Some effectivity results over primitive divisors of elliptic divisibility sequences

Matteo Verzobio

Abstract

Let $P$ be a non-torsion point on an elliptic curve in minimal form defined over a number field and consider $B_n$ the sequence 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.

1 Introduction

Let $E$ be an elliptic curve, in minimal form, defined by the equation

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

with the coefficients in a number field $K$. Take $P \in E(K)$ a non-torsion point. Let us define

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

with $A_n$ and $B_n$ two relatively prime integral ideals. We want to understand when a term of the sequence $\{B_n\}_{n>0}$ has a primitive divisor, i.e., when there exists a prime ideal $p$ such that

$$p \nmid B_1B_2\cdots B_{n-1} \text{ but } p \mid B_n.$$

In [4], Silverman proved that if $E$ is defined over $\mathbb{Q}$, then $B_n$ has not a primitive divisors for $n$ large enough. This result was generalized for every number field $K$ in [1]. For some class of curves there is some effective results, for example in [2] it was proved that if $E$ is defined over $\mathbb{Q}$ and $E(\mathbb{Q})[2]$ is not trivial, then $B_n$ has a primitive divisor for every $n$ even and bigger than an effective computable constant. We will generalize these results.

**Theorem 1.** There exists a constant $K(E, P)$, effectively computable, such that $B_n$ has a primitive divisor for $n > K(E, P)$. The constant can be written as

$$K(E, P) := \max\{H(P)^{1/[K:\mathbb{Q}]}, K_E\},$$

with $K_E$ depending only on $E$. 

1
2 Preliminaries

Let $M_K$ be the set of all places of $K$, take $\nu \in M_K$ and $|\cdot|_{\nu}$ be the absolute value associated to the valuation $\nu$, normalized as in [5, VIII.5]. Let $D = [K : \mathbb{Q}]$ and $n_{\nu}$ be the degree of the local extension $K_{\nu}/\mathbb{Q}_{\nu}$. Given $x \in K^*$, define

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

and

$$h(x) := \frac{1}{[K : \mathbb{Q}]} \sum_{\nu \in M_K} n_{\nu} h_{\nu}(x).$$

Moreover, for every point $R \neq O$ of the elliptic curve, we define

$$h_{\nu}(R) := h_{\nu}(x(R))$$

and the height of the point as

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

So,

$$h(R) = \frac{1}{[K : \mathbb{Q}]} \sum_{\nu \in M_K} n_{\nu} h_{\nu}(R).$$

Given a point $R$ in $E(K)$, we define the canonical height as in [5, Proposition VIII.9.1], i.e.

$$\hat{h}(R) = \lim_{N \to \infty} 4^{-N} h(2^N R).$$

First of all, we recall the properties of the height and of the canonical height that will be necessary in this paper. For the details see [5, Chapter VIII].

- There exists an effectively computable constant $C_E$ such that, for every $R \in E(K)$,

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

- The canonical height is quadratic, i.e.

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

  for every $R$ in $E(K)$.

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

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

The minimum of the canonical height for non-torsion points exists and it is effectively computable.
Take \( p \) a prime over a valuation \( \nu \in M^0_K \), that is the set of finite valuations. Given a point \( Q \) in \( E(K) \), it is easy to show that \( Q \) reduces to the identity modulo \( p \) if and only if \( \nu(x(Q)) < 0 \). The group of points of \( E(K_p) \) that reduce to the identity modulo \( p \) is a group that is isomorphic to a formal group, as proved in [3] Proposition VII.2.2]. Let \( Q \) be a point in this group and then, using the equation defining the elliptic curve, it is easy to show that \( 3\nu(x(Q)) = 2\nu(y(Q)) \) and therefore

\[
2\nu\left(\frac{x(Q)}{y(Q)}\right) = -\nu(x(Q)) > 0.
\]

We want to use the work in [5].

**Theorem 2.** [6] Lemma 10] Take \( \nu \in M^0_K \), let \( p \) be the prime associated to \( \nu \) and \( p = p \cap \mathbb{Z} \). Suppose \( \nu(x(Q)) < 0 \). Define \( z = x(Q)/y(Q) \) and so \( \nu(z) > 0 \). Put \( [n]z = x(nQ)/y(nQ) \). There exist \( b, j, h \) and \( w \) in \( \mathbb{Z}^0 \cup \{ \infty \} \), depending on \( E, \nu \) and \( Q \), such that

\[
\nu([n]z) = \begin{cases} 
2^j \nu(z) + \frac{b^j-1}{b-1}h + \nu((n) - j\nu(p) + w & \text{if } \nu(n) j\nu(p) + \frac{b^{\nu(n)/\nu(p)}-1}{b-1}h & \text{if } \nu(n) = j\nu(p).
\end{cases}
\]

(1)

In particular, if \( \nu \nmid 2 \) and \( \nu \) does not ramify, then

\[
\nu([n]z) = \nu(z) + \nu(n).
\]

**Proposition 3.** Take \( \nu \in M^0_K \) and \( q \) a rational prime. Suppose \( \nu(x(\frac{n}{q}P)) < 0 \). Then,

\[
h_\nu(nP) - h_\nu\left(\frac{n}{q}P\right) \leq \begin{cases} 
2h_\nu(q) & \text{or} \\
\frac{2h_\nu(q)}{C} & \text{or}
\end{cases}
\]

with \( C \) a constant that can be written in the form \( C = \hat{h}(P)D_1 + D_2 \), with \( D_1 \) and \( D_2 \) that depend only on \( E \) and \( K \). The second case can happen only if \( \nu \) is unramified or divides \( 2 \).

**Proof.** Let \( S \) be the set of finite absolute value such that \( \nu \mid 2 \) or \( \nu \) ramifies. Observe that, if \( \nu(x(Q)) < 0 \), then

\[
h_\nu(x(Q)) = \log |x(Q)|_\nu = -2\log \left|\frac{x(Q)}{y(Q)}\right|_\nu = -2\log |z(Q)|_\nu.
\]

Suppose \( \nu \) finite and not in \( S \). So,

\[
h_\nu(x(nP)) = -2\log |z(nP)|_\nu
\]

\[
= -2\log \left|z\left(\frac{n}{q}P\right)\right|_\nu - 2\log |q|_\nu
\]

\[
= h_\nu\left(\frac{n}{q}P\right) + 2h_\nu(q).
\]

3
Suppose now $\nu \in S$. Let $n_p$ be the smallest integer such that $n_p P$ reduces to the identity modulo $p$. Put $z' = [n_p]z$ and $n/n_p = n'$. We want to study $\nu([n']z')$.

Suppose $\nu(n'/q) \leq j\nu(p)$. Therefore,

$$\nu([n]z) = \nu([n']z') \leq \nu([p^j+1]z')$$

and thus

$$h_\nu(nP) \leq h_\nu([p^j+1]n_p P) \leq h(p^j+1)n_p P \leq (p^j+1)n_p 2^j h(P) + C_E.$$

Using the definition of $j$ in [6, Lemma 10], it is easy to show that $j \leq \log_2 D$ and so $p^j+1n_p$ can be bounded by a constant depending only on $E$ and $K$. If instead $\nu(n'/q) > j\nu(p)$, then

$$\nu([n]z) - \nu([n/q]z) = \nu([n']z') - \nu([n'/q]z') = \nu(q)$$

and we conclude as in the first case.

Define

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

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

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

**Lemma 4.** If $B_n$ has not a primitive divisor, then there exists an immersion $K \hookrightarrow \mathbb{C}$ such that

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

where with $|x(nP)|$ we mean the absolute value in the immersion.

**Proof.** Suppose $B_n$ has not a primitive divisor and take $\nu$ finite. We know that, if $h_\nu(nP) > 0$, then $h_\nu(n/q_\nu P) > 0$ for some prime $q_\nu$. So,

$$\sum_{\nu | \infty} n_\nu \nu(nP) = \sum_{\nu \in S} n_\nu h_\nu(nP) + \sum_{\nu \in M_k \setminus S} n_\nu h_\nu(nP)$$

$$\leq \sum_{\nu \in M_k \setminus S} n_\nu h_\nu(n/q_\nu P) + 2n_\nu h_\nu(q_\nu) +$$

$$+ \sum_{\nu \in S} n_\nu h_\nu(n/q_\nu P) + 2n_\nu h_\nu(q_\nu) + DC$$

$$\leq D\#SC + \sum_{q \mid n} Dh(n/q P) + 2Dh(q).$$

4
Thus,

\[
\frac{1}{[K : \mathbb{Q}]} \sum_{\nu | \infty} n_\nu h_\nu(nP) = \hat{h}(nP) - \frac{1}{[K : \mathbb{Q}]} \sum_{\nu | \infty} n_\nu h_\nu(nP) \\
\geq n^2 \hat{h}(P) - C_E - 2h(n) - \sum_{q | n} \left( \hat{h}(n/qP) + C_E \right) - \#SC \\
\geq \hat{h}(P)n^2(1 - \rho(n)) - 2\log n - C_E(\omega(n) + 1) - \#SC.
\]

Since \( h_\nu(nP) \geq 0 \) for all \( \nu \) and \( \sum_{\nu | \infty} n_\nu = D \), then at least one of the \( h_\nu(nP) \), for \( \nu | \infty \), is bigger than

\[
\hat{h}(P)n^2(1 - \rho(n)) - 2\log n - C_E(\omega(n) + 1) - \#SC.
\]

Now, we briefly recall the properties of the complex component of \( E \). For the details see [5, Chapter VI]. There is an isomorphism \( \phi : \mathbb{C}/\Lambda \rightarrow E(\mathbb{C}) \) for \( \Lambda \) a lattice with

\[
x(\phi(z)) = \varphi(z) := \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{(z - \omega)^2} + \frac{1}{\omega^2}.
\]

We will assume that the lattice \( \Lambda \) is generated by 1 and a complex number \( \tau \). Define \( \Lambda_1 \) as the set of points \( w \) of \( \mathbb{C} \) such that 0 is the element of \( \Lambda \) nearest to \( w \). If \( z \in \Lambda_1 \), then it is easy to show that there is an effectively computable constant \( C_1 \geq 1 \), depending only on \( E \), such that

\[
\left| \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{(z - \omega)^2} + \frac{1}{\omega^2} \right| \leq C_1.
\]

3 Proof of the theorem

**Proof of Theorem** Suppose that \( B_n \) has not a primitive divisor. Assume \( n \geq \max\{70000, D\} \). We take the immersion \( K \hookrightarrow \mathbb{C} \) such that it holds the inequality of Lemma [4]. With \( |\cdot| \) we denote the absolute value relative to the immersion. Consider the isomorphism \( \mathbb{C}/\Lambda \cong E(\mathbb{C}) \) as defined at the end of the previous section and take \( z \in \Lambda_1 \) such that \( \phi(z) = P \). If \( |x(nP)| < 2C_1 \), then

\[
\log 2C_1 \geq \log |x(nP)| \\
\geq \hat{h}(P)n^2(1 - \rho(n)) - 2\log n - C_E(\omega(n) + 1) - \#SC.
\]
Assume now $|x(nP)| \geq 2C_1$ and let $\delta$ be the $n$-torsion point of $C/\Lambda$ nearest to $z$. Then, 

$$|nz - n\delta| \leq \frac{1}{\sqrt{|x(nP)| - C_1}}$$

since $n(z - \delta) \in \Lambda_1$. Therefore,

$$|z - \delta|^2 \leq \frac{1}{n^2(|x(nP)| - C_1)} \leq \frac{1}{|x(nP)|}.$$

We want to apply the work in [3].

**Theorem 5** (Corollary 2.16, [3]). Suppose that $\Lambda$ is generated by $1$ and $\tau$. There exist two effective constants $K_1$ and $K_2$, depending only on $E$ with the following properties. Let $\log V_1 := \max\{K_1, h(P)\}$ and $\log V_2 = K_1$. Fix $n \in \mathbb{N}$ such that $\log n > \max\{\log V_1, \log V_2\}$/D. For all integers $0 \leq m_1, n_1, m_2, n_2 \leq n$ with $n_1, n_2 \neq 0$ we have

$$\log |z - \frac{m_1}{n_1}\tau - \frac{m_2}{n_2}| > -K_2D^6(\log n + \log D)(\log \log n + 1 + \log D)^3 \log V_1 \log V_2$$

where $\phi(z) = P$.

We want to apply this theorem to our case. Observe that $\delta$ is in the form $\frac{m_1}{n_1}\tau + \frac{m_2}{n_2}$. So,

$$\log |z - \delta| \geq -K_2D^6(\log n + \log D)(\log \log n + 1 + \log D)^3 \log V_1 \log V_2$$

and then

$$\hat{h}(P)n^2(1 - \rho(n)) - 2\log n - C_E(\omega(n) + 1) - #SC \leq \log |x(nP)|$$

$$\leq -2\log |z - \delta| \leq 2K_2D^6(\log n + \log D)(\log \log n + 1 + \log D)^3 \log V_1 \log V_2.$$

As we will show, this inequality holds only for $n$ small, since the LHS growth as $n^2$ and the RHS is logarithmic. Observe that $\omega(n) \leq \log_2 n$ and $(1 - \rho(n)) > 0.5$. Since $n > \max\{70000, D\}$, then

$$(\log n + \log D)(\log \log n + 1 + \log D)^3 \leq n.$$ 

Therefore, the inequality could hold only for

$$n < \frac{1}{(1 - \rho(n))n\hat{h}(P)} \left(2\log n + C_E(\omega(n) + 1) + #SC + 2K_2D^6(\log n + \log D)(\log \log n + 1 + \log D)^3 \log V_1 \log V_2\right)$$

$$< \frac{2}{\hat{h}(P)} \left(2C_E + 2 + 2D^6K_2 \log V_1 \log V_2 + #SC\right).$$
If $|x(nP)| \leq 2C_1$, then, proceeding as before, $B_n$ can have a primitive divisor only for
\[
  n < \frac{2}{h(P)} \left( 2C_E + 2 + 2 \log C_1 + \#SC \right).
\]
The constant $K_2$ is the constant $C_4$ of [Corollary 2.16, [3]] and it is independent from $E$. The constant $K_1$ can be taken as
\[
  K_1 := (\max_{z \in \Lambda_1} |z|)^2
\]
and let
\[
  J = \min_{R \in E(\mathbb{Q}) \setminus E_{\text{tor}}(\mathbb{Q})} \hat{h}(R).
\]
Observe that
\[
  \frac{h(P)}{\hat{h}(P)} \leq \frac{\hat{h}(P) + C_E}{\hat{h}(P)} \leq 1 + \frac{C_E}{J}.
\]
Thus, both the previous inequalities can hold only for
\[
  n \leq \frac{2}{J} \left( 2C_E + 2 + 2D^6K_2K_1^2(J + C_E) + \#SD_1 + \#SJD_2 + \log 2C_1 \right) := C_5.
\]
Observe that $C_5$ depends only on $E$. So, $B_n$ has a primitive divisor only for
\[
  n \leq \max \left\{ C_5, 70000, D, V_1^{1/D}, V_2^{1/D} \right\}.
\]
The constant is effectively computable since every constant involved is effective. We conclude using the definitions of $V_1$ and $V_2$. \qed

References

[1] 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):219–222, 1999.

[2] Graham Everest, Gerard Mclaren, and Thomas Ward. Primitive divisors of elliptic divisibility sequences. *J. Number Theory*, 118(1):71–89, 2006.

[3] Noriko Hirata-Kohno. Formes linéaires de logarithmes de points algébriques sur les groupes algébriques. *Invent. Math.*, 104(2):401–433, 1991.

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

[5] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.
[6] Katherine E. Stange. Integral points on elliptic curves and explicit valuations of division polynomials. *Canad. J. Math.*, 68(5):1120–1158, 2016.

UNIVERSITÀ DI PISA, DIPARTIMENTO DI MATEMATICA, LARGO BRUNO PONTECORVO 5, PISA, ITALY

E-mail address: verzobio@student.dm.unipi.it