Primitive divisors of elliptic divisibility sequences over function fields with constant j-invariant

Naskrecki, B.; Streng, T.C.

Journal of Number Theory 213 (2020) 152–186

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

Primitive divisors of elliptic divisibility sequences over function fields with constant j-invariant

Bartosz Naskręcki [a,*], Marco Streng [b,*]

[a] *Faculty of Mathematics and Computer Science, Adam Mickiewicz University in Poznań, Uniwersytetu Poznańskiego 4, 61-614 Poznań, Poland*
[b] *Mathematisch Instituut, Universiteit Leiden, P.O. box 9512, 2300 RA Leiden, the Netherlands*

ARTICLE INFO

Article history:
Received 1 October 2019
Received in revised form 22 December 2019
Accepted 31 December 2019
Available online 20 January 2020
Communicated by F. Pellarin

MSC:
11G05
11B39
14H52
11G07
11B83

Keywords:
Elliptic divisibility sequences
Elliptic surfaces
Primitive divisors
Function fields
Constant j-invariant

ABSTRACT

We prove an optimal Zsigmondy bound for elliptic divisibility sequences over function fields in case the j-invariant of the elliptic curve is constant.

In more detail, given an elliptic curve E with a point P of infinite order over a global field, the sequence D_1, $D_2, \dots$ of denominators of multiples P, $2P, \dots$ of P is a strong divisibility sequence in the sense that $\gcd(D_m, D_n) = D_{\gcd(m,n)}$. This is the genus-one analogue of the genus-zero Fibonacci, Lucas and Lehmer sequences.

A number N is called a Zsigmondy bound of the sequence if each term D_n with $n > N$ presents a new prime factor. The optimal uniform Zsigmondy bound for the genus-zero sequences over $\mathbf{Q}$ is 30 by Bilu-Hanrot-Voutier [2], but finding such a bound remains an open problem in genus one, both over $\mathbf{Q}$ and over function fields.

We prove that the optimal Zsigmondy bound for ordinary elliptic divisibility sequences over function fields is 2 if the j-invariant is constant. In the supersingular case, we give a complete classification of which terms can and cannot have a new prime factor.

* Corresponding authors.
E-mail addresses: bartnas@amu.edu.pl (B. Naskręcki), streng@math.leidenuniv.nl (M. Streng).

https://doi.org/10.1016/j.jnt.2019.12.002
0022-314X/

1. Introduction

An *elliptic divisibility sequence (EDS)* over $\mathbf{Q}$ is a sequence $D_1, D_2, D_3, \ldots$ of positive integers defined as follows. Given an elliptic curve E over $\mathbf{Q}$ and a point $P \in E(\mathbf{Q})$ of infinite order, choose a globally minimal Weierstrass equation for E and write for every $Q \in E(\mathbf{Q})$:

$$Q = \left(\frac{A_Q}{D_Q^2}, \frac{C_Q}{D_Q^3} \right), \tag{1.1}$$

where the fractions are in lowest terms. Then set $D_n = D_{nP}$.

A result of Silverman [26] shows that all but finitely many terms D_n have a *primitive divisor*, that is, a prime divisor $p \mid D_n$ such that $p \nmid D_m$ for all $1 \leq m < n$. Equivalently, this says that all but finitely many positive integers n occur as the order of $(P \bmod p)$ for some prime p. The question whether there is a uniform bound N such that D_n has a primitive divisor for all pairs (E, P) and all $n > N$ remains open, see [2], [4], [8], [14].

The definition of D_Q of (1.1) is equivalent to

$$v(D_Q) = \max\{-\frac{1}{2} v(x_v(Q)), 0\} \tag{1.2}$$

for all non-archimedean valuations v and x_v the x-coordinate function for a v-minimal Weierstrass equation. If E and P are defined over a number field F, then we define the *EDS* of the pair (E, P) to be the sequence of ideals $D_n = D_{nP}$ of $\mathcal{O}_F$ defined by (1.2).

Similarly, if E and P are defined over the function field $F = K(C)$ of a smooth, projective, geometrically irreducible curve C over a field K, then we define the *EDS* of the pair (E, P) to be the sequence of divisors $D_n = D_{nP}$ on C defined by (1.2). See Section 1.2 for an equivalent definition in the case of perfect K. Elliptic divisibility sequences over function fields are studied in [6,9,16,28].

From now on, we will speak of *primitive valuations* instead of primitive divisors, so as not to confuse with the terms themselves, which are divisors in the function field case. A positive integer N is a *Zsigmondy bound* of the sequence $(D_n)_n$ if for every $n > N$ the term D_n has a primitive valuation.

Silverman's result and proof are also valid in the number field case [15]. In the case of function fields of characteristic zero, the same result is true, as shown by Ingram, Mahé, Silverman, Stange and Streng [16, Theorems 1.7 and 5.5].

This was extended to ordinary elliptic curves E over function fields of characteristic $\neq 2, 3$ by Naskręcki [21]. Conditionally Naskręcki makes the result uniform in E. The special case of the results of [21] where $j(E)$ is constant gives a Zsigmondy bound N as follows.

- For fields $K(C)$ of characteristic 0 we have $N \leq 72$ (see [12, p. 437] and [21, Lemma 7.1]).

- For fields $K(C)$ with $p = \operatorname{char} K(C) \geq 5$ and field of constants $K = \mathbf{F}_q$, $q = p^s$ we have $N < 10^{100(15+20g(C))} \cdot p^{84}$ for 'tame' elliptic curves (cf. [21, Definition 8.3]) and a bound $N = N(g(C), p, \chi, s)$ for 'wild' ordinary elliptic curves where χ is the Euler characteristic of the elliptic surface attached to E over $K(C)$.

1.1. Our results

All previous Zsigmondy bound estimates exclude the case of supersingular curves. In this paper, we consider the case of function fields $F = K(C)$ and assume $j(E) \in K$, which includes the case of supersingular E. In a companion paper we will deal with the case $j(E) \in F \setminus K$, where we extend the results of Naskręcki [21] to arbitrary characteristic and improve the bound N.

In the ordinary case, we prove a bound $N = 2$ and show that it is optimal. In the supersingular case in characteristic p, we show that the terms D_n for $n > 8p$ have a primitive divisor if and only if $p \nmid n$, and we give a sharp version for every characteristic.

In more detail, the main results are as follows.

Theorem A *(Theorem 8.1). Let F be the function field of a smooth, projective, geometrically irreducible curve over a field K.*

Let E be an ordinary elliptic curve over F and let $P \in E(F)$ be a point of infinite order such that $j(E) \in K$, but the pair (E, P) is not constant, cf. Definition 2.1. Then for all integers $n > 2$, the term D_n has a primitive valuation.

Conversely, for all ordinary j-invariants $j \in K$ there exist an elliptic curve E/F with $j(E) = j$ and a point $P \in E(F)$ of infinite order such that the terms D_1 and D_2 do not have a primitive valuation and there exist an elliptic curve E/F with $j(E) = j$ and a point $P \in E(F)$ of infinite order such that all terms D_n for $n \geq 1$ have a primitive valuation.

Theorem B *(Theorem 8.2). Let F be the function field of a smooth, projective, geometrically irreducible curve over a field of characteristic $p > 0$. Let n be a positive integer.*

If the entry corresponding to n and p in Table 1 is 'yes' (respectively 'no'), then for every supersingular elliptic curve E over F, and every $P \in E(F)$ with (E, P) non-constant and P of infinite order, the term D_n has a (respectively no) primitive valuation.

If the entry is '$*$', then there exist E and P as in the previous paragraph such that D_n has a primitive valuation and there exist E and P such that D_n has no primitive valuation.

In the case where E itself is defined over K (and not just its j-invariant), the result is much stronger, as follows.

Theorem C *(Theorem 2.3). Let F be the function field of a smooth, projective, geometrically irreducible curve over a field K of characteristic $p \geq 0$. Let E be an elliptic curve over K and $P \in E(F) \setminus E(K)$ a point of infinite order. Let n be a positive integer,*

Table 1
Table referred to in Theorem B.

$p = 2$

n	1	$2(=p)$	3	$4(=2p)$	$6(=3p)$	$8(=4p)$	odd $n>4$	even $n>8$
D_n	$*$	$*$	$*$	$*$	$*$	$*$	*yes*	*no*

$p = 3$

n	1	2	$3(=p)$	$6(=2p)$	$9(=3p)$	$n>3$ $3\nmid n$	$n>9$ $3\mid n$
D_n	$*$	$*$	$*$	$*$	$*$	*yes*	*no*

$p \equiv 1 \bmod 3$

n	1	2	3	p	$2p$	$3p$	$n>3$ $p\nmid n$	$n>3p$ $p\mid n$
D_n	$*$	$*$	*yes*	$*$	$*$	*no*	*yes*	*no*

$p \equiv 2 \bmod 3, \quad p \neq 2$

n	1	2	3	p	$2p$	$3p$	$n>3$ $p\nmid n$	$n>3p$ $p\mid n$
D_n	$*$	$*$	*yes*	$*$	$*$	$*$	*yes*	*no*

1. *if $p \nmid n$ or E is ordinary, then D_n has a primitive valuation,*
2. *if $p \mid n$ and E is supersingular, then $D_n = p^2 D_{n/p}$ has no primitive valuation.*

1.2. Alternative definition

We now give a more standard, but more technical, definition of elliptic divisibility sequences over function fields in the case of perfect base fields K. It is proven in [16, Lemma 5.2] that this defines the same sequence $(D_{nP})_n$ in the case of number fields K; and the proof at [16] extends to perfect fields K.

Let E be an elliptic curve over the function field $K(C)$ of a smooth, projective, geometrically irreducible curve C over a perfect field K. Let S be the Kodaira–Néron model of E, i.e., a smooth, projective surface with a relatively minimal elliptic fibration $\pi : S \to C$ with generic fibre E and a section $O : C \to S$, cf. [24, §1], [27, III, §3]. For example, if the curve E is constant (that is, defined over K), then we can take $S = E \times C$ with the natural projection $\pi : E \times C \to C$.

Let P be a point of infinite order in the Mordell–Weil group $E(K(C))$. We define a family of effective divisors $D_{nP} \in \mathrm{Div}(C)$ parametrised by natural numbers n. For each $n \in \mathbf{N}$ the divisor D_{nP} is the pull-back of the image $\overline{O}$ of the section O through the morphism $\sigma_{nP} : C \to S$ induced by the point nP, that is,

$$D_{nP} = \sigma_{nP}^*(\overline{O}).$$

The delicate issues with non-perfect coefficient fields K are discussed in detail in Section 7 and Example 7.6.

1.3. Known results about divisibility sequences over function fields

Elliptic divisibility sequences over function fields $F = K(C)$ and related sequences were discussed in several places. We collect some known results here.

First of all, they satisfy the *strong divisibility property*

$$\gcd(B_m, B_n) = B_{\gcd(m,n)} \tag{1.3}$$

for all positive integers m, n, where $\gcd(B_m, B_n) := \sum_v \min\{v(B_m), v(B_n)\}[v]$. Indeed, the proof in e.g. [30, Lemma 3.3] carries over.

Theorem 1.5 of [16] shows that in case E/K with K a number field (and again $P \in E(F) \setminus E(K)$) the set of prime numbers n such that $D_{nP} - D_{1P}$ is irreducible has positive lower Dirichlet density.

Cornelissen and Reynolds [6] study perfect power terms in the case $j(E) \in F \setminus F^p$ for global function fields F of characteristic $p \geq 5$. Everest, Ingram, Mahé, and Stevens study primality of terms of elliptic divisibility sequences for $K(C) = \mathbf{Q}(t)$ in the context of magnified sequences, see [9, Theorem 1.5]. Silverman [28] and Ghioca-Hsia-Tucker [11] study the common subdivisor for two simultaneous divisibility sequences on elliptic curves over $K(t)$, where K is a field of characteristic 0.

In a broad context, Flatters and Ward [10] prove an analogue of Theorem 8.1 for divisibility sequences of Lucas type for polynomials and Akbar-Yazdani [1] study the greatest degree of the prime factors of certain Lucas polynomial divisibility sequences.

Hone and Swart [13] study examples of Somos 4 sequences over $K(t)$, which are constructed from specific elliptic divisibility sequences. They construct a certain elliptic surface and show that the corresponding sequence is a sequence of polynomials.

1.4. Overview and main ideas of the proof

The main idea behind the proof is to reduce to the case where E is defined over the base field K of $F = K(C)$. In that case $P \in E(F)$ can be viewed as a dominant morphism $C \to E$ over K. The primitive valuations of D_n then are exactly the pull-backs of points of order n on E, which gives Theorem C. For details, see Section 2.

For elliptic curves over F where only the j-invariant is in K, we find an elliptic curve $\widetilde{E}$ over K with the same j-invariant and an isomorphism $\phi : E \to \widetilde{E}$ over $\overline{F}$. Then Theorem 2.3 applies to the sequence $(D_{nP'})_n$ obtained from $(\widetilde{E}, \phi(P))$. See Section 3.

At that point, we know exactly which terms of $(D_{nP'})_n$ have primitive valuations, and the goal is to conclude which terms of $(D_{nP})_n$ have primitive valuations.

For this, we look at the *rank of apparition* $m(v)$ of a valuation v of F in the sequence $(D_{nP})_n$, which is the positive integer

$$m(v) = m(P, v) := \min\{n \geq 1 : \operatorname{ord}_v(D_{nP}) \geq 1\},$$

or ∞ if the set is empty. A valuation v is primitive in the term D_{nP} if and only if $n = m(v)$.

The key to our proof is to see how much the rank of apparition $m(v)$ of a valuation v of $\overline{F}$ can vary between the sequences $(D_{nP})_n$ and $(D_{nP'})_n$. Section 4 shows that this does not vary much, and bounds the variation in terms of the component group of the special fibre of the Néron model.

This is already enough to get a weaker version of the main results, which is not sharp, but is already uniform (Theorems 4.7 and 4.9).

In Section 5 we prove two auxiliary results about the order of a point P in the component group at v. This is needed in the proof of the main theorems to obtain a sharp result.

In Section 6 we show that the term D_{3P} for sequences in characteristic $\neq 2, 3$ always has a primitive valuation if $j(E) = 0$. This is also needed in order to obtain a sharp result.

Section 7 contains examples which we use to show that our main theorems are optimal, that is, to prove the converse statement in Theorem A and the $*$-entries in Theorem B.

Finally, in Section 8 we combine all of the above into a proof of Theorems A and B.

Acknowledgements

The authors would like to thank Peter Bruin and Hendrik Lenstra for helpful discussions and the anonymous referee for comments that improved the exposition.

2. Constant curves

Let C be a smooth, projective, geometrically irreducible curve over a field K and let $F = K(C)$ be its function field. Let E/F be an elliptic curve and $P \in E(F)$ a point. For a field extension $M \supset L$ and an elliptic curve E' over L, let E'_M be the base change of E' to M.

Definition 2.1. We say that E is *constant* if there exists an elliptic curve $\widetilde{E}/K$ and an isomorphism $\phi : E \to \widetilde{E}_F$ defined over F.

We say that the pair (E, P) is *constant* if there exist such $\widetilde{E}$ and ϕ that also satisfy $\phi(P) \in \widetilde{E}(K)$.

We say that the j-invariant $j(E)$ of the curve $E/K(C)$ is *constant* if $j(E) \in K$.

Lemma 2.2. *The pair* (E, P) *is* constant *if and only if* E *is constant and for* all *elliptic curves* $\widetilde{E}/K$ *and isomorphisms* $\phi : E \to \widetilde{E}_F$ *we have* $\phi(P) \in \widetilde{E}(K)$.

Proof. The 'if' implication follows from the definition, so it is enough to prove the 'only if' implication. Suppose that (E, P) is constant. There exists an elliptic curve $\widetilde{E}$ defined over K and an isomorphism $\phi : E \to \widetilde{E}_F$ of F-curves such that $\phi(P) \in \widetilde{E}(K)$. Let $\widetilde{E}'$ be an elliptic curve over K and $\phi' : E \to \widetilde{E}'_F$ another F-isomorphism. Let $\phi \circ {\phi'}^{-1}$:

$\widetilde{E}'_F \to \widetilde{E}_F$ denote the corresponding isomorphism of F-curves. It follows that the curves $\widetilde{E}'_F$ and $\widetilde{E}_F$ have equal j-invariant and since $\widetilde{E}$ and $\widetilde{E}'$ are defined over K there exists a $\overline{K}$-isomorphism $\psi : \widetilde{E}_{\overline{K}} \to \widetilde{E}'_{\overline{K}}$. Let F' denote the function field of the curve $C_{\overline{K}}$. We have

$$\eta \circ \psi_{F'} \circ \phi_{F'} = \phi'_{F'}$$

for some $\eta \in \mathrm{Aut}(\widetilde{E}'_{F'}) = \mathrm{Aut}(\widetilde{E}'_{\overline{K}})$. Since $P \in E(F)$, we have $\phi'(P) \in \widetilde{E}'(F)$. From our assumption it follows that $\phi(P) \in \widetilde{E}(K)$ and hence $\phi'(P) = (\eta \circ \psi_{F'} \circ \phi_{F'})(P) \in \widetilde{E}'(\overline{K})$. Combining these statements, we get $\phi(P) \in \widetilde{E}'(\overline{K} \cap F)$. As C is smooth and geometrically irreducible, it is geometrically integral, hence by [20, Corollary 3.2.14(c)], we get $\overline{K} \cap F = K$. □

2.1. Constant E

Suppose that E is constant. Then without loss of generality we consider $E = \widetilde{E}_F$. Then $P \in E(F)$ can be interpreted as a morphism of curves $P : C \to \widetilde{E}$ defined over K as follows. We give two interpretations, both leading to the same morphism.

Consider the constant elliptic surface (S, π, C) where $S = \widetilde{E} \times C$ and $\pi : S \to C$ is the projection on the second factor. Every point P on the generic fibre E corresponds to a unique section $\sigma_P : C \to S$. Composition $\mu \circ \sigma_P : C \to \widetilde{E}$ of σ_P with the projection $\mu : S \to \widetilde{E}$ on the first factor is a morphism defined over K. By abuse of notation we denote the morphism $\mu \circ \sigma_P$ by P.

Equivalently, the point $P \in E(F)$ has coordinates in $F = K(C)$, hence defines a rational map from C to E. All such rational maps are morphisms as C is smooth and E is projective.

Applying this abuse of notation to nP too, we get $nP = [n] \circ P$.

Note that the pair (E, P) is constant if and only if the morphism $P : C \to \widetilde{E}$ is a constant morphism, or equivalently, maps to a single point.

2.1.1. Constant P

If P maps to a single point, then so does $[n] \circ P$. In particular, for all n either $nP = O$ or the images of $[n] \circ P$ and O are disjoint. If P has infinite order, then this gives for all n:

$$D_{nP} = 0. \tag{2.1}$$

2.1.2. Non-constant P

Let us assume in this section that E is constant and the morphism $P : C \to \widetilde{E}$ is non-constant.

Theorem 2.3. *Let F be the function field of a smooth, projective, geometrically irreducible curve over a field K of characteristic $p \geq 0$. Let E be an elliptic curve over K and $P \in E(F) \setminus E(K)$ a point of infinite order. Let n be a positive integer,*

1. *if $p \nmid n$ or E is ordinary, then D_n has a primitive valuation,*
2. *if $p \mid n$ and E is supersingular, then $D_n = p^2 D_{n/p}$ has no primitive valuation.*

Proof. We have $D_{nP} = ([n] \circ P)^*(O) = P^*[n]^*(O)$. Note that

$$[n]^*(O) = \deg_i([n]) \sum_{Q \in E(\overline{K})[n]} (Q) \tag{2.2}$$

where $\deg_i([n])$ denotes the inseparable degree of $[n]$. If $p \mid n$ and E is supersingular, then the endomorphism $[p]$ is purely inseparable of degree p^2, hence $\deg_i([p \cdot \frac{n}{p}]) = p^2 \deg_i([\frac{p}{n}])$ and $E(\overline{K})[p] = \{O\}$; so formula (2.2) gives $D_n = p^2 D_{n/p}$, which proves (2).

Moreover, if E is ordinary or $p \nmid n$, then $E(\overline{K})$ contains a point Q_n of order n. Since P is a dominant morphism, there is a point that maps to Q_n under P, and the valuation associated with such a point is a primitive valuation of D_{nP}. □

Remark 2.4. The existence of a cover $P : C \to \widetilde{E}$ implies that C has genus greater than or equal to 1.

In fact, as all such covers factor through the identity map $\mathrm{id} : \widetilde{E} \to \widetilde{E}$, we see that for every elliptic curve $\widetilde{E}/K$, there is one prototypical example given by $P = \mathrm{id} : \widetilde{E} \to \widetilde{E}$. In other words, this example has $C = \widetilde{E}$ and $S = \widetilde{E} \times \widetilde{E}$. The point $P \in E(K(E))$ corresponds to the morphism $\mu \circ \Delta$ where $\Delta : \widetilde{E} \to \widetilde{E} \times \widetilde{E}$ is the diagonal map and μ is the projection on the first factor.

Example 2.5. Let $C = \widetilde{E} : y^2 = x^3 + x$ over $K = \mathbf{F}_3$ and $P = (x, y) \in \widetilde{E}(K(\widetilde{E}))$. Let i be a square root of -1 in a quadratic extension of $\mathbf{F}_3$. Then

$$\begin{aligned}
\widetilde{E}(\overline{K})[1] &= \{O\} \\
\widetilde{E}(\overline{K})[2] &= \widetilde{E}(\overline{K})[1] \cup \{(0,0), (\pm i, 0)\} \\
\widetilde{E}(\overline{K})[3] &= \widetilde{E}(\overline{K})[1] \\
\widetilde{E}(\overline{K})[4] &= \widetilde{E}(\overline{K})[2] \cup \{(1, \pm i), (-1, \pm 1), (\pm i + 1, \pm i), (\pm i - 1, \pm 1)\},
\end{aligned}$$

where all the signs are independent. In particular, we obtain

$$\begin{aligned}
D_{1P} &= O \\
D_{2P} &= D_{1P} + (0,0) + (i,0) + (-i,0) \\
D_{3P} &= 9O
\end{aligned}$$

$$D_{4P} = D_{2P} + \sum_{s\in\{\pm 1\}} \left[\begin{array}{l} (1,si)+(-1,s)+(i+1,si) \\ +(-i+1,si)+(i-1,s)+(-i-1,s) \end{array} \right]$$

$$D_{6P} = 9D_{2P}.$$

By symmetry, for $b \neq 0$ the points (a,b) and $(a,-b)$ only appear together. Because of that, we introduce the following notation. Let

$$D'_m = \begin{cases} D_{mP} - \mathrm{ord}_O(D_{mP})O & \text{if } 2 \nmid m, \\ D_{mP} - \mathrm{ord}_O(D_{mP})D_{2P} & \text{if } 2 \mid m. \end{cases}$$

The divisor D'_m is the pull-back $x^*\delta_m$ of an effective divisor δ_m on the affine x-line $\mathbf{A}^1$. Let $p(m)$ denote a monic polynomial with divisor of zeroes equal to δ_m. We get that the divisor D_{nP} has the form

$$D_{nP} = a(n)(O) + b(n)\mathrm{div}_0(y) + \mathrm{div}_0(p(n)), \tag{2.3}$$

where

$$a(n) = 9^{\mathrm{ord}_3(n)},$$

$$b(n) = \begin{cases} 0 & \text{if } n \text{ is odd}, \\ a(n) & \text{if } n \text{ is even}, \end{cases}$$

and we present below only the factorisation of the polynomial $p(n)$.

$$\begin{aligned}
p(1) &= 1 \\
p(2) &= 1 \\
p(3) &= 1 \\
p(4) &= (x+1)\cdot(x+2)\cdot(x^2+x+2)\cdot(x^2+2x+2) \\
p(5) &= (x^4+x+2)\cdot(x^4+2x+2)\cdot(x^4+x^2+2) \\
p(6) &= 1 \\
p(7) &= (x^3+x^2+2x+1)\cdot(x^3+2x^2+2x+2)\cdot(x^6+2x^4+x^2+1) \\
&\quad \cdot(x^6+x^5+2x^4+2x^3+2x^2+2x+1)\cdot(x^6+2x^5+2x^4+x^3+2x^2+x+1) \\
p(8) &= (x+1)\cdot(x+2)\cdot(x^2+x+2)\cdot(x^2+2x+2)\cdot(x^4+x^3+x^2+x+1) \\
&\quad \cdot(x^4+x^3+x^2+2x+2)\cdot(x^4+x^3+2x^2+2x+2) \\
&\quad \cdot(x^4+2x^3+x^2+x+2)\cdot(x^4+2x^3+x^2+2x+1) \\
&\quad \cdot(x^4+2x^3+2x^2+x+2)
\end{aligned}$$

$$
\begin{aligned}
p(9) &= 1\\
p(10) &= (x^4+x+2)\cdot(x^4+2x+2)\cdot(x^4+x^2+2)\cdot(x^4+x^2+x+1)\\
&\quad\cdot(x^4+x^2+2x+1)\cdot(x^4+2x^2+2)\cdot(x^4+x^3+2)\cdot(x^4+x^3+2x+1)\\
&\quad\cdot(x^4+x^3+x^2+1)\cdot(x^4+2x^3+2)\cdot(x^4+2x^3+x+1)\cdot(x^4+2x^3+x^2+1)\\
p(11) &= (x^{10}+x^7+x^5+x^4+2x^3+2x^2+x+2)\\
&\quad\cdot(x^{10}+2x^7+2x^5+x^4+x^3+2x^2+2x+2)\\
&\quad\cdot(x^{10}+2x^8+x^6+x^5+x^2+2x+2)\cdot(x^{10}+2x^8+x^6+2x^5+x^2+x+2)\\
&\quad\cdot(x^{10}+2x^8+x^7+x^6+x^5+2x^4+2x^3+x^2+2)\\
&\quad\cdot(x^{10}+2x^8+2x^7+x^6+2x^5+2x^4+x^3+x^2+2)\\
p(12) &= (x+1)^9\cdot(x+2)^9\cdot(x^2+x+2)^9\cdot(x^2+2x+2)^9
\end{aligned}
$$

This confirms the equality $D_{12P} = 9D_{4P}$ and the fact that terms D_{nP} with $3 \nmid n$ have primitive valuations.

3. Relating constant E to constant j globally

3.1. Definitions and example

Let E be an elliptic curve over $F = K(C)$ and let $P \in E(F)$ be a point of infinite order. Now suppose $j(E) \in K$. Note that this includes the case where E is supersingular by [29, V.3.1(a)(iii)].

The idea behind the proof of our main results is to relate the EDS $(D_{nP})_n$ obtained from P with constant j-invariant to an EDS $(D_{nP'})_n$ obtained from a point on a constant elliptic curve and then to apply Theorem 2.3 to $(D_{nP'})_n$.

Lemma 3.1. *Let K be a field, let C/K be a smooth, projective, geometrically irreducible curve and let $F = K(C)$. Let E/F be an elliptic curve with $j(E) \in K$.*

Then there exist

(i) an elliptic curve $\widetilde{E}/K$ with $j(\widetilde{E}) = j(E)$,
(ii) finite extensions $K' \supset K$ and $F' \supset F$ with $K' \subset F'$,
(iii) an isomorphism $\phi : E_{F'} \to \widetilde{E}_{F'}$,
(iv) a smooth, projective, geometrically irreducible curve C'/K' with $F' = K'(C')$, and
(v) a non-constant morphism $f : C' \to C_{K'}$ inducing the inclusion map $FK' \hookrightarrow F'$.

Notation 3.2. *On top of the notation of Lemma 3.1, we use the following notation. Given a point $P \in E(F)$,*

(vi) let $P' = \phi(P) \in \widetilde{E}(F')$,

(vii) let D_{nP} be the EDS obtained from (E, P) as defined in (1.2), and
(viii) let $D_{nP'}$ be the EDS obtained from $(\widetilde{E}, P')$.

The symbol v will denote a place of C and v' will denote a place of C' lying over v.

Proof. (i) Let $\widetilde{E}/K$ be an elliptic curve with $j(\widetilde{E}) = j(E)$, let $\overline{F}$ be an algebraic closure of F and let $\overline{K} \subset \overline{F}$ be an algebraic closure of K. Then there exists an isomorphism $\phi_{\overline{F}} : E_{\overline{F}} \to \widetilde{E}_{\overline{F}}$ by [29, Proposition III.1.4(b)]. Let $F'' \subset \overline{F}$ be generated over F by the coefficients $b_1, b_2, \ldots, b_r \in \overline{F}$ of $\phi_{\overline{F}}$.

If K is perfect, then we take $F' = F''$ and $K' = (\overline{K} \cap F'')$ (which satisfy (ii) and (iii)) and find by [29, Remark II.2.5] a curve C' satisfying (iv). The inclusion $FK' \subset F'$ then gives the morphism of (v).

If K is not perfect, then this construction does not always give a smooth curve (see Example 3.3), so we do some additional steps in our construction.

The field $F''' := F''\overline{K}$ is a finitely generated extension of transcendence degree 1 over the algebraically closed field $\overline{K}$, hence is the function field of a smooth, projective, (geometrically) irreducible curve $C'_{\overline{K}}/\overline{K}$ by [29, Remark II.2.5].

The inclusion $F\overline{K} \subset F'''$ induces a non-constant rational map $f_{\overline{K}} : C'_{\overline{K}} \to C_{\overline{K}}$, which is a morphism as the curves are regular and projective.

Choose embeddings $i : C \to \mathbf{P}^m$ over K and $j : C'_{\overline{K}} \to \mathbf{P}^n$ over $\overline{K}$. Then embed $C'_{\overline{K}}$ into $\mathbf{P}^n \times (\mathbf{P}^1)^r$ via $j \times b_1 \times \cdots \times b_r$.

(ii, iv) Then let K' be generated over K by the coefficients of a system of defining equations of $C'_{\overline{K}} \subset \mathbf{P}^n \times (\mathbf{P}^1)^r$ and $f_{\overline{K}}$. From now on we view $C'_{\overline{K}}$ as a projective curve C' over K', which is smooth and irreducible over $\overline{K}$. In particular, the curve C' is smooth, projective and geometrically irreducible over K'.

Moreover, the field $F' := K'(C')$ contains the coefficients $b_1, \ldots, b_r$ of $\phi_{\overline{F}}$ since they are coordinate functions on the r copies of $\mathbf{P}^1$. (iii) In particular the morphism $\phi_{\overline{F}}$ can be viewed as a morphism $\phi : E_{F'} \to \widetilde{E}_{F'}$. (v) Similarly K' contains the coefficients of $f_{\overline{K}}$, so $f_{\overline{K}}$ can be viewed as a morphism $f : C' \to C_{K'}$. □

The following two examples illustrate why the proof of Lemma 3.1 is so complicated for non-perfect base fields K. The reader who is interested mostly in the perfect case may wish to skip ahead to Example 3.5.

Example 3.3. Here is an example to show that we cannot just take $F' = F''$ if K is non-perfect. Let $K = \mathbf{F}_2(b)$, $F = K(u)$, and $E : y^2 + u^3 y = x^3 + b$, so $j(E) = 0$. Take $\widetilde{E} : y^2 + y = x^3$ and $\phi : (x, y) \mapsto (u^{-2}x, u^{-3}(y + t))$ where $t \in \overline{F}$ satisfies

$$t^2 + u^3 t + b = 0. \tag{3.1}$$

Then $F'' = F(t) = K(u, t)$ is the function field of a regular, projective, geometrically integral curve over K with affine open part given by (3.1), but this curve is not smooth. Indeed the given model is smooth exactly outside $u = 0$ and is regular at the place $u = 0$.

Example 3.4. To motivate why we embed $C'_{\overline{K}}$ in such a complicated way in the proof, let K be a field of characteristic $\neq 3$ in which -1 is not a square. Let $F = K(t)$, $E : y^2 = x^3+t^2$, $\widetilde{E} : y^2 = x^3-1$, $s = \sqrt[3]{t} \in \overline{F}$, and $\sqrt{-1} \in \overline{F}$. Take $\phi : (x, y) \mapsto (-s^{-2}x, \sqrt{-1}s^{-3}y)$, so $F'' = F(\sqrt{-1}s)$. Then $F''' = \overline{K}(s)$, so we can take $C' = \mathbf{P}^1$ with s as coordinate. The map f is then given by $t = s^3$.

Now we can take i and j to be the identity map. If we had defined K' using only f and the images of i and j, then we would have gotten $K' = K$ and $F' = K'(s) = K(s)$. But then ϕ is not defined over F'.

Here is an example where we compute both $(D_{nP})_n$ and $(D_{nP'})_n$ and compare them.

Example 3.5. Let E be the supersingular elliptic curve over $F = \mathbf{F}_3(t) = \mathbf{F}_3(\mathbf{P}^1)$ given by

$$E : y^2 = x^3 + tx - t \tag{3.2}$$

and let $P = (1, 1) \in E(F)$. We start by computing D_{nP} for a few values of n. The discriminant $\Delta(E)$ is $-t^3$, hence the given model is minimal for all finite places of $\mathbf{P}^1$. Therefore, we can compute these valuations of D_{nP} by computing the square root of the denominator of $x(nP)$. For the valuation at infinity, we take $(x', y') = (t^{-2}x, t^{-3}y)$, so

$$E : {y'}^2 = {x'}^3 + t^{-3}x' - t^{-5}, \qquad (x'(P), y'(P)) = (t^{-2}, t^{-3}),$$

which is minimal since the discriminant $-t^{-9}$ has valuation 9.

To keep the notation short, we write $p(t) \cdot \infty^k$ with $p(t) \in \mathbf{F}_3(t)$ to mean $\operatorname{div}_0(p(t)) + k(\infty) := \sum_{v \neq \infty} \operatorname{ord}_v(p(t))(v) + k(\infty)$. In this notation, we compute

$$\begin{aligned}
D_{1P} &= D_{2P} = 1, & D_{3P} &= t^2,\\
D_{4P} &= (t+2)^3, & D_{5P} &= (t^2+t+2)^3,\\
D_{6P} &= t^2 \cdot \infty^3, & D_{7P} &= (t+1)^3 \cdot (t^3+t^2+t+2)^3,\\
D_{8P} &= (t+2)^3 \cdot (t^4+2t^3+t+1)^3, & D_{9P} &= t^{20},\\
D_{10P} &= (t^2+t+2)^3 \cdot (t^2+2t+2)^3 & & \\
&\quad \cdot (t^4+t^3+t^2+1)^3, & & \\
D_{11P} &= (t^{10}+2t^9+2t^8+t^7+t^6+2t^5 & & \\
&\quad + 2t^4+2t^3+2t^2+1)^3, & D_{12P} &= t^2 \cdot (t+2)^{27} \cdot \infty^3.
\end{aligned}$$

All terms D_{nP} with $3 \nmid n$ listed here have a primitive valuation except D_{1P} and D_{2P}. All terms D_{nP} with $3 \mid n$ listed here have no primitive valuation except D_{3P} and D_{6P}.

As $j(E) = 0$, we find that E is isomorphic over $\overline{F}$ to

$$\widetilde{E} : Y^2 = X^3 + X. \tag{3.3}$$

Next, we look for an isomorphism $\phi : E_{\overline{F}} \to \widetilde{E}_{\overline{F}}$. All isomorphisms are given in case II of the proof of Proposition A.1.2(b) of Silverman [29] as

$$X = u^2 x + r, \qquad Y = u^3 y, \qquad \text{where} \tag{3.4}$$

$$u^4 = 1/t, \qquad 0 = r^3 + r + u^2. \tag{3.5}$$

We use the notation $v = -r$ and solve for u and v in (3.5). Choose a 4th root $u \in \overline{F}$ of $1/t$, and take $v \in \overline{F}$ such that $v^3 + v = u^2$. Then $F' = F(u, v)$ is an extension of F of degree 12 and is the function field of the curve

$$C' : u^2 = v^3 + v \tag{3.6}$$

over $K' = K$. The inclusion $F \to F'$ corresponds to the projection

$$u^{-4} : C' \to \mathbf{P}^1 : (v, u) \mapsto u^{-4},$$

which is a 12-fold covering. The isomorphism ϕ given by (3.4) is

$$\begin{aligned} \phi : E_{F'} &\to \widetilde{E}_{F'} \\ (x, y) &\mapsto (u^2 x - v, u^3 y). \end{aligned} \tag{3.7}$$

Then

$$P' = \phi(P) = (u^2 - v, u^3) = (v^3, u^3) = \mathrm{Frob}_3((v, u)) \in \widetilde{E}(F'). \tag{3.8}$$

In other words, if we identify C' with $\widetilde{E}$ via $(X, Y) = (v, u)$, then $P' : C' \to \widetilde{E}$ is the (purely inseparable) 3rd power Frobenius endomorphism Frob_3 (of degree 3). In particular, the EDS $(D_{nP'})_n$ obtained from $(\widetilde{E}, P')$ is 3 times the EDS of Example 2.5.

3.2. The point P' is non-constant

Next we show that if (E, P) is non-constant (cf. Definition 2.1), then the point $P' = \phi(P) \in \widetilde{E}(F')$ of Notation 3.2 is non-constant (that is, not in $\widetilde{E}(\overline{K})$).

Lemma 3.6 *(Tate normal form). Let E be an elliptic curve over a field L and let $P \in E(L)$ be a point of order ≥ 4. Then there are unique $b, c \in L$ and a change of coordinates over L such that*

$$E : y^2 + (1 - c)xy - by = x^3 - bx^2, \qquad P = (0, 0). \tag{3.9}$$

Proof. Starting with a general Weierstrass equation, first translate to get $P = (0, 0)$ (allowed as $P \neq O$). Then we have $E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x$.

With $y \mapsto y - a_4/a_3 x$ (allowed as $2P \neq O$), we get $a_4 = 0$. With $(x, y) \mapsto (u^2 x, u^3 y)$ and $u = a_2/a_3$ (allowed as $3P \neq O$), we get $a_2 = a_3$. Then let $b = -a_2$ and $c = 1 - a_1$. This proves existence.

Unicity follows as we used up all freedom for changes of Weierstrass equations $(x, y) \mapsto (u^2 x + r, u^3 y + u^2 s x + t)$ as in [29, III.3.1(b)]. □

Corollary 3.7. *Let K, F, E, $\widetilde{E}$, P, and P' be as in Notation 3.2 (this includes $j(E) \in K$). Suppose that P has order ≥ 4. If P' is constant (that is, is in $\widetilde{E}(\overline{K})$), then the pair (E, P) is constant as in Definition 2.1.*

Proof. If $P' \in \widetilde{E}(\overline{K})$, then the Tate normal form of $(\widetilde{E}, P')$ has b, $c \in \overline{K}$. The Tate normal form of (E, P) has b, $c \in F$. By uniqueness of the Tate normal form over $\overline{F}$, we get b, $c \in \overline{K} \cap F = K$, hence (E, P) is isomorphic over F to a pair defined over K. □

In particular, in our case where P has order $\infty > 4$, if the pair (E, P) is non-constant, then the point P' is non-constant.

4. Relating constant E to constant j locally

4.1. Reduction modulo primes of curves with constant j

Elliptic curves with constant j-invariant admit only places of good or additive reduction. We show that the valuations v of additive reduction appear early on in the sequence D_{nP} (Lemma 4.1(2–3)), while those of good reduction appear in the same place as in the corresponding constant sequence $D_{nP'}$ (Lemma 4.2).

Recall that the rank of apparition $m(v) = m(P, v)$ of a valuation v of F is the smallest positive integer n such that $v(D_{nP}) > 0$ (with $m(v) = \infty$ if it does not exist).

With the notation as in Notation 3.2, let F_v be the completion of F at v. Let $E_0(F_v)$ (respectively $E_1(F_v)$) be the subgroup of $E(F_v)$ consisting of points that reduce to a non-singular point (respectively the point O) on the reduction of the minimal Weierstrass equation. In particular, we have $v(D_n) > 0$ if and only if $nP \in E_1(F_v)$. Moreover the quotient $E(F_v)/E_0(F_v)$ is the component group of the special fibre of the Néron model of E at v (cf. [27, Corollary IV.9.2] and [5, Theorem 5.5]).

Lemma 4.1. *Let F be the function field of a smooth, projective, geometrically irreducible curve over a field K of characteristic $p \geq 0$. Let E be an elliptic curve over F and let $P \in E(F)$. Let v be a discrete valuation of F with $v(K) = \{0\}$ and $v(F) \neq \{0\}$, and let $d = d_v$ be the order of P in the component group $E(F_v)/E_0(F_v)$.*

1. *If $j(E) \in K$, then E has good or additive reduction at v.*
2. *If E has additive reduction at v, then*

   (a) if $p = 0$, then $m(v) = d$ or $m(v) = \infty$.

(b) if $p > 0$, then $m(v) = d$ or $m(v) = dp$.

3. If E has additive reduction at v, then $d \leq 4$.
4. If $j(E) \in K$, then

(a) if $p \neq 2$, then $d \leq 3$,
(b) if $p \neq 3$ and $j(E) \neq 0$, then $d \mid 4$,
(c) if $p \notin \{2, 3\}$ and $j(E) \neq 0$, then $d \leq 2$.

Proof. (1) As $j(E) \in K$, we have $v(j(E)) \geq 0$, hence E does not have multiplicative reduction at v by [29, Proposition VII.5.1(b) and $j = c_4^3/\Delta$].

(2) Note that $m(v)$ is the order of P in $E(F_v)/E_1(F_v)$. In the additive case, the subgroup $E_0(F_v)/E_1(F_v)$ is isomorphic to the additive group underlying the residue field of v. If $p = 0$, then the latter group is torsion-free, so that $m(v)$ is ∞ or d. If $p > 0$, then the latter group has exponent p, so that $m(v)$ is d or dp. Write $c = \#E(F_v)/E_0(F_v)$, so $d \mid c$. For parts (3) and (4), we will use tables of reduction types to find restrictions on c, hence on d.

If K is perfect, then the reduction types were classified by Kodaira and Néron and can be found in [27, Table 4.1 in §IV.9] (equivalently [29, Table 15.1 in Appendix C]). For general fields K, we need the generalization by Szydlo [32, Theorem 3.1 and Proposition 7.1.1]. All types that are in Szydlo's classification and were not already in the Kodaira-Néron classification have $c \in \{1, 2\}$ by [32, (20) on page 96], so we may assume that we are in one of the cases from the Kodaira-Néron classification.

(3) In the additive reduction case, we get $\#E(F_v)/E_0(F_v) = c$ with $c \in \{1, 2, 3, 4\}$ by [27, Table 4.1].

(4a) Suppose first that K is perfect. If $c = 4$, then the reduction type is I_n^*, hence by the bottom part of [27, Table 4.1], we get $\mathrm{char}(K) = 2$ or $v(j(E)) < 0$. For general fields Theorem 5.1 and Tables 1 and 4 of [32] give the same result.

(4b) In the same way, the case $c = 3$ only happens when $\mathrm{char}(K) = 3$ or $v(j(E)) > 0$. Indeed, the reduction type is IV or IV^*, the same reference works in the perfect case, and in the general case one needs Table 5 in [32] instead of Table 4. Combining (4a) with (4b) gives (4c). □

4.2. Relating $(D_{nP})_n$ with $(D_{nP'})_n$

To prove our main results, we link the EDS $(D_{nP})_n$ obtained from (E, P) to the EDS $(D_{nP'})_n$ obtained from $(\widetilde{E}, P')$. Let v' be a valuation of F' lying over a valuation v of F.

Lemma 4.2. *Let the notation be as in Notation 3.2 and suppose that P has infinite order.*

If E does not have additive reduction at v, then we have $v'(D_{mP'}) = v'(D_{mP})$ for all $m \in \mathbf{Z}_{>0}$.

Proof. Note that $\widetilde{E}_{F'}$ has good reduction at all valuations of F'. Suppose that E does not have additive reduction at v. As $j(E) \in K$, we find that E also has good reduction at v, hence the isomorphism $E_{F'} \to \widetilde{E}_{F'}$ is an isomorphism over the local ring at v', which does not affect the valuation of $x(mP)$. □

Example 4.3. We continue Example 3.5, so $E : y^2 = x^3 + tx - t$ and $P = (1, 1)$. In that example, we saw that the EDS $(D_{nP'})_n$ is 3 times the EDS of Example 2.5, with $X = v$, $Y = u$, $u^2 = v^3 + v$ and $t = u^{-4}$.

We compute the difference $D_{nP'} - D_{nP}$ for the first few terms. To help in this computation, note the following identities.

$$\begin{aligned} &\mathrm{div}_0(t) = \mathrm{div}_0(u^{-4}) = 12(O), \\ &\mathrm{div}_\infty(t) = 4\mathrm{div}_0(u), \qquad \text{where} \qquad \mathrm{div}_0(u) = (0,0) + (i,0) + (-i,0), \end{aligned}$$

and if p is a polynomial with $p(0) \neq 0$ and p^* is its reciprocal, then

$$\mathrm{div}_0(p(t)) = \mathrm{div}_0(p^*(u^4)) = \mathrm{div}_0(p^*((v^3+v)^2)).$$

We obtain

$$\begin{aligned}
D_{1P'} - D_{1P} &= && = 3(O) \\
D_{2P'} - D_{2P} &= && = 3(O) + 3\mathrm{div}_0(u) \\
D_{3P'} - D_{3P} &= 27(O) - 2\mathrm{div}_0(t) && = 3(O) \\
D_{4P'} - D_{4P} &= 3(O) + 3\mathrm{div}_0(u) && \\
&\quad + 3\mathrm{div}_0((v+1)(v+2)(v^2+v+2)(v^2+2v+2)) && \\
&\quad + \ -3\mathrm{div}_0(1+2u^4) && = 3(O) + 3\mathrm{div}_0(u) \\
D_{5P'} - D_{5P} &= && \\
&\quad \mathrm{div}_0((v^4+v+2)(v^4+2v+2)(v^4+v^2+2)) && \\
&\quad + \ -\mathrm{div}_0(1+u^4+2u^8) && = 3(O) \\
D_{6P'} - D_{6P} &= 27(O) + 27\mathrm{div}_0(u) - 2\mathrm{div}_0(t) - 3\mathrm{div}_\infty(t) && = 3(O) + 15\mathrm{div}_0(u) \\
D_{7P'} - D_{7P} &= && = 3(O) \\
D_{9P'} - D_{9P} &= 243(O) - 20\mathrm{div}_0(t) && = 3(O) \\
D_{12P'} - D_{12P} &= \cdots && = 3(O) + 15\mathrm{div}_0(u).
\end{aligned}$$

The difference is indeed only in the valuations lying over the places $t = 0$ and $t = \infty$ of additive reduction of E.

The following lemma shows how much the primitive valuations of the sequence $(D_{nP'})_n$ can be "postponed" to later terms of $(D_{nP})_n$.

Lemma 4.4. *Let K, F, E, P, v, P' and v' be as in Notation 3.2. Suppose that P has infinite order and that E has additive reduction at v. Let $d = d_v$ be the order of P in the component group $E(F_v)/E_0(F_v)$.*

Let $m = m(P, v)$ and $m' = m(P', v')$ be the ranks of apparition of the valuations v and v' in the elliptic divisibility sequences associated to P and P'.

1. *We have $m' \mid d$.*
2. *If K has characteristic 0, then $m = d$ or $m(v) = \infty$.*
3. *If K has characteristic $p > 0$, then $m = d$ or $m = dp$.*

Proof. Parts (2) and (3) are exactly part (2) of Lemma 4.1.

It remains to prove (1). After base-changing to $F'_{v'}$, we get a Weierstrass equation $\widetilde{E}$ over K. As $\widetilde{E}$ is defined over K, it has good reduction at v'. We have an isomorphism $\phi : E_{F'} \to \widetilde{E}_{F'}$. Claim: $\phi(E_0(F_v)) \subset (\widetilde{E}_{F'})_1(F'_{v'})$. Assuming the claim, we get $dP' = \phi(dP) \in (\widetilde{E}_{F'})_1(F'_{v'})$, hence $v(D_{dP'}) > 0$, hence $m' \mid d$. So in order to prove (1), it suffices to prove the claim.

Proof of the claim. By [29, VII.1.3(d)] there are u, r, s, $t \in \mathcal{O}_{v'}$ with $u \neq 0$ such that for all $Q = (x, y) \in E(F'_{v'})$ and $(x', y') = \phi(Q)$:

$$x = u^2 x' + r, \qquad \text{and} \qquad y = u^3 y' + u^2 s x' + t.$$

In fact, we have $v'(u) > 0$ as otherwise E has good reduction already with its model over F_v.

It now suffices to show that for points Q of good reduction (i.e., inside $E_0(F_v)$), we have $x(Q) \not\equiv r$ modulo v. Using a translation of the coordinates x and y of E by the elements r and t of $\mathcal{O}_{v'}$ we may assume without loss of generality that $r = t = 0$ (but now E is given by a non-minimal Weierstrass equation over $F'_{v'}$ and $Q \in E(F'_{v'})$). As we have $v'(u) > 0$, we find from [29, Table III.1.2] that $a_1 \equiv -2s$, $a_2 \equiv s^2$, $a_3 \equiv a_4 \equiv a_6 \equiv 0$, so the reduction of our model of E modulo v' is $y^2 - 2sxy = x^3 + s^2 x^2$. The only point with $x = 0$ is the singular point $(0, 0)$, so $x(Q) \not\equiv 0$ modulo v'. This proves the claim. □

Example 4.5. In Example 4.3 the valuations of F at which E has additive reduction are $t = 0$ and $t = \infty$, corresponding respectively to O and $\mathrm{div}_0(u)$ of C'.

The reduction at $t = 0$ is of type II, hence the component group there has order 2. As the point P does not reduce to the singular point, we have $d = 1$. In the sequence, we see $m = m(P, v) = 3 = p$ and $m' = m(P', v') = 1 = d$.

The reduction at $t = \infty$ is of type III^*, hence the component group has order 2. As the point P reduces to the singular point, we have $d = 2$. In the sequence, we see $m = m(P, v) = 6 = dp$ and $m' = m(P', v') = 2 = d$.

In both cases, we have $m' = m(P', v') \leq 2 \leq 4$.

Proposition 4.6. *Let F, E, P be as in Notation 3.2. Suppose that P has infinite order and that (E, P) is non-constant. Let n be a positive integer. If E is supersingular, assume that* $\mathrm{char}(F) \nmid n$. *Then*

1. *D_{nP} has a primitive valuation* or
2. *there is a valuation v of F such that n divides the order d_v of P in the component group $E(F_v)/E_0(F_v)$.*

Proof. Let v' be a primitive valuation of $D_{nP'}$, which exists by Theorem 2.3. Let v be the restriction of v' to F. Then E has good or additive reduction at v by Lemma 4.1(1). If E has good reduction, then $n = m(P', v') = m(P, v)$ by Lemma 4.2. If E has additive reduction, then $n = m(P', v') \mid d_v$ by Lemma 4.4(1). □

As we have $d_v \leq 4$ by Lemma 4.1(3), we get the following result.

Theorem 4.7. *Let E and P be as in Notation 3.2. Suppose that E is ordinary, that P has infinite order, and that (E, P) is non-constant. Then for all $n > 4$, the term D_{nP} has a primitive valuation.* □

Proposition 4.8. *Let E be a supersingular elliptic curve over F. Let $P \in E(F)$ be a point of infinite order. Suppose that (E, P) is non-constant. Let n be a positive integer. Then*

1. *D_{npP} has no primitive valuation* or
2. *there is a valuation v of F such that n divides the order d_v of P in the component group $E(F_v)/E_0(F_v)$.*

Proof. If D_{npP} has no primitive valuation, then we are done. Otherwise, let v be such a primitive valuation, so $m(P, v) = np$. Let v' be an extension of v to F'. Then E has good or additive reduction at v by Lemma 4.1(1). If E has good reduction, then $m(P', v') = m(P, v) = np$ by Lemma 4.2, but that contradicts Theorem 2.3. If E has additive reduction, then Lemma 4.4(3) gives $np = m(P, v) \mid d_v p$, so $n \mid d_v$. □

As we have $d_v \leq 4$ by Lemma 4.1(3), Propositions 4.6 and 4.8 imply the following result.

Theorem 4.9. *Let F, E, P be as in Notation 3.2. Suppose that E is supersingular, that P has infinite order, and that (E, P) is non-constant. Let p be the characteristic of F. Then*

1. *for all integers $n > 4$ with $p \nmid n$, the term D_n has a primitive valuation, and*
2. *for all integers $n > 4$, the term D_{pn} has* no *primitive valuation.* □

5. Component groups

In order to sharpen Theorems 4.7 and 4.9 further, we need to look at the component group. In this section we derive extra restrictions on the order d_v of a point in the component group.

By a *local function field*, we mean a completion $K(C)_v$ of the function field $K(C)$ of a smooth, projective, geometrically irreducible curve C over a field K at a discrete valuation v with $v(K) = \{0\}$ and $v(F) \neq \{0\}$.

Proposition 5.1. *Let F be a local function field of characteristic 2 with valuation v and constant field K. Let E be an elliptic curve over F with $j(E) \in K^*$. Then the component group $E(F)/E_0(F)$ does not have an element of order 4.*

Proof. Suppose that the component group $E(F)/E_0(F)$ has an element of order 4. We will show $v(j(E)) \neq 0$, which contradicts our assumption that $j(E)$ is a non-zero constant.

By the tables of reduction types in [27,32] (see the detailed references in the proof of Lemma 4.1(2) above), if $E(F)/E_0(F)$ has an element of order 4, then the elliptic curve E has reduction at v of type I_n^* for some $n = 2m+1$ with $m \geq 0$. By Szydlo [32, Table 7] (see also Theorems 5.1 and 6.1 of [32]), it follows that E has a v-minimal Weierstrass model with

$$v(a_1) \geq 1, \quad v(a_2) = 1, \quad v(a_3) = m+2, \quad v(a_4) \geq m+3, \quad v(a_6) \geq 2m+4. \tag{5.1}$$

As an alternative reference: under the assumption that K is perfect, one can also obtain (5.1) from Dokchitser and Dokchitser [7, Proposition 2], using the fact that (in characteristic 2) $b_6 = a_3^2$.

The j-invariant equals

$$j(E) = \frac{a_1^{12}}{\underbrace{a_1^4(a_2a_3^2 + a_1a_3a_4 + a_4^2 + a_1^2a_6)}_{\alpha} + \underbrace{a_1^3a_3^3}_{\beta} + \underbrace{a_3^4}_{\gamma}}.$$

Let $r = v(a_1)$, so $r \geq 1$. We find $v(\alpha) = v(a_1^4a_2a_3^2) = 4r + 2m + 5$ as all other terms in α have larger valuation.

Write $m = 2r - 1 + A$ for some $A \in \mathbf{Z}$. It follows that

$$v(\alpha) = 8r + 2A + 3, \quad v(\beta) = 9r + 3A + 3, \quad v(\gamma) = 8r + 4A + 4.$$

If $A \geq 0$, then $v(\alpha) < \min\{v(\beta), v(\gamma)\}$ and $v(j(E)) = 4r - 2A - 3$ is odd, hence non-zero. If $A < 0$, then $v(\gamma) < \min\{v(\alpha), v(\beta)\}$ and $v(j(E)) = 4(r - A - 1) > 0$. □

Proposition 5.2. *Let F be a local function field of characteristic 3 with valuation v and constant field K. Let E be an elliptic curve over F with $j(E) \in K^*$. Then the component group $E(F)/E_0(F)$ does not have an element of order 3.*

Proof. Suppose that the component group $E(F)/E_0(F)$ has an element of order 3. Then at the valuation v the elliptic curve E has reduction of type IV or IV^* (same reference as in the proof of Proposition 5.1).

Let $n = 1$ for type IV and $n = 2$ for type IV^*. By [32, Table 4] (see also Theorems 5.1 and 6.1 of [32]), there exists a minimal model of the form

$$y^2 = x^3 + a_2x^2 + a_4x + a_6$$

with

$$v(a_2) \geq n, \quad v(a_4) \geq n+1, \quad v(a_6) = 2n, \quad v(\Delta) \geq 4n. \tag{5.2}$$

The j-invariant of E is

$$j(E) = \frac{\overbrace{2a_2^6}^{\delta}}{\underbrace{2a_2^2a_4^2}_{\alpha} + \underbrace{a_4^3}_{\beta} + \underbrace{a_2^3a_6}_{\gamma}}.$$

We will show $v(j(E)) \neq 0$, which contradicts our assumption that $j(E)$ is a non-zero constant. Let $m = v(a_2) - n$ and $l = v(a_4) - 2n$, hence $m, l \geq 0$. It follows that $v(\delta) = 6m + 6n$, $v(\alpha) = 2m + 2l + 4n + 2$, $v(\beta) = 3l + 3n + 3$ and $v(\gamma) = 3m + 5n$.

- If $l \geq m$, then

$$v(j(E)) = \begin{cases} v(\delta) - v(\beta) = 3m + 3 > 0, \text{ if } n = 2,\ l = m, \\ v(\delta) - v(\gamma) = 3m + n > 0, \text{ otherwise.} \end{cases}$$

- If $l < m$, then

$$v(j(E)) = v(\delta) - v(\beta) = 6m + 3n - 3l - 3 > 0. \quad \square$$

6. The third term when $j = 0$

In this section we give a separate result, with an elementary proof, for the terms D_3 and D_{3p} in the case $j = 0$, because the local considerations of Section 5 do not apply to that case.

We first collect some well-known results about elliptic curves with j-invariant 0 in the following lemma, of which we give a proof for completeness.

Lemma 6.1. *Let E be an elliptic curve with j-invariant 0 over a field L of characteristic $p > 0$.*

1. *If $p \equiv 1 \bmod 3$, then E is ordinary.*
2. *If $p \not\equiv 1 \bmod 3$, then E is supersingular.*
3. *If $p > 3$, then E has a Weierstrass model of the form $y^2 = x^3 + A$ with $A \in L^*$.*
4. *If $p > 3$ and $p \equiv 2 \bmod 3$, then any Weierstrass model as in (3) satisfies*

$$[p]_E(x, y) = \left(A^{-\frac{p^2-1}{3}} x^{p^2}, -A^{-\frac{p^2-1}{2}} y^{p^2}\right).$$

Moreover, all elliptic curves with non-zero j-invariant over fields of characteristic 2 and 3 are ordinary.

Proof. Suppose that $\widetilde{E}$ is an elliptic curve over $\mathbf{F}_p$ with j-invariant 0. Then E and $\widetilde{E}$ are isomorphic over $\overline{L}$, and one is supersingular if and only if the other is (see e.g. [29, V.3.1(a)(i)]). For $p = 2$ (respectively $p = 3$) Example V.4.6 (respectively V.4.5) of [29] gives supersingular $\widetilde{E}/\mathbf{F}_p$ with $j(\widetilde{E}) = 0$. If $p > 3$, then we take $\widetilde{E} : y^2 = x^3 + 1$, which is ordinary if and only if $p \equiv 1 \bmod 3$ by Example V.4.4 of [29].

In characteristic $p > 3$, there is a short Weierstrass equation $y^2 = x^3 + Bx + A$ and as $j(E) = 0$, we get $B = 0$. This proves (3).

Let $a = \sqrt[6]{A} \in \overline{F}$ and $\phi : E \to \widetilde{E} : (x, y) \mapsto (x/a^2, y/a^3)$, where again $\widetilde{E} : y^2 = x^3 + 1$. If $p \equiv 2 \bmod 3$, then we claim $\#\widetilde{E}(\mathbf{F}_p) = p + 1$. Indeed, in that case the map $\mathbf{F}_p \to \mathbf{F}_p : x \mapsto x^3 + 1$ is a bijection, hence so is $\widetilde{E}(\mathbf{F}_p) \to \mathbf{P}^1(\mathbf{F}_p) : (x, y) \mapsto y$, which proves the claim. By [29, Theorem 2.3.1(b) in the Second Edition], we then get $\mathrm{Frob}_p^2 + [p] = 0$ inside $\mathrm{End}(\widetilde{E})$, so $[p]_{\widetilde{E}} : (x, y) \mapsto (x^{p^2}, -y^{p^2})$. We conclude:

$$\begin{aligned}
[p]_E(x, y) &= \phi^{-1} \circ [p]_{\widetilde{E}} \circ \phi(x, y) \\
&= (a^2 (x/a^2)^{p^2}, -a^3 (y/a^3)^{p^2}) \\
&= (A^{-2\frac{p^2-1}{6}} x^{p^2}, -A^{-3\frac{p^2-1}{6}} y^{p^2}),
\end{aligned}$$

which proves (4).

For the final remark, it suffices to know that there is exactly one supersingular j-invariant in each characteristic $p \in \{2, 3\}$. But this follows from the formula for the number of supersingular j-invariants in Corollary 12.4.6 of Katz-Mazur [19] (that formula needs the order of the automorphism group of the elliptic curve with j-invariant zero, which is computed in Proposition A.1.2(c) of [29]). □

Proposition 6.2. *Let K be a field of characteristic $p \geq 0$ with $p \neq 2, 3$, let C be a smooth, projective, geometrically irreducible curve over K and let $F = K(C)$. Let E be an elliptic curve over F with j-invariant 0 and let $P \in E(F)$ be a point of infinite order.*

If the pair (E, P) is not constant, then the term D_{3P} has a primitive valuation.

Proof. As the characteristic is not 2 or 3 and the j-invariant is 0, we get a Weierstrass equation $y^2 = x^3 + A$ with $A \in F^*$ (cf. Lemma 6.1(3)). If $A \in (F^*)^6 K^*$, then E is isomorphic over F to a curve over K and the result is a special case of Theorem 2.3. So we restrict to the remaining case: $A \notin (F^*)^6 K^*$. Write $P = (x_1, y_1) \in E(F)$. We claim that x_1^3/A is non-constant. Indeed, suppose it is $c \in K$. If $c = 0$, then P is 3-torsion, contradiction. So $c \in K^*$ and $y_1^2/A = c+1$. If $c = -1$, then P is 2-torsion, contradiction. So we get $c + 1 \in K^*$. Now compute

$$A = x_1^3 c^{-1} = y_1^2 (c+1)^{-1}, \qquad \text{so} \tag{6.1}$$

$$A = \frac{A^3}{A^2} = \left(\frac{y_1}{x_1}\right)^6 \frac{c^2}{(c+1)^3} \in (F^*)^6 K^*. \tag{6.2}$$

Contradiction, hence x_1^3/A is non-constant.

As a consequence, the function $h = x_1^3/A + 4$ is also non-constant, so let v be a valuation of F with $v(h) > 0$. We obtain $3v(x_1) - v(A) = v(h-4) = 0$ and $2v(y_1) - v(A) = v(h-3) = 0$, hence $v(A) \in 3\mathbf{Z} \cap 2\mathbf{Z} = 6\mathbf{Z}$. By the transformation $A \mapsto u^6 A$, $x \mapsto u^2 x$, $y \mapsto u^3 y$, which does not change h, we then get $v(A) = 0$, hence $v(x_1) = 0$. Write $x_3 = x(3P)$, which we compute to be

$$x_3 = \frac{x_1^9 - 96Ax_1^6 + 48A^2x_1^3 + 64A^3}{9x_1^2(x_1^3 + 4A)^2}. \tag{6.3}$$

Recall $v(x_1) = v(A) = 0$ and $v(x_1^3 + 4A) > 0$. In particular, the valuation of the denominator of this expression for x_3 is positive. The numerator is congruent to $-(12A)^3$ modulo $x_1^3 + 4A$, hence is $\not\equiv 0$ modulo v. We conclude $v(x_3) < 0$ and $v(x_1) = 0$ for the minimal Weierstrass equation $y^2 = x^3 + A$, hence $v(D_{3P}) > 0$ and $v(D_P) = 0$. □

Lemma 6.3. *Let K be a field of characteristic $p > 3$ with $p \equiv 2 \bmod 3$. Let C be a smooth, projective, geometrically irreducible curve over K and let $F = K(C)$.*

Then there exist a supersingular elliptic curve E over F with j-invariant 0 and a point $P \in E(F)$ of infinite order such that D_{3pP} has a primitive valuation and (E, P) is non-constant.

Proof. Take any valuation v and $x_1, y_1 \in F$ with $v(x_1) = v(y_1) = 1$. Let $A = y_1^2 - x_1^3$, let $E : y^2 = x^3 + A$ and let $P = (x_1, y_1) \in E(F)$. Write $3P = (x_3, y_3)$.

Note $v(A) = 2$, hence the model is minimal at v. As $v(x_1^3) > v(A)$, the triplication formula (6.3) gives $v(x_3) = 0$, so $v(D_{3P}) = 0$.

As $v(x_3) = 0$ and $v(A) = 2$, the multiplication-by-p formula of Lemma 6.1 gives $v(x(3pP)) = -\frac{p^2-1}{3} \cdot 2 + p^2 \cdot 0 < 0$, so $v(D_{3pP}) > 0$. As $v(x_1) = 1$ and $v(A) = 2$, the same multiplication-by-p formula also gives $v(x(pP)) = -\frac{p^2-1}{3} \cdot 2 + p^2 > 0$, so $v(D_{pP}) = 0$. We find that v is a primitive valuation of D_{3pP}. As $v(A) = 2 \notin 6\mathbf{Z}$, we find that A is not a 6th power, hence E is not isomorphic to a curve over K, hence the pair (E, P) is non-constant.

Repeated use of the multiplication-by-p formula gives that $v(x(3p^kP))$ is strictly decreasing with k, hence P is non-torsion. □

Example 6.4. Let $K = \mathbf{F}_5$ and $F = K(t)$. As in the proof of Lemma 6.3, take $P = (t, t)$ and $E : y^2 = x^3 + t^2 - t^3$. Then

$$\begin{aligned}
D_{1P} &= D_{2P} = 1, & D_{3P} &= t + 2,\\
D_{4P} &= t^2 + 2t + 4, & D_{5P} &= (t + 4)^4,\\
D_{6P} &= (t + 1) \cdot (t + 2) \cdot (t + 3) \cdot (t^2 + t + 2),\\
D_{7P} &= (t^2 + 2t + 3) \cdot (t^3 + t^2 + 2) \cdot (t^3 + 4t^2 + 3t + 4),\\
D_{8P} &= (t^2 + 2t + 4) \cdot (t^4 + 2t^2 + 2t + 1)\\
&\quad \cdot (t^4 + 3t^3 + 3t^2 + 2t + 2),\\
D_{9P} &= (t + 2) \cdot (t^3 + t + 4) \cdot (t^3 + 3t^2 + 4)\\
&\quad \cdot (t^6 + 3t^4 + 3t^3 + t + 3), & D_{10P} &= (t + 4)^4 \cdot \infty^{12},\\
D_{15P} &= (t + 4)^4 \cdot t^8 \cdot (t + 2)^{25},\\
D_{20P} &= (t + 4)^4 \cdot (t^2 + 2t + 4)^{25} \cdot \infty^{12}.
\end{aligned}$$

And indeed the term D_{15P} has a primitive valuation t.

7. Additional examples

In this section we gather examples that are crucial for the proof of optimality in the main theorems. In our examples, the function field F is always $F = K(t)$ for a field K, that is, the examples have $C = \mathbf{P}^1$. The following result shows that this suffices, in the sense that the existence of such examples implies the existence of examples over all function fields that we consider.

Theorem 7.1. *Let K be a field and let F be the function field of a smooth, projective, geometrically irreducible curve over K. Let E be an elliptic curve over $K(t)$ with $j(E) \in K$ and let $P \in E(K(t))$.*

If there is a rational place in $\mathbf{P}^1(K)$ of good reduction of E, then there exist an embedding $K(t) \hookrightarrow F$, an elliptic curve E' over F, and a point $P' \in E'(F)$ such that

1. *P' and P have the same order,*
2. *E' and E have the same j-invariant, and*
3. *for every valuation v' of F, if v is the restriction to $K(t)$, then*

$$m(P', v') = m(P, v).$$

The main idea for the proof of Theorem 7.1 is to base change via a suitable morphism of base curves. We will use the following results.

We denote by $\mathrm{Br}(f)$ the branch locus of a finite morphism $f : X \to Y$ of normal projective curves over K. This is the image through f of the set of closed points $x \in X$ for which the map f is not étale at x, cf. [20, Definition 7.4.15].

Proposition 7.2. *Let K be a field. Let C and C' be smooth projective curves defined over K. Let $\phi : C' \to C$ be a dominant morphism of curves over K. Let E be an elliptic curve over $K(C)$ and P a point in $E(K(C))$. Let E' denote the elliptic curve obtained from the pull-back by the map ϕ and P' the corresponding point on E'. We assume that the branch locus $\mathrm{Br}(\phi)$ of ϕ is disjoint with the set of places of bad reduction for E. Then for every valuation v' in $K(C')$ above v in $K(C)$ we have*

$$m(P, v) = m(P', v').$$

Proof. If v is a place of good reduction for E and v' is any place above v in $K(C')$, then the elliptic curve E' still has good reduction at v' and the order of the point P' modulo v' is the same as the order of the point P modulo v.

It remains to prove the result for places of bad reduction, so let v be such a place. Let $R \subset F = K(C)$ (respectively $R' \subset F' = K(C')$) denote the discrete valuation ring with valuation v (respectively v'). From our assumptions and [20, Definition 7.4.15] it follows that the extension R'/R has ramification index 1 and that the corresponding extension k'/k of residue fields is separable.

Let $\mathcal{E}$ be the Néron model of E over R. It follows from [3, Theorem 7.2.1(ii)] that the base change $\mathcal{E}' = \mathcal{E} \otimes_R R'$ is the Néron model of $E_{F'}$ over R'.

Let x (respectively x') be the x-coordinate function of a v-minimal (respectively v'-minimal) Weierstrass equation of E. For a point $Q \in E(F)$, we denote by $\widetilde{Q}$ the corresponding point in $\mathcal{E}(R)$. We have for every point $Q \in E(F)$ that $v(x(Q)) < 0$ holds if and only if $\widetilde{Q}$ restricts to the zero section of the special fibre, that is, satisfies $\widetilde{Q} \otimes_R k = O$ (see [27, Corollary IV.9.2] and [5, Theorem 5.5]). By base-changing from R to R', we see that this happens if and only if $\widetilde{Q'} \in \mathcal{E}(R') = \mathcal{E}'(R')$ satisfies $\widetilde{Q'} \otimes_{R'} k' = O$, hence if and only if $v(x'(Q)) < 0$ holds.

Applying this to $Q = nP$ for any n, we find $v(D_{nP}) > 0$ if and only if $v'(D_{nP'}) > 0$. In particular, we have $m(v, P) = m(v', P')$. □

In order to use Proposition 7.2, we need to find an appropriate morphism ϕ for every function field $F = K(C)$ and suitable examples over $K(t)$ for prime fields K. We use the following result to find such maps.

Theorem 7.3 *(Wild p-Belyi theorem of Katz [18, Lemma 16], [33, Theorem 11]). Let C be a smooth, projective, geometrically irreducible curve defined over a perfect field K of positive characteristic. Then there exists a non-constant morphism $\phi : C \to \mathbf{P}^1_K$ (over K) that is unramified above $\mathbf{A}^1$.* □

Proposition 7.4. *Let K be any field. Let $S \subset \mathbf{P}^1(\overline{K})$ be a finite set and C a smooth, projective, geometrically irreducible curve over K. If S does not contain $\mathbf{P}^1(K)$, then there exists a non-constant morphism $\phi : C \to \mathbf{P}^1_K$ (over K) that is unramified above S.*

[Note that the hypothesis of S not containing $\mathbf{P}^1(K)$ is automatically satisfied if K is infinite.]

Proof. We give a proof in the case where K is infinite and a proof in the case where K is perfect. Together, these two proofs cover all cases.

If K is infinite. Let $K(C)$ be the field of functions of C, so $\overline{K} \cap K(C) = K$. Since C is smooth, it is geometrically reduced. As the transcendence degree of $K(C)$ is one, it then follows from [20, Proposition 3.2.15] that $K(C)$ is a finite separable extension of a purely transcendental extension $K(t)$ of K. Hence there exists a separable finite morphism $f = t : C \to \mathbf{P}^1_K$. The set $\mathrm{Br}(f)$ is finite by [20, Corollary 4.4.12].

Write $K = \mathbf{A}^1(K) \subset \mathbf{P}^1(K)$ and let s be an element in $K \setminus \mathrm{Br}(f)$, which exists since K is infinite. We define a map $\eta = (x \mapsto 1/(x-s)) \circ f$. It follows that $\mathrm{Br}(\eta)$ does not contain ∞. The set $\{y - x : x \in \mathrm{Br}(\eta), y \in K \cap S\}$ is finite, so there exists an element $s' \in K$ that does not belong to it. The map $\phi = (x \mapsto x + s') \circ \eta$ suffices.

If K is perfect. By Theorem 7.3 there exists a morphism $f : C \to \mathbf{P}^1$ over K with $\mathrm{Br}(f) = \{\infty\}$. Take $s \in \mathbf{P}^1(K) \setminus S$. There exists a fractional linear map $\alpha : \mathbf{P}^1 \to \mathbf{P}^1$ over K which satisfies $\alpha(\infty) = s$. We define $\phi = \alpha \circ f$ and check that it satisfies the claim. □

Question 7.5. In Proposition 7.4 we have assumed that the set S is disjoint from $\mathbf{P}^1(K)$. In our situation this is enough for the applications, but it would be interesting to know in general whether one could drop this assumption. We leave it here as an open question to the reader.

Proof of Theorem 7.1. Let $S \subset \mathbf{P}^1(\overline{K})$ be the set of points such that E has bad reduction at the corresponding place. By assumption, the set S does not contain $\mathbf{P}^1(K)$, so by Proposition 7.4 there is a morphism $\phi : C \to \mathbf{P}^1_K$ that is unramified above S. Let E' (respectively P') be the base change of E (respectively P) to $F = K(C)$ via ϕ. Then (1) and (2) are clearly true, and (3) follows from Proposition 7.2. □

In Theorem 7.1 and Proposition 7.2, we do a change of base curve C, but we do not allow a change of the base field K of the base curve. Indeed, the following example shows that the results are false for inseparable changes of base field K.

Example 7.6. Let $K = \mathbf{F}_3(s)$, $F = K(t)$, $E : y^2 = x^3 + t^6 x + s^2$, and $P = (0, s)$. The discriminant of E is $-t^{18}$, hence E is minimal and of good reduction at all places except $t = 0, \infty$. At $t = 0$, the model is minimal and of reduction type Z_1 in Szydlo's tables [32, Table 4]. At $t = \infty$, we have the model $Y^2 = X^3 + t^{-2}X + t^{-12}s^2$, which is minimal because it has discriminant $-t^{-6}$ of valuation 6.

We get that P is integral, so $D_{1P} = 0$, which has no primitive valuation. Now take $r = -\sqrt[3]{s} \in \overline{K}$, let $K' = K(r) = \mathbf{F}_3(r)$, and let $F' = K'(t) \supset F$. Take $x' = t^{-2}(x + r^2)$ and $y' = t^{-3}y$, so $E' : y'^2 = x'^3 + t^2x' - r^2$ is a model over F', hence E is not minimal at $t = 0$ over F'. In fact, the model E' is minimal and of reduction type Z_1 over F'.

Over F', the resulting point P' satisfies $x'(P') = r^2/t^2$, so $D_{1P'} = (t)$, hence this term has a primitive valuation $t = 0$. We get $m(P, v) > 1 = m(P', v')$.

7.1. General characteristic examples

In the case of ordinary E with characteristic $\neq 2, 3$ and $j(E) \neq 0$, we will see in Theorem 8.1 that every term has a primitive valuation, except possibly D_{1P} and D_{2P}. The following examples show that sometimes these two remaining terms do not have a primitive valuation.

Lemma 7.7. *Let K be a field with $p := \mathrm{char}(K) \neq 2$. Let $j \in K$ be an element, such that if $p = 3$, then $j = 0$. Then there exists an elliptic curve E with $j(E) = j$ defined over the function field $K(t)$ of $\mathbf{P}^1_K$ and a point $P \in E(K(t))$ of infinite order such that*

1. *(E, P) is non-constant,*
2. *E has at least one rational place of good reduction,*
3. *$D_P = D_{2P} = 0$,*
4. *if E is supersingular, then D_{pP} and D_{2pP} have primitive valuations.*

Proof. If $p = 3$, take $a = 1$, $b = 0 \in K$. Otherwise, let $a, b \in K$ be such that

$$\widetilde{E} : y^2 = x^3 + ax + b \tag{7.1}$$

defines an elliptic curve over K with $j(\widetilde{E}) = j$. Let $r = t^3 + at + b \in K[t]$, which is square-free as the discriminant of $\widetilde{E}$ is non-zero. Let

$$E : y^2 = x^3 + r^2ax + r^3b, \tag{7.2}$$

so $j(E) = j(\widetilde{E}) = j$. We find a point $P = (rt, r^2) \in E(F)$. Note that the given Weierstrass equation is minimal at all primes of $K[t]$, and that the point P is integral at all such primes. Moreover, the curve E has places of additive reduction of type I_0^* hence by [25, Corollary 7.5] the point P (which does not have order 1 or 2) has infinite order.

The point P' of Notation 3.2 is $P' = (t, \sqrt{r}) \in \widetilde{E}(K(t, \sqrt{r}))$, which is non-constant. By Lemma 2.2 this proves (1).

Note that $K[t]$ has at most three primes at which E has bad reduction (the roots of r) and for all fields K except $\mathbf{F}_2$ and $\mathbf{F}_3$ there are more than 3 rational points in $\mathbf{A}^1(K)$, hence there is at least one rational place of good reduction. For $K = \mathbf{F}_3$, our choice of r has only one rational root, hence there are two rational affine places of good reduction. This proves (2).

We also find the following Weierstrass equation, which is minimal for the place at infinity of $K[t]$:

$$E : Y^2 = X^3 + t^{-8}r^2aX + t^{-12}r^3b, \qquad X = t^{-4}x, \quad Y = t^{-6}y. \tag{7.3}$$

Then $X(P) = t^{-4}rt$, so P is also integral at that place. We find that P is an integral point, so $D_{1P} = 0$.

The duplication formula gives

$$x(2P) = \frac{1}{4}(3t^2 + a)^2 - 2rt, \tag{7.4}$$

which is integral at all finite places of $K[t]$. We also get

$$X(2P) = \frac{1}{4}(3 + at^{-2})^2 - 2rt^{-3}, \tag{7.5}$$

which is integral at infinity. We find that $2P$ is an integral point, so $D_{2P} = 0$. This proves (3).

Now suppose that E is supersingular. Then $j \in \mathbf{F}_{p^2}$, so we take $a, b \in \mathbf{F}_{p^2}$ from the beginning. If $p = 3$, then we moreover have $j = 0$ and we take $a = 1$, $b = 0$. It remains only to prove that D_{mpP} does have primitive valuations for $m = 1, 2$.

We have $P' = (t, \sqrt{r}) \in \widetilde{E}(K(t, \sqrt{r}))$ and the valuation ∞ that appears in $D_{1P'}$ with multiplicity 1 does not appear in D_{1P}.

Next, we claim $[p] = \psi \circ \mathrm{Frob}_{p^2}$ on $\widetilde{E}$ with $\psi : (x, y) \mapsto (u^2x, u^3y)$ for some $u \in K^*$. If $p > 3$, then the claim follows from [29, Corollary II.2.12], which applies as $\mathbf{F}_{p^2}$ is perfect and $a, b \in \mathbf{F}_{p^2}$. In case $p = 3$, we have $\widetilde{E} : y^2 = x^3 + x$ over $\mathbf{F}_3$ and a direct calculation proves $[3] = \psi \circ \mathrm{Frob}_9$ with $u = -1$, cf. [29, Theorem 2.3.1(b) in the Second Edition].

We conclude that the valuation ∞ appears with multiplicity p^2 in $D_{pP'}$, hence appears in D_{pP} with multiplicity $p^2 - v_\infty(t^{-4}r) \geq p^2 - 8 - v_\infty(r) > -v_\infty(r) > 0$, hence $m(\infty) = p$.

The valuations v at the roots of r, which appear in $D_{2P'}$ do not appear in D_{2P}. They also do not appear in $D_{pP'}$ (otherwise by the strong divisibility property (1.3) and $\gcd(2, p) = 1$ they would appear in $D_{1P'} = 0$), hence they do not appear in D_{pP} either. They do appear with multiplicity p^2 in $D_{2pP'}$, hence appear in D_{2pP} with multiplicity at least $p^2 - v(r) = p^2 - 1 > 0$, thus $m(v) = 2p$. □

Example 7.8 *(Ordinary).* In Lemma 7.7, take $K = \mathbf{F}_5$, $a = b = 1$, so $j(E) = 1$. We obtain

$$D_{1P} = D_{2P} = 1, \qquad D_{3P} = (t + 3) \cdot (t + 4) \cdot (t^2 + 3t + 4),$$
$$D_{4P} = (t^3 + 2t^2 + 4t + 4) \cdot (t^3 + 3t^2 + 4), \qquad D_{5P} = (t^2 + 2t + 4)^5 \cdot \infty^2$$

where D_{1P} and D_{2P} are trivial, as we already saw in Lemma 7.7.

7.2. Examples in characteristic 3

Example 7.9 *(Ordinary).* Let K be a field of characteristic 3 and let $j \in K^*$. We consider the elliptic curve

$$E_0 : y^2 = x^3 + j^2x^2 + 2j^5$$

with j-invariant j. We consider the quadratic twist $E_0^{(d)}$ of the curve E_0 over $K(t)$ where $d = t^3 + j^2t^2 + 2j^5$. The curve $E_0^{(d)} : y^2 = x^3 + j^2dx^2 + 2j^5d^3$ is non-constant and has j-invariant j and discriminant $j^{11}d^6$.

This is a generic fibre of a Kummer K3 surface with places of bad reduction only at the roots of $d = 0$ and at $t = \infty$, all of type I_0^* (by e.g. [32, Table 4]). On the curve $E_0^{(d)}$ we have a point $P = (t \cdot d, d^2)$ of height 1 (hence non-torsion cf. [24]) which satisfies the condition $D_P = D_{2P} = 1$, since $x(2P) = t^4 + 2j^5t + j^7$.

Example 7.10 *(Supersingular).* Let K be a field of characteristic 3. We consider the curve

$$E_t : y^2 = x^3 + t^3x + t^4$$

over $K(t)$, which has a point $P = (0, t^2)$. The discriminant of the equation E_t is $2t^9$, hence there is no place of bad reduction away from $0, \infty$. By [32, §5 and Table 4] the reduction type at $t = 0$ is IV^* and at $t = \infty$ is III and our model is minimal at all places. By Shioda's height formula [24, Theorem 8.6] the point P has height $1/6$ hence is non-torsion. A direct computation of the divisors D_{nP} reveals

$$D_{1P} = D_{2P} = D_{3P} = 1, \quad D_{4P} = t + 2, \quad D_{5P} = t^2 + t + 2,$$
$$D_{6P} = \infty^2, \quad D_{9P} = t^6, \quad D_{27P} = t^{60}.$$

Remark 7.11. Here is how we came up with the curve and point in Example 7.10. We wanted a pair (E, P) such that $j(E) = 0$, $\operatorname{char} K = 3$, and P is a point of infinite order such that $D_P = 1$, $D_{3P} = 1$, and D_{9P} has a primitive valuation v. Such an elliptic curve E has a Weierstrass model $y^2 = x^3 + Ax + B$ with $A, B \in K(C)$. We look for a valuation v of bad additive reduction for E such that the group of components has order 3, that is, reduction of type IV or IV^* at v (see the proof of Lemma 4.1). Moreover, the point P should intersect a non-trivial component at v and the point $3P$ should intersect the component of the zero section but should not be zero itself. Automatically, by additive reduction in characteristic 3, the point $9P$ then hits the zero section at v.

From [22] it follows that there are only two possible structures for the Néron-Severi group of a rational elliptic surface $\mathcal{E} \to \mathbf{P}^1$ over an algebraically closed field of any characteristic which admit a primitive embedding of the lattice E_6 (which corresponds to the reduction type IV^*), namely $U \oplus E_6 \oplus A_1 \oplus \langle 1/6 \rangle$ (type 49) and $U \oplus E_6 \oplus A_2^*$ (type 27). Over the complex numbers both types of the Néron-Severi group exist, cf. [23].

An example of such an elliptic surface with type 49 over an algebraically closed field of characteristic 3 was constructed in [17, 4.2.18, case 6A, 5.]. The generic fibre over $\mathbf{F}_3(t)$ of that surface is $E_{49,t}$ where for $s \in \mathbf{F}_3(t)$, we define

$$E_{49,s} : y^2 = x^3 + s^3(s+2)x + s^4(s^2+s+1).$$

It has reduction of type III at $t = -2$, reduction type IV^* at $t = 0$ and no other singular fibres.

It is easy to verify that E_t from Example 7.10 is isomorphic over $\mathbf{F}_3(t)$ to $E_{49,\frac{t}{2+t}}$.

7.3. Examples in characteristic 2

Example 7.12 *(Supersingular).* We consider a rational elliptic surface with Weierstrass equation:

$$y^2 + ty = x^3 + t^2 x$$

over $K(t)$ for any field K of characteristic 2. We have that $j(E) = 0$ so the curve is supersingular. The equation above has discriminant t^4, hence there is no bad reduction away from $0, \infty$. It has bad additive reduction at $t = 0$ (type IV) and at $t = \infty$ (type I_1^*) over $K(t)$ by the extended Tate algorithm in [32] (Table 5 for $t = 0$ and Table 7 for $t = \infty$ with the model $y^2 + t^2 y = x^3 + tx^2$). From the Oguiso-Shioda classification [22] it follows that the rank of the group $E(\overline{K}(t))$ is 1 and the group is freely generated by a point of height $1/12$. We checked that the point $P = (t, 0)$ satisfies this condition.

It is easy to verify that the divisors D_P, D_{2P}, D_{3P} and D_{4P} are trivial and D_{6P} is supported at $t = 0$ and D_{8P} is supported at $t = \infty$. More precisely,

$$\begin{aligned}
D_{1P} &= D_{2P} = D_{3P} = D_{4P} = 1, & D_{5P} &= t+1,\\
D_{6P} &= t, & D_{7P} &= t^2+t+1,\\
D_{8P} &= \infty^2, & D_{9P} &= t^3+t^2+1,\\
D_{10P} &= (t+1)^4, & D_{11P} &= (t^5+t^4+t^3+t^2+1),\\
D_{12P} &= t^5, & D_{13P} &= (t^3+t+1)\cdot(t^4+t+1),\\
D_{14P} &= (t^2+t+1)^4, & D_{15P} &= (t+1)\cdot(t^8+t^7+t^3+t+1),\\
D_{16P} &= \infty^{10}, & D_{17P} &= (t^4+t^3+t^2+t+1)\\
& & &\quad\cdot(t^8+t^7+t^6+t^5+t^4+t^3+1),\\
D_{18P} &= t\cdot(t^3+t^2+1)^4, & D_{19P} &= (t^6+t^4+t^3+t+1)\\
& & &\quad\cdot(t^9+t^6+t^4+t^3+1),\\
D_{20P} &= (t+1)^{16}.
\end{aligned}$$

Example 7.13 *(Supersingular).* Let $E_k : y^2 + t^{2k}y = x^3 + t^2(t+1)x^2 + tx$, $k \geq 1$ be an elliptic curve over $K(t)$ for any field K of characteristic 2. The curve E_k has discriminant t^{8k} and no bad reduction away from $0, \infty$. We apply the extended Tate algorithm [32] to the places $t = 0$ and $t = \infty$. For $t = 0$ our model is minimal for each k and of type III. For $k = 1$ the model of E_k with $s = 1/t$

$$y^2 + s^4 y = x^3 + (s + s^2)x^2 + s^7 x$$

is minimal at $s = 0$ ($t = \infty$) and of reduction type I_5^* by the extended Tate algorithm and Table 7, cf. [32]. For $k = 2$ the model of E_k with $s = 1/t$

$$y^2 + s^2 y = x^3 + (s + s^2)x^2 + s^7 x$$

is minimal at $s = 0$ and of type I_1^*.

There exists a point $P = (0, 0)$ on E_k which is not of order 2 or 4, hence it is of infinite order on this curve by [25, Corollary 7.5].

(a) If $k = 1$, then D_{2P} and D_{4P} have a primitive valuation. More precisely,

$$D_{1P} = 1, \quad D_{2P} = t, \quad D_{3P} = (t^2 + t + 1) \cdot (t^3 + t + 1), \quad D_{4P} = t^6 \cdot \infty^2.$$

(b) If $k = 2$, then D_{2P} and D_{8P} have a primitive valuation. More precisely,

$$D_{1P} = 1, \quad D_{2P} = t^3, \quad D_{3P} = t^9 + t^8 + 1, \quad D_{4P} = t^{16},$$
$$D_{6P} = t^3 \cdot (t^9 + t^8 + 1)^4, \quad D_{8P} = t^{68} \cdot \infty^2.$$

Example 7.14 *(Ordinary).* Let K be a field of characteristic 2 and $j \in K^*$. For any $a \in K(t) \setminus K$ we have an elliptic curve

$$E_a : y^2 + xy = x^3 + (a + \frac{1}{a^2 j})x^2 + \frac{1}{j}$$

with a point $P = (a, 0)$. Let $a = t$. Then E_t is a generic fibre of an elliptic K3 surface with bad reduction at $t = 0$ and $t = \infty$. If j is a square in K, then we have type I_4^* at $t = 0$ and otherwise this is type K_8 according to [32, §5.1, §5.2]. In both cases the model

$$E_{min} : (y')^2 + tx'y' = (x')^3 + (t^3 + \frac{1}{j})(x')^2 + t^6 \frac{1}{j}$$

obtained via a transformation $x = 1/t^2 x'$, $y = 1/t^3 y'$ is minimal at $t = 0$ (see also [31, 6.12] with the model obtained from E_{min} by mapping $x \mapsto x + t^3$).

There is a model at $t = \infty$, of the form (with respect to $t = 1/s$)

$$E_{inf} : (y'')^2 + sx''y'' = (x'')^3 + (\frac{1}{j}s^4 + s)(x'')^2 + \frac{1}{j}s^6.$$

It is minimal and of type I_4^* if j is a square in K and of type T_3 if j is not a square in K, cf. [32] or [31, 6.14]. The point $(t, 0)$ is not a 2-torsion point, hence it is of infinite order by [25, Corollary 7.5]. The point P in the model E_{min} has the form $P_{min} = (t^3, 0)$ and the point $2P_{min}$ on E_{min} satisfies the condition $x(2P_{min}) = t^4 + 1/j$, so the points are integral and integral at infinity, hence the divisors D_P and D_{2P} have empty support.

8. Proof of the main theorems

We now have all the ingredients required for proving the following two main theorems.

Theorem 8.1. *Let F be the function field of a smooth, projective, geometrically irreducible curve over a field K.*

Let E be an ordinary elliptic curve over F and let $P \in E(F)$ be a point of infinite order such that $j(E) \in K$, but the pair (E, P) is not constant, cf. Definition 2.1. Then for all integers $n > 2$, the term D_n has a primitive valuation.

Conversely, for all ordinary j-invariants $j \in K$ there exist an elliptic curve E/F with $j(E) = j$ and a point $P \in E(F)$ of infinite order such that the terms D_1 and D_2 do not have a primitive valuation and there exist an elliptic curve E/F with $j(E) = j$ and a point $P \in E(F)$ of infinite order such that all terms D_n for $n \geq 1$ have a primitive valuation.

Proof. For the first assertion, by Theorem 4.7, it suffices to prove that D_{3P} and D_{4P} each have a primitive valuation. Let p be the characteristic of K.

Proof that D_{3P} has a primitive valuation. Recall that E is ordinary. By Proposition 4.6, in order to show that D_{3P} has a primitive valuation, it suffices to show that for every valuation v of F, the order d_v of P in the component group $E(F_v)/E_0(F_v)$ is not 3.

If $j(E) \neq 0$ and $p \neq 3$, then Lemma 4.1(4b) gives $d_v \neq 3$. If $j(E) \neq 0$ and $p = 3$, then Proposition 5.2 gives $d_v \neq 3$.

If $j(E) = 0$, then $p \neq 2, 3$ by Lemma 6.1(2), so in that case D_{3P} has a primitive valuation by Proposition 6.2.

Proof that D_{4P} has a primitive valuation. Again by Proposition 4.6 it suffices to prove that for every valuation $v \in F$, we have $d_v \neq 4$. If $p \neq 2$, then this is Lemma 4.1(4a). If $p = 2$, then this is Proposition 5.1. This proves the first assertion.

Examples (E, P) where the terms D_{1P} and D_{2P} also have a primitive valuation are trivial to find: just start from an arbitrary pair (E, Q) and take $P = 3Q$.

It remains to find examples (E, P) for every field $F = K(C)$ and every ordinary $j \in K$ where the terms D_{1P} and D_{2P} do not have primitive valuations.

By Theorem 7.1, it suffices to find such examples (E, P) for each rational function field $F = K(t)$, where K ranges over all fields, such that E has good reduction at at least one place of degree one in $\mathbf{P}^1(K)$.

Table 2
Expanded version of Table 1, referred to in Theorem 8.2 and its proof.

$p = 2$

n	1	$2(=p)$	3	$4(=2p)$	$6(=3p)$	$8(=4p)$	odd $n>4$	even $n>8$
D_n	$*$ B, H	$*$ G, BH	$*$ B, H	$*$ G, BH	$*$ H, B	$*$ GH, B	yes A	no A

$p = 3$

n	1	2	$3(=p)$	$6(=2p)$	$9(=3p)$	$n>3$ $3\nmid n$	$n>9$ $3\mid n$
D_n	$*$ B, FI	$*$ B, FI	$*$ F, BI	$*$ FI, B	$*$ I, B	yes A	no A

$p \equiv 1 \bmod 3$

n	1	2	3	p	$2p$	$3p$	$n>3$ $p\nmid n$	$n>3p$ $p\mid n$
D_n	$*$ B, F	$*$ B, F	yes CD	$*$ F, B	$*$ F, B	no D	yes A	no A

$p \equiv 2 \bmod 3, \quad p \neq 2$

n	1	2	3	p	$2p$	$3p$	$n>3$ $p\nmid n$	$n>3p$ $p\mid n$
D_n	$*$ B, F	$*$ B, F	yes C	$*$ F, B	$*$ F, B	$*$ E, B	yes A	no A

For K of characteristic not 2 or 3, and any ordinary j-invariant $j \in K$, Lemma 7.7 does the trick. Note that the example has at most three affine places of bad reduction and there are more than 3 rational affine places in $\mathbf{P}^1(K)$, hence at least one rational place of good reduction. We obtain $D_{1P} = D_{2P} = 0$, hence no primitive valuations.

Suppose that K has characteristic 2 or 3 and that $j \in K$ is an ordinary j-invariant. Then $j \neq 0$, so $j \in K^*$. For K of characteristic 3, we have Example 7.9 for any $j \in K^*$. Then $d(0) \in K^*$, hence E has good reduction at the affine rational place $t = 0$. We obtain $D_{1P} = D_{2P} = 0$, hence no primitive valuations.

For K of characteristic 2, we have Example 7.14 for any $j \in K^*$. It has good reduction at $t = 1$. We obtain $D_{1P} = D_{2P} = 0$, hence no primitive valuations. □

Theorem 8.2. *Let F be the function field of a smooth, projective, geometrically irreducible curve over a field of characteristic $p > 0$. Let n be a positive integer.*

If the entry corresponding to n and p in Table 2 is 'yes' (respectively 'no'), then for every supersingular elliptic curve E over F, and every $P \in E(F)$ with (E, P) non-constant and P of infinite order, the term D_n has a (respectively no) primitive valuation.

If the entry is '$*$', then there exist E and P as in the previous paragraph such that D_n has a primitive valuation and there exist E and P such that D_n has no primitive valuation.

Proof. For each entry, the letter(s) below it refer(s) to one or more of the proofs listed below. In case of $*$, the letters before the comma refer to examples where the term has

a primitive valuation, and the letters after the comma to examples where it does not. If multiple letters are given, then each separately gives a complete proof.

By Proposition 4.6, in order to prove that D_{nP} has a primitive valuation for $p \nmid n$, it suffices to prove for every additive valuation v of F that n does not divide the order d_v of P in the component group $E(F_v)/E_0(F_v)$.

By Proposition 4.8, in order to prove that D_{npP} has no primitive valuation, it also suffices to prove for every additive valuation v of F that n does not divide the order d_v of P in the component group $E(F_v)/E_0(F_v)$.

A. Lemma 4.1(3) states $d_v \leq 4$, and if $p \neq 2$, then Lemma 4.1(4a) states $d_v \neq 4$.
B. Take any pair (E, Q) with $Q \in E(F)$ of infinite order. Then for $P = 5Q$, the pair (E, P) is such an example. To see this, apply the result in the final two columns (or Theorem 4.9) to (E, Q).
C. Here $p > 3$. If $j(E) \neq 0$, then $d_v \neq 3$ by Lemma 4.1(4b). If $j(E) = 0$, then D_{3P} has a primitive valuation by Proposition 6.2.
D. Here $p \equiv 1 \bmod 3$, so $j(E) \neq 0$ by Lemma 6.1(1). But then $d_v \neq 3$ by Lemma 4.1(4b).
E. This is Lemma 6.3.

To prove the cases with $*$, by Theorem 7.1, it suffices to find examples (E, P) for each rational function field $F = K(t)$ (over every field K of the appropriate characteristic) such that E has good reduction at at least one place of degree one in $\mathbf{P}^1(K)$. The following are such examples.

F. Lemma 7.7 gives examples for all characteristics $p \geq 3$ where D_{1P} and D_{2P} do not have primitive valuations, and D_{pP} and D_{2pP} do. They have good reduction at at least one place.
G. In Example 7.13(a) the terms D_{2P} and D_{4P} have primitive valuations. In Example 7.13(b) the terms D_{2P} and D_{8P} have primitive valuations. These examples are supersingular over $\mathbf{F}_2(t)$ and have good reduction at $t = 1$.
H. Example 7.12 gives a supersingular elliptic curve and point in characteristic 2, where D_{nP} has a primitive valuation for $n = 6$ and $n = 8$, but not for $n \leq 4$. It has good reduction at the rational place $t = 1$.
I. Example 7.10 gives a supersingular elliptic curve and point in characteristic 3 such that D_{nP} has a primitive valuation for $n = 6$ and $n = 9$, but not for $n \leq 3$. It has good reduction at the rational place $t = 1$. □

References

[1] A. Akbary, S. Yazdani, On the greatest prime factor of some divisibility sequences, in: SCHOLAR—A Scientific Celebration Highlighting Open Lines of Arithmetic Research, in: Contemp. Math., vol. 655, Amer. Math. Soc., Providence, RI, 2015, pp. 1–13.
[2] Y. Bilu, G. Hanrot, P.M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, J. Reine Angew. Math. 539 (2001) 75–122, https://doi.org/10.1515/crll.2001.080, with an appendix by M. Mignotte.

[3] S. Bosch, W. Lütkebohmert, M. Raynaud, Néron Models, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) (Results in Mathematics and Related Areas (3)), vol. 21, Springer-Verlag, Berlin, 1990.
[4] J.H. Cheon, S.G. Hahn, The orders of the reductions of a point in the Mordell-Weil group of an elliptic curve, Acta Arith. 88 (3) (1999) 219–222, https://doi.org/10.4064/aa-88-3-219-111.
[5] B. Conrad, Minimal models for elliptic curves, preprint, available at, http://math.stanford.edu/~conrad/papers/minimalmodel.pdf, 2015.
[6] G. Cornelissen, J. Reynolds, The perfect power problem for elliptic curves over function fields, N.Y. J. Math. 22 (2016) 95–114, http://nyjm.albany.edu:8000/j/2016/22_95.html.
[7] T. Dokchitser, V. Dokchitser, A remark on Tate's algorithm and Kodaira types, Acta Arith. 160 (1) (2013) 95–100, https://doi.org/10.4064/aa160-1-6.
[8] G. Everest, G. Mclaren, T. Ward, Primitive divisors of elliptic divisibility sequences, J. Number Theory 118 (1) (2006) 71–89.
[9] G. Everest, P. Ingram, V. Mahé, S. Stevens, The uniform primality conjecture for elliptic curves, Acta Arith. 134 (2) (2008) 157–181.
[10] A. Flatters, T. Ward, A polynomial Zsigmondy theorem, J. Algebra 343 (2011) 138–142, https://doi.org/10.1016/j.jalgebra.2011.07.010.
[11] D. Ghioca, L.-C. Hsia, T. Tucker, A variant of a theorem by Ailon-Rudnick for elliptic curves, Pac. J. Math. 295 (1) (2018) 1–15, https://doi.org/10.2140/pjm.2018.295.1.
[12] M. Hindry, J.H. Silverman, The canonical height and integral points on elliptic curves, Invent. Math. 93 (2) (1988) 419–450.
[13] A.N.W. Hone, C. Swart, Integrality and the Laurent phenomenon for Somos 4 and Somos 5 sequences, Math. Proc. Camb. Philos. Soc. 145 (1) (2008) 65–85, https://doi.org/10.1017/S030500410800114X.
[14] P. Ingram, Elliptic divisibility sequences over certain curves, J. Number Theory 123 (2) (2007) 473–486.
[15] P. Ingram, J.H. Silverman, Uniform estimates for primitive divisors in elliptic divisibility sequences, in: Number Theory, Analysis and Geometry, Springer, New York, 2012, pp. 243–271.
[16] P. Ingram, V. Mahé, J.H. Silverman, K.E. Stange, M. Streng, Algebraic divisibility sequences over function fields, J. Aust. Math. Soc. 92 (1) (2012) 99–126.
[17] T. Jarvis, W.E. Lang, G. Rimmasch, J. Rogers, E.D. Summers, N. Petrosyan, Classification of singular fibers on rational elliptic surfaces in characteristic three, Commun. Algebra 33 (12) (2005) 4533–4566, https://doi.org/10.1080/00927870500274861.
[18] N.M. Katz, Travaux de Laumon, Astérisque 4 (161–162) (1988) 105–132, Exp. No. 691 (1989), séminaire Bourbaki, Vol. 1987/88.
[19] N.M. Katz, B. Mazur, Arithmetic Moduli of Elliptic Curves, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985.
[20] Q. Liu, Algebraic Geometry and Arithmetic Curves, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002.
[21] B. Naskręcki, Divisibility sequences of polynomials and heights estimates, N.Y. J. Math. 22 (2016) 989–1020.
[22] K. Oguiso, T. Shioda, The Mordell-Weil lattice of a rational elliptic surface, Comment. Math. Univ. St. Pauli 40 (1) (1991) 83–99.
[23] U. Persson, Configurations of Kodaira fibers on rational elliptic surfaces, Math. Z. 205 (1) (1990) 1–47, https://doi.org/10.1007/BF02571223.
[24] T. Shioda, On the Mordell-Weil lattices, Comment. Math. Univ. St. Pauli 39 (2) (1990) 211–240.
[25] T. Shioda, M. Schütt, Elliptic surfaces, in: J.H. Keum, S. Kondō, K. Konno, K. Oguiso (Eds.), Algebraic Geometry in East Asia – Seoul 2008, in: Adv. Stud. Pure Math., Mathematical Society of Japan, Tokyo, 2010, pp. 51–160.
[26] J.H. Silverman, Wieferich's criterion and the *abc*-conjecture, J. Number Theory 30 (2) (1988) 226–237.
[27] J.H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.
[28] J.H. Silverman, Common divisors of elliptic divisibility sequences over function fields, Manuscr. Math. 114 (4) (2004) 431–446.
[29] J.H. Silverman, The Arithmetic of Elliptic Curves, 2nd edition, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.
[30] M. Streng, Divisibility sequences for elliptic curves with complex multiplication, Algebra Number Theory 2 (2) (2008) 183–208.

[31] M. Szydlo, Flat regular models of elliptic schemes, thesis (Ph.D.)–Harvard University, ProQuest LLC, Ann Arbor, MI, 1999, http://gateway.proquest.com/openurl?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&res_dat=xri:pqdiss&rft_dat=xri:pqdiss:9921533.
[32] M. Szydlo, Elliptic fibers over non-perfect residue fields, J. Number Theory 104 (1) (2004) 75–99, https://doi.org/10.1016/j.jnt.2003.06.004.
[33] L. Zapponi, On the 1-pointed curves arising as étale covers of the affine line in positive characteristic, Math. Z. 258 (4) (2008) 711–727, https://doi.org/10.1007/s00209-007-0192-6.