THE UNIVERSITY OF
WARWICK

warwickpublicationswrap

highlight your research

http://wrap.warwick.ac.uk/

ALGEBRAIC DIVISIBILITY SEQUENCES OVER FUNCTION FIELDS

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

In memory of Alf van der Poorten: mathematician, colleague, friend

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.

1. Introduction

Integer sequences of the form

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

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 $p(x) = (x - 2)(x - 1)$.

Lucas sequences are associated to twisted forms of the multiplicative group $\mathbb{G}_m$. Replacing $\mathbb{G}_m$ 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

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

as a fraction in lowest terms. The integer sequence $(D_n)_{n \geq 1}$ is called the *elliptic divisibility sequence* (EDS) associated to the pair (E, P). Both Lucas sequences and EDSs are examples of *divisibility sequences*, that is,

$$\text{if } m \mid n, \quad \text{then both } L_m \mid L_n \text{ and } D_m \mid D_n.$$

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 has infinitely many prime terms unless it has a 'generic' factorization [8, 13, 17, 25]. On the other hand, because of the rapid growth rate of EDSs, which satisfy $\log |D_n| \gg n^2$, the prime number theorem suggests that EDSs should contain only finitely many primes [10].

In this paper we study the problem of irreducible elements in Lucas sequences and EDSs 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 1.1. Let C/K be a curve defined over a number field K. A divisor $D \in \text{Div}(C_{\overline{K}})$ is *defined over K* if it is fixed by $\text{Gal}(\overline{K}/K)$. It is *semi-reduced* if every point in the support of D occurs with multiplicity 1.

We say that D is *irreducible over K* if D is defined over K and semi-reduced and if $\text{Gal}(\overline{K}/K)$ acts transitively on the support of D.

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 3.2 in Section 3 for the full definition, but for example, amenable sequences include those of the form

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

where $f(T) - 1$ has prime degree and is 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 1.2. *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 $\text{div}(L_q)$ is irreducible over K has positive lower Dirichlet density.*

EXAMPLE 1.3. 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 $\text{div}(f) \in \text{Div}(C)$ is irreducible. As a specific example, the polynomial

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

is irreducible in $\mathbb{Q}[T]$ for all primes $q \equiv 3 \bmod 4$, 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 a more canonical notion of EDS over function fields that does not depend on a choice of model, but only depends on E/K and $P \in E(K)$.

DEFINITION 1.4. 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 (the minimal proper regular model is a smooth projective surface over K associated to E—see Section 5 for more information). Let $O \subset \mathcal{E}$ be the image of the zero section. Each point $P \in E(K(C))$ induces a map $\sigma_P : C \to \mathcal{E}$. The *elliptic divisibility sequence* associated to the pair (E, P) is the sequence of divisors

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

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

The general problem of irreducible elements in EDSs over function fields appears difficult. Even the case where the elliptic curve is defined over K, which we study in our next result, presents challenges.

THEOREM 1.5. *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 1.4, corresponding to a pair (E, P). Suppose further that:*

(i)   *E is the base change to $K(C)$ of an elliptic curve defined over K;*
(ii)   *the elliptic curve E does not have CM (complex multiplication);*
(iii) *the point $P \in E(K(C))$ is nonconstant;*
(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 1.6. 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 4.3 below. We will explain below in Theorem 1.7 why q must be prime.

The other conditions, that E is defined over K 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 has CM or is not defined over K. 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 3.7), but not in general.

The proofs of Theorems 1.2 and 1.5 are similar. In both cases, the sequence in question arises from a certain point P in an algebraic group (the multiplicative group $\mathbb{G}_m$ in the former case) over K. And in both cases, the point P is defined over $\overline{K(C)}$, and the qth 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 the 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 1.7. *Let $K(C)$ be the function field of a curve C over a field K of characteristic zero. Let $(D_{nP})_{n\geq 1}$ be the EDS over $K(C)$ associated to a pair (E, P), consisting of an elliptic curve $E/K(C)$ and a point $P \in E(K(C))$. Assume that P is nontorsion and that there is no isomorphism $\psi : E \to E'$ defined over $\overline{K}(C)$ to an elliptic curve $E'/\overline{K}$ such that $\psi(P) \in E'(\overline{K})$. Then for all but finitely many n, the divisor D_{nP} has a primitive divisor.*

REMARK 1.8. The conditions on E and P in Theorem 1.7 are necessary. Indeed, if an isomorphism ψ as above exists, then the EDS is trivial, and if P is torsion, then it is periodic. The point in the proof where these conditions are used is Proposition 5.8.

Theorem 1.5 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 1.7) 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 EDSs have only finitely many irreducible terms; see

Theorems 6.2 and 4.3 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 1.2 on the existence of irreducible terms in Lucas sequences, and Section 4 gives the proof of the analogous Theorem 1.5 for elliptic divisibility sequences. Section 5 contains the proof of Theorem 1.7 on the existence of primitive divisors in general EDSs over function fields. In Section 6 we take up the question of magnification in EDSs 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 nonisotrivial EDSs. We conclude in Section 7 with a number of examples illustrating our results.

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 17th century and continues today in the form of a distributed computer program currently running on nearly half a million CPUs [19]. More generally, most integer Lucas sequences are expected to have infinitely many prime terms [8, 17, 25]. 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,

$$L_n = \frac{f^{2n} - g^{2n}}{f^2 - g^2} = \left(\frac{f^n - g^n}{f - g}\right)\left(\frac{f^n + g^n}{f + g}\right), \tag{2.1}$$

contains only finitely many primes.

We remark that Seres [31, 32] has considered various irreducibility questions about compositions of the form $\Phi_n(f(x))$, where $\Phi_n(x)$ is the nth 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 [53, 54], although Watson [55] considered related sequences in his resolution of Lucas' square pyramid problem. Recently, the study of elliptic divisibility sequences has seen renewed interest [15, 41, 43, 44, 46, 49], including applications to Hilbert's 10th problem [6, 11, 29] and cryptography [24, 36, 45]. (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 nth 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 $q \leq X$ should grow like $\sum_{q \leq X} q^{-1} \approx \log\log(X)$. This argument fails to take into account some nuances, but a more careful heuristic analysis by Wagstaff [52] refines this argument and gives reason to believe that the number of $q \leq X$ 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

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

Building on the heuristic argument above, Einsiedler *et al.* [10] conjectured that an EDS has only finitely many prime terms, and this conjecture was later expanded upon by Everest *et al.* [13]. For some EDSs, finiteness follows from a type of generic factorization not unlike (2.1) (see, for example, [13, 14, 16, 26] and Section 6), but the general case appears difficult.

The study of primitive divisors in integral Lucas sequences goes back to the 19th-century work of Bang [2] and Zsigmondy [57], who showed that $a^n - b^n$ has a primitive divisor for all $n > 6$. The problem has a long history [4, 30, 48, 50], culminating in the work of Bilu *et al.* [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 EDSs is more recent, although we note that in 1986 the third author included the existence of primitive divisors in EDSs as an exercise in the first edition of [42] (see [37] for a proof). 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 $\text{End}(E) \neq \mathbb{Z}$; see [15, 21–23, 49, 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 1.2—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 3.1. The *degree* of a divisor

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

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

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

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

We are now ready to define amenability.

DEFINITION 3.2. Let

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

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

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

In general, we take f and g to be roots of a quadratic polynomial

$$X^2 - L_2 X + (L_2^2 - L_3) \quad \text{with } L_2, L_3 \in K[C].$$

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 say that the sequence (L_n) is *amenable* (*over* $K[C]$) if it is amenable over $K[C']$.

EXAMPLE 3.3. Suppose that we are in the case $C = \mathbb{A}^1$, that is, 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 $(L_n)_{n \ge 1}$ is amenable if and only if:

(1) $f - g$ is an irreducible polynomial of $K[T]$ of prime degree;
(2) $\deg(f - g) = \max\{\deg(f), \deg(g)\}$; and
(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) $\deg(f + g) \le \frac{1}{2} \deg((f - g)^2)$; and
(3) $f + g \ne 0$.

The following lemma provides the key tool in the proof of Theorem 1.2.

LEMMA 3.4. *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

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

and define two sets of primes by

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

$$M = \left\{ \mathfrak{q} \subset O_K \text{ prime} : \begin{array}{l} C \text{ is smooth over the finite field } O_K/\mathfrak{q} \\ \text{and } D_0 \text{ is irreducible over } O_K/\mathfrak{q} \end{array} \right\}.$$

Then there is a finite set S' *of primes of* O_K *such that*

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

PROOF. Let q be a prime, and let ζ be a primitive qth root of unity. Working in $K(\zeta)[C]$, the function L_q factors as

$$L_q = \frac{f^q - g^q}{f - g} = \prod_{j=1}^{q-1} (f - \zeta^j g). \tag{3.1}$$

Define the corresponding divisors on C by

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

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 $\mathrm{Gal}(K(\zeta)/K) \cong \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ acts transitively on the terms in the product (3.1), so it also acts transitively on the divisors D_j with $1 \le j \le q - 1$. Thus, in order to show that

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

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 $\mathfrak{Q} \subseteq O_{K(\zeta)}$ and $\mathfrak{q} \subseteq O_K$ 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 $O_{K(\zeta)}$ at $\mathfrak{Q}$.)

In general, there may be a finite set of rational primes q such that some point $P \in \operatorname{Supp}(D_j)$ 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 $K[C]$,

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

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

$$f - \zeta^j g \equiv f - g \quad \operatorname{mod} \ \mathfrak{Q}.$$

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 $\widetilde{D_0}$ mod $\mathfrak{q}$ is irreducible over $k_{\mathfrak{q}}$. Since $K(\zeta)/K$ is totally ramified at $\mathfrak{q}$, the residue fields

$$k_{\mathfrak{Q}} = O_{K(\zeta)}/\mathfrak{Q} \quad \text{and} \quad k_{\mathfrak{q}} = O_K/\mathfrak{q}$$

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 $\operatorname{div}(L_q)$ is irreducible over $K(\zeta)$. Since we have excluded only a finite number of primes, this proves the lemma. □

DEFINITION 3.5. 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 lim inf instead of lim.

We will use the following elementary relationship between densities of sets of primes of K and of $\mathbb{Q}$.

LEMMA 3.6. *Let K be a number field, and let $M \subset P_K$ be a set of primes of K. Then the lower density of the set*

$$M_{\mathbb{Q}} = \{p \in P_{\mathbb{Q}} : \text{there exists a } \mathfrak{p} \in M \text{ such that } N(\mathfrak{p}) = p\}$$

satisfies

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

PROOF. It is shown in [27, Section 13] that the limit defining $d_-(M)$ does not change if we remove from M all primes of degree strictly greater than one, nor if we replace the denominator by $\log(s-1)^{-1}$. So assume without loss of generality that M contains only primes of degree one. For every element of $M_{\mathbb{Q}}$, there are at most $[K:\mathbb{Q}]$ elements of M, hence we get

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

We will need the following easy consequence of the Chebotarev density theorem.

LEMMA 3.7. *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 $\widetilde{D}$ mod $\mathfrak{q}$ 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 $Q \in \mathrm{Supp}(D)$ is any point, then the irreducibility of D over K implies that $[K(Q):K] = p$, so $p \mid \# \mathrm{Gal}(L/K)$. It follows that the set $X \subseteq \mathrm{Gal}(L/K)$ of elements acting as a p-cycle on the support of D is nonempty, 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 $\mathrm{Gal}(k_{\mathfrak{Q}}/k_{\mathfrak{q}})$ 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 $k_{\mathfrak{q}}$. $\qquad \square$

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 1.2. Write $L_n = (f^n - g^n)/(f - g)$. Assume first that $f, g \in K[C]$. By Lemma 3.6 it suffices to prove that the set S of Lemma 3.4 has positive lower density. Since the set S' in Lemma 3.4 is finite, it suffices to prove that the set M in Lemma 3.4 has positive lower density. But this follows from the amenability assumption and Lemma 3.7, which finishes the proof in the case $f, g \in K[C]$.

In general, let $c : C' \to C$ be as in the definition of amenability. Then we find that there is a set of primes q of positive lower density such that

$$c^* \mathrm{div}(L_q) = \mathrm{div}(L_q \circ c) \in \mathrm{Div}[C'](K)$$

is irreducible. This implies that $\mathrm{div}(L_q) \in \mathrm{Div}[C](K)$ is irreducible as well. $\qquad \square$

4. Proof of Theorem 1.5—irreducible terms in EDSs

Recall that Theorem 1.5 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 $C \to E$ which, by an abuse of notation, we denote by σ_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 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 1.5 proceeds along similar lines to the proof of Theorem 1.2, 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 one. We begin with the key lemma, which is used in place of the fact that qth roots of unity generate totally ramified extensions.

LEMMA 4.1. *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-one prime ideal $\mathfrak{P} \mid \mathfrak{p}$ of the field $K(Q)$ such that $Q \equiv O \bmod \mathfrak{P}$.*

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;
- the Galois representation

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

  is surjective.

It is clear that the first two conditions eliminate only finitely many primes, and Serre's theorem [33, Property (7)] 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 $L = K(E[p])$ 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 [42, Corollary III.6.4], so we can find a nonzero point $Q_0 \in E[p]$ such that $Q_0 \equiv O \bmod \mathfrak{P}_0$. 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

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

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

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

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

Since we have assumed that $\mathfrak{p}$ has degree one 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. Let $D_{\mathfrak{P}} \subset \mathrm{Gal}(L/K)$ be the decomposition group of $\mathfrak{P}$, and $I_{\mathfrak{P}} \subset D_{\mathfrak{P}}$ the inertia group. Let $H = \mathrm{Gal}(L/L')$. We claim that the degree of $k_{\mathfrak{P}'}/k_{\mathfrak{p}}$ is one exactly if we have

$$D_{\mathfrak{P}} \subset I_{\mathfrak{P}}H. \tag{4.1}$$

Indeed, the degree of $k_{\mathfrak{P}}/k_{\mathfrak{p}}$ is $\#D_{\mathfrak{P}}/I_{\mathfrak{P}}$ by [27, Theorem II.9.9], while the degree of $k_{\mathfrak{P}}/k_{\mathfrak{P}'}$ is $\#(D_{\mathfrak{P}} \cap H)/(I_{\mathfrak{P}} \cap H)$ by the same result combined with [27, Theorem II.9.5]. The natural injection between these groups is surjective exactly when (4.1) holds, which proves the claim.

To finish the proof of Lemma 4.1, it now suffices to show that (4.1) holds. We prove this inclusion using Serre's results [33], which describe the $D_{\mathfrak{P}}$-module structure of $E[p]$. Recall that E has ordinary reduction at $\mathfrak{p}$ and that p is unramified in $K/\mathbb{Q}$, so Serre [33, Section 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 $\mathrm{GL}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$ associated to the basis (Q_1, Q_2), the following two facts are true.

- The image of $D_{\mathfrak{P}}$ under ρ_p is contained in the Borel subgroup $\{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)\}$ of $\mathrm{GL}_2(\mathbb{F}_p)$.
- The image of $I_{\mathfrak{P}}$ under ρ_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. Therefore H is the subgroup of $\mathrm{Gal}(L/K)$ consisting of all automorphisms of L/K that act trivially on Q_1. Since ρ_p is surjective, we get

$$\rho_p(H) = \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\} \subset \mathrm{GL}_2(\mathbb{F}_p).$$

We conclude that $\rho_p(D_{\mathfrak{P}}) \subset \rho_p(I_{\mathfrak{P}})\rho_p(H)$, which by injectivity of ρ_p implies (4.1). This finishes the proof. □

We next use Lemma 4.1 to prove an elliptic curve analogue of Lemma 3.4.

LEMMA 4.2. *Let E, P, and K be as in the statement of Theorem 1.5, and define sets of primes*

$$U_E = \left\{ \mathfrak{q} \subset O_K \text{ prime } : \begin{array}{l} N_{K/\mathbb{Q}}(\mathfrak{q}) \text{ is prime, that is, } \mathfrak{q} \text{ has degree one,} \\ \text{and } E \text{ has good ordinary reduction at } \mathfrak{q} \end{array} \right\},$$

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

$$M_P = \{ \mathfrak{q} \in U_E : D_P \text{ modulo } \mathfrak{q} \text{ is irreducible over } O_K/\mathfrak{q} \}.$$

Then there is a finite set S' of primes of O_K such that

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

PROOF. The point $P \in E(K(C))$ induces a map $\sigma_P : C \to E$, and our assumption that P is not constant, that is, $P \notin E(K)$, implies that σ_P is a finite covering. For any rational prime q,

$$D_{qP} - D_P = \sigma_{qP}^*(O) - \sigma_P^*(O) = \sum_{Q \in E[q] \smallsetminus \{O\}} \sigma_P^*(Q). \tag{4.2}$$

As noted in the proof of Lemma 4.1, if q is sufficiently large, then $\text{Gal}(\overline{K}/K)$ acts transitively on $E[q] \smallsetminus \{O\}$. Thus $\text{Gal}(\overline{K}/K)$ acts transitively on the summands on the right-hand side of (4.2), 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 one, 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 $\sigma_P^*(Q) \mod \mathfrak{Q}$ is irreducible over the finite field $O_{L'}/\mathfrak{Q}$. (This suffices, since the reduction modulo $\mathfrak{Q}$ of a reducible divisor is clearly reducible.)

Lemma 4.1 says that if q is sufficiently large, then there is a prime $\mathfrak{Q}$ in L' of degree one over $\mathfrak{q}$ such that $Q \equiv O \mod \mathfrak{Q}$. Thus

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

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

We have assumed that $\mathfrak{p} \in M_P$, so by the definition of M_P, we know that $D_P \mod \mathfrak{q}$ is irreducible over the finite field $O_K/\mathfrak{q}$. Since further $\mathfrak{Q}$ has degree one over $\mathfrak{q}$, this implies that $D_P \mod \mathfrak{Q}$ is irreducible over $O_{L'}/\mathfrak{Q}$, which completes the proof of the lemma. □

We now have the tools to complete the proof.

PROOF OF THEOREM 1.5. We continue with the notation in the statement of Lemma 4.2. We recall from Lemma 3.6 that if T is a set of primes of K having positive lower density, then the set of rational primes divisible by degree-one elements of T has positive lower density in the primes of $\mathbb{Q}$. So in order to prove Theorem 1.5, it suffices

to prove that the set S_P has positive lower density. Since the set S' in Lemma 4.2 is finite, it suffices to prove that the set M_P in Lemma 4.2 has positive lower density.

We are assuming that the divisor D_P is irreducible over K and has prime degree. By Lemma 3.7, 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, 34, 35], 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 1.5.   □

If D_P is reducible, then the conclusion of Theorem 1.5 may be false. A counter-example is the case where C is an elliptic curve and the section $\sigma_P : C \to E$ is an isogeny of degree at least two. 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 4.3. *We continue with the notation of the statement and proof of Theorem 1.5. 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 $\ker(\sigma_P) \setminus \{O_E\}$. 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

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

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 $L = K(\ker(\sigma_P))$. As remarked at the beginning of the proof of Lemma 4.1, Serre's theorem [33] implies that if q is sufficiently large, then $\mathrm{Gal}(\overline{K}/L)$ acts transitively on the set $C[q] \setminus \{O_C\}$. (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 $\mathrm{Gal}(\overline{K}/K)$ acts transitively on $\ker(\sigma_P) \setminus \{O_C\}$. 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) $\{(R, S) : R \in \ker(\sigma_P), S \in C[q], R \neq O_C \text{ and } S \neq O_C\}$.

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

REMARK 4.4. Theorem 4.3 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 EDSs that have only finitely many irreducible terms.

5. Proof of Theorem 1.7—primitive divisors in EDS

In this section we prove a characteristic-zero function field analogue of the classical result [37] which states that all but finitely many terms in an elliptic divisibility sequence have a primitive divisor.

Proving the existence of primitive valuations in EDSs 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 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 O in some v-adic metric, no multiple of P ever comes v-adically closer to O; see Lemma 5.6 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 *et al.* [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.

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 5.1. Let C be a smooth projective geometrically irreducible curve over a number field K, and let $E/K(C)$ be 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 $\pi : \mathcal{E} \to C$, all defined over K, whose generic fiber is isomorphic to $E/K(C)$.

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 [39, 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 [39, Ch. III]. If E is defined over K, then we can take $\mathcal{E} = E \times C$, as we noted in Section 4.

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

LEMMA 5.2. *Let v be a valuation of $K(C)$, and fix a minimal Weierstrass equation for E at v* [42, Ch. VII]. *Then*

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

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 nonsingular points. Since we are only interested in the pull-back of the image of the zero section 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 [39, Theorem IV.6.1 and Corollary 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 5.3. We illustrate Lemma 5.2. 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

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

over the rational function field $K(T)$. It is minimal at all finite values of T, but to compute $\sigma_P^* O$ at $T = \infty$, we must change variables, say $(x, y) = (T^2 X, T^3 Y)$. Letting $U = T^{-1}$, the new equation is

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

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 Lemma 5.2 applies. Since

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

we obtain

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

in spite of having

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

in the original model.

DEFINITION 5.4. 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*[1] *of* D_n is a normalized valuation γ of $\overline{K}(C)$ (equivalently, a point $\gamma \in C(\overline{K})$) such that

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

We now begin the proof of Theorem 1.7, which we restate with a small amount of added notation.

THEOREM 5.5. *Let* $K(C)$ *be the function field of a curve* C *over a field* K *of characteristic zero. Let* $(D_{nP})_{n \geq 1}$ *be the EDS over* $K(C)$ *associated to a pair* (E, P)*, consisting of an elliptic curve* $E/K(C)$ *and a point* $P \in E(K(C))$*. Assume that* P *is nontorsion and that there is no isomorphism* $\psi : E \to E'$ *defined over* $\overline{K}(C)$ *to an elliptic curve* $E'/\overline{K}$ *such that* $\psi(P) \in E'(\overline{K})$*. 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 $\mathrm{char}(K) = 0$. 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 [40, 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 5.6. *Let* $(D_{nP})_{n \geq 1}$ *be an EDS associated to a pair* (E, P) *over* $K(C)$ *as in Definition 1.4, let* $\gamma \in C(K)$ *be a point appearing in the support of some divisor in the EDS, and let*

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

Then for all $n \geq 1$,

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

PROOF. Let

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

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

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

These assertions follow from standard properties of the formal group of E over the completion $K(C)_\gamma$ of $K(C)$ at the valuation ord_γ; see [42, Ch. IV]. It also follows that

---

[1] To avoid confusion, we have changed terminology slightly and refer to primitive *valuations*, rather than primitive *prime divisors*. We do this because the terms in our EDSs 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 $\overline{K}(C)$.

there is an isomorphism of additive groups

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

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

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

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

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

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

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

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

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

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

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

Hence

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

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

DEFINITION 5.7. Let $E/K(C)$ and $\mathcal{E} \to C$ be as in Definition 1.4. The *canonical height* of a point $P \in E(K(C))$ is the quantity

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

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

PROPOSITION 5.8. *The limit defining the canonical height exists, and the function* $\widehat{h}_E : E(K(C)) \to [0, \infty)$ *is a quadratic form satisfying*

$$\widehat{h}_E(P) = \deg \sigma_P^* O + O_E(1) \quad \forall P \in E(K(C)). \tag{5.1}$$

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

Next, assume that there is no isomorphism $\psi : E \to E'$ *defined over* $\overline{K}(C)$ *to an elliptic curve* $E'/\overline{K}$ *satisfying* $\psi(P) \in E'(\overline{K})$. *Then*

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

PROOF. A proof is given in [39, Theorem III.4.3], except for the final equivalence in the case where E is isomorphic to a curve over K.

So assume that 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 σ_P is not constant, which means that $\deg(\sigma_p)$ is strictly positive. We show that $\widehat{h}_E(P) = \deg(\sigma_P)$.

An equation with coefficients in K is automatically a minimal Weierstrass equation for every valuation v of $K(C)$, so Lemma 5.2 says that

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

The map $x([n]P) : C \to \mathbb{P}^1$ is the composition $x([n]P) = x \circ [n] \circ \sigma_P$, so multiplicativity of degrees gives $\deg x([n]P) = 2n^2 \deg \sigma_P$.   □

REMARK 5.9. It is not hard to derive explicit upper and lower bounds for the $O_E(1)$ in (5.1) in terms of geometric invariants of the elliptic surface $\mathcal{E}$; see, for example, [38, 56].

PROOF OF THEOREM 5.5. The proof follows the lines of the proof over number fields; see, for example, [37]. The point P is not a torsion point. From Proposition 5.8 we know that $\widehat{h}_E(P) > 0$. Suppose that D_{nP} has no primitive valuations. Then

$$
\begin{aligned}
D_{nP} &= \sum_{\gamma \in C} \operatorname{ord}_\gamma(D_{nP})(\gamma) \\
&\leq \sum_{m<n} \sum_{\gamma \in \operatorname{Supp}(D_{mP})} \operatorname{ord}_\gamma(D_{nP})(\gamma) \quad \text{by assumption,} \\
&\leq \sum_{m \mid n, m<n} \sum_{\gamma \in \operatorname{Supp}(D_{mP})} \operatorname{ord}_\gamma(D_{mP})(\gamma) \quad \text{from Lemma 5.6,} \\
&= \sum_{m \mid n, m<n} D_{mP}.
\end{aligned}
$$

Taking degrees and using properties of the canonical height yields

$$
\begin{aligned}
n^2 \widehat{h}_E(P) &= \widehat{h}_E(nP) \\
&= \deg D_{nP} + O(1) \\
&\leq \sum_{m \mid n, m<n} \deg D_{mP} + O(1) \\
&= \sum_{m \mid n, m<n} \left(\widehat{h}_E(mP) + O(1)\right) \\
&= \sum_{m \mid n, m<n} \left(m^2 \widehat{h}_E(P) + O(1)\right)
\end{aligned}
$$

$$\leq n^2 \bigg(\sum_{m|n, m>1} \frac{1}{m^2} \bigg) \widehat{h}_E(P) + O(n)$$
$$< n^2(\zeta(2) - 1)\widehat{h}_E(P) + O(n)$$
$$< \tfrac{2}{3}n^2\widehat{h}_E(P) + O(n).$$

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

REMARK 5.10. It is an interesting problem to give an explicit upper bound for the value of $N(E, P)$ in Theorem 5.5, that is, 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 [20], and standard explicit estimates for the difference between the Weil height and the canonical height, it may be possible to prove that for EDSs 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 [23] for a weaker result over number fields, conditional on the validity of Lang's height lower bound conjecture for number fields.)

REMARK 5.11. Theorem 5.5 ensures, under some hypotheses, 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 γ, and so it follows from [39, Theorem III.11.4] (or elementary estimates if the fiber is singular) that the height of γ 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 $(D_{nP})_{n\geq 1}$ arising as in Definition 1.4 from a $K(C)$-point P on an elliptic curve $E/K(C)$. Suppose that E and P satisfy the hypotheses of Theorem 5.5. 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 1.5 provides examples of elliptic divisibility sequences such that for infinitely many indices n, the support of D_{nP} is exactly the $\mathrm{Gal}(\overline{K}/K)$-orbit of the single point γ_n.

The example of Lucas sequences with finitely many irreducible terms (2.1) suggests that the same should be true for some EDSs. In this section we describe properties of EDSs that ensure that for all sufficiently large n, the divisor D_{nP} contains at least two distinct Galois orbits.

DEFINITION 6.1. An elliptic divisibility sequence $(D_{nP})_{n\geq 1}$ attached to an elliptic curve $E/K(C)$ is said to be *magnified* over $K(C)$ if there exist an elliptic curve $E'/K(C)$, an isogeny $\tau : E' \longrightarrow E$ defined over $K(C)$ that is not an isomorphism, and a point $P' \in E'(K(C))$ such that $P = \tau(P')$.

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

THEOREM 6.2. *Assume that E and P satisfy the hypotheses of Theorem 5.5, 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 $\mathrm{Gal}(\overline{K}/K)$-conjugates of one another.*

PROOF. Let $\tau : E' \longrightarrow E$ and $P' \in E'(K(C))$ be defined as in Definition 6.1, and let $(D_{nP'})_{n\geq 1}$ be the elliptic divisibility sequence associated to P'. The isogeny τ induces a morphism τ 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 nonsingular points, so we know from the relationship between the minimal proper regular model and the Néron model [39, Theorem IV.6.1 and Corollary IV.9.1] that, for any index n, the divisor

$$D_{nP} - D_{nP'} = \sigma_{nP}^*(O_E) - \sigma_{nP'}^*(O_{E'}) = \sigma_{nP'}^*(\tau^*(O_E) - O_{E'}) \qquad (6.1)$$

is effective. (See [49, 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 5.5 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 5.5 only to show that $\widehat{h}(P) > 0$, which implies that $\widehat{h}(P') > 0$ via τ. 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 γ'_n occurs also in the support of D_{nP}. Further, since every divisor $D_{mP'} \in \mathrm{Div}(C)$ is defined over K, we see that every $\mathrm{Gal}(\overline{K}/K)$-conjugate of a primitive valuation of $D_{nP'}$ is again a primitive valuation of $D_{nP'}$. Hence Theorem 6.2 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 $\mathrm{ord}_{\gamma_n}(D_{nP'}) = 0$. We do this by modifying the proof of Theorem 5.5.

Suppose that n is an index such that $\mathrm{ord}_\gamma(D_{nP'}) > 0$ for *every* valuation γ belonging to the support of D_{nP}. We will show that n is bounded. Let $d = \deg(\tau) \geq 2$. Applying (6.1) and its analogue for the dual of τ,

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

for every valuation γ. If γ belongs to the support of D_{nP}, then by assumption we also have $\mathrm{ord}_\gamma(D_{nP'}) > 0$, so Lemma 5.6 tells us that the outermost orders are equal. In particular,

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

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

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

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

REMARK 6.3. The proof of Theorem 6.2 is based on the effectiveness of the divisor $D_{nP} - D_{nP'}$. Corrales-Rodrigáñez and Schoof [7] proved that, in number fields, the analogue 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 6.4. Theorem 6.2 implies that Theorem 1.5 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 [47].

We begin with examples of Lucas sequences over $K[T]$ that illustrate the two cases of Remark 3.3. 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 3.4 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 3.4, 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 $q \equiv 3 \bmod 4$. Hence in the Lucas sequence

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

the term L_q is irreducible in $\mathbb{Q}[T]$ for all primes $q \equiv 3 \bmod 4$. 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:

$L_1 = 1$,

$L_2 = T^2 + 3$,

$L_3 = T^4 + 5T^2 + 7$,

$L_4 = (T^2 + 3)(T^4 + 4T^2 + 5)$,

$L_5 = T^8 + 9T^6 + 31T^4 + 49T^2 + 31$,

$L_6 = (T^2 + 3)(T^4 + 3T^2 + 3)(T^4 + 5T^2 + 7)$,

$L_7 = T^{12} + 13T^{10} + 71T^8 + 209T^6 + 351T^4 + 321T^2 + 127$,

$L_8 = (T^2 + 3)(T^4 + 4T^2 + 5)(T^8 + 8T^6 + 24T^4 + 32T^2 + 17)$,

$L_9 = (T^4 + 5T^2 + 7)(T^{12} + 12T^{10} + 60T^8 + 161T^6 + 246T^4 + 204T^2 + 73)$,

$L_{10} = (T^2 + 3)(T^8 + 7T^6 + 19T^4 + 23T^2 + 11)(T^8 + 9T^6 + 31T^4 + 49T^2 + 31)$.

In general, the Chebotarev density theorem used in Lemma 3.7 provides us with a specific value for the lower density. In the case where 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 3.3, 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

$L_1 = 1$,

$L_2 = 2T$,

$L_3 = (T + 1)(T^2 + 2T - 2)$,

$L_4 = 4T(T - 1)(T^2 + 2T + 2)$,

$L_5 = T^6 + 10T^5 + 5T^4 - 4T^3 - 20T^2 + 4$,

$L_6 = 2T(T + 1)(T^2 + 2T - 2)(3T^3 + T^2 - 6)$,

$L_7 = T^9 + 21T^8 + 35T^7 + T^6 - 84T^5 - 70T^4 + 12T^3 + 84T^2 - 8$.

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.

We now turn to EDS for elliptic curves defined over the base field. 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 an 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

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

Then

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

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

$D_P = u^3 + 2,$

$D_{2P} = 2y(u^3 + 2),$

$D_{3P} = (u^3 + 2)(72u^{22} + 1008u^{19} + 5964u^{16} + 19\,320u^{13} - 49u^{12}$
$\qquad + 36\,960u^{10} - 392u^9 + 42u^8 + 41\,676u^7 - 1176u^6 + 168u^5$
$\qquad + 25\,551u^4 - 1568u^3 + 168u^2 + 6528u - 784),$

$D_{4P} = 4y(u^3 + 2)(288u^{42} + 8064u^{39} + 104\,160u^{36} + 822\,528u^{33}$
$\qquad + 4\,435\,592u^{30} + 504u^{28} + 17\,275\,648u^{27} + 9072u^{25}$
$\qquad + 50\,100\,936u^{24} + 71\,988u^{22} + 109\,870\,016u^{21} + 330\,456u^{19}$
$\qquad + 183\,006\,341u^{18} + 966\,672u^{16} + 230\,282\,052u^{15} + 441u^{14}$
$\qquad + 1\,867\,572u^{13} + 215\,342\,212u^{12} + 3528u^{11} + 2\,380\,539u^{10}$
$\qquad + 144\,988\,252u^9 + 10\,584u^8 + 192\,7548u^7 + 66\,365\,219u^6$
$\qquad + 14\,112u^5 + 897\,708u^4 + 18\,454\,080u^3 + 7056u^2$
$\qquad + 182\,784u + 2\,345\,536).$

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

7.1. An isogeny. As an example to which Theorem 4.3 applies, consider the elliptic curves

$$E : y^2 + y = x^3 - x^2 - 10x - 20,$$
$$C : v^2 + v = u^3 - u^2 - 7820u - 263\,580.$$

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

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

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

$D_P \ = (5u^2 + 505u + 12\,751)$

$D_{3P} = (5u^2 + 505u + 12\,751)(3u^4 - 4u^3 - 46\,920u^2 - 3\,162\,957u$

$\qquad\quad - \ 60\,098\,081)(u^{16} + 808u^{15} + 307\,664u^{14} + 73\,114\,536u^{13}$

$\qquad\quad + \ 12\,109\,319\,702u^{12} + 1\,478\,712\,412\,670u^{11} + 137\,408\,300\,375\,962u^{10}$

$\qquad\quad + \ 9\,888\,567\,316\,290\,696u^9 + 555\,597\,255\,218\,203\,792u^8$

$\qquad\quad + \ 24\,384\,290\,372\,532\,564\,144u^7 + 830\,287\,549\,319\,036\,362\,345u^6$

$\qquad\quad + \ 21\,602\,949\,256\,698\,317\,741\,635u^5$

$\qquad\quad + \ 418\,237\,794\,866\,116\,560\,977\,925u^4$

$\qquad\quad + \ 5\,763\,041\,398\,838\,852\,610\,101\,023u^3$

$\qquad\quad + \ 52\,312\,834\,246\,514\,003\,927\,525\,299u^2$

$\qquad\quad + \ 268\,864\,495\,959\,470\,526\,718\,080\,718u$

$\qquad\quad + \ 530\,677\,345\,945\,019\,287\,998\,317\,531).$

The factor

$$3u^4 - 4u^3 - 46\,920u^2 - 3\,162\,957u - 60\,098\,081$$

is the third division polynomial for C, as expected from the proof Theorem 4.3.

Acknowledgements

References

[1] M. Ayad, 'Points S-entiers des courbes elliptiques', *Manuscripta Math.* **76**(3–4) (1992), 305–324.

[2] A. S. Bang, 'Taltheoretiske undersøgelser', *Tidskrift f. Math.* **5** (1886), 70–80 and 130–137.

[3] Yu. Bilu, G. Hanrot and P. M. Voutier, 'Existence of primitive divisors of Lucas and Lehmer numbers', *J. reine angew. Math.* **539** (2001), 75–122 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) (1913/14), 30–70.

[5] D. V. Chudnovsky and G. V. Chudnovsky, 'Sequences of numbers generated by addition in formal groups and new primality and factorization tests', *Adv. Appl. Math.* **7**(4) (1986), 385–434.

[6] G. Cornelissen and K. Zahidi, 'Elliptic divisibility sequences and undecidable problems about rational points', *J. reine angew. Math.* **613** (2007), 1–33.

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

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

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

[10] M. Einsiedler, G. Everest and T. Ward, 'Primes in elliptic divisibility sequences', *LMS J. Comput. Math.* **4** (2001), 1–13 (electronic).

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

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

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

[14] G. Everest and H. King, 'Prime powers in elliptic divisibility sequences', *Math. Comp.* **74**(252) (2005), 2061–2071 (electronic).

[15] G. Everest, G. Mclaren and T. Ward, 'Primitive divisors of elliptic divisibility sequences', *J. Number Theory* **118**(1) (2006), 71–89.

[16] G. Everest, V. Miller and N. Stephens, 'Primes generated by elliptic curves', *Proc. Amer. Math. Soc.* **132**(4) (2004), 955–963 (electronic).

[17] G. Everest and T. Ward, 'Primes in divisibility sequences', *Cubo Mat. Educ.* **3**(2) (2001), 245–259.

[18] A. Flatters and T. Ward, 'Polynomial Zsigmondy theorems', *J. Algebra.* **343** (2011), 138–142.

[19] Great internet Mersenne prime search, Mersenne Research Inc. http://mersenne.org.

[20] M. Hindry and J. H. Silverman, 'The canonical height and integral points on elliptic curves', *Invent. Math.* **93**(2) (1988), 419–450.

[21] P. Ingram, 'Elliptic divisibility sequences over certain curves', *J. Number Theory* **123**(2) (2007), 473–486.

[22] P. Ingram, 'A quantitative primitive divisor result for points on elliptic curves', *J. Théor. Nombres Bordeaux* **21**(3) (2009), 609–634.

[23] 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)* (Springer, 2011), pp. 233–263.

[24] K. 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*, Lecture Notes in Computer Science, 5381 (Springer, Berlin, 2009), pp. 309–327.

[25] F. Luca and P. Stănică, 'Prime divisors of Lucas sequences and a conjecture of Skałba', *Int. J. Number Theory* **1**(4) (2005), 583–591.

[26] V. Mahé, 'Prime power terms in elliptic divisibility sequences', Preprint, January 2010.

[27] J. Neukirch, *Algebraic Number Theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Vol. 322 (Springer, Berlin, 1999), translated from the 1992 German original and with a note by Norbert Schappacher, with a foreword by G. Harder.

[28] P. Parent, 'Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres', *J. reine angew. Math.* **506** (1999), 85–116.

[29] B. Poonen, 'Hilbert's tenth problem and Mazur's conjecture for large subrings of $\mathbb{Q}$', *J. Amer. Math. Soc.* **16**(4) (2003), 981–990 (electronic).

[30] A. Schinzel, 'Primitive divisors of the expression $A^n - B^n$ in algebraic number fields', *J. reine angew. Math.* **268/269** (1974), 27–33. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, II.

[31] I. Seres, 'Über die Irreduzibilität gewisser Polynome', *Acta Arith.* **8** (1962/63), 321–341.

[32] I. Seres, 'Irreducibility of polynomials', *J. Algebra* **2** (1965), 283–286.

[33] J.-P. Serre, 'Propriétés galoisiennes des points d'ordre fini des courbes elliptiques', *Invent. Math.* **15**(4) (1972), 259–331.

[34] J.-P. Serre, 'Quelques applications du théorème de densité de Chebotarev', *Publ. Math. Inst. Hautes Études Sci.* **54** (1981), 323–401.

[35] J.-P. Serre, *Abelian l-adic Representations and Elliptic Curves*, Research Notes in Mathematics, 7 (A K Peters Ltd., Wellesley, MA, 1998).

[36] R. Shipsey, 'Elliptic divisibility sequences', PhD Thesis, Goldsmith's College, University of London, 2000.

[37] J. H. Silverman, 'Wieferich's criterion and the *abc*-conjecture', *J. Number Theory* **30**(2) (1988), 226–237.

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

[39] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 151 (Springer, New York, 1994).

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

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

[42] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd edn. Graduate Texts in Mathematics, 106 (Springer, Dordrecht, 2009).

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

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

[45] K. E. Stange, 'The Tate pairing via elliptic nets', in: *Pairing-based Cryptography—Pairing 2007*, Lecture Notes in Computer Science, 4575 (Springer, Berlin, 2007), pp. 329–348.

[46] K. E. Stange, 'Elliptic nets and elliptic curves', *Algebra Number Theory* **5**(2) (2011), 197–229.

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

[48] C. L. Stewart, 'Primitive divisors of Lucas and Lehmer numbers', in: *Transcendence Theory: Advances and Applications (Proc. Conf., Univ. Cambridge, Cambridge, 1976)* (Academic Press, London, 1977), pp. 79–92.

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

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

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

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

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

[54] M. Ward, 'Memoir on elliptic divisibility sequences', *Amer. J. Math.* **70** (1948), 31–74.

[55] G. N. Watson, 'The problem of the square pyramid', *Messenger of Math.* **48** (1918), 1–22.

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

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

PATRICK INGRAM, Department of Mathematics, Colorado State University,
Fort Collins, CO 80521, USA
e-mail: pingram@math.colostate.edu

VALÉRY MAHÉ, EPF Lausanne, SB-IMB-CSAG, Station 8,
CH-1015 Lausanne, Switzerland
e-mail: valery.mahe@epfl.ch

JOSEPH H. SILVERMAN, Mathematics Department, Brown University, Box 1917,
Providence, RI 02912, USA
e-mail: jhs@math.brown.edu

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

MARCO STRENG, Mathematics Institute, University of Warwick,
Coventry CV4 7AL, UK
e-mail: marco.streng@gmail.com