle(12), (34), (345)\rangle$ $\langle(12)(34), (345)\rangle$ $\langle(12), (345)\rangle$	12 6 6	$\{E_1\}, \{L_{12}, L_{13}, L_{14}\},$ $\{E_2, E_3, E_4, L_{23}, L_{24}, L_{34}\}$	2	2	$\frac{1}{2}$
$\langle(12), (123)\rangle$ $\langle(123)\rangle$	6 3	$\{E_1, E_2, L_{34}\}, \{E_3, L_{14}, L_{24}\},$ $\{E_4, L_{13}, L_{23}\}, \{L_{12}\}$	3	4	$\frac{5}{24}$
$\langle(12345)\rangle$	5	$\{E_1, E_4, L_{12}, L_{14}, L_{34}\},$ $\{E_2, E_3, L_{13}, L_{23}, L_{24}\}$	1	1	1
$\langle(12)(34), (13)(24)\rangle$	4	$\{E_1\}, \{E_2, E_3, L_{24}, L_{34}\},$ $\{E_4, L_{23}\}, \{L_{12}, L_{13}\}, \{L_{14}\}$	3	4	$\frac{1}{6}$
$\langle(12), (34)\rangle$	4	$\{E_1, E_3, L_{14}, L_{34}\}, \{E_2, L_{24}\},$ $\{E_4, L_{12}, L_{13}, L_{23}\}$	2	2	$\frac{2}{3}$
$\langle(12), (34), (13)(24)\rangle$ $\langle(1234)\rangle$	8 4	$\{E_1, L_{14}\}, \{E_2, L_{24}\}, \{E_3, L_{34}\},$ $\{E_4, L_{12}, L_{13}, L_{23}\}$	2	2	$\frac{2}{3}$
$\langle(12)(34)\rangle$	2	$\{E_1\}, \{E_2, L_{24}\}, \{E_3, L_{34}\},$ $\{E_4\ L_{23}\}, \{L_{12}, L_{13}\}, \{L_{14}\}$	3	4	$\frac{1}{6}$
$\langle(12)\rangle$	2	$\{E_1\}, \{E_2, L_{34}\}, \{E_3, L_{24}\},$ $\{E_4\ L_{23}\}, \{L_{12}\}, \{L_{13}\}, \{L_{14}\}$	4	7	$\frac{1}{24}$
$\langle e\rangle$	1	$\{E_1\}, \{E_2\}, \{E_3\}, \{E_4\}, \{L_{12}\},$ $\{L_{13}\}, \{L_{14}\}, \{L_{23}\}, \{L_{24}\}, \{L_{34}\}$	5	10	$\frac{1}{144}$

Table 8. Values of $\alpha(\overline{X}, H)$ for a split ordinary Del Pezzo surface $\overline{X}$ of degree 7.

correspondence between the edges of the diagram and the generating classes, where we use the notation $[ij]$ to indicate the edge connecting vertex i with vertex j.

The enumeration of the conjugacy classes of subgroups of $\mathfrak{S}_5$ has been made by Götz Pfeiffer and is available online [Pfeiffer 2007]. Table 8 contains the values of $\alpha(\overline{X}, H)$ for the various possible conjugacy classes of subgroups of $\mathfrak{S}_5$.

Acknowledgments

We thank Brian Harbourne and Brendan Hassett for encouragement and helpful comments.

References

[Batyrev and Manin 1990] V. V. Batyrev and Y. I. Manin, "Sur le nombre des points rationnels de hauteur borné des variétés algébriques", *Math. Ann.* **286**:1-3 (1990), 27–43. MR 91g:11069 Zbl 0679.14008

[Batyrev and Popov 2004] V. V. Batyrev and O. N. Popov, "The Cox ring of a del Pezzo surface", pp. 85–103 in *Arithmetic of higher-dimensional algebraic varietiesi* (Palo Alto, CA, 2002), Progr. Math. **226**, Birkhäuser Boston, Boston, MA, 2004. MR 2005h:14091 Zbl 1075.14035

[Batyrev and Tschinkel 1995] V. V. Batyrev and Y. Tschinkel, "Rational points of bounded height on compactifications of anisotropic tori", *Internat. Math. Res. Notices* **1995**:12 (1995), 591–635. MR 97a:14021 Zbl 0890.14008

[Batyrev and Tschinkel 1996] V. V. Batyrev and Y. Tschinkel, "Rational points on some Fano cubic bundles", *C. R. Acad. Sci. Paris Sér. I Math.* **323**:1 (1996), 41–46. MR 97j:14023 Zbl 0879.14007

[Boucksom et al. 2004] S. Boucksom, J.-P. Demailly, M. Paun, and T. Peternell, "The pseudo-effective cone of a compact Kähler manifold and varieties of negative Kodaira dimension", preprint, 2004. arXiv math.AG/0405285

[Bourbaki 2002] N. Bourbaki, *Lie groups and Lie algebras. Chapters 4–6*, Elements of Mathematics (Berlin), Springer, Berlin, 2002. Translated from the 1968 French original by Andrew Pressley. MR 2003a:17001 Zbl 0983.17001

[Colliot-Thélène and Sansuc 1987] J.-L. Colliot-Thélène and J.-J. Sansuc, "La descente sur les variétés rationnelles, II", *Duke Math. J.* **54**:2 (1987), 375–492. MR 89f:11082 Zbl 0659.14028

[Corn 2005] P. Corn, "Del Pezzo surfaces of degree 6", *Math. Res. Lett.* **12**:1 (2005), 75–84. MR 2006d.14035 Zbl 1074.14034

[Demazure 1980] M. Demazure, "Surfaces de Del Pezzo, I – V", pp. 21–69 in *Séminaire sur les singularités des surfaces* (Palaiseau, 1976–1977), edited by M. Demazure et al., Lecture Notes in Mathematics **777**, Springer, Berlin, 1980. MR 82d:14021 Zbl 0444.14024

[Derenthal 2007] U. Derenthal, "On a constant arising in Manin's conjecture for del Pezzo surfaces", *Math. Res. Lett.* **14**:3 (2007), 481–489. MR 2318651 Zbl pre05209039

[Hall 2003] B. C. Hall, *Lie groups, Lie algebras, and representations*, Graduate Texts in Mathematics **222**, Springer, New York, 2003. MR 2004i:22001 Zbl 1026.22001

[Harbourne 1985] B. Harbourne, "Blowings-up of $\mathbf{P}^2$ and their blowings-down", *Duke Math. J.* **52**:1 (1985), 129–148. MR 86m:14026 Zbl 0577.14025

[Hartshorne 1977] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics **52**, Springer, New York, 1977. MR 57 #3116 Zbl 0367.14001

[Hassett and Tschinkel 2004] B. Hassett and Y. Tschinkel, "Universal torsors and Cox rings", pp. 149–173 in *Arithmetic of higher-dimensional algebraic varieties* (Palo Alto, CA, 2002), Progr. Math. **226**, Birkhäuser Boston, Boston, MA, 2004. MR 2005a:14049 Zbl 1077.14046

[Hindry and Silverman 2000] M. Hindry and J. H. Silverman, *Diophantine geometry: an introduction*, Graduate Texts in Math. **201**, Springer, New York, 2000. MR 2001e:11058 Zbl 0948.11023

[Humphreys 1990] J. E. Humphreys, *Reflection groups and Coxeter groups*, Cambridge Studies in Advanced Mathematics **29**, Cambridge University Press, Cambridge, 1990. MR 92h:20002 Zbl 0725.20028

[Kac 1990] V. G. Kac, *Infinite-dimensional Lie algebras*, 3rd ed., Cambridge University Press, Cambridge, 1990. MR 92k:17038 Zbl 0716.17022

[Lahyane and Harbourne 2005] M. Lahyane and B. Harbourne, "Irreducibility of -1-classes on anticanonical rational surfaces and finite generation of the effective monoid", *Pacific J. Math.* **218**:1 (2005), 101–114. MR 2007b:14082 Zbl 1109.14030

[Lazarsfeld 2004] R. Lazarsfeld, *Positivity in algebraic geometry, II: Positivity for vector bundles, and multiplier ideals*, Ergebnisse der Mathematik (3) **49**, Springer, Berlin, 2004. MR 2005k:14001b Zbl 1093.14500

[Manin 1986] Y. I. Manin, *Cubic forms: Algebra, geometry, arithmetic*, 2nd ed., North-Holland Mathematical Library **4**, North-Holland, Amsterdam, 1986. MR 87d:11037 Zbl 0582.14010

[Peyre 1995] E. Peyre, "Hauteurs et mesures de Tamagawa sur les variétés de Fano", *Duke Math. J.* **79**:1 (1995), 101–218. MR 96h:11062 Zbl 0901.14025

[Pfeiffer 2007] G. Pfeiffer, "The subgroups of $\mathcal{S}_5$", 2007, Available at http://schmidt.nuigalway.ie/subgroups/s5.pdf.

[Urabe 1983] T. Urabe, "On singularities on degenerate del Pezzo surfaces of degree 1, 2", pp. 587–591 in *Singularities* (Arcata, CA, 1981), vol. 2, edited by P. Orlik, Proc. Sympos. Pure Math. **40**, Amer. Math. Soc., Providence, R.I., 1983. MR 84i:14024 Zbl 0515.14021

Communicated by János Kollár
Received 2007-07-27 Revised 2007-10-19 Accepted 2007-12-11

ulrich.derenthal@math.unizh.ch *Institut für Mathematik, Universität Zürich,*
Winterthurerstrasse 190, 8057 Zürich, Switzerland

mjoyce@math.tulane.edu *Department of Mathematics, Tulane University,*
Gibson Hall 424, New Orleans, LA 70118, United States

zteitler@selu.edu *Department of Mathematics, Southeastern Louisiana*
University, SLU 10687, Hammond, LA 70402, United States

Divisibility sequences for elliptic curves with complex multiplication

Marco Streng

Elliptic divisibility sequences arise as sequences of denominators of the integer multiples of a rational point on an elliptic curve. Silverman proved that almost every term of such a sequence has a primitive divisor (that is, a prime divisor that has not appeared as a divisor of earlier terms in the sequence). If the elliptic curve has complex multiplication, then we show how the endomorphism ring can be used to index a similar sequence and we prove that this sequence also has primitive divisors. The original proof fails in this context and will be replaced by an inclusion-exclusion argument and sharper diophantine estimates.

1. Introduction

Consider an elliptic curve E, given by a general Weierstrass model with coefficients in the ring of integers $\mathcal{O}_L$ of a number field L. Fix an L-valued point P of infinite order on E. For $n \in \mathbb{Z}$, define the coprime $\mathcal{O}_L$-ideals A_n and B_n by

$$x(nP)\,\mathcal{O}_L = A_n B_n^{-2}. \tag{1.1}$$

We call the sequence $B_1, B_2, B_3, \ldots$ an *elliptic divisibility sequence*. Such a sequence satisfies the *strong divisibility property*

$$\gcd(B_m, B_n) = B_{\gcd(m,n)} \qquad (m, n \in \mathbb{Z}),$$

which in particular implies the (*weak*) *divisibility property*: if $m \mid n$, then $B_m \mid B_n$.

By a *primitive divisor* of the term B_n, we mean a prime $\mathfrak{p} \mid B_n$ that does not divide any term B_m with $n \nmid m$. Silverman proved that almost every term in an elliptic divisibility sequence has a primitive divisor [Silverman 1988]. This is the elliptic curve analogue of a theorem of Zsigmondy for $\mathbb{Q}^*$ [Bang 1886; Zsigmondy 1892].

MSC2000: primary 14H52; secondary 14K22.

Keywords: complex multiplication, divisibility sequence, elliptic curve, endomorphism, primitive divisor, Zsigmondy.

If the curve E has complex multiplication, then (1.1) makes sense for all n in the endomorphism ring $\mathcal{O} = \mathrm{End}_L(E)$ and hence we get a sequence indexed by $\mathcal{O}$ instead of only $\mathbb{Z}$. We extend this definition to ideals $\mathfrak{a}$ of $\mathcal{O}$ by setting

$$B_{\mathfrak{a}} = \sum_{\alpha \in \mathfrak{a}} B_\alpha,$$

the ideal generated by the ideals B_α for $\alpha \in \mathfrak{a}$. We will prove that this indeed extends the definition (in the sense that $B_{\alpha\mathcal{O}} = B_\alpha$), and that the resulting ideal-indexed sequence satisfies the strong divisibility property $B_{\mathfrak{a}} + B_{\mathfrak{b}} = B_{\mathfrak{a}+\mathfrak{b}}$. By the *elliptic divisibility sequence associated to P*, we will mean this sequence, indexed by ideals of $\mathcal{O}$.

By a *primitive divisor* of the term $B_{\mathfrak{a}}$, we now mean a prime $\mathfrak{p} \mid B_{\mathfrak{a}}$ which does not divide any term $B_{\mathfrak{b}}$ with $\mathfrak{a} \nmid \mathfrak{b}$. Our main theorem is a Zsigmondy-type theorem for elliptic curves with complex multiplication.

Main Theorem. *Let $E, \mathcal{O}$ and P be as above. Then for all but finitely many invertible $\mathcal{O}$-ideals $\mathfrak{a}$, the ideal $B_{\mathfrak{a}}$ has a primitive divisor.*

The Main Theorem applies both in the case $\mathcal{O} = \mathbb{Z}$ and in the *complex multiplication* case, that is, when $\mathcal{O}$ is a quadratic order, but is a new result only in the latter case.

The number of primitive divisors. If not all endomorphisms of E over $\overline{L}$ are defined over L, then our Main Theorem implies the following result on the number of primitive divisors in the $\mathbb{Z}$-indexed sequence B_1, B_2, $B_3, \cdots$. Let K' be the field of fractions of $\mathcal{O}' = \mathrm{End}_{\overline{L}}(E)$.

Corollary 1.2. *Define, for $n \in \mathbb{Z}$, the numbers*

$$r_n = \#\{p \in \mathbb{N} :\ p \mid n,\ p \textit{ is a prime ramifying in } \mathcal{O}'\mathbb{Z} \textit{ and } p \nmid n,\ p \nmid [\mathcal{O}_{K'} : \mathcal{O}']\},$$
$$s_n = \#\{p \in \mathbb{N} :\ p \mid n \textit{ and } p \textit{ is a prime splitting in } \mathcal{O}'/\mathbb{Z}\}.$$

Then for almost all n, the term B_n has at least $r_n + s_n + 1$ primitive divisors, of which at least s_n split in $K'L/L$.

In particular, this shows the existence of lots of split primitive divisors in elliptic divisibility sequences coming from elliptic curves over $\mathbb{Q}$ that have complex multiplication. It seems that there are also many inert primitive divisors, but we cannot prove this. There are conjectures by Cornelissen and Zahidi [2007] about the existence of inert primitive divisors that imply results related to Hilbert's Tenth Problem over $\mathbb{Q}$.

The size of the primitive part. For any integer n, we define the *primitive part* $D_n^{\mathbb{Z}}$ of B_n to be the L-ideal dividing B_n such that every prime divisor of $D_n^{\mathbb{Z}}$ is a primitive divisor of B_n and no divisor of $B_n/D_n^{\mathbb{Z}}$ is a primitive divisor of B_n. Our methods also yield estimates on the size of the primitive part of $\mathbb{Z}$-indexed elliptic divisibility sequences that are sharper than what can be gotten with Silverman's original proof. We use the notation $\|D_n^{\mathbb{Z}}\| := N_{L/\mathbb{Q}}(D_n^{\mathbb{Z}})^{1/[L:\mathbb{Q}]}$ for the "size" of the ideal $D_n^{\mathbb{Z}}$ and we denote the canonical height of the point P by $\widehat{h}(P)$.

Silverman's proof can be optimized to give an estimate

$$\log \|D_n^{\mathbb{Z}}\| \geq \widehat{h}(P) \Big(1 - \sum_{p\,|\,n} \frac{1}{p^2} - o(1)\Big)\, n^2,$$

where $0.5477 < 1 - \sum_p p^{-2} < 0.5478$ for the sum over *all* primes. If we apply our methods, we get the following sharper estimate.

Proposition 1.3. *For all* $\epsilon > 0$,

$$\log \|D_n^{\mathbb{Z}}\| = \widehat{h}(P)\, s_n\, n^2 + O(n^{\epsilon}) \qquad (\textit{as } n \to \infty),$$

where

$$s_n = \sum_{m\,|\,n} \mu(m) m^{-2} = \prod_{p\,|\,n} (1 - p^{-2})$$

is between $\zeta(2)^{-1} > 0.6079$ *and* 1.

In fact, the proof gives $O(d(n)(\log n)(\log\log n)^4)$ instead of $O(n^{\epsilon})$, where $d(n)$ is the number of divisors of n.

Division polynomials. An alternative approach to defining elliptic divisibility sequences is by using division polynomials. If E/L is an elliptic curve, given by a Weierstrass model, then for any integer $n \in \mathbb{Z}$, the *n-th division polynomial of E* is the polynomial $\psi_n = \psi_{E,n} \in L[x, y] \subset L(E)$, as given for short Weierstrass models in [Silverman 1986] and [Washington 2003] and in general in [Ayad 1992]. If $P \in E(L)$ is a fixed L-valued point on E, then we call the sequence $(\psi_n(P))_{n\in\mathbb{Z}}$ an *elliptic divisibility sequence of division polynomial type*.

Along with the division polynomials ψ_n, one usually also defines polynomials $\phi_n = \phi_{E,n} \in L[x]$ for which we have

$$[n]^* x = \frac{\phi_n}{\psi_n^2}. \tag{1.4}$$

This explains the similarity between B_n and $\psi_n(P)$: both represent the square root of the denominator of $x(nP)$, but they can differ because $\psi_n(P)$ and $\phi_n(P)$ may not be integers, and because there may be cancellation of factors in (1.4). However, B_n and $\psi_n(P)$ differ only in finitely many valuations. For a more precise statement, see [Ayad 1992].

The division polynomials satisfy the recurrence relation

$$\psi_{m+n}\psi_{m-n} = \psi_{m+1}\psi_{m-1}\psi_n^2 - \psi_{n+1}\psi_{n-1}\psi_m^2 \quad \text{for } m, n \in \mathbb{Z}. \tag{1.5}$$

Ward [1948] extensively studied sequences of integers that satisfy both this recurrence and the divisibility property; he called them *elliptic divisibility sequences*. Later, his terminology was adopted for the sequences $(\psi_n(P))_n$ and $(B_n)_n$. In fact, every sequence of integers $(\psi_n)_n$ that satisfies (1.5) and the initial conditions $\psi_0 = 0$, $\psi_1 = 1$, $\psi_2\psi_3 \neq 0$, $\psi_2 \mid \psi_4$, excepting some degenerate cases, is of the form $\psi_n = \psi_{E,n}(P)$ for some elliptic curve $E/\mathbb{C}$ and some point $P \in E(\mathbb{C})$ [Ward 1948, Theorem 12.1].

Chudnovsky and Chudnovsky [1986] suggested letting sequences of division polynomial type be indexed by the endomorphism ring of the elliptic curve, using division polynomials ψ_α for arbitrary endomorphisms α. The special cases where the curve has complex multiplication by $\sqrt{-1}$ or a primitive third root of unity were studied by Ward [1950] and Durst [1952] respectively. The CM division polynomials ψ_α and their computational aspects have recently been studied in more detail by Satoh [2004].

2. Formal groups

Let L_v be the completion of the number field L with respect to a normalized discrete valuation v. Denote the ring of v-integers of L_v by R_v and let E be an elliptic curve, given by a Weierstrass equation

$$y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1}$$

with coefficients in R_v. For $n \geq 1$, define subsets $E_n(L_v)$ of $E(L_v)$ by

$$E_n(L_v) = \{P \in E(L_v) : v(x(P)) \leq -2n\} \cup \{O\}.$$

We want to study these sets because for $n \geq 1$, we have that

$$v(B_\alpha) \geq n \iff \alpha P \in E_n(L_v). \tag{2.2}$$

The formal group of E gives a means of studying $E_n(L_v)$.

We have two main goals in this section. First we will generalize part of the theory of formal groups as in [Silverman 1986] to arbitrary isogenies instead of only multiplication by integers in $\mathbb{Z}$. This will result in the identity

$$v(B_{\alpha\beta}) = v(B_\alpha) + v(\beta)$$

which holds if $v(B_\alpha)$ is sufficiently large (see Proposition 2.8 and Lemma 3.4). This is very useful, because it bounds the part of the growth of B_α that is caused by the occurrence of higher powers of nonprimitive divisors.

At the end of this section, we will prove that the sets $E_n(L_v)$ are modules over the endomorphism ring $\mathbb{O}$ (see Corollary 2.10). By (2.2), this implies the divisibility property

$$B_\alpha \mid B_{\alpha\beta} \quad \alpha, \beta \in \mathcal{O}.$$

Formal groups and isogenies. We start by associating homomorphisms of formal groups to arbitrary isogenies of elliptic curves.

Let $z = -x/y$ and $w = -1/y$. Then the Weierstrass equation of the elliptic curve E becomes

$$w = z^3 + a_1 zw + a_2 z^2 w + a_3 w^2 + a_4 z w^2 + a_6 w^3. \tag{2.3}$$

Let $w(T) \in L_v[[T]]$ be the unique power series such that (2.3) is satisfied with $z = T$. Then $(T, w(T))$ is a “formal point” on the curve (2.3).

We define a homomorphism of rings $\mathcal{P} : L_v(E) \to L_v((T))$ from the function field of E to the field of Laurent series over L_v by $z \mapsto T$, $w \mapsto w(T)$. One could think of $\mathcal{P}$ as the map which “evaluates” elliptic functions in the formal point $(T, w(T))$.

As z is a uniformizer at the point at infinity O of E, we see that $\mathcal{P}$ maps functions that are regular at O to power series in $L_v[[T]]$.

Suppose that E' is another elliptic curve, also given by a Weierstrass equation with coefficients in R_v. We use $'$ in the notation to specify functions and so on related to E'. To any isogeny $\phi : E \to E'$ that is defined over L_v, we associate a power series

$$F_\phi(T) = \mathcal{P}(\phi^* z') \in L_v[[T]]. \tag{2.4}$$

This power series is a homomorphism of formal groups. We will not check this, since it will follow trivially from Lemma 2.6 below. Notice that $F_\phi(T)$ has no constant term, so we get a map $F_\phi^* : L_v((T)) \to L_v((T))$, $f(T) \mapsto f(F_\phi(T))$. We now have a commutative diagram

$$\begin{tikzcd}
L_v(E) \arrow[r, "\mathcal{P}", "\substack{z\mapsto T\\ w\mapsto w(T)}"'] & L_v((T)) \\
L_v(E') \arrow[u, "\phi^*"] \arrow[r, "\mathcal{P}'", "\substack{z'\mapsto T\\ w'\mapsto w'(T)}"'] & L_v((T)). \arrow[u, "F_\phi^*"']
\end{tikzcd} \tag{2.5}$$

We only need to check the commutativity of the diagram for the generators z' and w' of $L_v(E')$. For z', it holds by definition. For w', it follows from the fact that its image on the top right satisfies the Weierstrass equation for E' with $z' = T$.

As z is a uniformizer at O, the space of differentials that are regular at O is $\Omega_{E,O} = L_{v,O}(E)\, dz$ and we get a map

$$L_{v,O}(E)\, dz \to L_v[[T]]\, dT, \qquad g dz \mapsto \mathcal{P}(g)\, dT,$$

which we also denote by $\mathcal{P}$.

Let $\omega \in \Omega_{E,O}$ denote the *invariant differential*

$$\omega = \frac{dx}{2y + a_1 x + a_3},$$

and write $\widehat{\omega}(T)$ for $\mathcal{P}(\omega)$. As ω is an invariant differential of the curve E, we see that $\widehat{\omega}(T)$ is an invariant differential of the formal group $\widehat{E}$ of E. In fact, the dz-coefficient of $\widehat{\omega}$ is 1, so it is the (unique) normalized invariant differential of the formal group $\widehat{E}$ of E.

The integral $\log(T)$ of $\widehat{\omega}$ is an isomorphism of formal groups from $\widehat{E}$ to the additive formal group $\mathbb{G}_a$. Denote the inverse by $\exp(T)$.

Lemma 2.6. *For any isogeny $\phi : E \to E'$ over L_v, we have*

$$F_\phi(T) = \exp_{\widehat{E'}}(c \log_{\widehat{E}}(T)),$$

where $c \in L_v$ is such that $\phi^*\omega' = c\omega$.

Proof. If we apply $\mathcal{P}$ to the identity $\phi^*\omega' = c\omega$, then we get $\widehat{\omega}'(F_\phi(T)) = c\widehat{\omega}(T)$. The result is obtained by integration, followed by application of $\exp_{\widehat{E'}}$. □

Recall that R_v is the ring of v-integers of L_v. Let $\mathfrak{M}$ be the maximal ideal of R_v and $l = R_v/\mathfrak{M}$ the residue field. Reduction of the Weierstrass equation gives a cubic curve $\widetilde{E}$ over l. We denote the group of nonsingular points by $\widetilde{E}^{\text{ns}}(l) \subset \widetilde{E}(l)$.

Let $E_0(L_v)$ be the group of L_v-valued points that reduce to points in $\widetilde{E}_{\text{ns}}(l)$ modulo v. Reduction modulo v then is a group homomorphism $E_0(L_v) \to \widetilde{E}_{\text{ns}}(l)$ with kernel $E_1(L_v)$. By [Silverman 1986, VII.2.2], we have an isomorphism of groups

$$\begin{aligned} E_1(L_v) &\to \widehat{E}(\mathfrak{M}), \\ P &\mapsto z(P), \end{aligned} \tag{2.7}$$

where the inverse sends $u \in \mathfrak{M}$ to the point $P \in E(L_v)$ with coordinates $z(P) = u$, $w(P) = w(u)$. For any point $P \in E_1(L_v)$, the fact that $(x(P), y(P))$ satisfies the Weierstrass equation implies that $2v(y(P)) = 3v(x(P))$, and hence $v(z(P)) = -\frac{1}{2}v(x(P))$. In particular, the sets $E_n(L_v)$ are subgroups of $E(L_v)$ and correspond to the groups $\widehat{E}(\mathfrak{M}^n)$ through the isomorphism (2.7).

Now let $\phi : E \to E'$ be an isogeny defined over L_v, where we assume that both E and E' are given by Weierstrass equations with coefficients in R. Furthermore, let c be the unique element of L_v such that $\phi^*\omega' = c\omega$.

Proposition 2.8. *If both $v(x(P))$ and $v(x(P)) - 2v(c)$ are strictly smaller than $-2v(p)/(p-1)$, then*

$$v\big(x'(\phi(P))\big) = v\big(x(P)\big) - 2v(c).$$

Proof. By the isomorphism $E_1(L_v) \cong \widehat{E}(\mathfrak{M})$ above and Lemma 2.6, we have

$$z'(\phi(P)) = F_\phi(z(P)) = \exp_{\widehat{E}'}\bigl(c \log_{\widehat{E}}(z(P))\bigr).$$

By [Silverman 1986, IV.6.4], both $\log_{\widehat{E}}(u)$ and $\exp_{\widehat{E}'}(u)$ converge for $u \in \mathfrak{M}$ with $v(u) > v(p)/(p-1)$ and both preserve the valuation. Therefore, we find that $v\bigl(x'(\phi(P))\bigr) = -2v\bigl(z'(\phi(P))\bigr) = -2v\bigl(z(P)\bigr) - 2v(c) = v\bigl(x(P)\bigr) - 2v(c)$. □

Formal groups and Complex Multiplication. The main theorem of this section is the following.

Theorem 2.9. *For any $\alpha \in \mathbb{O} = \operatorname{End}_{L_v}(E)$, the power series $F_\alpha(T) \in L_v[[T]]$ has v-integral coefficients. In other words, the homomorphism of formal groups $F_\alpha(T)$ is defined over R_v.*

Corollary 2.10. *For any $n \geq 1$, the group $E_n(L_v)$ is an $\mathbb{O}$-submodule of $E(L_v)$. Moreover, we have an isomorphism of $\mathbb{O}$-modules*

$$E_n(L_v)/E_{n+1}(L_v) \cong l,$$

where l is the residue field of L_v.

Proof of the corollary. First of all, the theorem shows that $\widehat{E}(\mathfrak{M}^n)$ is an $\mathbb{O}$-module with the action of α given by $z \mapsto F_\alpha(z)$. Now for any $P \in E_n(L_v)$, convergence of $F_\alpha(z(P))$ implies convergence of $w\bigl(F_\alpha(z(P))\bigr)$. But by (2.5), $F_\alpha(z(P))$ and $w\bigl(F_\alpha(z(P))\bigr)$ can only converge to $z(\alpha P)$ and $w(\alpha P)$ respectively. In particular, the isomorphism of groups $E_n(L_v) \cong \widehat{E}(\mathfrak{M}^n)$ is an isomorphism of $\mathbb{O}$-modules.

The second statement follows from the obvious isomorphism

$$\widehat{E}(\mathfrak{M}^n)/\widehat{E}(\mathfrak{M}^{n+1}) \cong \mathfrak{M}^n/\mathfrak{M}^{n+1}. \qquad \square$$

As we will see, Theorem 2.9 follows easily from the theory of Néron models. However, we will also give a more elementary proof. The elementary proof actually consists of proofs for two special cases that together cover every case. One proof uses continuity of the coefficients of $F_\alpha(T)$ as functions of α and works only if p splits in the field of fractions of $\mathbb{O}$. The other uses explicit equations for isogenies, but fails in the exceptional case where $p = 2$ and 2 splits in $\mathbb{O}$.

For both the Néron model proof and the elementary proof, we will need to deal with changes of coordinates in the Weierstrass equations, so we will use the following lemma.

Lemma 2.11. *Every isomorphism $\psi : E \to E'$ over L_v of elliptic curves given by Weierstrass equations is of the form*

$$\psi(x, y) = (u^2 x + r, u^3 y + u^2 s x + t)$$

with $u \in L_v^*$ and $r, s, t \in L_v$. Such an isomorphism satisfies $\psi^*\omega' = u^{-1}\omega$. Moreover, if $v(u) \geq 0$ and both E and E' have v-integral coefficients, then r, s and t are v-integral.

Proof. This is exactly what is proven in the proof of [Silverman 1986, VII.1.3(d)]. □

Corollary 2.12. *Let ψ and u be as above. If $v(u) = 0$, then the power series $F_\psi(T)$ associated to ψ as in* (2.4) *has v-integral coefficients.*

Proof. From the equations above, we compute

$$\phi^* z' = \frac{u^{-1}z + ru^{-3}w}{1 - su^{-1}z - tu^{-3}w}.$$

As $u^{-1}, r, s, t \in R_v$, we find that $F_\psi(T)$ has coefficients in R_v. □

Proof using Néron models. Suppose that the elliptic curves E_1 and E_2 are given by Weierstrass equations with coefficients in R_v and let $\phi : E_1 \to E_2$ be an isogeny, defined over L_v.

Lemma 2.13. *If the Weierstrass equation for E_2 is minimal, that is, $v(\Delta)$ is minimal among all Weierstrass models of E_2 with coefficients in R_v, then $F_\phi(T)$ has v-integral coefficients.*

Proof. Let $\mathscr{E}_1, \mathscr{E}_2$ be the closed subschemes of $\mathbb{P}^2_{R_v}$ given by the Weierstrass equations of E_1, E_2 and denote the smooth parts by $\mathscr{E}_1^0$, $\mathscr{E}_2^0$. We will prove, using the Néron model, that the map $\phi : E_1 \to E_2$ can be extended to a morphism of schemes $\phi : \mathscr{E}_1^0 \to \mathscr{E}_2^0$ over R_v.

We then localize this morphism at the closed point s of the zero section of $\mathscr{E}_2^0$. Let $z_2 = -x_2/y_2$, $w_2 = -1/y_2$ be the coordinate functions of E_2. The completion of the local ring

$$\mathbb{O}_{\mathscr{E}_2^0, s} = R_v[z_2, w_2]_{(z_2)}$$

with respect to the ideal (z_2) is exactly the ring $R_v[[z_2]]$ of power series in z_2, where we identify w_2 with the power series $w_2(z_2)$ that was defined below (2.3). As ϕ maps the zero section to the zero section, it induces a morphism $R_v[[z_2]] \to R_v[[z_1]]$. The image of z_2 under this morphism is exactly $F_\phi(z_1)$, so $F_\phi(T)$ has coefficients in R_v.

It remains to prove that the extension of ϕ exists. Let $\mathcal{N}$ denote the Néron model of E_2 over R_v as in [Bosch, Lütkebohmert and Raynaud 1990, 1.2.1 and 1.3.2] or [Silverman 1994, § IV.5 and IV.6.1]. Then $\mathcal{N}$ is a smooth R_v-scheme with generic fibre $\mathcal{N}_{L_v} = E_2$ which satisfies the following universal property: for any smooth R_v-scheme X and any morphism of L_v-schemes $f : X_{L_v} \to E_2$, there exists a unique morphism of R_v-schemes $g : X \to \mathcal{N}$ extending f in the sense that $g_{L_v} = f$.

The special fibre $\mathcal{N}_l$ of $\mathcal{N}$ may consist of multiple components. One of them contains the special fibre of the identity section. Let $\mathcal{N}^0$ denote $\mathcal{N}$ with all other components of $\mathcal{N}_l$ removed. Then by [Bosch, Lütkebohmert and Raynaud 1990, 1.5.5] or [Silverman 1994, IV.9.1], we have $\mathscr{E}_2^0 = \mathcal{N}^0$. Moreover, by the universal property of the Néron model, ϕ extends to a unique morphism of R_v-schemes $\phi : \mathscr{E}_1^0 \to \mathcal{N}$ and since the special fibre of $\mathscr{E}_1^0$ has only one component, the image lies inside $\mathcal{N}^0 = \mathscr{E}_2^0$. □

Proof of Theorem 2.9. If the Weierstrass model of E is minimal, then Lemma 2.13 proves Theorem 2.9. Otherwise, let E'' be a minimal model. By a change of coordinates $z' = u^{-1}z''$, $w' = u^{-3}w''$ with $v(u) \geq 0$, we obtain a model E' from the minimal model E'' such that $v(\Delta(E')) = v(\Delta(E))$. Write F_α, F'_α and F''_α for the power series associated to α with respect to the different models. We know that F''_α has v-integral coefficients, so $F'_\alpha(T) = u^{-1}F''_\alpha(uT)$ also has v-integral coefficients. As $v(\Delta(E)) = v(\Delta(E'))$, it follows from Corollary 2.12 that $F_\alpha(T)$ has v-integral coefficients. □

Elementary proof. Let K be the field of fractions of $\mathbb{O}$.

Proof of Theorem 2.9 assuming that p splits in $K/\mathbb{Q}$. For any nonnegative integer n, consider the map $\Phi_n : K_v \to L_v$, mapping $\alpha \in K_v$ to the n-th coefficient of the power series $\exp_{\widehat{E}'}(\alpha \log_{\widehat{E}}(T)) \in L_v[[T]]$. The goal is to prove that $\Phi_n(\mathbb{O}) \subset R_v$ for every n. As p splits in $K/\mathbb{Q}$, we have $\mathbb{Q}_p = K_v$, so $\mathbb{O} \subset \mathbb{Z}_p$. The map Φ_n is continuous, because it is a polynomial map. Moreover, as $\widehat{E}$ is defined over R, we have $\Phi_n(\mathbb{Z}) \subset R$. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, we are done. □

The ring $\mathbb{O} = \mathrm{End}_{L_v}(E)$ is an order in the imaginary quadratic field K; hence it is generated as a ring over $\mathbb{Z}$ by a single element α. We have a homomorphism of rings $\mathbb{O} \to \mathrm{End}_{L_v}(\widehat{E})$ and we wish to show that the image is contained in the subring $\mathrm{End}_{R_v}(\widehat{E})$. It therefore suffices to prove that the generator α of $\mathbb{O}$ maps to an element of $\mathrm{End}_{R_v}(\widehat{E})$. We will use the formulas of Vélu [1971] that describe an isogeny explicitly in terms of its kernel. Therefore, we want to pick α in such a way that $v(N(\alpha)) = 0$ so that we know that the α-torsion is v-integral.

We make such a choice as follows: let $p > 0$ be the rational prime such that $v(p) > 0$ and let α_0 be any generator of $\mathbb{O}$. Write $\alpha = \alpha_0 + n$ with $n \in \mathbb{Z}$. Then $N(\alpha) = N(\alpha_0) + n\mathrm{Tr}(\alpha_0) + n^2$ is a quadratic polynomial in n, and hence has at most two zeroes modulo p. The only case in which we cannot pick an integer n with $p \nmid N(\alpha)$ is when $p = 2$ and the polynomial has two distinct roots modulo 2, that is, $p = 2$ splits in $\mathbb{O}$.

Lemma 2.14. *Let E/L_v be an elliptic curve, given by a Weierstrass equation with coefficients $a_1, \ldots, a_6 \in R_v$ and let Γ be a finite subgroup of $E(L_v)$. Then there is an elliptic curve E', together with an isogeny $\sigma : E \to E'$ with kernel Γ such that* *the coefficients of* $F_\sigma(T)$ *and the coefficients of the Weierstrass equation for* E' *are in the ring* $B = \mathbb{Z}[a_1, \dots, a_6, x(Q), y(Q) : Q \in \Gamma]$ *and moreover* $\sigma^*\omega' = \omega$.

Proof. Vélu's article [1971] gives a Weierstrass equation for an elliptic curve E' and an isogeny $\sigma : E \to E'$ with kernel Γ. The coefficients of the Weierstrass equation are computed explicitly as elements of B. Moreover, the isogeny σ is given as follows. Let S be a complete set of representatives of $\Gamma/\{\pm 1\}$. Then

$$\sigma^* x' = x + \sum_{Q\in S}\Big(\frac{t_Q}{x - x_Q} + \frac{u_Q}{(x-x_Q)^2}\Big),$$
$$\sigma^* y' = y + \sum_{Q\in S}\Big(u_Q\frac{2y + a_1 x + a_3}{(x-x_Q)^3} + \frac{t_Q(a_1(x-x_Q) + (y-y_Q)) + v_Q}{(x-x_Q)^2}\Big),$$

where for each $Q \in S$, Vélu gives t_Q, u_Q and v_Q explicitly as elements of B.

The power series $w(T) = \mathcal{P}(-\frac{1}{y})$ has coefficients in $\mathbb{Z}[a_1, \dots, a_6]$ and starts with T^3. Therefore, $\mathcal{P}(x) = T/w(T)$ and $\mathcal{P}(y) = -1/w(T)$ have coefficients in $\mathbb{Z}[a_1, \dots, a_6]$ and start with T^{-2} and $-T^{-3}$ respectively. The formula above now shows that $\mathcal{P}(\sigma^* x')$ and $\mathcal{P}(\sigma^* y')$ have coefficients in B and the lowest degree terms are respectively T^{-2} and $-T^{-3}$. As a consequence, $F_\sigma(T) = -\mathcal{P}(\sigma^* y)$ is a power series over B with lowest degree term T. □

Proof of Theorem 2.9 if $v(2) = 0$ *or* 2 *does not split in* $\mathcal{O}/\mathbb{Z}$. As we have noted before, we can pick α such that $\mathcal{O} = \mathbb{Z}[\alpha]$ and $v(N(\alpha)) = 0$ and it suffices to prove the theorem for such an α.

Without loss of generality, we may assume that L_v contains the coordinates of all points in the kernel $E[\alpha]$ of α.

Apply Lemma 2.14 with $\Gamma = E[\alpha]$ to get an isogeny σ with kernel $E[\alpha]$. Then by [Silverman 1986, III.4.11], there is an isomorphism $\psi : E' \to E$ such that $\alpha = \psi \circ \sigma$.

Notice that every point in $E[\alpha]$ is $N(\alpha)$-torsion, so its coordinates are v-integral by [Silverman 1986, VII.3.4]. Therefore, both $F_\sigma(T)$ and E' have v-integral coefficients. The power series $F_\psi(T)$ also has v-integral coefficients because of Corollary 2.12 and $v(u) = -v(\alpha) = 0$. As $F_\alpha(T) = F_{\psi\circ\sigma}(T) = F_\psi(F_\sigma(T))$, this finishes the proof. □

Integrality of torsion points. We finish our discussion of formal groups with a result on integrality of $\mathcal{O}$-torsion points.

Let $\mathcal{F}$ be any formal group over R_v and suppose that $\mathrm{End}_{R_v}(\mathcal{F})$ contains a subring $\mathcal{O}$ isomorphic to an order in a number field. Identify $f(T) \in \mathcal{O}$ with $f'(0) \in R_v$ and let $\mathfrak{p} = \mathcal{O} \cap \mathfrak{M}$.

Lemma 2.15. *View $\mathscr{F}(\mathfrak{M})$ as an $\mathbb{O}$-module. Then for any torsion element $z \in \mathscr{F}(\mathfrak{M})$, the annihilator of z is $\mathfrak{p}$-primary, that is, not divisible by a prime different from $\mathfrak{p}$.*

Proof. For any $\alpha \in \mathbb{O} \subset R$, denote the corresponding element of $\operatorname{End}_{R_v}(\mathscr{F})$ by $[\alpha]$. Suppose that z has annihilator $\mathfrak{a}$. Write $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$, where $\mathfrak{c}$ is $\mathfrak{p}$-primary and $\mathfrak{b}$ is coprime to $\mathfrak{p}$. We need to prove $\mathfrak{b} = \mathbb{O}$. So suppose that $\mathfrak{b} \neq \mathbb{O}$. Take any pair of elements $\alpha \in \mathfrak{c} \setminus \mathfrak{a}$ and $\beta \in \mathfrak{b} \setminus \mathfrak{p}$, so $\alpha\beta \in \mathfrak{a}$. Now $[\alpha]z$ is a nonzero element of $\mathscr{F}(\mathfrak{M})$ that is in the kernel of $[\beta]$. But $[\beta](T) = \beta T + \cdots$ is an isomorphism, because $v(\beta) = 0$. Contradiction. □

Now suppose again that E/L_v is an elliptic curve, given by a Weierstrass equation with coefficients in R_v. Let $\mathbb{O} = \operatorname{End}_{L_v}(E)$ and $\mathfrak{p} = \mathfrak{M} \cap \mathbb{O}$.

Corollary 2.16. *Suppose that $Q \in E(L_v)$ is a torsion point. If the annihilator of Q is not $\mathfrak{p}$-primary, then $x(Q)$ is v-integral.* □

3. Elliptic divisibility sequences with complex multiplication

Let E/L be an elliptic curve, given by a Weierstrass equation with coefficients in the ring of integers of the number field L. Let $\mathbb{O} = \operatorname{End}_L(E)$ and let K be the field of fractions of $\mathbb{O}$. There is a natural choice of an embedding of K into L mapping an endomorphism to the element of L by which it multiplies invariant differentials of E.

Fix a point $P \in E(L)$ and let $(B_\alpha)_{\alpha\in\mathbb{O}}$ be defined by $x(\alpha P)\,\mathbb{O}_L = A_\alpha B_\alpha^{-2}$ (with A_α and B_α coprime). For an example, see Table 1.

In the previous section, we have defined $\mathbb{O}$-submodules $E_n(L_v)$ of $E(L_v)$ for which

$$v(B_\alpha) \geq n \Longleftrightarrow \alpha P \in E_n(L_v). \tag{3.1}$$

As a consequence, we get the following result.

Lemma 3.2. *For all $\alpha, \beta \in \mathbb{O}$, if $\alpha \mid \beta$, then $B_\alpha \mid B_\beta$.* □

The *elliptic divisibility sequence* associated to P is the sequence $(B_\mathfrak{a})_\mathfrak{a}$, indexed by ideals $\mathfrak{a}$ of $\mathbb{O}$ and given by

$$B_\mathfrak{a} = \sum_{\alpha\in\mathfrak{a}} B_\alpha.$$

In other words, for every discrete valuation v of L, we have

$$v(B_\mathfrak{a}) = \min_{\alpha\in\mathfrak{a}} v(B_\alpha).$$

By Lemma 3.2, we have $B_{\alpha\mathbb{O}} = B_\alpha$ for every $\alpha \in \mathbb{O}$. Moreover, by definition we have the weak divisibility property: if $\mathfrak{a} \mid \mathfrak{b}$, then $B_\mathfrak{a} \mid B_\mathfrak{b}$. Actually, we even have the following *strong divisibility property*.

α	B_α	
1	1	$= 1$
$1+i$	$1+i$	
2	$(1+i)^2$	$= 2$
$2+i$	$2-i$	
$2+2i$	$(3)(\underline{1+i})^3$	
3	$(3+2i)(3-2i)$	$= 13$
$3+i$	$(\underline{1+i})(\underline{2+i})(4-i)$	
$3+2i$	$(5+4i)(6-i)$	
$3+3i$	$(\underline{1+i})(\underline{3+2i})(\underline{3-2i})$	
4	$(\underline{1+i})^4(\underline{3})(7)$	$= \underline{2}^2 \cdot 3 \cdot 7$
$4+i$	$(5-2i)(14-i)$	
$4+2i$	$(\underline{1+i})^2(\underline{4+i})(\underline{2-i})(16+9i)$	
$4+3i$	$(\underline{2+i})(14-9i)(32+23i)$	
$4+4i$	$(\underline{1+i})^5(\underline{3})(\underline{7})(8+7i)(8-7i)$	
5	$(\underline{2+i})^2(\underline{2-i})^2(6+5i)(6-5i)$	$= 5^2 \cdot 61$
$5+i$	$(\underline{1+i})(\underline{6+i})(\underline{5-4i})(31-20i)$	
$5+2i$	$(11+4i)(2+7i)(40+17i)$	
$5+3i$	$(\underline{1+i})(\underline{14+i})(\underline{5+2i})(159-40i)$	
$5+4i$	$(17-10i)(27-2i)(173+172i)$	
$\vdots$		$\vdots$
6	$(\underline{1+i})^2(\underline{3+2i})(\underline{3-2i})(239)$	$= \underline{2} \cdot \underline{13} \cdot 239$
7	$(1469+84i)(1469-84i)$	$= 2165017$
8	$(\underline{1+i})^6(\underline{3})(\underline{7})(31)(\underline{8+7i})(\underline{8-7i})(16+i)(16-i)$	$= \underline{2}^3 \cdot \underline{3} \cdot \underline{7} \cdot 31 \cdot 113$ $\cdot 257$

Table 1. The curve $E : y^2 = x^3 - 2x$ has CM by $\mathbb{Z}[i]$ via $i(x, y) = (-x, iy)$. This table gives the sequence defined by $P = (-1, 1)$. The nonprimitive divisors are underlined in both the $\mathbb{Z}[i]$-indexed sequence on the left and the $\mathbb{Z}$-indexed sequence on the right. Some primitive divisors on the right are not primitive on the left.

Lemma 3.3. *For any pair of* $\mathcal{O}$*-ideals* $\mathfrak{a}$, $\mathfrak{b}$, *we have*

$$B_{\mathfrak{a}+\mathfrak{b}} = B_{\mathfrak{a}} + B_{\mathfrak{b}}.$$

Proof. The divisibility property implies that the left hand side divides the right. Now let v be a discrete valuation of L and let n be the valuation of the right hand side. Then $v(B_{\mathfrak{a}}), v(B_{\mathfrak{b}}) \geq n$, so αP and βP are in the group $E_n(L_v)$ for all $\alpha \in \mathfrak{a}, \beta \in \mathfrak{b}$. As every element of $\mathfrak{a} + \mathfrak{b}$ is of the form $\alpha + \beta$ and we have that

$(\alpha+\beta)P = \alpha P + \beta P$, it follows that $\gamma P \in E_n(L_v)$ for every $\gamma \in \mathfrak{a}+\mathfrak{b}$, so the valuation of the right hand side is at least n. □

Notice that any interpolation of the $\mathbb{O}$-indexed sequence to an ideal-indexed sequence is completely determined by the strong divisibility property.

We call a prime $\mathfrak{q}$ of L a *primitive divisor* of $B_{\mathfrak{a}}$ if it divides $B_{\mathfrak{a}}$, but does not divide any $B_{\mathfrak{b}}$ with $\mathfrak{a}\nmid\mathfrak{b}$. Given $\mathfrak{q}$, there is a unique ideal $\mathfrak{r}_{\mathfrak{q}}$ of $\mathbb{O}$ such that $\mathfrak{q}$ is a primitive divisor of $B_{\mathfrak{r}_{\mathfrak{q}}}$. We call $\mathfrak{r}_{\mathfrak{q}}$ the *rank of apparition* of $\mathfrak{q}$. Notice that $\mathfrak{r}_{\mathfrak{q}}$ is the annihilator of P in the $\mathbb{O}$-module $E(L_{\mathfrak{q}})/E_1(L_{\mathfrak{q}})$, which is the reduction of E modulo $\mathfrak{q}$ if E is nonsingular modulo $\mathfrak{q}$. For any ideal $\mathfrak{a}$ of $\mathbb{O}$, we have

$$\mathfrak{q} \mid B_{\mathfrak{a}} \quad \Longleftrightarrow \quad \mathfrak{r}_{\mathfrak{q}} \mid \mathfrak{a}.$$

For any $\mathfrak{a}$, we can factor the ideal $B_{\mathfrak{a}}$ as a product of an ideal $D_{\mathfrak{a}}$ and an ideal $B_{\mathfrak{a}}/D_{\mathfrak{a}}$ in such a way that all primes dividing $D_{\mathfrak{a}}$ are primitive divisors of $B_{\mathfrak{a}}$ and all primes dividing $B_{\mathfrak{a}}/D_{\mathfrak{a}}$ are not. We call $D_{\mathfrak{a}}$ the *primitive part of* $B_{\mathfrak{a}}$. In the same way, we can define the primitive part of the classical $\mathbb{Z}$-indexed sequence and denote it by $D_n^{\mathbb{Z}}$. The Main Theorem is equivalent to the statement that $D_{\mathfrak{a}} = \mathbb{O}_L$ for only finitely many $\mathfrak{a}$ coprime to the conductor.

Valuations. For any discrete valuation v of L, let p be the characteristic of the residue field. For any ideal $\mathfrak{a}$ of $\mathbb{O}$, set $v(\mathfrak{a}) = \min_{\alpha\in\mathfrak{a}} v(\alpha)$, or equivalently $v(\mathfrak{a}) = v(\mathfrak{a}\,\mathbb{O}_L)$. From the theory of formal groups, we get the following important property of elliptic divisibility sequences.

Lemma 3.4. *For every pair of nonzero integral $\mathbb{O}$-ideals $\mathfrak{a}$, $\mathfrak{b}$, if $v(B_{\mathfrak{a}}) > \frac{v(p)}{p-1}$, then*

$$v(B_{\mathfrak{a}\mathfrak{b}}) = v(B_{\mathfrak{a}}) + v(\mathfrak{b}).$$

Proof. Assume first that $\mathfrak{a}$ and $\mathfrak{b}$ are principal, say $\mathfrak{a} = \alpha\mathbb{O}$ and $\mathfrak{b} = \beta\mathbb{O}$. Then the statement follows immediately from Proposition 2.8 applied to the map β and the point αP.

Now let $\mathfrak{a}$ and $\mathfrak{b}$ be arbitrary. We claim

$$v(B_{\mathfrak{a}\mathfrak{b}}) = \min_{\substack{\alpha\in\mathfrak{a}\\ \beta\in\mathfrak{b}}} v(B_{\alpha\beta}).$$

Proof of the claim: If $\alpha\in\mathfrak{a}$, $\beta\in\mathfrak{b}$, then $\alpha\beta\in\mathfrak{a}\mathfrak{b}$, so "$\leq$" follows from the divisibility property. On the other hand, let $\gamma \in \mathfrak{a}\mathfrak{b}$ be such that $v(B_\gamma)$ is minimal. Then $v(B_{\mathfrak{a}\mathfrak{b}}) = v(B_\gamma)$. We can write γ in the form $\gamma = \alpha_1\beta_1 + \cdots + \alpha_n\beta_n$, so by (3.1), we have

$$v(B_\gamma) \geq \min_{1\leq i\leq n} v(B_{\alpha_i\beta_i}) \geq \min_{\substack{\alpha\in\mathfrak{a}\\ \beta\in\mathfrak{b}}} v(B_{\alpha\beta}),$$

which proves the claim.

Notice that by the divisibility property, $v(B_\alpha) \geq v(B_\mathfrak{a}) > \frac{v(p)}{p-1}$ for all $\alpha \in \mathfrak{a}$, so the claim implies

$$v(B_{\mathfrak{ab}}) = \min_{\substack{\alpha\in\mathfrak{a}\\ \beta\in\mathfrak{b}}}(v(B_\alpha)+v(\beta)) = \min_{\alpha\in\mathfrak{a}} v(B_\alpha) + \min_{\beta\in\mathfrak{b}} v(\beta) = v(B_\mathfrak{a}) + v(\mathfrak{b}). \qquad \square$$

Lemma 3.4 for $\mathbb{Z}$-indexed sequences is also given by Silverman [1988] for $L=\mathbb{Q}$ and Cheon and Hahn [1998; 1999] for L an arbitrary number field. The versions in [Silverman 1988] and [Cheon and Hahn 1999] are correct, but, unfortunately, [Cheon and Hahn 1998] omits the condition $v(B_m) > v(p)/(p-1)$ and mentions only the weaker condition $v(B_m) > 0$, which is too weak, as we can see from the following example.

Example 3.5. Let $E/\mathbb{Q}$ be given by the Weierstrass equation $y^2+xy=x^3+x^2-2x$ and let $P=(-\frac{1}{4},\frac{7}{8}) \in E(\mathbb{Q})$. Then P is a nontorsion point and $2P=(\frac{121}{64},\frac{913}{512})$, so $B_1=2$, $B_2=8$, so that $\mathrm{ord}_2(B_2) \neq \mathrm{ord}_2(B_1)+\mathrm{ord}_2(2)$, contradicting Lemma 1 of [Cheon and Hahn 1998].

Suppose that v is normalized, that is, $v(L^*)=\mathbb{Z}$. If $v(p)<p-1$, then the conditions $v(B_\mathfrak{a})>0$ and $v(B_\mathfrak{a})>v(p)/(p-1)$ are equivalent. Notice that we can only have $v(p)\geq p-1$ if v is ramified or $p=2$, so there are only finitely many valuations for which we cannot use the weaker condition $v(B_\mathfrak{a})>0$.

In fact, if $L=\mathbb{Q}$ and 2 divides the coefficient a_1 of the Weierstrass equation (2.1), then the duplication formula [Silverman 1986, III.2.3(d)] tells us that even in the case $v(2)>0$ we may use the condition $v(B_m)>0$.

For the finitely many remaining valuations, we will use an asymptotic version. The first step is the following lemma.

Lemma 3.6. *For any pair of elements $\alpha, \beta \in \mathbb{Z}$, if $v(B_\alpha)>0$, then*

$$v(B_{\alpha\beta}) \geq v(B_\alpha),$$

where we have equality if and only if $v(\beta)=0$.

Proof. Let $n=v(B_\alpha)$. By Corollary 2.10, the $\mathbb{O}$-module $E_n(L_v)/E_{n+1}(L_v)$ is isomorphic to the residue field l of L_v. If $v(\beta)=0$, then β induces an automorphism of l, and hence we have equality. Otherwise, β acts as multiplication by 0 on l and we have $v(B_{\alpha\beta})>n$. □

For any valuation v, let r be the positive generator of $\mathfrak{r}_v \cap \mathbb{Z}$, where $\mathfrak{r}_v$ is the rank of apparition of v.

Lemma 3.7. *There is a bound $F_v \in \mathbb{Z}$ such that for all integers $m \in r\mathbb{Z}$, we have $|v(B_m)-v(m)| \leq F_v$.*

Proof. Let $r>0$ be a generator of $\mathfrak{r}_v \cap \mathbb{Z}$, let k be the smallest integer greater than $v(p)/(p-1)$ and let p^l be the largest power of p dividing m/r. Then Lemma 3.6

gives $v(B_m) = v(B_{rp^l})$, so we may assume $m = rp^l$. If $l \geq k$, then Lemma 3.4 with $\mathfrak{b} = (p^{l-k})$, $\mathfrak{a} = (rp^k)$ gives $v(B_m) - v(m) = v(B_{rp^k}) - v(rp^k)$, which is constant and there are only finitely many remaining possibilities for l. □

Corollary 3.8. *For all pairs* $(m, n) \in (r\mathbb{Z} \times \mathbb{Z})$, *we have* $|v(B_{mn}) - v(B_m) - v(n)| \leq 2F_v$. □

For every ideal $\mathfrak{a}$ of $\mathbb{O}$, set $N(\mathfrak{a}) = [\mathbb{O} : \mathfrak{a}]$.

Corollary 3.9. *For every ideal* $\mathfrak{a}$ *of* $\mathbb{O}$, *we have* $v(B_{\mathfrak{a}}) \leq F_v + v(N(\mathfrak{a}))$.

Proof. By the divisibility property, we have $v(B_{\mathfrak{a}}) \leq v(B_{N(\mathfrak{a})}) \leq v(N(\mathfrak{a})) + F_v$. □

Silverman's proof. In [1988], Silverman proved that for $\mathbb{O} = \mathbb{Z}$, all but finitely many terms have a primitive divisor. His proof generalizes to arbitrary number fields L, but not to sequences indexed by quadratic imaginary orders. We will now look at Silverman's proof and see what goes wrong if we try to apply it to sequences indexed by (ideals of) the endomorphism ring.

Let V^∞ be the set of archimedean valuations of L that restrict to the standard absolute value on $\mathbb{Q}$. Let V^0 be the set of nonarchimedean valuations of L that are normalized in the sense that each satisfies $|\frac{1}{p}|_v = p$ for some prime number $p \in \mathbb{Z}$. For every $v \in V = V^\infty \cup V^0$, let $n_v = [L_v : \mathbb{Q}_v]$. For fractional ideals I of L, set $\|I\| = \left|N_{L/\mathbb{Q}}(I)\right|^{1/[L:\mathbb{Q}]}$. Let h_x be the height on E relative to x, defined by $h_x(P) = h(x(P))$, where h is the logarithmic height on $\overline{\mathbb{Q}}$ as given in [Silverman 1986, § VIII.6]. Then by definition

$$\begin{aligned} h_x(\alpha P) &= \sum_{v \in V} \frac{n_v}{[L:\mathbb{Q}]} \log \max\{|x(\alpha P)|_v, 1\} \\ &= \log \|B_\alpha^2\| + \sum_{v \in V^\infty} \frac{n_v}{[L:\mathbb{Q}]} \log \max\{|x(\alpha P)|_v, 1\}. \end{aligned} \tag{3.10}$$

A theorem of Siegel [Silverman 1986, IX.3.1] says that the (finitely many) terms in the final sum are $o(1)\, h_x(\alpha P)$ as $\|\alpha\|$ tends to infinity, where $o(1)$ denotes something which tends to 0. At the same time, those terms are clearly nonnegative, so

$$(1 - o(1))\, h_x(\alpha P) \leq \log \|B_\alpha^2\| \leq h_x(\alpha P) \qquad \text{as } \|\alpha\| \to \infty.$$

We express this in terms of the canonical height function $\widehat{h} : E(\overline{\mathbb{Q}}) \to \mathbb{R}$, as defined in [Silverman 1986, § VIII.9]. That function satisfies

$$\widehat{h}(P) = (\deg(f))^{-1} h(f(P)) + O(1)$$

for every function $f \in L(E)$ and hence $\widehat{h}(\phi(P)) = \deg(\phi)\, \widehat{h}(P)$ for every isogeny of elliptic curves ϕ. As the degree of multiplication by α is $\|\alpha\|^2$ and the degree of the function x is 2, we get

$$(1-o(1))\,\|\alpha\|^2\,\widehat{h}(P) \le \frac{1}{2}\log\|B_\alpha^2\| \le \|\alpha\|^2\,\widehat{h}(P) + O(1) \qquad \text{as } \|\alpha\| \to \infty.$$

The classical proof of the existence of primitive divisors is based on these estimates, combined with the following result. Let $D_n^{\mathbb{Z}}$ be the primitive part of B_n in the $\mathbb{Z}$-indexed sequence, so $B_n/D_n^{\mathbb{Z}}$ is the greatest $\mathbb{O}_L$-ideal dividing B_n that is not divisible by any primitive divisors of B_n.

Lemma 3.11. *There is a positive integer N such that for all $n \in \mathbb{Z}$,*

$$\frac{B_n}{D_n^{\mathbb{Z}}} \;\Big|\; N\prod_p p\; B_{n/p},$$

where the product ranges over the primes dividing n.

Proof. Let v be a discrete valuation of L, normalized by $v(L^*) = \mathbb{Z}$ and let $\mathfrak{q} \subset \mathbb{O}_L$ be the prime ideal corresponding to v.

Suppose that the valuation of the left hand side is positive. Then $\mathfrak{q}$ is not a primitive divisor of B_n, so there is a prime $p\,|\,n$ for which $v(B_{n/p}) > 0$.

Let $r > 0$ be such that $r\mathbb{Z} = \mathfrak{r}_v \cap \mathbb{Z}$ and let $q > 0$ be the rational prime such that $v(q) > 0$. If $v(q) < q-1$, then apply Lemma 3.4 with $\mathfrak{a} = (n/p)$ and $\mathfrak{b} = (p)$. This yields $v(B_n) = v(B_{n/p}) + v(p)$, which is at most equal to the valuation of the right hand side.

For the finitely many valuations with $v(q) \ge q-1$, we apply Corollary 3.8 and find that $v(B_n) \le v(B_{n/p}) + v(p) + 2F_v$. Hence the assertion follows if we take N such that $v(N) \ge 2F_v$ for those finitely many valuations. □

The lemma and the estimates together imply

$$\begin{aligned}\log\|D_n^{\mathbb{Z}}\| &\ge \log\|B_n\| - \log\|n\| - \sum_{p\,|\,n}\log\|B_{n/p}\| - \log\|N\| \\ &\ge \Big(1 - o(1) - \sum_{p\,|\,n} p^{-2}\Big)\, n^2\,\widehat{h}(P) \qquad (n \to \infty),\end{aligned}$$

where $1 - \sum_{p\,|\,n} p^{-2} \ge 0.547$. From some point on, $\|D_n^{\mathbb{Z}}\|$ has to be greater than 1, which proves the following theorem.

Theorem 3.12 ([Silverman 1988]). *For all but finitely many $n \in \mathbb{N}$, B_n has a primitive divisor in the $\mathbb{Z}$-indexed sequence.*
□

Unfortunately, this proof does not work for elliptic divisibility sequences with complex multiplication, since there are too many primes of small norm: if we repeat the argument for example with $\mathbb{O} = \mathbb{Z}[i]$, then the estimate becomes

$$\log \|D_\alpha\| \geq \Big(1 - o(1) - \sum_{\mathfrak{p}|\alpha} |\mathfrak{p}|^{-2}\Big) |\alpha|^2 \widehat{h}(P).$$

If $30|\alpha$, then $1+i, 2+i, 2-i$ and 3 are prime divisors of α and $\sum_{\mathfrak{p}|\alpha} |\mathfrak{p}|^{-2} \geq \frac{1}{2} + \frac{1}{9} + \frac{1}{5} + \frac{1}{5} > 1$, which makes the estimate useless.

The proof of Theorem 3.12 that we have seen is an inclusion-exclusion argument with a single inclusion and one exclusion for every prime, which is insufficient in the general case as we have just shown. Therefore, we will go all the way with the inclusion-exclusion principle.

Notice that every inclusion gives an $o(1)$, so if we have a growing number of inclusions, then we need to know more about the $o(1)$ functions involved. Furthermore, inclusion-exclusion works best with unique factorization, so we really need the ideal-indexed sequence and our estimates will need to hold for the ideal-indexed sequence as well.

We start with the estimates for the element-indexed sequence.

David's Theorem. The more explicit version of Siegel's theorem that we will use is David's theorem. It estimates linear forms in elliptic logarithms and the result is similar to Baker's result for ordinary logarithms.

Let $L \subset \mathbb{C}$ be a number field, k an integer and E/L an elliptic curve, together with a lattice Λ and a complex analytic isomorphism $f : \mathbb{C}/\Lambda \to E(\mathbb{C})$. For $1 \leq i \leq k$, fix an L-valued point $P_i \in E(L)$ and an elliptic logarithm u_i of P_i, that is, a complex number u_i such that $f(u_i) = P_i$.

Theorem 3.13 (David). *Let $\mathscr{L}$ be the linear form $X_1u_1+\cdots+X_ku_k$ in the variables $X_1, \ldots, X_k$. There exists a constant F, depending on E, L, f and the P_i, such that for all $b = (b_1, \ldots, b_k) \in L^n$, if $B = \max_i\{H(b_i)\}$ is sufficiently large and $\mathscr{L}(b) \neq 0$, then*

$$\log |\mathscr{L}(b)| > -F \log(B) (\log \log(B))^{k+1}.$$

Proof. This is a special case of [David 1995, Théorème 2.1]. □

Corollary 3.14. *Let E be an elliptic curve, given by a general Weierstrass equation with coefficients in a number field L and let $P \in E(L)$ be a point of infinite order. For any archimedean valuation v of L, there is a constant G such that for all $\alpha \in \mathbb{O}$ with $\|\alpha\|$ large enough,*

$$\log |x(\alpha P)|_v < G \log \|\alpha\| (\log \log \|\alpha\|)^4.$$

Proof. Completion with respect to v gives an embedding of L into $\mathbb{C}$. Now let $u_1, u_2 \in \mathbb{C}$ be generators of the period lattice Λ of E, define $\mathscr{F} = ([-\frac{1}{2}, \frac{1}{2}]u_1 + [-\frac{1}{2}, \frac{1}{2}]u_2)$ and let $u_3 \in \mathbb{C}$ be an elliptic logarithm of P. Take $b_3 = \alpha$ and let

$b_1, b_2 \in \mathbb{Z}$ be such that $\mathscr{L} = b_1u_1 + b_2u_2 + b_3u_3$ is in $\mathscr{F}$. Then $f(\mathscr{L}) = \alpha P$ and on the compact set $\mathscr{F}$, we have $x(f(z)) = z^{-2}g(z)$ for a holomorphic, hence bounded, function g. Therefore, there is a constant C such that

$$\begin{aligned}\log|x(\alpha P)| &\leq -2\log|\mathscr{L}| + C\\ &< 2F\log(B)(\log\log(B))^4 + C\end{aligned}$$

if $B = \max_i |b_i|$ is large enough.

As $-b_1u_1$ is the integer multiple of u_1 that is nearest to the intersection of the line $u_1\mathbb{R}$ with the line $\alpha u_3 + u_2\mathbb{R}$, we see that $|b_1|$ is bounded by a linear function in $|\alpha|$. In the same way, $|b_2|$ is also bounded by a linear function in $|\alpha|$. □

If we apply this to (3.10), then we get

$$\log\|B_\alpha\| = \|\alpha\|^2\,\widehat{h}(P) \;+\; O(\log\|\alpha\|\,(\log\log\|\alpha\|)^4) \quad (\|\alpha\| \to \infty).$$

Attaching points to the ideal-indexed sequence. David's theorem uses points on elliptic curves, but we need the estimates also for the ideal-indexed sequence. Therefore, for every ideal $\mathfrak{a}$ of $\mathbb{O}$, we will define a point $\mathfrak{a}P$. These points will not all lie on E, but they will lie on a finite set of isogenous curves.

For any $\alpha \in \mathbb{O}$, let $E[\alpha]$ be the kernel of $[\alpha]$. Then for any ideal $\mathfrak{a}$, we define

$$E[\mathfrak{a}] = \bigcap_{\alpha\in\mathfrak{a}} E[\alpha]$$

and we get a quotient isogeny

$$\mathfrak{a} : E \to E/E[\mathfrak{a}] =: E_{\mathfrak{a}}$$

which is defined over L [Silverman 1986, III.4.13.2]. Let $\mathscr{C}$ be the set of integral $\mathbb{O}$-ideals modulo equivalence, where we call $\mathfrak{a}$ and $\mathfrak{b}$ equivalent if there exists an element $x \in K^*$ such that $\mathfrak{a} = x\mathfrak{b}$. By [Cox 1989, Proposition 7.4], the set $\mathscr{C}$ is the union of the class groups of the orders $\mathbb{O}' \subset \mathbb{O}_K$ that contain $\mathbb{O}$, hence it is finite. If $\mathfrak{a}$ and $\mathfrak{b}$ are in the same class in $\mathscr{C}$, then the curves $E_{\mathfrak{a}}$ and $E_{\mathfrak{b}}$ are isomorphic over L. For each class $[\mathfrak{a}] \neq [\mathbb{O}]$ in $\mathscr{C}$, we fix an elliptic curve $E_{[\mathfrak{a}]}$, together with a Weierstrass equation with coefficients in $\mathbb{O}_L$, such that $E_{[\mathfrak{a}]}$ is isomorphic to $E_{\mathfrak{a}}$. For the trivial class, we take $E_{[\mathbb{O}]} = E$. Then we have an isogeny $\mathfrak{a} : E \to E_{[\mathfrak{a}]}$ which is defined up to automorphism of $E_{[\mathfrak{a}]}$.

For any pair of ideals $\mathfrak{a}$, $\mathfrak{b}$ such that $\mathfrak{a} \mid \mathfrak{b}$, there exists a unique quotient isogeny $\lambda = \lambda_{\mathfrak{a},\mathfrak{b}}$ such that $\mathfrak{b} = \lambda \circ \mathfrak{a}$ [Silverman 1986, III.4.11]. As both $\mathfrak{a}$ and $\mathfrak{b}$ are defined over L, so is λ.

For every ideal $\mathfrak{a}$, the point $\mathfrak{a}P \in E_{[\mathfrak{a}]}(L)$ is defined up to automorphism of $E_{[\mathfrak{a}]}$. We now define $\widetilde{A}_{\mathfrak{a}}$ and $\widetilde{B}_{\mathfrak{a}}$ to be the coprime $\mathbb{O}_L$-ideals such that

$$x(\mathfrak{a}P)\,\mathbb{O}_L = \widetilde{A}_{\mathfrak{a}}\widetilde{B}_{\mathfrak{a}}^{-2}.$$

It follows from Corollary 2.10 that $\widetilde{B}_{\mathfrak{a}}$ depends only on the ideal $\mathfrak{a}$ and the choice of Weierstrass equation, but not on the automorphism. Moreover, $\alpha P = (\alpha\mathbb{O})P$ (up to automorphism), so if $\mathfrak{a}$ is principal, then $\widetilde{B}_{\mathfrak{a}} = B_{\mathfrak{a}}$.

For every ideal class $[\mathfrak{a}]$, define the invariant differential

$$\omega_{[\mathfrak{a}]} = \omega_{E_{[\mathfrak{a}]}} = \frac{dx_{E_{[\mathfrak{a}]}}}{y_{E_{[\mathfrak{a}]}}}$$

and the fractional $\mathbb{O}_L$-ideal

$$C_{[\mathfrak{a}]} = \frac{\mathfrak{a}^*\omega_{[\mathfrak{a}]}}{\omega_E}\,(\mathfrak{a}\mathbb{O}_L)^{-1}.$$

Note that the ideal $C_{[\mathfrak{a}]}$ does not depend on the choice of a representative $\mathfrak{a}$ and that $C_{[\mathbb{O}]}$ equals $\mathbb{O}_L$.

Let V be the set of normalized discrete valuations of L. For any v in V, let $p = p_v$ be the prime number such that $v(p) > 0$ and let t_v be the least integer greater than $v(p)/(p-1) + C_{[\mathfrak{a}]} - C_{[\mathfrak{b}]}$ for all $[\mathfrak{a}]$, $[\mathfrak{b}]$. It exists, because the set of ideal classes is finite.

Lemma 3.15. *Let $\mathfrak{a}\,|\,\mathfrak{b}$ be $\mathbb{O}$-ideals and $v \in V$ a normalized discrete valuation. If $v(\widetilde{B}_{\mathfrak{a}}) \geq t_v$, then*

$$v(\widetilde{B}_{\mathfrak{b}}) = v(\widetilde{B}_{\mathfrak{a}}) + v(\mathfrak{b}) - v(\mathfrak{a}) + v(C_{[\mathfrak{b}]}) - v(C_{[\mathfrak{a}]}).$$

Proof. This result follows if we apply Proposition 2.8 to the isogeny $\lambda = \lambda_{\mathfrak{a},\mathfrak{b}}$, which satisfies $v(\lambda^*\omega_{[\mathfrak{b}]}/\omega_{[\mathfrak{a}]}) = v(\mathfrak{b}) - v(\mathfrak{a}) + v(C_{[\mathfrak{b}]}) - v(C_{[\mathfrak{a}]})$. □

Corollary 3.16. *Let v, $\mathfrak{a}$ be as above. If $v(\widetilde{B}_{\mathfrak{a}}) \geq t_v$, then $v(B_{\mathfrak{a}}) = v(\widetilde{B}_{\mathfrak{a}}) - v(C_{[\mathfrak{a}]})$.*

Proof. For any $\alpha \in \mathfrak{a}$, we have

$$v(B_\alpha) = v(\widetilde{B}_\alpha) = v(\widetilde{B}_{\mathfrak{a}}) + v(\alpha) - v(\mathfrak{a}) - v(C_{[\mathfrak{a}]}) \geq v(\widetilde{B}_{\mathfrak{a}}) - v(C_{[\mathfrak{a}]}),$$

where the inequality is an equality if $v(\alpha) = v(\mathfrak{a})$. As $v(B_{\mathfrak{a}}) = \min\{v(B_\alpha) : \alpha \in \mathfrak{a}\}$, the result follows. □

From now on we restrict to invertible ideals $\mathfrak{a}$. For the general case, see Section 4. Let S be the subset of valuations $v \in V$ such that $t_v = 1$.

Lemma 3.17. *For every $v \in S$ and every invertible $\mathbb{O}$-ideal $\mathfrak{a}$, we have $v(\widetilde{B}_{\mathfrak{a}}) = v(B_{\mathfrak{a}})$.*

Proof. Notice first of all that $v \in S$ implies $v(C_{[\mathfrak{a}]}) = 0$ for all $\mathfrak{a}$. By Corollary 3.16, the only thing we need to prove is that if $v(B_{\mathfrak{a}}) > 0$, then $v(\widetilde{B}_{\mathfrak{a}}) > 0$.

Let $\mathfrak{a} = \alpha\mathbb{O} + \beta\mathbb{O}$. Then $\alpha\mathfrak{a}^{-1}$ and $\beta\mathfrak{a}^{-1}$ are coprime $\mathbb{O}$-ideals, so we can take $a \in \alpha\mathfrak{a}^{-1}$ and $b \in \beta\mathfrak{a}^{-1}$ such that $a + b = 1$. Then $0 > v(x(\alpha P)) \geq v(x(a\mathfrak{a}P))$ and $0 > v(x(\beta P)) \geq v(x(b\mathfrak{a}P))$. As $E_{[\mathfrak{a}],1}(L_v)$ is a group, we find $v(x(\mathfrak{a}P)) < 0$, so we are done. □

For the finitely many valuations that are not in S, we will be satisfied with the following asymptotic version.

Lemma 3.18. *For any invertible $\mathcal{O}$-ideal $\mathfrak{a}$ and any $v \in V$, we have*

$$v(B_{\mathfrak{a}}) = v(\widetilde{B}_{\mathfrak{a}}) + O\big(v(N(\mathfrak{a}))\big) \qquad (N(\mathfrak{a}) \to \infty).$$

Proof. If $v(\widetilde{B}_{\mathfrak{a}}) \geq t_v$, then the assertion follows from Corollary 3.16. Otherwise, it is equivalent to Corollary 3.9. □

If we apply Lemma 3.17 to the valuations in S and Lemma 3.18 to the rest, then we find

$$\log N(B_{\mathfrak{a}}) = \log N(\widetilde{B}_{\mathfrak{a}}) + O(\log N(\mathfrak{a})) \qquad (N(\mathfrak{a}) \to \infty). \tag{3.19}$$

Next, we apply David's Theorem, so let v be any *archimedean* valuation of L.

Proposition 3.20. *There is a constant G such that for all but finitely many invertible $\mathcal{O}$-ideals $\mathfrak{a}$,*

$$\log |x(\mathfrak{a}P)|_v < G \log \|\mathfrak{a}\| \, (\log\log \|\mathfrak{a}\|)^4.$$

Proof. First of all, notice that it suffices to prove this for every ideal class separately. So fix $[\mathfrak{a}] \in \mathcal{C}$ and a representative $\widetilde{\mathfrak{a}}$ of $[\mathfrak{a}]$.

Let $\Lambda = u_1\mathbb{Z} + u_2\mathbb{Z}$ be a lattice such that $E_{[\mathfrak{a}],L_v}(\mathbb{C}) \cong \mathbb{C}/\Lambda$ and let $u_3 \in \mathbb{C}$ be such that $u_3 (\mathrm{mod}\ \Lambda)$ corresponds to $[\widetilde{\mathfrak{a}}]P$.

For any $\mathfrak{a} \in [\mathfrak{a}]$, let $b_3 = \alpha/\beta$ be a generator of $\mathfrak{a}/\widetilde{\mathfrak{a}}$. Then the point $\mathfrak{a}P$ corresponds to $b_3u_3 \pmod{\Lambda}$.

Let $b_1, b_2 \in \mathbb{Z}$ be such that $\mathscr{L} = b_1u_1 + b_2u_2 + b_3u_3$ is in a fixed fundamental parallelogram for Λ. Then by David's theorem,

$$\log |x(\mathfrak{a}P)| < 2F \log(B) \, (\log\log(B))^4$$

if $B = \max_i H(b_i)$ is large enough. Notice that the denominator of b_3 divides $\widetilde{\mathfrak{a}}$, so $\log H(b_3) = \log \|b_3\| + O(1) = \log \|\mathfrak{a}\| + O(1)$. At the same time, b_1 and b_2 are bounded by a linear function in $\|b_3\|$, so we find the desired result. □

Theorem 3.21. *For all invertible $\mathcal{O}$-ideals $\mathfrak{a}$, we have*

$$\log \|B_{\mathfrak{a}}\| = \|\mathfrak{a}\|^2 \, \widehat{h}(P) \ + \ O(\log \|\mathfrak{a}\| \, (\log\log \|\mathfrak{a}\|)^4) \quad (\|\mathfrak{a}\| \to \infty),$$

where $\|\mathfrak{a}\| = [\mathcal{O} : \mathfrak{a}]^{1/[K:\mathbb{Q}]}$.

Proof. If we apply Proposition 3.20 to (3.10), then we get

$$\log \|\widetilde{B}_{\mathfrak{a}}\| = \widehat{h}(\mathfrak{a}P) \ + \ O(\log \|\mathfrak{a}\|(\log\log \|\mathfrak{a}\|)^4).$$

The left hand side is $\log \|B_{\mathfrak{a}}\| + O(\log \|\mathfrak{a}\|)$ by (3.19). If $\mathcal{O} = \mathcal{O}_K$, then [Silverman 1994, II.1.5] says that $\mathfrak{a}$ has degree $\|\mathfrak{a}\|^2$. In general, it is [Shimura 1998, Proposition II.10]. □

Corollary 3.22. *For any pair of nonzero invertible $\mathbb{O}$-ideals $\mathfrak{a}$, $\mathfrak{b}$ such that $\|\mathfrak{a}\|$ is suitably large,*

$$B_{\mathfrak{a}} \mid B_{\mathfrak{b}} \iff \mathfrak{a} \mid \mathfrak{b}.$$

In particular, for any pair of nonzero elements α, β such that $\|\alpha\|$ is suitably large,

$$B_{\alpha} \mid B_{\beta} \iff \alpha \mid \beta.$$

Proof. Suppose that $B_{\mathfrak{a}} \mid B_{\mathfrak{b}}$. If $\mathfrak{d} = (\mathfrak{a}, \mathfrak{b})$, then $B_{\mathfrak{d}} = (B_{\mathfrak{a}}, B_{\mathfrak{b}}) = B_{\mathfrak{a}}$ and $\mathfrak{d} \mid \mathfrak{a}$. If $\mathfrak{d}$ strictly contains $\mathfrak{a}$, then this contradicts the bounds of Theorem 3.21. □

Proof of the Main Theorem. We will now use the estimates and an inclusion-exclusion argument to prove the existence of primitive divisors.

We have seen in Lemma 3.4 that only a small part of the growth of $B_{\mathfrak{a}}$ comes from higher powers of nonprimitive divisors. We "neglect" this by introducing $B'_{\mathfrak{a}} = \prod_{\mathfrak{b} \mid \mathfrak{a}} D_{\mathfrak{b}}$, in which these higher powers are eliminated.

Lemma 3.23. *For all $\mathfrak{a}$ and almost every discrete valuation v, we have*

$$v(B'_{\mathfrak{a}}) \le v(B_{\mathfrak{a}}) \le v(B'_{\mathfrak{a}}) + v(\mathfrak{a}).$$

With an added $F_v + \log N(\mathfrak{a})$ on the right hand side, the inequality holds for all v.

In particular,

$$\left|\log \|B_{\mathfrak{a}}\| - \log \|B'_{\mathfrak{a}}\|\right| \le \log \|\mathfrak{a}\| + C.$$

Proof. Let v be any discrete valuation of L. The first inequality is true by definition. Now suppose that $v(B_{\mathfrak{a}}) > 0$ and let $\mathfrak{r}$ be the rank of apparition of v. If $v(p) < p-1$, then Lemma 3.4 implies $v(B_{\mathfrak{a}}) \le v(B_{\mathfrak{a}\mathfrak{r}}) = v(B_{\mathfrak{r}}) + v(\mathfrak{a}) = v(B'_{\mathfrak{a}}) + v(\mathfrak{a})$. For the finitely many valuations with $v(p) \ge p-1$, Corollary 3.9 shows that the same holds with an added $F_v + \log N(\mathfrak{a})$.

The final statement follows if one sums over all v. □

We will now prove the Main Theorem for ideals coprime to the index $f = [\mathbb{O}_K : \mathbb{O}]$. For the general case, see Section 4.

Proof. Let μ be the Möbius function for the set of ideals of $\mathbb{O}$ coprime to f, so

$$\mu(\mathfrak{b}) = \begin{cases} 0 & \text{if a square of an ideal divides } \mathfrak{b}, \\ (-1)^n & \text{if } \mathfrak{b} \text{ is a product of } n \text{ distinct primes.} \end{cases}$$

The inclusion-exclusion principle yields

$$\begin{aligned} \log \|D_{\mathfrak{a}}\| &= \sum_{\mathfrak{b} \mid \mathfrak{a}} \mu(\mathfrak{b}) \log \|B'_{\mathfrak{a}/\mathfrak{b}}\| \\ &= \sum_{\mathfrak{b} \mid \mathfrak{a}} \mu(\mathfrak{b}) \log \|B_{\mathfrak{a}/\mathfrak{b}}\|\, O(\log \|\mathfrak{a}\|), \end{aligned}$$

to which we can apply Theorem 3.21 and get

$$\begin{aligned}\log \|D_{\mathfrak{a}}\| &= \widehat{h}(P) \sum_{\mathfrak{b}\,|\,\mathfrak{a}} \mu(\mathfrak{b})\, \|\mathfrak{a}/\mathfrak{b}\|^2 \;+\; \sum_{\mathfrak{b}\,|\,\mathfrak{a}} O(\log \|\mathfrak{a}\|\,(\log\log \|\mathfrak{a}\|)^4)\\ &= \|\mathfrak{a}\|^2\, \widehat{h}(P) \prod_{\mathfrak{p}\,|\,\mathfrak{a}} (1 - \|\mathfrak{p}\|^{-2}) \;+\; O(\|\mathfrak{a}\|^{\epsilon}).\end{aligned}$$

The product is at least

$$\prod_{p \le \|\mathfrak{a}\|} (1 - p^{-1})^2,$$

and Mertens' Theorem [Hardy and Wright 1938, 22.9 Theorem 430] states that

$$\prod_{p \le X} (1 - p^{-1}) \sim \frac{e^{-\gamma}}{\log X} \qquad (X \to \infty),$$

where $\gamma \approx 0.5772$ is the Euler constant. If we pick $\epsilon < 2$, then this finishes the proof of the Main Theorem for ideals coprime to the index f. In the general case, inclusion-exclusion is harder and we will show how to do it in Section 4.

For $\mathbb{Z}$-indexed sequences, regardless of whether the curve has complex multiplication, (3.24) is exactly Proposition 1.3. □

We will now prove the corollary about splitting behavior of primitive divisors in $\mathbb{Z}$-indexed sequences over CM curves. Let K' be the field of fractions of $\mathbb{O}' = \operatorname{End}_{\overline{L}}(E)$.

Corollary 3.24. *Suppose that not all endomorphisms of E over $\overline{L}$ are defined over L. Define for $n \in \mathbb{Z}$, the numbers*

$$\begin{aligned} r_n &= \#\{p \in \mathbb{N} : \; p \,|\, n,\ p \text{ is a prime ramifying in } \mathbb{O}'/\mathbb{Z} \text{ and } p \nmid [\mathbb{O}_{K'} : \mathbb{O}']\},\\ s_n &= \#\{p \in \mathbb{N} : \; p \,|\, n \text{ and } p \text{ is a prime splitting in } \mathbb{O}'/\mathbb{Z}\}.\end{aligned}$$

Then for almost all n, the term B_n has at least $r_n + s_n + 1$ primitive divisors, of which at least s_n split in $K'L/L$.

Proof. Let σ denote the unique nontrivial automorphism of KL/L. Notice that $B_{\sigma(\mathfrak{a})} = \sigma(B_{\mathfrak{a}})$ for every $\mathbb{O}$-ideal $\mathfrak{a}$.

Suppose that n is large enough such that $B_{\mathfrak{a}}$ has a primitive divisor (in the $\mathbb{O}$-ideal-indexed sequence) for all $\mathfrak{a}$ with $\|\mathfrak{a}\| \ge \sqrt{n}$.

For any prime number $p \,|\, n$ that splits in $K/\mathbb{Q}$, write $(p) = \mathfrak{p}\sigma(\mathfrak{p})$. Then $B_{n/\mathfrak{p}}$ has a primitive divisor $\mathfrak{q} \subset \mathbb{O}_L$. If $\mathfrak{q}$ is ramified or inert in KL/L, then $\sigma(\mathfrak{q}) = \mathfrak{q}$, so $\mathfrak{q}$ is also a divisor of $B_{n/\sigma(\mathfrak{p})}$, contradicting the assumption that $\mathfrak{q}$ is primitive at $B_{n/\mathfrak{p}}$. Therefore, $\mathfrak{q}$ is a prime of L that splits in KL/L and is a primitive of B_n in the $\mathbb{N}$-indexed sequence.

There are at least $r_n + 1$ more primitive divisors, because B_n itself also has a primitive divisor as well as each $B_{n/\mathfrak{p}}$ where $p = \mathfrak{p}^2$ is a ramifying prime divisor of n. □

4. The general case

We will now show how to give a proof of the Main Theorem even for ideals that may not be coprime to the index $[\mathcal{O}_K : \mathcal{O}]$. The set of all ideals does not have unique factorization, so the Möbius functions become more tricky. Moreover, when we do inclusion-exclusion with invertible ideals that are not coprime to $[\mathcal{O}_K : \mathcal{O}]$, we will encounter ideals that are not invertible. The first thing we need to do is therefore to generalize Theorem 3.21 to ideals that may not be invertible.

The only part of the proof of Theorem 3.21 that uses invertibility of the ideal $\mathfrak{a}$ is the part of the proof of Lemma 3.17 that states that if $v(B_{\mathfrak{a}}) > 0$, then $v(\widetilde{B}_{\mathfrak{a}}) > 0$. We prove this in the general case for a smaller set of valuations S'. Recall that S was the set of all normalized discrete valuations v of L for which $v(p) < p - 1$ and $v(C_{[\mathfrak{a}]}) = 0$ for all $[\mathfrak{a}]$. We let S' be the set of valuations in S for which also $v([\mathcal{O}_K : \mathcal{O}]) = 0$ and the Weierstrass equation of $E_{[\mathfrak{a}]}$ is nonsingular for every $[\mathfrak{a}] \in \mathscr{C}$. Notice that S' still contains all but finitely many valuations of V.

Lemma 4.1. *For every $v \in S'$ and every $\mathcal{O}$-ideal $\mathfrak{a}$, we have that $v(\widetilde{B}_{\mathfrak{a}}) = v(B_{\mathfrak{a}})$.*

Proof. The only thing left to prove is that if $v(B_{\mathfrak{a}}) > 0$, then $v(\widetilde{B}_{\mathfrak{a}}) > 0$. We already know this for invertible ideals $\mathfrak{a}$. Write $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$, where $\mathfrak{b}$ is coprime to the index $f = [\mathcal{O}_K : \mathcal{O}]$ and $\mathfrak{c}$ divides f^n for some integer n. Without loss of generality, we may assume that all points in $E_{[\mathfrak{c}]}[f^n]$ are defined over L_v and that $v(L_v) = \mathbb{Z}$. We claim that the reduction morphism

$$E_{[\mathfrak{b}]}(L_v)[f^n] \to (E_{[\mathfrak{b}]}(L_v)/E_{[\mathfrak{b}],1}(L_v))[f^n] \tag{4.2}$$

is an isomorphism of $\mathcal{O}$-modules. This morphism of $\mathcal{O}$-modules is injective by [Silverman 1986, VII.3.4] or Lemma 2.15 and since $E_{[\mathfrak{b}]}$ has good reduction modulo v and $v(f) = 0$, both sides have the same cardinality f^{2n} [Silverman 1986, III.6.4(b)], which proves the claim.

Now consider the point $\mathfrak{b}P \in E_{[\mathfrak{b}]}(L_v)$. Since the lemma is already proved for invertible ideals, we know that $(\mathfrak{b}P + E_{[\mathfrak{b}],1}(L_v))$ is γ-torsion for every $\gamma \in \mathfrak{c}$. As (4.2) is an isomorphism of $\mathcal{O}$-modules, this implies that there is a point $Q \in E_{[\mathfrak{b}]}(L_v)[\mathfrak{c}]$ such that $\mathfrak{b}P \equiv Q$ modulo $E_{[\mathfrak{b}],1}(L_v)$. In particular, by Lemma 2.13 (or also Proposition 2.8 if we remove some more valuations from S), $\mathfrak{c}\mathfrak{b}P \equiv \mathfrak{c}Q$ modulo $E_{[\mathfrak{b}\mathfrak{c}],1}(L_v)$ and $\mathfrak{c}Q = O$ on $E_{[\mathfrak{b}\mathfrak{c}]}$. □

It follows that Theorem 3.21 holds for all ideals $\mathfrak{a}$ of $\mathcal{O}$.

Next, we do inclusion-exclusion in general. Let $\mu(\mathfrak{a}, \mathfrak{b})$ be defined recursively for $\mathfrak{b} \mid \mathfrak{a}$ by

$$\mu(\mathfrak{a}, \mathfrak{a}) = 1 \quad \text{and} \quad \sum_{\mathfrak{c} \mid \mathfrak{b} \mid \mathfrak{a}} \mu(\mathfrak{a}, \mathfrak{b}) = 0 \quad (\text{for all } \mathfrak{c} \mid \mathfrak{a} \text{ with } \mathfrak{c} \neq \mathfrak{a}).$$

Previously, $\mu(\mathfrak{a}, \mathfrak{b})$ depended only on $\mathfrak{a}/\mathfrak{b}$ and we denoted it by $\mu(\mathfrak{a}/\mathfrak{b})$.

The inclusion-exclusion principle, Lemma 3.23 and Theorem 3.21 give

$$\log \|D_{\mathfrak{a}}\| = \widehat{h}(P) \sum_{\mathfrak{b} \mid \mathfrak{a}} \mu(\mathfrak{a}, \mathfrak{b}) \, \|\mathfrak{b}\|^2 + \sum_{\mathfrak{b} \mid \mathfrak{a}} O(\log \|\mathfrak{a}\| \, (\log\log \|\mathfrak{a}\|)^4).$$

The set of ideals of $\mathbb{O}$ is the direct sum of the sets of ideals of the localizations of $\mathbb{O}$ at its primes. Therefore, the Möbius function of the ideals of $\mathbb{O}$ is the product of the Möbius functions of the localizations at the primes of $\mathbb{O}$.

Lemma 4.3. *Let $\mathfrak{p}$ be a prime ideal of $\mathbb{O}$ and $I \subset \mathbb{O}_{\mathfrak{p}}$ a nontrivial invertible ideal of the localization. Then there is a unique ideal $J_0 \mid I$ (which is not necessarily invertible) such that $J_0 \neq I$ and such that for every ideal $J \mid I$ with $J \neq I$, we have $J \mid J_0$. Moreover, the norm of this ideal is $N(I)/N(\mathfrak{p})$.*

Note that in terms of the Möbius functions, we have $\mu(I, J_0) = -1$ and $\mu(I, J) = 0$ for all $J \neq I, J_0$.

Proof. It is clear that any two ideals as in the lemma are equal, so we only need to prove the existence. If $\mathfrak{p}$ is invertible, then the statement holds with $J_0 = I/\mathfrak{p}$.

So suppose that $\mathfrak{p}$ is singular and let p be the rational prime with $\mathfrak{p} \mid p$. Let n be such that $\mathbb{O} = \mathbb{Z} + n\mathbb{O}_K$ and set $\mathbb{O}' = \mathbb{Z} + (n/p)\,\mathbb{O}_K$. Let R and R' be the localizations of $\mathbb{O}$ and $\mathbb{O}'$ at the $\mathbb{O}$-ideal $\mathfrak{p}$. As I is invertible, it is principal, say $I = \alpha R$. Let $J_0 = \alpha R'$. We need to show that every R-ideal J that strictly contains I contains J_0.

If we allow fractional ideals, then without loss of generality, we may assume $\alpha = 1$, so $I = R$ and $J_0 = R'$. Let $\omega \in R'$ be such that $R' = \mathbb{Z}_{(p)} + \omega\mathbb{Z}_{(p)}$ and let $T, N \in \mathbb{Z}_{(p)}$ be such that $\omega^2 - T\omega + N = 0$. We need to prove $\omega \in J$. Take any element γ of $J \setminus R$. We have $\gamma = a + b\omega$ with $a, b \in \mathbb{Q}$. After multiplication by a power of p, we may assume $\gamma \in (1/p)R \setminus R$, so pa and b are both in $\mathbb{Z}_{(p)}$, but not both in $p\mathbb{Z}_{(p)}$. If $a \in \mathbb{Z}_{(p)}$, then $b \notin p\mathbb{Z}_{(p)}$, hence $\omega = b^{-1}(\gamma - a) \in J$. Otherwise, $\gamma p\omega = ap\omega + bp(T\omega - N)$ is in J and so is $p\omega$, hence $ap\omega$ is in J and $ap \in R^*$.

Finally, from the construction, we get $N(I)/N(J_0) = [R' : R] = p = [R : pR'] = N(\mathfrak{p})$. □

We conclude that if $\mathfrak{a}$ is invertible, then

$$\log \|D_{\mathfrak{a}}\| = \|\mathfrak{a}\|^2 \, \widehat{h}(P) \prod_{\mathfrak{p} \mid \mathfrak{a}} (1 - \|\mathfrak{p}\|^{-2}) + O(\|\mathfrak{a}\|^{\epsilon}), \tag{4.4}$$

which proves the Main Theorem.

The following example shows why we restrict to invertible ideals in our main result. Suppose that the index $[\mathbb{O}_K : \mathbb{O}]$ is a prime number p and that p is inert in $\mathbb{O}_K$. For any $\mathbb{O}$-ideal $\mathfrak{a}$, we have $\mathfrak{a}\mathbb{O}_K \supset \mathfrak{a} \supset p\mathfrak{a}\mathbb{O}_K$. If $\mathfrak{a}$ is $\mathfrak{p}$-primary, then $\mathfrak{a}\mathbb{O}_K = p^n\mathbb{O}_K$ for some n. On the other hand, any group $\mathfrak{a}$ which is strictly between $p^n\mathbb{O}_K$ and $p^{n+1}\mathbb{O}_K$, is an $\mathbb{O}$-module and there are $p+1$ such groups. We find

$$\mu(p^n\mathbb{O}_K, \mathfrak{a}) = \begin{cases} 1 & \text{if } \mathfrak{a} = p^n\mathbb{O}_K, \\ -1 & \text{if } \mathfrak{a} \text{ is strictly between } p^{n-1}\mathbb{O}_K \text{ and } p^n\mathbb{O}_K, \\ p & \text{if } \mathfrak{a} = p^{n-1}\mathbb{O}_K, \\ 0 & \text{otherwise.} \end{cases}$$

The inclusion-exclusion principle now gives

$$\begin{aligned} \log \|D_{p^{n-1}\mathbb{O}_K}\| &= \widehat{h}(P)(p^{2n-1} - (p+1)p^{2n-2} + pp^{2n-3}) + O(n\log(n)^4) \\ &= O(n\log(n)^4). \end{aligned}$$

Only the error term remains, so we cannot conclude from this that there exists a primitive divisor. On the other hand, the size of the error term does leave some space for primitive divisors, so other methods are needed to give a result on primitive divisors of $B_\mathfrak{a}$ for noninvertible ideals $\mathfrak{a}$.

Acknowledgments

The research for this paper was done as a Master's thesis at Universiteit Utrecht under supervision of Gunther Cornelissen, to whom the author expresses his gratitude. Thanks also to Peter Stevenhagen and the anonymous referees for many useful comments.

References

[Ayad 1992] M. Ayad, "Points S-entiers des courbes elliptiques", *Manuscripta Math.* **76**:3-4 (1992), 305–324. MR 93i:11064 Zbl 0773.14014

[Bang 1886] A. S. Bang, "Taltheoretiske undersøgelser", *Zeuthen Tidskr.* (5) **4** (1886), 70–80, 130–137. JFM 19.0168.02

[Bosch, Lütkebohmert and Raynaud 1990] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron Models*, Ergebnisse der Mathematik (3) **21**, Springer, Berlin, 1990. MR 91i:14034 Zbl 0705.14001

[Cheon and Hahn 1998] J. Cheon and S. Hahn, "Explicit valuations of division polynomials of an elliptic curve", *Manuscripta Math.* **97**:3 (1998), 319–328. MR 99i:11039 Zbl 0922.11048

[Cheon and Hahn 1999] J. Cheon and S. Hahn, "The orders of the reductions of a point in the Mordell–Weil group of an elliptic curve", *Acta Arith.* **88**:3 (1999), 219–222. MR 2000i:11084 Zbl 0933.11029

[Chudnovsky and Chudnovsky 1986] D. V. Chudnovsky and G. V. Chudnovsky, "Sequences of numbers generated by addition in formal groups and new primality and factorization tests", *Adv. in Appl. Math.* **7**:4 (1986), 385–434. MR 88h:11094 Zbl 0614.10004

[Cornelissen and Zahidi 2007] G. Cornelissen and K. Zahidi, "Elliptic divisibility sequences and undecidable problems about rational points", *J. Reine Angew. Math.* **613** (2007), 1–33.

[Cox 1989] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory and complex multiplication*, Wiley, New York, 1989. MR 90m:11016 Zbl 0701.11001

[David 1995] S. David, *Minorations de formes linéaires de logarithmes elliptiques*, Mém. Soc. Math. France (N.S.) **62**, Soc. math. de France, Paris, 1995. MR 98f:11078 Zbl 0859.11048

[Durst 1952] L. K. Durst, "The apparition problem for equianharmonic divisibility sequences", *Proc. Nat. Acad. Sci. U. S. A.* **38** (1952), 330–333. MR 14,139b Zbl 0046.28905

[Hardy and Wright 1938] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Clarendon Press, Oxford, 1938. MR 0067125 Zbl 0020.29201 JFM 64.0093.03

[Satoh 2004] T. Satoh, "Generalized division polynomials", *Math. Scand.* **94**:2 (2004), 161–184. MR 2005b:11078 Zbl 1064.11044

[Shimura 1998] G. Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton Mathematical Series **46**, Princeton University Press, Princeton, NJ, 1998. MR 99e:11076 Zbl 0908.11023

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986. MR 87g:11070 Zbl 0585.14026

[Silverman 1988] J. H. Silverman, "Wieferich's criterion and the abc-conjecture", *J. Number Theory* **30**:2 (1988), 226–237. MR 89m:11027 Zbl 0654.10019

[Silverman 1994] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, New York, 1994. MR 96b:11074 Zbl 0911.14015

[Vélu 1971] J. Vélu, "Isogénies entre courbes elliptiques", *C. R. Acad. Sci. Paris Sér. A* **273** (1971), 238–241. MR 45 #3414 Zbl 0225.14014

[Ward 1948] M. Ward, "Memoir on elliptic divisibility sequences", *Amer. J. Math.* **70** (1948), 31–74. MR 9,332j Zbl 0035.03702

[Ward 1950] M. Ward, "Arithmetical properties of polynomials associated with the lemniscate elliptic functions", *Proc. Nat. Acad. Sci. U. S. A.* **36** (1950), 359–362. MR 12,159h Zbl 0041.36804

[Washington 2003] L. C. Washington, *Elliptic curves: number theory and cryptography*, Chapman & Hall/CRC, Boca Raton, FL, 2003. MR 2004e:11061 Zbl 1034.11037

[Zsigmondy 1892] K. Zsigmondy, "Zur Theorie der Potenzreste", *Monatsh. Math. Phys.* **3**:1 (1892), 265–284. MR 1546236 JFM 24.0176.02

Communicated by Bjorn Poonen
Received 2007-07-30 Revised 2007-11-12 Accepted 2007-12-25

streng@math.leidenuniv.nl *Mathematisch Instituut, Universiteit Leiden, Postbus 9512,*
2300 RA Leiden, The Netherlands
http://www.math.leidenuniv.nl/~streng

The Coleman–Mazur eigencurve is proper at integral weights

Frank Calegari

We prove that the Coleman–Mazur eigencurve is proper (over weight space) at integral weights in the center of weight space.

1. Introduction

The eigencurve $\mathscr{E}$ is a rigid analytic space parameterizing overconvergent — and hence classical — modular eigenforms of finite slope. Since Coleman and Mazur's original work [1998], there have been numerous generalizations [Buzzard 2008; Chenevier 2004], as well as alternative constructions using modular symbols [Ash and Stevens $\geq$ 2008] and p-adic representation theory [Emerton 2006]. In spite of these advances, several elementary questions about the geometry of $\mathscr{E}$ remain. One such question was raised by Coleman and Mazur: does there exist a p-adic family of finite slope overconvergent eigenforms over a punctured disk, and converging, at the puncture, to an overconvergent eigenform of infinite slope? Another way of phrasing this question is to ask whether the projection $\pi : \mathscr{E} \rightarrow \mathscr{W}$ satisfies the valuative criterion for properness[1]. In [Buzzard and Calegari 2006], this was proved in the affirmative for the particular case of tame level $N = 1$ and $p = 2$. The proof, however, was quite explicit and required (at least indirectly) that the curve $X_0(Np)$ have genus zero. In this note, we work with general p and arbitrary tame level, although our result only applies at certain arithmetic weights in the center of weight space.

Recall that the $\mathbb{C}_p$-points of $\mathscr{W}$ are the continuous homomorphisms from the Iwasawa algebra

$$\Lambda := \mathbb{Z}_p[[\varprojlim(\mathbb{Z}/Np^k\mathbb{Z})^\times]]$$

to $\mathbb{C}_p$. Let χ denote the cyclotomic character. Our main theorem is:

MSC2000: 11F11.

Keywords: p-adic modular forms, the eigencurve, overconvergent modular forms.

Supported in part by the American Institute of Mathematics.

[1] The curve $\mathscr{E}$ has infinite degree over weight space $\mathscr{W}$, and so the projection $\pi : \mathscr{E} \rightarrow \mathscr{W}$ cannot technically be proper.

Theorem 1.1. *Let $\mathscr{E}$ be the p-adic eigencurve of tame level N. Let D denote the closed unit disk, and let $D^{\times}$ denote D with the origin removed. Let $h : D^{\times} \to \mathscr{E}$ be a morphism such that $\pi \circ h$ extends to D. Suppose, moreover, that $(\pi \circ h)(0) = \kappa$, where κ is of the form*

$$\kappa = \chi^{k} \cdot \psi,$$

for $k \in \mathbb{Z}$ and ψ a finite order character of conductor dividing N. Then there exists a map $\widetilde{h} : D \to \mathscr{E}$ making the following diagram commute:

$$\begin{tikzcd}
D^{\times} \arrow[r, "h"] \arrow[d] & \mathscr{E} \arrow[d, "\pi"] \\
D \arrow[r] \arrow[ur, "\widetilde{h}"] & \mathscr{W}
\end{tikzcd}$$

Our strategy in proving Theorem 1.1 follows that of [Buzzard and Calegari 2006]. We first try to prove that finite slope overconvergent eigenforms extend far into the supersingular region whereas forms of infinite slope do not. Then, since a limit of highly overconvergent forms is also highly overconvergent, this leads to a contradiction. The main technical improvement is Corollary 3.2, which we deduce from a lemma of Wan (who attributes the result to Coleman). It is plausible that the properness of the eigencurve is a global manifestation of a purely local theorem; such an idea was suggested to the author — at least at integral weights — by Mark Kisin. However, even with current advances in the technology of local Galois representations, a natural conjectural statement implying properness has not yet been formulated. One issue to bear in mind is that slightly stronger statements one may conjecture are false. For example, there exists a pointwise sequence of finite slope forms converging to an infinite slope form [Coleman and Stein 2004].

2. Overconvergent modular forms

Let $N \geq 5$ be an integer coprime to p; let $X = X_1(N)$; and let $X_0(p) = X(\Gamma_1(N) \cap \Gamma_0(p))$. Since $N \geq 5$, the curves X and $X_0(p)$ are the compactifications of smooth moduli spaces. The curve X comes equipped with a natural sheaf ω, which, away from the cusps, is the pushforward of the sheaf of differentials on the universal modular curve. If $p \geq 5$, let A be a characteristic zero lift of the Hasse invariant with coefficients in $W(\overline{\mathbb{F}}_p)[[q]]$, and thus, $A \in H^0(X/W(\overline{\mathbb{F}}_p), \omega^{\otimes(p-1)})$ by the q-expansion principle. We further insist that A has trivial character. Such an A always exists, for example, $A = E_{p-1}$. Let $X_0(p,r) \subseteq X_0^{\mathrm{an}}(p)$ denote the connected component containing ∞ of the affinoid $\{x \in X_0^{\mathrm{an}}(p);\ |A(x)| \geq |r|\}$. Standard arguments imply that $|A(x)|$ on $X_0(p,r)$ is independent of the choice of A, provided that $v(r) < 1$.

Let $r \in \mathbb{C}_p$ be an element with $p/(p+1) > v(r) > 0$. Let χ denote the cyclotomic character; let ψ denote a finite order character of conductor dividing N; and let $k \in \mathbb{Z}$.

Definition 2.1. The overconvergent modular forms of weight $\chi^k \cdot \psi$, level N, and radius of convergence r are sections of $H^0(X_0(p, r), \omega^{\otimes k})$ on which the diamond operators act via ψ. We denote this space by $M(\mathbb{C}_p, N, \chi^k \cdot \psi, r)$. The space of overconvergent modular forms of weight $\chi^k \cdot \psi$ and level N is

$$M(\mathbb{C}_p, N, \chi^k \cdot \psi) := \bigcup_{|r|<1} M(\mathbb{C}_p, N, \chi^k \cdot \psi, r).$$

The space $M(\mathbb{C}_p, N, \chi^k \cdot \psi, r)$ has a natural Banach space structure. If $\chi^k = 1$, the norm $\|\cdot\|$ is the supremum norm.

Let $\kappa \in \mathcal{W}(\mathbb{C}_p)$ denote a point in weight space. Recall that the Eisenstein series $E(\kappa)$ is defined away from zeroes of the Kubota–Leopoldt zeta function $\zeta(\kappa)$ by the following formulas:

$$E(\kappa) = 1 + \frac{2}{\zeta(\kappa)} \sum_{n=1}^{\infty} \sigma_\kappa^*(n) q^n, \qquad \sigma_\kappa^*(n) = \sum_{(d,p)=1}^{d|n} \kappa(d) d^{-1}.$$

The coefficients of $E(\kappa)$ are rigid analytic functions on $\mathcal{W}$ away from the zeroes of ζ. If κ is trivial on the roots of unity in $\mathbb{Q}_p$, then, as a q-expansion, $E(\kappa)$ is congruent to 1 modulo the maximal ideal of $\overline{\mathbb{Z}}_p$. Coleman's idea is to define overconvergent forms of weight κ using the formal q-expansion $E(\kappa)$. Before we recall the definition, we also recall some elementary constructions related to weight space. If

$$\mathbb{Z}_{p,N} := \varprojlim (\mathbb{Z}/Np^k\mathbb{Z})^\times,$$

there is a natural isomorphism $\mathbb{Z}_{p,N} \simeq (\mathbb{Z}/N\boldsymbol{q}\mathbb{Z})^\times \times (1 + \boldsymbol{q}\mathbb{Z}_p)$, where $\boldsymbol{q} = p$ if p is odd, and $\boldsymbol{q} = 4$ otherwise. If $a \in \mathbb{Z}_{p,N}$, then $\langle\langle a \rangle\rangle$ denotes the projection of a onto the second factor, and $\tau(a) = a/\langle\langle a \rangle\rangle$ the projection onto the first. The rigid analytic space $\mathcal{W}$ has a natural group structure. Denote the connected component of the identity of $\mathcal{W}$ by $\mathcal{B}$; the component group of $\mathcal{W}$ is $(\mathbb{Z}/N\boldsymbol{q}\mathbb{Z})^\times$. If $\kappa \in \mathcal{W}(\mathbb{C}_p)$, then let $\langle \kappa \rangle$ denote the weight $a \mapsto \kappa(\langle\langle a \rangle\rangle)$ and $\tau(\kappa)$ the weight $a \mapsto \kappa(\tau(a))$; $\langle \kappa \rangle$ is the natural projection of κ onto $\mathcal{B}$. If χ denotes the cyclotomic character, then for any character ψ of $(\mathbb{Z}/\boldsymbol{q}N\mathbb{Z})^\times$, there is a unique congruence class modulo $p-1$ (or modulo 2 if $p = 2$) such that for any $k \in \mathbb{Z}$ in this congruence class, $\tau(\eta \cdot \chi^{-k})$ has conductor dividing N. We fix once and for all a choice of representative $k \in \mathbb{Z}$ for this congruence class.

We now recall the definition of overconvergent modular forms of weight κ:

Definition 2.2. Overconvergent modular forms of weight κ and tame level N are q-expansions of the form $VE_{\langle\kappa\cdot\chi^{-k}\rangle}\cdot F$, where $F\in M(\mathbb{C}_p, N, \chi^k\cdot\tau(\kappa\cdot\chi^{-k}))$.

This is not exactly the definition that occurs in Section 2.4 of [Coleman and Mazur 1998], since we have chosen to work with $\Gamma_0(p)$ structure rather than $\Gamma_1(p)$ structure. Yet both definitions are easily seen to be equivalent, using, for example, Theorem 2.2.2 of the same reference. We do not define the radius of convergence of an overconvergent form of general weight.

3. Hasse invariants

In this section, we prove some estimates for the convergence of certain overconvergent modular forms related to Hasse invariants. As in Section 2, let A be a characteristic zero lift of the Hasse invariant with coefficients in $W(\overline{\mathbb{F}}_p)[[q]]$ for $p\geq 5$.

Lemma 3.1. *Let $v(r)<1/(p+1)$, and let x be a point on $X_0(p,r)$. Then*

$$\frac{A(x)}{VA(x)}\equiv 1 \mod \frac{p}{A(x)^{p+1}}.$$

Proof. This follows directly from Lemma 2.1 of [Wan 1998], after noting that the argument remains unchanged if E_{p-1} is replaced by A. □

Corollary 3.2. *Suppose that $v(r)<1/(p+1)$. Then* $\log(A/VA)\in M(\mathbb{C}_p, N, 1, r)$. *If $s\in\mathbb{C}_p$ is sufficiently small, then $(A/VA)^s\in M(\mathbb{C}_p, N, 1, r)$.*

Proof. From Lemma 3.1, we deduce that $A/VA-1$ has norm less than one on $X_0(p,r)$, which implies the first claim. Moreover, $\|s\cdot\log(A/VA)\|\ll 1$ for sufficiently small s, and hence, if s is sufficiently small,

$$(A/VA)^s=\exp\bigl(s\cdot\log(A/VA)\bigr)$$

is well defined and lies in $M(\mathbb{C}_p, N, 1, r)$. □

Remark. When $p=2$ or 3, the conclusions of Corollary 3.2 still hold with A replaced by the classical modular forms E_4 and E_6 respectively, as can be seen by a direct computation. To aid the reader in such a computation, let $f=\Delta(2\tau)/\Delta(\tau)$ and $g=(\Delta(3\tau)/\Delta(\tau))^{1/2}$ be uniformizers for $X_0(2)$ and $X_0(3)$ respectively. Then

$$\frac{E_4}{VE_4}=\frac{1+2^8 f}{1+2^4 f},\qquad \frac{E_6}{VE_6}=\frac{1-2\cdot 3^5 g-3^9 g^2}{1+2\cdot 3^2 g-3^3 g^2}.$$

4. Families of eigenforms

Let $h: D^\times\to\mathscr{E}$ denote an analytic family of overconvergent modular eigenforms of finite slope such that $\pi\circ h$ extends to D, and suppose that $(\pi\circ h)(0)=\kappa$, where κ is of the form $\kappa = \chi^k \cdot \psi$ with $k \in \mathbb{Z}$ and a finite order character ψ of conductor dividing N. We assume that the image of h lies in the cuspidal locus since the Eisenstein locus is finite and hence proper; see [Buzzard and Calegari 2006, Theorem 8.2]. Any weight in $\mathcal{W}(\mathbb{C}_p)$ sufficiently close to κ lies in the set $\kappa \cdot \mathcal{B}^*$, where $\mathcal{B}^*$ is defined as

$$\begin{aligned} &\{\eta(s) : a \mapsto \langle\langle a\rangle\rangle^{4s} \mid s \in \mathbb{C}_p,\ v(s) > -3\} && \text{if } p = 2,\\ &\{\eta(s) : a \mapsto \langle\langle a\rangle\rangle^{6s} \mid s \in \mathbb{C}_p,\ v(s) > -\tfrac{3}{2}\} && \text{if } p = 3,\\ &\Big\{\eta(s) : a \mapsto \langle\langle a\rangle\rangle^{s(p-1)} \,\Big|\, s \in \mathbb{C}_p,\ v(s) > -1 + \frac{1}{p-1}\Big\} && \text{if } p \geq 5. \end{aligned}$$

Our $\mathcal{B}^*$ is normalized slightly differently from that of [Coleman and Mazur 1998, p. 28], as we have included extra factors in the exponent, merely to avoid potentially troublesome notational issues later on. After shrinking D, if necessary, we may assume that $(\pi \circ h)(D^\times) \subset \kappa \cdot \mathcal{B}^*$. Given $t \in D$, we may consider $h(t)$ to be a normalized eigenform in $M(\mathbb{C}_p, N, \kappa \cdot \eta(s(t)))$, for some $\eta(s(t)) \in \mathcal{B}^*(\mathbb{C}_p)$ and analytic function $s(t)$. By assumption, $Uh(t) = \lambda(t)h(t)$ for some analytic function $\lambda(t)$ which does not vanish on $D^\times$. By considering q-expansions, we deduce that $h(0)$ exists as a p-adic modular form in the sense of Katz [1973] — for a more detailed proof, see [Buzzard and Calegari 2006, p. 229]. If $p \geq 5$, let A be as in Section 2, otherwise let $A = E_6$ if $p = 3$ or $A = E_4$ if $p = 2$. The modular form A has weight $\chi^{p-1} = \eta(1)$ if $p \geq 5$, and weights $\chi^6 = \eta(1)$ and $\chi^4 = \eta(1)$ if $p = 3$ and 2 respectively. Thus (shrinking D again if necessary), we may construct a map

$$g : D^\times \to M(\mathbb{C}_p, N, \kappa)$$

via the formula $g(t) = h(t)/A^{s(t)}$. This map is well defined as an easy consequence of Corollary B4.2.5 of [Coleman 1997], namely that E_s/A^s is overconvergent of weight zero where E_s is the Eisenstein series of weight $\eta(s)$.

Lemma 4.1. *Suppose that $v(r) < 1/(p+1)$. After shrinking D, if necessary, the image of g lands in $M(\mathbb{C}_p, N, \kappa, r^p)$.*

Proof. By construction, $g(t)$ lies in $M(\mathbb{C}_p, N, \kappa, \mu)$ for some μ with $v(\mu) > 0$. Since κ is of the form $\chi^k \cdot \psi$, we may therefore realize $g(t)$ as a section of $H^0(X_0(p, \mu), \omega^{\otimes k})$. Here we use the fact that ψ has conductor coprime to p. Consider the operator $U_t = U(A/VA)^{s(t)}$, where U is the usual operator on overconvergent modular forms [Coleman 1996; 1997]. If $s(t)$ is sufficiently small, then by Corollary 3.2, the factor $(A/VA)^{s(t)}$ lies in $M(\mathbb{C}_p, N, 1, r)$. On the other hand,

$$U_t(g(t)) = U(h(t)/VA^{s(t)}) = (\lambda(t)h(t)/A^{s(t)}) = \lambda(t)g(t).$$

If $g(t) \in M(\mathbb{C}_p, N, \kappa, \mu)$, then $(A/VA)^{s(t)}g(t) \in M(\mathbb{C}_p, N, \kappa, \max\{r, \mu\})$, and hence it follows that $U_t g(t)$ lies in $M(\mathbb{C}_p, N, \kappa, \max\{r^p, \mu^p\})$. Thus, since $\lambda(t) \neq 0$

for $t \in D^{\times}$, we deduce from the equality $g(t) = \lambda(t)^{-1}U_t(g(t))$ that $g(t)$ lies in $M(\mathbb{C}_p, N, \kappa, \max\{\mu^p, r^p\})$. By induction, we deduce that $g(t) \in M(\mathbb{C}_p, N, \kappa, r^p)$. □

As remarked above, the q-expansion $g(0) = h(0)$ is a Katz p-adic modular form of weight κ, and moreover, by assumption, lies in the kernel of U. The argument now proceeds exactly as in Section 8 of [Buzzard and Calegari 2006]. Namely, as in the proof of Theorem 8.2 of loc. cit., we deduce that $h(0)$ is lies in $M(\mathbb{C}_p, N, \chi^k \cdot \psi, r^p)$ for any r satisfying the conditions of Lemma 4.1, namely, $v(r) < 1/(p+1)$. In particular, we may choose an r such that $h(0) \in M(\mathbb{C}_p, N, \chi^k \cdot \psi, r^p)$ and $v(r^p) > 1/(p+1)$. Yet this is in direct contradiction to Lemma 6.13 of [Buzzard and Calegari 2006] (note Remark 6.14), which says that modular forms in the kernel of U cannot converge beyond $1/(p+1)$. This completes the proof.

Acknowledgements

It is a pleasure to thank Kevin Buzzard for pointing out a simplification in a previous argument. I also thank both referees for helpful remarks. The debt this paper owes to [Buzzard and Calegari 2006] is clear. I would also like to thank Matthew Emerton, Toby Gee, and Mark Kisin for useful conversations.

References

[Ash and Stevens $\geq$ 2008] A. Ash and G. Stevens, "p-adic deformations of cohomology on GL(n): the non-ordinary case", in preparation.

[Buzzard 2008] K. Buzzard, "Eigenvarieties", in *Proceedings of the LMS Symposium on L-functions and Galois representations* (Durham, 2004), 2008. To appear.

[Buzzard and Calegari 2006] K. Buzzard and F. Calegari, "The 2-adic eigencurve is proper", *Doc. Math.* Extra Vol. (2006), 211–232. MR 2007j:11055 Zbl 05165898

[Chenevier 2004] G. Chenevier, "Familles p-adiques de formes automorphes pour GL$_n$", *J. Reine Angew. Math.* **570** (2004), 143–217. MR 2006b:11046 Zbl 1093.11036

[Coleman 1996] R. F. Coleman, "Classical and overconvergent modular forms", *Invent. Math.* **124**:1-3 (1996), 215–241. MR 97d:11090a Zbl 0851.11030

[Coleman 1997] R. F. Coleman, "p-adic Banach spaces and families of modular forms", *Invent. Math.* **127**:3 (1997), 417–479. MR 98b:11047 Zbl 0918.11026

[Coleman and Mazur 1998] R. Coleman and B. Mazur, "The eigencurve", pp. 1–113 in *Galois representations in arithmetic algebraic geometry* (Durham, 1996), London Math. Soc. Lecture Note Ser. **254**, Cambridge Univ. Press, Cambridge, 1998. MR 2000m:11039 Zbl 0932.11030

[Coleman and Stein 2004] R. F. Coleman and W. A. Stein, "Approximation of eigenforms of infinite slope by eigenforms of finite slope", pp. 437–449 in *Geometric aspects of Dwork theory*, vol. 1, de Gruyter, Berlin, 2004. MR 2005h:11092 Zbl 02128075

[Emerton 2006] M. Emerton, "On the interpolation of systems of eigenvalues attached to automorphic Hecke eigenforms", *Invent. Math.* **164**:1 (2006), 1–84. MR 2007k:22018 Zbl 1090.22008

[Katz 1973] N. M. Katz, “p-adic properties of modular schemes and modular forms”, pp. 69–190 in *Modular functions of one variable, III*, Lecture Notes in Mathematics **350**, Springer, Berlin, 1973. MR 56 #5434 Zbl 0271.10033

[Wan 1998] D. Wan, “Dimension variation of classical and p-adic modular forms”, *Invent. Math.* **133**:2 (1998), 449–463. MR 99d:11039 Zbl 0907.11016

Communicated by Brian D. Conrad
Received 2007-08-17 Revised 2007-11-20 Accepted 2007-12-18

fcale@math.northwestern.edu *Department of Mathematics, Northwestern University,*
2033 Sheridan Road, Evanston, IL 60208
http://www.math.northwestern.edu/~fcale/

A finiteness property of torsion points

Matthew Baker, Su-ion Ih and Robert Rumely

Let k be a number field, and let G be either the multiplicative group $\mathbb{G}_m/k$ or an elliptic curve E/k. Let S be a finite set of places of k containing the archimedean places. We prove that if $\alpha \in G(\bar{k})$ is nontorsion, then there are only finitely many torsion points $\xi \in G(\bar{k})_{\text{tors}}$ that are S-integral with respect to α. We also formulate conjectural generalizations for dynamical systems and for abelian varieties.

Introduction

Let k be a number field, with ring of integers $\mathbb{O}_k$ and algebraic closure $\bar{k}$. In this paper we prove finiteness theorems for torsion points that are integral with respect to a given nontorsion point, for the multiplicative group $\mathbb{G}_m/k$ and for elliptic curves E/k. We then attempt to place these results in a conceptual framework, and conjecture generalizations to dynamical systems and abelian varieties.

Let S be a finite set of places of k containing the archimedean places. Given $\alpha, \beta \in \mathbb{P}^1(\bar{k})$, let $\text{cl}(\alpha), \text{cl}(\beta)$ be their Zariski closures in $\mathbb{P}^1_{\mathbb{O}_k}$. By definition, β is S-integral relative to α if $\text{cl}(\beta)$ does not meet $\text{cl}(\alpha)$ outside S. Thus, β is S-integral relative to α if and only if for each place v of k not in S, and each pair of k-embeddings $\sigma : k(\beta) \hookrightarrow \bar{k}_v$, $\tau : k(\alpha) \hookrightarrow \bar{k}_v$, we have $\|\sigma(\beta), \tau(\alpha)\|_v = 1$ under the spherical metric on $\mathbb{P}^1(\bar{k}_v)$. Equivalently, for all σ, τ,

$$\begin{cases} |\sigma(\beta) - \tau(\alpha)|_v \geq 1 & \text{if } |\tau(\alpha)|_v \leq 1, \\ |\sigma(\beta)|_v \leq 1 & \text{if } |\tau(\alpha)|_v > 1. \end{cases}$$

Theorem 0.1. *Let k be a number field, and let S be a finite set of places of k containing all the archimedean places. Fix $\alpha \in \mathbb{P}^1(\bar{k})$ with Weil height $h(\alpha) > 0$; that is, identifying $\mathbb{P}^1(\bar{k})$ with $\bar{k} \cup \{\infty\}$, α is not* 0 *or* ∞ *or a root of unity. Then there are only finitely many roots of unity in $\bar{k}$ that are S-integral with respect to α.*

Similarly, let E/k be an elliptic curve, and let $\mathscr{E}/\text{Spec}(\mathbb{O}_k)$ be a model of E.

MSC2000: primary 11G05; secondary 11J71, 11J86, 37F10, 11G50.
Keywords: elliptic curve, equidistribution, canonical height, torsion point, integral point.
Work supported in part by NSF grant DMS-0300784.

Theorem 0.2. *Let k be a number field, and let S be a finite set of places of k containing all the archimedean places. If $\alpha \in E(\bar{k})$ is nontorsion (has canonical height $\hat{h}(\alpha) > 0$), there are only finitely many torsion points $\xi \in E(\bar{k})_{\mathrm{tors}}$ which are S-integral with respect to α.*

By S-integrality we mean that the Zariski closures of ξ and α in $\mathscr{E}/\mathrm{Spec}(\mathbb{O}_k)$ do not meet outside fibres above S. Since any two models are isomorphic outside a finite set of places, it follows from the theorem that the finiteness property is independent of the choice of the set S and the model $\mathscr{E}$.

The main ingredients of the proofs of Theorems 0.1 and 0.2 are linear forms in logarithms (Baker's theorem for $\mathbb{G}_m$, and David/Hirata-Kohno's theorem for elliptic curves), properties of local height functions, and a strong form of equidistribution for torsion points at all places v. In outline, both theorems are proved as follows. By base change, one reduces to the case where α is rational over k. Given a place v of k, let $\bar{k}_v$ be the algebraic closure of the completion k_v, and let λ_v be the normalized canonical local height occurring in the decomposition of the global height. On the one hand, well known properties of local and global heights can be used to show that since α is nontorsion, for any torsion point ξ_n one has

$$0 < \hat{h}(\alpha) = \frac{1}{[k(\xi_n):k]} \sum_{v} \sum_{\sigma : k(\xi_n)/k \hookrightarrow \bar{k}_v} \lambda_v(\alpha - \sigma(\xi_n)), \tag{1}$$

where $\sigma : k(\xi_n)/k \hookrightarrow \bar{k}_v$ means σ is an embedding of $k(\xi_n)$ in $\bar{k}_v$ fixing k. On the other hand, if $\{\xi_n\}$ is a sequence of distinct torsion points which are S-integral with respect to α, then for each v, by equidistribution and the normalization of λ_v,

$$\lim_{n\to\infty} \frac{1}{[k(\xi_n):k]} \sum_{\sigma : k(\xi_n)/k \hookrightarrow \bar{k}_v} \lambda_v(\alpha - \sigma(\xi_n)) = 0. \tag{2}$$

By the integrality hypothesis, the outer sum in (1) can be restricted to $v \in S$, allowing the limit and the sum to be interchanged. This gives $\hat{h}(\alpha) = 0$, contradicting the assumption that α is nontorsion.

Examples show that the conclusion is false if α is a torsion point, and that it can fail if $\{\xi_n\}$ is merely a sequence of small points (that is, a sequence of points with $\hat{h}(\xi_n) \to 0$). In particular, our results cannot be strengthened to theorems of Bogomolov type.

The paper is divided into three sections. In Section 1, we prove Theorem 0.1 for $\mathbb{G}_m$; in Section 2, we prove Theorem 0.2 for elliptic curves. In Section 3, we attempt to provide perspective on these results, comparing them with other arithmetic finiteness theorems, and formulating conjectural generalizations.

Throughout the paper, we use the following notation. For each place v of k, let k_v be the completion of k at v and let $|x|_v$ be the normalized absolute value which coincides with the modulus of additive Haar measure on k_v. If v is archimedean and $k_v \cong \mathbb{R}$, then $|x|_v = |x|$, while if $k_v \cong \mathbb{C}$ then $|x|_v = |x|^2$. If v is nonarchimedean and lies over the rational prime p, then $|p|_v = p^{-[k_v:\mathbb{Q}_p]}$. For $0 \neq \alpha \in k$, the product formula reads

$$\prod_v |\alpha|_v = 1.$$

If $\bar{k}_v$ is an algebraic closure of k_v, there is a unique extension of $|x|_v$ to $\bar{k}_v$, also denoted $|x|_v$. Given a finite extension L/k, for each place w of L we have the normalized absolute value $|x|_w$ on L_w. If we embed L_w in $\bar{k}_v$, then $|x|_w = |x|_v^{[L_w:k_v]}$ for each $x \in L_w$. Write $\log x$ for the natural logarithm of x. Given $\beta \in L$ and a place v of k, as σ ranges over all embeddings of L into $\bar{k}_v$ fixing k we have

$$\sum_{\sigma : L/k \hookrightarrow \bar{k}_v} \log|\sigma(\beta)|_v = \sum_{w|v} \log|\beta|_w. \tag{3}$$

The absolute Weil height of $\alpha \in k$ (also called the naive height) is defined to be

$$h(\alpha) = \frac{1}{[k:\mathbb{Q}]} \sum_v \max(0, \log|\alpha|_v),$$

with the convention that $\log 0 = -\infty$. It is well known that for $\alpha \in \overline{\mathbb{Q}}$, $h(\alpha)$ is independent of the field k containing $\mathbb{Q}(\alpha)$ used to compute it, so h extends to a function on $\overline{\mathbb{Q}}$. Furthermore $h(\alpha) \geq 0$, with $h(\alpha) = 0$ if and only if $\alpha = 0$ or α is a root of unity.

1. The finiteness theorem for $\mathbb{G}_m$

Limitations. Before giving the proof of Theorem 0.1, we note some examples that limit possible strengthenings of the theorem.

(A) The hypothesis $h(\alpha) > 0$ is necessary. To see this, take $k = \mathbb{Q}$. If $\alpha = 0$ or $\alpha = \infty$, then each root of unity ζ_n is integral with respect to α at all finite places. If $\alpha = 1$, then each root of unity whose order is divisible by at least two distinct primes is integral with respect to α at all finite places. If $\alpha = \zeta_N$ is a primitive N-th root of unity with $N > 1$, let ζ_m be a primitive m-th root of unity with $(m, N) = 1$ and $m > 1$. Then $\zeta_N^{-1}\zeta_m$ is a primitive mN-th root of unity whose order is divisible by at least two distinct primes, so $1 - \zeta_N^{-1}\zeta_m$ is a unit in $\overline{\mathbb{Z}}$, the ring of all algebraic integers, and $\zeta_N - \zeta_m$ is also a unit. This holds for all conjugates of ζ_N and ζ_m. Hence ζ_m is integral with respect to α at all finite places.

(B) When $h(\alpha) > 0$, one can ask if the theorem could be strengthened to a result of Bogomolov type: is there a number $B = B(\alpha) > 0$ such that there are only finitely many points $\beta \in \bar{k}$ with $h(\beta) < B$ which are S-integral with respect to α? That is, could finiteness for roots of unity be strengthened to finiteness for small points?

The following example[1] shows this is not possible (see [Autissier 2006] for similar examples). Take $k = \mathbb{Q}$, $\alpha = 2$, and $S = \{\infty\}$. For each n, let β_n be a root of the polynomial

$$f_n(x) \;=\; x^{2^n-1}(x-2)-1\,.$$

Here $f_n(x+1)$ is Eisenstein with respect to the prime $p=2$, so $f_n(x)$ is irreducible over $\mathbb{Q}$. Note that each β_n is a unit. By Rouché's theorem, β_n has one conjugate very near 2 and the rest of its conjugates very close to the unit circle; this can be used to show that $\lim_{n\to\infty} h(\beta_n) = 0$. Finally, $\beta_n - 2$ is also a unit, so β_n is integral with respect to 2 at all finite places.

Proof of Theorem 0.1. By replacing k with $k(\alpha)$, and S with the set of places $S_{k(\alpha)}$ lying over S, we are reduced to proving the theorem when $\alpha \in k$. Indeed, if ζ is a root of unity which is S-integral with respect to α over k, then each k-conjugate of ζ is $S_{k(\alpha)}$-integral with respect to α over $k(\alpha)$.

Suppose $\alpha \in k$, and that there are infinitely many distinct roots of unity ζ_n which are S-integral with respect to α. For each n, we will evaluate the sum

$$A_n \;=\; \frac{1}{[k(\zeta_n):\mathbb{Q}]}\sum_{v \text{ of } k}\;\sum_{\sigma:\,k(\zeta_n)/k\hookrightarrow \bar{k}_v} \log(|\sigma(\zeta_n)-\alpha|_v) \tag{4}$$

in two different ways. On the one hand, we will see that each $A_n = 0$. On the other hand, by applying the integrality hypothesis, A. Baker's theorem on linear forms in logarithms, and a strong form of equidistribution for roots of unity, we will show that $\lim_{n\to\infty} A_n = h(\alpha) > 0$. This contradiction will give the desired result. The details are as follows.

First, using (3), formula (4) can be rewritten as

$$A_n \;=\; \frac{1}{[k(\zeta_n):\mathbb{Q}]}\sum_{w \text{ of } k(\zeta_n)} \log|\zeta_n-\alpha|_w\,.$$

Since α is not a root of unity, we have $\zeta_n - \alpha \neq 0$; hence the product formula gives $A_n = 0$.

Next, take $v \notin S$. If $|\alpha|_v > 1$, we have $|\sigma(\zeta_n)-\alpha|_v = |\alpha|_v$ for each $\sigma : k(\zeta_n)/k \hookrightarrow \bar{k}_v$, by the ultrametric inequality. On the other hand, if $|\alpha|_v \le 1$, the integrality hypothesis gives $|\sigma(\zeta_n)-\alpha|_v = 1$. It follows that for each $v \notin S$

$$\frac{1}{[k(\zeta_n):\mathbb{Q}]}\sum_{\sigma:\,k(\zeta_n)/k\hookrightarrow \bar{k}_v} \log(|\sigma(\zeta_n)-\alpha|_v) \;=\; \frac{1}{[k:\mathbb{Q}]}\max(0,\log|\alpha|_v), \tag{5}$$

[1] The authors thank Pascal Autissier for correcting an error in an earlier version of this example.

so

$$A_n = \sum_{v\in S} \frac{1}{[k(\zeta_n):\mathbb{Q}]} \sum_{\sigma : k(\zeta_n)/k \hookrightarrow \bar{k}_v} \log(|\sigma(\zeta_n)-\alpha|_v) + \frac{1}{[k:\mathbb{Q}]} \sum_{v\notin S} \max(0, \log|\alpha|_v).$$

Now let $n \to \infty$. Since S is finite, we can interchange the limit and the sum over $v \in S$, obtaining

$$0 = \sum_{v\in S} \left(\lim_{n\to\infty} \frac{1}{[k(\zeta_n):\mathbb{Q}]} \sum_{\sigma : k(\zeta_n)/k \hookrightarrow \bar{k}_v} \log(|\sigma(\zeta_n)-\alpha|_v) \right) + \frac{1}{[k:\mathbb{Q}]} \sum_{v\notin S} \max(0, \log|\alpha|_v).$$

We will now show that for each $v \in S$,

$$\lim_{n\to\infty} \frac{1}{[k(\zeta_n):\mathbb{Q}]} \sum_{\sigma : k(\zeta_n)/k \hookrightarrow \bar{k}_v} \log(|\sigma(\zeta_n)-\alpha|_v) = \frac{1}{[k:\mathbb{Q}]} \max(0, \log|\alpha|_v). \quad (6)$$

Inserting this in the previous equation gives $h(\alpha) = 0$, a contradiction.

For each nonarchimedean $v \in S$, (6) is trivial if $|\alpha|_v > 1$ or $|\alpha|_v < 1$. In the first case $|\sigma(\zeta_n)-\alpha|_v = |\alpha|_v$ for all n and all σ, and in the second case $|\sigma(\zeta_n)-\alpha|_v = 1$ for all n and all σ. Hence we can assume that $|\alpha|_v = 1$. We can then apply the following result, part (i) of which is a special case of the Tate–Voloch conjecture for semiabelian varieties proved by Scanlon [1999].

Lemma 1.1. *Let v be nonarchimedean, and suppose $|\alpha|_v = 1$. Then*

(i) *there is a bound $M(\alpha) > 0$ such that $|\zeta - \alpha|_v \geq M(\alpha)$ for all roots of unity $\zeta \in \bar{k}_v$ and*

(ii) *for each $0 < r < 1$, there are only finitely many roots of unity $\zeta \in \bar{k}_v$ with $|\zeta - \alpha|_v < r$.*

Proof. Since α is not a root of unity, (i) follows immediately from (ii). For (ii), note that if ζ and ζ' are roots of unity with $|\zeta - \alpha|_v < r$ and $|\zeta' - \alpha|_v < r$, then $|\zeta - \zeta'|_v < r$ and so $\zeta'' = \zeta^{-1}\zeta'$ is a root of unity with $|1 - \zeta''|_v < r$. There are only finitely many such ζ''. Indeed, if p is the rational prime under v, the only roots of unity $\xi \in \bar{k}_v$ with $|1-\xi|_v < 1$ are those with order p^n for some n. If ξ is a primitive p^n-th root of unity, then $|1-\xi|_v = p^{-[k_v:\mathbb{Q}_p]/p^{n-1}(p-1)}$ so $1 > r > |1-\xi|_v$ for only finitely many n. □

Assuming v is nonarchimedean and $|\alpha|_v = 1$, let $M(\alpha)$ be as in Lemma 1.1. Fix $0 < r < 1$, and let $N(r)$ be the number of roots of unity in $\bar{k}_v$ with $|\zeta - \alpha|_v < r$.

For each ζ_n and each $\sigma : k(\zeta_n)/k \to \bar{k}_v$, we have $|\sigma(\zeta_n) - \alpha|_v \le 1$, so

$$\begin{aligned} 0 &\ge \lim_{n\to\infty} \frac{1}{[k(\zeta_n):\mathbb{Q}]} \sum_{\sigma : k(\zeta_n)/k \hookrightarrow \bar{k}_v} \log(|\sigma(\zeta_n) - \alpha|_v) \\ &\ge \lim_{n\to\infty} \frac{1}{[k(\zeta_n):\mathbb{Q}]} \big(([k(\zeta_n):k] - N(r)) \log r + N(r) \cdot \log M(\alpha)\big) = \frac{1}{[k:\mathbb{Q}]} \log r. \end{aligned}$$

Since $r < 1$ is arbitrary, the limit in (6) is 0, verifying (6) in this case.

Now suppose v is archimedean. To simplify notation, view k as a subfield of $\mathbb{C}$ and identify $\bar{k}_v$ with $\mathbb{C}$. (Thus, the way k is embedded depends on the choice of v.)

By Jensen's formula [Conway 1973, p. 280] applied to $f(z) = z - \alpha$,

$$\frac{1}{2\pi} \int_0^{2\pi} \log |e^{i\theta} - \alpha| \, d\theta \; = \; \max(0, \log |\alpha|). \tag{7}$$

Here $|x|$ can be replaced by $|x|_v$, since $|x|_v$ is either $|x|$ or $|x|^2$.

The $\mathrm{Gal}(\bar{k}/k)$-conjugates of roots of unity equidistribute in the unit circle. We will give a direct proof of this below, but we note that it also follows from Bilu's theorem [1997] and restriction of scalars, or from the equidistribution theorem for polynomial dynamical systems given in [Baker and Hsia 2005]. Those theorems show that if μ_n is the discrete measure

$$\mu_n \; = \; \frac{1}{[k(\zeta_n):k]} \sum_{\sigma : k(\zeta_n)/k \hookrightarrow \mathbb{C}} \delta_{\sigma(\zeta_n)}(x),$$

where $\delta_P(x)$ is the Dirac measure with mass 1 at P, then the μ_n converge weakly to the Haar measure $\mu = (1/2\pi) d\theta$ on the unit circle.

If $|\alpha|_v > 1$ or $|\alpha|_v < 1$ then $\log |z - \alpha|_v$ is continuous on the unit circle. In these cases, (6) follows from (7) and weak convergence. If $|\alpha|_v = 1$ then $\log |z - \alpha|_v$ is not continuous on $|z| = 1$ and weak convergence is not enough to give $\int_{|z|=1} \log |z - \alpha|_v \, d\mu_n(z) \to 0$: there could be a problem if some conjugate of ζ_n were extremely close to α,or if too many conjugates of ζ_n clustered near α.

The first problem is solved by A. Baker's theorem on lower bounds for linear forms in logarithms [Baker 1975, Theorem 3.1, p. 22]. We are assuming that $|\alpha|_v = 1$, and α is not a root of unity. Fix a branch of log with $\log z = \log |z| + i\theta$, for $-\pi < \theta \le \pi$, and write $\log \alpha = i\theta_0$. For another branch, $\log 1 = 2\pi i$. The following is a special case of Baker's theorem. (In his statement of the theorem, Baker uses an exponential height having bounded ratio with $H(\beta) = e^{h(\beta)}$.)

Proposition 1.2 (A. Baker). *There is a constant $C = C(\alpha) > 0$ such that for each $\beta = a/N \in \mathbb{Q}$, with $a, N \in \mathbb{Z}$ coprime,*

$$|\, i\theta_0 - \beta \cdot 2\pi i \,| \; \ge \; e^{-C \cdot \max(1, h(\beta))},$$

where $h(\beta) = \log \max(|a|, |N|)$ is the Weil height of β.

The second problem is settled by a strong form of equidistribution for roots of unity, proved starting on page 226. It says that for any $0 < \gamma < 1$, the conjugates of the ζ_n are asymptotically equidistributed in arcs of length $[k(\zeta_n) : k]^{-\gamma}$. Note that weak convergence is equivalent to equidistribution in arcs of fixed length.

Proposition 1.3 (Strong equidistribution). *Let $k \subset \mathbb{C}$ be a number field. Then the $\mathrm{Gal}(\bar{k}/k)$-conjugates of the roots of unity in $\bar{k}$ (viewed as embedded in $\mathbb{C}$) are strongly equidistributed in the unit circle, in the following sense.*

Given an arc I in the unit circle, write $\mu(I) = \frac{1}{2\pi}\mathrm{length}(I)$ for its normalized Haar measure. If $\zeta \in \bar{k}$ is a root of unity, put

$$N(\zeta, I) = \#\{\sigma(\zeta) \in I : \sigma \in \mathrm{Gal}(\bar{k}/k)\}.$$

Fix $0 < \gamma < 1$. Then for all roots of unity ζ and all I,

$$\frac{N(\zeta, I)}{[k(\zeta) : k]} = \mu(I) + O_{k,\gamma}([k(\zeta) : k]^{-\gamma}). \tag{8}$$

Assuming Proposition 1.3, we will now complete the proof of Theorem 0.1 by showing that (6) holds for archimedean v such that $|\alpha|_v = 1$.

Let $\mu = (1/2\pi)\, d\theta$ be the normalized Haar measure on the unit circle, and for each n, put

$$\mu_n = \frac{1}{[k(\zeta_n) : k]} \sum_{\sigma : k(\zeta_n)/k \to \mathbb{C}} \delta_{\sigma(\zeta_n)}(x).$$

Then the μ_n are supported on the unit circle and converge weakly to μ as $n \to \infty$. We must show that

$$\int_{|z|=1} \log|z - \alpha|\, d\mu_n(z) = \frac{1}{[k(\zeta_n) : k]} \sum_{\sigma} \log(|\sigma(\zeta_n) - \alpha|) \to 0.$$

The idea is to split the integrand $\log|z - \alpha|$ into two parts: a continuous "background" function that can be handled by weak convergence, and a function with a logarithmic pole at α supported in a small neighborhood of α. The terms nearest α can then be dealt with using Baker's theorem, while the other terms can be treated by strong equidistribution. Define

$$\mathrm{larg}_{\alpha,\varepsilon}(z) = \min(0, \log(|\theta - \theta_0|/\varepsilon)),$$

taking $\mathrm{larg}_{\alpha,\varepsilon}(\theta_0) = -\infty$. Then there is a continuous function $g_{\alpha,\varepsilon}(z)$ on $|z| = 1$ for which $\log|z - \alpha| = \mathrm{larg}_{\alpha,\varepsilon}(z) + g_{\alpha,\varepsilon}(z)$.

Fix $0 < \epsilon < 1$. We will show that for all sufficiently large n,

$$\left|\int_{|z|=1} \log|z - \alpha|\, d\mu_n(z)\right| < 6\epsilon. \tag{9}$$

Note that $\int_0^\varepsilon \log(t/\varepsilon)\,dt = -\varepsilon$. For the remainder of the proof, we restrict to $|z| = 1$; write $\alpha = e^{i\theta_0}$ where $-\pi < \theta_0 \le \pi$, and write $z = e^{i\theta}$ where $\theta_0 - \pi < \theta \le \theta_0 + \pi$. Recalling that $\int_{|z|=1} \log|z - \alpha|\,d\mu(z) = 0$, we have

$$\int_{|z|=1} g_{\alpha,\varepsilon}(z)\,d\mu(z) \;=\; -\int_{|z|=1} \operatorname{larg}_{\alpha,\varepsilon}(z)\,d\mu(z) \;=\; -2\int_0^\varepsilon \log(\theta/\varepsilon)\,\frac{d\theta}{2\pi} \;=\; \frac{\varepsilon}{\pi}\,.$$

By weak convergence, it follows that for all sufficiently large n,

$$\Big|\int_{|z|=1} g_{\alpha,\varepsilon}(z)\,d\mu_n(z)\Big| \;<\; \varepsilon\,. \tag{10}$$

To obtain (9), it suffices to show that for all sufficiently large n,

$$\Big|\int_{|z|=1} \operatorname{larg}_{\alpha,\varepsilon}(z)\,d\mu_n(z)\Big| \;<\; 5\varepsilon\,.$$

For each interval $[c, d]$ let $I_\alpha([c, d])$ be the arc $\{\alpha e^{2\pi i t} : t \in [c, d]\}$. Noting that $\operatorname{larg}_{\alpha,\varepsilon}(z)$ is supported on $I_\alpha([-\varepsilon, \varepsilon])$, put $D = D_n = \lceil [k(\zeta_n) : k]^{1/2} \rceil$ and divide $I_\alpha([-\varepsilon, \varepsilon])$ into $2D$ equal subarcs. Taking $\gamma = 2/3$ in Proposition 1.3, it follows that if n is sufficiently large, each such subarc contains at most $2\varepsilon[k(\zeta_n) : k]^{1/2}$ conjugates of ζ_n.

First consider the union of the two central subarcs, $I_\alpha([-\varepsilon/D, \varepsilon/D])$. Let N be the order of ζ_n. Let $\sigma_0(\zeta_n) = e^{2\pi i a/N}$ be the conjugate of ζ_n closest to $\alpha = e^{i\theta_0}$. We can assume that $|a/N| \le 1$, which implies that $h(a/N) = \max(\log|a|, \log N) = \log N$. By Baker's theorem,

$$|\,2\pi(a/N) - \theta_0| \;>\; e^{-C\max(1,\log N)}\,.$$

Hence if n is sufficiently large,

$$\operatorname{larg}_{\alpha,\varepsilon}(\sigma_0(\zeta_n)) \;>\; -C\log N - \log\varepsilon \;\ge\; -C\log N\,.$$

Since there are at most $4\varepsilon[k(\zeta_n) : k]^{1/2}$ conjugates of ζ_n in $I_\alpha([-\varepsilon/D, \varepsilon/D])$,

$$0 \ge \int_{I_\alpha([-\varepsilon/D,\varepsilon/D])} \operatorname{larg}_{\alpha,\varepsilon}(|z-\alpha|)\,d\mu_n(z) \;>\; -4\frac{C\log N}{[k(\zeta_n) : k]^{1/2}}\varepsilon\,.$$

Note that $[k(\zeta_n) : k] \ge [\mathbb{Q}(\zeta_n) : \mathbb{Q}]/[k : \mathbb{Q}] = \varphi(N)/[k : \mathbb{Q}]$. For all large N, $\varphi(N) \ge N^{1/2}$, so there is a constant B such that $[k(\zeta_n) : k]^{1/2} \ge BN^{1/4}$. Thus for all sufficiently large n,

$$\Big|\int_{I_\alpha([-\varepsilon/D,\varepsilon/D])} \log|z-\alpha|\,d\mu_n(z)\Big| \;<\; \varepsilon\,. \tag{11}$$

Finally, consider the remaining subarcs. For $\ell = 1, \dots, D-1$, if

$$z \in I_\alpha\big([\ell\varepsilon/D, (\ell+1)\varepsilon/D]\big) \quad\text{or}\quad z \in I_\alpha\big([-(\ell+1)\varepsilon/D, -\ell\varepsilon/D]\big)$$

then $0 \geq \mathrm{larg}_{\alpha,\varepsilon}(z) \geq \log(\ell/D)$. As before, by Proposition 1.3, for sufficiently large n, each subarc contains at most $2\,[k(\zeta_n):k]\,(\varepsilon/D)$ conjugates of ζ_n. It follows that

$$\begin{aligned} 0 \geq & \int_{I_\alpha([-\varepsilon,\varepsilon])\setminus I_\alpha([-\varepsilon/D,\varepsilon/D])} \mathrm{larg}_{\alpha,\varepsilon}(z)\, d\mu_n(z) \\ \geq & \ 2 \cdot \sum_{\ell=1}^{D-1} \log\bigl((\frac{\ell\varepsilon}{D})/\varepsilon\bigr) \cdot \frac{2\varepsilon}{D} \ > \ 4 \int_0^\varepsilon \log(t/\varepsilon)\, dt \ = \ -4\epsilon . \end{aligned} \tag{12}$$

Combining (10), (11), and (12) gives (9), which completes the proof of Theorem 0.1. □

In the course of writing this paper, the authors learned of several results related to Theorem 0.1, some of which imply it in special cases.

A. Bang's theorem [1886] says that if $\alpha \neq \pm 1$ is a nonzero rational number, then for all sufficiently large integers n there is a prime p such that the order of α modulo p is exactly n. This can be rephrased as saying that for all sufficiently large n, there exists a primitive n-th root of unity ζ_n and a nonzero prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\zeta_n]$ such that $\alpha \equiv \zeta_n \pmod{\mathfrak{p}}$. Since all primitive n-th roots are conjugate over $\mathbb{Q}$, this implies Theorem 0.1 in the case $\alpha \in \mathbb{Q}$. A. Schinzel [1974] gave an effective generalization of Bang's theorem to arbitrary number fields; Schinzel's theorem implies Theorem 0.1 for number fields k which are linearly disjoint from the maximal cyclotomic field $\mathbb{Q}^{ab}$, and $\alpha \in k$.

J. Silverman [1995] has shown that if $\alpha \in \overline{\mathbb{Q}}$ is an algebraic unit which is not a root of unity, there are only finitely many m for which $\Phi_m(\alpha)$ is a unit, where $\Phi_m(x)$ is the m-th cyclotomic polynomial. In fact, if $d = [\mathbb{Q}(\alpha):\mathbb{Q}]$ he shows there is an absolute, effectively computable constant C such that the number of such m's is at most

$$C \cdot d^{1+0.7/\log\log d} .$$

In the case when α is a unit, this yields Theorem 0.1 in the same situations as Schinzel's theorem.

G. Everest and T. Ward [1999, Lemma 1.10] show that if $F(x) \in \mathbb{Z}[x]$ is monic and irreducible, with roots $\alpha_1, \ldots, \alpha_d$, and if $F(x)$ is not a constant multiple of x or a cyclotomic polynomial $\Phi_m(x)$, then the quantity $\Delta_n(F) = \prod_{i=1}^d (\alpha_i^n - 1)$ satisfies

$$\lim_{n\to\infty} \frac{1}{n} \log \Delta_n(F) \ = \ m(F) \ > \ 0 , \tag{13}$$

where $m(F) = \deg(F) \cdot h(\alpha_i)$ is the logarithm of the Mahler measure of $F(x)$. When $k = \mathbb{Q}$, and $\alpha = \alpha_1$ is an algebraic integer, the product formula tells us that $\prod_{v \text{ of } \mathbb{Q}} |\Delta_n(F)|_v = 1$, so for all large n there must be some nonarchimedean v and some α_i such that $|\alpha_i^n - 1|_v < 1$, and this in turn means there is some n-th root of unity ζ with $|\alpha_i - \zeta|_v < 1$. This implies there are infinitely many roots of unity which are not integral with respect to some α_i, as also follows from Theorem 0.1. However, the Everest–Ward theorem does not yield Theorem 0.1.

Strong equidistribution for roots of unity. We will now prove Proposition 1.3, the strong equidistribution theorem for roots of unity. At least when $k = \mathbb{Q}$, the result is well known to analytic number theorists, but we are not aware of a reference in the literature.

The proof rests on the following lemma, for which we thank Carl Pomerance. Let $\varphi(N)$ denote Euler's function and let $d(N) = \sum_{m \mid N, m \geq 1} 1$ be the divisor function. We write $\lambda(m)$ for the number of distinct primes dividing m, and use $\theta(x)$ to denote a quantity satisfying $-|x| \leq \theta(x) \leq |x|$.

Lemma 1.4 (Pomerance). *Fix an integer $Q > 1$ and an integer b coprime to Q. Then for each integer $N \geq 1$ divisible by Q and each interval $(C, D] \subset \mathbb{R}$,*

$$\#\big\{a \in (C, D] \cap \mathbb{Z} : (a, N) = 1,\ a \equiv b \pmod{Q}\big\} = \frac{\varphi(N)}{N\varphi(Q)}(D - C) + \theta(d(N)).$$

In particular, the error depends only on N, and not on Q or $(C, D]$.

Proof. Let $p_1, \dots, p_r$ be the distinct primes dividing N but not Q. (If there are no such primes, take $p_1 \cdots p_r = 1$ below.) Take $b_0 \in \mathbb{Z}$ with $b_0 \equiv b \pmod{Q}$, $b_0 \equiv 0 \pmod{p_1 \dots p_r}$. Then

$$\big\{a \in (C, D] \cap \mathbb{Z} :\ a \equiv b \pmod{Q},\ (a, N) = 1\}$$
$$= \{a \in (C, D] \cap \mathbb{Z} :\ Q \,|\, a - b_0,\ p_1,\ \dots,\ p_r \nmid a - b_0\big\}.$$

If m is a positive integer dividing $p_1 \cdots p_r$, put

$$r_{m,b,Q}(C, D) = \#\{a \in (C, D] \cap \mathbb{Z} :\ Qm \,|\, a - b_0\}\,.$$

Then

$$r_{m,b,Q}(C, D) = \left\lfloor \frac{d - b_0}{Qm} \right\rfloor - \left\lfloor \frac{c - b_0}{Qm} \right\rfloor = \frac{1}{Qm}(D - C) + \theta(1)\,.$$

Carrying out inclusion/exclusion relative to the primes $p_1, \dots, p_r$, we have

$$\#\big\{a \in (C, D] \cap \mathbb{Z} : a \equiv b \pmod{Q},\ (a, N) = 1\big\}$$
$$= \sum_{m \,|\, p_1 \cdots p_r} (-1)^{\lambda(m)}\, r_{m,b,Q}(C, D) = \frac{1}{Q}\prod_{i=1}^{r}\Big(1 - \frac{1}{p_i}\Big)(D - C) + \theta(d(p_1 \cdots p_r))$$
$$= \frac{\varphi(N)}{N\varphi(Q)}(D - C) + \theta(d(N))\,. \qquad \square$$

Proof of Proposition 1.3. Let ζ_N denote a primitive N-th root of unity. There are only finitely many subfields of k, so there are only finitely subfields of the form $k_N = k \cap \mathbb{Q}(\zeta_N)$ for some N. For each N there is a minimal Q for which $k_N = k_Q$, and then $\mathbb{Q}(\zeta_Q) \subset \mathbb{Q}(\zeta_N)$ so $Q \mid N$. We will call $Q = Q_N$ the cyclotomic conductor of ζ_N relative to k, and write $T_N = [\mathbb{Q}(\zeta_{Q_N}) : k_N]$.

As $\mathbb{Q}(\zeta_N)$ is galois over $\mathbb{Q}$, it is linearly disjoint from k over k_N, and

$$\mathrm{Gal}(k(\zeta_N)/k) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_N)/k_N).$$

Since $k_N \subset \mathbb{Q}(\zeta_{Q_N}) \subset \mathbb{Q}(\zeta_N)$, the conjugates of ζ_N over k are a union of T_N sets of the form

$$\{e^{2\pi i a/N} : a \equiv b_i (\mathrm{mod}\ Q_N),\ (a, N) = 1\},$$

for certain numbers b_i coprime to Q_N.

Let I be an arc of the unit circle corresponding to an angular interval $(\theta_1, \theta_2]$. Put $(C, D] = (N/2\pi)(\theta_1, \theta_2]$. Then $e^{2\pi i a/N} \in I$ if and only if $a \in (C, D]$. By Lemma 1.4,

$$N(\zeta_N, I) = T_N \cdot \frac{\varphi(N)}{N\varphi(Q_N)} \cdot \frac{N}{2\pi}(\theta_2 - \theta_1) + \theta(T_N \cdot d(N)). \tag{14}$$

Recall that for any $\delta > 0$, if N is sufficiently large then $d(N) \le N^\delta$ and $\varphi(N) \ge N^{1-\delta}$ [Hardy and Wright 1954, Theorem 315, p. 260, and Theorem 327, p. 267]. Take δ such that $0 < 2\delta < 1 - \gamma$. Noting that $[k(\zeta_N) : k] = T_N\, \varphi(N)/\varphi(Q_N)$, and that $\varphi(Q_N)$ is bounded independent of N, (14) gives

$$\frac{N(\zeta_N, I)}{[k(\zeta_N) : k]} = \mu(I) + O_\gamma(N^{-\gamma}). \tag{15}$$

Since $[k(\zeta_N) : k] \le N$, the error bound in (15) holds with N replaced by $[k(\zeta_N) : k]$. Since $[k(\zeta_N) : k]/N^\gamma \to \infty$ as $N \to \infty$, adjoining or removing endpoints of I will not affect the form of the estimate, so (8) applies to all intervals. □

2. The finiteness theorem for elliptic curves

Preliminaries. Let k be a number field, and let E/k be an elliptic curve. We can assume E is defined by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{16}$$

with coefficients in $\mathcal{O}_k$. More precisely, E is the hypersurface in $\mathbb{P}^2/\mathrm{Spec}(k)$ defined by the homogenization of (16). Let Δ be its discriminant.

Given a nonarchimedean place v of k and points $\alpha, \beta \in E(\bar{k})$, we will say that β is integral with respect to α at v if the Zariski closures $\mathrm{cl}(\beta)$ and $\mathrm{cl}(\alpha)$ do not meet in the model $\mathcal{E}_v/\mathrm{Spec}(\mathcal{O}_v)$ defined by the homogenization of (16). Equivalently, if $\|z, w\|_v$ is the restriction of the spherical metric on $\mathbb{P}^2(\bar{k}_v)$ to $E(\bar{k}_v)$ [Rumely 1989, § 1.1], then for each pair of embeddings $\sigma, \tau : \bar{k}/k \hookrightarrow \bar{k}_v$,

$$\|\sigma(\beta), \tau(\alpha)\|_v = 1.$$

If S is a set of places of k containing all the archimedean places, we say β is S-integral with respect to α if β is integral with respect to α at each $v \notin S$.

Write $\hat{h}(\alpha)$ for the canonical height on $E(\bar{k})$, defined by

$$\hat{h}(\alpha) = \frac{1}{2}\lim_{n\to\infty}\frac{1}{4^n}h_{\mathbb{P}^1}(x([2^n]\alpha)) = \frac{1}{3}\lim_{n\to\infty}\frac{1}{4^n}h_{\mathbb{P}^2}([2^n]\alpha),$$

where $h_{\mathbb{P}^1}$ (respectively, $h_{\mathbb{P}^2}$) is the naive height on $\mathbb{P}^1(\bar{k})$ (respectively, $\mathbb{P}^2(\bar{k})$), x is the coordinate function on the Weierstrass model (16), and $[m]$ is multiplication by m on $E(\bar{k})$. (For a discussion of $\hat{h}(\alpha)$ and its properties, see [Silverman 1986, pp. 227–231 and 365–366; or 1994, § VI].) Recall that $\hat{h}(\alpha) \geq 0$, that $\hat{h}([m]\alpha) = m^2\,\hat{h}(\alpha)$ for all m, and that $\hat{h}(\alpha) = 0$ if and only if $\alpha \in E(\bar{k})_{\text{tors}}$. From these facts it follows (as is well known) that if $\xi \in E(\bar{k})_{\text{tors}}$, then

$$\hat{h}(\alpha) = \hat{h}(\alpha - \xi). \tag{17}$$

There is also a decomposition of $\hat{h}(\alpha)$ as a sum of local terms. For each place v of k, let $\lambda_v(P)$ be the local Néron–Tate height function on $E(\bar{k}_v)$. For compatibility with our absolute values we normalize $\lambda_v(P)$ so that $\lambda_v(P) = [k_v : \mathbb{Q}_p]\cdot\lambda_{v,\text{Sil}}(P)$, where $\lambda_{v,\text{Sil}}(P)$ is the local Néron–Tate height defined in Silverman [1986, p. 365]. For each $0 \neq \alpha \in E(k)$ we have

$$\hat{h}(\alpha) = \frac{1}{[k:\mathbb{Q}]}\sum_{v \text{ of } k}\lambda_v(\alpha); \tag{18}$$

see [Silverman 1986, Theorem 18.2, p. 365]. Only finitely many terms in the sum are nonzero.

If L/k is a finite extension, for each place w of L there is a normalized local Néron–Tate height $\lambda_w(P)$ on $E(\bar{L}_w)$. If we fix a k_v-isomorphism $\bar{L}_w \cong \bar{k}_v$, then for all $P \in E(\bar{k}_v)$,

$$\lambda_w(P) = [L_w : k_v]\,\lambda_v(P). \tag{19}$$

It follows that if $\beta \in E(L)$, then for each place v of k, as σ runs over all embeddings of L into $\bar{k}_v$ fixing k,

$$\sum_{\sigma : L/k \hookrightarrow \bar{k}_v}\lambda_v(\sigma(\beta)) = \sum_{w\mid v}\lambda_w(\beta). \tag{20}$$

We will use the following explicit formulas.

Proposition 2.1. *Let k be a number field, and let E/k be an elliptic curve. Let v be a place of k.*

(i) *If v is archimedean, fix an isomorphism $E(\bar{k}_v) \cong \mathbb{C}/\Lambda$ for an appropriate lattice $\Lambda \subset \mathbb{C}$. Let $\sigma(z, \Lambda)$ be the Weierstrass σ-function, let $\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2$ be the discriminant of Λ, and let $\eta : \mathbb{C} \to \mathbb{R}$ be the $\mathbb{R}$-linearized* *period map associated to the Weierstrass ζ-function $\zeta(z,\Lambda)$. If $P \in E(\bar{k}_v)$ corresponds to $z \in \mathbb{C}$, then*

$$\lambda_v(P) = -\log\bigl(|\Delta(\Lambda)^{1/12} e^{-z\eta(z)/2}\sigma(z,\Lambda)|_v\bigr).$$

If $\mu_v(z)$ is the additive Haar measure on $E(\bar{k}_v)$ that gives $E(\bar{k}_v) \cong \mathbb{C}/\Lambda$ total mass 1, *then*

$$\int_{E(\bar{k}_v)} \lambda_v(z)\, d\mu_v(z) = 0.$$

(ii) *If v is nonarchimedean and E has split multiplicative reduction at v* (*so E is k_v-isomorphic to a Tate curve*), *fix a Tate isomorphism $E(\bar{k}_v) \cong \bar{k}_v^\times/q^{\mathbb{Z}}$ where $q \in \bar{k}_v^\times$ satisfies $|q|_v = |1/j(E)|_v < 1$. Let $B_2(x) = x^2 - x + \frac{1}{6}$ be the second Bernoulli polynomial*, *and put*

$$\tilde{\lambda}_v(x) = \frac{1}{2} B_2\Bigl(\frac{x}{\mathrm{ord}_v(q)}\Bigr)(-\log|q|_v).$$

If $P \in E(\bar{k}_v)$ corresponds to $z \in \bar{k}_v^\times$, with z chosen so that $|q|_v < |z|_v \le 1$, then

$$\lambda_v(P) = -\log|1-z|_v + \tilde{\lambda}_v(\mathrm{ord}_v(z)).$$

If μ_v is the Haar measure $dx/\mathrm{ord}_v(q)$, which gives the loop $\mathbb{R}/(\mathbb{Z}\cdot\mathrm{ord}_v(q))$ total mass 1, *then*

$$\int_0^{\mathrm{ord}_v(q)} \tilde{\lambda}_v(x)\, d\mu_v(x) = 0.$$

(iii) *If v is nonarchimedean and E has good reduction at v, let $\|z,w\|_v$ be the spherical metric on $E(\bar{k}_v)$ induced by a projective embedding $E \hookrightarrow \mathbb{P}^2$ corresponding to a minimal Weierstrass model for E at v. Then for each $P \in E_v(\bar{k}_v)$*

$$\lambda_v(P) = -\log\|P, O\|_v.$$

Proof. This is a summary of results in [Silverman 1994, § VI]; see in particular Theorems 1.1 (p. 455), 3.2 (p. 466), 3.3 (p. 468) and 4.1 (p. 470). □

The finiteness theorem. For the convenience of the reader, we recall Theorem 0.2 from the Introduction:

Theorem 0.2. *Let k be a number field*, *and let S be a finite set of places of k containing all the archimedean places. If $\alpha \in E(\bar{k})$ is nontorsion* (*has canonical height $\hat{h}(\alpha) > 0$*), *there are only finitely many torsion points $\xi \in E(\bar{k})_{\mathrm{tors}}$ which are S-integral with respect to α.*

Again there are limitations to possible strengthenings of the theorem:

(A) As noted by Silverman, it is necessary that α be nontorsion. If $\alpha = O$ and S is the set of archimedean places, then by Cassels' generalization of the Lutz–Nagell theorem (Proposition 2.4 below), each torsion point whose order is divisible by at least two distinct primes is S-integral with respect to α.

Similarly, if α is a torsion point of order $N > 1$, let S contain all places of bad reduction for E. Then for each q coprime to N, all q-torsion points are S-integral with respect to α.

(B) When $\hat{h}(\alpha) > 0$, Zhang has pointed out that Theorem 0.2 cannot in general be strengthened to a result of Bogomolov type. A result of E. Ullmo [1995, Theorem 2.4] shows that if E has good reduction at all finite places, then for each $\varepsilon > 0$, there are infinitely many distinct points $\beta \in E(\bar{k})$ with $\hat{h}(\beta) < \varepsilon$ which are S_∞-integral with respect to α, where S_∞ is the set of archimedean places of k.

Proof of Theorem 0.2. The argument is similar to the proof of Theorem 0.1, but requires more machinery. It should be possible to axiomatize some of the arguments and combine both proofs, but for overall clarity of exposition we have chosen not to.

We begin with some reductions.

First, after replacing k by $k(\alpha)$, and S by the set $S_{k(\alpha)}$ of places lying over S, we can assume that $\alpha \in k$.

Second, after replacing k by a finite extension K/k, and replacing S with the set S_K of places of K lying above places in S, we can assume that E has semistable reduction. Thus we can assume without loss of generality that for nonarchimedean v, either E has good reduction, or E is k_v-isomorphic to a Tate curve.

Third, after enlarging S if necessary, we can assume that S contains all v for which $|\Delta|_v \neq 1$. In particular, we can assume that the model of E defined by (16) has good reduction for all $v \notin S$.

We claim that if $\xi_n \in E(\bar{k})_{\text{tors}}$ is any torsion point, then

$$\hat{h}(\alpha) = \frac{1}{[k(\xi_n):\mathbb{Q}]} \sum_v \sum_{\sigma : k(\xi_n)/k \hookrightarrow \bar{k}_v} \lambda_v(\alpha - \sigma(\xi_n)). \tag{21}$$

To see this, let L be the galois closure of $k(\xi_n)$ in $\bar{k}$ over k. By (17) and (18), for each conjugate $\sigma(\xi_n)$,

$$\hat{h}(\alpha) = \hat{h}(\alpha - \sigma(\xi_n)) = \frac{1}{[L:\mathbb{Q}]} \sum_{w \text{ of } L} \lambda_w(\alpha - \sigma(\xi_n)).$$

Averaging over all k-embeddings $\sigma : L \hookrightarrow \bar{k}$, fixing a k-embedding $\bar{k} \hookrightarrow \bar{k}_v$ for each place v of K, using (19), and noting that there are only finitely many nonzero terms in each sum, we have

$$\begin{aligned}\hat{h}(\alpha) &= \frac{1}{[L:k]}\sum_{\sigma:\,L/k\hookrightarrow\bar{k}}\frac{1}{[L:\mathbb{Q}]}\sum_{w\text{ of }L}\lambda_w(\alpha-\sigma(\xi_n))\\ &= \frac{1}{[L:\mathbb{Q}]}\sum_{v\text{ of }k}\sum_{\sigma:\,L/k\hookrightarrow\bar{k}_v}\frac{1}{[L:k]}\sum_{w\,|\,v}[L_w:k_v]\cdot\lambda_v(\alpha-\sigma(\xi_n))\\ &= \frac{1}{[L:\mathbb{Q}]}\sum_{v\text{ of }k}\sum_{\sigma:\,L/k\hookrightarrow\bar{k}_v}\lambda_v(\alpha-\sigma(\xi_n)).\end{aligned}$$

Since each conjugate $\sigma(\xi_n)$ occurs $[L:k(\xi_n)]$ times in the final inner sum, this is equivalent to (21).

Suppose there were an infinite sequence of distinct torsion points $\{\xi_n\}$ which were S-integral with respect to α.

If $v\notin S$, our initial reductions assure that E has good reduction at v. By Proposition 2.1(iii) and the integrality hypothesis, $\lambda_v(\alpha-\sigma(\xi_n))=0$ for each n and σ. It follows that

$$\hat{h}(\alpha) = \sum_{v\in S}\frac{1}{[k(\xi_n):k]}\sum_{\sigma:\,k(\xi_n)/k\hookrightarrow\bar{k}_v}\lambda_v(\alpha-\sigma(\xi_n)). \tag{22}$$

From now through page 237, we will show in a series of cases that for each $v\in S$,

$$\lim_{n\to\infty}\left(\frac{1}{[k(\xi_n):\mathbb{Q}]}\sum_{\sigma:\,k(\xi_n)/k\hookrightarrow\bar{k}_v}\lambda_v(\alpha-\sigma(\xi_n))\right) = 0. \tag{23}$$

This will complete the proof of Theorem 0.2, for then, combining (22) and (23) and letting $n\to\infty$ in (22), we would have $\hat{h}(\alpha)=0$, contradicting the assumption that α is nontorsion.

The archimedean case. Let v be an archimedean place of k. To simplify notation we view k as embedded in $\mathbb{C}$ and fix an isomorphism of $\bar{k}_v$ with $\mathbb{C}$. Thus, the way k is embedded depends on the choice of v.

To prove (23) we will need a theorem of David and Hirata-Kohno on linear forms in elliptic logarithms and a strong form of equidistribution for torsion points.

Proposition 2.2 (a special case of [David and Hirata-Kohno 2002, Theorem 1]). *Let E/k be an elliptic curve defined over a number field $k\subset\mathbb{C}$. Fix an isomorphism $\theta:\mathbb{C}/\Lambda\cong E(\mathbb{C})$ for an appropriate lattice $\Lambda\subset\mathbb{C}$. Let ω_1,ω_2 be generators for Λ. Fix a nontorsion point $\alpha\in E(k)$ and let $a\in\mathbb{C}$ be such that $\theta(a \bmod \Lambda)=\alpha$. There is a constant $C=C(E,\alpha)>0$ such that for all rational numbers ℓ_1/N, ℓ_2/N with $\ell_1,\ell_2,N\in\mathbb{Z}$,*

$$\left|a-\left(\frac{\ell_1}{N}\omega_1+\frac{\ell_2}{N}\omega_2\right)\right| \geq e^{-C\max(1,\log N)}.$$

By the Szpiro–Ullmo–Zhang theorem [1997], the galois conjugates of the ξ_n are equidistributed in $E(\mathbb{C})$. As we will see, they are in fact strongly equidistributed, in a sense analogous to that in Proposition 1.3.

If $\xi \in E(\bar{k})_{\mathrm{tors}}$, write $\mathrm{Gal}(\bar{k}/k) \cdot \xi$ for the orbit $\{\sigma(\xi) : \sigma \in \mathrm{Gal}(\bar{k}/k)\}$. For each set $U \subset E(\mathbb{C})$, write

$$N(\xi, U) = \#\big((\mathrm{Gal}(\bar{k}/k) \cdot \xi) \cap U\big).$$

Let $\mathcal{S} \subset \mathbb{C}$ be a bounded, convex, centrally symmetric set with 0 in its interior. For each $a \in \mathbb{C}$ and $0 \le r \in \mathbb{R}$, write $\mathcal{S}(a, r) = \{a + rz : z \in \mathcal{S}\}$. For example, if $\mathcal{S} = B(0, 1)$ then $\mathcal{S}(a, r) = B(a, r)$.

Let $\Lambda \subset \mathbb{C}$ be a lattice such that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$. Let $r_0 = r_0(\mathcal{S}, \Lambda) > 0$ be the largest number such that $\mathcal{S}(a, r)$ injects into $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ under the natural projection for all $a \in \mathbb{C}$ and all $0 \le r < r_0$. Write $\mathcal{S}_E(a, r)$ for the image of $\mathcal{S}(a, r)$ in $E(\mathbb{C})$.

Proposition 2.3 (Strong equidistribution). *Let $k \subset \mathbb{C}$ be a number field, and let E/k be an elliptic curve. Then the* $\mathrm{Gal}(\bar{k}/k)$*-conjugates of the torsion points in $E(\bar{k})$ are strongly equidistributed in $E(\mathbb{C})$ in the following sense*:

Let μ be the additive Haar measure on $E(\mathbb{C})$ with total mass 1. *Fix γ with $0 < \gamma < 1/2$, and fix a bounded, convex, centrally symmetric set $\mathcal{S}$ with* 0 *in its interior. Then for each r such that $\mathcal{S}(a, r)$ injects into $E(\mathbb{C})$, and for all $\xi \in E(\bar{k})_{\mathrm{tors}}$,*

$$\frac{N\big(\xi, \mathcal{S}_E(a, r)\big)}{[k(\xi) : k]} = \mu\big(\mathcal{S}_E(a, r)\big) + O([k(\xi) : k]^{-\gamma})$$

where the implied constant depends only on k, $\mathcal{S}$, E, and γ.

The proof will be given starting on page 237.

We can now complete the proof of (23) in the archimedean case. The argument is similar to the one in the proof of Theorem 0.1. By the Szpiro–Ullmo–Zhang theorem [1997], or by Proposition 2.3 when $\mathcal{S}$ has the shape of a period parallelogram (so E can be tiled with sets $\mathcal{S}_E(a, r)$), one knows that as $n \to \infty$ the discrete measures

$$\mu_n = \frac{1}{[k(\xi_n) : k]} \sum_{\sigma : k(\xi_n)/k \hookrightarrow \mathbb{C}} \delta_{\sigma(\xi_n)}(x)$$

converge weakly to the Haar measure μ on $E(\mathbb{C})$ having total mass 1. Proving (23) is equivalent to showing that

$$\lim_{n \to \infty} \int_{E(\mathbb{C})} \lambda_v(\alpha - z)\, d\mu_n(z) = 0.$$

Choose a lattice $\Lambda \subset \mathbb{C}$ such that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, and let F be the area of a fundamental domain for Λ. After scaling Λ, if necessary, we can assume that

$F = 1$. After this normalization, μ coincides with Lebesgue measure. Let $\theta : \mathbb{C}/\Lambda \cong E(\mathbb{C})$ be an isomorphism as in the David/Hirata-Kohno theorem, and let $a \in \mathbb{C}$ be a point with $\theta(a \bmod \Lambda) = \alpha$.

Fix $\varepsilon > 0$ small enough that $B(a, \varepsilon)$ injects into $\mathbb{C}/\Lambda$, and identify $B(a, \varepsilon)$ with its image $B_E(a, \varepsilon) = \theta(B(a, \varepsilon)) \subset E(\mathbb{C})$. (In particular, identify a with α). Without loss, we can assume that $\varepsilon < 1/\pi$, so $\pi\varepsilon^2 < \varepsilon$. We will show that for all large n,

$$\Big|\int_{E(\mathbb{C})} \lambda_v(\alpha - z)\, d\mu_n(z)\Big| < 6\varepsilon. \tag{24}$$

Put

$$\mathrm{labs}_{\alpha,\varepsilon}(z) = \begin{cases} \infty & \text{if } z = a, \\ -[k_v : \mathbb{R}] \log \dfrac{|z-a|}{\varepsilon} & \text{if } z \in B(a, r)\backslash\{a\}, \\ 0 & \text{if } z \in E(\mathbb{C})\backslash B(a, r), \end{cases}$$

and note that

$$0 < \int_{E(\mathbb{C})} \mathrm{labs}_{\alpha,\varepsilon}(z)\, d\mu(z) = \int_{B(a,\varepsilon)} -[k_v : \mathbb{R}] \log(|z-a|/\varepsilon)\, d\mu(z)$$
$$= [k_v : \mathbb{R}] \int_0^\varepsilon -2\pi t \log\frac{t}{\varepsilon}\, dt = [k_v : \mathbb{R}]\, \frac{\pi\varepsilon^2}{2} < \varepsilon.$$

By Proposition 2.1(i) there is a continuous function $g_{\alpha,\varepsilon}(z)$ on $E(\mathbb{C})$ such that

$$\lambda_v(\alpha - z) = \mathrm{labs}_{\alpha,\varepsilon}(z) + g_{\alpha,\varepsilon}(z).$$

Since $\int_{E(\mathbb{C})} \lambda_v(\alpha - z)\, d\mu(z) = 0$ (also by Proposition 2.1(i)), we get

$$\Big|\int_{E(\mathbb{C})} g_{\alpha,\varepsilon}(z)\, d\mu(z)\Big| = \Big|\int_{B(a,\varepsilon)} -\mathrm{labs}_{\alpha,\varepsilon}(z)\, d\mu(z)\Big| < \varepsilon.$$

By weak convergence, it follows that for all sufficiently large n,

$$\Big|\int_{E(\mathbb{C})} g_{\alpha,\varepsilon}(z)\, d\mu_n(z)\Big| < 2\varepsilon. \tag{25}$$

To complete the proof of (24), it suffices to show that for all sufficiently large n,

$$\Big|\int_{B(a,r)} \log(|z-a|/\varepsilon)\, d\mu_n(z)\Big| < 2\varepsilon. \tag{26}$$

For this, put $D = D_n = \lceil [k(\xi_n) : k]^{1/8} \rceil$, and subdivide $B(a, \varepsilon)$ into a disc $A_0(n) = B(a, \varepsilon/D)$ and annuli $A_\ell(n) = B(a, (\ell+1)\varepsilon/D)\backslash B(a, \ell\varepsilon/D)$ for $\ell = 1, \dots, D-1$.

For the central disc, we have $\mu(A_0(n)) = \pi\varepsilon^2/D^2 \le \pi\varepsilon^2/[k(\xi_n) : k]^{1/4}$. Applying Proposition 2.3 when $\mathcal{S}$ is a disc, taking $\gamma = 3/8$, gives

$$N(\xi_n, A_0(n))/[k(\xi_n) : k] \le 2\mu(A_0(n))$$

for all sufficiently large n. If ξ_n has order N_n, the David/Hirata-Kohno theorem tells us that for each conjugate $\sigma(\xi_n) \in A_0(n)$ (where as before we are identifying $B(a, \varepsilon)$ with its image $\theta(B(a, \varepsilon)) \subset E(\mathbb{C})$)

$$\bigl|\log|\sigma(\xi_n) - a|\bigr| \le C \log N_n .$$

Using (41) and (42) below, one sees that $[k(\xi_n) : k] \ge N_n^{1/2}$ for all sufficiently large n. Thus $0 \le \bigl|\log|\sigma(\xi_n) - \alpha|\bigr| \le 2C \log[k(\xi_n) : k]$ and

$$0 \le \biggl|\int_{A_0(n)} \log|z - \alpha|\, d\mu_n(z)\biggr| \le 4\pi\varepsilon^2 C \frac{\log[k(\xi_n) : k]}{[k(\xi_n) : k]^{1/4}} < \varepsilon \tag{27}$$

for all sufficiently large n.

For each annulus $A_\ell(n)$, $\ell = 1, \dots, D-1$, one has

$$\mu(A_\ell(n)) = \pi(2\ell+1)\,\varepsilon^2/D^2 \cong \pi(2\ell+1)\,\varepsilon^2/[k(\xi) : k]^{1/4}.$$

Since $A_\ell(n)$ is the difference of two sets to which Proposition 2.3 applies, we find as above that for sufficiently large n,

$$N(\xi_n, A_\ell(n))/[k(\xi_n) : k] \le 2\mu(A_\ell(n)).$$

Note that on $A_\ell(n)$, $\bigl|\log(|z - \alpha|/\varepsilon)\bigr| \le -\log(\ell/D)$. Summing over these annuli, and bounding the resulting Riemann sum by an integral, we find that

$$\begin{aligned}\biggl|\int_{B(a,\varepsilon)\backslash A_0(n)} \log\frac{|z-a|}{\varepsilon}\, d\mu_n(z)\biggr| &\le \sum_{\ell=1}^{D-1} -\log\Bigl(\frac{\ell\varepsilon/D}{\varepsilon}\Bigr)\cdot 2\mu(A_\ell(n))\\ &< 2\int_{B(a,\varepsilon)} -2\pi t \log(t/\varepsilon)\, dt = \pi\varepsilon^2 < \varepsilon.\end{aligned}$$

Combining this with (27) gives (26), which completes the proof of (23) in the archimedean case (assuming Proposition 2.3).

The nonarchimedean case. In the nonarchimedean case, the proof of (23) depends on a well known result of Cassels on the denominators of torsion points [Silverman 1986, Theorem 3.4, p. 177]. Write $\overline{\mathbb{O}}_v$ for the ring of integers of $\bar{k}_v$.

Proposition 2.4 (Cassels). *Let k_v be a local field of characteristic* 0 *and residue characteristic $p > 0$, and let E/k_v be an elliptic curve defined by a Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

whose coefficients belong to $\mathbb{O}_v$ (note that the Weierstrass equation need not be minimal). Let $P \in E(\bar{k}_v)_{\text{tors}}$ be a point of exact order $m \ge 2$.

(i) *If m is not a power of p, then $x(P), y(P) \in \overline{\mathbb{O}}_v$.*

(ii) *If* $m = p^n$, *then* $x(P) = a/D^2$, $y(P) = b/D^3$ *where* $a, b, D \in \overline{\mathbb{O}}_v$ *and*

$$\mathrm{ord}_v(D) \le \frac{\mathrm{ord}_v(p)}{p^n - p^{n-1}}.$$

Proof. Silverman [1986, Theorem 3.4] states the theorem for torsion points belonging to $E(k_v)$, with $a, b, D \in k_v$ in part (ii) and D satisfying

$$\mathrm{ord}_v(D) = \left\lfloor \frac{\mathrm{ord}_v(p)}{p^n - p^{n-1}} \right\rfloor, \tag{28}$$

where $\lfloor x \rfloor$ denotes the floor of x. Since the Weierstrass equation for E need not be minimal, we can replace k_v by an arbitrary finite extension L_w/k_v, and if $e_{w/v}$ is the ramification index of L_w/k_v, then for $P \in E(L_w)_{\mathrm{tors}}$ and $a, b, D \in L_w$, (28) becomes

$$\mathrm{ord}_v(D) = \frac{1}{e_{w/v}} \cdot \left\lfloor \frac{e_{w/v}\,\mathrm{ord}_v(p)}{p^n - p^{n-1}} \right\rfloor. \tag{29}$$

This yields the result for all $P \in E(\bar{k}_v)_{\mathrm{tors}}$. □

As a consequence, we obtain the following result, part (i) of which is a special case of the Tate–Voloch conjecture proved in [Scanlon 1999].

Corollary 2.5. *Let E/k_v be an elliptic curve defined over a nonarchimedean local field. Then for each nontorsion point $\alpha \in E(\bar{k}_v)$:*

(i) *There is a number $M = M(\alpha)$ such that for all $\xi \in E(\bar{k}_v)_{\mathrm{tors}}$,*

$$\lambda_v(\alpha - \xi) \le M.$$

(ii) *If E has good reduction, then for each $\varepsilon > 0$, there are only finitely many $\xi \in E(\bar{k}_v)_{\mathrm{tors}}$ with $\lambda_v(\alpha - \xi) > \varepsilon$. If E is a Tate curve, then for each $\varepsilon > 0$, there are only finitely many $\xi \in E(\bar{k}_v)_{\mathrm{tors}}$ with $\lambda_v(\alpha - \xi) > \varepsilon + \frac{1}{12}(-\log|\Delta(E)|_v)$.*

Proof. After a finite base extension, we can assume that E either has good reduction or is a Tate curve. Since (ii) implies (i), it suffices to prove (ii). Fix $\varepsilon > 0$.

First suppose E has good reduction. Then $\lambda_v(x - y) = -\log \|x, y\|_v$, where $\|x, y\|_v$ is the spherical distance on the minimal Weierstrass model for E/k_v. If $\xi_1, \xi_2 \in E(\bar{k}_v)_{\mathrm{tors}}$ satisfy $\lambda_v(\alpha - \xi_i) > \varepsilon$, then $\|\xi_1, \alpha\|_v$, $\|\xi_2, \alpha\|_v < (Nv)^{-\varepsilon}$, where Nv is the order of the residue field of $\mathbb{O}_v$. By the ultrametric inequality for the spherical distance [Rumely 1989, § 1.1], $\|\xi_1, \xi_2\|_v < (Nv)^{-\varepsilon}$. By translation invariance, $\|\xi_1 - \xi_2, 0\|_v < (Nv)^{-\varepsilon}$. Put $\xi := \xi_1 - \xi_2$. By the definition of the spherical distance, if x, y are the coordinate functions in the minimal Weierstrass model,

$$-\log \|\xi, 0\|_v = \min\bigl(\mathrm{ord}_v(x(\xi)), \mathrm{ord}_v(y(\xi))\bigr) \cdot \log(Nv).$$

By Cassels' theorem, there are only finitely many torsion points for which

$$\min\bigl(\mathrm{ord}_v(x(\xi)), \mathrm{ord}_v(y(\xi))\bigr) > \varepsilon/\log(Nv).$$

Next suppose E is a Tate curve. Fix a Tate isomorphism $E(\bar{k}_v) \cong \bar{k}_v^\times/q^{\mathbb{Z}}$ where $|q|_v = |\Delta(E)|_v < 1$, and let $y^2 + xy = x^3 + a_4(q)x + a_6(q)$ be the corresponding Weierstrass equation. Let $a, u_1, u_2 \in \bar{k}_v^\times$ correspond to α, ξ_1, ξ_2 respectively; we can assume that $|q|_v < |a|_v, |u_1|_v, |u_2|_v \le 1$. By the formula for $\lambda_v(x-y)$ in Proposition 2.1(ii), if $\lambda_v(\alpha - \xi_i) > \varepsilon + \frac{1}{12}(-\log|\Delta(E)|_v)$, then $|\,a|_v = |u_1|_v = |u_2|_v$ and

$$-\log|1 - a^{-1}u_i|_v \;=\; \operatorname{ord}_v(1 - a^{-1}u_i)\cdot\log(Nv) \;>\; \varepsilon\,.$$

Put $\xi = \xi_1 - \xi_2$ and $u = u_2^{-1}u_1$. Then ξ corresponds to u under the Tate isomorphism, and $\operatorname{ord}_v(1-u) > \varepsilon/\log(Nv)$. By the formulas for $x(\xi)$, $y(\xi)$ in [Silverman 1994, p. 425],

$$\operatorname{ord}_v(x(\xi)) = 2\operatorname{ord}_v(1-u) \quad\text{and}\quad \operatorname{ord}_v(y(\xi)) = 3\operatorname{ord}_v(1-u).$$

Again by Cassels' theorem, only finitely many torsion points ξ can satisfy

$$\min\bigl(\operatorname{ord}_v(x(\xi)), \operatorname{ord}_v(y(\xi))\bigr) > \varepsilon/\log(Nv). \qquad \square$$

We can now prove (23) when E has good reduction at v.

Fix $\varepsilon > 0$. Let M be the upper bound in Corollary 2.5(i), and let N be the number of points $\xi \in E(\bar{k}_v)_{\text{tors}}$ with $\lambda_v(\alpha - \xi) > \varepsilon$ given by Corollary 2.5(ii). For all sufficiently large n, $MN/[k(\xi_n):k] < \varepsilon$, giving

$$0 \le \frac{1}{[k(\xi_n):k]} \sum_{\sigma:\bar{k}/k\hookrightarrow\bar{k}_v} \lambda_v(\alpha - \sigma(\xi_n)) \le \frac{([k(\xi_n):k] - N)}{[k(\xi_n):k]}\,\varepsilon + \frac{N}{[k(\xi_n):k]}\,M \;<\; 2\varepsilon\,.$$

Thus

$$\lim_{n\to\infty} \frac{1}{[k(\xi_n):k]} \sum_{\sigma:\bar{k}/k\hookrightarrow\bar{k}_v} \lambda_v(\sigma(\xi_n) - \alpha) \;=\; 0\,.$$

To prove (23) when E is a Tate curve at v, we will need the following equidistribution theorem of Chambert-Loir [2006, corollaire 5.5].

Fix a Tate isomorphism $E(\bar{k}_v) \cong \bar{k}_v/q^{\mathbb{Z}}$, put $L = \mathbb{Z}\cdot\operatorname{ord}_v(q) \subset \mathbb{R}$, and define a "reduction map" $r : E(\bar{k}) \to \mathbb{R}/L$ by setting $r(P) = \operatorname{ord}_v(a) \pmod{L}$ if $P \in E(\bar{k}_v)$ corresponds to $a \in \bar{k}_v^\times$.

For each global point $P \in E(\bar{k})$, define a measure $\mu_{P,v}$ on $\mathbb{R}/L$ by

$$\mu_{P,v}(z) \;=\; \frac{1}{[k(P):k]} \sum_{\sigma:\bar{k}/k\hookrightarrow\bar{k}_v} \delta_{r(\sigma(P))}(z)$$

and let μ_v be the Haar measure on $\mathbb{R}/L$ with total mass 1.

Proposition 2.6 (Chambert-Loir). *For each sequence of distinct points $\{P_n\}$ in $E(\bar{k})$ with $\hat{h}(P_n) \to 0$, the sequence of measures $\{\mu_{P_n,v}\}$ converges weakly to μ_v.*

We can now prove (23) when E is a Tate curve. Recall that $\{\xi_n\}$ is a sequence of distinct torsion points which are S-integral with respect to α.

Fix $\varepsilon > 0$. Let M be the upper bound in Corollary 2.5(i). Put $a = r(\alpha)$ and let $\delta > 0$ be such that $\mu((a-\delta, a+\delta)) < \varepsilon/M$, where by abuse of notation we identify a sufficiently short interval in $\mathbb{R}$ with its image in $\mathbb{R}/L$. By Chambert-Loir's theorem, $\mu_{\xi_n,v}((a-\delta, a+\delta)) < 2\varepsilon/M$ for all sufficiently large n.

By the formulas in Proposition 2.1(ii), $\int_{\mathbb{R}/L} \tilde{\lambda}_v(z)\, d\mu_v(z) = 0$ and

$$\Big|\frac{1}{[k(\xi_n):k]} \sum_{\sigma:\bar{k}/k\hookrightarrow\bar{k}_v} \lambda_v(\sigma(\xi_n)-\alpha)\Big| \\ \leq \left|\int_{\mathbb{R}/L} \tilde{\lambda}_v(z-a)\, d\mu_{\xi_n,v}(z)\right| + M\,\mu_{\xi_n,v}((a-\delta, a+\delta)).$$

For all sufficiently large n the right side is at most 3ε. Hence

$$\lim_{n\to\infty} \frac{1}{[k(\xi_n):k]} \sum_{\sigma:\bar{k}/k\hookrightarrow\bar{k}_v} \lambda_v(\sigma(\xi_n)-\alpha) \;=\; 0.$$

This completes the proof of Theorem 0.2. □

Several results in the literature use methods related to ours.

J. Cheon and S. Hahn [1999] proved an elliptic curve analogue of Schinzel's theorem [1974]. Likewise, Everest and B. Ní Flathúin [1996] evaluate "elliptic Mahler measures" in terms of limits involving division polynomials, obtaining results similar to (13). They use David/Hirata-Kohno's theorem on elliptic logarithms in place of Baker's theorem, much as we do.

More recently, L. Szpiro and T. Tucker [2005] proved that local canonical heights for a dynamical system can be evaluated by taking limits over "division polynomials" for the dynamical system. (These polynomials have periodic points as their roots.) Their work uses Roth's theorem rather than Baker's or David/Hirata-Kohno's theorem. It would be interesting to see if this could be brought to bear on Conjecture 3.1 below.

Strong equidistribution for torsion points on elliptic curves. We will now prove Proposition 2.3, the strong equidistribution theorem for galois orbits of torsion points on elliptic curves, which was used in the proof of Theorem 0.2.

Proof of Proposition 2.3. The proof breaks into two cases, depending on whether or not E has complex multiplication. Both cases are similar, and are modeled on Proposition 1.3. We find an extension field over which there is a two-dimensional geometric interpretation of the galois orbits, and by carrying out inclusion/exclusion, we are able to count the number of conjugates over that field lying in a convex, centrally symmetric set, with a good error bound. The conjugates over the original field can then be counted by breaking into cosets.

Case 1. Suppose E does not have complex multiplication. The action of $\mathrm{Gal}(\bar{k}/k)$ on $E(\bar{k})_{\mathrm{tors}}$ induces an injective homomorphism

$$\eta : \mathrm{Gal}(\bar{k}/k) \to \varprojlim \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \cong \prod_p \mathrm{GL}_2(\mathbb{Z}_p).$$

By Serre's theorem [1972, théorème 3], the image of $\mathrm{Gal}(\bar{k}/k)$ in $\prod_p \mathrm{GL}_2(\mathbb{Z}_p)$ is open. Hence there is a number Q such that $\mathrm{Im}(\eta)$ contains the subgroup

$$\prod_{p\,|\,Q} (1 + QM_2(\mathbb{Z}_p)) \times \prod_{p\nmid Q} \mathrm{GL}_2(\mathbb{Z}_p).$$

Let $G_Q \subset \mathrm{Gal}(\bar{k}/k)$ be the preimage of this subgroup.

Step 1: Determining the size of a galois orbit under G_Q. Let $\xi \in E(\bar{k})_{\mathrm{tors}}$ have order N, and put $Q_N = \gcd(Q, N)$. For suitable right coset representatives $\sigma_1, \dots, \sigma_T$ of G_Q in $\mathrm{Gal}(\bar{k}/k)$, the galois orbit $\mathrm{Gal}(\bar{k}/k) \cdot \xi$ decomposes as a disjoint union of G_Q-orbits:

$$\mathrm{Gal}(\bar{k}/k) \cdot \xi = \bigcup_{i=1}^{T} G_Q \cdot \sigma_i(\xi).$$

Since G_Q is normal in $\mathrm{Gal}(\bar{k}/k)$, the orbits $G_Q \cdot \sigma_i(\xi) = \sigma_i(G_Q \cdot \xi)$ all have the same size. Thus $[k(\xi) : k] = T \cdot \#(G_Q \cdot \xi)$. By considering the action of G_Q on the p-parts of ξ, one sees that

$$\#(G_Q \cdot \xi) = \prod_{p\,|\,Q_N} p^{2(\mathrm{ord}_p(N) - \mathrm{ord}_p(Q_N))} \prod_{\substack{p\,|\,N \\ p\nmid Q_N}} p^{2\,\mathrm{ord}_p(N)} \Bigl(1 - \frac{1}{p^2}\Bigr) = \frac{N^2}{Q_N^2} \cdot \prod_{\substack{p\,|\,N \\ p\nmid Q}} \Bigl(1 - \frac{1}{p^2}\Bigr). \tag{30}$$

Indeed, let ξ_p be the p-component of ξ in $E[N] \cong \prod_{p\,|\,N} (\mathbb{Z}/p^{\mathrm{ord}_p(N)}\mathbb{Z})^2$. Identify ξ_p with an element of $(\mathbb{Z}/p^{\mathrm{ord}_p(N)}\mathbb{Z})^2$: then ξ_p generates that group. If p divides Q_N, the image of G_Q in $\mathrm{GL}_2(\mathbb{Z}/p^{\mathrm{ord}_p(N)}\mathbb{Z})$ is $I + p^{\mathrm{ord}_p(Q_N)} M_2(\mathbb{Z}/p^{\mathrm{ord}_p(N)}\mathbb{Z})$, and

$$G_Q \cdot \xi_p = \xi_p + p^{\mathrm{ord}_p(Q_N)} \cdot (\mathbb{Z}/p^{\mathrm{ord}_p(N)}\mathbb{Z})^2.$$

On the other hand, if $p \nmid Q_N$, the image of G_Q in $\mathrm{GL}_2(\mathbb{Z}/p^{\mathrm{ord}_p(N)}\mathbb{Z})$ is the full group, so

$$G_Q \cdot \xi_p = (\mathbb{Z}/p^{\mathrm{ord}_p(N)}\mathbb{Z})^2 \backslash p \cdot (\mathbb{Z}/p^{\mathrm{ord}_p(N)}\mathbb{Z})^2.$$

Step 2: Counting translated lattice points in convex domains. Let $\mathcal{F}$ be a fundamental domain for Λ; we can assume $\mathcal{F}$ is bounded and contains 0. Let C be such that $\mathcal{F} \subset \mathcal{S}(0, C)$. Note that since $\mathcal{S}$ is convex, if $z_1 \in \mathcal{S}(a_1, r_1)$ and $z_2 \in \mathcal{S}(a_2, r_2)$, then $z_1 + z_2 \in \mathcal{S}(a_1 + a_2, r_1 + r_2)$. Put $F = \text{area}\ \mathcal{F}$ and $S = \text{area}\ \mathcal{S}$.

For each $0 < t \in \mathbb{R}$, we have $\operatorname{area}(t\mathcal{F}) = t^2 F$ and $\operatorname{area} \mathcal{S}(a, r) = r^2 S$. Each lattice $t\Lambda_N$ is homothetic to Λ_N, and hence has fundamental domain $t\mathcal{F} \subset \mathcal{S}(0, tC)$. Fix $x_0 \in \mathbb{C}$. As y runs over $x_0 + t\Lambda$, the sets $y + t\mathcal{F}$ are pairwise disjoint and cover $\mathbb{C}$. If $y \in \mathcal{S}(a, r)$, then $y + t\mathcal{F} \subset \mathcal{S}(a, r + tC)$. Hence

$$\#\big((x_0+t\Lambda)\cap\mathcal{S}(a,r)\big) \le \frac{\operatorname{area}\big(\mathcal{S}(a,r+tC)\big)}{\operatorname{area}(t\mathcal{F})} = \frac{r^2S}{F}\cdot\frac{1}{t^2}+\frac{2CSr}{F}\cdot\frac{1}{t}+\frac{C^2S}{F}. \quad (31)$$

Similarly, if $r > tC$, take $z \in \mathcal{S}(a, r - tC)$, and let $y \in x_0 + t\Lambda$ be such that $z \in y + t\mathcal{F}$. Then $z - y \in t\mathcal{F}$, so $z - y \in \mathcal{S}(0, tC)$, and since $\mathcal{S}$ is centrally symmetric $y - z \in \mathcal{S}(0, tC)$. Thus $y = z + (y - z) \in \mathcal{S}(a, r)$. It follows that $\mathcal{S}(a, r - tC) \subset \bigcup_{y\in(x_0+t\Lambda)\cap\mathcal{S}(a,r)}(y + t\mathcal{F})$, so

$$\#\big((x_0+t\Lambda)\cap\mathcal{S}(a,r)\big) \ge \frac{\operatorname{area}\big(\mathcal{S}(a,r-tC)\big)}{\operatorname{area}(t\mathcal{F})} > \frac{r^2S}{F}\cdot\frac{1}{t^2}-\frac{2CSr}{F}\cdot\frac{1}{t}-\frac{C^2S}{F}. \quad (32)$$

If $r \le tC$, the right side of (32) is negative, so the inequality between the first and last quantities holds trivially.

Now let D be a positive divisor of N/Q_N. Taking $t = Q_N D/N$, and combining (31), (32), we obtain

$$\left|\#\left(\left(x_0+\frac{Q_ND}{N}\Lambda_N\right)\cap\mathcal{S}(a,r)\right)-\frac{\operatorname{area}\big(\mathcal{S}(a,r)\big)}{\operatorname{area}(\mathcal{F})}\cdot\frac{N^2}{Q_N^2D^2}\right| \le \frac{2CSr}{F}\cdot\frac{N}{Q_ND}+\frac{C^2S}{F}. \quad (33)$$

Step 3: Inclusion/exclusion. Write $\Lambda_N = \frac{1}{N}\Lambda$, fix σ_i, and let $x \in \Lambda_N$ correspond to $\sigma_i(\xi)$. Since $E[N] \cong \Lambda_N/\Lambda$, the considerations above show there is a one-to-one correspondence between elements of $G_Q \cdot \sigma_i(\xi)$, and cosets $y + \Lambda$ for $y \in \Lambda_N$ such that $y - x \in Q_N\Lambda_N$ and $y + \Lambda$ has exact order N in Λ_N/Λ. Equivalently, $y - x \in Q_N\Lambda_N$ and $y \notin p\Lambda_N$ for each prime p dividing N but not Q.

Let $p_1, \dots, p_R$ be the distinct primes dividing N but not Q; if there are no such primes, take $p_1 \cdots p_R = 1$. Since Q_N and $p_1, \cdots, p_R$ are pairwise coprime, there is an $x_0 \in \Lambda_N$ such that $x_0 \equiv x \pmod{Q_N\Lambda_N}$ and $x_0 \equiv 0 \pmod{p_1 \cdots p_R\Lambda_N}$. Then $y - x_0 \in Q_N\Lambda_N$ if and only if $y \in x_0 + Q_N\Lambda_N$, and $y \in p_i\Lambda_N$ if and only if $y \in x_0 + p_i\Lambda_N$. Note that if $D|p_1 \cdots p_R$ then $Q_N\Lambda_N \cap D\Lambda_N = Q_N D\Lambda_N$. Recalling that r_0 is the supremum over positive numbers r for which $\mathcal{S}(a, r)$ injects into $\mathbb{C}/\Lambda$, take $a \in \mathbb{C}$ and take $0 < r \le r_0$. Applying inclusion/exclusion, we obtain

$$\#\big(G_Q\cdot\sigma_i(\xi)\cap\mathcal{S}_E(a,r)\big) = \sum_{D\,|\,p_1\cdots p_R}(-1)^{\lambda(D)}\cdot\#\big((x_0+Q_ND\Lambda_N)\cap\mathcal{S}(a,r)\big), \quad (34)$$

where $\lambda(D)$ is the number of distinct primes dividing D.

Inserting (33) in (34) and summing over all $\sigma_i(\xi)$, $i = 1, \dots, T$, we find

$$\begin{aligned} N\big(\xi, \mathcal{S}_E(a,r)\big) = \frac{\operatorname{area} \mathcal{S}(a,r)}{\mathcal{F}} \cdot \frac{TN^2}{Q_N^2} \prod_{\substack{p \mid N \\ p \nmid Q}} \Big(1 - \frac{1}{p^2}\Big) \\ + \theta\bigg(\frac{2CSr}{F} \cdot \frac{TN}{Q_N} \prod_{\substack{p \mid N \\ p \nmid Q}} \Big(1 + \frac{1}{p}\Big)\bigg) + \theta\Big(\frac{C^2 S}{F} \cdot T 2^R\Big), \end{aligned}$$

where, as before, $\theta(x)$ denotes a quantity with $-x \le \theta(x) \le x$. By (30),

$$[k(\xi) : k] \,=\, T \cdot \#(G_Q \cdot \xi) \,=\, \frac{TN^2}{Q_N^2} \prod_{\substack{p \mid N \\ p \nmid Q}} \Big(1 - \frac{1}{p^2}\Big). \tag{35}$$

Since $r \le r_0$, it follows that

$$\begin{aligned} \frac{N\big(\xi, \mathcal{S}_E(a,r)\big)}{[k(\xi) : k]} = \frac{\operatorname{area} \mathcal{S}(a,r)}{\operatorname{area} \mathcal{F}} \,+\, \theta\Bigg(\frac{2CSr_0}{F} \cdot \frac{Q_N}{N \prod_{\substack{p \mid N \\ p \nmid Q}} \Big(1 - \frac{1}{p}\Big)}\Bigg) \\ + \theta\Bigg(\frac{C^2 S}{F} \cdot \frac{2^R Q_N^2}{N^2 \prod_{\substack{p \mid N \\ p \nmid Q}} \Big(1 - \frac{1}{p^2}\Big)}\Bigg). \end{aligned}$$

Here $\operatorname{area} \mathcal{S}(a,r)/\operatorname{area} \mathcal{F} = \mu(\mathcal{S}_E(a,r))$. Note that T is bounded by the order of $\mathrm{GL}_2(\mathbb{Z}/Q\mathbb{Z}))$, Q_N is bounded by Q, and

$$N \prod_{p \mid N} \Big(1 - \frac{1}{p}\Big) \,\ge\, N^{1-\varepsilon}$$

for each $\varepsilon > 0$ and each sufficiently large N. Using (35) and the fact that

$$1 \,\ge\, \prod_{p \mid N, p \nmid Q} \Big(1 - \frac{1}{p^2}\Big) \,\ge\, 1/\zeta(2)$$

one sees that the first error term is $O_\gamma([k(\xi) : k]^{-\gamma})$ for each $\gamma < 1/2$. Similarly, $2^R \le d(N) \le N^\varepsilon$ for each $\varepsilon > 0$ and each sufficiently large N. Thus the second error term is negligible in comparison with the first. This completes the proof when E does not have complex multiplication.

Case 2. Suppose E has complex multiplication. Let K be the CM field of E, and let $\mathcal{O} \subset \mathcal{O}_K$ be the order corresponding to E. After enlarging k if necessary, we can assume that $K \subset k$. Let $\Lambda \subset \mathbb{C}$ be a lattice such that $E \cong \mathbb{C}/\Lambda$. Without loss of generality, we can assume that $\Lambda \subset K$. Fix an analytic isomorphism $\vartheta : \mathbb{C}/\Lambda \cong E(\mathbb{C})$.

By the theory of complex multiplication (see [Shimura 1971], [Lang 1973], or [Silverman 1994, Chapter II]), $E(\bar{k})_{\text{tors}}$ is rational over k^{ab}, the maximal abelian extension of k. Let $k_{\mathbb{A}}^{\times}$ be the idèle ring of k, and for $s \in k_{\mathbb{A}}^{\times}$ let $[s, k]$ be the Artin map acting on k^{ab}. Given $\sigma \in \mathrm{Gal}(\bar{k}/k)$, take $s \in k_{\mathbb{A}}^{\times}$ with $\sigma|_{k^{ab}} = [s, k]$, and put $w = N_{k/K}(s) \in K_{\mathbb{A}}^{\times}$. There is an action of $K_{\mathbb{A}}^{\times}$ on lattices, defined semilocally, which associates to w and Λ a new lattice $w^{-1}\Lambda$. This action extends to a map $w^{-1} : K/\Lambda \to K/w^{-1}\Lambda$. There is also a homomorphism $\psi : k_{\mathbb{A}}^{\times} \to K^{\times}$, the grössencharacter of E, which has the property that $\psi(s)N_{k/K}(s)^{-1}\Lambda = \Lambda$. Put $\kappa = \psi(s) \in K^{\times}$.

With this notation, there is a commutative diagram

$$\begin{tikzcd}
K/\Lambda \arrow[r, hook] \arrow[d, "w^{-1}"'] & \mathbb{C}/\Lambda \arrow[r, "\vartheta"] & E(\bar{k})_{\text{tors}} \arrow[d, "\sigma"] \\
K/w^{-1}\Lambda \arrow[r, hook] \arrow[d, "\kappa"'] & \mathbb{C}/w^{-1}\Lambda \arrow[r] & E(\bar{k})_{\text{tors}} \arrow[d, "id"] \\
K/\Lambda \arrow[r, hook] & \mathbb{C}/\Lambda \arrow[r, "\vartheta"] & E(\bar{k})_{\text{tors}}
\end{tikzcd}$$

in which the vertical arrows on the left are multiplication by w^{-1} and κ respectively, and those on the right are the galois action (see [Shimura 1971, Proposition 7.40, p. 211], or [Lang 1973, Theorem 8, p. 137]). Note that the same analytic isomorphism ϑ appears in the top and bottom rows. Thus, if $\xi \in E(\bar{k})_{\text{tors}}$ corresponds to $x \in K/\Lambda$, and $\sigma|_{k^{ab}} = [s, k]$, then

$$\sigma(\xi) = \vartheta(\psi(s)N_{k/K}(s)^{-1}x).$$

This gives an explicit description of the galois action on torsion points in terms of adelic "multiplication".

The action of $K_{\mathbb{A}}^{\times}$ in the diagram is as follows. Let $L \subset K$ be a lattice. For each rational prime p of $\mathbb{Q}$, write $L_p = L \otimes_{\mathbb{Z}} \mathbb{Z}_p$ and $K_p = K \otimes_{\mathbb{Q}} \mathbb{Q}_p$; if $w \in K_{\mathbb{A}}^{\times}$, let w_p be its p-component. Then $w_p^{-1}L_p$ is a $\mathbb{Z}_p$-lattice in K_p. There is a unique lattice $M \subset K$ such that $M_p = w_p^{-1}L_p$ for each p [Lang 1973, Theorem 8, p. 97], and $w^{-1}L$ is defined to be M. Likewise, if $x \in K/L$, lift it to an element of $K \subset K_{\mathbb{A}}$ and write $x_p \in K_p$ for its p-component; there is a $y \in K$ such that $w_p^{-1}x_p \pmod{w^{-1}L_p} = y \pmod{M_p}$ for each p, and $w^{-1}(x \pmod{L})$ is defined to be $y \pmod{M}$.

The order $\mathbb{O}$ has the form $\mathbb{O} = \mathbb{Z} + c\mathbb{O}_K$ for some integer $c \geq 1$, and c is called the conductor of $\mathbb{O}$. The lattice Λ is a proper $\mathbb{O}$-lattice, meaning that $\mathbb{O} = \{x \in K : x\Lambda \subset \Lambda\}$. For any order $\mathbb{O}$, there are only finitely many homothety classes of proper $\mathbb{O}$-lattices [Lang 1973, Theorem 7, p. 95]. Write $\mathbb{O}_p = \mathbb{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ and $\mathbb{O}_{K,p} = \mathbb{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

If $p \nmid c$, then $\mathcal{O}_p = \mathcal{O}_{K,p} \cong \prod_{\mathfrak{p}\,|\,p} \mathcal{O}_{K,\mathfrak{p}}$, where $\mathfrak{p}$ runs over the primes of K lying over p, and $\mathcal{O}_{K,\mathfrak{p}}$ is the completion of $\mathcal{O}_K$ at $\mathfrak{p}$.

Let U be the kernel of the grössencharacter $\psi : k_{\mathbb{A}}^{\times} \to K^{\times}$, and take $W = N_{k/K}(U) \subset K_{\mathbb{A}}^{\times}$. Since ψ is continuous, there is an integer $Q \geq 1$ such that, for each $p \,|\, Q$, the subgroup $1 + Q\mathcal{O}_{K,p} \subset \mathcal{O}_{K,p}^{\times}$ is contained in W_p and for each $p \nmid Q$, $\mathcal{O}_{K,p}^{\times} \subset W_p$. If $w \in W$, then $w^{-1}\Lambda = \Lambda$, so $w_p \in \mathcal{O}_p^{\times}$. Hence $c \,|\, Q$.

Noting that $\mathcal{O}_p = \mathcal{O}_{K,p}$ if $p \nmid Q$, let $W_Q \subset K_{\mathbb{A}}^{\times}$ be the subgroup

$$\mathbb{C}^{\times} \times \prod_{p\,|\,Q} (1 + Q\mathcal{O}_p) \times \prod_{p \nmid Q} \mathcal{O}_p^{\times} \subset W,$$

and let U_Q be its preimage in $k_{\mathbb{A}}^{\times}$ under the norm map. Put

$$G_Q = \{\sigma \in \mathrm{Gal}(\bar{k}/k) : \sigma|_{k^{ab}} = [s, k] \text{ for some } s \in U_Q\}.$$

Then G_Q is open and normal in $\mathrm{Gal}(\bar{k}/k)$.

Step 1: Determining the size of a galois orbit under G_Q. Fix $\xi \in E(\bar{k})_{\mathrm{tors}}$. Suppose ξ has order N; put $Q_N = \gcd(Q, N)$. For suitable right coset representatives $\sigma_1, \ldots, \sigma_T$ of G_Q in $\mathrm{Gal}(\bar{k}/k)$, the orbit $\mathrm{Gal}(\bar{k}/k) \cdot \xi$ decomposes as a disjoint union of G_Q-orbits:

$$\mathrm{Gal}(\bar{k}/k) \cdot \xi = \bigcup_{i=1}^{T} G_Q \cdot \sigma_i(\xi).$$

As before, the orbits $G_Q \cdot \sigma_i(\xi) = \sigma_i(G_Q \cdot \xi)$ all have the same size, and $[k(\xi) : k] = T \cdot \#(G_Q \cdot \xi)$.

Let ξ correspond to $x + \Lambda \in K/\Lambda$. Write $\Lambda(x)$ for the $\mathcal{O}$-lattice $\mathcal{O}x + \Lambda$; since ξ has order N, $[\Lambda(x) : \Lambda] \geq N$. More generally, for any integer m, put $\Lambda(mx) = \mathcal{O} \cdot mx + \Lambda = m\mathcal{O}x + \Lambda$. Note that

$$\Lambda(mx)/\Lambda \cong \prod_{p\,|\,N} \Lambda(mx)_p/\Lambda_p = \prod_{p\,|\,N} (m\mathcal{O}_p x + \Lambda_p)/\Lambda_p.$$

If $p \,|\, Q$, then G_Q acts on ξ_p through the subgroup $1 + p^{\mathrm{ord}_p(Q)}\mathcal{O}_p \subset \mathcal{O}_p^{\times}$. Noting that $\mathrm{ord}_p(Q_N) = \min(\mathrm{ord}_p(Q), \mathrm{ord}_p(N))$ and that $p^{\mathrm{ord}_p(Q)}x \in \Lambda_p$ if $\mathrm{ord}_p(Q) \geq \mathrm{ord}_p(N)$, we have

$$G_Q \cdot \xi_p \cong (x + p^{\mathrm{ord}_p(Q)}\mathcal{O}_p x + \Lambda_p)/\Lambda_p = (x + \Lambda(p^{\mathrm{ord}_p(Q_N)}x)_p)/\Lambda_p.$$

Thus $\#(G_Q \cdot \xi_p) = [\Lambda(p^{\mathrm{ord}_p(Q_N)}x)_p : \Lambda_p]$.

If $p \nmid Q$, then $\mathcal{O}_p = \mathcal{O}_{K,p}$ and G_Q acts on ξ_p through $\mathcal{O}_p^{\times} \cong \prod_{\mathfrak{p}\,|\,p} \mathcal{O}_{K,\mathfrak{p}}^{\times}$. For each $\mathfrak{p} \,|\, p$, and each $\mathcal{O}$-lattice L, we have $L_{\mathfrak{p}} \cong (\mathcal{O}_K L)_{\mathfrak{p}}$ where $\mathcal{O}_K L$ is an $\mathcal{O}_K$-fractional ideal. Thus $\mathrm{ord}_{\mathfrak{p}}(L) := \mathrm{ord}_{\mathfrak{p}}(\mathcal{O}_K L)$ is well defined. Write $\mathrm{ord}_{\mathfrak{p}}(\xi) =$

$\mathrm{ord}_{\mathfrak{p}}(\Lambda)-\mathrm{ord}_{\mathfrak{p}}(\Lambda(x))$. Then $\Lambda(x)_p/\Lambda_p \cong \prod_{\mathfrak{p}|p}\mathbb{O}_K/\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\xi)}$ and

$$\#(G_Q\cdot\xi_p) = [\Lambda(x)_p:\Lambda_p]\cdot \prod_{\substack{\mathfrak{p}|p\\ \mathrm{ord}_{\mathfrak{p}}(\xi)>0}} \Big(1-\frac{1}{N\mathfrak{p}}\Big),$$

where $N\mathfrak{p}=\#(\mathbb{O}_K/\mathfrak{p})$ is the norm of $\mathfrak{p}$.

Combining these formulas, and using that

$$\prod_{p|N}[\Lambda(p^{\mathrm{ord}_p(Q_N)}x)_p:\Lambda_p]=[\Lambda(Q_Nx):\Lambda],$$

we obtain

$$\#(G_Q\cdot\xi) = [\Lambda(Q_Nx):\Lambda]\cdot \prod_{\substack{\mathfrak{p}|N,\mathfrak{p}\nmid Q\\ \mathrm{ord}_{\mathfrak{p}}(\xi)>0}} \Big(1-\frac{1}{N\mathfrak{p}}\Big). \tag{36}$$

Step 2: Counting translated lattice points in convex domains. If L is any $\mathbb{O}$-lattice, and $F(L)$ is the area of a fundamental domain for $\mathbb{C}/L$, then by Minkowski's theorem there is a point $0\neq\ell\in L$ with $|\ell|\le(4/\pi)^{1/2}F(L)^{1/2}$. Here L is a proper $\mathbb{O}'$-lattice for some order $\mathbb{O}'$ with conductor $c'\,|\,c$. There are only finitely many such orders $\mathbb{O}'$, and for each $\mathbb{O}'$ there are only finitely many homothety classes of proper $\mathbb{O}'$-lattices, so there are only finitely many homothety classes of $\mathbb{O}$-lattices. Hence there is a constant C_1, independent of L, such that L has a fundamental domain $\mathcal{F}(L)$ contained in the ball $B(0,C_1\cdot F(L)^{1/2})$. In turn, there is a constant C, independent of L, such that $\mathcal{F}(L)\subset\mathcal{S}(0,C\cdot F(L)^{1/2})$. This fact is the crux of the argument in the CM case.

Again, if L is an $\mathbb{O}$-lattice, then for each ideal ϖ of $\mathbb{O}_K$ coprime to c, there is a unique lattice ϖL defined by the property that $(\varpi L)_q=(\varpi\mathbb{O}_K L)_q$ for all primes $q\,|\,N\varpi$, and $(\varpi L)_q=L_q$ for all primes $q\nmid N\varpi$. This lattice has index $[L:\varpi L]=N\varpi$.

We will apply this taking $L=\Lambda(Q_Nx)=Q_N\mathbb{O}x+\Lambda$. Note that the fundamental domain $\mathcal{F}(\varpi\Lambda(Q_Nx))$ has area $F\cdot N\varpi/[\Lambda(Q_Nx):\Lambda]$, where F is the area of a fundamental domain $\mathcal{F}$ for Λ. By the same argument leading to (33) we find that for each $x_0\in\mathbb{C}$

$$\Big|\#\big((x_0+\varpi\Lambda(Q_Nx))\cap\mathcal{S}(a,r)\big)-\frac{\mathrm{area}\,\mathcal{S}(a,r)}{\mathrm{area}\,\mathcal{F}}\cdot\frac{[\Lambda(Q_Nx):\Lambda]}{N\varpi}\Big| \le \frac{2CSr}{F}\cdot\Big(\frac{[\Lambda(Q_Nx):\Lambda]}{N\varpi}\Big)^{1/2}+\frac{C^2S}{F}. \tag{37}$$

Step 3: Inclusion/exclusion. Now consider a set $\mathcal{S}(a,r)$, where $a\in\mathbb{C}$ and $r\le r_0$. For each $\sigma_i(\xi)$, we will compute $\#\big((G_Q\cdot\sigma_i(\xi))\cap\mathcal{S}_E(a,r)\big)$. Fix σ_i, and replace ξ by $\sigma_i(\xi)$ in the discussion above. Let $x\in K/\Lambda$ correspond to $\sigma_i(\xi)$, and let $\mathfrak{p}_1,\dots,\mathfrak{p}_R$ be the distinct primes of $\mathbb{O}_K$ dividing N but not Q, for which

$\mathrm{ord}_{\mathfrak{p}}(\Lambda(x)) \neq \mathrm{ord}_{\mathfrak{p}}(\Lambda)$. If there are no such primes, take $\mathfrak{p}_1 \cdots \mathfrak{p}_R = 1$ in the argument below. (Note that the $\mathfrak{p}_j$ are independent of σ_i, since $K \subset k$ and for $p \nmid Q$, σ_i acts on ξ through $\mathbb{O}_p^\times$.) Thus there is a one-to-one correspondence between elements of $G_Q \cdot \sigma_i(\xi)$, and cosets $y + \Lambda$ for $y \in K$ such that $y \in x + \Lambda(Q_N x)$ and $y \notin \mathfrak{p}_j \Lambda(x)$ for $j = 1, \dots, R$. Since $\Lambda(Q_N x) \subset \Lambda(x)$, such y necessarily belong to $\Lambda(x)$. The index $[\Lambda(Q_N x) : \Lambda]$ in (37) is independent of σ_i by (36), since $\#(G_Q \cdot \sigma_i(\xi))$ and the $\mathfrak{p}_j$ are independent of σ_i.

The lattices $\Lambda(Q_N x)$ and $\mathfrak{p}_1 \cdots \mathfrak{p}_R \Lambda(x)$ have coprime indices in $\Lambda(x)$, so there is an $x_0 \in \Lambda(x)$ such that $x_0 \equiv x \pmod{\Lambda(Q_N x)}$ and $x_0 \equiv 0 \pmod{\mathfrak{p}_1 \cdots \mathfrak{p}_R \Lambda(x)}$. Further, for any $\mathbb{O}_K$-ideal ϖ dividing $\mathfrak{p}_1 \cdots \mathfrak{p}_R$,

$$\Lambda(Q_N x) \cap \left(\textstyle\bigcap_{\mathfrak{p}_j \mid \varpi} \mathfrak{p}_j \Lambda(x) \right) = \varpi \Lambda(Q_N x).$$

Clearly $y \in x + \Lambda(Q_N x)$ if and only if $y \in x_0 + \Lambda(Q_N x)$, and $y \in \mathfrak{p}_j \Lambda(x)$ if and only if $y \in x_0 + \mathfrak{p}_j \Lambda(x)$. Since $\mathcal{G}(a, r)$ injects into $\mathbb{C}/\Lambda$, by inclusion/exclusion

$$\begin{aligned} &\#\big((G_Q \cdot \sigma_i(\xi)) \cap \mathcal{G}_E(a, r)\big) \\ &\qquad = \sum_{\varpi \mid \mathfrak{p}_1 \cdots \mathfrak{p}_R} (-1)^{\lambda_K(\varpi)} \cdot \#\big((x_0 + \varpi \Lambda(Q_N x)) \cap \mathcal{G}(a, r)\big), \end{aligned} \tag{38}$$

where $\lambda_K(\varpi)$ is the number of distinct prime ideals of $\mathbb{O}_K$ dividing ϖ.

Inserting (37) in the inclusion/exclusion formula (38) and summing over all $\sigma_i(\xi)$, we get

$$\begin{aligned} &N\big(\xi, \mathcal{G}_E(a, r)\big) \\ &\quad = \frac{\operatorname{area} \mathcal{G}(a, r)}{\operatorname{area} \mathcal{F}} \cdot T[\Lambda(Q_N x) : \Lambda] \prod_{j=1}^{R} \Big(1 - \frac{1}{N\mathfrak{p}_j}\Big) \\ &\qquad + \theta\Big(\frac{2CSr}{F} \cdot T[\Lambda(Q_N x) : \Lambda]^{1/2} \prod_{j=1}^{R} \Big(1 + \frac{1}{N\mathfrak{p}_j^{1/2}}\Big)\Big) + \theta\Big(\frac{C^2 S}{F} \cdot T 2^R\Big). \end{aligned}$$

By (36), $[k(\xi) : k] = T[\Lambda(Q_N x) : \Lambda] \prod_{j=1}^{R} \big(1 - \frac{1}{N\mathfrak{p}_j}\big)$. Since $r \le r_0$ and

$$\prod_{j=1}^{R} \Big(1 + \frac{1}{N\mathfrak{p}_j^{1/2}}\Big) \le 2^R,$$

we have

$$\begin{aligned} \frac{N\big(\xi, \mathcal{G}_E(a, r)\big)}{[k(\xi) : k]} &= \frac{\operatorname{area} \mathcal{G}(a, r)}{\operatorname{area} \mathcal{F}} + \theta\Big(\frac{C^2 S}{F} \cdot \frac{T 2^R}{[k(\xi) : k]}\Big) \\ &\quad + \theta\bigg(\frac{2CSr_0}{F} \cdot \frac{T^{1/2} 2^R}{\big(\prod_{j=1}^{R} (1 - 1/N\mathfrak{p}_j)\big)^{1/2}} \cdot \frac{1}{[k(\xi) : k]^{1/2}}\bigg). \end{aligned} \tag{39}$$

As before, area $\mathcal{S}(a,r)/\text{area}\,\mathcal{F} = \mu(\mathcal{S}_E(a,r))$. Here $T \le [\mathrm{Gal}(\bar{k}/k) : G_Q]$ is fixed. For each $\varepsilon > 0$ and each sufficiently large N, $2^R \le 2^{\Lambda_K(N)} \le 2^{2\lambda(N)} \le d(N)^2 \le N^{\varepsilon}$. Likewise, $\prod_{j=1}^{R}(1-1/N\mathfrak{p}) \ge \prod_{p\,|\,N}(1-1/p)^2 \ge C/(\log\log N)^2$ for some constant $C > 0$, where the last inequality follows from [Hardy and Wright 1954, Theorem 328, p. 267]. Finally, since ξ has order N and $Q_N \le Q$ is bounded, $[\Lambda(Q_N x) : \Lambda] \ge N/Q$, and so

$$[k(\xi):k] \ \ge\ T\cdot N/Q\cdot C/(\log\log N)^2 \ \ge\ TC/Q\cdot N^{1-\varepsilon} \tag{40}$$

for all large N. Combining these shows that for each $0 < \gamma < 1/2$, the first error term is $\mathbb{O}_\gamma([k(\xi):k]^{-\gamma})$. The same estimates show the second error term is negligible in comparison to the first. This completes the proof when E has complex multiplication. □

Before leaving this section, we note that the arguments above provide lower bounds for the degree $[k(\xi):k]$ in terms of the order N of ξ, as required by (27). When E does not have complex multiplication, then since T is fixed, $Q_N \le Q$, and $\prod_p(1-1/p^2)$ converges to a nonzero limit, (35) shows there is a constant C_1 depending only on E such that

$$[k(\xi):k] \ \ge\ C_1 N^2. \tag{41}$$

When E has complex multiplication, then since T and Q are fixed, (40) shows that there is a constant C_2 depending only on E such that

$$[k(\xi):k] \ \ge\ C_2 N/(\log\log N)^2. \tag{42}$$

3. Context

Theorems 0.1 and 0.2 are the first known cases of general conjectures by the second author (which were refined through conversations with J. Silverman and S. Zhang) concerning dynamical systems and abelian varieties.

As before, let k be a number field, and let S be a finite set of places of k containing the archimedean places. Let $\mathbb{O}_{k,S}$ be the ring of S-integers of k.

Conjecture 3.1 (Su-Ion Ih). *Let $R(x) \in k(x)$ be a rational function of degree at least* 2, *and consider the dynamical system associated to the map $R_* : \mathbb{P}^1 \to \mathbb{P}^1$. Let $\alpha \in \mathbb{P}^1(\bar{k})$ be nonpreperiodic for R_*. Then there are only finitely many preperiodic points $\xi \in \mathbb{P}^1(\bar{k})$ that are S-integral with respect to α, that is, whose Zariski closures in $\mathbb{P}^1/\mathrm{Spec}(\mathbb{O}_{k,S})$ do not meet the Zariski closure of α.*

Conjecture 3.2 (Su-Ion Ih). *Let A/k be an abelian variety, and let $\mathcal{A}_S/\mathrm{Spec}(\mathbb{O}_{k,S})$ be a model of A. Let D be a nonzero effective divisor on A, defined over $\bar{k}$, at least one of whose irreducible components is not the translate of an abelian subvariety by a torsion point, and let $\mathrm{cl}(D)$ be its Zariski closure in $\mathcal{A}_S$. Then the set*

Type of variety	Type of rationality	k	$\bar{k}$
Compact	k,$\bar{k}$-rationality	Mordell–Lang Conjecture	Manin–Mumford Conjecture
Noncompact	$\mathbb{O}_k$,$\overline{\mathbb{Z}}$-rationality	Lang's Conjecture	Ih's Conjecture 3.2

$A_{D,S}(\overline{\mathbb{Z}})_{\mathrm{tors}}$, *consisting of all torsion points of* $A(\bar{k})$ *whose closure in* $\mathscr{A}_S$ *is disjoint from* $\mathrm{cl}(D)$, *is not Zariski dense in* A.

Theorem 0.1 establishes Conjecture 3.1 for the maps $R(x) = x^d$ with $|d| \geq 2$, whose preperiodic points are 0, ∞ and the roots of unity. It is possible to prove the conjecture for Chebyshev maps by similar methods, though we do not do so here.

Theorem 0.2, in addition to being the one-dimensional case of Conjecture 3.2, is equivalent to Conjecture 3.1 for Lattès maps. That is, if E/k is an elliptic curve, let $R \in k(x)$ be the degree 4 map on the x-coordinate corresponding to the doubling map on E, so that the following diagram commutes:

$$\begin{tikzcd}
E \arrow[r, "{[2]}"] \arrow[d, "x"'] & E \arrow[d, "x"] \\
\mathbb{P}^1 \arrow[r, "R_*"] & \mathbb{P}^1
\end{tikzcd}$$

Then $\beta \in E(\bar{k})$ is a torsion point if and only $x(\beta)$ is preperiodic for R_*.

Part of the motivation for Conjecture 3.2 is the following analogy between diophantine theorems over k and $\bar{k}$, and over $\mathbb{O}_k$ and $\overline{\mathbb{Z}}$ (the ring of all algebraic integers). Let A/k be an abelian variety, and let X be a nontorsion subvariety of A (that is, X is not the translate of an abelian subvariety by a torsion point). Recall that the Mordell–Lang Conjecture (proved by Faltings) says that $A(k) \cap X$ is not Zariski dense in X; while the Manin–Mumford Conjecture (first proved by Raynaud) says that $A(\bar{k})_{\mathrm{tors}} \cap X$ is not Zariski dense in X. Likewise, Lang's conjecture (also proved by Faltings) says that if D is an effective ample divisor on A, then the set $A_D(\mathbb{O}_k)$ of $\mathbb{O}_k$-integral points of A not meeting $\mathrm{supp}(D)$ is finite. Note that A is compact, whereas $A_D = A \backslash \mathrm{supp}(D)$ is noncompact.

Conjecture 3.1 is motivated by Conjecture 3.2 and the familiar analogy between torsion points of abelian varieties and preperiodic points of rational maps.

J. Silverman [1993] proved the following result, which is somewhat related to Conjecture 3.1: If the backward orbit of $\alpha \in \mathbb{P}^1(\bar{k})$ under a rational function R of degree ≥ 2 is infinite, then for every $\beta \in \mathbb{P}^1(\bar{k})$, there are only finitely many points in the forward orbit of β under R that are S-integral with respect to α.

More recently, C. Petsche [2007] has proved Conjecture 3.1 under the additional hypothesis that α is "totally Fatou", meaning that for every place v of k and every embedding σ of $\bar{k}$ into $\bar{k}_v$, $\sigma(\alpha)$ is in the v-adic Fatou set of R.

In closing, we note that an important ingredient of the proofs of Theorems 0.1 and 0.2 was a quantitative equidistribution theorem for torsion points. A quantitative equidistribution theorem for points of small height with respect to an arbitrary dynamical system on $\mathbb{P}^1$ has recently been proved by C. Favre and J. Rivera-Letelier [2006, théorème 6].

Acknowledgments

The authors would like to thank the referee for some useful pointers to the literature. The second author would also like to thank J. Silverman and S. Zhang for helping to refine the conjectures in Section 3.

References

[Autissier 2006] P. Autissier, "Sur une question d'équirépartition de nombres algébriques", *C. R. Math. Acad. Sci. Paris* **342**:9 (2006), 639–641. MR 2007b:11163 Zbl pre05045962

[Baker 1975] A. Baker, *Transcendental number theory*, Cambridge University Press, London, 1975. MR 54 #10163 Zbl 0297.10013

[Baker and Hsia 2005] M. H. Baker and L.-C. Hsia, "Canonical heights, transfinite diameters, and polynomial dynamics", *J. Reine Angew. Math.* **585** (2005), 61–92. MR 2006i:11071 Zbl 1071.11040

[Bang 1886] A. S. Bang, "Taltheoretiske undersøgelser", *Zeuthen Tidskr.* **4** (1886), 70–80, 130–137. JFM 19.0168.02

[Bilu 1997] Y. Bilu, "Limit distribution of small points on algebraic tori", *Duke Math. J.* **89**:3 (1997), 465–476. MR 98m:11067 Zbl 0918.11035

[Chambert-Loir 2006] A. Chambert-Loir, "Mesures et équidistribution sur les espaces de Berkovich", *J. Reine Angew. Math.* **595** (2006), 215–235. MR 2008b:14040 Zbl 05039459

[Cheon and Hahn 1999] J. Cheon and S. Hahn, "The orders of the reductions of a point in the Mordell–Weil group of an elliptic curve", *Acta Arith.* **88**:3 (1999), 219–222. MR 2000i:11084 Zbl 0933.11029

[Conway 1973] J. B. Conway, *Functions of one complex variable*, Graduate Texts in Mathematics **11**, Springer, New York, 1973. MR 56 #5843 Zbl 0277.30001

[David and Hirata-Kohno 2002] S. David and N. Hirata-Kohno, "Recent progress on linear forms in elliptic logarithms", pp. 26–37 in *A panorama of number theory or the view from Baker's garden* (Zürich, 1999), edited by G. Wüstholz, Cambridge Univ. Press, Cambridge, 2002. MR 2004e:11076 Zbl 1041.11053

[Everest and Fhlathúin 1996] G. R. Everest and B. N. Fhlathúin, "The elliptic Mahler measure", *Math. Proc. Cambridge Philos. Soc.* **120**:1 (1996), 13–25. MR 97e:11064 Zbl 0865.11068

[Everest and Ward 1999] G. Everest and T. Ward, *Heights of polynomials and entropy in algebraic dynamics*, Universitext, Springer, London, 1999. MR 2000e:11087 Zbl 0919.11064

[Favre and Rivera-Letelier 2006] C. Favre and J. Rivera-Letelier, “Équidistribution quantitative des points de petite hauteur sur la droite projective”, *Math. Ann.* **335**:2 (2006), 311–361. MR 2007g:11074 Zbl pre05035986

[Hardy and Wright 1954] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 3rd ed., Clarendon Press, Oxford, 1954. MR 16,673c Zbl 0058.03301

[Lang 1973] S. Lang, *Elliptic functions*, Addison-Wesley, Reading, MA, 1973. MR 53 #13117 Zbl 0316.14001

[Petsche 2007] C. Petsche, “S-integral preperiodic points for dynamical systems over number fields”, preprint, 2007. arXiv 0709.3879v2

[Rumely 1989] R. S. Rumely, *Capacity theory on algebraic curves*, Lecture Notes in Mathematics **1378**, Springer, Berlin, 1989. MR 91b:14018 Zbl 0679.14012

[Scanlon 1999] T. Scanlon, “The conjecture of Tate and Voloch on p-adic proximity to torsion”, *Internat. Math. Res. Notices* 17 (1999), 909–914. MR 2000i:11100 Zbl 0986.11038

[Schinzel 1974] A. Schinzel, “Primitive divisors of the expression $A^n - B^n$ in algebraic number fields”, *J. Reine Angew. Math.* **268/269** (1974), 27–33. MR 49 #8961 Zbl 0287.12014

[Serre 1972] J.-P. Serre, “Propriétés galoisiennes des points d’ordre fini des courbes elliptiques”, *Invent. Math.* **15**:4 (1972), 259–331. MR 52 #8126 Zbl 0235.14012

[Shimura 1971] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan **11**, Iwanami Shoten, Tokyo, 1971. MR 47 #3318 Zbl 0221.10029

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986. MR 87g:11070 Zbl 0585.14026

[Silverman 1993] J. H. Silverman, “Integer points, Diophantine approximation, and iteration of rational maps”, *Duke Math. J.* **71**:3 (1993), 793–829. MR 95e:11070 Zbl 0811.11052

[Silverman 1994] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, New York, 1994. MR 96b:11074 Zbl 0911.14015

[Silverman 1995] J. H. Silverman, “Exceptional units and numbers of small Mahler measure”, *Experiment. Math.* **4**:1 (1995), 69–83. MR 96j:11150 Zbl 0851.11064

[Szpiro and Tucker 2005] L. Szpiro and T. Tucker, “Equidistribution and generalized Mahler measures”, preprint, 2005. arXiv math/0510404v3

[Szpiro, Ullmo and Zhang 1997] L. Szpiro, E. Ullmo, and S. Zhang, “Équirépartition des petits points”, *Invent. Math.* **127**:2 (1997), 337–347. MR 98i:14027 Zbl 0991.11035

[Ullmo 1995] E. Ullmo, “Points entiers, points de torsion et amplitude arithmétique”, *Amer. J. Math.* **117**:4 (1995), 1039–1055. MR 96j:14016 Zbl 0863.14016

Communicated by Karl Rubin
Received 2007-10-29 Revised 2008-01-11 Accepted 2008-01-11

mbaker@math.gatech.edu *School of Mathematics, Georgia Institute of Technology,*
Atlanta, Georgia 30332-0160, United States

ih@math.colorado.edu *Department of Mathematics, University of Colorado at*
Boulder, Campus Box 395, Boulder, CO 80309-0395,
United States

rr@math.uga.edu *Department of Mathematics, University of Georgia,*
Athens, Georgia 30602-0002, United States

Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the Submission page at the ANT website.

Originality. Submission of a manuscript acknowledges that the manuscript is original and and is not, in whole or in part, published or under consideration for publication elsewhere. It is understood also that the manuscript will not be submitted elsewhere while under consideration for publication in this journal.

Language. Articles in ANT are usually in English, but articles written in other languages are welcome.

Required items. A brief abstract of about 150 words or less must be included. It should be self-contained and not make any reference to the bibliography. If the article is not in English, two versions of the abstract must be included, one in the language of the article and one in English. Also required are keywords and subject classifications for the article, and, for each author, postal address, affiliation (if appropriate), and email address.

Format. Authors are encouraged to use LaTeX but submissions in other varieties of TeX, and exceptionally in other formats, are acceptable. Initial uploads should be in PDF format; after the refereeing process we will ask you to submit all source material.

References. Bibliographical references should be complete, including article titles and page ranges. All references in the bibliography should be cited in the text. The use of BibTeX is preferred but not required. Tags will be converted to the house format, however, for submission you may use the format of your choice. Links will be provided to all literature with known web locations and authors are encouraged to provide their own links in addition to those supplied in the editorial process.

Figures. Figures must be of publication quality. After acceptance, you will need to submit the original source files in vector graphics format for all diagrams in your manuscript: vector EPS or vector PDF files are the most useful.

Most drawing and graphing packages (Mathematica, Adobe Illustrator, Corel Draw, MATLAB, etc.) allow the user to save files in one of these formats. Make sure that what you are saving is vector graphics and not a bitmap. If you need help, please write to graphics@mathscipub.org with details about how your graphics were generated.

White Space. Forced line breaks or page breaks should not be inserted in the document. There is no point in your trying to optimize line and page breaks in the original manuscript. The manuscript will be reformatted to use the journal's preferred fonts and layout.

Proofs. Page proofs will be made available to authors (or to the designated corresponding author) at a Web site in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.

Algebra & Number Theory

Volume 2 No. 2 2008

1937-0652(2008)2:2;1-E