PRIMITIVE DIVISORS OF ELLIPTIC DIVISIBILITY SEQUENCES

GRAHAM EVEREST, GERARD MCLAREN AND TOM WARD

September 28, 2004

Abstract. Silverman proved the analogue of Zsigmondy's Theorem for elliptic divisibility sequences. For elliptic curves in global minimal form, it seems likely this result is true in a uniform manner. We present such a result for certain infinite families of curves and points. Our methods allow the first explicit examples of the elliptic Zsigmondy Theorem to be exhibited.

1. Introduction

Let $A = (A_n)_{n\geq 1}$ be an integer sequence. A prime p dividing a term A_n is called a *primitive divisor* of A_n if p does not divide any term A_m, $1 \leq m < n$. Thus, in the list of prime factors of the terms of the sequence, a primitive divisor is a new prime factor. Sequences with the property that all terms (or all terms beyond some point) have a primitive divisor are of great interest.

Definition 1.1. Let $A = (A_n)_{n\geq 1}$ be an integer sequence. Define

$$\mathsf{Z}(A) = \max\{n \mid A_n \text{ does not have a primitive divisor}\}$$

if this set is finite, and $\mathsf{Z}(A) = \infty$ if not. The number $\mathsf{Z}(A)$ will be called the *Zsigmondy bound* for A.

A striking early result is that of Zsigmondy [15]. For the Mersenne sequence $M = (2^n - 1)$, he showed that

$$\mathsf{Z}(M) = 6.$$

More generally, Zsigmondy also showed that for any coprime integers a and b,

$$\mathsf{Z}\left((a^n - b^n)\right) \leq 6.$$

This line of development culminated in a deep result due to Bilu, Hanrot and Voutier [3]: for any non-trivial Lucas or Lehmer sequence L,

$$\mathsf{Z}(L) \leq 30.$$

Much of the arithmetic of linear recurrence sequences extends to elliptic and bilinear recurrence sequences (see [7, Chap. 10] for an overview), and

1991 *Mathematics Subject Classification.* 11G05, 11A41.

Key words and phrases. elliptic curve, primitive divisor, Zsigmondy's Theorem, elliptic divisibility sequence, prime.

Our thanks go to Mike Bennett for help in applying his results.

it is natural to ask if results like that of Zsigmondy might hold for elliptic divisibility sequences.

Let E denote an elliptic curve defined over $\mathbb{Q}$, given in generalized Weierstrass form, and suppose $P = (x(P), y(P))$ denotes a non-torsion rational point on E. See [5], [8], [10] or [13] for background on elliptic curves. For any non-zero $n \in \mathbb{Z}$, write

$$x(nP) = \frac{A_n}{B_n},$$

in lowest terms, with $A_n \in \mathbb{Z}$ and $B_n \in \mathbb{N}$. The sequence $B_{E,P} = (B_n)$ is a divisibility sequence, meaning that

$$m|n \implies B_m|B_n.$$

Such sequences have become known as *elliptic divisibility sequences* (this terminology follows a suggestion of Silverman; the term has also been used for more general sequences related to rational points on elliptic curves). Silverman [11] showed that $B_{E,P}$ satisfies an analogue of Zsigmondy's theorem.

Theorem 1.2. [Silverman] *With E and P as above,*

$$\mathsf{Z}(B_{E,P}) < \infty.$$

Our purpose here is to show that uniform explicit bounds in Theorem 1.2 can be found for certain infinite families of curves, after the manner of [3]. The methods allow explicit versions of the theorem for particular examples. Many of the bounds arrived at below can be improved, similar methods may be extended to other elliptic surfaces, and the techniques used here may be applied to bound the number of times an elliptic divisibility sequence is a prime square; further details in these directions may be found in the thesis of the second named author [9].

2. Main results

The behaviour along the odd and even subsequences of an elliptic divisibility sequence requires slightly different treatment, so the following refinement of Definition 1.1 will be useful.

Definition 2.1. Let $A = (A_n)_{n\geq 1}$ be an integer sequence. Define the *even Zsigmondy bound*

$$\mathsf{Z}_{\mathsf{e}}(A) = \max\{2n \mid A_{2n} \text{ does not have a primitive divisor}\}$$

if this set is finite, and $\mathsf{Z}_{\mathsf{e}}(A) = \infty$ if not. Similarly define the *odd Zsigmondy bound*

$$\mathsf{Z}_{\mathsf{o}}(A) = \max\{2n-1 \mid A_{2n-1} \text{ does not have a primitive divisor}\}$$

if this set is finite, and $\mathsf{Z}_{\mathsf{o}}(A) = \infty$ if not.

Clearly $\mathsf{Z}(A) = \max\{\mathsf{Z}_{\mathsf{e}}(A), \mathsf{Z}_{\mathsf{o}}(A)\}$; in certain cases our methods can bound explicitly either one of Z_{e} and Z_{o} but not both.

Theorem 2.2. *Suppose the curve E is given by a Weierstrass equation*

$$E: \quad y^2 = x^3 - T^2x,$$

with T square-free, and suppose that E has a non-torsion point P in $E(\mathbb{Q})$. Then

$$\mathsf{Z_e}\left(B_{E,P}\right) \le 18.$$

If $x(P) < 0$, then

$$\mathsf{Z_o}\left(B_{E,P}\right) \le 5.$$

If $x(P)$ or $x(P) \pm T$ is a square, then

$$\mathsf{Z_o}\left(B_{E,P}\right) \le 21.$$

Notice that the existence of the point P certainly implies that $T \ge 5$, and this will be used several times in the calculations below.

Example 2.3. Consider the curve

$$E: \quad y^2 = x^3 - 25x,$$

with $P = (-4, 6)$. We will show below that $\mathsf{Z}\left(B_{E,P}\right) = 1$.

The assumption about T being square-free guarantees that E is in global minimal form. Clearly an assumption of this kind is necessary. It is always possible to clear arbitrarily many denominators of the multiples $x(nP)$ by applying suitable isomorphisms, making an explicit bound impossible. Assuming the curve is in minimal form prevents this possibility.

The most general form of result we can exhibit with our current techniques will now be stated. Lang's Conjecture says that if E denotes an elliptic curve defined over $\mathbb{Q}$ defined by a Weierstrass equation in minimal form and if P denotes a non-torsion rational point on E, then

$$\hat{h}(P) \ge c \log \Delta(E). \tag{1}$$

In (1), $\Delta(E)$ denotes the discriminant of E and the constant $c > 0$ is uniform, independent of E and P. The family of curves in Theorem 2.2 is one for which Lang's Conjecture is known to hold.

Theorem 2.4. *Let $\mathfrak{F}$ denote a family of elliptic curves E, given by Weierstrass models in global minimal form, and rational points $P, Q \in E(\mathbb{Q})$, with P a non-torsion point and Q a 2-torsion point. Suppose that Lang's Conjecture holds for the family; in other words, there is a uniform constant $c = c(\mathfrak{F}) > 0$ such that for every triple $(E, P, Q) \in \mathfrak{F}$, the inequality (1) holds. Then $\mathsf{Z_e}(B_{E,P})$ is bounded uniformly for $\mathfrak{F}$, and the bound depends on c only. If either of the following conditions hold:*

(1) *P does not lie in the (real) connected component of the identity;*
(2) *$x(P) - x(Q)$ is a square,*

then $\mathsf{Z_o}(B_{E,P})$ is bounded uniformly.

Infinite families satisfying the conditions of Theorem 2.4 are easy to manufacture.

Example 2.5. Fix $T \in \mathbb{N}$, $T > 1$, and let E denote the elliptic curve

$$E: \quad y^2 = x^3 - T^2(T^2 - 1)x,$$

together with the non-torsion point $P = (1 - T^2, 1 - T^2)$ and the 2-torsion point $Q = (0, 0)$. Using the methods in [4], an explicit form of Lang's Conjecture is provable for the family $\mathfrak{F} = \{(E, P, Q)\}$. This gives an example of case (1) in Theorem 2.4. Taking $P = (T^2, T^2)$ on the same curve yields an example of case (2).

Example 2.6. For all $T > 0$ consider the curve

$$E: \quad y^2 = (x + 1)(x - T)(x - 4T),$$

together with the non-torsion point $P = (0, 2T)$ and the 2-torsion point $Q = (-1, 0)$. Lang's Conjecture holds for this family and, in principle, the constant c can be computed explicitly. For this family both (1) and (2) in Theorem 2.4 hold.

The proofs of the theorems seem to need some form of Siegel's Theorem on the finiteness of the number of integral points on the curve. Indeed, $\mathsf{Z}(B_{E,P})$ being finite requires that B_n grows with n. There are effective versions of Siegel's Theorem, however – as far as we can see – no routine application of these will yield our results. The strongest forms of Siegel's Theorem are proved using elliptic transcendence theory. These methods give good bounds in terms of the shape of error terms and they work in great generality. However, the dependence upon the discriminant does not allow uniformity results – also the size of the constants gives excessively large estimates for the Zsigmondy bound in particular cases. This is discussed further after equation (6) below.

2.1. **Curves without rational 2-torsion.** The strongest results in the paper require the presence of a rational 2-torsion point. The following example illustrates how knowledge about the odd Zsigmondy bound can outstrip that for the even bound when no such point is present.

Example 2.7. Consider the pair (E, P) with

$$E: \quad y^2 + y = x^3 - x \text{ and } P = (0, 0).$$

The methods we describe allow a painless proof that $\mathsf{Z}_{\mathsf{o}}(B_{E,P}) = 5$. Notice that in this case nP is integral for $n = 1, \ldots, 6$ so we could not expect the bound to be any smaller. However, we are unable to prove that the even Zsigmondy bound is 6. Given any example where P does not lie in the real connected component of the identity, the methods in this paper would allow the odd Zsigmondy bound to be computed.

Our final example is a family of curves for which knowledge about the even Zsigmondy bound outstrips that for the odd bound. This is included because it uses a new technique.

Theorem 2.8. *Consider the pair* (E, P) *where*

$$E: \quad y^2 = x^3 + T^3 + 1 \text{ and } P = (-T, 1).$$

Then $\mathsf{Z}_{\mathsf{e}}(B_{E,P})$ *is uniformly bounded for all* $T > 1$.

In the setting of Theorem 2.8, we are unable to prove such a statement for the odd Zsigmondy bound.

The proof of Theorem 2.2 is given in Section 3, using a sharpening of Silverman's original approach, together with results of Bremner, Silverman and Tzanakis concerning the difference between the naïve height and the canonical height of a rational point on an elliptic curve. In Section 4 we will further illustrate the method by explaining Examples 2.3 and 2.7. In Section 5, a proof of Theorem 2.4 will be given. Much of this is routine and we will not labour it; however some explanation is required for case (1) in order to preserve the dependence of the error term upon the discriminant. Theorem 2.8 is proved in Section 6.

3. Proof of Theorem 2.2

We begin with some basic facts about divisibility properties of the sequence $B_{E,P} = (B_n)$.

Lemma 3.1. *Suppose* p *denotes any prime divisor of* B_n. *Then*

$$\mathrm{ord}_p(B_{nk}) = \mathrm{ord}_p(B_n) + 2\mathrm{ord}_p(k). \tag{2}$$

This is proved in [10] and requires some local analysis of elliptic curves. Note that the property of being a divisibility sequence follows from (2). Indeed a stronger property follows immediately.

Lemma 3.2. *For any* $m, n \in \mathbb{N}$

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

Proof. Let $d = \gcd(m, n)$ and write $m = kd$, $n = \ell d$. Then for any prime p dividing B_d, one of $\mathrm{ord}_p(k)$ and $\mathrm{ord}_p(\ell)$ must be zero. By (2),

$$\mathrm{ord}_p(B_m) = \mathrm{ord}_p(B_d) + 2\,\mathrm{ord}_p(k) \text{ and } \mathrm{ord}_p(B_n) = \mathrm{ord}_p(B_d) + 2\,\mathrm{ord}_p(\ell),$$

so

$$\begin{aligned}\mathrm{ord}_p\left(\gcd(B_m, B_n)\right) &= \min\left\{\mathrm{ord}_p(B_d) + 2\,\mathrm{ord}_p(k), \mathrm{ord}_p(B_d) + 2\,\mathrm{ord}_p(\ell)\right\} \\ &= \mathrm{ord}_p(B_d),\end{aligned}$$

proving the lemma. □

These two lemmas will now be used to prove the fundamental property shared by those terms B_n which do not have a primitive divisor.

Lemma 3.3. *If* B_n *does not have a primitive divisor then*

$$B_n \Big| \prod_{p|n} p^2 B_{n/p}. \tag{3}$$

If (3) *holds, then any primitive divisor of* B_n *divides* n.

Proof. Assume that B_n does not have a primitive divisor. Let q be any prime, and p a prime dividing n. If $\mathrm{ord}_q(B_{n/p}) > 0$ for some prime $p \big| n$, then by Lemma 3.1

$$\mathrm{ord}_q(B_n) = \mathrm{ord}_q(B_{n/p}) + 2\,\mathrm{ord}_q(p) \leq \mathrm{ord}_q(B_{n/p}) + 2.$$

If $\mathrm{ord}_q(B_{n/p}) = 0$ for all primes $p \big| n$ then $q \not| \, B_n$. To see this, notice that if $q \big| B_n$ then by assumption $q \big| B_m$ for some $m \big| n$, hence $q \big| B_{n/p}$ for some prime p, contradicting $\mathrm{ord}_q(B_{n/p}) = 0$.

The partial converse follows in a similar way: if (3) holds and q is a primitive divisor of B_n, then

$$q \big| \prod_{p|n} p^2,$$

so $q \big| n$. □

Lemma 3.3 will play a practical as well as a theoretical role in the sequel. Our methods typically show that $\mathsf{Z}(B_{E,P}) \leq C$ for some moderately large C. The terms with $n \leq C$ need to be checked to find the lowest bound. The quadratic-exponential growth rate of the B_n means we wish to avoid factorizing terms to do the checking. Lemma 3.3 is an easily implemented method for performing the check which is factorization-free.

Finally, we gather some well-known facts about heights on elliptic curves. Recall that P is a non-torsion point in $E(\mathbb{Q})$, where the curve E is

$$E: \quad y^2 = x^3 - T^2 x,$$

with $T \in \mathbb{Z}$ square-free.

Write $h(\frac{a}{b}) = \log \max\{|a|, |b|\}$ for the Weil height of a rational number, so

$$h(x(nP)) = \log \max\{|A_n|, B_n\}.$$

Lemma 3.4. *Let $\hat{h}(P)$ denote the global canonical height of P. Then*

$$n^2\hat{h}(P) - \tfrac{1}{2}\log(T^2+1) - 0.116 \leq h(x(nP)) \leq n^2\hat{h}(P) + \log T + 0.347, \quad (4)$$

and

$$\hat{h}(P) \geq \tfrac{1}{4}\log T. \quad (5)$$

Proof. By [4, Eqn. (15)], for any point $Q \in E(\mathbb{Q})$,

$$-0.347 - \log T < \hat{h}(Q) - h(x(Q)) < \tfrac{1}{2}\log(T^2+1) + 0.116$$

(notice that the canonical height we are working with is twice the value used in [4]). In particular,

$$\begin{aligned} h(x(nP)) &\leq \hat{h}(nP) + \log T + 0.347 \\ &= n^2\hat{h}(P) + \log T + 0.347 \end{aligned}$$

and

$$\begin{aligned} h(x(nP)) &\geq \hat{h}(nP) - \tfrac{1}{2}\log(T^2+1) - 0.116 \\ &= n^2\hat{h}(P) - \tfrac{1}{2}\log(T^2+1) - 0.116 \end{aligned}$$

proving (4).

The other result we call upon also appeared in [4, Prop. 2.1]. If P denotes any non-torsion rational point on E, then

$$\tfrac{1}{8}\log(2T^2) \le \hat{h}(P),$$

from which (5) is immediate. $\square$

Proof of Theorem 2.2. Assume that B_n does not have a primitive divisor. Taking logarithms in Lemma 3.3 gives

$$\log B_n \le 2\sum_{p|n}\log p + \sum_{p|n}\log B_{n/p}. \tag{6}$$

The proof proceeds using various upper and lower estimates for $\log B_k$ to make quantitative the observation that (6) automatically bounds n.

It is possible to use a deep general result from elliptic transcendence theory to obtain a lower bound of the form

$$\log B_n \ge n^2\hat{h}(P) - \mathrm{O}(\log n \log\log n). \tag{7}$$

Inserting this into (6) shows that $\mathsf{Z}(B_{E,P})$ is finite because the right-hand side is bounded by cn^2 with $c<1$.

Results of the form (7) have been obtained by David [6]. The form of the implied constant in (7) is given explicitly in [14]. However, the shape of the constant is too unwieldy for our purposes. For one thing, the dependence upon T comes as a power of $\log T$ – to obtain a uniformity result we need it to be linear in $\log T$. Another problem is that the implied constants are enormous. The quadratic-exponential growth rate of the sequence $B_{E,P}$ means that applying this method would greatly complicate the computation of the Zsigmondy bound.

Our approach is to use an inferior lower bound in respect of the leading term: typically $n^2\hat{h}(P)$ will be replaced by one half or even one quarter of this. However, the resulting error term is more readily controlled.

By (4), for any $p\big|n$,

$$\begin{aligned}\log B_{n/p} &\le h(x(\tfrac{n}{p}P))\\ &\le \hat{h}(\tfrac{n}{p}P) + \log T + 0.347\\ &= \tfrac{n^2}{p^2}\hat{h}(P) + \log T + 0.347. \end{aligned}\tag{8}$$

We will call on three arithmetical functions. Denote by $\omega(n)$ the number of distinct prime divisors of n. Clearly

$$\omega(n) \le \log n/\log 2 \le (1.443)\log n.$$

Denote by $\rho(n)$ the sum $\sum_{p|n}\frac{1}{p^2}$ over prime divisors of n. A calculation shows that

$$\rho(n) \le 0.453 \text{ for all } n \ge 1.$$

Finally define

$$\eta(n) = 2\sum_{p|n} \log p.$$

Substituting (8) into (6) gives

$$\begin{aligned} \log B_n &\leq \eta(n) + \sum_{p|n} \left(\tfrac{n^2}{p^2} \hat{h}(P) + \log T + 0.347 \right) \\ &\leq \eta(n) + n^2 \rho(n) \hat{h}(P) + \omega(n) \left(\log T + 0.347 \right) \end{aligned} \tag{9}$$

Assume first that $n = 2m$ is even. From the duplication formula on the curve E,

$$\frac{A_n}{B_n} = \frac{A_{2m}}{B_{2m}} = x(nP) = x(2mP) = \frac{(A_m^2 + T^2 B_m^2)^2}{4A_m B_m (A_m^2 - T^2 B_m^2)}. \tag{10}$$

It follows that

$$B_{2m} = \frac{4A_m B_m (A_m^2 - T^2 B_m^2)}{\gcd\left((A_m^2 + T^2 B_m^2)^2, 4A_m B_m (A_m^2 - T^2 B_m^2)\right)}$$

To bound the size of the greatest common divisor, note that A_m and B_m are coprime by definition. Now work through the factors of the denominator $4A_m B_m (A_m^2 - T^2 B_m^2)$ in turn. We must count 4 in case it divides the numerator. If A_m has a common factor with the numerator it must divide T^2 – to be maximally pessimistic suppose it divides both terms in the numerator maximally. However, B_m has no factor in common with the numerator. Finally, if $A_m^2 - T^2 B_m^2$ has a factor in common with $A_m^2 + T^2 B_m^2$ then this must divide their sum and difference – and hence must divide $2T^2$. Thus

$$\gcd\left((A_m^2 + T^2 B_m^2)^2, 4A_m B_m (A_m^2 - T^2 B_m^2)\right) \leq 4T^2 \left(2T^2\right)^2 = 16T^6. \tag{11}$$

The greatest common divisor may also be bounded using the following argument. From (4), trivial estimates for the numerator and denominator in (10) show that the logarithm of each is bounded by $4\hat{h}m^2 + \mathrm{O}(1)$, with a uniform error. However (4) shows that $\log \max\{|A_{2m}|, B_{2m}\}$ is bounded below by $4\hat{h}m^2 - \mathrm{O}(\log T)$; thus bounding the possible cancellation by a power of T as before. For even n this approach is not needed, but we will make essential use of it later for one of the odd n cases.

From (11) we deduce the important lower bound

$$\frac{|A_m B_m (A_m^2 - T^2 B_m^2)|}{4T^6} \leq B_{2m},$$

or in logarithmic form,

$$\begin{aligned} \log |A_m| + \log B_m + \log |A_m^2 - T^2 B_m^2| & \\ - \log 4 - 6 \log T &\leq \log B_{2m} = \log B_n. \end{aligned} \tag{12}$$

Lemma 3.5. *For $T \geq 5$,*

$$2\log\max\{|A_m|, B_m\} - \log T - 0.155$$

$$\leq \log|A_m| + \log B_m + \log|A_m^2 - T^2B_m^2|. \tag{13}$$

Proof. If

$$|A_mB_m| \leq |A_m^2 - T^2B_m^2|$$

then

$$\begin{aligned}\log|A_m| + \log B_m + \log|A_m^2 - T^2B_m^2| &\geq 2\left(\log|A_m| + \log B_m\right) \\ &\geq 2\log\max\{|A_m|, B_m\}.\end{aligned}$$

which gives (13). So assume that

$$|A_mB_m| > |A_m^2 - T^2B_m^2|.$$

Then

$$\left|\frac{A_m}{B_m}\right| > \left|\left|\frac{A_m}{B_m}\right|^2 - T^2\right|,$$

so

$$T - \tfrac{1}{2} \leq \left|\frac{A_m}{B_m}\right| \leq T + \tfrac{1}{2}$$

and hence

$$|\log|A_m| - \log B_m| \leq \log(T + \tfrac{1}{2}) \leq \log T + 0.155$$

since $T \geq 5$. It follows that

$$\begin{aligned}2\log\max\{|A_m|, B_m\} - \log T - 0.155 &\leq \log|A_m| + \log B_m \\ &\leq \log|A_m| + \log B_m \\ &\qquad + \log|A_m^2 - T^2B_m^2|.\end{aligned}$$

□

By (12) and (13),

$$\begin{aligned}\log B_n &\geq 2\log\max\{|A_m|, B_m\} - 7\log T - 1.542 \\ &= 2h(x(mP)) - 7\log T - 1.542,\end{aligned}$$

so by (4) and (9),

$$\begin{aligned}\tfrac{1}{2}n^2\hat{h}(P) - 7\log T - \log(T^2+1) - 1.774 &\leq 2h(x(mP)) - 7\log T - 1.542 \\ &\leq \log B_n \\ &\leq \eta(n) + n^2\rho(n)\hat{h}(P) \\ &\qquad + \omega(n)\left(\log T + 0.347\right).\end{aligned}$$

It follows that

$$\begin{aligned}n^2\hat{h}(P)\left(\tfrac{1}{2} - \rho(n)\right) &\leq \eta(n) + \omega(n)\left(\log T + 0.347\right) \\ &\qquad + 7\log T + \log(T^2+1) + 1.774.\end{aligned} \tag{14}$$

Recall that $T \geq 5$ so $\log T > 1.609$. Divide (14) by $\log T$, note that

$$\frac{\log(T^2+1)}{\log T} \leq 2.024 \text{ for } T \geq 5,$$

and combine (14) with (5) to deduce that

$$n^2\left(\tfrac{1}{2}-\rho(n)\right) \leq 4\left(0.621\eta(n)+1.216\omega(n)+10.127\right).$$

This implies that $n \leq 19$, so $\mathsf{Z}_{\mathsf{e}}(B_{E,P}) \leq 18$.

The bound obtained so far (when n is even) takes a similar form in general. Assume that $x(P) < 0$ and n is odd. If $B_n \geq |A_n|$ then

$$\log B_n \geq h(x(nP)) \geq n^2\hat{h}(P) - \tfrac{1}{2}\log(T^2+1) - 0.116. \tag{15}$$

If $B_n < |A_n|$, use the fact that if n is odd then $x(nP) < 0$ and so

$$-T \leq x(nP) < 0.$$

Thus $|A_n/B_n| \leq T$, so

$$\log|A_n| - \log T \leq \log B_n.$$

Therefore

$$\begin{aligned} \log B_n &\geq h(x(nP)) - \log T \\ &\geq n^2\hat{h}(P) - \tfrac{1}{2}\log(T^2+1) - \log T - 0.116. \end{aligned}$$

This lower bound, being smaller than (15), covers both cases. By (6) we have

$$\begin{aligned} n^2\hat{h}(P) - \tfrac{1}{2}\log(T^2+1) - \log T - 0.116 &\leq \log B_n \\ &\leq \eta(n) + n^2\rho(n)\hat{h}(P) \\ &\quad +\omega(n)\log T + 0.174\omega(n). \end{aligned}$$

Since $T \geq 5$, the bound (5) then implies that

$$n^2(1-\rho(n)) \leq 4\left(0.621\eta(n)+1.109\omega(n)+2.128\right).$$

It follows that $n \leq 6$, so $\mathsf{Z}_{\mathsf{o}}(B_{E,P}) \leq 5$. This dramatic improvement in the size of the bound is mainly accounted for by the fact that $\rho(n) \leq 0.203$ for all odd n, and the very good lower bound for $\log B_n$. The fact that the bound for $\rho(n)$ over odd n is strictly smaller than $\frac{1}{4}$ will play a critical role later.

Finally, assume that $x(P)$ is a square. The cases $x(P) \pm T$ being squares are dealt with similarly; in any event, Theorem 2.4 deals with the general case. For this part of Theorem 2.2, we are going to use the fact that $x(nP)$ is a square for all $n \in \mathbb{N}$. This follows from the proof of the Weak Mordell Theorem: The map $E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ given by

$$P \mapsto x(P)\mathbb{Q}^{*2} \text{ and } (0,0) \mapsto -\mathbb{Q}^{*2}$$

is a group homomorphism. Write

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

Assume that $n = 2m+1$ is odd and write

$$nP = mP + (m+1)P.$$

Then

$$x(nP) = \frac{A_{2m+1}}{B_{2m+1}} = \left(\frac{y((m+1)P) + y(mP)}{x((m+1)P) - x(mP)} \right)^2 - x(mP) - x((m+1)P).$$

Inserting the explicit form of $nP = mP + (m+1)P$ into this formula yields

$$\frac{(A_m A_{m+1} - T^2 B_m B_{m+1})(A_m B_{m+1} + A_{m+1} B_m) - 2C_m C_{m+1} B_m^{1/2} B_{m+1}^{1/2}}{(A_{m+1} B_m - A_m B_{m+1})^2}. \tag{16}$$

Once again we wish to bound the possible size of the greatest common divisor of the numerator N and the denominator D in (16). An additional complication here is the appearance of terms arising from $y(P)$. Since nP lies on the curve $y^2 = x^3 - T^2 x$,

$$C_n^2 = A_n^3 - T^2 A_n B_n^2.$$

It follows that

$$\begin{aligned} \log|C_n| &\le \tfrac{1}{2}\left(\log 2 + \max\log\{A_n^3, T^2 A_n B_n^2\}\right) \\ &\le \tfrac{1}{2}\left(\log 2 + 3n^2 \hat{h}(P) + 5\log T + 1.041\right). \end{aligned} \tag{17}$$

Now write

$$\alpha = (A_m A_{m+1} - T^2 B_m B_{m+1})(A_m B_{m+1} + A_{m+1} B_m)$$

and

$$\beta = 2C_m C_{m+1} B_m^{1/2} B_{m+1}^{1/2}.$$

By using (4) and (17),

$$\begin{aligned} \log|\alpha| &\le \log 4 + \log\max\{A_m A_{m+1}, T^2 B_m B_{m+1}\} \\ &\qquad + \log\max\{A_m B_{m+1}, A_{m+1} B_m\} \\ &\le (4m^2 + 4m + 2)\hat{h}(P) + 6\log T + 2.775 \end{aligned}$$

and

$$\log|\beta| \le (4m^2 + 4m + 2)\hat{h}(P) + 6\log T + 2.775.$$

Thus the numerator and denominator of (16) satisfy

$$\begin{aligned} \max\{\log|N|, \log|D|\} &\le \log 2 + \log\max\{|\alpha|, |\beta|\} \\ &\le (4m^2 + 4m + 2)\hat{h}(P) + 6\log T + 3.469. \end{aligned} \tag{18}$$

On the other hand, by the lower bound in (4),

$$\begin{aligned}\max\{\log|A_n|,\log B_n\} &\geq n^2\hat{h}(P)-\tfrac{1}{2}\log(T^2+1)-0.116\\ &= (4m^2+4m+1)\hat{h}(P)-\tfrac{1}{2}\log(T^2+1)-0.116.\end{aligned}$$

It follows that

$$\gcd(N,D)\leq \hat{h}(P)+6\log T+\tfrac{1}{2}\log(T^2+1)+3.584,$$

so by (16) and (9)

$$\begin{aligned}&2\log\left(A_{m+1}B_m-A_mB_{m+1}\right)-\hat{h}(P)-6\log T-\tfrac{1}{2}\log(T^2+1)-3.584\\ &<\ \log B_n\\ &<\ \eta(n)+n^2\rho(n)\hat{h}(P)+\omega(n)\left(\log T+0.347\right). \qquad (19)\end{aligned}$$

Now by assumption A_m, A_{m+1}, B_m and B_{m+1} are all squares; write $A_* = a_*^2$ and $B_* = b_*^2$ with $a_*, b_* > 0$. Then

$$\begin{aligned}\max\{\log|a_{m+1}|,|b_{m+1}|\} &\leq \log\left(|a_{m+1}|+|b_{m+1}|\right)\\ &\leq \log\left(|a_{m+1}b_m|+|a_mb_{m+1}|\right)\\ &\leq \log\left|a_{m+1}^2b_m^2-a_m^2b_{m+1}^2\right|, \qquad (20)\end{aligned}$$

so by (19)

$$\begin{aligned}h\left((m+1)P\right) &= \max\{\log A_{m+1},B_{m+1}\}\\ &\leq \eta(n)+(n^2+1)\rho(n)\hat{h}(P)+\omega(n)\left(\log T+0.347\right)\\ &\qquad +6\log T+\tfrac{1}{2}\log(T^2+1)+3.584.\end{aligned}$$

Using (4), (5) and the assumption that $T\geq 5$, this shows that

$$\tfrac{1}{4}(n+1)^2-(n^2+1)\rho(n)\leq 4\left(0.621\eta(n)+10.596+1.216\omega(n)\right). \qquad (21)$$

It is not clear that the left-hand side of (21) grows at all. However, as noted earlier, for odd n we have $\rho(n) < 0.203 < \frac{1}{4}$, so the left-hand side of (21) grows at least like $0.047n^2$ for odd n. Thus (21) does bound n. Indeed (21) implies that $n \leq 21$, showing that $\mathsf{Z}_{\mathsf{o}}(B_{E,P}) \leq 21$. □

4. Explicit Examples

Theorem 2.2 supplies such good bounds that the remaining cases can be checked using Lemma 3.3. Inserting explicit values for the canonical heights in specific examples reduces the checking even further. From the proof in Section 3 we have the following inequalities under the assumption that B_n does not have a primitive divisor. If $x(P) < 0$ and n is odd, then

$$\begin{aligned}n^2\hat{h}(P)\left(1-\rho(n)\right) &\leq \eta(n)+\omega(n)\log T+0.174\omega(n)\\ &\qquad +\tfrac{1}{2}\log(T^2+1)+\log T+0.0578; \quad (22)\end{aligned}$$

whilst if n is even, then

$$\begin{aligned}n^2\hat{h}(P)\left(\tfrac{1}{2}-\rho(n)\right) &\leq \eta(n)+\omega(n)\left(\log T+0.347\right)\\ &\qquad +7\log T+\log(T^2+1)+1.774. \qquad (23)\end{aligned}$$

4.1. **Example 2.3.** Here $T = 5$ and the canonical height of $P = (-4, 6)$ is given by $\hat{h}(P) = 1.899\ldots$. Theorem 2.2 predicts $\mathsf{Z}_{\mathsf{e}}(B_{E,P}) \leq 18$. Now B_{18} is an integer with 267 decimal digits – itself the square of an integer with 134 decimal digits. Factorizing integers of that size cannot easily be guaranteed in reasonable time. However, using Lemma 3.3, the checking of the remaining cases is quick. Inserting the explicit estimate for $\hat{h}(P)$ reduces this calculation still further. Assuming that B_n does not have a primitive divisor, (22) and (23) imply $\mathsf{Z}_{\mathsf{o}}(B_{E,P}) = 1$ and $\mathsf{Z}_{\mathsf{e}}(B_{E,P}) \leq 8$. The remaining cases can easily be checked almost by hand, but certainly using Lemma 3.3.

4.2. **Example 2.7.** This is proved in similar fashion to Example 2.3 so it is not discussed it in detail.

5. Proof of Theorem 2.4

Suppose without loss of generality that $Q = (0, 0)$ in every case, since translation preserves both the discriminant of the curve and the kind of result sought. Assume the defining equation for E has the form

$$E: \quad y^2 = x(x^2 + ax + b) = x(x - r_1)(x - r_2).$$

The discriminant $\Delta = \Delta(E)$ of the curve is given by

$$\Delta = (r_1 r_2 (r_1 - r_2))^2. \tag{24}$$

Lemma 5.1.

$$\max\{|\log|r_1||, |\log|r_2||\} = \mathrm{O}(\log|\Delta|). \tag{25}$$

Proof. Clearly

$$\max\{|\log|r_1||, |\log|r_1||\} = \mathrm{O}\left(|\log|r_1|| + |\log|r_2|| + |\log|r_1 - r_2||\right). \tag{26}$$

If $|r_1 - r_2| \geq 1$ then the right-hand side of (26) is $\mathrm{O}(\log \Delta)$.

Assume now that $|r_1 - r_2| < 1$. The formula (24) together with the fact that $\Delta \geq 1$ implies that

$$1 \leq |r_2 r_2| \cdot |r_1 - r_2| = \sqrt{\Delta},$$

so

$$0 \leq \log|r_1 r_2| + \log|r_1 - r_2| = \tfrac{1}{2}\log\Delta.$$

Now $\log|r_1 r_2| \geq 0$, so $|\log|r_1 - r_2|| \leq \log|r_1 r_2|$. It follows that the right-hand side of (26) is again $\mathrm{O}(\log \Delta)$. □

In the situation of Theorem 2.4, we need a bound of the form

$$|\hat{h}(P) - h(P)| \leq c \log \Delta,$$

and this follows from the result in [12] which bounds $|\hat{h}(P) - h(P)|$ in terms of the height of the j-invariant (and hence the height of the discriminant) of the curve.

Proof of Theorem 2.4. In the even case, writing $n = 2m$ and applying the duplication formula shows that

$$\log|A_m| + \log B_m + \log|A_m^2 + aA_mB_m + bB_m^2| - \mathrm{O}(\log\Delta) \le \log B_n.$$

If $|A_m^2 + aA_mB_m + bB_m^2| \ge |A_mB_m|$ then we are done as before. On the other hand, using the same argument as before shows

$$\log|A_m| - \log B_m = \mathrm{O}(\max\{|\log|r_1||, |\log|r_2||\} = \mathrm{O}(\log\Delta)$$

by (25). The proof follows as before.

In case (2), the argument for the odd Zsigmondy bound is essentially identical to that given before. In case (1) the existence of two connected components requires there to be three real 2-torsion points. There are various cases to consider depending upon the signs and relative sizes of the roots, and these can be summarized as follows. Notice the inequality

$$\log|A_n/B_n| \le \max\{|\log|r_1||, |\log|r_2||, \log|r_1 - r_2|\}.$$

Each of the terms on the right is $\mathrm{O}(\log\Delta)$ and the following lower bound holds:

$$hn^2 - \mathrm{O}(\log\Delta) \le \log B_n.$$

The proof is completed exactly as before. □

6. Proof of Theorem 2.8

This may be shown using strong results of Bennett [1], [2] on Diophantine approximation in addition to the methods of Section 3. Writing $n = 2m$ as usual, the crucial point is to find an explicit estimate for

$$B_m\left|A_m^3 + (T^3+1)B_m^3\right|.$$

If A_m/B_m is bounded away from $\theta = (T^3+1)^{\frac{1}{3}}$ then we can proceed as before without difficulty. Otherwise, we need some kind of explicit lower bound from Diophantine approximation, of the form

$$\frac{a}{q^\lambda} < \left|\theta - \frac{p}{q}\right|$$

for all rationals p/q in lowest terms. Probably the best results of this kind have been found by Bennett [1], [2]. Applying these shows we may take

$$\log a = \mathrm{O}(\log T)$$

and

$$\lambda = 1 + \frac{2\log(\sqrt{T^3} + \sqrt{T^3+1}) + \log(3\sqrt{3}/2)}{2\log(\sqrt{T^3} + \sqrt{T^3+1}) - \log(3\sqrt{3}/2)},$$

where all implied constants are explicit and uniform. Examination of our method shows we need $\lambda < 2.188$ and T needs to be at least 26 to achieve this. Inserting this data into our machine yields an inequality of the form

$$\hat{h}\left(0.047 + \mathrm{O}(1/\log T)\right)n^2 < 2\log n + \mathrm{O}(\log T).$$

Finally, the canonical height of P satisfies

$$\hat{h} = \hat{h}(P) \sim \tfrac{1}{2} \log T.$$

Using the same methods as in [4], it is possible to give an explicit, positive lower bound for $\hat{h}(P)/\log T$ and the uniformity result follows. For this class of examples we have not tried to state the most explicit result possible.

References

[1] M. A. Bennett. Effective measures of irrationality for certain algebraic numbers. *J. Austral. Math. Soc. Ser. A*, 62(3):329–344, 1997.

[2] M. A. Bennett. Explicit lower bounds for rational approximation to algebraic numbers. *Proc. London Math. Soc. (3)*, 75(1):63–78, 1997.

[3] Y. 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.

[4] 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(2):187–208, 2000.

[5] J. W. S. Cassels. *Lectures on elliptic curves*, volume 24 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991.

[6] S. David. Minorations de formes linéaires de logarithmes elliptiques. *Mém. Soc. Math. France (N.S.)*, (62):iv+143, 1995.

[7] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward. *Recurrence sequences*, volume 104 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2003.

[8] G. Everest and T. Ward. *An introduction to number theory*. Springer-Verlag, London, 2005.

[9] G. Mclaren. PhD thesis, University of East Anglia, 2006.

[10] J. H. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, New York, 1986.

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

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

[13] J. H. Silverman and J. Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[14] R. J. Stroeker and N. Tzanakis. Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. *Acta Arith.*, 67(2):177–196, 1994.

[15] K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math.*, 3:265–284, 1892.

School of Mathematics, University of East Anglia, Norwich NR4 7TJ, UK.
E-mail address: g.everest@uea.ac.uk