New York Journal of Mathematics

New York J. Math. **28** (2022) 230–249.

Primitive divisors of sequences associated to elliptic curves over function fields

Robert Slob

Abstract. We study the existence of a Zsigmondy bound for a sequence of divisors associated to points on an elliptic curve over a function field. More precisely, let k be an algebraically closed field, let $\mathcal{C}$ be a nonsingular projective curve over k, and let K denote the function field of $\mathcal{C}$. Suppose E is an ordinary elliptic curve over K and suppose there does not exist an elliptic curve E_0 defined over k that is isomorphic to E over K. Suppose $P \in E(K)$ is a non-torsion point and $Q \in E(K)$ is a torsion point of order r. The sequence of points $\{nP + Q\} \subset E(K)$ induces a sequence of effective divisors $\{D_{nP+Q}\}$ on $\mathcal{C}$. We provide conditions on r and the characteristic of k for there to exist a bound N such that D_{nP+Q} has a primitive divisor for all $n \geq N$. This extends the analogous result of Verzobio in the case where K is a number field.

Contents

1. Introduction

Let K be a number field with ring of integers $\mathcal{O}_K$. Let E/K be an elliptic curve that is given by a Weierstrass equation with integral coefficients, and suppose $P \in E(K)$ is a non-torsion point. For each positive integer n, we can write $(x(nP)) = \frac{A_n}{D_n^2}$, where A_n and D_n are coprime ideals in $\mathcal{O}_K$. The sequence of ideals $\{D_n\}$ forms a *divisibility sequence*, meaning that if m and n are positive integers with m dividing n, then D_m divides D_n.

Some famous sequences such as the Mersenne sequence and Lucas sequence are examples of divisibility sequences. The divisibility sequence obtained from

Received March 11, 2021.

2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 11B83, 14H52, 14J27.

Key words and phrases. Elliptic divisibility sequences; primitive divisors; Zsigmondy bound; elliptic curves; function fields; elliptic surfaces.

ISSN 1076-9803/2022

a non-torsion point on an elliptic curve is an example of an *elliptic divisibility sequence*, which were first studied by Morgan Ward [War48]. The book [EvdPSW03, Chapter 10] of Everest et al. gives a gentle introduction into the subject of elliptic divisibility sequences and provides a great historical account. For an interesting connection between matrix divisibility sequences and (elliptic) divisibility sequences, see [CR12]. Additionally, see the introduction of [op. cit.] for some recent research and applications of (elliptic) divisibility sequences.

Returning to our sequence $\{D_n\}$, let n be a positive integer, then we say that D_n has a *primitive divisor* if there exists a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ that divides D_n and does not divide D_m for any $1 \leq m < n$. If $K = \mathbb{Q}$, then D_n is simply an integer, and in this case, it was proved by Silverman in 1988 that there exists a bound N such that D_n has a primitive divisor for all $n \geq N$ [Sil88]. Such a bound is sometimes called a *Zsigmondy bound* in the literature, dating back to Zsigmondy's study of the divisibility sequence $d_n = a^n - b^n$ for $a > b > 0$ positive coprime integers in the late 19th century. Zsigmondy showed that if $n \notin \{1, 2, 6\}$, then d_n has a primitive divisor [Zsi92]. This generalises an earlier result of Bang with b equal to 1, see [Ban86]. An immediate application of the existence of a Zsigmondy bound would be to try and use this result to search for large prime numbers. For this to be computationally feasible, one wants the values D_n to be prime themselves. In this direction, the Chudnovsky brothers found some promising results in 1986 in their experiments for certain values of D_n coming from elliptic divisibility sequences as above [ChC86]. However, later research indicated that these sequences may not be very suitable for this application [EEW01, EMS04]. Nevertheless, there are other applications. Elliptic nets are a generalisation of elliptic divisibility sequences, which have been used by Stange for applications in cryptography [Sta07]. Additionally, there have been applications to a generalisation of Hilbert's tenth problem for large subrings of the rational numbers [Poo03, CZ07, EG09].

A natural question is whether it is possible to extend Silverman's result to other fields. In 1999, Cheon and Hahn proved the result when K is a number field [CH99]. The fact that the sequence $\{D_n\}$ is a divisibility sequence plays a major role in both this and Silverman's proof. Effective versions of these theorems have been proved as well [IS12, Ver20b]. In a different direction, one can also consider other sequences of points in $E(K)$ and raise similar questions. Suppose $Q \in E(K)$ is a point with $Q \neq -nP$ for any positive integer n. For each positive integer n, we can then similarly write $(x(nP + Q)) = \frac{A'_n}{{D'_n}^2}$ with A'_n and D'_n ideals in $\mathcal{O}_K$ that are relatively prime. In general, the sequence of ideals $\{D'_n\}$ will no longer be a divisibility sequence, but one can still pose the question whether there exists a bound N such that D'_n has a primitive divisor for all $n \geq N$. For a number field as base field, questions related to this are considered in [ES05], and Verzobio proves in [Ver20a] that for Q a torsion point of prime order r, such a bound exists. In a later note, Verzobio extended this result to the case where Q is an arbitrary torsion point [Ver21]. Actually, much more is proved in [op. cit.]. Namely, for $R \subset \mathrm{End}(E)$ a Dedekind domain, the author proves results concerning primitive divisors for the sequence of points $\{\alpha(P) + Q\}_{\alpha \in R}$, including a result when Q is not assumed to be a torsion point. This is an extension of the work by Streng in [Str08], where for $R \subset \mathrm{End}(E)$ an arbitrary subring, results concerning primitive divisors for the sequence of points $\{\alpha(P)\}_{\alpha \in R}$ are proved.

In this paper, we extend one of the aforementioned results of Verzobio to the setting where K is the function field of a nonsingular projective curve $\mathcal{C}$ over an algebraically closed field k of characteristic p. Suppose E/K is an elliptic curve with point at infinity $O \in E(K)$. We next state some results concerning elliptic surfaces, see for example [Sil94, Chapters III & IV] for details. We can associate an elliptic surface to E, and among those there exists a minimal proper regular model, unique up to K-isomorphism. Fix such a minimal proper regular model for E and denote it by $\mathcal{E}$. Suppose $R \in E(K)$ is a point, then we obtain an associated section $\sigma_R : \mathcal{C} \to \mathcal{E}$. Let $\mathcal{O}$ denote the image of σ_O. If R is non-zero, it can be shown that $\sigma_R^*(\mathcal{O})$ is an effective divisor on $\mathcal{C}$. Given a non-zero point $R \in E(K)$, we denote $D_R := \sigma_R^*(\mathcal{O}) \in \mathrm{Div}(\mathcal{C})$.

Then, given a sequence of non-zero points $\{P_n\} \subset E(K)$, we obtain a sequence of effective divisors $\{D_{P_n}\} \subset \mathrm{Div}(\mathcal{C})$. Extending the earlier definitions, we say that a sequence of effective divisors $\{\mathcal{D}_n\} \subset \mathrm{Div}(\mathcal{C})$ is a *divisibility sequence* if for all positive integers m, n with m dividing n, we have that $\mathcal{D}_n - \mathcal{D}_m$ is effective. Similarly, given a positive integer n, we say that $\mathcal{D}_n$ has a *primitive divisor* if there exists γ in the support of $\mathcal{D}_n$ such that γ does not lie in the support of $\mathcal{D}_m$ for any $1 \leq m < n$. We next state some results from [IMSSS12] and [Nas16], where the former concerns $\mathrm{char}(k) = p = 0$ and the latter $p > 0$. Suppose $P \in E(K)$ is a non-torsion point, then the sequence of divisors $\{D_{nP}\}$ is a divisibility sequence. Suppose that E is ordinary and that E is not isomorphic over K to some elliptic curve E_0/k. Additionally, suppose $p \neq 2, 3$, then there exists a bound N such that for all $n \geq N$, D_{nP} has a primitive divisor. Given these results, it is natural to pose the question whether the aforementioned results of Verzobio over number fields also hold in the setting of K a function field as above. In this paper, we study one of these results. That is, we study the following question: let $Q \in E(K)$ be a torsion point of order r and consider the sequence of divisors $\{D_{nP+Q}\}$, does there then exist a bound N such that D_{nP+Q} has a primitive divisor for all $n \geq N$? We prove that this is indeed true if we assume some minor conditions on p and r. More precisely, we prove the following theorem.

Theorem 1.1. *Let k be an algebraically closed field of characteristic p, let $\mathcal{C}$ be a nonsingular projective curve over k and let K be the function field of $\mathcal{C}$. Suppose E/K is an ordinary elliptic curve that is not isomorphic over K to some elliptic curve E_0/k. Suppose $P \in E(K)$ is a non-torsion point and $Q \in E(K)$ is a torsion point of order r. If either $r = 1$ and $p \neq 2, 3$ or the values of p and r are entries* *in Table 1, then there exists a constant N such that for all $n \geq N$, D_{nP+Q} has a primitive divisor.*

p	0	5	7	$11, 13$	≥ 17
r	≥ 2	5 or ≥ 10	≥ 4	≥ 3	≥ 2

TABLE 1. Pairs (p, r) with $r > 1$ for which D_{nP+Q} has a primitive divisor for all n sufficiently large.

Remark 1.2. In an earlier version of this paper, we assumed in Theorem 1.1 that Q had prime order unequal to p. We required this assumption to prove the corresponding versions of Proposition 3.1 and Corollary 3.2. It was pointed out to the author that we could get around this assumption by Verzobio. Additionally, Ulmer has pointed out to the author that the paper [UU20] of Ulmer and Ursúa could be used to lift this restriction in the $p = 0$ case, see especially [Remark 2.4, op. cit.].

Remark 1.3. Our proof of Theorem 1.1 follows the same ideas as the proof of Verzobio in the number field case [Ver20a]. However, there are some difficulties in generalising this approach to the function field case when the characteristic of the ground field is positive. Foremost, Proposition 2.7 is more difficult to work with in positive characteristic than its analogue in the number field case. This leads to several challenges in the approximations done in the proof of Theorem 1.1, which do not appear in the number field case. Additionally, one can use Siegel's theorem [Sil09, Theorem IX.3.1] to deal with problematic valuations in the number field case. We do not have Siegel's theorem in the function field case, so we have to resort to Corollary 2.9 to deal with problematic points in $\mathcal{C}(k)$.

This paper is organised as follows. In Section 2, we recall some preliminaries on height functions and properties of the divisor associated to a point on an elliptic curve over a function field. Afterwards, we present the proof of Theorem 1.1 in Section 3. Lastly, we discuss the necessity of some of the assumptions of Theorem 1.1 in Section 4. In particular, we provide counterexamples if E is not ordinary and we discuss the case where k is not algebraically closed.

Notation. Throughout Sections 2 and 3 of this paper, we fix the following notation. For k a field, a *curve* over k is a scheme X over k that is integral, separated, of finite type, and of dimension 1. We let k be an algebraically closed field of characteristic $p \neq 2, 3$. We let $\mathcal{C}$ be a nonsingular projective curve over k and we let K be the function field of $\mathcal{C}$. We let E/K be an elliptic curve with point at infinity $O \in E(K)$. We assume that $E(K)$ has non-zero rank and is given by a Weierstrass equation in short form. Additionally, we assume that E is not isomorphic over K to some elliptic curve E_0/k, and if $p > 0$, we assume that E is ordinary. We let $\mathcal{E}$ be an elliptic surface associated to E that is a minimal proper regular model. We let $P \in E(K)$ be a non-torsion point and we let $Q \in E(K)$ be a torsion point of order r. For a non-zero point $R \in E(K)$ and $\sigma_R : \mathcal{C} \to \mathcal{E}$ the associated section, we denote $D_R := \sigma_R^*(\mathcal{O}) \in \mathrm{Div}(\mathcal{C})$, where $\mathcal{O}$ equals the image of the section σ_O. In Section 4, we will use above notation as well, but we will relax some of the assumptions, which will be indicated clearly. Lastly, we will frequently use the big O and little o notation. The subscripts in the O indicate that the chosen constant depends on these subscripts, e.g. for $\alpha, \beta \in \mathbb{R}$, $\alpha = \beta + O_{E,P}(1)$ means that $|\alpha - \beta| \leq C$ for some constant C depending on E and P.

2. Preliminaries

We first provide a more explicit description of the divisor associated to a non-zero point in $E(K)$.

Lemma 2.1. *Suppose R is a non-zero point in $E(K)$ and $\gamma \in \mathcal{C}(k)$. Let E'/K be an elliptic curve given by a Weierstrass equation that is minimal at ord_γ and isomorphic to E over K via the isomorphism $\varphi : E \to E'$, then*

$$\mathrm{ord}_\gamma D_R = \max\left\{0, -\frac{1}{2}\mathrm{ord}_\gamma(x(\varphi(R)))\right\}.$$

Proof. This is proved in [IMSSS12, Lemma 5.2], where we note that although the lemma stated there only concerns D_{nP}, the proof holds in this more general setting as well. □

2.1. Heights. We next recall some properties of the (canonical) height map on E. We define the *height* $h : E(K) \to \mathbb{Z}_{\geq 0}$ by

$$h(R) = \begin{cases} 0, & \text{if } R = O, \\ \deg(x(R)), & \text{otherwise.} \end{cases}$$

The height of a non-zero point and the degree of its associated divisor are closely related. To show this, we require the following lemma.

Lemma 2.2. *Let $\gamma \in \mathcal{C}(k)$, then there exists $u \in K^\times$ such that the change of coordinates $(x, y) \mapsto (u^2x, u^3y)$ is minimal at ord_γ.*

Proof. By [Sil09, Proposition VII.1.3], we know that there exists a change of variables with values in K such that we obtain a minimal equation at ord_γ for E, say

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

Let $R \subset K$ be the valuation ring corresponding to ord_γ, then we also obtain from [loc. cit.] that a change of variables $(x, y) \mapsto (x + r, y + sx + t)$ with $r, s, t \in R$ again results in a minimal equation at ord_γ. Since $\mathrm{char}(K) \neq 2$ and $a_1, a_3, -\frac{1}{2} \in R$, the change of coordinates $(x, y) \mapsto (x, y - \frac{1}{2}(a_1x + a_3))$ then results in a Weierstrass equation for E that is minimal at ord_γ of the form

$$y^2 = x^3 + a_2'x^2 + a_4'x + a_6'.$$

Similarly, since $\operatorname{char}(K) \neq 3$, we can make the substitution $(x, y) \mapsto (x, y - \frac{1}{3}a_2')$ to obtain a Weierstrass equation in short form that is minimal at $\operatorname{ord}_\gamma$. It can be shown that if the initial equation is in short form, then the only change of variables such that the resulting equation is again in short form is of the form $(x, y) \mapsto (u^2x, u^3y)$ for some $u \in K^\times$. Since both our original equation and the equation obtained from the composition of these changes of variables are in short form, this composition of changes of variables is of the required form, thus proving the lemma. □

Lemma 2.3. *Let R be a non-zero point in $E(K)$, then*

$$h(R) = 2 \deg D_R + O_E(1).$$

Proof. There exist only finitely many points $\gamma \in \mathcal{C}(k)$ for which the Weierstrass equation of E is not minimal at $\operatorname{ord}_\gamma$, say at all but $\gamma_1, \gamma_2, \dots, \gamma_n \in \mathcal{C}(k)$ for some positive integer n. Using Lemma 2.1, we have

$$\begin{aligned} h(R) = \deg(x(R)) &= \sum_{\gamma \in \mathcal{C}(k)} \max\{0, -\operatorname{ord}_\gamma(x(R))\} \\ &= 2 \sum_{\gamma \in \mathcal{C}(k)} \max\{0, -1/2 \operatorname{ord}_\gamma(x(R))\} \\ &= 2 \deg D_R + 2 \sum_{i=1}^{n} \left(\max\{0, -1/2 \operatorname{ord}_{\gamma_i}(x(R))\} - \operatorname{ord}_{\gamma_i} D_R\right). \end{aligned}$$

By Lemmas 2.1 and 2.2, there exists for each $1 \le i \le n$ some $u_i \in K^\times$ such that $\operatorname{ord}_{\gamma_i} D_R = \max\{0, \operatorname{ord}_{\gamma_i}(u_i) - 1/2 \operatorname{ord}_{\gamma_i}(x(R))\}$, so above summands are bounded by $\operatorname{ord}_{\gamma_i}(u_i)$. Since $\operatorname{ord}_{\gamma_i}(u_i)$ depends only on E, this proves the lemma. □

Given points $R, S \in E(K)$, we let (RS) denote the intersection number of the curves $(R) := \sigma_R(\mathcal{C})$ and $(S) := \sigma_S(\mathcal{C})$ on the surface $\mathcal{E}$. If R is non-zero, then (RO) is simply equal to $\deg D_R$. We next recall some properties of the *canonical height* $\widehat{h}$ on E/K.

Proposition 2.4. *There exists a map $\hat{h} : E(K) \to \mathbb{R}_{\ge 0}$ such that for all $R \in E(K)$ we have*

(i) $\hat{h}(R) = \frac{1}{2}h(R) + O_E(1)$, *and if R is non-zero, then* $\hat{h}(R) = \deg D_R + O_E(1)$;
(ii) $\hat{h}(jR) = j^2\hat{h}(R)$ *for all* $j \in \mathbb{Z}$;
(iii) $\hat{h}(R) = 0$ *if and only if R is a torsion point.*

We call $\hat{h}$ the canonical height on $E(K)$. Additionally, the pairing $\langle \cdot, \cdot \rangle : E(K) \times E(K) \to \mathbb{R}$ defined by $\langle R, S \rangle = \hat{h}(R + S) - \hat{h}(R) - \hat{h}(S)$ is symmetric and bilinear.

Proof. In the $p = 0$ case, this is [Sil94, Theorem III.4.3] and Lemma 2.3. Suppose $p > 3$ and let $\chi(\mathcal{E})$ denote the arithmetic genus of $\mathcal{E}$. In [Shi90, p. 228], a function $C(R, S)$ is defined for all $R, S \in E(K)$ and this function is used there to prove that the pairing $\langle \cdot, \cdot \rangle_1 : E(K) \times E(K) \to \mathbb{R}$ defined by

$$\langle R, S\rangle_1 = \chi(\mathcal{E}) + (RO) + (SO) - (RS) - C(R,S)$$

for all $R, S \in E(K)$, is symmetric and bilinear. If R and S are non-zero points in $E(K)$, then

$$\langle R, S\rangle_1 = \chi(\mathcal{E}) + \deg D_R + \deg D_S - (RS) - C(R,S).$$

We define $\hat{h}(R) = \frac{1}{2}\langle R, R\rangle_1$ for all $R \in E(K)$. A calculation then shows that the pairings $\langle \cdot, \cdot \rangle$ and $\langle \cdot, \cdot \rangle_1$ are equal, so $\langle \cdot, \cdot \rangle$ is symmetric and bilinear.

Since $\langle \cdot, \cdot \rangle = \langle \cdot, \cdot \rangle_1$ is bilinear, assertion (ii) follows. Suppose R and S are arbitrary points in $E(K)$. In [Nas16, Lemma 7.3], it is proved that the function $C(R,S)$ can be bounded by a constant depending only on E. Combining this with [Shi90, Lemma 2.7] and using that $\chi(\mathcal{E})$ depends only on E, we obtain $\hat{h}(R) = (RO) + O_E(1)$. Since $\hat{h}(O) = 0$, we may assume that R is non-zero for assertion (i). Then $\hat{h}(R) = \deg D_R + O_E(1)$ and assertion (i) follows from Lemma 2.3. By [Shi90, Theorem 8.4], we obtain assertion (iii) and $\hat{h}(R) \geq 0$. □

We end this section with a lemma on height functions.

Lemma 2.5. *Let R, S be points in $E(K)$, then*

(i) *there exists a positive constant $C_{R,S,E}$ that depends only on R, S and E such that $\hat{h}(nR + S) \geq \hat{h}(nR) - nC_{R,S,E}$;*
(ii) $h(R+S) \leq 2h(R) + 2h(S) + O_E(1)$.

Proof. Let $\langle \cdot, \cdot \rangle$ denote the pairing of Proposition 2.4. We have

$$\begin{aligned} 0 &= \langle nR, S\rangle - n\langle R, S\rangle \\ &= \hat{h}(nR+S) - \hat{h}(nR) - \hat{h}(S) - n\left(\hat{h}(R+S) - \hat{h}(R) - \hat{h}(S)\right). \end{aligned}$$

Since $\hat{h}(T) \geq 0$ for all $T \in E(K)$, we then obtain

$$\begin{aligned} \hat{h}(nR+S) &= \hat{h}(nR) + \hat{h}(S) + n\left(\hat{h}(R+S) - \hat{h}(R) - \hat{h}(S)\right) \\ &\geq \hat{h}(nR) - n\left(\hat{h}(R) + \hat{h}(S)\right). \end{aligned}$$

The first assertion then follows by putting $\hat{h}(R) + \hat{h}(S) = C_{R,S,E}$.

For the second assertion, the statement is trivial if either R or S is zero, so assume that both are non-zero. We have in the $p = 0$ case by [Sil94, Theorem III.4.2] that

$$h(R+S) = 2h(R) + 2h(S) - h(R-S) + O_E(1),$$

and the result follows since $h(R-S) \geq 0$. If $p > 3$, we have by (the proof of) Proposition 2.4 that

$$\begin{aligned} h(R+S) = 2\hat{h}(R+S) + O_E(1) &= 2\left(\hat{h}(R) + \hat{h}(S) + \langle R, S\rangle\right) + O_E(1) \\ &= h(R) + h(S) + 2\left(\deg D_R + \deg D_S - (RS) - C(R,S)\right) + O_E(1). \end{aligned}$$

Since (R) and (S) are irreducible, it follows from [Har77, Proposition 1.4] that if $(R) \neq (S)$, then $(RS) \geq 0$. If $(R) = (S)$, we have by [Shi90, Lemma 2.7] that

$(RS) = O_E(1)$. Since $C(R,S)$ can be bounded by a constant depending only on E (see the proof of Proposition 2.4), it then follows by Lemma 2.3 that

$$\begin{aligned} h(R+S) &\leq h(R) + h(S) + 2\,(\deg D_R + \deg D_S) + O_E(1) \\ &= 2h(R) + 2h(S) + O_E(1), \end{aligned}$$

as desired. □

2.2. Values of D_R for specific points $R \in E(K)$. Suppose $\gamma \in \mathcal{C}(k)$ is a point. We let K_γ denote the completion of K at $\operatorname{ord}_\gamma$, and we let R_γ denote the corresponding valuation ring with maximal ideal $\mathcal{M}_\gamma$. For n a positive integer, we denote

$$E(K)_{\gamma,n} := \{R \in E(K) \setminus \{O\} : \operatorname{ord}_\gamma D_R \geq n\} \cup \{O\}. \tag{1}$$

Since K can be embedded in K_γ, we can view K as a subfield of K_γ. In particular, we can view E as an elliptic curve over K_γ. We next define a similar subset as (1) for $E(K_\gamma)$. Let E_γ/K be an elliptic curve that is minimal at $\operatorname{ord}_\gamma$ and isomorphic to E over K with isomorphism $\varphi_\gamma : E \to E_\gamma$. One can show that E_γ is then also minimal at $\operatorname{ord}_\gamma$ when considered as an elliptic curve over K_γ. Since K is a subfield of K_γ, we may view φ_γ as an isomorphism over K_γ between curves over K_γ. For all positive integers n, we then define

$$E(K_\gamma)_n := \left\{R \in E(K_\gamma) \setminus \{O\} : -\frac{1}{2}\operatorname{ord}_\gamma(x(\varphi_\gamma(R))) \geq n\right\} \cup \{O\}.$$

We can view any point R in $E(K)$ as a point in $E(K_\gamma)$, and it then follows that $E(K)_{\gamma,n} \subset E(K_\gamma)_n$ under this identification. Using Lemma 2.1 and the formal group associated to an elliptic curve, one can show that $E(K)_{\gamma,n}$ and $E(K_\gamma)_n$ are groups. Additionally, for n a positive integer, there exists a group isomorphism $E(K_\gamma)_n/E(K_\gamma)_{n+1} \cong \mathcal{M}_\gamma^n \,/\, \mathcal{M}_\gamma^{n+1}$. See [Sil09, Chapter IV & Proposition VII.2.2] for details.

Lemma 2.6. *Suppose R is an s-torsion point in $E(K)$ for some integer $s > 1$ that is not divisible by p. Then $D_R = 0$.*

Proof. Suppose $\gamma \in \operatorname{Supp} D_R$ and view R as a point of $E(K_\gamma)$. Denote $d := \operatorname{ord}_\gamma D_R > 0$, then it follows from the discussion preceding this lemma that $R \in E(K_\gamma)_d$. Let $[R]$ denote the image of R in the quotient $E(K_\gamma)_d/E(K_\gamma)_{d+1}$. Then $[R]$ is non-zero. By the discussion preceding this lemma, we have

$$E(K_\gamma)_d/E(K_\gamma)_{d+1} \cong \mathcal{M}_\gamma^d \,/\, \mathcal{M}_\gamma^{d+1} \cong k.$$

Since p does not divide s, it then follows that $s[R] \neq [O]$, but this contradicts $s[R] = [sR] = [O]$. □

Suppose R is a non-torsion point of $E(K)$ and let n be a positive integer. If $\gamma \in \operatorname{Supp} D_R$, it is possible to relate the values $\operatorname{ord}_\gamma D_{nR}$ and $\operatorname{ord}_\gamma D_R$ through the formal group associated to an elliptic curve. This relation is much simpler in the $p = 0$ case, so we will focus on the $p > 0$ case.

Suppose $p > 0$. We first require some notation. For each point $\gamma \in \mathcal{C}(k)$, let E_γ denote an elliptic curve given by a Weierstrass equation that is minimal at $\operatorname{ord}_\gamma$ and isomorphic to E over K. The following is from [Sil09, Chapter IV]. Fix some $\gamma \in \mathcal{C}(k)$, and let $\widehat{E}_\gamma$ denote the formal group associated to E_γ. Then the multiplication-by-p map $[p] : \widehat{E}_\gamma \to \widehat{E}_\gamma$ is defined by the formal power series $T \mapsto H_{E_\gamma} T^p + a_2 T^{2p} + \dots$. Since E is ordinary, we have $H_{E_\gamma} \neq 0$, and since E_γ is minimal at $\operatorname{ord}_\gamma$, we have $\operatorname{ord}_\gamma H_{E_\gamma} \geq 0$. The value $\operatorname{ord}_\gamma H_{E_\gamma}$ does not depend on the chosen E_γ. For each point $\gamma \in \mathcal{C}(k)$, we define

$$h_{E,\gamma} := \operatorname{ord}_\gamma H_{E_\gamma}.$$

We have $h_{E,\gamma} = \operatorname{ord}_\gamma H_E$ for $\gamma \in \mathcal{C}(k)$ outside the finite set of $\gamma' \in \mathcal{C}(k)$ for which E is not minimal at $\operatorname{ord}_{\gamma'}$. Since H_E has only finitely many zeroes, it follows that there are only finitely many points $\gamma \in \mathcal{C}(k)$ for which $h_{E,\gamma} \neq 0$.

We next provide the proposition that relates $\operatorname{ord}_\gamma D_{nR}$ to $\operatorname{ord}_\gamma D_R$. The $p = 0$ part is due to Ingram et al. [IMSSS12] and the $p > 0$ part is due to Naskręcki [Nas16].

Proposition 2.7 ([IMSSS12, Lemma 5.6] & [Nas16, Lemma 8.2]). *Suppose R is a non-torsion point of $E(K)$ and $\gamma \in \operatorname{Supp} D_{mR}$ for some positive integer m. Denote $m(\gamma) := \min\{n \geq 1 : \gamma \in \operatorname{Supp} D_{nR}\}$ and let n be a positive integer, then,*

(i) *if $m(\gamma) \nmid n$, $\operatorname{ord}_\gamma D_{nR} = 0$;*
(ii) *if $m(\gamma) \mid n$ and $p = 0$, $\operatorname{ord}_\gamma D_{nR} = \operatorname{ord}_\gamma D_{m(\gamma)R}$;*
(iii) *if $m(\gamma) \mid n$ and $p > 0$, denote $e := \operatorname{ord}_p \left(\frac{n}{m(\gamma)}\right)$. Then,*
   (a) *if $h_{E,\gamma} \leq p - 1$, $\operatorname{ord}_\gamma D_{nP} = p^e \operatorname{ord}_\gamma D_{m(\gamma)P} + \frac{p^e - 1}{p-1} h_{E,\gamma}$;*
   (b) *if $h_{E,\gamma} \geq p$, there exists a non-negative integer j and a map*

$$\delta_{\gamma,m(\gamma)R} : \{0, 1, \dots, j\} \to \mathbb{Z}_{\geq 0}$$

with $\delta_{\gamma,m(\gamma)R}(0) = 0$ such that

$$\operatorname{ord}_\gamma D_{nR} = p^e \operatorname{ord}_\gamma D_{m(\gamma)R} + \begin{cases} \delta_{\gamma,m(\gamma)R}(e), & \text{if } e \leq j, \\ \frac{p^{e-j}-1}{p-1} h_{E,\gamma} + p^{e-j} \delta_{\gamma,m(\gamma)R}(j), & \text{otherwise.} \end{cases}$$

The integer j is independent of γ and depends only on E. The function $\delta_{\gamma,m(\gamma)R}$ depends only on γ, R and E.

Lemma 2.8. *Suppose $p > 0$. Suppose $R \in E(K)$ is a non-torsion point and let n be a positive integer. Suppose $\gamma \in \operatorname{Supp} D_{nR}$ with $h_{E,\gamma} \geq p$ and let j be as in Proposition 2.7. Let $m(\gamma)$ be the smallest positive integer such that $\gamma \in \operatorname{Supp} D_{m(\gamma)R}$ and* *denote $e = \operatorname{ord}_p(n/m(\gamma))$. Then for any non-negative integer $s \leq j$, we have*

$$\begin{aligned}\delta_{\gamma,nR}(s) &= \begin{cases} \delta_{\gamma,m(\gamma)R}(e+s) - p^s\delta_{\gamma,m(\gamma)R}(e), & \text{if } e+s \leq j,\\ \frac{p^s-1}{p-1}h_{E,\gamma}, & \text{if } e > j,\\ \frac{p^{e+s-j}-1}{p-1}h_{E,\gamma} + p^{e+s-j}\delta_{\gamma,m(\gamma)R}(j) - p^s\delta_{\gamma,m(\gamma)R}(e), & \text{otherwise,}\end{cases}\\ &= O_{E,R}(n).\end{aligned}$$

Proof. Fix some non-negative integer $s \leq j$. The first equality follows by applying Proposition 2.7 on np^sR for both $m(\gamma)R$ and nR as initial point. There are only finitely many $\gamma' \in \mathcal{C}(k)$ for which $h_{E,\gamma'} \neq 0$, so

$$C_1 := \max\{h_{E,\gamma'} : \gamma' \in \mathcal{C}(k)\}$$

exists and depends only on E. By the hypotheses of the lemma, we have $C_1 \geq p$. Since $s \leq j$ and j depends only on E, we then have that

$$\frac{p^s-1}{p-1}h_{E,\gamma} \leq p^jC_1 \leq C_1^{j+1} = O_E(1)$$

and so we may assume that $e \leq j$ for the second equality. Let S denote the finite set of $\gamma' \in \mathcal{C}(k)$ for which $h_{E,\gamma'} \geq p$ and for which $\gamma' \in \operatorname{Supp} D_{mR}$ for some positive integer m. Given $\gamma' \in S$, we let $m(\gamma')$ denote the smallest positive integer for which $\gamma' \in \operatorname{Supp} D_{m(\gamma')R}$. The constant

$$C_2 := \max\{\delta_{\gamma',m(\gamma')R}(t) : 0 \leq t \leq j, \gamma' \in S\}$$

then exists and only depends on E and R. So $C := 2\max\{C_1, C_2\}$ depends only on E and R. Since $\delta_{\gamma,nR}(s)$ and $p^s\delta_{\gamma,m(\gamma)R}(e)$ are non-negative, it suffices for the second equality to show that $\delta_{\gamma,nR}(s) + p^s\delta_{\gamma,m(\gamma)R}(e) = O_{E,R}(n)$ and by the first equality we have

$$\delta_{\gamma,nR}(s) + p^s\delta_{\gamma,m(\gamma)R}(e) \leq p^eC \leq nC = O_{E,R}(n). \qquad \square$$

Corollary 2.9. *Suppose $R \in E(K)$ is a non-torsion point and let $\gamma \in C(k)$. For each positive integer n, we have $\operatorname{ord}_\gamma D_{nR} = O_{E,R,\gamma}(n)$.*

Proof. Let n be a positive integer. We may assume that $\operatorname{ord}_\gamma D_{nR} > 0$. Let $m(\gamma)$ be the smallest positive integer such that $\gamma \in \operatorname{Supp} D_{m(\gamma)R}$. Denote $e = \operatorname{ord}_p(n/m(\gamma))$ if $p > 0$ and $e = 0$ if $p = 0$. By Proposition 2.7 and (the proof of) Lemma 2.8, we obtain that

$$\operatorname{ord}_\gamma D_{nR} - p^e \operatorname{ord}_\gamma D_{m(\gamma)R} = p^eO_{E,R}(m(\gamma)) \leq nO_{E,R}(m(\gamma)) = O_{E,R,\gamma}(n).$$

Since $\operatorname{ord}_\gamma D_{m(\gamma)R}$ depends only on E, R and γ, we have

$$p^e \operatorname{ord}_\gamma D_{m(\gamma)R} = O_{E,R,\gamma}(n),$$

from which the result then follows. $\square$

3. Proof of Theorem 1.1

If $r = 1$, then the proof is due to Ingram et al. if $p = 0$ [IMSSS12, Theorem 1.7] and due to Naskręcki if $p > 3$ [Nas16, Theorem 8.11]. So we may assume $r > 1$. We denote $S := \bigcup_{b|r, b<r} \operatorname{Supp} D_{bQ}$, then S is finite. Moreover, if p does not divide r, then S is empty by Lemma 2.6. The next proposition and corollary are key ingredients of the proof. This propostion and corollary, and their proofs, are adaptations of the analogous results that Verzobio obtains in the number field case [Ver20a, pp. 384-386]. One important difference is that we do not assume that Q is of prime order (cf. Remark 1.2).

Proposition 3.1. *Let n be a positive integer and suppose D_{nP+Q} does not have a primitive divisor. Suppose γ lies in the support of D_{nP+Q} and does not lie in S. Then there exists a positive integer $d > r$ that divides n and is coprime with r such that γ lies in the support of $D_{\frac{rn}{d}P}$ as well.*

Proof. Since D_{nP+Q} does not have a primitive divisor, there exists an integer $1 \leq j < n$ such that $\gamma \in \operatorname{Supp} D_{(n-j)P+Q}$. So both $nP + Q$ and $(n-j)P + Q$ are elements of $E(K)_{\gamma,1}$. Since $E(K)_{\gamma,1}$ is a group, we then have $jP \in E(K)_{\gamma,1}$. Similarly, we have that $r(nP + Q) = rnP \in E(K)_{\gamma,1}$, so for $s = \gcd(rn, j)$, we have $sP \in E(K)_{\gamma,1}$. Write $s = \frac{rn}{d}$ for some positive integer d and denote $c = \gcd(r, d)$. Now write $r = r_1c$ and $d = d_1c$, then $s = \frac{r_1n}{d_1}$. Now if $c > 1$, then $r_1Q = r_1(nP + Q) - d_1sP \in E(K)_{\gamma,1}$, which contradicts that $\gamma \notin S$ since $r_1 \mid r$ and $r_1 < r$. So $c = 1$ and d is coprime with r. Since d divides rn, it then follows that d divides n. Since s divides j and $j < n$, we have $d > r$. Since $\gamma \in \operatorname{Supp} D_{sP}$ and $s = \frac{rn}{d}$, the proposition is proved. □

To improve readability, we write $h_\gamma(R) := \operatorname{ord}_\gamma D_R$ for a non-zero point $R \in E(K)$ and $\gamma \in \mathcal{C}(k)$.

Corollary 3.2. *Assume the same hypotheses as in the preceding proposition. Let d be the positive integer obtained from that proposition. If $p = 0$, put $e = 0$ and if $p > 0$, put $e = \operatorname{ord}_p(d)$. There then exist non-negative integers $b < r$ and $\epsilon_{d,\gamma}$, where b depends only on d and r, such that*

$$h_\gamma(nP + Q) \leq p^e h_\gamma\left(\frac{n}{d}P + bQ\right) + \epsilon_{d,\gamma}.$$

Moreover, let j and $\delta_{\gamma,\frac{rn}{d}P}$ be as in Proposition 2.7(iii), then

$$\epsilon_{d,\gamma} = \begin{cases} \frac{p^e-1}{p-1} h_{E,\gamma}, & \text{if } h_{E,\gamma} < p, \\ \delta_{\gamma,\frac{rn}{d}P}(e), & \text{if } h_{E,\gamma} \geq p \text{ and } e \leq j, \\ \frac{p^{e-j}-1}{p-1} h_{E,\gamma} + p^{e-j}\delta_{\gamma,\frac{rn}{d}P}(j), & \text{otherwise.} \end{cases}$$

Proof. We denote $P_1 = \frac{rn}{d}P$ and $P_2 = nP + Q$. Since $\gcd(r, d) = \gcd(r, d-r) = 1$, there exists $a, c \in \mathbb{Z}$ such that $ar + c(d-r) = 1$ and so

$$\begin{aligned}\frac{n}{d}P + cQ = ar\frac{n}{d}P + c(d-r)\frac{n}{d}P + cQ &= (a-c)\frac{rn}{d}P + c(nP+Q)\\ &= (a-c)P_1 + cP_2.\end{aligned}$$

First suppose $p \mid r$, then $p \nmid d$. Since $h_\gamma(P_1), h_\gamma(P_2) \geq 1$, we then have by Proposition 2.7 that $h_\gamma(P_1) = h_\gamma(dP_1) = h_\gamma(rP_2) \geq h_\gamma(P_2)$. Denote $s := h_\gamma(P_2)$, then $P_1, P_2 \in E(K)_{\gamma,s}$ and so $\frac{n}{d}P + cQ = (a-c)P_1 + cP_2 \in E(K)_{\gamma,s}$. Since $\frac{n}{d}P + cQ$ is non-zero, we then have

$$h_\gamma(nP+Q) = h_\gamma(P_2) = s \leq h_\gamma\left(\frac{n}{d}P + cQ\right).$$

Now suppose $p \nmid r$. Again, by Proposition 2.7, we then have $h_\gamma(P_2) = h_\gamma(rP_2) = h_\gamma(dP_1) = p^e h_\gamma(P_1) + \epsilon_{d,\gamma}$. Denote $t := h_\gamma(P_1) \geq 1$, then $P_1, P_2 \in E(K)_{\gamma,t}$ and so $\frac{n}{d}P + cQ \in E(K)_{\gamma,t}$. We obtain $h_\gamma\left(\frac{n}{d}P + cQ\right) \geq t$ and so

$$h_\gamma(nP+Q) = h_\gamma(P_2) = p^e h_\gamma(P_1) + \epsilon_{d,\gamma} \leq p^e h_\gamma\left(\frac{n}{d}P + cQ\right) + \epsilon_{d,\gamma}.$$

In both cases, the corollary follows by using that Q is an r-torsion point and putting $0 \leq b < r$ with $b \equiv c \pmod r$. □

We are now able to prove Theorem 1.1. Suppose n is a positive integer such that D_{nP+Q} does not have a primitive divisor. Combining Proposition 2.4 with Lemma 2.5, we have for some positive constant $C_{P,Q,E}$, depending only on P, Q and E, that

$$\begin{aligned}n^2\hat{h}(P) = \hat{h}(nP) \leq \hat{h}(nP+Q) + nC_{P,Q,E} &= \deg D_{nP+Q} + O_{E,P,Q}(n)\\ &= \sum_{\gamma \in \operatorname{Supp} D_{nP+Q}} h_\gamma(nP+Q) + O_{E,P,Q}(n).\end{aligned} \tag{2}$$

We will apply Corollary 3.2 to bound the latter sum. However, we cannot apply Corollary 3.2 to the $\gamma \in \operatorname{Supp} D_{nP+Q}$ that also lie in S. For those, we use the next lemma.

Lemma 3.3. $\sum_{\gamma \in S} h_\gamma(nP+Q) = O_{E,P,Q}(n)$.

Proof. By Proposition 2.7, we have for each $\gamma \in C(k)$ that $h_\gamma(nP+Q) \leq h_\gamma(r(nP+Q)) = h_\gamma(rnP)$, since Q has order r. By Corollary 2.9, we have $h_\gamma(rnP) = O_{E,P,\gamma}(rn)$. Combining, we obtain

$$\sum_{\gamma \in S} h_\gamma(nP+Q) \leq \sum_{\gamma \in S} h_\gamma(rnP) = \sum_{\gamma \in S} O_{E,P,\gamma}(rn) = O_{E,P,Q}(n),$$

where the last step follows since both r and S depend only on E and Q. □

Denote $T := \operatorname{Supp} D_{nP+Q} \setminus S$. By Proposition 3.1, we find for each $\gamma \in T$ an associated positive integer d_γ dividing n, coprime with r, and larger than r. We define

$$\mathcal{D}_n := \{d \in \mathbb{N} : d \mid n,\ d > r \text{ and } \gcd(d,r) = 1\}.$$

Given $d \in \mathcal{D}_n$, we obtain from the proof of Corollary 3.2 an associated non-negative integer $b_d < r$. Given a positive integer d, we denote $e_d = 0$ if $p = 0$ and $e_d = \operatorname{ord}_p(d)$ if $p > 0$. Suppose $\gamma \in T$, then we have by Proposition 3.1 and Corollary 3.2 that

$$h_\gamma(nP+Q) \leq p^{e_{d_\gamma}} h_\gamma\left(\frac{n}{d_\gamma}P + b_{d_\gamma}Q\right) + \epsilon_{d_\gamma,\gamma}.$$

Since b_{d_γ} only depends on d_γ and r, we obtain for any divisor $d \in \mathcal{D}_n$ an associated non-negative integer $b_d < r$, such that above inequality holds if $d = d_\gamma$ for some $\gamma \in T$. We can thus make the approximation

$$\begin{aligned}\sum_{\gamma\in T} h_\gamma(nP+Q) &\leq \sum_{\gamma \in T} p^{e_{d_\gamma}} h_\gamma\left(\frac{n}{d_\gamma}P + b_{d_\gamma}Q\right) + \epsilon_{d_\gamma,\gamma}\\ &\leq \sum_{d\in\mathcal{D}_n}\sum_{\gamma\in T} p^{e_d} h_\gamma\left(\frac{n}{d}P + b_dQ\right) + \underbrace{\sum_{\gamma\in T}\epsilon_{d_\gamma,\gamma}}_{W(n,P,Q)}\\ &\leq \sum_{d\in\mathcal{D}_n} p^{e_d}\deg\left(D_{\frac{n}{d}P+b_dQ}\right) + W(n,P,Q)\\ &= \sum_{d\in\mathcal{D}_n} p^{e_d}\left(\frac{1}{2}h\left(\frac{n}{d}P+b_dQ\right) + O_E(1)\right) + W(n,P,Q), \qquad (3)\end{aligned}$$

where the last equality follows from Lemma 2.3.

Lemma 3.4. *$W(n,P,Q) = O_{E,P,Q}(n)$.*

Proof. Fix some $\gamma \in T$ for which $\epsilon_{d_\gamma,\gamma} > 0$. Since $r < d_\gamma \leq n$, it follows from (the proof of) Lemma 2.8 and the definition of $\epsilon_{d_\gamma,\gamma}$ that $\epsilon_{d_\gamma,\gamma} = O_{E,P}(rn) = O_{E,P,Q}(n)$. If $\gamma' \in T$ such that $h_{E,\gamma'} = 0$, then $\epsilon_{d_{\gamma'},\gamma'} = 0$. The lemma then follows since there are only finitely many $\gamma \in \mathcal{C}(k)$ such that $h_{E,\gamma} \neq 0$ and $\#\{\gamma \in \mathcal{C}(k) : h_{E,\gamma} \neq 0\}$ depends only on E. □

By Lemma 2.5, we find a constant $C := \max_{0\leq b<r} C_{bQ}$, depending only on Q and E, such that for each $d \in \mathcal{D}_n$, we have $h\left(\frac{n}{d}P + b_dQ\right) \leq 2h\left(\frac{n}{d}P\right) + C$.

Combining this with Proposition 2.4 and the definition of $\mathcal{D}_n$, we obtain

$$\begin{aligned}\sum_{d\in\mathcal{D}_n} p^{e_d}\left(\frac{1}{2}h\left(\frac{n}{d}P+b_dQ\right)+O_E(1)\right) &\leq \sum_{d\in\mathcal{D}_n} p^{e_d}\left(h\left(\frac{n}{d}P\right)+O_{E,Q}(1)\right)\\ &= \sum_{d\in\mathcal{D}_n} p^{e_d}\left(2\hat{h}\left(\frac{n}{d}P\right)+O_{E,Q}(1)\right) \qquad (4)\\ &\leq 2n^2\hat{h}(P)\sum_{d\in\mathcal{D}_n} p^{e_d}\frac{1}{d^2}+\sum_{d|n} p^{e_d}O_{E,Q}(1).\end{aligned}$$

For the last term, we apply the following lemma.

Lemma 3.5. *For any positive constant $\alpha \in \mathbb{R}$, we have $\sum_{d|n} p^{e_d} = o(n^{1+\alpha})$.*

Proof. The statement is immediate if $p = 0$, so suppose $p > 0$ and denote $e := \operatorname{ord}_p(n)$. We let $\delta : \mathbb{N} \to \mathbb{N}, m \mapsto \sum_{d|m} 1$ denote the divisor function, then one can show that

$$\sum_{d|n} p^{\operatorname{ord}_p(d)} = \frac{p^{e+1}-1}{(e+1)(p-1)}\delta(n) \leq 2p^e\delta(n) \leq 2n\delta(n).$$

By [Apo13, p. 296], we have for any positive constant α that $\delta(n) = o(n^\alpha)$, so the lemma follows. □

For the rest of this section, fix some constant $0 < \alpha < 1$, then

$$\sum_{d|n} p^{e_d}O_{E,Q}(1) = o(n^{1+\alpha}).$$

Combining this with Lemma 3.4, (3) and (4), we have proved the following corollary.

Corollary 3.6. $\sum_{\gamma\in T} h_\gamma(nP+Q) \leq 2n^2\hat{h}(P)\sum_{d\in\mathcal{D}_n} p^{e_d}\frac{1}{d^2} + o(n^{1+\alpha})$.

Putting everything together, it follows by (2), Lemma 3.3 and Corollary 3.6 that if D_{nP+Q} does not have a primitive divisor, then

$$\begin{aligned}n^2\hat{h}(P) &= \sum_{\gamma\in\operatorname{Supp} D_{nP+Q}} h_\gamma(nP+Q)+O_{E,P,Q}(n)\\ &= \sum_{\gamma\in T} h_\gamma(nP+Q)+\sum_{\gamma\in S} h_\gamma(nP+Q)+O_{E,P,Q}(n)\\ &\leq 2n^2\hat{h}(P)\sum_{d\in\mathcal{D}_n} p^{e_d}\frac{1}{d^2}+o(n^{1+\alpha}).\end{aligned}$$

Since $\hat{h}(P) > 0$ by Proposition 2.4 and $0 < \alpha < 1$, we see that if

$$\sum_{d\in\mathcal{D}_n} p^{e_d}\frac{1}{d^2} < 1/2$$

for all n, then above inequality can only hold for bounded n. So the theorem follows if we can prove that when p and r are entries in Table 1, then

$\sum_{d\in\mathcal{D}_n} p^{e_d}\frac{1}{d^2} < 1/2$ for all n. If $p = 0$ or $p > 3$ and $p \mid r$, then $e_d = 0$ for all $d \in \mathcal{D}_n$ and so

$$\sum_{d\in\mathcal{D}_n} p^{e_d}\frac{1}{d^2} = \sum_{d\in\mathcal{D}_n} \frac{1}{d^2} \le \sum_{d|n,d>2} \frac{1}{d^2} \le \zeta(2) - 1 - \frac{1}{4} \approx .395 < 1/2. \tag{5}$$

Now assume $p > 3$. We are left with the values in Table 1 with $p \nmid r$. Denote $e = \mathrm{ord}_p(n)$ and write $n = n_0 p^e$. Then

$$\sum_{d\in\mathcal{D}_n} p^{e_d}\frac{1}{d^2} \le \sum_{d|n,d>r} p^{\mathrm{ord}_p(d)}\frac{1}{d^2} = \sum_{d_0|n_0,d_0>r} \frac{1}{d_0^2} + \sum_{i=1}^{e} p^{-i} \sum_{d_0|n_0,d_0p^i>r} \frac{1}{d_0^2}. \tag{6}$$

We approximate the last two terms separately. First note that

$$\sum_{d_0|n_0,d_0>r} \frac{1}{d_0^2} \le \zeta(2) - 1 - 1/4 - 1/9 - \ldots - 1/r^2. \tag{7}$$

Next, by using that $\sum_{i=1}^{e} p^{-i} = \frac{1-p^{-e}}{p-1} < \frac{1}{p-1}$, we have

$$\sum_{i=1}^{e} p^{-i} \sum_{d_0|n_0,d_0p^i>r} \frac{1}{d_0^2} \le \frac{1}{p-1} \sum_{d_0|n_0} \frac{1}{d_0^2} \le \frac{1}{p-1}\zeta(2). \tag{8}$$

Combining (6), (7) and (8), we obtain

$$\sum_{d\in\mathcal{D}_n} p^{e_d}\frac{1}{d^2} \le \zeta(2)\left(1 + \frac{1}{p-1}\right) - 1 - 1/4 - 1/9 - \ldots - 1/r^2.$$

A calculation shows that the entries in Table 1 with p not dividing r are precisely those for which

$$\zeta(2)\left(1 + \frac{1}{p-1}\right) - 1 - 1/4 - 1/9 - \ldots - 1/r^2 < 1/2,$$

thus finishing the proof of Theorem 1.1.

4. Necessity of the conditions in Theorem 1.1

We end this paper by discussing the necessity of some of the hypotheses in Theorem 1.1.

4.1. Assumption that the elliptic curve is ordinary. Suppose that p is positive. Suppose all our previous assumptions hold, except that E is no longer ordinary, and we also allow $p = 2, 3$. First consider the sequence $\{D_{nP}\}$. In [Nas16, Section 9], it is shown that there then exist examples for which there does not exist a bound N such that D_{nP} has a primitive divisor for all $n \ge N$. We extend the constructions in [loc. cit.] to obtain counterexamples for the sequence $\{D_{nP+Q}\}$ as well.

Example 4.1. Suppose $p > 2$ is a prime number. Let $\alpha, \beta \in \mathbb{F}_p$ be such that $E_0 : y^2 = x^3 + \alpha x + \beta$ is a supersingular elliptic curve (this is possible by [Cox13, Theorem 14.18] for $p \geq 5$ and for $p = 3$ we take the equation $y^2 = x^3 + x$). Following [Nas16, Example 9.3], consider the function field $K_0 := \mathbb{F}_p(t)$ and put $s = t^3 + \alpha t + \beta$. The curve E_0 is then isomorphic over the algebraic closure $\overline{K_0}$ to the elliptic curve E/K_0 given by the equation $y^2 = x^3 + \alpha s^2 x + \beta s^3$ through the isomorphism $(x, y) \mapsto (xs, ys^{3/2})$. Since E_0 is defined over $\mathbb{F}_p$, we have for $[p] : E_0 \to E_0$ that $x([p](x, y)) = x^{p^2}$, see [Sil09, Exercise 5.16]. Combining with the isomorphism $E_0 \cong E$, we have for each positive integer k and $p^k : E \to E$ that $x\left([p^k](x, y)\right) = s\left(\frac{x}{s}\right)^{p^{2k}}$. From this formula, we deduce that $P = (ts, s^2) \in E(K_0)$ is non-torsion. Denote $K := \overline{\mathbb{F}_p}(t)$ and let L/K be some finite field extension that does not contain $s^{1/2}$. Then E is not L-isomorphic to an elliptic curve defined over $\overline{\mathbb{F}_p}$ and L is a function field over an algebraically closed field. Suppose $Q \in E(L)$ is an r-torsion point for some integer $r > 1$. Since E_0 is supersingular, p does not divide r and so there exists a positive integer k such that $p^k \equiv 1 \pmod{r}$. Fix such an integer k and denote $P + Q = (x', y')$. Then, for each positive integer ℓ, we have $[p^{\ell k}](P + Q) = p^{\ell k}P + Q$ and so $x\left([p^{\ell k}]P + Q\right) = s\left(\frac{x'}{s}\right)^{p^{2\ell k}}$. From this expression, it follows that there are infinitely many terms in the sequence of divisors $\{D_{nP+Q}\}$ that do not have a primitive divisor. To finish the counterexample, we are left with proving the existence of a field extension L/K such that $E(L)[r]$ is non-trivial for some positive integer $r > 1$ and $s^{1/2} \notin L$. Consider the 2-torsion on E. The non-zero 2-torsion points in $E(\overline{K})$ are given by the points $(\gamma, 0)$ with γ a root of $f := X^3 + \alpha s^2 X + \beta s^3 \in K[X]$. Since f is a degree 3 polynomial over K, either f contains a root in K, or f is irreducible over K. In the first case, $E(K)$ already contains a non-trivial 2-torsion point and we can take $L = K$. In the second case, we let L be the field obtained by adjoining a root of f to K, and it follows by comparing degrees that $s^{1/2} \notin L$. In both cases, $E(L)[2]$ is not trivial and $s^{1/2} \notin L$, so this produces a counterexample.

A similar approach works for $p = 2$. The elliptic curve $E_0 : y^2 + y = x^3$ is supersingular over $\mathbb{F}_2$. Denote $K_0 = \mathbb{F}_2(t)$, then the curve E/K_0 given by the equation $y^2 + (t^3 - 1)y = x^3$ is isomorphic to E_0 over an algebraic closure $\overline{K_0}$ of K_0. Namely, fix some root $\alpha \in \overline{K_0}$ to the equation $f := X^3 - t^3 + 1$ in $K_0[X]$, then an isomorphism $E \to E_0$ is given by $(x, y) \mapsto (\alpha^{-2}x, \alpha^{-3}y)$. A calculation shows that f is irreducible over $K := \overline{\mathbb{F}_2}(t)$, so E is not K-isomorphic to an elliptic curve defined over $\overline{\mathbb{F}_2}$. On E_0, we have $x([2](x, y)) = x^4$, so on E we have for each positive integer k that $x([2^k](x, y)) = x^{4^k}\alpha^{2(1-4^k)}$. We deduce that the point $P = (t, 1) \in E(K)$ is non-torsion and it again follows, similar to the $p > 2$ case, that for $L/\overline{\mathbb{F}_2}(t)$ some finite field extension and $Q \in E(L)$ a torsion point of order $r > 1$, there are infinitely many terms in the sequence of divisors $\{D_{nP+Q}\}$ that do not have a primitive divisor. The point $(0, 0) \in E(K)$ is

3-torsion, so since f is irreducible over K, we can take $L = K$ and $Q = (0, 0)$ to produce a counterexample.

Remark 4.2. The point Q in Example 4.1 has small order. Let us explain why this is necessary in our counterexample. Let p be a prime number and use the same notation as in Example 4.1. Let $Q' \in E(\overline{K})$ be some torsion point of order $\ell > 1$, then we showed that the sequence $\{D_{nP+Q'}\}$ will contain infinitely many terms that do not have a primitive divisor. However, the issue is that if L/K is a field extension such that $Q' \in E(L)$, then E will be isomorphic to E_0 over L unless $\ell = 2$ if $p > 2$ and $\ell = 3$ if $p = 2$. To see this, let $\varphi : E \to E_0$ denote the isomorphism, then we have the description $E[\ell] = \varphi^{-1}(E_0[\ell])$. Suppose $p > 2$, then φ^{-1} maps (x, y) to $(xs^{-1}, ys^{-3/2})$. So $Q' = (xs^{-1}, ys^{-3/2})$ for certain $x, y \in \overline{\mathbb{F}_p}$. It follows that if $Q' \in E(L)$ for some field extension L/K, then $s^{1/2} \in L$ unless $y = 0$, which is the case if and only if $\ell = 2$. The $p = 2$ case works similarly.

4.2. Assumption that *k* is algebraically closed. It is possible to relax the condition of k being algebraically closed if we assume that our elliptic curve is not isomorphic over $\overline{k}K$ to an elliptic curve over $\overline{k}$. We fix the following notation for this subsection. Let k be a field of characteristic p and let $\mathcal{C}/k$ be a non-singular, projective and geometrically integral curve. Let $\overline{k}$ denote an algebraic closure of k and let $\mathcal{C}_{\overline{k}}$ denote the base extension of $\mathcal{C}$ to $\overline{k}$. Let K denote the function field of $\mathcal{C}$ and let $K' = \overline{k}K$ denote the function field of $\mathcal{C}_{\overline{k}}$. Let E/K be an ordinary elliptic curve. Suppose $P \in E(K)$ is a non-torsion point and suppose $Q \in E(K)$ is a torsion point of order r. We let $E_{K'}$ denote the base extension of E to K'.

Given a non-zero point $R \in E(K)$, we can define an effective divisor $D'_R \in \mathrm{Div}(\mathcal{C})$ similar to what we did in the algebraically closed case. Let $|\mathcal{C}| \subset \mathcal{C}$ denote the subset of closed points. Given $\gamma \in |\mathcal{C}|$, we have a corresponding valuation v_γ on K, and an elliptic curve E_γ/K that is minimal at v_γ and isomorphic to E over K. Let $\varphi_\gamma : E \to E_\gamma$ denote this isomorphism, then we obtain for each $\gamma \in |\mathcal{C}|$ a non-negative integer

$$n_{\gamma,R} := \max\left\{0, -1/2 v_\gamma(x(\varphi_\gamma(R)))\right\}.$$

There will only be finitely many $\gamma \in |\mathcal{C}|$ such that $n_{\gamma,R} \neq 0$. We define the effective divisor

$$D'_R := \sum_{\gamma \in |\mathcal{C}|} n_{\gamma,R}\gamma \in \mathrm{Div}(\mathcal{C}).$$

Given a sequence of non-zero points $\{P_n\} \subset E(K)$, we again say that P_n has a *primitive divisor* if there exists $\gamma \in \operatorname{Supp} D'_{P_n}$ such that $\gamma \notin \operatorname{Supp} D'_{P_m}$ for any $1 \leq m < n$.

Corollary 4.3. *Suppose E is not isomorphic over K' to some elliptic curve $E_0/\overline{k}$. If either $r = 1$ and $p \neq 2, 3$ or the values of p and r are entries in Table 1, then D'_{nP+Q} has a primitive divisor for all n sufficiently large.*

Proof. Under the hypotheses, we know by Theorem 1.1 that there exists a bound N_1 such that D_{nP+Q} has a primitive divisor for all $n \geq N_1$. Let $\gamma_1, \dots, \gamma_m$ be the points in $\mathcal{C}_{\overline{k}}(\overline{k})$ such that $E_{K'}$ is not minimal at ord_{γ_i}. Let N_2 be a positive integer such that if $\gamma_i \in \operatorname{Supp} D_{nP+Q}$ for some positive integer $n \geq N_2$, then $\gamma_i \in \operatorname{Supp} D_{mP+Q}$ as well for some $1 \leq m < N_2$. Put $N = \max\{N_1, N_2\}$ and let $n \geq N$, then there exists $\gamma \in \operatorname{Supp} D_{nP+Q}$ with $\gamma \notin \operatorname{Supp} D_{mP+Q}$ for any $1 \leq m < n$. Let $\gamma' \in |\mathcal{C}|$ be such that $\mathrm{ord}_\gamma |_K = v_{\gamma'}$. Then E is minimal at $v_{\gamma'}$ since $E_{K'}$ is minimal at ord_γ. Since $x(nP+Q) \in K$, we have $-\frac{1}{2} v_{\gamma'}(x(nP+Q)) = -\frac{1}{2} \mathrm{ord}_\gamma(x(nP+Q)) > 0$ and so $\gamma' \in \operatorname{Supp} D'_{nP+Q}$. Similarly, if $\gamma' \in \operatorname{Supp} D'_{mP+Q}$ for some $1 \leq m < n$, then $\gamma \in \operatorname{Supp} D_{mP+Q}$, which we assumed not to be the case. So D'_{nP+Q} has a primitive divisor for all $n \geq N$. □

4.3. Remaining pairs of p and r.

The $p \neq 2, 3$ assumption is used at several steps in our proof. Most importantly, if $p = 2$ or $p = 3$ and $r > 1$ any integer, then

$$\zeta(2)\left(1 + \frac{1}{p-1}\right) - 1 - 1/4 - \dots - 1/r^2 \geq \zeta(2)\left(1 + \frac{1}{2}\right) - \zeta(2)$$
$$= \frac{1}{2}\zeta(2) \approx 0.822 > 1/2. \qquad (9)$$

For a reason similar to the equality not holding in (9), the proof that D_{nP} has a primitive divisor for all n sufficiently large does not work if $p = 2, 3$. To the author's knowledge, this is still an open problem. Interestingly enough, we see from our proof that if $p = 2, 3$ and p divides the order of Q, then (5) does hold, however our proof does not work in this case because we already use the assumption that $p \neq 2, 3$ in Section 2. All in all, it would be very interesting to further investigate the remaining $p = 2, 3$ case, either for D_{nP+Q} or the classical D_{nP} case. Additionally, it would be interesting to investigate what happens for the remaining pairs of p and r, or what happens if Q is a non-torsion point.

Acknowledgements. This work originated from the author's master's thesis, which was written under supervision of Gunther Cornelissen. The author would like to thank him for the valuable conversations during this time. The author would also like to express his gratitude towards Jeroen Sijsling, Matteo Verzobio, and the anonymous referee for useful comments on an earlier draft of this paper.

References

[Apo13] Apostol, Tom M. Introduction to analytic number theory. Undergraduate Texts in Mathematics. *Springer-Verlag, New York-Heidelberg*, 1976. xii+338 pp. MR434929, Zbl 0335.10001. 243

[Ban86] Bang, A. S. Taltheoretiske Undersøgelser. *Tidsskrift Math.* **5, IV** (1886), 70–80, 130–137. JFM 19.0168.02, `https://www.jstor.org/stable/24539988`. 231

[CH99] Cheon, Jung Hee; Hahn, Sang-Geun. The orders of the reductions of a point in the Mordell-Weil group of an elliptic curve. *Acta Arith.* **88** (1999), no. 3, 219–222. MR1683630, Zbl 0933.11029, doi: 10.4064/aa-88-3-219-111. 231

[ChC86] Chudnovsky, David V.; Chudnovsky, Gregory V. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Adv. in Appl. Math.* **7** (1986), no. 4, 385–434. MR0866702, Zbl 0614.10004, doi: 10.1016/0196-8858(86)90023-0. 231

[CR12] Cornelissen, Gunther; Reynolds, Jonathan. Matrix divisibility sequences. *Acta Arith.* **156** (2012), no. 2, 177–188. MR2997565, Zbl 1271.11061, arXiv:1107.2203, doi: 10.4064/aa156-2-5. 231

[CZ07] Cornelissen, Gunther; Zahidi, Karim. Elliptic divisibility sequences and undecidable problems about rational points. *J. Reine Angew. Math.* **613** (2007), 1–33. MR2377127, Zbl 1178.11076, arXiv:math/0412473, doi: 10.1515/CRELLE.2007.089. 231

[Cox13] Cox, David A. Primes of the form $x^2 + ny^2$. Fermat, class field theory, and complex multiplication. Second edition. Pure and Applied Mathematics (Hoboken). *John Wiley & Sons, Inc., Hoboken, NJ*, 2013. xviii+356 pp. ISBN: 978-1-118-39018-4. MR3236783, Zbl 1275.11002. 245

[EEW01] Einsiedler, Manfred; Everest, Graham; Ward, Thomas. Primes in elliptic divisibility sequences. *LMS J. Comput. Math.* **4** (2001), 1–13. MR1815962, Zbl 1037.11089, doi: 10.1112/S1461157000000772. 231

[EG09] Eisenträger, Kirsten; Everest, Graham. Descent on elliptic curves and Hilbert's tenth problem. *Proc. Amer. Math. Soc.* **137** (2009), no. 6, 1951–1959. MR2480276, Zbl 1267.11120, doi: 10.1090/S0002-9939-08-09740-2. 231

[EMS04] Everest, Graham; Miller, Victor; Stephens, Nelson. Primes generated by elliptic curves. *Proc. Amer. Math. Soc.* **132** (2004), no. 4, 955–963. MR2045409, Zbl 1043.11051, doi: 10.1090/S0002-9939-03-07311-8. 231

[ES05] Everest, Graham; Shparlinski, Igor E. Prime divisors of sequences associated to elliptic curves. *Glasg. Math. J.* **47** (2005), no. 1, 115–122. MR2200959, Zbl 1066.11023, arXiv:math/0404129, doi: 10.1017/S0017089504002113. 231

[EvdPSW03] Everest, Graham; van der Poorten, Alf; Shparlinski, Igor; Ward, Thomas. Recurrence sequences. Mathematical Surveys and Monographs, 104. *American Mathematical Society, Providence, RI*, 2003. xiv+318 pp. ISBN: 0-8218-3387-1. MR1990179, Zbl 1033.11006. 231

[Har77] Hartshorne, Robin. Algebraic geometry. Graduate Texts in Mathematics, 52. *Springer-Verlag, New York-Heidelberg*, 1977. xvi+496 pp. ISBN: 0-387-90244-9. MR463157, Zbl 0367.14001. 236

[IMSSS12] Ingram, Patrick; Mahé, Valéry; Silverman, Joseph H.; Stange, Katherine E.; Streng, Marco. Algebraic divisibility sequences over function fields. *J. Aust. Math. Soc.* **92** (2012), no. 1, 99–126. MR2945679, Zbl 1251.11008, arXiv:1105.5633, doi: 10.1017/S1446788712000092. 232, 234, 238, 240

[IS12] Ingram, Patrick; Silverman, Joseph H. Uniform estimates for primitive divisors in elliptic divisibility sequences. *Number theory, analysis and geometry*, 243–271. *Springer, New York*, 2012. MR2867920, Zbl 1276.11092, doi: 10.1007/978-1-4614-1260-1_12. 231

[Nas16] Naskręcki, Bartosz. Divisibility sequences of polynomials and heights estimates. *New York J. Math.* **22** (2016), 989–1020. MR3576279, Zbl 1417.11110. 232, 236, 238, 240, 244, 245

[Poo03] Poonen, Bjorn. Hilbert's tenth problem and Mazur's conjecture for large subrings of $\mathbb{Q}$. *J. Amer. Math. Soc.* **16** (2003), no. 4, 981–990. MR1992832, Zbl 1028.11077, arXiv:math/0306277, doi: 10.1090/S0894-0347-03-00433-8. 231

[Shi90] Shioda, Tetsuji. On the Mordell–Weil lattices. *Comment. Math. Univ. St. Pauli* **39** (1990), no. 2, 211–240. MR1081832, Zbl 0725.14017. 235, 236

[Sil88] Silverman, Joseph H. Wieferich's criterion and the *abc*-conjecture. *J. Number Theory* **30** (1988), no. 2, 226–237. MR961918, Zbl 0654.10019, doi: 10.1016/0022-314X(88)90019-4. 231

[Sil94] Silverman, Joseph H. Advanced topics in the arithmetic of elliptic curves. Graduate Texts in Mathematics, 151. *Springer-Verlag, New York*, 1994. xiv+525 pp. ISBN: 0-387-94328-5. MR1312368, Zbl 0911.14015. 232, 235, 236

[Sil09] Silverman, Joseph H. The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics, 106. *Springer, Dordrecht*, 2009. xx+513 pp. ISBN: 978-0-387-09493-9. MR2514094, Zbl 1194.11005, doi: 10.1007/978-0-387-09494-6. 233, 234, 237, 238, 245

[Sta07] Stange, Katherine E. The Tate pairing via elliptic nets. *Pairing-based cryptography—Pairing 2007*, 329–348, Lecture Notes in Comput. Sci., 4575. *Springer, Berlin,* 2007. MR2423649, Zbl 1151.94570, doi: 10.1007/978-3-540-73489-5_19. 231

[Str08] Streng, Marco. Divisibility sequences for elliptic curves with complex multiplication. *Algebra Number Theory* **2** (2008), no. 2, 183–208. MR2377368, Zbl 1158.14029, doi: 10.2140/ant.2008.2.183. 232

[UU20] Ulmer, Douglas; Urzúa, Giancarlo. Transversality of sections on elliptic surfaces with applications to elliptic divisibility sequences and geography of surfaces. *Selecta Math. (N.S.)* **28** (2022), no. 2, Paper No. 25. MR4357480, Zbl 07453886, arXiv:1908.02208, doi: 10.1007/s00029-021-00747-x. 233

[Ver20a] Verzobio, Matteo. Primitive divisors of sequences associated to elliptic curves. *J. Number Theory* **209** (2020), 378–390. MR4053074, Zbl 07152998, arXiv:1906.00632, doi: 10.1016/j.jnt.2019.09.003. 231, 233, 240

[Ver20b] Verzobio, Matteo. Some effectivity results for primitive divisors of elliptic divisibility sequences. Preprint, 2020. arXiv:2001.02987. 231

[Ver21] Verzobio, Matteo. Primitive divisors of sequences associated to elliptic curves with complex multiplication. *Res. Number Theory* **7** (2021), no. 2, Paper No. 37, 29 pp. MR4265034, Zbl 07357692, doi: 10.1007/s40993-021-00267-9. 232

[War48] Ward, Morgan. Memoir on elliptic divisibility sequences. *Amer. J. Math.* **70** (1948), 31–74. MR23275, Zbl 0035.03702, doi: 10.2307/2371930. 231

[Zsi92] Zsigmondy, Karl. Zur Theorie der Potenzreste. *Monatsh. Math. Phys.* **3** (1892), no. 1, 265–284. MR1546236, Zbl 24.0176.02, doi: 10.1007/BF01692444. 231

(Robert Slob) Institut für Reine Mathematik, Universität Ulm, Helmholtzstrasse 18, 89081 Ulm, Germany
robert.slob@uni-ulm.de

This paper is available via http://nyjm.albany.edu/j/2022/28-10.html.