Journal of Number Theory 279 (2026) 170–183

Contents lists available at ScienceDirect

Journal of Number Theory

journal homepage: www.elsevier.com/locate/jnt

General Section

Divisibility sequences related to abelian varieties isogenous to a power of an elliptic curve

Stefan Barańczuk [a], Bartosz Naskręcki [a], Matteo Verzobio [b,*]

[a] *Faculty of Mathematics and Computer Science, Adam Mickiewicz University in Poznań, ul. Uniwersytetu Poznańskiego 4, 61-614, Poznań, Poland*
[b] *Institute of Science and Technology Austria, Am Campus 1, Klosterneuburg, Austria*

ARTICLE INFO

Article history:
Received 22 November 2024
Received in revised form 13 June 2025
Accepted 13 June 2025
Available online 18 July 2025
Communicated by S.J. Miller

Keywords:
Divisibility sequences
Abelian varieties
Elliptic divisibility sequences
Isogenies
Primitive divisors

ABSTRACT

Let A be an abelian variety defined over a number field K, E/K be an elliptic curve, and $\phi : A \to E^m$ be an isogeny defined over K. Let $P \in A(K)$ be such that $\phi(P) = (Q_1, \ldots, Q_m)$ with $\mathrm{Rank}_{\mathbb{Z}}(\langle Q_1, \ldots, Q_m \rangle) = 1$. We will study a divisibility sequence related to the point P and show its relation with elliptic divisibility sequences.

© 2025 The Author(s). Published by Elsevier Inc. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

1. Introduction

Let A be an abelian variety defined over a number field K and P be a non-torsion point in $A(K)$. Let $\mathcal{O}_K$ denote the ring of integers of K and $\mathcal{A}/\mathcal{O}_K$ be the Néron model for A/K.

* Corresponding author.
E-mail addresses: stefbar@amu.edu.pl (S. Barańczuk), bartosz.naskrecki@amu.edu.pl (B. Naskręcki), matteo.verzobio@gmail.com (M. Verzobio).

https://doi.org/10.1016/j.jnt.2025.06.001
0022-314X/© 2025 The Author(s). Published by Elsevier Inc. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

Let S be a finite set of primes in K. For each $n \geq 1$, define the integral ideal $C_n(\mathcal{A}, P, S)$ in $\mathcal{O}_K$ as

$$C_n(\mathcal{A}, P, S) = \prod_{\substack{\mathfrak{p}: nP \equiv O \bmod \mathfrak{p} \\ \mathfrak{p} \notin S}} \mathfrak{p}$$

where with $nP \equiv O \mod \mathfrak{p}$ we mean that nP reduces to the identity in $\mathcal{A}$ reduced modulo $\mathfrak{p}$.

The goal of this paper is to find some examples of sequences $C_n(\mathcal{A}, P, S)$ such that, for all but finitely many n, $C_n(\mathcal{A}, P, S)$ has a primitive divisor, i.e. there exists a prime $\mathfrak{p}$ that divides C_n and does not divide C_k for $k < n$. Notably, it is worth mentioning that the presence of a primitive divisor for almost all values of n remains unaffected if we substitute the set S with another finite set of primes.

In the case when A is an elliptic curve, P is a point on it, and the curve $\mathcal{A}$ is defined via its Weierstrass equation, every term $C_n(A, P, S)$ is the product of the prime ideals not in S which divide the n-term of the corresponding elliptic divisibility sequence $B_n(E, P)$, defined by the denominators of the x-coordinate of the point nP. For the properties of elliptic divisibility sequences, see [14]. It is well-established that, for all but finitely many values of n, $B_n(E, P)$ contains a primitive divisor, as shown in [10, Proposition 10] and [3, Main Theorem].

Since the case when A is an elliptic curve is well understood, we focus on higher-dimension cases. Let A be an abelian variety of dimension ≥ 2 defined over a number field K and let $P \in A(K)$. Assume that $\mathbb{Z}P$ is Zariski dense in A. It is conjectured [11, Proposition 9 and Conjecture 10] that there are infinitely many n such that nP does not reduce to the identity modulo any prime, outside a finite set of primes S. So, $C_n(\mathcal{A}, P, S)$ does not have a primitive divisor for infinitely many $n \in \mathbb{N}$. For a nice potential application of these sequences to Hilbert's tenth problem, see [4, Remark (i), page 4].

Since we are interested in sequences that have a primitive divisor for all but finitely many terms, we will focus on examples where $\mathbb{Z}P$ is not Zariski dense in A. More precisely, we will study the following case. Let A be an abelian variety defined over a number field K and let $P \in A(K)$. Assume that there is an elliptic curve E and an isogeny ϕ, both defined over K, such that $\phi : A \to E^m$ and $\phi(P) = (Q_1, \ldots, Q_m)$. Assume that $\mathrm{Rank}_{\mathbb{Z}}(\langle Q_1, \ldots, Q_m \rangle) = 1$, i.e. the subgroup $\langle Q_1, \ldots, Q_m \rangle$ of E is isomorphic to $\mathbb{Z} \oplus T$ where T is a torsion group. Note that $\mathbb{Z}P$ is not Zariski dense in any subvariety of dimension at least 2, so in particular it is not Zariski dense when A has dimension at least 2. We will prove the following.

Theorem 1.1. *Let A be an abelian variety defined over a number field K, let $\mathcal{A}/\mathcal{O}_K$ be the Néron model for A/K, and let $P \in A(K)$. Let us assume the following:*

- *there is an elliptic curve E and an isogeny ϕ, both defined over K, such that $\phi : A \to E^m$ and $\phi(P) = (Q_1, \ldots, Q_m)$;*

- $\mathrm{Rank}_{\mathbb{Z}}(\langle Q_1, \dots, Q_m \rangle) = 1$.

Then, there exists a finite set of primes S in K, an integer $n_1 \geq 1$, an elliptic curve E_0 defined over K, and $Q_0 \in E_0(K)$ such that

$$C_n(\mathcal{A}, P, S) = \begin{cases} 1 \text{ if } n_1 \nmid n, \\ C_{n/n_1}(E_0, Q_0, S) \text{ if } n_1 \mid n. \end{cases}$$

Let $Q_0' \in E_0(\overline{K})$ be such that $n_1 Q_0' = Q_0$, and K' be a Galois finite extension of K such that $Q_0' \in E_0(K')$. Up to enlarging S in Theorem 1.1, we can assume that singular primes of $\mathcal{A}$ and E_0, and the prime divisors of the discriminant of K'/K are in S. Let S' be the set of primes in K' that are over primes in S. Whence, we have

$$C_n(\mathcal{A}, P, S)\mathcal{O}_{K'} = \begin{cases} 1 \text{ if } n_1 \nmid n, \\ C_n(E_0, Q_0', S') \text{ if } n_1 \mid n. \end{cases}$$

So, one can see $C_n(\mathcal{A}, P, S)$ as an elliptic divisibility sequence with all entries with index not divisible by n_1 blanked out. The elliptic divisibility sequence $C_n(E_0, Q_0', S)$ is not defined over K but over the finite extension K'.

After the proof of this theorem, we will show how to compute the unique integer n_1 of Theorem 1.1 and we will show some examples.

Regarding the problem of primitive divisors, we will prove the following.

Corollary 1.2. *Let A be an abelian variety defined over a number field K, let $\mathcal{A}/\mathcal{O}_K$ be the Néron model for A/K, let $P \in A(K)$, and let S be a finite set of primes. Let us assume the following:*

- *there is an elliptic curve E and an isogeny ϕ, both defined over K, such that $\phi : A \to E^m$ and $\phi(P) = (Q_1, \dots, Q_m)$;*
- $\mathrm{Rank}_{\mathbb{Z}}(\langle Q_1, \dots, Q_m \rangle) = 1$.

Let d_ϕ be the degree of ϕ and let $\bar{\phi} : E^m \to A$ be such that $\phi \circ \bar{\phi} = d_\phi$. Then, $C_n(\mathcal{A}, P, S)$ has a primitive divisor for all but finitely many n if and only if there exists $U' \in E(\overline{K})$ and $a_1, \dots, a_m \in \mathbb{Z}$ such that $\bar{\phi}(a_1 U', \dots, a_m U') = P$.

Remark 1.3. In the case when A is defined over $\mathbb{Q}$, one can compute the terms of the sequence $C_n(\mathcal{A}, P, S)$ using a recursion formula. This can be done by combining the recurrence relation in [13, Theorem 1.9] and Theorem 1.1.

Acknowledgments

We thank the anonymous referees for several useful comments that improved the exposition of this paper. In particular, we thank one of the referees for suggesting the alternative proof of Theorem 1.1 given in Remark 2.7.

The second author acknowledges the support by Dioscuri program initiated by the Max Planck Society, jointly managed with the National Science Centre (Poland) Grant number: 2019/02/H/ST1/00001, and mutually funded by the Polish Ministry of Science and Higher Education and the German Federal Ministry of Education and Research.

The third author has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie Grant Agreement No. 101034413.

We are also grateful to the University of Bristol for providing us with the access to Magma cluster CREAM.

2. Proof of the main theorem

In the sequel, let A be an abelian variety and E be an elliptic curve defined over a number field K, and $\mathcal{A}/\mathcal{O}_K$ be the Néron model for A/K.

Lemma 2.1. *Let $\phi' : E^m \to A$, let $a_1, \dots, a_m \in \mathbb{Z}$ with $\gcd_i(a_i) = 1$, and let $Z_1, \dots, Z_m \in E(\overline{K})$. For each $n \in \mathbb{N}$, define*

$$G_n = \{V \in E(\overline{K}) \mid \phi'(a_1 V + nZ_1, \dots, a_m V + nZ_m) = O\}.$$

There exists a unique non-negative integer d such that for every integer n the following equivalence holds: $G_n \neq \emptyset$ if and only if $d \mid n$. If $G_n = \emptyset$ for all $n \neq 0$, we have $d = 0$. Moreover, for each $k \in \mathbb{Z}$, $\#G_{kd} = \#G_0$.

Proof. If $G_n = \emptyset$ for all $n \geq 1$, the lemma is trivial. So, we assume that there exists $n \geq 1$ such that G_n is not empty.

Note that if G_a and G_b are not empty, then G_{a+b} is not empty. Indeed, if $V_a \in G_a$ and $V_b \in G_b$, then $V_a + V_b \in G_{a+b}$. Let $d > 0$ be the minimum positive integer such that G_d is not empty. Then G_n is not empty if and only if $n = kd$. If G_n is not empty, then $\exists V_n \in G_n$ and there is a bijection between G_0 and G_n given by $V \to V + V_n$. □

Remark 2.2. The subset G_0 is always a subgroup of E but in general the set G_n does not form a group with the standard operations in E.

Definition 2.3. Let $\phi : A \to E^m$ be an isogeny. Let d_ϕ be the degree of the isogeny and $\bar{\phi} : E^m \to A$ be the unique isogeny such that $\phi \circ \bar{\phi} = d_\phi$. Such an isogeny exists due to [9, Section II.7]. Hence, $\deg(\bar{\phi}) = (d_\phi)^{2m-1}$ since $\deg(d_\phi) = (d_\phi)^{2m}$ by [5, Theorem A.7.2.7].

Lemma 2.4. *Let $\phi : A \to E^m$ and $\mathfrak{p}$ be a prime in K where E has good reduction. Assume that $Z_1, \dots, Z_m \in E(\overline{K})$ are torsion points of order that divides d_ϕ. Let $a_1, \dots, a_m \in \mathbb{Z}$ with $\gcd_i(a_i) = 1$. If $\mathfrak{p}$ does not divide d_ϕ, there is a bijection between G_n, defined as*

$$\{V \in E(\overline{K}) \mid \bar{\phi}(a_1V + nZ_1, \ldots, a_mV + nZ_m) = O \in E(\overline{K})\}, \tag{1}$$

and

$$\{V \in E(\overline{\mathbb{F}_\mathfrak{p}}) \mid \bar{\phi}(a_1V + nZ_1, \ldots, a_mV + nZ_m) = O \in E(\overline{\mathbb{F}_\mathfrak{p}})\}.$$

Proof. Notice that $G_n \subseteq E(\overline{K})[d_\phi]$. Indeed, for $V \in G_n$,

$$\begin{aligned}(d_\phi a_1V, \ldots, d_\phi a_mV) &= d_\phi(a_1V + nZ_1, \ldots, a_mV + nZ_m)\\ &= \phi \circ \bar{\phi}(a_1V + nZ_1, \ldots, a_mV + nZ_m)\\ &= \phi(O)\\ &= (O, \ldots, O).\end{aligned}$$

Hence, $d_\phi V = O$ since $\gcd(a_i) = 1$. We conclude by observing that there is a bijection between $E(\overline{K})[d_\phi]$ and the reduction modulo $\mathfrak{p}$ of $E[d_\phi]$, cf. [5, Thm C.1.4], since $\mathfrak{p}$ does not divide d_ϕ. □

We are now ready to prove Theorem 1.1. The techniques involved are related to those used in [1]. In Remark 2.7, we show how to give a more geometric proof. Our argument here is more constructive, which will be useful later in Section 3. For readers primarily interested in the result and not in the computational details, we recommend consulting the alternative proof in Remark 2.7, which is shorter and easier to follow. We begin by sketching the overall strategy. The proof is divided into three parts:

1. By assumption, $\phi(P) = (a_1R+T_1, \ldots, a_mR+T_m)$ for $R \in E(K)$ a non-torsion point and $T_i \in E(K)$ torsion points. We show that, outside finitely many primes, $nP \equiv O \mod \mathfrak{p}$ implies $nT_i = 0$ for all $1 \leq i \leq m$. So, if n is not a multiple of the order of T_i for all i, then $C_n(\mathcal{A}, P, S) = 1$. In the case when n is a multiple of the order of T_i for all i, it is easy to see that this case is equivalent to the case $T_1 = T_2 = \cdots = T_m = O$ and so $\phi(P) = (a_1R, \ldots, a_mR)$.
2. If $\phi(P) = (a_1R, \ldots, a_mR)$, we have $\overline{\phi}(a_1U'+Z_1, \ldots, a_mU'+Z_m) = P$ for $U' \in E(\overline{K})$ a non-torsion point and $Z_i \in E(\overline{K})$ torsion points of order dividing the degree of ϕ. We show that, if G_n, as defined in (1), is empty, then $C_n(\mathcal{A}, P, S) = 1$. This follows from the fact that $nP \equiv O \mod \mathfrak{p}$ implies $nU' \in G_n$ modulo $\mathfrak{p}$, and this cannot happen by Lemma 2.4. So, we focus on the case when G_n is non-empty and, after replacing n with an appropriate multiple, we can assume G_1 is non-empty.
3. Let $V_1 \in G_1$ and notice $nV_1 \in G_n$. By definition, $nP \equiv O \mod \mathfrak{p}$ if and only if $nU' \in G_n$ modulo $\mathfrak{p}$, or equivalently if and only if $n(U' - V_1) \in G_0$ modulo $\mathfrak{p}$. So, if $E_0 = E/G_0$ and $Q_0 = U' - V_1 \in E_0$, then $nP \equiv O \mod \mathfrak{p}$ if and only if $nQ_0 \equiv O \mod \mathfrak{p}$ in $E_0(\mathbb{F}_\mathfrak{p})$. We conclude that $C_n(\mathcal{A}, P, S) = C_n(E_0, Q_0, S)$.

Proof of Theorem 1.1. Since the rank of the subgroup of $E(K)$ generated by the points $Q_1, \ldots, Q_m$ is equal to 1, there exist a non-torsion point $R \in E(K)$, some integers $a_1, \ldots, a_m$ with $\gcd(a_1, \ldots, a_m) = 1$, and torsion points $T_i \in E(K)$ such that, for every $i = 1, \ldots, m$,

$$Q_i = a_i R + T_i. \tag{2}$$

Put

$$U = \sum_{i=1}^{m} b_i Q_i,$$

where $b_1, \ldots, b_m$ are integers such that $\sum a_i b_i = \gcd(a_1, \ldots, a_m) = 1$. Let us introduce the following notation for the sake of simplification of the exposition. Put

$$\underline{Q} = [Q_1, \ldots, Q_m],\ \underline{a} = [a_1, \ldots, a_m],\ \underline{T} = [T_1, \ldots, T_m],\ \underline{b} = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}.$$

So,

$$\underline{Q} = \underline{a} R + \underline{T} \tag{3}$$

and

$$U = \underline{Q} \cdot \underline{b} = \underline{a} \cdot \underline{b} R + \underline{T} \cdot \underline{b} = R + \underline{T} \cdot \underline{b}. \tag{4}$$

Let $\mathfrak{p}$ be a prime of good reduction. If $nP \equiv O \mod \mathfrak{p}$, then $nQ_i \equiv O \mod \mathfrak{p}$ for each i since $\phi(nP) = (nQ_1, \ldots, nQ_m)$. Hence, $nU \equiv O \mod \mathfrak{p}$ because $U = \underline{Q} \cdot \underline{b}$. Moreover, by (3) and (4),

$$\underline{Q} - \underline{a} U = \underline{a} R + \underline{T} - \underline{a} R - \underline{a}(\underline{T} \cdot \underline{b}) = \underline{T} - \underline{a}(\underline{T} \cdot \underline{b}),$$

so $Q_j - a_j U$ is a torsion point for all $1 \leq j \leq m$. Let $u_j > 0$ be the order of $Q_j - a_j U$ and

$$u = \operatorname{lcm}_{1 \leq j \leq m}\{u_j\}. \tag{5}$$

Let S contain the primes where A and E have bad reduction, and the primes that divide d_ϕ and u. Recall that a non-trivial u-torsion point is not the identity modulo a prime that does not divide u (see [12, Theorem VIII.7.1]). Hence, if $n(Q_j - a_j U) \neq O$ and $n(Q_j - a_j U) \equiv O \mod \mathfrak{p}$, then $\mathfrak{p}$ must be in S since $n(Q_j - a_j U)$ is a u-torsion point.

If $nP \equiv O \mod \mathfrak{p}$ for $\mathfrak{p} \notin S$ and $u \nmid n$, then there exists j such that $n(Q_j - a_jU) \neq O$. As we said, $n(Q_j - a_jU) \equiv O \mod \mathfrak{p}$ and this contradicts the hypothesis $\mathfrak{p} \notin S$. Therefore, if $u \nmid n$, then $C_n(\mathcal{A}, P, S) = 1$. So, if $nP \equiv O \mod \mathfrak{p}$ for $\mathfrak{p} \notin S$, then $u \mid n$. From now on, we will focus on this case since we already know that $C_n(\mathcal{A}, P, S) = 1$ if $u \nmid n$.

Let n be a multiple of u and put $n_2 = n/u$. Therefore, $nQ_j = na_jU + n(Q_j - a_jU) = na_jU$ since $n(Q_j - a_jU) = O$. Thus,

$$n\underline{Q} = \underline{a}(nU).$$

Let $\underline{Q'} = (Q'_1, \ldots, Q'_m) \in E^m(\overline{K})$ be such that $\bar{\phi}(\underline{Q'}) = P$. Note that $d_\phi(n\underline{Q'}) = \underline{a}(nU)$ since

$$d_\phi(n\underline{Q'}) = \phi\left(\bar{\phi}(n\underline{Q'})\right) = \phi(nP) = n\underline{Q} = \underline{a}(nU).$$

Let $U' \in E(\overline{K})$ be such that $d_\phi(U') = U$. Therefore, for each j, $u\underline{Q'}_j - a_j uU'$ is a torsion point of order that divides d_ϕ since

$$d_\phi(u\underline{Q'}_j - a_j uU') = a_j(uU) - a_j(uU) = O.$$

Hence, there exists $\underline{Z} = [Z_1, \ldots, Z_m]$ with $Z_i \in E(\overline{K})[d_\phi]$, such that

$$\bar{\phi}(\underline{a}(nU') + n_2\underline{Z}) = \bar{\phi}(n\underline{Q'}) = nP. \tag{6}$$

Let

$$G_n = \{V \in E(\overline{K}) \mid \bar{\phi}(a_1V + nZ_1, \ldots, a_mV + nZ_m) = O\}. \tag{7}$$

As we proved in Lemma 2.4, given $\mathfrak{p} \notin S$, G_n is bijective to its reduction modulo $\mathfrak{p}$. Let d be the smallest positive integer such that G_d is not empty. Note that $O \in G_{d_\phi}$ since $Z_i \in E(\overline{K})[d_\phi]$ and so, by Lemma 2.1, $d \mid d_\phi$.

Assume $d \nmid n_2$ and $nP \equiv O \mod \mathfrak{p}$ for $\mathfrak{p} \notin S$. Then,

$$\bar{\phi}(a(nU') + n_2\underline{Z}) = nP \equiv O \mod \mathfrak{p}$$

and nU' belongs to the reduction modulo $\mathfrak{p}$ of G_{n_2}. So, G_{n_2} modulo $\mathfrak{p}$ is not empty and this contradicts the hypothesis that $d \nmid n_2$ since G_{n_2} must be empty. Hence, if $d \nmid n_2$, $C_n(\mathcal{A}, P, S) = 1$. Therefore, we focus on the case $d \mid n$. Put $n_3 = n_2/d$ (and so $n = udn_3$).

Since G_d is not empty, let $V_d \in G_d$ and $W = (udU' - V_d) \in E(\overline{K})$. Note that $(n/d)V_d \in G_n$ since $V_d \in G_d$. Let $E_0 = E/G_0$ and $Q_0 \in E(\overline{K})$ be the image of W under the isogeny $E \to E_0$. Notice that there exists a finite field extension K' of K such that E_0 and Q_0 are defined over K'. Let S' be the set of primes in $\mathcal{O}_{K'}$ that are over the primes in S.

Let $\mathfrak{p}' \notin S'$. We have $nP \equiv O \mod \mathfrak{p}'$ if and only if

$$\bar{\phi}(\underline{a}(nU') + n_2\underline{Z}) = nP \equiv O \mod \mathfrak{p}'$$

by Equation (6). Moreover, $\bar{\phi}(\underline{a}(nU') + n_2\underline{Z}) \equiv O \mod \mathfrak{p}'$ if and only if $nU' \in G_{n_2} = (n_2/d)V_d + G_0 = n_3V_d + G_0$ in the reduction modulo $\mathfrak{p}'$. So, if $\mathfrak{p}' \mid C_n(\mathcal{A}, P, S)\mathcal{O}_{K'}$, then $n_3W = n_3(udU' - V_d) = nU' - n_3V_d \in G_0$. Thus, n_3Q_0 reduces to the identity modulo $\mathfrak{p}'$. Therefore, $\mathfrak{p}' \mid C_{n_3}(E_0, Q_0, S')$.

If $\mathfrak{p}' \mid C_{n_3}(E_0, Q_0, S')$, then $nU' - n_3V_d = n_3W \in G_0$ modulo $\mathfrak{p}'$. Therefore, $nU' \in G_{n_2} = (n_3)V_d + G_0$ modulo $\mathfrak{p}'$ and then $nP = \bar{\phi}(n\underline{a}U' + n_2\underline{Z}) = O \mod \mathfrak{p}'$. Thus, $\mathfrak{p}' \mid C_n(\mathcal{A}, P, S)\mathcal{O}_{K'}$. In conclusion,

$$C_n(\mathcal{A}, P, S)\mathcal{O}_{K'} = C_{n_3}(E_0, Q_0, S') = C_{\frac{n}{ud}}(E_0, Q_0, S').$$

To conclude the proof, we just need to show that E_0 and Q_0 are defined over K. Recall that E_0 and Q_0 are defined over K'. We can assume that K'/K is a Galois extension. Note that G_0 is $\mathrm{Gal}(K'/K)$-invariant since, if $V \in G_0$, then

$$\bar{\phi}(a_1V^\sigma, \ldots, a_mV^\sigma) = \bar{\phi}(a_1V, \ldots, a_mV)^\sigma = O$$

for all $\sigma \in \mathrm{Gal}(K'/K)$. Therefore, by [12, Remark III.4.13.2], $E_0 = E/G_0$ is defined over K. Moreover,

$$\bar{\phi}(\underline{a}W) = \bar{\phi}(\underline{a}udU' - \underline{a}V_d) = \bar{\phi}(\underline{a}udU' + d\underline{Z}) = udP$$

since $V_d \in G_d$ and by (6). Therefore, for all $\sigma \in \mathrm{Gal}(K'/K)$,

$$\bar{\phi}(\underline{a}(W - W^\sigma)) = \bar{\phi}(\underline{a}(W)) - \bar{\phi}(\underline{a}(W))^\sigma = udP - udP^\sigma = O$$

and then $W - W^\sigma \in G_0$. Since Q_0 is the image of W under the isogeny $E \to E/G_0$, we have $Q_0^\sigma = Q_0$ for all $\sigma \in \mathrm{Gal}(K'/K)$. Then, Q_0 is defined over K. □

Remark 2.5. Notice that the constant n_1, as defined in the statement of Theorem 1.1, is equal to ud, where u is defined in (5) and d is defined just after (7).

Remark 2.6. Observe that if A is just E^m, and $P = (Q_1, \ldots, Q_m) \in E^m(K)$, then we immediately get the following: there exists a finite set of primes S in K, an integer $u \geq 1$, and $Q_0 \in E(K)$ such that

$$C_n(\mathcal{A}, P, S) = \begin{cases} 1 \text{ if } u \nmid n, \\ C_n(E, Q_0, S) \text{ if } u \mid n. \end{cases}$$

Remark 2.7. As suggested by one of the anonymous referees, one can give an alternative, more geometric proof of Theorem 1.1. However, in comparison to the proof written above we cannot directly extract the value n_1 from this alternative proof.

Let P be a fixed K-rational point on A. Let V be the Zariski closure of the set $\mathbb{Z}P$. This is a 1-dimensional algebraic subgroup of A, hence is smooth and is the union of disjoint irreducible components over $\overline{K}$. Let E_0 be the component containing $O = 0P$. As E_0 contains O, it is defined over K. Moreover, V is the union of the varieties $kP + E_0$ where k ranges over $\mathbb{Z}$. Let n_1 be the smallest positive integer such that $n_1 P \in E_0$. We get that V is the disjoint union of E_0, $P + E_0$, $2P + E_0$, ..., $(n_1 - 1)P + E_0$ and we let $Q_0 = n_1 P \in E_0(K)$.

Let R be the image of P in the quotient abelian variety A/E_0. The point R has finite order. Choose defining equations of $A, E_0 \subset A$, and A/E_0 in such a way that the map $A \to A/E_0$ is just a restriction to the first so many coordinates and let S contain all primes of bad reduction of these chosen sets of equations, as well as all primes $\mathfrak{p}$ for which there is a $k \in \{1, 2, ..., n_1 - 1\}$ with $kR \equiv 0 \mod \mathfrak{p}$.

Then for all primes outside S and all n with $n_1 \nmid n$, we have

$$C_n(A, P, S) \mid C_n(A/E_0, R, S) = 1.$$

Moreover, if $n_1 \mid n$, then $nP = (n/n_1)Q_0$, hence $C_n(A, P, S) = C_{n/n_1}(E_0, Q_0, S)$.

Corollary 2.8. *Let A be an abelian variety defined over a number field K, let $\mathcal{A}/\mathcal{O}_K$ be the Néron model for A/K, and let $P \in A(K)$ be a non-torsion point. Assume that there is an elliptic curve E and an isogeny ϕ, both defined over K, such that $\phi : A \to E^m$. Assume* $\mathrm{Rank}_K(E) = 1$. *Then, there exists a finite set of primes S, an integer n_1, an elliptic curve E_0 defined over K, and $Q_0 \in E_0(K)$ such that*

$$C_n(\mathcal{A}, P, S) = \begin{cases} 1 \text{ if } n_1 \nmid n, \\ C_{n/n_1}(E_0, Q_0, S) \text{ if } n_1 \mid n. \end{cases}$$

Proof. We have $\phi(P) = (Q_1, \ldots, Q_m)$ and $\mathrm{Rank}(\langle Q_1, \ldots, Q_m \rangle) \leq \mathrm{Rank}_K(E) = 1$. Since P is a non-torsion point, we have $\mathrm{Rank}(\langle Q_1, \ldots, Q_m \rangle) = 1$. Hence, we apply Theorem 1.1. □

3. Some considerations and examples

By the proof of Theorem 1.1, $C_n(\mathcal{A}, P, S)$ is equal to $C_n(E, Q_0, S)$ if and only if $Q_j = a_j U$ for each $1 \leq j \leq m$ (see (5)) and G_1 is not empty (see Equation (7)). In the next example, we show a case when this happens.

Example 3.1. The isogeny of this example is taken by [6, Proposition 4]. Let $a_0 = 0$, $a_1 = 1$, and $a_2 = -9$. Let E be defined by $y^2 = (x - a_1)(x - a_2)(x - a_3)$ and take

$Q' = (9, -36) \in E(\mathbb{Q})$. There is an isogeny $\phi' : E^2 \to J$ with J the Jacobian of the hyperelliptic curve

$$y^2 = 30233088x^6 + 305690112x^4 + 305690112x^2 + 30233088,$$

with $\deg \phi' = 4$, and $\ker \phi' \subseteq E^2[2]$. So, there exists $\phi : J \to E^2$ with $\phi' \circ \phi = 2$. Following the proof of [6, Proposition 4],

$$\phi'(Q', Q') = P = \left(x^2 + \frac{64}{7}x + 1, \frac{23639040}{49}x + \frac{414720}{7}\right) \in J(\mathbb{Q})$$

where we are using the Mumford representation for the points on the Jacobian of a hyperelliptic curve. Note that,

$$\phi(P) = \phi(\phi'(Q', Q')) = (2Q', 2Q') = (Q, Q)$$

where $Q = 2Q' = (25/16, -195/64) \in E(\mathbb{Q})$.

Since $\deg(\phi) = 4$, there exists $\bar{\phi}$ such that $\bar{\phi} \circ \phi = 4$ and we can take $\bar{\phi} = 2\phi'$. Let $\overline{Q} \in E(\overline{\mathbb{Q}})$ be such that $Q' = 2\overline{Q}$ and so $\bar{\phi}(\overline{Q}, \overline{Q}) = \phi'(Q', Q') = P$. Therefore, defining G_n as in the proof of Theorem 1.1 (see in particular (7)), we have $G_0 = \{V \in E(\overline{\mathbb{Q}}) \mid \bar{\phi}(V, V) = O\}$ and $G_1 = G_0$. One can easily check that G_0 is the group of points $R \in E(\overline{\mathbb{Q}})$ such that $2R = (0, 0)$ or $2R = O$. Using MAGMA [2], we can compute that $E_0 = E/G_0$ is the elliptic curve $y^2 = x^3 + 8x^2 + 36x + 288$ and $Q_0 = (8, -40) \in E_0(\mathbb{Q})$, where Q_0 is the image of $\overline{Q}$ under the isogeny $E \to E_0$. Hence, replicating the work in the proof of Theorem 1.1, we have $C_n(J, P, S) = C_n(E_0, Q_0, S)$, where $S = \{2\}$. Using MAGMA, we compute the first terms of the two sequences.

n	$C_n(J, P, S)$	$C_n(E, Q_0, S)$
1	1	1
2	1	1
3	$7 \cdot 17 \cdot 41$	$7 \cdot 17 \cdot 41$
4	$13 \cdot 29 \cdot 101$	$13 \cdot 29 \cdot 101$
5	$103 \cdot 113 \cdot 1087 \cdot 2377$	$103 \cdot 113 \cdot 1087 \cdot 2377$
6	$7 \cdot 11 \cdot 17 \cdot 41 \cdot 89 \cdot 2713 \cdot 8329$	$7 \cdot 11 \cdot 17 \cdot 41 \cdot 89 \cdot 2713 \cdot 8329$
7	$23 \cdot 23497 \cdot 156671 \cdot 48883577521$	$23 \cdot 23497 \cdot 156671 \cdot 48883577521$

In particular, by [10, Proposition 10], $C_n(J, P, S)$ has a primitive divisor for all but finitely many terms. Note that this agrees with Corollary 1.2.

Remark 3.2. Notice that the abelian variety of the previous example is not isomorphic to the square of an elliptic curve. Indeed, there is no genus 2 curves on E^2. To prove this, it is sufficient to check that E does not have complex multiplication, as shown in [7, Theorem 1]. The endomorphism ring of E is $\mathbb{Z}$ and it is computed in the LMFDB database [8].

One may wonder if G_1 can be empty. In the next remark, we show that this can happen.

Remark 3.3. Let K be a number field, and let E/K be an elliptic curve with $E(K)[2] = \langle T_1, T_2 \rangle$ for $T_1, T_2 \in E(K)$ being two different points of order 2 and $\mathrm{Rank}_K(E) \geq 1$. Let $H \subseteq E^2$ be the subgroup generated by (T_1, T_1), (T_2, T_2), and (T_1, T_2). Let $A = E^2/H$ and $\bar{\phi} : E^2 \to A$ be the isogeny with kernel H. So, $\bar{\phi}$ has degree 8 and $\ker \bar{\phi} \subseteq E^2[2]$. By the properties of the quotient, there exists a map $\phi : A \to E^2$ such that $\phi \circ \bar{\phi} = [2]$. Let $U' \in E(K)$ be a non-torsion point and $P = \bar{\phi}(U' + T_1, U')$. So,

$$\phi(P) = \phi(\bar{\phi}(U' + T_1, U')) = 2(U' + T_1, U') = (2U', 2U').$$

Hence, we are in the hypothesis of Theorem 1.1. Following the definition of G_n in (7),

$$G_1 = \{V \in E(\overline{K}) \mid \bar{\phi}(V + T_1, V) = O\}.$$

As we proved in Lemma 2.4, we have $G_1 \subseteq E(\overline{K})[2]$. By definition, $\bar{\phi}(V, V) = O$ for each $V \in E(\overline{K})[2]$. Hence, $\bar{\phi}(V + T_1, V) = \bar{\phi}(T_1, O) \neq O$ since $(T_1, O) \notin H$. So, G_1 is empty.

Example 3.4. Let A and P be as in the previous remark. Let S be the set of primes over 2 and where A has bad reduction. We compute $C_n(\mathcal{A}, P, S)$.

Let n be odd and $\mathfrak{p} \notin S$. Then $\mathfrak{p} \mid C_n(\mathcal{A}, P, S)$ if and only if $(nU' + nT_1, nU') = (nU' + T_1, nU')$ reduces to a point in H modulo $\mathfrak{p}$ since $nP = \bar{\phi}(nU' + nT_1, nU')$ and $\ker(\bar{\phi}) = H$. Notice that every point $(R_1, R_2) \in H$ is such that $R_1 - R_2$ is equal to O or $T_1 - T_2$. Since $nU' + T_1 - nU' = T_1$, we have that $(nU' + T_1, nU')$ does not reduce to a point in H modulo $\mathfrak{p}$. So, $C_n(\mathcal{A}, P, S) = 1$.

Let n be even and $\mathfrak{p} \notin S$. So, $\mathfrak{p} \mid C_n(\mathcal{A}, P, S)$ if and only if $(nU' + nT_1, nU') = (nU', nU')$ reduces to a point in H modulo $\mathfrak{p}$. Hence, $\mathfrak{p} \mid C_n(\mathcal{A}, P, S)$ if and only if nU' is a 2-torsion point modulo $\mathfrak{p}$ and then if and only if $2nU'$ reduces to the identity modulo $\mathfrak{p}$. So, $C_n(\mathcal{A}, P, S) = C_n(E, 2U', S)$. In conclusion,

$$C_n(\mathcal{A}, P, S) = \begin{cases} 1 \text{ if } 2 \nmid n, \\ C_n(E, 2U', S) \text{ if } 2 \mid n. \end{cases}$$

Example 3.5. We make Example 3.4 explicit in one case. Let E be defined by $y^2 = x^3 - 20x - 21$, let $U' = (-3, 4) \in E(\mathbb{Q})$ be a non-torsion point, and let $T_1 = (-1, 0)$ and $T_2 = (5, 0)$ be two 2-torsion points in E. This is the curve 288.b3 in the LMFDB [8]. We have that $E(\mathbb{Q})$ is generated by U', T_1, and T_2. Let $H \subseteq E^2$ be the subgroup generated by (T_1, T_1), (T_2, T_2), and (T_1, T_2). Let $A = E^2/H$ and let $T = (T_1, O) \in A(\mathbb{Q})$, that is the only rational non-trivial 2-torsion point in A. Let $P = (U', U') + T \in A(\mathbb{Q})$ and $S = \{2, 3\}$. Following Example 3.4,

$$C_n(\mathcal{A}, P, S) = \begin{cases} 1 \text{ if } 2 \nmid n, \\ C_n(E, 2U', S) \text{ if } 2 \mid n. \end{cases}$$

We show that the equality holds also for $S = \{\emptyset\}$. Let p be equal to 2 or 3, and notice $T_1 \equiv T_2 \mod p$ is a non-singular point. If $nP \equiv O \mod p$, then $(nU' + nT_1, nU') \in H$ modulo p and so $nT_1 = nU' + nT_1 - nU'$ must be equal to the identity modulo p. This happens if and only if n is even. If n is even, then $nP = (nU', nU')$. If $p = 2$, then $nU' \equiv O \mod p$ for all n even and so $nP \equiv O \mod p$. If $p = 3$, then $nU' \notin H$ modulo p for $n \equiv 1, 2 \mod 3$ and $nU' \equiv O \mod p$ for $n \equiv 0 \mod p$. We conclude that

$$C_n(\mathcal{A}, P, \{\emptyset\}) = \begin{cases} 1 \text{ if } 2 \nmid n, \\ C_n(E, 2U', \{\emptyset\}) \text{ if } 2 \mid n. \end{cases}$$

We compute the first few terms.

n	$C_n(\mathcal{A}, P, \{\emptyset\})$	$C_n(E, 2U', \{\emptyset\})$
1	1	2
2	$2 \cdot 5 \cdot 11 \cdot 13$	$2 \cdot 5 \cdot 11 \cdot 13$
3	1	$2 \cdot 3 \cdot 7 \cdot 17 \cdot 19 \cdot 23 \cdot 263$
4	$2 \cdot 5 \cdot 11 \cdot 13 \cdot 67 \cdot 197 \cdot 19249 \cdot 21649$	$2 \cdot 5 \cdot 11 \cdot 13 \cdot 67 \cdot 197 \cdot 19249 \cdot 21649$
5	1	$2 \cdot 37 \cdot 43 \cdot 73 \cdot 937 \cdot 1583 \cdot$ $\cdot 1867 \cdot 2089 \cdot 3041 \cdot 21601$
6	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 191 \cdot 251 \cdot$ $\cdot 263 \cdot 311 \cdot 16103 \cdot 1786451 \cdot 385044001$	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 191 \cdot 251 \cdot$ $\cdot 263 \cdot 311 \cdot 16103 \cdot 1786451 \cdot 385044001$

Now, we prove Corollary 1.2. To do that, we need a preliminary lemma. We will use the same notation of Section 2.

Lemma 3.6. *Let G_n be as in (7). Let $\alpha : E^m \to E^m$ be the isogeny that sends*

$$(P_1, \dots, P_m) \to (a_1 P_1, \dots, a_m P_m).$$

Then, G_n is empty if and only if the following hold:

- $\alpha(\Delta[d_\phi]) \subseteq \ker(\bar{\phi})$;
- $\bar{\phi}(nZ_1, \dots, nZ_m) \neq O$.

With $\Delta[d_\phi]$ we mean $\{(V, \dots, V) \in E^m(\overline{K}) \mid V \in E(\overline{K})[d_\phi]\}$.

Proof. Recall that $G_n \subseteq E(\overline{K})[d_\phi]$, that is a 2-dimensional module over $\mathbb{Z}/d_\phi\mathbb{Z}$. Note that $\ker(\bar{\phi})$ is a $(2m-1)$-dimensional sub-module of $E^m(\overline{K})[d_\phi]$ and that $\alpha(\Delta[d_\phi])$ is a 2-dimensional sub-module. Moreover, the image of $\bar{\phi}(E^m(\overline{K})[d_\phi])$ has dimension 1.

Assume that G_n is empty. If $\bar{\phi}(nZ_1, \dots, nZ_m) = O$, then $O \in G_n$, contradiction. So, $\bar{\phi}(nZ_1, \dots, nZ_m) \neq O$. If $\alpha(\Delta[d_\phi]) \not\subseteq \ker(\bar{\phi})$, then there is $V \in E[d_\phi]$ such that $\bar{\phi}(a_1V, \dots, a_mV) \neq O$. The image of $\bar{\phi}(E^m(\overline{K})[d_\phi])$ has dimension 1 and so there is $i \leq d_\phi$ such that

$$-i\bar{\phi}(a_1V, \dots, a_mV) = \bar{\phi}(nZ_1, \dots, nZ_m).$$

So, $iV \in G_n$ and G_n is not empty, contradiction. Therefore, $\alpha(\Delta[d_\phi]) \subseteq \ker(\bar{\phi})$.

Now, we prove the only if statement. We have

$$\begin{aligned}\bar{\phi}(a_1V + nZ_1, \dots, a_mV + nZ_m) &= \bar{\phi}(\alpha(V, \dots, V)) + \bar{\phi}(nZ_1, \dots, nZ_m)\\ &= \bar{\phi}(nZ_1, \dots, nZ_m)\\ &\neq O\end{aligned}$$

for each $V \in E(\overline{K})[d_\phi]$ and then G_n is empty. □

Proof of Corollary 1.2. Notice that, if S and S' are two finite sets of primes in K, then, by definition, $C_n(\mathcal{A}, P, S)$ has a primitive divisor for all but finitely many n if and only if $C_n(\mathcal{A}, P, S')$ does. So, we have to prove the corollary only for the set of primes S as in Theorem 1.1.

By [10, Proposition 10] and Theorem 1.1, $C_n(\mathcal{A}, P, S)$ has a primitive divisor for all but finitely many n if and only if $n_1 = 1$, where n_1 is defined in the statement of Theorem 1.1.

As we noted at the beginning of Section 3, this happens if and only if $Q_j - a_jU = O$ for each j and G_1 is not empty (see Equation (7)).

Assume that $C_n(\mathcal{A}, P, S)$ has a primitive divisor for all but finitely many n. Therefore, $\phi(P) = (a_1U, \dots, a_mU)$. Moreover, G_1 is non-empty and then, by Lemma 3.6, $\alpha(\Delta[d_\phi]) \not\subseteq \ker(\bar{\phi})$ or $\bar{\phi}(Z_1, \dots, Z_m) = O$. In the second case,

$$\bar{\phi}(a_1U', \dots, a_mU') = \bar{\phi}(a_1U' + Z_1, \dots, a_mU' + Z_m) = P$$

by (6). Assume that $\bar{\phi}(Z_1, \dots, Z_m) \neq O$ and then $\alpha(\Delta[d_\phi]) \not\subseteq \ker(\bar{\phi})$. Since $\bar{\phi}(E^m[d_\phi])$ has dimension 1 as $\mathbb{Z}/d_\phi\mathbb{Z}$-module, there exists $V \in E(\overline{K})[d_\phi]$ such that

$$\bar{\phi}(a_1V, \dots, a_mV) = \bar{\phi}(Z_1, \dots, Z_m).$$

So,

$$\bar{\phi}(a_1(U' + V), \dots, a_m(U' + V)) = \bar{\phi}(a_1U' + Z_1, \dots, a_mU' + Z_m) = P.$$

In both cases, we can find a point U' (or $U' + V$) such that

$$\bar{\phi}(a_1U', \dots, a_mU') = P$$

and we are done.

Now, we prove the only if statement. By hypotheses, $Z_j = O$ for each j and then G_1 is not empty (by Lemma 3.6). So, $C_n(\mathcal{A}, P, S)$ is equal to an elliptic divisibility sequence and then $C_n(\mathcal{A}, P, S)$ has a primitive divisor for all but finitely many n. □

Data availability

No data was used for the research described in the article.

References

[1] Stefan Barańczuk, Piotr Rzonsowski, A remark on certain simultaneous divisibility sequences, in: Colloquium Mathematicum, vol. 2, 2014, pp. 209–213.
[2] Wieb Bosma, John Cannon, Catherine Playoust, The Magma algebra system. I. The user language, in: Computational Algebra and Number Theory, London, 1993, J. Symb. Comput. 24 (3–4) (1997) 235–265.
[3] Jung H. Cheon, Sang G. 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.
[4] Gunther Cornelissen, Karim Zahidi, Elliptic divisibility sequences and undecidable problems about rational points, J. Reine Angew. Math. 613 (2007) 1–33.
[5] Marc Hindry, Joseph H. Silverman, Diophantine Geometry: An Introduction, vol. 201, Springer Science & Business Media, 2013.
[6] Everett W. Howe, Franck Leprévost, Bjorn Poonen, Large torsion subgroups of split Jacobians of curves of genus two or three, Forum Math. 12 (3) (2000) 315–364.
[7] Ernst Kani, Jacobians isomorphic to a product of two elliptic curves and ternary quadratic forms, J. Number Theory 139 (2014) 138–174.
[8] The LMFDB Collaboration, The L-functions and modular forms database, https://www.lmfdb.org, 2025. (Accessed 10 June 2025) (Online).
[9] David Mumford, Abelian Varieties, Tata Studies in Mathematics, 1970.
[10] Joseph H. Silverman, Wieferich's criterion and the *abc*-conjecture, J. Number Theory 30 (2) (1988) 226–237.
[11] Joseph H. Silverman, Generalized greatest common divisors, divisibility sequences, and Vojta's conjecture for blowups, Monatshefte Math. 145 (2005) 333–350.
[12] Joseph H. Silverman, The Arithmetic of Elliptic Curves, second edition, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.
[13] Matteo Verzobio, A recurrence relation for elliptic divisibility sequences, Riv. Mat. Univ. Parma 13 (2022) 223–242.
[14] Matteo Verzobio, Primitive divisors of elliptic divisibility sequences, PhD thesis, Università di Pisa, June 2021.