COMPOSITIO MATHEMATICA

# Integral division points on curves

David Grant and Su-Ion Ih

Compositio Math. **149** (2013), 2011–2035.

doi:10.1112/S0010437X13007318

Compositio Math. 149 (2013) 2011–2035
doi:10.1112/S0010437X13007318

# Integral division points on curves

David Grant and Su-Ion Ih

*Dedicated to Wolfgang M. Schmidt on his 80th birthday*

Abstract

Let $k$ be a number field with algebraic closure $\overline{k}$, and let $S$ be a finite set of primes of $k$ containing all the infinite ones. Let $E/k$ be an elliptic curve, $\Gamma_0$ be a finitely generated subgroup of $E(\overline{k})$, and $\Gamma \subseteq E(\overline{k})$ the division group attached to $\Gamma_0$. Fix an effective divisor $D$ of $E$ with support containing either: (i) at least two points whose difference is not torsion; or (ii) at least one point not in $\Gamma$. We prove that the set of 'integral division points on $E(\overline{k})$', i.e., the set of points of $\Gamma$ which are $S$-integral on $E$ relative to $D$, is finite. We also prove the $\mathbb{G}_{\mathrm{m}}$-analogue of this theorem, thereby establishing the 1-dimensional case of a general conjecture we pose on integral division points on semi-abelian varieties.

## 1. Introduction

We will state a general conjecture about integral points on semi-abelian varieties, explain its genesis, and then describe what part of the conjecture we can prove. First we need some preliminaries.

Let $k$ be a number field with algebraic closure $\overline{k}$, and ring of integers $\mathcal{O}_k$. Let $S$ be a finite set of primes of $k$ including all the infinite ones, $\mathcal{O}_{k,S}$ be the ring of $S$-integers of $k$, and $\overline{\mathcal{O}}_{k,S}$ be the integral closure of $\mathcal{O}_{k,S}$ in $\overline{k}$. When we refer to a variety defined over $k$ we mean a separated and geometrically integral scheme of finite type over $k$. We follow [Voj87] for the following definitions.

Let $X$ be a complete variety defined over $k$, and $\mathcal{X}$ an $\mathcal{O}_k$-integral model of $X/k$ (so coming equipped with a $k$-isomorphism of its generic fibre with $X$). Let $T$ be any closed subset of $X$, and $\mathrm{cl}(T)$ be its Zariski closure in $\mathcal{X}$.

Take $P \in X(\overline{k})$, and suppose $\mathrm{cl}(\{P\})$ does not meet $\mathrm{cl}(T)$ on $\mathcal{X}$ outside the fibers over the elements of $S$. Then we say $P$ is *$S$-integral relative to $T$*, or for short, that $P$ is *$(T, S)$-integral* (on $X$). This notion depends of course on the choice of $\mathcal{X}$, but since the only property of $(T, S)$-integral points we will be considering in Conjecture 1.1 below (when they are Zariski non-dense for all sufficiently large $S$) is independent of the choice of $\mathcal{X}$, we will employ a standard abuse of notation that suppresses this choice and write

$$X_T(\overline{\mathcal{O}}_{k,S}) := \{\text{all } (T, S)\text{-integral points of } X(\overline{k})\}.$$

More generally, if $X$ is any variety defined over $k$, we embed it into a completion $\overline{X}$, and identify $X$ as a dense open subset of $\overline{X}$. Let $\partial X := \overline{X} - X$. Let $T$ be any subset of $\overline{X}$ (in particular, $T$ can be any subset of $X$), and let $\overline{T}$ be its Zariski closure in $\overline{X}$. For any $P \in X(\overline{k})$, we say it is *$S$-integral relative to $T$*, or *$(T, S)$-integral*, on $X$, if it is $(\overline{T} \cup \partial X, S)$-integral on $\overline{X}$.

Received 30 October 2011, accepted in final form 20 November 2012, published online 9 September 2013.
*2010 Mathematics Subject Classification* 11G05, 11G35, 11G50, 14G05, 37P05 (primary), 37P35 (secondary).
*Keywords:* division group, division point, integral point, primitive divisor, Schinzel's theorem, Siegel's theorem.

As above, the veracity of our results in this paper is independent of the choice of $\overline{X}$, so by a similar abuse of notation, we write

$$\begin{aligned} X_T(\overline{\mathcal{O}}_{k,S}) &:= \{\text{all } (T,S)\text{-integral points of } X(\overline{k})\} \\ &= \overline{X}_{\overline{T} \cup \partial X}(\overline{\mathcal{O}}_{k,S}). \end{aligned}$$

We will usually be interested in $S$-integral points in the case that $T = \operatorname{Supp} D$ for some effective divisor $D$ of $X$, in which case we write $X_D(\overline{\mathcal{O}}_{k,S}) := X_{\operatorname{Supp} D}(\overline{\mathcal{O}}_{k,S})$, and say its elements are $S$-integral relative to $D$, or are $(D,S)$-integral points of $X$. In general, we define $X_T(\mathcal{O}_{k,S}) := X_T(\overline{\mathcal{O}}_{k,S}) \cap X(k)$.

Let $A$ be a semi-abelian variety defined over $k$. Let $\Gamma_0$ be a finitely generated subgroup of $A(\overline{k})$, and let $\Gamma \subseteq A(\overline{k})$ be the division group of $\Gamma_0$, i.e.,

$$\Gamma := \{P \in A(\overline{k}) : nP \in \Gamma_0 \text{ for some integer } n \geqslant 1\}.$$

The elements of $\Gamma$ are called the *division points* of $\Gamma_0$, or simply *division points*, if the choice of $\Gamma_0$ is clear from context. We will call an arbitrary subgroup of $A(\overline{k})$ a *division group* if it is the division group of some finitely generated $\Gamma_0$.

DEFINITION. Let $A/k$ be a semi-abelian variety.

(i) For any point $P$ of $A(\overline{k})$, the *translate* of a divisor $D$ of $A$ by $P$ is the divisor obtained from $D$ by translating each irreducible component of $D$ by $P$ (without changing multiplicities).

(ii) A *torsion divisor* of $A$ is a divisor of $A$ each of whose irreducible components is a torsion subvariety, i.e., is the translate of a semi-abelian subvariety by a torsion point.

We now propose the following conjecture.

CONJECTURE 1.1. Keep $k$ and $S$ as above. Let $A/k$ be a semi-abelian variety, and let $\Gamma$ be a division group in $A(\overline{k})$. Suppose that $D$ is a non-zero effective divisor on $A$ which is not the translate of any torsion divisor by any point of $\Gamma$. Then the set

$$A_D(\overline{\mathcal{O}}_{k,S})_\Gamma := \{P \in \Gamma : P \text{ is } S\text{-integral relative to } D\}$$

is not Zariski dense in $A$.

*Remarks.* (i) Note that to establish the conjecture, it suffices to do so after enlarging $S$ or extending $k$. In particular, as noted above, the veracity of the conjecture is independent of the choice of completion $\overline{A}$ of $A$ or the choice of integral model for $\overline{A}$.

(ii) Enlarging $S$ if necessary, we can assume that $A$ extends to a group scheme over $\mathcal{O}_{k,S}$. Then since $\Gamma_0$ is finitely generated, we can further enlarge $S$ if necessary to guarantee that every point of $\Gamma$ is $S$-integral relative to $\partial A$. Hence the veracity of the conjecture will be unaffected if we replace $A_D(\overline{\mathcal{O}}_{k,S})_\Gamma = \overline{A}_{\overline{\operatorname{Supp} D} \cup \partial A}(\overline{\mathcal{O}}_{k,S}) \cap \Gamma$ by $\overline{A}_{\overline{\operatorname{Supp} D}}(\overline{\mathcal{O}}_{k,S}) \cap \Gamma$ in the statement of the conjecture.

When $\Gamma_0$ is the trivial subgroup of $A(\overline{k})$, $\Gamma$ is equal to $A(\overline{k})_{\mathrm{tor}}$, the torsion subgroup of $A$, and hence in this special case the conjecture reduces to [BIR08, Conjecture 3.2] on $S$-integrality of torsion points. Conjecture 1.1 grew out of an attempt to understand what the analogue for integral points should be for a conjecture of Lang for division points on abelian varieties.

This is best explained in a chart, in which Conjecture 1.1 could naturally be expected to fit into the lower right corner.

| Variety type | Type of rationality | $k$ | $\overline{k}$ |
|---|---|---|---|
| Compact | $k$, $\overline{k}$-rationality | Faltings's theorem<br>Mordell–Lang Conj. | McQuillan's theorem<br>Lang's Div. Point Conj. |
| Noncompact | $\mathcal{O}_{k,S}$, $\overline{\mathcal{O}}_{k,S}$-integrality | Faltings's theorem<br>Lang's Int. Point Conj. | Conjecture 1.1 |

For the moment, let $A/k$ be an abelian variety, let $\Gamma$ be as above, and let $X/k$ be a closed subvariety of $A$.

The Mordell–Lang conjecture, proved by Faltings, says that $X(k)$ is a finite union of translates by points in $A(k)$ of the $k$-rational points of abelian subvarieties of $A$. In other words, $X(k)$ is not Zariski dense in $X$ if $X$ is not a translate of an abelian subvariety of $A$ by a point in $A(k)$ (see [Fal91, Theorem 1] and also [Fal94, Theorem 4.2]). Lang's division point conjecture, proved by McQuillan, says that $X(\overline{k}) \cap \Gamma$ is a finite union of translates by points in $\Gamma$ of the points in $\Gamma$ on abelian subvarieties of $A$. In other words, $X(\overline{k}) \cap \Gamma$ is not Zariski dense in $X$ if $X$ is not a translate of an abelian subvariety of $A$ by a point of $\Gamma$. (McQuillan actually proved this for semi-abelian varieties, see [Mcq95].) For a general survey, see [HS00].

The integral point conjecture of Lang, also proved by Faltings, says that if $D$ is an effective ample divisor on $A$, then the set $A_D(\mathcal{O}_{k,S})$ of $\mathcal{O}_{k,S}$-integral points of $A$ relative to $D$ is finite [Fal91, Corollary 6.2]. We also note that Vojta proved a generalization of this result for $\mathcal{O}_{k,S}$-integral points on semi-abelian varieties, see [Voj99].

The goal in this paper is to prove Conjecture 1.1 for 1-dimensional semi-abelian varieties, which is to say, for elliptic curves and 1-dimensional tori. Taking a finite extension of $k$, we can assume such a torus is actually the multiplicative group $\mathbb{G}_{\mathrm{m}}$. Let us now unravel the above definitions to see what the conjecture says in these cases.

*Example* 1.2. (i) In the case that $A = \mathbb{G}_{\mathrm{m}}$, every irreducible divisor is of the form $(\alpha)$ for some $\alpha \in \overline{k}^{\times}$, so is the translate of the torsion divisor $(1)$ by $\alpha$. Likewise, for any $\alpha_1, \alpha_2 \in \overline{k}^{\times}$, the divisor $(\alpha_1) + (\alpha_2)$ is the translate of a torsion divisor $\Leftrightarrow \alpha_1/\alpha_2$ is a root of unity. So to say that a non-zero effective divisor $D$ is not the translate of a torsion divisor by a point of $\Gamma$ is to say that $\mathrm{Supp}(D)$ contains either a point not in $\Gamma$ or at least two points whose quotient is not a root of unity.

Note that $\Gamma_0$ will always be a subgroup of $\mathcal{O}_{k,S}^{\times}$, the unit group of $\mathcal{O}_{k,S}$, for some $k$ and $S$. Conversely, for any $k$ and $S$, since $\mathcal{O}_{k,S}^{\times}$ is finitely generated by Dirchlet's unit theorem, we can take $\Gamma_0$ to be any subgroup of any $\mathcal{O}_{k,S}^{\times}$.

(ii) In the case that $A$ is an elliptic curve $E$ with identity $O$, every irreducible divisor is of the form $(Q)$ for some $Q \in E(\overline{k})$, so is the translate of the torsion divisor $(O)$ by $Q$. Likewise, for any $Q_1, Q_2 \in E(\overline{k})$, $(Q_1) + (Q_2)$ is a translate of a torsion divisor $\Leftrightarrow Q_1 - Q_2$ is torsion. So to say that a non-zero effective divisor $D$ is not the translate of a torsion divisor by a point of $\Gamma$ is to say that $\mathrm{Supp}(D)$ either contains a point not in $\Gamma$ or contains at least two points whose difference is not a torsion point.

Note that $\Gamma_0$ will always be a subgroup of $E(k)$ for some $k$, and conversely, since for any $k$, $E(k)$ is finitely generated by the Mordell–Weil theorem, we can take $\Gamma_0$ to be any subgroup of any $E(k)$.

The main result of the paper is the following theorem.

Theorem 1.3. *Let $k$ be a number field with algebraic closure $\overline{k}$, and let $S$ be a finite set of primes of $k$ containing all the infinite ones. Let $G$ be $\mathbb{G}_\mathrm{m}/k$ (respectively an elliptic curve $E/k$), and let $\Gamma$ be a division group in $G(\overline{k})$. Let $D$ be an effective divisor on $G$. Suppose that either of the following two conditions holds:*

(i) $\mathrm{Supp}(D)$ *contains at least two points whose quotient (respectively difference) is not an element of $G(\overline{k})_{\mathrm{tor}}$, i.e., is not a torsion point of $G(\overline{k})$;*

(ii) $\mathrm{Supp}(D)$ *contains at least one point not in $\Gamma$.*

*Then the set*

$$G_D(\overline{\mathcal{O}}_{k,S})_\Gamma := \{\xi \in \Gamma : \xi \text{ is } S\text{-integral relative to } D\}$$

*is finite, i.e., there are only finitely many points in $\Gamma$ which are $S$-integral on $G$ relative to $D$.*

*Remark.* Note that if $\Gamma_0$ is the trivial subgroup of $G$, we have $\Gamma = G(\overline{k})_{\mathrm{tor}}$, and the second case of the theorem implies the main theorems (Theorem 0.1/0.2) of [BIR08]. Our proof is independent of this previous result, so should be considered as a new and more general (and to our minds simpler) proof of the earlier result. In addition, we can see the necessity of the hypotheses in our theorem, since they are needed in the case $\Gamma_0$ is the trivial group, as shown by example in (A) on p. 219 and (A) on p. 230 of [BIR08].

The proof for $\mathbb{G}_\mathrm{m}$ is given in the next section. The proof for elliptic curves, given in § 3, very much depends on whether the curves have complex multiplication (CM) or not.

In the proofs, we first use Kummer theory for $\mathbb{G}_\mathrm{m}$ and its elliptic curve analogue due to Bashmakov. We then exploit theorems on the Galois groups generated by roots of unity and their elliptic analogues due to CM theory and to Serre. We then apply the theory of primitive divisors (based on linear forms in logarithms) due to Schinzel, Silverman, and Stewart, and the elliptic curve analogues due to Cheon–Hahn, Silverman, and Streng. These steps reduce the theorem to Siegel's fundamental theorems on the finiteness of $S$-integral points over a number field on $\mathbb{P}^1$ relative to three distinct points and on an elliptic curve relative to one point. In contrast to Siegel's theorem, which is about integral points over a number field, we emphasize that Theorem 1.3 is about integral points over $\overline{k}$.

Because it fits in well with the overall theme of this paper, we include in § 4 an additional conjecture on a dynamical system analogue to Conjecture 1.1. It generalizes a previous related one, [BIR08, Conjecture 3.1].

## 2. The case of $\mathbb{G}_\mathrm{m}$

We first gather some preliminary results and establish some notation. For any integer $n \geqslant 1$, let $\mu_n$ be the set of all the $n$th-roots of unity, and let $\mu_\infty := \bigcup_{n\geqslant 1} \mu_n$ be the set of all roots of unity. We let $\phi(n)$ denote the Euler totient function.

Let $k$ be a number field, $\overline{k}$ an algebraic closure of $k$, and $\mathrm{Gal}(\overline{k}/k)$ the Galois group of $\overline{k}$ over $k$. If $S$ is a set upon which $\mathrm{Gal}(\overline{k}/k)$ acts, we will say $s_1$ and $s_2$ in $S$ are *$k$-Galois conjugate* if there is a $\sigma \in \mathrm{Gal}(\overline{k}/k)$ such that $s_2 = \sigma(s_1)$.

For a divisor $D = \sum_i m_i(x_i)$ on $\mathbb{G}_\mathrm{m}/k$, $x_i \in \mathbb{G}_\mathrm{m}(k)$, we let $[n]_*D = \sum_i m_i(x_i^n)$.



 https://doi.org/10.1112/S0010437X13007318

### 2.1 Galois action on $\mathbb{G}_{\mathbf{m}}$

Let $k$ be a number field with algebraic closure $\overline{k}$, and let $S$ be a finite set of primes of $k$ containing all the infinite ones. We call a point $P \in \mathcal{O}_{k,S}^{\times}$ *indivisible* (in $\mathcal{O}_{k,S}^{\times}$) if it is not an $n$th-power of any point in $\mathcal{O}_{k,S}^{\times}$ for any integer $n \geqslant 2$. Note that indivisible points cannot be roots of unity.

*Remark.* Note this definition is more restrictive than another definition of indivisibility found in the literature, i.e. that $P$ is indivisible if for any $Q \in \mathcal{O}_{k,S}^{\times}$, if $P = Q^m$ for some $m \in \mathbb{Z}$, then $Q = P^n$ for some $n \in \mathbb{Z}$. We take our definition so that indivisible points cannot be torsion.

The following is stated in [Lan78].

PROPOSITION 2.1. *Keep notation as above. There is a bound $C$, depending only on $k$ and $S$, such that if $P \in \mathcal{O}_{k,S}^{\times}$ is an indivisible point, then for any positive integers $\ell$ and $m$, the Galois group of $k(\mu_{m\ell}, P^{1/m})/k(\mu_{m\ell})$ can be identified with a subgroup of $\mathbb{Z}/m\mathbb{Z}$ of index bounded by $C$.*

The following is a restatement of the fact that an open subgroup of $(\widehat{\mathbb{Z}})^{\times} = \varprojlim(\mathbb{Z}/n\mathbb{Z})^{\times} = \mathrm{Gal}(\mathbb{Q}(\mu_\infty)/\mathbb{Q})$ contains a basic open subgroup.

LEMMA 2.2. *Let $k$ be a number field. The Galois group of $k(\mu_\infty)/k$ is an open subgroup of $\widehat{\mathbb{Z}}^{\times}$, so contains a subgroup $J$ of finite index of the form*

$$J = \prod_{p \notin T} \mathbb{Z}_p^{\times} \times \prod_{p \in T} (1 + p^{c_p}\mathbb{Z}_p),$$

*where $T$ is a finite set of prime numbers and the $c_p$ ($p \in T$) are positive integers.*

We will once and for all make a choice of $J$ for each number field $k$ so that $J$ will be a function of $k$.

### 2.2 Primitive divisors on $\mathbb{G}_{\mathbf{m}}$

We state a fundamental theorem of Schinzel, which has been subsequently strengthened by Stewart and then by Silverman, and which will be used later in this section.

PROPOSITION 2.3 (Schinzel [Sch74]). *Let $k$ be a number field, and let $S$ be a finite set of primes of $k$ including the infinite ones. Then there is an effectively computable constant integer $n_0 = n_0(k, S)$, such that for all $n \geqslant n_0$ and all $S$-units $u$ in $k - \mu_\infty$, $\Phi_n(1, u)$ is not an $S$-unit, where $\Phi_n$ is the $n$th-homogeneous cyclotomic polynomial.*

*Proof.* Every $S$-unit $u$ in $k$ defines a principal fractional ideal $(u)$, which has well-defined integral ideal numerator $\mathfrak{n}$ and denominator $\mathfrak{m}$ which are coprime. Note that $\mathfrak{n}$ and $\mathfrak{m}$ are in the same ideal class. By assumption, the support of $\mathfrak{n}$ and $\mathfrak{m}$ consists only of primes in $S$, so if $h$ is the class number of $k$, there is an ideal $\mathfrak{a}$ of the form $\prod_{\mathfrak{p} \in S_{\mathrm{fin}}} \mathfrak{p}^{h_\mathfrak{p}}$ $(0 \leqslant h_\mathfrak{p} < h)$, where $S_{\mathrm{fin}}$ is the set of finite primes in $S$, such that $\mathfrak{n}\mathfrak{a}$ and $\mathfrak{m}\mathfrak{a}$ are principal integral ideals.

So we can write $u = B_0/A_0$, where $A_0$ and $B_0$ are algebraic integers in $k$ which are also $S$-units, and the greatest common divisor ideal of $A_0$ and $B_0$ has norm bounded in terms of $k$ and $S$. Now let $C$ be an integer that generates the principle ideal $\prod_{\mathfrak{p} \in S_{\mathrm{fin}}} \mathfrak{p}^h$, and set $A = A_0 C$ and $B = B_0 C$. Then $A$ and $B$ are divisible by every prime in $S_{\mathrm{fin}}$, the greatest common divisor ideal of $A$ and $B$ has norm bounded in terms of $k$ and $S$, and

$$u = B/A.$$

We now note that Schinzel's theorem [Sch74, Corollary 1] says that there is a bound $n_0 = n_0([\mathbb{Q}(u):\mathbb{Q}], S) = n_0(k, S)$ such that for all $n \geqslant n_0$, $A^n - B^n$ has a primitive divisor, i.e., is divisible by a (non-zero) prime ideal $\mathfrak{P}$ in $\mathcal{O}_k$ which does not divide $A^m - B^m$ for any $1 \leqslant m < n$. Since we have taken $A$ and $B$ divisible by every finite prime in $S$, it follows that for any $n \geqslant n_0$, $A^n - B^n$ is divisible by a primitive divisor $\mathfrak{P}$ not in $S$. So $\mathfrak{P}$ divides $\Phi_d(A, B)$ for some positive $d|n$. If $d < n$, then $\mathfrak{P}$ divides $A^d - B^d$, violating that $\mathfrak{P}$ is a primitive divisor. So in fact $\mathfrak{P}$ divides $\Phi_n(A, B)$, so $\Phi_n(A, B)$ is not an $S$-unit. Since $A$ is an $S$-unit, this means that $\Phi_n(1, u) = \Phi_n(1, B/A) = A^{-\phi(n)}\Phi_n(A, B)$ is not an $S$-unit, giving the bound on $n$. □

### 2.3 Integrality of division points under power maps

We will need a simple lemma based on the use of the $S$-unit equation (see [EGST88] and [ESS02]).

LEMMA 2.4. *Let $k$ be a number field with algebraic closure $\overline{k}$, and let $S$ be a finite set of primes of $k$ containing all the infinite ones. Let $\Gamma$ be a division group in $\mathbb{G}_{\mathrm{m}}(\overline{k})$.*

(i) *Suppose $\alpha, \beta \in \mathcal{O}_{k,S}^{\times}$ and $\alpha/\beta$ is not a root of unity. Then the set*

$$U_1 = \{(\gamma, t) \in (\Gamma \cap \mathcal{O}_{k,S}^{\times}) \times \mathbb{Z} : \gamma \in \mathbb{G}_{\mathrm{m},(\alpha^t)+(\beta^t)}(\mathcal{O}_{k,S})\}$$

*is finite.*

(ii) *For any $\alpha \in \mathcal{O}_{k,S}^{\times} - \Gamma$, the set*

$$U_2 = \{(\gamma, t) \in (\Gamma \cap \mathcal{O}_{k,S}^{\times}) \times \mathbb{Z} : \gamma \in \mathbb{G}_{\mathrm{m},(\alpha^t)}(\mathcal{O}_{k,S})\}$$

*is finite.*

*Proof.* The $k$-rational points on $\mathbb{G}_{\mathrm{m}}$ integral with respect to (1) can be identified with the (finite) set $U$ of $k$-rational points in $\mathbb{P}^1$ which are $S$-integral relative to $(0) + (1) + (\infty)$. Indeed for any $x \in U$, both $x$ and $1 - x$ are $S$-units in $k$, and the theory of the famed $S$-unit equation says there are only finitely many such $x$.

(i) It suffices to show that the (well-defined) map $f_1 : U_1 \to U \times U$, defined by

$$f_1(\gamma, t) = (\gamma/\alpha^t, \gamma/\beta^t),$$

is injective. Suppose $f_1(\gamma_1, t_1) = f_1(\gamma_2, t_2)$. Eliminating $\gamma_1$ and $\gamma_2$ from the resulting equations gives $(\alpha/\beta)^{t_1 - t_2} = 1$, and since $\alpha/\beta$ is not a root of unity, we then have $t_1 = t_2$. It follows that $\gamma_1 = \gamma_2$ and that $f_1$ is injective.

(ii) It suffices to show that the (well-defined) map $f_2 : U_2 \to U$, defined by

$$f_2(\gamma, t) = \gamma/\alpha^t,$$

is injective. Suppose $f_2(\gamma_1, t_1) = f_2(\gamma_2, t_2)$. Then $\gamma_1/\alpha^{t_1} = \gamma_2/\alpha^{t_2}$, and so $\alpha^{t_1 - t_2} = \gamma_1/\gamma_2 \in \Gamma$. If $t_1 \neq t_2$, we would have $\alpha \in \Gamma$, so $t_1 = t_2$ and $\gamma_1 = \gamma_2$, so $f_2$ is injective. □

### 2.4 Proof of the main theorem for $\mathbb{G}_{\mathrm{m}}$

Now we are ready to prove Theorem 1.3 for $\mathbb{G}_{\mathrm{m}}$. For convenience, we restate the main theorem adapted to this case.

THEOREM 2.5 (Rephrasing of Theorem 1.3 for $\mathbb{G}_{\mathrm{m}}$). *Let $k$ be a number field with algebraic closure $\overline{k}$, $S$ a finite set of primes of $k$ containing all the infinite ones, $\Gamma$ a division group in $\mathbb{G}_{\mathrm{m}}(\overline{k})$, and $D$ an effective divisor on $\mathbb{G}_{\mathrm{m}}$. Suppose that either of the following two conditions holds.*

(i) (The 'two-point case'.) $\mathrm{Supp}(D)$ *contains at least two points whose quotient is not a root of unity.*

(ii) (The 'one-point case'.) $\mathrm{Supp}(D)$ *contains at least one point not in $\Gamma$.*

*Then the set*

$$\mathbb{G}_{\mathrm{m},D}(\overline{\mathcal{O}}_{k,S})_\Gamma := \{\xi \in \Gamma : \xi \text{ is } S\text{-integral relative to } D\}$$

*is finite, i.e., there are only finitely many points in $\Gamma$ which are $S$-integral on $\mathbb{G}_\mathrm{m}$ relative to $D$.*

*Proof.* Since removing points from the support of $D$ only makes the problem harder, we can enlarge $k$ and $S$ if necessary, so that without loss of generality we may assume the following is satisfied:

(I) in the two-point case, that $D = (\alpha) + (\beta)$, where $\alpha, \beta \in \mathcal{O}_{k,S}^\times$, and $\alpha/\beta$ is not a root of unity;

(II) in the one-point case, that $D = (\alpha)$ with $\alpha \in \mathcal{O}_{k,S}^\times$ and $\alpha \notin \Gamma$;

(III) $\Gamma_0 \subseteq \mathcal{O}_{k,S}^\times$.

Note that with this expansion of $S$, all the elements of $\Gamma_0$ and $\Gamma$ are $S$-integral on $\mathbb{P}^1$ relative to the divisor $(0) + (\infty)$.

Now take $x \in \Gamma$, and assume that $x$ is $S$-integral on $\mathbb{G}_\mathrm{m}$ relative to a divisor $D$ as in (I) for the two-point case, and as in (II) for the one-point case. Or equivalently, that $x$ is $S$-integral on $\mathbb{P}^1$ relative to the divisor $(0) + (\infty) + D$.

We will principally make use of two facts. The first is that all the Galois conjugates of $x$ under the action of $\mathrm{Gal}(\overline{k}/k)$ are also $S$-integral on $\mathbb{G}_\mathrm{m}$ relative to $D$, and the second is as follows.

($*$) If $n \geqslant 1$ is an integer, and $x\nu$ is $S$-integral on $\mathbb{G}_\mathrm{m}$ relative to $D$ for all $\nu \in \mu_n$, then $x^n$ is $S$-integral on $\mathbb{G}_\mathrm{m}$ relative to $[n]_* D$.

Let $m$ be the minimal positive integer such that $(\zeta x)^m \in \mathcal{O}_{k,S}^\times$ for some root of unity $\zeta$, and set

$$y = \zeta x.$$

Then if $\Gamma'$ is the division group of $\mathcal{O}_{k,S}^\times$, it follows that $y \in \Gamma'$ and that $m$ is the order of $x$ as an element in $\Gamma'/(\mu_\infty \mathcal{O}_{k,S}^\times)$. Note that $\zeta \in \Gamma$, so $y$ is actually an element of $\Gamma$.

We want to look at the action on $y$ of $\mathrm{Gal}(k(\zeta, \mu_m, y)/k(\zeta, \mu_m))$, the Galois group of $k(\zeta, \mu_m, y)$ over $k(\zeta, \mu_m)$. Proposition 2.1 will give us the required information. Indeed, write

$$y^m = P_0^n$$

for some integer $n \geqslant 0$ and some $P_0 \in \mathcal{O}_{k,S}^\times$ which is indivisible in $\mathcal{O}_{k,S}^\times$. (If $x$ is a root of unity, then we can take $y = 1$ and $m = 1$. In this case, $n = 0$ and we choose $P_0$ to be any (necessarily non-root-of-unity) indivisible point in $\mathcal{O}_{k,S}^\times$. Note that the assumptions (I) and (II) above enable us to find such a point $P_0$.) Then clearly $k(\mu_m, y) \subseteq k(\mu_m, P_0^{1/m})$, where $P_0^{1/m}$ denotes any choice of an $m$th root of $P_0$, but in fact the reverse inclusion holds as well. For if $d > 1$ divides $m$ and $n$, then $y^{m/d}/P_0^{n/d} \in \mu_d$. If we choose $\nu_1 \in \mu_\infty$ with $\nu_1^{m/d} = y^{m/d}/P_0^{n/d}$ and write $\nu_2 = \zeta/\nu_1$, then $(x\nu_2)^{m/d} = (x\zeta/\nu_1)^{m/d} = (y/\nu_1)^{m/d} = P_0^{n/d} \in \mathcal{O}_{k,S}^\times$, i.e., the order of $x\nu_2$ (and hence also of $x$) in $\Gamma'/(\mu_\infty \mathcal{O}_{k,S}^\times)$ is $\leqslant m/d < m$, violating the minimality of $m$. Hence $m$ and $n$ are relatively prime, and there are integers $a$ and $b$ such that $am + bn = 1$. So $P_0 = (P_0^a)^m (P_0^n)^b = (P_0^a)^m (y^m)^b = (P_0^a y^b)^m$. Since $P_0 \in \mathcal{O}_{k,S}^\times \subset k$, this gives the reverse inclusion and

$$k(\mu_m, y) = k(\mu_m, P_0^{1/m}).$$

Let $\ell$ be the order of $\zeta$. The number of $k(\zeta, \mu_m)$-Galois conjugates of $y$ is at least as big as the number of $k(\mu_{m\ell})$-Galois conjugates of $y$, which is the number of $k(\mu_{m\ell})$-Galois conjugates of $P_0^{1/m}$. By Proposition 2.1 this is bounded below by $m/C$ for some bound $C$ depending only on $k$ and $S$, so independent of the choice of $x$. Hence there is a positive divisor $r$ of $m$, with

$$r \geqslant m/C,$$

such that the set of the $k(\zeta, \mu_m)$-Galois conjugates of $y$ includes $y\mu$ for all $\mu \in \mu_r$. Hence the set of the $k$-Galois conjugates of $x$ includes $x\mu$ for all $\mu \in \mu_r$, and each of these conjugates is $S$-integral on $\mathbb{G}_{\mathrm{m}}$ relative to $D$. Hence by $(*)$, we have that $x^r$ is $S$-integral on $\mathbb{G}_{\mathrm{m}}$ relative to the divisor $[r]_*D$. Now let

$$L = k\biggl(\bigcup_{1\leqslant c\leqslant C} (\mathcal{O}_{k,S}^{\times})^{1/c}\biggr),$$

a finite extension of $k$, where $(\mathcal{O}_{k,S}^{\times})^{1/c}$ denotes all the $c$th roots of the elements of $\mathcal{O}_{k,S}^{\times}$. Thus we have

$$x^r = \zeta' z,$$

where $\zeta' = \zeta^{-r}$ is a root of unity and $z = y^r$ is an $S$-unit in $L$.

We now want to look at the action of $\mathrm{Gal}(L(\zeta', z)/L(z))$ on $\zeta'$. We apply Lemma 2.2 with $k = L$, and let $J$, $T$, and the $c_p$ be as given in the lemma. Now let $M$ be the fixed subfield of $L(\mu_\infty)$ under $J$, which is a finite extension of $L$ depending only on our choice of $J$, so independent of our choice of $x$.

We can decompose $\zeta' = \prod_p u_p$ ($p$ running over the set of all prime numbers), where $u_p$ is a primitive $(p^{d_p})$th-root of unity for some $d_p \geqslant 0$. It follows that for every $p \in T$, $u_p$ has Galois conjugates under the action of the elements of $J$ fixing all the $u_q$ (for a prime $q$ different from $p$) and $z$, which are equal to itself times any $(p^{\max(d_p - c_p, 0)})$th-root of unity. Hence $x^r$ has Galois conjugates under $J$ that are equal to itself times any element of $\mu_s$, where

$$s := \prod_{p\in T} p^{\max(d_p - c_p, 0)}.$$

Let

$$t = rs.$$

Thus again by $(*)$, $x^t = x^{rs}$ is $S$-integral on $\mathbb{G}_{\mathrm{m}}$ relative to the divisor $[t]_*D$, and

$$x^t = uv$$

for $u := z^s \prod_{p\in T} u_p^s$ an $S$-unit in $M$ and $v := \prod_{p\notin T} u_p^s$ a primitive $n$th-root of unity, where $n$ is some positive divisor of $\prod_{p\notin T} p^{d_p}$, and $v$ has $\phi(n)$ distinct $M$-Galois conjugates. In addition, note that $u \in \Gamma$ since $x \in \Gamma$ and $v \in \mu_\infty \subset \Gamma$.

Our next goal is to bound $n$. Suppose first we are in the two-point case. Then $x^t$ is an $S$-unit which is $S$-integral relative to $(\alpha^t)$ and $(\beta^t)$. Since $\alpha/\beta$ is not a root of unity, either $u/\alpha^t$ or $u/\beta^t$ is not a root of unity. Reversing the role of $\alpha$ and $\beta$ if necessary, say $u/\alpha^t$ is not a root of unity. Suppose now we are in the one-point case. Then $u/\alpha^t$ is again not a root of unity (or else $\alpha$ would be in $\Gamma$, a contradiction). In either case, we have that the product of the $M$-Galois conjugates of $1 - x^t/\alpha^t$, each one of which is an $S$-unit, is $\Phi_n(1, u/\alpha^t)$ where $\Phi_n$ is the $n$th-homogeneous cyclotomic polynomial, and $n$ is the order of $v$. Since $u/\alpha^t \in M - \mu_\infty$, applying Proposition 2.3 with $k = M$ shows that $n$ is bounded by some constant integer $n_0$ depending only on $M$ and $S$, so is independent of the choice of $x$.

So we get a finite extension $Y$ of $M$,

$$Y := M\biggl(\bigcup_{1\leqslant n< n_0} \mu_n\biggr),$$

such that $x^t$ is an $S$-unit in $Y$ which is $S$-integral on $\mathbb{G}_{\mathrm{m}}$ relative to $[t]_*D$. Applying Lemma 2.4 (part (i) in the two-point case and part (ii) in the one-point case) for $k=Y$, and considering $(x^t,t)$, we get that $t\geqslant 1$ is bounded by some positive constant $B$ that depends only on $Y$, $S$, and $D$, so is independent of the choice of $x$. Since $x^t\in Y$, $x$ is in the finite extension

$$W:=Y\biggl(\bigcup_{1\leqslant b\leqslant B}(\mathcal{O}_{Y,S}^{\times})^{1/b}\biggr)$$

of $Y$. Applying Siegel's theorem on $\mathbb{P}^1$ over $W$, since $x$ is $S$-integral on $\mathbb{P}^1$ relative to the divisor $(0)+(\infty)+D$, there are only finitely many such $x$. □

## 3. The case of elliptic curves

The proof will involve a series of results that are analogues to those used in the previous section, but whose derivations generally require deeper results.

For any positive integer $n$, we let $\phi_2(n)=n^2\prod_{p\mid n}(1-1/p^2)$, where $p$ runs over the set of prime numbers dividing $n$. For any non-zero ideal $\mathfrak{a}$ in the ring of integers $R$ of a number field, we let $\phi(\mathfrak{a})$ denote the order of the unit group of the ring $R/\mathfrak{a}$.

If $E$ is an elliptic curve, then for any $m\in\mathbb{Z}\subset\mathrm{End}(E)$ and any $P\in E(\overline{k})$, we let $mP$ denote the image of $P$ under the multiplication-by-$m$ map. To avoid confusion, if $m\in\mathrm{End}(E)$ and it is not specified that $m$ is in $\mathbb{Z}$, we let $m(P)$ denote the image of $P$ under $m$. In addition, for any $f$ and $g$ in $R=\mathrm{End}(E)$, we write $fg$ for their product when emphasizing the ring structure of $R$ and $f\circ g$ when emphasizing their role as maps.

For a $k$-isogeny $\rho$ mapping an elliptic curve $E/k$ to an elliptic curve $E'/k$ and for a divisor $D=\sum_i m_i(P_i)$ on $E$, $P_i\in E(k)$, we set $[\rho]_*D=\sum_i m_i(\rho(P_i))$. We let $E[\rho]$ denote the points of $E(\overline{k})$ in the kernel of $\rho$.

### 3.1 Galois action on an elliptic curve

Proposition 3.1. *Let $E$ be an elliptic curve defined over a number field $k$. Let*

$$r=\begin{cases}1 & \text{if } E \text{ has complex multiplication over } \overline{k},\\ 2 & \text{otherwise.}\end{cases}$$

*Suppose that $\mathrm{End}(E)$ is the ring of integers $\mathcal{O}_F$ in its fraction field $F$. Then there is a finite set of non-zero primes $T\subset\mathrm{Spec}(\mathcal{O}_F)$, a positive integer $c_{\mathfrak{p}}$ for every $\mathfrak{p}\in T$, and a finite extension $M$ of $k$, such that the Galois group of $M(E(\overline{k})_{\mathrm{tor}})/M$ is of the form*

$$J=\prod_{\mathfrak{p}\in\mathrm{Spec}(\mathcal{O}_F)-T\cup\{(0)\}}\mathrm{GL}_r(\mathcal{O}_{F_{\mathfrak{p}}})\times\prod_{\mathfrak{p}\in T}(1+\mathrm{Norm}_{F/\mathbb{Q}}(\mathfrak{p})^{c_{\mathfrak{p}}}\mathrm{M}_r(\mathcal{O}_{F_{\mathfrak{p}}})),$$

*where $\mathcal{O}_{F_{\mathfrak{p}}}$ is the ring of integers in the completion of $F$ at $\mathfrak{p}$, $\mathrm{M}_r(\mathcal{O}_{F_{\mathfrak{p}}})$ denotes the ring of $r\times r$ matrices with entries from the ring $\mathcal{O}_{F_{\mathfrak{p}}}$, and '1' is the $r\times r$ identity matrix.*

The case $r=1$ ($F$ a quadratic imaginary number field) follows from the theory of complex multiplication (see Theorem 2.8 on p. 101 and the discussion on [Lan83, p. 148]), and the case $r=2$ ($F=\mathbb{Q}$) is a theorem of Serre (see [Ser72, p. 260, (3)]).

We will once and for all make a choice of $J$ for every number field $k$ and elliptic curve $E$ defined over $k$, so that $J$ is a function of $E$ and $k$.

Let $E$ be an elliptic curve defined over a number field $k$. We call a point $P\in E(k)$ *indivisible* (in $E(k)$) if it is not of the form $r(Q)$ for any point $Q$ in $E(k)$ with $r$ a non-unit in the ring $\mathrm{End}_k(E)$.

*Remark.* Note that this definition is more restrictive than another definition of indivisibility found in the literature, e.g., [Hin88, p. 584], where $P$ being indivisible means that if $P = r(Q)$ for some $r$ and $Q$ as above, then there is some $s \in \mathrm{End}_k(E)$ with $Q = s(P)$. We take our definition so that indivisible points cannot be torsion.

Proposition 3.2. *Let $E$ be an elliptic curve defined over a number field $k$, all of whose endomorphisms are defined over $k$. Then there is a bound $C$, depending only on $E$ and $k$, such that if $P \in E(k)$ is an indivisible point, then for any positive integers $\ell$ and $m$, the Galois group of $k(E[\ell m], (1/m)P)/k(E[\ell m])$, where $(1/m)P$ denotes any point of $E(\overline{k})$ in the inverse image of $P$ under multiplication-by-$m$ map, can be identified with a subgroup of $E[m]$ of index bounded by $C$.*

This follows from the discussion in [Lan78], where Lang expounds on the original results of Bashmakov. We have the following corollary.

Corollary 3.3. *Let $E$ be an elliptic curve defined over a number field $k$, with complex multiplication by the ring of integers $\mathcal{O}_F$ of an imaginary quadratic field $F$, all of whose endomorphisms are also defined over $k$. Then there is a bound $C$ depending only on $E$ and $k$ such that if $P \in E(k)$ is an indivisible point, then for any non-zero endomorphisms $\alpha$ and $\beta$ of $E$, the Galois group of $k(E[\alpha\beta], (1/\alpha)P)/k(E[\alpha\beta])$ can be identified with a subgroup of $E[\alpha]$ of index bounded by $C$.*

*Proof.* Set

$$a = \mathrm{Norm}_{F/\mathbb{Q}}(\alpha) \quad \text{and} \quad b = \mathrm{Norm}_{F/\mathbb{Q}}(\beta).$$

The Galois group of $k(E[\alpha\beta], (1/\alpha)P)/k(E[\alpha\beta])$ can be identified with a subgroup of $E[\alpha]$, and contains as a subgroup the Galois group $G_\alpha$ of $k(E[ab], (1/\alpha)P)/k(E[ab])$. Likewise, the Galois group $G_a$ of $k(E[ab], (1/a)P)/k(E[ab])$ can be identified with a subgroup of $E[a]$, and after doing so, $\overline{\alpha}G_a \subseteq G_\alpha$, where $\overline{\alpha}$ denotes the conjugate of $\alpha$. By the previous proposition, $G_a$ is a subgroup of index at most $C$ in $E[a]$, so the same is true of $G_\alpha$ as a subgroup of $E[\alpha]$. □

### 3.2 Primitive divisors on an elliptic curve

The following is a modified statement of the elliptic version of Schinzel's theorem given in the last section, due over the rationals to Silverman [Sil88] and due in general to Cheon and Hahn [CH99].

Proposition 3.4. *Let $E$ be an elliptic curve defined over a number field $k$, and let $S$ be a finite set of primes of $k$ including the infinite ones and the primes of bad reduction for $E$. Then there exists a constant integer $n_0 = n_0(E, k, S)$ such that for any integer $n \geqslant n_0$ and non-torsion point $P \in E(k)$:*

(i) *there is a prime $\mathfrak{p}$ of $k$ not in $S$ such that $P$ reduces to a primitive $n$-torsion point modulo $\mathfrak{p}$; and*

(ii) *$P$ is not $S$-integral relative to all primitive $n$-torsion points of $E$.*

*Proof.* (i) The theorem stated by Cheon and Hahn is that given any non-torsion $P \in E(k)$, there exists an integer $\ell_0$ (depending on $P$) such that for any integer $\ell \geqslant \ell_0$, there is a prime $\mathfrak{p}$ of good reduction such that $P$ reduces to a primitive $\ell$-torsion point modulo $\mathfrak{p}$, and that for all but finitely many $P$, one can take $\ell_0 = 1$. It follows immediately that if one takes $m_0$ to be the maximum of the $\ell_0$ for each of these finitely many exceptional $P$, then for any integer $m \geqslant m_0$ and any non-torsion point $P \in E(k)$, there exists a prime $\mathfrak{p}$ of good reduction such that $P$ reduces to a primitive $m$-torsion point modulo $\mathfrak{p}$. To get the statement we give, i.e., that we can guarantee that $\mathfrak{p}$ is not in any given set $S$, we need only take $n_0$ bigger than $m_0$ and bigger than the order of the group of $\mathcal{O}_k/\mathfrak{q}$-rational points on the reduction of $E$ modulo $\mathfrak{q}$ for every finite prime $\mathfrak{q}$ in $S$ of good reduction.

(ii) To get this statement from (i), it suffices to show that for any prime $\mathfrak{p}$ of good reduction for $E$, the reduction-mod-$\mathfrak{p}$-map from the primitive $n$-torsion points $E[n]^*$ on $E$ to the primitive $n$-torsion points $E_{\mathfrak{p}}[n]^*$ on the reduced curve $E_{\mathfrak{p}}$ $(= E \bmod \mathfrak{p})$ is surjective. This follows from the well-known fact that the reduction map $\rho$ from $E[n]$ to $E_{\mathfrak{p}}[n]$ is surjective, once one notes that $\rho$ maps $E[n] - E[n]^*$ into $E_{\mathfrak{p}}[n] - E_{\mathfrak{p}}[n]^*$. □

This was recently generalized to the case that the elliptic curve has complex multiplication, by Streng in [Str08].

Let $E$ be an elliptic curve defined by a generalized Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with all $a_i$ in the ring of integers $\mathcal{O}_k$ of a number field $k$. For any $P \in E(k)$ of infinite order and any $\alpha \in \mathrm{End}_k(E) - \{0\}$, let $(B_\alpha)^2$ be the denominator ideal in $\mathcal{O}_k$ of $x(\alpha(P))$. Set $B_0 = (0)$. For any non-zero ideal $\mathfrak{a} \subseteq \mathrm{End}_k(E)$, let $B_{\mathfrak{a}} = \sum_{\alpha\in\mathfrak{a}} B_\alpha$. We say a (finite) prime $\mathfrak{q}$ of $\mathcal{O}_k$ is a *primitive divisor* of $B_{\mathfrak{a}}$ if $\mathfrak{q}$ divides $B_{\mathfrak{a}}$ and $\mathfrak{q}$ does not divide $B_{\mathfrak{b}}$ for any ideal $\mathfrak{b}$ with $\mathfrak{a} \nmid \mathfrak{b}$.

Proposition 3.5. *Keep notation as above. Suppose $E$ is an elliptic curve defined over a number field $k$, which has complex multiplication by the ring of integers $\mathcal{O}_F$ of a quadratic imaginary field $F$, and all of whose endomorphisms are defined over $k$.*

(i) *Given a point $P \in E(k)$ of infinite order, define $B_{\mathfrak{a}}$ as above. For all non-zero ideals $\mathfrak{a}$ of $\mathcal{O}_F$, with only finitely many exceptions, $B_{\mathfrak{a}}$ has a primitive divisor. Moreover, for all but finitely many $P \in E(k)$, $B_{\mathfrak{a}}$ has a primitive divisor for all $\mathfrak{a}$.*

(ii) *Furthermore, if $S$ is a finite set of primes of $k$ including the infinite ones and the primes of bad reduction for $E$, then there is a constant integer $n_0 = n_0(E, k, S)$ with the property that for any non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_F$ whose norm is greater than or equal to $n_0$, and any non-torsion point $P \in E(k)$, there is a prime $\mathfrak{p}$ of $k$ not in $S$ such that $P$ reduces to a primitive $\mathfrak{a}$-torsion point modulo $\mathfrak{p}$.*

(iii) *We conclude that for $\mathfrak{a}$ as in (ii) above, $P$ is not $S$-integral relative to all primitive $\mathfrak{a}$-torsion points.*

*Proof.* (i) The first claim is the main theorem in [Str08]. The second claim follows from [Str08, Proposition 1.3], where Streng shows that if the canonical height of $P$ is sufficiently large, then $B_{\mathfrak{a}}$ has a primitive divisor for all $\mathfrak{a}$. Since there are only finitely many points of $E(k)$ of bounded height, the result follows.

(ii) First of all, we take $n_0$ large enough to make sure by (i) that $B_{\mathfrak{a}}$ has a primitive divisor for every non-torsion point $P \in E(k)$.

Next we note that if a prime $\mathfrak{q}$ is a divisor of $B_\alpha$, then $\alpha(P)$ is a point (over the completion $\mathcal{O}_{k_{\mathfrak{q}}} = (\mathcal{O}_k)_{\mathfrak{q}}$ of $\mathcal{O}_k$ at $\mathfrak{q}$) in the formal group $E_0$ at the kernel of reduction of a minimal Weierstrass model $\mathcal{E}$ for $E$ at $\mathfrak{q}$ (whether or not our defining Weierstrass equation is minimal at $\mathfrak{q}$). Let $E_{\mathfrak{q}}$ be the reduction of $\mathcal{E}$ at $\mathfrak{q}$. Therefore if $\mathfrak{q}$ is a primitive divisor of $B_{\mathfrak{a}}$, then for all $\alpha \in \mathfrak{a}$, $\alpha(P)$ is in $E_0(\mathcal{O}_{k_{\mathfrak{q}}})$. Hence so long as $n_0$ is sufficiently large so that the norm of $\mathfrak{a}$ is greater than the order of the group of non-singular points on $E_{\mathfrak{q}}(\mathcal{O}_k/\mathfrak{q})$ for all $\mathfrak{q} \in S_{\mathrm{fin}}$, no primitive divisor of $B_{\mathfrak{a}}$ will be in $S$.

(iii) This comes as in the previous proposition from the fact that the primitive $\mathfrak{a}$-torsion points of $E$ surject modulo any prime of good reduction for $E$ onto the primitive $\mathfrak{a}$-torsion points on the reduced curve. □

### 3.3 Integrality of division points under isogenies

We will need a lemma based on Siegel's theorem, that for an elliptic curve $E$ defined over a number field $k$ and a point $P_0 \in E(k)$, there are only finitely many points in $E(k)$ which are $S$-integral relative to $P_0$, where $S$ is a finite set of primes of $k$ containing all the infinite ones.

Let $k$ be a number field with algebraic closure $\overline{k}$, and let $E$ be an elliptic curve defined over $k$. Let $\Gamma_0$ be a finitely generated subgroup of $E(\overline{k})$, and let $\Gamma$ be the division group attached to $\Gamma_0$. Let $R = \mathrm{End}(E)$. We write $R\Gamma_0$ (respectively, $R\Gamma$) for the $R$-submodule of $E(\overline{k})$ generated by the set $\{\psi(\gamma) \in E(\overline{k}) : \psi \in R \text{ and } \gamma \in \Gamma_0\}$ (respectively, $\{\psi(\gamma) \in E(\overline{k}) : \psi \in R \text{ and } \gamma \in \Gamma\}$). Then we note

$$\begin{aligned} R\Gamma &= \{P \in E(\overline{k}) : \psi(P) \in R\Gamma \text{ for some non-zero } \psi \in R\} \\ &= \{P \in E(\overline{k}) : \psi(P) \in R\Gamma_0 \text{ for some non-zero } \psi \in R\}. \end{aligned}$$

Lemma 3.6. *Let $E$ and $E'$ be elliptic curves defined over a number field $k$. Assume that all the endomorphisms of $E$ and $E'$ are defined over $k$. Let $S$ be a finite set of primes of $k$ containing all the infinite ones and the ones of bad reduction for $E$. Let $\Gamma_0 \subseteq E(\overline{k})$ be a finitely generated subgroup, and $\Gamma$ its division group. Then the following are true.*

(i) *Suppose $\alpha, \beta \in E(k)$ and $\alpha - \beta$ is not a torsion point. Then the set*

$$U_1 = \{(\phi(\gamma), \phi) : \gamma \in \Gamma, \phi \in \mathrm{Hom}_k(E, E'), \text{ and } \phi(\gamma) \in E'_{(\phi(\alpha))+(\phi(\beta))}(\mathcal{O}_{k,S})\}$$

*is finite.*

(ii) *For any $\alpha \in E(k) - R\Gamma$, the set*

$$U_2 = \{(\phi(\gamma), \phi) : \gamma \in \Gamma, \phi \in \mathrm{Hom}_k(E, E'), \text{ and } \phi(\gamma) \in E'_{(\phi(\alpha))}(\mathcal{O}_{k,S})\}$$

*is finite.*

(iii) *For any $\alpha \in E(k) - \Gamma$, the set*

$$U_3 = \{(\phi(\gamma), \phi) : \gamma \in \Gamma, \phi \in \mathrm{Hom}_k(E, E'), \text{ and } \phi(\gamma) \in E'_{(\phi(\alpha))}(\mathcal{O}_{k,S})\}$$

*is finite.*

*Proof.* The lemma is trivial if $E$ and $E'$ are not $k$-isogenous, so we suppose that they are. Let $U = E'_{(O')}(\mathcal{O}_{k,S})$ (a finite set by Siegel's theorem), where $O'$ is the identity element of $E'$.

(i) It suffices to show that the (well-defined) map $f_1 : U_1 \to U \times U$, defined by

$$f_1(\phi(\gamma), \phi) = (\phi(\gamma) - \phi(\alpha), \phi(\gamma) - \phi(\beta)),$$

is injective. Suppose $f_1(\phi_1(\gamma_1), \phi_1) = f_1(\phi_2(\gamma_2), \phi_2)$. Eliminating $\phi_1(\gamma_1)$ and $\phi_2(\gamma_2)$ from the resulting equations gives $(\phi_1 - \phi_2)(\alpha - \beta) = O$, and since $\alpha - \beta$ is not torsion, $\phi_1 = \phi_2$. It follows that $\phi_1(\gamma_1) = \phi_2(\gamma_2)$ and that $f_1$ is injective.

(ii) It suffices to show that the (well-defined) map $f_2 : U_2 \to U$, defined by

$$f_2(\phi(\gamma), \phi) = \phi(\gamma) - \phi(\alpha),$$

is injective. Suppose $f_2(\phi_1(\gamma_1), \phi_1) = f_2(\phi_2(\gamma_2), \phi_2)$. Then $(\phi_1 - \phi_2)(\alpha) = \phi_1(\gamma_1) - \phi_2(\gamma_2)$. Let $\psi$ be any non-zero $k$-isogeny $E' \to E$. Then $\psi \circ \phi_i = r_i \in R$ for some $r_i$, $i = 1, 2$, so $(r_1 - r_2)(\alpha) = r_1(\gamma_1) - r_2(\gamma_2) \in R\Gamma$. Since $\alpha$ is not in $R\Gamma$, we must have $r_1 - r_2 = 0$. Since $\psi \neq 0$, we then have $\phi_1 = \phi_2$. Hence $\phi_1(\gamma_1) = \phi_2(\gamma_2)$, and $f_2$ is injective.

(iii) It suffices to show that the (well-defined) map $f_3 : U_3 \to U$, defined by

$$f_3(\phi(\gamma), \phi) = \phi(\gamma) - \phi(\alpha),$$

is finite-to-one. This is already proved in (ii) if $\Gamma_0$ is an $R$-module (since in that case $R\Gamma = \Gamma$), so assume it is not, hence in particular that $E$ has complex multiplication. The division group of $\Gamma_0$ depends only on a free subgroup which is a complement to the torsion subgroup of $\Gamma_0$, so we can assume $\Gamma_0$ is torsion free as well as not being an $R$-module. Let $R = \mathbb{Z} + \omega\mathbb{Z}$ (an order in an imaginary quadratic field). So $\omega$ is a root of a $\mathbb{Z}$-coefficient equation of the form $x^2 + ex + f$, with discriminant $e^2 - 4f < 0$.

Then $\Gamma_0 \cap \omega(\Gamma_0)$ is a finitely generated free abelian subgroup $M_0$ of $\Gamma_0$ which is an $R$-module. By the structure theorem of finitely generated abelian groups, there is a decomposition $\Gamma_0 = C_0 \oplus B_0$ as the direct sum of free abelian subgroups, where $M_0 \subseteq C_0$, and $C_0/M_0$ is torsion. Note that by construction, $B_0 \cap \omega(B_0) = \{O\}$.

Note that $C_0$ is in the division group of $M_0$, so we can replace $\Gamma_0$ by $M_0 \oplus B_0$ without changing $\Gamma$, and $M_0$ is an $R$-module. Again we can assume that $\Gamma_0$ is not an $R$-module, which implies $B_0 \neq \{O\}$.

We will consider the $R$-module

$$D_0 = (M_0 \oplus B_0) \otimes R = M_0 \oplus (B_0 \otimes R) = M_0 \oplus B_0 \oplus \omega(B_0).$$

Note that the decomposition of

$$\Gamma_0 = M_0 \oplus B_0$$

gives a corresponding (non-direct) sum of $\Gamma$ as $M + B$, the sum of the division groups of $M_0$ and $B_0$. The intersection of $M$ and $B$ consists of all the torsion points. Likewise, the division group $D$ of $D_0$ is

$$M + B + \omega(B),$$

where the intersection of any two summands consists of all the torsion points.

Note (iii) is proved in (ii) if $\alpha$ is not in $R\Gamma$, which equals $D$, so we might as well assume that $\alpha \in R\Gamma$ but not in $\Gamma$. This means for some integer $m$, $m\alpha \in D_0$, but not in $\Gamma_0$. In other words, $m\alpha$ has a non-trivial $\omega(B_0)$-component. Moreover, the truth of the result is invariant under shifting $\alpha$ by a point in $\Gamma$ (we just shift each $\gamma$ as well), so we might as well assume $m\alpha \in \omega(B_0)$, so $\alpha \in \omega(B)$.

Suppose, for a contradiction, that we have an infinite sequence of pairs $(\phi_i(\gamma_i), \phi_i)$, $i \geqslant 0$, which all map under $f_3$ to the same element in $E'(\overline{k})$. Let $\psi$ be any non-zero $k$-isogeny $E' \to E$. Then $\psi \circ \phi_i = t_i \in R$ for some $t_i$ in $R$. Then for any $i > 0$,

$$(t_i - t_0)(\alpha) = t_i(\gamma_i) - t_0(\gamma_0).$$

Write $t_i = a_i + b_i\omega$, $a_i, b_i \in \mathbb{Z}$, and $\gamma_i = \gamma_{i,M} + \gamma_{i,B}$, where $\gamma_{i,M} \in M$ and $\gamma_{i,B} \in B$ (which are only defined up to torsion, but we make fixed choices of $\gamma_{i,M}$ and $\gamma_{i,B}$ for each $\gamma_i$).

Then from the equation above, equating $\omega(B)$- and $B$-components, we have the following, which are equalities up to torsion, i.e.,

$$((a_i - a_0) - e(b_i - b_0))\alpha \equiv b_i\omega(\gamma_{i,B}) - b_0\omega(\gamma_{0,B}) \mod E(\overline{k})_{\mathrm{tor}}$$

and

$$-f(b_i - b_0)\alpha' \equiv a_i\gamma_{i,B} - a_0\gamma_{0,B} \mod E(\overline{k})_{\mathrm{tor}},$$

writing $\alpha = \omega(\alpha')$ for some $\alpha' \in B$. Eliminating $\gamma_{i,B}$, we have the following equality up to torsion

$$(a_i(a_i - a_0) + (fb_i - ea_i)(b_i - b_0))\alpha \equiv (b_i a_0 - b_0 a_i)\omega(\gamma_{0,B}) \mod E(\overline{k})_{\mathrm{tor}}.$$

Let

$$g(a_i, b_i) = a_i(a_i - a_0) + (fb_i - ea_i)(b_i - b_0).$$

There is a positive integer $n$ such that $n\alpha \in \omega(B_0)$ and $n\gamma_{0,B} \in B_0$. Then there is a torsion point $P \in E(k)$ such that

$$g(a_i, b_i)n\alpha = (b_i a_0 - b_0 a_i)\omega(n\gamma_{0,B}) + P,$$

and by our construction of $B_0$, $P = 0$. Since $B_0 \neq \{O\}$ and is free, it is easy to check that $\omega(B_0)$ is non-zero and free, so there is a basis for $\omega(B_0)$ containing some point of infinite order $Q$ such that $n\alpha$ and $n\omega(\gamma_{0,B})$ have with respect to this basis non-zero coordinates $r$ and $s$ at $Q$. So equating $Q$-coordinates we have

$$rg(a_i, b_i) = s(b_i a_0 - b_0 a_i).$$

Note that $r$, $s$, $a_0$, $b_0$, $e$, and $f$ are all fixed, so this equation is a quadratic equation in $a_i$ and $b_i$. Dividing by $r$, we can write it as

$$a_i^2 - e a_i b_i + f b_i^2 + \delta a_i + \epsilon b_i = 0$$

for some fixed rational numbers $\delta$ and $\epsilon$, hence as

$$(a_i - e b_i/2)^2 + (f - e^2/4) b_i^2 + \kappa(a_i - e b_i/2) + (f - e^2/4)\lambda b_i = 0$$

for some fixed rational numbers $\kappa$ and $\lambda$. Completing squares, this equation can be written as

$$(a_i - e b_i/2 + \kappa/2)^2 + (f - e^2/4)(b_i + \lambda/2)^2 = \kappa^2/4 + (f - e^2/4)\lambda^2/4.$$

Since $e^2 - 4f < 0$, the left-hand side is a positive-definite quadratic form, and there are only finitely many solutions for integers $a_i$ and $b_i$. Hence there are only finitely many $t_i$, hence only finitely many $\phi_i$ and $\phi_i(\gamma_i)$, a contradiction, and therefore $f_3$ is finite-to-one as claimed. □

### 3.4 Proof of the main theorem for elliptic curves

We are now ready to prove Theorem 1.3 for elliptic curves. For convenience, we restate the main theorem adapted to this case.

Theorem 3.7 (Rephrasing of Theorem 1.3 for elliptic curves). *Let $k$ be a number field with algebraic closure $\overline{k}$, and let $S$ be a finite set of primes of $k$ containing all the infinite ones. Let $E$ be an elliptic curve defined over $k$, and let $\Gamma$ be a division group in $E(\overline{k})$. Let $D$ be an effective divisor on $E$. Suppose that either of the following two conditions holds.*

(i) (The 'two-point case'.) Supp$(D)$ *contains at least two points whose difference is not a torsion point.*

(ii) (The 'one-point case'.) Supp$(D)$ *contains at least one point not in $\Gamma$.*

*Then the set*

$$E_D(\overline{\mathcal{O}}_{k,S})_\Gamma := \{\xi \in \Gamma : \xi \text{ is } S\text{-integral relative to } D\}$$

*is finite, i.e., there are only finitely many points in $\Gamma$ which are $S$-integral on $E$ relative to $D$.*

The proof of this theorem for all elliptic curves is very similar in structure to the proof for $\mathbb{G}_\mathrm{m}$, though the details are very different depending on whether $E$ does not or does have complex multiplication. At some point in the proof we will consider these cases separately.

*Proof.* Since removing points from the support of $D$ only makes the problem harder, we can enlarge $k$ if necessary, so that without loss of generality we may assume the following is satisfied.

(I) In the two-point case, that $D = (\alpha) + (\beta)$, where $\alpha, \beta \in E(k)$, and $\alpha - \beta$ is not a torsion point of $E$.

(II) In the one-point case, that $D = (\alpha)$ with $\alpha \in E(k)$ and $\alpha \notin \Gamma$.

We fix a Weierstrass equation with coefficients in $\mathcal{O}_k$ for $E/k$, and then likewise, without loss of generality, we can expand $S$ so that it contains all the primes of bad reduction for this equation for $E$.

Now take $x \in \Gamma$, and assume that $x$ is $S$-integral on $E$ relative to a divisor $D$ as in (I) for the two-point case, and as in (II) for the one-point case.

*Case* 1. When $E$ does not have complex multiplication.

We will principally make use of two facts. The first is that all the Galois conjugates of $x$ under the action of $\mathrm{Gal}(\overline{k}/k)$ are also $S$-integral on $E$ relative to $D$, and the second is that since $S$ contains all the primes of bad reduction for $E$,

(∗∗) *if $n \geqslant 1$ is an integer and $x + u$ is $S$-integral on $E$ relative to $D$ for all $u \in E[n]$, then $nx$ is $S$-integral on $E$ relative to $[n]_* D$.*

We let $\Gamma'$ denote the division group of $E(k)$. Let $m$ be the order of $x$ in the group $\Gamma'/(E(k) + E(\overline{k})_{\mathrm{tor}})$. Thus $m$ is the minimal positive integer such that we can write

$$x = y + \nu,$$

with $\nu$ a torsion point, and $y \in \Gamma'$ such that $my \in E(k)$. Hence $y$ as an element of $\Gamma'/E(k)$ has order $m$. Note $y = x - \nu$ actually lies in $\Gamma$.

We want to look at the action of $\mathrm{Gal}(k(\nu, E[m], y)/k(\nu, E[m]))$ on $y$. Write

$$my = nP_0$$

for some integer $n \geqslant 0$ and some $P_0 \in E(k)$ which is indivisible. (If $x$ is torsion, then we can take $y = O$ and $m = 1$. In this case, $n = 0$ and we choose $P_0$ to be any (necessarily non-torsion) indivisible point in $E(k)$. Note that the assumptions (I) and (II) above enable us to find such a point $P_0$.) Then clearly, $k(E[m], y) \subseteq k(E[m], (1/m)P_0)$, but in fact the reverse inclusion holds as well. Indeed, if $d > 1$ divides $m$ and $n$, then $(m/d)y - (n/d)P_0 \in E[d] \subseteq E(\overline{k})_{\mathrm{tor}}$. If we choose $\nu_1 \in E(\overline{k})_{\mathrm{tor}}$ with $(m/d)\nu_1 = (m/d)y - (n/d)P_0$ and write $\nu_2 := \nu + \nu_1 \in E(\overline{k})_{\mathrm{tor}}$, then $(m/d)(x - \nu_2) = (n/d)P_0 \in E(k)$, i.e., the order of $x - \nu_2$ in $\Gamma'/E(k)$ is $\leqslant m/d$, so the order of $x$ in $\Gamma'/(E(k) + E(\overline{k})_{\mathrm{tor}})$ is $\leqslant m/d < m$, violating the minimality of $m$. Hence $m$ and $n$ are relatively prime, and there are integers $a, b$ such that $am + bn = 1$. So $P_0 = m(aP_0) + b(nP_0) = m(aP_0) + b(my) = m(aP_0 + by)$. Since $P_0 \in E(k)$, this gives the reverse inclusion and

$$k(E[m], y) = k\left(E[m], \frac{1}{m}P_0\right).$$

Let $\ell$ be the order of $\nu$. Then the number of $k(\nu, E[m])$-Galois conjugates of $y$ is bounded below by the number of $k(E[\ell m])$-Galois conjugates of $y$, which by the equality above, is the same as the number of $k(E[\ell m])$-Galois conjugates of $(1/m)P_0$. Applying Proposition 3.2 gives that the number of $k(E[\ell m])$-Galois conjugates of $(1/m)P_0$ is bounded below by $m^2/C$ for some bound $C$ depending only on $E$ and $k$. Since all subgroups of $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$ are products of two cyclic groups of order dividing $m$, the above bound implies that there is a positive divisor $r$ of $m$ such that

$$r \geqslant m/C$$

and such that the set of the $k(\nu, E[m])$-Galois conjugates of $y$ includes $y + \mu$ for all $\mu \in E[r]$. Hence the set of the $k$-Galois conjugates of $x$ includes $x + \mu$ for all $\mu \in E[r]$, and each of these Galois conjugates is $S$-integral on $E$ relative to $D$. Hence by (∗∗), $rx$ is $S$-integral on $E$ relative to $[r]_* D$.

Now let

$$L = k\biggl(\bigcup_{1\leqslant a\leqslant C} \frac{1}{a}E(k)\biggr),$$

which is a finite extension of $k$ depending only on $E$ and $k$, so is independent of the choice of $x$. Then, noting that the order of $y$ in $\Gamma'/E(k)$ is $m \leqslant rC$, we have

$$rx = z + \nu',$$

where $z := ry \in E(L)$, and $\nu' := r\nu \in E(\bar{k})_{\mathrm{tor}}$. We now want to look at the action of $\mathrm{Gal}(k(\nu', z)/k(z))$ on $\nu'$. To do so, we apply Proposition 3.1 with $k = L$. (Since in this case $F = \mathbb{Q}$, we will write $p$ instead of $\mathfrak{p}$ to denote a non-zero prime of $\mathcal{O}_F$.) We let $J$, $T$, and $c_p$ be as in the proposition, and let $M$ be the finite extension of $L$ which is the fixed field of $J$, i.e.,

$$M := L\biggl(\bigcup_{p\in T} E[p^{c_p}]\biggr),$$

which depends only on $E$, $L$, and the choice of $J$, so is independent of the choice of $x$. We decompose $\nu'$ into its $p$-primary parts $u_p$ for all primes $p$. Let $p^{d_p}$ $(d_p \geqslant 0)$ be the order of $u_p$, and let

$$s = \prod_{p\in T} p^{\max(d_p - c_p, 0)}.$$

Then there are Galois elements of $J$ which fix the points of $E(L)$, and hence $z$ and all $u_p$ for $p \notin T$, but which map

$$u := \sum_{p\in T} u_p$$

to $u$ plus every element in $E[s]$. Hence these Galois elements map $rx$ to $rx$ plus every element in $E[s]$, and all these Galois conjugates are $S$-integral on $E$ relative to $[r]_*D$. So by $(**)$, if

$$t := rs,$$

then $tx$ is $S$-integral on $E$ relative to $[t]_*D$. Since $su \in E(M)$, $tx$ is the sum of a point

$$P := sz + su$$

in $E(M)$ and a torsion point

$$Q := s(\nu' - u) = s \cdot \sum_{p\notin T} u_p.$$

If $n$ is the order of $Q$, then by the choice of $J$, $Q$ has $\phi_2(n)$-many Galois conjugates over $M$ constituting exactly the primitive $n$-torsion points, so $tx$ has $\phi_2(n)$-many Galois conjugates over $M$, too, each being a shift of $P$ by a primitive $n$-torsion point.

In the two-point case, by assumption, either $t(x - \alpha)$ or $t(x - \beta)$ is not torsion, and renaming if necessary, we can assume $t(x - \alpha)$ is not torsion. In the one-point case, $t(x - \alpha)$ is not torsion, or else $x - \alpha$ would be torsion, putting $\alpha \in \Gamma$, a contradiction, since $\Gamma$ contains all the torsion points of $E$. In either case, we have that $t(x - \alpha)$ is of infinite order, and we have just shown that $t(x - \alpha)$ and all its conjugates are $S$-integral on $E$ relative to $(O)$. Since $t(x - \alpha) = (P - t\alpha) + Q$, it follows that $-(P - t\alpha) \in E(M)$ is non-torsion and $S$-integral on $E$ relative to every primitive $n$-torsion point of $E$. Hence Proposition 3.4, applied with $k := M$, and $P := -(P - t\alpha)$ gives that $n$ (the order of $Q$) is less than some fixed positive integer $n_0$, depending only on $E$, $M$, and $S$, and is hence independent of the choice of $x$.

So adjoining to $M$ all the torsion on $E$ of order at most $n_0$, we get a finite extension $Y$ of $M$, i.e.,

$$Y := M\biggl(\bigcup_{1\leqslant n<n_0} E[n]\biggr),$$

over which $tx$ is rational. We now want to bound $t$. Applying Lemma 3.6 (part (i) in the two-point case, and part (ii) in the one-point case) for $k = Y$, and considering $(tx, t)$, we get that $t$ is less than some bound $B$ that depends only on $E$, $Y$, $S$, and $D$, so is independent of the choice of $x$. Since $tx \in E(Y)$, $x \in E(W)$, where $W$ is the finite extension

$$W := Y\biggl(\bigcup_{1\leqslant b\leqslant B} \frac{1}{b}E(Y)\biggr).$$

Applying Siegel's theorem on $E$ over $W$, since $x$ is $S$-integral on $E$ relative to the divisor $D$, there are only finitely many such $x$.

*Case* 2. When $E$ has complex multiplication.

We start with a lemma.

Lemma 3.8. (i) *If Theorem 3.7 is true for an elliptic curve $E$ defined over $k$, it is true for any elliptic curve $E'$ defined over $k$ which is isogenous to $E$ over $k$.*

(ii) *Every elliptic curve $E$ defined over $k$ with complex multiplication is isogenous over $k$ to an elliptic curve defined over $k$ whose endomorphism ring $R$ over $\overline{k}$ is the ring of integers $\mathcal{O}_F$ of some imaginary quadratic number field $F$.*

*Proof.* (i) Let $\phi : E \to E'$ be a non-zero isogeny over $k$, $\Gamma'$ a division group in $E'(\overline{k})$, and $D'$ an effective divisor on $E'$ containing at least two points in its support whose difference is not torsion, or one point not in $\Gamma'$. Then we have $\phi^{-1}(E'_{D'}(\overline{\mathcal{O}}_{k,S})_{\Gamma'}) \subseteq E_D(\overline{\mathcal{O}}_{k,S})_{\Gamma}$, where $D := \phi^*(D')$ and $\Gamma := \phi^{-1}(\Gamma')$. Since $\phi$ has finite kernel, $\Gamma$ is a division group in $E(\overline{k})$. It is clear that $D$ is an effective divisor which must contain at least two points in its support which do not differ by a torsion point, or one point which is not in $\Gamma$. Thus Theorem 3.7 for $E$ implies Theorem 3.7 for $E'$.

(ii) This is stated in [Sil94, #2.12, p. 180]. □

So in proving the theorem we can assume that

$$\mathrm{End}(E) = R = \mathcal{O}_F,$$

which is to say, a Dedekind Domain.

Without loss of generality, we can assume by extending $k$ if necessary that all the endomorphisms in $R$ are defined over $k$. We let $\Gamma'$ denote the division group of $E(k)$.

Let $x$ be as in the first part of the proof. Again we will principally make use of two facts, the first that all the Galois conjugates of $x$ under the action of $\mathrm{Gal}(\overline{k}/k)$ are also $S$-integral relative to $D$, and the second that since $S$ contains all the primes of bad reduction for $E$,

(∗∗∗) *if $V$ is an ideal in $R$ and $x + u$ is $S$-integral on $E$ relative to $D$ for all $u \in E[V]$, then $\rho(x)$ is $S$-integral on $E_V$ relative to $\rho_*(D)$, where $\rho$ is the natural isogeny from $E$ to $E_V := E/V$.*

There are several things we should note.

(a) The elliptic curve $E_V$ has the same endomorphism ring as $E$, which is to say, $\mathcal{O}_F$.

(b) If we let $\mathcal{E}$ and $\mathcal{E}_V$ denote the Néron models over $\mathcal{O}_{k,S}$ of $E$ and $E_V$, respectively, then since $S$ contains all the primes of bad reduction for $E$ (and hence for $E_V$), $\mathcal{E}$ and $\mathcal{E}_V$ are abelian schemes over $\mathcal{O}_{k,S}$, and $\rho$ extends to an $\mathcal{O}_{k,S}$-isogeny between them. (Note that since we are concerned with $\mathcal{O}_{k,S}$-integral points on $E$ and $E_V$, we can work with $\mathcal{O}_{k,S}$-integral models rather than $\mathcal{O}_k$-integral ones.)

(c) Via these isogenies, we can identify $(E_U)_V$ and $E_{UV}$, and likewise $(\mathcal{E}_U)_V$ and $\mathcal{E}_{UV}$, for any two non-zero ideals $U, V$ in $\mathcal{O}_F$.

(d) If $V$ and $V'$ are in the same ideal class, there are $\alpha, \alpha' \in \mathcal{O}_F - \{0\}$ such that $\alpha V = \alpha' V'$ that induce $k$-isomorphisms $E_V \cong E_{\alpha V} = E_{\alpha' V'} \cong E_{V'}$, which extend to an $\mathcal{O}_{k,S}$-isomorphism between $\mathcal{E}_V$ and $\mathcal{E}_{V'}$.

(e) We will fix once and for all a set of representatives $\mathfrak{a}_i$, $1 \leqslant i \leqslant h$, for the $h$ distinct ideal classes of $\mathcal{O}_F$, and will set $E_i = E_{\mathfrak{a}_i}$, and $\mathcal{E}_i = \mathcal{E}_{\mathfrak{a}_i}$. For each non-zero ideal $U$ of $\mathcal{O}_F$, there is a unique $i$ such that $\mathfrak{a}_i$ is in the same ideal class as $U$, and we will denote this by $i = \lambda(U)$. Let $\eta_U$ be a fixed $k$-isomorphism from $E_U$ to $E_i$ as described in (d).

We let $I_x$ denote the (necessarily non-zero) annihilator ideal of $x$ in $\Gamma'/(E(k) + E(\bar{k})_{\mathrm{tor}})$. Let

$$m \in I_x - \{0\}$$

be an element of minimal norm (so $\operatorname{Norm}_{F/\mathbb{Q}}(m)/\operatorname{Norm}_{F/\mathbb{Q}}(I_x)$ is bounded by the Minkowski bound $B$ for $F$, equal to $(2/\pi)\sqrt{|\mathrm{disc}(\mathcal{O}_F)|}$.) Then

$$m(x) = z + \mu$$

for some $z \in E(k)$ and $\mu \in E(\bar{k})_{\mathrm{tor}}$, so picking any $y \in E(\bar{k})$ with

$$m(y) = z,$$

we have

$$\nu := x - y \in E(\bar{k})_{\mathrm{tor}},$$

so $y = x - \nu \in \Gamma$. Let $J_y$ be the annihilator ideal of $y$ in $\Gamma'/E(k)$. Then we have $(m) \subseteq J_y \subseteq I_x$. Moreover, for any $y' \in \Gamma'$ with $x - y'$ being torsion, and for any $m' \in R - \{0\}$ with $m'(y') \in E(k)$, we also have $(m') \subseteq J_{y'} \subseteq I_x$, so

$$\operatorname{Norm}_{F/\mathbb{Q}}(m') \geqslant \operatorname{Norm}_{F/\mathbb{Q}}(m)$$

by the minimality of the choice of $m$.

We want to look at the action of $\mathrm{Gal}(k(\nu, E[J_y], y)/k(\nu, E[J_y]))$ on $y$. Note

$$z = \sigma(z_0)$$

for some non-torsion indivisible $z_0 \in E(k)$ and some $\sigma \in R$. (If $x$ is torsion, we can take $y = z = O$ and $m = 1$. In this case, $\sigma = 0$ and we choose $z_0$ to be any (necessarily non-torsion) indivisible point in $E(k)$. Note that the assumptions (I) and (II) above obtained by enlarging $k$ enable us to find such a point $z_0$.) We have information on Galois conjugates of $(1/m)z_0$ coming from Corollary 3.3 which we want to exploit to understand the $k(\nu, E[J_y])$-Galois conjugates of $y$.

For this we consider the ideal $I = (\sigma, m) \neq (0)$, which we claim has bounded norm, so in this sense $\sigma$ and $m$ can be regarded as being '*almost relatively prime*'. Let $I'$ be an ideal of minimal norm in the ideal class of $I$, hence of norm bounded by $B$. Then

$$I'/I = (\beta)$$

for some $\beta \in F^{\times}$. By assumption, $\sigma\beta = \sigma'$ and $m\beta = m'$ for some $\sigma' \in R$ and some $m' \in R - \{0\}$. One checks that $m'(y) - \sigma'(z_0)$ is annihilated by any element of $I$, so is torsion in $E[I]$. So there is a torsion point $\nu'$ such that $m'(y - \nu') \in E(k)$. By the minimality of the norm of $m$, $\operatorname{Norm}_{F/\mathbb{Q}}(m) \leqslant \operatorname{Norm}_{F/\mathbb{Q}}(m')$, so $\operatorname{Norm}_{F/\mathbb{Q}}(\beta) \geqslant 1$. Then, by the choice of $I'$, we must have $\operatorname{Norm}_{F/\mathbb{Q}}(I) = \operatorname{Norm}_{F/\mathbb{Q}}(I')$, so

$$\operatorname{Norm}_{F/\mathbb{Q}}(I) \leqslant B,$$

establishing our claim.

Let $\ell \in R - \{0\}$ annihilate $\nu$. From $m(y) = \sigma(z_0)$ we have,

$$k(E[\ell m], y) \subseteq k\bigg(E[\ell m], \frac{1}{m}(z_0)\bigg),$$

and the reverse is 'almost true' in the following sense: let $\delta \in I - \{0\}$ have norm bounded by $B \cdot \operatorname{Norm}_{F/\mathbb{Q}}(I) \leqslant B^2$. Then $\delta = am + b\sigma$ for some $a, b \in R$. It follows that $\delta(z_0) = am(z_0) + b\sigma(z_0) = m(a(z_0) + b(y))$, and so

$$k\bigg(E[\ell m], \frac{1}{m}\delta(z_0)\bigg) \subseteq k(E[\ell m], y) \subseteq k\bigg(E[\ell m], \frac{1}{m}(z_0)\bigg).$$

Hence if $Z$ is the Galois group of $k(E[\ell m], (1/m)(z_0))$ over $k(E[\ell m])$ identified as a subgroup of $E[m]$, the Galois group $H$ of $k(E[\ell m], y)$ over $k(E[\ell m])$ contains $\delta Z$. By Corollary 3.3, there is a constant $C_0$ independent of $\ell$ and $m$ (and hence $x$) such that $|Z| \geqslant C_0 \cdot \operatorname{Norm}_{F/\mathbb{Q}}(m)$. It follows that $H$ is a subgroup of $E[m]$ of index bounded by the constant $C_1 = C_0 B^2$, depending only on $E$ and $k$.

Write $R = \mathbb{Z} \oplus \omega\mathbb{Z}$. Then $\omega H$ is also of index in $E[m]$ bounded by some constant $C_2$ depending only on $E$ and $k$ (because $\omega H \subseteq \omega E[m]$ is of index bounded by $C_1$, and the index of $\omega E[m]$ in $E[m]$ is bounded by $\operatorname{Norm}_{F/\mathbb{Q}}(\omega)$). Therefore $(H + \omega H)/\omega H$ is a finite group of order bounded by $C_2$, so the same is true of the isomorphic group $H/(H \cap \omega H)$. So $H \cap \omega H$ is of index in $E[m]$ bounded by $C_3 = C_1 C_2$, and is an $R$-module. Hence there is an ideal $U$ of $R$, with $m \in U$ and

$$\operatorname{Norm}_{F/\mathbb{Q}}(m)/\operatorname{Norm}_{F/\mathbb{Q}}(U) \leqslant C_3, \tag{1}$$

such that

$$E[U] \subseteq \operatorname{Gal}(k(E[\ell m], y)/k(E[\ell m])).$$

Now let $\rho : E \to E_U$ be the natural projection, which is an isogeny of degree $\operatorname{Norm}_{F/\mathbb{Q}}(U)$. Then since $U$ divides $(m)$, $\rho$ is a factor of $m : E \to E$, i.e., $m = \psi \circ \rho$ for some other non-zero isogeny $\psi : E_U \to E$, of degree bounded by $C_3$ by (1). If $\widehat{\psi}$ is the dual isogeny of $\psi$, then $\psi \circ \widehat{\psi} = [\deg(\psi)]$, an endomorphism of $E$. Therefore if $y' = \rho(y) \in E_U(\overline{k})$, then $y'$ is actually defined over $k((1/\deg(\psi))E(k))$.

Recalling that $\ell \in R - \{0\}$ annihilates $\nu$, by Corollary 3.3, the $k(E[\ell m])$-Galois conjugates of $y$ include those of the form $y$ plus every element of $E[U]$, hence the $k$-Galois conjugates of $x$ include those of the form $x$ plus every element of $E[U]$.

Now let

$$L = k\bigg(\bigcup_{1 \leqslant a \leqslant C_3} \frac{1}{a} E(k)\bigg),$$

which is a finite extension of $k$, depending only on $E$ and $k$, so independent of the choice of $x$. Then recalling that $x = y + \nu$, we know from $(*{*}*)$ that

$$\rho(x) = y' + \nu'$$

is $S$-integral on $E_U$ relative to $(\rho(\alpha))+(\rho(\beta))$, where $y'\in E_U(L)$ and $\nu':=\rho(\nu)\in E_U(\overline{k})_{\mathrm{tor}}$. Let $i=\lambda(U)$.

We now apply Proposition 3.1 with $k=L$ and $E=E_i$. Let $J$, $T$ and $c_{\mathfrak{p}}$ for $\mathfrak{p}\in T$ be as in Proposition 3.1, where we can take $M_i$ (denoted by $M$ in Proposition 3.1) to be the finite extension of $L$ generated by the $E_i[\mathfrak{p}^{c_{\mathfrak{p}}}]$ for all $\mathfrak{p}$ in $T$, i.e.,

$$M_i=L\biggl(\bigcup_{\mathfrak{p}\in T}E_i[\mathfrak{p}^{c_{\mathfrak{p}}}]\biggr).$$

Decompose $\nu'$ into its $\mathfrak{p}$-primary parts $u_{\mathfrak{p}}$ for all non-zero prime ideals $\mathfrak{p}\subset R$. Let $\mathfrak{p}^{d_{\mathfrak{p}}}$ be the order (ideal) of $u_{\mathfrak{p}}$ ($d_{\mathfrak{p}}\geqslant 0$), and let

$$\mathfrak{s}=\prod_{\mathfrak{p}\in T}\mathfrak{p}^{\max(d_{\mathfrak{p}}-c_{\mathfrak{p}},0)}.$$

Then there are Galois elements of $J$ which fix the points of $E_i(L)$, and hence via $\eta_U^{-1}$ they fix $y'$ and all $u_{\mathfrak{p}}$ for $\mathfrak{p}\notin T$, but which map

$$u:=\sum_{\mathfrak{p}\in T}u_{\mathfrak{p}}$$

to $u$ plus every element in $E_U[\mathfrak{s}]$. Hence these Galois elements map $\rho(x)$ to $\rho(x)$ plus every element in $E_U[\mathfrak{s}]$, and all these Galois conjugates are $S$-integral on $E_U$ relative to $(\rho(\alpha))+(\rho(\beta))$. Let $j=\lambda(U\mathfrak{s})$, so $E_j$ is isomorphic to $E_{U\mathfrak{s}}$ via $\eta_{U\mathfrak{s}}$. So by $(***)$ with $E:=E_U$ and $V:=\mathfrak{s}$, if

$$\psi:E_U\to(E_U)_{\mathfrak{s}}$$

is the natural projection, then $\psi(\rho(x))$ is $S$-integral on $E_{U\mathfrak{s}}$ relative to $(\psi(\rho(\alpha)))+(\psi(\rho(\beta)))$. Then $\psi(u)\in E_{U\mathfrak{s}}(M_i)$, so $\psi(\rho(x))$ is the sum of a point

$$P:=\psi(y')+\psi(u)$$

in $E_{U\mathfrak{s}}(M_i)$, and a torsion point

$$Q:=\psi(\nu'-u)=\psi\biggl(\sum_{\mathfrak{p}\notin T}u_{\mathfrak{p}}\biggr).$$

Note that $\sum_{\mathfrak{p}\notin T}u_{\mathfrak{p}}$ has some order (ideal) $\mathfrak{n}$ which has $\phi(\mathfrak{n})$-many Galois conjugates over $M_i$, constituting exactly the primitive $\mathfrak{n}$-torsion points of $E_U$. Since $\mathfrak{n}$ is prime to $\mathfrak{s}$, $Q$ also has $\phi(\mathfrak{n})$-many Galois conjugates over $M_i$, constituting exactly the primitive $\mathfrak{n}$-torsion points of $E_{U\mathfrak{s}}$. So $\psi(\rho(x))$ has $\phi(\mathfrak{n})$-many Galois conjugates over $M_i$, too, consisting of $P$ shifted by the primitive $\mathfrak{n}$-torsion points of $E_{U\mathfrak{s}}$.

Now in the two-point case, either $\psi(\rho(x-\alpha))$ or $\psi(\rho(x-\beta))$ is not torsion in $E_{U\mathfrak{s}}(\overline{k})$, hence renaming $\alpha$ and $\beta$ if necessary, we can assume that $\psi(\rho(x-\alpha))$ is not torsion. In the one-point case, $\psi(\rho(x-\alpha))$ cannot be torsion, or else $x-\alpha$ would be torsion, putting $\alpha\in\Gamma$, a contradiction. In any case, we can apply Proposition 3.5(iii) with $k=M_i$ to $E_{U\mathfrak{s}}$. Note $\psi(\rho(x-\alpha))=(P-\psi(\rho(\alpha)))+Q$. Thus, since $\psi(\rho(x-\alpha))$ and all its Galois conjugates are $S$-integral on $E_{U\mathfrak{s}}$ relative to the origin on $E_{U\mathfrak{s}}$ and $S$ contains all the primes of bad reduction for $E_{U\mathfrak{s}}$, it follows that $-(P-\psi(\rho(\alpha)))$ is a point of infinite order in $E_{U\mathfrak{s}}(M_i)$ which is $S$-integral relative to all the primitive $\mathfrak{n}$-torsion points on $E_{U\mathfrak{s}}$. So via $\eta_{U\mathfrak{s}}$ we get $(n_0)_{ij}$, a bound on the norm of $\mathfrak{n}$ (the order ideal of $Q$) by the proposition. Since there are only $h$ choices for $i$ and $j$, we can set $n_0$ to be the maximum of $(n_0)_{ij}$ over all $i$ and $j$.

Let $M$ be the compositum of all the $M_i$ over $1 \leqslant i \leqslant h$. Hence we get a finite extension $Y$ of $M$,

$$Y := M\Bigg(\bigcup_{\substack{\mathfrak{n}\neq(0),\text{ an ideal of } R\\ \mathrm{Norm}_{F/\mathbb{Q}}(\mathfrak{n})\leqslant n_0, 1\leqslant j\leqslant h}} E_j[\mathfrak{n}]\Bigg),$$

over which $\psi(\rho(x))$ is rational. Note that $Y$ depends only on $E$ and $M$ so is independent of the choice of $x$. We now want to bound the degree of

$$\tau := \eta_{U_{\mathfrak{s}}} \circ \psi \circ \rho.$$

We have $\tau \in \mathrm{Hom}_k(E, E_j)$ for some $1 \leqslant j \leqslant h$, so we can apply Lemma 3.6 for each $1 \leqslant j \leqslant h$ and $E' = E_j$ (part (i) in the two-point case, and part (iii) in the one-point case), and considering $(\tau(x), \tau)$, bound the degree of $\tau$ by some positive integer $C$ that depends only on $E$, $Y$, $D$, and $\Gamma_0$, so is independent of the choice of $x$.

Since $\tau(x) \in E_j(Y)$, $x \in E(W)$, where $W$ is the finite extension

$$W := Y\Bigg(\bigcup_{\substack{\tau\in\mathrm{Hom}_k(E,E_j)\\ \deg\tau\leqslant C,\ 1\leqslant j\leqslant h}} \tau^{-1}(E_j(Y))\Bigg)$$

of $Y$. Applying Siegel's theorem on $E$ over $W$, since $x$ is $S$-integral on $E$ relative to the divisor $D$, there are only finitely many such $x$. □

When $\Gamma_0$ is an $R$-module, its division group $\Gamma$ is an $R$-module, and is the '$R$-division group of $\Gamma_0$'. Therefore we have the following theorem.

THEOREM 3.9. *Let $k$ be a number field with algebraic closure $\overline{k}$, and let $S$ be a finite set of primes of $k$ containing all the infinite ones. Let $E$ be an elliptic curve defined over $k$. Let $\Gamma_0$ be a finitely generated* $\mathrm{End}(E)$*-submodule of $E(\overline{k})$, and let*

$$\Gamma = \{\xi \in E(\overline{k}) : \lambda(\xi) \in \Gamma_0 \text{ for some non-zero } \lambda \in \mathrm{End}(E)\}.$$

*Let $D$ be an effective divisor on $E$. Suppose that either of the following two conditions holds:*

(i) $\mathrm{Supp}(D)$ *contains at least two points whose difference is not an element of $E(\overline{k})_{\mathrm{tor}}$, i.e., is not a torsion point of $E(\overline{k})$;*

(ii) $\mathrm{Supp}(D)$ *contains at least one point not in $\Gamma$.*

*Then the set*

$$E_D(\overline{\mathcal{O}}_{k,S})_\Gamma := \{\xi \in \Gamma : \xi \text{ is } S\text{-integral relative to } D\}$$

*is finite, i.e., there are only finitely many points in $\Gamma$ which are $S$-integral on $E$ relative to $D$.*

## 4. The case of dynamical systems

### 4.1 The formulation of a dynamical system analogue conjecture

We start by recalling case (ii) of Theorem 1.3: for any $\alpha \in \mathbb{G}_{\mathrm{m}}(\overline{k}) - \Gamma$,

$$\#(\mathbb{G}_{\mathrm{m},(\alpha)}(\overline{\mathcal{O}}_{k,S}) \cap \Gamma) < \infty,$$

i.e., there are only finitely many points in $\Gamma$ which are $S$-integral on $\mathbb{G}_{\mathrm{m}}$ relative to $\alpha \in \overline{k}^{\times} - \Gamma$.

In order to consider a dynamical system analogue of this result for $\mathbb{P}^1$, we fix throughout choices of

$\varphi$: a $k$-morphism $\mathbb{P}^1 \to \mathbb{P}^1$, of finite degree $\geqslant 2$, and

$Q_0$: a point in $\mathbb{P}^1(k)$.

Definition. We define the following:

$$[\varphi] = \{\phi : \mathbb{P}^1 \to \mathbb{P}^1 : \phi \text{ is a } k\text{-morphism of finite degree } \geqslant 2 \text{ such that } \phi \circ \varphi = \varphi \circ \phi\};$$
$$\Gamma_0 = \bigcup_{\phi \in [\varphi]} \phi^+(Q_0);$$

and

$$\Gamma = \left(\bigcup_{\phi \in [\varphi]} \phi^-(\Gamma_0)\right) \cup \mathbb{P}^1(\overline{k})_{\varphi\text{-preper}},$$

where for $\phi \in [\varphi]$ and any subset $Y$ of $\mathbb{P}^1(\overline{k})$, $\phi^+(Y)$ and $\phi^-(Y)$ denote respectively the forward and backward orbits under $\phi$, that is:

$$\phi^0 := \text{identity};$$
$$\phi^n := \phi \circ \cdots \circ \phi \quad (n \geqslant 1 \text{ times});$$
$$\phi^{-n}(Y) := (\phi^n)^{-1}(Y);$$
$$\phi^+(Y) := \bigcup_{n \geqslant 0} \phi^n(Y);$$

and

$$\phi^-(Y) := \bigcup_{n \geqslant 0} \phi^{-n}(Y).$$

Here also $\mathbb{P}^1(\overline{k})_{\varphi\text{-preper}}$ denotes the $\varphi$-preperiodic points on $\mathbb{P}^1(\overline{k})$, that is, those points whose forward orbits are finite sets. For background materials on arithmetical dynamical systems, see [Sil07].

We now propose a dynamical system analogue to Theorem 1.3.

Conjecture 4.1. Keep the notation as above. If $Q \in \mathbb{P}^1(\overline{k}) - \Gamma$, then

$$\#(\mathbb{P}^1_{(Q)}(\overline{\mathcal{O}}_{k,S}) \cap \Gamma) < \infty,$$

i.e., there are only finitely many points in $\Gamma$ which are $S$-integral on $\mathbb{P}^1$ relative to $Q$.

Some related results can be found in [BIR08, Ih11a, Ih11b, IT10, Pet08], and [Soo10].

### 4.2 Some comments on the case of dynamical systems

(i) Conjecture 4.1 can be modified by changing the definition of $[\varphi]$. In other words, according to one's taste, $[\varphi]$ can be enlarged or shrunk in various ways (and consequently, $\Gamma_0$ and $\Gamma$ would be, too). For example, it would be interesting to define $[\varphi]$ to be any interesting nonempty subset of the following first set, especially its three subsequent subsets below:

$$\begin{aligned}
&\big\{\phi:\mathbb{P}^1\to\mathbb{P}^1 : \phi \text{ is a } k\text{-morphism of finite degree } \geqslant 2 \text{ such that } \langle\varphi,\phi\rangle=0\big\}\\
&\supset\left\{\phi:\mathbb{P}^1\to\mathbb{P}^1 : \begin{array}{l}\phi \text{ is a } k\text{-morphism of finite degree } \geqslant 2 \text{ such that for some } n\geqslant 1,\\ \text{some } k\text{-morphisms } \phi_1,\dots,\phi_n:\mathbb{P}^1\to\mathbb{P}^1 \text{ of finite degree}\geqslant 2,\\ \text{and some } l,l_1,\dots,l_n,m,m_1,\dots,m_n\geqslant 1,\\ \phi^l\circ\phi_1^{l_1}=\phi_1^{l_1}\circ\phi^l,\ \phi_1^{m_1}\circ\phi_2^{l_2}=\phi_2^{l_2}\circ\phi_1^{m_1},\\ \phi_2^{m_2}\circ\phi_3^{l_3}=\phi_3^{l_3}\circ\phi_2^{m_2},\dots,\phi_{n-1}^{m_{n-1}}\circ\phi_n^{l_n}=\phi_n^{l_n}\circ\phi_{n-1}^{m_{n-1}},\phi_n^{m_n}\circ\varphi^m=\varphi^m\circ\phi_n^{m_n}\end{array}\right\}\\
&\supset\left\{\phi:\mathbb{P}^1\to\mathbb{P}^1 : \begin{array}{l}\phi \text{ is a } k\text{-morphism of finite degree } \geqslant 2 \text{ such that}\\ \phi^l\circ\varphi^m=\varphi^m\circ\phi^l \text{ for some } l,m\geqslant 1\end{array}\right\}\\
&\supset\{\varphi\},
\end{aligned}$$

where $\langle\varphi,\phi\rangle$ is the so-called Petsche–Szpiro–Tucker or Arakelov–Zhang pairing of the two morphisms $\varphi$ and $\phi$. See [PST12] for the details of its definition, which we omit here. See also [KS07].

(ii) In Conjecture 4.1 it would also be interesting to enlarge $\Gamma_0$ and $\Gamma$ along the lines of Silverman's idea in [Sil93]. For example, we could take:

$$\Gamma_0 := \bigcup_{\phi_1,\dots,\phi_n\in[\varphi],\, n\geqslant 1} \phi_n^+(\cdots(\phi_1^+(Q_0))\cdots);\quad \text{and}$$

$$\Gamma := \left(\bigcup_{\phi_1,\dots,\phi_n\in[\varphi],\, n\geqslant 1} \phi_n^-(\cdots(\phi_1^-(\Gamma_0))\cdots)\right)\cup\mathbb{P}^1(\overline{k})_{\varphi\text{-preper}}.$$

These are the forward and backward orbits under the maps in the monoid generated by the elements of $[\varphi]$ under the composition of maps. There are reasonable ways to consider even larger sets $\Gamma_0$ and $\Gamma$ by taking unions over larger classes of morphisms, but their consideration would lead to more complicated formulations of the conjecture, so we content ourselves with the above.

(iii) It is interesting to compare Conjecture 4.1 with other current work. Indeed, V. Sookdeo and T. Tucker also recently had a conjecture along the lines of Conjecture 4.1. For example, keep the above notation, and let

$$\Gamma' = \left(\bigcup_{\phi\in[\varphi]} \phi^-(Q_0)\right)\cup\mathbb{P}^1(\overline{k})_{\varphi\text{-preper}},$$

and

$$\Gamma'' = \left(\bigcup_{n\geqslant 1,\, \phi_1,\dots,\phi_n\in[\varphi]} \phi_n^-(\cdots(\phi_1^-(Q_0))\cdots)\right)\cup\mathbb{P}^1(\overline{k})_{\varphi\text{-preper}}.$$

Then their conjecture in [Soo10] may be reformulated in our terms above as follows:

$$\text{if } Q\in\mathbb{P}^1(\overline{k})-\mathbb{P}^1(\overline{k})_{\varphi\text{-preper}},\quad \text{then } \#(\mathbb{P}^1_{(Q)}(\overline{\mathcal{O}}_{k,S})\cap\Gamma'')<\infty.$$

In particular, their conjecture would imply that $\#(\mathbb{P}^1_{(Q)}(\overline{\mathcal{O}}_{k,S})\cap\Gamma')<\infty$.

## Acknowledgements

The first named author would like to thank Concordia University in Montreal and the University of Texas at Austin, whose hospitality he was enjoying as this paper was being completed. Both authors would like to thank Marco Streng for useful discussions on his work, V. Sookdeo and T. Tucker for useful discussions on their work and the material in § 4, and the referee, for many

useful suggestions on improving the exposition of the paper. The referee also asked whether the results in the paper are effective. While we see no barrier to their effectivity, we have not done the work of verifying that they are.

## References

BIR08 M. Baker, S. Ih and R. Rumely, *A finiteness property of torsion points*, Algebra Number Theory **2** (2008), 217–248.

CH99 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** (1999), 219–222.

EGST88 J.-H. Evertse, K. Győry, C. L. Stewart and R. Tijdeman, *On S-unit equations in two unknowns*, Invent. Math. **92** (1988), 461–477.

ESS02 J.-H. Evertse, H. P. Schlickewei and W. M. Schmidt, *Linear equations in variables which lie in a multiplicative group*, Ann. of Math. (2) **155** (2002), 807–836.

Fal91 G. Faltings, *Diophantine approximation on abelian varieties*, Ann. of Math. (2) **133** (1991), 549–576.

Fal94 G. Faltings, *The general case of S. Lang's conjecture*, in *Barsotti Symposium in Algebraic Geometry, Abano Terme, 1991*, Perspectives in Mathematics, vol. 15 (Academic Press, San Diego, CA, 1994), 175–182.

Hin88 M. Hindry, *Autour d'une conjecture de Serge Lang*, Invent. Math. **94** (1988), 575–603.

HS00 M. Hindry and J. Silverman, *Diophantine geometry; An introduction*, Graduate Texts in Mathematics, vol. 201 (Springer, New York, 2000).

Ih11a S. Ih, *A nondensity property of preperiodic points on Chebyshev dynamical systems*, J. Number Theory **131** (2011), 750–780.

Ih11b S. Ih, *A nondensity property of preperiodic points on the projective plane*, J. Lond. Math. Soc. (2) **83** (2011), 691–710.

IT10 S. Ih and T. J. Tucker, *A finiteness property for preperiodic points of Chebyshev polynomials*, Int. J. Number Theory **6** (2010), 1011–1025.

KS07 S. Kawaguchi and J. Silverman, *Dynamics of projective morphisms having identical canonical heights*, Proc. Lond. Math. Soc. (3) **95** (2007), 519–544.

Lan78 S. Lang, *Elliptic curves: Diophantine analysis*, Grundlehren der Mathematischen Wissenschaften, vol. 231 (Springer-Verlag, Berlin–New York, 1978).

Lan83 S. Lang, *Complex multiplication*, Grundlehren der Mathematischen Wissenschaften, vol. 255 (Springer-Verlag, New York, 1983).

Mcq95 M. McQuillan, *Division points on semiabelian varieties*, Invent. Math. **120** (1995), 575–603.

Pet08 C. Petsche, *S-integral preperiodic points by dynamical systems over number fields*, Bull. Lond. Math. Soc. **40** (2008), 749–758.

PST12 C. Petsche, L. Szpiro and T. Tucker, *A dynamical pairing between two rational maps*, Trans. Amer. Math. Soc. **364** (2012), 1687–1710.

Sch74 A. Schinzel, *Primitive divisors of the expression $A^n - B^n$ in algebraic number fields*, Crelle **268/269** (1974), 27–33.

Ser72 J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

Sil88 J. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory **30** (1988), 226–237.

Sil93 J. Silverman, *Integer points, Diophantine approximation, and iteration of rational maps*, Duke Math. J. **71** (1993), 793–829.

Sil94 J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151 (Springer-Verlag, New York, 1994).

Sil07 J. Silverman, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics, vol. 241 (Springer, New York, 2007).

Soo10 V. Sookdeo, *Integer points in backward orbits*, J. Number Theory **131** (2011), 1229–1239.

Str08 M. Streng, *Divisibility sequences for elliptic curves with complex multiplication*, Algebra and Number Theory **2** (2008), 183–208.

Voj87 P. Vojta, *Diophantine approximations and value distribution theory*, Lecture Notes in Mathematics, vol. 1239 (Springer-Verlag, New York, 1987).

Voj99 P. Vojta, *Integral points on subvarieties of semiabelian varieties, II*, Amer. J. Math. **121** (1999), 283–313.



David Grant grant@colorado.edu
Department of Mathematics, University of Colorado at Boulder, Boulder, CO 80309-0395, USA

Su-Ion Ih ih@math.colorado.edu
Department of Mathematics, University of Colorado at Boulder, Boulder, CO 80309-0395, USA