

A quantitative primitive divisor result for points on elliptic curves

par PATRICK INGRAM

RÉSUMÉ. Soient E/K une courbe elliptique définie sur un corps de nombres, et $P \in E(K)$ un point d'ordre infini. Il est naturel de se demander combien de nombres entiers $n \geq 1$ n'apparaissent pas pour l'ordre du point P congruent un idéal premier de K . Dans le cas où $K = \mathbb{Q}$, E est une tors quadratique de $y^2 = x^3 - x$, et $P \in E(\mathbb{Q})$ comme ci-dessus, nous démontrons qu'il existe au plus un tel $n \geq 3$.

ABSTRACT. Let E/K be an elliptic curve defined over a number field, and let $P \in E(K)$ be a point of infinite order. It is natural to ask how many integers $n \geq 1$ fail to occur as the order of P modulo a prime of K . For $K = \mathbb{Q}$, E a quadratic twist of $y^2 = x^3 - x$, and $P \in E(\mathbb{Q})$ as above, we show that there is at most one such $n \geq 3$.

1. Introduction

Let R be an integral domain, let K be its field of fractions, and let G be an algebraic group defined over R , with identity \mathcal{O} . For each $\mathfrak{p} \in \text{Spec}(R)$, let $G_{\mathfrak{p},0} \subseteq G$ be the kernel of reduction modulo \mathfrak{p} , and for $P \in G(K)$, let $r(\mathfrak{p}; P, G)$ be the order of P in $G/G_{\mathfrak{p},0}$ (which may be infinite). It is reasonable to ask, for a fixed $P \in G(K)$ of infinite order, which values fail to occur as $r(\mathfrak{p}; P, G)$, as $\mathfrak{p} \in \text{Spec}(R)$ varies. To this end, set

$$Z(P, G) = \mathbb{Z}^+ \setminus \{r(\mathfrak{p}; P, G) : \mathfrak{p} \in \text{Spec}(R)\}$$

and

$$Z_{\text{gd}}(P, G) = \mathbb{Z}^+ \setminus \{r(\mathfrak{p}; P, G) : G \text{ has good reduction at } \mathfrak{p} \in \text{Spec}(R)\},$$

so that $Z(P, G) \subseteq Z_{\text{gd}}(P, G)$. What can we say about the sets $Z(P, G)$ and $Z_{\text{gd}}(P, G)$?

Manuscrit reçu le septembre 2008.

2000 *Mathematics Subject Classification.* 11G05, 11B39.

This research was supported in part by a PDF from NSERC of Canada.

In the case where $R = \mathbb{Z}$, and G is a (possibly trivial) quadratic twist of the multiplicative group, the question is a classical one. In particular, to each $P \in G(\mathbb{Q})$, we may assign a Lucas sequence

$$L_n = \frac{\alpha^n - \beta^n}{\alpha - \beta},$$

where α and β are algebraic integers (in the extension of \mathbb{Q} over which G is isomorphic to \mathbb{G}_m) such that $\alpha + \beta$ and $\alpha\beta$ are non-zero, coprime rational integers. It turns out that $r(p; P, G)$ is precisely the least n such that $p \mid L_n$, and so the set $Z_{\text{gd}}(P, G)$, in classical parlance, is the set of indices of terms without *primitive divisors*, that is, prime divisors that divide no earlier term in the sequence. A celebrated result of Bilu, Hanrot, and Voutier [2] (for a history of partial results, see [1, 5, 16, 22, 26]) sheds a great deal of light on this case.

Theorem 1 (Bilu, Hanrot, Voutier [2]). *Let G/\mathbb{Q} be a (possibly trivial) quadratic twist of the multiplicative group, and let $P \in G(\mathbb{Q})$ be a point of infinite order. Then $\max(Z_{\text{gd}}(P, G)) \leq 30$.*

One may ask if a similar result is true when the multiplicative group is replaced with, say, an elliptic curve.

Conjecture 2. *Let K be a number field, and let E/K be an elliptic curve. Then there is a constant $M = M(E, K)$, such that for every quadratic twist E' of E , and every non-torsion point $P \in E'(K)$, we have $\max(Z_{\text{gd}}(P, E)) \leq M$.*

Silverman [19] demonstrated that the sets $Z_{\text{gd}}(P, E)$ are always finite, but the proof is ineffective, and gives no uniform result. More recently, the author and Silverman [11] have derived uniform quantitative results.

Theorem 3 (Ingram, Silverman [11]). *Let K be a number field, and for each elliptic curve E/K let $\nu(E/K)$ be the number of primes at which E has split multiplicative reduction, and let*

$$\sigma(E/K) = \frac{\log |\text{discriminant}(E/K)|}{\log |\text{conductor}(E/K)|}$$

be the Szpiro ratio of E . Then there exist constants $M_1 = M_1(K, \nu(E/K))$ and $M_2 = M_2(K, \sigma(E/K))$ such that $\#Z(P, E) \leq \min(M_1, M_2)$ for each point $P \in E(K)$ of infinite order.

Note that $\nu(E'/K)$ is bounded as E' varies over quadratic twists of a fixed elliptic curve E/K (and so from Theorem 3 follows a weaker form of Conjecture 2), while $\sigma(E/K)$ is bounded in terms of K alone if the *abc* Conjecture holds. The aim of this paper is simply to provide a more explicit version of Theorem 3 for a particular family of quadratic twists of an elliptic curve over \mathbb{Q} (applied to the set $Z_{\text{gd}}(P, E)$ rather than $Z(P, E)$).

Theorem 4. *Let $N \geq 70$ be a square-free integer, let $E_N : y^2 = x^3 - N^2x$ be the congruent number curve corresponding to N , and let $P \in E_N(\mathbb{Q})$ be a point of infinite order. Then the set $Z_{\text{gd}}(P, E_N)$ contains at most one value greater than 2.*

The condition $N \geq 70$ is spurious, and could be eliminated with only a finite amount of computation.

Before proceeding with the technical details, it is worth mentioning how results of this type are generally proven. If G is an algebraic group defined over R , $P \in G(K)$ is fixed, and $n \geq 1$, let D_n be the maximal ideal of R modulo which nP is congruent to \mathcal{O} (in case R is a PID, we will associate D_n with one of its generators). In the case $R = \mathbb{Z}$ and G a twist of the multiplicative group, $(D_n)_{n \geq 1}$ is a Lucas sequence; if G is an elliptic curve, then $(D_n)_{n \geq 1}$ is an *elliptic divisibility sequence* (see below). In classical language, $r(\mathfrak{p}; P, G)$ is the *rank of apparition* of the prime \mathfrak{p} in the sequence $(D_n)_{n \geq 1}$ (that is, the index of the first term divisible by \mathfrak{p}), and we say that \mathfrak{p} is a *primitive divisor* of the term D_n if $n = r(\mathfrak{p}; P, G)$. In other words, the results above are results about primitive divisors in various types of sequences.

In general, one proves the existence of primitive divisors by showing that the appropriate sequence $(D_n)_{n \geq 1}$ grows slowly in each \mathfrak{p} -adic valuation, but grows rapidly in norm. The ‘old primes’ dividing D_n cannot account for the large norm of D_n , and so there must be ‘new primes’, or primitive divisors. In general, the first step is the same for any algebraic group, and follows from fairly simple facts about formal groups.

The second step, showing that D_n grows quickly in norm, is a question of diophantine approximation, and depends more on the structure of G . For example, if G is a (twist) of the multiplicative group, then one can show that

$$\log |\text{Norm } D_n| = nh(P) + O(1)$$

using Roth’s Theorem [15]. If G is an elliptic curve, then Theorem 3 above may be derived from an estimate of the form

$$\log |\text{Norm } D_n| = n^2 \hat{h}(P) + O(1),$$

which again follows indirectly from Roth’s Theorem. Theorem 1 and Theorem 4, on the other hand, follow from more explicit techniques in diophantine approximation (lower bounds on linear forms in logarithms). To see how wildly this part of the argument can vary with the underlying group, let $G = \text{GL}_2$, and let

$$P = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in \text{GL}_2(\mathbb{Z}),$$

so that $D_n = \text{gcd}(a^n - 1, b^n - 1)$. While the formal group arguments limiting the p -adic growth of D_n proceed much as in the multiplicative and

elliptic cases, the diophantine approximation is complete different: a result of Bugeaud, Corvaja, and Zannier [4] demonstrates that

$$\log D_n = \epsilon n + O(1)$$

for any $\epsilon > 0$ (see [21] for similar results for other algebraic groups, assuming Vojta's Conjecture). It is unknown if the set $Z_{\text{gd}}(P, G)$ should be finite in this case. Indeed, in the example $G = \mathbb{G}_a$ and $P = 1$, the first part of the argument still goes through, but the growth of the sequence D_n is much slower. This case is genuinely different from the multiplicative or elliptic case, as $Z(1, \mathbb{G}_a)$ is the set of positive composite integers, which is certainly not finite.

The paper is organized as follows: Section 2 is concerned with preliminaries; we define elliptic divisibility sequences and elliptic logarithms. Section 3 consists of various technical estimates which are needed in the main argument, while Section 4 contains the proof of Theorem 4. This theorem contains a restriction on N which is due only to computational difficulties. In Section 5, we show that the result holds for $N = 5$, as well, indicating how one would go about verifying the theorem in the handful of cases omitted by the main result. Section 7 is devoted to showing that Conjecture 2 follows from an appropriate formulation of Vojta's Conjecture, while Section 6 is devoted to a related problem of determining when terms in elliptic divisibility sequences admit primitive divisors which remain inert in quadratic extensions, a problem of interest in the decidability of the first-order theories of rings of integer in number fields.

2. Primitive divisors in elliptic divisibility sequences

For a fixed \mathbb{Q} -rational point P on the elliptic curve E/\mathbb{Q} , we define the *elliptic divisibility sequence* $\mathcal{D} = (D_n)_{n \in \mathbb{Z}}$ attached to P by

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

taking $\gcd(A_n, D_n) = 1$ and $D_n > 0$. (Note that D_n is precisely the object defined in the introduction.) By a *primitive divisor* of D_n , we mean a prime divisor $p \mid D_n$ such that $p \nmid D_1 D_2 \cdots D_{n-1}$, and by a *good primitive divisor* we mean one at which E has good reduction. We will write $Z(\mathcal{D})$ and $Z_{\text{gd}}(\mathcal{D})$ for the sets $Z(P, E)$ and $Z_{\text{gd}}(E, P)$ defined above. These are simply the sets of indices of terms in the sequence failing to have primitive divisors, or failing to have primitive divisors of good reduction for E , respectively.

We will also define a sequence $(h_n)_{n \in \mathbb{Z}}$ by $h_n = \psi_n(P)$, where ψ_n is the usual n -division polynomial for E/\mathbb{Q} (see, for example, [18]). Note that $D_1^{n^2} h_n$ is always an integer divisible by D_n . The sequence h_n is an elliptic divisibility sequence in the sense of Ward [25] (with the exception that the

terms are not, typically, integers), and in general

$$\text{ord}_p(D_1^{n^2} h_n) = \text{ord}_p(D_n)$$

unless P has singular reduction modulo p . In certain cases, a bound on the difference in these orders when P has singular reduction modulo p is available, as in the proof of Lemma 9 below. For more details on the relation between the classical ‘elliptic divisibility sequences’ studied by Ward, and the sequences \mathcal{D} , the reader is referred to Shipsey [17].

We are concerned only with elliptic curves of the form

$$E_N : y^2 = x^3 - N^2x,$$

so-called *congruent number curves*, where $N > 0$ is a square-free integer (we will suppress the subscript when it is not needed). The particular family of curves chosen has many atypical properties, including full 2-torsion over \mathbb{Q} as well as complex multiplication by $\mathbb{Z}[i]$. While these properties are not used in a fundamental way in the proof of Theorem 4, and a similar result could in principal be derived for any family of quadratic twists, we are able to obtain such a sharp result only for this family, for practical reasons. In particular, we make use of computations from [9], wherein the complex multiplication on E_N makes certain quantities which are in general only ‘effectively computable’, practically computable. Furthermore we have strong estimates on heights of points, due to Bremner, Silverman, and Tzanakis [3], which may in principle be computed for any family of twists. These estimates state that for any $P \in E_N(\mathbb{Q})$ of infinite order,

$$(1) \quad -\frac{1}{2} \log N - \frac{1}{4} \log 2 \leq \hat{h}(P) - \frac{1}{2}h(P) \leq \frac{1}{4} \log(N^2 + 1) + \frac{1}{12} \log 2,$$

and

$$(2) \quad \hat{h}(P) \geq \frac{1}{16} \log(2N^2),$$

where $h(a/b) = \log \max\{|a|, |b|\}$ is the usual height on \mathbb{Q} , the quantity $h(P)$ is defined to be $h(x(P))$, and $\hat{h}(P)$ is the canonical height

$$\hat{h}(P) = \frac{1}{2} \lim_{n \rightarrow \infty} \frac{h([n]P)}{n^2}.$$

The method of proof hinges on the explicit lower bounds on linear forms in elliptic logarithms from David [7], and so we recall some basic facts here (see also [23]). The group of \mathbb{C} -rational points on the curve $E : y^2 = x^3 - N^2x$ is isomorphic to $\mathbb{C}/(\omega\mathbb{Z}[i])$, where ω is the real period of E . The isomorphism may be given explicitly in one direction by the Weierstrass \wp function of the lattice $\omega\mathbb{Z}[i]$, specifically

$$z \mapsto \left(\wp(z), \frac{1}{2}\wp'(z) \right) \in E(\mathbb{C}).$$

The inverse of this map is given by the elliptic logarithm. If we restrict attention to P on the non-compact connected component of $E(\mathbb{R})$, one may verify that

$$u(P) = \frac{\text{sign}(y_P)}{2} \int_{x(P)}^{\infty} \frac{dt}{\sqrt{t^3 - N^2t}}$$

provides an inverse to the map above which takes (real) values between $-\omega/2$ and $\omega/2$, our chosen branch of the elliptic logarithm. We will modify the results of [8] and [9] to provide a primitive divisor result when $x(P) < 0$, and so we will only need to consider points on this component.

An examination of the Laurent expansion for $\wp(z)$ at zero shows that, as z approaches 0, $\wp(z) = z^{-2} + O(1)$. More precisely, we have the following estimate, which relates $u(P)$ to $x(P)$.

Lemma 5. *Let $P \in E(\mathbb{Q})$, and suppose that $x(P) > 2N$. Then*

$$(3) \quad \log \frac{2}{3} \leq 2 \log |u(P)| + \log x(P) \leq \log 2.$$

Proof. The lemma requires only basic calculus, and is nearly identical to the analogous result in [23]. If $x(P) > 2N$, then we have, for all $t \geq x(P)$,

$$\frac{1}{2}t^3 \leq t^3 - N^2t \leq \frac{3}{2}t^3.$$

Taking square roots and reciprocals, and integrating with respect to t , we have

$$\sqrt{\frac{2}{3}}x(P)^{-1/2} \leq \frac{1}{2} \int_{x(P)}^{\infty} \frac{dt}{\sqrt{t^3 - N^2t}} \leq \sqrt{2}x(P)^{-1/2}.$$

The central term is $|u(P)|$, and the lemma follows by taking logarithms. \square

3. Technical lemmata

The proof of Theorem 4 requires a litany of detailed estimates which, in the end, conspire to preclude the existence of two very large elements of $Z_{\text{gd}}(\mathcal{D})$. Throughout, we fix a sequence \mathcal{D} corresponding to a point P of infinite order on a congruent number curve E . It might be mentioned that several of the results after Lemma 6 use only the conclusion of this lemma, and no information about primitive divisors. They are purely diophantine estimates and could be stated in greater generality (although at the cost of the sharp bound obtained in the end).

We will make frequent use of the computations of the author in [9], which show that $n \notin Z_{\text{gd}}(\mathcal{D})$ for $3 \leq n \leq 10$ (for sequences arising, specifically, from congruent number curves). The results in [9] concern only the set $Z(\mathcal{D})$, but an examination of the proofs show that they apply to $Z_{\text{gd}}(\mathcal{D})$. Thus if $n \in Z_{\text{gd}}(\mathcal{D})$ is greater than 2, we shall assume without loss of generality that $n \geq 11$. Computations similar to those in [9] are, in principal, possible for any family of quadratic twists of elliptic curves (see [11]). In

particular, the methods here may be applied to any such family, although the computations may turn out to be impractical.

The first lemma is a variation of the estimates in the proof of Lemma 9 of [19] or Lemma 3.3 of [8] (note that D_n^2 is called B_n in [8], which also uses a different normalization of the canonical height, while D_n is called d_n in [19]). To facilitate the stating of the result, let

$$\begin{aligned}\rho(n) &= \sum_{p|n} p^{-2}, \\ \omega(n) &= \#\{p : p \mid n\},\end{aligned}$$

where p ranges over primes, and

$$n^* = \begin{cases} n & \text{if } n \text{ or } n/2 \text{ is prime} \\ 1 & \text{otherwise.} \end{cases}$$

Lemma 6. *Suppose that $n \in Z_{\text{gd}}(\mathcal{D})$ and that $n \geq 3$. Then*

$$\log D_n \leq n^2 \rho(n) \hat{h}(P) + \omega(n) \left(\frac{1}{2} \log N + \frac{1}{4} \log 2 \right) + \log n^* + \log n.$$

of Lemma 6. Let

$$r(q) = \min\{n : q \mid D_n\}$$

be the rank of apparition of the prime q in the sequence \mathcal{D} . We will make frequent use of the fact that for all n and m ,

$$\gcd(D_n, D_m) = D_{\gcd(n,m)},$$

and that if $q \mid D_n$, then

$$(4) \quad \text{ord}_q(D_{mn}) = \text{ord}_q(D_n) + \text{ord}_q(m)$$

(note that special attention must be paid to the case $q = 2$, but the result is the same for the curves under consideration). Our aim is to show that if $n \in Z_{\text{gd}}(\mathcal{D})$ is greater than 2, then

$$(5) \quad D_n \mid n^* \left(\prod_{p|n} p D_{n/p} \right),$$

from which the estimate in the lemma will follow by taking logarithms.

So suppose that $n \geq 3$ is an element of $Z_{\text{gd}}(\mathcal{D})$, and suppose that $q \mid D_n$. It is possible that $r(q) < n$, in which case $q \mid D_{\gcd(n,r(q))}$, and hence $q \mid D_{n/p}$ for some $p \mid n$. It follows from (4) that

$$\text{ord}_q(D_n) \leq \text{ord}_q(D_{n/p}) + 1$$

(where equality holds just in case $q = p$). If $r(q) = n$ then, as D_n has no primitive divisors of good reduction, we have $q \mid \Delta(E)$. Note that $r(2) \leq 2$

(by an easy modification of the proof of Lemma 5 of [10]), and so we may take q to be odd. Consider the exact sequence

$$0 \longrightarrow E_1(\mathbb{Q}_q) \longrightarrow E_0(\mathbb{Q}_q) \longrightarrow E_{\text{ns}}(\mathbb{F}_q) \cong \mathbb{G}_a(\mathbb{F}_q)$$

where (just as in [18]) $E_{\text{ns}}(\mathbb{F}_q)$ is the group of non-singular points in $E(\mathbb{F}_q)$, and $E_0(\mathbb{Q}_q)$ is the group of points with non-singular reduction modulo q . If $P \in E_0(\mathbb{Q}_q)$, then $r(q)$ is the order of the image of P in $E_{\text{ns}}(\mathbb{F}_q)$, which is either 1 or q . If $P \notin E_0(\mathbb{Q}_q)$ then, as $E(\mathbb{Q}_q)/E_0(\mathbb{Q}_q) \cong \mathbb{Z}/2\mathbb{Z}$ (see, for example, [18] Table 15.1), we have $2P \in E_0(\mathbb{Q}_q)$, and so $r(q)$ is 2 or $2q$.

Thus $r(q) = n \geq 3$ is only possible if $n = q$ or $n = 2q$. We wish to bound the degree to which q occurs in $D_{r(q)}$. Note that, if

$$E_n(\mathbb{Q}_q) = \{Q \in E(\mathbb{Q}_q) : \text{ord}_q(x(Q)) \leq -2n\} \cup \{\mathcal{O}\},$$

then $E_n(\mathbb{Q}_q)/E_{n+m}(\mathbb{Q}_q) \cong \mathbb{G}_a(\mathbb{F}_{q^m})$ for all $n, m \geq 1$. As $E_0(\mathbb{Q}_q)/E_1(\mathbb{Q}_q) \cong \mathbb{G}_a(\mathbb{F}_q)$, we have immediately that $\text{ord}_q(D_{r(q)}) \leq 2$, as $r(q)P \in E_3(\mathbb{Q}_q)$ would imply $\frac{r(q)}{q}P \in E_2(\mathbb{Q}_q)$, contradicting the definition of $r(q)$. To show that $\text{ord}_q(D_{r(q)}) = 1$, we need something slightly stronger (in particular, that $E_0(\mathbb{Q}_q)/E_2(\mathbb{Q}_q) \cong \mathbb{Z}/q^2\mathbb{Z}$).

If $P \in E_0(\mathbb{Q}_q)$, and hence $n = q$, then an examination of the q -division polynomial of E , as in [9], shows that

$$D_q \mid \psi_q(A_1, ND_1^2) \equiv qA_k^{(q^2-1)/2} \pmod{q^2}.$$

Note that $q \nmid A_1$, as $A_1 \equiv 0 \pmod{q}$ would imply that P is the singular point on E modulo q . In particular, we have

$$\text{ord}_q(D_n) = 1 = \text{ord}_q(n^*)$$

(note that we are in the case where $n = n^* = q$). The same holds true when $r(q) = 2q$.

Taking a product over all primes, we obtain (5). Weakening (5) to an inequality, and taking logarithms, we have

$$\begin{aligned} \log D_n &\leq \log n^* + \sum_{p|n} \log p + \sum_{p|n} \log D_{n/p} \\ &\leq \log n^* + \log n + \sum_{p|n} \frac{1}{2} h\left(\frac{n}{p}P\right) \\ &\leq \log n^* + \log n + \sum_{p|n} \hat{h}\left(\frac{n}{p}P\right) + \sum_{p|n} \left(\frac{1}{2} \log N + \frac{1}{4} \log 2\right) \\ &\leq \log n^* + \log n + n^2 \rho(n) \hat{h}(P) + \omega(n) \left(\frac{1}{2} \log N + \frac{1}{4} \log 2\right). \end{aligned}$$

□

Note that, as

$$\log D_n = n^2 \hat{h}(P)(1 + o(1))$$

as $n \rightarrow \infty$, for a given sequence, the conditions above immediately imply that $Z(\mathcal{D})$ is finite. The constants involved in this estimation, however, are ineffective, and we are seeking an effective statement.

We wish to apply parts of Theorem 1 of [9] to simplify the problem at hand, but this result speaks to the question of the existence of primitive divisors, not good primitive divisors *per se*. We need to strengthen this result slightly.

Lemma 7. *If $p = 2$ or 5 then*

$$Z_{\text{gd}}(\mathcal{D}) \cap p\mathbb{Z} \subseteq \{2\}.$$

If $x(P) < 0$, then $Z_{\text{gd}}(\mathcal{D}) \subseteq \{1, 2\}$.

Proof. Suppose that $n \in Z_{\text{gd}}(\mathcal{D}) \cap 2\mathbb{Z}$ is greater than 2, and note that

$$\rho(n) \leq \sum_p p^{-2} \leq 0.453 \quad \text{and} \quad \omega(n) \leq \frac{\log n}{\log 2}.$$

Then we have (by the previous lemma, as n is composite)

$$\log D_n \leq 0.453n^2 \hat{h}(P) + \frac{\log n}{\log 2} \left(\frac{1}{2} \log N + \frac{1}{4} \log 2 + 1 \right).$$

On the other hand, by inequalities (13) and (14) of [8], we have

$$\log D_n \geq \frac{3}{4}n^2 \hat{h}(P) - \frac{3}{4} \log(N^2 + 1) - \frac{5}{2} \log N - \frac{3}{4} \log 2.$$

Using (2), we may conclude that $n \leq 12$ and, applying Lemma 6 of [9], we see that this is impossible.

Now suppose that $n \in Z_{\text{gd}}(\mathcal{D}) \cap 5\mathbb{Z}$. By Lemma 6 of [9], we know that $n \neq 5, 15, 25$, and in particular n is composite. We have just shown that n is odd, and so $n \geq 35$. Also,

$$(6) \quad \rho(n) \leq \sum_{p \neq 2} p^{-2} \leq 0.203 \quad \text{and} \quad \omega(n) \leq \frac{\log n}{\log 3}.$$

Lemma 6 now provides

$$\log D_n \leq \rho(n)n^2 \hat{h}(P) + \omega(n) \left(\frac{1}{2} \log N + \frac{1}{4} \log 2 \right) + \log n.$$

On the other hand, the proof of Lemma 7 of [9] shows that (noting the different definitions of the canonical height)

$$\log D_n \geq \frac{9}{25}n^2 \hat{h}(P) - \frac{43}{2} \log N - 7.33.$$

Comparing these two estimates, (2), and (6) shows that $n \leq 35$, while using exact values of $\rho(n)$ and $\omega(n)$ shows that $n \neq 35$. All possible values of n have been exhausted.

Finally, suppose that $x(P) < 0$ and $n \in Z_{\text{gd}}(\mathcal{D})$ so that, by the above, n is odd. Then we have $x(nP) < 0$, and hence $|x(nP)| \leq N$. It follows that

$$\begin{aligned} n^2 \hat{h}(P) &\leq \frac{1}{2} h(x(nP)) + \frac{1}{4} \log(N^2 + 1) + \frac{1}{12} \log 2 \\ &= \frac{1}{2} \log \max\{|A_n|, D_n^2\} + \frac{1}{4} \log(N^2 + 1) + \frac{1}{12} \log 2 \\ &\leq \log D_n + \frac{1}{2} \log N + \frac{1}{4} \log(N^2 + 1) + \frac{1}{12} \log 2. \end{aligned}$$

Comparing this with the bound in Lemma 6 and (2), we obtain $n \leq 5$. By the proof thus far, this implies $n \leq 2$. \square

In general, we can use the methods above to obtain a bound on the largest element of $Z_{\text{gd}}(\mathcal{D}) \cap p\mathbb{Z}$ for any $p \equiv 1 \pmod{4}$, but the main benefit of the above lemma is that it will allow use to suppose, for $n \in Z_{\text{gd}}(\mathcal{D})$ greater than 2, that

$$\omega(n) \leq \frac{\log n}{\log 3} \quad \text{and} \quad \rho(n) \leq \sum_{p \nmid 10} p^{-2} < 0.163.$$

This, in turn, allows us to conclude (by Lemma 6) that

$$(7) \quad \log D_n \leq 0.163 n^2 \hat{h}(P) + \log n \left(\frac{\log N}{2 \log 3} + \frac{\log 2}{4 \log 3} + 1 \right)$$

if n is composite, and

$$(8) \quad \log D_p \leq \hat{h}(P) + \frac{1}{2} \log N + \frac{\log 2}{4} + 2 \log p$$

if $n = p$ is prime. Note that (8) is stronger than (7) for $N \geq 5$ and $p \geq 7$. As $3, 5, 7 \notin Z_{\text{gd}}(\mathcal{D})$, we may use (7) when n is prime, as well.

We have now a bound on D_n when $n \in Z_{\text{gd}}(\mathcal{D})$. The following lemma gives a bound on the elliptic logarithm of nP if $n \in Z_{\text{gd}}(\mathcal{D})$, which is again much stronger if n is prime.

Lemma 8. *Suppose that $n \geq 3$ and $n \in Z_{\text{gd}}(\mathcal{D})$ is composite. Then we have*

$$\begin{aligned} \log |u(nP)| &< -0.837 n^2 \hat{h}(P) + \log n \left(\frac{1}{2 \log 3} \log N + \frac{\log 2}{4 \log 3} + 1 \right) \\ &\quad + \frac{1}{4} \log(N^2 + 1) + \frac{7}{12} \log 2. \end{aligned}$$

If $p \in Z_{\text{gd}}(\mathcal{D})$ is an odd prime, then

$$\log |u(pP)| < -(p^2 - 1) \hat{h}(P) + 2 \log p + \log N + 0.59.$$

Proof. Suppose that $n \in Z_{\text{gd}}(\mathcal{D})$, $n \geq 3$, and so the bound on $\log D_n$ from Lemma 6 holds. Note that we have supposed that $x(nP) > 0$, and so $x(nP) > N \geq 1$. In particular, $h(nP) = \log |A_n|$, in the notation of Section 2. If we have $|x(nP)| \leq 2N$, then

$$\begin{aligned}
n^2 \hat{h}(P) &= \hat{h}(nP) \\
&\leq \frac{1}{2} h(nP) + \frac{1}{4} \log(N^2 + 1) + \frac{1}{12} \log 2 \\
&\leq \frac{1}{2} \log |A_n| + \frac{1}{4} \log(N^2 + 1) + \frac{1}{12} \log 2 \\
&\leq \log |D_n| + \frac{1}{2} \log(2N) + \frac{1}{4} \log(N^2 + 1) + \frac{1}{12} \log 2 \\
&\leq 0.163 n^2 \hat{h}(P) + \log n \left(\frac{\log N}{2 \log 3} + \frac{\log 2}{4 \log 3} + 1 \right) \\
&\quad + \frac{1}{2} \log(2N) + \frac{1}{4} \log(N^2 + 1) + \frac{1}{12} \log 2, \\
n^2 &\leq \frac{1}{0.837 \hat{h}(P)} \left(\log n \left(\frac{\log N}{2 \log 3} + \frac{\log 2}{4 \log 3} + 1 \right) \right. \\
&\quad \left. + \frac{1}{2} \log(2N) + \frac{1}{4} \log(N^2 + 1) + \frac{1}{12} \log 2 \right),
\end{aligned}$$

which, using (2) implies $n \leq 4$.

If this is not the case, then we have $|x(nP)| > 2N$ and so by Lemma 5 and the proof of Lemma 6,

$$\begin{aligned}
\log |u(nP)| &\leq \frac{1}{2} \log 2 - \frac{1}{2} \log |x(nP)| \\
&= \frac{1}{2} \log 2 + \log |D_n| - \frac{1}{2} \log |A_n| \\
&\leq \frac{1}{2} \log 2 + n^2 \rho(n) \hat{h}(P) + \omega(n) \left(\frac{\log N}{2} + \frac{\log 2}{4} \right) + \log n \\
&\quad - \frac{1}{2} h(nP) \\
&\leq n^2 (\rho(n) - 1) \hat{h}(P) + \omega(n) \left(\frac{\log N}{2} + \frac{\log 2}{4} \right) + \log n \\
&\quad + \frac{1}{4} \log(N^2 + 1) + \frac{7}{12} \log 2.
\end{aligned}$$

Again, we have our two bounds by noting that $\rho(n) \leq 0.163$ and $\omega(n) \leq \log n / \log 3$, in general, while $\rho(p) = p^{-2}$ and $\omega(p) = 1$ for a prime p . Note that in this second case we have also used the fact that

$$\log(N^2 + 1) \leq \log \frac{26}{25} + 2 \log N$$

for $N \geq 5$. □

At this point we have shown that if D_n has no primitive divisor (of good reduction for E), then $x(nP)$ must be particularly large (and $u(nP)$ particularly small). Eventually we will use lower bounds on linear forms in logarithms to bound n in terms of N , but first we require an upper bound on $x(nP)$ as well.

Lemma 9. *If $n \geq 3$ and $n \in Z_{\text{gd}}(\mathcal{D})$, then*

$$\log |x(P)| < \max \left\{ 2 \log n + \log N, \frac{1}{3} \hat{h}(P) + 2 \log N + 1 + \log 2 \right\}.$$

Proof. Recall the sequence $h_n = \psi_n(P)$ from Section 2. It follows from the proof of [10, Claim 19] that

$$D_1^{n^2} |h_n| \leq (2N)^{(n^2-1)/2} |D_n|,$$

and by definition that

$$(9) \quad |h_n|^2 = n^2 \prod_{Q \in E[n] \setminus \{\mathcal{O}\}} |x(P) - x(Q)|.$$

It is also the case that $|x(Q)| < \frac{1}{2} n^2 N$ for all $Q \in E[n]$ (see [10, Claim 18]). Suppose

$$\log |x(P) - x(Q)| \geq \frac{1}{3} \hat{h}(P) + 2 \log N + 1$$

for all Q . Then as the product in (9) has $n^2 - 1$ factors, and as $D_1 \leq 1$,

$$\log n + \frac{n^2 - 1}{2} \left(\frac{1}{3} \hat{h}(P) + 2 \log N + 1 \right) \leq \frac{n^2 - 1}{2} \log(2N) + \log |D_n|$$

and so

$$\begin{aligned} \log n + \frac{n^2 - 1}{2} \left(\frac{1}{3} \hat{h}(P) + \log N + 1 - \log 2 \right) \\ \leq 0.163 n^2 \hat{h}(P) + \log n \left(\frac{1}{2 \log 3} \log N + \frac{\log 2}{4 \log 3} + 1 \right), \end{aligned}$$

which implies

$$a \hat{h}(P) + b \log N + c < 0,$$

where

$$\begin{aligned} a &= \frac{n^2 - 1}{6} - 0.163 n^2 \\ b &= \frac{n^2 - 1}{2} - \frac{\log n}{2 \log 3} \end{aligned}$$

and

$$c = \frac{(1 - \log 2)(n^2 - 1)}{2} - \frac{\log n \log 2}{4 \log 3}.$$

This is a contradiction for $n \geq 7$, as all three summands are positive.

It follows that $\log |x(P) - x(Q)| < \frac{1}{3}\hat{h}(P) + 2 \log N + 1$ for some $Q \in E[n]$, and so

$$\begin{aligned} \log |x(P)| &\leq \log(|x(Q)| + |x(P) - x(Q)|) \\ &\leq \log \left(\frac{1}{2}n^2N + \exp \left(\frac{1}{3}\hat{h}(P) + 2 \log N + 1 \right) \right) \\ &\leq \log \left(2 \max \left\{ \frac{1}{2}n^2N, \exp \left(\frac{1}{3}\hat{h}(P) + 2 \log N + 1 \right) \right\} \right) \\ &\leq \max \left\{ 2 \log n + \log N, \frac{1}{3}\hat{h}(P) + 2 \log N + 1 + \log 2 \right\}. \end{aligned}$$

□

Finally, we need an understanding of the quantity $u(nP) - nu(P)$. As the function $u : E(\mathbb{C}) \rightarrow \mathbb{C}$ defined above yields the principal value of the elliptic logarithm, $u(nP) \equiv nu(P)$ modulo the lattice $\omega\mathbb{Z}[i]$. The proof in the next section, however, requires that we not have $u(nP) = nu(P)$ for $n \geq 3$.

Lemma 10. *Suppose that $n \in Z_{\text{gd}}(\mathcal{D})$, that $u(nP) = nu(P) + m\omega$, and that $n \geq 3$. Then $\text{gcd}(m, n) = 1$ (in particular, $m \neq 0$).*

Proof. Recasting notation somewhat, write $d = \text{gcd}(n, m)$, $n = ds$, and $m = dt$. Note that since $nu(P) + m\omega$ is in the fundamental parallelogram of $\omega\mathbb{Z}[i]$, it certainly follows that $su(P) + t\omega$ is. So we have

$$u(dsP) = nu(P) + m\omega = du(sP).$$

Given that $ds \in Z_{\text{gd}}(\mathcal{D})$, our aim is to show that $d = 1$, or $n = ds \leq 2$. As in the proof of Lemma 8, we may assume that $x(dsP) > 2N$, or else we have $n \leq 2$, and as usual we may suppose that $n \geq 11$.

Suppose first that $x(sP) \leq 2N$. In this case, we have

$$|u(sP)| = \frac{1}{2} \int_{x(sP)}^{\infty} \frac{dt}{\sqrt{t^3 - N^2t}} \geq \frac{1}{2} \int_{2N}^{\infty} \frac{dt}{\sqrt{t^3 - N^2t}} \geq \frac{7}{10\sqrt{N}},$$

by a simple calculation. By hypothesis, $ds = n \in Z_{\text{gd}}(\mathcal{D})$, and so we have

$$\begin{aligned}
-\frac{1}{2} \log N + \log 7 - \log 10 &\leq \log |u(sP)| \\
&\leq \log |u(sP)| + \log d = \log |u(nP)| \\
&\leq -0.837n^2 \hat{h}(P) + \log(n) \left(\frac{\log N}{2 \log 3} + 1.158 \right) \\
&\quad + \frac{1}{4} \log(N^2 + 1) + \frac{7}{12} \log 2.
\end{aligned}$$

Using the lower bound on $\hat{h}(P)$, we may use the above inequality to show that (with $N \geq 5$), we must have $n \leq 5$, a contradiction.

Now suppose that $x(sP) > 2N$. We have, by Lemmas 5 and 8,

$$\begin{aligned}
\log |x(sP)| &\geq -2 \log |u(sP)| + \log 2 - \log 3 \\
&= -2 \log |u(nP)| + 2 \log d + \log 2 - \log 3 \\
&> 1.674n^2 \hat{h}(P) - 2 \log n \left(\frac{\log N}{2 \log 3} + \frac{\log 2}{4 \log 3} + 1 \right) \\
&\quad - \frac{1}{2} \log(N^2 + 1) - \frac{1}{6} \log 2 - \log 3 + 2 \log d.
\end{aligned}$$

On the other hand, we may obtain an upper bound on $|x(sP)|$ in a fashion very similar to that in the proof of Lemma 9. In particular, using the observation that

$$D_s^{d^2} d^2 \prod_{Q \in E[d] \setminus \{\mathcal{O}\}} |x(sP) - x(Q)| \leq (2N)^{(d^2-1)/2} D_{ds}^2,$$

and the estimate on D_{ds} that comes from $ds \in Z_{\text{gd}}(\mathcal{D})$, we have

$$\begin{aligned}
\log |x(sP)| &\leq \max\{2 \log d + \log N, \\
&\quad 0.054n^2 \hat{h}(P) + \log(n) \left(\frac{\log N}{2 \log 2} + 2.16 \right) \\
&\quad \quad - 2 \log d + 2 \log(2) + \log N\}.
\end{aligned}$$

There are two cases. If

$$\log |x(sP)| \leq 2 \log d + \log N,$$

then

$$\begin{aligned}
1.674n^2 \hat{h}(P) &\leq 2 \log n \left(\frac{\log N}{2 \log 3} + \frac{\log 2}{4 \log 3} + 1 \right) + \frac{1}{2} \log(N^2 + 1) \\
&\quad + \log N + 1.22.
\end{aligned}$$

Estimates as above show that $n \leq 5$, contradicting the assumption that $n \in Z_{\text{gd}}(\mathcal{D})$ and $n \geq 2$.

If, on the other hand,

$$\begin{aligned} \log |x(sP)| &\leq 0.054n^2\hat{h}(P) + \log(n) \left(\frac{\log N}{2\log 2} + 2.16 \right) \\ &\quad - 2\log d + 2\log(2) + \log N, \end{aligned}$$

then

$$\begin{aligned} 1.62n^2\hat{h}(P) &\leq \log(n) (1.632\log N + 4.476) + \frac{1}{2}\log(N^2 + 1) - \log N \\ &\quad + 2\log d + 2.601. \end{aligned}$$

As $d \geq 2$, the above again yields $n \leq 6$, whence $n \notin Z_{\text{gd}}(\mathcal{D})$ (unless $n \leq 2$). \square

4. The proof of the main result

We may now proceed with the proof of the main result, which is similar to the proof of the main result in [10]. The proof will proceed as follows: We will prove that if $n_1, n_2 \in Z_{\text{gd}}(\mathcal{D})$ are ‘large’, and $n_i u(P) + m_i \omega = u(n_i P)$ for each i , then $n_1 m_2 = n_2 m_1$. Lemma 10 then ensures that then $n_1 = n_2$, as $\text{gcd}(n_i, m_i) = 1$ for each i . To show that we must have $n_1 m_2 = n_2 m_1$, suppose that $n_1, n_2 \in Z_{\text{gd}}(\mathcal{D})$ are both greater than 2, and $n_1 m_2 \neq n_2 m_1$, so that we have

$$\begin{aligned} N^{-1/2}\omega_1 &\leq \omega |n_1 m_2 - n_2 m_1| \\ &\leq n_2 |n_1 u(P) + m_1 \omega| + n_1 |n_2 u(P) + m_2 \omega| \\ &= n_2 |u(n_1 P)| + n_1 |u(n_2 P)| \\ &\leq 2n_1 |u(n_2 P)|, \end{aligned}$$

(without loss of generality). Taking logarithms, we obtain

$$(10) \quad -\log |u(n_2 P)| \leq \frac{1}{2}\log N + \log n_1 + \log 2 - \log \omega_1.$$

We will show that $\log n_1 = O(\log \hat{h}(P))$ which, in light of Lemma 8, will bound n_2 absolutely.

In producing the bound above, and those below, we frequently need estimates on the solutions to inequalities of the form

$$n^2 < a \log n + b,$$

where a and b are rather daunting functions of N and/or $\hat{h}(P)$. It is not actually that difficult to see how these inequalities are treated. The function $n^2 - a \log n - b$ is (for $a \geq 0$) increasing to the right of $\sqrt{a/2}$. In particular,

if one finds a value M (depending on N and $\hat{h}(P)$) satisfying

$$(11) \quad M^2 - a \log M - b \geq 0$$

$$(12) \quad 2M^2 - a \geq 0,$$

then $n^2 \geq a \log n + b$ for all with $n \geq M$. More generally, if $g(x)$ is any polynomial whose coefficients are functions in N and $\hat{h}(P)$, and M satisfies

$$(13) \quad 2^k M^2 - g^{(k)}(\log M) \geq 0$$

for all k (where $g^{(k)}$ is the k th derivative of g in x), then $n^2 < g(\log n)$ implies $n \leq M$. Thus, we can select some $M = M(\log N, \hat{h}(P))$, and verify that (13) holds for each k (a matter of single-variable calculus, once $\hat{h}(P)$ is replaced by its lower bound (2)), in order to be sure that $n^2 \geq g(\log n)$ for all $n \geq M$.

Returning to the proof, we apply estimates due to David [7] on lower bounds on linear forms in elliptic logarithms to obtain a bound on n_1 (which depends on N and $\hat{h}(P)$). We will assume that $N \geq 70$ in these estimates, to reduce the number of cases. This assumption ensures that

$$h(E) = \max \log\{1728, 4N^2\} = \log(4N^2) > 3\pi,$$

simplifying the values called for in David's estimates. For each $N \leq 69$, one may carry out the same procedure with the exact value of N and a sharp lower bound on $\hat{h}(P)$, and one will obtain the same results. A sample computation, for $N = 5$, is given in Section 5 below.

If we set

$$\begin{aligned} \log(V_2) &= \log(4N^2) \\ \log(V_1) &= \max\{2\hat{h}(P), \log(4N^2)\} \\ \log(B) &= \max\{e \log(4N^2), \log |n_1|, 2\hat{h}(P)\}, \end{aligned}$$

then the results of David (note that our canonical height is twice that in [7]) ensure that

$$(14) \quad -\log |u(n_1 P)| < 4 \times 10^{41} (\log(B) + 1) (\log \log(B) + \log(4N^2) + 1)^3 \log(V_1) \log(V_2).$$

There are several cases to consider. Note that, throughout, we make frequent use of (2) to provide an upper bound on $1/\hat{h}(P)$ in terms of N .

If $\log(4N^2) > 2\hat{h}(P)$, and $e \log(4N^2) > \log |n_1|$, then we may take

$$\log(V_1) = \log(4N^2) \text{ and } \log(B) = e \log(4N^2).$$

The right-hand side of (14) is in this case a function of N , and a simple over-estimate shows that

$$-\log |u(n_1 P)| < 4 \times 10^{42} \log(N)^6.$$

By Lemma 8, we have the estimate

$$-\log |u(n_1 P)| > 0.837 n_1^2 \hat{h}(P) \\ - \log n_1 \left(\frac{1}{2 \log 3} \log N + \frac{\log 2}{4 \log 3} + 1 \right) - \frac{1}{4} \log(N^2 + 1) - \frac{7}{12} \log 2,$$

which combines with the above to yield an inequality of the form

$$n_1^2 < a \log n_1 + b,$$

where

$$a = \frac{1}{0.837 \hat{h}(P)} \left(\frac{1}{2 \log 3} \log N + \frac{\log 2}{4 \log 3} + 1 \right) \leq 9.24$$

and

$$b = \frac{1}{4} \log(N^2 + 1) + \frac{7}{12} \log 2 + 4 \times 10^{45} \log(N)^6.$$

If we set $M = 2 \times 10^{23} \log(N)^{5/2}$ then it is easy to check that (12) and (11) will be satisfied for all $N \geq 70$, and so we have $n_1 \leq M$. This bound may now be used to bound n_2 , by an appeal to (10). Specifically, inserting the bound $n_1 \leq 2 \times 10^{23} \log(N)^{5/2}$ into (10) yields, with an application of Lemma 8 to estimate $-|u(n_2 P)|$ from below,

$$n_2^2 < a \log n_2 + b,$$

where

$$a = \frac{1}{0.837 \hat{h}(P)} \left(\frac{\log 2}{4 \log 3} + \frac{\log N}{2 \log 3} + 1 \right) \leq 9.24 \\ b = \frac{1}{0.837 \hat{h}(P)} \left(\log N + \frac{5}{2} \log \log N + 54.49 \right) \leq 135.6.$$

(In this estimation we are using the hypothesis that $N \geq 70$). One can now easily verify that $n_2 \leq 12$. This is, unfortunately, just slightly worse an estimate than we might like, as we know that $n_2 \leq 2$ or $n_2 \geq 11$. However, using the second estimate in Lemma 8, we may give a much better upper bound on n_2 when n_2 is prime. We do so below, but first dispatch the other cases in this bound.

Now suppose that $2\hat{h}(P) \geq \log(4N^2)$, and $2\hat{h}(P) > \log |n_1|$. We may select $\log(V_1) = 2\hat{h}(P)$, $\log(B) = e2\hat{h}(P)$. We may also bound $\log(4N^2)$ in (14) by $2\hat{h}(P)$, yielding

$$-\log |u(n_1 P)| < 8.7 \times 10^{43} \hat{h}(P)^6,$$

and hence, by the methods above, $n_1 \leq 1.2 \times 10^{22} \hat{h}(P)^{5/2}$. Inserting this into (14) produces $n_2 \leq 3$ for $N \geq 70$ (using the improvement on (2) that holds in this case).

The two remaining cases correspond to

$$\log |n_1| \geq \max\{2\hat{h}(P), e \log(4N^2)\},$$

in which case we take $\log(B) = \log |n_1|$. Estimating as above, we have $n_1 \leq 6.8 \times 10^{22} \log(N)^2$. This gives $n_2 \leq 11$ for $N \geq 70$.

Our result is now that $n_2 \leq 2$ or $n_2 = 11$. Although it is possible to find all examples of elliptic divisibility sequences \mathcal{D} on congruent number curves such that $11 \in Z_{\text{gd}}(\mathcal{D})$, this involves solving Thue equations of higher degree than seems feasible at the moment (although one may verify, under the assumption of the Generalized Riemann Hypothesis, that there are no such sequences; see [9]). Instead, we note that the second estimate in Lemma 8 is much stronger than the first, and so if $n_2 = p$ is prime, we can obtain a better bound. In particular, we have

$$\log |u(pP)| < -(p^2 - 1)\hat{h}(P) + \log N + 2 \log p + 0.59,$$

and so (10) becomes

$$p^2 \leq \left(\frac{2}{\hat{h}(P)} \right) \log p + \frac{1}{\hat{h}(P)} \left(\frac{3}{2} \log N + \log n_1 + 0.32 \right) + 1.$$

Applying the three bounds on n_1 found above, we see that $p = n_2 \leq 7$ in every case. This completes the proof of the main result.

5. The case $N = 5$

As noted in Section 4, Theorem 4 must be checked for each $N \leq 69$. We are, of course, only interested in N square-free such that $\text{rank}(E/\mathbb{Q}) \geq 1$. For each of these N we may find, using the computational package Pari/GP [13], an explicit lower bound for $\hat{h}(P)$ which improves (2), typically yielding stronger estimates than those in the case $N \geq 70$. As an example, we reproduce the calculations for $N = 5$. Recall that we have two integers n_1 and n_2 such that $n_1, n_2 \in Z(\mathcal{D})$, and such that (10) holds.

For the curve $E : y^2 = x^3 - 25x$, we have $h(E) = \log 1728$. We have as well that $\hat{h}(P) \geq 1.9$ for all $P \in E(\mathbb{Q})$. As $h(E) < 3\pi$, the quantities appearing in the lower bound on $u(n_1P)$ from [7] become

$$\begin{aligned} \log(V_2) &= 3\pi \\ \log(V_1) &= \max \left\{ 2\hat{h}(P), 3\pi \right\} \\ \log(B) &= \max \left\{ \log n_1, 2\hat{h}(P), e \log 1728 \right\}. \end{aligned}$$

We have a number of cases to consider, but in at least one the bound on n_1 is trivial. In particular, if $e \log 1728 \geq \log n_1$, then $n_1 \leq 1728^e < 6.4 \times 10^8$, and no further estimation is required. We assume, then, that $\log n_1 > e \log 1728$.

Suppose that $2\hat{h}(P) \leq 3\pi$, so that $\log(V_1) = \log(V_2) = 3\pi$, while $\log(B) = \log n_1$. Applying Lemma 8 to the bound in (14), we obtain

$$0.837n_1^2\hat{h}(P) \leq 1.9\log n_1 + 1.22 \\ + 4 \times 10^{41}(\log n_1 + 1)(\log \log n_1 + \log 1728 + 1)^3(3\pi)^2,$$

leading one to conclude that $n_1 \leq 2.3 \times 10^{24}$.

On the other hand, suppose that $3\pi \leq 2\hat{h}(P)$. We may note in this case that $e \log 1728$ is at most $4.31\hat{h}(P)$, and so we can combine three cases into two by taking $\log(V_1) = 2\hat{h}(P)$ and

$$\log(B) = \max\{\log n_1, 2.16\hat{h}(P)\}.$$

If $\log n_1 \geq 2.16\hat{h}(P)$, our Lemma 8 and (14) produce

$$0.837n_1^2\hat{h}(P) \leq 1.9\log n_1 + 1.22 \\ + 4 \times 10^{41}(\log n_1 + 1)(\log \log n_1 + \log 1728 + 1)^3 3\pi(2.16\hat{h}(P)).$$

From this it is a simple matter to deduce that $n_1 \leq 1.1 \times 10^{24}$. Finally, if $\log n_1 < 2.16\hat{h}(P)$, we have

$$0.837n_1^2\hat{h}(P) \leq 1.9\log n_1 + 1.22 \\ + 4 \times 10^{41}(2.16\hat{h}(P) + 1)(\log(2.16\hat{h}(P) + \log 1728 + 1))^3 3\pi(2.16\hat{h}(P)),$$

an inequality of the form $n_1^2 < a \log n_1 + b$. Estimating as above, we obtain $n_1 \leq 1.5 \times 10^{23}\hat{h}(P)$.

We now have

$$n_1 \leq 10^{23} \max\{23, 1.5\hat{h}(P)\}.$$

Applying Lemma 8 to (10) as before, we obtain $n_2 \leq 9$ in either case.

6. Splitting of primitive divisors

Once one knows that every term (or almost every) in a given sequence has a primitive prime divisor, certain questions naturally arise. For example, how many primitive divisors does a given term have? How are the primitive divisors distributed among the various congruence classes modulo m , for a given m ? These questions have certain interest outside of number theory. Cornelissen and Zahidi [6] have shown that a certain conjecture on the inertia over quadratic fields of primitive divisors of terms in elliptic divisibility sequences implies that the Σ_3 theory of the ring \mathbb{Q} is undecidable (a result in the direction of a negative answer to Hilbert's Tenth Problem for \mathbb{Q}). In light of a recent result of Poonen [14], which proves the same claim unconditionally, this application seems to have been superseded, but the conjecture itself is still of some interest.

Specifically, Cornelissen and Zahidi conjecture that if E is an elliptic curve, and \mathcal{D} is an elliptic divisibility sequence over E corresponding to a point of sufficiently large height, then there is some set $\{d_1, \dots, d_r\} \subseteq \mathbb{Z}$ such that every term in \mathcal{D} has a primitive divisor that occurs to an odd power and is inert in at least one of the fields $\mathbb{Q}(\sqrt{d_i})$. In fact, the authors only require terms of the form $D_{2^a p^b}$ to have such primitive divisors, where p ranges over odd primes. An argument in favour of the plausibility of this conjecture is given in terms of an heuristic due to Landau and Serre. The type of elliptic divisibility sequence used in their result is a slight variant of the typical sequences considered, but their conjecture is stated for conventional elliptic divisibility sequences as well.

As the authors of [6] point out, the conjecture would be hard to falsify, as any proclaimed counterexample could be remedied by expanding the set of d_i , or requiring the height of the base point to be greater. Below we demonstrate, however, a reason that this conjecture might be difficult to prove for congruent number curves in particular. The results of this section, unlike those in the rest of the paper, utilize the complex multiplication of the curves $y^2 = x^3 - N^2x$, and so are in no way generic. In their paper, Cornelissen and Zahidi observe that, as opposed to the elliptic case, “an inertial *classical* [primitive divisor result] is almost certainly false”, and provide an heuristic argument. To motivate the result for elliptic divisibility sequences, we verify their remark. For any sequence $\mathcal{A} = (A_n)_{n \geq 1}$, let

$$Z(\mathcal{A}; d) = \left\{ n : \text{every primitive divisor of } A_n \text{ splits in } \mathbb{Q}(\sqrt{d}) \right\},$$

a set that surely contains $Z(\mathcal{A})$. Thus, the conjecture above is that for any elliptic divisibility sequence \mathcal{D} , a set $\{d_1, \dots, d_r\} \subseteq \mathbb{Z}$ may be chosen such that $\bigcap_{1 \leq i \leq r} Z(\mathcal{D}; d_i)$ is finite. We may define $Z_{\text{gd}}(\mathcal{D}; d)$ similarly, but considering the most general notion of primitive divisor gives more general results here.

Proposition 11. *Let a and b be two coprime integers, let $d_1, d_2, \dots, d_r \in \mathbb{Z}$, and let $\mathcal{A} = (a^n - b^n)_{n \geq 1}$. Then the set $\bigcap_{1 \leq i \leq r} Z(\mathcal{A}; d_i)$ is infinite.*

Proof. Our proof rests on the easy observation that if p is a primitive divisor of $a^n - b^n$, then $p \equiv 1 \pmod{n}$. Indeed, if p is a primitive divisor of $a^n - b^n$ then n is the order of the image of $\left(\frac{a}{b} - 1\right)$ in $\mathbb{G}_m(\mathbb{F}_p)$, a group of order $p - 1$. Consider any primitive divisor p of the n th term in the sequence, where $4d_1 d_2 \cdots d_r \mid n$. We have $p \equiv 1 \pmod{4}$ and $p \equiv 1 \pmod{d_i}$, for all i , and so

$$\left(\frac{d_i}{p}\right) = \left(\frac{p}{|d_i|}\right) = \left(\frac{1}{|d_i|}\right) = 1$$

for all i . This is precisely the condition under which p splits in all of the fields $\mathbb{Q}(\sqrt{d_i})$. \square

Note that the proof does substantially more than claimed. We are in fact proving that for any m , every m th term in the sequence $(a^n - b^n)_{n \geq 1}$ (a positive proportion) has all of its primitive divisors congruent to 1 modulo m . Choosing m correctly gives

$$m\mathbb{Z}^+ \subseteq \bigcap_{1 \leq i \leq r} Z(\mathcal{A}; d_i).$$

The proof of our result about the splitting of primitive divisors in elliptic divisibility sequences will be similar, but one can already see the difficulty in transferring this argument to the elliptic case: while we know that $\#\mathbb{G}_m(\mathbb{F}_p) = p - 1$, the number of elements in $E(\mathbb{F}_p)$, for a given elliptic curve E , is a subtle quantity. We may gain a certain purchase on the problem, however, by considering curves with complex multiplication, such as the congruent number curves treated above.

Proposition 12. *Let $d_1, d_2, \dots, d_r > 0$ be integers whose prime divisors are all congruent to 3 (mod 4), and let \mathcal{D} be an elliptic divisibility sequence arising from a congruent number curve. Then for some positive integer m ,*

$$m\mathbb{Z}^+ \subseteq \bigcap_{1 \leq i \leq r} Z(\mathcal{D}; d_i).$$

Proof. The argument is the same as above. If p is a primitive divisor of D_n , and a prime of good reduction for E , then n divides $\#E(\mathbb{F}_p)$. It is well known (see, for example, [12]) that if $p \equiv 3 \pmod{4}$ then $\#E(\mathbb{F}_p) = p + 1$, while if $p \equiv 1 \pmod{4}$,

$$\#E(\mathbb{F}_p) = p + 1 - \left(\frac{N^2}{\mathfrak{p}}\right)_4 \mathfrak{p} - \left(\frac{N^2}{\mathfrak{p}}\right)_4 \bar{\mathfrak{p}},$$

where $(\cdot)_4$ denotes the quartic residue symbol, and $\mathfrak{p} \in \mathbb{Z}[i]$ is a prime with $\mathfrak{p} \equiv 1 \pmod{2 + 2i}$ and $p = \mathfrak{p}\bar{\mathfrak{p}}$. Since $\left(\frac{N^2}{\mathfrak{p}}\right)_4 = \mp 1$, this is in fact

$$\#E(\mathbb{F}_p) = p + 1 \pm 2a,$$

where $\mathfrak{p} = a + bi$.

Let $q \mid \#E(\mathbb{F}_p)$ be an odd prime, and suppose for now that $p \equiv 3 \pmod{4}$. Then

$$p \equiv -1 \pmod{q},$$

and hence

$$\left(\frac{q}{p}\right) = (-1)^{(q-1)/2} \left(\frac{p}{q}\right) = (-1)^{(q-1)/2} \left(\frac{-1}{q}\right) = 1.$$

Now suppose that $p \equiv 1 \pmod{4}$, and write $p = a^2 + b^2$ as above, with a odd. Then

$$(a \pm 1)^2 + b^2 \equiv a^2 + b^2 + 1 \pm 2a \equiv \#E(\mathbb{F}_p) \equiv 0 \pmod{q}$$

(for one of the values of \mp). If $q \mid b$, then

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{a \pm 1}{q}\right)^2 = 1.$$

If $q \nmid b$ then suppose $q \mid a \pm 1$. Then

$$0 \equiv \#E(\mathbb{F}_p) = p + 1 \pm 2a \equiv p - 1 \pmod{q},$$

whatever the value of \pm . Thus

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{1}{q}\right) = 1.$$

Finally, we have the case where neither b nor $a \pm 1$ is divisible by q . In this case, let \bar{b} be the multiplicative inverse of $b \pmod{q}$, so that

$$(a - 1)^2(\bar{b})^2 \equiv -1 \pmod{q}.$$

This implies $q \equiv 1 \pmod{4}$.

Thus we have shown that if $q \equiv 3 \pmod{4}$ and $q \mid n$, then all primitive divisors $p \nmid \Delta(E)$ of D_n satisfy $\left(\frac{q}{p}\right) = 1$. The result follows immediately by letting m be the product $d_1 d_2 \cdots d_r$, except for primitive divisors that are primes of bad reduction for E . We may, however, simply increase m so that all of these appear in the sequence before D_m . \square

It is perhaps worth noting that Proposition 12 also shows that *every* term in the elliptic divisibility sequence attached to the point $mP \in E(\mathbb{Q})$ has at least one primitive divisor which splits in all of the quadratic fields $\mathbb{Q}(d_i)$, as the set of primitive divisors of the n th term in this sequence contains all primitive divisors of the nm th term of the sequence corresponding to P .

7. Vojta's Conjecture

We close the paper with the observation that Conjecture 2 is a consequence of an appropriate formulation of Vojta's Conjecture. For simplicity, we will work over \mathbb{Q} . For The definitions involved, we direct the reader to [24].

Conjecture 13 (Vojta [24]). *Let V be a smooth projective variety, let D be a divisor on V with normal crossings, let A be an ample divisor on V , let S be some set of places of K containing all archimedean places, let $r \geq 1$, and let $\epsilon > 0$. Let \mathcal{K}_V be the canonical divisor of V , and let $\lambda_{D,v}$ be local v -adic heights on V with respect to D . Then the set of points $P \in V(\bar{K})$ such that $[K(P) : K] \leq r$ and*

$$\sum_{v \in S} \lambda_{D,v}(P) + h_{\mathcal{K}_V}(P) \geq \epsilon h_A(P) + (\dim V) d_K(P)$$

lies in a proper subvariety of V .

Note that if V is an elliptic curve, $\mathcal{K}_V = 0$, so $h_{\mathcal{K}_V}(P) = O(1)$. In this case, we may also take $\lambda_{D,v}$ to be the usual local heights, and h_A to be the usual canonical height. The proper subvariety alluded to above will necessarily be a finite set.

Theorem 14. *Let E/\mathbb{Q} be an elliptic curve, and suppose that Vojta's Conjecture holds for E . Then Conjecture 2 is true for E .*

If E/\mathbb{Q} is an elliptic curve in minimal Weierstrass form, and $P \in E(\mathbb{Q})$, then let

$$P = \left(\frac{A_P}{D_P^2}, \frac{B_P}{D_P^3} \right),$$

as above (changing notation slightly to make the dependence on P explicit). The sequence of D_{nP} is clearly the same object as mentioned in the introduction. In particular, To ease notation we will, for a set of primes S , let

$$\log |x|_S = \sum_{v \notin S} \max\{v(x^{-1}), 0\}.$$

Note (we shall be more explicit below) that $\log |D_P|_S$ is essentially the sum of the local heights of P away from S , which is precisely the observation that will allow us to exploit Vojta's Conjecture. We will also set

$$h(E) = \max\{\log |\Delta(E)|, h(j(E)), 1\}.$$

The following lemma is a variation of Lemma 6 above.

Lemma 15. *Let S be a finite set of primes including all infinite primes, and all primes at which E has bad reduction. Suppose that $\mathcal{D} = (D_{nP})_{n \geq 1}$ is an elliptic divisibility sequence attached to a point P on a minimal twist E' of E and that D_n has no primitive divisor outside of S other than those dividing $\Delta(E')$. Then if $n \geq 5$,*

$$\log |D_{nP}|_S \leq \frac{1}{2} \hat{h}(nP) + O(h(E') \log n).$$

Proof of Lemma 15. The proof is exactly as the proof Lemma 6, with the principal observation being that primes of bad reduction for E' which do not divide $\Delta(E)$ are necessarily primes of additive reduction. If p is a prime of additive reduction for E' , then $r(p; P, E) \geq 5$ implies $r(p; P, E) = dp$ for some $d \mid 4$. The argument then proceeds as above, after showing that this implies $\text{ord}_p(D_{r(p; P, E)}) \leq 2$. \square

Lemma 16. *Suppose Vojta's conjecture holds (for points on E over quadratic extensions of \mathbb{Q}). Then for every $\epsilon > 0$, there is some finite set of pairs (P, E') so that for all but those,*

$$(15) \quad \log |D_P|_S \geq (1 - \epsilon) \hat{h}(P) + O(h(E')).$$

Proof of Lemma 16. First, we fix some notation. For each place v , we let λ_v denote the canonical v -adic height on E , so that

$$\hat{h}(P) = \sum_v \lambda_v(P)$$

for all $P \in E(K)$. We extend each of these functions to $\overline{\mathbb{Q}}$ in the usual way, that is, by setting

$$\lambda_v(P) = \sum_{\substack{w \in M_L \\ w|v}} \frac{[L_v : K_v]}{[K : L]} \lambda_w(P)$$

for any number field L/\mathbb{Q} and any $P \in E(L)$, and then noting that this definition is independent of the choice of $L \supseteq \mathbb{Q}(P)$. We will extend the function $\log |x|_S$ similarly.

Vojta's Conjecture, in this context, implies that for all but finitely many points $P \in E(\overline{\mathbb{Q}})$ with $[\mathbb{Q}(P) : \mathbb{Q}] \leq 2$, and any fixed set of primes S , we have

$$\sum_{v \in S} \lambda_v(P) \leq \epsilon \hat{h}(P) + d_{\mathbb{Q}}(P),$$

where

$$d_{\mathbb{Q}}(P) = \frac{1}{[\mathbb{Q}(P) : \mathbb{Q}]} \log |\text{disc}(\mathbb{Q}(P)/\mathbb{Q})|.$$

The first remark one should make is that if $j = j(E)$, then (see [20])

$$-\frac{1}{24} \max\{v(j^{-1}), 0\} \leq \lambda_v(P) - v(D_P) \leq \frac{1}{12} v(\Delta(E)).$$

In particular, summing over places in S ,

$$-\frac{1}{24} h(j) \leq \sum_{v \notin S} \lambda_v(P) - \log |D_P|_S \leq \frac{1}{12} \log |\Delta(E)|,$$

a bound which does not depend on the field $\mathbb{Q}(P)$.

Now suppose that E' is a (minimal) quadratic twist of E , and that $P \in E'(\mathbb{Q})$. Then E' and E are isomorphic over $\overline{\mathbb{Q}}$ (indeed, over a quadratic extension of \mathbb{Q}), and P corresponds to a point $Q \in E(\overline{\mathbb{Q}})$ with $[\mathbb{Q}(Q) : \mathbb{Q}] \leq 2$. It is easy to see that

$$|\log |D_Q|_S - \log |D_P|_S| \leq d_{\mathbb{Q}}(Q).$$

So we have

$$\begin{aligned}
\log |D_P|_S &\geq \log |D_Q|_S - d_{\mathbb{Q}}(Q) \\
&\geq \sum_{v \notin S} \lambda_v(Q) - \frac{1}{12} \log |\Delta(E)| - d_{\mathbb{Q}}(Q) \\
&= \hat{h}(Q) - \sum_{v \in S} \lambda_v(Q) - \frac{1}{12} \log |\Delta(E)| - d_{\mathbb{Q}}(Q) \\
&\geq \hat{h}(Q) - \epsilon \hat{h}(Q) - \frac{1}{12} \log |\Delta(E)| - 2d_{\mathbb{Q}}(Q) \\
&\geq (1 - \epsilon) \hat{h}(Q) - \frac{1}{12} \log |\Delta(E)| - 2d_{\mathbb{Q}}(Q) - \frac{\epsilon}{24} h(j(E')).
\end{aligned}$$

Noting that $\hat{h}(P) = \hat{h}(Q)$, that $j(E') = j(E)$, and that $d_{\mathbb{Q}}(Q) = O(h(E'))$, we have the lemma. \square

Proof of Theorem 14. It is now reasonably easy to see that Vojta's Conjecture implies the conjecture above. If D_{nP} has no primitive divisor of good reduction outside of S , then (unless nP is in the finite number of exceptions to (15)), taking $\epsilon = \frac{1}{4}$, we have

$$\frac{3n^2}{4} \hat{h}(P) \leq \frac{n^2}{2} \hat{h}(P) + O(h(E') \log n).$$

It is known for points P on quasi-minimal twists E' of E that

$$h(E') = O(\hat{h}(P)),$$

and so clearing $\hat{h}(P)$ we obtain

$$\frac{3n^2}{4} \leq \frac{n^2}{2} + O(\log n).$$

This clearly bounds n , and this bound may be increased to accommodate the finite number of exceptions allowed by Vojta's Conjecture. \square

References

- [1] A. S. Bang, Taltheoretiske Undersølgelser, *Tidskrift f. Math.* **5** (1886).
- [2] Y. Bilu, G. Hanrot, and P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, *J. Reine Angew. Math.* **539** (2001), (with an appendix by M. Mignotte).
- [3] A. Bremner, J. H. Silverman and N. Tzanakis, Integral points in arithmetic progression on $y^2 = x(x^2 - n^2)$, *J. Number Theory*, **80** (2000).
- [4] Y. Bugeaud, P. Corvaja, and U. Zannier, An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$, *Mathematische Zeitschrift* **243** (2003).
- [5] R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Annals of Math. 2nd series*, **15** (1914), 30–48 and 49–70.
- [6] G. Cornelissen and K. Zahidi, Elliptic divisibility sequences and undecidable problems about rational points. *J. Reine Angew. Math.* **613** (2007).
- [7] S. David, Minorations de formes linéaires de logarithmes elliptiques, *Mém. Soc. Math. France* No. 62 (1995).

- [8] G. Everest, G. McLaren, and T. Ward, Primitive divisors of elliptic divisibility sequences, *J. Number Theory* **118** (2006).
- [9] P. Ingram, Elliptic divisibility sequences over certain curves, *J. Number Theory* **123** (2007).
- [10] P. Ingram, Multiples of integral points on elliptic curves. *J. Number Theory*, to appear (arXiv:0802.2651v1)
- [11] P. Ingram and J. H. Silverman, Uniform bounds for primitive divisors in elliptic divisibility sequences. (preprint)
- [12] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1998.
- [13] PARI/GP, version 2.3.0, Bordeaux, 2005, <http://pari.math.u-bordeaux.fr/>.
- [14] B. Poonen, Characterizing integers among rational numbers with a universal-existential formula, (arXiv:math/0703907)
- [15] K. F. Roth, Rational approximations to algebraic numbers. *Mathematika* **2** (1955).
- [16] A. Schinzel, Primitive divisors of the expression $A^n - B^n$ in algebraic number fields, *J. Reine Angew. Math.* **268/269** (1974).
- [17] R. Shipsey, *Elliptic divisibility sequences*. Ph.D. thesis, Goldsmiths, University of London, 2001.
- [18] J. H. Silverman, *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.
- [19] J. H. Silverman, Wieferich's criterion and the *abc*-conjecture, *J. Number Theory* **30** (1988).
- [20] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.
- [21] J. H. Silverman, Generalized greatest common divisors, divisibility sequences, and Vojta's conjecture for blowups. *Monatshefte für Mathematik* **145** (2005).
- [22] C. L. Stewart, Primitive divisors of Lucas and Lehmer numbers, in *Transcendence theory: advances and applications (Proc. Conf., Univ. Cambridge, Cambridge, 1976)*, Academic Press, London, 1977.
- [23] R. J. Stroeker and N. Tzanakis, Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms, *Acta Arithmetica* **67** (1994).
- [24] P. Vojta, *Diophantine approximations and value distribution theory*, volume 1239 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1987
- [25] M. Ward, Memoir on elliptic divisibility sequences, *Amer. J. Math.* **70** (1948).
- [26] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math.* **3** (1892).

Patrick INGRAM
 Department of Mathematics
 University of Toronto
 Toronto, Canada
Current address: Department of Pure Mathematics
 University of Waterloo
 Waterloo, Canada
E-mail : pingram@math.utoronto.ca
URL: <http://www.math.uwaterloo.ca/~pingram>