

Uniform estimates for primitive divisors in elliptic divisibility sequences

Dedicated to the memory of Serge Lang

Patrick Ingram and Joseph H. Silverman

Department of Mathematics, University of Toronto, Toronto, Ontario, Canada
M5S 2E4. <pingram@math.utoronto.ca>

Mathematics Department, Box 1917 Brown University, Providence, RI 02912 USA.
<jhs@math.brown.edu>

Summary. Let $P \in E(\mathbb{Q})$ be a nontorsion point on an elliptic curve given by a minimal Weierstrass equation and write $x(nP) = A_n/D_n^2$ as a fraction in lowest terms. The sequence $\mathcal{D}_P = (D_n)_{n \geq 1}$ is the *elliptic divisibility sequence* (EDS) associated to P . A prime p is a *primitive divisor* of D_n if $p|D_n$ and $p \nmid D_1 D_2 \cdots D_{n-1}$. The Zsigmondy set $Z(P)$ is the set of n such that D_n has no primitive divisors. It is known that $Z(P)$ is finite. In the first part of the paper we prove various uniform bounds for the size of the set $Z(P)$ including: (1) if $j(E) \in \mathbb{Z}$, then $\#Z(P)$ is bounded independently of E and P , and (2) if the *abc*-conjecture is true, then $\#Z(P)$ is bounded independently of E and P for all curves and points. In the second part of the paper we derive upper bounds for the maximum element in $Z(P)$ for points on twists of a fixed elliptic curve.

Introduction

Let E/\mathbb{Q} be an elliptic curve given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_1, \dots, a_6 \in \mathbb{Z} \quad (1.1)$$

and let $P \in E(\mathbb{Q})$ be a point of infinite order. For each $n \geq 1$ the n^{th} iterate of P has the form

$$nP = \left(\frac{A_n}{D_n^2}, \frac{B_n}{D_n^3} \right),$$

where the fractions are written in lowest terms and we assume that $D_n > 0$. The sequence $\mathcal{D}_{E,P} = (D_n)_{n \geq 1}$ is called the *elliptic divisibility sequence* associated to E and P . It is a divisibility sequence in the sense that if $m|n$,

* The first author's research supported in part by a grant from NSERC of Canada.

The second author's research supported by NSA grant H98230-04-1-0064

Subject Class. Primary: 11G05; Secondary 11B37, 14G25, 14H52.

Key Words: elliptic divisibility sequence, elliptic curve, primitive divisor

then $D_m | D_n$, and in fact it satisfies the stronger divisibility relation

$$D_{\gcd(m,n)} = \gcd(D_m, D_n) \quad \text{for all } m, n \geq 1.$$

(See Section 1.1 for a general statement over Dedekind domains.)

The study of the arithmetic properties of elliptic divisibility sequences was initiated by Morgan Ward in the 1940's [34, 35] and has seen a surge of interest in recent years, see for example [1, 2, 5, 6, 8, 9, 10, 11, 12, 13, 18, 23, 31, 32, 33].

If $\mathcal{C} = (C_n)_{n \geq 1}$ is any divisibility sequence, one says that a prime p is a *primitive divisor of C_n* if $p | C_n$ but $p \nmid C_1 C_2 \cdots C_{n-1}$. Primitive divisors of certain divisibility sequences were studied by Zsigmondy [37] in the 19th century. We define the *Zsigmondy set* of a divisibility sequence \mathcal{C} to be

$$Z(\mathcal{C}) = \{n \geq 1 : C_n \text{ does not have a primitive divisor}\}.$$

Zsigmondy was especially interested in divisibility sequences defined by binary linear recurrences satisfying appropriate growth conditions. Bilu, Hanrot, and Voutier [4] recently completed the proof that all of these Lucas and Lehmer sequences satisfy $\max Z(\mathcal{C}) \leq 30$, and there are examples to show that this bound is sharp. They also completely describe all such sequences with $\max Z(\mathcal{C}) \geq 12$. We note that Lucas divisibility sequences are associated to singular elliptic curves, so the material in this paper is, in some sense, a direct generalization of these earlier results.

It is a nontrivial fact that the Zsigmondy set $Z(\mathcal{D}_{E,P})$ of an elliptic divisibility sequence is finite, see [29]. It is natural to ask if there is a uniform bound for $Z(\mathcal{D}_{E,P})$ as there is for the case of binary linear recurrences. The answer is no unless some care is taken, since a simple change of variables $(x, y) \mapsto (u^2 x, u^3 y)$ allows one to multiply every term of the sequence by a power of u . This is the same trick that allows the creation of elliptic curves with arbitrarily many integer points, and the solution to both problems is the same, namely restrict attention to minimal Weierstrass equations. With this restriction, we prove a reasonably strong uniform bound for the number of elements in the set $Z(\mathcal{D}_{E,P})$, and assuming the *abc*-conjecture, we show that $\#Z(\mathcal{D}_{E,P})$ is bounded independently of E and P .

Theorem 1. *Let E/\mathbb{Q} be an elliptic curve given by a minimal Weierstrass equation (1.1), let $P \in E(\mathbb{Q})$ be a point of infinite order, and let $\mathcal{D}_{E,P}$ be the associated elliptic divisibility sequence.*

- (a) *$\#Z(\mathcal{D}_{E,P})$ is bounded by a constant depending only on the number of primes at which E has split multiplicative reduction.*
- (b) *If the *abc*-conjecture over \mathbb{Q} is true, then there is an absolute bound for $\#Z(\mathcal{D}_{E,P})$ that is completely independent of E and P .*

Remark 1. Primes of split multiplicative reduction necessarily divide the denominator of the j -invariant, so a slightly weaker version of (a) is that $\#Z(\mathcal{D}_{E,P})$ is bounded by a constant depending only on number of primes

dividing the denominator of $j(E)$. So for example it is unconditionally true that there is an absolute bound for $\#Z(\mathcal{D}_{E,P})$ as E varies over all elliptic curves with integral j -invariant.

For (b), we prove an unconditional theorem that implies the stated result. We show that $\#Z(\mathcal{D}_{E,P})$ is bounded by a constant depending only on the *Szpiro ratio* of E/\mathbb{Q} defined by

$$\text{Szpiro Ratio}(E/\mathbb{Q}) = \frac{\log |\text{Discriminant } E/\mathbb{Q}|}{\log |\text{Conductor } E/\mathbb{Q}|}.$$

It is well known that the (weak) *abc*-conjecture implies that the Szpiro ratio is bounded independently of E . More precisely, Szpiro has conjectured that for any $\epsilon > 0$ there are only finitely many elliptic curves E/\mathbb{Q} whose Szpiro ratio exceeds $6 + \epsilon$. See [16] for a discussion.

Remark 2. We actually prove a general version of Theorem 1 over number fields. See Theorem 7 in Section 1.3 for the exact statement.

Theorem 1 gives uniform bounds for the size of the Zsigmondy set $Z(\mathcal{D}_{E,P})$, but it does not provide an effective bound for the largest element. Such upper bounds are not known in general for elliptic divisibility sequences, but various partial results are known. For illustrative purposes, we quote a result due to the first author.

Theorem 2. (Ingram [18]) *Let N be a squarefree integer, let E be the elliptic curve $y^2 = x^3 - N^2x$, and let $P \in E(\mathbb{Q})$ be a point of infinite order. Then*

$$Z(\mathcal{D}_{E,P}) \cap 2\mathbb{Z} \subset \{2\} \quad \text{and} \quad Z(\mathcal{D}_{E,P}) \cap 5\mathbb{Z} = \emptyset.$$

Further, if $P \in 2E(\mathbb{Q})$ or if $x(P) < 0$, then $Z(\mathcal{D}_{E,P}) \subset \{1, 2\}$.

The main contribution of [18] is to provide, for fixed $n \geq 3$, an effective method for finding all elliptic divisibility sequences $\mathcal{D}_{E,P}$ arising from curves of the above form, such that $n \in Z(\mathcal{D}_{E,P})$. The problem of finding all such sequences is reduced to that of solving a certain Thue-Mahler equation involving the binary form

$$\prod_Q (X - x_Q Y),$$

where Q ranges over points on $E(\bar{\mathbb{Q}})$ of exact order n . Note that this is entirely analogous to the method used in [4], originally outlined by Schinzel [21], wherein the problem of finding all Lucas sequences \mathcal{C} such that $n \in Z(\mathcal{C})$ is reduced to solving a Thue-Mahler equation involving the n th cyclotomic polynomial. Unfortunately, the analogy to [4] doesn't provide a bound on $\max Z(\mathcal{D}_{E,P})$, but bounds produced by *ad hoc* methods in [10] can be reduced, using the above observation, to those presented in Theorem 2.

This idea rests on the observation that the points of order n on E vary predictably as E runs over a family of quadratic twists of a fixed curve. Thus, one

may show that, for fixed $n \geq 3$, the collection of elliptic divisibility sequences $\mathcal{D}_{E,P}$ such that $n \in Z(\mathcal{D}_{E,P})$, where E runs over the quadratic twists of *any* fixed elliptic curve, is finite and effectively computable. In Section 1.4, we present a result to this effect over number fields. Note that the proof can easily be modified to treat families of curves defined by quartic or sextic twisting, as in [18].

The methods used in [10] to obtain bounds on the largest element of $Z(\mathcal{D}_{E,P}) \cap 2\mathbb{Z}$ make critical use of the existence of rational points of order two on the curves in question, affording one a strong, explicit lower bound on the denominators of points that are divisible by two in the Mordell-Weil group. If one is willing to forsake the effective computability of these bounds, one may generalize these techniques. In the proof of Theorem 6 we use Roth's Theorem on diophantine approximation to show that

$$\max(Z(\mathcal{D}_{E,P}) \cap p\mathbb{Z})$$

may be bounded for any sufficiently large prime p if E ranges, again, over the quadratic twists of a fixed elliptic curve.

Finally, in Section 1.5 we turn our attention back to elliptic divisibility sequences over \mathbb{Q} with the aim of seeing what certain common conjectures tell us about $\max Z(\mathcal{D}_{E,P})$. We show that if Hall's Conjecture is true, then $Z(\mathcal{D}_{E,P}) \subseteq \{1, 2, 3, 4\}$ for all but finitely many elliptic divisibility sequence arising from (minimal) curves of the form $E : y^2 = x^3 + M$. Analogous results can be obtained for other families with fixed j -invariant if one accepts a generalization of Hall's Conjecture due to Lang. Even with these generous assumptions, a uniform bound on $Z(\mathcal{D}_{E,P})$ seems out of reach.

1.1 Elliptic divisibility sequences over Dedekind domains

In this section we prove some basic theorems concerning elliptic divisibility sequences over a characteristic 0 Dedekind domains R . Let K be the fraction field of R and let E/K be an elliptic curve given by a Weierstrass equation (1.1) with coefficients $a_i \in R$. For any nonzero point $P = (x_P, y_P) \in E(K)$ we define the *denominator ideal of P* to be the ideal $D_P \subset R$ specified by

$$\text{ord}_{\mathfrak{p}}(D_P) = \frac{1}{2} \max\{0, -\text{ord}_{\mathfrak{p}}(x_P)\} \quad \text{for all } 0 \neq \mathfrak{p} \in \text{Spec}(R).$$

Here $\text{ord}_{\mathfrak{p}} : K^* \rightarrow \mathbb{Z}$ is the normalized valuation associated to \mathfrak{p} . The *elliptic divisibility sequence* (EDS) associated to a nontorsion point $P \in E(K)$ is the sequence of ideals

$$\mathcal{D}_{E,P} = (D_{nP})_{n \geq 1}.$$

Proposition 1. *Let $\mathcal{D}_{E,P}$ be an EDS as above and let $\mathfrak{p} \in \text{Spec}(R)$ be a nonzero prime ideal. Let p be the characteristic of R/\mathfrak{p} and let $e_{\mathfrak{p}} = \text{ord}_{\mathfrak{p}}(p)$ be the ramification index of p .*

- (a) $\text{ord}_{\mathfrak{p}}(D_{\gcd(m,n)P}) = \min\{\text{ord}_{\mathfrak{p}}(D_{mP}), \text{ord}_{\mathfrak{p}}(D_{nP})\}$ for all $m, n \geq 1$.
- (b) If $\text{ord}_{\mathfrak{p}}(D_{nP}) > e_{\mathfrak{p}}/(p-1)$, then

$$\text{ord}_{\mathfrak{p}}(D_{knP}) = \text{ord}_{\mathfrak{p}}(D_{nP}) + \text{ord}_{\mathfrak{p}}(k) \quad \text{for all } k \geq 1.$$

Proof. It suffices to prove the proposition after localizing and completing R and K at \mathfrak{p} . For each integer $i \geq 1$ let

$$E_i(K) = \{Q \in E(K) : -\text{ord}_{\mathfrak{p}}(x_Q) \geq 2i\}.$$

We also let $E_0(K) = E(K)$, which is not quite standard notation, but suffices for our purposes. Then all of the $E_i(K)$ are subgroups of E , see for example [27, Chap. IV]. We also observe that

$$\text{ord}_{\mathfrak{p}}(D_Q) = \max\{i \geq 0 : Q \in E_i(K)\}.$$

Let m and n be positive integers and let $d = \gcd(m, n)$. Write $d = am + bn$ for some $a, b \in \mathbb{Z}$. Further let

$$i = \text{ord}_{\mathfrak{p}}(D_{mP}), \quad j = \text{ord}_{\mathfrak{p}}(D_{nP}), \quad \text{and} \quad k = \text{ord}_{\mathfrak{p}}(D_{dP})$$

Thus $mP \in E_i(K)$ and $nP \in E_j(K)$. The fact that the $E_i(K)$ are subgroups of $E(K)$ allows us to conclude that

$$dP = a(mP) + b(nP) \in E_i(K) + E_j(K) = E_{\min\{i,j\}}(K).$$

Hence

$$k = \text{ord}_{\mathfrak{p}}(D_{dP}) \geq \min\{i, j\}.$$

For the opposite inequality, we use the fact that $d|m$ to conclude that

$$mP = \frac{m}{d} \cdot dP \in \frac{m}{d} E_k(K) \subset E_k(K),$$

so $i = \text{ord}_{\mathfrak{p}}(D_{mP}) \geq k$. Similarly $j \geq k$, which completes the proof of (a).

In order to prove (b), we use the fact that the subgroup $E_1(K)$ has the structure of a formal group and the $E_i(K)$ form a filtration of subgroups of $E_1(K)$. Further, for $i > e_{\mathfrak{p}}/(p-1)$, there are filtration compatible isomorphisms

$$E_i(K) \longrightarrow \mathfrak{p}^i, \tag{1.2}$$

where the group structure on \mathfrak{p}^i is simply addition. (See [27, Chap. IV] for proofs of these basic facts.)

Now suppose that $\text{ord}_{\mathfrak{p}}(D_{nP}) > e_{\mathfrak{p}}/(p-1)$. Then we can identify nP with some $z \in R$ satisfying $\text{ord}_{\mathfrak{p}}(z) = \text{ord}_{\mathfrak{p}}(D_{nP})$, and the formal group isomorphism (1.2) tells us that

$$\text{ord}_{\mathfrak{p}}(D_{knP}) = \text{ord}_{\mathfrak{p}}(kz) = \text{ord}_{\mathfrak{p}}(k) + \text{ord}_{\mathfrak{p}}(z) = \text{ord}_{\mathfrak{p}}(k) + \text{ord}_{\mathfrak{p}}(D_{nP}).$$

This completes the proof of (b).

Definition 1. Let $\mathcal{D}_{E,P}$ be an elliptic divisibility sequence as above. The rank of apparition of $\mathcal{D}_{E,P}$ at the prime \mathfrak{p} is the smallest integer $r_{\mathfrak{p}} = r_{\mathfrak{p}}(E, P)$ with the property that \mathfrak{p} divides $D_{r_{\mathfrak{p}}P}$.

Definition 2. We say that a prime \mathfrak{p} is exceptional for the elliptic divisibility sequence $D_{E,P}$ if

$$\text{ord}_{\mathfrak{p}}(D_{r_{\mathfrak{p}}P}) \leq \frac{e_{\mathfrak{p}}}{p-1}.$$

We define a modified rank of apparition $s_{\mathfrak{p}}$ by

$$s_{\mathfrak{p}} = \min \left\{ s \geq 1 : \text{ord}_{\mathfrak{p}}(D_{sP}) > \frac{e_{\mathfrak{p}}}{p-1} \right\}. \quad (1.3)$$

Thus \mathfrak{p} is exceptional if and only if $s_{\mathfrak{p}} > r_{\mathfrak{p}}$.

Remark 3. If \mathfrak{p} is exceptional, then necessarily

$$1 \leq \text{ord}_{\mathfrak{p}}(D_{r_{\mathfrak{p}}P}) \leq \frac{e_{\mathfrak{p}}}{p-1} \leq \frac{[K : \mathbb{Q}]}{p-1},$$

so $p \leq [K : \mathbb{Q}] + 1$. In particular, if K is a number field, then there are only finitely many exceptional primes.

Remark 4. If the given Weierstrass equation for E has good reduction at \mathfrak{p} , then $r_{\mathfrak{p}}$ is the order of P in the group $E(\mathbb{F}_{\mathfrak{p}})$.

Proposition 2. Let K/\mathbb{Q} be a number field of degree d and let $\mathcal{D}_{E,P}$ be an elliptic divisibility sequence. Suppose that $m \in Z(\mathcal{D}_{E,P})$ is in the Zsigmondy set of $\mathcal{D}_{E,P}$. Then either $m = s_{\mathfrak{p}}$ for some exceptional prime \mathfrak{p} or else

$$\log N_{K/\mathbb{Q}} D_{mP} \leq \sum_{\substack{k|m \text{ with} \\ m/k \text{ prime}}} \log N_{K/\mathbb{Q}} D_{kP} + d \log(2d) + d \log(m).$$

Proof. Let \mathfrak{p} be a prime dividing D_{mP} , let $r = r_{\mathfrak{p}}$ be the rank of apparition of \mathfrak{p} , and let $s = s_{\mathfrak{p}}$ be the modified rank of apparition of \mathfrak{p} defined by (1.3). We consider several cases:

Case 1. $s \nmid m$.

We know that $r|m$, so in particular we see that $s \neq r$. In other words, the prime \mathfrak{p} is exceptional. Using the strong divisibility property Proposition 1(a), we find that

$$\text{ord}_{\mathfrak{p}}(D_{\gcd(s,m)P}) = \min\{\text{ord}_{\mathfrak{p}}(D_{sP}), \text{ord}_{\mathfrak{p}}(D_{mP})\}.$$

The assumption that $s \nmid m$ implies that $\gcd(s,m)$ is strictly smaller than s , so the definition of the modified rank of apparition tells us that

$$\text{ord}_{\mathfrak{p}}(D_{\gcd(s,m)P}) \leq \frac{e_{\mathfrak{p}}}{p-1} < \text{ord}_{\mathfrak{p}}(D_{sP}).$$

We conclude that

$$\text{ord}_{\mathfrak{p}}(D_{mP}) = \text{ord}_{\mathfrak{p}}(D_{\gcd(s,m)P}) \leq \frac{e_{\mathfrak{p}}}{p-1}.$$

Hence the product over all primes in Case 1 satisfies

$$\prod_{\substack{\mathfrak{p} \\ s_{\mathfrak{p}} \nmid m}} \mathfrak{p}^{\text{ord}_{\mathfrak{p}}(D_{mP})} \left| \prod_p \prod_{\mathfrak{p}|p} \mathfrak{p}^{\lfloor e_{\mathfrak{p}}/(p-1) \rfloor} \right| \prod_{p \leq [K:\mathbb{Q}] + 1} p^{1/(p-1)} \leq 2[K:\mathbb{Q}].$$

(For our purposes, it would suffice to know that the penultimate product is bounded by a constant depending only on $[K:\mathbb{Q}]$. We do not actually need the sharp bound of $2[K:\mathbb{Q}]$.)

Case 2. $s|m$ and $s < m$.

In this case we can apply Proposition 1(b) to obtain the estimate

$$\text{ord}_{\mathfrak{p}}(D_{mP}) = \text{ord}_{\mathfrak{p}}(D_{s(m/s)P}) = \text{ord}_{\mathfrak{p}}(D_{sP}) + \text{ord}_{\mathfrak{p}}(m/s).$$

We also note that if $s_{\mathfrak{p}}|m$ with $s_{\mathfrak{p}} \neq m$, then $s_{\mathfrak{p}}$ necessarily divides some divisor k of m having the property that m/k is prime. Hence the product over all primes satisfying Case 2 is bounded by

$$\prod_{\substack{\mathfrak{p} \\ s_{\mathfrak{p}}|m \\ s_{\mathfrak{p}} \neq m}} \mathfrak{p}^{\text{ord}_{\mathfrak{p}}(D_{mP})} \left| \prod_{\substack{k|m \text{ with} \\ m/k \text{ prime}}} \prod_{\mathfrak{p}} \mathfrak{p}^{\text{ord}_{\mathfrak{p}}(D_{kP}) + \text{ord}_{\mathfrak{p}}(m/k)} \right| m \prod_{\substack{k|m \text{ with} \\ m/k \text{ prime}}} D_{kP}.$$

(In this last expression, the factor of m may be replaced by the squarefree part of m .)

Case 3. $s = m$.

If \mathfrak{p} is exceptional, we have ruled this out by assumption. And if \mathfrak{p} is not exceptional, then $s = r$, and the assumption that m is in the Zsigmondy set implies that $m \neq r$. Hence Case (3) cannot occur.

We now combine the three cases to estimate the norm of D_{mP} . To ease notation, we let $d = [K:\mathbb{Q}]$. Then

$$\begin{aligned} \log N_{K/\mathbb{Q}} D_{mP} &= \sum_{\mathfrak{p} \in \text{Case 1}} \text{ord}_{\mathfrak{p}}(D_{mP}) \log N_{K/\mathbb{Q}} \mathfrak{p} + \sum_{\mathfrak{p} \in \text{Case 2}} \text{ord}_{\mathfrak{p}}(D_{mP}) \log N_{K/\mathbb{Q}} \mathfrak{p} \\ &\leq d \log(2d) + d \log(m) + \sum_{\substack{k|m \text{ with} \\ m/k \text{ prime}}} \log N_{K/\mathbb{Q}} D_{kP}. \end{aligned}$$

This completes the proof of Proposition 2.

We next prove an inequality relating the terms in an elliptic divisibility sequence $\mathcal{D}_{E,P}$ to the heights of the multiples of P . Roughly speaking, the

quantity $\log \mathbf{N}_{K/\mathbb{Q}} D_Q$ is the nonarchimedean contribution to the canonical height $\hat{h}_E(Q)$, so we would expect $\log \mathbf{N}_{K/\mathbb{Q}} D_Q$ to be bound by $\hat{h}_E(Q)$. This is indeed true, and we can make the dependence on E explicit by using standard results relating naive heights to canonical heights. Thus the following result is comparatively elementary compared to Theorem 3 that we prove in Section 1.2.

Proposition 3. *Let E/K be an elliptic curve given by a Weierstrass equation (1.1), let $P \in E(K)$ be a nontorsion point, and define the height of E to be*

$$h(E) = 1 + h([1, a_1^{12}, a_2^6, a_3^4, a_4^3, a_6^2]).$$

Then

$$\frac{1}{[K : \mathbb{Q}]} \log \mathbf{N}_{K/\mathbb{Q}} D_P \leq \hat{h}_E(P) + O(h(E)),$$

where the big- O constant is absolute.

Proof. With appropriate normalizations on the absolute values in K , the absolute logarithmic Weil height of $x(P)$ is

$$h(x(P)) = \sum_{v \in M_K} \max\{0, -v(x(P))\}.$$

If we sum over only the nonarchimedean places we obtain

$$h(x(P)) \geq \sum_{v \in M_K^0} \max\{0, -v(x(P))\} = \frac{2}{[K : \mathbb{Q}]} \log \mathbf{N}_{K/\mathbb{Q}} D_P.$$

Finally, we use a uniform estimate for the difference between the Weil height and the canonical height

$$\hat{h}(P) = \frac{1}{2} h(x(P)) + O(1 + h(E)), \quad (1.4)$$

see [7, 30, 36] for example, where the big- O constant is absolute.

1.2 A uniform quantitative version of Siegel's integrality theorem for elliptic curves

A famous theorem of Siegel says that an elliptic curve has only finitely many integral points. Siegel actually proved something much stronger. For any point $P \in E(\mathbb{Q})$, we write $x(P) = A_P/D_P^2$ in lowest terms with $D_P \geq 1$ and we set

$$h(P) = \frac{1}{2} \log \max\{|A_P|, D_P^2\}.$$

Then Siegel proved that

$$\lim_{\substack{P \in E(\mathbb{Q}) \\ h(P) \rightarrow \infty}} \frac{\log D_P^2}{h(P)} = 1. \quad (1.5)$$

(See [27, IX.3.3].) Using the fact that $h(nP) \sim n^2 \hat{h}(P)$, where \hat{h} is the canonical height on E , this shows that elliptic divisibility sequences over \mathbb{Q} grow very rapidly,

$$\lim_{n \rightarrow \infty} \frac{\log D_{nP}}{n^2} = \hat{h}(P) > 0. \quad (1.6)$$

And indeed it is an easy exercise using Siegel's deep result (1.6) and the elementary estimates given in Proposition 1 to prove that the Zsigmondy set $Z(D_{nP})$ of an elliptic divisibility sequence is finite, see [29] or [27, Exercise 9.4].

Siegel's proof of the finiteness of $E(\mathbb{Z})$ can be used to give an upper bound for $\#E(\mathbb{Z})$, but the bound depends rather badly on the equation defining E . Dem'janenko in a special case and Lang in general [19] made the following conjecture.

Conjecture 1. (Lang-Dem'janenko) Let E/\mathbb{Q} be an elliptic curve given by a minimal Weierstrass equation. Then $\#E(\mathbb{Z})$ is bounded by a constant that depends only on the rank of $E(\mathbb{Q})$.

As in Siegel's work, rather than simply bounding the size of $E(\mathbb{Z})$, one can ask for a uniform bound for the number of points in $E(\mathbb{Q})$ that do not satisfy some inequality related to the limit (1.5). An bound of this sort was proven by the second author in [28], and in this section we apply the results from [28] to deduce uniform information about Zsigmondy sets of elliptic divisibility sequences.

However, we need to take some care, because an elliptic curve E/\mathbb{Q} and a nontorsion point $P \in E(\mathbb{Q})$ do not completely determine an elliptic divisibility sequence. The reason is that the definition of the associated EDS uses a specific Weierstrass equation for E/\mathbb{Q} . One solution is to take a global minimal Weierstrass equation, which works fine over \mathbb{Q} , but unfortunately if K has class number larger than 1, then there exist elliptic curves E/K that do not have a global minimal Weierstrass equation [3, 26]. In this case one could work with a Néron model for E/K , but instead we will simply put the dependence on the choice of Weierstrass equation into our notation.

Let K be a number field and let R_K be its ring of integers. For a given 5-tuple of values $\mathbf{a} = (a_1, a_2, a_3, a_4, a_6) \in R_K^5$, let $E_{\mathbf{a}}$ denote the Weierstrass equation (1.1) with the given coefficients and define the height of $E_{\mathbf{a}}$ to be

$$h(E_{\mathbf{a}}) = 1 + h([1, a_1^{12}, a_2^6, a_3^4, a_4^3, a_6^2]).$$

The canonical height \hat{h} is a positive definite quadratic form on the Mordell-Weil group $E_{\mathbf{a}}(K)$ modulo torsion, and we write

$$\lambda(E_{\mathbf{a}}/K) = \min\{\hat{h}(Q) : Q \in E_{\mathbf{a}}(K), Q \text{ nontorsion}\}.$$

In the language of the geometry of numbers, $\lambda(E_{\mathbf{a}}/K)$ is the first minimum of the quadratic form \hat{h} on the lattice $E_{\mathbf{a}}(K)/E_{\mathbf{a}}(K)_{\text{tors}}$.

We can now state the special case of [28] that we need to give a uniform bound for the size of the Zsigmondy set of an EDS.

Theorem 3. *With notation as above, for all $\epsilon > 0$ and all $d \geq 1$ there is a constant $C = C(\epsilon, d)$ with the following property: Let K/\mathbb{Q} be a number field of degree at most d , let $\mathbf{a} \in R_K^5$ be a 5-tuple so that $E_{\mathbf{a}}$ is an elliptic curve, let $P \in E_{\mathbf{a}}(K)$ be a nontorsion point, and let $M \geq 1$. Form the elliptic divisibility sequence $(D_{nP})_{n \geq 1}$ as described in Section 1.1. Then the set*

$$\left\{ n \geq 1 : \frac{1}{[K : \mathbb{Q}]} \log \mathbf{N}_{K/\mathbb{Q}}(D_{nP}) \leq (1 - \epsilon)n^2 \hat{h}(P) + Mh(E_{\mathbf{a}}) \right\}$$

has at most $C \sqrt{Mh(E_{\mathbf{a}})/\lambda(E_{\mathbf{a}}/K)}$ elements.

Proof. This is a version of Theorem 4.1 in [28], see also [14] for similar results with explicit (albeit huge) constants. We briefly indicate how the results in [28] imply our statement. A direct application of [28, Theorem 4.1] to the family of Weierstrass equations $E \rightarrow \mathbb{P}^5$ yields

$$\begin{aligned} & \# \left\{ P \in E_{\mathbf{a}}(K) : \sum_{v \in S} \lambda_{E_{\mathbf{a}},(O)}(P, v) \geq \epsilon \hat{h}_{E_{\mathbf{a}}}(P) - Mh(E_{\mathbf{a}}) \right\} \\ & \leq \#E_{\mathbf{a}}(K)_{\text{tors}} \cdot C^{1+\#S+\text{rank } E_{\mathbf{a}}(K)} \left(\frac{Mh(E_{\mathbf{a}})}{\lambda(E_{\mathbf{a}}/K)} \right)^{\frac{1}{2} \text{rank } E_{\mathbf{a}}(K)}. \end{aligned} \quad (1.7)$$

(We refer the reader to [28] for a complete description of the notation. In particular, the constant C depends only on $[K : \mathbb{Q}]$ and ϵ .) This is not quite what we want, since we are dealing with a rank one torsion-free subgroup of $E_{\mathbf{a}}(K)$, namely the subgroup generated by a particular point $P \in E_{\mathbf{a}}(K)$. However, the proof in [28] is easily adapted to subgroups of $E(K)$, so in (1.7) we can replace $E_{\mathbf{a}}(K)$ by the set $\{nP : n \in \mathbb{Z}\}$, which also means that we put $\#E_{\mathbf{a}}(K)_{\text{tors}} = 1$ and $\text{rank } E_{\mathbf{a}}(K) = 1$. Further, we take $S = M_K^{\infty}$ to be the set of archimedean places of K , so we can absorb the dependence on $\#S$ into the constant C . Then for $P \in E_{\mathbf{a}}(K)$ we have the estimate (for a new constant $C = C([K : \mathbb{Q}], \epsilon)$)

$$\# \left\{ n \geq 1 : \sum_{v \in M_K^{\infty}} \lambda_{E_{\mathbf{a}},(O)}(nP, v) \geq \epsilon \hat{h}_{E_{\mathbf{a}}}(nP) - Mh(E_{\mathbf{a}}) \right\} \leq C \sqrt{\frac{Mh(E_{\mathbf{a}})}{\lambda(E_{\mathbf{a}}/K)}}. \quad (1.8)$$

The local height function $\lambda_{E_{\mathbf{a}},(O)}$ is given by

$$\lambda_{E_{\mathbf{a}},(O)}(Q, v) = \frac{1}{2} \max\{0, -v(x(Q))\},$$

where the valuations are normalized so that the absolute logarithmic height of $\alpha \in K^*$ is given by the formula $h(\alpha) = \sum_v \max\{0, -v(\alpha)\}$. Hence

$$\begin{aligned} \sum_{M_K^\infty} \lambda_{E_{\mathbf{a}},(O)}(Q, v) &= \frac{1}{2} \sum_{M_K^\infty} \max\{0, -v(x(Q))\} \\ &= \frac{1}{2} h(x(Q)) - \frac{1}{2} \sum_{M_K^0} \max\{0, -v(x)\} \\ &= \frac{1}{2} h(x(Q)) - \frac{1}{[K : \mathbb{Q}]} \log \mathbf{N}_{K/\mathbb{Q}}(D_Q) \\ &= \hat{h}_{E_{\mathbf{a}}}(Q) + O(h(E_{\mathbf{a}})) - \frac{1}{[K : \mathbb{Q}]} \log \mathbf{N}_{K/\mathbb{Q}}(D_Q). \end{aligned}$$

(For the last line we have again used (1.4). Note that the big- O constant is absolute.) Putting $Q = nP$ yields

$$\sum_{M_K^\infty} \lambda_{E_{\mathbf{a}},(O)}(nP, v) = \hat{h}_{E_{\mathbf{a}}}(nP) - \frac{1}{[K : \mathbb{Q}]} \log \mathbf{N}_{K/\mathbb{Q}}(D_{nP}) + O(h(E_{\mathbf{a}})).$$

Substituting this into (1.8) gives

$$\begin{aligned} \#\left\{n \geq 1 : (1 - \epsilon)\hat{h}_{E_{\mathbf{a}}}(nP) + (M - C')h(E_{\mathbf{a}}) \geq \frac{1}{[K : \mathbb{Q}]} \log \mathbf{N}_{K/\mathbb{Q}}(D_{nP})\right\} \\ \leq C \sqrt{\frac{Mh(E_{\mathbf{a}})}{\lambda(E_{\mathbf{a}}/K)}}, \quad (1.9) \end{aligned}$$

where $C' \geq 0$ is an absolute constant. Finally, we replace M by $M + C'$, use the inequality $M + C' \leq (1 + C')M$, and increase the value of C accordingly. Then (1.9) and the canonical height property $\hat{h}(nP) = n^2\hat{h}(P)$ give the desired result, which completes the proof of Theorem 3.

1.3 A uniform Zsigmondy estimate

We have now assembled all the tools needed to prove a uniform bound for the size of the Zsigmondy set of an elliptic divisibility sequence.

Theorem 4. *Continuing with the notation from Sections 1.2 and 1.1, let $\mathbf{a} \in R_K^5$ so that $E_{\mathbf{a}}$ is an elliptic curve and let $P \in E_{\mathbf{a}}(K)$ be a nontorsion point. Then there is a constant $C = C([K : \mathbb{Q}])$ such that*

$$\#Z(\mathcal{D}_{E_{\mathbf{a}},P}) \leq Ch(E_{\mathbf{a}})/\lambda(E_{\mathbf{a}}/K).$$

Proof. As noted in Remark 3, the number of exceptional primes is bounded by a constant depending only on $[K : \mathbb{Q}]$, so without loss of generality we

may discard from $Z(\mathcal{D}_{E_{\mathbf{a}},P})$ all m with the property that $m = s_{\mathfrak{p}}$ for some exceptional prime \mathfrak{p} .

Let $m \in Z(\mathcal{D}_{E_{\mathbf{a}},P})$. Then Theorem 3 (with $\epsilon = \frac{1}{4}$ and $M = 1$) says that with at most $O(\sqrt{h(E_{\mathbf{a}})/\lambda(E_{\mathbf{a}}/K)})$ exceptions, we have

$$\frac{1}{[K : \mathbb{Q}]} \log \mathbf{N}_{K/\mathbb{Q}}(D_{mP}) \geq \frac{3}{4} m^2 \hat{h}(P). \quad (1.10)$$

In the other direction, Propositions 2 and 3 allow us to estimate

$$\begin{aligned} & \frac{1}{[K : \mathbb{Q}]} \log \mathbf{N}_{K/\mathbb{Q}} D_{mP} \\ & \leq \sum_{k|m, k \neq m} \frac{1}{[K : \mathbb{Q}]} \log \mathbf{N}_{K/\mathbb{Q}} D_{kP} + \log(2[K : \mathbb{Q}]) + \sqrt{m} \log(m) \\ & \leq \sum_{k|m, k \neq m} (\hat{h}(kP) + O(h(E_{\mathbf{a}}))) + \log(2[K : \mathbb{Q}]) + \sqrt{m} \log(m) \\ & \leq \sum_{k|m, k \neq m} k^2 \hat{h}(P) + O(mh(E_{\mathbf{a}})) \end{aligned} \quad (1.11)$$

We also have the trivial estimate

$$\sum_{k|m, k \neq m} k^2 \leq m^2 \sum_{k|m, k \geq 2} \frac{1}{k^2} \leq m^2 (\zeta(2) - 1). \quad (1.12)$$

Combining (1.10), (1.11) and (1.12) yields

$$\left(\frac{7}{4} - \zeta(2)\right) m^2 \hat{h}(P) \leq O(mh(E_{\mathbf{a}})).$$

Since $\frac{7}{4} - \zeta(2) \approx 0.105 > 0$, we find that

$$m \leq O(h(E_{\mathbf{a}})/\hat{h}(P)) \leq O(h(E_{\mathbf{a}})/\lambda(E_{\mathbf{a}}/K)).$$

All of the big- O constants depend only on $[K : \mathbb{Q}]$, so this completes the proof of Theorem 4.

In order to apply Theorem 4, we need some sort of upper bound for the ratio $h(E_{\mathbf{a}})/\lambda(E_{\mathbf{a}}/K)$. The denominator depends only on the K -isomorphism class of $E_{\mathbf{a}}$, while the numerator depends on the particular Weierstrass model. For example, if we let

$$u \star \mathbf{a} = [1, ua_1, u^2 a_2, u^3 a_3, u^4 a_4, u^6 a_6],$$

then $E_{u \star \mathbf{a}}$ is K -isomorphic to $E_{\mathbf{a}}$, but it is not hard to see that $h(E_{u \star \mathbf{a}}) = h(E_{\mathbf{a}}) + 12h(u) + O(1)$. Thus in order to obtain a completely uniform upper bound in Theorem 4, we must put some restriction on the choice of \mathbf{a} .

Definition 3. Put a partial order on R_K^5 by setting $\mathbf{a} \leq \mathbf{b}$ if

$$E_{\mathbf{a}} \cong_{/K} E_{\mathbf{b}} \quad \text{and} \quad N_{K/\mathbb{Q}} \text{Disc}(E_{\mathbf{a}}) \leq N_{K/\mathbb{Q}} \text{Disc}(E_{\mathbf{b}}).$$

A Weierstrass equation $E_{\mathbf{a}}$ is called K -quasiminimal if \mathbf{a} is a minimal element for this partial order.

It is clear that every elliptic curve has a quasiminimal Weierstrass equation. The following is a natural generalization of a conjecture of Lang [19], which he made based on some preliminary work of Dem'janenko.

Conjecture 2. (Lang) Let K/\mathbb{Q} be a number field. There is a positive constant $C = C(K)$ such that for all K -quasiminimal Weierstrass equations $E_{\mathbf{a}}$ over K we have

$$\lambda(E_{\mathbf{a}}/K) \geq Ch(E_{\mathbf{a}}).$$

Clearly Lang's Conjecture 2 combined with Theorem 4 imply that the size of the Zsigmondy set of an elliptic divisibility sequence on a K -quasiminimal elliptic curve is bounded by a constant depending only on K/\mathbb{Q} . We mention two other conjectures that turn out to be related to Lang's conjecture.

Definition 4. The Szpiro ratio of an elliptic curve E/K is the quantity

$$\sigma(E/K) = \frac{\log N_{K/\mathbb{Q}} \text{Disc}(E/K)}{\log N_{K/\mathbb{Q}} \text{Cond}(E/K)},$$

where $\text{Cond}(E/K)$ is the conductor of E/K . (For our purposes, it would suffice to replace $\text{Cond}(E/K)$ with the product of the primes at which E/K has bad reduction.)

Conjecture 3. (Szpiro) For any $\epsilon > 0$ there are only finitely many elliptic curves E/K satisfying $\sigma(E/K) \geq 6 + \epsilon$.

It is well known that the abc -conjecture of Masser and Osterlé implies Szpiro's conjecture. Less obvious is the fact that Lang's conjecture is a consequence of Szpiro's conjecture.

Theorem 5. (Hindry-Silverman [16]) *Szpiro's Conjecture 3 implies Lang's Conjecture 2. More precisely, there is a positive constant $C = C(K)$ such that for all K -quasiminimal Weierstrass equations $E_{\mathbf{a}}$ over K we have*

$$\lambda(E_{\mathbf{a}}/K) \geq C^{1+\sigma(E_{\mathbf{a}})} h(E_{\mathbf{a}}).$$

We also quote another partial result on Lang's conjecture in which the constant depends in a mild way on the elliptic curve.

Theorem 6. (Silverman [25]) *With notation as above, let $\nu(E_{\mathbf{a}})$ be the number of primes of K at which $E_{\mathbf{a}}$ has split multiplicative reduction. Then*

$$\lambda(E_{\mathbf{a}}/K) \geq C^{1+\nu(E_{\mathbf{a}})} h(E_{\mathbf{a}}).$$

Combining all of this material yields a number field version of the result (Theorem 1) stated in the introduction.

Theorem 7. *Let K/\mathbb{Q} be a number field, let E/K be an elliptic curve given by a K -quasiminimal Weierstrass equation, let $\sigma(E/K)$ be the Szpiro ratio of E/K , and let $\nu(E/K)$ be the number of primes of K at which E/K has split multiplicative reduction. Let $P \in E(K)$ be a point of infinite order, let $\mathcal{D}_{E,P}$ be the associated elliptic divisibility sequence, and consider its Zsigmondy set $Z(\mathcal{D}_{E,P})$. There is a constant $C = C(K)$ depending only on K such that:*

$$(a) \#Z(\mathcal{D}_{E,P}) \leq C^{1+\nu(E/K)}.$$

$$(b) \#Z(\mathcal{D}_{E,P}) \leq C^{1+\sigma(E/K)}.$$

If Szpiro's conjecture or the abc-conjecture is true, then $\#Z(\mathcal{D}_{E,P})$ is bounded by a constant that depends only on K .

Proof. The estimate in (a) follows by combining Theorems 4 and 6, and the estimate in (b) follows similarly by combining Theorems 4 and 5. The final statement is clear, since Szpiro's conjecture says that $\sigma(E/K)$ is bounded independently of E , and it is well known that the *abc*-conjecture implies Szpiro's conjecture. (Note that we actually only need a weak version of either conjecture, i.e., it suffices to have any exponent, we do not need $6 + \epsilon$ in Szpiro's conjecture or $1 + \epsilon$ in the *abc*-conjecture.)

1.4 Results for quadratic twists

Theorem 7 bounds $\#Z(\mathcal{D}_{E,P})$ for all curves E/K given by a K -quasiminimal Weierstrass equation with at most a fixed number of primes dividing the denominator of $j(E)$. It is certainly true, then, that $\#Z(\mathcal{D}_{E,P})$ is bounded as E varies over the K -quasiminimal quadratic twists of a fixed curve. It is natural to ask whether, in this specific context, one can bound $\max Z(\mathcal{D}_{E,P})$ uniformly. Although a result of this sort seems out of reach at the moment, we can prove a strong bound in the case that P is in the image of an isogeny. In particular, if we consider, for a sufficiently large prime p , nontorsion points $P \in pE(K)$ as E runs over (minimal) quadratic twists of some fixed curve, we can show that $\max Z(\mathcal{D}_{E,P})$ is bounded by a constant depending only on $j(E)$ and p .

Explicit results along these lines, over \mathbb{Q} and with $p = 2$, are given in [10], and we use similar techniques to obtain the more general results described above. In [18], the first author gave sharpened estimates for $\max Z(\mathcal{D}_{E,P})$ when $P \in E(\mathbb{Q})$ and $j(E) \in \{0, 1728\}$. Specifically, if we consider minimal E/\mathbb{Q} of the form

$$y^2 = x^3 + Ax \quad \text{or} \quad y^2 = x^3 + A,$$

then for a fixed integer k greater than 3 in the first case and 4 in the second, it was proven that the set of pairs $\{(A, P) : k \in Z(\mathcal{D}_{E,P})\}$ is finite and effectively computable. Thus any bound on $\max Z(\mathcal{D}_{E,P})$ for a family of elliptic divisibility sequences arising from these curves may be, with a finite number of exceptions, reduced to a bound of 3 or 4, respectively. Furthermore, this finite set of exceptions is effectively (although often not practically) computable. We will extend these results to families of twists over number fields. For the remainder of the section we will, for simplicity, work with elliptic curves in short Weierstrass form (i.e., with $a_1 = a_2 = a_3 = 0$, in the notation above). We will say that such a model is K -quasiminimal if it has minimal discriminant amongst K -isomorphic curves in the same form. Such curves might not be K -quasiminimal in the sense above, but will be away from primes dividing 2 and 3.

To prove the next two theorems, we require tools that trace back, in spirit, to the original paper of Ward [35]. Ward considers sequences $(h_n)_{n \in \mathbb{Z}}$ satisfying the relation

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2, \tag{1.13}$$

with $h_0 = 0$, $h_1 = 1$, and $h_2|h_4$ (a definition that makes sense over any integral domain). It is worth noting that the sequences described in [35] do not correspond directly to the sequences discussed here, and we reserve the term *elliptic divisibility sequence* for the latter. For example, if we consider the elliptic divisibility sequence $\mathcal{D}_{E,P}$ defined by the point (12, 36) on the elliptic curve $y^2 = x^3 - 36x$, we have

$$D_P = (1), D_{2P} = (2), D_{3P} = (23), D_{4P} = (140), D_{5P} = (52487) \dots$$

It is clear that we cannot choose generators $h_n \in \mathbb{Z}$ of the ideals D_{nP} which satisfy the recursion (1.13), in particular because this would require (setting $m = 3$ and $n = 2$)

$$52487 = |h_5| \leq |h_4h_2^3| + |h_3^3h_1| = 13287.$$

Although our sequence $\mathcal{D}_{E,P}$ is not necessarily an elliptic divisibility sequence in the sense of Ward, one may associate a Ward-type sequence to it. Recall (from, e.g., [27, p. 105]) the division polynomials of an elliptic curve

$$E : y^2 = x^3 + Ax + B.$$

They are elements of the function field $K(E)$ defined by setting

$$\begin{aligned} \psi_0 &= 0, & \psi_1 &= 1, & \psi_2 &= 2y, & \psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2, \\ \psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3), \end{aligned}$$

and then using the recursion (1.13) to define the other ψ_n . It is an easy exercise to show that ψ_n^2 may be written as a polynomial in x for all n . More

precisely, ψ_n (respectively ψ_n/y) may be written as a polynomial in x if n is odd (respectively even). We will abuse notation by writing either $\psi_n(P)$ or $\psi_n(x_P)$ when $\psi_n \in K(x)$.

If $P \in E(K)$, then $(\psi_n(P))_{n \in \mathbb{Z}}$ is a sequence (in K) satisfying (1.13), by construction. While we would like to consider sequences in R , rather than K , which relate to $\mathcal{D}_{E,P}$, it is difficult to do this if R is not a principal ideal domain. Note that if S_0 is a finite set of primes of R , it is always possible to extend S_0 to a finite set S such that the localization R_S of R at S is a principal ideal domain. If the R_S -ideal $D_P R_S$ is principal, and is generated by t , then a simple induction shows that the sequence

$$h_n = t^{n^2-1} \psi_n(P) \tag{1.14}$$

is a sequence in R_S satisfying (1.13). This sequence depends on the choice of t , but only up to multiplication by S -units. The following proposition, due essentially to Ward [35] and Ayad [1, 2] indicates how this sequence relates to $\mathcal{D}_{E,P}$.

Proposition 4. *Let E be an elliptic curve as above, let $P \in E(K)$ be a point of infinite order, let S be a finite set of primes such that R_S is a PID, and let $\mathfrak{p} \in \text{Spec}(R_S)$ be a nonzero prime ideal.*

(a) *For all n ,*

$$\text{ord}_{\mathfrak{p}}(h_n) \geq \text{ord}_{\mathfrak{p}}(D_{nP}/D_P).$$

(b) *If $\text{ord}_{\mathfrak{p}}(h_n) > \text{ord}_{\mathfrak{p}}(D_{nP}/D_P)$ for any n , then \mathfrak{p} is a prime of bad reduction for E , and P has singular reduction modulo \mathfrak{p} .*

Proof. To prove (a), we note that if $t \in R_S$ is a generator for $D_P R_S$, and we set

$$k_n = t^{2n^2} (x_P \psi_n(P)^2 - \psi_{n+1}(P) \psi_{n-1}(P)) \in R_S,$$

for each n , then $x_{nP} = k_n / (th_n)^2$ (see [27, p. 105]). As k_n and h_n are S -integral, and

$$\text{ord}_{\mathfrak{p}}(D_{nP}) = \frac{1}{2} \max\{0, -\text{ord}_{\mathfrak{p}}(x_{nP})\}$$

it follows at once that $\text{ord}_{\mathfrak{p}}(D_{nP}) \leq \text{ord}_{\mathfrak{p}}(th_n)$, and part (a) follows. Part (b) follows from Théorème A of [1].

We now turn our attention to families of quadratic twists of a fixed elliptic curve over K . Let $A, B \in R$, and let

$$E : y^2 = x^3 + Ax + B$$

be a K -quasiminimal elliptic curve. Another elliptic curve

$$E' : y^2 = x^3 + A'x + B'$$

with $A', B' \in R$, is a *quadratic twist* of E if there is a \overline{K} -isomorphism from E to E' . Writing down the possible isomorphisms between curves of this form [27, p. 49], we see that we must have $A' = \tau^4 A$ and $B' = \tau^6 B$, for some $\tau \in \overline{K}$. Furthermore,

$$\tau^2 = \frac{AB'}{A'B} \in K.$$

Note that if $S \subseteq \text{Spec}(R)$ is a set of nonzero primes containing all primes dividing $AB(4A^3 + 27B^2)$, and such that R_S is a principal ideal domain, then E' can be K -quasiminimal only if $\tau^2 \in R_S$, and $\text{ord}_{\mathfrak{p}}(\tau^2) \leq 1$ for all $\mathfrak{p} \notin S$. If S is such a set of primes, if $P \in E(K)$, and if h_n is defined as in (1.14), then

$$\text{ord}_{\mathfrak{p}}(h_n) = \text{ord}_{\mathfrak{p}}(D_{nP}/D_P)$$

for all $\mathfrak{p} \notin S$ and all n , by Proposition 4. This is, however, not the case for sequences $(h_n)_{n \geq \mathbb{Z}}$ and $\mathcal{D}_{E', P}$ corresponding to points on twists of E , since E' may have bad reduction at primes outside of S . The following proposition allows us to restrict the amount by which the orders of these quantities vary at primes of bad reduction for E' .

Proposition 5. *Let E be as above, and let S be a finite set of primes containing all divisors of $AB(4A^3 + 27B^2)$ and all ramified primes, such that R_S is a principal ideal domain. Let E' be a K -quasiminimal twist of E , and let $P \in E'(K)$ be a point of infinite order. If P has bad reduction at $\mathfrak{p} \notin S$, then*

$$\text{ord}_{\mathfrak{p}}(h_n) = \begin{cases} \frac{n^2-1}{2} & \text{if } 2 \nmid n \\ \frac{n^2-4}{2} + \text{ord}_{\mathfrak{p}}(h_2) + \text{ord}_{\mathfrak{p}}(n) & \text{if } 2 \mid n. \end{cases}$$

Proof. Let $\tau \in \overline{K}$ be as above, so that $\tau^2 \in R_S$

$$E' : y^2 = x^3 + \tau^4 Ax + \tau^6 B.$$

The isomorphism $\phi : E \rightarrow E'$ is given by

$$\phi(x, y) = (x\tau^2, y\tau^3).$$

As E' has bad reduction at $\mathfrak{p} \notin S$, and as $\text{Disc}(E') = \tau^{12} \text{Disc}(E)$, we have $\text{ord}_{\mathfrak{p}}(\tau^2) = 1$. Note that P can have singular reduction at \mathfrak{p} only if $\text{ord}_{\mathfrak{p}}(x_P) \geq 1$. If $\text{ord}_{\mathfrak{p}}(x_P) > 1$, then we have $\text{ord}_{\mathfrak{p}}(x_P^3 + \tau^4 Ax_P) > 3$, and so

$$2 \text{ord}_{\mathfrak{p}}(y_P) = \text{ord}_{\mathfrak{p}}(y_P^2) = \text{ord}_{\mathfrak{p}}(x_P^3 + \tau^4 Ax_P + \tau^6 B) = \text{ord}_{\mathfrak{p}}(\tau^6 B) = 3$$

(recalling that $\text{ord}_{\mathfrak{p}}(B) = 0$ for $\mathfrak{p} \notin S$). This is impossible, as $\text{ord}_{\mathfrak{p}}(y_P) \in \mathbb{Z}$, and hence we must have $\text{ord}_{\mathfrak{p}}(x_P) = 1$.

Let $L = K(\tau)$, let $\mathfrak{p} = \mathfrak{q}^2$ in the ring of integers of L , and let $Q = \phi^{-1}(P) \in E(L)$. While Q is not K -rational, it should be noted that $x_Q = x_P/\tau^2 \in K$. As $\text{ord}_{\mathfrak{p}}(x_P) = 1$, we have $\text{ord}_{\mathfrak{p}}(x_Q) = 0$, and in particular $\mathfrak{q} \nmid D_Q$. From this, and the fact that E has good reduction at \mathfrak{q} , we see from Proposition 4 that

$$\text{ord}_{\mathfrak{q}}(D_{nQ}) = \text{ord}_{\mathfrak{q}}(\psi_{E,n}(Q))$$

for all n (where $\psi_{E,n}$ is the n th division polynomial for E). In particular,

$$\begin{aligned} \text{ord}_{\mathfrak{q}}(D_{2Q}) &= \text{ord}_{\mathfrak{q}}(y_Q) \\ &= \text{ord}_{\mathfrak{q}}(y_P) - 3 \text{ord}_{\mathfrak{q}}(\tau). \end{aligned}$$

We have seen that

$$\text{ord}_{\mathfrak{q}}(y_P) = 2 \text{ord}_{\mathfrak{p}}(y_P) = \text{ord}_{\mathfrak{p}}(x_P^3 + \tau^4 Ax_P + \tau^6 B) \geq 3,$$

and so (as $\text{ord}_{\mathfrak{q}}(y_P)$ is even)

$$\text{ord}_{\mathfrak{q}}(D_{2Q}) > 0.$$

Because $\mathfrak{p} \notin S$, we must have $e_{\mathfrak{p}} = 1$, and thus $e_{\mathfrak{q}} = 2$ (in the extension L/\mathbb{Q}). It follows from Proposition 1(b) that

$$\text{ord}_{\mathfrak{q}}(\psi_{E,n}(Q)) = \text{ord}_{\mathfrak{q}}(D_{nQ}) = \begin{cases} 0 & \text{if } 2 \nmid n \\ \text{ord}_{\mathfrak{q}}(D_{2Q}) + \text{ord}_{\mathfrak{q}}(n) & \text{if } 2 \mid n. \end{cases}$$

An examination of the division polynomials shows that

$$\psi_{E',n}(P) = \tau^{n^2-1} \psi_{E,n}(Q),$$

and so (recalling that $\text{ord}_{\mathfrak{p}}(D_P) = 0$),

$$\begin{aligned} \text{ord}_{\mathfrak{q}}(h_n) &= \text{ord}_{\mathfrak{q}}(\psi_{E',n}(P)) \\ &= (n^2 - 1) \text{ord}_{\mathfrak{q}}(\tau) + \text{ord}_{\mathfrak{q}}(\psi_{E,n}(Q)). \end{aligned}$$

For n odd, the proposition follows immediately, since $\text{ord}_{\mathfrak{q}}(\tau) = 1$, and $\mathfrak{p} = \mathfrak{q}^2$. For n even, note that

$$\text{ord}_{\mathfrak{q}}(D_{2Q}) = \text{ord}_{\mathfrak{q}}(y_P) - 3 \text{ord}_{\mathfrak{q}}(\tau) = \text{ord}_{\mathfrak{q}}(h_2) - 3,$$

and so

$$\text{ord}_{\mathfrak{q}}(h_n) = (n^2 - 1) + \text{ord}_{\mathfrak{q}}(h_2) - 3.$$

Again, we are done as $\mathfrak{p} = \mathfrak{q}^2$.

Theorem 8. *Let E be as above, and fix an integer $k \geq 3$. Then there are only finitely many pairs (P, E') such that E' is a K -quasiminimal twist of E , $P \in E'(K)$ is a point of infinite order, and $k \in Z(\mathcal{D}_{E',P})$.*

Proof. Let S be a set of primes of R which contain all prime divisors of $kAB(4A^3 + 27B^2)$, all ramified primes, and such that R_S is a PID.

By Möbius inversion we write the division polynomials of E as

$$\psi_{E,n} = \prod_{d|n} \psi_{E,n}^*,$$

for some functions $\psi_{E,n}^* \in K(E)$, and the same for E' . Note that for $n \geq 3$, $\psi_{E',n}^* \in K(x)$. For functions $f(x) \in K(x)$, we will write

$$\tilde{f}(x, y) = y^{\deg(f)} f(x/y).$$

Now suppose that $P \in E'(K)$ is as in the statement of the theorem, so that D_{kP} has no primitive divisors. As R_S is a principal ideal domain, we will select $s, t \in R_S$ with $(t) = D_P$ and $s = x_P t^2$. Our first observation, from the definition of the division polynomials, is that

$$\tilde{\psi}_{E',n}(s, t^2) = \tilde{\psi}_{E,n}(s, t^2 \tau^2)$$

for all n (recall that $\tau^2 \in R_S$ is square-free in R_S). Again, to simplify notation, we will set $h_n = \tilde{\psi}_{E',n}(s, t^2)$.

Let $\mathfrak{p} \notin S$ be a prime of R , and consider $\text{ord}_{\mathfrak{p}}(\tilde{\psi}_{E,k}^*(s, t^2 \tau^2))$. There are several cases.

Case 1. P has good reduction at \mathfrak{p} and $r_{\mathfrak{p}} = 1$: In this case, by Proposition 4, we see that

$$\text{ord}_{\mathfrak{p}}(D_{nP}/D_P) = \text{ord}_{\mathfrak{p}}(h_n)$$

for all n . Note that $r_{\mathfrak{p}} = 1$ implies $\mathfrak{p} \mid t$, and hence $\mathfrak{p} \nmid s$. It is an easy exercise [27, p. 105] to show that

$$\psi_{E',m}^2(x) = m^2 x^{m^2-1} + \text{lower order terms}$$

for each m . Recalling that S contains all divisors of k , we have $\text{ord}_{\mathfrak{p}}(d^2 s^{d^2-1}) = 0$ for any $d \mid k$, and so $\text{ord}_{\mathfrak{p}}(h_d) = 0$ for any $d \mid k$. It follows at once that

$$\text{ord}_{\mathfrak{p}}(\tilde{\psi}_k^*(s, t^2)) = 0.$$

Case 2. P has good reduction at \mathfrak{p} and $r_{\mathfrak{p}} > 1$: In this case $\text{ord}_{\mathfrak{p}}(D_P) = 0$, and so Proposition 4 gives us

$$\text{ord}_{\mathfrak{p}}(D_{nP}) = \text{ord}_{\mathfrak{p}}(h_n)$$

for all n . Furthermore, \mathfrak{p} is not a primitive divisor of D_{kP} , and so either $\mathfrak{p} \nmid D_{kP}$, or else $r_{\mathfrak{p}}$ is a proper divisor of k . In the former case it is clear that $\text{ord}_{\mathfrak{p}}(\tilde{\psi}_{E',n}^*(s, t^2)) = 0$, and so we'll suppose that we are in the latter case. We have

$$\text{ord}_{\mathfrak{p}}(D_{r_{\mathfrak{p}}mP}) = \text{ord}_{\mathfrak{p}}(D_{r_{\mathfrak{p}}P}) + \text{ord}_{\mathfrak{p}}(m)$$

for all m , and so if μ is the Möbius function, then

$$\begin{aligned}
\text{ord}_{\mathfrak{p}}(\tilde{\psi}_{E',k}^*(s, t^2)) &= \sum_{d|k} \mu(d) \text{ord}_{\mathfrak{p}}(h_{\frac{k}{d}}) \\
&= \sum_{d|k} \mu(d) \text{ord}_{\mathfrak{p}}(D_{\frac{k}{d}P}) \\
&= \sum_{d|(k/r_{\mathfrak{p}})} \mu(d) \text{ord}_{\mathfrak{p}}(D_{\frac{k}{d}P}),
\end{aligned}$$

as $\text{ord}_{\mathfrak{p}}(D_{mP}) = 0$ if $r_{\mathfrak{p}} \nmid m$. Writing $k = k'r_{\mathfrak{p}}$, we obtain

$$\begin{aligned}
\text{ord}_{\mathfrak{p}}(\tilde{\psi}_{E',k}^*(s, t^2)) &= \sum_{d|k'} \mu(d) \text{ord}_{\mathfrak{p}}(D_{\frac{r_{\mathfrak{p}}k'}{d}P}) \\
&= \sum_{d|k'} \mu(d) (\text{ord}_{\mathfrak{p}}(D_{r_{\mathfrak{p}}P}) + \text{ord}_{\mathfrak{p}}(k'/d)) \\
&= 0,
\end{aligned}$$

as $\text{ord}_{\mathfrak{p}}(k) = 0$, and as $\sum_{d|m} \mu(d) = 0$ for any $m \geq 2$.

Case 3. P has bad reduction at \mathfrak{p} : In this case, Proposition 5 ensures that $\text{ord}_{\mathfrak{p}}(t) = 0$, $\text{ord}_{\mathfrak{p}}(s) = 1 = \text{ord}_{\mathfrak{p}}(\tau^2)$. Also, we have

$$\text{ord}_{\mathfrak{p}}(h_n) = \begin{cases} \frac{n^2-1}{2} & \text{if } 2 \nmid n \\ \frac{n^2-4}{2} + \text{ord}_{\mathfrak{p}}(h_2) + \text{ord}_{\mathfrak{p}}(n) & \text{if } 2 \mid n. \end{cases}$$

If k is odd, we have

$$\begin{aligned}
\text{ord}_{\mathfrak{p}}(\tilde{\psi}_{E',n}^*(s, t^2)) &= \sum_{d|k} \mu(d) \text{ord}_{\mathfrak{p}}(h_{\frac{k}{d}}) \\
&= \sum_{d|k} \mu(d) \deg(\psi_{E',k/d}) = \deg(\psi_{E',n}^*).
\end{aligned}$$

If k is even, we have (recall that $\text{ord}_{\mathfrak{p}}(k) = 0$)

$$\begin{aligned}
\text{ord}_{\mathfrak{p}}(\tilde{\psi}_{E',n}^*(s, t^2)) &= \sum_{d|k} \mu(d) \text{ord}_{\mathfrak{p}}(h_{\frac{k}{d}}) \\
&= \sum_{d|k} \mu(d) \deg(\psi_{E',k/d}) + \sum_{\substack{d|k \\ k/d \text{ even}}} \mu(d) \left(\text{ord}_{\mathfrak{p}}(h_2) - \frac{3}{2} \right) \\
&= \deg(\psi_{E',n}^*).
\end{aligned}$$

The second term in the penultimate line vanishes as $\sum_{d|(k/2)} \mu(d) = 0$.

We now have a value for $\text{ord}_{\mathfrak{p}}(\tilde{\psi}_{E',n}^*(s, t^2))$ in each case. To summarize, if we choose a generator $(g) = sR_S + \tau^2R_S$, we have

$$\text{ord}_{\mathfrak{p}}(\tilde{\psi}_{E',n}^*(s, t^2)) = \deg(\psi_{E',n}^*) \text{ord}_{\mathfrak{p}}(g)$$

for each $\mathfrak{p} \notin S$. In particular,

$$\tilde{\psi}_{E,n}^*(s/g, t^2\tau^2/g) = g^{-\deg(\psi_{E',n}^*)} \tilde{\psi}_{E',n}^*(s, t^2) \tag{1.15}$$

is an S -unit. But s/g and $t^2\tau^2/g$ are S -integers, and

$$\psi_{E,n}^*(x) = \tilde{\psi}_{E,n}^*(x, 1)$$

has at least three distinct roots for $n \geq 3$. Thus (1.15) defines a Thue-Mahler equation which may have only finitely many solutions. Each solutions traces back to a unique pair $(E', \pm P)$, proving the result.

We now turn our attention to the claim that, for a sufficiently large prime p , $\max Z(\mathcal{D}_{E',P})$ may be bounded for points $P \in pE'(K)$ as E' varies through a family of quadratic twists. Translating the problem back to E , this will require us to obtain a lower bound on sizes of the ‘denominators’ D_Q of points $Q \in E(\overline{K})$ such that $[K(Q) : K] \leq 2$. As mentioned above, Siegel’s Theorem allows us to conclude that

$$(1 - \epsilon)\hat{h}(Q) \leq \frac{1}{[K(Q) : \mathbb{Q}]} \log \mathbf{N}_{K(Q)/\mathbb{Q}} D_Q + O(1),$$

but the implied constant depends on the particular field $K(Q)$. This is insufficient for our needs. It turns out, though, that if p is large enough, we can obtain more uniform estimate for points $Q = pQ'$ with $Q' \in E(\overline{K})$ such that $x_{Q'} \in K$.

Proposition 6. *Let E be as above, fix a rational prime $p \geq 3$, and let $\delta > 0$. Let $Q \in E(\overline{K})$ be such that $x_Q \in K$. Then*

$$\left(1 - \frac{[K : \mathbb{Q}](2 + \delta)}{p^2}\right) \hat{h}(pQ) \leq \frac{1}{[K(Q) : \mathbb{Q}]} \log \mathbf{N}_{K(Q)/\mathbb{Q}} D_{pQ} + O(1),$$

where the implied constant depends only on E , K , δ , and p .

Proof. We begin by noting that there is a map $f : \mathbb{P}^1 \rightarrow \mathbb{P}^1$ of degree p^2 such that

$$x_{pQ} = f(x_Q)$$

for all $Q \in E(\overline{K})$. Explicitly, in terms of the division polynomials, we may write

$$f = x - \frac{\psi_{n+1}\psi_{n-1}}{\psi_n^2}.$$

This is, *a priori*, an element of $K(E)$, but is easily shown to lie in $K(x)$.

Writing $\|x\|_v = |x|_v^{[K_v:\mathbb{Q}_v]}$ for all $v \in M_K$, and letting S denote the set of archimedean places of K , we have

$$\begin{aligned} \frac{1}{[K(Q) : \mathbb{Q}]} \log N_{K(Q)/\mathbb{Q}} D_{pQ} &= \frac{1}{[K : \mathbb{Q}]} \sum_{v \notin S} \frac{1}{2} \max \{0, \log \|x_{pQ}\|_v\} \\ &= \frac{1}{2} h(x_{pQ}) - \frac{1}{2[K : \mathbb{Q}]} \sum_{v \in S} \max \{0, \log \|x_{pQ}\|_v\}. \end{aligned}$$

We have (by the basic properties of heights; see Theorems 5.6 and 9.3(e) of [27])

$$h(x_{pQ}) = h(f(x_Q)) = p^2 h(x_Q) = 2p^2 \hat{h}(Q) + O(1),$$

where the implied constant depends on E and p .

We will now apply a version of Roth's Theorem to the poles of $f(x)$. Specifically, by Theorem D.9.3 of [17] applied to $\frac{1}{f} \in K(x)$, we find that there is a constant $c > 0$ such that

$$\sum_{v \in S} \min \left\{ 0, \log \left\| \frac{1}{f(x)} \right\|_v \right\} \geq -[K : \mathbb{Q}] \#S(2 + \epsilon) h(x) - \log c$$

for all $x \in K$. In particular, we have

$$\frac{-1}{2[K : \mathbb{Q}]} \sum_{v \in S} \max \{0, \log \|f(x_Q)\|_v\} \geq -\#S(2 + \epsilon) \hat{h}(Q) - c',$$

for some constant c' depending only on E , p , and K . Combining these estimates, and noting that $\#S \leq [K : \mathbb{Q}]$, we see that

$$\begin{aligned} \frac{1}{2} h(x_{pQ}) - \frac{1}{2[K : \mathbb{Q}]} \sum_{v \in S} \max \{0, \log \|x_{pQ}\|_v\} \\ \geq (p^2 - [K : \mathbb{Q}](2 + \epsilon)) \hat{h}(Q) - c'', \end{aligned}$$

for some c'' . This proves the proposition, as $\hat{h}(pQ) = p^2 \hat{h}(Q)$.

Ultimately, under the assumption that the n th term of $\mathcal{D}_{E',P}$ has no primitive divisor, we wish to apply Proposition 2 to derive an upper bound on D_{mP} . The proposition provides no such bound, though, if $m = s_{\mathfrak{p}}$ for some exceptional prime \mathfrak{p} . In the proof of Theorem 4 we overcame this by employing the observation that the number of exceptional primes is bounded in terms of $[K : \mathbb{Q}]$. The next proposition shows that, once attention is restricted to a family of quadratic twists, $\max\{s_{\mathfrak{p}} : \mathfrak{p} \text{ is exceptional}\}$ may be similarly constrained.

Proposition 7. *Let E' be an elliptic curve over K , let $P \in E'(K)$, and let \mathfrak{p} be an exceptional prime for $\mathcal{D}_{E',P}$. Then $s_{\mathfrak{p}} \leq M$, for some quantity M depending only on K and $j(E')$.*

Proof. Let \mathfrak{p} be an exceptional prime for $\mathcal{D}_{E',P}$, and let p be the characteristic of R/\mathfrak{p} . Let

$$E'_i(K) = \{Q \in E'(K) : -\text{ord}_{\mathfrak{p}}(x_Q) \geq 2i\},$$

as in Proposition 1, and note that $s_{\mathfrak{p}}$ is simply the order of P in $E'(K)/E'_N(K)$, for N the least integer greater than $e_{\mathfrak{p}}/(p-1)$. Note, as per [27, Ch. IV] and the proof of Proposition 1, that $E'_1(K_{\mathfrak{p}})$ is isomorphic to a formal group, and that if z is the coordinate corresponding to $Q \in E'_1(K)$, then $\text{ord}_{\mathfrak{p}}(z) = \text{ord}_{\mathfrak{p}}(D_Q)$. Furthermore, the multiplication-by- p map in the formal group is given by power series of the form

$$[p]z = pz + O(z^2).$$

Now suppose that $Q \in E'_1(K)$ is not trivial modulo $E'_N(K)$, i.e., that $\text{ord}_{\mathfrak{p}}(D_Q) \leq e_{\mathfrak{p}}/(p-1)$. Then

$$\text{ord}_{\mathfrak{p}}(D_{pQ}) = \text{ord}_{\mathfrak{p}}([p]z) = \text{ord}_{\mathfrak{p}}(z) + \text{ord}_{\mathfrak{p}}(p + O(z)) \geq 2\text{ord}_{\mathfrak{p}}(z),$$

since

$$\text{ord}_{\mathfrak{p}}(z) \leq \frac{e_{\mathfrak{p}}}{p-1} \leq e_{\mathfrak{p}} = \text{ord}_{\mathfrak{p}}(p).$$

By induction, the order of Q in $E'_1(K)/E'_N(K)$ is at most p^n , where n is the least integer greater than $\log_2 N$. This bounds the order of any element of $E'_1(K)/E'_N(K)$ in terms of $e_{\mathfrak{p}}$ and p .

It now suffices to bound $r_{\mathfrak{p}}$, which is the order of P in $E'(K)/E'_1(K)$. If E' has good reduction at \mathfrak{p} , then

$$E'(K)/E'_1(K) \cong \tilde{E}(R/\mathfrak{p}),$$

where \tilde{E} is the reduction of E' modulo \mathfrak{p} . Thus, by Hasse's theorem the order of P in $E'(K)/E'_1(K)$ is at most $(\sqrt{\#(R/\mathfrak{p})} + 1)^2$. If E' has bad reduction at \mathfrak{p} , let $E'_0(K) \subseteq E'(K)$ be the subgroup of points with nonsingular reduction modulo \mathfrak{p} . Hasse's theorem again bounds the size of $E'_0(K)/E'_1(K)$, while the size of $E'(K)/E'_0(K)$ is at most $\max\{4, -\text{ord}_{\mathfrak{p}}(j(E'))\}$, by a theorem of Kodaira and Néron [27, Theorem 6.1].

Thus, for each \mathfrak{p} , we have $s_{\mathfrak{p}} \leq M_{\mathfrak{p}}$ for some quantity $M_{\mathfrak{p}}$ depending only on \mathfrak{p} and $j(E')$ (in fact, we have not yet needed the fact that \mathfrak{p} is exceptional). As noted in Remark 3, \mathfrak{p} can be exceptional only if $p \leq [K : \mathbb{Q}] + 1$. Considering the maximum of the $M_{\mathfrak{p}}$ over the finitely many primes \mathfrak{p} with $p \leq [K : \mathbb{Q}] + 1$, we have our bound M .

Theorem 9. *Let E be a K -quasiminimal elliptic curve, let $\epsilon > 0$, and let $p \geq \sqrt{[K : \mathbb{Q}]}(4 + \epsilon)$ be a rational prime. Then for each K -quasiminimal twist E' of E and each nontorsion point $P \in pE'(K)$, $\max Z(\mathcal{D}_{E',P}) < C$ for some constant C which depends on E and K , but not E' or P .*

Proof. Suppose that D_{mP} has no primitive divisor. By Proposition 7 there is a quantity M , depending only on K and $j(E') = j(E)$, such that $s_{\mathfrak{p}} \leq M$ for

all exceptional primes \mathfrak{p} . As our goal is to provide a bound on m that depends only on E and K , we will assume that $m > M$. By Proposition 2, then, we see that

$$\log |\mathbf{N}_{K/\mathbb{Q}} D_{mP}| \leq \sum_{\substack{k|m \text{ with} \\ m/k \text{ prime}}} \log \mathbf{N}_{K/\mathbb{Q}} D_{kP} + d \log(2d) + d \log(m),$$

where $d = [K : \mathbb{Q}]$. Note that

$$\begin{aligned} \sum_{\substack{k|m \text{ with} \\ m/k \text{ prime}}} \log \mathbf{N}_{K/\mathbb{Q}} D_{kP} &\leq \sum_{\substack{k|m \text{ with} \\ m/k \text{ prime}}} \frac{d}{2} h(x_{kP}) \\ &\leq \sum_{\substack{k|m \text{ with} \\ m/k \text{ prime}}} (d\hat{h}(kP) + O(h(E'))) \\ &\leq d\hat{h}(mP) \sum_{p|m} \frac{1}{p^2} + O(\log(m)h(E')). \end{aligned}$$

As before, we have an isomorphism $E \rightarrow E'$ by $(x, y) \mapsto (x\tau^2, y\tau^3)$ for some $\tau \in \bar{K}$ with $\tau^2 \in K$. Taking d to be fixed, and noting that $h(E') \ll 1 + h(\tau)$, we have (if $m \in Z(\mathcal{D}_{E',P})$),

$$\log |\mathbf{N}_{K/\mathbb{Q}} D_{mP}| \leq d\rho(m)\hat{h}(m^2P) + O(\log(m)(1 + h(\tau))),$$

where $\rho(m) = \sum_{p|m} p^{-2}$.

On the other hand, we have $x_{mQ} = x_{mP}/\tau^2$, and so

$$\frac{1}{[K(Q) : K]} \log \mathbf{N}_{K(Q)/\mathbb{Q}} D_{mQ} \leq \log \mathbf{N}_{K/\mathbb{Q}} D_{mP} + dh(\tau).$$

Finally, if $P \in pE(K)$, we may write $P = pP'$, for some $P' \in E(K)$, and set $Q' = \phi^{-1}(P')$. It follows from Proposition 6 (applied with $Q = Q'$ and $\delta = \epsilon/2$) that

$$\begin{aligned} \left(1 - \frac{d(2 + \epsilon/2)}{p^2}\right) d\hat{h}(mP) &= \left(1 - \frac{d(2 + \epsilon/2)}{p^2}\right) d\hat{h}(mQ) \\ &\leq \frac{1}{[K(Q) : K]} \log \mathbf{N}_{K(Q)/\mathbb{Q}} D_{mQ} + O(1) \\ &\leq \log \mathbf{N}_{K/\mathbb{Q}} D_{mP} + O(h(\tau)) \\ &\leq d\rho(m)\hat{h}(m^2P) + O(\log(m)h(\tau)). \end{aligned} \quad (1.16)$$

By Theorem 6, there is a constant $\delta > 0$ depending only on $j(E)$ and K such that $\hat{h}(P) \geq \delta(1 + h(\tau))$ (on the assumption that P is not a point of finite order). Dividing both sides of (1.16) by $m^2\hat{h}(P)$, then, yields

$$1 - \frac{d(2 + \epsilon/2)}{p^2} \leq \rho(m) + O\left(\frac{\log(m)}{m^2}\right), \tag{1.17}$$

where the implied constant depends only on E , K , and p . But

$$\rho(m) \leq \sum_{p \text{ prime}} p^{-2} \leq \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{13^2} + \sum_{n=17}^{\infty} \frac{1}{n^2} < \frac{1}{2},$$

and so (1.17) bounds m , since our condition on p ensures that

$$\frac{d(2 + \epsilon/2)}{p^2} \leq \frac{1}{2}.$$

This proves the result.

Finally, we should note that restriction in this section to curves in short Weierstrass form is not, strictly speaking, necessary. Any elliptic curve over K may be written in short Weierstrass form with a change of variables. If $\mathcal{D}_{E,P}$ is a given elliptic divisibility sequence, we may choose this transformation such that the values of D_{nP} are unchanged at primes not dividing 6. By enlarging the set S in the statement of Theorem 8, then, we can treat all K -quasiminimal models of elliptic curves in a given family of quadratic twists (as long as the finiteness in the conclusion of the theorem is now interpreted as finiteness up to this sort of change of variables). Similarly, Theorem 9 may be made independent of finitely many primes (for example, those above 2 and 3) by increasing the set S appearing in the proof of Proposition 6 to include these primes. In this case, however, we must require that $p > \sqrt{\#S(4 + \epsilon)}$ (where S contains at least all infinite primes).

1.5 Speculative results over \mathbb{Q}

As we have seen in Theorem 7, there is a uniform bound on the size of the set $Z(\mathcal{D}_{E,P})$ if one is prepared to accept the conjecture of Szpiro. It seems, not surprisingly, rather more difficult to establish a uniform bound on the largest element in the set $Z(\mathcal{D}_{E,P})$. However, if one restricts attention to certain families of elliptic curves, then a bound may be obtained under similar assumptions. For simplicity, we work over \mathbb{Q} .

Conjecture 4. (Hall [15]) For every $\epsilon > 0$ there exists a constant C_ϵ such that whenever x , y , and $M \neq 0$ are integers satisfying

$$y^2 = x^3 + M,$$

then there is a bound of the form $|x| < C_\epsilon M^{2+\epsilon}$.

Theorem 10. *Suppose Hall's Conjecture 4 holds. Then there is a finite set \mathcal{E} such that if M is a sixth-power free integer, $E : y^2 = x^3 + M$, and $P \in E(\mathbb{Q})$ is nontorsion, then $(M, P) \in \mathcal{E}$ or*

$$Z(\mathcal{D}_{E,P}) \subseteq \{1, 2, 3, 4\}.$$

Proof. In light of Theorem 3 of [18] (the analogue of Theorem 8 in this paper), it suffices to produce a uniform bound on $\max Z(\mathcal{D}_{E,P})$ for all E of the above form. Suppose $Q \in E(\mathbb{Q})$ is a point of infinite order, and let

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

as usual. We have $B_Q^2 = A_Q^3 + MD_Q^6$, and thus, for a fixed $\epsilon > 0$, the conjecture of Hall tells us that

$$|A_Q| < C_\epsilon (MD_Q^6)^{2+\epsilon}.$$

It follows that

$$h_x(Q) \leq 6(2 + \epsilon) \log |D_Q| + O(\log |M|),$$

where the implied constant depends on ϵ . So we have, for any $Q \in E(\mathbb{Q})$ of infinite order,

$$\log |D_Q| \geq \frac{1}{3(2 + \epsilon)} \hat{h}(Q) + O(\log |M|). \quad (1.18)$$

Now let $P \in E(\mathbb{Q})$. We have by Propositions 2 and 3 that $n \in Z(\mathcal{D}_{E,P})$ only if

$$\log |D_{nP}| \leq \rho(n)n^2 \hat{h}(P) + O(\log(n) \log |M|), \quad (1.19)$$

with explicit constants. Consider (1.18) with $Q = nP$. Noting that

$$\log |M| \leq O(\hat{h}(P)),$$

we have

$$\frac{1}{3(2 + \epsilon)} n^2 < \rho(n)n^2 + O(\log(n)).$$

If we take $\epsilon \leq 1$, we see that n is bounded by some N so long as $\rho(n) < 0.1$, say. The latter condition is ensured if $(n, 6) = 1$. Appealing to Theorem 6, our bound is

$$\max\{N, \max(Z(\mathcal{D}_{E,P}) \cap 2\mathbb{Z}), \max(Z(\mathcal{D}_{E,P}) \cap 3\mathbb{Z})\}.$$

Remark 5. Note that, much as in Theorem 7, we only really need the weaker assumption that Hall's Conjecture holds for sufficiently large ϵ . If (1.18) holds for any value of ϵ , then (1.19) yields an upper bound on the values $n \in Z(\mathcal{D}_{E,P})$ such that $\rho(n) < \frac{1}{6(2+\epsilon)}$, for example. But it is easy to check that if $\rho(n) \geq \frac{1}{6(2+\epsilon)}$, then n has a prime divisor $p \leq 6(2 + \epsilon)$. Computing a bound as in Theorem 6 for each such p , we obtain a uniform bound on $\max Z(\mathcal{D}_{E,P})$ for $j(E) = 0$.

Extending this idea, one can prove a general result if one accepts two stronger conjectures, both due to Lang. The first was already stated over number fields (Conjecture 2), but we restate it here over \mathbb{Q} for the convenience of the reader, while the other is a generalization of Conjecture 4.

Conjecture 5. (Lang [19]) There is an absolute constant $C > 0$ such that for every minimal E/\mathbb{Q} and every nontorsion $P \in E(\mathbb{Q})$,

$$\hat{h}(P) > Ch(E).$$

Conjecture 6. (Hall-Lang [20]) There exist absolute constants C_1 and C_2 such that if x, y, A, B are integers with $4A^3 + 27B^2 \neq 0$ and

$$y^2 = x^3 + Ax + B,$$

then $|x| < C_1 \max\{|A|, |B|\}^{C_2}$.

Theorem 11. *Suppose that Conjectures 5 and 6 hold. Then there exist absolute constants M_1 and M_2 such that for all E/\mathbb{Q} and $P \in E(\mathbb{Q})$, if $n \in Z(\mathcal{D}_{E,P})$ then either $n < M_1$ or there is a prime $p < M_2$ such that $p|n$.*

The proof of this theorem is nearly identical to the proof of Theorem 10.

Remark 6. If one restricts attention to a given family of quadratic twists, then Conjecture 5 is known to hold. Thus, if one assumes that Conjecture 6 holds, at least for the given family of twists, one may apply Theorems 8 and 6 to obtain a statement analogous to Theorem 10. That is, one deduces that except for a finite number of exceptions, elliptic divisibility sequences $\mathcal{D}_{E,P}$ arising from this family of twists satisfy $Z(\mathcal{D}_{E,P}) \subseteq \{1, 2\}$. Note also that, under the assumption of Conjecture 6 for all elliptic curves, a uniform version of Theorem 6 would provide a uniform bound on $Z(\mathcal{D}_{E,P})$ for curves E/\mathbb{Q} . Such a uniform statement, however, requires a refinement of Roth's Theorem that is far beyond current Diophantine analysis.

References

1. Mohamed Ayad. Points S -entiers des courbes elliptiques. *Manuscripta Math.*, 76(3-4):305–324, 1992.
2. Mohamed Ayad. Périodicité (mod q) des suites elliptiques et points S -entiers sur les courbes elliptiques. *Ann. Inst. Fourier (Grenoble)*, 43(3):585–618, 1993.
3. Ebru Bekyel. The density of elliptic curves having a global minimal Weierstrass equation. *J. Number Theory*, 109(1):41–58, 2004.
4. Yu. Bilu, G. Hanrot, and P. M. Voutier. Existence of primitive divisors of Lucas and Lehmer numbers. *J. Reine Angew. Math.*, 539:75–122, 2001. With an appendix by M. Mignotte.

5. J. Cheon and S. Hahn. Explicit valuations of division polynomials of an elliptic curve. *Manuscripta Math.*, 97(3):319–328, 1998.
6. D. V. Chudnovsky and G. V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Adv. in Appl. Math.*, 7(4):385–434, 1986.
7. V. A. Dem’janenko. An estimate of the remainder term in Tate’s formula. *Mat. Zametki*, 3:271–278, 1968.
8. Manfred Einsiedler, Graham Everest, and Thomas Ward. Primes in elliptic divisibility sequences. *LMS J. Comput. Math.*, 4:1–13 (electronic), 2001.
9. Graham Everest and Helen King. Prime powers in elliptic divisibility sequences. *Math. Comp.*, 74(252):2061–2071 (electronic), 2005.
10. Graham Everest, Gerald McLaren, and Thomas Ward. Primitive divisors of elliptic divisibility sequences. preprint, 2005.
11. Graham Everest, Victor Miller, and Nelson Stephens. Primes generated by elliptic curves. *Proc. Amer. Math. Soc.*, 132(4):955–963 (electronic), 2004.
12. Graham Everest and Igor E. Shparlinski. Prime divisors of sequences associated to elliptic curves. *Glasg. Math. J.*, 47(1):115–122, 2005.
13. Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward. *Recurrence sequences*, volume 104 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2003.
14. Robert Gross and Joseph Silverman. S -integer points on elliptic curves. *Pacific J. Math.*, 167(2):263–288, 1995.
15. Marshall Hall, Jr. The Diophantine equation $x^3 - y^2 = k$. In *Computers in number theory (Proc. Sci. Res. Council Atlas Sympos. No. 2, Oxford, 1969)*, pages 173–198. Academic Press, London, 1971.
16. M. Hindry and J. H. Silverman. The canonical height and integral points on elliptic curves. *Invent. Math.*, 93(2):419–450, 1988.
17. M. Hindry and J. H. Silverman. *Diophantine geometry, and introduction*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.
18. Patrick Ingram. Elliptic divisibility sequences over certain curves. preprint, 2005.
19. Serge Lang. *Elliptic curves: Diophantine analysis*, volume 231 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1978.
20. Serge Lang. Conjectured Diophantine estimates on elliptic curves. In *Arithmetic and geometry, Vol. I*, volume 35 of *Progr. Math.*, pages 155–171. Birkhäuser Boston, Boston, MA, 1983.
21. A. Schinzel. Primitive divisors of the expression $A^n - B^n$ in algebraic number fields. *J. Reine Angew. Math.*, 268/269:27–33, 1974. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, II.
22. Wolfgang M. Schmidt. *Diophantine approximation*, volume 785 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.
23. Rachel Shipsey. *Elliptic divisibility sequences*. PhD thesis, Goldsmith’s College (University of London), 2000.
24. T. N. Shorey and R. Tijdeman. *Exponential Diophantine equations*, volume 87 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1986.
25. Joseph H. Silverman. Lower bound for the canonical height on elliptic curves. *Duke Math. J.*, 48(3):633–648, 1981.

26. Joseph H. Silverman. Weierstrass equations and the minimal discriminant of an elliptic curve. *Mathematika*, 31(2):245–251 (1985), 1984.
27. Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.
28. Joseph H. Silverman. A quantitative version of Siegel’s theorem: integral points on elliptic curves and Catalan curves. *J. Reine Angew. Math.*, 378:60–100, 1987.
29. Joseph H. Silverman. Wieferich’s criterion and the *abc*-conjecture. *J. Number Theory*, 30(2):226–237, 1988.
30. Joseph H. Silverman. The difference between the Weil height and the canonical height on elliptic curves. *Math. Comp.*, 55(192):723–743, 1990.
31. Joseph H. Silverman. Common divisors of elliptic divisibility sequences over function fields. *Manuscripta Math.*, 114(4):431–446, 2004.
32. Joseph H. Silverman. p -adic properties of division polynomials and elliptic divisibility sequences. *Math. Ann.*, 332(2):443–471, 2005. Addendum 473–474.
33. Christine Swart. *Elliptic divisibility sequences*. PhD thesis, Royal Holloway (University of London), 2003.
34. Morgan Ward. The law of repetition of primes in an elliptic divisibility sequence. *Duke Math. J.*, 15:941–946, 1948.
35. Morgan Ward. Memoir on elliptic divisibility sequences. *Amer. J. Math.*, 70:31–74, 1948.
36. Horst Günter Zimmer. On the difference of the Weil height and the Néron-Tate height. *Math. Z.*, 147(1):35–51, 1976.
37. K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math.*, 3:265–284, 1892.