# ALGEBRAIC DIVISIBILITY SEQUENCES OVER FUNCTION FIELDS

PATRICK INGRAM, VALÉRY MAHÉ, JOSEPH H. SILVERMAN,
KATHERINE E. STANGE, AND MARCO STRENG

Abstract. In this note we study the existence of primes and of primitive divisors in function field analogues of classical divisibility sequences. Under various hypotheses, we prove that Lucas sequences and elliptic divisibility sequences over function fields defined over number fields contain infinitely many irreducible elements. We also prove that an elliptic divisibility sequence over a function field has only finitely many terms lacking a primitive divisor.

*In Memory of Alf van der Poorten,*
*Mathematician, Colleague, Friend*

## 1. Introduction

Integer sequences of the form

$$L_n = \frac{f^n - g^n}{f - g} \in \mathbb{Z} \tag{1}$$

are called *Lucas sequences* (of the first kind). Necessarily, $f$ and $g$ are the roots of a monic quadratic polynomial $p(x) \in \mathbb{Z}[x]$. The most famous examples are the Fibonacci numbers and the Mersenne numbers, with $p(x) = x^2 - x - 1$ and $p(x) = (x-2)(x-1)$, respectively.

Lucas sequences are associated to twisted forms of the multiplicative group $\mathbb{G}_\mathrm{m}$. Replacing $\mathbb{G}_\mathrm{m}$ with an elliptic curve yields an analogous class of sequences. Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation, let $P \in E(\mathbb{Q})$ be a nontorsion point, and write

$$x\big([n]P\big) = A_n/D_n^2 \in \mathbb{Q}$$

as a fraction in lowest terms. The integer sequence $(D_n)_{n\ge1}$ is called the *elliptic divisibility sequence* (EDS) associated to the pair $(E,P)$. Both Lucas

*Date*: October 27, 2011.
2010 *Mathematics Subject Classification.* Primary 11B39; Secondary 11G05.
*Key words and phrases.* Lucas sequence, elliptic divisibility sequence.
Ingram's research is supported by a grant from NSERC of Canada. Mahé's research is supported by the université de Franche-Comté. Silverman's research is supported by DMS-0854755. Stange's research has been supported by NSERC PDF-373333 and NSF MSPRF 0802915. Streng's research is supported by EPSRC grant number EP/G004870/1.

sequences and EDS are examples of *divisibility sequences*, i.e.,

$$m \mid n \implies L_m \mid L_n \quad \text{and} \quad D_m \mid D_n.$$

The primality of terms in integer sequences is an old question. For example, a long-standing conjecture says that the Mersenne sequence $M_n = 2^n - 1$ contains infinitely many primes, and more generally it is expected that a Lucas sequence will have infinitely many prime terms [8, 17, 24] unless it has a "generic" factorization [13]. On the other hand, because of the rapid growth rate of EDS, which satisfy $\log |D_n| \gg n^2$, the prime number theorem suggests that EDS should contain only finitely many primes [10].

In this paper we study the problem of irreducible elements in Lucas sequences and EDS defined over one-dimensional function fields $K(C)$, where $K$ is a number field. We note that this is different from the case of function fields over finite fields, where one would expect the theory to be similar to the case of sequences defined over number fields. We begin with a definition.

**Definition 1.** Let $C/K$ be a curve defined over a number field $K$. A divisor $D \in \operatorname{Div}(C_{\overline{K}})$ is *defined over* $K$ if it is fixed by $\operatorname{Gal}(\overline{K}/K)$. It is *semi-reduced* if every point occurs with multiplicity 0 or 1.

If $D$ is defined over $K$ and semi-reduced, and $\operatorname{Gal}(\overline{K}/K)$ acts transitively on the support of $D$, then we say that $D$ is *irreducible over* $K$.

Let $K$ be a number field. We consider first Lucas sequences over the coordinate ring $K[C]$ of an affine curve $C$. As we have noted, it is not true that all Lucas sequences have infinitely many prime terms, so we impose a technical restriction which we call *amenability.* See Definition 10 in Section 3 for the full definition, but for example, amenable sequences include those of the form

$$L_n = \frac{f(T)^n - 1}{f(T) - 1}$$

with $f(T) - 1$ of prime degree and irreducible in the polynomial ring $K[T]$. With the amenability hypothesis, we are able to prove that $L_q$ is irreducible for a set of primes $q$ of positive lower density (we recall the definition of Dirichlet density in Section 3).

**Theorem 2.** *Let $K$ be a number field, let $C/K$ be an affine curve, let $K[C]$ denote the affine coordinate ring of $C/K$, and let $L_n \in K[C]$ be an amenable Lucas sequence. Then the set of primes $q$ such that* $\operatorname{div}(L_q)$ *is irreducible over $K$ has positive lower Dirichlet density.*

**Example 3.** Let $C$ be the affine line, so $K[C] = K[T]$. Then a function $f(T) \in K[T]$ is irreducible if and only if its divisor $\operatorname{div}(f) \in \operatorname{Div}(C)$ is irreducible. As a specific example, the polynomial

$$L_q = \frac{(T^2+2)^q - 1}{T^2 + 1} \in \mathbb{Q}[T]$$

is irreducible in $\mathbb{Q}[T]$ for all primes $q \equiv 3 \pmod 4$, although we note that computations suggest that these $L_q$ are in fact irreducible for all primes $q$. See Section 7 for more details on this example.

The definition of elliptic divisibility sequences over $\mathbb{Q}$ depends on writing a fraction in lowest terms. We observe that the denominator of the $x$-coordinate of a point $P$ on a Weierstrass curve measures the primes at which $P$ reduces to the point $O$ at infinity. We use this idea in order to define our more canonical notion of EDS over function fields, which does not depend on a choice of model, only on $E/K$ and $P \in E(K)$.

**Definition 4.** Let $K(C)$ be the function field of a smooth projective curve $C$, let $E/K(C)$ be an elliptic curve defined over the function field of $C$, and let $\mathcal{E} \to C$ be the minimal proper regular model of $E$ over $C$. [1] Let $\mathcal{O} \subset \mathcal{E}$ be the image of the zero section. Each point $P \in E\big(K(C)\big)$ induces a map $\sigma_P : C \to \mathcal{E}$. The *elliptic divisibility sequence* associated to the pair $(E, P)$ is the sequence of divisors

$$D_{nP} = \sigma_{nP}^*(\mathcal{O}) \in \operatorname{Div}(C), \qquad n \geq 1.$$

(If $nP = O$, we leave $D_{nP}$ undefined.)

The general problem of irreducible elements in EDS over function fields appears difficult. Even the case of a split elliptic curve, which we study in our next result, presents challenges.

**Theorem 5.** *Let $K$ be a number field, let $K(C)$ be the function field of a curve $C$, and let $(D_{nP})_{n\geq 1}$ be an elliptic divisibility sequence, as described in Definition 4, corresponding to a pair $(E, P)$. Suppose further that*

*i) the elliptic curve $E$ is split, i.e., $E$ is isomorphic to a curve over $K$;*
*ii) the elliptic curve $E$ does not have CM;*
*iii) the point $P \in E\big(K(C)\big)$ is nonconstant; and*
*iv) the divisor $D_P$ is irreducible over $K$ and has prime degree.*

*Then the set of rational primes $q$ such that the divisor $D_{qP} - D_P$ is irreducible has positive lower Dirichlet density.*

**Remark 6.** If $P$ is constant, then the EDS is trivial. The condition that $D_P$ is irreducible is also necessary, as counterexamples can be obtained from Theorem 18 below. We will explain below Theorem 7 why $q$ must be prime.

The other conditions, that $E$ is split and non-CM, and that $D_P$ has prime degree, are consequences of our methods. We will use the Galois theory of $E[q]$ over $K$, which looks very different if $E$ is non-split or CM. And we will employ the fact that $q$ is inert in the field extension $K(D_P)/K$ for a positive density of primes $q$, a fact that is true by Chebotarev's density theorem if the degree of the field extension is prime (Lemma 15), but not in general.

[1] The minimal proper regular model is a smooth projective surface over $K$ associated to $E$. See Section 5 for more information.

The proofs of Theorems 2 and 5 are similar. In both cases, the sequence in question arises from a certain point $P$ in an algebraic group (the multiplicative group $\mathbb{G}_\mathrm{m}$ in the former case) over $K$. And in both cases, the point $P$ is defined over $\overline{K(C)}$, and the $q^{\text{th}}$ term of the sequence corresponds to the divisor on $C$ over which the point $P$ meets the $q$-torsion of the group. If the absolute Galois group of $K$ acts transitively on the points of order $q$, then proving the irreducibility of the divisor is the same as proving the irreducibility of the divisor of intersection of $P$ with a single $q$-torsion point. We complete the proof by analyzing the divisor locally at primes lying above $q$.

Although the question of whether or not there are infinitely many Mersenne primes is perhaps the best known problem concerning primes in divisibility sequences, another question that has received a great deal of attention in both the multiplicative and elliptic cases is the existence of *primitive divisors.* A primitive divisor of a term $a_n$ in an integer sequence is a prime divisor of $a_n$ that divides no earlier term in the sequence.

Here we give a result for general one-dimensional function fields of characteristic zero. We refer the reader to Section 5 for definitions and further details, and to Section 2 for a discussion of work on primitive divisors in other contexts.

**Theorem 7.** *Let $K$ be a field of characteristic zero, and let $(D_{nP})_{n\geq 1}$ be an EDS defined over $K(C)$, the function field of a curve. Assume further that there is no isomorphism $\psi : E \to E'$ over $\overline{K}(C)$ with $E'$ defined over $\overline{K}$ and $\psi(P) \in E'(\overline{K})$, and assume the point $P$ is nontorsion. Then for all but finitely many $n$, the divisor $D_{nP}$ has a primitive divisor.*

**Remark 8.** The conditions on $E$ and $P$ in Theorem 7 are necessary. Indeed, if an isomorphism $\psi$ as above exists, then the EDS is trivial, and if $P$ is torsion, then it is periodic.

Theorem 5 focuses on the study of irreducible terms $D_{nP}$ in elliptic divisibility sequences over $K(C)$ when the index $n$ is prime. The fact that $D_{nP}$ is a divisibility sequence suggests that this restriction to prime indices is necessary, since if $m \mid n$, then $D_{nP}$ always decomposes into a sum $D_{nP} = D_{mP} + (D_{nP} - D_{mP})$ of divisors defined over $K$. Thus $D_{nP}$ is reducible unless either $D_{mP} = 0$ or $D_{nP} = D_{mP}$, and the theorem on primitive divisors (Theorem 7) says that $D_{nP} \neq D_{mP}$ if $n$ is sufficiently large. More generally, a *magnified EDS* is an EDS that admits a type of generic factorization. We will prove that magnified EDS have only finitely many irreducible terms; see Theorem 32, and Theorem 18 for a related stronger result. We also refer the reader to [13, Theorem 1.5] for effective bounds (for $K(C) = \mathbb{Q}(t)$) that are proven using the function field analogue of the ABC conjecture.

We conclude our introduction with a brief overview of the contents of this paper. In Section 2 we motivate our work with some historical remarks on the study of primes and primitive divisors in divisibility sequences. Section 3 gives the proof of Theorem 2 on the existence of irreducible terms in Lucas sequences, and Section 4 gives the proof of the analogous Theorem 5 for (split) elliptic divisibility sequences. Section 5 contains the proof of Theorem 7 on the existence of primitive divisors in general EDS over function fields. In Section 6 we take up the question of magnification in EDS and use it to show that a magnified EDS contains only finitely many irreducible terms. We also briefly comment on the difficulties of extending our irreducibility methods to non-isotrivial EDS. We conclude in Section 7 with a number of examples illustrating our results.

**Acknowledgments.** This project was initiated at a conference at the International Centre for Mathematical Sciences in Edinburgh in 2007 and originally included the five authors, Graham Everest, and Nelson Stephens. Graham is unfortunately no longer with us, but his ideas suffuse this work, and we take this opportunity to remember and appreciate his life as a valued colleague and friend. We also thank Nelson for his input during the original meeting, and Maarten Derickx, Michael Rosen, and Jonathan Wise for helpful discussions as the project approached completion.

## 2. History and Motivation

In this section we briefly discuss some of the history of primes and primitive divisors in divisibility sequences over various types of rings and fields. This is primarily meant to provide background and to help motivate our work over function fields.

The search for Mersenne primes $2^n - 1$ was initiated by the French monk Marin Mersenne in the early $17^{\text{th}}$-century and continues today in the form of a distributed computer program currently running on nearly half a million CPUs [26]. More generally, most integer Lucas sequences are expected to have infinitely many prime terms [8, 17, 24]. The only obvious exceptions occur with a type of generic factorization [13]. For example, if $f$ and $g$ are positive coprime integers, then the Lucas sequence associated to $f^2$ and $g^2$,

$$L_n = \frac{f^{2n} - g^{2n}}{f^2 - g^2} = \left(\frac{f^n - g^n}{f - g}\right)\left(\frac{f^n + g^n}{f + g}\right), \tag{2}$$

contains only finitely many primes.

We remark that Seres [32, 33] has considered various irreducibility questions about compositions of the form $\Phi_n\bigl(f(x)\bigr)$, where $\Phi_n(x)$ is the $n^{\text{th}}$ cyclotomic polynomial. These results, however, all focus on the case where $f(x) \in \mathbb{Z}[x]$ has many integer roots, while we focus on the case where $f - 1$ is irreducible.

Elliptic divisibility sequences were first studied formally by Ward [54, 55], although Watson [56] considered related sequences in his resolution of Lucas' square pyramid problem. Recently, the study of elliptic divisibility sequences has seen renewed interest [15, 42, 44, 45, 46, 50], including applications to Hilbert's 10th problem [6, 11, 29] and cryptography [23, 37, 47]. (We remark that some authors use a slightly different definition of EDS via the division polynomial recursion. See the cited references for details. These definitions differ only in finitely many valuations (see [1, Théorème A]).)

The $n^{\text{th}}$ Mersenne number $M_n$ can be prime only if $n$ is prime, and the prime number theorem suggests that $M_q$ has probability $1/\log M_q$ of being prime. Thus the number of prime terms $M_q$ with $q \le X$ should grow like $\sum_{q\le X} q^{-1} \approx \log\log(X)$. This argument fails to take into account some nuances, but a more careful heuristic analysis by Wagstaff [53] refines this argument and gives reason to believe that the number of $q \le X$ such that $M_q$ is prime should be asymptotic to $e^{\gamma}\log\log_2(X)$.

The study of prime terms of elliptic divisibility sequences began with Chudnovsky and Chudnovsky [5], who searched for primes computationally. An EDS over $\mathbb{Z}$ grows much faster: $\log|D_n| \gg n^2$, and again only prime indices can give prime terms (with finitely many exceptions), so a reasonable guess is that

$$\#\{n \ge 1 : D_n \text{ is prime}\} \ll \sum_{q \text{ prime}} \frac{1}{\log D_q} \ll \sum_{q \text{ prime}} \frac{1}{q^2} \ll 1.$$

Building on the heuristic argument above, Einsiedler, Everest, and Ward [10] conjectured that an EDS has only finitely many prime terms, and this conjecture was later expanded upon by Everest, Ingram, Mahé and Stevens [13]. For some EDS, finiteness follows from a type of generic factorization not unlike (2) (cf. [13, 14, 16, 25] and Section 6), but the general case appears difficult.

The study of primitive divisors in integral Lucas sequences goes back to the $19^{\text{th}}$-century work of Bang [2] and Zsigmondy [58], who showed that $a^n - b^n$ has a primitive divisor for all $n > 6$, and has a long history [4, 31, 49, 52], culminating in the work of Bilu, Hanrot, and Voutier [3], who proved that a Lucas sequence has primitive divisors for each index $n > 30$. Flatters and Ward considered the analogous question over polynomial rings [18].

Work on primitive divisors in EDS is more recent, although we note that in 1986 the third author included the existence of primitive divisors in EDS as an exercise in the first edition of [43] (for the full proof, see [38]). A number of authors have given bounds on the number of terms and/or the largest term that have no primitive divisor for various types of EDS, as well as studying generalized primitive divisors when $\operatorname{End}(E) \ne \mathbb{Z}$; see [15, 20, 21, 22, 50, 51]. The proofs of such results generally require deep quantitative and/or effective versions of Siegel's theorem on integrality of points on elliptic curves.

## 3. Proof of Theorem 2—Irreducible Terms in Lucas Sequences

For this section, we let $K$ be a number field, we take $C/K$ to be a smooth affine curve defined over $K$, and we write $K[C]$ for the affine coordinate ring of $C/K$. We begin with the definition of amenability, after which we prove that amenable Lucas sequences over $K[C]$ have infinitely many irreducible terms.

**Definition 9.** The degree of a divisor

$$D = \sum_{P \in C} n_P (P) \in \mathrm{Div}(C_{\overline{K}}) \quad \text{is the sum} \quad \deg(D) = \sum_{P \in C} n_P.$$

For a regular function $f \in K[C]$, we write $\deg(f)$ for the degree of the divisor of zeros of $f$, i.e.,

$$\deg(f) = \sum_{P \in C} \mathrm{ord}_P(f).$$

We note that since $C$ is affine, there may be some zeros of $f$ "at infinity" that aren't counted. It need not be true that $\deg(f+g) \leq \max\bigl\{\deg(f), \deg(g)\bigr\}$.

We are now ready to define our notion of amenability.

**Definition 10.** Let

$$L_n = \frac{f^n - g^n}{f - g} \in K[C]$$

be a Lucas sequence. First assume $f, g \in K[C]$. We then say that the sequence is *amenable* (*over* $K[C]$) if the following three conditions hold:

(1) $\mathrm{div}(f-g)$ is irreducible over $K$ and of prime degree,
(2) $\deg(f-g)$ is the generic degree of $af + bg$ as $a, b$ range through $K$,
(3) $f$ and $g$ have no common zeroes.

In general, $f$ and $g$ are the roots of the quadratic polynomial

$$X^2 - L_2 X + (L_2^2 - L_3)$$

over $K[C]$. Let $C' \to C$ be a cover such that $K[C']$ is the integral closure of $K[C]$ in the field extension $K(C, f, g)/K(C)$. Now we have $f, g \in K[C']$ and either $C'$ equals $C$, or $C' \to C$ is a double cover. We call $L_n$ *amenable* (*over* $K[C]$) if it is amenable over $K[C']$.

**Example 11.** Suppose that we are in the case $C = \mathbb{A}^1$, i.e., $L_n$ is a Lucas sequence in the polynomial ring $K[T]$. There are two cases. First, if $f$ and $g$ are themselves in $K[T]$, then $(L_n)_{n \geq 1}$ is amenable if and only if

(1) $f - g$ is an irreducible polynomial of $K[T]$ of prime degree,
(2) $\deg(f-g) = \max\{\deg(f), \deg(g)\}$,
(3) $f$ is not a constant multiple of $g$.

Second, if $f$ and $g$ are quadratic over $K[T]$, then they are conjugate, and both $f + g$ and $(f-g)^2$ are in $K[T]$. In this case, the sequence is amenable if and only if

(1) $(f-g)^2$ is an irreducible polynomial of $K[T]$ of prime degree,
(2) $\deg(f+g) \leq \frac{1}{2} \deg\bigl((f-g)^2\bigr)$,
(3) $f + g \neq 0$.

The following lemma provides the key tool in the proof of Theorem 2.

**Lemma 12.** *Let $f, g \in K[C]$ be such that the associated Lucas sequence*

$$L_n = \frac{f^n - g^n}{f - g}$$

*is amenable, let*

$$D_0 = \operatorname{div}(f - g),$$

*and define two sets of primes by*

$$S = \left\{ \mathfrak{q} \subset \mathcal{O}_K \text{ prime } : \begin{array}{c} \text{there is a rational prime } q \text{ such that} \\ \mathfrak{q} \mid q \text{ and } \operatorname{div}(L_q) \text{ is irreducible over } K \end{array} \right\},$$

$$M = \left\{ \mathfrak{q} \subset \mathcal{O}_K \text{ prime } : \begin{array}{c} C \text{ is smooth over } (\mathcal{O}_K/\mathfrak{q}) \text{ and} \\ D_0 \text{ is irreducible over } (\mathcal{O}_K/\mathfrak{q}) \end{array} \right\}.$$

*Then there is a finite set $S'$ of primes of $\mathcal{O}_K$ such that*

$$M \subseteq S \cup S'.$$

*Proof.* Let $q$ be a prime, and let $\zeta$ be a primitive $q^{th}$-root of unity. Working in $K(\zeta)[C]$, the function $L_q$ factors as

$$L_q = \frac{f^q - g^q}{f - g} = \prod_{j=1}^{q-1} \left( f - \zeta^j g \right). \tag{3}$$

Define the corresponding divisors on $C$ by

$$D_j = \operatorname{div}(f - \zeta^j g) \quad \text{for } 0 \le j \le q-1.$$

We claim that the divisors $D_0, \ldots D_{q-1}$ have pairwise disjoint support. To see this, suppose that $P \in C(\overline{K})$ is a common zero of $f - \zeta^i g$ and $f - \zeta^j g$ for some $i \ne j$. Then $P$ is a common zero of $f$ and $g$, which contradicts Property (3) of amenability.

We now assume that $q$ is chosen sufficiently large so that $q$ is unramified in $K$. This implies that $\mathbb{Q}(\zeta)$ is linearly disjoint from $K$ over $\mathbb{Q}$ (because $q$ is totally ramified in $\mathbb{Q}(\zeta)$ and unramified in $K$). Then the group $\operatorname{Gal}(K(\zeta)/K) \cong \operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ acts transitively on the terms in the product (3), so it also acts transitively on the divisors $D_j$ with $1 \le j \le q-1$. Thus, in order to show that

$$\operatorname{div}(L_q) = \sum_{j=1}^{q-1} D_j$$

is irreducible over $K$, it suffices to show that $D_j$ is irreducible over $K(\zeta)$ for some $1 \le j \le q-1$. We do this by showing that the reduction $\widetilde{D_j}$ modulo some prime of $K(\zeta)$ is irreducible and has the same degree as $D_j$.

Choose primes $\mathfrak{Q} \subseteq \mathcal{O}_{K(\zeta)}$ and $\mathfrak{q} \subseteq \mathcal{O}_K$ with $\mathfrak{Q} \mid \mathfrak{q} \mid q$. We may suppose that $q$ is taken large enough so that the reductions of $f$ and $g$ modulo $\mathfrak{Q}$, which we denote by $\tilde{f}, \tilde{g} \in k_{\mathfrak{Q}}[\tilde{C}]$, are well-defined and satisfy

$$\deg \tilde{f} = \deg f \quad \text{and} \quad \deg \tilde{g} = \deg g.$$

(Here $k_{\mathfrak{Q}}$ denotes the residue field of $\mathcal{O}_{K(\zeta)}$ at $\mathfrak{Q}$.)

In general, there may be a finite set of rational primes $q$ such that some point $P \in \mathrm{Supp}(D_j)$ reduces modulo $\mathfrak{Q}$ to a point not on the affine curve $C$. If this happens, then

$$\deg(\widetilde{D_j}) < \deg(D_j).$$

We wish to rule out this possibility. For $D_0$, which does not depend on $q$, it suffices to assume that $q$ is sufficiently large. For $D_j$, we compare the degree before and after reduction.

Let $d = \deg(D_0)$ over $K[C]$. By part (2) of the amenability hypothesis over $K[C]$, we have

$$\deg(D_j) \leq d = \deg(D_0).$$

Further, since $1 - \zeta^j \in \mathfrak{Q}$, we see that

$$f - \zeta^j g \equiv f - g \pmod{\mathfrak{Q}}. \tag{4}$$

Hence $\widetilde{D_j} = \widetilde{D_0}$, and the degree of $D_j$ is $d$ both before and after reduction modulo $\mathfrak{Q}$.

We now assume that $\mathfrak{q} \in M$, so that $\widetilde{D_0} \bmod \mathfrak{q}$ is irreducible over $k_{\mathfrak{q}}$. Since $K(\zeta)/K$ is totally ramified at $\mathfrak{q}$, the residue fields

$$k_{\mathfrak{Q}} = \mathcal{O}_{K(\zeta)}/\mathfrak{Q} \quad \text{and} \quad k_{\mathfrak{q}} = \mathcal{O}_K/\mathfrak{q} \quad \text{are equal,}$$

and hence $\widetilde{D_j} = \widetilde{D_0}$ is irreducible over this finite field. The degrees of $D_j$ and $\widetilde{D_j}$ being equal, it follows that $D_j$ is irreducible over $K$, and so $\mathrm{div}(L_q)$ is irreducible over $K(\zeta)$. Since we have excluded only a finite number of primes, this proves the lemma. □

**Definition 13.** Let $K$ be a number field and $P_K$ its set of primes. The *Dirichlet density* of a subset $M \subset P_K$ is defined as

$$d(M) = \lim_{s \downarrow 1} \frac{\sum_{\mathfrak{p} \in M} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \in P_K} N(\mathfrak{p})^{-s}},$$

if that limit exists. We define the *lower* Dirichlet density $d_-(M)$ by taking $\liminf$ instead of $\lim$.

We will relate densities of sets of primes of $K$ and $\mathbb{Q}$ as follows.

**Lemma 14.** *Let $K$ be a number field and $M_K \subset P_K$. Let $M_{\mathbb{Q}} = \{p \in P_{\mathbb{Q}} \mid \exists \mathfrak{p} \in M : N(\mathfrak{p}) = p\}$. Then we have*

$$d_-(M_{\mathbb{Q}}) \geq \frac{d_-(M_K)}{[K : \mathbb{Q}]}$$

*Proof.* It is shown in [27, § 13] that the limit defining $d_-(M_K)$ does not change if we remove from $M_K$ all primes of degree $> 1$, and replace the denominator by $\log(1/(s-1))$. So assume without loss of generality that

$M_K$ contains only primes of degree 1. For every element of $M_{\mathbb{Q}}$, there are at most $[K:\mathbb{Q}]$ elements of $M_K$, hence we get

$$d_-(M_{\mathbb{Q}}) = \lim_{s\downarrow 1} \frac{\sum_{p\in M_{\mathbb{Q}}} p^{-s}}{\log\frac{1}{s-1}} \geq \frac{1}{[K:\mathbb{Q}]} \lim_{s\downarrow 1} \frac{\sum_{\mathfrak{p}\in M_K} N(\mathfrak{p})^{-s}}{\log\frac{1}{s-1}} = \frac{d_-(M_K)}{[K:\mathbb{Q}]}.$$

□

We will need the following easy consequence of the Chebotarev Density Theorem.

**Lemma 15.** *Let $D$ be a divisor of prime degree defined over $K$ such that $D$ is irreducible over $K$. Then there is a set $T$ of primes of $K$ of positive density such that $\widetilde{D} \bmod \mathfrak{q}$ is irreducible over $k_{\mathfrak{q}}$ for all $\mathfrak{q} \in T$.*

*Proof.* Let $p = \deg(D)$, which by assumption is prime. By excluding a finite set of primes, we may suppose that $C$ has good reduction at every $\mathfrak{q}$ under consideration. Let $L/K$ be the Galois extension of $K$ generated by the points in the support of $D$. If $Q \in \operatorname{Supp}(D)$ is any point, then the irreducibility of $D$ over $K$ implies that $[K(Q):K] = p$, so $p \mid \#\operatorname{Gal}(L/K)$. It follows that the set $X \subseteq \operatorname{Gal}(L/K)$ of elements acting as a $p$-cycle on the support of $D$ is non-empty, and this set is conjugacy-invariant. By the Chebotarev Density Theorem ([27, Theorem 13.4]), there is a set of primes $T$ of $K$ of density $\#X/[L:K]$ such that for $\mathfrak{Q} \mid \mathfrak{q} \in T$, the Frobenius element of $\operatorname{Gal}(k_{\mathfrak{Q}}/k_{\mathfrak{q}})$ acts as a $p$-cycle on the support of the reduction of $D$ modulo $\mathfrak{Q}$. In particular, for these $\mathfrak{q}$ the reduction of $D$ modulo $\mathfrak{q}$ is irreducible over $k_{\mathfrak{q}}$. □

We now have the tools needed to prove that amenable Lucas sequences over $K[C]$ contain a significant number of irreducible terms.

*Proof of Theorem* 2. Write $L_n = (f^n - g^n)/(f-g)$. Assume first $f, g \in K[C]$. By Lemma 14 it suffices to prove that the set $S$ of Lemma 12 has positive lower density. Since the set $S'$ in Lemma 12 is finite, it suffices to prove that the set $M$ in Lemma 12 has positive lower density. But this follows from the amenability assumption and Lemma 15, which finishes the proof in case $f, g \in K[C]$.

In general, let $c : C' \to C$ be as in the definition of amenable. Then We find that there is a set of primes $q$ of positive lower density such that $c^* \operatorname{div}(L_q) = \operatorname{div}(L_q \circ c) \in \operatorname{Div}[C'](K)$ is irreducible. This implies that $\operatorname{div}(L_q) \in \operatorname{Div}[C](K)$ is irreducible as well. □

## 4. Proof of Theorem 5—Irreducible Terms in EDS

Recall that Theorem 5 assumes that the elliptic curve $E$ is defined over $K$. We postpone the general definition of the minimal proper regular model to Section 5, and for now claim that if $E$ is defined over $K$, then its minimal proper regular model is $\mathcal{E} = E \times C$. Note that a point $Q \in E(K(C))$ induces a map $C \to E$ that by abuse of notation we denote by $\sigma_Q$. The map

$\sigma_Q : C \to \mathcal{E}$ from the introduction is now given by $\sigma_Q = (\sigma_Q \times \mathrm{id}_C)$. As a consequence, the EDS associated to $P$ is simply given by

$$D_{nP} = \sigma_{nP}^*(O) \in \mathrm{Div}(C), \quad n \geq 1,$$

and we will not use $\mathcal{E}$ in this section.

The proof of Theorem 5 proceeds along similar lines to the proof of Theorem 2, but the proof is complicated by the fact that there are no totally ramified primes, so we must use another argument to find appropriate primes of degree 1. We begin with the key lemma, which is used in place of the fact that $q^{\mathrm{th}}$-roots of unity generate totally ramified extensions.

**Lemma 16.** *Let $E/K$ be an elliptic curve defined over a number field, and assume that $E$ does not have CM. Then for all prime ideals $\mathfrak{p}$ of $K$ such that $p = N_{K/\mathbb{Q}}(\mathfrak{p})$ is prime and sufficiently large and such that $E$ has ordinary reduction at $\mathfrak{p}$, and for all points $Q \in E[p]$, there exists a degree 1 prime ideal $\mathfrak{P} \mid \mathfrak{p}$ of the field $K(Q)$ such that $Q \equiv O \pmod{\mathfrak{P}}$.*

*Proof.* Given $E/K$, for all sufficiently large primes $p$, the following conditions hold:

- $p$ is unramified in $K$,
- $E$ has good reduction at all primes lying over $p$, and
- the Galois group $\mathrm{Gal}\big(K\big(E[p]\big)/K\big)$ acts transitively on $E[p]$.

It is clear that the first two conditions eliminate only finitely many primes, and Serre's theorem [34] says that the same is true for the third, since we have assumed that $E$ does not have CM.

Let $\mathfrak{p}$ and $Q$ be as in the lemma. To ease notation, let $L = K\big(E[p]\big)$ and $L' = K(Q)$. Let $\mathfrak{P}_0$ be a prime of $L$ lying over $\mathfrak{p}$. The reduction-mod-$\mathfrak{P}_0$ map is not injective on $p$-torsion [43, III.6.4], so we can find a nonzero point $Q_0 \in E[p]$ such that $Q_0 \equiv O \pmod{\mathfrak{P}_0}$. Since $\mathrm{Gal}(L/K)$ acts transitively on $E[p]$, we can find a $g \in \mathrm{Gal}(L/K)$ such that $g(Q_0) = Q$. Then setting

$$\mathfrak{P} = g(\mathfrak{P}_0), \quad \text{and} \quad \mathfrak{P}' = \mathfrak{P} \cap L',$$

we have

$$\mathfrak{p} = \mathfrak{P}' \cap K, \quad \text{and} \quad Q \equiv O \pmod{\mathfrak{P}'}.$$

For the convenience of the reader, the following display shows the fields and primes that we are using:

$$\begin{array}{ccc} L = K\big(E[p]\big) & & \mathfrak{P} \\ | & & | \\ L' = K(Q) & & \mathfrak{P}' \\ | & & | \\ K & & \mathfrak{p} \\ | & & | \\ \mathbb{Q} & & p \end{array}$$

It remains to prove that $\mathfrak{P}'$ is a prime of degree 1.

Since we have assumed that $\mathfrak{p}$ has degree 1 over $\mathbb{Q}$, it suffices to prove that the extension of residue fields $k_{\mathfrak{P}'}/k_{\mathfrak{p}}$ is trivial. This is done using ramification theory. We denote by $D_{\mathfrak{P}}$ and $I_{\mathfrak{P}}$, respectively, the decomposition group and the inertia group of $\mathfrak{P}$. The degree of $\mathfrak{P}'$ is 1 exactly when $D_{\mathfrak{P}} \subset I_{\mathfrak{P}} \operatorname{Gal}(L/L')$. We prove this inclusion of sets using Serre's results [34] that describe the $\operatorname{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$-module structure of $E[p]$, where $L_{\mathfrak{P}}$, $L'_{\mathfrak{P}'}$, and $K_{\mathfrak{p}}$ denote the completions of $L$, $L'$, and $K$, respectively.

Let

$$\rho_p : \operatorname{Gal}(L/K) \longrightarrow \operatorname{GL}(E[p])$$

be the Galois representation associated to $E[p]$. Recall that $E$ has ordinary reduction at $\mathfrak{p}$ and that $p$ is unramified in $K/\mathbb{Q}$, so Serre [34, §1.11] shows the existence of a basis $(Q_1, Q_2)$ of $E[p]$ with $Q_1 \equiv O \pmod{\mathfrak{P}'}$, and such that under the isomorphism $\operatorname{GL}(E[p]) \cong \operatorname{GL}_2(\mathbb{F}_p)$ associated to the basis $(Q_1, Q_2)$, the following two facts are true:

- The image of $D_{\mathfrak{P}}$ under $\rho_p$ is contained in the Borel subgroup $\{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)\}$ of $\operatorname{GL}_2(\mathbb{F}_p)$.
- The image of $I_{\mathfrak{P}}$ under $\rho_p$ contains the subgroup $\{\left(\begin{smallmatrix} * & 0 \\ 0 & 1 \end{smallmatrix}\right)\}$ of order $p-1$.

Under our assumption that $E$ has ordinary reduction, the kernel of reduction modulo $\mathfrak{P}$ is cyclic of order $p$, so $Q_1$ is a multiple of the point $Q$. Hence $\operatorname{Gal}(L/L')$ is the subgroup of $\operatorname{Gal}(L/K)$ consisting in automorphisms acting trivially on $Q_1$. Since $\operatorname{Gal}(L/K)$ acts transitively on $E[p]$, the image of $\rho_p$ satisfies

$$\rho_p\bigl(\operatorname{Gal}(L/L')\bigr) = \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\} \subset \operatorname{GL}_2(\mathbb{F}_p).$$

In particular, $\rho_p\bigl(\operatorname{Gal}(L/L')\bigr)$ has order $p(p-1)$. It follows that

$$\rho_p(D_{\mathfrak{P}}) \subset \rho_p\bigl(I_{\mathfrak{P}} \operatorname{Gal}\bigl(L/L'\bigr)\bigr).$$

□

We next use Lemma 16 to prove an elliptic curve analogue of Lemma 12.

**Lemma 17.** *Let $E$, $P$, and $K$ be as in the statement of Theorem* 5*, and define sets of primes*

$$U_E = \left\{ \mathfrak{q} \subset \mathcal{O}_K \text{ prime } : \begin{array}{c} N_{K/\mathbb{Q}}(\mathfrak{q}) \text{ is prime, i.e., } \mathfrak{q} \text{ has degree } 1, \\ \text{and } E \text{ has good ordinary reduction at } \mathfrak{q} \end{array} \right\},$$

$$S_P = \bigl\{ \mathfrak{q} \in U_E : D_{qP} - D_P \text{ is irreducible over } K, \text{ where } q = N_{K/\mathbb{Q}}(\mathfrak{q}) \bigr\},$$

$$M_P = \bigl\{ \mathfrak{q} \in U_E : D_P \text{ modulo } \mathfrak{q} \text{ is irreducible over } \mathcal{O}_K/\mathfrak{q} \bigr\}.$$

*Then there is a finite set $S'$ of primes of $\mathcal{O}_K$ such that*

$$M_P \subseteq S_P \cup S'.$$

*Proof.* The point $P \in E\bigl(K(C)\bigr)$ induces a map $\sigma_P : C \to E$, and our assumption that $P$ is not a constant point, i.e., $P \notin E(K)$, implies that $\sigma_P$ is a finite covering. For any rational prime $q$, we have

$$D_{qP} - D_P = \sigma_{qP}^*(O) - \sigma_P^*(O) = \sum_{Q \in E[q] \smallsetminus \{O\}} \sigma_P^*(Q). \tag{5}$$

As noted in the proof of Lemma 16, if $q$ is sufficiently large, then $\operatorname{Gal}(\overline{K}/K)$ acts transitively on $E[q] \smallsetminus \{O\}$. Thus $\operatorname{Gal}(\overline{K}/K)$ acts transitively on the summands in the right side of (5), so in order to prove that $D_{qP} - D_P$ is irreducible over $K$, it suffices to take a nonzero point $Q \in E[q]$ and show that $\sigma_P^*(Q)$ is irreducible over $L' := K(Q)$.

Let $\mathfrak{q} \in M_P$, so in particular $\mathfrak{q}$ has degree 1, and let $q = N_{K/\mathbb{Q}}(\mathfrak{q})$. We want to show that $\mathfrak{q} \in S_P$ (if $q$ is sufficiently large.) We will do this by finding a prime $\mathfrak{Q}$ in $L'$ such that $\sigma_P^*(Q) \bmod \mathfrak{Q}$ is irreducible over the finite field $\mathcal{O}_{L'}/\mathfrak{Q}$. (This suffices, since the reduction modulo $\mathfrak{Q}$ of a reducible divisor is clearly reducible.)

Lemma 16 says that if $q$ is sufficiently large, then there is a prime $\mathfrak{Q}$ in $L'$ of degree 1 over $\mathfrak{q}$ such that $Q \equiv O \pmod{\mathfrak{Q}}$. Thus

$$\sigma_P^*(Q) \equiv \sigma_P^*(O) \pmod{\mathfrak{Q}},$$

so it suffices to prove that $\sigma_P^*(O) \bmod \mathfrak{Q}$ is irreducible over $\mathcal{O}_{L'}/\mathfrak{Q}$.

We have assumed that $\mathfrak{p} \in M_P$, so by the definition of $M_P$, we know that $D_P \bmod \mathfrak{q}$ is irreducible over the finite field $\mathcal{O}_K/\mathfrak{q}$. Since further $\mathfrak{Q}$ has degree 1 over $\mathfrak{q}$, this implies that $D_P \bmod \mathfrak{Q}$ is irreducible over $\mathcal{O}_{L'}/\mathfrak{Q}$, which completes the proof of the lemma. $\square$

We now have the tools to complete the proof.

*Proof of Theorem* 5. We continue with the notation in the statement of Lemma 17. We recall from Lemma 14 that if $T$ is a set of primes of $K$ having positive lower density, then the set of rational primes divisible by elements of $T$ has positive lower density in the primes of $\mathbb{Q}$. So in order to prove Theorem 5, it suffices to prove that the set $S_P$ has positive lower density. Since the set $S'$ in Lemma 17 is finite, it suffices to prove that the set $M_P$ in Lemma 17 has positive lower density.

We are assuming that the divisor $D_P$ is irreducible over $K$ and has prime degree. By Lemma 15, the divisor $D_P$ modulo $\mathfrak{q}$ is irreducible for a set of primes of positive density; and since the primes where $E$ has supersingular reduction have density zero [12, 35, 36], the same is true if we restrict to primes where $E$ has ordinary reduction. This proves that $M_P$ has positive lower density, which completes the proof of Theorem 5. $\square$

If $D_P$ is reducible, then the conclusion of Theorem 5 may be false. A counterexample is the case that $C$ is an elliptic curve and the section $\sigma_P : C \to E$ is an isogeny of degree at least 2. Notice that in this case, the divisor $D_P$ is never irreducible, because its support contains $O_C$, the zero point of $C$. The same holds for $D_{qP} - D_P$, as its support contains $\sigma_P^*(O_E)$.

However, if we remove this divisor $\sigma_P^*(O_E)$, then under a mild hypothesis, we can prove that the remaining divisor $\sigma_P^*[q]^*(O_E) - \sigma_P^*(O_E)$ *is* irreducible for *almost all* primes $q$, not just a positive density. This is the following theorem.

**Theorem 18.** *We continue with the notation of the statement and proof of Theorem* 5. *Suppose that $C$ is an elliptic curve isogenous to $E$ and $\sigma_P : C \to E$ is an isogeny of degree $d > 1$. Further, assume that* $\mathrm{Gal}(\overline{K}/K)$ *acts transitively on* $\ker(\sigma_P) \smallsetminus \{O_E\}$. *Then for all sufficiently large rational primes $q$, the divisor $D_{qP} - D_P$ is a sum of exactly two irreducible divisors, one of degree $(d-1)(q^2-1)$ and one of degree $q^2-1$.*

*Proof.* Let $q$ be a rational prime with $q \nmid d$. Then

$$D_{qP} - D_P = \sigma_P^*[q]^*(O_E) - \sigma_P^*(O_E) = \sum_{Q \in \ker(\sigma_P \circ [q]) \smallsetminus \ker(\sigma_P)} (Q).$$

The decomposition of $D_{qP} - D_P$ into a sum of irreducible divisors over $K$ will follow from the decomposition of $\ker(\sigma_P \circ [q]) = \ker(\sigma_P) \oplus C[q]$ into a union of orbits under the action of $\mathrm{Gal}(\overline{K}/K)$.

To ease notation, we let $L = K\bigl(\ker(\sigma_P)\bigr)$. As remarked at the beginning of the proof of Lemma 16, Serre's theorem [34] implies that if $q$ is sufficiently large, then $\mathrm{Gal}(\overline{K}/L)$ acts transitively on the set $C[q] \smallsetminus \{O_C\}$. (Note that we are assuming that $E$ does not have CM, so the same holds for the isogenous elliptic curve $C$.) Further, we have assumed that $\mathrm{Gal}\left(\overline{K}/K\right)$ acts transitively on $\ker(\sigma_P) \smallsetminus \{O_C\}$. Therefore the set $\ker(\sigma_P) \oplus C[q]$ decomposes into the following four Galois orbits:

(i) $\{(O_C, O_C)\}$,
(ii) $\{(R, O_C) : R \in \ker(\sigma_P), R \neq O_C\}$,
(iii) $\{(O_C, S) : S \in C[q], S \neq O_C\}$,
(iv) $\{(R, S) : R \in \ker(\sigma_P), S \in C[q], R \neq O_C$ and $S \neq O_C\}$.

Since $D_{qP} - D_P$ consists of orbits (iii) and (iv), which have the correct cardinalities, this concludes the proof. $\square$

**Remark 19.** Theorem 18 gives a factorization of a division polynomial associated to a composition of isogenies. In the general case, the same proof can be used to deduce for $q$ large enough a decomposition of $D_{qP} - D_P$ into a sum of irreducible divisors over $K$ from a decomposition of $\ker(\sigma_P)$ as a union of orbits under the action of $\mathrm{Gal}(\overline{K}/K)$. In section 6 we use similar ideas to give examples of EDS arising from points on nonsplit elliptic curves which have only finitely many irreducible terms.

## 5. Proof of Theorem 7—Primitive Divisors in EDS

In this section we prove a characteristic zero function field analogue of the classical result [38] that all but finitely many terms in an elliptic divisibility sequence have a primitive divisor.

Proving the existence of primitive valuations in EDS is much easier over function fields than it is over number fields because there are no archimedean absolute values. Over number fields, multiples $nP$ of $P$ will come arbitrarily close to $\mathcal{O}$ in the archimedean metrics, necessitating the use of deep results from Diophantine approximation. Over characteristic zero function fields, once some multiple $nP$ comes close to $\mathcal{O}$ in some $v$-adic metric, no multiple of $P$ ever comes $v$-adically closer to $\mathcal{O}$; cf. Lemma 25 below.

Inquiry into the number field analogues of the results in this section has been motivated by the parallel question for Lucas sequences, answered definitively by Bilu, Hanrot, and Voutier [3]. It is therefore natural to ask if one can prove similar results for Lucas sequences over function fields. Along these lines, Flatters and Ward [18] have shown that, for a polynomial ring over any field, all terms beyond the second with indices coprime to the characteristic have a primitive valuation.

5.1. **Minimal proper regular models.** We begin with the somewhat technical definition of a minimal proper regular model, immediately followed by equivalent definitions and properties that may be more suitable for thinking about elliptic divisibility sequences.

**Definition 20.** Let $C$ be a smooth projective geometrically irreducible curve over a number field $K$, and $E/K(C)$ an elliptic curve. A proper regular model for $E/K(C)$ is a pair $(\mathcal{E}, \pi)$ consisting of a regular scheme $\mathcal{E}$ and a proper flat morphism $\pi : \mathcal{E} \to C$ with its generic fiber identified with $E$.

A proper regular model is *minimal* if, given any other proper regular model $(\mathcal{E}', \pi')$, the birational map $f : \mathcal{E}' \dashrightarrow \mathcal{E}$ satisfying $\pi \circ f = \pi'$ induced by the identification of the generic fibers, is a morphism.

For any elliptic curve $E/K(C)$, there is a unique minimal proper regular model ([40, IV.4.5]), and it is projective over $K$. In particular, the minimal proper regular model is an elliptic surface according to the definition of [40, III].

If $E$ is defined over $K$, then we can simply take $\mathcal{E} = E \times C$, as we claimed in Section 4.

The following lemma shows how to determine the terms in an EDS without computing a minimal proper regular model.

**Lemma 21.** *Let $v$ be a valuation of $K(C)$, and write $E$ in terms of a minimal Weierstrass equation at $v$ (as in* [43, VII]*). Then we have*

$$v(D_{nP}) = \max\{0, -\frac{1}{2}v(x([n]P))\}.$$

*Proof.* The minimal proper regular model $(\mathcal{E}, \pi)$ of $E/K(C)$ may have singular fibers. The zero section intersects fibers of $(\mathcal{E}, \pi)$ only at non-singular points. Since we are only interested in the pull-back of the image of the zero section $\mathcal{O}$ by some other section $\sigma : C \to \mathcal{E}$, we only need to consider the identity component of the smooth part of each fiber. But the identity component of the smooth part of a fiber is given by the minimal Weierstrass equation ([40, IV.6.1 and IV.9.1]). □

A Weierstrass equation over $K(C)$ is minimal at all but finitely many valuations. For those valuations where it is not minimal, a change of coordinates makes the Weierstrass equation minimal, which changes $v(D_{nP})$ by an amount bounded independently of $n$ (but depending on the chosen Weierstrass equation).

**Example 22.** We illustrate Lemma 21. Take $\mathcal{E}$ to be a minimal proper regular model. Fix a minimal Weierstrass equation for $E$ over some affine piece of $C$ and write $P = (x_P, y_P)$. Then $2D_{nP}$ is close to the polar divisor of the function $x_P \in K(C)$, but may differ at valuations of $K(C)$ where the coefficients are not regular or the discriminant is not invertible.

For example, consider the curve and point

$$E : y^2 = x^3 - T^2 x + 1, \qquad P = (x_P, y_P) = (T, 1) \in E\big(K(T)\big),$$

over the rational function field $K(T)$. It is minimal at all finite values for $T$, but to compute $\sigma_P^* \mathcal{O}$ at $T = \infty$, we must change variables, say $(x, y) = (T^2 X, T^3 Y)$. The new equation is

$$E : Y^2 = X^3 - U^2 X + U^6,$$

with $U = T^{-1}$, and the point $P$ has coordinates $(X_P, Y_P) = (U, U^3)$. This Weierstrass model is not smooth at $U = 0$ (not even as a surface over $K$), so to find a regular model, we would have to blow up the singularity. However, the discriminant $16U^6(4 - 27U^6)$ is not divisible by $U^{12}$, hence this is a minimal Weierstrass equation at $U = 0$, so so Lemma 21 applies. Since

$$-\frac{1}{2} \operatorname{ord}_{U=0} X_P = -\frac{1}{2} \operatorname{ord}_{U=0} U = -\frac{1}{2} < 0,$$

we obtain

$$\operatorname{ord}_\infty D_P = \operatorname{ord}_\infty \sigma_P^* \mathcal{O} = 0,$$

in spite of having

$$-\frac{1}{2} \operatorname{ord}_\infty x_P = -\frac{1}{2} \operatorname{ord}_\infty T = \frac{1}{2} > 0$$

in the original model.

### 5.2. **Primitive valuations.**

**Definition 23.** Let $K$ be a field, let $C/K$ be a smooth projective curve, and let $(D_n)_{n \geq 1}$ be a sequence of effective divisors on $C$. A *primitive valuation*[2]

[2] To avoid confusion, we have changed terminology slightly and refer to primitive *valuations*, rather than primitive *prime divisors*. The reason that we do this is because the terms in our EDS are divisors on $C$, and it is confusing to refer to divisors of divisors. Note that our "prime divisors" are points of $C(\overline{K})$, which correspond to normalized valuations of the function field $\overline{K}(C)$.

*of* $D_n$ is a normalized valuation $\gamma$ of $\overline{K}(C)$ (equivalently, a point $\gamma \in C(\overline{K})$) such that

$$\operatorname{ord}_\gamma(D_n) \geq 1 \qquad \text{and} \qquad \operatorname{ord}_\gamma(D_i) = 0 \quad \text{for all } i < n.$$

We now begin the proof of Theorem 7, which we restate with a small amount of added notation.

**Theorem 24.** *Let $K$ be a field of characteristic 0 and let $(D_{nP})_{n\geq 1}$ be an elliptic divisibility sequence as in Definition 4. Assume further that there is no isomorphism $\psi : E \to E'$ over $\overline{K}(C)$ with $E'$ defined over $\overline{K}$ and $\psi(P) \in E'(\overline{K})$, and that the point $P \in E\big(K(C)\big)$ is nontorsion. Then there exists an $N = N(E,P)$ such that for every $n \geq N$, the divisor $D_{nP}$ has a primitive valuation.*

To ease notation, we assume for the remainder of this section that the constant field $K$ is algebraically closed, and of course we retain the assumption that $\operatorname{char}(K) = 0$. Note that there is no loss of generality in this assumption, since we have adopted the convention of considering valuations on $\overline{K}(C)$.

We start with a standard lemma (cf. [41, Lemma 4]) whose conclusion over function fields is much stronger than the analogous statement over number fields. The term *rigid divisibility* has been used for sequences with this strong property. For the convenience of the reader, we include a proof via basic properties of the formal group.

**Lemma 25.** *Let $(D_{nP})_{n\geq 1}$ be an EDS associated to an elliptic surface as in Definition 4, let $\gamma \in C(K)$ be a point appearing in the support of some divisor in the EDS, and let*

$$m = \min\{n \geq 1 : \operatorname{ord}_\gamma D_{nP} \geq 1\}.$$

*Then*

$$\operatorname{ord}_\gamma D_{nP} = \begin{cases} \operatorname{ord}_\gamma D_{mP} & \text{if } m \mid n, \\ 0 & \text{if } m \nmid n. \end{cases}$$

*Proof.* Let

$$E\big(K(C)\big)_{\gamma,r} = \big\{P \in E\big(K(C)\big) : \operatorname{ord}_\gamma \sigma_P^*\mathcal{O} \geq r\big\} \cup \{\mathcal{O}\}.$$

Then $E\big(K(C)\big)_{\gamma,r}$ is a subgroup of $E\big(K(C)\big)$, and

$$\operatorname{ord}_\gamma D_{nP} = \max\{r \geq 0 : nP \in E\big(K(C)\big)_{\gamma,r}\}.$$

This all follows from standard properties of the formal group of $E$ over the completion $K(C)_\gamma$ of $K(C)$ at the valuation $\operatorname{ord}_\gamma$; see [43, Chapter IV]. It also follows that there is an isomorphism of additive groups

$$\frac{E\big(K(C)_\gamma\big)_{\gamma,r}}{E\big(K(C)_\gamma\big)_{\gamma,r+1}} \cong \frac{\mathcal{M}_\gamma^r}{\mathcal{M}_\gamma^{r+1}} \cong K \qquad \text{for all } r \geq 1,$$

where we use the notation $\mathcal{M}_\gamma$ to denote $K(C)_\gamma$'s maximal ideal. The quotient is torsion-free since $\operatorname{char}(K) = 0$.

Let $d = \operatorname{ord}_\gamma D_{mP}$. By assumption, we have $d \geq 1$ and

$$mP \in E\bigl(K(C)\bigr)_{\gamma,d} \smallsetminus E\bigl(K(C)\bigr)_{\gamma,d+1}.$$

Since the quotient is torsion-free, it follows that every multiple also satisfies

$$mkP \in E\bigl(K(C)\bigr)_{\gamma,d} \smallsetminus E\bigl(K(C)\bigr)_{\gamma,d+1},$$

so $\operatorname{ord}_\gamma D_{mkP} = d = \operatorname{ord}_\gamma D_{mP}$.

Conversely, suppose that $\operatorname{ord}_\gamma D_{nP} \geq 1$. To ease notation, let $e = \operatorname{ord}_\gamma D_{nP}$. Then

$$nP \in E\bigl(K(C)\bigr)_{\gamma,e} \quad \text{and} \quad mP \in E\bigl(K(C)\bigr)_{\gamma,d},$$

so the fact that $\bigl\{E\bigl(K(C)\bigr)_{\gamma,r}\bigr\}_{r\geq 0}$ give a filtration of subgroups of $E\bigl(K(C)\bigr)$ implies that

$$\gcd(m,n)P \in E\bigl(K(C)\bigr)_{\gamma,\min(d,e)}.$$

Hence

$$\operatorname{ord}_\gamma D_{\gcd(m,n)P} \geq \min(d,e) \geq 1,$$

so by the minimality of $m$ we have $m \leq \gcd(m,n)$. Therefore $m \mid n$, which completes the proof of the lemma. □

**Definition 26.** Let $E/K(C)$ and $\mathcal{E} \to C$ be as in Definition 4. The *canonical height* of a point $P \in E\bigl(K(C)\bigr)$ is the quantity

$$\widehat{h}_E(P) = \lim_{n\to\infty} \frac{\deg \sigma_{nP}^* \mathcal{O}}{n^2}.$$

(If $nP = \mathcal{O}$, we set $\sigma_{nP}^*\mathcal{O} = 0$.)

**Proposition 27.** *The limit defining the canonical height exists, and the function $\widehat{h}_E : E\bigl(K(C)\bigr) \to [0,\infty)$ is a quadratic form satisfying*

$$\widehat{h}_E(P) = \deg \sigma_P^* \mathcal{O} + O_E(1) \quad \textit{for all } P \in E\bigl(K(C)\bigr). \tag{6}$$

*(The $O_E(1)$ depends on $E/K(C)$.)*

*Next, assume that there is no isomorphism $\psi : E \to E'$ with $E'$ defined over $K$ and $\psi(P) \in E'(K)$. Then we have*

$$\widehat{h}_E(P) = 0 \quad \Longleftrightarrow \quad P \in E\bigl(K(C)\bigr)_{\text{tors}}.$$

*Proof.* A proof is given in [40, III.4.3], except for the final equivalence in the case where $E$ is isomorphic to a curve over $K$.

So assume $E$ is given by a Weierstrass equation with coefficients in $K$. The point $P$ is not in $E(K)$, so $P$ is not a torsion point. The point $P$ induces a map $\sigma_P : C \to E$. Since $P \notin E(K)$, the map $\sigma_P$ is not constant, i.e. $\deg(\sigma_p)$ is strictly positive. We show $\widehat{h}_E(P) = \deg(\sigma_P)$.

An equation with coefficients in $K$ is automatically a minimal Weierstrass equation for every valuation $v$ of $K(C)$, so Lemma 21 tells us

$$\widehat{h}_E(P) = \lim_{n\to\infty} n^{-2} \sum_v \max\{0, -\frac{1}{2}v(x([n]P))\} = \lim_{n\to\infty} n^{-2} \deg x([n]P).$$

Here $\deg x([n]P)$ is the degree of the map $x([n]P) : C \to \mathbf{P}^1$, and we have $x([n]P) = x \circ [n] \circ \sigma_P$. In particular, multiplicativity of degrees tells us $\deg x([n]P) = 2n^2 \deg \sigma_P$. □

**Remark 28.** It is not hard to derive explicit upper and lower bounds for the $O_E(1)$ in (6) in terms of geometric invariants of the elliptic surface $\mathcal{E}$; see for example [39, 57].

*Proof of Theorem* 24. The proof follows the lines of the proof over number fields; cf. [38]. The point $P$ is not a torsion point. From Proposition 27 we know $\widehat{h}_E(P) > 0$. Suppose that $D_{nP}$ has no primitive valuations. Then

$$\begin{aligned} D_{nP} &= \sum_{\gamma \in C} \operatorname{ord}_\gamma(D_{nP})(\gamma) \\ &\le \sum_{m<n} \sum_{\gamma \in \operatorname{Supp}(D_{mP})} \operatorname{ord}_\gamma(D_{nP})(\gamma) && \text{by assumption,} \\ &\le \sum_{m|n, m<n} \sum_{\gamma \in \operatorname{Supp}(D_{mP})} \operatorname{ord}_\gamma(D_{mP})(\gamma) && \text{from Lemma 25,} \\ &= \sum_{m|n, m<n} D_{mP}. \end{aligned}$$

Taking degrees and using properties of the canonical height yields

$$\begin{aligned} n^2 \widehat{h}_E(P) &= \widehat{h}_E(nP) \\ &= \deg D_{nP} + O(1) \\ &\le \sum_{m|n, m<n} \deg D_{mP} + O(1) \\ &= \sum_{m|n, m<n} \big(\widehat{h}_E(mP) + O(1)\big) \\ &= \sum_{m|n, m<n} \big(m^2 \widehat{h}_E(P) + O(1)\big) \\ &\le n^2 \Bigg( \sum_{m|n, m>1} \frac{1}{m^2} \Bigg) \widehat{h}_E(P) + O(n) \\ &< n^2 \big(\zeta(2) - 1\big) \widehat{h}_E(P) + O(n) \\ &< \frac{2}{3} n^2 \widehat{h}_E(P) + O(n). \end{aligned}$$

Since $\widehat{h}_E(P) > 0$, this gives an upper bound for $n$. □

**Remark 29.** It is an interesting question to give an explicit upper bound for the value of $N(E, P)$ in Theorem 24, i.e., for the largest value of $n$ such $D_{nP}$ has no primitive valuation. Using the function field version of Lang's height lower bound conjecture, proven in [19], and standard explicit estimates for the difference between the Weil height and the canonical height, it may be possible to prove that for EDS associated to a minimal model, the bound $N(E,P)$ may be chosen to depend only on the genus of the function field $K(C)$, independent of $E$ and $P$. However, the details are sufficiently intricate that we will leave the argument for a subsequent note. (See [22] for a weaker result over number fields, conditional on the validity of Lang's height lower bound conjecture for number fields.)

**Remark 30.** Theorem 24 ensures, in the non-split case, that all but finitely many terms in an EDS over a function field have a primitive valuation. If the base field $K$ is a number field, then these valuations correspond to divisors defined over $K$, and thus are attached to a Galois orbit of points. It is natural to ask about the degrees of these primitive valuations. Note that if $\gamma \in C(\overline{K})$ is in the support of one of these primitive valuations, then $P$ specializes to a torsion point on the fiber above $\gamma$, and so it follows from [40, Theorem III.11.4] (or elementary estimates if the fiber is singular) that the height of $\gamma$ is bounded by a quantity depending only on $E$. One immediately obtains an $O(\log n)$-lower bound on the degree of the smallest primitive valuation of $D_{nP}$. Maarten Derickx has pointed out to the authors that one can prove a weaker, but more uniform, lower bound using deep results of Merel, Oesterlé, and Parent (see [28] and the addendum to [9]). In particular, one obtains a lower bound which is logarithmic in the largest prime divisor of $n$, with constants depending only on the underlying number field, independent of $E$.

## 6. Magnification and Elliptic Divisibility Sequences

As usual, let $C/K$ be a smooth projective curve defined over a field $K$ of characteristic zero and consider an elliptic divisibility sequence $(D_{nP})_{n\ge1}$ arising as in Definition 4 from a $K(C)$-point $P$ on an elliptic curve $E/K(C)$. Suppose that $E$ and $P$ satisfy the hypotheses of Theorem 24. That theorem then says that there exists a sequence $\gamma_1,\gamma_2,\gamma_3,\ldots$ of closed points of $C$ such that

$$\operatorname{ord}_{\gamma_n}(D_{mP}) > 0 \quad\Longleftrightarrow\quad n \mid m.$$

Theorem 5 provides examples of elliptic divisibility sequences such that for infinitely many indices $n$, the support of $D_{nP}$ is exactly the $\operatorname{Gal}(\overline{K}/K)$-orbit of the single point $\gamma_n$.

However, the example of Lucas sequences with finitely many irreducible terms (2) suggests that the same should be true for some EDS. In this section we describe properties of EDS that ensure that for all sufficiently large $n$, the divisor $D_{nP}$ contains at least two distinct Galois orbits.

**Definition 31.** An elliptic divisibility sequence $(D_{nP})_{n\ge1}$ attached to an elliptic curve $E/K(C)$ is said to be *magnified* over $K(C)$ if there is an elliptic curve $E'/K(C)$, an isogeny $\tau : E' \longrightarrow E$ defined over $K(C)$ that is not an isomorphism, and a point $P' \in E'\bigl(K(C)\bigr)$ such that $P = \tau(P')$.

The following result is a variant of [13, Theorem 1.5].

**Theorem 32.** *Assume that $E$ and $P$ satisfy the hypotheses of Theorem 24, and that $(D_{nP})_{n\geq 1}$ is magnified over $K(C)$. Then there is a constant $M = M(E,P)$ such that for every index $n > M$, the support of the divisor $D_{nP}$ includes at least two valuations that are not* $\operatorname{Gal}\big(\overline{K}/K\big)$*-conjugates of one another.*

*Proof.* Let $\tau : E' \longrightarrow E$ and $P' \in E'\big(K(C)\big)$ be defined as in Definition 31, and let $(D_{nP'})_{n\geq 1}$ be the elliptic divisibility sequence associated to $P'$.

The isogeny $\tau$ induces a morphism $\tau$ from the Néron model of $E'$ to the Néron model of $E$. The zero section intersects fibers of the minimal proper regular model only at non-singular points, so we know from the relationship between the minimal proper regular model and the Néron model [40, IV.6.1 and IV.9.1] that, for any index $n$, the divisor

$$D_{nP} - D_{nP'} = \sigma^*_{nP}(\mathcal{O}_E) - \sigma^*_{nP'}(\mathcal{O}_{E'}) = \sigma^*_{nP'}\big(\tau^*(\mathcal{O}_E) - \mathcal{O}_{E'}\big) \tag{7}$$

is effective (cf. [50, Lemma 2.13] for a complete proof of the analogous result for elliptic divisibility sequences defined over number fields).

We required the hypotheses of Theorem 24 only for $(E,P)$, but the proof of that theorem holds for $(E',P')$ as well. Indeed, the hypotheses are used in the proof of Theorem 24 only for showing $\widehat{h}(P) > 0$, which implies $\widehat{h}(P') > 0$ via $\tau$. In particular, there is a bound $N(E',P')$ such that for every $n > N(E',P')$, the divisor $D_{nP'}$ has a primitive valuation, say $\gamma'_n \in C(\overline{K})$. Then $\gamma'_n$ occurs also in the support of $D_{nP}$. Further, since every divisor $D_{mP'} \in \operatorname{Div}(C)$ is defined over $K$, we see that every $\operatorname{Gal}\big(\overline{K}/K\big)$-conjugate of a primitive valuation of $D_{nP'}$ is again a primitive valuation of $D_{nP'}$. Hence Theorem 32 is proven once we show that for all sufficiently large $n$, the support of $D_{nP}$ contains a valuation $\gamma_n \in C(\overline{K})$ with $\operatorname{ord}_{\gamma_n}(D_{nP'}) = 0$. We do this by modifying the proof of Theorem 24.

Suppose that $n$ is an index such that $\operatorname{ord}_\gamma(D_{nP'}) > 0$ for *every* valuation $\gamma$ belonging to the support of $D_{nP}$. We will show that $n$ is bounded. Let $d = \deg(\tau) \geq 2$. Applying (7) and its analogue for the dual of $\tau$, we get

$$\operatorname{ord}_\gamma(D_{ndP'}) \geq \operatorname{ord}_\gamma(D_{nP}) \geq \operatorname{ord}_\gamma(D_{nP'})$$

for every valuation $\gamma$. If $\gamma$ belongs to the support of $D_{nP}$, then by assumption we also have $\operatorname{ord}_\gamma(D_{nP'}) > 0$, so Lemma 25 tells us that the outermost orders are equal. In particular, we get

$$\operatorname{ord}_\gamma(D_{nP}) = \operatorname{ord}_\gamma(D_{nP'}),$$

which is also true if $\gamma$ does not belong to the support of $D_{nP}$. It follows that $D_{nP} = D_{nP'}$. Taking degrees, this implies

$$\begin{aligned} n^2 d\widehat{h}(P') = \widehat{h}(nP) &\leq \deg D_{nP} + O(1) = \deg D_{nP'} + O(1) \\ &\leq \widehat{h}(nP') + O(1) \leq n^2\widehat{h}(P') + O(1). \end{aligned}$$

In particular, the index $n$ is bounded since $d > 1$. □

**Remark 33.** The proof of Theorem 32 is based on the effectiveness of the divisor $D_{nP} - D_{nP'}$. Corrales-Rodrigáñez and Schoof [7] proved that, in number fields, the analog to the magnification condition is the only way to construct a pair of elliptic divisibility sequences $(B_n)_{n\geq 1}$ and $(D_n)_{n\geq 1}$ such that $B_n \mid D_n$ for every $n \geq 1$.

**Remark 34.** Theorem 32 implies that Theorem 5 cannot be generalized to magnified points.

## 7. Examples

In this section we provide examples of Lucas sequences and elliptic divisibility sequences over function fields that illustrate some of our results. Computations were performed with Sage Mathematics Software [48].

7.1. **Lucas sequences over $K[T]$.** We provide some examples illustrating the two cases of Remark 11. If $f(T) \in K[T]$ has prime degree and $f(T)-1$ is irreducible, then the Lucas sequence

$$L_n = \frac{f(T)^n - 1}{f(T) - 1}$$

is amenable. Lemma 12 then tells us that $L_q$ is irreducible for all sufficiently large $q$ such that $f(T)$ is irreducible modulo some $\mathfrak{q} \mid q$. Looking at the proof of Lemma 12, we see that the following notion of "sufficiently large" suffices.

(1) $f(T)$ has $\mathfrak{q}$-integral coefficients, and leading coefficient a $\mathfrak{q}$-unit.
(2) $\mathbb{Q}(\zeta_q)$ is linearly disjoint from $K$.

For example, $f(T) = T^2 + 1 \in \mathbb{Q}[T]$ is irreducible modulo all primes $q \equiv 3 \pmod 4$. Hence in the Lucas sequence

$$L_n = \frac{(T^2+2)^n - 1}{T^2+1},$$

the term $L_q$ is irreducible for all primes $q \equiv 3 \pmod 4$. In fact, we checked that $L_q$ is irreducible for all primes $q \leq 1009$, which suggests that $L_q$ may be irreducible for all primes. The first few terms, in factored form, are:

$$\begin{aligned}
L_1 &= 1,\\
L_2 &= T^2+3,\\
L_3 &= T^4+5T^2+7,\\
L_4 &= (T^2+3)(T^4+4T^2+5),\\
L_5 &= T^8+9T^6+31T^4+49T^2+31,\\
L_6 &= (T^2+3)(T^4+3T^2+3)(T^4+5T^2+7),\\
L_7 &= T^{12}+13T^{10}+71T^8+209T^6+351T^4+321T^2+127,\\
L_8 &= (T^2+3)(T^4+4T^2+5)(T^8+8T^6+24T^4+32T^2+17),\\
L_9 &= (T^4+5T^2+7)(T^{12}+12T^{10}+60T^8+161T^6+246T^4+204T^2+73),\\
L_{10} &= (T^2+3)(T^8+7T^6+19T^4+23T^2+11)(T^8+9T^6+31T^4+49T^2+31).
\end{aligned}$$

In general, the Chebotarev density theorem used in Lemma 15 provides us with a specific value for the lower density. In the case that the extension of $K$ generated by a root of $f(T)$ is Galois of prime degree $p$, the lower density provided by our proof is $(p-1)/p$.

For a concrete example of the second type of Lucas sequence described in Remark 11, we consider

$$L_n = \frac{f^n - g^n}{f - g} \in \mathbb{Z}[T],$$

where

$$f = T + S, \quad g = T - S, \quad S^2 = T^3 - 2.$$

The first few terms of this sequence are

$$\begin{aligned}
&L_1 = 1,\\
&L_2 = 2T,\\
&L_3 = (T+1)(T^2+2T-2),\\
&L_4 = 4T(T-1)(T^2+2T+2),\\
&L_5 = T^6 + 10T^5 + 5T^4 - 4T^3 - 20T^2 + 4,\\
&L_6 = 2T(T+1)(T^2+2T-2)(3T^3+T^2-6),\\
&L_7 = T^9 + 21T^8 + 35T^7 + T^6 - 84T^5 - 70T^4 + 12T^3 + 84T^2 - 8.
\end{aligned}$$

We have checked that $L_q$ is irreducible for all primes $5 \le q \le 1009$, but we note that $L_q$ is reducible for $q = 3$. It seems likely that all but finitely many prime-indexed terms of this sequence are irreducible, but this sequence illustrates the fact that amenability does not imply that *every* prime-indexed term is irreducible.

7.2. **Split elliptic divisibility sequences.** Let

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

be an elliptic curve defined over $K$. Then for any curve $C/K$, we may consider $E$ as a split elliptic curve over the function field $K(C)$.

We now take $C = E$ and consider $E$ as an elliptic curve over its own function field $K(E) = K(x, y)$. Then $D_{nP}$ for $P = (x, y)$ is essentially the divisor of the division polynomial $\Psi_n(x, y)$. This constitutes a universal example in the following sense. Suppose $C$ is a curve defined over $K$ with a rational map $C \to E$. Then, considering $E$ as a curve over $K(E)$, pulling back by this map gives $E$ as a curve over $K(C)$:

$$\begin{array}{ccc}
E_{/K(C)} & \longrightarrow & E_{/K(E)}\\
\downarrow & & \downarrow\\
\operatorname{Spec} K(C) & \longrightarrow & \operatorname{Spec} K(E)
\end{array}$$

Pulling back the point $P = (x, y)$ across the top gives rise to a $K(C)$-point on $E$. Conversely, any $K(C)$-point on $E$ gives rise to a map $C \to E$. In particular, the only $K(T)$-points of $E$ are its $K$-points, since the only maps $\mathbb{P}^1 \to E$ are constant.

To illustrate this construction, suppose that

$$E : y^2 = x^3 - 7x + 6.$$

Consider the curve

$$C : v^2 = u^3 - 7(u^3 + 2)^4 u + 6(u^3 + 2)^6$$

and the map

$$C \longrightarrow E, \qquad (u, v) \longmapsto (u/(u^3 + 2)^2, v/(u^3 + 2)^3).$$

Then

$$P = (u/(u^3 + 2)^2, v/(u^3 + 2)^3) \in E\bigl(K(C)\bigr),$$

and the associated sequence of $D_{nP}$ (in factored form, where we identify $D_Q$ with a function on $C$ whose divisor is $D_Q - \deg(D_Q)(\mathcal{O})$) begins

$$\begin{aligned}
D_P &= (u^3 + 2),\\
D_{2P} &= 2y(u^3 + 2),\\
D_{3P} &= (u^3 + 2)(72u^{22} + 1008u^{19} + 5964u^{16} + 19320u^{13} - 49u^{12}\\
&\quad + 36960u^{10} - 392u^9 + 42u^8 + 41676u^7 - 1176u^6 + 168u^5\\
&\quad + 25551u^4 - 1568u^3 + 168u^2 + 6528u - 784),\\
D_{4P} &= 4y(u^3 + 2)(288u^{42} + 8064u^{39} + 104160u^{36} + 822528u^{33}\\
&\quad + 4435592u^{30} + 504u^{28} + 17275648u^{27} + 9072u^{25}\\
&\quad + 50100936u^{24} + 71988u^{22} + 109870016u^{21} + 330456u^{19}\\
&\quad + 183006341u^{18} + 966672u^{16} + 230282052u^{15} + 441u^{14}\\
&\quad + 1867572u^{13} + 215342212u^{12} + 3528u^{11} + 2380539u^{10}\\
&\quad + 144988252u^9 + 10584u^8 + 1927548u^7 + 66365219u^6\\
&\quad + 14112u^5 + 897708u^4 + 18454080u^3 + 7056u^2\\
&\quad + 182784u + 2345536).
\end{aligned}$$

We also computed $D_{5P} - D_P$, which has degree 84 and is irreducible (as a polynomial in $u$).

7.3. **An isogeny.** As an example to which Theorem 18 applies, consider the elliptic curves

$$\begin{aligned}
E &: y^2 + y = x^3 - x^2 - 10x - 20,\\
C &: v^2 + v = u^3 - u^2 - 7820u - 263580.
\end{aligned}$$

There is an isogeny $\sigma_P : C \to E$ of degree 5 such that the divisor

$$\sum_{Q \in \ker(\sigma_P)} (Q) - (\mathcal{O})$$

is irreducible over $\mathbb{Q}$. The map $\sigma_P$ gives a point $P$ on $E$ as a curve over $K(C)$. We find that, in factored form,

$$\begin{aligned} D_P &= (5u^2 + 505u + 12751) \\ D_{3P} &= (5u^2 + 505u + 12751)(3u^4 - 4u^3 - 46920u^2 - 3162957u \\ &\quad - 60098081)(u^{16} + 808u^{15} + 307664u^{14} + 73114536u^{13} \\ &\quad + 12109319702u^{12} + 1478712412670u^{11} + 137408300375962u^{10} \\ &\quad + 9888567316290696u^9 + 555597255218203792u^8 \\ &\quad + 24384290372532564144u^7 + 830287549319036362345u^6 \\ &\quad + 21602949256698317741635u^5 + 418237794866116560977925u^4 \\ &\quad + 5763041398838852610101023u^3 + 52312834246514003927525299u^2 \\ &\quad + 268864495959470526718080718u + 530677345945019287998317531). \end{aligned}$$

The factor

$$3u^4 - 4u^3 - 46920u^2 - 3162957u - 60098081$$

is the third division polynomial for $C$, as expected from the proof Theorem 18.

## References


[1] M. Ayad. Points $S$-entiers des courbes elliptiques. *manuscripta math.*, 76(3–4):305–324, 1992.

[2] A. S. Bang. Taltheoretiske undersølgelser. *Tidskrift f. Math.*, 5:70–80 and 130–137, 1886.

[3] Yu. Bilu, G. Hanrot, and P. M. Voutier. Existence of primitive divisors of Lucas and Lehmer numbers. *J. Reine Angew. Math.*, 539:75–122, 2001. With an appendix by M. Mignotte.

[4] R. D. Carmichael. On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. *Ann. of Math. (2)*, 15(1-4):30–70, 1913/14.

[5] 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):385–434, 1986.

[6] G. Cornelissen and K. Zahidi. Elliptic divisibility sequences and undecidable problems about rational points. *J. Reine Angew. Math.*, 613:1–33, 2007.

[7] C. Corrales-Rodrigáñez and R. Schoof. The support problem and its elliptic analogue. *Journal of Number Theory*, 64(2):276–290, 1997.

[8] H. Dubner and W. Keller. New Fibonacci and Lucas primes. *Math. Comp.*, 68(225):417–427, S1–S12, 1999.

[9] B. Edixhoven. Rational torsion points on elliptic curves over number fields (after Kamienny and Mazur). *Astérisque*, (227):Exp. No. 782, 4, 209–227, 1995. Séminaire Bourbaki, Vol. 1993/94.

[10] M. Einsiedler, G. Everest, and T. Ward. Primes in elliptic divisibility sequences. *LMS J. Comput. Math.*, 4:1–13 (electronic), 2001.

[11] K. Eisenträger and G. Everest. Descent on elliptic curves and Hilbert's tenth problem. *Proc. Amer. Math. Soc.*, 137(6):1951–1959, 2009.

[12] N. D. Elkies. Distribution of supersingular primes. *Astérisque*, (198-200):127–132 (1992), 1991.

[13] G. Everest, P. Ingram, V. Mahé, and S. Stevens. The uniform primality conjecture for elliptic curves. *Acta Arith.*, 134(2):157–181, 2008.

[14] G. Everest and H. King. Prime powers in elliptic divisibility sequences. *Math. Comp.*, 74(252):2061–2071 (electronic), 2005.
[15] G. Everest, G. Mclaren, and T. Ward. Primitive divisors of elliptic divisibility sequences. *J. Number Theory*, 118(1):71–89, 2006.
[16] G. Everest, V. Miller, and N. Stephens. Primes generated by elliptic curves. *Proc. Amer. Math. Soc.*, 132(4):955–963 (electronic), 2004.
[17] G. Everest and T. Ward. Primes in divisibility sequences. *Cubo Mat. Educ.*, 3(2):245–259, 2001.
[18] A. Flatters and T. Ward. Polynomial Zsigmondy theorems, 2010. `arXiv:1002.4829`.
[19] M. Hindry and J. H. Silverman. The canonical height and integral points on elliptic curves. *Invent. Math.*, 93(2):419–450, 1988.
[20] P. Ingram. Elliptic divisibility sequences over certain curves. *J. Number Theory*, 123(2):473–486, 2007.
[21] P. Ingram. A quantitative primitive divisor result for points on elliptic curves. *J. Théor. Nombres Bordeaux*, 21(3):609–634, 2009.
[22] P. Ingram and J. H. Silverman. Uniform estimates for primitive divisors in elliptic divisibility sequences. In *Number theory, Analysis and Geometry (In memory of Serge Lang)*, pages 233–263. Springer-Verlag, 2011.
[23] K. E. Lauter and K. E. Stange. The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences. In *Selected Areas in Cryptography 2008*, volume 5381 of *Lecture Notes in Comput. Sci.*, pages 309–327. Springer, Berlin, 2009.
[24] F. Luca and P. Stănică. Prime divisors of Lucas sequences and a conjecture of Skałba. *Int. J. Number Theory*, 1(4):583–591, 2005.
[25] V. Mahé. Prime power terms in elliptic divisibility sequences. preprint, january 2010.
[26] Mersenne Research Inc. Great internet mersenne prime search. `http://mersenne.org`.
[27] J. Neukirch *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999.
[28] P. Parent. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *J. Reine Angew. Math.*, 506:85–116, 1999.
[29] B. Poonen. Hilbert's tenth problem and Mazur's conjecture for large subrings of $\mathbb{Q}$. *J. Amer. Math. Soc.*, 16(4):981–990 (electronic), 2003.
[30] J. Reynolds. On the pre-image of a point under an isogeny and siegel's theorem. *New York Journal of Mathematics*, 17:163–172, 2011.
[31] A. Schinzel. Primitive divisors of the expression $A^n - B^n$ in algebraic number fields. *J. Reine Angew. Math.*, 268/269:27–33, 1974. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, II.
[32] I. Seres. Über die Irreduzibilität gewisser Polynome. *Acta Arith.*, 8:321–341, 1962/1963.
[33] I. Seres. Irreducibility of polynomials. *J. Algebra*, 2:283–286, 1965.
[34] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.
[35] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.
[36] J.-P. Serre. *Abelian l-adic representations and elliptic curves*, volume 7 of *Research Notes in Mathematics*. A K Peters Ltd., Wellesley, MA, 1998.
[37] R. Shipsey. *Elliptic divisibility sequences*. PhD thesis, Goldsmith's College (University of London), 2000.
[38] J. H. Silverman. Wieferich's criterion and the *abc*-conjecture. *J. Number Theory*, 30(2):226–237, 1988.

[39] J. H. Silverman. The difference between the Weil height and the canonical height on elliptic curves. *Math. Comp.*, 55(192):723–743, 1990.

[40] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[41] J. H. Silverman. Common divisors of elliptic divisibility sequences over function fields. *Manuscripta Math.*, 114(4):431–446, 2004.

[42] J. H. Silverman. $p$-adic properties of division polynomials and elliptic divisibility sequences. *Math. Ann.*, 332(2):443–471 (Addendum 473–474), 2005.

[43] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[44] J. H. Silverman and K. E. Stange. Terms in elliptic divisibility sequences divisible by their indices. *Acta Arith.*, 146(4):355–378, 2011.

[45] J. H. Silverman and N. Stephens. The sign of an elliptic divisibility sequence. *J. Ramanujan Math. Soc.*, 21(1):1–17, 2006.

[46] K. E. Stange. Elliptic nets and elliptic curves. preprint, April 2010.

[47] K. E. Stange. The Tate pairing via elliptic nets. In *Pairing-based cryptography—Pairing 2007*, volume 4575 of *Lecture Notes in Comput. Sci.*, pages 329–348. Springer, Berlin, 2007.

[48] W. A. Stein et al. *Sage Mathematics Software (Version 4.6.2)*. The Sage Development Team, 2011. `http://www.sagemath.org`.

[49] C. L. Stewart. Primitive divisors of Lucas and Lehmer numbers. In *Transcendence theory: advances and applications (Proc. Conf., Univ. Cambridge, Cambridge, 1976)*, pages 79–92. Academic Press, London, 1977.

[50] M. Streng. Divisibility sequences for elliptic curves with complex multiplication. *Algebra Number Theory*, 2(2):183–208, 2008.

[51] P. M. Voutier and M. Yabuta. Primitive divisors of certain elliptic divisibility sequences, 2010. `arXiv:1009.0872`.

[52] P. M. Voutier. Primitive divisors of Lucas and Lehmer sequences. *Math. Comp.*, 64(210):869–888, 1995.

[53] S. S. Wagstaff, Jr. Divisors of Mersenne numbers. *Math. Comp.*, 40(161):385–397, 1983.

[54] M. Ward. The law of repetition of primes in an elliptic divisibility sequence. *Duke Math. J.*, 15:941–946, 1948.

[55] M. Ward. Memoir on elliptic divisibility sequences. *Amer. J. Math.*, 70:31–74, 1948.

[56] G. N. Watson. The problem of the square pyramid. *Messenger of Math.*, 48:1–22, 1918.

[57] H. G. Zimmer. On the difference of the Weil height and the Néron-Tate height. *Math. Z.*, 147(1):35–51, 1976.

[58] K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math. Phys.*, 3(1):265–284, 1892.

Department of Mathematics, Colorado State University, Fort Collins, CO 80521, USA

*E-mail address*: `pingram@math.colostate.edu`

EPF Lausanne, SB-IMB-CSAG, Station 8, CH-1015 Lausanne, Switzerland

*E-mail address*: `valery.mahe@epfl.ch`

Mathematics Department, Brown University, Box 1917, Providence, RI 02912 USA

*E-mail address*: `jhs@math.brown.edu`

Mathematics Institute, University of Warwick, Coventry CV4 7AL, United Kingdom
*E-mail address*: marco.streng@gmail.com

Department of Mathematics, Stanford University, 450 Serra Mall, Building 380, Stanford, CA 94305 USA
*E-mail address*: stange@math.stanford.edu