PRIME POWER TERMS IN ELLIPTIC DIVISIBILITY SEQUENCES.

VALÉRY MAHÉ

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 [27]).

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 [26]). 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 [6]).

Conjecture 1.1 (Primality conjecture)**.** 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 [9] (see below for a definition of the magnification condition). Although the magnification condition is a strong assumption, the study of prime terms in magnified elliptic divisibility sequences has applications to logic. It is studied in [7] as part of a further investigation of a result of Poonen on Hilbert's tenth problem (see [17]).

In this article we explain how the primality conjecture for magnified elliptic divisibility sequences is linked to classical problems in diophantine

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

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

This work began at the university of East Anglia (and was funded by an EPSRC grant). It was done while the author was working at the université de Montpellier 2 and at the université de Franche-Comté. The author want to thank Professor Everest, Professor Silverman, Professor Stevens and the anonymous referee for helpful discussions and comments.

geometry. The main result of this paper consists of a computation of explicit bounds on the index n of a prime power term B_n in a magnified elliptic divisibility sequence. Such explicit bounds are crucial when considering the problem of sieving for all prime power terms in a magnified elliptic divisibility sequence. Our 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 also show the existence of a uniform bound on the index of a prime power term in a normalized magnified elliptic divisibility sequence. This third theorem is conditional on conjectures of Lang and of Hall–Lang. This result improves the main theorem in [8]: 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.

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 E defined over $\mathbb{Q}$ by a Weierstrass equation with integral coefficients*

$$E : y^2 + a_1y + a_3xy = x^3 + a_2x^2 + a_4x + a_6. \tag{1}$$

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 and $a_1, a_3 \in \{0, 1\}$ 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 Weierstrass equation for E. Given any integer N there is a well-chosen Weiestrass 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. The prime factors of terms in an elliptic divisibility sequence B can easily be computed using the prime factors of terms in the normalized elliptic divisibility sequence associated to B. This is why 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 [27] 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};
- $nP \equiv 0_E \mod l$ (where 0_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*

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

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 predicts that the answer to Problem 1.1.3 depends strongly on the choice of the algebraic group G. However, many tools introduced to study the Mersenne problem have an analog which leads to a better understanding of the primality conjecture. The magnification condition has been introduced to study the analog for elliptic divisibility sequences of an easy result on Mersenne prime powers: 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 $\mathbb{Q}$ 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 [4] 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 B is a magnified. 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 $\displaystyle\sum_{k=0}^{m-1} 2^{kn}$ are coprime and 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 degree at least 3 between two elliptic curves defined over $\mathbb{Q}$ by minimal equations. Denote by $\Delta_{E'}$ the minimal discriminant of E'.*

Then there is an 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 $P' \in E'(\mathbb{Q})$ for which every prime factor of $B_{\sigma(P')}$ divides $B_{P'}$.

The existence of the polynomial F_σ is not surprising. It can easily be derived from the existence of division polynomials (see the proof of Theorem 1.2.1 for an explicit formula for F_σ). The originality of Theorem 1.2.1 lies in the relation $|d| \leq \deg(\sigma)^2|\Delta_{E'}|^{\deg(\sigma)/4}$ and the method used to obtain it. This 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 [24]. As explained above in the case $\sigma = [m]$, a term $B_{n\sigma(P')}$ 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 issue by adopting a different approach to the Mersenne problem for elliptic curves. We adapt results from [24] 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 $(B_{n\sigma(P')})_{n\in\mathbb{N}}$ be the normalized elliptic divisibility sequence associated to the image $\sigma(P')$ of some $\mathbb{Q}$-point $P' \in E'(\mathbb{Q})$ of infinite order on an elliptic curve E' under an isogeny $\sigma : E' \longrightarrow E$ defined over $\mathbb{Q}$. Then $B_{n\sigma(P')}$ has two distinct prime factors coprime to $B_{P'}$ for all prime numbers*

$$n > \max\left\{4.2 \times 10^{30} C(P'), 4 \times 10^{27} C(P')^{7/2} \widehat{h}(\sigma(P'))^{5/2}\right\}$$

and all composite numbers

$$n > 18C(P') \times \max\left\{28000, \left(\log(70C(P'))\right)^2\right\},$$

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

$$N_i > 77C(P')$$

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

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 $(B_{n\sigma(P')}/B_{P'})_{n\in\mathbb{N}}$.

Theorem 1.2.2 gives three bounds on the index of a prime power term in a magnified elliptic divisibility 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.

As in algorithms for the search for integer points on elliptic curves, the general bound should only be used when applying the Fincke-Pohst algorithm to compute the exceptional indices N_1 and N_2 if they exist. The two other bounds are then used to find 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 bounds on the archimedean heights of the multiples of P' and $\sigma(P')$ are known.

Example 1.2.3. *We consider Notation 1.1.1 when equation* (1) *is*

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

where A is a positive integer with no nonarchimedean valuation greater than 3*.*

- *Assume P is a $\mathbb{Q}$-point of infinite order on E_A with $x(P) \in \mathbb{Q}^{\times 2}$. Then B_{nP} is composite*
  - *whenever $n \geq 5$ if $A \not\equiv 12 \bmod 16$;*
  - *whenever $n \geq 10$ if $A \equiv 12 \bmod 16$.*
- *Assume $P = mP'$ with m odd and P' a $\mathbb{Q}$-point on the bounded component of E_A. Then B_{nP} is composite*
  - *whenever $n \geq 4$ if $A \not\equiv 12 \bmod 16$;*
  - *whenever $n \geq 8$ if $A \equiv 12 \bmod 16$.*

This example is obtained in section 9 by computing an upper bound for the number $C(P')$ introduced in Theorem 1.2.2. This is achieved by applying Tate's algorithm for the computation of the reduction type of E_A at each prime integer. This bound on $C(P')$ was previously known for curves E_{N^2} with $N \in \mathbb{N}$ squarefree. This is a particular case of the following conjecture of Lang.

Conjecture 1.2.4 (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 [11] that Lang's conjecture is a consequence of the Szpiro conjecture. This result was improved in [16]: 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.

While all previously stated results were unconditional, Corollary 1.2.6 below is a generalization of the second part in Example 1.2.3 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 1.2.5 (Hall–Lang)**.** *There are two constant $K, M > 0$ such that, for every quadruple of integers (A, B, x, y) with $y^2 = x^3 + Ax + B$ the following inequality holds*

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

Corollary 1.2.6. *Let $(B_{n\sigma(P')})_{n\in\mathbb{N}}$ be an elliptic divisibility sequence associated to the image $\sigma(P')$ of some $\mathbb{Q}$-point $P' \in E'(\mathbb{Q})$ of infinite order on*

an elliptic curve E' under an isogeny $\sigma : E' \longrightarrow E$ defined over $\mathbb{Q}$. We assume

(a) *that E and E' are defined by minimal short Weierstrass equations;*
(b) *the Lang conjecture 1.2.4 holds;*
(c) *the Hall–Lang conjecture 1.2.5 holds with $M < \frac{\deg(\sigma)}{4}$.*

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 1.2.6 is an improvement on the main result in [8]: 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 sequences 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 set of indices n such that B_{nP} has at most one prime factor.

2. Sketches of the proofs.

2.1. **The division polynomial and Thue equations.** The quotient of an elliptic curve E by $\{-1, 1\} \subset \mathrm{End}(E)$ is isomorphic as an algebraic variety to $\mathbb{P}^1$. Denote by $x_E : E \longrightarrow \mathbb{P}^1$ the composition of this isomorphism with the canonical map $E \longrightarrow E/\{-1, 1\}$. Since any isogeny $\sigma : E' \longrightarrow E$ is a morphism of algebraic groups, we have $x_E \circ \sigma = \varphi_\sigma \circ x_{E'}$, for some $\varphi_\sigma \in \mathbb{Q}(x)$.

We use the notation of Theorem 1.2.1. Assume $\deg(\sigma)$ is odd and E' and E are given by Weierstrass equations. Then the maps x_E and $x_{E'}$ are x-coordinates on E and E', and $\varphi_\sigma = \frac{\phi_\sigma}{\psi_\sigma^2}$ for some $\phi_\sigma, \psi_\sigma \in \mathbb{Z}[x]$. The roots of ψ_σ are the x-coordinates of the elements of $\ker(\sigma)$. Thus the degree of ψ_σ is $\frac{\deg(\sigma)-1}{2}$. Up to a choice of its leading coefficient, the polynomial ψ_σ is the division polynomial associated to σ. Our choice for the F_σ is its homogeneization $F_\sigma(X, Z) := Z^{(\deg(\sigma)-1)/2} \psi_\sigma(X/Z)$.

The denominator $B_{P'}$ divides $B_{\sigma(P')}$. Since $B_{\sigma(P')}$ divides the integer $B_{P'} F_\sigma\left(A_{P'}, B_{P'}^2\right)$ we get a factorization in $\mathbb{Z}$

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

The theory of formal groups shows that, if every prime factor $B_{\sigma(P')}$ 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:

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

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

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-parallelogramm 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 two following facts:

- the theory of formal groups shows that, if $n \in \mathbb{N}$ is any integer such that each prime factor of $B_{n\sigma(P')}$ divides $B_{nP'}$, then
$$\log\left|B_{n\sigma(P')}\right| \leq \log|B_{nP'}| + \log\left(\deg(\sigma)\right); \tag{2}$$
- Siegel's theorem can be used to show the existence of two numbers $h > h' > 0$ 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 explicit 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 1.2.6 by assuming the Hall-Lang conjecture 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 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 Mumford's gap principle to obtain a refinement of David's lower bound, which is stated in a nonexplicit way in [12].

For a simplified example of the techniques above we refer the reader to the proof of Example 1.2.3 in section 9.

3. Notations

We use the following notations:

Notation 3.1.

E', E	elliptic curves defined over $\mathbb{Q}$ by standardized minimal equations
$\sigma : E' \longrightarrow E$	an isogeny defined over $\mathbb{Q}$
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'
$(B_{n\sigma(P')})_{n\in\mathbb{N}}$	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
$\Delta_{\mathcal{E}}$	minimal discriminant of an elliptic curve $\mathcal{E}$
$h(\mathcal{E})$	naive height of an elliptic curve $\mathcal{E}$ defined by $h(\mathcal{E}) := \frac{1}{12}\max\{h(j(\mathcal{E})), h(\Delta_{\mathcal{E}})\}$

All height functions are defined using the same normalizations as in [21]. 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 issues when studying the primality conjecture for magnified points is to compute the image of a given point under a given isogeny in an appropriated 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.

4.1. **Background on division polynomials.**

Notation 4.1.1. *We use notation 3.1. Let*

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

$$E' : y^2 + a'_1 y + a'_3 xy = x^3 + a'_2 x^2 + a'_4 x + a'_6$$

be the (standardized) minimal Weierstrass equations for E and E'. Let ω_E (respectively $\omega_{E'}$) be the (minimal) invariant differential form associated to E (respectively E'). Let $d_\sigma \in \mathbb{Q}$ be such that $\sigma^*\omega_E = d_\sigma \omega_{E'}$. We denote

- *by $\psi_\sigma \in \mathbb{Q}(E)$ the division polynomial associated to σ i.e. the unique function ψ_σ on E such that $\psi_\sigma^2 = d_\sigma^2 \prod_{T \in \ker(\sigma)} (x - x(T))$;*
- *by ϕ_σ the polynomial $\phi_\sigma := \prod_{Q \in E'(\mathbb{Q}), x(\sigma(Q))=0} (x - x(Q))$.*

Lemma 4.1.2. *We use notation 4.1.1. Then d_σ is an element of $\mathbb{Z}$ (equal to m^2 when $\sigma = [m]$) and for every $P' \in E'(\mathbb{Q})$ we have*

$$x(\sigma(P')) = \frac{\phi_\sigma(P')}{\psi_\sigma(P')^2}.$$

Proof. In [25] Vélu defines an elliptic curve $\mathcal{E}$ using a Weierstrass equation with integral coefficients

$$\mathcal{E} : \widetilde{y}^2 + \alpha_1 \widetilde{y} + \alpha_3 \widetilde{x}\widetilde{y} = \widetilde{x}^3 + \alpha_2 \widetilde{x}^2 + \alpha_4 \widetilde{x} + \alpha_6$$

and an isomorphism $\varphi : E \longrightarrow \mathcal{E}$ such that

$$\widetilde{x}(\varphi(\sigma(P'))) = x(P') + \sum_{Q \in \ker(\sigma),\ Q \neq 0} \left(\frac{t_Q}{x(P') - x(Q)} + \frac{u_Q}{(x(P') - x(Q))^2} \right)$$

for every $\mathbb{Q}$-point $P' \notin \ker(\sigma)$ (where $t_Q \in \mathbb{C}$ and $u_Q \in \mathbb{C}$ are independent of P'). Since E is given by a minimal equation and since $\mathcal{E}$ is a model of E, we have $\widetilde{x} \circ \varphi = s^2 x + t$ where s and t are two integers. The invariant differential form on E associated to $\mathcal{E}$ is equal to $\varphi^*\omega_{\mathcal{E}} = s^{-1}\omega_E$. In [25] Vélu asserts that $(\varphi \circ \sigma)^*\omega_{\mathcal{E}} = \omega_{E'}$, i.e. that $\sigma^*\omega_E = s\omega_{E'}$. In other words $s = d_\sigma$ and it follows that $d_\sigma \in \mathbb{Z}$. See [18, Chapter III, Corollary 5.3] for the computation of d_σ when $\sigma = [m]$.

The divisors associated to the two functions $x \circ \sigma$ and $\frac{\phi_\sigma}{\psi_\sigma^2}$ are equal. It follows that $(x \circ \sigma)\frac{\psi_\sigma^2}{\phi_\sigma}$ is an element in $\mathbb{Q}$. In fact, using Vélu's formula to evaluate $\frac{x \circ \sigma}{x}$ at the point at infinity on E', and using the definition of the invariant differential, we see that $x \circ \sigma = \left(\frac{d_\sigma}{s}\right)^2 \frac{\phi_\sigma}{\psi_\sigma^2} = \frac{\phi_\sigma}{\psi_\sigma^2}$. □

Lemma 4.1.3. *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 $\psi_{\tau\circ\sigma}^2$ and ; see [13, appendix 1] for a more general result. The assertion for $\phi_{\tau\circ\sigma}$ follows since $\frac{\phi_{\tau\circ\sigma}}{\psi_{\tau\circ\sigma}^2} = x \circ \tau \circ \sigma = \frac{\phi_\tau\circ\sigma}{(\psi_\tau\circ\sigma)^2}$. □

Lemma 4.1.4. *We use notation 4.1.1. Then the two polynomials ϕ_σ and ψ_σ^2 have integral coefficients.*

Proof. Every point on E with x-coordinate 0 is integral. Any preimage of an integral point under an isogeny is integral. In particular the roots of ϕ_σ are integral. This proves that ϕ_σ has integral coefficients. The integrality of the coefficients of ψ_σ^2 is a classical generalization of the Nagell–Lutz theorem. □

Notation 4.1.5. *We keep the hypotheses of Lemma 4.1.3 and we assume that* $\deg(\tau)$ *and* $\deg(\sigma)$ *are coprime. We denote by $\widehat{\sigma}$ the dual isogeny of σ. Then the restriction of $\widehat{\sigma}$ to* $\ker(\tau)$ *gives a group isomorphism between* $\ker(\tau)$ *and a Gal$(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant subgroup of $E[\deg(\tau)]$. This subgroup $\widehat{\sigma}(\ker(\tau))$ is the kernel of an isogeny $\tau_\sigma : E \longrightarrow E_{\tau_\sigma}$ of degree* $\deg(\tau)$ *where E_{τ_σ} denotes an elliptic curve defined over $\mathbb{Q}$ by a standardized minimal equation. Using τ_σ, a natural factorization of division polynomials can be deduced from Lemma 4.1.3.*

Lemma 4.1.6. *We use notation 4.1.5 (in particular* $\deg(\sigma)$ *and* $\deg(\tau)$ *are coprime). Then $\psi_\sigma^2\psi_{\tau_\sigma}^2$ divides $\psi_{\tau\circ\sigma}^2$ in $\mathbb{Z}[x]$.*

Proof. Denote by $\widehat{\sigma}$ the dual isogeny of σ and by $\widehat{\tau_\sigma}$ the dual isogeny of τ_σ. Then we have $\ker(\tau \circ \sigma) = \ker(\sigma) + \widehat{\sigma}(\ker(\tau)) = \ker(\sigma_{\widehat{\tau_\sigma}} \circ \tau_\sigma)$. In particular the definition of division polynomials implies that $\psi_{\tau\circ\sigma}^2 = \psi_{\sigma_{\widehat{\tau_\sigma}}\circ\tau_\sigma}^2$. Applying Lemma 4.1.3, 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 $\ker(\sigma) \cap \ker(\tau_\sigma) = \{0_E\}$. We conclude, using two consequences of Cassels' statement of the Nagell–Lutz theorem:

- the quotient $\frac{\psi_{\tau\circ[m]}^2}{\psi_\tau^2\psi_m^2}$ is an element of $\mathbb{Z}[x]$ because $x(T)$ is an algebraic integer for every $T \in \ker(\sigma) + \widehat{\sigma}(\ker(\tau))$ that does not belong to $\ker(\tau)$ or $\widehat{\sigma}(\ker(\tau))$;
- the polynomials ψ_σ^2 and $\psi_{\tau_\sigma}^2$ belong also to $\mathbb{Z}[x]$ (see Lemma 4.1.2).

□

4.2. **Division polynomials and elliptic divisibility sequences.** Elliptic divisibility sequences are closely related to evaluations of division polynomials (see [1, 27]). For points with good reduction everywhere this link is quite simple.

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 0_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 [21]). 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 $\frac{B_P^{2\deg(\sigma)}\psi_\sigma(P)^2}{B^2_{\sigma(P)}}$ 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 $P' \in E'(\mathbb{Q})$ we have*

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

Proof. The proof is based on [10, 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 quasiparallelogram 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 $P, Q, P \pm Q \neq 0_E$.

When $\sigma = [n]$, equation (3) is proven recursively using the quasiparallelogram 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 [10, 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 quasiparallelogram law for $\widehat{h_\infty}$ implies that

$$\lim_{n\to+\infty}\sum_{T\in\ker(\sigma),T\neq 0}\frac{\log|x([n]P')-x([n]T)|}{n^2} = 0. \quad (4)$$

Applying [10, Theorem 6.18] to $\sigma(P')$ together with Lemma 4.1.3, we get

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

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

$$\lim_{n\to+\infty}\frac{\log|\psi_\sigma([n]P')|}{n^2}=\lim_{n\to+\infty}\sum_{T\in\ker(\sigma),T\neq 0}\frac{\log|x([n]P')-x([n]T)|}{n^2}=0,$$

and using equation (4) and [10, 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 into 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 [14, Chapter III, Theorem 4.5] for details). □

Lemma 4.1.3 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 4.2.4. *We use notation 3.1. Recall that $d=\deg(\sigma)$. Then we have*

$$v\left(B_P\right)\leq v\left(B_{\sigma(P)}\right).$$

If E' is also minimal, then $v(B_P)>0$ implies

$$v\left(B_{\sigma(P)}\right)\leq v\left(B_P\right)+v(d).$$

Proof. Under the assumption that E' is minimal at v, it is not hard to show that the isogeny σ induces a map of formal groups $F_\sigma : \hat{E}' \to \hat{E}$ defined over $\mathcal{O}_v$ with $F_\sigma(0) = 0$. (See, for example, the exposition in [22]); Streng proves this for number fields, but the proof works for any local field.) As $F_\sigma(z) \in z\mathcal{O}_v[[z]]$ vanishes at 0, it follows immediately that, if $v(x(P)) < 0$, then

$$v(B_{\sigma(P)}) = v(F_\sigma(z)) \geq v(z) = v(B_P).$$

If E is minimal as well, we may apply the same argument to the dual isogeny $\hat{\sigma} : E \to E'$, noting that the composition is the multiplication-by-d map. The argument above now tells us that $v(B_{\sigma(P)}) \leq v(B_{dP}) \leq v(B_P) + v(d)$. □

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 Lemma 4.2.4 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 canonical 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.

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

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

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

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

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

The map $x \longmapsto \log(x) - \frac{x}{A^{1/d}d}$ is decreasing on $[A^{1/d}d, +\infty[$. It follows that

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

and, in particular, that $\log(n^{1/d}) \leq \frac{n^{1/d}}{A^{1/d}d} - 1$, for any integer $d \geq 1$ and any integer $n \geq A\left(2d\log(2d) + 2\log(A)\right)^d$. From this inequality and the inequality

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

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

Theorem 5.2. *We use notation 3.1. Let M', M and $1 > \epsilon \geq 0$ be three real numbers such that $d(1-\epsilon) > 1$. Let I be the set of indices $n \in \mathbb{N}$ such that*

$$\begin{aligned} &\widehat{h_\infty}(nP') \leq \epsilon\widehat{h}(nP') + M' \text{ and} \\ &\widehat{h_\infty}(nP) \leq \epsilon\widehat{h}(nP) + M. \end{aligned} \tag{8}$$

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

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

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

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

Proof. The key ingredients are the inequalities (8), which play a role analogous to Roth's theorem in the classical proof of Siegel's theorem.

Let $n \in I$ be an integer such that every prime factor of $B_{nP'}$ divides $B_{P'}$. The decomposition of $\widehat{h}$ into local canonical heights gives

$$n^2\widehat{h}(P') = \widehat{h}(nP') = \widehat{h_\infty}(nP') + \sum_{v(B_{nP'}\Delta_{E'})>0} \widehat{h_v}(nP').$$

This equation, with inequalities (8), implies that

$$(1-\epsilon)n^2\widehat{h}(P') \leq M' + \sum_{v(B_{nP'}\Delta_{E'})>0} \widehat{h_v}(nP'). \tag{9}$$

Using [14, Chapter III, Theorem 4.5], inequality (9) becomes

$$(1-\epsilon)n^2\widehat{h}(P') \leq M' + h(E') + \sum_{v(B_{nP'})>0} \widehat{h_v}(nP') \tag{10}$$

Let v be a place such that $v(B_{nP'}) > 0$. Then our hypothesis on the prime factors of $B_{nP'}$ asserts that $v(B_{P'}) > 0$. In particular P' and nP' have good reduction at v. It follows that $\widehat{h_v}(nP') = h_v(nP') + \frac{v(\Delta_{E'})}{12}$ and $\widehat{h_v}(P') = h_v(P') + \frac{v(\Delta_{E'})}{12}$. Since $v(B_{P'}) > 0$, Lemma 4.2.4 implies that

$$\widehat{h_v}(nP') \leq \widehat{h_v}(P') + 2h_v(n).$$

We deduce from this inequality and inequality (10) that

$$(1-\epsilon)n^2\widehat{h}(P') \leq M' + h(E') + \sum_{v(B_{nP'})>0} \left(\widehat{h_v}(P') + 2h_v(n)\right).$$

Using the inequality $\widehat{h_\infty}(P') \geq 0$ (see [14, Chapter III, Theorem 4.5]), we get

$$(1-\epsilon)n^2\widehat{h}(P') \leq M' + h(E') + \widehat{h}(P') + 2\log(n). \tag{11}$$

If $n \geq 2\log(2)$, applying Lemma 5.1 with $A = 1$, inequality (11) becomes

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

Let $n \in I$ be an integer such that every prime factor of B_{nP} divides $B_{nP'}B_{\sigma(P')}$. The computations above are valid with P' replaced by P and E' by E. We get an analog to inequality (10):

$$(1-\epsilon)n^2\widehat{h}(\sigma(P')) \leq M + h(E) + \sum_{v\left(B_{nP'}B_{\sigma(P')}\right)>0} \widehat{h_v}(n\sigma(P')) \tag{12}$$

Lemma 4.2.4 implies that

$$\sum_{v(B_{nP'})>0} \widehat{h_v}(n\sigma(P')) \leq \left(\sum_{v(B_{nP'})>0} \widehat{h_v}(nP')\right) + \log(d) \leq \widehat{h}(nP') + \log(d)$$

and $\displaystyle\sum_{v\left(B_{\sigma(P')}\right)>0} \widehat{h_v}(n\sigma(P')) \leq \widehat{h}(\sigma(P')) + 2\log(n)$. Thus inequality (12) gives

$$(d - d\epsilon - 1)n^2\widehat{h}(P') \leq M + h(E) + \widehat{h}(\sigma(P')) + 2\log(n) + \log(d). \tag{13}$$

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

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

□

To deduce a uniform bound on the indices of prime power terms in magnified elliptic divisibility sequences from Theorem 5.2, one needs to compare the naive heights $h(E')$ and $h(E)$ of the two isogenous elliptic curves E' and E. Such a comparison follows from the good behaviour of the Faltings height under isogeny.

Proposition 5.3. *We use notation 3.1. Then we have*

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

with $\alpha = 5$ *if* $h(j(E)) > 4$ *and* $\alpha = 16$ *if* $h(j(E)) \leq 4$.

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:

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

When E is a semi-stable elliptic curve, an explicit bound on the difference between the Faltings height $h_{Falt}(E)$ of E and the height $h(j(E))$ can be found in [15]. In the general case, the proof of [15, Lemma 5.2]) gives

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

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

The term $\log\max\{|j(E)\Delta_E|, |\Delta_E|\}$ can be expressed in terms of $h(E)$ using the two inequalities:

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

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

Using Theorem 5.2, many bounds on integer points of 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 [8]: 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 1.2.6.

Let A, B, A', B' be four integers such that E and E' are given by the equations

$$\begin{aligned} E &: y^2 = x^3 + Ax + B, \\ E' &: y^2 = x^3 + A'x + B'. \end{aligned}$$

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

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

which can be rephrased as

$$h(nP') \leq 3M(h(nP') - h_\infty(nP')) + 6Mh(E') + \frac{1}{2}\log(K). \qquad (14)$$

Using the two inequalities $\widehat{h_\infty}(Q) \leq h_\infty(Q) + \frac{h(j(E'))}{12} + 1.07$ and $h(Q) \leq \widehat{h}(Q) + \frac{h(j(E'))}{8} + 1.205$ (proven in [20]) inequality (14) becomes

$$\widehat{h_\infty}(nP') \leq \left(1 - \frac{1}{3M}\right)\widehat{h}(nP') + 4h(E') + \frac{\log(K)}{6M} + 1.88.$$

In the same way we prove that

$$\widehat{h_\infty}(nP) \leq \left(1 - \frac{1}{3M}\right)\widehat{h}(nP) + 4h(E) + \frac{\log(K)}{6M} + 1.88.$$

We apply Theorem 5.2 noting that, if $\deg(\sigma) > 4M$, then $\frac{\log(\deg(\sigma))}{\deg(\sigma)-3M} \leq 4$ and $\frac{h(E')}{\widehat{h}(P')} \leq C$ and $\frac{h(E)}{\widehat{h}(\sigma(P'))} \leq C$ and $\frac{1}{\widehat{h}(P')} \leq \frac{C}{h(E')} \leq \frac{12C}{\log(2)}$. In particular, we get the existence of a function $N : \mathbb{R}^3 \longrightarrow \mathbb{R}^+$ (independent of the choice of (E, P, σ)) such that, if at most one prime factor of $B_{n\sigma(P')}$ divides $B_{P'}$, then $n \leq N\left(M, \log(K), C\right)$.

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

We study Corollary 1.2.6 for two examples of magnified elliptic divisibility sequences:

- first we study the case when P is in the unbounded component of E;
- then we consider the case when P is doubly magnified.

In those two particular cases we prove that Corollary 1.2.6 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 7.1. 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

$$\mathcal{E} : \widetilde{y}^2 = \widetilde{x}^3 + a\widetilde{x} + b \qquad (15)$$

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 (15) is not minimal so $\Delta_\mathcal{E}$ is not the minimal discriminant of $\mathcal{E}$. The heights of $\mathcal{E}$ and E are related by two inequalities $h(E) \leq h(\mathcal{E}) \leq h(E) + \log(6)$. Since

$$\begin{aligned} h(4a^3) = h\left(\tfrac{j(\mathcal{E})\Delta_\mathcal{E}}{16\times 12^3}\right) &= h\left(4 \times 3^9 \times j(\mathcal{E}) \times \Delta_E\right) \\ &\leq h(j(\mathcal{E})) + h(\Delta_E) + 2\log(2) + 9\log(3) \end{aligned}$$

$$\begin{aligned}\text{and } h(27b^2) &= h\left(\tfrac{\Delta_{\mathcal{E}}}{16} - 4a^3\right)\\ &\leq \max\{h(\Delta_E) + 8\log(2) + 12\log(3), h(4a^3)\} + \log(2)\end{aligned}$$

the following inequality holds

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

The left hand side of inequality (16) appears in David's lower bound on linear forms in elliptic logarithms [5, Théorème 2.1], a result used in section 8.

Proposition 7.2. *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 7.1. Denote by $\alpha_1, \alpha_2, \alpha_3$ the three roots of the polynomial $\widetilde{x}^3 + a\widetilde{x} + b$. Following the Cardan Formula, there are two complex numbers u_i, v_i such that $\alpha_i = u_i + v_i$ and

$$\Delta_{\mathcal{E}} = -16 \times 27 \times (b + 2u_i^3)^2 = -16 \times 27 \times (b + 2v_i^3)^2.$$

Since $-16 \times 27b^2 = \frac{(j(\mathcal{E})+1728)\Delta_{\mathcal{E}}}{1728}$ and $\Delta_{\mathcal{E}} = 6^{12}\Delta_E$ and $j(\mathcal{E}) = j(E)$ we have

$$\begin{aligned}2|u_i|^3 \leq |b| + |b + 2u_i^3| &\leq e^{6h(E)+6\log(6)}\left(\tfrac{1}{2^4\times 3^3} + \tfrac{e^{12h(E)}}{2^{10}\times 3^6}\right)^{1/2}\\ &\quad + \tfrac{e^{6h(E)+6\log(6)}}{12\sqrt{3}}\\ &\leq \tfrac{e^{6h(E)+6\log(6)}}{12\sqrt{3}} + \tfrac{e^{12h(E)+6\log(6)}}{864} + \tfrac{e^{6h(E)+6\log(6)}}{12\sqrt{3}}\\ &\leq \tfrac{e^{12h(E)+6\log(6)}}{4\sqrt{3}}.\end{aligned}$$

In the same way, we prove that $|v_i| \leq \frac{e^{4h(E)+2\log(6)}}{2\times 3^{1/6}}$. An upper bound for $|\alpha_i|$ follows: $|\alpha_i| \leq \frac{e^{4h(E)+2\log(6)}}{3^{1/6}}$. 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 [20, 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 $Q \in \mathcal{E}(\mathbb{Q})$. □

Remark 7.3. We keep the notation of the proof. 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.

Now we consider the primality conjecture, for an elliptic divisibility sequence associated to a point 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.

Proposition 7.4. *We use notation 3.1. Let $\tau : E'' \longrightarrow E'$ be an isogeny defined over $\mathbb{Q}$ (with E'' an elliptic curve defined over $\mathbb{Q}$ by a standardized minimal equation), which we allow to be the identity map. If every prime factor of $B_{\sigma(\tau(P'))}$ divides $B_{\tau(P')}$, then*

$$\widehat{h_\infty}(P') \leq 7h(E') + 8 + \log(\deg(\sigma \circ \tau)).$$

Proof. Assume every prime factor of $B_{\sigma(\tau(P'))}$ divides $B_{\tau(P')}$. Let $T_0 \notin \ker(\tau)$ be a $\sigma \circ \tau$-torsion point such that $|x(P') - x(T_0)| \leq |x(P') - x(T)|$, for every $\sigma \circ \tau$-torsion point $T \notin \ker(\tau)$. Since the leading coefficient $d_{\sigma\circ\tau}$ of $\psi_{\sigma\circ\tau}$ is an integer divisible by the leading coefficient d_τ of ψ_τ, we have

$$\left|x(P') - x(T_0)\right|^{\deg(\sigma\circ\tau)-\deg(\tau)} \leq \frac{d_{\sigma\circ\tau}^2}{d_\tau^2} \prod_{T\in\ker(\sigma\circ\tau), T\notin\ker(\tau)} \left|x(P') - x(T)\right| = \frac{\psi_{\sigma\circ\tau}^2(P')}{\psi_\tau^2(P')}.$$

From this inequality, and Proposition 4.2.3, we deduce that

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

Applying Lemma 4.2.4, we get

$$\begin{aligned} |x(P') - x(T_0)|^{(\deg(\sigma)-1)\deg(\tau)} &\leq \deg(\sigma)^2 e^{3\deg(\sigma\circ\tau)h(E')} \\ &\leq e^{2\deg(\sigma)-2} e^{3\deg(\sigma\circ\tau)h(E')} \end{aligned}$$

and, in particular, $|x(P') - x(T_0)| \leq e^{2+6h(E')}$. The triangle inequality gives

$$|x(P')| \leq 2\max\left\{|x(T_0)|, e^{2+6h(E')}\right\}. \tag{17}$$

Let $\mathcal{E}'$ be the model for E' deduced from the change of variable $(\widetilde{x}, \widetilde{y}) = (36x + 3a_1^2 + 12a_2, 216y + 108a_1x + 108a_3)$; this is also the model for E' considered in notation 7.1. Now inequality (16) and [5, Lemme 10.1] give

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

It follows from inequality (17) and [20, Theorem 5.5] that

$$\widehat{h_\infty}(P') \leq h_\infty(P') + h(E') + \frac{1}{2}\log(2) + 1.07 \leq 7h(E') + 8 + \log(\deg(\sigma\circ\tau)).$$

(Note that [20, Theorem 5.5] is applied to a standardized equation and that $h_\infty(P') = \frac{1}{2}\log\max\{1, |x(P')|\}$.) □

Corollary 7.5. *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 $\mathbb{Q}$. 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 two distinct prime factors coprime to $B_{P'}$. Then, for each index i, we have*

$$\begin{aligned} \textit{either} \quad & \sqrt{\deg(\tau_i)} \leq \tfrac{2}{\sqrt{\widehat{h}(P')}} \log\left(\tfrac{2}{\sqrt{\widehat{h}(P')}}\right), \\ \textit{or} \quad & \sqrt{\deg(\tau_i)} \leq \tfrac{144}{\sqrt{\widehat{h}(P')}} + 2\sqrt{1 + \tfrac{128h(E_0)+135}{\widehat{h}(P')}}. \end{aligned}$$

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 4.1.5 for details), we can assume without loss of generality that $d_1 \geq \max\{d_2, d_3\}$.

Assume, for now, that l divides $B_{\tau_1(P')}$. Following Lemma 4.2.4, 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 $\log(d_3) \leq \log(d_1)$, Proposition 7.4 gives

$$\widehat{h_\infty}\left((\tau_2 \circ \tau_1)(P')\right) \leq 7h(E_2) + 8 + \log(d_1).$$

Each prime factor of $B_{(\tau_2\circ\tau_1)(P')}$ divides $B_{\tau_1(P')}$. In particular, the following analog to inequality (13) holds:

$$\frac{d_1 d_2 \widehat{h}(P')}{4} \leq (d_2-1)(d_1-1)\widehat{h}(P') \leq 8h(E_2) + 8 + \log(d_1) + \log(d_2) + \widehat{h}(P').$$

Following Proposition 5.3, this inequality implies that

$$d_1 d_2 \widehat{h}(P') \leq 4 \times \left(128h(E_0) + 135 + 9\log(d_1 d_2) + \widehat{h}(P')\right).$$

Applying Lemma 5.1 with $n = \sqrt{d_1 d_2}$ and $A = \frac{1}{\sqrt{\widehat{h}(P')}}$, we get that either $\sqrt{d_1 d_2} \leq \frac{2}{\sqrt{\widehat{h}(P')}} \log\left(\frac{2}{\sqrt{\widehat{h}(P')}}\right)$ or $\sqrt{d_1 d_2} \leq \frac{144}{\sqrt{\widehat{h}(P')}} + 2\sqrt{1 + \frac{128h(E_0)+135}{\widehat{h}(P')}}$.

Assume now that l does not divide $B_{\tau_1(P')}$. 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, since $\log(d_2) \leq \log(d_1)$, Proposition 7.4 gives

$$\widehat{h_\infty}\left(\tau_1(P')\right) \leq 7h(E_1) + 8 + \log(d_1).$$

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, since $\log(d_2 d_3) \leq 2\log(d_1)$, Proposition 7.4 (applied with $\sigma := \tau_3$ and $\tau := \tau_2$) gives

$$\widehat{h_\infty}\left(\tau_1(P')\right) \leq 7h(E_1) + 8 + 2\log(d_1).$$

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, the following analog to inequality (11) follows, using Proposition 5.3:

$$d_1 \widehat{h}(P') \leq 128h(E_0) + 135 + 10\log(d_1) + \widehat{h}(P').$$

Applying Lemma 5.1 with $n = \sqrt{d_1}$ and $A = \frac{1}{\sqrt{\widehat{h}(P')}}$, we get that either $\sqrt{d_1} \leq \frac{2}{\sqrt{\widehat{h}(P')}} \log\left(\frac{2}{\sqrt{\widehat{h}(P')}}\right)$ or $\sqrt{d_1} \leq \frac{20}{\sqrt{\widehat{h}(P')}} + \sqrt{1 + \frac{128h(E_0)+135}{\widehat{h}(P')}}$. □

Corollary 7.6. *We use notation 3.1. 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*

$$\begin{aligned} \textit{either} \quad & n > \frac{4}{\sqrt{\widehat{h}(P')}} \log\left(\frac{2}{\sqrt{\widehat{h}(P')}}\right) \\ \textit{or} \quad & n > \frac{288}{\sqrt{\widehat{h}(P')}} + 4\sqrt{1 + \frac{128h(E')+135}{\widehat{h}(P')}}. \end{aligned}$$

Proof. When n is even, Corollary 7.6 follows from Corollary 7.5 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. Since $\deg(\sigma) \geq 3$, applying Proposition 7.2, we get two analogs to inequalities (11) and (13):

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

if every prime factor of $B_{nP'}$ divides $B_{P'}$, and (using Proposition 5.3)

$$\begin{aligned} n^2(\deg(\sigma) - 1)\widehat{h}(P') &\leq 4h(E) + \widehat{h}(\sigma(P')) + \log(6) + 1.07 + \log(n^2\deg(\sigma)) \\ &\leq 128h(E') + \widehat{h}(\sigma(P')) + 67 + 5\log(\deg(\sigma)) + 2\log(n), \end{aligned}$$

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

8. Elliptic divisibility sequences and linear forms in elliptic logarithms.

Since no effective version of Siegel's theorem 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 non-uniform bound can be computed using work of David on lower bounds for linear forms in elliptic logarithms.

Notation 8.0.1. *We use notation 7.1. We consider the map ϕ defined on the unbounded component $\mathcal{E}(\mathbb{R})_0$ of $\mathcal{E}$ by the formula*

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

The map ϕ is linked to the archimedean height by the following inequality (see [23, section 3, Inequality 2]*): for every point $P \in \mathcal{E}(\mathbb{R})_0$, we have*

$$-\log|\phi(P)| - \frac{1}{2}\log(2) \leq h_\infty(P) \leq -\log|\phi(P)| + \frac{5}{2}\log(2). \qquad (18)$$

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 8.0.1. We apply [5, Théorème 2.1] to the curve $\mathcal{E}$ with $k = 2$, $D \leq 3$, $E = e$, $\gamma_1 = P$, $\gamma_2 = T_0$,

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

(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

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

(note that $|m| \leq |n|$). This gives the inequality

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

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

- we do not use the same definition for $\widehat{h}$ as in [5];

- 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 [5]; inequality (16) gives an upper bound on h that is linear in $h(E)$ (see notation 7.1).

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 (18) that

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

We conclude by using [20, Theorem 5.5]. □

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

Proposition 8.2.1. *We use notation 3.1. Then $B_{nP'}$ has a prime factor coprime to $B_{P'}$ for every index*

$$n > \max\left\{2.1 \times 10^{30}, \frac{4.3 \times 10^{27}}{\widehat{h}(P')}, 8.7 \times 10^{23}\widehat{h}(P')^{5/2}, \frac{2 \times 10^{27} h(E')^{7/2}}{\widehat{h}(P')}\right\},$$

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

$$n > \max\left\{4.2 \times 10^{30}, \frac{4.3 \times 10^{27}}{\widehat{h}(P')}, 1.7 \times 10^{24}\widehat{h}(\sigma(P'))^{5/2}, \frac{4 \times 10^{27} h(E)^{7/2}}{\widehat{h}(\sigma(P'))}\right\}.$$

Proof. Let $n \in \mathbb{N}$ be such that $B_{nP'}$ has no prime factor coprime to $B_{P'}$. Lemma 8.1.1 (applied with $b' := \max\left\{2\widehat{h}(P'); 12eh(E') + 5e\log(6)\right\}$) asserts that either $\widehat{h_\infty}(nP') \leq 5.9 \times 10^{43} \times (b' + 2.1)^6 + h(E') + 2.81$ or $\log|2n| > b'$. We assume for now that $\log|2n| \leq b'$. Applying Theorem 5.2 we get that

$$\begin{aligned} n &\leq \frac{2}{\widehat{h}(P')} + \sqrt{\frac{5.9\times10^{43}(b'+2.1)^6 + 2h(E') + \widehat{h}(P') + 2.81}{\widehat{h}(P')}} \\ &\leq \frac{2 + \sqrt{5.91\times10^{43}(b'+2.1)^7}}{\widehat{h}(P')} \\ &\leq \frac{8.7\times10^{21}\left(\max\left\{\widehat{h}(P') + 1.05, 17h(E') + 14\right\}\right)^{7/2}}{\widehat{h}(P')} \\ &\leq \frac{8.7\times10^{21}\left(\max\left\{2\widehat{h}(P'), 34h(E'), 28\right\}\right)^{7/2}}{\widehat{h}(P')}. \end{aligned}$$

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

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

Applying Lemma 5.1

- with $A = 10^{18}$ and $d = 6$ when $n^2\widehat{h}(P') \leq 11,8 \times 10^{43}(\log|6n|+1)^6$,
- with $A = 4d = 4$ when $n^2\widehat{h}(P') \leq 4\log(n) + 2\widehat{h}(P') + 4h(E') + 5.62$,

we get that either

$$\begin{aligned} n &\leq \max\left\{2.06\times 10^{30}, \tfrac{4.3\times 10^{27}}{\widehat{h}(P')}\right\} \\ \text{or}\quad n &\leq \max\left\{16.7, \tfrac{1}{\widehat{h}(P')} + \sqrt{2 + \tfrac{5.62}{\widehat{h}(P')} + \tfrac{4h(E')}{\widehat{h}(P')}}\right\} \\ &\leq \max\left\{16.7, \left(1+\sqrt{3}\right)\max\left\{\tfrac{1}{\widehat{h}(P')}, \sqrt{2}, \sqrt{\tfrac{5.62}{\widehat{h}(P')}}, 2\sqrt{\tfrac{h(E')}{\widehat{h}(P')}}\right\}\right\} \end{aligned}$$

In the same way, we prove that

$$\begin{aligned} \text{either}\quad n &\leq \frac{1.8\times 10^{22}\left(\max\left\{2\widehat{h}(\sigma(P')), 34h(E), 28\right\}\right)^{5/2}}{\widehat{h}(\sigma(P'))} \\ \text{or}\quad n &\leq \max\left\{4.2\times 10^{30}, \tfrac{8.6\times 10^{27}}{\widehat{h}(\sigma(P'))}\right\} \\ \text{or}\quad n &\leq \max\left\{16.7, \tfrac{1}{(\deg(\sigma)-1)\widehat{h}(P')} + \sqrt{4 + \tfrac{5.62+2\log(\deg(\sigma))}{(\deg(\sigma)-1)\widehat{h}(P')} + \tfrac{8h(E)}{\widehat{h}(\sigma(P'))}}\right\} \\ &\leq \max\left\{16.7, \left(1+\sqrt{3}\right)\max\left\{\tfrac{2}{\widehat{h}(\sigma(P'))}, \sqrt{\tfrac{7.62}{\widehat{h}(P')}}, \sqrt{\tfrac{8h(E)}{\widehat{h}(\sigma(P'))}}\right\}\right\}, \end{aligned}$$

whenever $B_{n\sigma(P')}$ has no prime factor coprime to $B_{nP'}$. □

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. As explained for example in [24], the bound $M(B)$ can be reduced applying the LLL algorithm or Mumford's gap principle.

Notation 8.3.1. *We use notation 3.1. Following notation 8.0.1 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*

$$n > \max\left\{8, \frac{2}{\widehat{h}(P')} + \sqrt{3 + \max\left\{\frac{5h(E')}{\widehat{h}(P')}, \frac{9h(E)}{\widehat{h}(P)}\right\} + \frac{7}{\widehat{h}(P')}}\right\}.$$

be such that $B_{n\sigma(P')}$ has at most one prime factor coprime to $B_{P'}$.

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

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

Proof. When $|x(nR')| \leq 2\max\{|x(T)| : T \in \mathcal{E}'[2]\}$, Lemma 7.2 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 5.2 implies that, if every prime factor of $B_{nP'}$ divides $B_{P'}$ and $n > \frac{2}{\widehat{h}(P')} + \sqrt{1 + \frac{4h(E')+3.21}{\widehat{h}(P')}}$, then $|x(nR')| \geq 2\max\{|x(T)| : T \in \mathcal{E}'[2]\}$; this implies that $R' \in \mathcal{E}'(\mathbb{R})_0$.

In the same way, since $n > \frac{2}{\widehat{h}(P')} + \sqrt{2 + \frac{8h(E)}{\widehat{h}(P)} + \frac{4.21}{\widehat{h}(P')}}$, we deduce from Theorem 5.2 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, $R \in \mathcal{E}(\mathbb{R})_0$.

Assume that $|x(nR')| \geq 2\max\{|x(T)| : T \in \mathcal{E}'[2]\}$ and $n\phi_{\mathcal{E}'}(R') \neq \phi_{\mathcal{E}'}(nR')$ Then inequality (18) 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 [20, 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 [20, Theorem 5.5] to $\widehat{h_\infty}(nP') = \widehat{h_\infty}(nR')$ we get

$$\widehat{h_\infty}(nP') + \log(n) \leq \widehat{h}(P') + \frac{7}{2}h(E') + 2\log(6) + 3\log(2) + 2.043. \quad (19)$$

If every prime factor of $B_{nP'}$ divides $B_{P'}$ and $n\phi_{\mathcal{E}'}(R') \neq \phi_{\mathcal{E}'}(nR')$ and $3\log(2) \leq \log(n)$, then it follows from inequality (19) and Theorem 5.2 that $n \leq \frac{2}{\widehat{h}(P')} + \sqrt{2 + \frac{5h(E')+6}{\widehat{h}(P')}}$. The proof of inequality (19) 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 $n\phi_{\mathcal{E}}(R) \neq \phi_{\mathcal{E}}(nR)$ and $3\log(2) \leq \log(n)$, then $n \leq \frac{2}{\widehat{h}(P')} + \sqrt{3 + \frac{9h(E')}{\widehat{h}(P)} + \frac{7}{\widehat{h}(P')}}$. □

Proposition 8.3.3. *We use notation 3.1 and we assume that E and E' are given by minimal Weierstrass equations. Let $n_3 > n_2 > n_1 > 8$ be three pairwise coprime integers with*

$$n_3 > n_2 > n_1 > \frac{2}{\widehat{h}(P')} + \sqrt{3 + \max\left\{\frac{5h(E')}{\widehat{h}(P')}, \frac{9h(E)}{\widehat{h}(P)}\right\} + \frac{7}{\widehat{h}(P')}}$$

such that B_{n_iP} has at most one prime factor coprime to $B_{P'}$. Then we have

$$\begin{aligned} \textit{either} \quad & n_1 \leq \tfrac{2}{\widehat{h}(P')} + \sqrt{2 + \tfrac{2\log(n_3)+52h(E)}{\widehat{h}(\sigma(P'))} + \tfrac{24.42}{\widehat{h}(P')}} \\ \textit{or} \quad & n_1 \leq \tfrac{2}{\widehat{h}(P')} + \sqrt{1 + \tfrac{\log(n_i)+26h(E')+23.42}{\widehat{h}(P')}}, \end{aligned}$$

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

Proof. 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

$$\begin{aligned} \phi_{\mathcal{E}'}(n_iP') &= n_i\phi_{\mathcal{E}'}(P') + 2m_i\phi_{\mathcal{E}'}(T_0) \\ \text{and} \quad \phi_{\mathcal{E}'}(n_jP') &= n_j\phi_{\mathcal{E}'}(P') + 2m_j\phi_{\mathcal{E}'}(T_0). \end{aligned}$$

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 $|m_i| < |n_i|$. However 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

$$\begin{aligned} 2\left|\phi_{\mathcal{E}'}(T_0)\right| &\leq 2\left|\phi_{\mathcal{E}'}(T_0)\right| |n_jm_i - n_im_j| \\ &\leq \left|n_j\phi_{\mathcal{E}'}(n_iP') - n_i\phi_{\mathcal{E}'}(n_jP')\right| \\ &\leq 2\max\left\{|n_j|\left|\phi_{\mathcal{E}'}(n_iP')\right|, |n_i|\left|\phi_{\mathcal{E}'}(n_jP')\right|\right\}. \end{aligned} \tag{20}$$

We deduce from inequality (18) and inequality (20) that

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

Applying [15, Lemme 2.1] and inequality (16), we get

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

Theorem 5.2 and [20, Theorem 5.5] show that

$$n_1 \leq \min\{n_i, n_j\} \leq \frac{2}{\widehat{h}(P')} + \sqrt{1 + \frac{\log\left(\max\{n_i, n_j\}\right) + 26h(E') + 23.42}{\widehat{h}(P')}}.$$

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

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

From this inequality, Theorem 5.2, and [20, Theorem 5.5], we deduce that

$$n_1 \leq \frac{2}{\widehat{h}(P')} + \sqrt{2+\frac{2\log(n_3)+52h(E)}{\widehat{h}(\sigma(P'))}+\frac{23.42}{\widehat{h}(P')}+\frac{\log(d)}{(d-1)\widehat{h}(P')}}$$

(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 5.3. 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 $h(E') \geq \frac{1}{12}\log(2)$ implies that

$$\frac{2}{\widehat{h}(\sigma(P'))} \leq \frac{1}{\widehat{h}(P')} \leq \frac{12\Gamma}{\log(2)} \leq 17.32\times\Gamma.$$

Let n be an integer such that at most one prime factor $B_{n\sigma(P')}$ is not a prime factor of $B_{P'}$. If $n=n_1n_2$ with $n_1 \geq n_2 > 1$, then Corollary 7.5 implies that either $n \leq n_1^2 \leq \frac{4}{\widehat{h}(P')}\left(\frac{1}{2}\log\left(\frac{4}{\widehat{h}(P')}\right)\right)^2 \leq 18\Gamma\left(\log(70\Gamma)\right)^2$ or

$$n \leq n_1^2 \leq \left(\frac{144}{\sqrt{\widehat{h}(P')}}+2\sqrt{1+\frac{128h(E')+135}{\widehat{h}(P')}}\right)^2 \leq 490000\Gamma$$

Proposition 8.2.1 asserts that

$$N_1 \leq \max\left\{4.2\times10^{30}\Gamma, 1.7\times10^{24}\widehat{h}(\sigma(P'))^{5/2}, 4\times10^{27}\Gamma^{7/2}\widehat{h}(\sigma(P'))^{5/2}\right\}.$$

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

$$\frac{\log(N_1)}{\widehat{h}(\sigma(P'))} \leq 600\Gamma + 31\Gamma\log(\Gamma)+\frac{5}{2}. \tag{21}$$

Noticing that $\frac{2}{\widehat{h}(P')}+\sqrt{3+\max\left\{\frac{5h(E')}{\widehat{h}(P')},\frac{9h(E)}{\widehat{h}(P)}\right\}+\frac{7}{\widehat{h}(P')}} \leq 47\Gamma$, we deduce from Proposition 8.3.3 and inequality (21) that either $N_3 \leq 47\Gamma$

$$\text{or} \quad N_3 \leq \frac{2}{\widehat{h}(P')}+\sqrt{2+\frac{2\log(N_1)+52h(E)}{\widehat{h}(\sigma(P'))}+\frac{24.42}{\widehat{h}(P')}} \leq 77\Gamma$$

$$\text{or} \qquad N_3 \leq \frac{2}{\widehat{h}(P')}+\sqrt{1+\frac{\log(N_i)+26h(E')+23.42}{\widehat{h}(P')}}, \tag{22}$$

for some $i \in \{1,2\}$ such that every prime factor of $B_{N_i P'}$ divides $B_{P'}$. When inequality (22) holds, Proposition 8.2.1 gives $\frac{\log(N_i)}{\widehat{h}(P')} \leq 1202\Gamma + 62\Gamma\log(\Gamma)$. In that case inequality (22) implies that $N_3 \leq 77\Gamma$.

9. Elliptic curves with j-invariant 1728.

In this section we compute the bound from Corollary 7.6 in the particular case of an elliptic curve E_A defined by a Weierstrass equation

$$E_A : y^2 = x(x^2 - A), \tag{23}$$

where A denotes a positive integer with no valuation greater than 3. 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 (23) (see Notation 1.1.1). This sequence $(B_{nP})_{n\in\mathbb{N}}$ might not be normalized: equation (23) is not be minimal in general.

For congruent number curves our results can be deduced from results on integer points on E_{N^2}. In the case $A \notin \mathbb{Q}^{\times 2}$, the main issue is to get the following explicit version of Lang's conjecture. (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 unbounded connected component of $E_A(\mathbb{R})$. Denote by $\widehat{h}_A$ the canonical height on E_A. Then*

$$\widehat{h}_A(P) \geq \frac{1}{16}\log|2A|. \tag{24}$$

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

$$\widehat{h}_A(P) \geq \frac{1}{64}\log|2A|. \tag{25}$$

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

$$-\frac{1}{4}\log|A| - \frac{3}{8}\log(2) \leq \widehat{h}_A(P) - \frac{1}{4}\log|A_P^2 + AB_P^4| \leq \frac{1}{12}\log(2) \tag{26}$$

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

$$0 \leq \widehat{h}_\infty(P) - \frac{1}{4}\log|x(P)^2 + A| + \frac{1}{12}\log(\Delta_A) \leq \frac{1}{12}\log(2). \tag{27}$$

Non-archimedean canonical heights are computed using the algorithm presented in [19]. 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

$$-\tfrac{v(A)}{4} \leq \widehat{h_v}(P) - \tfrac{1}{2}\max\{0, -v(x(P))\} - \tfrac{v(\Delta_A)}{12} \leq 0. \tag{28}$$

(The only technical issue 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 [19] gives

$$-\frac{v_2(A)}{4} - \frac{3}{8}\log(2) \leq \widehat{h_2}(P) - \frac{1}{2}\max\{0, -v_2(x(P))\} - \frac{v_2(\Delta_A)}{12} \leq 0. \tag{29}$$

We compute the canonical height by summing local canonical heights. Doing so inequality (26)) becomes a consequence of inequalities (27), (28) and (29).

Now we prove the two inequalities (24) and (25). When $Q \in E_A(\mathbb{Q})$ has good reduction everywherewe we have

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

Adding this equation and the inequality (27) we get

$$\widehat{h}_A(Q) \geq \frac{1}{4}\log|A_Q^2 + AB_Q^4|. \tag{30}$$

If Q is a point in the unbounded real connected component of E_A, then $|A_Q| = |x(Q)|B_Q^2 \geq \sqrt{|A|}B_Q^2 \geq \sqrt{|A|}$. Inequality (30) becomes

$$\widehat{h}_A(Q) \geq \frac{1}{4}\log|2A|. \tag{31}$$

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 (24) and (25) follow from inequality (31) 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 (26) gives:

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

Using inequalities (24) and (25) 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 (26) gives:

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

Using inequalities (24) and (25) 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 $B_{nP} = B_{nmP'}$ 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

$$n^2\widehat{h}_A(P') \leq \log(B_{nP'}) + \frac{1}{4}\log(2A) + \frac{1}{12}\log(2) \text{ and} \tag{32}$$

$$m^2n^2\widehat{h}_A(P') \leq \log(B_{nP}) + \frac{1}{4}\log(2A) + \frac{1}{12}\log(2). \tag{33}$$

Equation (32) 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 [8, Lemma 2.3] implies that B_{nP} divides $m^2B_{nP'}$. As a consequence, equation (33) 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 (26), 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 (24) and (25) 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] M. Ayad, *Points S-entiers des courbes elliptiques*, Manuscripta Math. **76** (1992), 305–324.

[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(2):187–208, 2000.

[3] Cheon, J.; Hahn, S, *Explicit valuations of division polynomials of an elliptic curve.* Manuscripta Math. **97** (1998), no. 3, 319–328.

[4] C. Corrales-Rodrigáñez, R. Schoof. The support problem and its elliptic analogue *J. Number Theory*, 64(2):276–290, 1997.

[5] S. David, Minorations de formes linéaires de logarithmes elliptiques. *Mém. Soc. Math. France (N.S.) No. 62 (1995).*

[6] M. Einsiedler, G. Everest and T. Ward, *Primes in elliptic divisibility sequences,* LMS J. Comp. Math. 4 (2001), 1–13.

[7] K. Eisentraeger and G. Everest, *Descent on elliptic curves and Hilbert's tenth problem*, Proc. Amer. Math. Soc. 137 (2009), 1951–1959.

[8] G. Everest, P. Ingram, V. Mahé, S. Stevens *The uniform primality conjecture for elliptic curves,* Acta Arith. 134(2): 157–181, 2008.

[9] G. Everest, V. Miller and N. Stephens, *Primes generated by elliptic curves,*. Proc. Amer. Math. Soc. 132 (2004), 955–963.

[10] G. Everest and T. Ward, *Heights of Polynomials and Entropy in Algebraic Dynamics,* Springer, London, 1999

[11] M. Hindry and J. Silverman *The canonical height and integral points on elliptic curves,* Invent. Math. 93, No.2, (1998), 419–450.

[12] P. Ingram, *Multiples of integral points on elliptic curves*, J. Number Theory 129 (2009), 182–208.

[13] B. Mazur ; J. Tate, The p-adic sigma function. *Duke Math. J. 62 (3), 663–688, (1991).*

[14] S. Lang *Elliptic Curves Diophantine Analysis* Springer-Verlag, Grundlehren der mathematischen Wissenschaften,volume 231, Berlin-Heidelberg, 1978

[15] F. Pellarin *Sur une majoration explicite pour un degré d'isogénie liant deux courbes elliptiques.* Acta Arith., 100(3): 203–243, 2001.

[16] C. Petsche *Small rational points on elliptic curves over number fields.* New York J. Math., 12 (2006), 257–268.

[17] B. Poonen *Hilbert's tenth problem and Mazur's conjecture for large subrings of* $\mathbb{Q}$. J. Amer. Math. Soc. 16 No.4 (2003), 981–990.

[18] J. H. Silverman, *The Arithmetic of Elliptic Curves,* Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1986.
[19] J. H. Silverman. Computing heights on elliptic curves. *Math. Comp.*, 51(183):339–358, 1988.
[20] J. H. Silverman. The difference between the Weil height and the canonical height on elliptic curves. *Math. Comp.*, 55(192):723–743, 1990.
[21] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves,* Graduate Texts in Mathematics 151, Springer-Verlag, New York, 1994.
[22] M. Streng, Divisibility sequences for elliptic curves with complex multiplication. Algebra Number Theory 2 (2008), no. 2, 183–208.
[23] R. L. Stroeker and N. Tzanakis *Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithm.* Acta Arith., 67(2): 177-196, 1994.
[24] N. Tzanakis and B. M. M. de Weger How to explicitly solve a Thue-Mahler equation. Compositio Math. 84 (1992), no. 3, 223–288.
[25] J. Vélu *Isogénies entre courbes elliptiques* C. R. Acad. Sc. Paris, 273 (1971), 238-241.
[26] S. S. Wagstaff, Divisors of Mersenne numbers. *Math. Comp.*, 40:385–397, 1983.
[27] M. Ward. *Memoir on elliptic divisibility sequences.* Amer. J. Math., 70 (1948), 31–74.

Université de Franche-Comté, 16 route de Gray, 25000 Besançon.
E-mail address: valery.mahe@univ-fcomte.fr