PRIMITIVE DIVISORS OF CERTAIN ELLIPTIC DIVISIBILITY SEQUENCES

PAUL VOUTIER AND MINORU YABUTA

Abstract. We establish conditions necessary for the n-th element of any elliptic divisibility sequence generated by points on $E_a : y^2 = x^3 + ax$ to not have a primitive divisor. As a consequence of this, along with our explicit and uniform version of Lang's conjecture for the relevant curves, we show that if $a < 0$ and fourth-power-free and $n > 3$, then n-th element of any such elliptic divisibility sequence always has a primitive divisor.

1. Introduction

A sequence $C = (C_n)_{n \geq 1}$ is called a *divisibility sequence* if $C_m | C_n$ whenever $m|n$. 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 [20] 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 [3] showed that if $n > 12$ then the n-th term of any Lucas sequence has a primitive divisor in the case of positive discriminant. Ward [17] and Durst [5] extended Carmichael's result to Lehmer sequences. In 2001, Bilu, Hanrot and Voutier [1] proved that if $n > 30$ then every n-th 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 and Voutier are all best possible (in the sense that for $n = 6$, $n = 12$ and $n = 30$, respectively, sequences whose n-th 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

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

Key words and phrases. Elliptic curve, Elliptic divisibility sequence, Primitive divisor, Canonical height.

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 known as an *elliptic divisibility sequence.*

Ward [16] first studied the arithmetic properties of elliptic divisibility sequences. Silverman [12] 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 [6] 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 [6]). *With $E : y^2 = x^3 - T^2x$ 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 [6] 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 $n \leq 2$.

The purpose of this paper is obtain results on the existence of primitive divisors in the more general case of $E_a : y^2 = x^3 + ax$ with $a \in \mathbb{Z}$, fourth-power-free.

In the case of $a < 0$, we use the ideas in [6], along with our explicit version of Lang's conjecture for such curves to prove that for $n > 3$, the n-th element of any such elliptic divisibility sequence always has a primitive divisor.

2. Results

Denote by h the absolute logarithmic height on $\mathbb{Q}$ and by $\widehat{h}$ the canonical height on $E(\mathbb{Q})$, for an elliptic curve $E/\mathbb{Q}$.

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

Further, we define

$$\rho(n) = \sum_{p|n} p^{-2} \quad \text{and} \quad \eta(n) = 2\sum_{p|n} \log p, \tag{2.1}$$

where the sums range over all prime divisors of n. We set the following notation:

$$K = \frac{1}{2}\log|a| + 2.542 \quad \text{and} \quad L = \frac{1}{2}\log|a| + 1.040. \tag{2.2}$$

In the remainder of this work, 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.

Then we obtain the following theorem.

Theorem 2.1. *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*

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

(c) *Suppose $a < 0$. If n is even and divisible by an odd prime, p, then*

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

Remark 2.2. Note the condition that the left-hand sides of these inequalities must be positive. This is the reason for the inclusion of part (c). If the positivity condition prevents our use of parts (a) or (b), then the conditions of part (c) will be satisfied.

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

Corollary 2.3. *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*

$$0.482\widehat{h}(P)n^2 < 2\log(n) + \frac{1.3841\log(n)}{\log\log(n)}K + K + L.$$

(b) *Suppose $a < 0$. Let n be a positive even integer. If $B_n(P)$ does not have a primitive divisor, then either $n \leq 4$ or n is not a power of 2 and*

$$0.039\hat{h}(P)n^2 < 2\log(n) + \frac{1.3841\log(n)}{\log\log(n)}K + 2L + \log(|a|).$$

Remark 2.4. We can obtain a version of part (b) for $a > 0$ as well, subject to $\rho(n) < 4/9$.

Applied to $\mathbb{Q}$, Lang's conjecture states that

$$\widehat{h}(P) \geq C_1 \log|\Delta(E)| - C_2$$

holds for any elliptic curve $E/\mathbb{Q}$ and any point $P \in E(\mathbb{Q})$ of infinite order, where $\Delta(E)$ denotes the discriminant of the curve E and $C_1 > 0$ and C_2 are absolute constants. Silverman [9] showed that Lang's conjecture holds for any elliptic curve with integral j-invariant (note that this includes our curves, E_a, since their j-invariant is 1728), but provided no explicit evaluation of the constants.

We provide an explicit version for E_a here for $a < 0$.

Proposition 2.5. *Let a be a negative fourth-power-free integer. Let $P \in E_a(\mathbb{Q})$ be a nontorsion point. Denote by $\widehat{h}$ the canonical height on E_a. Then*

$$\widehat{h}(P) \geq \frac{1}{16}\log(|a|) + \begin{cases} \dfrac{1}{16}\log(2) & \text{if } a \not\equiv 4 \bmod 16 \\ -\dfrac{1}{16}\log(2) & \text{if } a \equiv 4 \bmod 16. \end{cases} \tag{2.3}$$

Using these estimates, we obtain a uniform and explicit bound such that for n exceeding this bound, the n-th element of elliptic divisibility sequences obtained from E_a always has a primitive divisor.

Theorem 2.6. *Let a be a negative integer which is fourth power free. 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 n is even or if n is odd and $x(P)$ is a rational square, then $n \leq 3$.

It is easy to show that there are infinitely many values of a and points $P \in E_a(\mathbb{Q})$ such that $x([3]P)$ is an integer (i.e., $B_3(P) = 1$), so this theorem is best-possible. E.g.,

a	P	a	P
-2	$(2,2)$	28	$(2,8)$
-12	$(6,12)$	180	$(6,36)$
-420	$(30,120)$	5850	$(30,450)$

From calculations performed using Ingram's ideas in [7], it appears that Theorem 2.6 is also true for $a > 0$ and without any conditions on $x(P)$.

3. Preliminary Lemmas

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 [6]. □

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 [6]. □

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

$$\log(B_n) \leq 2 \sum_{p|n} \log(p) + \sum_{p|n} \log\left(B_{n/p}\right). \tag{3.1}$$

Here the sums range over prime divisors of n.

Proof. This is the first part of Lemma 3.3 of [6]. □

For a rational number s/t in lowest terms, we define the *logarithmic height* by $h(s/t) = \log \max\{|s|, |t|\}$. For a rational point $P \in E(\mathbb{Q})$, we define the *logarithmic height* of P by $h(P) = h(x(P))$, and the *canonical height* of P by

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

Let $E/\mathbb{K}$ be an elliptic curve in long Weierstrass form over the number field $\mathbb{K}$,

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

We define as usual

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2, \\
b_4 &= 2a_4 + a_1a_3, \\
b_6 &= a_3^2 + 4a_6, \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.
\end{aligned}$$

Let $M_{\mathbb{K}}$ be the set of valuations of $\mathbb{K}$ and for $v \in M_{\mathbb{K}}$, let n_v be the local degree at v. For $x \in \mathbb{K}$ and $v \in M_{\mathbb{K}}$, we define $v(x) = -\log |x|_v$. Let

$$\begin{aligned}
\lambda_v &= \min\left\{ v\left(b_2\right), \frac{1}{2}v\left(b_4\right), \frac{1}{3}v\left(b_6\right), \frac{1}{4}v\left(b_8\right) \right\}, \\
\lambda &= \frac{-1}{[\mathbb{K} : \mathbb{Q}]} \sum_{v \in M_{\mathbb{K}}} n_v\lambda_v.
\end{aligned}$$

Lemma 3.4 (Zimmer [19]). *Let $E/\mathbb{K}$ be an elliptic curve in long Weierstrass form over the number field $\mathbb{K}$. Let h and $\widehat{h}$ be the logarithmic height and the canonical height on $E/\mathbb{K}$ respectively. Then for all points $P \in E(\mathbb{K})$,*

$$\begin{aligned}
&\frac{1}{2[\mathbb{K} : \mathbb{Q}]} \sum_{v \in M_{\mathbb{K}}} n_v \min\{0, \lambda_v\} - \frac{1}{2}\log(2) \\
\leq\ & \frac{1}{2}h(P) - \widehat{h}(P) \leq \frac{1}{2[\mathbb{K} : \mathbb{Q}]} \sum_{v \in M_{\mathbb{K}}} n_v \max\{0, \lambda_v\} + \lambda + \frac{4}{3}\log(2).
\end{aligned}$$

We now apply this theorem to E_a.

Lemma 3.5. *For all points $P \in E_a(\mathbb{Q})$,*

$$-\frac{1}{4}\log|a| - 0.520 \leq \frac{1}{2}h(P) - \widehat{h}(P) \leq \frac{1}{4}\log|a| + 1.271.$$

Proof. If v is an archimedean absolute value, then

$$\lambda_v = \frac{1}{2} v\left(b_4\right) = -\frac{1}{2}\log(2) - \frac{1}{2}\log|a|.$$

If v is a non-archimedean absolute value, then

$$\lambda_v = \frac{1}{4} v\left(b_8\right) = -\frac{1}{2}\log|a|_v.$$

Since $n_v = 1$ for all $v \in M_{\mathbb{Q}}$, we have

$$\lambda = -\sum_{v \in M_{\mathbb{Q}}} \lambda_v = \frac{1}{2}\log(2).$$

Substituting these values into Zimmer's result, we obtain

$$-\frac{1}{4}\log|a| - \frac{3}{4}\log(2) \leq \frac{1}{2}h(P) - \widehat{h}(P) \leq \frac{1}{4}\log|a| + \frac{11}{6}\log(2).$$

Thus we obtain the lemma. □

Lemma 3.6. *If the term B_n does not have a primitive divisor, then*

$$\begin{aligned} \log\left(B_n\right) &\leq 2\sum_{p \mid n}\log(p) + \sum_{p \mid n}\left(2\left(\frac{n}{p}\right)^2 \widehat{h}(P) + K\right) \qquad (3.2)\\ &= \eta(n) + 2n^2\rho(n)\widehat{h}(P) + \omega(n)K. \end{aligned}$$

Here the inequality (3.2) is analogous to the inequality (9) of [6].

Proof. Recalling that $K = (1/2)\log|a| + 2.542$, Lemma 3.5 implies that for any prime divisor p of n,

$$\begin{aligned} \log\left(B_{n/p}\right) &\leq h\left(\frac{n}{p}P\right)\\ &\leq 2\widehat{h}\left(\frac{n}{p}P\right) + K = 2\left(\frac{n}{p}\right)^2 \widehat{h}(P) + K. \qquad (3.3) \end{aligned}$$

The last equality is a property of the canonical height (see Theorem 9.3 of [10]). Combining (3.1) and (3.3), we obtain the lemma. □

Lemma 3.7. *Let $P \in E_a(\mathbb{Q})$ be a point of infinite order.*
(a) *Let $x(P) = uv^2$ with $u \in \mathbb{Z}$ square-free and $v \in \mathbb{Q}$. If n is even, then $x(nP)$ is a rational square. If n is odd, then $x(nP) = uw^2$ for some $w \in \mathbb{Q}$.*
(b) *Suppose $x(P) = A_1/B_1$ is a rational square. Writing $x(2P) = A_2/B_2$ in lowest terms, we have* $\operatorname{ord}_2\left(B_2\right) > \operatorname{ord}_2\left(B_1\right)$.

Proof. (a) Let $\mathbb{Q}^*$ be the multiplicative group of non-zero rational numbers, and let $\mathbb{Q}^{*2}$ denote the subgroup of squares of elements of $\mathbb{Q}^*$. We define a map α from $E(\mathbb{Q})$ to $\mathbb{Q}^*/\mathbb{Q}^{*2}$ by

$$\begin{aligned}&\alpha(\mathcal{O}) = 1,\ \alpha((0,0)) = a,\\ &\alpha((x,y)) = s \quad \text{if } x = st^2 \text{ with } s \text{ square-free},\end{aligned}$$

where $\mathcal{O}$ is the zero element in $E(\mathbb{Q})$. Then α is homomorphism (see p.85 [14]). Let $x(P) = uv^2$ with $u \in \mathbb{Z}$ square-free and $v \in \mathbb{Q}$. Then

$$\begin{aligned}\alpha(2P) &= \alpha(P+P) = \alpha(P)^2 = 1,\\ \alpha(3P) &= \alpha(2P+P) = \alpha(2P)\alpha(P) = u.\end{aligned}$$

Using induction shows that if n is even, then $\alpha(nP) = 1$, and if n is odd then $\alpha(nP) = u$. Therefore, if n is even, then $x(nP)$ is a rational square, and if n is odd, then $x(nP) = uw^2$ for some $w \in \mathbb{Q}$.

(b) Since $x(P)$ is a rational square, we can write $P = (b_1^2M^2/e^2, b_1^2MN/e^3)$ in lowest terms, where $a = b_1^2b_2$ with $\gcd(M,N) = \gcd(e,N) = 1$ (see [14], p. 93).

Suppose a prime p divides both b_1 and N. Since a is fourth power free, we observe that $p^2 \| b_1^2$. Since $P \in E_a(\mathbb{Q})$, we can write $N^2 = b_1^2M^4 + b_2e^4$. As $\gcd(e,N) = 1$, it follows that $p^2 | b_2$, therefore p^4 divides a, which contradicts the assumption that a is fourth power free. Hence $\gcd(b_1,N) = 1$.

For any $Q = (x,y)$, by the duplication formula, we have

$$x(2Q) = \frac{(x^2-a)^2}{4y^2} = \frac{(2x^3-y^2)^2}{4x^2y^2}.$$

Applying that with the expression we just found for P we have, we obtain

$$x(2P) = \frac{(b_1^2M^4 - b_2e^4)^2}{4M^2N^2e^2} = \frac{(2b_1^2M^4 - N^2)^2}{4M^2N^2e^2}.$$

If N is odd, then $2b_1^2M^4 - N^2$ is odd and so $\mathrm{ord}_2(B_2) > \mathrm{ord}_2(e^2) = \mathrm{ord}_2(B_1)$. If N is even, then $b_1^2M^4$ is odd, since we saw that $\gcd(b_1,N) = \gcd(M,N) = 1$. Hence, $2^2 \| (2b_1^2M^4 - N^2)^2$, but $2^3 | 4M^2N^2$. So, in this case too, $\mathrm{ord}_2(B_2) > \mathrm{ord}_2(e^2) = \mathrm{ord}_2(B_1)$. □

Lemma 3.8. *Let $P \in E_a(\mathbb{Q})$ be any point of infinite order. Let m and n be positive integers and write $x(mP) = A_m/B_m$, $x(nP) = A_n/B_n$ in lowest terms. If m is even, n is odd and $x(P)$ is a rational square or if m and n*

are both even with $\operatorname{ord}_2(m) > \operatorname{ord}_2(n) > 0$, *then*

$$0 < (A_m B_n - A_n B_m)^2 \leq B_{m+n} B_{|m-n|}. \tag{3.4}$$

Proof. Since P is of infinite order, $x(mP) \neq x(nP)$ and hence $A_m B_n - A_n B_m \neq 0$.

Assume that either m is even, n is odd and $x(P)$ is a rational square or that m and n are both even with $\operatorname{ord}_2(m) > \operatorname{ord}_2(n) > 0$. Write

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

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

$$x(|m \pm n|P) = \left(\frac{y_m \mp y_n}{x_m - x_n} \right)^2 - x_m - x_n \tag{3.5}$$

$$= \frac{\left(C_m B_n^{3/2} \mp C_n B_m^{3/2} \right)^2}{B_m B_n \left(A_m B_n - A_n B_m \right)^2} - \frac{A_m B_n + A_n B_m}{B_m B_n}. \tag{3.6}$$

Substituting $y_m = x_m^3 + a x_m$ and $y_n = x_n^3 + a x_n$ into (3.5), we have

$$\begin{aligned} & x((m+n)P) x(|m-n|P) \\ = & \frac{\left((x_m + x_n)(x_m + x_n + a) - 2 y_m y_n \right) \left((x_m + x_n)(x_m + x_n + a) + 2 y_m y_n \right)}{(x_m - x_n)^4} \\ = & \frac{(x_m + x_n)^2 (x_m + x_n + a)^2 - 4 \left(x_m^3 + a x_m \right) \left(x_n^3 + a x_n \right)}{(x_m - x_n)^4} \\ = & \frac{(x_m x_n - a)^2}{(x_m - x_n)^2} = \frac{(A_m A_n - a B_m B_n)^2}{(A_m B_n - A_n B_m)^2}. \end{aligned}$$

Therefore, we have

$$(A_m B_n - A_n B_m)^2 A_{m+n} A_{|m-n|} = (A_m A_n - a B_m B_n)^2 B_{m+n} B_{|m-n|}. \tag{3.7}$$

So, to complete the proof, it suffices to prove that $A_m A_n - a B_m B_n$ and $A_m B_n - A_n B_m$ are coprime, as this implies from (3.7) that if $p^k | \left(A_m B_n - A_n B_m \right)^2$, then $p^k | B_{m+n} B_{|m-n|}$ as well.

Step 1: $p = 2$. Under the hypotheses of the lemma, we will prove that $2 \nmid \gcd \left(A_m A_n - a B_m B_n, A_m B_n - A_n B_m \right)$.

Assume that m is even and n is odd. Then $B_2 | B_m$ and hence $\operatorname{ord}_2(B_m) \geq \operatorname{ord}_2(B_2)$ and $\gcd(B_2, B_n) = B_{\gcd(2,n)} = B_1$, from Lemma 3.2. Hence, by Lemma 3.7(b), $\operatorname{ord}_2(B_n) = \operatorname{ord}_2(B_1) < \operatorname{ord}_2(B_2) \leq \operatorname{ord}_2(B_m)$. If B_n is odd, then B_m is even and so A_m is odd, since A_m and B_m are coprime. Therefore $A_mB_n - A_nB_m$ is odd. If B_n is even, then B_m is even and so A_mA_n is odd, and again $A_mA_n - aB_mB_n$ is odd. Hence $2 \nmid \gcd(A_mA_n - aB_mB_n, A_mB_n - A_nB_m)$.

Next assume that m and n are both even with $\mathrm{ord}_2(m) > \mathrm{ord}_2(n) > 0$. From Lemma 3.7(a), $x\left(2^kP\right)$ is a square for $k \geq 1$, so by Lemma 3.7(b) applied to 2^kP rather than P, we find that $\mathrm{ord}_2\left(B_{2^{k+1}}\right) > \mathrm{ord}_2\left(B_{2^k}\right)$. Hence $\mathrm{ord}_2(B_m) > \mathrm{ord}_2(B_n)$. By the same argument as in the case when m is even and n is odd, we obtain $2 \nmid \gcd(A_mA_n - aB_mB_n, A_mB_n - A_nB_m)$.

Step 2: p, odd. Next we will prove, under the hypotheses of the lemma, that $A_mA_n - aB_mB_n$ and $A_mB_n - A_nB_m$ have no common odd prime divisor. The proof is by contradiction.

Suppose that $A_mA_n - aB_mB_n$ and $A_mB_n - A_nB_m$ have a common odd prime divisor p. Then

$$A_mA_n - aB_mB_n \equiv 0 \bmod p \tag{3.8}$$

$$A_mB_n - A_nB_m \equiv 0 \bmod p. \tag{3.9}$$

If $B_m \equiv 0 \bmod p$, then, from (3.9), $A_mB_n \equiv 0 \bmod p$. 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 (3.8) we have $A_mA_n \equiv 0 \bmod p$, 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 $B_n \not\equiv 0 \bmod p$.

Next from (3.8) and (3.9) we have

$$aB_m^2B_n \equiv A_mA_nB_m \equiv A_m^2B_n \bmod p.$$

Since $B_n \not\equiv 0 \bmod p$, we have $aB_m^2 \equiv A_m^2 \bmod p$. In the same way, we obtain $aB_n^2 \equiv A_n^2 \bmod p$. Therefore,

$$C_m^2 \equiv A_m^3 + aA_mB_m^2 \equiv 2A_m^3 \bmod p \tag{3.10}$$

$$C_n^2 \equiv A_n^3 + aA_nB_n^2 \equiv 2A_n^3 \bmod p. \tag{3.11}$$

Since $A_mA_n - aB_mB_n$ and $A_mB_n - A_nB_m$ have a common odd prime divisor p, from (3.6) it must be the case that

$$C_mB_n^{3/2} - C_nB_m^{3/2} \equiv C_mB_n^{3/2} + C_nB_m^{3/2} \equiv 0 \bmod p.$$

Therefore $2C_mB_n^{3/2} \equiv 0 \bmod p$. From $B_n \not\equiv 0 \bmod p$, we have $C_m \equiv 0 \bmod p$ and then $C_n \equiv 0 \bmod p$. Hence from (3.10) and (3.11) we have $A_m \equiv A_n \equiv 0 \bmod p$. Since $\gcd(A_m, B_m) = \gcd(A_n, B_n) = 1$, we have

$B_m B_n \not\equiv 0 \bmod p$, so from (3.8) $a \equiv 0 \bmod p$. It follows that E_a has additive reduction at p and mP has bad reduction at p.

On the other hand, using Tate's algorithm (see [13, Section IV.9]), we determine that E_a has reduction type I_0, III, I_0^* or III^*. From the characterisation of $E(\mathbb{Q})/E_0(\mathbb{Q})$ in Table 4.1 of [13, p. 365], we see that $2P$ has good reduction at p. So mP has good reduction at p, since m is even. This is a contradiction. Hence $A_m A_n - aB_m B_n$ and $A_m B_n - A_n B_m$ have no common odd prime divisor.

It follows that $0 < (A_m B_n - A_n B_m)^2 \leq B_{m+n} B_{|m-n|}$, as desired. □

4. Proof of Theorem 2.1

We are now ready to prove Theorem 2.1. Our proof is based upon ideas found in [6].

4.1. **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 [18]). 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 both cases, by Lemma 3.8, we have

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

Taking the logarithm of both sides gives

$$2 \log |A_m B_{m'} - A_{m'} B_m| \leq \log (B_n) + \log (B_{m-m'}) . \tag{4.1}$$

Assume that the term B_n does not have a primitive divisor. Then, by Lemma 3.6, we have

$$\log(B_n) \leq \eta(n) + 2n^2\rho(n)\widehat{h}(P) + \omega(n)K. \tag{4.2}$$

Lemma 3.5 gives

$$\begin{aligned}\log(B_{m-m'}) &\leq h((m-m')P) \\ &\leq 2\widehat{h}((m-m')P) + K = 2(m-m')^2\widehat{h}(P) + K.\end{aligned} \tag{4.3}$$

Combining (4.2) and (4.3) with (4.1) gives

$$\begin{aligned}&2\log|A_mB_{m'} - A_{m'}B_m| \\ &\leq \eta(n) + 2n^2\rho(n)\widehat{h}(P) + \omega(n)K + 2(m-m')^2\widehat{h}(P) + K.\end{aligned} \tag{4.4}$$

Lemma 3.7(a) 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

$$\begin{aligned}2\log|A_mB_{m'} - A_{m'}B_m| &= 2\log\left|a_m^2b_{m'}^2 - a_{m'}^2b_m^2\right| \\ &\geq 2\log(|a_mb_{m'}| + |a_{m'}b_m|) \\ &\geq 2\log(|a_m| + |b_m|) \\ &\geq 2\log\max\{|a_m|, |b_m|\} \\ &= h(mP) \geq 2\widehat{h}(mP) - L,\end{aligned}$$

recalling from Lemma 3.8 that $A_mB_{m'} - A_{m'}B_m \neq 0$. Note that the last inequality is obtained by Lemma 3.5 and the definition of L in (2.2). Since $\widehat{h}(mP) = m^2\widehat{h}(P)$, we have

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

Combining this estimate and (4.4) gives

$$\begin{aligned}&2m^2\widehat{h}(P) - L \\ \leq\ &\eta(n) + 2n^2\rho(n)\widehat{h}(P) + \omega(n)K + 2(m-m')^2\widehat{h}(P) + K.\end{aligned}$$

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

$$\begin{aligned}\eta(n) + \omega(n)K + K + L &\geq 2\left(\frac{1}{3} - \frac{r^2}{3N^2} - \rho(n)\right)\widehat{h}(P)n^2 \\ &\geq 2\left(\frac{1}{3} - \frac{1}{3N^2} - \rho(n)\right)\widehat{h}(P)n^2.\end{aligned} \tag{4.5}$$

4.2. **Proof of part (b).** Assume that n is a positive integer divisible by 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 3.6 and 3.8, we have

$$\begin{aligned}
&2\log\left|A_{(p+1)k/2}B_{(p-1)k/2} - A_{(p-1)k/2}B_{(p+1)k/2}\right| \\
&\leq \log\left(B_n\right) + \log\left(B_k\right) \leq \eta(n) + 2n^2\rho(n)\widehat{h}(P) + \omega(n)K + \log\left(B_k\right). \qquad (4.6)
\end{aligned}$$

On the other hand,

$$\begin{aligned}
& 2\log\left|A_{(p+1)k/2}B_{(p-1)k/2} - A_{(p-1)k/2}B_{(p+1)k/2}\right| \\
= \; & 2\log\left|a_{(p+1)k/2}^2 b_{(p-1)k/2}^2 - a_{(p-1)k/2}^2 b_{(p+1)k/2}^2\right| \\
= \; & 2\log\left|\left|a_{(p+1)k/2}b_{(p-1)k/2}\right| - \left|a_{(p-1)k/2}b_{(p+1)k/2}\right|\right| \\
& +2\log\left(\left|a_{(p+1)k/2}b_{(p-1)k/2}\right| + \left|a_{(p-1)k/2}b_{(p+1)k/2}\right)\right| \\
\geq \; & 2\log\left|b_k\right| + 2\log\left(\left|a_{(p+1)k/2}\right| + \left|b_{(p+1)k/2}\right|\right) \qquad \text{since } b_k \mid b_{(p\pm1)k/2}, \\
\geq \; & \log\left(B_k\right) + h([(p+1)k/2]P) \\
(4.7) \geq \; & \log\left(B_k\right) + 2((p+1)k/2)^2\widehat{h}(P) - L.
\end{aligned}$$

Combining (4.6) and (4.7) 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

$$2\left(\frac{(p+1)^2}{4p^2} - \rho(n)\right)\widehat{h}(P)n^2 \leq \eta(n) + \omega(n)K + L. \qquad (4.8)$$

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

4.3. **Proof of part (c).** Assume that n is a positive even integer divisible by p. Write $n = 2pk$ for some positive integer k. Assume that B_n does not have a primitive divisor. Put $m = (p+1)k$ and $m' = (p-1)k$. Then by Lemmas 3.6 and 3.8, we have

$$\begin{aligned}
& 2\log\left|A_m B_{m'} - A_{m'}B_m\right| \leq \log\left(B_n\right) + \log\left(B_{m-m'}\right) \\
\leq \; & \eta(n) + 2n^2\rho(n)\widehat{h}(P) + \omega(n)K + \log\left(B_{2k}\right). \qquad (4.9)
\end{aligned}$$

On the other hand,

$$\begin{aligned} & 2\log\left|A_m B_{m'} - A_{m'} B_m\right| \\ = \; & 2\log\left|a_m^2 b_{m'}^2 - a_{m'}^2 b_m^2\right| \\ = \; & 2\log\left|\left|a_m b_{m'}\right| - \left|a_{m'} b_m\right|\right| + 2\log\left(\left|a_m b_{m'}\right| + \left|a_{m'} b_m\right|\right) \\ \geq \; & 2\log\left|b_{2k}\right| + 2\log\left(\left|a_m b_{m'}\right| + \left|a_{m'} b_m\right|\right) \qquad \text{since } b_{2k} \mid b_m \text{ and } b_{2k} \mid b_{m'}. \end{aligned}$$

Since m' is even, $x(m'P)$ is a rational square and hence $x(m'P)$ is non-negative. If $x(m'P)=0$, then since $x(m'P) = \left(x(m'P)^2 - a\right)^2 / \left(2y(m'P)\right)^2$, we must have $y(m'P)=0$. But if $(x,0) \in E_a(\mathbb{C})$, then $[2](x,0) = \mathcal{O}$, the zero element. So $x(m'P) > 0$, and therefore $x(m'P) \geq \sqrt{|a|}$ (this is the place in the proof where we require $a<0$). Hence $A_{m'} \geq \sqrt{|a|} B_{m'}$.

Then

$$\begin{aligned} 2\log\left(\left|a_m b_{m'}\right| + \left|a_{m'} b_m\right|\right) & \geq 2\log\left(\left|a_m b_{m'}\right| + \left|b_{m'} b_m\right|\right) \\ & \geq 2\log\left|b_{m'}\right| + 2\log\left(\left|a_m\right| + \left|b_m\right|\right) \\ & \geq \log\left(B_{m'}\right) + h(mP). \end{aligned}$$

Thus we have

$$2\log\left|A_m B_{m'} - A_{m'} B_m\right| \geq \log\left(B_{2k}\right) + \log\left(B_{m'}\right) + h(mP).$$

Now we can write $(m'/2)P = \left(sU^2/B, sUV/B^{3/2}\right)$ in lowest terms, where $s|a$ and $\gcd(U,V)=1$ (see [14], p. 93). By the duplication formula, we have

$$x\left(m'P\right) = \frac{\left(2sU^4 - V^2\right)^2}{4U^2V^2B}.$$

Since $\gcd(U,V)=1$, we have $U^2B|B_{m'}$, therefore

$$B_{m'} \geq |s|^{-1} A_{m'/2} B_{m'/2} \geq |s|^{-1} \max\left\{\left|A_{m'/2}\right|, \left|B_{m'/2}\right|\right\}.$$

Hence

$$\begin{aligned} & 2\log\left|A_m B_{m'} - A_{m'} B_m\right| \\ \geq \; & \log\left(B_{2k}\right) + h\left((m'/2)P\right) - \log|s| + h(mP) \\ \geq \; & \log\left(B_{2k}\right) + 2(m'/2)^2 \widehat{h}(P) + 2m^2 \widehat{h}(P) - 2L - \log|s|. \end{aligned} \tag{4.10}$$

Combining (4.9) and (4.10) gives

$$2\left(m'/2\right)^2 \widehat{h}(P) + 2m^2 \widehat{h}(P) - 2L - \log|s| \leq \eta(n) + 2n^2 \rho(n) \widehat{h}(P) + \omega(n) K.$$

Substituting $m = n(1 + 1/p)/2$ and $m' = n(1 - 1/p)/2$, we obtain

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

Part (c) follows, completing the proof of the Theorem. □

5. Proof of Corollary 2.3

To prove Corollary 2.3, we use Robin's estimate for $\omega(n)$ (see Théorème 11 of [8]):

$$\omega(n) < \frac{1.3841\log(n)}{\log\log(n)} \qquad \text{for all } n \geq 3. \tag{5.1}$$

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

$$\begin{aligned} \rho(n) &< \sum_{p<10^6} p^{-2} + \left(\zeta(2) - \sum_{m \leq 10^6} m^{-2}\right) < 0.452248 + 0.000001 \\ &< 0.45225, \end{aligned} \tag{5.2}$$

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

5.1. Proof of Corollary 2.3(a).

Let $P \in E_a(\mathbb{Q})$ be a point of infinite order. Let $n \geq 3$ 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 3 and 5. Then $n \geq 7$ and $\rho(n) < 0.45225 - 1/4 - 1/9 - 1/25 < 0.052$. Here we apply Theorem 2.1(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 $\rho(n) < 0.45225 - 1/4 < 0.203$. Here we apply Theorem 2.1(b) with $p = 3$, so

$$2\left(\frac{(p+1)^2}{4p^2} - \rho(n)\right) = 2\left(\frac{4}{9} - \rho(n)\right) > 0.482,$$

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 we apply Theorem 2.1(b) with $p = 5$, so

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

Therefore, the Corollary follows in this case too, completing the proof of part (a).

5.2. **Proof of Corollary 2.3(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 $n \leq 4$, 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 three cases.

Case 1. Assume that n is not divisible by 3 and 5. From (5.2), $\rho(n) < 0.45225 - 1/9 - 1/25 < 0.302$.

Here we apply Theorem 2.1(a) and write $n = 2^e N$ with $e \geq 1$ and $N \geq 7$ 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 5, but not by 3. Then $\rho(n) < 0.45225 - 1/9 < 0.342$. Here we apply Theorem 2.1(c) with $p = 5$, so

$$2\left(\frac{5p^2+6p+5}{16p^2} - \rho(n)\right) = 2\left(\frac{2}{5} - \rho(n)\right) > 0.116,$$

and the Corollary follows in this case.

Case 3. Assume that n is divisible by 3. Then $\rho(n) < 0.45225$. Here we apply Theorem 2.1(c) with $p = 3$, so

$$2\left(\frac{5p^2+6p+5}{16p^2} - \rho(n)\right) = 2\left(\frac{17}{36} - \rho(n)\right) > 0.039,$$

and the Corollary follows in this case.

We have thus completed the proof. □

6. Proof of Proposition 2.5

The proof is similar to [2, Proposition 2.1]: based on the decomposition of the canonical height into a sum of local canonical heights. The proof is slightly more complicated by the fact that in this case $2P$ does not always have good reduction.

6.1. **Archimedean Estimates.** We will estimate the archimedean contribution to the canonical height by using Tate's series. In order to describe Tate's series for our curve E_a (see [11] or [19]), let

$$t(P) = 1/x(P), \quad w(P) = 4t(P) + 4at(P)^3, \quad z(P) = (-at(P)^2 + 1)^2,$$

where $P \in E_a(\mathbb{R})$.

Then the archimedean local height of $P \in E_a(\mathbb{R})$ is given by the series

$$\widehat{\lambda}_\infty(P) = \frac{1}{2}\log|x(P)| + \frac{1}{8}\sum_{k=0}^{\infty} 4^{-k}\log|z(2^k P)| - \frac{1}{12}\log|\Delta_a|.$$

$E_a(\mathbb{R})$ has two components, and every point, (x, y), in the identity component $E_a^0(\mathbb{R})$ satisfies $x \geq \sqrt{|a|}$. From Lemma 3.7(a), $x(2P)$ is a square and hence $x(2P)$ is non-negative. If $x(2P) = 0$, then since $x(2P) = (x(P)^2 - a)^2/(2y(P))^2$, we must have $y(P) = 0$ (since $x(P)^2 - a = 0$ has no solution for $x(P) \in \mathbb{R}$). But if $(x, 0) \in E_a(\mathbb{C})$, then $[2](x, 0) = O$, the zero element). Hence $x(2P) > 0$. Therefore, $2P$, and $2^k P$ for all $k \geq 1$, is in $E_a^0(\mathbb{R})$.

For any $Q \in E_a^0(\mathbb{R})$, we have

$$x(Q) \geq \sqrt{|a|}, \quad 0 \leq t(Q) \leq \frac{1}{\sqrt{|a|}}, \quad 1 \leq z(Q) \leq 4.$$

Therefore, for every $P \in E_a(\mathbb{R})$,

$$\widehat{\lambda}_\infty(P) = \frac{1}{2}\log|x(P)| + \frac{1}{8}\log|z(P)| + \frac{1}{8}\sum_{k=1}^{\infty} 4^{-k} z_k - \frac{1}{12}\log|\Delta_a|,$$

where $0 \leq z_k \leq \log(4)$.

Using the definition of $z(P)$, we get

$$0 \leq \widehat{\lambda}_\infty(P) - \left(\frac{1}{4}\log\left(x(P)^2 - a\right) - \frac{1}{12}\log|\Delta_a|\right) \leq \frac{1}{12}\log(2). \tag{6.1}$$

6.2. **Non-archimedean Estimates for v odd.** Non-archimedean canonical heights are computed using the algorithm presented in [11]. If v is an odd prime number, then Tate's algorithm (see [13], Section IV.9) can be used to prove that E_a has reduction type:

- I_0 at v when $\operatorname{ord}_v(a) = 0$;
- III at v when $\operatorname{ord}_v(a) = 1$;

- I_0^* at v when $\mathrm{ord}_v(a) = 2$;
- III^* at v when $\mathrm{ord}_v(a) = 3$;

From the characterisation of $E(K)/E_0(K)$ in Table 4.1 of [13] for these reduction types, we see that $2P$ always has good reduction at v and we have

$$\widehat{\lambda}_v(2P) = \frac{1}{2}\max\{0, -v(x(2P))\} + \frac{v(\Delta_a)}{12}, \tag{6.2}$$

from Theorem 4.1 of [13, Chapter VI].

6.3. **Non-archimedean Estimates for $v = 2$.** For $v = 2$, Tate's algorithm shows that E_a has reduction type:

- II at 2 when $a \equiv 1 \bmod 4$;
- III at 2 when $a \equiv 3 \bmod 4$;
- III at 2 when $\mathrm{ord}_2(a) = 1$;
- I_2^* at 2 when $a \equiv 12 \bmod 16$;
- I_3^* at 2 when $a \equiv 4 \bmod 16$;
- III^* at 2 when $\mathrm{ord}_2(a) = 3$;

Again, according to Table 4.1 of [13], we see that $2P$ has good reduction unless the reduction type is I_3^*, which only happens for $a \equiv 4 \bmod 16$.

So for $a \not\equiv 4 \bmod 16$, we can apply Theorem 4.1 of [13, Chapter VI] again.

For $a \equiv 4 \bmod 16$, we appeal to the case of Kodiara type I_m^*, m odd and $c_v = 2$ or 4 in the proof of Proposition 6 of [4]. Our $2P$ here must be of order 2 in $E(K_2)$ (since $4P \in E_0(K_2)$) and hence it must equal P_1 in their proof of this case (namely, we are in the $c_v = 2$ subcase). They calculate that their $\lambda_v(P_1) = -\log(q_v)/n_v$. Since $n_v = 1$ and $q_v = 2$ here, their $\lambda_v(P_1) = -\log(2)$. As noted in Section 4 of [4] (see in particular, their equation (11) there), their λ_v is twice the λ_v that we use here. Hence our $\lambda_v(P_1) = -\log(2)/2$ and we must subtract $\log(2)/2$ here.

So

$$\begin{aligned} \widehat{\lambda}_v(2P) &= \frac{1}{2}\max\{0, -v(x(2P))\} + \frac{v(\Delta_a)}{12} \\ &\quad - \begin{cases} 0 & \text{if } a \not\equiv 4 \bmod 16 \\ \frac{1}{2}\log(2) & \text{if } a \equiv 4 \bmod 16. \end{cases} \end{aligned} \tag{6.3}$$

6.4. **Conclusion.** We compute the canonical height by summing local canonical heights.

Writing $2P = \alpha/\delta^2$ as a fraction in lowest terms and taking the sum of (6.3) and (6.2) over all primes gives the exact formula

$$\sum_{v\neq\infty} \widehat{\lambda}_v(2P) = \log|\delta| + \frac{1}{12}\log|\Delta_a| - \begin{cases} 0 & \text{if } a \not\equiv 4 \bmod 16 \\ \frac{1}{2}\log(2) & \text{if } a \equiv 4 \bmod 16. \end{cases}$$

Adding this last equation to the lower bound (6.1) for $\widehat{\lambda}_\infty(2P)$, we obtain

$$\widehat{h}(2P) \geq \frac{1}{4}\log|\alpha^2 - a\delta^4| - \begin{cases} 0 & \text{if } a \not\equiv 4 \bmod 16 \\ \frac{1}{2}\log(2) & \text{if } a \equiv 4 \bmod 16. \end{cases}$$

Since $2P \in E^0(\mathbb{R})$, $\alpha/\delta^2 \geq \sqrt{|a|}$ and therefore $\alpha^2 - a\delta^4 \geq |2a|\delta^4 \geq |2a|$. This gives the lower bound

$$\widehat{h}(2P) \geq \frac{1}{4}\log|2a| - \begin{cases} 0 & \text{if } a \not\equiv 4 \bmod 16 \\ \frac{1}{2}\log(2) & \text{if } a \equiv 4 \bmod 16. \end{cases}$$

The proposition follows since $\widehat{h}(2P) = 4\widehat{h}(P)$.

7. Proof of Theorem 2.6

7.1. n **odd,** $n > 7$**.** Let n be a positive odd integer and assume that $x(P)$ is a rational square. Assume that the term $B_n(P)$ does not have a primitive divisor.

Part (*a*). Assume that $a \not\equiv 4 \mod 16$. From Proposition 2.5, we have

$$\widehat{h}(P) \geq \frac{1}{16}\log|2a|. \tag{7.1}$$

Assume further that $a \leq -5$. Then

$$\frac{1}{\log|2a|} < 0.435, \qquad \frac{K}{\log|2a|} < 1.454, \qquad \frac{L}{\log|2a|} < 0.802. \tag{7.2}$$

Substituting (7.1) into Corollary 2.3(a) yields

$$0.482\left(\frac{1}{16}\log|2a|\right)n^2 < 2\log(n) + \frac{1.3841\log(n)}{\log\log(n)}K + K + L.$$

Dividing both sides of this equation by $\log|2a|$ and substituting the estimates (7.2) yields

$$\begin{aligned} 0.030n^2 &< 0.870\log(n) + 1.454\frac{1.3841\log(n)}{\log\log(n)} + 2.256 \\ &< \log(n)\left(0.870 + \frac{2.013}{\log\log(n)}\right) + 2.256. \end{aligned}$$

Using this inequality, we obtain the bound $n < 18.6$, so $n \leq 17$.

We will next give the better bounds by using the inequalities of Theorem 2.1(b).

If n is odd and divisible by p, then, by Theorem 2.1(b), (7.1) and (7.2),

$$\begin{aligned} 0 < \frac{1}{8}\left(\frac{(p+1)^2}{4p^2} - \rho(n)\right) n^2 &\leq \frac{\eta(n) + \omega(n)K + L}{\log|2a|} \\ &< 0.435\eta(n) + 1.454\omega(n) + 0.802. \end{aligned}$$

Using this inequality, we can eliminate $n = 9$, 11, 13, 15 and 17 (with $p = 3$, 11, 13, 3 and 17, respectively) for $a \leq -5$.

Next assume $-5 < a < 0$. Using PARI, we find that such E_a have rank one for $a = -2$ and rank zero otherwise. If $a = -2$, then $P = (-1, 1)$ is a generator for $E_a(\mathbb{Q})$. However, for n odd, we require that $x(P)$ is a rational square. All such elements of $E_a(\mathbb{Q})$ are generated by $2P = (9/4, 21/8)$ and the torsion element of $E_a(\mathbb{Q})$ (its torsion subgroup is of order 2).

Substituting $a = -2$ and $\widehat{h}(2P) = 2.4348\ldots$ into the inequality in Corollary 2.3(a), we find that $K = 2.889$, $L = 1.387$ and

$$1.173n^2 < \left(2 + \frac{4}{\log\log(n)}\right)\log(n) + 4.276.$$

Using this inequality, we find that if $a = -2$, then $n \leq 3$.

Part (*b*). Assume that $a \equiv 4 \mod 16$. From Proposition 2.5, we have

$$\widehat{h}(P) \geq \frac{1}{16}\log|a/2|. \tag{7.3}$$

We first assume that $a \leq -44$. Hence

$$\frac{1}{\log|a/2|} < 0.324, \quad \frac{K}{\log|a/2|} < 1.435, \quad \frac{L}{\log|a/2|} < 0.949. \tag{7.4}$$

Using the same argument as above, from Corollary 2.3(a) we have

$$0.03n^2 < \left(0.648 + \frac{1.987}{\log\log(n)}\right)\log(n) + 2.384.$$

Using this inequality, we obtain the bound $n < 17.95$, so $n \leq 17$.

Moreover, from Theorem 2.1(b), (7.3) and (7.4), we have

$$\frac{1}{8}\left(\frac{(p+1)^2}{4p^2} - \rho(n)\right) n^2 < 0.324\eta(n) + 1.435\omega(n) + 0.949.$$

Using this inequality, we obtain $n \leq 7$ for $a \leq -44$.

Now consider the remaining cases with $-44 < a < 0$. We find that such E_a have rank one for $a = -12$ and rank zero for $a = -28$.

For $a = -12$, using PARI, we found that $P = (-2, -4)$ is a generator of $E_a(\mathbb{Q})$. As above, we need to consider $2P = (4, -4)$ and $\widehat{h}(2P) = 1.0023\ldots$. In the same way as in the case of $a \not\equiv 4 \bmod 16$, first using the inequality in Corollary 2.3(a) and then using the inequality in Theorem 2.1(b), we obtain $n \leq 7$ for $a = -12$, completing the proof of part (a) here.

7.2. n **even,** $n > 22$**.** Let n be a positive even integer and not a power of two. Assume that $B_n(P)$ does not have a primitive divisor.

Part (a). Assume that $a \not\equiv 4 \mod 16$.

Suppose that $a \leq -12$. Then

$$\frac{1}{\log|2a|} < 0.315, \quad \frac{K}{\log|2a|} < 1.191, \quad \frac{L}{\log|2a|} < 0.719. \tag{7.5}$$

By the same argument as above, substituting the estimates (7.1) and (7.5) into the inequality of Corollary 2.3(b) implies that

$$0.002n^2 < \left(0.63 + \frac{1.649}{\log\log(n)}\right)\log(n) + 2.22.$$

Using this inequality, we obtain the bound $n < 69.8$, so $n \leq 68$.

We will next give better bounds. If n is even, we obtain

$$\begin{aligned} 0 < \frac{1}{8}\left(\frac{5p^2+6p+5}{16p^2} - \rho(n)\right)n^2 &\leq \frac{\eta(n) + \omega(n)K + 2L + \log|a|}{\log|2a|} \\ &\leq 0.315\eta(n) + 1.191\omega(n) + 2.22, \end{aligned}$$

from Theorem 2.1(c), (7.1) and (7.5). Using this inequality, we find that if $a \leq -12$, then $n \leq 22$, excluding $n = 8$ and $n = 16$.

Next assume $-12 < a < 0$. We find that such E_a have rank one for $a = -2, -5, -6, -7$ and -10, and rank zero otherwise. The generators for $E_a(\mathbb{Q})$ with rank one and their canonical heights are as follows:

a	P	$\widehat{h}(P)$	a	P	$\widehat{h}(P)$
-2	$(-1,-1)$	$0.6087\ldots$	-7	$(4,-6)$	$1.6342\ldots$
-5	$(-1,-2)$	$0.6355\ldots$	-10	$(-1,-3)$	$1.2815\ldots$
-6	$(-2,-2)$	$0.8442\ldots$			

Let $a = -2$. Substituting $a = -2$ and $\widehat{h}(P) = 0.6087\ldots$ into the inequality in Corollary 2.3(b), we have

$$0.023n^2 < \left(2 + \frac{4}{\log\log(n)}\right)\log(n) + 3.467,$$

since $K < 2.889$ and $L < 1.387$.

Using this inequality, we obtain the bound $n < 30.6$ and hence $n \leq 30$.

Next substituting $a = -2$ and $\widehat{h}(P) = 0.6087\ldots$ into the inequality in Theorem 2.1(c), we obtain

$$1.217 \left(\frac{5p^2+6p+5}{16p^2} - \rho(n) \right) n^2 < \eta(n) + 2.889\omega(n) + 3.467.$$

Using this inequality, we can eliminate $n = 24$, 26, 28 and 30.

By the same argument, we can show that $n \leq 22$ for $a = -5$, -6, -7 and -10 as well.

Hence $n \leq 22$, excluding 8 and 16.

Part (*b*). Assume that $a \equiv 4 \mod 16$.

Suppose that $a \leq -140$. Then

$$\frac{1}{\log|a/2|} < 0.236, \quad \frac{K}{\log|a/2|} < 1.18, \quad \frac{L}{\log|a/2|} < 0.827. \tag{7.6}$$

From Corollary 2.3(b), we have

$$0.002n^2 < \left(0.472 + \frac{1.634}{\log\log(n)} \right) \log(n) + 2.818.$$

By using this inequality, we obtain the bound $n < 69.94$, so $n \leq 68$.

Moreover, from Theorem 2.1(c), (7.3) and (7.6), we have

$$\frac{1}{8} \left(\frac{5p^2+6p+5}{16p^2} - \rho(n) \right) n^2 < 0.236\eta(n) + 1.18\omega(n) + 2.818.$$

Using this inequality, we obtain $n \leq 22$, excluding $n = 8$ and $n = 16$, for $a \leq -140$.

Now assume that $-140 < a < 0$. We find that such E_a have rank one for $a = -12$, -60, -76 and -124 and rank zero for $a = -28$, -44, -92 and -108. The generators for $E_a(\mathbb{Q})$ with rank one and their canonical heights are as follows:

a	P	$\widehat{h}(P)$	a	P	$\widehat{h}(P)$
-12	$(-2,-4)$	$0.2505\ldots$	-76	$(2,-12)$	$1.0493\ldots$
-60	$(-6,-12)$	$0.5673\ldots$	-124	$(18,60)$	$1.9118\ldots$

Using the same argument as in the case of $a \not\equiv 4 \bmod 16$, we obtain $n \leq 22$, excluding $n = 8$ and $n = 16$, for these values of a, completing the proof. □

7.3. $4 \leq n < 22$. In this subsection and the following one, we use the ideas and results in [7] to conclude the proof of Theorem 2.6.

In fact, Ingram has proven that there are no solutions for $n = 5$, 6, 7, 10, 12 (since there are none for $n = 6$), 14, 18 and 20 (since there are none for $n = 10$). So it only remains to consider $n = 22$.

7.4. $n = 22$. In Ingram's notation, we find that $\Psi_{22}(X, Y)$ is of degree 90 and reducible. It has two irreducible factors over $\mathbb{Q}[X, Y]$. There is one of degree 30 and another of degree 60. Let us call these irreducible forms, $F_{22,1}(X, Y)$ and $F_{22,2}(X, Y)$, respectively.

Using Maple, we see that if $2|F_{22,1}(X, Y)$, then $X + Y \equiv 0 \bmod 2$. So in this case, we put $Y = 2Y_1 - X$ and find that if $2|F_{22,1}(X, Y)$, then 2^{30} must divide $F_{22,1}(X, Y)$ (since 2^{30} divides all the coefficients of $F_{22,1}(X, 2Y_1 - X)$ expanded as a polynomial in X and Y_1).

Writing $F_{22,1}\left(X, 2Y_1 - X\right)/2^2 = F_{22,1,1}(X, Y_1)$, we find that $F_{22,1,1}\left(X, Y_1\right) \equiv \left(X + Y_1\right)^{30} \bmod 2$. Hence, if $2^{31}|F_{22,1}(X, Y)$, then $Y_1 = 2Y_2 - X$ and, in fact, again by considering the content, 2^{45} must divide $F_{22,1}(X, Y)$.

Writing $F_{22,1,1}(X, 2Y_2 - X)/2^{15} = F_{22,1,2}\left(X, Y_2\right)$, we find that $F_{22,1,2}(X, Y_2) \equiv X^{30} \bmod 2$. And if $2^{46}|F_{22,1}(X, Y)$, then $X = 2X_1$. This means that $2|X$ and $2|Y$, but we are assuming that $\gcd(X, Y) = 1$.

Hence $F_{22,1}(X, Y) = \pm 2^{\alpha} 11^{\beta}$ where $\alpha = 0, 30, 45$. Similarly, $F_{22,2}(X, Y) = \pm 2^{\alpha} 11^{\beta}$ where $\alpha = 0, 60, 90$.

Again, using Maple, we see that if $11|F_{22,1}(X, Y)$, then $Y = 11Y_1$. Performing this substitution, we find that the resulting polynomial has 11 as its content. Writing $F_{22,1}(X, 11Y_1)/11 = F_{22,1,1}(X, Y_1)$, we find that $F_{22,1,1}(X, Y_1) \equiv X^{30} \bmod 11$. Hence, if $11^2|F_{22,1}(X, Y)$, then $11|\gcd(X, Y)$, which is not possible.

Hence $F_{22,1}(X, Y) = \pm 2^{\alpha} 11^{\beta}$ where $\alpha = 0, 30, 45$ and $\beta = 0, 1$. Similarly, $F_{22,2}(X, Y) = \pm 2^{\alpha} 11^{\beta}$ where $\alpha = 0, 60, 90$ and $\beta = 0, 1$.

Using the gcdex command in Maple for each possible combination of values of $F_{22,1}(X, Y)$ and $F_{22,2}(X, Y)$ to eliminate a variable and then search for rational roots of the resulting single-variable polynomials, we find no non-trivial solutions that lead to elliptic divisibility sequences whose 22-nd element has no primitive divisor.

An alternative proof is possible by observing that for $a \not\equiv 4 \bmod 16$, $a < -46$ and for $a \equiv 4 \bmod 16$, $a < -956$, the inequalities in Section 7.2 hold.

Hence we need only solve $F_{22,1}(X,Y) = \pm 2^{\alpha} 11^{\beta}$ for X where $\alpha = 0, 30, 45$, $\beta = 0, 1$ and $-956 \leq a < 0$.

This completes the proof.

References

1. Y. Bilu, G. Hanrot, P. 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. A. Bremner, J.H. Silverman, N. Tzanakis, *Integral points in arithmetic progression on $y^2 = x\left(x^2 - n^2\right)$*, J. Number Theory 80(2) (2000), 187–208.
3. R. D. Carmichael, *On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$*, Ann. of Math. 15 (1913), 30–70.
4. J. E. Cremona, M. Prickett, S. Siksek, *Height difference bounds for elliptic curves over number fields*, J. Number Theory 116 (2006), 42–68.
5. L. K. Durst, *Exceptional real Lehmer sequences*, Pacific J. Math. 9 (1959), 437–441.
6. G. Everest, G. Mclaren, T. Ward, *Primitive divisors of elliptic divisibility sequenses*, J. Number Theory 118 (2006), 71–89.
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. XLII (1983), 367–389.
9. J. H. Silverman, *Lower bound for the canonical height on elliptic curves*, Duke Math. J. 48 (1981), 633–648.
10. J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. 106, Springer-Verlag, New York, 1986.
11. J. H. Silverman. *Computing heights on elliptic curves*, Math. Comp. 51 (1988), 339–358.
12. J. H. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory 30 (1988), 226–237.
13. J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Math. 151, Springer-Verlag, New York, 1994.
14. J. H. Silverman, J. Tate, *Rational Points on Elliptic curves*, Undergraduate Texts in Math., Springer-Verlag, New York, 1992.
15. J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, in *"Modular Functions of One Variable* IV", Lecture Notes in Math. 476, Springer-Verlag, Berlin, 1975
16. M. Ward, *Memoir on elliptic divisibility sequences*, Amer. J. Math. 7 (1948), 31–74.
17. M. Ward, *The intrinsic divisors of Lehmer numbers*, Ann. of Math. (2) 62 (1955), 230–236.
18. M. Yabuta, *Primitive divisors of certain elliptic divisibility sequences*, Exp. Math. 18(3) (2009), 303–310.
19. H. Zimmer, *On the difference of the Weil height and the Néron-Tate height*, Math. Zeit. 174 (1976), 35–51.
20. K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. 3 (1892), 265–284.

Current address: London, UK
E-mail address: paul.voutier@gmail.com

Current address: Senri High School, 17-1, 2 chome, Takanodai, Suita, Osaka, 565-0861, Japan
E-mail address: yabutam@senri.osaka-c.ed.jp