MATHEMATICS OF COMPUTATION
Volume 83, Number 288, July 2014, Pages 1951–1991
S 0025-5718(2013)02790-1
Article electronically published on November 12, 2013

PRIME POWER TERMS IN ELLIPTIC DIVISIBILITY SEQUENCES

VALÉRY MAHÉ

Abstract. We study a problem on specializations of multiples of rational points on elliptic curves analogous to the Mersenne problem. We solve this problem when descent via isogeny is possible by giving explicit bounds on the indices of prime power terms in elliptic divisibility sequences associated to points in the image of a nontrivial isogeny. We also discuss the uniformity of these bounds assuming the Hall–Lang conjecture.

1. Introduction

The classical Mersenne problem consists of the search for all prime integers of the form $2^n - 1$. This article is dedicated to the study of an analogous problem for elliptic divisibility sequences. A divisibility sequence is a sequence of integers $(B_n)_{n\in\mathbb{N}}$ satisfying the divisibility relation $B_n \mid B_m$ for every pair $(n, m) \in \mathbb{N}^2$ such that $n \mid m$. Elliptic divisibility sequences are a particular case of divisibility sequences, arising from the study of denominators of multiples of points on elliptic curves. The first systematic study of elliptic divisibility sequences is due to Ward (see [35]).

The Lenstra–Pomerance–Wagstaff conjecture asserts the number of primes p less than x with $2^p - 1$ being prime is asymptotically $e^\gamma \log_2(x)$ where γ denotes the Euler–Mascheroni constant (see [34]). In particular, we expect the Mersenne sequence to have infinitely many prime terms. This contrasts with the behaviour of elliptic divisibility sequences. An analog to the Lenstra–Pomerance–Wagstaff heuristic suggests the following conjecture (see [8]).

Conjecture 1.1 (Primality conjecture: Einsiedler–Everest–Ward)**.** *Let $B = (B_n)_{n\in\mathbb{N}}$ be an elliptic divisibility sequence. Then B contains only finitely many prime terms.*

The primality conjecture is supported by many computations and has been proved for *magnified* elliptic divisibility sequences by Everest, Miller and Stephens in [11] (see below for a definition of the magnification condition). Although the

Received by the editor December 24, 2009 and, in revised form, October 15, 2011 and October 31, 2012.

2010 *Mathematics Subject Classification.* Primary 11G05, 11A41.

Key words and phrases. Siegel's Theorem, elliptic curves, isogeny, division polynomials, Thue equations, canonical height, local height.

This work was supported by EPSRC grant EP/E012590/1, the Université de Montpellier 2, the Université de Franche-Comté and the École Polytechnique Fédérale de Lausanne. The author thanks Professor Everest, Professor Silverman, Professor Stevens and the anonymous referee for helpful discussions and comments.

magnification condition is a strong assumption, the study of prime terms in magnified elliptic divisibility sequences has applications to logic; it is studied in [9] as part of a further investigation of a result of Poonen on Hilbert's tenth problem (see [22]).

Our main result consists of a computation of explicit bounds on the index n of a prime power term B_n in a magnified elliptic divisibility sequence $(B_n)_{n\in\mathbb{N}}$. Such explicit bounds are crucial when considering the problem of sieving for all prime power terms in a magnified elliptic divisibility sequence. This main result applies only to elliptic divisibility sequences that are both magnified and normalized, in the sense that they are defined over $\mathbb{Q}$ using elliptic curves given by minimal Weierstrass equations. No other condition is required.

Using the same method we show the existence of a uniform bound on the index of a prime power term in a normalized magnified elliptic divisibility sequence. Unlike our main result, this second theorem is conditional on conjectures of Lang and of Hall–Lang. This result improves the main theorem in [10] which asserts the existence of a uniform bound on the number (and not the indices) of prime power terms in normalized magnified elliptic divisibility sequences, assuming Lang's conjecture.

Before proving those two results, we explain how the primality conjecture for magnified elliptic divisibility sequences is linked to two classical problems in diophantine geometry: solving Thue equations and finding integer points on elliptic curves.

1.1. **Background.**

Notation 1.1.1. Elliptic divisibility sequences can be defined by considering the rank one subgroup generated by a point P of infinite order on an elliptic curve $\mathcal{E}$ defined over $\mathbb{Q}$ by a Weierstrass equation with integral coefficients

$$\mathcal{E} : y^2 + a_1 y + a_3 xy = x^3 + a_2 x^2 + a_4 x + a_6. \tag{1}$$

For each integer $n \in \mathbb{N}$, we consider the *"denominator"* B_{nP} of the multiple $[n]P$ of P; we write

$$[n]P = \left(\frac{A_{nP}}{B_{nP}^2}, \frac{C_{nP}}{B_{nP}^3}\right)$$

with $A_{nP} \in \mathbb{Z}$ and $B_{nP} \in \mathbb{N}$ such that $\gcd(A_{nP}, B_{nP}) = \gcd(C_{nP}, B_{nP}) = 1$.

Definition 1.1.2. We use Notation 1.1.1.

(a) The sequence $B = (B_{nP})_{n\in\mathbb{N}}$ is called the *elliptic divisibility sequence associated to the point P and equation* (1).
(b) The sequence $B = (B_{nP})_{n\in\mathbb{N}}$ is the *normalized elliptic divisibility sequence associated to P* if equation (1) is a standardized minimal Weierstrass equation, meaning that equation (1) is minimal with $a_1, a_3 \in \{0, 1\}$ and $a_2 \in \{-1, 0, 1\}$.

The definition of the elliptic divisibility sequence associated to a point P on an elliptic curve E depends on a choice of a Weierstrass equation for E. If equation (1) is the standardized minimal Weierstrass equation for E, then any other Weiestrass equation for E with integral coefficients can be derived from equation (1)

using a change of variables $(x', y') = (u^2x + s,\ u^3y + vu^2x + t)$ for some $s, t, u, v \in \mathbb{Z}$ (with $u \neq 0$). Moreover, if $(B_n)_{n\in\mathbb{N}}$ is the normalized elliptic divisibility sequence associated to P, then the elliptic divisibility sequence associated to P and the Weierstrass equation for E obtained using those new coordinates $(x', y') = (u^2x + s,\ u^3y + vu^2x + t)$ is

$$(B'_n)_{n\in\mathbb{N}} := \left(\frac{B_n}{\gcd(B_n, u)}\right)_{n\in\mathbb{N}}.$$

In particular, given any integer N there is a well-chosen Weierstrass equation for E for which the elliptic divisibility sequence associated to P has at least N prime power terms. The normalization condition is introduced because each point P on an elliptic curve has only one normalized elliptic divisibility sequence associated to it. From now on all elliptic divisibility sequences will be assumed to be normalized.

Our definition of elliptic divisibility sequence is slightly different from the definition given in [35] but is better suited to the definition of an analog of the Mersenne problem in the context of the theory of elliptic curves. Using Notation 1.1.1, if E has good reduction at a prime l, then for each integer n we have equivalence between the conditions:

- l divides B_{nP};
- $nP \equiv \mathcal{O}_E \mod l$ (where $\mathcal{O}_E$ denotes the point at infinity on E).

Thus the search for prime power terms in normalized elliptic divisibility sequences is a particular case of the following problem which arises naturally when studying specializations of algebraic groups.

Problem 1.1.3. Given a $\mathbb{Q}$-point $P \in G(\mathbb{Q})$ on an algebraic group G defined over $\mathbb{Q}$ (whose group law is denoted multiplicatively), are there infinitely many integers $n \in \mathbb{N}$ such that

$$\operatorname{Supp}(P^n) := \{v \text{ finite place of } \mathbb{Q} \ :\ P^n \equiv 1_G \bmod v\}$$

has cardinality one?

When $G = \mathbb{G}_m$ and $P = 2$, Problem 1.1.3 consists of the following unsolved variant of the Mersenne problem: Are there infinitely many prime power terms in the sequence $(2^n - 1)_{n\in\mathbb{N}}$?

The Lenstra–Pomerance–Wagstaff conjecture and Conjecture 1.1 suggest that the answer to Problem 1.1.3 depends strongly on the choice of the algebraic group G. Thus finding common properties between Lucas sequences and elliptic divisibility sequences can lead to a better understanding of the Mersenne problem. The magnification condition has been introduced to study the analog for elliptic divisibility sequences of an easy result on Mersenne primes: if p is an integer such that $2^p - 1$ is a prime, then p must be prime since

$$2^{nm} - 1 = (2^n - 1)\left(\sum_{k=0}^{m-1} 2^{kn}\right)$$

for all $n, m \in \mathbb{N}^*$.

Definition 1.1.4.

(a) A $\mathbb{Q}$-point P on an elliptic curve E defined over $\mathbb{Q}$ is magnified if $P = \sigma(Q)$, for some isogeny $\sigma : E' \longrightarrow E$ defined over $\mathbb{Q}$ different from the identity map and some $\mathbb{Q}$-point Q on E'.

(b) An elliptic divisibility sequence B is magnified if B is the normalized elliptic divisibility sequence associated to some magnified point on an elliptic curve defined over $\mathbb{Q}$.

In [5] Corrales-Rodrigáñez and Schoof proved that if $B' = (B'_n)_{n\in\mathbb{N}}$ and $B = (B_n)_{n\in\mathbb{N}}$ are two normalized elliptic divisibility sequences such that B'_n divides B_n for every $n \in \mathbb{N}$, then either $B = B'$ or B is a magnified elliptic divisibility sequence. The converse is true: terms in magnified elliptic divisibility sequences admit natural factorization by terms in another associated elliptic divisibility sequence. For example, any elliptic divisibility sequence $B = (B_n)_{n\in\mathbb{N}}$ satisfies the strong divisibility property

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

and, in particular, B_n divides B_{nm} for any $n, m \in \mathbb{N}$. When $m \geq 2$ is an integer, the primality conjecture for the elliptic divisibility sequence $(B_{nm})_{n\in\mathbb{N}}$ is true if

- B_n **has a prime factor and**
- B_{nm} **has a prime factor coprime to** B_n

for all but a finite number of indices n. However, checking these two conditions is not as easy as proving that $2^n - 1$ and $\sum_{k=0}^{m-1} 2^{kn}$ are greater than 1; it requires the use of diophantine approximation to prove strong versions of Siegel's theorem on integer points on elliptic curves.

1.2. **Statement of the results.** A first approach to the problem of computing the set prime power terms in a magnified normalized elliptic divisibility sequence consists of relating it to solved questions in diophantine geometry.

Theorem 1.2.1. *Let $\sigma : E' \longrightarrow E$ be an isogeny of odd degree greater than 2 between two elliptic curves defined over $\mathbb{Q}$ by minimal equations. Denote by $\Delta_{E'}$ the minimal discriminant of E'. We use Notation* 1.1.1.

Then there is a homogeneous polynomial $F_\sigma \in \mathbb{Z}[X, Y]$ of degree $\frac{\deg(\sigma)-1}{2}$ such that the set

$$E_\sigma := \bigcup_{|d|\leq \deg(\sigma)|\Delta_{E'}|^{\deg(\sigma)/4}} \left\{(A, B) \in \mathbb{Z}^2 \ : \ F_\sigma(A, B^2) = d\right\}$$

contains all pairs $(A_{P'}, B_{P'})$ associated to $\mathbb{Q}$-points $P' \in E'(\mathbb{Q})$ such that every prime factor of $B_{\sigma(P')}$ divides $B_{P'}$.

Without the upper bound $|d| \leq \deg(\sigma)^2|\Delta_{E'}|^{\deg(\sigma)/4}$, the existence of the polynomial F_σ would not be surprising. It would be an easy consequence of the existence of division polynomials (see the proof of Theorem 1.2.1 in subsection 4.3 for an explicit formula for F_σ). The true strength of Theorem 1.2.1 lies in the inequality $|d| \leq \deg(\sigma)^2|\Delta_{E'}|^{\deg(\sigma)/4}$. This upper bound being explicit, the set E_σ can be computed in theory by solving a finite number of explicit Thue equations:

$$F_\sigma(A, B^2) = d,$$

using the algorithm described in [31]. As explained above in the case $\sigma = [m]$, a term $B_{n\sigma(P')}$ fails to be prime if $B_{nP'} > 1$ and $B_{n\sigma(P')}$ has a prime factor coprime to $B_{nP'}$. In particular, $B_{n\sigma(P')}$ fails to be prime if $B_{nP'} > 1$ and $(A_{nP'}, B_{nP'}) \notin E_\sigma$. Since the condition $B_{nP'} > 1$ can be checked using algorithms for the search for integer points on elliptic curves, Theorem 1.2.1 leads to a theoretical method for the computation of all prime power terms in magnified elliptic divisibility sequences. However, in practice the set E_σ can be computed only when $\deg(\sigma)$ is small: the number of Thue equations involved in the definition of E_σ in Theorem 1.2.1 grows exponentially with $\deg(\sigma)$. We address this difficulty by adopting a different approach to the Mersenne problem for elliptic curves. We adapt results from [15] and use height theory to compute explicit bounds on the index of prime power terms in magnified elliptic divisibility sequences.

Theorem 1.2.2. *Let $\sigma : E' \longrightarrow E$ be an isogeny defined over $\mathbb{Q}$ between two elliptic curves defined by minimal equations. Let $P' \in E'(\mathbb{Q})$ be a $\mathbb{Q}$-point on E' of infinite order. We use Notation* 1.1.1.

Then $B_{n\sigma(P')}$ has two distinct prime factors coprime to $B_{P'}$ for all prime numbers

$$n > \max\left\{3.5 \times 10^{29} C(P'), 4 \times 10^{27} C(P')^{7/2} \widehat{h}(\sigma(P'))^{5/2}\right\}$$

and all composite numbers

$$n > \max\left\{7089 C(P'), 5C(P') \left(\log(18C(P'))\right)^2\right\},$$

where $\widehat{h}$ denotes the canonical height, h_{Falt} denotes the Faltings height and

$$C(P') := \max\left\{1, \frac{2h_{Falt}(E') + 10}{\widehat{h}(P')}\right\}.$$

Moreover, there are at most two prime numbers N_1 and N_2 with

$$N_i > 34C(P')$$

and $B_{N_i\sigma(P')}$ having no more than one prime factor coprime to $B_{P'}$.

Remark 1.2.3. If n is coprime to $\deg(\sigma)$, then, under the same hypotheses as in Theorem 1.2.2, we can show that $B_{n\sigma(P')}$ has in fact two distinct prime factors coprime to $B_{\sigma(P')}$ (see the proof of Theorem 5.3 for details).

In Remark 8.4.1 we give bounds on indices n such that $B_{n\sigma(P')}$ has at most one prime factor coprime to $B_{\sigma(P')}$ (without any coprimality condition of n and $\deg(\sigma)$). Those bounds depend on $\deg(\sigma)$. This is not the case for the bounds given in Theorem 1.2.2. In fact, if Lang's Conjecture 1.2.6 the bounds given in Theorem 1.2.2 can be bounded above by an absolute constant (i.e., a constant that does not depend on (E', E, P', P, σ)).

Remark 1.2.4. Theorem 1.2.2 is part of a two-step method to compute the set of prime power terms in sequences $\left(B_{n\sigma(P')}/B_{P'}\right)_{n\in\mathbb{N}}$:

(a) compute a bound N on the index of a prime power term in the sequence $\left(B_{n\sigma(P')}/B_{P'}\right)_{n\in\mathbb{N}}$;
(b) use the bound N to sieve for all prime power terms in $(B_{n\sigma(P')}/B_{P'})_{n\in\mathbb{N}}$.

The second part can be done by adapting the algorithms for the search for integer points on elliptic curves or for the computation of solutions to Thue equations (see

for example [31]), since $B_{n\sigma(P')}/B_{P'}$ cannot be a prime power if $B_{n\sigma(P')}/B_{nP'}$ and $B_{n(P')}/B_{P'}$ are coprime and greater than or equal to 2.

Theorem 1.2.2 gives three bounds on the index of a prime power term in the sequence $\left(B_{n\sigma(P')}/B_{P'}\right)_{n\in\mathbb{N}}$:

- one very large general bound;
- two far more reasonable bounds which are valid for all but at most two prime indices N_1 and N_2.

The general bound should only be used when searching for the exceptional indices N_1 and N_2 if they exist. The two other bounds are far smaller, thus better suited to the computation of the set of all integers $n \notin \{N_1, N_2\}$ such that $B_{n\sigma(P')}/B_{P'}$ is a prime power.

The proof of Theorem 1.2.2 is based on Siegel's theorem on integer points on elliptic curves and, more precisely, on upper bounds for archimedean heights of multiples of P' and $\sigma(P')$. Theorem 1.2.2 can be refined when good bounds on the archimedean heights of the multiples of P' and $\sigma(P')$ are known.

Example 1.2.5. We consider Notation 1.1.1 when equation (1) is

$$E_A : y^2 = x(x^2 - A),$$

where A is a positive integer not divisible by a fourth power. Let P' be a $\mathbb{Q}$-point of infinite order on E_A. Let m be an integer. Assume that either m is even or P' is on the bounded real connected component of E_A. Then $B_{nmP'}$ is a composite

- whenever $n \geq 5$ if $A \not\equiv 12 \bmod 16$;
- whenever $n \geq 10$ if $A \equiv 12 \bmod 16$.

Example 1.2.5 is obtained in section 9 by computing an upper bound for the number $C(P')$ introduced in Theorem 1.2.2 that does not depend on (E', P'), i.e., by proving a particular case of the following conjecture of Lang.

Conjecture 1.2.6 (Lang)**.** *There is an absolute constant $C > 0$ such that, for every $\mathbb{Q}$-point P of infinite order on an elliptic curve E defined over $\mathbb{Q}$ by a minimal equation, the following inequality holds:*

$$h_{Falt}(E) \leq C\widehat{h}(P).$$

Hindry and Silverman proved in [13] that Lang's conjecture is a consequence of the Szpiro conjecture. This result was improved in [21]: Petsche showed that

$$\frac{\log|\Delta_E|}{\widehat{h}(P)} \leq 10^{15}\left(\frac{\log|\Delta_E|}{\log|\mathcal{F}_E|}\right)^6 \log^2\left(104613\left(\frac{\log|\Delta_E|}{\log|\mathcal{F}_E|}\right)^2\right),$$

where $\mathcal{F}_E$ (respectively Δ_E) denotes the conductor (respectively the minimal discriminant) of E.

In [2], Lang's conjecture is proven unconditionally for curves E_{N^2} with $N \in \mathbb{N}$ squarefree. Example 1.2.5 has been obtained by generalizing this result to curves E_A with A positive. The main difficulty for this generalization is the computation of the reduction type of E_A at each prime integer. This is achieved by applying Tate's algorithm. This example is also studied in [33] but without any condition on the sign of A.

While all previously stated results were unconditional, Corollary 1.2.8 below is a generalization of Example 1.2.5 which can be obtained only when assuming Lang's

conjecture and the following conjecture of Hall and Lang, which gives a very strong version of Siegel's theorem.

Conjecture 1.2.7 (Hall–Lang)**.** *There are two constants $K, \gamma > 0$ such that, for every quadruple of integers (A, B, x, y) with $y^2 = x^3 + Ax + B$ the following inequality holds:*

$$\max\{|x|, |y|\} \leq K \max\{|A|, |B|\}^{\gamma}.$$

Corollary 1.2.8. *Let $\sigma : E' \longrightarrow E$ be an isogeny defined over $\mathbb{Q}$ between two elliptic curves. Let $P' \in E'(\mathbb{Q})$ be a $\mathbb{Q}$-point on E' of infinite order. We use Notation* 1.1.1*. We assume*

(a) *that E and E' are defined by minimal short Weierstrass equations;*
(b) *the Lang Conjecture* 1.2.6 *holds;*
(c) *the Hall–Lang Conjecture* 1.2.7 *holds with $\gamma < \frac{\deg(\sigma)}{4}$.*

Then there is a constant $N \geq 0$ independent of (E, E', P', σ) such that $B_{n\sigma(P')}$ has two distinct prime factors coprime to $B_{P'}$ for every index $n > N$.

Corollary 1.2.8 is an improvement on the main result in [10]: assuming the Lang conjecture and the Hall–Lang conjecture we state the existence of a uniform bound on the index (and not only on the number) of prime power terms in elliptic divisibility sequences.

Given a point P on an elliptic curve, the multiple nP is an integer point if and only if the n-th term in the elliptic divisibility sequence associated to P is a unit (i.e., has no prime factor). This explains why we need the Hall–Lang conjecture to prove the existence of a uniform bound on the maximal index n such that B_{nP} has at most one prime factor.

2. Sketches of the proofs

2.1. **The division polynomial and Thue equations.** We use the notation of Theorem 1.2.1. The x-coordinates $x_{\mathcal{E}} : \mathcal{E} \longrightarrow \mathbb{P}^1$ on an elliptic curve $\mathcal{E}$ in Weierstrass form is a 2-covering of $\mathbb{P}^1$ such that $x_{\mathcal{E}} \circ [-1] = x_{\mathcal{E}}$. Since $\deg(\sigma)$ is odd, our isogeny $\sigma : E' \longrightarrow E$ commutes with $[-1]$. In particular, σ induces a morphism of algebraic varieties $\varphi_\sigma : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ such that $x_E \circ \sigma = \varphi_\sigma \circ x_{E'}$. The poles of φ_σ are the x-coordinates of the elements of $\ker(\sigma)$. Moreover, φ_σ has even valuation at its poles, i.e., $\varphi_\sigma = \phi_\sigma / \psi_\sigma^2$ for some $\phi_\sigma, \psi_\sigma \in \mathbb{Z}[x]$. Up to a choice of its leading coefficient, the polynomial ψ_σ is the division polynomial associated to σ. Our choice for the polynomial F_σ is the homogeneization $F_\sigma(X, Z) := Z^{(\deg(\sigma)-1)/2} \psi_\sigma(X/Z)$ of the division polynomial associated to σ.

The denominator $B_{P'}$ divides $B_{\sigma(P')}$. From our definition for F_σ we know the denominator $B_{\sigma(P')}$ divides the integer $B_{P'} F_\sigma\left(A_{P'}, B_{P'}^2\right)$. We get a factorization in $\mathbb{Z}$,

$$F_\sigma\left(A_{P'}, B_{P'}^2\right) = \frac{B_{\sigma(P')}}{B_{P'}} \frac{B_{P'}^{deg(\sigma)} \psi_\sigma(x(P'))}{B_{\sigma(P')}}.$$

Since $\deg(\sigma)$ is odd, the theory of formal groups shows that, if every prime factor of $B_{\sigma(P')}$ divides $B_{P'}$, then $\frac{B_{\sigma(P')}}{B_{P'}}$ divides $\deg(\sigma)$. The proof of Theorem 1.2.1 consists of using height theory to bound $\frac{B_{P'}^{deg(\sigma)} \psi_\sigma(x(P'))}{B_{\sigma(P')}}$. More precisely, the denominators

$B_{P'}$ and $B_{\sigma(P')}$ can be defined using naive local heights:

$$\log|B_{P'}| = \sum_{v \text{ prime}} (h_v(\sigma(P'))),$$

$$\log\left|B_{\sigma(P')}\right| = \sum_{v \text{ prime}} h_v(\sigma(P')).$$

In the same way $\log|\psi_\sigma(P')|$ can be expressed in terms of canonical local heights after proving a consequence of a generalized quasi-parallelogram law for canonical local heights:

$$\log|\psi_\sigma(P')| = \frac{\deg(\sigma)\log|\Delta_{E'}| - \log|\Delta_E|}{12} + \sum_{v \text{ prime}} \left(\widehat{h}_v(\sigma(P')) - \deg(\sigma)\widehat{h}_v(P')\right).$$

Theorem 1.2.1 follows from these three formulas, by invoking bounds on the difference between naive local heights and canonical local heights.

2.2. **Computing bounds on the index of prime power terms in magnified elliptic divisibility sequences.** The proof of the primality conjecture for magnified elliptic divisibility sequences relies on:

- the theory of formal groups which shows that, if $n \in \mathbb{N}$ is any integer such that each prime factor of $B_{n\sigma(P')}$ divides $B_{nP'}$, then

$$\log\left|B_{n\sigma(P')}\right| \leq \log|B_{nP'}| + \log|B_{sP'}| + \log(\deg(\sigma)); \tag{2}$$

  with $1 \leq s \leq 10$.
- Siegel's theorem which implies the existence of $h > h' > 0$ such that

$$\lim_{n\longrightarrow\infty} \frac{\log|B_{nP'}|}{n^2} = h' \quad \text{and} \quad \lim_{n\longrightarrow\infty} \frac{\log\left|B_{n\sigma(P')}\right|}{n^2} = h.$$

Since $h' < h$, the difference between the growth rate of $B_{nP'}$ and $B_{n\sigma(P')}$ implies that equation (2) holds only for finitely many n. In particular, $B_{n\sigma(P')}$ has a prime factor l_n coprime to $B_{nP'}$ for all but finitely many n. Siegel's theorem asserts that $B_{nP'}$ has a prime factor l'_n for all but finitely many n. Since l'_n and l_n both divide $B_{n\sigma(P')}$ and are coprime, $B_{n\sigma(P')}$ is a prime power only for finitely many indices n. In section 5 we explain how this argument can be made explicit assuming more precise statements of Siegel's theorem, namely inequalities from diophantine approximation of the form

$$\widehat{h_\infty}(P) \leq \epsilon\widehat{h}(P) + M,$$

where P is a point on an elliptic curve E defined over $\mathbb{Q}$, $\widehat{h_\infty}$ and $\widehat{h}$ are, respectively, the canonical archimedean height and the canonical height on E, and $\epsilon \in]0,1[$ and $M > 0$ are constants (independent of P). The remainder of the article is dedicated to the study of various statements of Siegel's theorem:

- in section 6 we prove Corollary 1.2.8 by assuming the Hall–Lang Conjecture 1.2.7 on the archimedean height of integer points on elliptic curves;
- in section 7 we explain how division polynomials can be used to prove a sharp version of Siegel's theorem for integral multiples of magnified points, which implies a bound on the composite integers which are the index of a prime power term in a given magnified elliptic divisibility sequence;

- in section 8 we use David's lower bound on linear forms in two elliptic logarithms to prove a general bound on the index of a prime power term in a given magnified elliptic divisibility sequence;
- in section 8 we prove the last statement in Theorem 1.2.2 using a gap principle to obtain a refinement of David's lower bound for linear forms in elliptic logarithms, which is stated without numerical values in [15].

For a simplified example of the techniques above we refer the reader to the proof of Example 1.2.5 in section 9.

3. Notation

We use the following notation:

Notation 3.0.1.

E', E	elliptic curves defined over $\mathbb{Q}$ by standardized minimal equations
$\sigma : E' \longrightarrow E$	an isogeny defined over $\mathbb{Q}$ of degree at least 2
d	degree of σ
P'	a $\mathbb{Q}$-point of infinite order on E'
$(B_{nP'})_{n\in\mathbb{N}}$	normalized elliptic divisibility sequence associated to P'
$r_{l,P'}$	the rank of apparition of a prime l in $(B_{nP'})_{n\in\mathbb{N}}$ (see Def. 4.2.4)
P	the image $\sigma(P')$
$(B_{n\sigma(P')})_{n\in\mathbb{N}}$	normalized elliptic divisibility sequence associated to $P := \sigma(P')$
h	naive height
$\widehat{h}$	canonical height
h_∞	naive archimedean height
$\widehat{h_\infty}$	canonical archimedean height
h_v	naive local height at a place v
$\widehat{h_v}$	canonical local height at a place v
$\Delta_{\mathcal{E}}$	discriminant of an elliptic curve $\mathcal{E}$
$h(\mathcal{E})$	naive height of an elliptic curve $\mathcal{E}$
$h_{Falt}(\mathcal{E})$	Faltings height of an elliptic curve $\mathcal{E}$

All height functions are defined using the same normalizations as in [27]. In particular, naive local heights functions are defined by

$$h_v(x) = \max\{0, -v(x)\} = \max\{0, -\operatorname{ord}_v(x)\log(p)\}$$

for any $x \in \mathbb{Q}$ and

$$h_v(P) = \frac{1}{2}h_v(x(P))$$

for any $\mathbb{Q}$-point P on an elliptic curve $\mathcal{E}$ as in Notation 1.1.1. Moreover, if $\mathcal{E}$ is given by a minimal Weierstrass equation, then

$$h(\mathcal{E}) = \frac{1}{12}\max\{h(j(\mathcal{E})), h(\Delta_{\mathcal{E}})\}.$$

The isogeny σ and all other isogenies in this article will be assumed to be different from the identity map.

4. Computing the set of indices of prime power terms in magnified elliptic divisibility sequences

One of the main difficulties when studying the primality conjecture for magnified points is to compute the denominator of the image of a given point under a given isogeny in an appropriate way. This can be done using division polynomials to reformulate a formula from Vélu. For the convenience of the reader, we begin by recalling some basic facts on division polynomials. We refer to [18, appendix 1] for details.

4.1. **Background on division polynomials.**

Notation 4.1.1. We use Notation 3.0.1. An elliptic curve $\mathcal{E} \in \{E', E\}$ is given by a minimal Weierstrass equation

$$\mathcal{E} : y_{\mathcal{E}}^2 + a_1 x_{\mathcal{E}} y_{\mathcal{E}} + a_3 y_{\mathcal{E}} = x_{\mathcal{E}}^3 + a_2 x_{\mathcal{E}}^2 + a_4 x_{\mathcal{E}} + a_6$$

in coordinates $(x_{\mathcal{E}}, y_{\mathcal{E}})$. The function $z_{\mathcal{E}} := -x_{\mathcal{E}}/y_{\mathcal{E}}$ is a uniformizer at $\mathcal{O}_{\mathcal{E}}$.

As in Theorem 1.2.1 we assume $d = \deg(\sigma)$ is odd. Then the divisor $\sigma^* (\mathcal{O}_E) - \deg(\sigma)\mathcal{O}_{E'}$ being principal, we can associate with σ a nonzero function ψ_σ on E whose divisor $\operatorname{div}(\psi_\sigma)$ is

$$\operatorname{div}(\psi_\sigma) = \sigma^* (\mathcal{O}_E) - \deg(\sigma)\mathcal{O}_{E'}.$$

The function ψ_σ is defined only up to multiplication by a constant. To define ψ_σ in a unique way we introduce a normalization condition

$$\left(\frac{z_{E'}^d \psi_\sigma}{z_E \circ \sigma}\right)(\mathcal{O}_{E'}) = 1,$$

where $z_{E'}$ and z_E are the two uniformizers at $\mathcal{O}_{E'}$ and $\mathcal{O}_E$ defined above.

Since $d = \deg(\sigma)$ is odd, the function ψ_σ is a polynomial in $x_{E'}$ called the division polynomial associated to σ. From now on we will denote by $d_\sigma \in \mathbb{Z}$ the leading coefficient of ψ_σ.

Remark 4.1.2. Consider the differential form

$$\omega_{\mathcal{E}} = \frac{dx_{\mathcal{E}}}{2y_{\mathcal{E}} + a_1 x_{\mathcal{E}} + a_3} = \left(1 + a_1 z_{\mathcal{E}} + \left(a_1^2 + a_2\right) z_{\mathcal{E}} + \cdots\right) dz_{\mathcal{E}}.$$

We have $\left(\frac{dz_{\mathcal{E}}}{\omega_{\mathcal{E}}}\right)(\mathcal{O}_{\mathcal{E}}) = 1$. In particular, our definition of the division polynomial ψ_σ is consistant with [18, appendix 1]: it corresponds to the division polynomial associated to σ and the differential forms $\omega_{E'}$ and ω_E.

Lemma 4.1.3. *We use Notation* 4.1.1. *Then the functions ψ_σ and $\phi_\sigma := (x_E \circ \sigma)\,\psi_\sigma^2$ are elements of $\mathbb{Z}[x_{E'}]$. Moreover, ϕ_σ is a monic polynomial in $x_{E'}$ of degree* $\deg(\sigma)$.

Proof. The two functions ψ_σ and ϕ_σ are given by

$$\begin{aligned} \psi_\sigma^2 &= d_\sigma^2 \prod_{T \in \ker(\sigma),\ T \neq \mathcal{O}_{E'}} \left(x_{E'} - x_{E'}(T)\right), \\ \phi_\sigma &= \prod_{T \in E'(\overline{\mathbb{Q}}),\ x_E(\sigma(T)) = 0} \left(x_{E'} - x_{E'}(T)\right), \end{aligned}$$

where $d_\sigma \in \mathbb{Q}$ is such that $\sigma^* \omega_E = d_\sigma \omega_{E'}$. We wish to show that the coefficients of ϕ_σ and ψ_σ^2 are in $\mathbb{Z}$.

For any number field K, and any finite place v of K, the set

$$E_1'(K_v) := \{P \in E'(K_v) \ : \ P \equiv \mathcal{O}_{E'} \mod v\}$$

is a subgroup of $E'(K_v)$. The image $\sigma(E_1'(K_v))$ is included in $E_1(K_v)$. In particular, the points $T \in E'(\overline{\mathbb{Q}})$ with $x_E(\sigma(T)) = 0$ are integral. Thus ϕ_σ is in $\mathbb{Z}[x_{E'}]$.

The study of ψ_σ is implicitly done in [29]. While the main results in [29] focus on endomorphisms of elliptic curves, the intermediate results on formal groups we need are proven for a general isogeny. For background on formal groups, we refer the reader to [24, Chapter IV].

Let p pe a prime number. Every rational function on $\mathcal{E} \in \{E', E\}$ can be expressed as a Laurent series in $z_{\mathcal{E}}$. This means that we have an embedding $\mathcal{P}_{\mathcal{E}} : \mathbb{Q}_p(\mathcal{E}) \longrightarrow \mathbb{Q}_p((T))$ (see [24, Chapter IV.1] for computations of $\mathcal{P}_{E'}(x_{E'})$ and $\mathcal{P}_{E'}(y_{E'})$). Let

$$F_\sigma := \mathcal{P}_{E'}(z_E \circ \sigma) = \exp_{\widehat{E}}(d_\sigma \log_{\widehat{E'}}(T))$$

(where $\widehat{E}$ and $\widehat{E'}$ are the formal groups associated to E and E'). The power series F_σ gives an homomorphism of formal groups

$$F_\sigma^* : \mathbb{Q}_p((T)) \longrightarrow \mathbb{Q}_p((T)), \ f(T) \longmapsto f(F_\sigma(T))$$

such that $\mathcal{P}_{E'} \circ (\sigma^*) = F_\sigma^* \circ \mathcal{P}_E$.

The elliptic curves E and E' being given by minimal equations, we know from [29] that the power series F_σ has p-integral coefficients. In particular, $\mathcal{P}_{E'}\left(\frac{1}{x_E \circ \sigma}\right) = F_\sigma^* \mathcal{P}_E\left(\frac{1}{x_E}\right)$ has p-integral coefficients. Since ϕ_σ has integral coefficients, $\mathcal{P}_{E'}(\phi_\sigma) = \phi_\sigma(\mathcal{P}_{E'}(x_{E'}))$ has p-integral coefficients. This implies that $\mathcal{P}_{E'}(\psi_\sigma^2) = \mathcal{P}_{E'}\left(\frac{\phi_\sigma}{x_E \circ \sigma}\right)$ has p-integral coefficients. It follows that the coefficients of ψ_σ^2 are p-integral because $\mathcal{P}_{E'}(\psi_\sigma^2) = \psi_\sigma^2(\mathcal{P}_{E'}(x_{E'}))$ and

$$\mathcal{P}_{E'}(x_{E'}) = \frac{1}{T^2} - \frac{a_1}{T} - a_2 - a_3 T - \cdots,$$

where the integers a_i are coefficients of the minimal equation defining E' (in fact, one could even recursively retrieve the coefficients of ψ_σ^2 as polynomials in some coefficients of $\psi_\sigma^2(\mathcal{P}_{E'}(x_{E'}))$). □

Lemma 4.1.4. *Let E, E', E'' be three elliptic curves defined over $\mathbb{Q}$ by Weierstrass equations with integral coefficients. Let $\sigma : E \longrightarrow E'$ and $\tau : E' \longrightarrow E''$ be two isogenies defined over $\mathbb{Q}$. Then the two following equalities hold:*

$$(\phi_\tau \circ \sigma)\psi_\sigma^{2\deg(\tau)} = \phi_{\tau\circ\sigma},$$
$$(\psi_\tau \circ \sigma)^2 \psi_\sigma^{2\deg(\tau)} = \psi_{\tau\circ\sigma}^2.$$

Proof. The formula for $\psi_{\tau\circ\sigma}^2$ is obtained by comparing the divisors of the two functions $(\psi_\tau \circ \sigma)^2 \psi_\sigma^{2\deg(\tau)}$ and $\psi_{\tau\circ\sigma}^2$; see [18, Appendix 1] for a more general result. The assertion for $\phi_{\tau\circ\sigma}$ follows since $\frac{\phi_{\tau\circ\sigma}}{\psi_{\tau\circ\sigma}^2} = x \circ \tau \circ \sigma = \frac{\phi_\tau \circ \sigma}{(\psi_\tau \circ \sigma)^2}$. □

Remark 4.1.5. When τ is the dual isogeny of σ, Lemma 4.1.4 implies that the leading coefficient d_σ of ψ_σ must be a divisor of $\deg(\sigma)$.

Notation 4.1.6. We keep the hypotheses of Lemma 4.1.4. Then the intersection $F := E[\deg(\tau)] \bigcap \ker(\tau \circ \sigma)$ is invariant under the action of the absolute Galois group of $\mathbb{Q}$. In particular, there is an elliptic curve E_{τ_σ} defined over $\mathbb{Q}$ by a minimal standardized equation, an isogeny $\tau_\sigma : E \longrightarrow E_{\tau_\sigma}$ defined over $\mathbb{Q}$ with $\ker(\tau_\sigma) = F$, and an isogeny $\sigma_\tau : E_{\tau_\sigma} \longrightarrow E''$ defined over $\mathbb{Q}$ such that the following diagram commutes

$$\begin{array}{ccc} E & \xrightarrow{\sigma} & E' \\ {\scriptstyle \tau_\sigma}\downarrow & & \downarrow{\scriptstyle \tau} \\ E_{\tau_\sigma} & \xrightarrow[\sigma_\tau]{} & E'' \end{array}$$

The isogeny σ induces an isomorphism between $E[\deg(\tau)]/\left(\ker(\sigma) \bigcap E[\deg(\tau)]\right)$ and $E'[\deg(\tau)]$. The restriction of this isomorphism to $F/\left(\ker(\sigma) \bigcap E[\deg(\tau)]\right)$ is an isomorphism between $F/\left(\ker(\sigma) \bigcap E[\deg(\tau)]\right)$ and $\ker(\tau)$. In particular, we have $\deg(\tau_\sigma) \geq \deg(\tau)$. Moreover, if $E[\deg(\tau)] \bigcap \ker(\sigma) = \{\mathcal{O}_E\}$ (for example if $\deg(\sigma)$ and $\deg(\tau)$ are coprime), then $\deg(\tau_\sigma) = \deg(\tau)$. In this particular case, using τ_σ, we point out in Lemma 4.1.7 that a natural factorization of division polynomials can be deduced from Lemma 4.1.4.

Lemma 4.1.7. *We use Notation* 4.1.6 *and we assume that* $\deg(\sigma)$ *and* $\deg(\tau)$ *are coprime. Then* $\psi_\sigma^2 \psi_{\tau_\sigma}^2$ *divides* $\psi_{\tau\circ\sigma}^2$ *in* $\mathbb{Z}[x]$.

Proof. Comparing the orders of $\ker(\sigma)$ and $\ker(\tau_\sigma)$, we show that

$$\ker(\tau \circ \sigma) = \ker(\sigma_\tau \circ \tau_\sigma) = \ker(\sigma) + \ker(\tau_\sigma).$$

The definition of a division polynomial implies that $\psi_{\tau\circ\sigma}^2 = \psi_{\sigma_\tau \circ \tau_\sigma}^2$. Applying Lemma 4.1.4, we get that $\psi_{\tau\circ\sigma}^2$ is divisible in $\mathbb{Q}[x]$ by ψ_σ^2 and by $\psi_{\tau_\sigma}^2$. The two polynomials ψ_σ^2 and $\psi_{\tau_\sigma}^2$ are coprime because $\ker(\sigma) \cap \ker(\tau_\sigma) = \{\mathcal{O}_E\}$. Both polynomials are in $\mathbb{Z}[x_E]$ (see Lemma 4.1.3); the quotient $\frac{\psi_{\tau\circ\sigma}^2}{\psi_\tau^2 \psi_\sigma^2}$ is also an element of $\mathbb{Z}[x_E]$ because its leading coefficient is an integer and its roots are the x-coordinates of points of order dividing $\deg(\sigma)\deg(\tau)$ but neither $\deg(\sigma)$ nor $\deg(\tau)$ (see [24, Theorem VII.3.4 (a)]). □

4.2. **Division polynomials and elliptic divisibility sequences.** Elliptic divisibility sequences are closely related to evaluations of division polynomials (see [35]). For points with good reduction everywhere this link is given by [1, Théorème A] which we recall in a slightly weaker form.

Theorem 4.2.1 (Ayad)**.** *Let* v *be a place of* $\mathbb{Q}$. *Let* $P \in E(\mathbb{Q})$ *be a point on* E *whose reduction at* v *is not the reduction at* v *of* $\mathcal{O}_E$. *Then the following assertions are equivalent:*

(a) *the reduction of* P *at* v *is a singular point;*
(b) *there is an integer* m *such that* $v(\psi_m(P)) > 0$ *and* $v(\phi_m(P)) > 0$*;*
(c) *for every integer* n, *we have* $v(\psi_n(P)) > 0$ *and* $v(\phi_n(P)) > 0$.

Ayad's theorem does not predict the valuation $v(\psi_m(P))$ when P has bad reduction at v. In [3] the valuations $v(\psi_m(P))$ and $v(\phi_m(P))$ are studied in terms of the smallest positive integer $N_{P,v}$ such that $N_{P,v}P$ has good reduction at v. This integer $N_{P,v}$ can easily be computed using Tate's algorithm (see [27]). However, the computation of an explicit uniform upper bound for the number of prime power terms in magnified elliptic divisibility sequences requires an estimate for

$\frac{B_P^{2\deg(\sigma)}\psi_\sigma(P)^2}{B_{\sigma(P)}^2}$ that does not depend on $N_{P,v}$. Such an estimate can be obtained from a comparison between naive local heights and their associated canonical local heights.

Lemma 4.2.2. *We use Notation* 4.1.1. *For every $P' \in E'(\mathbb{Q})$ of infinite order we have*

$$\log|\psi_\sigma(P')| = \deg(\sigma)\widehat{h_\infty}(P') - \widehat{h_\infty}(\sigma(P')) + \frac{\deg(\sigma)\log|\Delta_{E'}| - \log|\Delta_E|}{12}. \tag{3}$$

Proof. The proof is based on [12, Theorem 6.18], which states that

$$\widehat{h_\infty}(Q) = \lim_{n\to+\infty}\frac{\log|\psi_n(Q))|}{n^2} - \frac{1}{12}\log|\Delta_E|,$$

for any $Q \in E(\mathbb{Q})$, and on the quasi-parallelogram law for $\widehat{h_\infty}$, which asserts that

$$\widehat{h_\infty}(P+Q) + \widehat{h_\infty}(P-Q) = 2\widehat{h_\infty}(P) + 2\widehat{h_\infty}(Q) - \log|x(P)-x(Q)| + \frac{1}{6}\log|\Delta_E|,$$

for every $P, Q \in E(\mathbb{Q})$ such that $P, Q, P \pm Q \neq \mathcal{O}_E$.

When $\sigma = [n]$, equation (3) is proven recursively using the quasi-parallelogram law for $\widehat{h_\infty}$ and the equation $x([n]P) = x(P) - \frac{\psi_{n+1}(P)\psi_{n-1}(P)}{\psi_n(P)^2}$. This particular case of equation (3) and [12, Theorem 6.18] imply that $\lim_{n\to+\infty}\frac{\widehat{h_\infty}([n]Q)}{n^2} = 0$, for any $Q \in E'(\mathbb{Q})$. Hence the quasi-parallelogram law for $\widehat{h_\infty}$ implies that

$$\lim_{n\to+\infty,\gcd(\deg(\sigma),n)=1}\sum_{T\in\ker(\sigma),T\neq\mathcal{O}_{E'}}\frac{\log|x([n]P') - x([n]T)|}{n^2} = 0. \tag{4}$$

Applying [12, Theorem 6.18] to $\sigma(P')$ together with Lemma 4.1.4, we get

$$\begin{aligned}&\widehat{h_\infty}(\sigma(P'))\\ &\quad= \lim_{n\to+\infty,\gcd(\deg(\sigma),n)=1}\frac{\log|\psi_\sigma([n]P')\psi_n(P')^{\deg(\sigma)}\psi_\sigma(P')^{-n^2})|}{n^2} - \frac{1}{12}\log|\Delta_E|.\end{aligned}$$

From this equation we deduce equation (3) in the general case, noting that

$$\begin{aligned}&\lim_{n\to+\infty,\gcd(\deg(\sigma),n)=1}\frac{\log|\psi_\sigma([n]P')|}{n^2}\\ &\quad= \lim_{n\to+\infty,\gcd(\deg(\sigma),n)=1}\sum_{T\in\ker(\sigma),T\neq\mathcal{O}_{E'}}\frac{\log|x([n]P') - x([n]T)|}{n^2} = 0,\end{aligned}$$

and using [12, Theorem 6.18] (applied to P'). □

Proposition 4.2.3. *We use Notation* 4.1.1.

(a) *If P' has good reduction everywhere, then*

$$B_{\sigma(P')} = B_{P'}^{\deg(\sigma)}\psi_\sigma(P'). \tag{5}$$

(b) *In the general case, the quotient $\frac{B_P^{\deg(\sigma)}\psi_\sigma(P')}{B_{\sigma(P')}}$ satisfies the inequalities*

$$\log\left|B_{\sigma(P')}\right| \leq \log\left|B_{P'}^{\deg(\sigma)}\psi_\sigma(P')\right| \leq \log\left|B_{\sigma(P')}\right| + \frac{1}{8}\deg(\sigma)\log|\Delta_{E'}|. \tag{6}$$

Proof. We use the decomposition of the canonical height in a sum of local canonical heights and the equation $\widehat{h}(\sigma(P')) = \deg(\sigma)\widehat{h}(P')$ to reformulate equation (3) as

$$\log|\psi_\sigma(P')| = \frac{\deg(\sigma)\log|\Delta_{E'}| - \log|\Delta_E|}{12} + \sum_{v \text{ prime}} \left(\widehat{h}_v(\sigma(P')) - \deg(\sigma)\widehat{h}_v(P')\right).$$

Equation (5) follows, since

$$\widehat{h_v}(Q) = \frac{1}{2}\max\{0, -v(x(Q))\} + \frac{1}{12}v(\Delta_{\mathcal{E}}) = v(B_Q) + \frac{1}{12}v(\Delta_{\mathcal{E}}), \tag{7}$$

for any point $Q \in \mathcal{E}(\mathbb{Q})$ with good reduction at v (where $\mathcal{E} \in \{E', E\}$).

Inequality (6) is obtained in the same way as equation (5), except that we replace equation (7) by the following inequality:

$$\frac{1}{24}\min(0, v(j(\mathcal{E}))) \leq \widehat{h_v}(Q) - \frac{1}{2}\max\{0, -v(x(Q))\} = \widehat{h_v}(Q) - v(B_Q) \leq \frac{1}{12}v(\Delta_{\mathcal{E}})$$

(which holds for any $\mathbb{Q}$-point Q on an elliptic curve $\mathcal{E}$ given by a minimal Weierstrass equation; see [17, Chapter III, Theorem 4.5] for details). □

The proof of Theorem 1.2.1 is based on two results: Proposition 4.2.3, which compare elliptic divisibility sequences with evaluations of division polynomials, and an explicit description of the behaviour of the l-adic norms of the terms in an elliptic divisibility sequence $(B_n)_{n\in\mathbb{N}}$ when n varies among multiples of the rank of apparition of l (see Lemma 4.2.6 below).

Definition 4.2.4. Let Q be a $\mathbb{Q}$-point on an elliptic curve E defined over $\mathbb{Q}$. Let l be a prime number. We call the *rank of apparition* of l in the elliptic divisibility sequence $(B_{nQ})_{n\in\mathbb{N}}$ associated to Q the order

$$\begin{aligned} r_{l,Q} &:= \min\{n \in \mathbb{N}\setminus\{0\} \ : \ nQ \equiv \mathcal{O}_E \mod l\} \\ &= \min\{n \in \mathbb{N}\setminus\{0\} \ : \ B_{nQ} \equiv 0 \mod l\} \end{aligned}$$

of the reduction of Q modulo l

Lemma 4.2.5. *Let Q be a $\mathbb{Q}$-point on an elliptic curve E defined over $\mathbb{Q}$ and let $(B_{nQ})_{n\in\mathbb{N}}$ be the elliptic divisibility sequence associated to Q. Let l be a prime number. Then we have:*

- *$v_l(B_{nQ}) > 0$ if and only if $r_{l,Q}$ divides n;*
- *$r_{l,Q} \leq l + 1 + 2\sqrt{l}$.*

Proof. The second assertion is a consequence of the Hasse-Weil bound on the number of rational points on an elliptic curve defined over a finite field. The first assertion is proven by noticing that $r_{l,P}$ is a generator of the kernel of the group homomorphism $\mathrm{red}_l : \mathbb{Z} \longrightarrow E(\mathbb{F}_l), n \longmapsto nQ \mod l$. □

Lemma 4.1.4 explains how the division polynomial associated to the composition of two isogenies factorizes in a natural way. The following key lemma gives an analogous property for terms in a magnified elliptic divisibility sequence.

Lemma 4.2.6. *We use Notation* 3.0.1. *Recall that $d = \deg(\sigma)$. Let l be a prime number. Let $n \in \mathbb{N}$ be an integer.*

(a) *In all cases we have*

$$v_l(B_{nP'}) \leq v_l\left(B_{n\sigma(P')}\right)$$

(b) *If* $v_l(B_{nP'}) > 0$, *and either* $v_2(B_{nP'}) > 1$ *or* $l \neq 2$ *or* $\deg(\sigma)$ *is odd, then*

$$v_l\left(B_{n\sigma(P')}\right) \leq v_l\left(B_{r_{l,P'}P'}\right) + v_l\left(\frac{n\deg(\sigma)}{r_{l,P'}}\right).$$

(c) *If* $l = 2$ *and* $v_2(B_{nP'}) = 1$, *then*

$$v_2\left(B_{n\sigma(P')}\right) \leq v_2\left(B_{sP'}\right) + v_2(n\deg(\sigma))$$

with $s = 2r_{2,P'}$ *(in particular, the Hasse-weil bound implies that* $s \leq 10$*).*

Proof. We use Notation 4.1.1 (but we do not assume that $\deg(\sigma)$ is odd). Let $\widehat{E}$ and $\widehat{E'}$ be the formal groups associated respectively to E and E'. As in the proof of Lemma 4.1.3, for $\mathcal{E} \in \{E', E\}$, we define an embedding $\mathcal{P}_{\mathcal{E}} : \mathbb{Q}_l(\mathcal{E}) \longrightarrow \mathbb{Q}_l((T))$ by expressing every rational function on $\mathcal{E}$ as a Laurent series in $z_{\mathcal{E}}$. We know from [29] that the power series

$$F_\sigma := \mathcal{P}_{E'}(z_E \circ \sigma) = \exp_{\widehat{E}}(d_\sigma \log_{\widehat{E'}}(T))$$

has l-integral coefficients. In particular, F_σ converges over the disc D_l in $\mathbb{Q}_l$ of center 0 and radius 1, and, since $F_\sigma(0) = 0$, we have $|F_\sigma(z)|_l \leq |z|_l$ for any $z \in D_l$.

The proof Lemma 4.2.6 is straightforward when $v_l(B_{nP'}) = 0$. From now on we assume that l divides $B_{nP'}$ or equivalently that nP' and $\mathcal{O}_{E'}$ have the same reduction modulo l. This implies that $\sigma(nP')$ and $\mathcal{O}_E$ have the same reduction modulo l. In particular, l divides $B_{n\sigma(P')}$. The divisibility of $B_{nP'}$ and $B_{n\sigma(P')}$ by l means that $|z_{E'}(nP')|_l < 1$ and $|z_E(n\sigma(P')|_l < 1$. Assertion (a) follows:

$$v_l(B_{n\sigma(P')}) = v_l(z_E(n\sigma(P'))) = v_l(F_\sigma(z_{E'}(nP'))) \geq v_l((z_{E'}(nP')) = v_l(B_{nP'}).$$

Replacing nP' by $n\sigma(P')$ and σ by the dual isogeny of σ, we get

$$v_l(B_{nP'}) \leq v_l(B_{n\sigma(P')}) \leq v_l(B_{n\deg(\sigma)P'}). \tag{8}$$

Using inequalities (8) we deduce assertions (b) and (c) from the particular case when $\sigma = [m]$ is the multiplication-by-m map on E'. In fact, we know from [28, Lemma 1.2] that:

(i) $v_l(B_{kmP'}) \geq v_l(B_{kP'}) + v_l(m)$ always;

(ii) $v_l(B_{kmP'}) > v_l(B_{kP'}) + v_l(m)$ if and only if the two following conditions are satisfied:
- $l = 2$, and 2 divides m, and $v_2(B_{kP'}) = 1$;
- E' has ordinary or multiplicative reduction at 2.

If l does not divide $\deg(\sigma)$, then $v_l(B_{n\deg(\sigma)P'}) = v_l(B_{nP'})$. In that case, inequalities (8) imply that $v_l(B_{n\sigma(P')}) = v_l(B_{nP'})$. From now on we assume that l divides $\deg(\sigma)$.

The power series $\exp_{\widehat{E}}(z)$ and $\log_{\widehat{E'}}(z)$ converge for any $z \in \mathbb{Q}_l$ with $v_l(z) > \frac{1}{l-1}$. Moreover, both power series preserve the l-adic valuation of any such $z \in \mathbb{Q}_l$ with $v_l(z) > \frac{1}{l-1}$. In [29], this observation is used to deduce from the equality $F_\sigma = exp_{\widehat{E}}(d_\sigma \log_{\widehat{E'}}(T))$ that

$$v_l(B_{n\sigma(P')}) = v_l(B_{nP'}) + v_l(d_\sigma)$$

whenever $v_l(B_{nP'}) > \frac{1}{l-1}$. Since $v_l(d_\sigma) \leq v_l(\deg(\sigma))$, this implies Lemma 4.2.6 when $v_l(B_{nP'}) > 1$ or $1 > \frac{1}{l-1}$, i.e., when $v_l(B_{nP'}) \geq 2$ or $l > 2$. From now on we assume that $l = 2$ and $v_2(B_{nP'}) = 1$.

Since $v\left(B_{r_{2,P'}P'}\right) \geq 1$, we obtain from assertion (i) above that

$$v_2(B_{2r_{2,P'}P'}) \geq v\left(B_{r_{2,P'}P'}\right) + 1 \geq 2.$$

In particular, assertion (ii) above implies that

$$v_2(B_{2mr_{2,P'}P'}) = v_2(B_{2r_{2,P'}P'}) + v_2(m)$$

for any $m \in \mathbb{N}$. Since $v_2(B_{nP'}) > 0$ we know that $r_{2,P'}$ divides n. Moreover, we have assumed that 2 divides $\deg(\sigma)$. It follows that

$$v_2(B_{n\sigma(P')}) \leq v_2(B_{\deg(\sigma)nP'}) = v_2(B_{2r_{2,P'}P'}) + v_2\left(\frac{\deg(\sigma)n}{2r_{2,P'}}\right). \qquad \square$$

4.3. **The proof of Theorem 1.2.1.** Let $P' \in E'(\mathbb{Q})$ be a point such that every prime factor of $B_{\sigma(P')}$ divides $B_{P'}$. Then, since $\deg(\sigma)$ is odd, Lemma 4.2.6 implies that $B_{\sigma(P')}$ divides $\deg(\sigma)B_{P'}$. Applying inequality (6) to the point P' and simplifying, we get

$$\left|B_{P'}^{\deg(\sigma)-1}\psi_\sigma(P')\right| \leq \deg(\sigma)|\Delta_{E'}|^{\deg(\sigma)/4}.$$

5. Prime power terms in elliptic divisibility sequences and Siegel's theorem

In this section we explain how an explicit statement for the primality conjecture for magnified elliptic divisibility sequences can be derived from explicit variants of Siegel's theorem and, more precisely, from upper bounds on the archimedean heights of multiples of a point.

We begin with the following lemma, which is useful when trying to solve various inequalities appearing in the proof of the primality conjecture. The technical introduction of the real number A helps to optimize the size of the bound obtained. Such an optimization will not be important in this section as we will choose $A = 1$. However, we will need to apply Lemma 5.1 with $A = \frac{1}{\sqrt{\hat{h}(P')}}$ in the proofs of Corollary 7.2.2 and Corollary 7.3.1. We will also need to apply Lemma 5.1 with $A = 10^{18}$ and $\delta = 6$ in the proof of Proposition 8.2.1.

Lemma 5.1. *Let a, b and $A \geq 1$ be three positive real numbers. Let $n, \delta \geq 1$ be two positive integers such that*

$$n^2 \leq a(\log(n) + 1)^\delta + b.$$

Then we have $n \leq \max\left\{A\left(2\delta\log(2\delta) + 2\log(A)\right)^\delta, \frac{a}{A} + \sqrt{b}\right\}$.

Proof. Assume $n \geq A\left(2\delta\log(2\delta) + 2\log(A)\right)^\delta$. The map $x \longmapsto \log(x) - \frac{x}{A^{1/\delta}\delta}$ is decreasing on $[A^{1/\delta}\delta, +\infty[$. It follows that

$$\log(n^{1/\delta}) - \frac{n^{1/\delta}}{A^{1/\delta}\delta} \leq \log\left(A^{1/\delta}\left(2\delta\log(2\delta) + 2\log(A)\right)\right) - 2\log(2\delta) - \frac{2\log(A)}{\delta}.$$

Since $\log(x) \leq \frac{x}{2\delta} + \log(2\delta) - 1$ for every $x \geq 2\delta$, we have

$$\begin{aligned}\log\left(A^{1/\delta}\left(2\delta\log(2\delta) + 2\log(A)\right)\right) &= \log\left(2\delta\log(2\delta) + 2\log(A)\right) + \tfrac{\log(A)}{\delta} \\ &\leq 2\log(2\delta) + \tfrac{2\log(A)}{\delta} - 1.\end{aligned}$$

In particular, we get

$$\log(n^{1/\delta}) \leq \frac{n^{1/\delta}}{A^{1/\delta}\delta} - 1.$$

From this inequality and the inequality

$$n^2 \leq a(\log(n)+1)^\delta + b \leq a(\delta\log(n^{1/\delta})+1)^\delta + b,$$

we deduce that either $n^2 \leq \frac{a}{A}n + b$ or $n \leq A\left(2\delta\log(2\delta) + 2\log(A)\right)^\delta$. □

Lemma 4.2.6 describes the difference between the v-height of a point P' on an elliptic curve and the v-adic height of the image $\sigma(P')$ of P' by an isogeny σ. In Proposition 5.2, we apply Lemma 4.2.6 to the study of the canonical height of $\sigma(P')$.

Proposition 5.2. *Let P be a $\mathbb{Q}$-point on an elliptic curve E defined over $\mathbb{Q}$ by a standardized minimal Weierstrass equation and let $(\sigma_i : E_i \longrightarrow E)_{i\in I}$ be a finite family of isogenies between elliptic curves defined over $\mathbb{Q}$ by standardized minimal Weierstrass equations. For each $i \in I$ we consider a $\mathbb{Q}$-point P_i on E_i and an integer $n_i \in \mathbb{N}$ such that $\sigma_i(n_iP_i) = P$. We assume:*

- *the existence of two real numbers M and $\epsilon \geq 0$ such that*

$$\widehat{h_\infty}(P) \leq \epsilon\widehat{h}(P) + M; \tag{9}$$

- *for any prime factor l of the denominator B_P of P, the existence of an index $i_l \in I$ such that l divides the denominator $B_{P_{i_l}}$ of P_{i_l}.*

Then we have

$$(1-\epsilon)\widehat{h}(P) \quad \leq \quad M + 2h(E) + \log\left(lcm\left\{n_i\deg(\sigma_i) : i\in I\right\}\right) + \Theta_2 + \sum_{i\in I}\widehat{h}(P_i),$$

where

$$\Theta_2 := \begin{cases} 3\widehat{h}(P_{i_2}) & \text{if } v_2(B_P) > 0 \text{ and } v_2(B_{P_{i_2}}) = 1 \text{ and } v_2(n_i\deg(\sigma_{i_2})) > 0, \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, if $E_i = E$ for all $i \in I$, then we have

$$(1-\epsilon)\widehat{h}(P) \quad \leq \quad M + h(E) + \log\left(lcm\left\{n_i\deg(\sigma_i) : i\in I\right\}\right) + \Theta_2 + \sum_{i\in I}\widehat{h}(P_i).$$

Proof. The decomposition of the canonical height into local canonical heights gives

$$\widehat{h}(P) = \widehat{h_\infty}(P) + \sum_{v(B_P)>0 \text{ or } v(\Delta_E)>0} \widehat{h_v}(P).$$

This equation, with inequalities (9), implies that

$$(1-\epsilon)\widehat{h}(P) \leq M + \sum_{v(B_P)>0 \text{ or } v(\Delta_E)>0} \widehat{h_v}(P). \tag{10}$$

Using [17, Chapter III, Theorem 4.5], inequality (10) becomes

$$(1-\epsilon)\widehat{h}(P) \leq M + h(E) + \sum_{v(B_P)>0} \widehat{h_v}(P). \tag{11}$$

Let v be a finite place such that $v(B_P) > 0$. The point P has good reduction at v. It follows that

$$\widehat{h_v}(P) = h_v(P) + \frac{v(\Delta_E)}{12}. \tag{12}$$

By definition of i_v, the point $B_{P_{i_v}}$ and the point at infinity on E_{i_v} have the same reduction at v. In particular, the points P_{i_v} and $2P_{i_v}$ have good reduction at v and it follows that

$$\widehat{h_v}(P_{i_v}) = h_v(P_{i_v}) + \frac{v(\Delta_{E_{i_v}})}{12}, \tag{13}$$

$$\widehat{h_v}(2P_{i_v}) = h_v(2P_{i_v}) + \frac{v(\Delta_{E_{i_v}})}{12}. \tag{14}$$

We deduce from Lemma 4.2.6 that

$$\widehat{h_v}(P) \leq \widehat{h_v}(P_{i_v}) + h_v(n_{i_v}\deg(\sigma_{i_v})) + \frac{1}{12}\left(v(\Delta_E) - v\left(\Delta_{E_{i_v}}\right)\right) \tag{15}$$

if $v(2) = 0$ or $v_2(B_{P_{i_2}}) > 1$ or $v(n_{i_2}\deg(\sigma_{i_v})) = 0$, and

$$\widehat{h_2}(P) \leq \widehat{h_2}(2P_{i_2}) + h_v(n_{i_2}\deg(\sigma_{i_2})) + \frac{1}{12}\left(v\left(\Delta_E\right) - v\left(\Delta_{E_{i_2}}\right)\right) \tag{16}$$

if $v_2(B_P) > 0$ and $v_2(B_{P_{i_2}}) = 1$ and $v_2(n_{i_v}\deg(\sigma_{i_2})) > 0$. Applying inequality (15) and inequality (16) we deduce from inequality (11) that

$$\begin{aligned}(1-\epsilon)\widehat{h}(P) \quad \leq \quad & M + h(E) + \theta_2 + \sum_{v(B_P)>0, v(2)=0} \widehat{h_v}(P_{i_v}) \\ & + \sum_{v(B_P)>0}\left(h_v(n_{i_v}\deg(\sigma_{i_v})) + \frac{1}{12}\left(v\left(\Delta_E\right) - v\left(\Delta_{E_{i_v}}\right)\right)\right),\end{aligned}$$

where

$$\theta_2 := \begin{cases} \widehat{h_2}(2P_{i_2}) & \text{if } v_2(B_P) > 0 \text{ and } v_2(B_{P_{i_2}}) = 1 \text{ and } v_2(n_i\deg(\sigma_{i_2})) > 0, \\ \widehat{h_2}(P_{i_2}) & \text{if } v_2(B_P) > 0 \text{ but either } v_2(B_{P_{i_2}}) > 1 \text{ or } v_2(n_i\deg(\sigma_{i_2})) = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 5.2 follows from this inequality and the decomposition of the canonical heights $\widehat{h}(P_i)$ and $\widehat{h}(2P_{i_2})$ into local canonical heights, the inequality

$$\sum_{v(B_P)>0} \frac{1}{12}\left(v\left(\Delta_E\right) - v\left(\Delta_{E_{i_v}}\right)\right) \leq h(E)$$

and the inequality

$$\theta_2 + \sum_{v(B_P)>0, i_v = i_2} \widehat{h_v}(P_{i_v}) \leq \Theta_2 + \widehat{h}(P_{i_2}),$$

which holds since Lemma 4.2.6 implies that $\widehat{h_v}(P_{i_v}) \leq \widehat{h_v}(2P_{i_v})$ for any finite place v such that $v(B_P) = v(B_{\sigma_{i_v}(P_{i_v})}) > 0$. □

If n is the index of a prime power term in a magnified elliptic divisibility sequence $\left(B_{n\sigma(P')}\right)_{n\in\mathbb{N}}$, then either every prime factor of $B_{n\sigma(P')}$ divides $B_{nP'}$ or every prime factor of $B_{nP'}$ divides $B_{P'}$. In particular, Theorem 5.3 below can be used to deduce upper bounds on such indices n from strong variants of Siegel's theorem (inequalities (17)).

Theorem 5.3. *We use Notation* 3.0.1. *Let M', M and $\epsilon \geq 0$ be three real numbers such that $d(1-\epsilon) > 1$. Let J be the set of indices $n \in \mathbb{N}$ such that*

$$\begin{aligned}\widehat{h_\infty}(nP') &\leq \epsilon\widehat{h}(nP') + M', \\ \widehat{h_\infty}(nP) &\leq \epsilon\widehat{h}(nP) + M.\end{aligned} \tag{17}$$

Then $B_{nP'}$ has a prime factor coprime to $B_{P'}$ for every integer $n \in J$ such that $n \geq 2$ and

$$n > \frac{1}{(1-\epsilon)\widehat{h}(P')} + \sqrt{\frac{M' + h(E') + 4\widehat{h}(P')}{(1-\epsilon)\widehat{h}(P')}}.$$

This prime factor can be chosen coprime to $B_{\sigma(P')}$ if n is coprime to $\deg(\sigma)$ or if

$$n > \frac{1}{(1-\epsilon)\widehat{h}(P')} + \sqrt{\frac{M' + 2h(E') + (100+d)\widehat{h}(P')}{(1-\epsilon)\widehat{h}(P')}}.$$

Moreover, $B_{n\sigma(P')}$ has a prime factor coprime to $B_{\sigma(P')}B_{nP'}$ for any $n \in J$ such that $n \geq 2$ and

$$n > \frac{1}{(d-d\epsilon-1)\widehat{h}(P')} + \sqrt{\frac{M + 2h(E) + (100+d)\widehat{h}(P') + \log(d)}{(d-d\epsilon-1)\widehat{h}(P')}}.$$

Proof. Let $n \in J$ be an integer such that every prime factor of $B_{nP'}$ divides $B_{P'}$. Applying Proposition 5.2 with $I = \{1\}$ and $[n_1] \circ \sigma_1 = [n]$, the multiplication by n map on E', we get

$$(1-\epsilon)n^2\widehat{h}(P') \leq M' + h(E') + 4\widehat{h}(P') + \log(n). \tag{18}$$

If $n \geq 2\log(2)$, applying Lemma 5.1 with $A = 1$, inequality (18) becomes

$$n \leq \frac{1}{(1-\epsilon)\widehat{h}(P')} + \sqrt{\frac{M' + h(E') + 4\widehat{h}(P')}{(1-\epsilon)\widehat{h}(P')}}.$$

Let $n \in J$ be an integer such that every prime factor of $B_{nP'}$ divides $B_{\sigma(P')}$. We know from Lemma 4.2.5 that $B_{\sigma(P')}$ divides $B_{\deg(\sigma)P'}$ and that any common prime factor of $B_{nP'}$ and $B_{\deg(\sigma)P'}$ divides $B_{\gcd(n,\deg(\sigma))P'}$. In particular, if n is coprime to $\deg(\sigma)$, then every prime factor of $B_{nP'}$ divides $B_{P'}$. In that case we still have

$$n \leq \frac{1}{(1-\epsilon)\widehat{h}(P')} + \sqrt{\frac{M' + h(E') + 4\widehat{h}(P')}{(1-\epsilon)\widehat{h}(P')}}.$$

In the general case, the finite group $\ker(\sigma) \cap E'[n]$ is invariant under the action of the absolute galois group of $\mathbb{Q}$ and contained in $E'[\gcd(n, \deg(\sigma))]$. In particular, the multiplication by $\gcd(n, \deg(\sigma))$ map on E' can be written as the composition $[\gcd(n, \deg(\sigma))] = \tau_{n,1} \circ \tau_{n,2}$ of two isogenies $\tau_{n,1}$ and $\tau_{n,2}$ defined over $\mathbb{Q}$ such that $\ker(\tau_{n,2}) = \ker(\sigma) \cap E'[n]$. A prime l divides $B_{nP'}$ (respectively $B_{\sigma(P')}$) if and only if the reduction of P' modulo l belongs to the reduction modulo l of $E'[n]$ (respectively $\ker(\sigma)$). If l is a common prime factor of $B_{nP'}$ and $B_{\sigma(P')}$, then the reduction of P' modulo l belongs to the reduction modulo l of $\ker(\tau_{n,2}) = \ker(\sigma) \cap E'[n]$. This means that l divides $B_{\tau_{n,2}(P')}$ whenever l is a common prime factor of $B_{nP'}$ and $B_{\sigma(P')}$. Applying Proposition 5.2 with

- $I = \{1\}$ and $[n_1] \circ \sigma_1 = \left[\frac{n}{\gcd(n,\deg(\sigma))}\right] \circ \tau_{n,1}$ when 2 does not divide $B_{nP'}$,
- $I = \{1;2\}$ and $[n_1] \circ \sigma_1 = \left[\frac{n}{\gcd(n,\deg(\sigma))}\right] \circ \tau_{n,1}$ and $[n_2] \circ \sigma_2 = \left[\frac{n}{r_{2,P'}}\right]$ and $i_2 = 2$ when 2 divides $B_{nP'}$, i.e., when $r_{2,P'}$ divides n,

we get

$$\begin{aligned}(1-\epsilon)n^2\widehat{h}(P') &\leq M' + 2h(E') + \left(4r_{2,P'}^2 + \deg(\tau_{n,1})\right)\widehat{h}(P') + \log(n)\\ &\leq M' + 2h(E') + (100+d)\,\widehat{h}(P') + \log(n).\end{aligned}$$

If $n \geq 2\log(2)$ we deduce from Lemma 5.1, applied with $A = 1$, that

$$n \leq \frac{1}{(1-\epsilon)\widehat{h}(P')} + \sqrt{\frac{M' + 2h(E') + (100+d)\widehat{h}(P')}{(1-\epsilon)\widehat{h}(P')}}.$$

Let $n \in J$ be an integer such that every prime factor of $B_{n\sigma(P')}$ divides either $B_{nP'}$ or $B_{\sigma(P')}$. If 2 divides $B_{nP'}$, Lemma 4.2.5 implies that the rank of apparition $r_{2,P'}$ divides n. Since $\ker(\tau_{r_{2,P'},1}) \subset \ker(\sigma)$, there exists an isogeny $\tau_{r_{2,P'},3}$ such that $\sigma = \tau_{r_{2,P'},3} \circ \tau_{r_{2,P'},1}$. If 2 divides $B_{\sigma(P')}$, then, as above, we have that 2 divides $B_{\tau_{r_{2,P'},1}P'}$. Since $\deg(\tau_{r_{2,P'},1}) \leq r_{2,P'}^2$, applying Proposition 5.2 with

- $I = \{1;2\}$ and $[n_1] \circ \sigma_1 = [n]$ the multiplication by n map on E and $\sigma_2 = \sigma$ when 2 divides neither $B_{nP'}$ nor $B_{\sigma(P')}$,
- $I = \{1;2;3\}$ and $[n_1] \circ \sigma_1 = [n]$ and $\sigma_2 = \sigma$ and $[n_3] \circ \sigma_3 = \left[\frac{n}{r_{2,P'}}\right] \circ \sigma$ and $i_2 = 3$ when 2 divides $B_{nP'}$,
- $I = \{1;2;3\}$ and $[n_1] \circ \sigma_1 = [n]$ the multiplication by n map on E and $\sigma_2 = \sigma$ and $[n_3] \circ \sigma_3 = [n] \circ \tau_{r_{2,P'},3}$ and $i_2 = 3$ when 2 divides $B_{\sigma(P')}$,

we get

$$(1-\epsilon)dn^2\widehat{h}(P') \leq M + 2h(E) + (4r_{2,P'}^2 + n^2 + d)\widehat{h}(P') + \log(nd).$$

This inequality and the inequality $r_{2,P'} \leq 5$ given by Lemma 4.2.5 imply that

$$(d - d\epsilon - 1)n^2\widehat{h}(P') \leq M + 2h(E) + (100+d)\widehat{h}(P') + \log(n) + \log(d).$$

If $n \geq 2\log(2)$ we deduce from Lemma 5.1, applied with $A = 1$, that

$$n \leq \frac{1}{(d - d\epsilon - 1)\widehat{h}(P')} + \sqrt{\frac{M + 2h(E) + (100+d)\widehat{h}(P') + \log(d)}{(d - d\epsilon - 1)\widehat{h}(P')}}. \qquad \square$$

We conclude this section by discussing a variation on Theorem 5.3: the study of terms in a magnified elliptic divisibility sequences which have only one primitive divisor. We refer the reader to [16] for effective (but non-explicit) results on primitive divisors in elliptic divisibility sequences. While we will not use Theorem 5.5 in this article, we hope this discussion enlightens the limits of the method used to prove Theorem 5.3.

Definition 5.4. Let $(u_n)_{n\in\mathbb{N}}$ be a sequence of integers. A prime number l is called the *primitive divisor* of u_n if the two following conditions are satisfied:

- l divides u_n and
- l is coprime to u_m for any $m < n$.

Theorem 5.5. *We use Notation* 3.0.1. *We denote by ζ the usual Riemann zeta-function. Let M', M and $1 > \epsilon \geq 0$ be three real numbers such that $d(2-\zeta(2)-\epsilon) > 1$. Let J be the set of indices $n \in \mathbb{N}$ such that*

$$\begin{aligned} \widehat{h_\infty}(nP') &\leq \epsilon\widehat{h}(nP') + M', \\ \widehat{h_\infty}(nP) &\leq \epsilon\widehat{h}(nP) + M. \end{aligned} \tag{19}$$

Then $B_{nP'}$ has a primitive divisor for every integer $n \in J$ such that

$$n > \frac{1}{(2-\zeta(2)-\epsilon)\,\widehat{h}(P')} + \sqrt{\frac{M' + h(E') + 100\widehat{h}(P')}{(2-\zeta(2)-\epsilon)\,\widehat{h}(P')}}.$$

Moreover, $B_{n\sigma(P')}$ has a primitive divisor coprime to $B_{nP'}$ for any $n \in J$ such that

$$n > \frac{1}{(2d - d\zeta(2) - d\epsilon - 1)\,\widehat{h}(P')} + \sqrt{\frac{M + 2h(E) + 100\widehat{h}(P')}{(2d - d\zeta(2) - d\epsilon - 1)\,\widehat{h}(P')}}.$$

Proof. Let $n \in J$ be an integer such that $B_{nP'}$ does not have a primitive divisor. If l is a common prime factor of $B_{nP'}$ and $B_{mP'}$ for some integer $0 < m < n$, then we know from Lemma 4.2.5 that l divides $B_{\gcd(m,n)P'}$. In particular, for every prime factor l of $B_{nP'}$ there is a prime factor q_l of n such that l divides $B_{\frac{n}{q_l}P'}$. Applying Proposition 5.2 with

- I' the set of prime factors of n,
- $I = I'$ when 2 does not divide $B_{nP'}$,
- $I = \{\star\} \cup I'$ and $i_2 = \star$ and $[n_\star] = \left[\frac{n}{r_{2,P'}}\right]$ the multiplication by $\frac{n}{r_{2,P'}}$ map on E', when $2 \mid B_{nP'}$, i.e., when $r_{2,P'} \mid n$,
- $[n_q] = [q]$ the multiplication by q map on E' when $q \in I'$,

we get

$$\begin{aligned}(1-\epsilon)n^2\widehat{h}(P') &\le M' + h(E') + \log(n) + \left(4r_{2,P'}^2 + \left(\sum_{q \text{ prime},\ q \mid n} \frac{n^2}{q^2}\right)\right)\widehat{h}(P') \\ &\le M' + h(E') + \log(n) + \left(100 + n^2\left(\zeta(2) - 1\right)\right)\widehat{h}(P'),\end{aligned}$$

i.e.,

$$(2 - \zeta(2) - \epsilon)\, n^2\widehat{h}(P') \le M' + h(E') + 100\widehat{h}(P') + \log(n) + \log(d).$$

If $n \ge 2\log(2)$, applying Lemma 5.1 with $A = 1$, this inequality becomes

$$n \le \frac{1}{(2 - \zeta(2) - \epsilon)\,\widehat{h}(P')} + \sqrt{\frac{M' + h(E') + 100\widehat{h}(P')}{(2 - \zeta(2) - \epsilon)\,\widehat{h}(P')}}.$$

Let $n \in J$ be an integer such that every primitive divisor of $B_{n\sigma(P')}$ divides $B_{nP'}$. As in the previous case, Lemma 4.2.5 and the definition of a primitive divisor imply that for every prime factor l of $B_{n\sigma(P')}$ we have

- either l divides $B_{nP'}$,
- or l is not a primitive divisor of $B_{n\sigma(P')}$, in which case Lemma 4.2.5 implies as above the existence of a prime factor q_l of n such that l divides $B_{\frac{n}{q_l}\sigma(P')}$.

Applying Proposition 5.2 with

- I' the set of prime factors of n,
- $I = \{\diamond\} \cup I'$ when 2 does not divide $B_{nP'}$,
- $I = \{\star, \diamond\} \cup I'$ and $i_2 = \star$ and $[n_\star] \circ \sigma_\star = \left[\frac{n}{r_{2,P'}}\right] \circ \sigma$ the composition of the multiplication by $\frac{n}{r_{2,P'}}$ map on E and σ, when $2 \mid B_{nP'}$, i.e., when $r_{2,P'} \mid n$,
- $[n_q] = [q]$ the multiplication by q map on E when $q \in I'$,
- $\sigma_\diamond = \sigma$

we get

$$(1-\epsilon)n^2d\widehat{h}(P') \leq M + 2h(E) + \log(nd) + \left(4r_{2,P'}^2 + n^2 + \sum_{q \text{ prime},\ q|n} \frac{n^2 d}{q^2}\right)\widehat{h}(P')$$
$$\leq M + 2h(E) + \left(100 + n^2\left(1 + d\zeta(2) - d\right)\right)\widehat{h}(P') + \log(nd),$$

i.e.,

$$\left(2d - d\zeta(2) - d\epsilon - 1\right)n^2\widehat{h}(P') \leq M + 2h(E) + 100\widehat{h}(P') + \log(n) + \log(d).$$

If $n \geq 2\log(2)$, applying Lemma 5.1 with $A = 1$, this inequality becomes

$$n \leq \frac{1}{\left(2d - d\zeta(2) - d\epsilon - 1\right)\widehat{h}(P')} + \sqrt{\frac{M + 2h(E) + 100\widehat{h}(P')}{\left(2d - d\zeta(2) - d\epsilon - 1\right)\widehat{h}(P')}}. \qquad \square$$

Remark 5.6. In Theorem 5.5, we show that $B_{nP'}$ has a primitive divisor l_n. This prime number l_n is a divisor of $B_{n\sigma(P')}$. However, we do not claim that l_n is a primitive divisor of the n-th term in the sequence $\left(B_{n\sigma(P')}\right)_{n\in\mathbb{N}}$.

Remark 5.7. Theorem 5.5 can be proven only because the series $\displaystyle\sum_{q \text{ prime}} \frac{1}{q^2}$ converges and has limit less than $1 - \epsilon - \frac{1}{d}$. The nonconvergence of some similar series is an obstruction to some naive generalizations of the proof of Theorem 5.5

Using Theorem 5.3, many bounds on integer points of an elliptic curve can be generalized to the case of prime power terms in magnified elliptic divisibility sequences. In the next section we give an improvement of the main result of [10]: the existence of a uniform bound on the index of a prime power term in a magnified elliptic divisibility sequence, assuming the Lang conjecture and the Hall–Lang conjecture.

6. The proof of Corollary 1.2.8

Corollary 1.2.8 is a consequence of Theorem 5.3 applied to a uniform version of inequalities (17) which will be deduced in this section from the Hall–Lang conjecture 1.2.7. This uniform version of inequalities (17) was already used in [16] to study primitive divisors in elliptic divisibility sequences. Let A, B, A', B' be four integers such that E and E' are given by the short minimal equations

$$E : y^2 = x^3 + Ax + B,$$
$$E' : y^2 = x^3 + A'x + B'.$$

Let $n \geq 3$ be an integer. Using Notation 1.1.1, the point $(A_{nP'}, C_{nP'})$ on the elliptic curve given by the equation $y^2 = x^3 + A'B_{nP'}^4 + B'B_{nP'}^6$ is an integer point. Thus the Hall–Lang Conjecture 1.2.7 gives

$$\frac{1}{2}\log|A_{nP'}| \leq 3\gamma\log|B_{nP'}| + \frac{\gamma}{2}\log\max\{|A'|, |B'|\} + \frac{1}{2}\log(K). \tag{20}$$

If the Hall–Lang Conjecture 1.2.7 is true for every quadruple of integers $(2T^4, T^6, T^2, 2T^3)$, then $\gamma \geq \frac{1}{2}$. Since $h(nP') = \frac{1}{2}\log\max\left\{|A_{nP'}|, B_{nP'}^2\right\}$ and $\log|B_{nP'}| = h(nP') - h_\infty(nP')$, it follows from inequality (20) that

$$h(nP') \leq 3\gamma(h(nP') - h_\infty(nP')) + 6\gamma h(E') + \frac{1}{2}\log(K). \tag{21}$$

From [26, Theorem 1.1] and [26, Theorem 5.5] we know that

$$h(Q) \le \widehat{h}(Q) + \tfrac{h(j(E'))}{8} + \tfrac{h(\Delta_{E'})}{12} + 0.973,$$
$$\widehat{h_\infty}(Q) \le h_\infty(Q) + \tfrac{h(j(E'))}{12} + 1.07.$$

Inequality (21) becomes

$$\widehat{h_\infty}(nP') \le \left(1 - \frac{1}{3\gamma}\right)\widehat{h}(nP') + 6h(E') + \frac{\log(K)}{6\gamma} + 2.043.$$

In the same way we prove that

$$\widehat{h_\infty}(nP) \le \left(1 - \frac{1}{3\gamma}\right)\widehat{h}(nP) + 6h(E) + \frac{\log(K)}{6\gamma} + 2.043.$$

Applying Theorem 5.3 to those inequalities, we get

$$\text{either} \quad n \le \tfrac{3\gamma}{\widehat{h}(P')} + \sqrt{21\gamma\tfrac{h(E')}{\widehat{h}(P')} + 12\gamma + \tfrac{\log(K)+12.258\gamma}{2\widehat{h}(P')}}$$
$$\text{or} \quad n \le \frac{3\gamma}{(\deg(\sigma)-3\gamma)\widehat{h}(P')} + \frac{\sqrt{24\gamma\frac{\gamma h(E)}{\widehat{h}(\sigma(P'))}+3\gamma+\frac{300\gamma}{\deg(\sigma)}+\frac{\log(K)+12.258\gamma+6\gamma\log(\deg(\sigma))}{2\deg(\sigma)\widehat{h}(P')}}}{\sqrt{1-\frac{3\gamma}{\deg(\sigma)}}}$$

whenever $B_{n\sigma(P')}$ is a prime power. The hypothesis $\deg(\sigma) \ge 4\gamma$ implies that $\sqrt{1-\frac{3\gamma}{\deg(\sigma)}} \ge \frac{1}{2}$. We conclude noting that Lang's Conjecture 1.2.6 gives upper bounds on $\frac{h(E')}{\widehat{h}(P')}$ and $\frac{h(E)}{\widehat{h}(\sigma(P'))}$ and $\frac{1}{\widehat{h}(P')}$ that do not depend on (E, E', P', σ).

7. Elliptic divisibility sequences associated to points in the bounded connected component of an elliptic curve

In this section we improve Corollary 1.2.8 for two examples of magnified elliptic divisibility sequences:

- first we study the case when P is in the bounded real connected component of E;
- then we consider the case when P is doubly magnified, i.e., when P is the image of a magnified point under an isogeny defined over $\mathbb{Q}$.

In those two particular cases we prove that Corollary 1.2.8 holds even if the Hall–Lang conjecture is not known. The results obtained in this section will be used in the proof of Theorem 1.2.2.

Notation 7.0.1. Let E be an elliptic curve defined over $\mathbb{Q}$ by a minimal Weierstrass equation. This minimal equation might not be a short Weierstrass equation. In fact, E might not have a short Weierstrass equation that is minimal at 2 and minimal at 3. However, the elliptic curve E is isomorphic to an elliptic curve $\mathcal{E}$ given by a nonminimal short Weierstrass equation,

$$\mathcal{E} : \widetilde{y}^2 = \widetilde{x}^3 + a\widetilde{x} + b, \tag{22}$$

where a and b are integers such that the discriminant of $\Delta_{\mathcal{E}}$ of $\mathcal{E}$ is given by $\Delta_{\mathcal{E}} = 6^{12}\Delta_E$. Equation (22) is not minimal so $\Delta_{\mathcal{E}}$ is not the minimal discriminant of $\mathcal{E}$. Since $j(\mathcal{E}) = j(E)$ and $\Delta_{\mathcal{E}} = 2^{12}3^{12}\Delta_E$ we have

$$a^3 = -\tfrac{j(\mathcal{E})\Delta_{\mathcal{E}}}{2^{12}3^3} = -3^9 j(E)\Delta_E$$

and

$$b^2 = \left|\tfrac{\Delta_{\mathcal{E}}}{2^4 3^3} - \tfrac{4a^3}{3^3}\right| \le \left|\tfrac{\Delta_{\mathcal{E}}}{2^4 3^3}\right| + \left|\tfrac{4a^3}{3^3}\right| \le 2^8 3^9 \left|\Delta_E\right| + 2^2 3^6 \left|j(E)\Delta_E\right|.$$

The coefficients a and b being integers, it follows that

$$\begin{aligned} h\left(1,-\tfrac{a}{4},-\tfrac{b}{16}\right) &\leq \max\left\{\log|a|,\log|b|,4\log(2)\right\} \\ &\leq \tfrac{9}{2}\log(6)+\tfrac{1}{2}h\left(j\left(E\right)\right)+\tfrac{1}{2}h\left(\Delta_E\right). \end{aligned}$$

In particular, we get

$$\max\left\{1,h\left(1,-\tfrac{a}{4},-\tfrac{b}{16}\right),h(j(\mathcal{E}))\right\}\leq 12h(E)+5\log(6). \tag{23}$$

The left-hand side of inequality (23) appears in David's lower bound on linear forms in elliptic logarithms [7, Théorème 2.1], a result used in section 8.

7.1. **Two particular cases of Siegel's theorem.** Corollary 1.2.8 is a consequence of Theorem 5.3 proven using the Hall–Lang conjecture to get a uniform version of inequalities (17). For points in the bounded component of an elliptic curve, a sharp version of inequalities (17) is given by the following proposition.

Proposition 7.1.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ by a minimal Weierstrass equation. We assume that $E(\mathbb{R})$ has two connected components. Then, for every rational point Q in the bounded connected component of $E(\mathbb{R})$, the following inequality holds:*

$$\widehat{h_\infty}(Q)\leq 3h(E)+\log(6)+1.07.$$

Proof. We use Notation 7.0.1. Denote by $\alpha_1,\alpha_2,\alpha_3$ the three roots of the polynomial $\widetilde{x}^3+a\widetilde{x}+b$ whose discriminant is $-2^{-4}3^{-3}\Delta_{\mathcal{E}}$. From Cardano's formula we know the existence of $u_i,v_i\in\mathbb{C}$ such that $\alpha_i=u_i+v_i$ and

$$\left(b+2u_i^3\right)^2=\left(b+2v_i^3\right)^2=-2^{-4}3^{-3}\Delta_{\mathcal{E}}=-2^8 3^9\Delta_E. \tag{24}$$

Equations (24) and the bounds on b^2 recalled in Notation 7.0.1 show that

$$\begin{aligned} 2|u_i|^3 &\leq |-b|+\left|b+2u_i^3\right| \\ &\leq \sqrt{2^8 3^9\left|\Delta_E\right|+2^2 3^6\left|j(E)\Delta_E\right|}+\sqrt{2^8 3^9\left|\Delta_E\right|} \\ &\leq 54\left(\sqrt{1+2^6 3^3}+\sqrt{2^6 3^3}\right)e^{12h(E)} \\ &\leq 2e^{12h(E)+3\log(14)}. \end{aligned}$$

In the same way, we prove that $|v_i|\leq e^{4h(E)+\log(14)}$. This leads to an upper bound $|\alpha_i|\leq 2e^{4h(E)+\log(14)}$. Since $|x(Q)|\leq \max_{i=1}^{3}(|\alpha_i|)$, for every point Q in the bounded real connected component of $\mathcal{E}$, we get

$$h_\infty(Q)\leq 2h(E)+\log(6).$$

We conclude by applying [26, Theorem 5.5], which asserts that

$$\widehat{h_\infty}(Q)\leq h_\infty(Q)+\frac{1}{12}h(j(\mathcal{E}))+1.07,$$

for every point $Q\in\mathcal{E}(\mathbb{Q})$. Note that while the archimedean height h_∞ might not be the same for E and for $\mathcal{E}$, the canonical archimedean height $\widehat{h_\infty}$ does not depend on the choice of model for the elliptic curve E. □

Proposition 7.1.2. *We use Notation* 3.0.1. *In particular, $\sigma:E'\longrightarrow E$ is an isogeny of degree at least* 2. *Let E'' and E''' be elliptic curves defined over $\mathbb{Q}$ by a standardized minimal equation, and let $\sigma_2:E''\longrightarrow E'$ and $\sigma_3:E'''\longrightarrow E''$ be isogenies defined over $\mathbb{Q}$, which we allow to be the identity map. Let P' be a $\mathbb{Q}$-point on E'''.*

If every prime factor of $B_{\sigma\circ\sigma_2\circ\sigma_3(P')}$ divides $B_{\sigma_2\circ\sigma_3(P')}$, then

$$\widehat{h_\infty}(\sigma_3(P')) \leq \frac{8r_{2,P'}^2\widehat{h}(P')}{\deg(\sigma\circ\sigma_2)} + 7h(E'') + \frac{5h(E''')}{2} + 9 + \log(\deg(\sigma\circ\sigma_2\circ\sigma_3)).$$

Proof. We assume that every prime factor of $B_{\sigma\circ\sigma_2\circ\sigma_3(P')}$ divides $B_{\sigma_2\circ\sigma_3(P')}$. Let $T_0 \in \ker(\sigma\circ\sigma_2)\setminus\ker(\sigma_2)$ be such that

$$|x(\sigma_3(P')) - x(T_0)| \leq |x(\sigma_3(P')) - x(T)|$$

for every $T \in \ker(\sigma\circ\sigma_2)\setminus\ker(\sigma_2)$. Since the leading coefficient $d_{\sigma\circ\sigma_2}$ of the division polynomial $\psi_{\sigma\circ\sigma_2}$ associated to $\sigma\circ\sigma_2$ is an integer divisible by the leading coefficient d_{σ_2} of the division polynomial ψ_{σ_2} associated to σ_2, we have

$$\begin{aligned}|x(\sigma_3(P')) - x(T_0)|^{\deg(\sigma\circ\sigma_2)-\deg(\sigma_2)} &\leq \frac{d_{\sigma\circ\sigma_2}^2}{d_{\sigma_2}^2}\prod_{T\in\ker(\sigma\circ\sigma_2)\setminus\ker(\sigma_2)}|x(\sigma_3(P')) - x(T)| \\ &= \left|\frac{\psi_{\sigma\circ\sigma_2}^2(\sigma_3(P'))}{\psi_{\sigma_2}^2(\sigma_3(P'))}\right|.\end{aligned}$$

From this inequality, and Proposition 4.2.3, we deduce that

$$\begin{aligned}|x(\sigma_3(P')) - x(T_0)|^{\deg(\sigma\circ\sigma_2)-\deg(\sigma_2)} &\leq \frac{\left|B_{\sigma\circ\sigma_2(\sigma_3(P'))}\right|^2 e^{3\deg(\sigma\circ\sigma_2)h(E'')}}{\left|\psi_{\sigma_2}(\sigma_3(P'))\right|^2\left|B_{\sigma_3(P')}\right|^{2\deg(\sigma\circ\sigma_2)}} \\ &\leq \frac{\left|B_{\sigma\circ\sigma_2\circ\sigma_3(P')}\right|^2}{\left|B_{\sigma_2\circ\sigma_3(P')}\right|^2}e^{3\deg(\sigma\circ\sigma_2)h(E'')}.\end{aligned}$$

Let $r_{2,\sigma_2\circ\sigma_3(P')}$ be the rank of apparition of 2 in the elliptic divisibility sequence associated to $\sigma_2\circ\sigma_3(P')$. If 2 divides $B_{\sigma_2\circ\sigma_3(P')}$, then $r_{2,\sigma_2\circ\sigma_3(P')} = 1$. Since every prime factor of $B_{\sigma\circ\sigma_2\circ\sigma_3(P')}$ divides $B_{\sigma_2\circ\sigma_3(P')}$, applying Lemma 4.2.6, we get

$$\begin{aligned}\log\left|\frac{B_{\sigma\circ\sigma_2\circ\sigma_3(P')}}{B_{\sigma_2\circ\sigma_3(P')}}\right| &\leq \log(\deg(\sigma)) + v_2\left(B_{2(\sigma_2\circ\sigma_3(P'))}\right) - v_2\left(B_{\sigma_2\circ\sigma_3(P')}\right) \\ &\leq \log(\deg(\sigma)) + v_2\left(B_{2\deg(\sigma_2\circ\sigma_3)P'}\right) - v_2\left(B_{\sigma_2\circ\sigma_3(P')}\right) \\ &\leq \log(\deg(\sigma)) + v_2\left(B_{2r_{2,P'}P'}\right) + v_2(\deg(\sigma_2\circ\sigma_3)) - v_2\left(B_{P'}\right).\end{aligned}$$

As a consequence we have

$$\begin{aligned}|x(\sigma_3(P')) - x(T_0)|^{\deg(\sigma)\deg(\sigma_2)/2} &\leq |x(\sigma_3(P')) - x(T_0)|^{(\deg(\sigma)-1)\deg(\sigma_2)} \\ &\leq \left|\frac{B_{2r_{2,P'}P'}}{B_{P'}}\right|^2 (\deg(\sigma\circ\sigma_2\circ\sigma_3))^2 e^{3\deg(\sigma\circ\sigma_2)h(E'')} \\ &\leq \left|\frac{B_{2r_{2,P'}P'}}{B_{P'}}\right|^2 \deg(\sigma_3)^2 e^{2\log(\deg(\sigma\circ\sigma_2))+3\deg(\sigma\circ\sigma_2)h(E'')}\end{aligned}$$

and, in particular,

$$|x(P') - x(T_0)| \leq \left|\frac{\deg(\sigma_3)B_{2r_{2,P'}P'}}{B_{P'}}\right|^{4/\deg(\sigma\circ\sigma_2)} e^{2+6h(E'')}.$$

The triangle inequality gives

$$|x(P')| \leq 2\max\left\{|x(T_0)|, \left|\frac{\deg(\sigma_3)B_{2r_{2,P'}P'}}{B_{P'}}\right|^{4/\deg(\sigma\circ\sigma_2)} e^{2+6h(E'')}\right\}. \tag{25}$$

The short Weierstrass equation for E'' introduced in Notation 7.0.1 can be obtained from the standardized minimal equation

$$y^2 + a_1 y + a_3 xy = x^3 + a_2 x^2 + a_4 x + a_6$$

of E'' using the change of variable

$$(\widetilde{x}, \widetilde{y}) = (36x + 3a_1^2 + 12a_2, 216y + 108a_1 x + 108a_3).$$

Since $a_1, a_2 \in \{-1, 0, 1\}$, from inequality (23) and [7, Lemme 10.1] we get

$$|36x(T_0)| - 15 \leq \left|36x(T_0) + 3a_1^2 + 12a_2\right| \leq 480 \deg(\sigma \circ \sigma_2)^2 e^{12h(E'')+5\log(6)}.$$

It follows from inequality (25) and [26, Theorem 5.5] that

$$\begin{aligned}
\widehat{h_\infty}(\sigma_3(P')) &\leq h_\infty(\sigma_3(P')) + h(E'') + \tfrac{1}{2}\log(2) + 1.07 \\
&\leq \frac{2\log\left|\frac{\deg(\sigma_3) B_{2r_{2,P'}P'}}{B_{P'}}\right|}{\deg(\sigma\circ\sigma_2)} + 7h(E'') + 8 + \log(\deg(\sigma \circ \sigma_2)) \\
&\leq \frac{2h(2r_{2,P'}P') + 2\log(\deg(\sigma_3))}{\deg(\sigma\circ\sigma_2)} + 7h(E'') + 8 + \log(\deg(\sigma \circ \sigma_2)).
\end{aligned}$$

(Note that [26, Theorem 5.5] is applied to a standardized equation and that $h_\infty(P')$ $= \frac{1}{2}\log\max\{1, |x(P')|\}$.) Applying [26, Theorem 1.1] we get

$$\begin{aligned}
\widehat{h_\infty}(\sigma_3(P')) \leq \frac{8r_{2,P'}^2 \widehat{h}(P') + 5h(E''') + 1.946 + 2\log(\deg(\sigma_3))}{\deg(\sigma \circ \sigma_2)} \\
+ 7h(E'') + 8 + \log(\deg(\sigma \circ \sigma_2)).
\end{aligned}$$

□

7.2. **Prime power terms of composite index.** We consider the primality conjecture, for an elliptic divisibility sequence associated to a point $\sigma(P')$ that is magnified by an isogeny σ, when the point P' is also magnified. This case will be used to study the primality conjecture for elliptic divisibility sequences associated to points belonging to the bounded real connected component of an elliptic curve.

The proof consists of an adaptation of the proof of Theorem 5.3. In this proof we need to compare the naive heights $h(E')$ and $h(E)$ of two isogenous elliptic curves E' and E. Such a comparison follows from the good behaviour of the Faltings height under isogeny.

Proposition 7.2.1. *We use Notation* 3.0.1. *Then we have*

$$h(E') \leq \alpha h(E) + h(\deg(\sigma)) + 15.8$$

with $\alpha = 5$ *if* $h(j(E)) > 48$ *and* $\alpha = 16$ *if* $h(j(E)) \leq 48$.

Proof. The proof is based on the good behaviour of the Faltings height h_{Falt} under isogeny: if $\sigma : E' \longrightarrow E$ is an isogeny between elliptic curves, then the Faltings heights $h_{Falt}(E)$ of E and $h_{Falt}(E')$ of E' satisfy the inequality:

$$|h_{Falt}(E) - h_{Falt}(E')| \leq \frac{1}{2}\log(\deg(\sigma)). \tag{26}$$

Given $\mathcal{E} \in \{E', E\}$, the proof of [20, Lemme 5.2] gives explicit bounds on the Faltings height $h_{Falt}(\mathcal{E})$ of $\mathcal{E}$ that depend linearly in the j-invariant height $h(j(\mathcal{E}))$:

$$12h_{Falt}(\mathcal{E}) \leq \log\max\{|j(\mathcal{E})\Delta_{\mathcal{E}}|, |\Delta_{\mathcal{E}}|\} + 6\log(1 + h(j(E)) + 47.15,$$

$$\log\max\{|j(\mathcal{E})\Delta_{\mathcal{E}}|, |\Delta_{\mathcal{E}}|\} \leq 94.3 + 24\max\{1, h_{Falt}(\mathcal{E})\}.$$

The elliptic curve $\mathcal{E}$ is given by a minimal Weierstrass equation. The term $\log\max\{|j(\mathcal{E})\Delta_{\mathcal{E}}|, |\Delta_{\mathcal{E}}|\}$ can be bounded linearly in $h(\mathcal{E})$ using the two inequalities:

$$\begin{aligned} 12h(\mathcal{E}) &\leq \max\{h(j(\mathcal{E})), h(\Delta_{\mathcal{E}})\} \\ &\leq \log\max\{|j(\mathcal{E})\Delta_{\mathcal{E}}|, |\Delta_{\mathcal{E}}|\} \leq 24h(\mathcal{E}). \end{aligned}$$

It follows that

$$\begin{aligned} 12h(E') &\leq 24\max\{1, h_{Falt}(E')\} + 94.3 \\ &\leq \max\{24, 24h_{Falt}(E) + 12\log(\deg(\sigma))\} + 94.3 \\ &\leq 48h(E) + 12\log(1 + h(j(E)) + 12\log(\deg(\sigma)) + 188.6. \end{aligned}$$

We conclude by observing that $\log(1 + h(j(E))) \leq \frac{h(j(E))}{12} \leq h(E)$ whenever the inequality $h(j(E)) > 48$ holds. □

Corollary 7.2.2. *Let E_0, E_1, E_2, E_3 be four elliptic curves defined over $\mathbb{Q}$ by standardized minimal equations. For each $i \in \{1, 2, 3\}$ let $\tau_i : E_{i-1} \longrightarrow E_i$ be an isogeny defined over $\mathbb{Q}$ of degree at least 2. Let $P' \in E_0(\mathbb{Q})$ be a point of infinite order such that $B_{(\tau_3\circ\tau_2\circ\tau_1)(P')}$ has at most one prime factor coprime to $B_{P'}$. Then, for each index i, we have*

$$\begin{aligned} \textit{either} \quad & \sqrt{\deg(\tau_i)} \leq \tfrac{2}{\sqrt{\widehat{h}(P')}} \log\left(\tfrac{2}{\sqrt{\widehat{h}(P')}}\right) \\ \textit{or} \quad & \sqrt{\deg(\tau_i)} \leq \tfrac{26}{\sqrt{\widehat{h}(P')}} + \sqrt{200 + \tfrac{147h(E_0)+129}{\widehat{h}(P')}}. \end{aligned}$$

Proof. We denote by d_i the degree $d_i := \deg(\tau_i)$ of τ_i. Replacing τ_i with $(\tau_{i+1})_{\tau_i}$ if needed (see Notation 4.1.6 for details), we can assume without loss of generality that $d_1 \geq d_2 \geq d_3$.

Assume, for now, that l is a prime number dividing $B_{\tau_1(P')}$ and coprime to $B_{P'}$. Following Lemma 4.2.6, the prime l divides $B_{(\tau_2\circ\tau_1)(P')}$. Thus each prime factor of $B_{(\tau_3\circ\tau_2\circ\tau_1)(P')}$ divides $B_{(\tau_2\circ\tau_1)(P')}$. Since $1 \leq r_{2,P'} \leq 5$, Proposition 7.1.2 applied with $\sigma = \tau_3$ and $\sigma_2 = \mathrm{Id}$ and $\sigma_3 = \tau_2 \circ \tau_1$ gives

$$\widehat{h_\infty}((\tau_2 \circ \tau_1)(P')) \leq 100\widehat{h}(P') + 7h(E_2) + \frac{5}{2}h(E_0) + 9 + \log(d_1d_2d_3). \tag{27}$$

Since each prime factor of $B_{(\tau_2\circ\tau_1)(P')}$ divides $B_{\tau_1(P')}$, Proposition 5.2 can now be used to give a bound on d_1 as in the proof of Theorem 5.3. This requires a careful analysis of the behaviour of the canonical local height $\widehat{h_2}(\tau_1(P'))$. The finite group $\ker(\tau_1) \cap E_0[r_{2,P'}]$ is invariant under the action of the absolute galois group of $\mathbb{Q}$. In particular, τ_1 can be written as the composition $\tau_1 = \eta_1 \circ \eta_2$ of two isogenies η_1 and η_2 defined over $\mathbb{Q}$ such that $\ker(\eta_2) = \ker(\tau_1) \cap E_0[r_{2,P'}]$. If 2 divides $B_{\tau_1(P')}$, then, the reduction of P' modulo 2 belongs to the reduction modulo 2 of $\ker(\tau_1)$. In that case, by definition of $r_{2,P'}$, the reduction of P' modulo 2 belongs to the reduction modulo 2 of $\ker(\eta_2) = \ker(\tau_1) \cap E_0[r_{2,P'}]$. This means that 2 divides $B_{\eta_2(P')}$ whenever 2 divides $B_{\tau_1(P')}$. Since $\log(d_3) \leq \log\left(\sqrt{d_1d_2}\right)$, applying Proposition 5.2 with $I = \{1, 2\}$, $i_2 = 1$, $\sigma_1 = \tau_2 \circ \eta_1$, $\sigma_2 = \tau_2$, and $\epsilon = 0$, we get:

$$d_1d_2\widehat{h}(P') \leq 9h(E_2) + \frac{5h(E_0)}{2} + 9 + 5\log\left(\sqrt{d_1d_2}\right) + (100 + 4\deg(\eta_2) + d_1)\,\widehat{h}(P').$$

Following Proposition 7.2.1, since $\deg(\eta_2) \leq r_{2,P'}^2 \leq 25$, this inequality implies that

$$d_1(d_2-1)\widehat{h}(P') \leq 200\widehat{h}(P') + 147h(E_0) + 152 + 23\log\left(\sqrt{d_1 d_2}\right).$$

Since $\log\left(\sqrt{\frac{d_2}{d_2-1}}\right) \leq \frac{1}{2}$, applying Lemma 5.1 with $n = \sqrt{d_1(d_2-1)}$ and $A = \frac{1}{\sqrt{\widehat{h}(P')}}$ we get

$$\begin{aligned} \text{either} \quad & \sqrt{d_1(d_2-1)} \leq \tfrac{2\log(2)}{\sqrt{\widehat{h}(P')}} + \tfrac{2}{\sqrt{\widehat{h}(P')}}\log\left(\tfrac{1}{\sqrt{\widehat{h}(P')}}\right) \\ \text{or} \quad & \sqrt{d_1(d_2-1)} \leq \tfrac{23}{\sqrt{\widehat{h}(P')}} + \sqrt{200 + \tfrac{147h(E_0)+129}{\widehat{h}(P')}}. \end{aligned}$$

Assume now that l is a prime number dividing $B_{(\tau_3\circ\tau_2\circ\tau_1)(P')}$ and coprime to $B_{\tau_1(P')}$. If l does not divide $B_{\tau_2\circ\tau_1(P')}$, then every prime factor of $B_{(\tau_2\circ\tau_1)(P')}$ divides $B_{\tau_1(P')}$. In that case, Proposition 7.1.2 applied with $\sigma = \tau_2$ and $\sigma_2 = \mathrm{Id}$ and $\sigma_3 = \tau_1$ gives

$$\widehat{h_\infty}(\tau_1(P')) \leq 100\widehat{h}(P') + 7h(E_1) + \frac{5}{2}h(E_0) + 9 + \log(d_1 d_2 d_3).$$

If l divides $B_{\tau_2\circ\tau_1(P')}$, then every prime factor of $B_{\tau_3\circ\tau_2\circ\tau_1(P')}$ divides $B_{\tau_2\circ\tau_1(P')}$. In that case, Proposition 7.1.2 applied with $\sigma = \tau_3$, $\sigma_2 = \tau_2$, and $\sigma_3 = \tau_1$ gives

$$\widehat{h_\infty}(\tau_1(P')) \leq 50\widehat{h}(P') + 7h(E_1) + \frac{5}{2}h(E_0) + 9 + \log(d_1 d_2 d_3).$$

In both cases, since l is coprime to $B_{\tau_1(P')}$, each prime factor of $B_{\tau_1(P')}$ divides $B_{P'}$. In particular, since $\log(d_1 d_2 d_3) \leq 3\log(d_1)$, Proposition 5.2 and Proposition 7.2.1 give:

$$d_1\widehat{h}(P') \leq 104\widehat{h}(P') + 147h(E_0) + 152 + 26\log\left(\sqrt{d_1}\right).$$

Applying Lemma 5.1 with $n = \sqrt{d_1}$ and $A = \frac{1}{\sqrt{\widehat{h}(P')}}$, we get

$$\begin{aligned} \text{either} \quad & \sqrt{d_1} \leq \tfrac{2\log(2)}{\sqrt{\widehat{h}(P')}} + \tfrac{2}{\sqrt{\widehat{h}(P')}}\log\left(\tfrac{1}{\sqrt{\widehat{h}(P')}}\right) \\ \text{or} \quad & \sqrt{d_1} \leq \tfrac{26}{\sqrt{\widehat{h}(P')}} + \sqrt{104 + \tfrac{147h(E_0)+126}{\widehat{h}(P')}}. \end{aligned}$$

□

7.3. **The primality conjecture for magnified points in the bounded connected component of an elliptic curve over $\mathbb{R}$.**

Corollary 7.3.1. *We use Notation* 3.0.1. *We assume that $E(\mathbb{R})$ has two connected components and that* $\deg(\sigma)$ *is odd. We assume that $P = \sigma(P')$ belongs to the bounded connected component of $E(\mathbb{R})$. Then $B_{n\sigma(P')}$ has two distinct prime factors coprime to $B_{P'}$, for every integer n such that*

$$\begin{aligned} n &> \tfrac{4}{\sqrt{\widehat{h}(P')}}\log\left(\tfrac{2}{\sqrt{\widehat{h}(P')}}\right), \\ n &> \tfrac{52}{\sqrt{\widehat{h}(P')}} + 2\sqrt{200 + \tfrac{147h(E')+129}{\widehat{h}(P')}}. \end{aligned}$$

Proof. When n is even, Corollary 7.3.1 follows from Corollary 7.2.2 applied with $\tau_1 = n/2$ and $\tau_2 = 2$. We assume now that n is odd.

Since σ is an isogeny of odd degree and $E(\mathbb{R})$ has two connected components, $E'(\mathbb{R})$ also has two connected components. Moreover, since $\sigma(P')$ is on the bounded connected component of $E(\mathbb{R})$, the point P' is on the bounded connected component of $E'(\mathbb{R})$.

As n is odd, the points nP' and $nP = n\sigma(P')$ are in the bounded connected components of $E'(\mathbb{R})$ and $E(\mathbb{R})$ respectively. We use Proposition 7.1.1, Proposition 7.2.1, and Proposition 5.2 to bound n. More precisely, adapting the proof of Theorem 5.3, we show that

$$n^2\widehat{h}(P') \leq 4h(E') + 4\widehat{h}(P') + \log(n) + \log(6) + 1.07,$$

if every prime factor of $B_{nP'}$ divides $B_{P'}$, and

$$\begin{aligned} n^2(\deg(\sigma)-1)\widehat{h}(P') &\leq 5h(E)+(100+\deg(\sigma))\widehat{h}(P')+\log(6)+1.07+\log(n\deg(\sigma)) \\ &\leq 80h(E')+(100+\deg(\sigma))\widehat{h}(P')+82+6\log(\deg(\sigma))+\log(n), \end{aligned}$$

if every prime factor of $B_{n\sigma(P')}$ divides $B_{nP'}$. We conclude the proof by applying Lemma 5.1 with $A = \frac{1}{\sqrt{\widehat{h}(P')}}$. □

8. Elliptic divisibility sequences and linear forms in elliptic logarithms

Since no uniform upper bound on the canonical height of integer points on an elliptic curve is known, we cannot hope to get an explicit uniform bound on the index of a prime power term in an elliptic divisibility sequence. However, an explicit nonuniform bound can be computed using the work of David on lower bounds for linear forms in elliptic logarithms.

Notation 8.0.2. We use Notation 7.0.1. We consider the map ϕ defined on the unbounded real connected component $\mathcal{E}(\mathbb{R})_0$ of $\mathcal{E}$ by the formula

$$\phi(P) = \phi_{\mathcal{E}}(P) := \mathrm{Sign}(\widetilde{y}(P)) \int_{\widetilde{x}(P)}^{+\infty} \frac{dt}{\sqrt{t^3+at+b}}.$$

The map ϕ is linked to the archimedean height by the following inequality (see [30, section 3, inequality 2]): for every point $P \in \mathcal{E}(\mathbb{R})_0$, we have

$$-\log|\phi(P)| - \frac{1}{2}\log(2) \leq h_\infty(P) \leq -\log|\phi(P)| + \frac{5}{2}\log(2). \tag{28}$$

Let $\wp$ be the Weierstrass $\wp$-function relative to the elliptic curve $\mathcal{E}$. Let $T_0 \in \mathcal{E}(\mathbb{R})$ be the real 2-torsion point with the highest x-coordinate. Let $P \in \mathcal{E}(\mathbb{Q})$ be a point in the unbounded connected component $\mathcal{E}(\mathbb{R})_0$ of $\mathcal{E}(\mathbb{R})$. Then $\wp\left(\frac{\phi(P)}{2\phi(T_0)}\right) = \frac{x(P)}{4}$ and, for every $n \in \mathbb{Z}$, there is an integer m such that

$$\phi(nP) = n\phi(P) + 2m\phi(T_0).$$

Moreover, since $|\phi(nP)| < |\phi(T_0)|$ and $|\phi(P)| < |\phi(T_0)|$, we have $|m| \leq |n|$.

8.1. **David's lower bounds on linear forms in elliptic logarithms.**

Lemma 8.1.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ by a minimal Weierstrass equation with integral coefficients. Let $P \in E(\mathbb{Q})$ be a point on E. For any integer $n > 0$ denote by b_n the maximum*

$$b_n := \max\left\{\log|2n|, 2\widehat{h}(P), 12eh(E) + 5e\log(6)\right\}.$$

Then, for $n > 1$, the inequality

$$\widehat{h_\infty}(nP) \leq c_1(b_n + \log(3) + 1)^6 + c_2$$

holds, with $c_1 = 5.9 \times 10^{43}$ and $c_2 = h(E) + 2.81$.

Proof. We use Notation 8.0.2. We apply [7, Théorème 2.1] to the short Weierstrass equation introduced in Notation 7.0.1 with $k = 2$, $D \leq 3$, $E = e$, $\gamma_1 = P$, $\gamma_2 = T_0$,

$$\begin{aligned}\log(V_1) = \log(V_2) &= \max\left\{2\widehat{h}(P), 12eh(E) + 5e\log(6)\right\}\\ &\geq \max\left\{2\widehat{h}(P), e\max\left\{1, h\left(1, -\frac{a}{4}, -\frac{b}{16}\right), h(j(\mathcal{E}))\right\}, 2\pi\sqrt{3}\right\}\\ &\geq \max\left\{2\widehat{h}(P), \max\left\{1, h\left(1, -\frac{a}{4}, -\frac{b}{16}\right), h(j(\mathcal{E}))\right\}, \frac{3\pi|\phi(P)|^2}{|2\phi(T_0)|^2\mathrm{Im}(\tau)}\right\}\end{aligned}$$

(where τ is a complex number such that $\mathcal{E}(\mathbb{C}) \simeq \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ and $\mathrm{Im}(\tau) \geq \frac{\sqrt{3}}{2}$), and

$$\begin{aligned}\log(B) &= \max\{\log|2n|, \log(V_1)\}\\ &\geq \max\left\{e\max\left\{1, h\left(1, -\tfrac{a}{4}, -\tfrac{b}{16}\right), h(j(\mathcal{E}))\right\}, h(n, 2m), \tfrac{\log(V_1)}{D}\right\},\end{aligned}$$

where m is an integer such that $\phi(nP) = n\phi(P) + 2m\phi(T_0)$. (Note that $|m| \leq |n|$). This application of [7, Théorème 2.1] gives

$$\begin{aligned}\log|n\phi(P) + 2m\phi(T_0)| \geq &- C\log(V_1)\log(V_2)(\log(B) + \log(3) + 1)\\ &\times(\log(\log(B)) + 12h(E) + 5\log(6) + \log(3) + 1)^3,\end{aligned}$$

where $C = 2.3 \times 10^{43}$. Note that:

- we do not use the same definition for naive height functions as in [7];
- the number $h := \max\left\{1, h\left(1, -\frac{a}{4}, -\frac{b}{16}\right), h(j(\mathcal{E}))\right\}$ is equal to the number denoted by h in [7]; inequality (23) gives an upper bound on h that is linear in $h(E)$ (see Notation 7.0.1).

Using the inequalities $\log(x) \leq x - 1$ (which holds for every real number $x > 0$) and

$$12h(E) + 5\log(6) \leq e^{-1}\log(V_1),$$

we deduce from inequality (28) that

$$h_\infty(nP) \leq (1 + e^{-1})^3 C\,(1 + \log(3) + \log(B))^6 + \frac{5}{2}\log(2).$$

We conclude by using [26, Theorem 5.5]. □

8.2. **A nonuniform bound on the index of a prime power term in an elliptic divisibility sequence.**

Proposition 8.2.1. *We use Notation* 3.0.1. *Then $B_{nP'}$ has a prime factor coprime to $B_{P'}$ for every index*

$$n > \max\left\{3.5\times 10^{29}, \frac{1.1\times 10^{27}}{\widehat{h}(P')}, 10^{23}\widehat{h}(P')^{5/2}, \frac{2\times 10^{27}h(E')^{7/2}}{\widehat{h}(P')}\right\}.$$

This prime factor can be chosen coprime to $B_{\sigma(P')}$ if n is coprime to $\deg(\sigma)$ *or*

$$n > \sqrt{d} + \max\left\{3.5\times 10^{29}, \frac{1.1\times 10^{27}}{\widehat{h}(P')}, 10^{23}\widehat{h}(P')^{5/2}, \frac{2\times 10^{27}h(E')^{7/2}}{\widehat{h}(P')}\right\}.$$

Moreover, $B_{n\sigma(P')}$ has a prime factor coprime to $B_{nP'}$ for every index

$$n > \max\left\{3.5\times 10^{29}, \frac{1.1\times 10^{27}}{\widehat{h}(P')}, 2\times 10^{23}\widehat{h}(\sigma(P'))^{5/2}, \frac{4\times 10^{27}h(E)^{7/2}}{\widehat{h}(\sigma(P'))}\right\}.$$

Proof. Let $n\in\mathbb{N}$ be such that $B_{nP'}$ has no prime factor coprime to $B_{P'}$. Then Lemma 8.1.1 (applied with $b' := \max\{2\widehat{h}(P'); 12eh(E') + 5e\log(6)\}$) asserts that either $\widehat{h_\infty}(nP') \le 5.9\times 10^{43}\times(b'+2.1)^6 + h(E') + 2.81$ or $\log|2n| > b'$. We assume for now that $\log|2n| \le b'$. Applying Theorem 5.3 we get that

$$\begin{aligned} n &\le \tfrac{1}{\widehat{h}(P')} + \sqrt{\tfrac{5.9\times 10^{43}(b'+2.1)^6 + 2h(E') + 4\widehat{h}(P') + 2.81}{\widehat{h}(P')}} \\ &\le \tfrac{1+\sqrt{5.91\times 10^{43}(b'+2.1)^7}}{\widehat{h}(P')} \\ &\le \tfrac{8.7\times 10^{21}\left(\max\left\{\widehat{h}(P')+1.05, 17h(E')+14\right\}\right)^{7/2}}{\widehat{h}(P')} \\ &\le \tfrac{8.7\times 10^{21}\left(\max\left\{2\widehat{h}(P'), 34h(E'), 28\right\}\right)^{7/2}}{\widehat{h}(P')}. \end{aligned}$$

Now we assume that $\log|2n| \ge b'$. The proof of Theorem 5.3 is still valid when M and M' are replaced with polynomials in $\log(n)$. In particular, Lemma 8.1.1 and Proposition 5.2 imply that

$$\begin{aligned} n^2\widehat{h}(P') &\le 5.9\times 10^{43}(\log|6n|+1)^6 + \log(n) + 4\widehat{h}(P') + 2h(E') + 2.81 \\ &\le 2\max\left\{5.9\times 10^{43}(\log|6n|+1)^6, \log(n) + 4\widehat{h}(P') + 2h(E') + 2.81\right\}. \end{aligned}$$

Applying Lemma 5.1

- with $A = 10^{18}$ and $\delta = 6$ when $(6n)^2\widehat{h}(P') \le 4,3\times 10^{45}(\log|6n|+1)^6$;
- with $A = 2\delta = 2$ when $n^2\widehat{h}(P') \le 2\log(n) + 8\widehat{h}(P') + 4h(E') + 5.62$,

we get that

$$\begin{aligned} \text{either}\quad n &\le \max\left\{3.5\times 10^{29}, \tfrac{7.1\times 10^{26}}{\widehat{h}(P')}\right\} \\ \text{or}\quad n &\le \max\left\{5.6, \tfrac{1}{\widehat{h}(P')} + \sqrt{8 + \tfrac{3.62}{\widehat{h}(P')} + \tfrac{4h(E')}{\widehat{h}(P')}}\right\} \\ &\le \max\left\{5.6, \left(1+\sqrt{3}\right)\max\left\{\tfrac{1}{\widehat{h}(P')}, 2\sqrt{2}, \sqrt{\tfrac{3.62}{\widehat{h}(P')}}, \sqrt{\tfrac{4h(E')}{\widehat{h}(P')}}\right\}\right\}. \end{aligned}$$

In the proof of Theorem 5.3 we have seen that if n is coprime to $\deg(\sigma)$, then any common prime divisor of $B_{nP'}$ and $B_{\sigma(P')}$ is a prime factor of $B_{P'}$. In the general case, when $B_{nP'}$ has no prime factor coprime to $B_{\sigma(P')}$, we can deduce as above from, Lemma 8.1.1 and Proposition 5.2 that

$$n \leq \sqrt{d} + \max\left\{3.5\times 10^{29}, \frac{1.1\times 10^{27}}{\widehat{h}(P')}, 10^{23}\widehat{h}(P')^{5/2}, \frac{2\times 10^{27}h(E')^{7/2}}{\widehat{h}(P')}\right\}.$$

(Note that $\sqrt{a+b} \leq \sqrt{a}+\sqrt{b}$ for all real numbers a and b.)

In the same way, when $B_{n\sigma(P')}$ has no prime factor coprime to $B_{nP'}$ and $B_{\sigma(P')}$, we can prove using the inequalities $\frac{\deg(\sigma)}{\deg(\sigma)-1} \leq 2$ and $\frac{\log(\deg(\sigma))}{\deg(\sigma)-1} \leq 1$ that

$$\begin{aligned}
\text{either}\quad n &\leq \frac{1.8\times 10^{22}\left(\max\left\{2\widehat{h}(\sigma(P')), 34h(E), 28\right\}\right)^{7/2}}{\widehat{h}(\sigma(P'))}\\
\text{or}\quad n &\leq \max\left\{3.5\times 10^{29}, \frac{7.1\times 10^{26}}{(\deg(\sigma)-1)\widehat{h}(P')}\right\}\\
\text{or}\quad n &\leq \max\left\{16.7, \frac{1}{(\deg(\sigma)-1)\widehat{h}(P')} + \sqrt{204 + \frac{3.62+2\log(\deg(\sigma))}{(\deg(\sigma)-1)\widehat{h}(P')} + \frac{12h(E)}{\widehat{h}(\sigma(P'))}}\right\}\\
&\leq \max\left\{16.7, \left(1+\sqrt{3}\right)\max\left\{\frac{2}{\widehat{h}(\sigma(P'))}, \sqrt{204}, \sqrt{\frac{5.62}{\widehat{h}(P')}}, \sqrt{\frac{12h(E)}{\widehat{h}(\sigma(P'))}}\right\}\right\}.
\end{aligned}$$

□

8.3. **An explicit version of the gap principle.** David's theorem on lower bounds for linear forms in elliptic logarithms leads to a bound $M(B)$ on the index of a prime term in a magnified elliptic divisibility sequence B that is quite large. The bound $M(B)$ can be reduced by applying the LLL algorithm (see [30,31]) or a gap principle (see [15]).

Notation 8.3.1. We use Notation 3.0.1. Following Notation 8.0.2 we denote by $\mathcal{E}$ (respectively $\mathcal{E}'$) a model of E (respectively E') given by a short Weierstrass equation with coefficients in $\mathbb{Z}$ such that $\Delta_{\mathcal{E}} = 6^{12}\Delta_E$ (respectively $\Delta_{\mathcal{E}'} = 6^{12}\Delta_{E'}$). Let P' be a $\mathbb{Q}$-point on E'. We denote by $R' \in \mathcal{E}'(\mathbb{Q})$ (respectively $R \in \mathcal{E}(\mathbb{Q})$) the point on $\mathcal{E}'$ (respectively $\mathcal{E}$) associated to P' (respectively $\sigma(P')$).

Lemma 8.3.2. *We use Notation* 8.3.1. *Let $n \in \mathbb{N}$ and $\delta \in \{0, d\}$ be such that*

$$n > \frac{1}{\widehat{h}(P')} + \sqrt{103 + \delta + \max\left\{\frac{6h(E')}{\widehat{h}(P')}, \frac{12h(E)}{\widehat{h}(\sigma(P'))}\right\} + \frac{7}{\widehat{h}(P')}}.$$

(a) *Assume that every prime factor of $B_{nP'}$ divides $B_{P'}$ and that $\delta = 0$. Then $|x(nR')| \geq 2\max\{|x(T)| : T \in \mathcal{E}'[2]\}$ and $n\phi_{\mathcal{E}'}(R') \neq \phi_{\mathcal{E}'}(nR')$.*

(b) *Assume that every prime factor of $B_{nP'}$ divides $B_{\sigma(P')}$ and that $\delta = d$. Then $|x(nR')| \geq 2\max\{|x(T)| : T \in \mathcal{E}'[2]\}$ and $n\phi_{\mathcal{E}'}(R') \neq \phi_{\mathcal{E}'}(nR')$.*

(c) *Assume that every prime factor of $B_{n\sigma(P')}$ divides either $B_{nP'}$ or $B_{\sigma(P')}$ and that $\delta = 0$. Then $|x(nR)| \geq 2\max\{|x(T)| : T \in \mathcal{E}'[2]\}$ and $n\phi_{\mathcal{E}}(R) \neq \phi_{\mathcal{E}}(nR)$.*

Proof. The sole difference between the proofs of assertion (a) and assertion (b) is the bound given by Theorem 5.3; we give the proof only in the two cases when $\delta = 0$.

When $|x(nR')| \leq 2\max\{|x(T)| : T \in \mathcal{E}'[2]\}$, the proof of Lemma 7.1.1 gives

$$\widehat{h_\infty}(nP') = \widehat{h_\infty}(nR') \leq 3h(E') + \log(6) + \frac{1}{2}\log(2) + 1.07 \leq 3h(E') + 3.21.$$

Thus Theorem 5.3 implies that, if every prime factor of $B_{nP'}$ divides $B_{P'}$ and $n > \frac{1}{\widehat{h}(P')} + \sqrt{4 + \frac{4h(E')+3.21}{\widehat{h}(P')}}$, then $|x(nR')| \geq 2\max\{|x(T)| : T \in \mathcal{E}'[2]\}$; this implies that R' is in the unbounded real connected component $\mathcal{E}'(\mathbb{R})_0$.

In the same way, since $n > \frac{1}{\widehat{h}(P')} + \sqrt{102 + \frac{10h(E)}{\widehat{h}(\sigma(P'))} + \frac{4.21}{\widehat{h}(P')}}$, we deduce from Theorem 5.3 that, if every prime factor of $B_{n\sigma(P')}$ divides $B_{nP'}$, then we have $|x(nR)| \geq 2\max\{|x(T)| : T \in \mathcal{E}[2]\}$; in particular, R is in the unbounded real connected component $\mathcal{E}(\mathbb{R})_0$.

Assume that $|x(nR')| \geq 2\max\{|x(T)| : T \in \mathcal{E}'[2]\}$ and $n\phi_{\mathcal{E}'}(R') = \phi_{\mathcal{E}'}(nR')$. Then inequality (28) gives

$$\begin{aligned} h_\infty(nR') - \tfrac{5}{2}\log(2) &\leq -\log|\phi_{\mathcal{E}'}(nR')| \\ &\leq -\log(n) - \log|\phi_{\mathcal{E}'}(R')| \\ &\leq -\log(n) + h_\infty(R') + \tfrac{1}{2}\log(2). \end{aligned}$$

Now [26, Theorem 1.1] asserts that

$$\begin{aligned} h_\infty(R') \leq h(R') &\leq \widehat{h}(R') + h(\mathcal{E}') + \tfrac{3}{24}h(j(\mathcal{E}')) + 0.973 \\ &\leq \widehat{h}(R') + \tfrac{5}{2}h(E') + \log(6) + 0.973. \end{aligned}$$

Applying [26, Theorem 5.5] to $\widehat{h_\infty}(nP') = \widehat{h_\infty}(nR')$ we get

$$\widehat{h_\infty}(nP') + \log(n) \leq \widehat{h}(P') + \frac{7}{2}h(E') + 2\log(6) + 3\log(2) + 2.043. \tag{29}$$

If every prime factor of $B_{nP'}$ divides $B_{P'}$ and $n\phi_{\mathcal{E}'}(R') = \phi_{\mathcal{E}'}(nR')$ and $3\log(2) \leq \log(n)$, then it follows from inequality (29) and Theorem 5.3 that $n \leq \frac{1}{\widehat{h}(P')} + \sqrt{5 + \frac{5h(E')+6}{\widehat{h}(P')}}$. The proof of inequality (29) holds also when replacing E', P' and R' respectively by E, P and R. It follows that, if every prime factor of $B_{n\sigma(P')}$ divides $B_{nP'}$ and $n\phi_{\mathcal{E}}(R) = \phi_{\mathcal{E}}(nR)$ and $3\log(2) \leq \log(n)$, then $n \leq \frac{2}{\widehat{h}(P')} + \sqrt{103 + \frac{12h(E)}{\widehat{h}(\sigma(P'))} + \frac{7}{\widehat{h}(P')}}$. □

Proposition 8.3.3. *We use Notation* 3.0.1 *and we assume that E and E' are given by minimal Weierstrass equations. Let δ be either* 0 *or $d = \deg(\sigma)$. Let $n_3 > n_2 > n_1 > 8$ be three pairwise coprime integers with*

$$n_3 > n_2 > n_1 > \frac{1}{\widehat{h}(P')} + \sqrt{103 + \delta + \max\left\{\frac{6h(E')}{\widehat{h}(P')}, \frac{12h(E)}{\widehat{h}(\sigma(P'))}\right\} + \frac{7}{\widehat{h}(P')}}\,.$$

If $\delta = 0$ (respectively $\delta = d$) we set $B := B_{P'}$ (respectively $B := B_{\sigma(P')}$). We assume that $B_{n_i\sigma(P')}$ has at most one prime factor coprime to B. Then we have

$$\text{either} \quad n_1 \leq \frac{1}{\widehat{h}(P')} + \sqrt{102 + \frac{2\log(n_3)+54h(E)}{\widehat{h}(\sigma(P'))} + \frac{24.42}{\widehat{h}(P')}}$$

$$\text{or} \quad n_1 \leq \frac{1}{\widehat{h}(P')} + \sqrt{100 + \delta + \frac{\log(n_i)+27h(E')+23.42}{\widehat{h}(P')}},$$

with $i \in \{2,3\}$ an index such that every prime factor of $B_{n_iP'}$ divides B.

Proof. The proof is the same when $\delta = 0$ and when $\delta = d$, except in the bounds obtained when we apply Theorem 5.3 and Lemma 8.3.2. This is why we give the proof only in the case when $\delta = 0$. We use Notation 8.3.1. For every $l \in \{1,2,3\}$ at most one prime factor of $B_{n_l\sigma(P')}$ does not divide $B_{P'}$. In particular, there are two indices $i \neq j$ such that

- either every prime factor of $B_{n_iP'}$ divides $B_{P'}$ and every prime factor of $B_{n_jP'}$ divides $B_{P'}$;
- or every prime factor of $B_{n_i\sigma(P')}$ divides $B_{n_iP'}$ and every prime factor of $B_{n_j\sigma(P')}$ divides $B_{n_jP'}$.

We assume for now that every prime factor of $B_{n_iP'}$ divides $B_{P'}$ and every prime factor of $B_{n_jP'}$ divides $B_{P'}$. Lemma 8.3.2 asserts that

- $|x(n_iP')| \geq 2\max\{|x(T)| \ : \ T \in \mathcal{E}'[2]\}$ and $\phi_{\mathcal{E}'}(n_iP') \neq n_i\phi_{\mathcal{E}'}(P')$;
- $|x(n_jP')| \geq 2\max\{|x(T)| \ : \ T \in \mathcal{E}'[2]\}$ and $\phi_{\mathcal{E}'}(n_jP') \neq n_j\phi_{\mathcal{E}'}(P')$.

We denote by $m_i \neq 0$ and $m_j \neq 0$ two integers such that

$$\phi_{\mathcal{E}'}(n_iP') = n_i\phi_{\mathcal{E}'}(P') + 2m_i\phi_{\mathcal{E}'}(T_0),$$
$$\phi_{\mathcal{E}'}(n_jP') = n_j\phi_{\mathcal{E}'}(P') + 2m_j\phi_{\mathcal{E}'}(T_0).$$

Since $|n_i\phi_{\mathcal{E}'}(P') + 2m_i\phi_{\mathcal{E}'}(T_0)| \leq |\phi_{\mathcal{E}'}(T_0)|$ and $|\phi_{\mathcal{E}'}(P')| \leq |\phi_{\mathcal{E}'}(T_0)|$, we have $|m_i| < |n_i|$. If $n_im_j = n_jm_i$, then n_i is a divisor of m_i (because n_i and n_j are coprime). It follows that $n_jm_i - n_im_j \neq 0$. In particular, we get

$$\begin{aligned} 2\left|\phi_{\mathcal{E}'}(T_0)\right| &\leq 2\left|\phi_{\mathcal{E}'}(T_0)\right|\left|n_jm_i - n_im_j\right| \\ &\leq \left|n_j\phi_{\mathcal{E}'}(n_iP') - n_i\phi_{\mathcal{E}'}(n_jP')\right| \\ &\leq 2\max\left\{|n_j|\left|\phi_{\mathcal{E}'}(n_iP')\right|, |n_i|\left|\phi_{\mathcal{E}'}(n_jP')\right|\right\}. \end{aligned} \tag{30}$$

We deduce from inequality (28) and inequality (30) that

$$\min\{h_\infty(n_jP') - \log(n_i), h_\infty(n_iP') - \log(n_j)\} \leq -\log\left|\phi_{\mathcal{E}'}(T_0)\right| + \frac{5}{2}\log(2).$$

Applying [20, Lemme 2.1] and inequality (23), we get

$$\min\{h_\infty(n_jP') - \log(n_i), h_\infty(n_iP') - \log(n_j)\} \leq 24h(E') + 22.35.$$

Theorem 5.3 and [26, Theorem 5.5] show that

$$n_1 \leq \min\{n_i, n_j\} \leq \frac{1}{\widehat{h}(P')} + \sqrt{4 + \frac{\log\left(\max\{n_i, n_j\}\right) + 26h(E') + 23.42}{\widehat{h}(P')}}.$$

Now we assume that every prime factor of $B_{n_i\sigma(P')}$ divides $B_{n_iP'}$ and every prime factor of $B_{n_j\sigma(P')}$ divides $B_{n_jP'}$. An analogous argument shows that

$$\min\{h_\infty(n_j\sigma(P')) - \log(n_i), h_\infty(n_i\sigma(P')) - \log(n_j)\} \leq 24h(E) + 22.35.$$

From this inequality, Theorem 5.3, and [26, Theorem 5.5], we deduce that

$$n_1 \leq \frac{1}{\widehat{h}(P')} + \sqrt{102 + \frac{2\log(n_3) + 54h(E)}{\widehat{h}(\sigma(P'))} + \frac{23.42}{\widehat{h}(P')} + \frac{\log(d)}{(d-1)\widehat{h}(P')}}.$$

(Note that $n_1 \leq \min\{n_i, n_j\}$ and $\max\{n_i, n_j\} \leq n_3$). □

8.4. **The proof of Theorem 1.2.2.** The bounds we prove in this section are expressed as a function of $\Gamma := \max\left\{1, \frac{h(E')}{\widehat{h}(P')}, \frac{h(E)}{\widehat{h}(\sigma(P'))}\right\}$. The statement of Theorem 1.2.2 is deduced by using the inequality $\Gamma \leq C(P')$, which was already used in the proof of Proposition 7.2.1. The use of the number $C(P')$ in the statement of Theorem 1.2.2 is motivated by the fact that, unlike $C(P')$, the number Γ has a definition which depends on the choice of equations for E and E'. However, Γ is easier to compute in practice than $C(P')$. The inequality $h(E') \geq \frac{\log(16)}{12} = \frac{\log(2)}{3}$ implies that

$$\frac{2}{\widehat{h}(\sigma(P'))} \leq \frac{1}{\widehat{h}(P')} \leq \frac{3\Gamma}{\log(2)} \leq 4.33 \times \Gamma.$$

Let n be an integer such that at most one prime factor of $B_{n\sigma(P')}$ is not a prime factor of $B_{P'}$. We have either

- each prime factor of $B_{n\sigma(P')}$ divides $B_{nP'}$,
- or each prime factor of $B_{nP'}$ divides $B_{P'}$.

If $n = n_1 n_2$ with $n_1 \geq n_2 > 1$, then Corollary 7.2.2 implies that either

$$n \leq n_1^2 \leq \frac{4}{\widehat{h}(P')}\left(\frac{1}{2}\log\left(\frac{4}{\widehat{h}(P')}\right)\right)^2 \leq 5\Gamma\left(\log(18\Gamma)\right)^2$$

or

$$n \leq n_1^2 \leq \left(\frac{26}{\sqrt{\widehat{h}(P')}} + \sqrt{200 + \frac{147h(E') + 129}{\widehat{h}(P')}}\right)^2 \leq 7089\Gamma.$$

Let N_i be the i-th largest prime integer such that $B_{N_i\sigma(P')}$ has at most one prime factor coprime to $B_{P'}$. Proposition 8.2.1 asserts that

$$N_1 \leq \max\left\{3.5 \times 10^{29}\Gamma, 2 \times 10^{23}\widehat{h}(\sigma(P'))^{5/2}, 4 \times 10^{27}\Gamma^{7/2}\widehat{h}(\sigma(P'))^{5/2}\right\}.$$

In particular, since $h \geq \log(h)$ for every $h \geq 1$, we have

$$\frac{\log(N_1)}{\widehat{h}(\sigma(P'))} \leq 295\Gamma + 8\Gamma\log(\Gamma) + \frac{5}{2}. \tag{31}$$

Noticing that $\frac{1}{\widehat{h}(P')} + \sqrt{103 + \max\left\{\frac{5h(E')}{\widehat{h}(P')}, \frac{12h(E)}{\widehat{h}(\sigma(P'))}\right\} + \frac{7}{\widehat{h}(P')}} \leq 17\Gamma$, we deduce from Proposition 8.3.3 and inequality (31) that either $N_3 \leq 17\Gamma$

$$\text{or} \quad N_3 \leq \frac{1}{\widehat{h}(P')} + \sqrt{102 + \frac{2\log(N_1) + 54h(E)}{\widehat{h}(\sigma(P'))} + \frac{24.42}{\widehat{h}(P')}} \leq 34\Gamma$$

$$\text{or} \quad N_3 \leq \frac{1}{\widehat{h}(P')} + \sqrt{100 + \frac{\log(N_i) + 27h(E') + 23.42}{\widehat{h}(P')}}, \tag{32}$$

for some $i \in \{1, 2\}$ such that every prime factor of $B_{N_i P'}$ divides $B_{P'}$. When inequality (32) holds, Proposition 8.2.1 gives $\frac{\log(N_i)}{\widehat{h}(P')} \leq 590\Gamma + 16\Gamma\log(\Gamma) + \frac{5}{2}$. In that case inequality (32) implies that $N_3 \leq 34\Gamma$.

Remark 8.4.1. The proof of Theorem 1.2.2 can be adapted to give an upper bound on indices n such that $B_{n\sigma(P')}$ has at most one prime factor coprime to $B_{\sigma(P')}$. Let $\widetilde{N_i}$ be the i-th largest integer such that $B_{\widetilde{N_i}\sigma(P')}$ has at most one prime factor coprime to $B_{\sigma(P')}$. Then Proposition 8.2.1 asserts that

$$\widetilde{N_i} \leq \sqrt{d} + \max\left\{3.5\times 10^{29}\Gamma, 2\times 10^{23}\widehat{h}(\sigma(P'))^{5/2}, 4\times 10^{27}\Gamma^{7/2}\widehat{h}(\sigma(P'))^{5/2}\right\}.$$

In particular, since $\log(x+y) \leq \log\left(2\max\{x,y\}\right)$ pour tous $x, y > 0$, we have

$$\frac{\log(\widetilde{N_i})}{\widehat{h}(P')} \leq \max\left\{5\log\left(2\sqrt{d}\right)\Gamma; 590\Gamma + 16\Gamma\log(\Gamma) + 5 + \log(2)\right\}$$

and it follows from Proposition 8.3.3 that

$$\begin{aligned}\widetilde{N_3} &\leq \tfrac{1}{\widehat{h}(P')} + \sqrt{100 + d + \tfrac{\log(\widetilde{N_i})+24.42}{\widehat{h}(P')} + \max\left\{\tfrac{27h(E')}{\widehat{h}(P')}, \tfrac{54h(E)}{\widehat{h}(\sigma(P'))}\right\}} \\ &\leq \max\left\{34\Gamma + \Gamma\sqrt{d}; 21\Gamma + \Gamma\sqrt{d + \tfrac{5}{2}\log(d)}\right\}.\end{aligned}$$

9. Elliptic curves with j-invariant 1728

In this section we compute the bound from Corollary 7.3.1 in the particular case of an elliptic curve E_A defined by a Weierstrass equation

$$E_A : y^2 = x(x^2 - A), \tag{33}$$

where A denotes a positive integer not divisible by a fourth power. The results are stated for the elliptic divisibility sequence $(B_{nP})_{n\in\mathbb{N}}$ arising from a $\mathbb{Q}$-point P on E_A of infinite order, relative to equation (33) (see Notation 1.1.1). This sequence $(B_{nP})_{n\in\mathbb{N}}$ might not be normalized; equation (33) is not minimal in general.

For congruent number curves our results can be deduced from results on integer points on E_{N^2}. For nonsquare A, the main difficulty is to get the following explicit version of Lang's conjecture 1.2.6. (Note that Lang's conjecture is known to be true for elliptic curves with integral j-invariant).

Proposition 9.1. *Let $P \in E_A(\mathbb{Q})$ be a nontorsion point lying on the bounded connected component of $E_A(\mathbb{R})$. Denote by $\widehat{h}_A$ the canonical height on E_A. Then*

$$\widehat{h}_A(P) \geq \frac{1}{16}\log|2A| \tag{34}$$

when $A \not\equiv 12 \bmod 16$ and

$$\widehat{h}_A(P) \geq \frac{1}{64}\log|2A| \tag{35}$$

when $A \equiv 12 \bmod 16$. Moreover, writing $x(P) = A_P/B_P^2$, we have

$$-\frac{1}{4}\log|A| - \frac{3}{8}\log(2) \leq \widehat{h}_A(P) - \frac{1}{4}\log|A_P^2 + AB_P^4| \leq \frac{1}{12}\log(2). \tag{36}$$

Proof. The proposition is similar to [2, Proposition 2.1] so we do not give a full proof here. However, more reduction types have to be considered than in the case $A = N^2$, leading to a more complicated proof. The proof is based on the decomposition of the canonical height as a sum of local canonical heights.

Denote by $\Delta_A = 64A^3$ the discriminant of E_A. The contribution of the archimedean height is computed using Tate's series as in [2]. We get

$$0 \leq \widehat{h}_\infty(P) - \frac{1}{4}\log|x(P)^2 + A| + \frac{1}{12}\log(\Delta_A) \leq \frac{1}{12}\log(2). \tag{37}$$

Nonarchimedean canonical heights are computed using the algorithm presented in [25]. If v is an odd prime number, then Tate's algorithm can be used to prove that E_A has reduction type:

- I_0 at v when $\mathrm{ord}_v(A) = 0$;
- III at v when $\mathrm{ord}_v(A) = 1$;
- I_0^* at v when $\mathrm{ord}_v(A) = 2$;
- III^* at v when $\mathrm{ord}_v(A) = 3$.

In particular, $2P$ always has good reduction at v, and we get

$$-\tfrac{v(A)}{4} \leq \widehat{h_v}(P) - \tfrac{1}{2}\max\{0, -v(x(P))\} - \tfrac{v(\Delta_A)}{12} \leq 0. \tag{38}$$

(The only technical difficulty is the case $\mathrm{ord}_v(A) = 2\,\mathrm{ord}_v(x(P)) = 2$; in that case, the equation for E_A implies that $\mathrm{ord}_v(x(P)^2 - A) \equiv \mathrm{ord}_v(x(P)) \bmod 2$ and it follows that $\mathrm{ord}_v(x(P)^2 + A) = \mathrm{ord}_v(2A) = 2$.)

Considering the specialization of E_A at 2, Tate's Algorithm gives reduction type:

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

In particular, every double $2P$ in $E_A(\mathbb{Q})$ has good reduction everywhere if and only if $A \not\equiv 12 \bmod 16$. When $A \equiv 12 \bmod 16$, every $\mathbb{Q}$-point on E_A in the image of the multiplication-by-4 map has good reduction everywhere. Moreover, the algorithm described in [25] gives

$$-\frac{v_2(A)}{4} - \frac{3}{8}\log(2) \leq \widehat{h_2}(P) - \frac{1}{2}\max\{0, -v_2(x(P))\} - \frac{v_2(\Delta_A)}{12} \leq 0. \tag{39}$$

We compute the canonical height by summing local canonical heights. By doing so, inequality (36) becomes a consequence of inequalities (37), (38) and (39).

Now we prove the two inequalities (34) and (35). When $Q \in E_A(\mathbb{Q})$ has good reduction everywhere we have

$$\sum_{v \neq \infty} \widehat{h_v}(Q) = \log|B_Q| + \frac{1}{4}\log|4A|.$$

By adding this equation and the inequality (37) we get

$$\widehat{h}_A(Q) \geq \frac{1}{4}\log|A_Q^2 + AB_Q^4|. \tag{40}$$

If Q is a point in the bounded real connected component of E_A, then $|A_Q| = |x(Q)|B_Q^2 \geq \sqrt{|A|}B_Q^2 \geq \sqrt{|A|}$. Inequality (40) becomes

$$\widehat{h}_A(Q) \geq \frac{1}{4}\log|2A|. \tag{41}$$

Finally, let P be any $\mathbb{Q}$-point on E_A. As shown above $2P$ has good reduction everywhere whenever $A \not\equiv 12 \bmod 16$, and $4P$ has good reduction everywhere in all cases. The two inequalities (34) and (35) follow from inequality (41) applied with $Q \in \{2P, 4P\}$. □

Proposition 9.2. *Let P be a $\mathbb{Q}$-point of infinite order on E_A. Then B_{2kP} is composite in the following two cases:*

- *when $k \geq 5$ and $A \not\equiv 12 \bmod 16$;*
- *when $k \geq 10$ and $A \equiv 12 \bmod 16$;*

Proof. Since $\gcd(A_{kP}, B_{kP}) = 1$, the equation

$$x(2kP) = \frac{(A_{kP}^2 + AB_{kP}^4)^2}{4B_{kP}^2 A_{kP}(A_{kP}^2 - AB_{kP}^4)}$$

shows that B_{2kP} is composite in the following three cases:

- when $B_{kP} > 1$ and $|A_{kP}| > A^2$;
- when $B_{kP} > 1$ and $AB_{kP}^4 - A_{kP}^2 > 4A^2$;
- when $|A_{kP}| > A^3$ and $A_{kP}^2 - AB_k^4 > 4A^2$.

(Note that $4A^2 \geq \gcd\left(AB_{kP}^4 - A_{kP}^2, (A_{kP}^2 + AB_{kP}^4)^2\right)$.) We assume that we are not in the first case, i.e., that either $B_{kP} = 1$ or $|A_{kP}| \leq A^2$. We show then that the second case happens whenever $x(kP) < 0$, and the third case happens whenever $x(kP) > 0$.

Case 1: $x(kP) < 0$. Then $|x(kP)| < \sqrt{|A|}$, which implies that

$$\log|A_{kP}^2 + AB_{kP}^4| \leq \log(2AB_{kP}^4).$$

Now inequality (36) gives

$$k^2 \widehat{h}_A(P) \leq \frac{1}{4}\log(2AB_{kP}^4) + \frac{1}{12}\log(2).$$

Using inequalities (34) and (35) we get

$$\frac{k^2}{16}\log(2A) \leq \frac{1}{4}\log(2AB_{kP}^4) + \frac{1}{12}\log(2),$$

when $A \not\equiv 12 \bmod 16$, and

$$\frac{k^2}{64}\log(2A) \leq \frac{1}{4}\log(2AB_{kP}^4) + \frac{1}{12}\log(2),$$

when $A \equiv 12 \bmod 16$. In particular:

- the inequality $B_{kP} > 1$ holds for $k \geq 3$ when $A \not\equiv 12 \bmod 16$, and for $k \geq 5$ when $A \equiv 12 \bmod 16$;
- the inequality $AB_{kP}^4 > 5A^4$ holds for $k \geq 4$ when $A \not\equiv 12 \bmod 16$, and for $k \geq 8$ when $A \equiv 12 \bmod 16$.

Note that if $|B_{kP}| > 1$, then (by assumption) $|A_{kP}| \leq A^2$. It follows that the inequality

$$AB_k^4 - A_{kP}^2 \geq AB_{kP}^4 - A^4 > 4A^2$$

holds, whenever $|B_{kP}| > 1$ and $AB_{kP}^4 > 5A^4 \geq 4A^2 + A^4$.

Case 2: $x(kP) > 0$. Then $|x(kP)| > \sqrt{|A|}$ which implies that

$$\log|A_{kP}^2 + AB_{kP}^4| \leq 2\log|2A_{kP}| - \log(2).$$

Now inequality (36) gives

$$k^2\widehat{h}_A(P) \leq \frac{1}{2}\log|2A_{kP}| - \frac{1}{6}\log(2).$$

Using inequalities (34) and (35) we get

$$\frac{k^2}{16}\log(2A) \leq \frac{1}{2}\log|2A_{kP}| - \frac{1}{6}\log(2),$$

when $A \not\equiv 12 \bmod 16$, and

$$\frac{k^2}{64}\log(2A) \leq \frac{1}{2}\log|2A_{kP}| - \frac{1}{6}\log(2),$$

when $A \equiv 12 \bmod 16$. In particular:

- the inequality $|A_{kP}| > A^3$ holds for $k \geq 5$ if $A \not\equiv 12 \bmod 16$, and for $k \geq 10$ if $A \equiv 12 \bmod 16$;
- the inequality $A_{kP}^2 > 5A^2$ holds for $k \geq 3$ if $A \not\equiv 12 \bmod 16$, and for $k \geq 6$ if $A \equiv 12 \bmod 16$.

Suppose $|A_{kP}| > A^3$. Then $|A_{kP}| > A^2$ and it follows that $B_{kP} = 1$. In particular, the inequality

$$A_{kP}^2 - AB_k^4 \geq A_{kP}^2 - A^2 > 4A^2$$

holds, whenever $A_{kP}^2 > 5A^2 \geq 4A^2 + A$ and $|A_{kP}| > A^3$. □

Proposition 9.3. *Let m be an odd integer. Let P' be a $\mathbb{Q}$-point of infinite order on E_A. Denote by P the multiple mP'. Assume $P \in E_A(\mathbb{Q})$ is a point on the bounded component of E_A. Then B_{nP} is composite:*

- *when $n \geq 4$ and $A \not\equiv 12 \bmod 16$;*
- *when $n \geq 8$ and $A \equiv 12 \bmod 16$.*

Proof. When n is even, Proposition 9.2 applied to P' shows that $B_{nP} = B_{nmP'}$ is composite:

- when $n \geq \frac{10}{m}$ and $A \not\equiv 12 \bmod 16$;
- when $n \geq \frac{20}{m}$ and $A \equiv 12 \bmod 16$.

From now on we assume that n is odd. In that case nP lies on the bounded component of the curve. As in the proof of Proposition 9.2, this implies that

$$n^2\widehat{h}_A(P') \leq \log(B_{nP'}) + \frac{1}{4}\log(2A) + \frac{1}{12}\log(2), \tag{42}$$

$$m^2n^2\widehat{h}_A(P') \leq \log(B_{nP}) + \frac{1}{4}\log(2A) + \frac{1}{12}\log(2). \tag{43}$$

Equation (42) shows that the inequality $B_{nP'} > 1$ holds, for $n \geq 3$ when $A \not\equiv 12 \bmod 16$, and for $n \geq 6$ when $A \equiv 12 \bmod 16$.

From now on we assume that each prime factor of B_{nP} divides $B_{nP'}$. Then [10, Lemma 2.3] implies that B_{nP} divides $m^2B_{nP'}$. As a consequence, equation (43) gives

$$m^2n^2\widehat{h}_A(P') \leq 2\log(m) + \frac{1}{4}\log(B_{nP'}^4) + \frac{1}{4}\log(A) + \frac{1}{3}\log(2).$$

Using the first inequality (36), we get

$$\begin{aligned} m^2n^2\widehat{h}_A(P') &\leq \tfrac{1}{4}\log|A^2_{nP'} + AB^4_{nP'}| + 2\log(m) + \tfrac{1}{3}\log(2) \\ &\leq n^2\widehat{h}_A(P') + \tfrac{1}{4}\log|A| + 2\log(m) + \tfrac{17}{24}\log(2). \end{aligned}$$

Now it follows from inequalities (34) and (35) that

$$\frac{(m^2-1)n^2}{16}\log|2A| \leq \frac{1}{4}\log|2A| + 2\log(m) + \frac{11}{24}\log(2),$$

when $A \not\equiv 12 \bmod 16$, and

$$\frac{(m^2-1)n^2}{64}\log|2A| \leq \frac{1}{4}\log|2A| + 2\log(m) + \frac{11}{24}\log(2),$$

when $A \equiv 12 \bmod 16$. Since $m \geq 3$, these inequalities imply $n < 4$ when $A \not\equiv 12 \bmod 16$, and $n < 8$ when $A \equiv 12 \bmod 16$. □

References

[1] Mohamed Ayad, *Points S-entiers des courbes elliptiques*, Manuscripta Math. **76** (1992), no. 3-4, 305–324, DOI 10.1007/BF02567763 (French). MR1185022 (93i:11064)

[2] A. Bremner, J. H. Silverman, and N. Tzanakis, *Integral points in arithmetic progression on $y^2 = x(x^2 - n^2)$*, J. Number Theory **80** (2000), no. 2, 187–208, DOI 10.1006/jnth.1999.2430. MR1740510 (2001i:11066)

[3] J. Cheon and S. Hahn, *Explicit valuations of division polynomials of an elliptic curve*, Manuscripta Math. **97** (1998), no. 3, 319–328, DOI 10.1007/s002290050104. MR1654780 (99i:11039)

[4] D. V. Chudnovsky and G. V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests*, Adv. in Appl. Math. **7** (1986), no. 4, 385–434, DOI 10.1016/0196-8858(86)90023-0. MR866702 (88h:11094)

[5] Capi Corrales-Rodrigáñez and René Schoof, *The support problem and its elliptic analogue*, J. Number Theory **64** (1997), no. 2, 276–290, DOI 10.1006/jnth.1997.2114. MR1453213 (98c:11049)

[6] Gary Cornell and Joseph H. Silverman (eds.), *Arithmetic geometry*, Springer-Verlag, New York, 1986. Papers from the conference held at the University of Connecticut, Storrs, Connecticut, July 30–August 10, 1984. MR861969 (89b:14029)

[7] Sinnou David, *Minorations de formes linéaires de logarithmes elliptiques*, Mém. Soc. Math. France (N.S.) **62** (1995), iv+143 (French, with English and French summaries). MR1385175 (98f:11078)

[8] Manfred Einsiedler, Graham Everest, and Thomas Ward, *Primes in elliptic divisibility sequences*, LMS J. Comput. Math. **4** (2001), 1–13 (electronic). MR1815962 (2002e:11181)

[9] Kirsten Eisenträger and Graham Everest, *Descent on elliptic curves and Hilbert's tenth problem*, Proc. Amer. Math. Soc. **137** (2009), no. 6, 1951–1959, DOI 10.1090/S0002-9939-08-09740-2. MR2480276 (2009k:11201)

[10] Graham Everest, Patrick Ingram, Valéry Mahé, and Shaun Stevens, *The uniform primality conjecture for elliptic curves*, Acta Arith. **134** (2008), no. 2, 157–181, DOI 10.4064/aa134-2-7. MR2429645 (2009d:11088)

[11] Graham Everest, Victor Miller, and Nelson Stephens, *Primes generated by elliptic curves*, Proc. Amer. Math. Soc. **132** (2004), no. 4, 955–963 (electronic), DOI 10.1090/S0002-9939-03-07311-8. MR2045409 (2005a:11076)

[12] Graham Everest and Thomas Ward, *Heights of polynomials and entropy in algebraic dynamics*, Universitext, Springer-Verlag London Ltd., London, 1999. MR1700272 (2000e:11087)

[13] M. Hindry and J. H. Silverman, *The canonical height and integral points on elliptic curves*, Invent. Math. **93** (1988), no. 2, 419–450, DOI 10.1007/BF01394340. MR948108 (89k:11044)

[14] Patrick Ingram, *Elliptic divisibility sequences over certain curves*, J. Number Theory **123** (2007), no. 2, 473–486, DOI 10.1016/j.jnt.2006.08.007. MR2301226 (2007k:11090)

[15] Patrick Ingram, *Multiples of integral points on elliptic curves*, J. Number Theory **129** (2009), no. 1, 182–208, DOI 10.1016/j.jnt.2008.08.001. MR2468477 (2010a:11102)

[16] Patrick Ingram and Joseph H. Silverman, *Uniform estimates for primitive divisors in elliptic divisibility sequences*, Number theory, Analysis and Geometry, Springer, New York, (2012), 243–271.
[17] Serge Lang, *Elliptic curves: Diophantine analysis*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 231, Springer-Verlag, Berlin, 1978. MR518817 (81b:10009)
[18] B. Mazur and J. Tate, *The p-adic sigma function*, Duke Math. J. **62** (1991), no. 3, 663–688, DOI 10.1215/S0012-7094-91-06229-0. MR1104813 (93d:11059)
[19] D. W. Masser and G. Wüstholz, *Estimating isogenies on elliptic curves*, Invent. Math. **100** (1990), no. 1, 1–24, DOI 10.1007/BF01231178. MR1037140 (91d:11060)
[20] Federico Pellarin, *Sur une majoration explicite pour un degré d'isogénie liant deux courbes elliptiques*, Acta Arith. **100** (2001), no. 3, 203–243, DOI 10.4064/aa100-3-1 (French). MR1865384 (2003c:11058)
[21] Clayton Petsche, *Small rational points on elliptic curves over number fields*, New York J. Math. **12** (2006), 257–268 (electronic). MR2259240 (2007g:11061)
[22] Bjorn Poonen, *Hilbert's tenth problem and Mazur's conjecture for large subrings of* $\mathbb{Q}$, J. Amer. Math. Soc. **16** (2003), no. 4, 981–990 (electronic), DOI 10.1090/S0894-0347-03-00433-8. MR1992832 (2004f:11145)
[23] Takakazu Satoh, *Generalized division polynomials*, Math. Scand. **94** (2004), no. 2, 161–184. MR2053737 (2005b:11078)
[24] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR817210 (87g:11070)
[25] J. H. Silverman. Computing heights on elliptic curves. *Math. Comp.*, 51(183):339–358, 1988.
[26] Joseph H. Silverman, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. **55** (1990), no. 192, 723–743, DOI 10.2307/2008444. MR1035944 (91d:11063)
[27] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR1312368 (96b:11074)
[28] Joseph H. Silverman and Katherine E. Stange, *Terms in elliptic divisibility sequences divisible by their indices*, Acta Arith. **146** (2011), no. 4, 355–378, DOI 10.4064/aa146-4-4. MR2747036 (2012c:11126)
[29] Marco Streng, *Divisibility sequences for elliptic curves with complex multiplication*, Algebra Number Theory **2** (2008), no. 2, 183–208, DOI 10.2140/ant.2008.2.183. MR2377368 (2009e:11110)
[30] R. J. Stroeker and N. Tzanakis, *Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arith. **67** (1994), no. 2, 177–196. MR1291875 (95m:11056)
[31] N. Tzanakis and B. M. M. de Weger, *How to explicitly solve a Thue-Mahler equation*, Compositio Math. **84** (1992), no. 3, 223–288. MR1189890 (93k:11025)
[32] Jacques Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241 (French). MR0294345 (45 #3414)
[33] P. M. Voutier and M. Yabuta, *Lang's conjecture for the elliptic curve* $y^2 = x\left(x^2 + ax\right)$, International Journal of Number Theory **9** (2013), 1141–1170.
[34] Samuel S. Wagstaff Jr., *Divisors of Mersenne numbers*, Math. Comp. **40** (1983), no. 161, 385–397, DOI 10.2307/2007383. MR679454 (84j:10052)
[35] Morgan Ward, *Memoir on elliptic divisibility sequences*, Amer. J. Math. **70** (1948), 31–74. MR0023275 (9,332j)

École Polytechnique Fédérale de Lausanne, SB-IMB-CSAG, Station 8, CH-1015 Lausanne, Switzerland.
E-mail address: valery.mahe@epfl.ch