ACTA ARITHMETICA
151.2 (2012)

Primitive divisors of certain elliptic divisibility sequences

by

Paul Voutier (London) and Minoru Yabuta (Osaka)

1. Introduction. A sequence $C = (C_n)_{n\geq 1}$ is called a *divisibility sequence* if $C_m \mid C_n$ whenever $m \mid n$. For such a sequence C, a prime p is called a *primitive divisor* of the term C_n if p divides C_n but does not divide C_k for any $0 < k < n$. Primitive divisors have been studied by many authors. In 1892, Zsigmondy [18] showed that for the sequence $C_n = a^n - b^n$ the term C_n has a primitive divisor for all $n > 6$, where a and b are positive coprime integers. In 1913, Carmichael [2] showed that if $n > 12$ then the nth term of any Lucas sequence has a primitive divisor in the case of positive discriminant. Ward [16] and Durst [4] extended Carmichael's result to Lehmer sequences. In 2001, Bilu, Hanrot and Voutier [1] proved that if $n > 30$ then every nth Lucas and Lehmer number has a primitive divisor, and listed all Lucas and Lehmer numbers without a primitive divisor. The results of Zsigmondy, Carmichael–Ward–Durst and Bilu–Hanrot–Voutier are all best possible (in the sense that for $n = 6$, $n = 12$ and $n = 30$, respectively, sequences whose nth element has no primitive divisor do exist).

Let E be an elliptic curve defined over $\mathbb{Q}$ and denote by $E(\mathbb{Q})$ the additive group of all rational points on the curve E. Let $P \in E(\mathbb{Q})$ be a point of infinite order, and for any non-zero integer n write

$$x(nP) = \frac{A_n(P)}{B_n(P)}, \tag{1.1}$$

in lowest terms with $A_n(P) \in \mathbb{Z}$ and $B_n(P) \in \mathbb{N}$. The sequence $(B_n(P))_{n\geq 1}$ is often called an *elliptic divisibility sequence* in the literature. Strictly speaking, this is not correct as it is the so-called "division polynomials" $(\psi_n(P))_{n\geq 1}$ (where $x(nP) = \phi_n(P)/\psi_n^2(P)$) which satisfy the required recurrence relation (see [6, Section 10.1] and [10, Exercise 3.7]).

2010 *Mathematics Subject Classification*: Primary 11G05, 11A41.
Key words and phrases: elliptic curve, elliptic divisibility sequence, primitive divisor.

DOI: 10.4064/aa151-2-2

Ward [15] first studied the arithmetic properties of elliptic divisibility sequences. Silverman [11] first showed that for any elliptic curve $E/\mathbb{Q}$ in long Weierstrass form and any point $P \in E(\mathbb{Q})$ of infinite order, there exists a positive integer $N_{E,P}$ such that the term $B_n(P)$ has a primitive divisor for all integers $n \geq N_{E,P}$. The bound given by Silverman is not explicit and not uniform. Everest, Mclaren and Ward [5] obtained a uniform and quite small bound beyond which a primitive divisor is guaranteed for congruent number curves $y^2 = x^3 - T^2x$ with $T > 0$ square-free.

THEOREM 1.1 (Everest, Mclaren, Ward [5]). *For $E : y^2 = x^3 - T^2x$ with $T > 0$ square-free, let $P \in E(\mathbb{Q})$ be a point of infinite order. If $B_n(P)$ does not have a primitive divisor, then*

(a) *$n \leq 10$ if n is even,*
(b) *$n \leq 3$ if n is odd and $x(P)$ is negative,*
(c) *$n \leq 21$ if n is odd and $x(P)$ is a rational square.*

Ingram [7] sharpened the bounds obtained in [5] as follows.

THEOREM 1.2 (Ingram [7]). *Let E and P be as Theorem 1.1. If $B_n(P)$ does not have a primitive divisor, then $5 \nmid n$, and either n is odd or $n = 2$. Furthermore, if*

(a) *$x(P) < 0$, or*
(b) *$\{x(P), x(P) + T, x(P) - T\}$ contains a rational square,*

then $n \leq 2$.

In what follows, a will denote a non-zero integer which is fourth-power-free and $E_a : y^2 = x^3 + ax$ will be an elliptic curve. The purpose of this paper is to generalise the above results on the existence of primitive divisors to all such E_a.

This condition on a poses no restriction here, since the minimal model of any E_a is of this form. Furthermore, we require a minimal model, since otherwise, $B_n(P)$ can be without a primitive divisor for arbitrarily large n: for any n, let $u = \sqrt{B_n(P)}$, E'_a be the image of E_a under the map $(x, y) \mapsto (u^2x, u^3y)$ and P' the image of P under this map, then $B_n(P') = 1$.

THEOREM 1.3. *Let $P \in E_a(\mathbb{Q})$ be a point of infinite order. Let n be a positive integer and assume that $B_n(P)$ does not have a primitive divisor. If* (i) *n is odd and either $x(P)$ is a rational square or $x(P) < 0$, or* (ii) *n is even, then $n \leq 2$.*

REMARK 1.4. It is easy to show that there are infinitely many values of a and points $P \in E_a(\mathbb{Q})$ such that $x(2P)$ is an integer, so $B_2(P) = 1$. For instance, let P be an integer point on E_a for $a \equiv 4 \bmod 16$, existing by Lemma 6.1 of [14] and the duplication formula. So this theorem is best possible.

REMARK 1.5. If we remove the conditions on $x(P)$ for odd n, then it is again easy to find infinitely many values of a and points $P \in E_a(\mathbb{Q})$ such that $B_3(P) = 1$. For example, $P = (30, 120) \in E_{-420}(\mathbb{Q})$ and $P = (30, 450) \in E_{5850}(\mathbb{Q})$.

From our use of Ingram's ideas [7] in Subsection 5.5, it appears that $n \leq 3$ is the best possible bound for E_a without any conditions on $x(P)$.

Indeed, in this paper, we show that if B_n does not have a primitive divisor for any elliptic divisibility sequence generated from any non-torsion point on any E_a for $n > 3$, then $5 \nmid n$ and either $n = 9, 11, 19$ or $n > 20$.

REMARK 1.6. Although $x(2P)$ is a square for $P \in E_a(\mathbb{Q})$ (see Lemma 6.1(a) in [14]), it is not the case that if $x(P)$ is a perfect square then $P = 2Q$ where $Q \in E_a(\mathbb{Q})$. The significance of this statement is that our result for n odd and $x(P)$ a perfect square is not a trivial consequence of the result for even n.

Lastly, we note that Everest, Mclaren and Ward [5, Theorem 2.4] proved an analogous result to Theorem 1.3 (with an absolute, though unspecified, bound for n) for any elliptic curve over $\mathbb{Q}$ with non-trivial 2-torsion, provided Lang's conjecture holds for the curve. Using Cremona's elliptic curve data as available via PARI, we found that the elliptic divisibility sequence defined by

$$y^2 + xy = x^3 - 15607620x + 23668880400$$

and $P = (-3780, -167400)$ has no primitive divisor for $n = 18$ ($B_9 = B_{18} = 289 = 17^2$) and satisfies the conditions in Theorem 2.4 of [5]. There are also five examples up to conductor 130 000 of such sequences whose 14th element has no primitive divisor.

And although it does not satisfy the conditions in Theorem 2.4 of [5] the elliptic divisibility sequence defined by

$$y^2 + xy = x^3 - 628340x + 887106192$$

and $P = (20824, -3013412)$ has no primitive divisor for $n = 21$ ($B_7 = B_{21} = 289 = 17^2$). We believe this is the largest index, n, such that B_n has no primitive divisor for a sequence generated by an elliptic curve with non-trivial 2-torsion.

Our paper is structured as follows. In the next section, we state our version of Lang's conjecture for $E_a(\mathbb{Q})$ as well as bounds on the difference between the canonical height and the logarithmic (Weil) height for any point on $E_a(\mathbb{Q})$. In Section 3, we prove some required results about elliptic divisibility sequences. Section 4 contains upper bounds on the height of a point $P \in E_a(\mathbb{Q})$ generating an elliptic divisibility sequence whose nth element does not have a primitive divisor, along with their proofs. Finally Section 5 combines the results of Sections 2–4 to obtain a small upper bound on such n. We then apply some results of Ingram [7] to complete the proof of Theorem 1.3.

2. Heights of points on $E_a(\mathbb{Q})$. We shall require two results regarding the height of points on elliptic curves. We require a lower bound in terms of a on the height of nontorsion points on $E_a(\mathbb{Q})$. We shall also need bounds on the difference between the canonical height and the logarithmic (Weil) height for any point on $E_a(\mathbb{Q})$.

We start by defining these heights.

For a rational point $P \in E(\mathbb{Q})$, we define the *canonical height* of P by

$$\widehat{h}(P) = \frac{1}{2} \lim_{n\to\infty} \frac{h(2^n P)}{4^n},$$

where $h(P) = h(x(P))$ is the *logarithmic height* of P and

$$h(s/t) = \log \max\{|s|, |t|\}$$

for a rational number s/t in lowest terms is the *logarithmic height* of s/t.

Remark 2.1. This definition of the canonical height follows that in Silverman's book [12]. This is one-half that found in [3], as well as one-half that returned from the height function, `ellheight`, in PARI (which is important to note here as we use PARI in some of our calculations).

Lemma 2.2. *Suppose a is a fourth-power-free integer. Let $P \in E_a(\mathbb{Q})$ be a nontorsion point. Then*

$$\widehat{h}(P) \geq \frac{1}{16}\log|a| + \begin{cases} (1/2)\log 2 & \text{if } a > 0 \text{ and } a \equiv 1,5,7,9,13,15 \bmod 16, \\ (1/4)\log 2 & \text{if } a > 0 \text{ and } a \equiv 2,3,6,8,10,11,12,14 \bmod 16, \\ -(1/8)\log 2 & \text{if } a > 0 \text{ and } a \equiv 4 \bmod 16, \\ (9/16)\log 2 & \text{if } a < 0 \text{ and } a \equiv 1,5,7,9,13,15 \bmod 16 \\ (5/16)\log 2 & \text{if } a < 0 \text{ and } a \equiv 2,3,6,8,10,11,12,14 \bmod 16, \\ -(1/16)\log 2 & \text{if } a < 0 \text{ and } a \equiv 4 \bmod 16. \end{cases} \tag{2.1}$$

Proof. This is Theorem 1.2 of [14]. ∎

Lemma 2.3. *For all points $P \in E_a(\mathbb{Q})$,*

$$-\frac{1}{4}\log|a| - 0.16 \leq \frac{1}{2}h(P) - \widehat{h}(P) \leq \frac{1}{4}\log|a| + 0.26.$$

Proof. This is Theorem 1.4 of [14]. ∎

3. Properties of elliptic divisibility sequences. Let $P \in E_a(\mathbb{Q})$ be a point of infinite order. Write

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

in lowest terms with $A_n, C_n \in \mathbb{Z}$ and $B_n \in \mathbb{N}$.

LEMMA 3.1. *Let p be any prime divisor of the term B_n. Then*

$$\operatorname{ord}_p(B_{kn}) = \operatorname{ord}_p(B_n) + 2\operatorname{ord}_p(k).$$

Proof. This is Lemma 3.1 of [5]. ∎

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

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

Proof. This is Lemma 3.2 of [5]. ∎

LEMMA 3.3. *If the term B_n does not have a primitive divisor, then*

$$\log B_n \le 2\sum_{p|n} \log p + \sum_{p|n} \log B_{n/p}. \tag{3.1}$$

Here the sums range over prime divisors of n.

Proof. This is the first part of Lemma 3.3 of [5]. ∎

We let $\omega(n)$ denote the number of distinct prime divisors of n. Further, we define

$$\rho(n) = \sum_{p|n} p^{-2} \quad \text{and} \quad \eta(n) = 2\sum_{p|n} \log p, \tag{3.2}$$

where the sums range over all prime divisors of n, and put

$$K = \frac{1}{2}\log|a| + 0.52. \tag{3.3}$$

LEMMA 3.4. *If the term B_n does not have a primitive divisor, then*

$$\begin{aligned} \log B_n &\le 2\sum_{p|n} \log p + \sum_{p|n} \left(2\left(\frac{n}{p}\right)^2 \widehat{h}(P) + K\right) \\ &= \eta(n) + 2n^2\rho(n)\widehat{h}(P) + \omega(n)K. \end{aligned} \tag{3.4}$$

Here, inequality (3.4) is analogous to inequality (9) of [5].

Proof. Lemma 2.3 implies that for any prime divisor p of n,

$$\log B_{n/p} \le h\left(\frac{n}{p}P\right) \le 2\widehat{h}\left(\frac{n}{p}P\right) + K = 2\left(\frac{n}{p}\right)^2 \widehat{h}(P) + K. \tag{3.5}$$

The last equality is a property of the canonical height (see Theorem 9.3 of [10]). Combining (3.1) and (3.5), we obtain the lemma. ∎

LEMMA 3.5. *Let $P \in E_a(\mathbb{Q})$ be any point of infinite order. Let m and n be positive integers with mn even.*

(a) *If $a \not\equiv 4 \bmod 16$ or $\operatorname{ord}_2(x(P)) \ne 1$ or $\operatorname{ord}_2(m) > 1$ or $\operatorname{ord}_2(n) > 1$, then*

$$0 < (A_m B_n - A_n B_m)^2 = B_{m+n}B_{|m-n|}. \tag{3.6}$$

(b) *If* $a \equiv 4 \bmod 16$, $\mathrm{ord}_2(x(P)) = 1$, $\mathrm{ord}_2(m) = 1$ *and* n *is odd, then*

$$0 < (A_mB_n - A_nB_m)^2 = 4B_{m+n}B_{|m-n|}. \tag{3.7}$$

REMARK 3.6. For mn even, there is one case excluded from this lemma: $\mathrm{ord}_2(m) = \mathrm{ord}_2(n) = 1$, $a \equiv 4 \bmod 16$ and $\mathrm{ord}_2(x(P)) = 1$. Here we have $0 < (A_mB_n - A_nB_m)^2 = 16B_{m+n}B_{|m-n|}$, but since we do not need that result in this work, we do not prove that here.

Also the condition that mn is even is a natural one here. Without this condition, we get additional prime divisors, p, of a arising on the right-hand side when $\mathrm{ord}_p(x(P)) > 0$ from Case 2-b in the proof since mP modulo p is no longer a non-singular point.

Proof of Lemma 3.5. Since P is of infinite order, $x(mP) \neq x(nP)$ and hence $A_mB_n - A_nB_m \neq 0$.

For any $P \in E_a(\mathbb{Q})$ of infinite order and any positive integers m and n, write

$$mP = (x_m, y_m) = \left(\frac{A_m}{B_m}, \frac{C_m}{B_m^{3/2}}\right), \qquad nP = (x_n, y_n) = \left(\frac{A_n}{B_n}, \frac{C_n}{B_n^{3/2}}\right)$$

in lowest terms. By the addition formula on the curve E_a, we have

$$x(|m \pm n|P) = \left(\frac{y_m \mp y_n}{x_m - x_n}\right)^2 - x_m - x_n \tag{3.8}$$

$$= \frac{(C_mB_n^{3/2} \mp C_nB_m^{3/2})^2}{B_mB_n(A_mB_n - A_nB_m)^2} - \frac{A_mB_n + A_nB_m}{B_mB_n}. \tag{3.9}$$

Substituting $y_m^2 = x_m^3 + ax_m$ and $y_n^2 = x_n^3 + ax_n$ into (3.8), we have

$$\begin{aligned} &x((m+n)P)x(|m-n|P) \\ &\quad = \frac{((x_m + x_n)(x_mx_n + a) - 2y_my_n)((x_m + x_n)(x_mx_n + a) + 2y_my_n)}{(x_m - x_n)^4} \\ &\quad = \frac{(x_m + x_n)^2(x_mx_n + a)^2 - 4(x_m^3 + ax_m)(x_n^3 + ax_n)}{(x_m - x_n)^4} \\ &\quad = \frac{(x_mx_n - a)^2}{(x_m - x_n)^2} = \frac{(A_mA_n - aB_mB_n)^2}{(A_mB_n - A_nB_m)^2}. \end{aligned}$$

Therefore,

$$(A_mB_n - A_nB_m)^2A_{m+n}A_{|m-n|} = (A_mA_n - aB_mB_n)^2B_{m+n}B_{|m-n|}. \tag{3.10}$$

Put

$$\begin{aligned} &G_{m,n} = \gcd(A_{m+n}A_{|m-n|}, B_{m+n}B_{|m-n|}), \\ &U_{m,n} = (A_mA_n - aB_mB_n)^2, \qquad V_{m,n} = (A_mB_n - A_nB_m)^2. \end{aligned}$$

Then

$$(A_mB_n - A_nB_m)^2 = \frac{\gcd(U_{m,n}, V_{m,n})}{G_{m,n}} B_{m+n}B_{|m-n|}. \tag{3.11}$$

All the above holds without any further conditions on m, n and P.

To complete the proof, we will show that $\gcd(U_{m,n}, V_{m,n})/G_{m,n} = 1$, under the hypotheses of the lemma.

STEP 1: $p = 2$. Under the hypotheses of part (a) of the lemma, we will prove that $2 \nmid \gcd(U_{m,n}, V_{m,n})$ and under the hypotheses of part (b) of the lemma that $\mathrm{ord}_2(\gcd(U_{m,n}, V_{m,n})/G_{m,n}) = 2$.

First notice that if B_m and B_n are both even, then A_mA_n is odd and so is $A_mA_n - aB_mB_n$. Hence $2 \nmid \gcd(U_{m,n}, V_{m,n})$.

Also if exactly one of B_m and B_n is even (suppose without loss of generality that B_m is even), then A_m is odd and so is $A_mB_n - A_nB_m$. Hence $2 \nmid \gcd(U_{m,n}, V_{m,n})$.

Therefore, we need only consider the case when both B_m and B_n are odd. Furthermore, in this case, if exactly one of A_m and A_n is even, then $V_{m,n}$ is odd and again $2 \nmid \gcd(U_{m,n}, V_{m,n})$.

If 4 divides either m or n (say m, without loss of generality), then since $x(2P)$ is a rational square by Lemma 6.1(a) of [14], it follows from Lemma 6.1(c) of [14] that $B_4(P)$, and hence $B_m(P)$, is even. We saw above that this implies that $2 \nmid \gcd(U_{m,n}, V_{m,n})$. So we can assume that $\mathrm{ord}_2(m), \mathrm{ord}_2(n) \le 1$ and that at least one of m and n is even (again, suppose m is even).

From Lemma 6.1(c) of [14], unless $a \equiv 4 \bmod 16$ and $\mathrm{ord}_2(x(P)) = 1$, we have $\mathrm{ord}_2(B_m(P)) \ge \mathrm{ord}_2(B_2(P)) > 0$, which we saw above implies that $2 \nmid \gcd(U_{m,n}, V_{m,n})$. So we can assume that $a \equiv 4 \bmod 16$ and $\mathrm{ord}_2(x(P)) = 1$.

We have now handled the hypotheses of part (a) of the lemma, so we now assume that n is odd and consider part (b).

If A_mA_n is odd, then $U_{m,n}$ is odd too and $2 \nmid \gcd(U_{m,n}, V_{m,n})$. So it must be the case that both A_m and A_n are even.

From the arguments on pages 92–93 of [13], we can write

$$P = (b_1M^2/e^2, b_1MN/e^3)$$

in lowest terms, where $a = b_1b_2$ with $\gcd(b_1, e) = \gcd(b_2, M) = \gcd(e, M) = \gcd(M, N) = \gcd(e, N) = 1$. Furthermore, since $\mathrm{ord}_2(x(P)) = 1$, we have $2 \parallel b_1$. Hence e is odd.

Since $2 \parallel b_1$, we can put $u = 2$ in Lemma 6.1(c) of [14]. Therefore, we can write $nP = (b_1M_n^2/e_n^2, b_1M_nN_n/e_n^3)$ in lowest terms, where e_n is odd with $\gcd(b_2, M_n) = \gcd(M_n, N_n) = 1$. Since $a = b_1b_2 \equiv 4 \bmod 16$ and $2 \parallel b_1$, we have $2 \parallel b_2$. Since b_2 and M_n are coprime, M_n must be odd. Hence $2 \parallel A_n$.

Since m is even, by Lemma 6.1(a) of [14], A_m is a square, so $4 \mid A_m$, since A_m is even. Therefore, $4 \parallel V_{m,n}$ and so $\mathrm{ord}_2(\gcd(U_{m,n}, V_{m,n})) = 2$, since $4 \mid U_{m,n}$ too.

Since B_4 must be even by Lemma 6.1 of [14] and $|m \pm n|$ is odd, it must be the case that both B_{m+n} and $B_{|m-n|}$ are odd (otherwise $\gcd(4, |m \pm n|) = 1$ and so B_1 is even). Hence $G_{m,n} = 1$ and so if $m \equiv 2 \bmod 4$, n is odd, $a \equiv 4 \bmod 16$ and $\mathrm{ord}_2(x(P)) = 1$, then $\mathrm{ord}_2(\gcd(U_{m,n}, V_{m,n})/G_{m,n}) = 2$.

Step 2: p odd. We will next prove that if m and n are not both odd, then either $p \nmid \gcd(U_{m,n}, V_{m,n})$ or, if $p \mid \gcd(U_{m,n}, V_{m,n})$, then

$$\mathrm{ord}_p(\gcd(U_{m,n}, V_{m,n})/G_{m,n}) = 0,$$

for any odd prime p.

Put

$$W_{m,n} = (C_m B_n^{3/2} - C_n B_m^{3/2})^2 - (A_m B_n + A_n B_m)(A_m B_n - A_n B_m)^2,$$
$$W'_{m,n} = (C_m B_n^{3/2} + C_n B_m^{3/2})^2 - (A_m B_n + A_n B_m)(A_m B_n - A_n B_m)^2.$$

Note that $W_{m,n} W'_{m,n} = B_m^2 B_n^2 U_{m,n} V_{m,n}$.

We distinguish four cases.

Case 2-a. Assume that $p \nmid W_{m,n}$ and $p \nmid W'_{m,n}$. Then $p \nmid \gcd(U_{m,n}, V_{m,n})$.

Case 2-b. Assume that $p \mid W_{m,n}$ and $p \mid W'_{m,n}$. We will prove, by contradiction, that $p \nmid \gcd(U_{m,n}, V_{m,n})$.

Suppose that p divides $\gcd(U_{m,n}, V_{m,n})$. Then

$$A_m A_n - a B_m B_n \equiv 0 \bmod p, \tag{3.12}$$

$$A_m B_n - A_n B_m \equiv 0 \bmod p. \tag{3.13}$$

If $B_m \equiv 0 \bmod p$, then from (3.13), $A_m B_n \equiv 0 \bmod p$. Since A_m and B_m are coprime, we have $A_m \not\equiv 0 \bmod p$. Therefore $B_n \equiv 0 \bmod p$. From (3.12) we have $A_m A_n \equiv 0 \bmod p$, and since $A_m \not\equiv 0 \bmod p$, it follows that $A_n \equiv 0 \bmod p$. But this contradicts our assumption that A_n and B_n are coprime. Hence $B_m \not\equiv 0 \bmod p$.

By the same argument, we obtain $B_n \not\equiv 0 \bmod p$.

Since mP and nP are on E_a,

$$C_m^2 \equiv A_m(A_m^2 + a B_m^2) \bmod p, \tag{3.14}$$

$$C_n^2 \equiv A_n(A_n^2 + a B_n^2) \bmod p. \tag{3.15}$$

From our assumption that $p \mid W_{m,n}$ and $p \mid W'_{m,n}$, along with (3.13), we find that

$$C_m B_n^{3/2} - C_n B_m^{3/2} \equiv C_m B_n^{3/2} + C_n B_m^{3/2} \equiv 0 \bmod p,$$

and hence obtain $2 C_n B_m^{3/2} \equiv 0 \bmod p$. From $B_m \not\equiv 0 \bmod p$, we have $C_n \equiv 0 \bmod p$. Furthermore, since $B_n \not\equiv 0 \bmod p$, we also have $C_m \equiv 0 \bmod p$.

First assume that $A_mA_n \equiv 0 \bmod p$. From (3.12), we have $aB_mB_n \equiv 0 \bmod p$. Since $B_mB_n \not\equiv 0 \bmod p$, it follows that $a \equiv 0 \bmod p$.

Next assume that $A_mA_n \not\equiv 0 \bmod p$. Then from (3.14) and $C_m \equiv 0 \bmod p$, we have

$$A_m^2 + aB_m^2 \equiv 0 \bmod p. \tag{3.16}$$

Multiplying both sides of (3.12) by B_m and substituting $A_nB_m \equiv A_mB_n \bmod p$ (from (3.13)) and dividing both sides by B_n, we obtain $A_m^2 - aB_m^2 \equiv 0 \bmod p$. Subtracting it from (3.16) gives that $2aB_m^2 \equiv 0 \bmod p$ and therefore $a \equiv 0 \bmod p$.

In both cases $a \equiv 0 \bmod p$ and so from Proposition VII.5.1 of [10], E_a has bad reduction at p (additive reduction, in fact) and the reduction of mP modulo p is singular.

On the other hand, from Lemma 4.1(b) of [14], mP modulo p is non-singular, since m is even. This is a contradiction. Hence p does not divide $\gcd(U_{m,n}, V_{m,n})$.

Case 2-c. Assume that $p \mid W_{m,n}$ and $p \nmid W'_{m,n}$. Assume that p divides $\gcd(U_{m,n}, V_{m,n})$ and let $\operatorname{ord}_p(\gcd(U_{m,n}, V_{m,n})) = \alpha > 0$.

First assume that $\operatorname{ord}_p(V_{m,n}) \geq \operatorname{ord}_p(U_{m,n})$. Then we can put $\operatorname{ord}_p(U_{m,n}) = \alpha$ and $\operatorname{ord}_p(V_{m,n}) = \alpha + \beta$ with $\beta \geq 0$. From (3.9) we obtain

$$A_{|m-n|}B_mB_nV_{m,n} = B_{|m-n|}W'_{m,n}. \tag{3.17}$$

Since $A_{|m-n|}$ and $B_{|m-n|}$ are coprime and p does not divide $W'_{m,n}$, we have $\operatorname{ord}_p(A_{|m-n|}) = 0$. We saw, in Case 2-b, that if p divides $\gcd(U_{m,n}, V_{m,n})$, then both B_m and B_n are prime to p. Hence, from (3.17) we obtain $\operatorname{ord}_p(B_{|m-n|}) = \alpha + \beta$.

From (3.10), we can write

$$A_{m+n}A_{|m-n|}V_{m,n} = B_{m+n}B_{|m-n|}U_{m,n}.$$

Here $\operatorname{ord}_p(U_{m,n}) = \alpha$, $\operatorname{ord}_p(V_{m,n}) = \alpha + \beta$, $\operatorname{ord}_p(A_{|m-n|}) = 0$ and $\operatorname{ord}_p(B_{|m-n|}) = \alpha + \beta$. Since A_{m+n} and B_{m+n} are coprime, we find that $\operatorname{ord}_p(A_{m+n}) = \alpha$ and $\operatorname{ord}_p(B_{m+n}) = 0$. Hence

$$\operatorname{ord}_p(G_{m,n}) = \operatorname{ord}_p(\gcd(A_{m+n}A_{|m-n|}, B_{m+n}B_{|m-n|})) = \alpha$$

and $\operatorname{ord}_p(\gcd(U_{m,n}, V_{m,n})/G_{m,n}) = 0$.

For the case $\operatorname{ord}_p(U_{m,n}) \geq \operatorname{ord}_p(V_{m,n})$, in the same way, we again obtain $\operatorname{ord}_p(G_{m,n}) = \alpha$.

It follows that $\operatorname{ord}_p(\gcd(U_{m,n}, V_{m,n})/G_{m,n}) = 0$.

Case 2-d. Assume that $p \nmid W_{m,n}$ and $p \mid W'_{m,n}$. Then by the same argument as in Case 2-c, if $p \mid \gcd(U_{m,n}, V_{m,n})$, then $\operatorname{ord}_p(\gcd(U_{m,n}, V_{m,n})/G_{m,n}) = 0$.

Step 3: $G_{m,n}$. We show that for any prime p, if $p \nmid \gcd(U_{m,n}, V_{m,n})$, then $p \nmid G_{m,n}$.

Put $\gcd(B_m, B_n) = g_{m,n}$. Then we can write $B_m = g_{m,n}b_m$ and $B_n = g_{m,n}b_n$, where b_m and b_n are coprime. Since $g_{m,n}^3 \mid W_{m,n}$ (recall the definition of $W_{m,n}$ from Step 2 as the common numerator of the expression in (3.9)), we can write $W_{m,n} = g_{m,n}^3 W_{m,n,1}$, and from (3.9), we have

$$x((m+n)P) = \frac{W_{m,n,1}}{g_{m,n}b_m b_n (A_m b_n - A_n b_m)^2}.$$

From Lemma 3.2, we have $\gcd(B_{m+n}, B_m) = B_{\gcd(m+n,m)} = B_{\gcd(m,n)} = g_{m,n}$, and similarly $\gcd(B_{m+n}, B_n) = g_{m,n}$.

Therefore, we can write $B_{m+n} = g_{m,n}b_{m+n}$ where b_{m+n} is prime to both b_m and b_n. Therefore neither of b_m and b_n divides B_{m+n}. Hence

$$B_{m+n} \mid (A_m B_n - A_n B_m)^2. \tag{3.18}$$

Now assume that $p \nmid \gcd(U_{m,n}, V_{m,n})$. We will show by contradiction that p does not divide $G_{m,n}$.

Recall that $G_{m,n} = \gcd(A_{m+n}A_{|m-n|}, B_{m+n}B_{|m-n|})$. Suppose that p divides $G_{m,n}$. Since $\gcd(A_{m+n}, B_{m+n}) = \gcd(A_{|m-n|}, B_{|m-n|}) = 1$, without loss of generality, we may assume that p divides both $A_{|m-n|}$ and B_{m+n}.

Let $\operatorname{ord}_p(A_{|m-n|}) = s > 0$, $\operatorname{ord}_p(B_{m+n}) = t > 0$ and $2\operatorname{ord}_p(A_m B_n - A_n B_m) = u > 0$. From (3.18), we have $t \le u$. On the other hand, from (3.10) we have $u + s = t$ since $p \nmid \gcd(U_{m,n}, V_{m,n})$. Hence $s \le 0$. This contradiction allows us to conclude that p does not divide $G_{m,n}$.

From these three steps, it follows that

$$0 < (A_m B_n - A_n B_m)^2 = B_{m+n}B_{|m-n|},$$

as desired. ∎

4. Upper bounds. Recall our definitions $\rho(n)$ and $\eta(n)$ from (3.2), as well as K from (3.3), and set

$$L = \frac{1}{2}\log|a| + 0.32. \tag{4.1}$$

We obtain the following proposition.

Proposition 4.1. *Let $P \in E_a(\mathbb{Q})$ be a point of infinite order. Let n be a positive integer and assume that the term $B_n(P)$ does not have a primitive divisor.*

(a) *If n is odd and $x(P)$ is a rational square or if n is even, write $n = 2^e N$ where e is a non-negative integer and N is an odd integer. Then*

$n = 1, 2, 4$ *or* $N \geq 3$ *and*

$$0 < 2\left(\frac{1}{3} - \frac{1}{3N^2} - \rho(n)\right)\widehat{h}(P)n^2 \leq \eta(n) + \omega(n)K + K + L.$$

(b) *Let p be an odd prime. If n is odd, divisible by p and $x(P)$ is a rational square, or if n is even and divisible by p, then*

$$0 < 2\left(\frac{(p+1)^2}{4p^2} - \rho(n)\right)\widehat{h}(P)n^2 \leq \eta(n) + \omega(n)K + L.$$

REMARK 4.2. Note that part (b) can be improved for n even and $a < 0$:

$$0 < 2\left(\frac{5p^2 + 6p + 5}{16p^2} - \rho(n)\right)\widehat{h}(P)n^2 \leq \eta(n) + \omega(n)K + 2L + \log|a| + 0.385.$$

However, due to the restriction to $a < 0$, we will not use this here and so we do not include the proof (it is available on request). We mention it so other researchers know that improvements can be made.

By using estimates for $\rho(n)$, $\omega(n)$ and $\eta(n)$, we obtain the following corollary.

COROLLARY 4.3. *Let $P \in E_a(\mathbb{Q})$ be a point of infinite order.*

(a) *Let $n \geq 3$ be an odd integer and assume that $x(P)$ is a rational square. If $B_n(P)$ does not have a primitive divisor, then*

$$0.484\,\widehat{h}(P)n^2 < 2\log n + \frac{1.3841\log n}{\log\log n}K + K + L.$$

(b) *Let n be a positive even integer not divisible by 5. If $B_n(P)$ does not have a primitive divisor, then either $n \leq 4$ or n is not a power of 2 and*

$$0.049\,\widehat{h}(P)n^2 < 2\log n + \frac{1.3841\log n}{\log\log n}K + L.$$

4.1. Proof of Proposition 4.1. We are now ready to prove Proposition 4.1. Our proof is based upon ideas found in [5].

4.1.1. *Proof of part* (a). Assume that either $n > 1$ is an odd integer and $x(P)$ is a rational square or n is even.

If $B_{2^m}(P)$ does not have a primitive divisor, then $m \leq 2$ (see Theorem 1.2 of [17]). Hence we may assume that n is not a power of two, and write $n = 2^e N$, where e is a non-negative integer and N is an odd integer with $N \geq 3$.

Write $N = 3k + r$ with $r = 0, \pm 1$, and put $m = 2^e(2k + r)$ and $m' = 2^e k$. Since $N > 1$, we have $k > 0$ and so $m' > 0$ and $m - m' = 2^e(k + r) > 0$. Also $n = m + m'$.

If $r = \pm 1$, then k is even and $2k + r$ is odd. If n is odd, then m is odd and m' is even. If n is even, then m and m' are both even with $\mathrm{ord}_2(m') > \mathrm{ord}_2(m) > 0$.

If $r = 0$, then k is odd and $2k + r$ is even. If n is odd, then m is even and m' is odd. If n is even, then m and m' are both even with $\mathrm{ord}_2(m) > \mathrm{ord}_2(m') > 0$.

In each case, by Lemma 3.5(a) (which is applicable for n odd since $x(P)$ is assumed to be a rational square in this case), we have

$$(A_m B_{m'} - A_{m'} B_m)^2 \le B_{m+m'} B_{m-m'}.$$

Taking the logarithm of both sides gives

$$2 \log |A_m B_{m'} - A_{m'} B_m| \le \log B_n + \log B_{m-m'}. \tag{4.2}$$

Assume that the term B_n does not have a primitive divisor. Then, by Lemma 3.4, we have

$$\log B_n \le \eta(n) + 2n^2 \rho(n) \widehat{h}(P) + \omega(n) K. \tag{4.3}$$

Lemma 2.3 gives

$$\begin{aligned} \log B_{m-m'} &\le h((m-m')P) \\ &\le 2\widehat{h}((m-m')P) + K = 2(m-m')^2 \widehat{h}(P) + K. \end{aligned} \tag{4.4}$$

Combining (4.3) and (4.4) with (4.2) gives

$$\begin{aligned} &2 \log |A_m B_{m'} - A_{m'} B_m| \\ &\qquad \le \eta(n) + 2n^2 \rho(n) \widehat{h}(P) + \omega(n) K + 2(m-m')^2 \widehat{h}(P) + K. \end{aligned} \tag{4.5}$$

Lemma 6.1(a) of [14] implies that A_m and $A_{m'}$ are both squares, so we can write $A_m = a_m^2$, $A_{m'} = a_{m'}^2$, $B_m = b_m^2$ and $B_{m'} = b_{m'}^2$. Thus

$$\begin{aligned} 2 \log |A_m B_{m'} - A_{m'} B_m| &= 2 \log |a_m^2 b_{m'}^2 - a_{m'}^2 b_m^2| \ge 2 \log (|a_m b_{m'}| + |a_{m'} b_m|) \\ &\ge 2 \log (|a_m| + |b_m|) \ge 2 \log \max\{|a_m|, |b_m|\} \\ &= h(mP) \ge 2\widehat{h}(mP) - L, \end{aligned}$$

recalling from Lemma 3.5 that $A_m B_{m'} - A_{m'} B_m \ne 0$. Note that the last inequality is obtained by Lemma 2.3 and the definition of L in (4.1). Since $\widehat{h}(mP) = m^2 \widehat{h}(P)$, we have

$$2 \log |A_m B_{m'} - A_{m'} B_m| \ge 2m^2 \widehat{h}(P) - L.$$

Combining this estimate and (4.5) gives

$$2m^2 \widehat{h}(P) - L \le \eta(n) + 2n^2 \rho(n) \widehat{h}(P) + \omega(n) K + 2(m-m')^2 \widehat{h}(P) + K.$$

Substituting $m = 2^e(2N + r)/3$ and $m' = 2^e(N - r)/3$ gives

$$\eta(n) + \omega(n)K + K + L \geq 2\left(\frac{1}{3} - \frac{r^2}{3N^2} - \rho(n)\right)\widehat{h}(P)n^2 \geq 2\left(\frac{1}{3} - \frac{1}{3N^2} - \rho(n)\right)\widehat{h}(P)n^2. \tag{4.6}$$

4.1.2. *Proof of part* (b). Assume that n is a positive integer divisible by an odd prime p and $x(P)$ is a rational square, if n is odd. Write $n = pk$ for some positive integer k. Assume that B_n does not have a primitive divisor. Then by Lemmas 3.4 and 3.5(a) (observe that $\operatorname{ord}_2(p-1) \neq \operatorname{ord}_2(p+1)$ so 3.5(a) is also applicable if n is even), we have

$$\begin{aligned} 2\log|A_{(p+1)k/2}B_{(p-1)k/2} - A_{(p-1)k/2}B_{(p+1)k/2}| \\ \leq \log B_n + \log B_k \leq \eta(n) + 2n^2\rho(n)\widehat{h}(P) + \omega(n)K + \log B_k. \end{aligned} \tag{4.7}$$

On the other hand,

$$\begin{aligned} &2\log|A_{(p+1)k/2}B_{(p-1)k/2} - A_{(p-1)k/2}B_{(p+1)k/2}| \\ &\quad = 2\log|a^2_{(p+1)k/2}b^2_{(p-1)k/2} - a^2_{(p-1)k/2}b^2_{(p+1)k/2}| \\ &\quad = 2\log\big||a_{(p+1)k/2}b_{(p-1)k/2}| - |a_{(p-1)k/2}b_{(p+1)k/2}|\big| \\ &\qquad + 2\log(|a_{(p+1)k/2}b_{(p-1)k/2}| + |a_{(p-1)k/2}b_{(p+1)k/2}|) \\ &\quad \geq 2\log|b_k| + 2\log(|a_{(p+1)k/2}| + |b_{(p+1)k/2}|) \quad \text{since } b_k \mid b_{(p\pm1)k/2}, \\ &\quad \geq \log B_k + h(((p+1)k/2)P) \\ &\quad \geq \log B_k + 2((p+1)k/2)^2\widehat{h}(P) - L. \end{aligned} \tag{4.8}$$

Combining (4.7) and (4.8) gives

$$2((p+1)k/2)^2\widehat{h}(P) - L \leq \eta(n) + 2n^2\rho(n)\widehat{h}(P) + \omega(n)K.$$

Substituting $k = n/p$, we obtain

$$2\left(\frac{(p+1)^2}{4p^2} - \rho(n)\right)\widehat{h}(P)n^2 \leq \eta(n) + \omega(n)K + L. \tag{4.9}$$

We have thus completed the proof of part (b). ∎

4.2. Proof of Corollary 4.3. To prove Corollary 4.3, we use Robin's estimate for $\omega(n)$ (see Théorème 11 of [8]):

$$\omega(n) < \frac{1.3841\log n}{\log\log n} \quad \text{for all } n \geq 3. \tag{4.10}$$

Furthermore, we use the following estimate for $\rho(n)$:

$$\rho(n) < \sum_{p<10^6} p^{-2} + \left(\zeta(2) - \sum_{m\le 10^6} m^{-2}\right) < 0.452248 + 0.000001 < 0.45225, \tag{4.11}$$

where the first sum is over primes, p, and the second sum over positive integers, m.

4.2.1. *Proof of Corollary 4.3(a).* Let $P \in E_a(\mathbb{Q})$ be a point of infinite order. Let $n \ge 3$ be an odd integer, and assume that $x(P)$ is a rational square. We will distinguish three cases.

Case 1. Assume that n is not divisible by either 3 or 5. Then $n \ge 7$ and $\rho(n) < 0.45225 - 1/4 - 1/9 - 1/25 < 0.052$. Here we apply Proposition 4.1(a), so we have $N = n$ and

$$2\left(\frac{1}{3} - \frac{1}{3N^2} - \rho(n)\right) > 0.549,$$

and the corollary follows in this case.

Case 2. Assume that n is divisible by 3. Then $\rho(n) < 0.45225 - 1/4 < 0.2023$. Here we apply Proposition 4.1(b) with $p = 3$, so

$$2\left(\frac{(p+1)^2}{4p^2} - \rho(n)\right) = 2\left(\frac{4}{9} - \rho(n)\right) > 0.484,$$

and the corollary follows in this case.

Case 3. Assume that n is divisible by 5, but not by 3. Then $\rho(n) < 0.45225 - 1/4 - 1/9 < 0.092$. Here Proposition 4.1(b) with $p = 5$ yields

$$2\left(\frac{(p+1)^2}{4p^2} - \rho(n)\right) = 2\left(\frac{9}{25} - \rho(n)\right) > 0.536,$$

and the corollary follows in this case as well, completing the proof of part (a).

4.2.2. *Proof of Corollary 4.3(b).* Let n be a positive even integer and assume that $B_n(P)$ does not have a primitive divisor. If n is a power of two, then $n \le 4$, so by excluding these values of n in the hypotheses of the corollary, we may assume here that n is not a power of two. We will distinguish two cases.

Case 1. Assume that n is not divisible by either 3 or 5. From (4.11), we have $\rho(n) < 0.45225 - 1/9 - 1/25 < 0.302$.

Here we apply Proposition 4.1(a) and write $n = 2^e N$ with $e \ge 1$ and $N \ge 7$ odd. In this way, we obtain

$$2\left(\frac{1}{3} - \frac{1}{3N^2} - \rho(n)\right) > 0.049,$$

and the corollary follows in this case.

CASE 2. Assume that n is divisible by 3 and not by 5. Then $\rho(n) < 0.41225$. Here we apply Proposition 4.1(b) with $p = 3$, so

$$2\left(\frac{(p+1)^2}{4p^2} - \rho(n)\right) = 2\left(\frac{4}{9} - \rho(n)\right) > 0.064,$$

and the corollary follows in this case.

We have thus completed the proof. ∎

5. Proof of Theorem 1.3

5.1. n divisible by 5

LEMMA 5.1. *Let $P \in E_a(\mathbb{Q})$ be a point of infinite order, and $(B_n) = (B_n(E_a, P))$ an elliptic divisibility sequence. For all positive integers m, B_{5m} has a primitive divisor.*

REMARK 5.2. This technique can be applied for other values than 5, provided that $\psi_n(a, x)$ is reducible over $\mathbb{Q}$ (e.g., $n = 13, 17, \ldots$, but not $n = 7, 11, 19, \ldots$, for which $\psi_n(a, x)$ are irreducible).

Proof of Lemma 5.1. We can handle $m = 1, 2, 3, 4$ and 5 using the arguments in Section 3 of [7] as they readily generalise to our curves.

For $m \geq 6$, we follow the idea of Ingram [7, Lemma 7].

For a point $P = (x, y) \in E_a(\mathbb{Q})$, we can factor $\psi_5(P) = \psi_5(a, x)$, the 5-th division polynomial, as

$$(a^2 + 2ax^2 + 5x^4)(x^8 + 12ax^6 - 26a^2x^4 - 52a^3x^2 + a^4).$$

Writing $x([m]P) = u/v^2$ with $\gcd(u, v) = 1$, we obtain

$$x([5m]P) = \frac{\phi_5(a, u/v^2)}{\psi_5^2(a, u/v^2)},$$

where $\psi_5(a, x)$ is a binary form in a and x^2 of degree 12, while $\phi_5(a, x)$ is x times a binary form in a and x^2 of degree 24. It follows that $v^{50}\phi_5(a, u/v^2)$, $v^{50}\psi_5^2(a, u/v^2) \in \mathbb{Z}$ and

$$B_{5m} = v^{50}\psi_5^2(a, u/v^2)/g,$$

where $g = \gcd(v^{50}\phi_5(a, u/v^2), v^{50}\psi_5^2(a, u/v^2))$.

We can write $v^{25}\psi_5(a, u/v^2) = v f_{5,1}(u^2, v^4) f_{5,2}(u^2, v^4)$, where

$$f_{5,1}(x, y) = x^4 + 12ax^3y - 26a^2x^2y^2 - 52a^3xy^3 + a^4y^4$$

and

$$f_{5,2}(x, y) = 5x^2 + 2axy + a^2y^2.$$

Lower bounds in terms of y. The roots of $f_{5,1}(x, 1)$ are at the points $r_{1,1} = -13.6275\ldots a$, $r_{1,2} = -1.3167\ldots a$, $r_{1,3} = 0.0190\ldots a$ and $r_{1,4} = 2.9252\ldots a$.

The roots of $f_{5,2}(x,1)$ are $r_{2,1}=(-1-2i)a/5$ and $r_{2,2}=(-1+2i)a/5$. Hence $f_{5,2}(x,y)=5(x-r_{2,1}y)(x-r_{2,2}y)$.

For any integers, x and y, with $y\neq 0$, there will be an i and a j such that $|x/y-r_{i,j}|$ is minimal.

Suppose the closest root to $z=x/y$ is either $r_{2,1}$ or $r_{2,2}$. The nearest roots of $f_{5,1}(x,1)$ to $r_{2,1}$ and $r_{2,2}$ are $r_{1,2}$ and $r_{1,3}$, so by solving $(z-(-1.3167a))^2=(z-(-a/5))^2+(2a/5)^2$ and $(z-(0.019a))^2=(z-(-a/5))^2+(2a/5)^2$ respectively for z, we find that x/y must lie between $-0.455a$ and $-0.687a$.

For such x and y,

$$\begin{aligned}&|f_{5,1}(x,y)|\\ &\quad>y^4\,|-0.687a-r_{1,1}|\,|-0.687a-r_{1,2}|\,|-0.455a-r_{1,3}|\,|-0.455a-r_{1,4}|\\ &\quad>13a^4y^4\end{aligned}$$

and

$$|f_{5,2}(x,y)|>5y^2\,|-0.455a-r_{2,1}|\,|-0.455a-r_{2,2}|\,1.125a^2y^2.$$

In this case,

$$|y^{1/4}|\,|f_{5,1}(x,y)|\,|f_{5,2}(x,y)|>14.6a^6|y|^{25/4}.$$

If the closest root to x/y is one of the $r_{1,j}$'s, then $|f_{5,2}(x,y)|\geq 5I_y^2=4a^2y^2/5$ where $I_y=|2ay/5|$ is the absolute value of the imaginary part of $r_{2,1}$ and $r_{2,2}$.

In this case,

$$|y^{1/4}|\,|f_{5,1}(x,y)|\,|f_{5,2}(x,y)|\geq(4/5)a^2|y|^{9/4}>3.8|y|^{9/4}/|a|^{1/4},\tag{5.1}$$

since $|a|\geq 2$ and $|f_{5,1}(x,y)|\geq 1$ here.

Hence this last inequality always holds (including for $y=0$).

Lower bounds in terms of x. The roots of $f_{5,1}(1,y)$ are at the points $s_{1,1}=-0.7594\ldots/a$, $s_{1,2}=-0.0733\ldots/a$, $s_{1,3}=0.3418\ldots/a$ and $s_{1,4}=52.4909\ldots/a$.

And the roots of $f_{5,2}(1,y)$ are $s_{2,1}=(-1-2i)/a$ and $s_{2,2}=(-1+2i)/a$. Hence $f_{5,2}(x,y)=a^2\,(y-s_{2,1}x)\,(y-s_{2,2}x)$.

For any integers, x and y, with $x\neq 0$, there will be an i and a j such that $|y/x-s_{i,j}|$ is minimal.

Suppose the closest root to y/x is either $s_{2,1}$ or $s_{2,2}$. The nearest root of $f_{5,1}(1,y)$ is $s_{1,1}$. By solving $(z-(-0.7594/a))^2=(z-(-1/a))^2+(2/a)^2$ for $z=y/x$, we find that y/x must lie beyond $-9.192/a$.

For such x and y, $|f_{5,2}(x,y)|>71.1x^2$ and $|f_{5,1}(x,y)|>45,200x^4$.

In this case,

$$|y^{1/4}|\,|f_{5,1}(x,y)|\,|f_{5,2}(x,y)|>3.2\cdot 10^6x^6|y^{1/4}|.$$

Since $|y/x| > 9.192/|a|$,

$$|y^{1/4}|\,|f_{5,1}(x,y)|\,|f_{5,2}(x,y)| > 5.5\cdot 10^6|x|^{25/4}/|a|^{1/4}.$$

If the closest root to y/x is one of the $s_{1,j}$'s, then $|f_{5,2}(x,y)| \geq a^2(2/a)^2x^2 = 4x^2$.

If $|y/x| > 0.045/|a|$, then

$$|y^{1/4}|\,|f_{5,1}(x,y)|\,|f_{5,2}(x,y)| > (0.045)^{1/4}|x|^{1/4}/|a|^{1/4}\cdot 4x^2 > 1.83|x|^{9/4}/|a|^{1/4}, \tag{5.2}$$

since $|f_{5,1}(x,y)| \geq 1$.

If $|y/x| \leq 0.045/|a|$, we find that $|f_{5,1}(x,y)| > 0.3145x^4 > 0.374x^4/|a|^{1/4}$ and $|f_{5,2}(x,y)| > 4.912x^2$, so

$$|y^{1/4}|\,|f_{5,1}(x,y)|\,|f_{5,2}(x,y)| > 0.374x^4\cdot 4.912x^2/|a|^{1/4} \geq 1.83x^6/|a|^{1/4}$$

for $|y| \geq 1$ and $|a| \geq 2$.

So (5.2) always holds.

Combining (5.1) and (5.2) with $x = u^2$ and $y = v^4$, we find that

$$\begin{aligned}|v|\,|f_{5,1}(u^2,v^4)|\,|f_{5,2}(u^2,v^4)| &> \min\{1.83|u|^{4.5}/|a|^{1/4}, 3.8|v|^9/|a|^{1/4}\}\\ &\geq 1.83|a|^{-1/4}\min\{|u|^{4.5},|v|^9\}.\end{aligned} \tag{5.3}$$

Hence

$$\log|B_{5m}| > 2\log(1.83) + 9h(u/v^2) - (1/2)\log|a| - \log(g).$$

Next, using the Maple command `gcdex(psi[5]^2,phi[5],x,'s','t');` and factoring the common denominator, we find that this gcd must divide $2^{45}a^{24}$. As in the proof of Lemma 4 of [7], we have $g \mid 2^{45}a^{24}$ and

$$\log|B_{5m}| > 9h(u/v^2) - (49/2)\log|a| - 29.983.$$

From Lemma 2.3,

$$h(mP) = h(u/v^2) \geq 2\widehat{h}(mP) - (1/2)\log|a| - 0.32,$$

so

$$\begin{aligned}\log|B_{5m}| &> 18\widehat{h}(mP) - (9/2)\log|a| - 2.88 - (49/2)\log|a| - 29.983\\ &> 18m^2\widehat{h}(P) - 29\log|a| - 32.863,\end{aligned}$$

since $\widehat{h}(mP) = m^2\widehat{h}(P)$.

From Lemma 3.4 applied with $n = 5$ and using mP here in place of P there, we get

$$\begin{aligned}\log|B_{5m}| &\leq 2\log 5 + 2\widehat{h}(mP) + (1/2)\log|a| + 0.52\\ &< 2m^2\widehat{h}(P) + (1/2)\log|a| + 3.739.\end{aligned}$$

Hence

$$16m^2\widehat{h}(P) \leq (59/2)\log|a| + 36.602. \tag{5.4}$$

Unless $a \equiv 4 \bmod 16$, from Lemma 2.2 we find that

$$\widehat{h}(P) \geq (1/16)\log|a| + (1/4)\log 2. \tag{5.5}$$

Furthermore, if $a \equiv 4 \bmod 16$ and $x(2P) \notin \mathbb{Z}$, then $\delta \geq 2$ if $\mathrm{ord}_2(x(2P)) = 0$ and $\delta \geq 3$ otherwise. In both cases, we find from Proposition 1.1 of [14] that (5.5) holds.

Hence excluding the case of $a \equiv 4 \bmod 16$ and $x(2P) \in \mathbb{Z}$, we have

$$m^2\,(\log|a| + 4\log 2) \leq (59/2)\log|a| + 36.602.$$

For $m \geq 6$, this can never hold.

For $a \equiv 4 \bmod 16$ and $a > 0$, we have

$$m^2\,(\log|a| - 2\log 2) \leq (59/2)\log|a| + 36.602,$$

or

$$|a| < \exp((36.602 + 2m^2\log 2)/(m^2 - (59/2))).$$

For $m \geq 6$, this last inequality is false once $a > \exp(13.31)$ and hence for $a > 604,200$, since the right-hand side is decreasing for $m \geq 6$.

For $a \equiv 4 \bmod 16$ and $a < 0$, we have

$$m^2(\log|a| - \log 2) \leq (59/2)\log|a| + 36.602,$$

or

$$|a| < \exp((36.602 + m^2\log 2)/(m^2 - (59/2))).$$

For $m \geq 6$, this last inequality is false once $|a| > \exp(9.471)$ and hence for $|a| > 13,000$, since the right-hand side is decreasing for $m \geq 6$.

For $m \geq 7$, the required inequalities hold for $a < -37$ and $a > 213$.

Search. For each of the remaining values of a with $a \equiv 4 \bmod 16$, we use PARI to search for possible counterexamples to our lemma.

We search for any points, P, with $x(2P) \in \mathbb{Z}$, satisfying (5.4) for $m = 6$ and then check to ensure that $B_{30}(P)$ always has a primitive divisor for such points.

Using Lemma 2.3 and since $\widehat{h}(2P) = 4\widehat{h}(P)$, we require

$$\begin{aligned} h(2P) = \log|x(2P)| &\leq 2\left((1/4)\log|a| + 0.26 + 4\frac{29.5\log|a| + 36.602}{16\cdot 36}\right) \\ &< 0.91\log|a| + 1.03. \end{aligned}$$

Furthermore, $x(2P)$ must be a square by Lemma 6.1(a) of [14].

In this way, we were able to check all the remaining values in 4 minutes using PARI on an ordinary laptop. We found 29 pairs (a, P) such that (5.4) holds and a is fourth-power-free (6 with $-9996 \leq a \leq -12$ and 23 with $180 \leq a \leq 515\,508$).

For all of them, $B_{30}(P)$ has a primitive divisor. This completes the proof for $m = 6$.

Since the left-hand side of (5.4) is increasing in m, any pair (a, P) satisfying (5.4) for $m > 6$, must be among these 29 examples. As we noted above, we must have $-37 \le a \le 213$ if $B_{5m}(P)$ does not have a primitive divisor for $m > 6$, so this leaves only $a = -12, 180$.

For $a = -12$, the point is $P = (-2, 4)$ and $\widehat{h}(P) = 0.1252\ldots$. For $m \ge 8$, (5.4) is no longer satisfied in this case and we check that $B_{35}(P)$ has a primitive divisor.

For $a = 180$, the point is $P = (-6, 36)$ with $\widehat{h}(P) = 0.2564\ldots$. We proceed in the same way for this case. ∎

5.2. n **odd,** $n > 7$**.** Let n be a positive odd integer and assume that either $x(P)$ is a rational square or $x(P) < 0$. Suppose that the term $B_n(P)$ does not have a primitive divisor.

5.2.1. $x(P) < 0$. This only occurs for $a < 0$. In this case, $E_a(\mathbb{R})$ has two components and we are considering points, P, on the non-identity component of $E_a(\mathbb{R})$.

Remark 5.3. Since Lemma 3.4 applies for any elliptic curve and since we can obtain results like Lemma 2.3 for any elliptic curve (see, for example, Proposition 5.18(a) and Theorem 5.35(c) of [9]), if E is an elliptic curve such that $E(\mathbb{R})$ has two components and if we have an explicit version of Lang's conjecture for $E(\mathbb{Q})$, then the same idea can be applied to bound from above the odd indices n, such that B_n has no primitive divisor when P is on the non-identity component of $E(\mathbb{R})$.

If $B_n \ge |A_n|$, then

$$\log B_n = h(x(nP)) \ge 2\widehat{h}(nP) - \frac{1}{2}\log|a| - 0.32 \tag{5.6}$$
$$= 2n^2\widehat{h}(P) - \frac{1}{2}\log|a| - 0.32,$$

from Lemma 2.3.

If $B_n < |A_n|$, then

$$-\sqrt{|a|} \le x(nP) < 0,$$

since $x(P) < 0$ and n odd implies $x(nP) < 0$.

Thus $|A_n/B_n| \le \sqrt{|a|}$, so

$$\log|A_n| - \frac{1}{2}\log|a| \le \log B_n.$$

Therefore, from Lemma 2.3,

$$\log B_n > h(x(nP)) - \frac{1}{2}\log|a| \ge 2n^2\widehat{h}(P) - \log|a| - 0.32. \tag{5.7}$$

Since this lower bound is weaker than (5.6), we shall use it in what follows.

Applying Lemma 3.4, we have

$$2n^2(1-\rho(n))\widehat{h}(P) < \eta(n) + \omega(n)K + \log|a| + 0.32. \tag{5.8}$$

From Lemma 2.2,

$$\frac{n^2}{8}(1-\rho(n))(\log|a| - 2\log 2) < \eta(n) + \omega(n)K + \log|a| + 0.32.$$

For $|a| \geq 8$,

$$\frac{1}{\log|a| - 2\log 2} < 1.443, \qquad \frac{K}{\log|a| - 2\log 2} < 2.251,$$
$$\frac{\log|a| + 0.32}{\log|a| - 2\log 2} < 3.462.$$

Hence,

$$\frac{n^2}{8}(1-\rho(n)) < 1.443\eta(n) + 2.251\omega(n) + 3.462. \tag{5.9}$$

Since n is odd, from (4.11), $\rho(n) < 0.20225$ and applying (4.10)

$$0.0997n^2 < 2.886\log n + 3.116\frac{\log n}{\log\log n} + 3.462.$$

Using this inequality, we obtain the bound $n < 14.01$, so $n \leq 13$. We can directly calculate both sides of (5.9) and find that it fails for $n = 9$ and $n = 11$, proving our desired result for $|a| \geq 8$.

Using PARI, we find that for $-8 < a < 0$, $E_a(\mathbb{Q})$ is non-trivial only for $a = -2, -5, -6$ and -7. Each of these is of rank 1 and the generator, P, satisfies $\widehat{h}(P) \geq 0.3043\ldots$ (attained for $a = -2$). Applying this lower bound for the height and $\rho(n) < 0.20225$ to (5.8), we find that

$$0.485n^2 > 2\log n + 2.16\frac{\log n}{\log\log n} + 2.4 > 2\log n + \omega(n)K + \log|a| + 0.32$$

for $-8 \leq a \leq -2$ and $n > 5.2$, as required.

NOTE. Recall that the height function, `ellheight`, in PARI returns a value that is twice our height here.

5.2.2. *$x(P)$, a rational square.* From Lemma 2.2, we have

$$\widehat{h}(P) \geq \frac{1}{16}\log|a| - \frac{1}{8}\log 2. \tag{5.10}$$

Assume further that $|a| \geq 33$. Then

$$\frac{1}{\log|a| - 2\log 2} < 0.474, \qquad \frac{K}{\log|a| - 2\log 2} < 1.075,$$
$$\frac{L}{\log|a| - 2\log 2} < 0.981. \tag{5.11}$$

Substituting (5.10) into Corollary 4.3(a) shows that

$$0.484\left(\frac{1}{16}\log|a|-\frac{1}{8}\log 2\right)n^2<2\log n+\frac{1.3841\log n}{\log\log n}K+K+L$$

must hold if $B_n(P)$ does not have a primitive divisor.

Dividing both sides of this equation by $\log|a|-2\log 2$ and substituting the estimates (5.11) yields

$$\begin{aligned}0.030n^2&<0.948\log n+1.075\frac{1.3841\log n}{\log\log n}+2.056\\&<(\log n)\left(0.948+\frac{1.488}{\log\log n}\right)+2.056.\end{aligned}$$

Using this inequality, we obtain the bound $n<17.13$, so $n\le 17$, if $B_n(P)$ does not have a primitive divisor.

We will next give the better bounds by using the inequalities of Proposition 4.1(b).

If n is odd and divisible by p, then, by Proposition 4.1(b), (5.10) and (5.11),

$$\begin{aligned}0<\frac{1}{8}\left(\frac{(p+1)^2}{4p^2}-\rho(n)\right)n^2&\le\frac{\eta(n)+\omega(n)K+L}{\log|a|-2\log 2}\\&<0.474\eta(n)+1.075\omega(n)+0.981.\end{aligned}$$

Using this inequality, we can eliminate $n=9$, 11, 13, 15 and 17 (with $p=3$, 11, 13, 3 and 17, respectively) for $|a|\ge 33$.

Next using Lemma 2.3, if $x(P)$ is a rational square and $\widehat{h}(P)\le(\log|a|)/4$, then $h(P)\le(1/2)\log|a|+(1/2)\log|a|+0.52=\log|a|+0.52$. That is, writing $x(P)=r/s$, $\max(|r|,|s|)<1.7|a|$. Using this bound on $x(P)$ we can enumerate all points with $x(P)$ a rational square, $\widehat{h}(P)\le(\log|a|)/4$ and $|a|\le 32$ (in PARI, say):

Table 1

a	P	$\widehat{h}(P)$
-12	$(4,\pm 4)$	$0.5011\ldots$
3	$(1,\pm 2)$	$0.2505\ldots$
15	$(1,\pm 4)$	$0.5673\ldots$
20	$(4,\pm 12)$	$0.6355\ldots$

Repeating the above arguments with $|a|\ge 2$ (noting the $E_{-1}(\mathbb{Q})$ and $E_1(\mathbb{Q})$ contain only torsion points) and $\widehat{h}(P)\ge(\log|a|)/4$, we obtain

$$0.12n^2<(\log n)\left(2.886+\frac{1.732}{\log\log n}\right)+2.213$$

from Corollary 4.3(a), and

$$0 < \frac{1}{2}\left(\frac{(p+1)^2}{4p^2} - \rho(n)\right) n^2 < 1.443\eta(n) + 1.251\omega(n) + 0.962$$

from Proposition 4.1(b).

From the first of these inequalities, we find that $n < 10.8$ and so $n \leq 9$ for all a and $P \in E_a(\mathbb{Q})$ with $|a| \geq 2$ and $\widehat{h}(P) \geq (\log|a|)/4$. The second inequality allows us to eliminate $n = 9$. Hence we find that $n \leq 7$ for all elliptic divisibility sequences such that $B_n(P)$ does not have a primitive divisor, with the exception of those generated by the 8 points, P, in Table 1.

Substituting $a = 3$ and $\widehat{h}(P) = 0.2505\ldots$ into the inequality in Corollary 4.3(a), we find that

$$0.484n^2 < \left(7.984 + \frac{5.912}{\log\log n}\right)\log n + 7.744.$$

Using this inequality, we find that $n \leq 9$. For $n = 9$, we use Proposition 4.1(b) with $p = 3$. The left-hand side exceeds the right-hand side, and so we can eliminate $n = 9$ too.

We proceed in the same way for $a = -12$ and 15 and 20.

This completes the proof for n odd.

5.3. n **even,** $n \geq 20$**.** Let n be a positive even integer and not a power of two. Assume that $B_n(P)$ does not have a primitive divisor.

We suppose that $|a| \geq 384$. Then

$$\frac{1}{\log|a| - 2\log 2} < 0.22, \qquad \frac{K}{\log|a| - 2\log 2} < 0.766, \qquad \frac{L}{\log|a| - 2\log 2} < 0.722. \tag{5.12}$$

From (5.10), (5.12) and using the same argument as for n odd, with Corollary 4.3(b), we have

$$0.003n^2 < \left(0.44 + \frac{1.061}{\log\log n}\right)\log n + 0.722.$$

By using this inequality, we obtain the bound $n < 42.4$, so $n \leq 42$.

From Proposition 4.1(a), (5.10) and (5.12), we have

$$\frac{1}{8}\left(\frac{1}{3} - \frac{1}{3N^2} - \rho(n)\right) n^2 < 0.22\eta(n) + 0.766\omega(n) + 1.488.$$

Using this inequality, we obtain $n \leq 20$ or $n = 24$, 30, 32, 36, 42, for $|a| \geq 384$. Furthermore, recall that we need not consider $n = 30$, since we have already eliminated those n divisible by 5.

Applying Proposition 4.1(b), (5.10) and (5.12), we have

$$\frac{1}{8}\left(\frac{(p+1)^2}{4p^2}-\rho(n)\right)n^2 < 0.22\eta(n)+0.766\omega(n)+0.722.$$

Using this inequality for the remaining values of n, we obtain $n < 20$ for $|a| \geq 384$ ($n \leq 14$, in fact).

Now assume that $-384 < a < 384$. Again, we can proceed as in the case of n odd. First, we use Corollary 4.3(b), Proposition 4.1(a) and Proposition 4.1(b) to shows that if $B_n(P)$ has no primitive divisor, then $n \leq 20$ for $|a| \geq 2$ and $\widehat{h}(P) \geq (\log|a|)/4$.

Then we use Lemma 2.3 to find all points on $E_a(\mathbb{Q})$ with $|a| \leq 384$ and $0 < \widehat{h}(P) \leq (\log|a|)/4$ and calculate $B_n(P)$ until the inequality in Corollary 4.3(b) is no longer satisfied. Using PARI, 410 such points, P, were found. Typically, we needed to check $B_n(P)$ for n up to $20-25$, although for $a=-12$, the search had to continue to $n=52$. The entire calculation took 11 minutes on an ordinary laptop.

5.4. $n = 3$**.** As mentioned in the proof of Lemma 3.5, from the arguments on pages 92–93 of [13], we can write $P = \left(b_1M^2/e^2, b_1MN/e^3\right)$ in lowest terms. By the duplication formula, we have

$$x(2P) = \frac{(2b_1M^4-N^2)^2}{4M^2N^2e^2}.$$

$x(P)$ is a square. Applying Lemma 3.5(a) with $m=2$ and $n=1$, we have

$$0 < (A_2B_1 - A_1B_2)^2 \leq B_1B_3. \tag{5.13}$$

Since $B_1 \mid B_2$, we can write $B_2 = k^2B_1$ for some integer $k \geq 1$. Substituting this expression into (5.13), we obtain

$$0 < B_1(A_2 - k^2A_1)^2 \leq B_3. \tag{5.14}$$

If $|A_2 - k^2A_1| > 3$, then from (5.14), this implies that $B_3 > 3^2B_1$ holds. Therefore from Lemma 3.3, B_3 has a primitive divisor.

Assume that $|A_2 - k^2A_1| \leq 3$. Then writing $A_1 = a_1^2$ and $A_2 = a_2^2$ with $a_1, a_2 \geq 1$, we have

$$|A_2 - k^2A_1| = |(a_2 - ka_1)(a_2 + ka_1)| \leq 3. \tag{5.15}$$

From Lemma 6.1(c) of [14], we have $\mathrm{ord}_2(B_2) \geq \mathrm{ord}_2(B_1) + 2$ and so $k \geq 2$. By the left-hand inequality of (5.14), $a_2 \neq ka_1$ and so $a_2 + ka_1 \leq 3$. Together, these two statements imply that $a_1 = a_2 = 1$ and $k = 2$. Since $A_1 = 1$ and $\gcd(b_1, e) = \gcd(M, e) = 1$, it follows that $b_1 = M = \pm 1$ and so $P = (1/e^2, \pm N/e^3)$. Therefore, $x(2P) = (\pm 2 - N^2)^2/(4N^2e^2) = 1/\left(4e^2\right)$, since $A_2 = 1$ and $B_2 = k^2B_1 = 4e^2$. Hence, $N = \pm 1, \pm 2$.

If $N = \pm 1$, then $P = (1/e^2, \pm 1/e^3)$, which is impossible. Next assume that $N = \pm 2$. Then $P = \left(1/e^2, \pm 2/e^3\right)$. Substituting $x = 1/e^2$ and $y = \pm 2/e^3$ into $y^2 = x^3 + ax$, we obtain $a = 3$ and $e = \pm 1$. That is, $P = (1, \pm 2)$. In this case, $B_2 = 4$ and $B_3 = 9$. Thus B_3 has a primitive divisor.

$x(P) < 0$. Applying Lemma 3.5(b) with $m = 2$ and $n = 1$, we have

$$0 < (A_2B_1 - A_1B_2)^2 \le 4B_1B_3.$$

Once again we can write $B_2 = k^2B_1$ for some integer $k \ge 1$ and we have

$$0 < B_1(A_2 - k^2A_1)^2 \le 4B_3.$$

In fact, from Lemma 3.5(a), we have

$$0 < B_1(A_2 - k^2A_1)^2 \le B_3,$$

unless $a \equiv 4 \bmod 16$ and $\mathrm{ord}_2(x(P)) = 1$.

If $|A_2 - k^2A_1| > 6$, then $B_3 > 3^2B_1$ holds. Therefore from Lemma 3.3, B_3 has a primitive divisor.

Assume that $|A_2 - k^2A_1| \le 6$ with $2 \parallel A_1$ or $|A_2 - k^2A_1| \le 3$ otherwise. Since $A_1 < 0$ and A_2 is a square, we have $(A_1, A_2, k) = (-2, 4, 1)$, $(-2, 1, 1)$ or $(-1, 1, 1)$.

In the first case, $b_1 = -2$ and $M = \pm 1$, so $P = (-2/e^2, \pm 2N/e^3)$. Therefore, $x(2P) = (-4 - N^2)^2/(4N^2e^2) = 4/e^2$ since $A_2 = 4$ and $B_2 = k^2B_1 = e^2$. Hence $(-4 - N^2)/(2N) = \pm 2$, that is $N = \pm 2$ and so $P = (-2/e^2, \pm 4/e^3)$. In order for P to be on the curve E_a, $a = -12/e^4$. This implies that $e = \pm 1$ and $a = -12$. In this case, $B_1 = B_2 = 1$ and $B_3 = 3$, so B_3 has a primitive divisor.

In the second case (i.e., $(A_1, A_2, k) = (-2, 1, 1)$), once again we have $x(2P) = (-4 - N^2)^2/(4N^2e^2)$ and $B_2 = k^2B_1 = e^2$. Since $A_2 = 1$, $x(2P) = 1/e^2$, so $(-4 - N^2)/(2N) = \pm 1$. There are no such rational N and hence this case is impossible too.

Lastly, we consider $(A_1, A_2, k) = (-1, 1, 1)$. Here we have $b_1 = -1$ and $M = \pm 1$, so $P = (-1/e^2, \pm N/e^3)$. Therefore, $x(2P) = (-2 - N^2)^2/(4N^2e^2) = 1/e^2$ since $A_2 = 1$ and $B_2 = k^2B_1 = e^2$. Hence $(-2 - N^2)/(2N) = \pm 1$. There are no such rational N and hence this case is impossible too.

Thus B_3 always has a primitive divisor in this case too.

5.5. $4 \le n \le 20$**.** In Section 2 of [7], Ingram showed that there are no solutions for $n = 5$ and 7. In Section 3 of the same paper, he proves the same for $n = 4$, 6, 10, 12, 14, 18 and 20, provided that $a = -N^2$. However, writing $x(P) = A/B^2$ and setting $X = A^2/(A^2, a)$ and $Y = aB^4/(A^2, a)$, rather than Ingram's values, we find that the polynomials, Ψ_n, are still reducible (although not always with as many factors as in the $a = -N^2$ case). Hence his same arguments hold (basically, for each of the possible values of the

factors use a reduction technique to eliminate one of the variables and then factor the resulting single-variable polynomial to solve for X).

One can easily show that if $B_n(E,P)$ has no primitive divisor, then neither does $B_{\mathrm{rad}(n)}(E,(n/\mathrm{rad}(n))P)$.

This completes the proof.

Lastly, note that the results for these values of n hold without any conditions on $x(P)$ and thus provide evidence for our claim in Remark 1.5.

References

[1] Yu. Bilu, G. Hanrot and P. M. Voutier (with an appendix by M. Mignotte), *Existence of primitive divisor of Lucas and Lehmer numbers*, J. Reine Angew. Math. 539 (2001), 75–122.

[2] R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. of Math. 15 (1913), 30–70.

[3] J. E. Cremona, M. Prickett and S. Siksek, *Height difference bounds for elliptic curves over number fields*, J. Number Theory 116 (2006), 42–68.

[4] L. K. Durst, *Exceptional real Lehmer sequences*, Pacific J. Math. 9 (1959), 437–441.

[5] G. Everest, G. Mclaren and T. Ward, *Primitive divisors of elliptic divisibility sequences*, J. Number Theory 118 (2006), 71–89.

[6] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, *Recurrence Sequences*, Math. Surveys Monogr. 104, Amer. Math. Soc., Providence, RI, 2003.

[7] P. Ingram, *Elliptic divisibility sequences over certain curves*, J. Number Theory 123 (2007), 473–486.

[8] G. Robin, *Estimation de la fonction de Tchebychef* θ *sur le* k*-ième nombre premier et grandes valeurs de la fonction* $\omega(n)$ *nombre de diviseurs premiers de* n, Acta Arith. 42 (1983), 367–389.

[9] S. Schmitt and H. G. Zimmer (with an appendix by A. Pethő), *Elliptic Curves: A Computational Approach*, de Gruyter Stud. Math. 31, de Gruyter, Berlin, 2003.

[10] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, New York, 1986.

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

[12] —, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, New York, 1994.

[13] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Undergrad. Texts in Math., Springer, New York, 1992.

[14] P. Voutier and M. Yabuta, *Lang's conjecture and sharp height estimates for the elliptic curves* $y^2 = x^3 + ax$, submitted.

[15] M. Ward, *Memoir on elliptic divisibility sequences*, Amer. J. Math. 70 (1948), 31–74.

[16] —, *The intrinsic divisors of Lehmer numbers*, Ann. of Math. (2) 62 (1955), 230–236.

[17] M. Yabuta, *Primitive divisors of certain elliptic divisibility sequences*, Experiment. Math. 18 (2009), 303–310.

[18] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. 3 (1892), 265–284.

Paul Voutier
London, UK
E-mail: paul.voutier@gmail.com

Minoru Yabuta
Senri High School
17-1, 2 chome, Takanodai, Suita
Osaka, 565-0861, Japan
E-mail: yabutam@senri.osaka-c.ed.jp
rinri216@msf.biglobe.ne.jp

Received on 4.9.2010
and in revised form on 21.5.2011 (6482)