

*Pacific  
Journal of  
Mathematics*

**SOME EFFECTIVITY RESULTS FOR PRIMITIVE DIVISORS  
OF ELLIPTIC DIVISIBILITY SEQUENCES**

MATTEO VERZOBIO

Volume 325 No. 2

August 2023



## SOME EFFECTIVITY RESULTS FOR PRIMITIVE DIVISORS OF ELLIPTIC DIVISIBILITY SEQUENCES

MATTEO VERZOBIO

**Let  $P$  be a nontorsion point on an elliptic curve defined over a number field  $K$  and consider the sequence  $\{B_n\}_{n \in \mathbb{N}}$  of the denominators of  $x(nP)$ . We prove that every term of the sequence of the  $B_n$  has a primitive divisor for  $n$  greater than an effectively computable constant that we will explicitly compute. This constant will depend only on the model defining the curve.**

### 1. Introduction

Let  $E$  be an elliptic curve defined by the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with coefficients in a number field  $K$ . Let  $P \in E(K)$  be a nontorsion point and let  $\mathcal{O}_K$  be the ring of integers of  $K$ . Let us define the fractional ideal

$$(1) \quad (x(nP))\mathcal{O}_K = \frac{A_n}{B_n}$$

with  $A_n$  and  $B_n$  two relatively prime integral  $\mathcal{O}_K$ -ideals. We want to study the sequence of integral  $\mathcal{O}_K$ -ideals  $\{B_n\}_{n \in \mathbb{N}}$ . These are the so-called *elliptic divisibility sequences*. In particular, we want to study when a term  $B_n$  has a primitive divisor, i.e., when there exists a prime ideal  $\mathcal{P}$  such that

$$\mathcal{P} \nmid B_1 B_2 \cdots B_{n-1} \quad \text{but} \quad \mathcal{P} \mid B_n.$$

Silverman [1988, Proposition 10] proved that, if  $E$  is defined over  $\mathbb{Q}$ , then  $B_n$  has a primitive divisor for  $n$  large enough. This result was generalized for every number field  $K$  in [Cheon and Hahn 1999], where the following theorem is proved.

**Theorem 1.1** [Cheon and Hahn 1999, main theorem]. *Let  $E$  be an elliptic curve defined over a number field  $K$  and let  $P$  be a nontorsion point in  $E(K)$ . Consider the sequence  $\{B_n\}_{n \in \mathbb{N}}$  of integral  $\mathcal{O}_K$ -ideals as defined in (1). Then  $B_n$  has a primitive divisor for all but finitely many  $n \in \mathbb{N}$ .*

*MSC2020:* 11B39, 11G05, 11G50.

*Keywords:* elliptic curves, primitive divisors, elliptic divisibility sequences.

The previous theorem is not effective. Indeed, the proof relies on Siegel's ineffective theorem about integral points on elliptic curves. The aim of this paper is to make the work of [Cheon and Hahn 1999] effective. Indeed, we will explicitly compute a constant  $C$  so that  $B_n$  has always a primitive divisor for  $n > C$ .

**Theorem 1.2.** *Let  $E$  be an elliptic curve defined over a number field  $K$  and let  $P$  be a nontorsion point in  $E(K)$ . Consider the sequence  $\{B_n\}_{n \in \mathbb{N}}$  of integral  $\mathcal{O}_K$ -ideals as defined in (1). There exists a constant  $C(E/K, \mathcal{M}) > 0$ , effectively computable and depending only on the curve  $E$  over the field  $K$  equipped with a model  $\mathcal{M}$  also defined over  $K$ , such that  $B_n$  has a primitive divisor for*

$$n > C(E/K, \mathcal{M}).$$

In Section 8, we explicitly compute such a constant  $C(E/K, \mathcal{M})$  (see (13)).

**Remark 1.3.** The dependence on the model  $\mathcal{M}$  is necessary. Indeed, given a nontorsion point  $P$  on an elliptic curve  $E$  and a positive constant  $C$ , it is easy to show that we can find a model of  $E$  such that  $B_n$  does not have a primitive divisor for all  $n \leq C$ .

**Remark 1.4.** It is conjectured that, in the case when  $\mathcal{M}$  is minimal, the constant  $C(E/K, \mathcal{M})$  should depend only on the field  $K$ . In [Ingram and Silverman 2012, Theorem 1] it is proved that the number of terms without a primitive divisor of an elliptic divisibility sequence can be bounded by a constant that does not depend on  $E$  and  $P$ , in the case when  $E$  is given by a minimal model,  $K = \mathbb{Q}$ , and assuming the *abc*-conjecture.

**Remark 1.5.** We believe that the techniques used in this paper can be applied also to a generalization of elliptic divisibility sequences. Let  $\mathcal{O}$  be the endomorphism ring of  $E$  and, given  $\alpha \in \mathcal{O}$ , define  $B_\alpha$  as the denominator of  $(x(\alpha P))\mathcal{O}_K$ . The sequence  $\{B_\alpha\}_{\alpha \in \mathcal{O}}$  is a sequence of ideals and one can give a definition of primitive divisors also for these sequences (see [Streng 2008, Section 1]). It has been shown in [Streng 2008, main theorem] that also in this case there are only finitely many terms that do not have a primitive divisor (see also [Verzobio 2021b]). In the case when  $\text{End}(E) = \mathbb{Z}$  this is a trivial corollary of Theorem 1.1, but in the case  $\text{End}(E) \neq \mathbb{Z}$  (i.e., when  $E$  has complex multiplication) this is far from being easy. We believe that using the techniques of this paper one can find an explicit upper bound for the degree of  $\alpha$  such that  $B_\alpha$  does not have a primitive divisor, in the case when  $\text{End}(E)$  is a maximal order and it is a principal ideal domain.

## 2. Notation

The curve  $E$  is defined by the equation

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

with coefficients in the number field  $K$ .

The following notation will be used during the paper:

$\Delta$  is the discriminant of the equation defining the curve.

$\Delta_{E/K}$  is the minimal discriminant of the elliptic curve.

$j(E)$  is the  $j$ -invariant of the curve.

$D = [K : \mathbb{Q}]$  is the degree of the number field  $K$ .

$\mathcal{O}_K$  is the ring of integers of  $K$ .

$\Delta_K$  is the discriminant of the field  $K$ .

$f_{E/K}$  is the conductor of the curve.

$\sigma_{E/K} = \log|\mathbb{N}_{K/\mathbb{Q}}(\Delta_{E/K})|/\log|\mathbb{N}_{K/\mathbb{Q}}(f_{E/K})|$ , where  $\mathbb{N}_{K/\mathbb{Q}}$  is the norm of the field extension, is the Szpiro quotient; if  $E/K$  has everywhere good reduction (and then  $f_{E/K} = 1$ ), we put  $\sigma_{E/K} = 1$ .

If  $x \in \mathcal{O}_K$  is nonzero, then  $\text{gpf}(x)$  is the greatest rational prime  $p$  so that  $\text{ord}_p(\mathbb{N}_{K/\mathbb{Q}}(x)) > 0$ .

If  $n \in \mathbb{N}$  is nonzero, then  $\omega(n)$  is the number of rational prime divisors of  $n$ .

If  $x \in K^*$ , define  $\mathfrak{m}(x) = \max_{\mathcal{P}}\{\text{ord}_{\mathcal{P}}(x)\}$ , where the maximum runs over all primes in  $\mathcal{O}_K$ .

### 3. Preliminaries

Let  $M_K$  be the set of all places of  $K$ , take  $v \in M_K$ , and let  $|\cdot|_v$  be the absolute value associated with  $v$ . Let  $n_v$  be the degree of the local extension  $K_v/\mathbb{Q}_v$ . We normalize the absolute values as in [Silverman 2009, Section VIII.5, after Example VIII.5.1]. If  $v$  is finite, then  $|p|_v = p^{-1}$ , where  $p$  is the rational prime associated to  $v$ . If  $v$  is infinite, then  $|x|_v = \max\{x, -x\}$  for every  $x \in \mathbb{Q}$ . Thanks to this choice, we have the usual product formula, i.e.,

$$\prod_{v \in M_K} |x|_v^{n_v} = 1$$

for every  $x \in K^*$ . Define  $M_K^\infty$  as the set of infinite places of  $K$  and  $M_K^0$  as the set of finite places.

Now, we define the height of a point on the curve; more details can be found in [Silverman 2009, Chapter VIII]. Given  $x \in K^*$ , define

$$h_v(x) := \max\{0, \log|x|_v\}$$

and

$$h(x) := \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} n_v h_v(x).$$

For every point  $R \neq O$  of  $E(K)$ , define

$$h_v(R) := h_v(x(R))$$

and the height of the point as

$$h(R) := h(x(R)).$$

So, for every  $R \in E(K) \setminus \{O\}$ ,

$$h(R) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} n_v h_v(R).$$

Finally, put

$$h(O) = 0,$$

where  $O$  is the identity of the curve.

Given a point  $R$  in  $E(K)$ , define the canonical height as in [Silverman 2009, Proposition VIII.9.1], i.e.,

$$\hat{h}(R) = \frac{1}{2} \lim_{N \rightarrow \infty} \frac{h(2^N R)}{4^N}.$$

We recall the properties of the height and of the canonical height that will be necessary for this paper.

- It is known that the difference between the height and the canonical height can be bounded by an explicit constant. In particular, we will use the following result. Let

$$C_E = \frac{h(j(E))}{4} + \frac{h(\Delta)}{6} + 2.14.$$

If  $E$  is defined by a Weierstrass equation in short form and with integer coefficients, then, for every  $R \in E(K)$ ,

$$|h(R) - 2\hat{h}(R)| \leq C_E.$$

This is proved in [Silverman 1990, equation 3].

- The canonical height is quadratic, i.e.,

$$\hat{h}(nR) = n^2 \hat{h}(R)$$

for every  $R$  in  $E(K)$  and  $n \in \mathbb{N}$ .

- For every nontorsion point  $R \in E(K)$ ,

$$\hat{h}(R) > 0.$$

There exists a positive constant  $J_E$ , effectively computable and depending only on  $E$  and  $K$ , such that

$$J_E \leq \hat{h}(P)$$

for every nontorsion point  $P \in E(K)$ . Thanks to [Petsche 2006, Theorem 2], we can take

$$J_E = \frac{\log|\mathbb{N}_{K/\mathbb{Q}}(\Delta_{E/K})|}{10^{15} D^3 \sigma_{E/K}^6 \log^2(104613 D \sigma_{E/K}^2)}$$

where  $\mathbb{N}_{K/\mathbb{Q}}$  is the norm of the field extension,  $D = [K : \mathbb{Q}]$ , and

$$\sigma_{E/K} = \frac{\log|\mathbb{N}_{K/\mathbb{Q}}(\Delta_{E/K})|}{\log|\mathbb{N}_{K/\mathbb{Q}}(f_{E/K})|}.$$

If  $f_{E/K} = 1$ , we put  $\sigma_{E/K} = 1$ . The conductor  $f_{E/K}$  is defined in [Silverman 2009, beginning of Section VIII.11].

In order to prove that  $B_n$  has a primitive divisor for all but finitely many terms, Silverman [1988] and Cheon and Hahn [1999] used a theorem of Siegel that says

$$\lim_{n \rightarrow \infty} \frac{h_\nu(nP)}{h(nP)} = 0$$

for every  $\nu \in M_K$ , as is proved in [Silverman 2009, Theorem IX.3.1]. This result is not effective and hence their results are not effective. We will use some results that tell us effectively how this limit goes to 0. As we will show later, for the finite places we will use some results on the formal group of the elliptic curve, and for the infinite places we will use the work in [David 1995]. The idea of using the result of David to study primitive divisors of elliptic divisibility sequences was introduced, as far as we know, by Streng [2008, Section 3].

We conclude this section by showing that we can focus only on the case when  $E$  is defined by a Weierstrass equation in short form and with integer coefficients. We will do that in Lemma 3.2. In order to prove that lemma, we need the following.

**Lemma 3.1.** *Let  $E$  be an elliptic curve defined over  $K$  by a Weierstrass equation with integer coefficients and let  $P \in E(K)$ . Let  $\nu \in M_K^0$ ,  $\mathcal{P}$  be the associated prime, and  $p$  be the associated rational prime. There exists*

$$k \leq p^{\frac{\nu(\Delta(E))}{12}} (2\mathbb{N}_{K/\mathbb{Q}}(\mathcal{P}) + 1) \max\{4, \text{ord}_{\mathcal{P}}(j(E)^{-1})\}$$

such that  $\nu(x(kP)) < 0$ .

*Proof.* Let  $E_{\mathcal{P}}$  be a minimal model for the elliptic curve over  $K_{\mathcal{P}}$  and let  $P_{\mathcal{P}}$  be the image of  $P$  under the change of variables from  $E$  to  $E_{\mathcal{P}}$ . So,  $x(P) = u_{\mathcal{P}}^2 x(P_{\mathcal{P}}) + r_{\mathcal{P}}$  for some  $u_{\mathcal{P}}, r_{\mathcal{P}} \in K_{\mathcal{P}}$ . By [Silverman 2009, Proposition VII.1.3.d],  $\nu(u_{\mathcal{P}}) \geq 0$  and  $\nu(r_{\mathcal{P}}) \geq 0$ . Note that  $12\nu(u_{\mathcal{P}}) = \nu(\Delta(E)) - \nu(\Delta(E_{\mathcal{P}})) \leq \nu(\Delta(E))$  and so

$v(u_{\mathcal{P}}) \leq v(\Delta(E))/12$ . There exists a multiple  $kP_{\mathcal{P}}$  with  $k \leq \max\{4, \text{ord}_{\mathcal{P}}(j(E_{\mathcal{P}})^{-1})\}$  such that  $kP_{\mathcal{P}}$  is not a singular point in  $E_{\mathcal{P}}(\mathbb{F}_{\mathcal{P}})$  (see [Silverman 2009, Corollary C.15.2.1]). Observe that  $\mathbb{F}_{\mathcal{P}}$  has  $\mathbb{N}_{K/\mathbb{Q}}(\mathcal{P})$  elements and then the group of nonsingular points in  $E_{\mathcal{P}}(\mathbb{F}_{\mathcal{P}})$  has at most  $2\mathbb{N}_{K/\mathbb{Q}}(\mathcal{P}) + 1$  elements. So, the order of  $kP_{\mathcal{P}}$  in the group of nonsingular points modulo  $\mathcal{P}$  is at most  $2\mathbb{N}_{K/\mathbb{Q}}(\mathcal{P}) + 1$ . Hence, there exists

$$n_{\mathcal{P}}(P_{\mathcal{P}}) \leq (2\mathbb{N}_{K/\mathbb{Q}}(\mathcal{P}) + 1) \max\{4, \text{ord}_{\mathcal{P}}(j(E_{\mathcal{P}})^{-1})\}$$

such that  $n_{\mathcal{P}}(P_{\mathcal{P}})P_{\mathcal{P}}$  reduces to the identity modulo  $\mathcal{P}$ . Given a point  $Q$  in  $E(K)$ , it is easy to show that  $Q$  reduces to the identity modulo  $\mathcal{P}$  if and only if  $v(x(Q)) < 0$ . Therefore,  $v(x(n_{\mathcal{P}}(P_{\mathcal{P}})P_{\mathcal{P}})) < 0$ .

From a classic result on formal groups,

$$v(x(p^{v(u_{\mathcal{P}})}n_{\mathcal{P}}(P_{\mathcal{P}})P_{\mathcal{P}})) < -2v(u_{\mathcal{P}}).$$

For more details on formal groups, see Lemma 5.2 or [Silverman 2009, Corollary IV.4.4]. Using that  $v(u_{\mathcal{P}}) \geq 0$  and  $v(r_{\mathcal{P}}) \geq 0$ , we have

$$\begin{aligned} v(x(p^{v(u_{\mathcal{P}})}n_{\mathcal{P}}(P_{\mathcal{P}})P_{\mathcal{P}})) &= v(u_{\mathcal{P}}^2x(p^{v(u_{\mathcal{P}})}n_{\mathcal{P}}(P_{\mathcal{P}})P_{\mathcal{P}}) + r_{\mathcal{P}}) \\ &= v(x(p^{v(u_{\mathcal{P}})}n_{\mathcal{P}}(P_{\mathcal{P}})P_{\mathcal{P}})) + 2v(u_{\mathcal{P}}) \\ &< 0. \end{aligned}$$

We conclude recalling that  $v(u_{\mathcal{P}}) \leq v(\Delta(E))/12$ . □

**Lemma 3.2.** *Let  $E/K$  be an elliptic curve defined over  $K$  by a Weierstrass model  $\mathcal{M}$ . Then, there exists an elliptic curve  $E'$  defined over  $K$  by a short Weierstrass model  $\mathcal{M}'$  with integer coefficients that is isomorphic over  $K$  to  $E$ , and a positive rational integer  $s(E/K, \mathcal{M})$  such that: if Theorem 1.2 holds with  $C(E'/K, \mathcal{M}')$  for  $E', \mathcal{M}'$ , then it holds with*

$$C(E/K, \mathcal{M}) = \max\{C(E'/K, \mathcal{M}'), s(E/K, \mathcal{M})\}$$

for  $E, \mathcal{M}$ . The constant  $s(E/K, \mathcal{M})$  is effectively computable and will be defined during the proof (see (2)). It depends only on  $E$  and  $\mathcal{M}$ .

*Proof.* Recall that  $E$  is defined by the equation

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

Let  $u$  be the smallest positive rational integer such that, after the change of variables,

$$(x, y) \rightarrow (x', y') = \left(u^2\left(x + \frac{a_1^2}{12} + \frac{a_2}{3}\right), u^3\left(y + \frac{a_1}{2}x + \frac{a_3}{2}\right)\right)$$

we have that  $E$  is isomorphic to a curve  $E'$  of the form  $y'^2 = x'^3 + ax' + b$  with  $a$  and  $b$  in  $\mathcal{O}_K$ . Let  $P'$  be the image of  $P$  under this isomorphism. So,  $x' = u^2x + r$



for  $u \in \mathbb{Z}_{\neq 0}$  and  $r \in K$ . Let  $q$  be the integral  $\mathcal{O}_K$ -ideal such that, for every  $v \in M_K^0$ ,

$$v(q) = \max\{|v(u^2)|, -v(r)\}.$$

If  $r = 0$ , we take  $q$  such that  $v(q) = |v(u^2)|$  for every  $v \in M_K^0$ . Note that  $q$  depends only on  $E$  and  $\mathcal{M}$ . Let  $B'_n$  be the elliptic divisibility sequence associated with  $E'$  and  $P'$ .

Let  $v$  be the absolute value associated with a prime  $\mathcal{P}$  coprime with  $q$ . We have  $v(u^2) = 0$  and  $v(r) \geq 0$ . If  $\mathcal{P}$  divides  $B_n$ , then  $v(x(nP)) < 0$  and

$$v(u^2x(nP) + r) = v(u^2x(nP)) = v(x(nP)) = -v(B_n) < 0.$$

Therefore,

$$v(B'_n) = v(B_n) > 0.$$

In the same way, if  $\mathcal{P}$  divides  $B'_n$ , then

$$v(B'_n) = v(B_n) > 0.$$

So, if  $\mathcal{P}$  is coprime with  $q$ , then  $\mathcal{P}$  divides  $B_n$  if and only if it divides  $B'_n$ .

Let

$$(2) \quad s = \max_{\mathcal{P}|q} \left\{ p^{(12v_{\mathcal{P}}(u) + v_{\mathcal{P}}(\Delta(E)))/12} (2\mathbb{N}_{K/\mathbb{Q}}(\mathcal{P}) + 1) (\max\{4, \text{ord}_{\mathcal{P}}(j(E')^{-1})\}) \right\},$$

where  $p$  is the rational prime associated with  $\mathcal{P}$ .

Assume  $n > s$ . We will show that, if  $\mathcal{P}$  is a primitive divisor of  $B'_n$ , then  $\mathcal{P}$  is a primitive divisor also for  $B_n$ .

Let  $\mathcal{P}$  be a primitive divisor of  $B'_n$ . Suppose that  $\mathcal{P}$  divides  $q$ . By Lemma 3.1, there exists

$$\begin{aligned} k &\leq p^{(v(\Delta(E')))/12} (2\mathbb{N}_{K/\mathbb{Q}}(\mathcal{P}) + 1) (\max\{4, \text{ord}_{\mathcal{P}}(j(E')^{-1})\}) \\ &= p^{(12v(u) + v(\Delta(E)))/12} (2\mathbb{N}_{K/\mathbb{Q}}(\mathcal{P}) + 1) (\max\{4, \text{ord}_{\mathcal{P}}(j(E')^{-1})\}) \\ &\leq s \end{aligned}$$

such that  $v(B'_k) > 0$ . But, since  $\mathcal{P}$  is a primitive divisor of  $B'_n$  we know that  $k \geq n$ . Hence,  $n \leq s$  and this is absurd since we assumed  $n > s$ . So,  $\mathcal{P}$  does not divide  $q$ . Since  $\mathcal{P}$  is a primitive divisor of  $B'_n$  and  $\mathcal{P}$  is coprime with  $q$ , then  $\mathcal{P}$  divides  $B_n$  and does not divide  $B_k$  for  $k < n$ . Therefore, it is a primitive divisor for  $B_n$ .

In conclusion, if  $n > \max\{C(E'/K, \mathcal{M}'), s\}$ , then  $B'_n$  has a primitive divisor  $\mathcal{P}$ . As we showed,  $\mathcal{P}$  is also a primitive divisor for  $B_n$ . Therefore,  $B_n$  has a primitive divisor for all  $n > \max\{C(E'/K, \mathcal{M}'), s\}$ .

Observe that  $s$  depends on  $j(E')$ ,  $\Delta(E)$ ,  $u$ ,  $r$ , and  $q$ . It is easy to show these five values depend only on  $E$  and the model defining the curve. So, we are done.  $\square$

From now on, we will assume that  $E$  is defined by a short Weierstrass equation with coefficients in  $\mathcal{O}_K$  of the form

$$y^2 = x^3 - (g_2/4)x - (g_3/4).$$

Once we prove Theorem 1.2 under this assumption, then we can prove it in general using Lemma 3.2. It is useful to have  $E$  in this form in order to apply the work in [David 1995], as we will do in Section 6.

#### 4. Structure of the proof

We start by recalling the structure of the proof of Cheon and Hahn of Theorem 1.1.

- (1) If  $\mathcal{P}$  is a nonprimitive divisor of  $B_n$ , then  $\mathcal{P}$  divides  $B_{n/q}$  for  $q$  a prime divisor of  $n$ . Moreover, if  $\nu$  is the place associated to  $\mathcal{P}$ , then  $h_\nu(nP)$  and  $h_\nu(\frac{n}{q}P)$  are roughly the same.
- (2) If  $B_n$  does not have a primitive divisor, then, for every  $\nu \in M_K^0$ , we have

$$h_\nu(nP) \leq \sum_{q|n} h_\nu\left(\frac{n}{q}P\right) + O(\log n),$$

using Step (1). Therefore,

$$\sum_{\nu \in M_K^0} h_\nu(nP) \leq \sum_{\nu \in M_K^0} \left( \sum_{q|n} h_\nu\left(\frac{n}{q}P\right) + O(\log n) \right).$$

- (3) For every  $\nu$  infinite,  $h_\nu(nP)$  is negligible compared to  $h(nP)$ . In particular,

$$\sum_{\nu \in M_K^\infty} h_\nu(nP) = o(n^2).$$

- (4) Putting together the inequalities of (2) and (3), we obtain

$$\begin{aligned} 2n^2\hat{h}(P) &= 2\hat{h}(nP) \\ &= h(nP) + O(1) \\ &= \frac{1}{D} \sum_{\nu \in M_K^0} n_\nu h_\nu(nP) + \frac{1}{D} \sum_{\nu \in M_K^\infty} n_\nu h_\nu(nP) + O(1) \\ &\leq \sum_{q|n} h\left(\frac{n}{q}P\right) + o(n^2) \\ &= 2\hat{h}(P) \sum_{q|n} \frac{n^2}{q^2} + o(n^2) \\ &= 2n^2\hat{h}(P) \left( \left( \sum_{q|n} \frac{1}{q^2} \right) + o(1) \right). \end{aligned}$$

Note that one can use even sharper arguments using a complete inclusion-exclusion to find better inequalities (see for example [Streng 2008, Proof of the main theorem]).

- (5) For every  $n$  we have  $\sum_{q|n} q^{-2} < 1$  and then the inequality of (4) does not hold for  $n$  large enough. So,  $B_n$  does not have a primitive divisor only for finitely many  $n \in \mathbb{N}$ .

In order to make this proof effective, we need to make Steps (1) and (3) effective. In Section 5, we bound  $h_v(nP) - h_v((n/q)P)$  as in Step (1). In Section 6, we make effective Step (3).

### 5. Finite places

Take  $\mathcal{P}$  a prime over a valuation  $v \in M_K^0$ . Let  $p$  be the rational prime under  $\mathcal{P}$ . Recall that  $E$  is defined by a Weierstrass equation with integer coefficients. The group of points of  $E(K_{\mathcal{P}})$  that reduce to the identity modulo  $\mathcal{P}$  is a group that is isomorphic to a formal group, as proved in [Silverman 2009, Proposition VII.2.2]. Observe that, in the hypotheses of this proposition, there is the requirement that  $E$  is in minimal form. Anyway, the proof works in the exact same way only requiring that the coefficients of  $E$  are integers in  $K_{\mathcal{P}}$ , that is our case. Let  $Q \in E(K_{\mathcal{P}})$  and, using the equation defining the elliptic curve, it is easy to show that  $3v(x(Q)) = 2v(y(Q))$  and therefore

$$(3) \quad 2v\left(\frac{x(Q)}{y(Q)}\right) = -v(x(Q)) > 0.$$

Define

$$z(Q) = \frac{x(Q)}{y(Q)} \in K_{\mathcal{P}}.$$

**Lemma 5.1.** *Take  $v \in M_K^0$  and let  $\mathcal{P}$  be the associated prime. Define  $n_{\mathcal{P}}$  as the smallest integer such that  $n_{\mathcal{P}}P$  reduces to the identity modulo  $\mathcal{P}$ . Then,  $kP$  reduces to the identity modulo  $\mathcal{P}$  if and only if  $k$  is a multiple of  $n_{\mathcal{P}}$ . Moreover,  $v(x(kP)) < 0$  if and only if  $k$  is a multiple of  $n_{\mathcal{P}}$ .*

*Proof.* Let  $E_{\text{ns}}(\mathbb{F}_{\mathcal{P}})$  be the group of nonsingular points of the curve  $E$  reduced (with respect to the given model) modulo  $\mathcal{P}$ . Suppose by contradiction that  $kP$  reduces to the identity but  $k$  is not a multiple of  $n_{\mathcal{P}}$ . Take  $q$  and  $r$  the quotient and the remainder of the division of  $k$  by  $n_{\mathcal{P}}$ . Since  $n_{\mathcal{P}}$  does not divide  $k$ , we have that  $0 < r < n_{\mathcal{P}}$ . So,

$$rP \equiv nP - kqP \equiv O - O \equiv O \pmod{\mathcal{P}}$$

and this is absurd since  $n_{\mathcal{P}}$  is the smallest positive integer such that  $n_{\mathcal{P}}P \equiv O \pmod{\mathcal{P}}$ . Vice versa, if  $k = qn_{\mathcal{P}}$ , then

$$kP \equiv q(n_{\mathcal{P}}P) \equiv qO \equiv O \pmod{\mathcal{P}}.$$

Now, we conclude by observing that a point  $Q$  reduces to the identity modulo  $\mathcal{P}$  if and only if  $v(x(Q)) < 0$ . □

**Lemma 5.2.** *Let  $Q \in E(K)$  be such that  $v(z(Q)) > 0$ . Recall that  $p$  is the rational prime such that  $v(p) > 0$ . Then  $v(z(p^e Q)) \geq e + v(z(Q))$ . In particular, if  $p^e \mid n$ , then  $v(z(nQ)) > e$ .*

*Proof.* By [Silverman 2009, Corollary IV.4.4],  $v(z(pQ)) \geq 1 + v(z(Q))$ . Now, we proceed by induction. The case  $e = 0$  is trivial. Assume that we know that  $v(z(p^{e-1}Q)) \geq e - 1 + v(z(Q))$ . Put  $Q' = p^{e-1}Q$  and for the observation at the beginning of the proof we know  $v(z(pQ')) \geq 1 + v(z(Q'))$ . Therefore,

$$v(z(p^e Q)) = v(z(pQ')) \geq 1 + v(z(Q')) = 1 + v(z(p^{e-1}Q)) \geq e + v(z(Q)).$$

Now, we deal with the second part of the lemma. Let  $n = p^e n'$  and, by Lemma 5.1,  $v(z(n'Q)) > 0$ . For the first part of the lemma,  $v(z(nQ)) \geq e + v(z(n'Q)) > e$ . □

**Lemma 5.3.** *Let  $Q \in E(K)$  be such that  $v(z(Q)) > v(p)/(p - 1)$ . Then,*

$$v(z(nQ)) = v(z(Q)) + v(n)$$

for all  $n \geq 1$ .

*Proof.* This follows by [Silverman 1988, Theorem IV.6.4, Proposition VII.2.2]. □

**Definition 5.4.** Let  $S$  be the set of finite places of  $K$  such that  $v \mid 2$  or  $v$  ramifies over  $\mathbb{Q}$ . Observe that this set is finite.

**Corollary 5.5.** *Let  $Q \in E(K)$  be such that  $v(z(Q)) > 0$ . If  $v \notin S$ , then*

$$v(z(nQ)) = v(z(Q)) + v(n)$$

for all  $n \geq 1$ .

*Proof.* Since  $v \notin S$ , we have  $v(p) = 1$  and  $p - 1 \geq 2$ . So,  $v(z(Q)) \geq 1 > v(p)/(p - 1)$  and we apply Lemma 5.3. □

**Proposition 5.6.** *Let  $E$  be an elliptic curve defined over a number field  $K$  and let  $P \in E(K)$  be a nontorsion point. Take  $v \in M_K^0$ , let  $\mathcal{P}$  be the associated prime, and  $p$  be the rational prime under  $\mathcal{P}$ . Recall that  $n_{\mathcal{P}}$  is the smallest positive integer such that  $n_{\mathcal{P}}P$  reduces to the identity modulo  $\mathcal{P}$ . Assume that  $n_{\mathcal{P}} \mid n$  and  $n_{\mathcal{P}} \neq n$ . Then, one of the following hold:*

- *There exists a prime  $q \mid n$  such that  $v(z((n/q)P)) > 0$  and*

$$v(z(nP)) = v\left(z\left(\frac{n}{q}P\right)\right) + v(q).$$

- $v \in S$  and

$$n < n_{\mathcal{P}} p^{\frac{v(p)}{p-1}+1}.$$

*Proof.* Assume  $v \notin S$  and let  $Q = n_{\mathcal{P}}P$ . Since  $n/n_{\mathcal{P}}$  is an integer greater than 1, there is a prime  $q$  that divides it. By Corollary 5.5,

$$\begin{aligned} v(z(nP)) - v\left(z\left(\frac{n}{q}P\right)\right) &= v\left(z\left(\frac{n}{n_{\mathcal{P}}}Q\right)\right) - v\left(z\left(\frac{n}{qn_{\mathcal{P}}}Q\right)\right) \\ &= v\left(\frac{n}{n_{\mathcal{P}}}\right) - v\left(\frac{n}{qn_{\mathcal{P}}}\right) = v(q). \end{aligned}$$

So, we focus on the case  $v \in S$ . Assume that there exists  $q \neq p$  such that  $q \mid n/n_{\mathcal{P}}$ . Then,

$$v(z(nP)) = v\left(z\left(\frac{n}{q}P\right)\right)$$

by [Silverman 1988, Corollary IV.4.4] and we are done since  $v(q) = 0$ . Assume now that there is no  $q \neq p$  such that  $q \mid n/n_{\mathcal{P}}$ . So,  $n = p^e n_{\mathcal{P}}$  with  $e \geq 1$  (since  $n \neq n_{\mathcal{P}}$ ) and recall that we defined  $Q = n_{\mathcal{P}}P$ .

Assume that  $e - 1 \geq v(p)/(p - 1)$ . Then, by Lemma 5.2,  $v(z(p^{e-1}Q)) > e - 1 \geq v(p)/(p - 1)$ . Therefore, by Lemma 5.3,

$$v(z(nP)) = v(z(p^e Q)) = v(z(p^{e-1} Q)) + v(p) = v\left(z\left(\frac{n}{p}P\right)\right) + v(p).$$

It remains the case  $e - 1 < v(p)/(p - 1)$ . In this case,

$$n = n_{\mathcal{P}} p^e < n_{\mathcal{P}} p^{\frac{v(p)}{p-1}+1}. \quad \square$$

**Remark 5.7.** To explicitly compute  $v(z(nP))$  in the second case of the previous proposition one can use [Stange 2016, Lemma 5.1].

**Lemma 5.8.** *Let  $v \in S$ ,  $\mathcal{P}$  be the associated prime, and  $p$  be the associated rational prime. It holds that*

$$n_{\mathcal{P}} p^{\frac{v(p)}{p-1}+1} \leq \text{gpf}(2\Delta_K)^{\frac{m(\Delta_E)}{12}} \max\{4, m(j(E)^{-1})\} (2 \text{gpf}(2\Delta_K)^D + 1) \text{gpf}(2\Delta_K)^{D+1}.$$

See Section 2 for the definition of the constants involved.

*Proof.* Recall that we are working with an elliptic curve  $E$  defined by a Weierstrass equation with integer coefficients. By Lemma 3.1,

$$n_{\mathcal{P}} \leq p^{\frac{v(\Delta(E))}{12}} (2\mathbb{N}_{K/\mathbb{Q}}(\mathcal{P}) + 1) \max\{4, \text{ord}_{\mathcal{P}}(j(E)^{-1})\}.$$

Since  $\mathcal{P}$  is a prime over a place in  $S$  and the primes that ramify divide the discriminant of the field  $\Delta_K$ , we have  $\mathbb{N}_{K/\mathbb{Q}}(\mathcal{P}) \leq \text{gpf}(2\Delta_K)^D$ . Therefore,

$$n_{\mathcal{P}} \leq \text{gpf}(2\Delta_K)^{\frac{v(\Delta(E))}{12}} \max\{4, m(j(E)^{-1})\} (2 \text{gpf}(2\Delta_K)^D + 1).$$

Moreover,  $p \leq \text{gpf}(2\Delta_K)$  and  $v(p)/(p - 1) \leq v(p) \leq D$ . □

**Definition 5.9.** Define

$$C_1 = \text{gpf}(2\Delta_K)^{\frac{m(\Delta_E)}{12}} \max\{4, m(j(E)^{-1})\} (2 \text{gpf}(2\Delta_K)^D + 1) \text{gpf}(2\Delta_K)^{D+1}.$$

**Proposition 5.10.** *Let  $E$  be an elliptic curve defined over a number field  $K$  and let  $P \in E(K)$  be a nontorsion point. Take  $v \in M_K^0$  and let  $\mathcal{P}$  be the associated prime. Assume that  $n_{\mathcal{P}} \mid n$ , that  $n_{\mathcal{P}} \neq n$ , and that  $n \geq C_1$ . Then, there exists a prime  $q \mid n$  such that*

$$h_v(nP) = h_v\left(\frac{n}{q}P\right) + 2h_v(q^{-1}).$$

*Proof.* Observe that we are in the hypotheses of Proposition 5.6. By Lemma 5.8 we know that, since  $n \geq C_1$ , we cannot be in the second case of Proposition 5.6. Therefore, there exists a prime  $q \mid n$  such that

$$v(z(nP)) = v\left(z\left(\frac{n}{q}P\right)\right) + v(q).$$

Observe that, given  $Q \in E(K)$  with  $v(x(Q)) < 0$ , then by (3),

$$h_v(x(Q)) = \log|x(Q)|_v = -2 \log \left| \frac{x(Q)}{y(Q)} \right|_v = -2 \log|z(Q)|_v.$$

Therefore,

$$h_v(nP) = -2 \log|z(nP)|_v = -2 \log \left| qz\left(\frac{n}{q}P\right) \right|_v = h_v\left(\frac{n}{q}P\right) + 2h_v(q^{-1}). \quad \square$$

### 6. Infinite places

We know that  $2n^2\hat{h}(P)$  is close to  $h(nP)$  and that

$$h(nP) = \frac{1}{D} \sum_{v \in M_K^0} h_v(nP) + \frac{1}{D} \sum_{v \in M_K^\infty} h_v(nP).$$

Thanks to the previous section, we know how to bound  $h_v(nP)$  for  $v$  finite in the case when  $B_n$  does not have a primitive divisor. Now, we need to bound  $h_v(nP)$  for  $v$  infinite. We show that, for  $n$  large enough,  $h_v(nP)$  is negligible compared to  $n^2\hat{h}(P)$ .

Recall that we are working with an elliptic curve  $E$  defined by the equation  $y^2 = x^3 - (g_2/4)x - (g_3/4)$  with  $g_2, g_3 \in \mathcal{O}_K$ . Fix an embedding  $K \hookrightarrow \mathbb{C}$  and consider the group of complex points  $E(\mathbb{C})$ . We briefly recall the properties of  $E(\mathbb{C})$ . For the details see [Silverman 2009, Chapter VI]. There is a unique lattice  $\Lambda \subseteq \mathbb{C}$  such that  $\mathbb{C}/\Lambda$  is isomorphic to  $E(\mathbb{C})$  via the map  $\phi : z \rightarrow (\wp(z), \wp'(z)/2, 1)$  (see [Silverman 2009, Theorem VI.5.1]). Thanks to [Silverman 1994, Proposition 1.1.5], we can take  $\omega_1$  and  $\omega_2$  two generators of  $\Lambda$  such that  $\tau = \omega_2/\omega_1 \in \mathbb{C}$  is in the fundamental domain. In particular,  $\Im\tau \geq \sqrt{3}/2$ , where  $\Im\tau$  is the imaginary part of  $\tau$ . We need to make this choice in order to use [David 1995, Theorem 2.1].

Before proceeding, we need to define some constants. Let

$$h = \max\{1, h(1 : g_2 : g_3), h(j(E))\},$$

where  $h(1 : g_2 : g_3)$  is the usual height on  $\mathbb{P}^2$  (for a definition see [Silverman 2009, Section VIII.5]). Let

$$\begin{aligned} \log V_1 &= \max\{h, (3\pi)/(D \cdot \mathfrak{S}\tau)\}, \\ \log V_2 &= \max\{h, (3\pi|\omega_2|^2)/(|\omega_1|^2 \cdot D \cdot \mathfrak{S}\tau)\}. \end{aligned}$$

Let  $c_1 := 3.6 \cdot 10^{41}$ , that is the constant  $c_1$  of [David 1995, Theorem 2.1] evaluated in  $k = 2$ . Define

$$(4) \quad C_3 = \max\{30, eh, \log V_1/D, \log V_2/D, D\},$$

$$(5) \quad C_2 = 54 \cdot c_1 \cdot D^6 \log V_1 \log V_2.$$

**Proposition 6.1.** *Let  $E$  be an elliptic curve defined by the equation*

$$y^2 = x^3 - (g_2/4)x - (g_3/4)$$

*for  $g_2, g_3 \in K$  and take  $P \in E(K)$ . Let  $z \in \mathbb{C}$  be so that  $\phi(z) = P$  and suppose  $\log n > C_3$ . If  $0 \leq m_1, n_1, m_2, n_2 \leq n$  with  $n_1, n_2 \neq 0$ , then*

$$\log \left| z - \frac{m_1}{n_1} \omega_1 - \frac{m_2}{n_2} \omega_2 \right| > -C_2 n^{1/2}.$$

*Proof.* David [1995, Theorem 2.1] proved that, for all integers  $0 \leq m_1, n_1, m_2, n_2 \leq n$  with  $n_1, n_2 \neq 0$ , we have

$$\log \left| z - \frac{m_1}{n_1} \omega_1 - \frac{m_2}{n_2} \omega_2 \right| > -c_1 D^6 (\log BD) (\log \log B + 1 + \log D + h)^3 \log V_1 \log V_2,$$

where

$$\log B := \max\{eh, \log n, \log V_1/D, \log V_2/D\}.$$

Since  $\log n > C_3$ , we have  $\log n > D, \log n > eh > h + 1$ , and  $\log n = \log B$ . Hence,

$$c_1 D^6 (\log BD) (\log \log B + 1 + \log D + h)^3 \log V_1 \log V_2 < C_2 \log^4 n.$$

Moreover, since  $\log n > 30$ , we have

$$\log^4 n < n^{1/2}$$

and then

$$\log \left| z - \frac{m_1}{n_1} \omega_1 - \frac{m_2}{n_2} \omega_2 \right| > -C_2 n^{1/2}. \quad \square$$

**7. Proof of Theorem 1.2**

Define

$$\rho(n) = \sum_{p|n} \frac{1}{p^2}$$

and  $\omega(n)$  as the number of prime divisors of  $n$ . It is easy to prove, by direct computation, that

$$\rho(n) < \sum_{p \text{ prime}} \frac{1}{p^2} < \frac{1}{2}.$$

Recall that  $C_1$  is defined in Definition 5.9.

**Lemma 7.1.** *Let  $n \geq C_1$ . If  $B_n$  does not have a primitive divisor, then there exists an embedding  $K \hookrightarrow \mathbb{C}$  such that*

$$\max\{\log|x(nP)|, 0\} \geq 2\hat{h}(P)n^2(1 - \rho(n)) - 2 \log n - C_E(\omega(n) + 1),$$

where with  $|x(nP)|$  we mean the absolute value in the embedding and  $C_E$  is defined in Section 2.

*Proof.* Suppose that  $B_n$  does not have a primitive divisor and take  $\nu$  finite. Let  $\mathcal{P}$  be the associated prime and assume  $\nu(B_n) > 0$ . Hence,  $n_{\mathcal{P}} | n$  but  $n \neq n_{\mathcal{P}}$  since  $B_n$  does not have a primitive divisor. So, using Proposition 5.10, there is a prime  $q_{\nu} | n$  such that

$$h_{\nu}(nP) = h_{\nu}\left(\frac{n}{q_{\nu}}P\right) + 2h_{\nu}(q_{\nu}^{-1}).$$

Let  $M_K^{0,n}$  be the set of finite places  $\nu$  such that  $h_{\nu}(nP) > 0$ . Therefore,

$$\begin{aligned} \sum_{\nu \in M_K^0} n_{\nu} h_{\nu}(nP) &= \sum_{\nu \in M_K^{0,n}} n_{\nu} h_{\nu}(nP) \\ &\leq \sum_{\nu \in M_K^{0,n}} n_{\nu} h_{\nu}\left(\frac{n}{q_{\nu}}P\right) + 2n_{\nu} h_{\nu}(q_{\nu}^{-1}) \\ &\leq \left( \sum_{q|n} Dh\left(\frac{n}{q}P\right) + 2Dh(q^{-1}) \right). \end{aligned}$$

Here we are using that  $h_{\nu}(kP) \geq 0$  for all  $\nu \in M_K$  and all  $k \geq 1$ . Thus,

$$\begin{aligned} \frac{1}{D} \sum_{\nu \in M_K^{\infty}} n_{\nu} h_{\nu}(nP) &= h(nP) - \frac{1}{D} \sum_{\nu \in M_K^0} n_{\nu} h_{\nu}(nP) \\ &\geq 2\hat{h}(nP) - C_E - \sum_{q|n} \left( h\left(\frac{n}{q}P\right) + 2 \log q \right) \end{aligned}$$



$$\begin{aligned} &\geq 2\hat{h}(nP) - C_E - 2 \log n - \sum_{q|n} \left( 2\hat{h}\left(\frac{n}{q}P\right) + C_E \right) \\ &= 2\hat{h}(P)n^2 \left( 1 - \sum_{q|n} \frac{1}{q^2} \right) - 2 \log n - C_E(\omega(n) + 1) \\ &= 2\hat{h}(P)n^2(1 - \rho(n)) - 2 \log n - C_E(\omega(n) + 1). \end{aligned}$$

Since  $h_\nu(nP) \geq 0$  for all  $\nu \in M_K$  and  $\sum_{\nu \in M_K^\infty} n_\nu = D$ , at least one of the  $h_\nu(nP)$ , for  $\nu \in M_K^\infty$ , is larger than the right-hand side. Recalling that

$$h_\nu(x(P)) = \max\{\log|x(nP)|_\nu, 0\}$$

we conclude that

$$\max\{\log|x(nP)|, 0\} \geq 2\hat{h}(P)n^2(1 - \rho(n)) - 2 \log n - C_E(\omega(n) + 1). \quad \square$$

We briefly recall the hypotheses that we are assuming. As we said in the previous section, we are assuming that  $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$  with the lattice  $\Lambda$  generated by the complex numbers  $\omega_1$  and  $\omega_2$ . Moreover, we are working with an elliptic curve defined by a Weierstrass equation with integer coefficients and in short form. Recall that  $C_2$  is defined in (5) and define

$$C_4 = 2 \max_{\nu \in M_K^\infty} \{\max\{|x(T)|_\nu \mid T \in E(\bar{K})[2] \setminus \{O\}\}\}.$$

**Proposition 7.2.** *Assume that*

$$(6) \quad 2\hat{h}(P)n^2(1 - \rho(n)) - 2 \log n - C_E(\omega(n) + 1) > 0,$$

*that  $n \geq C_1$ , and that  $\log n \geq C_3$ , as defined in (4). If  $B_n$  does not have a primitive divisor, then*

$$(7) \quad \hat{h}(P)n^2 \leq n^{1/2}(2C_2 + 4 + 2C_E + \log C_4).$$

*Proof.* Fix the embedding  $K \hookrightarrow \mathbb{C}$  of Lemma 7.1. Since  $B_n$  does not have a primitive divisor, we have

$$(8) \quad \log|x(nP)| \geq 2\hat{h}(P)n^2(1 - \rho(n)) - 2 \log n - C_E(\omega(n) + 1)$$

thanks to Lemma 7.1 and the assumption in (6). Consider the isomorphism  $\mathbb{C}/\Lambda \cong E(\mathbb{C})$  as in Section 6 and take  $z \in \mathbb{C}$  in the fundamental parallelogram of the period lattice of  $E$  such that  $\phi(z) = P$ . Assume

$$|x(nP)| \geq C_4$$

and let  $\delta$  be the  $n$ -torsion point of  $\mathbb{C}/\Lambda$  closest to  $z$  (if it is not unique, we choose one of them). Then,

$$(9) \quad \log|x(nP)| \leq -2 \log|nz - n\delta| + \log 8$$

thanks to [Ingram 2009, Lemma 8] (here we are using the assumption  $|x(nP)| \geq C_4$ ). This lemma is stated for  $K = \mathbb{Q}$ , but the proof works in the exact same way for  $K$  number field. Since  $\delta$  is an  $n$ -torsion point, we have

$$\delta = \frac{m_1}{n}\omega_1 + \frac{m_2}{n}\omega_2$$

for  $0 \leq m_1, m_2 \leq n$ . Using Proposition 6.1 and the assumption that  $\log n > C_3$ , we have

$$\log|z - \delta| = \log \left| z - \frac{m_1}{n}\omega_1 - \frac{m_2}{n}\omega_2 \right| \geq -C_2 n^{1/2}.$$

Applying inequalities (8) and (9) we have

$$(10) \quad \begin{aligned} \log 8 + 2C_2 n^{1/2} &\geq -2 \log|z - \delta| + \log 8 \\ &= 2 \log|n| - 2 \log|nz - n\delta| + \log 8 \\ &\geq -2 \log|nz - n\delta| + \log 8 \\ &\geq \log|x(nP)| \\ &\geq 2\hat{h}(P)n^2(1 - \rho(n)) - 2 \log n - C_E(\omega(n) + 1). \end{aligned}$$

Observe that  $\omega(n) \leq \log_2 n$  and  $(1 - \rho(n)) > 0.5$ . Thus, rearranging (10), we have

$$\begin{aligned} \hat{h}(P)n^2 &\leq 2\hat{h}(P)n^2(1 - \rho(n)) \\ &\leq 2 \log n + C_E(\omega(n) + 1) + \log 8 + 2C_2 n^{1/2} \\ &\leq n^{1/2}(2C_2 + 4 + 2C_E). \end{aligned}$$

Here we are using that  $n^{1/2} > \log n$  thanks to the hypothesis  $\log n > C_3$ . Recall that we obtained this inequality assuming  $|x(nP)| \geq C_4$ . If  $|x(nP)| < C_4$ , applying again (8), we have

$$\begin{aligned} \log C_4 &\geq \log|x(nP)| \\ &\geq 2\hat{h}(P)n^2(1 - \rho(n)) - 2 \log n - C_E(\omega(n) + 1). \end{aligned}$$

Therefore, one can easily show that, both in the case  $|x(nP)| < C_4$  and in the case  $|x(nP)| \geq C_4$ , we have

$$\hat{h}(P)n^2 \leq n^{1/2}(2C_2 + 4 + 2C_E + \log C_4). \quad \square$$

We are now ready to prove our main theorem. We will show that (7) does not hold if  $n$  is large enough.

*Proof of Theorem 1.2.* Define

$$C_5 = J_E^{-1}(2C_2 + 4 + 2C_E + \log C_4)$$

and take

$$(11) \quad n > \max\{C_1, C_5^{2/3}, V_1, V_2, \exp(D), (\exp(eh)), e^{30}\}.$$

We want to show that  $B_n$  has a primitive divisor.

Observe that, thanks to the assumption in (11) and the definition of  $C_3$  in (4), we have  $\log n > C_3$ . Moreover,

$$n^{3/2} > C_5 = J_E^{-1}(2C_2 + 4 + 2C_E + \log C_4) > \hat{h}(P)^{-1}(4 + 2C_E)$$

and then

$$n^2 > \log n \cdot \hat{h}(P)^{-1}(4 + 2C_E).$$

Therefore, equation (6) holds. Finally,  $n \geq C_1$ . Hence, we are in the hypotheses of Proposition 7.2.

We assume that  $B_n$  does not have a primitive divisor and we find a contradiction. Since  $B_n$  does not have a primitive divisor, we know that we can apply Proposition 7.2 and (7) must hold. But

$$\begin{aligned} n^{3/2} &\geq J_E^{-1}(2C_2 + 4 + 2C_E + \log C_4) \\ &\geq \frac{2C_2 + 4 + 2C_E + \log C_4}{\hat{h}(P)}. \end{aligned}$$

and then (7) does not hold. Therefore, we find a contradiction and then  $B_n$  must have a primitive divisor.

In conclusion, define

$$(12) \quad C_6(E/K, \mathcal{M}) = \max\{C_1, V_1, V_2, \exp(D), \exp(eh), e^{30}, C_5^{2/3}\}$$

and  $B_n$  has a primitive divisor for  $n > C_6(E/K, \mathcal{M})$ . Observe that every constant involved in the definition of  $C_6(E/K, \mathcal{M})$  does not depend on  $P$  and it is effectively computable (we will give more details in the next section). So, we are done.

Recall that we are working under the assumption that  $E$  is defined by a short Weierstrass equation with integer coefficients. In order to conclude for the general case, one has to use Lemma 3.2. □

### 8. Explicit computation

Now, we explicitly write a constant  $C(E/K, \mathcal{M})$  such that Theorem 1.2 holds. We assume that  $E$  is defined by a short Weierstrass equation with integer coefficients, the general case can be done using Lemma 3.2. Recall that we defined many constants in Section 2.

First of all, we show how to bound  $|\tau|$ , as defined at the beginning of Section 6. Recall that we are working under the assumption that  $\tau$  is in the fundamental domain. Hence, we know  $|\Re\tau| \leq 1/2$  and then we study  $\Im\tau$ , the imaginary part of  $\tau$ . Put  $q = e^{2\pi i\tau}$  and then

$$|q| = e^{-2\pi\Im\tau}.$$

So,

$$\log|q| = -2\pi\Im\tau.$$

Thanks to [Silverman 1990, Lemma 5.2.b], we have

$$|\log|q|| \leq 5.7 + \max\{\log|j(E)|, 0\}.$$

Therefore,

$$|\Im\tau| = \frac{|\log|q||}{2\pi} \leq \frac{5.7 + \max\{\log|j(E)|, 0\}}{2\pi}.$$

We obtain

$$|\tau|^2 = |\Re\tau|^2 + |\Im\tau|^2 \leq \frac{1}{4} + \left(\frac{5.7 + \max\{\log|j(E)|, 0\}}{2\pi}\right)^2.$$

Let

$$\begin{aligned} \log V'_1 &= \max\{h, (2\sqrt{3}\pi)/D\}, \\ \log V'_2 &= \max\left\{h, \left(2\sqrt{3}\pi\left(\frac{1}{4} + \left(\frac{5.7 + \max\{\log|j(E)|, 0\}}{2\pi}\right)^2\right)\right)/D\right\}, \\ C'_2 &= 54 \cdot c_1 \cdot D^6 \log V'_1 \log V'_2. \end{aligned}$$

By the definitions of  $V_1$ ,  $V_2$ , and  $C_2$  given at the beginning of Section 6, we have  $V'_1 \geq V_1$ ,  $V'_2 \geq V_2$ , and  $C'_2 \geq C_2$ . Hence, by (12), Theorem 1.2 holds for

$$(13) \quad C(E/K, \mathcal{M}) = \max\left\{C_1, V'_1, V'_2, \exp(D), \exp(eh), e^{30}, \left(\frac{2C'_2 + 4 + 2C_E + \log C_4}{J_E}\right)^{2/3}\right\}$$

where

$$\begin{aligned} h &= \max\{1, h(1 : g_2 : g_3), h(j(E))\}, \quad c_1 = 3.6 \cdot 10^{41}, \\ C_1 &= \text{gpf}(2\Delta_K)^{\frac{m(\Delta_E)}{12}} \max\{4, m(j(E)^{-1})\} (2 \text{gpf}(2\Delta_K)^D + 1) \text{gpf}(2\Delta_K)^{D+1}, \\ \log V'_1 &= \max\{h, (2\sqrt{3}\pi)/D\}, \\ \log V'_2 &= \max\left\{h, \left(2\sqrt{3}\pi\left(\frac{1}{4} + \left(\frac{5.7 + \max\{\log|j(E)|, 0\}}{2\pi}\right)^2\right)\right)/D\right\}, \end{aligned}$$

$$\begin{aligned}
 C'_2 &= 54 \cdot c_1 \cdot D^6 \log V'_1 \log V'_2, \\
 C_E &= \frac{h(j(E))}{4} + \frac{h(\Delta)}{6} + 2.14, \\
 C_4 &= 2 \max\{|x(T)| \mid T \in E(\bar{\mathbb{Q}})[2] \setminus \{O\}\}, \\
 J_E &= \frac{\log|\mathbb{N}_{K/\mathbb{Q}}(\Delta_{E/K})|}{10^{15} D^3 \sigma_{E/K}^6 \log^2(104613 D \sigma_{E/K}^2)}.
 \end{aligned}$$

### 9. Examples

We apply our main theorem to a couple of examples.

**Example 9.1.** Let  $E$  be the rational elliptic curve defined by the equation  $y^2 = x^3 - 4x + 4$ . In this case,  $D = \Delta_K = 1$ ,  $h \approx 10.23$ ,  $j(E) = -27648/11$ ,  $\Delta_{E/K} = -2816$ ,  $\sigma_{E/K} \approx 1.78$ , and  $C_4 \approx 4.76$ . Using (13), we have

$$C(E/K, \mathcal{M}) \approx 5.88 \cdot 10^{42} < 6 \cdot 10^{42}.$$

With our methods, even if we optimize all the estimates in the proof, we cannot hope to find a constant for Theorem 1.2 much smaller than the one of Example 9.1. Indeed, in the definition of  $c_1$  and of  $J_E$  appear constants that are very large (namely  $10^{41}$  and  $10^{15}$ ) and so, even if the other constants involved are small, we cannot find a constant much smaller than  $10^{38}$ . In order to find better constants, one would need to have better constants in the bound of canonical height and in logarithmic approximation.

Now, we present another example where we show the techniques that one can use to find the terms without a primitive divisor.

**Example 9.2.** We focus on the elliptic curve  $y^2 = x^3 - 2x$  and  $P = (2, 2) \in E(\mathbb{Q})$ . The first terms of the sequence are  $B_1 = 1$ ,  $B_2 = 2^2$ ,  $B_3 = 1$ ,  $B_4 = (2^4)(3^2)(7^2)$ , and  $B_5 = (17)^2(19)^2$ . Hence,  $B_1$  and  $B_3$  do not have a primitive divisor. For the terms that have very large indexes, we can use Theorem 1.2. So, we apply Theorem 1.2 with  $C(E/K, \mathcal{M})$  as defined in (13). In the definition of  $C(E/K, \mathcal{M})$  we substitute  $J_E$  with 0.3. Indeed, for every rational nontorsion point of  $E$ , we have  $\hat{h}(P) > 0.3$  and  $J_E$  is a constant such that  $J_E < \hat{h}(P)$ . The minimum of the canonical height of the rational nontorsion points of  $E$  is computed in [LMFDB], where the canonical height is defined as the double of our canonical height. By Theorem 1.2 we have that, for  $n \geq 2 \cdot 10^{31}$ ,  $B_n$  has a primitive divisor.

To deal with the terms with indexes smaller than  $2 \cdot 10^{31}$ , we can use the following techniques. By [Voutier and Yabuta 2012, Theorem 1.3] and [Verzobio 2021a],  $B_n$  has a primitive divisor for  $n$  even. So, we focus on the terms with odd indexes. As an easy corollary of [Voutier and Yabuta 2012, Lemma 3.4], we have that if  $B_n$  does not have a primitive divisor, then  $\log B_n \leq 0.18n^2$ . So, we can compute the

values of  $B_n$  and check if the inequality holds (this is much faster than computing the factorization of the terms). As far as we know, the faster way to compute  $B_n$  is to use [Verzobio 2022, Theorem 1.9], where it is proved that, for  $k \geq 9$ ,

$$(14) \quad b_k = \frac{b_{k-2}b_{k-6}b_4^2 - b_{k-4}^2b_6b_2}{b_{k-8}b_2^2}$$

where  $b_k = \pm\sqrt{B_k}$  for an appropriate choice of the sign (for more details, see [Verzobio 2022, Definition B]). One can check that  $\log B_n > 0.18n^2$  for  $4 \leq n \leq 10^5$  using PARI/GP [2018] and then  $B_n$  has a primitive divisor for  $4 \leq n \leq 10^5$ . So, our bound is too large to be computationally useful and then new methods are needed to bridge the gap.

### Acknowledgements

This paper is part of the author’s PhD thesis at Università di Pisa. Moreover, this project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Grant Agreement No. 101034413.

I thank the referee for many helpful comments.

### References

- [Cheon and Hahn 1999] J. Cheon and S. Hahn, “The orders of the reductions of a point in the Mordell–Weil group of an elliptic curve”, *Acta Arith.* **88**:3 (1999), 219–222. MR Zbl
- [David 1995] S. David, “Minorations de formes linéaires de logarithmes elliptiques”, *Mém. Soc. Math. France (N.S.)* 62 (1995), iv+143. MR Zbl
- [Ingram 2009] P. Ingram, “Multiples of integral points on elliptic curves”, *J. Number Theory* **129**:1 (2009), 182–208. MR Zbl
- [Ingram and Silverman 2012] P. Ingram and J. H. Silverman, “Uniform estimates for primitive divisors in elliptic divisibility sequences”, pp. 243–271 in *Number theory, analysis and geometry*, edited by D. Goldfeld et al., Springer, 2012. MR Zbl
- [LMFDB] The LMFDB Collaboration, “The  $L$ -functions and modular forms database”, electronic reference, available at <http://www.lmfdb.org>.
- [PARI/GP 2018] “PARI/GP version 2.11.1”, 2018, available at <http://pari.math.u-bordeaux.fr>.
- [Petsche 2006] C. Petsche, “Small rational points on elliptic curves over number fields”, *New York J. Math.* **12** (2006), 257–268. MR Zbl
- [Silverman 1988] J. H. Silverman, “Wieferich’s criterion and the  $abc$ -conjecture”, *J. Number Theory* **30**:2 (1988), 226–237. MR Zbl
- [Silverman 1990] J. H. Silverman, “The difference between the Weil height and the canonical height on elliptic curves”, *Math. Comp.* **55**:192 (1990), 723–743. MR Zbl
- [Silverman 1994] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, 1994. MR Zbl

- [Silverman 2009] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics **106**, Springer, 2009. MR Zbl
- [Stange 2016] K. E. Stange, “Integral points on elliptic curves and explicit valuations of division polynomials”, *Canad. J. Math.* **68**:5 (2016), 1120–1158. MR Zbl
- [Streng 2008] M. Streng, “Divisibility sequences for elliptic curves with complex multiplication”, *Algebra Number Theory* **2**:2 (2008), 183–208. MR Zbl
- [Verzobio 2021a] M. Verzobio, “Primitive divisors of elliptic divisibility sequences for elliptic curves with  $j = 1728$ ”, *Acta Arith.* **198**:2 (2021), 129–168. MR Zbl
- [Verzobio 2021b] M. Verzobio, “Primitive divisors of sequences associated to elliptic curves with complex multiplication”, *Res. Number Theory* **7**:2 (2021), art. id. 37. MR Zbl
- [Verzobio 2022] M. Verzobio, “A recurrence relation for elliptic divisibility sequences”, *Riv. Math. Univ. Parma (N.S.)* **13**:1 (2022), 223–242. MR Zbl
- [Voutier and Yabuta 2012] P. Voutier and M. Yabuta, “Primitive divisors of certain elliptic divisibility sequences”, *Acta Arith.* **151**:2 (2012), 165–190. MR Zbl

Received March 10, 2022. Revised September 4, 2023.

MATTEO VERZOBIO  
INSTITUTE OF SCIENCE AND TECHNOLOGY AUSTRIA  
KLOSTERNEUBURG  
AUSTRIA  
matteo.verzobio@gmail.com





# PACIFIC JOURNAL OF MATHEMATICS

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

[msp.org/pjm](http://msp.org/pjm)

## EDITORS

Don Blasius (Managing Editor)  
Department of Mathematics  
University of California  
Los Angeles, CA 90095-1555  
[blasius@math.ucla.edu](mailto:blasius@math.ucla.edu)

Paul Balmer  
Department of Mathematics  
University of California  
Los Angeles, CA 90095-1555  
[balmer@math.ucla.edu](mailto:balmer@math.ucla.edu)

Vyjayanthi Chari  
Department of Mathematics  
University of California  
Riverside, CA 92521-0135  
[chari@math.ucr.edu](mailto:chari@math.ucr.edu)

Matthias Aschenbrenner  
Fakultät für Mathematik  
Universität Wien  
Vienna, Austria  
[matthias.aschenbrenner@univie.ac.at](mailto:matthias.aschenbrenner@univie.ac.at)

Atsushi Ichino  
Department of Mathematics  
Kyoto University  
Kyoto 606-8502, Japan  
[atsushi.ichino@gmail.com](mailto:atsushi.ichino@gmail.com)

Robert Lipshitz  
Department of Mathematics  
University of Oregon  
Eugene, OR 97403  
[lipshitz@uoregon.edu](mailto:lipshitz@uoregon.edu)

Kefeng Liu  
Department of Mathematics  
University of California  
Los Angeles, CA 90095-1555  
[liu@math.ucla.edu](mailto:liu@math.ucla.edu)

Dimitri Shlyakhtenko  
Department of Mathematics  
University of California  
Los Angeles, CA 90095-1555  
[shlyakht@ipam.ucla.edu](mailto:shlyakht@ipam.ucla.edu)

Paul Yang  
Department of Mathematics  
Princeton University  
Princeton NJ 08544-1000  
[yang@math.princeton.edu](mailto:yang@math.princeton.edu)

Ruixiang Zhang  
Department of Mathematics  
University of California  
Berkeley, CA 94720-3840  
[ruixiang@berkeley.edu](mailto:ruixiang@berkeley.edu)

## PRODUCTION

Silvio Levy, Scientific Editor, [production@msp.org](mailto:production@msp.org)

---

See inside back cover or [msp.org/pjm](http://msp.org/pjm) for submission instructions.

---

The subscription price for 2023 is US \$605/year for the electronic version, and \$820/year for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and Web of Knowledge (Science Citation Index).


---

The Pacific Journal of Mathematics (ISSN 1945-5844 electronic, 0030-8730 printed) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

---

PJM peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**  
nonprofit scientific publishing

<http://msp.org/>

© 2023 Mathematical Sciences Publishers

# PACIFIC JOURNAL OF MATHEMATICS

Volume 325    No. 2    August 2023

---

|  |     |
|--|-----|
| Totally geodesic hyperbolic 3-manifolds in hyperbolic link complements of tori in $S^4$  | 191 |
| MICHELLE CHU and ALAN W. REID  |     |
| Infinite homotopy stable class for 4-manifolds with boundary   | 209 |
| ANTHONY CONWAY, DIARMUID CROWLEY and MARK POWELL   |     |
| Counterexamples to the nonsimply connected double soul conjecture  | 239 |
| JASON DEVITO   |     |
| The fundamental group of an extension in a Tannakian category and the unipotent radical of the Mumford–Tate group of an open curve | 255 |
| PAYMAN ESKANDARI and V. KUMAR MURTY  |     |
| The size of semigroup orbits modulo primes   | 281 |
| WADE HINDES and JOSEPH H. SILVERMAN  |     |
| Tropical Lagrangian multisections and toric vector bundles   | 299 |
| YAT-HIN SUEN   |     |
| Some effectivity results for primitive divisors of elliptic divisibility sequences   | 331 |
| MATTEO VERZOBIO  |     |
| Poisson manifolds of strong compact type over 2-tori   | 353 |
| LUKA ZWAAN   |     |