ACTA ARITHMETICA
Online First version

Bogomolov property of some infinite nonabelian extensions of a totally v-adic field

by

Arnaud Plessis (Beijing)

Abstract. Let E be an elliptic curve defined over a number field K, and let v be a finite place of K. Write K^{tv} for the maximal totally v-adic field, and denote by L the field generated over K^{tv} by all torsion points of E. Under some conditions, we will show that the absolute logarithmic Weil height (resp. Néron–Tate height) of any element of L (resp. $E(L)$) is either 0 or bounded from below by a positive constant depending only on E, K and v. This constant will be explicit in the toric case.

1. Introduction. Let $h : \overline{\mathbb{Q}} \to \mathbb{R}$ denote the (absolute, logarithmic) Weil height. It is a non-negative function vanishing precisely at μ_∞, the set of all roots of unity, and 0 by a theorem of Kronecker. It satisfies $h(\alpha^n) = |n|h(\alpha)$ and $h(\zeta\alpha) = h(\alpha)$ for all $\alpha \in \overline{\mathbb{Q}}$, $\zeta \in \mu_\infty$ and all $n \in \mathbb{Z}$ as well as the inequality $h(\alpha\beta) \leq h(\alpha) + h(\beta)$ for all $\alpha, \beta \in \overline{\mathbb{Q}}$. For further information on this height, we refer to [7].

Given a field $K \subset \overline{\mathbb{Q}}$, an interesting question is whether there exists a positive constant c such that $h(\alpha) \geq c$ for all non-zero $\alpha \in K \setminus \mu_\infty$. Such a field is said to have the Bogomolov property. This notion was introduced by Bombieri and Zannier [8]. The field $\overline{\mathbb{Q}}$ does not have the Bogomolov property since $h(2^{1/n}) = (\log 2)/n \to 0$.

By Northcott's theorem, each number field has the Bogomolov property. Schinzel gave the first example of an infinite extension of $\mathbb{Q}$ having the Bogomolov property [28], namely the maximal totally real field extension $\mathbb{Q}^{tr}$ of $\mathbb{Q}$. The p-adic version of this theorem was proved by Bombieri and Zannier [8]. More precisely, they proved that the maximal totally p-adic extension $\mathbb{Q}^{tp}$ of $\mathbb{Q}$ has the Bogomolov property.

In recent years, the study of this property mushroomed; see for example [2, 3, 19, 1, 18, 13, 17, 14, 24, 23].

2020 *Mathematics Subject Classification*: Primary 11G50; Secondary 11G05.
Key words and phrases: Diophantine geometry, elliptic curves, Bogomolov property.
Received 16 February 2022; revised 24 April 2023.
Published online 3 April 2024.

DOI: 10.4064/aa220216-31-1

The study of this property is not limited to this situation and we can easily define it for abelian varieties. Let A be an abelian variety defined over a number field K, and let $\mathcal{L}$ be a symmetric ample line bundle on A/K. Let $\hat{h}_A : A(\overline{K}) \to \mathbb{R}$ denote the Néron–Tate height attached to $\mathcal{L}$. It is a non-negative function vanishing precisely at A_{tors}, the group of torsion points of A. Again, given a field $L \subset \overline{K}$, the group $A(L)$ is said to have the Bogomolov property (with respect to $\mathcal{L}$) if there exists a positive constant c such that $\hat{h}_A(P) \geq c$ for all $P \in A(L)\backslash A_{\mathrm{tors}}$. It is well-known that $A(\overline{K})$ does not have the Bogomolov property.

Northcott's theorem cited above also states that $A(L)$ has the Bogomolov property if L is a number field. Zhang showed the abelian analogue of Schinzel's theorem, that is, $A(\mathbb{Q}^{tr})$ has the Bogomolov property [34]. Later, Baker and Petsche proved that $A(\mathbb{Q}^{tp})$ has the Bogomolov property when $p > 2$ and $A/\mathbb{Q}$ is an elliptic curve with semistable reduction at p [5, Theorem 6.6]. For more examples concerning the Bogomolov property in the case of an abelian variety, see [6, 23] (which handle the case of any abelian variety) and [4, 32, 19, 26, 25] (which treat the special case of an elliptic curve).

A very special case of a recent conjecture due to the author predicts the following.

Conjecture 1.1 ([25, Conjecture 1.4]). *Let A be an abelian variety defined over a number field K, let $\mathcal{L}$ be a symmetric ample line bundle on A/K, and let L/K be a finite extension. Then $L(A_{\mathrm{tors}})$ and $A(L(A_{\mathrm{tors}}))$ have the Bogomolov property.*

Remark 1.2. The abelian part of this conjecture is due to David.

Conjecture 1.1 was proved to be true when A has complex multiplication (CM). More precisely, the toric part is due to Amoroso, David and Zannier [1] (see Theorem 1.9 below for a more general statement) and the abelian part was proved by Baker and Silverman [6, Section 9]; see also [9, Théorème 1.8].

The case where A has no CM is much harder. To my knowledge, Habegger was the first one to provide a result going in the direction of Conjecture 1.1.

Theorem 1.3 (Habegger, [19]). *Let $E/\mathbb{Q}$ be an elliptic curve. Then $\mathbb{Q}(E_{\mathrm{tors}})$ and $E(\mathbb{Q}(E_{\mathrm{tors}}))$ have the Bogomolov property.*

For any elliptic curve E and any integer $N \in \mathbb{N} = \{1, 2, \dots\}$, write $E[N]$ for the group of N-torsion points of E and define j_E to be the j-invariant of E.

Set $\mathrm{Mat}_2(A)$ to be the ring of 2×2 matrices whose coefficients lie in a ring A. The set of its invertible elements is denoted by $\mathrm{GL}_2(A)$. Define $\mathrm{SL}_2(A)$ as the kernel of the determinant map $\mathrm{GL}_2(A) \to A^*$ (here, A^* is the set of invertible elements in A).

Given a number field K, a finite place v of K and an algebraic extension L/K, we say that L *has bounded local degree* at v if $d_v(L) = \sup_w [L_w : K_v]$ is finite, where w ranges over all extensions of v to L. In that case, we denote by $e_w(L|K)$ (resp. $f_w(L|K)$) the ramification index (resp. inertia degree) of the extension $w|v$. Finally, we define K^{tv} as the maximal totally v-adic field, that is, the set of $\alpha \in \overline{K}$ such that v is totally split in $K(\alpha)$. It is Galois over K and $d_v(K^{tv}) = 1$.

Recently, Frey pointed out a quite remarkable fact: Conjecture 1.1 may be true for some infinite extensions L/K.

THEOREM 1.4 (Frey, [16, Theorem 7.1]). *Let $E/\mathbb{Q}$ be a non-CM elliptic curve, and let $L/\mathbb{Q}$ be a Galois extension such that the exponent $\exp(L)$ of its Galois group is finite. Then there exists a rational prime p satisfying:*

(a) *E has supersingular reduction at p and $j_E \not\equiv 0, 1728$ (p);*
(b) *the natural representation $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is surjective;*
(c) *$p \geq \max\{2\sup_q d_q(L)+2, \exp(L)\}$, where q runs over all rational primes,*

and for such a p, for all $\alpha \in L(E_{\mathrm{tors}})^* \setminus \mu_\infty$ we have

$$h(\alpha) \geq \frac{(\log p)^4}{p^{5p^4}}.$$

REMARK 1.5. By a theorem of Checcoli [10, Theorem 1], if $L/\mathbb{Q}$ is Galois, then the exponent of its Galois group is finite if and only if $\sup_q d_q(L)$ is finite, where q ranges over all rational primes. So item (c) makes sense here.

The main goal of this paper is to establish that Conjecture 1.1 is true for some Galois extensions L/K whose Galois group has infinite exponent.

THEOREM 1.6. *Let E be an elliptic curve defined over a number field K, and let L/K be a finite Galois extension. If there is a finite place v of K satisfying:*

(a) *E has supersingular reduction at v and $j_E \not\equiv 0, 1728$ (v);*
(b) *the image of the natural representation $\mathrm{Gal}(L(E[p])/L) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ contains $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, where $p\mathbb{Z} = v \cap \mathbb{Z}$;*
(c) *$p > \max\{3, 2d_v(L)\}$;*
(d) *$e_v(K|\mathbb{Q}) = 1$ and $f_v(K|\mathbb{Q}) \leq 2$,*

then for all $\alpha \in LK^{tv}(E_{\mathrm{tors}})^* \setminus \mu_\infty$, we have

$$h(\alpha) \geq \frac{1}{4^{p^2 d_v(L)} + 1} \left(\frac{\log p}{d_v(L)(40\sqrt{2}+2)[K:\mathbb{Q}]p^{2p^2 d_v(L)+2}} \right)^{2+\frac{4}{p^{p^2 d_v(L)/4}-2}}.$$

Moreover, if v is unramified in L and if the natural representation in (b) *is surjective, then $E(LK^{tv}(E_{\mathrm{tors}}))$ has the Bogomolov property.*

Remark 1.7. (1) Lemma 5.10 prevents us from providing an explicit lower bound of the Néron–Tate height for points lying in $E(LK^{tv}(E_{\mathrm{tors}}))$.

(2) Assume that $K = \mathbb{Q}(\sqrt{D})$ with $D \in \mathbb{N}$ and that E/K has no CM. Then (a) is satisfied for infinitely many places by Elkies' thesis [12]. The natural representation in (b) is surjective for all but finitely many rational primes by Serre's open image theorem [30]. Item (c) holds for all p large enough since $d_v(L) \leq [L : K]$. Finally, all but finitely many finite places of K are unramified in L and satisfy (d). So we can find a place v of K satisfying all conditions of Theorem 1.6. Thus $LK^{tv}(E_{\mathrm{tors}})$ and $E(LK^{tv}(E_{\mathrm{tors}}))$ have the Bogomolov property. In particular, Conjecture 1.1 is true for elliptic curves defined over a real quadratic field.

Nonetheless, Theorem 1.6 does not permit us to treat the case $D < 0$ in full generality. For example, we do not know so far if the elliptic curve

$$E : iy^2 = x^3 + (i-2)x^2 + x$$

defined over $\mathbb{Q}(i)$ has at least one place of supersingular reduction (it is however conjectured that there exist infinitely many) [12, Section 5.2].

(3) Our lower bound is much stronger than that of Theorem 1.4. Let us see this through a concrete example. Consider the elliptic curve

$$E : y^2 + y = x^3 - x^2 - 10x - 20$$

defined over $K = \mathbb{Q}$. According to [21, elliptic curve 11.a2], E has conductor $N = 11$ and j-invariant $j_E = -2^{12}11^{-5}31^3$. By the same reference, (b) with $L = \mathbb{Q}$ holds for all $p \geq 7$. Next, $j_E \not\equiv 0 \ (p)$ for all $p \notin \{2, 11, 31\}$ and $j_E \not\equiv 1728 \ (p)$, that is,

$$2^6 41^2 61^2 = 11^5 1728 + 2^{12}31^3 \not\equiv 0 \ (p),$$

for all $p \notin \{2, 41, 61\}$. Finally, E has supersingular reduction at $p = 19$ [33, Chapter 5, Example 4.6]. From all this, Theorem 1.6 claims that for all $\alpha \in \mathbb{Q}^{t19}(E_{\mathrm{tors}})^* \setminus \mu_\infty$,

$$h(\alpha) \geq \frac{1}{4^{19^2}+1}\left(\frac{\log 19}{(40\sqrt{2}+2)19^{2\cdot 19^2+2}}\right)^{2+\frac{4}{19^{19^2/4-2}}} \geq 2.6 \cdot 10^{-2072}.$$

We cannot deduce this lower bound from Theorem 1.4 because $\mathrm{Gal}(\mathbb{Q}^{t19}/\mathbb{Q})$ has infinite exponent. Consider a number field $F \subset \mathbb{Q}^{t19}$ of degree $d \geq 9$. Even under this restriction, it is not always possible to get the lower bound above from Theorem 1.4 since $p = 19$ is not a suitable choice there, item (c) not being satisfied.

Let $n \in \mathbb{N}$ be an integer and write $\mathcal{V}(n) = \sum_{p \text{ prime} \leq n} \log p$. We have the inequality $\mathcal{V}(n) < 1.01624n$ [27]. Applying [14, Theorem 4.13] to $M = 2d+2$ proves the existence of a rational prime p between $n = \max\{2d+2, 7654\}$

and

$$e^{1.3\times 10^8 e^{2\mathcal{V}(n)+\frac{11}{15}e^{\mathcal{V}(n)}}} < e^{e^{e^{\mathcal{V}(n)}}} < e^{e^{e^{1.01624n}}}$$

such that E has supersingular reduction at p. For such a choice of p, items (a)–(c) of Theorem 1.4 are all satisfied, which leads to the lower bound

$$\forall \alpha \in F(E_{\mathrm{tors}})^* \setminus \mu_\infty, \quad h(\alpha) \geq \left(e^{e^{e^{e^{1.02n}}}}\right)^{-1}.$$

We can compare the two lower bounds above and check that ours is much better.

Our theorem suggests that Conjecture 1.1 can be extended as follows.

Conjecture 1.8. *Let A be an abelian variety defined over a number field K. Let $\mathcal{L}$ be a symmetric ample line bundle on A/K, and let L/K be an algebraic extension. If $d_v(L)$ is finite for at least one finite place v of K, then $L(A_{\mathrm{tors}})$ and $A(L(A_{\mathrm{tors}}))$ have the Bogomolov property.*

The best argument in favor of this statement is probably the result below.

Theorem 1.9 (Amoroso–David–Zannier [1]). *Let A be a CM abelian variety defined over a number field K. Let $\mathcal{L}$ be a symmetric ample line bundle on A/K, and let L/K be a Galois extension. If $d_v(L)$ is finite for at least one finite place v of K, then $L(A_{\mathrm{tors}})$ has the Bogomolov property.*

Proof. As A is CM, there exists a finite Galois extension M/K such that $M(A_{\mathrm{tors}})/M$ is abelian. Choose $\sigma \in \mathrm{Gal}(LM(A_{\mathrm{tors}})/LM)$ and a $\tau \in \mathrm{Gal}(LM(A_{\mathrm{tors}})/M)$. If $\alpha \in M(A_{\mathrm{tors}})$, then $\sigma\tau\alpha = \tau\sigma\alpha$ since $M(A_{\mathrm{tors}})/M$ is abelian. If $\alpha \in LM$, then $\sigma(\tau\alpha) = \tau(\sigma\alpha) = \tau\alpha$ since LM/M is Galois (because L/K is by assumption) and σ fixes the elements of LM. From all this, we get $\sigma\tau = \tau\sigma$, i.e., $\mathrm{Gal}(LM(A_{\mathrm{tors}})/LM)$ is contained in the center of $\mathrm{Gal}(LM(A_{\mathrm{tors}})/M)$. As $d_v(LM)$ is bounded from above by $d_v(L)d_v(M) < \infty$, the theorem now arises from [1, Theorem 1.2]. ∎

2. An elementary result. Write $\langle X \rangle$ for the group generated by a subset X of a group G. Let L/K be a Galois extension of number fields, and let w be a finite place of L. Set $D(w|w \cap K)$ to be the decomposition group of the extension $w|w \cap K$, that is, the set of $\psi \in \mathrm{Gal}(L/K)$ such that $\psi w = w$.

Fix for this section a number field K as well as a finite place v of K. For any finite extension L/K, we write V_L for the set of places of L above v.

Lemma 2.1. *Consider a totally v-adic finite Galois extension M/K and a tower of number fields $K \subset K' \subset L$ with L/K' Galois. Assume that*

$$H' := \Big\langle \bigcup_{w \in V_L} D(w|w \cap K') \Big\rangle = \mathrm{Gal}(L/K').$$

Then

$$H := \Big\langle \bigcup_{w\in V_{LM}} D(w|w\cap K'M)\Big\rangle = \mathrm{Gal}(LM/K'M).$$

Proof. Choose a $w \in V_{LM}$, and let $\mathrm{Res} : \mathrm{Gal}(LM/K'M) \to \mathrm{Gal}(L/K')$ be the restriction map. It is injective and induces a homomorphism from $\mathrm{Gal}((LM)_w/(K'M)_w)$ to $\mathrm{Gal}(L_w/K'_w)$, and so from $D(w|w\cap K'M)$ to $D(w\cap L|w\cap K')$. As M is a totally v-adic field, we have $M_w = K_v$, whence $\mathrm{Gal}((LM)_w/(K'M)_w) = \mathrm{Gal}(L_w/K'_w)$. In particular, $D(w|w\cap K'M)$ and $D(w\cap L|w\cap K')$ have the same cardinality, and so $\mathrm{Res} : D(w|w\cap K'M) \to D(w\cap L|w\cap K')$ is an isomorphism for all $w \in V_{LM}$. Hence, $\mathrm{Res} : H \to H'$ is an isomorphism too. By assumption, we have the chain of inclusions $\mathrm{Gal}(L/K') = H' = \mathrm{Res}(H) \subset \mathrm{Res}(\mathrm{Gal}(LM/K'M)) \subset \mathrm{Gal}(L/K')$ and the lemma follows. ∎

Keep the notation of Lemma 2.1 and assume that both K'/K and L/K are Galois. Let w be a finite place of L. Then $\psi D(w|w\cap K')\psi^{-1} = D(\psi w|\psi w\cap K')$ for all $\psi \in \mathrm{Gal}(L/K)$. The fact that $\mathrm{Gal}(L/K)$ acts transitively on V_L leads to

$$\langle \psi D(w|w\cap K')\psi^{-1}, \psi \in \mathrm{Gal}(L/K)\rangle = \Big\langle \bigcup_{w'\in V_L} D(w'|w'\cap K')\Big\rangle. \tag{1}$$

Corollary 2.2. *Consider a totally v-adic finite Galois extension M/K and a tower of number fields $K \subset K' \subset L$ with K'/K and L/K Galois. Let w be a place of LM above v and assume that*

$$\mathrm{Gal}(L/K') = \langle \psi D(w\cap L|w\cap K')\psi^{-1},\ \psi \in \mathrm{Gal}(L/K)\rangle.$$

If $\gamma \in LM$ with $\sigma\gamma \in K'_w$ for all $\sigma \in \mathrm{Gal}(LM/K)$, then $\gamma \in K'M$.

Proof. By assumption, it follows from (1) that

$$\mathrm{Gal}(L/K') = \Big\langle \bigcup_{w'\in V_L} D(w'|w'\cap K')\Big\rangle.$$

Using Lemma 2.1, then (1) applied to $L = LM$ and $K' = K'M$, gives

$$\begin{aligned}\mathrm{Gal}(LM/K'M) &= \Big\langle \bigcup_{w'\in V_{LM}} D(w'|w'\cap K'M)\Big\rangle \\ &= \langle \psi D(w|w\cap K'M)\psi^{-1},\ \psi \in \mathrm{Gal}(LM/K)\rangle.\end{aligned}$$

We have $M_w = K_v$ since M is a totally v-adic field. Thus $D(w|w\cap K'M)$ is equal to $\mathrm{Gal}((LM)_w/(K'M)_w) = \mathrm{Gal}(L_w/K'_w)$. The lemma follows since γ is fixed by $\psi D(w|w\cap K'M)\psi^{-1}$ for all $\psi \in \mathrm{Gal}(LM/K)$. ∎

3. Some results extracted from [16]. For any number field K and any finite place v of K, we denote by K_v the completion of K with respect to $|\cdot|_v$, the normalized v-adic absolute value, that is, $|p|_v = p^{-1}$, where

$p\mathbb{Z} = v \cap \mathbb{Z}$. Further, write K_v^{ur} for the maximal unramified extension of K_v and $\mathbb{Q}_{p^2}$ for the unramified extension of degree 2 of $\mathbb{Q}_p$ inside $\overline{\mathbb{Q}_p}$.

In [16, Section 3], Frey fixed the following notation: a non-CM elliptic curve $E/\mathbb{Q}$, a Galois extension $L/\mathbb{Q}$ whose Galois group has finite exponent, a rational prime p satisfying the conditions (a)–(c) of Theorem 1.4, a number field $K \subset L$, which is Galois over $\mathbb{Q}$, and a finite Galois extension $F/\mathbb{Q}_{p^2}$ containing K_v, where v denotes the place of K associated to a fixed field embedding $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}_p}$.

Actually, we can prove most of the results mentioned in [16] without involving most of the conditions above. Strictly speaking, we should reprove them all using only the minimal conditions. But they are very technical, making it impossible without considerably burdening this text. As a compromise, we mention below the hypotheses and references that Frey used to prove each one of her results, then we detail one by one the conditions required to use these references.

3.1. Results extracted from [16, Section 3]. Here, p denotes a rational prime.

We review the assumptions of Frey's results:

- In [16, Lemma 3.1], she used $[F : \mathbb{Q}_p] < p, \mathbb{Q}_{p^2} \subset F$ and [19, Lemma 3.4].
- In [16, Lemma 3.2], she used $[F : \mathbb{Q}_p] < p, \mathbb{Q}_{p^2} \subset F$ and [19, Lemmas 3.3 and 3.4].
- In [16, Lemma 3.3], she used $[F : \mathbb{Q}_p] < p, \mathbb{Q}_{p^2} \subset F$ and [19, Lemma 3.3].
- In [16, Lemma 3.4], she used the fact that $F/\mathbb{Q}_{p^2}$ is a finite Galois extension as well as [19, Lemmas 2.1, 3.3, 3.4] and [22, Proposition II.7.12].
- In [16, Lemma 3.5], she used the fact that $F/\mathbb{Q}_{p^2}$ is a finite Galois extension as well as [19, Lemmas 2.1 and 3.3] and [29, Lemme IV.5, Proposition IV.12].
- In [16, Lemma 3.6], she used [19, Lemma 3.5], [22, Proposition II.7.13], Goursat's lemma, $[F : \mathbb{Q}_p] < p$ and $\mathbb{Q}_{p^2} \subset F$.
- In [16, Lemma 3.7], she used [22, Proposition II.7.12].
- In [16, Lemma 3.8], she used results of [16].

Now, to prove [16, Lemmas 3.1–3.8], we only need to assume that $F/\mathbb{Q}_{p^2}$ is a finite Galois extension such that $[F : \mathbb{Q}_p] < p$, as well as the conditions that are necessary for [19, Lemmas 2.1, 3.3–3.5], [22, Propositions II.7.12–II.7.13], [29, Lemme IV.5, Proposition IV.12] and Goursat's lemma to hold. Goursat's lemma is a general fact about group theory, [29, Lemme IV.5, Proposition IV.12] are general results about ramification groups, [22, Propositions II.7.12–II.7.13] are general facts about cyclotomic fields, and [19, Lemma 2.1] is a general lemma on local fields. Finally, the results in [19, Sections 3–5] hold for every rational prime $p \geq 5$ and every elliptic curve E defined over $\mathbb{Q}_{p^2}$ with supersingular re-

duction and whose j-invariant is neither 0 nor 1728 in the residual field of $\mathbb{Q}_{p^2}$.

In conclusion, all the results of [16, Section 3] work in the following situation, which we will refer to from now on as (S):

- $p \geq 5$ is a rational prime;
- E is an elliptic curve defined over $\mathbb{Q}_{p^2}$ with supersingular reduction and its j-invariant is neither 0 nor 1728 in the residual field of $\mathbb{Q}_{p^2}$;
- $F/\mathbb{Q}_{p^2}$ is a finite Galois extension such that $[F : \mathbb{Q}_p] < p$.

Choose $N \in \mathbb{N}$. Denote by μ_N the set of all Nth roots of unity and by $\operatorname{Aut} E[N]$ the set of automorphisms of $E[N]$. Let L/K be a finite Galois extension of local fields, and let π be the prime ideal of L. For $i \geq 0$, we define $G_i(L/K)$ as the ith ramification group of L/K, that is, the set of $\psi \in \operatorname{Gal}(L/K)$ such that $\psi x - x \in \pi^{i+1}$ for all $x \in L$ with $|x|_\pi \leq 1$. It is well-known that $G_0(L/K) = \operatorname{Gal}(L/L \cap K^{ur})$.

We can now state some results extracted from [16, Section 3].

LEMMA 3.1. *Let p, E and F be as in (S). Let $N \in \mathbb{N}$ be an integer with p-adic valuation n. Then:*

(i) *The extension $F(E[p^n])/F(E[p])$ is totally ramified of degree $p^{2(n-1)}$.*
(ii) *The extension $F(E[N])/F(E[p^n])$ is unramified.*
(iii) $\operatorname{Gal}(F(E[N])/F(E[N/p])) \simeq \operatorname{Gal}(F(E[p^n])/F(E[p^{n-1}])) \simeq (\mathbb{Z}/p\mathbb{Z})^2$ *if $n \geq 2$.*
(iv) *For $m \in \mathbb{N}$ coprime to p, the image of $\operatorname{Gal}(F(E[p^n])/F) \to \operatorname{Aut} E[p^n]$ contains the multiplication-by-$m^{[F:\mathbb{Q}_{p^2}]}$ map.*
(v) *For $M \in \mathbb{N}$ coprime to p, the order of $\operatorname{Gal}(F(E[pM])/F(E[M]))$ divides $p^2 - 1$.*
(vi) $\operatorname{Gal}(F(E[N])/F(E[N/p])) \subset G_s(F(E[N])/F)$ *if $n \geq 2$, where $s = p^{2(n-1)} - 1$.*
(vii) *If $n \geq 2$, then $F(E[N]) \cap \bigcup_{m \in \mathbb{N}} \mu_{p^m} = \mu_{p^n}$.*
(viii) *Let $n \geq 2$. If $\psi \in \operatorname{Gal}(F(E[N])/F(E[N/p]))$ and $a \in F(E[N])^*$ satisfy $(\psi a/a)^{p^2} \neq 1$, then $\psi a/a \notin \mu_\infty$ (in particular, $(\psi a/a)^{p^2} \notin \mu_\infty$).*

Proof. See [16, Lemmas 3.3–3.6, 3.8]. ∎

3.2. Some results extracted from [16, Section 4]. In [16, Lemma 4.1(i, ii, iv, v)], Frey only used [19, Lemmas 2.1, 3.1, 5.1]. In [16, Lemmas 4.2–4.5], she only used results of [16, Section 4] except [16, Lemma 4.1(iii)]. All these statements therefore hold in the situation (S).

LEMMA 3.2. *Let p, E and F be as in (S) and put $\mathcal{E} = (p^2 - 1)[F : \mathbb{Q}_{p^2}]$. Take an integer $N \in \mathbb{N}$ not divisible by p^2 and denote by n its p-adic valuation. Then there is $\phi \in \operatorname{Gal}(F(E[N])/F(E[p^n]))$ such that:*

(i) *ϕ acts on $E[N/p^n]$ as multiplication by $p^{\mathcal{E}}$;*
(ii) *for all $a \in F(E[N])$, we have $|\phi a - a^{p^{2\mathcal{E}}}|_p \le p^{-1/\mathcal{E}} \max\{1, |a|_p\}^{1+p^{2\mathcal{E}}}$.*

Proof. (i) Let $\tilde{\phi} \in \mathrm{Gal}(\mathbb{Q}_p^{ur}/\mathbb{Q}_{p^2})$ be the lift of the Frobenius automorphism squared. Write $N/p^n = \prod_l l^{v_l}$ for the decomposition of N/p^n into a product of rational primes. Let l be a rational prime dividing N/p^n. Then $l \neq p$ and [19, Lemma 3.2] implies that $\tilde{\phi}$ acts on $E[l^{v_l}]$ as multiplication by $\pm p$. The isomorphism $\bigoplus_l E[l^{v_l}] \simeq E[N/p^n]$ being compatible with the action of the Galois group, we deduce that $\tilde{\phi}$ acts on $E[N/p^n]$ as multiplication by $\pm p$. By [16, Lemma 4.1(ii)], there is $\phi \in \mathrm{Gal}(F(E[N])/F(E[p^n]))$ such that ϕ and $\tilde{\phi}^{\mathcal{E}}$ coincide on $E[N/p^n]$. This shows (i) since $\mathcal{E}$ is even.

(ii) This follows from [16, Lemma 4.4] and from the equality $|\phi a|_p = |a|_p$, which holds since any two Galois conjugates of $\overline{\mathbb{Q}_p}$ have the same p-adic absolute value [29, Chapter II, §2, Corollaire 3]. ∎

A proof of the next lemma can be found in [15, Lemma 3.5]. It is based only on elementary calculations.

Lemma 3.3. *Let $0 < \delta < 1/2$, and let $\beta \in \overline{\mathbb{Q}}^* \setminus \mu_\infty$ be such that $[\mathbb{Q}(\beta) : \mathbb{Q}] \ge 16$ and $h(\beta) \le 1/4$. Then*

$$\frac{1}{[\mathbb{Q}(\beta) : \mathbb{Q}]} \sum_{\tau : \mathbb{Q}(\beta) \hookrightarrow \mathbb{C}} \log|\tau\beta - 1| \le \frac{40}{\delta^4} h(\beta)^{1/2-\delta}.$$

3.3. Some results extracted from [16, Sections 5–6]. In [16, Lemmas 5.1–5.2], Frey only used results proved in [16, Section 3]. So we can use [16, Lemma 5.2] under the more general conditions of the situation (S), which gives:

Lemma 3.4. *Let p, E and F be as in (S), and let $N \in \mathbb{N}$ be an integer divisible by p^2. Then for all $a \in F(E[N])$ and all $\psi \in \mathrm{Gal}(F(E[N])/F(E[N/p]))$, we have*

$$|\psi a^{p^2} - a^{p^2}|_p \le p^{-1/[F:\mathbb{Q}_{p^2}]} \max\{1, |a|_p\}^{2p^2}.$$

(Again, we have exploited the fact that $|\psi a|_p = |a|_p$).

The cardinality of a finite set X is denoted by $\#X$. Apparently, [16, Lemma 5.3] seems to involve the conditions (a)–(c) of Theorem 1.4. Actually, they are not needed and we prove a more general fact below.

Lemma 3.5. *Let L/K be a Galois extension of number fields, and let H be a normal subgroup of $\mathrm{Gal}(L/K)$. Let $\psi \in H$, and set*

$$C = \{\sigma \in \mathrm{Gal}(L/K) : \sigma\psi\sigma^{-1} = \psi\},$$

the centralizer of ψ. Then for all finite places w of L, the cardinality of the orbit $Cw := \{\sigma w : \sigma \in C\}$ is at least $[L : K]/([L_w : K_w]\#H)$.

Proof. The orbit of ψ under the conjugation action of $\mathrm{Gal}(L/K)$ on itself is included in H since the latter is normal in $\mathrm{Gal}(L/K)$. The orbit-stabilizer theorem ensures us that $\#C \geq [L:K]/\#H$. Let w be a finite place of L. The Galois group $\mathrm{Gal}(L/K)$ acts transitively on all places of L above $w \cap K$ and the total number of such places is $[L:K]/[L_w:K_w]$. So the orbit Cw has cardinality at least

$$\frac{1}{[\mathrm{Gal}(L/K):C]}\frac{[L:K]}{[L_w:K_w]} \geq \frac{[L:K]}{[L_w:K_w]\#H},$$

which concludes the proof of the lemma. ∎

The proof of [16, Lemma 6.1] only requires results present in [16, Section 3].

Lemma 3.6. *Let p, E and F be as in (S). Let $N \in \mathbb{N}$ be an integer whose p-adic valuation n is at least 2. Take an integer $m \in \mathbb{N}$ coprime to p. Then there is $\tau_m \in \mathrm{Gal}(F(E[N])/F)$ such that*

(i) *τ_m acts by raising to the power of $m^{2[F:\mathbb{Q}_{p^2}](p^2-1)}$ on μ_{p^n};*
(ii) *τ_m acts by multiplication by $m^{[F:\mathbb{Q}_{p^2}](p^2-1)}$ on $E[p^n]$;*
(iii) *τ_m acts trivially on $E[N/p^n]$.*

Proof. For (i) and (ii), see [16, Lemma 6.1] (Frey gave the proof for $m = 2$, but it easily extends to m coprime to p thanks to Lemma 3.1(iv)). For (iii), see the last paragraph in the proof of [16, Lemma 6.1]. ∎

The next statement is a general lemma of linear algebra.

Lemma 3.7. *Consider an odd rational prime p. Let U be a $\mathbb{Z}/p\mathbb{Z}$-vector subspace of $\mathrm{Mat}_2(\mathbb{Z}/p\mathbb{Z})$ of cardinality greater than p, that contains at least one non-zero scalar matrix. Then $\langle AUA^{-1}, A \in \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})\rangle = \mathrm{Mat}_2(\mathbb{Z}/p\mathbb{Z})$.*

Proof. See [16, Lemma 6.4]. ∎

For the convenience of the reader, we give a (quick) proof of the last lemma of this section although it is only a "copy-paste" of that of [16, Lemma 6.5(i)].

Lemma 3.8. *Let p, E and F be as in (S), and let $L \subset F$ be a number field. Assume that E is defined over L and that the image of the natural representation $\mathrm{Gal}(L(E[p])/L) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ contains $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Take $N \in \mathbb{N}$ such that its p-adic valuation n is at least 2 and put $G = \mathrm{Gal}(F(E[N])/F(E[N/p]))$. Then*

$$H := \langle \psi G \psi^{-1}, \psi \in \mathrm{Gal}(L(E[N])/L)\rangle = \mathrm{Gal}(L(E[N])/L(E[N/p])) =: H'.$$

Proof. Let $\rho : \mathrm{Gal}(L(E[N])/L) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be the natural representation. As $n \geq 2$, it is well-known that we can define an injective homomorphism $\mathcal{L}$ from H' to $\mathrm{Mat}_2(\mathbb{Z}/p\mathbb{Z})$ as follows: For $\sigma \in H'$, $\mathcal{L}(\sigma)$ is the unique

element of $\mathrm{Mat}_2(\mathbb{Z}/p\mathbb{Z})$ satisfying $\rho(\sigma) = 1 + (N/p)\mathcal{L}(\sigma)$, where 1 denotes the identity matrix.

By definition, H is the normal closure of G in $\mathrm{Gal}(L(E[N])/L)$, whence $H \subset H'$. Let $\pi : \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ be the natural projection. If $\psi \in G \subset H \subset H'$ and if $\sigma \in \mathrm{Gal}(L(E[N])/L)$, then $\sigma\psi\sigma^{-1} \in H \subset H'$ and an easy calculation gives

$$\begin{aligned}\rho(\sigma\psi\sigma^{-1}) &= \rho(\sigma)\rho(\psi)\rho(\sigma)^{-1} = \rho(\sigma)(1 + (N/p)\mathcal{L}(\psi))\rho(\sigma)^{-1} \\ &= 1 + (N/p)\rho(\sigma)\mathcal{L}(\psi)\rho(\sigma)^{-1} = 1 + (N/p)\pi\rho(\sigma)\mathcal{L}(\psi)\pi\rho(\sigma)^{-1},\end{aligned}$$

leading to $\mathcal{L}(\sigma\psi\sigma^{-1}) = \pi\rho(\sigma)\mathcal{L}(\psi)\pi\rho(\sigma)^{-1} \in \mathcal{L}(H)$. By assumption, the image of $\pi\rho$ contains $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. This implies that $\langle A\mathcal{L}(G)A^{-1}, A \in \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})\rangle \subset \mathcal{L}(H)$.

Lemma 3.1(iii) tells us that G, and so $\mathcal{L}(G)$, has cardinality p^2. If $\mathcal{L}(G)$ contains a non-zero scalar matrix, then Lemma 3.7 applied to $U = \mathcal{L}(G)$ shows that $\mathrm{Mat}_2(\mathbb{Z}/p\mathbb{Z}) = \mathcal{L}(H) \subset \mathcal{L}(H') \subset \mathrm{Mat}_2(\mathbb{Z}/p\mathbb{Z})$, and so $H = H'$ by injectivity of $\mathcal{L}$.

Let m be a generator of $(\mathbb{Z}/p^n\mathbb{Z})^*$. As $[F : \mathbb{Q}_p] < p$, and so is coprime to p, it follows that $M = m^{[F:\mathbb{Q}_{p^2}](p^2-1)p^{n-2}}$ has order p in $(\mathbb{Z}/p^n\mathbb{Z})^*$. Moreover, $M \equiv 1\ (p^{n-1})$ by Euler's theorem. Consequently, the multiplication-by-M map has order p in $\mathrm{Aut}\, E[p^n]$ and acts trivially on $E[p^{n-1}]$.

Lemma 3.6(ii) applied to $N = p^n$ and $m = m^{p^{n-2}}$ tells us that there exists $\tau \in \mathrm{Gal}(F(E[p^n])/F)$ acting on $E[p^n]$ as multiplication by M. By the foregoing, τ is an element of $\mathrm{Gal}(F(E[p^n])/F(E[p^{n-1}]))$ with order p.

By Lemma 3.1(iii), the restriction map $G \to \mathrm{Gal}(F(E[p^n])/F(E[p^{n-1}]))$ is an isomorphism. Let $\tilde{\tau} \in G$ be the element that gets mapped to τ under this map. As $\tilde{\tau}$ acts on $E[p^n]$ as scalar multiplication, we deduce that $\mathcal{L}(\tilde{\tau}) \in \mathcal{L}(G)$ is a scalar matrix, which cannot be zero since $\tilde{\tau}$ has order p and $\mathcal{L}$ is injective. ∎

4. Proof of Theorem 1.4: toric case. Fix for this section the notation (and assumptions) of Theorem 1.6 in the toric case and a field embedding $\overline{K} \to \overline{K_v}$. As everything is now fixed, we ease the notation by putting $M(N) = M(E[N])$ for any field $M \subset \overline{K_v}$ and any integer $N \in \mathbb{N}$.

Item (d) leads to either $K_v = \mathbb{Q}_p$ or $K_v = \mathbb{Q}_{p^2}$. Our elliptic curve is therefore defined over $\mathbb{Q}_{p^2}$. Moreover, by (a), it has supersingular reduction and its j-invariant is neither 0 nor 1728 in the residual field of $\mathbb{Q}_{p^2}$. Put $F = L_{w_0}\mathbb{Q}_{p^2}$, where w_0 is the place of L associated to the fixed embedding $\overline{K} \to \overline{K_v}$. It is Galois over $\mathbb{Q}_{p^2}$ since L/K is Galois. Next, it follows from (c) that $p \geq 5$ and

$$p > 2d_v(L) \geq [\mathbb{Q}_{p^2} : \mathbb{Q}_p][L_{w_0} : K_v] \geq [F : \mathbb{Q}_p]. \tag{2}$$

To summarize, our scope is a particular case of the situation (S). By (b),

E is defined over $L \subset F$ and the natural representation $\mathrm{Gal}(L(p)/L) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ contains $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. We thus have access to all the results of Section 3.

The next two results will serve us both in the toric case and in the elliptic case. We start by putting in place our descent argument.

LEMMA 4.1. *Let $N \in \mathbb{N}$ be an integer divisible by $p(p^2-1)$ such that*

$$\left\langle \psi \mathrm{Gal}(F(N)/F(N/p))\psi^{-1}, \psi \in \mathrm{Gal}(L(N)/L) \right\rangle = \mathrm{Gal}(L(N)/L(N/p)).$$

Let M/K be a totally v-adic finite Galois extension. If $\gamma \in LM(N)$ with $\sigma\gamma \in F(N/p)$ for all $\sigma \in \mathrm{Gal}(LM(N)/K)$, then $\gamma \in LM(N/p)$.

Proof. Since N/p is divisible by p^2-1, basic properties of the Weil pairing prove that $\zeta_{p^2-1} \in K(N/p)$. As $\mathbb{Q}_{p^2} = \mathbb{Q}_p(\zeta_{p^2-1})$, we get $\mathbb{Q}_{p^2} \subset K_v(N/p) \subset K_v(N)$.

Denote by w the place of $LM(N)$ associated to the embedding $\overline{K} \to \overline{K_v}$. Then $L(N)_w = L_{w_0}\mathbb{Q}_{p^2}(N) = F(N)$. Similarly, $L(N/p)_w = F(N/p)$. In conclusion, $\mathrm{Gal}(F(N)/F(N/p)) = D(w|w\cap L(N/p))$. The lemma now follows from Corollary 2.2 applied to $K' = L(N/p)$ and $L = L(N)$. ∎

LEMMA 4.2. *Take an integer $N \in \mathbb{N}$ of p-adic valuation n and $\psi \in \mathrm{Gal}(F(N)/F)$. If ψ acts as scalar multiplication on both $E[p^n]$ and $E[N/p^n]$, then it belongs to the center of $\mathrm{Gal}(LK^{tv}(N)/K)$. In particular, the elements ϕ and τ_m introduced in Lemmas 3.2 and 3.6, respectively, lie in the center of $\mathrm{Gal}(LK^{tv}(N)/K)$.*

Proof. Clearly, ψ fixes $LK^{tv} \subset F$. Taking the sum of points gives an isomorphism between $E[p^n] \times E[N/p^n]$ and $E[N]$, which is compatible with the action of $\mathrm{Gal}(\overline{K}/K)$. We infer that ψ must lie in the center of $\mathrm{Gal}(LK^{tv}(N)/K)$. ∎

A proof of the well-known result below can be found in [11, Lemma 2(i)].

LEMMA 4.3. *Let $a \in \overline{\mathbb{Q}}^*$, and let $\psi \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. If $a \notin \mu_\infty$, then $\psi a^b/a^c \notin \mu_\infty$ for all distinct integers $b, c \in \mathbb{N}$.*

Let $\alpha \in LK^{tv}(E_{\mathrm{tors}})^* \backslash \mu_\infty$. There is a totally v-adic finite Galois extension M/K such that $\alpha \in LM(E_{\mathrm{tors}})$. For brevity, put $L' = LM$.

The proof of the proposition below is largely inspired by that of [16, Lemma 4.6].

PROPOSITION 4.4. *Let $N \in \mathbb{N}$ be an integer with p-adic valuation n, and let $a \in L'(N)^* \setminus \mu_\infty$. Assume that $n \leq 1$ or that $n \geq 2$ and $a^{p^2} \notin F(N/p)$. Then*

$$h(a) \geq k = \left(\frac{\log p}{d_v(L)(40\sqrt{2}+2)[K:\mathbb{Q}]p^{2p^2 d_v(L)+2}} \right)^{2+\frac{4}{p^{p^2 d_v(L)/4-2}}}.$$

Proof. Construct $\psi \in \mathrm{Gal}(L'(N)/L')$ as follows: If $n \leq 1$, then ψ is the homomorphism ϕ of Lemma 3.2. Otherwise, define ψ to be any element of $\mathrm{Gal}(F(N)/F(N/p))$ satisfying $\psi a^{p^2} \neq a^{p^2}$ (such an element exists by assumption). Next, put

$$t = \begin{cases} 0 & \text{if } n \leq 1, \\ 4 & \text{if } n \geq 2, \end{cases}$$

$$\mathcal{E} = \begin{cases} (p^2-1)[F:\mathbb{Q}_{p^2}] & \text{if } n \leq 1, \\ [F:\mathbb{Q}_{p^2}] & \text{if } n \geq 2, \end{cases}$$

$$(b,c) = \begin{cases} (1, p^{2\mathcal{E}}) & \text{if } n \leq 1, \\ (p^2, p^2) & \text{if } n \geq 2, \end{cases}$$

and $x = \psi a^b - a^c$. Note that the latter is non-zero (for $n \geq 2$, it is by construction and for $n \leq 1$, it is by Lemma 4.3).

Denote by v_0 the place of $L'(N)$ associated to the embedding $\overline{K} \to \overline{K_v}$. Let C be the centralizer of ψ in $\mathrm{Gal}(L'(N)/K)$. Lemma 4.2 gives $C = \mathrm{Gal}(L'(N)/K)$ if $n \leq 1$, and so the orbit Cv_0 is the set of all places of $L'(N)$ above v. In particular, it has cardinality $[L'(N):K]/[L'(N)_{v_0}:K_v]$. If $n \geq 2$, then Lemma 3.5 applied to $L = L'(N)$ and $H = \mathrm{Gal}(L'(N)/L'(N/p))$, which has cardinality at most p^4, proves that Cv_0 has cardinality at least $[L'(N):K]/(p^4[L'(N)_{v_0}:K_v])$.

Let w be a place of $L'(N)$. If w is a finite place, the ultrametric inequality gives

$$|x|_w \leq \max\{|\psi a^b|_w, |a|_w^c\} \leq (\max\{1, |\psi a|_w\})^b (\max\{1, |a|_w\})^c. \tag{3}$$

If we further assume that $w \in Cv_0$, then there is $\sigma \in C$ such that $w = \sigma^{-1} v_0$. Thus,

$$|x|_w = |x|_{\sigma^{-1}v_0} = |\sigma x|_{v_0} = |\sigma(\psi a)^b - \sigma a^c|_{v_0} = |\psi(\sigma a)^b - \sigma a^c|_{v_0}.$$

Lemma 3.2 (if $n \leq 1$) or Lemma 3.4 (if $n \geq 2$) applied to $a = \sigma a$ gives

$$|x|_w \leq p^{-1/\mathcal{E}} (\max\{1, |\sigma a|_{v_0}\})^{b+c} = p^{-1/\mathcal{E}} (\max\{1, |a|_w\})^{b+c}. \tag{4}$$

If w is an infinite place, we have to take a little detour. Put $\beta = \psi a^b / a^c \neq 1$ and note that $h(\beta) \leq h(\psi a^b) + h(a^c) = (b+c)h(\alpha) \leq 2p^{2\mathcal{E}} h(a)$. Moreover, $\beta \notin \mu_\infty$ (it is clear by Lemma 3.1(viii) if $n \geq 2$ and by Lemma 4.3 otherwise). Clearly,

$$|x|_w = |\beta - 1|_w |a|_w^c \leq |\beta - 1|_w \max\{1, |a|_w^{b+c}\}. \tag{5}$$

Recall that $x \neq 0$. Collecting (3)–(5), it follows from the product formula

that

$$
\begin{aligned}
(6)\quad 0 &= \sum_w [L'(N)_w : \mathbb{Q}_p] \log |x|_w \\
&\le \sum_{w \in Cv_0} [L'(N)_w : \mathbb{Q}_p] \log\big(p^{-1/\mathcal{E}} (\max\{1, |a|_w\})^{b+c}\big) \\
&\quad + \sum_{w \notin Cv_0, w \nmid \infty} [L'(N)_w : \mathbb{Q}_w] \log\big((\max\{1, |\psi a|_w\})^b (\max\{1, |a|_w\})^c\big) \\
&\quad + \sum_{w|\infty} [L'(N)_w : \mathbb{Q}_w] \log(|\beta - 1|_w \max\{1, |a|_w^{b+c}\}).
\end{aligned}
$$

As $L'(N)/K$ is Galois, the degree of the extension $L'(N)_w/K_v$ does not depend on the place w of $L'(N)$ above v. Thus

$$
\begin{aligned}
\sum_{w \in Cv_0} [L'(N)_w : \mathbb{Q}_p] &= [K_v : \mathbb{Q}_p][L'(N)_{w_0} : K_v] \#(Cv_0) \\
&\ge \frac{[K_v : \mathbb{Q}_p][L'(N) : K]}{p^t}.
\end{aligned}
$$

After dividing (6) by $[L'(N) : \mathbb{Q}]$, we infer, thanks to a small calculation, that

$$
(7)\quad \frac{[K_v : \mathbb{Q}_p] \log p}{\mathcal{E}[K : \mathbb{Q}] p^t} \le (b+c) h(a) + \frac{1}{[L'(N) : \mathbb{Q}]} \sum_{w|\infty} [L'(N)_w : \mathbb{Q}_w] \log |\beta - 1|_w.
$$

If $h(\beta) \ge 1/4$, then the proposition follows from the inequality $h(\beta) \le 2p^{2\mathcal{E}} h(a)$. If $[\mathbb{Q}(\beta) : \mathbb{Q}] \le 15$, then Dobrowolski's inequality [11] gives

$$
h(\beta) \ge \frac{1}{15} \log\left(1 + \frac{1}{1200} \left(\frac{\log\log 15}{\log 15}\right)^3\right) \ge 10^{-6}
$$

and the proposition arises from the inequality $h(\beta) \le 2p^{2\mathcal{E}} h(a)$. If $h(\beta) \le 1/4$ and $[\mathbb{Q}(\beta) : \mathbb{Q}] \ge 16$, then Lemma 3.3 applied to $\delta = 1/p^{\mathcal{E}/4}$ gives

$$
\begin{aligned}
\frac{1}{[L'(N) : \mathbb{Q}]} \sum_{w|\infty} [L'(N)_w : \mathbb{Q}_w] \log |\beta - 1|_w &\le 40 p^{\mathcal{E}} h(\beta)^{(1/2)-\delta} \\
&\le 40\sqrt{2} p^{2\mathcal{E}} h(a)^{(1/2)-\delta}.
\end{aligned}
$$

The proposition is trivial if $h(a) \ge 1$. Otherwise, from (7) we get

$$
\frac{\log p}{\mathcal{E}[K : \mathbb{Q}] p^t} \le 2p^{2\mathcal{E}} h(a) + 40\sqrt{2} p^{2\mathcal{E}} h(a)^{(1/2)-\delta} \le (40\sqrt{2} + 2) p^{2\mathcal{E}} h(a)^{1/2-\delta}
$$

since $b + c \le 2p^{\mathcal{E}}$. Recall that $[F : \mathbb{Q}_p] = 2[F : \mathbb{Q}_{p^2}] \le 2d_v(L)$ by (2). So we have $\mathcal{E} \le p^2 d_v(L)$ and $2\mathcal{E} + t \le 2p^2 d_v(L)$. We finally get

$$
h(a) \ge \left(\frac{\log p}{d_v(L)(40\sqrt{2} + 2)[K : \mathbb{Q}] p^{2p^2 d_v(L)+2}}\right)^{\frac{2}{1-2\delta}}.
$$

The proposition follows since

$$2/(1-2\delta) = 2 + 4/(p^{\mathcal{E}/4} - 2) > 2 + 4/(p^{p^2 d_v(L)/4} - 2). \blacksquare$$

Proof of Theorem 1.6, toric case. Let $N \in \mathbb{N}$ be an integer such that $\alpha \in L'(N)$. By enlarging N if needed, we can assume that it is divisible by $p^2(p^2-1)$. Let $n \geq 2$ denote the p-adic valuation of N. Recall that $[F : \mathbb{Q}_p] < 2d_v(L)$ by (2).

Put $\tau = \tau_2 \in \mathrm{Gal}(F(N)/F)$, the homomorphism introduced in Lemma 3.6, as well as $\gamma = (\tau\alpha)/\alpha^D \in L'(N)$, where $D = 4^{[F:\mathbb{Q}_{p^2}](p^2-1)} \leq 4^{p^2 d_v(L)}$. We get

$$h(\gamma) \leq h(\tau\alpha) + h(\alpha^D) = (1+D)h(\alpha) \leq (1 + 4^{p^2 d_v(L)})h(\alpha)$$

and $\gamma \notin \mu_\infty$ by Lemma 4.3. Our theorem will follow if we show $h(\gamma) \geq k$ (see Proposition 4.4). Let $n' \in \mathbb{N}$ be the least integer such that $\sigma\gamma \in F(p^{n'-n}N)$ for all $\sigma \in \mathrm{Gal}(L'(N)/K)$. We have $n' \leq n$ since $\gamma \in L'(N)$.

We show by decreasing induction on t that $\gamma \in L'(p^{t-n}N)$ for all $t \in \{n', \ldots, n\}$. The base case $t = n$ is obvious. We now assume that our assertion is true for $t > n' \geq 1$ and show that it also holds for $t-1$. Recall that p^n divides N.

Clearly, $p^2(p^2-1)$ divides $N_t = p^{t-n}N$. Lemma 3.8 applied to $N = N_t$ gives

$$\langle \psi \mathrm{Gal}(F(N_t)/F(N_t/p))\psi^{-1}, \psi \in \mathrm{Gal}(L(N_t)/L)\rangle = \mathrm{Gal}(L(N_t)/L(N_t/p)).$$

By assumption, $\sigma\gamma \in F(N_t/p)$ for all $\sigma \in \mathrm{Gal}(L'(N_t)/K)$ and Lemma 4.1 applied to $N = N_t$ ends the induction. In particular, $\gamma \in L'(N')$ where $N' = N_{n'}$.

Case $n' = 1$. As $\gamma \in L'(N')$ is neither 0 nor a root of unity, we can apply Proposition 4.4 to $N = N'$ and $a = \gamma$, which gives us $h(\gamma) \geq k$.

Case $n' \geq 2$. The minimality of n' proves that there is $\sigma \in \mathrm{Gal}(L'(N)/K)$ such that $\sigma\gamma \notin F(N'/p)$. We want to apply Proposition 4.4 to $N = N'$ and $a = \sigma\gamma$, which would prove our theorem since $h(\gamma) = h(\sigma\gamma)$. As $\gamma \in L'(N')$, it remains to show that $\sigma\gamma^{p^2} \notin F(N'/p)$. For this, assume by contradiction that it is the case.

Since $\sigma\gamma \notin F(N'/p)$, there is $\psi \in \mathrm{Gal}(F(N)/F(N'/p))$ such that $\psi\sigma\gamma \neq \sigma\gamma$. Moreover, $\psi\sigma\gamma^{p^2} = \sigma\gamma^{p^2}$ by assumption. Thus $\psi\sigma\gamma = \zeta\sigma\gamma$ for some $\zeta \in \mu_{p^2}\backslash\{1\}$. As τ commutes with both ψ and σ by Lemma 4.2, we get

$$\zeta = \frac{\psi\sigma\gamma}{\sigma\gamma} = \frac{\psi((\sigma\tau\alpha)/\sigma\alpha^D)}{(\sigma\tau\alpha)/\sigma\alpha^D} = \frac{\tau(\psi\sigma\alpha)}{\tau(\sigma\alpha)} \frac{(\sigma\alpha)^D}{(\psi\sigma\alpha)^D} = \frac{\tau\eta}{\eta^D},$$

where $\eta = (\psi\sigma\alpha)/\sigma\alpha$. As $\zeta \in \mu_\infty$, we have $\eta \in \mu_\infty$ by the contrapositive of Lemma 4.3. Let $T \in \mathbb{N}$ be an integer coprime to p such that η^T has order a power of p. Lemma 3.1(vii) gives $\eta^T \in \mu_{p^n}$ and Lemma 3.6 proves that

$\tau\eta^T = (\eta^T)^D$. We conclude that $\zeta^{p^2} = \zeta^T = 1$, and so $\zeta = 1$ since T and p are coprime, a contradiction. □

5. Proof of Theorem 1.6: elliptic case. We now fix the notation (and assumptions) of Theorem 1.6 in the elliptic setting as well as a field embedding $\overline{K} \to \overline{K_v}$. Let w_0 be the place of L associated to this embedding and put $F = L_{w_0}\mathbb{Q}_{p^2}$. Recall that E, p and F satisfy the conditions of the situation (S) and that every result of [19, Sections 3–5] works in this setting. For the convenience of the reader, we state [19, Lemmas 3.3(iii), 3.4(ii, iv)].

LEMMA 5.1. *Let $N \in \mathbb{N}$ be an integer with p-adic valuation n. Then:*

(i) $\mathrm{Gal}(\mathbb{Q}_{p^2}(p^n)/\mathbb{Q}_{p^2})$ *acts transitively on the torsion points of order p^n;*
(ii) *The extension $\mathbb{Q}_{p^2}(N)/\mathbb{Q}_{p^2}(N/p^n)$ is totally ramified;*
(iii) *If $n = 1$, then $\mathrm{Gal}(\mathbb{Q}_{p^2}(N)/\mathbb{Q}_{p^2}(N/p))$ is cyclic of order $p^2 - 1$.*

Note that $F/\mathbb{Q}_{p^2}$ is unramified since v is unramified in L by assumption. The proof of the next lemma becomes obvious thanks to Lemma 5.1(ii).

LEMMA 5.2. *Let $N \in \mathbb{N}$ be an integer with p-adic valuation n. Then $F(N)/F(N/p^n)$ is totally ramified and*

$$\mathrm{Gal}(F(N)/F(N/p^n)) \simeq \mathrm{Gal}(\mathbb{Q}_{p^2}(N)/\mathbb{Q}_{p^2}(N/p^n)).$$

We now state our descent argument.

LEMMA 5.3. *Let $N \in \mathbb{N}$ be an integer divisible by $p(p^2 - 1)$ with p-adic valuation n, and let M/K be a totally v-adic finite Galois extension. If $\gamma \in LM(N)$ with $\sigma\gamma \in F(N/p)$ for all $\sigma \in \mathrm{Gal}(LM(N)/K)$, then $\gamma \in LM(N/p)$.*

Proof. By Lemma 4.1, it suffices to establish that

$$H := \langle \psi G \psi^{-1}, \psi \in \mathrm{Gal}(L(N)/L) \rangle = \mathrm{Gal}(L(N)/L(N/p)),$$

where $G = \mathrm{Gal}(F(N)/F(N/p))$. This holds when $n \geq 2$ by Lemma 3.8. Assume then that $n = 1$. The left-hand side is the normal closure of $G \subset \mathrm{Gal}(L(N)/L(N/p))$ in $\mathrm{Gal}(L(N)/L)$; it is therefore contained in the right-hand one. Moreover, as p does not divide N/p, we know we can identify $\mathrm{Gal}(L(N)/L(N/p))$ with a subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. To obtain what we wish, it suffices to show $\#H \geq \#\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Let $\rho : \mathrm{Gal}(L(N)/L) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ be the composition of the two natural maps $\mathrm{Gal}(L(N)/L) \to \mathrm{Gal}(L(p)/L)$ and $\mathrm{Gal}(L(p)/L) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. It is surjective by assumption and Galois theory tells us that its kernel is $\mathrm{Gal}(L(N)/L(p))$. Thus,

$$\begin{aligned}\rho(H) &= \langle \rho(\psi)\rho(G)\rho(\psi)^{-1}, \psi \in \mathrm{Gal}(L(N)/L) \rangle \\ &= \langle h\rho(G)h^{-1}, h \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \rangle.\end{aligned}$$

Combining Lemma 5.1(iii) with Lemma 5.2 shows that G is a cyclic group

of order p^2-1. As

$$G \cap \mathrm{Gal}(L(N)/L(p)) \subset \mathrm{Gal}(L(N)/L(N/p)) \cap \mathrm{Gal}(L(N)/L(p)) = \{1\},$$

it follows that ρ restricted to G is injective. Hence, $\rho(G)$ is a cyclic group of order p^2-1. This finishes the proof since [19, Lemma 6.1] shows that $\rho(H) = \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. ∎

The rest of the proof faithfully follows the lines of [19, Section 8.2].

LEMMA 5.4. *Let $N \in \mathbb{N}$ be an integer with p-adic valuation $n \geq 1$. Then $E(F(N)) \cap \bigcup_{m\in\mathbb{N}} E[p^m] = E[p^n]$.*

Proof. The $\supset$ inclusion is obvious. Let $T \in E(F(N))$ be a torsion point of order $p^{n'}$ and obtain $n' \leq n$. By Lemma 5.1(i), for each $T' \in E[p^{n'}]$, there is σ in $\mathrm{Gal}(\mathbb{Q}_{p^2}(p^{n'})/\mathbb{Q}_{p^2})$ such that $T' = \sigma T$. The field $F(N)$ being Galois over $\mathbb{Q}_{p^2}$, we get $T' \in E(F(N))$. Hence, $E[p^{n'}] \subset E(F(N))$ or, equivalently, $F(p^{n'}) \subset F(N)$.

The lemma is obvious if $n' = 0$. So assume that $n' \geq 1$. By Lemma 3.1(i), the extension $F(p^{n'})/F(p)$ has ramification index $p^{2(n'-1)}$. Next, $F(N)/F(p^n)$ is unramified by Lemma 3.1(ii). Again, Lemma 3.1(i) shows that the ramification index of $F(N)/F(p)$ is $p^{2(n-1)}$. We conclude that $n' \leq n$ since $F(p^{n'}) \subset F(N)$. ∎

As $E/\mathbb{Q}_{p^2}$ has good reduction, the criterion of Néron–Ogg–Shafarevich asserts that $F(N)/F$ is unramified for all integers $N \in \mathbb{N}$ coprime to p.

LEMMA 5.5. *Let $N = p^n M \in \mathbb{N}$ be an integer with M coprime to p and $n \geq 1$. Consider $\psi \in \mathrm{Gal}(F(N)/F(N/p))$ and $A \in E(F(N))$ such that $B = \psi A - A \in E_{\mathrm{tors}}$. Then $B \in E[Q(n)]$, where $Q(n) = p^2(p^2-1)$ if $n = 1$ and $Q(n) = p^2$ otherwise.*

Proof. The order of B is $N' = p^{n'}M'$ for some integers $n' \geq 0$ and $M' \in \mathbb{N}$ coprime to p. Put $T = [p^{n'}]B$ and note that T has order M'.

The extension $F(MM')/F$ is unramified since MM' is coprime to p. As $F(M)(T)$ is included in $F(MM')$, we infer that $F(M)(T)/F(M)$ is unramified. Moreover, $T \in E(F(N))$, which implies that $F(M)(T)/F(M)$ is totally ramified by Lemma 5.2. In conclusion, $T \in E(F(M))$. In particular, T is fixed by ψ.

The order of $[M']B \in E(F(N))$ is $p^{n'}$. So by Lemma 5.4 we see that $[M']B \in E[p^n]$. Hence, $[pM']B \in E[p^{n-1}] \subset E[N/p]$ is fixed by ψ too.

Bézout's identity tells us that $1 = ap^{n'} + bM'$ for some integers $a, b \in \mathbb{Z}$. Then $B = [a]T + [bM']B$ and by the foregoing, we conclude that $[p]B$ is fixed by ψ. Let t be the order of ψ. A small calculation proves that $B \in E[pt]$ since

$$[pt]B = (\psi^{t-1}+\cdots+1)([p]B) = [p](\psi^{t-1}+\cdots+1)(\psi A - A) = [p](\psi^t A - A) = 0.$$

Lemma 3.1(iii) (when $n \geq 2$) and Lemma 3.1(v) (if $n = 1$) now prove the desired conclusion. ∎

Recall that $\hat{h} = \hat{h}_E : E(\overline{K}) \to \mathbb{R}$ denotes the Néron–Tate height. It is non-negative, invariant under the action of $\mathrm{Gal}(\overline{K}/K)$ and vanishes precisely at E_{tors}. It is also quadratic, that is,

$$\forall m \in \mathbb{Z}\ \forall P \in E(\overline{K}), \quad \hat{h}([m]P) = m^2\hat{h}(P).$$

This implies

$$\forall P \in E(\overline{K})\ \forall T \in E_{\mathrm{tors}}, \quad \hat{h}(P+T) = \hat{h}(P).$$

Finally, it also satisfies the parallelogram law, that is,

$$\forall P, Q \in E(\overline{K}), \quad \hat{h}(P+Q) + \hat{h}(P-Q) = 2(\hat{h}(P) + \hat{h}(Q)).$$

For more information on $\hat{h}$, we refer to [33, Chapter VIII, §9].

Lemma 5.6. *Let $P \in E(\overline{K})$, and let $\sigma \in \mathrm{Gal}(\overline{K}/K)$. If $[n]\sigma P - [m]P \in E_{\mathrm{tors}}$ for some distinct $n, m \in \mathbb{N}$, then $P \in E_{\mathrm{tors}}$.*

Proof. The properties of $\hat{h}$ recalled above show that

$$m^2\hat{h}(P) = \hat{h}([m]P) = \hat{h}([m]P + [n]\sigma P - [m]P) = n^2\hat{h}(\sigma P) = n^2\hat{h}(P)$$

and the lemma follows since $n, m \in \mathbb{N}$ are distinct. ∎

Let O be the neutral element of E. For each place w of a finite extension M of K, denote by $\lambda_w : E(\overline{M_w})\backslash\{O\} \to \mathbb{R}$ the local Néron height function on E associated to w. It can be described in an explicit way, see [31, Chapter VI]. For the purpose of our text, we only need to know that if E has good reduction at w, then $\lambda_w(P) = (1/2)\max\{0, \log|x(P)|_w\}$, where $x(P)$ is the first coordinate of a point $P \in E(\overline{M_w})$ with respect to some Weierstrass model of E/K that we fix from now.

Let $A \in E(M)$. If ν is a place of K, we define the partial height function at ν as

$$\hat{h}_\nu(A) = \frac{1}{[M:\mathbb{Q}]}\sum_{w|\nu}[M_w : \mathbb{Q}_w]\lambda_w(A),$$

where w ranges over all places of M above ν. It is well-known that $\hat{h}_\nu$ does not depend on the choice of the finite extension $M/K(A)$. By [31, Chapter VI, Theorem 2.1], we have $\hat{h} = \sum_\nu \hat{h}_\nu$ on $E(M)$, where ν runs over all places of M. Finally, put $\hat{h}_\infty$ to be the sum of all $\hat{h}_\nu$, where ν runs over all infinite places of K.

Lemma 5.7. *Take an integer $N \in \mathbb{N}$ with p-adic valuation $n \geq 1$. If $A \in E(LK^{tv}(N))$ satisfies $[Q(n)]A \notin E(F(N/p))$, then there exists a non-torsion point $B \in E(\overline{K})$ with $\hat{h}(B) \leq 4\hat{h}(A)$ and*

$$\hat{h}_v(B) \geq l := \frac{\log p}{2p^4[K:\mathbb{Q}][F(p):\mathbb{Q}_p]}.$$

Proof. Let $L' \subset LK^{tv} \subset F$ be a number field, Galois over K, such that $A \in E(L'(N))$. By hypothesis, we can find a $\psi \in \mathrm{Gal}(F(N)/F(N/p)) \subset \mathrm{Gal}(L'(N)/L'(N/p))$ such that $\psi[Q(n)]A \neq [Q(n)]A$. Note that $B = \psi A - A \notin E_{\mathrm{tors}}$ by Lemma 5.5. Moreover, the parallelogram law implies $\hat{h}(B) \leq 2(\hat{h}(\psi A) + \hat{h}(A)) = 4\hat{h}(A)$.

We prove the lower bound for $\hat{h}_v(B)$. Denote by w_0 the place of $L'(N)$ associated to the fixed embedding $\overline{K} \to \overline{K_v}$. Let C be the centralizer of ψ in $\mathrm{Gal}(L'(N)/K)$. Let $w \in Cw_0 = \{\psi w_0, \psi \in C\}$. Then $w = \sigma^{-1}w_0$ for some $\sigma \in C$, and so

$$|x(B)|_w = |x(B)|_{\sigma^{-1}w_0} = |x(\sigma(\psi A - A))|_{w_0} = |x(\psi\sigma A - \sigma A)|_v.$$

As $\sigma B = \psi\sigma A - \sigma A \neq O$, we get $\lambda_w(B) = \lambda_v(\psi\sigma A - \sigma A)$.

We check that ψ lies in the ramification group $G_s(F(N)/F)$, where $s = p^{2(n-1)} - 1$. This is obvious when $n \geq 2$ thanks to Lemma 3.1(vi). If $n = 1$, then it suffices to check that $F(N)/F(N/p)$ is totally ramified, which is true thanks to Lemma 5.2.

Let $\mathfrak{P}$ be the maximal ideal of the ring of integers of $F(N)$. Then $\psi\sigma A$ and σA map to the same element on E reduced modulo $\mathfrak{P}^{p^{2(n-1)}}$. Thus, $\log|x(\psi\sigma A - \sigma A)|_v \geq (p^{2(n-1)}/e)\log p$, where e denotes the ramification index of $F(N)/\mathbb{Q}_p$. By Lemma 3.1(i), we have $e \leq p^{2(n-1)}[F(p) : \mathbb{Q}_p]$. From all of this, we get

$$\lambda_w(B) \geq \frac{\log p}{2[F(p) : \mathbb{Q}_p]}$$

for all $w \in Cw_0$. As $L'(N)/K$ is Galois, it follows that $[L'(N)_w : K_v] = [L'(N)_{w_0} : K_v]$ for all places w of $L'(N)$ above v. In conclusion,

$$\begin{aligned}\hat{h}_v(B) &= \frac{[K_v : \mathbb{Q}_p][L'(N)_{w_0} : K_v]}{[L'(N) : \mathbb{Q}]} \sum_{w|v} \lambda_w(B) \geq \frac{[L'(N)_{w_0} : \mathbb{Q}_p]}{[L'(N) : \mathbb{Q}]} \sum_{w \in Cw_0} \lambda_w(B) \\ &\geq \frac{[L'(N)_{w_0} : \mathbb{Q}_p]}{[L'(N) : \mathbb{Q}]} \frac{\log p}{2[F(p) : \mathbb{Q}_p]} \#(Cw_0) \geq \frac{\log p}{2p^4[K : \mathbb{Q}][F(p) : \mathbb{Q}_p]},\end{aligned}$$

the last inequality coming from Lemma 3.5 applied to $L = L'(N)$ and $H = \mathrm{Gal}(L'(N)/L'(N/p))$, which has cardinality at most p^4. ∎

Let $\tilde{\Phi} \in \mathrm{Gal}(\overline{\kappa}/\kappa)$ be the Frobenius element, where κ denotes the residual field of F. By [20, Chapter 13, Theorem 6.3], there are $k, m \in \mathbb{N}$ satisfying $\tilde{\Phi}^k = [p^m]$ on $\tilde{E}$, the reduction of E modulo v. As $F/\mathbb{Q}_p$ is unramified, $\tilde{\Phi}$ identifies with an element $\Phi \in \mathrm{Gal}(\mathbb{Q}_p^{ur}/F)$.

Lemma 5.8. *Take $N \in \mathbb{N}$ divisible by $p^2 - 1$, but not by p^2. If $A \in E(LK^{tv}(N))\backslash E_{\mathrm{tors}}$, then there is $B \in E(\overline{K})\backslash E_{\mathrm{tors}}$ with $\hat{h}(B) \leq 4p^{2m+8}\hat{h}(A)$ and $\hat{h}_v(B) \geq l$.*

Proof. By replacing N with pN if needed, we can assume that $p \mid N$ and $p^2 \nmid N$.

Let $M \subset K^{tv}$ be a number field, Galois over K, such that $A \in E(LM(N))$. Suppose that some conjugate A' of A over K satisfies $[p^2(p^2-1)]A' \notin E(F(N/p))$. Then the lemma is a trivial consequence of Lemma 5.7 applied to $A = A'$. So assume that $\sigma A' = [p^2(p^2-1)]\sigma A \in E(F(N/p))$ for all $\sigma \in \mathrm{Gal}(LM(N)/K)$, where $A' = [p^2(p^2-1)]A$. We can apply Lemma 5.3 to the coordinates of A' with respect to our fixed Weierstrass model to find that A' actually lies in $E(LM(N/p))$.

The extension $F(N/p)/F$ is unramified since p does not divide N/p. By abuse of notation, we denote the restriction of Φ to $F(N/p)$ also by Φ. As N/p is coprime to p, we see that $E[N/p] \simeq \tilde{E}[N/p]$. As $\tilde{\Phi}^k = [p^m]$, we deduce from the last isomorphism that Φ^k acts on $E[N/p]$ as multiplication by $[p^m]$. By Lemma 4.2 applied to $N = N/p$, we conclude that Φ^k belongs to the center of $\mathrm{Gal}(LM(N/p)/K)$.

Put $B = \Phi^k A' - [p^m]A'$, which is non-zero by Lemma 5.6. We have

$$\hat{h}(B) \leq 2(\hat{h}(\Phi^k A') + \hat{h}([p^m]A')) = 2(1+p^{2m})\hat{h}(A') \leq 4p^{2m+8}\hat{h}(A).$$

Denote by v_0 the place of $LM(N/p)$ associated to the embedding $\overline{K} \to \overline{K_v}$. Let w be a place of $LM(N/p)$ above v. There is $\sigma \in \mathrm{Gal}(LM(N/p)/K)$ such that $w = \sigma^{-1}v_0$. A small calculation gives

$$\lambda_w(B) = \frac{1}{2}\log\max\{1, |x(B)|_w\} = \frac{1}{2}\log\max\{1, |x(\sigma B)|_{v_0}\} = \lambda_v(\sigma B).$$

As Φ^k commutes with σ, we get $\sigma B = \Phi^k \sigma A' - [p^m]\sigma A' \neq O$. However, it is clear that σB reduces to O modulo v. Thus $|x(\sigma B)|_v \geq p$ since $F(N/p)/\mathbb{Q}_p$ is unramified. In conclusion, $\lambda_w(B) \geq (\log p)/2$ for all places w of $LM(N/p)$ above v and the definition of $\hat{h}_v$ leads to $\hat{h}_v(B) \geq (\log p)/2 \geq l$, which finishes the proof. ∎

Proposition 5.9. *Let $A \in E(LK^{tv}(E_{\mathrm{tors}}))\backslash E_{\mathrm{tors}}$. Then there is $B \in E(\overline{K})\backslash E_{\mathrm{tors}}$ with $\hat{h}(B) \leq 16D^2p^{2m+8}\hat{h}(A)$ and $\hat{h}_v(B) \geq l$, where $D = 2^{[F:\mathbb{Q}_{p^2}](p^2-1)}$.*

Proof. There are $N \in \mathbb{N}$ divisible by p^2-1 and a number field $M \subset K^{tv}$, Galois over K, such that $A \in E(LM(N))$. Put $L' = LM$ and write n for the p-adic valuation of N. Let $\tau = \tau_2$ be the homomorphism coming from Lemma 3.6 and set $C = \tau A - [D]A \in E(L'(N))$. It is not a torsion point by Lemma 5.6. Moreover, the parallelogram equality and other basic properties of the Néron–Tate height give

$$\hat{h}(C) \leq 2(\hat{h}(\tau A) + \hat{h}([D]A)) \leq 4D^2\hat{h}(A).$$

Let $n' \geq 0$ be the least integer such that $C \in E(L'(p^{n'-n}N))$. Of course, $n' \leq n$.

If $n' \leq 1$, then Lemma 5.8 applied to $A = C$ provides a non-torsion point $B \in E(\overline{K})$ satisfying $\hat{h}(B) \leq 4p^{2m+8}\hat{h}(C) \leq 16D^2p^{2m+8}\hat{h}(A)$ and $\hat{h}_v(B) \geq l$, which proves the proposition. So assume that $n' \geq 2$. By minimality of n' and by Lemma 5.3, there exists $\sigma \in \mathrm{Gal}(L'(N)/K)$ such that $C' = \sigma C \notin E(F(N'/p))$, where $N' = p^{n'-n}N$. Choose $\psi \in \mathrm{Gal}(F(N)/F(N'/p))$ such that $\psi C' \neq C'$.

Set $A' = \sigma A$. As τ and σ commute by Lemma 4.2, we obtain

$$C' = \tau A' - [D]A' \in E(L'(N')).$$

To deduce the proposition, it suffices to apply Lemma 5.7 to $A = C'$ and $N = N'$. For this, we only need to show that $[p^2]C' \notin E(F(N'/p))$. Suppose that the contrary is true. Then $\psi C' - C' = T \in E[p^2]\backslash\{O\}$. As ψ and τ commute by Lemma 4.2, it follows from the definition of C' that

$$C' + T = \psi C' = \tau\psi A' - [D]\psi A'.$$

A short calculation proves that $T = \tau P - [D]P$, where $P = \psi A' - A' \in E(L'(N))$. By Lemma 5.6, P is a torsion point. We fix $M' \in \mathbb{N}$ coprime to p such that $[M']P$ has order a power of p. By Lemma 5.4, $[M']P \in E[p^n]$ and Lemma 3.6(ii) ensure that $\tau([M']P) = [DM']P$. Hence, $[M']T = [p^2]T = O$, which is possible only if $T = O$ since M' and p are coprime, a contradiction. ∎

A proof of the next lemma can be found in [25, Lemme 4.4].

LEMMA 5.10. *Let (Q_n) be a sequence in $E(\overline{K})\backslash E_{\mathrm{tors}}$ such that $\hat{h}(Q_n) \to 0$. Then $\liminf_{n\to\infty} \hat{h}_\infty(Q_n) \geq 0$. Also, $\liminf_{n\to\infty} \hat{h}_\nu(Q_n) \geq 0$ if ν is a finite place of K. More precisely, $\hat{h}_\nu(Q_n) \geq 0$ for all n if E has good reduction at ν.*

Proof of Theorem 1.6, elliptic case. Assume by contradiction that there is a sequence (A_n) of non-torsion points in $E(LK^{tv}(E_{\mathrm{tors}}))$ with $\hat{h}(A_n) \to 0$. Proposition 5.9 yields a new sequence (B_n) of non-torsion points in $E(\overline{K})$ such that $\hat{h}(B_n) \to 0$ and $\hat{h}_v(B_n) \geq l$ for all n. Lemma 5.10 shows that

$$\begin{aligned}\hat{h}(B_n) = \sum_\nu \hat{h}_\nu(B_n) &\geq \hat{h}_v(B_n) + \hat{h}_\infty(B_n) + \sum_{\nu\in\mathcal{M}} \hat{h}_\nu(B_n) \\ &\geq l + \hat{h}_\infty(B_n) + \sum_{\nu\in\mathcal{M}} \hat{h}_\nu(B_n),\end{aligned}$$

where $\mathcal{M}$ is the (finite) set of places of K with bad reduction. Again, Lemma 5.10 allows us to conclude that $\liminf_{n\to\infty} \hat{h}(B_n) \geq l$, a contradiction. □

Acknowledgements. I thank P. Habegger and L. Pottmeyer for replying to my questions as well as F. Amoroso and L. Terracini for pointing out a mistake in an earlier version of this text. This work was funded by Morningside Center of Mathematics, CAS.

References

[1] F. Amoroso, S. David and U. Zannier, *On fields with the property (B)*, Proc. Amer. Math. Soc. 142 (2014), 1893–1910.

[2] F. Amoroso and R. Dvornicich, *A lower bound for the height in abelian extensions*, J. Number Theory 595 (2000), 260–272.

[3] F. Amoroso and U. Zannier, *A uniform relative Dobrowolski's lower bound over abelian extensions*, Bull. London Math. Soc. 42 (2010), 489–498.

[4] M. Baker, *Lower bound for the canonical height on elliptic curves over abelian extensions*, Int. Math. Res. Notices 2003, 1571–1589.

[5] M. Baker and C. Petsche, *Global discrepancy and small points on elliptic curves*, Int. Math. Res. Notices 2005, 3791–3834.

[6] M. Baker and J. H. Silverman, *A lower bound for the canonical height on abelian varieties over abelian extensions*, Math. Res. Lett. 11 (2004), 377–396.

[7] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge Univ. Press, Cambridge, 2006.

[8] E. Bombieri and U. Zannier, *A note on heights in certain infinite extensions of* $\mathbb{Q}$, Rend. Lincei Mat. Appl. 12 (2001), 5–14.

[9] M. Carrizosa, *Petits points et multiplication complexe*, Int. Math. Res. Notices 2009, 3016–3097.

[10] S. Checcoli, *Fields of algebraic numbers with bounded local degrees and their properties*, Trans. Amer. Math. Soc. 365 (2013), 2223–2240.

[11] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. 34 (1979), 391–401.

[12] N. D. Elkies, *Supersingular primes of a given elliptic curve over a number field*, Ph.D. thesis, Univ. of Harvard, 1987.

[13] P. Fili and Z. Milner, *Equidistribution and the heights of totally real and totally p-adic numbers*, Acta Arith. 170 (2015), 15–25.

[14] L. Frey, *Height lower bounds in some non-abelian extensions*, Ph.D. thesis, Basel Univ., 2018.

[15] L. Frey, *Explicit small heights in infinite non-abelian extensions*, Acta Arith. 199 (2021), 111–133.

[16] L. Frey, *Small heights in large non-Abelian extensions*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (5) 23 (2022), 1357–1393.

[17] A. Galateau, *Small height in fields generated by singular moduli*, Proc. Amer. Math. Soc. 144 (2016), 2771–2786.

[18] R. Grizzard, *Relative Bogomolov extensions*, Acta Arith. 170 (2015), 1–13.

[19] P. Habegger, *Small height and infinite nonabelian extensions*, Duke Math. J. 162 (2013), 2027–2076.

[20] D. Husemöller, *Elliptic Curves*, Grad. Texts in Math. 111, Springer, New York, 2004.

[21] LMFDB Collaboration, http://www.lmfdb.org, 2013.

[22] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer, Berlin, 1999.

[23] F. Pazuki and R. Pengo, *On the Northcott property for special values of L-functions*, Rev. Mat. Iberoamer. 40 (2024), 1–42.

[24] A. Plessis, *Minoration de la hauteur de Weil dans un compositum de corps de rayon*, J. Number Theory 205 (2019), 246–276.

[25] A. Plessis, *Points de petite hauteur sur une variété semi-abélienne isotriviale de la forme* $\mathbb{G}_m^n \times A$, Bull. London Math. Soc. 54 (2022), 2278–2296.

[26] L. Pottmeyer, *Heights of points with bounded ramification*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (5) 14 (2015), 965–981.
[27] J. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), 64–94.
[28] A. Schinzel, *On the product of the conjugates outside the unit circle of an algebraic number*, Acta Arith. 24 (1973), 385–399.
[29] J.-P. Serre, *Corps locaux*, 2nd ed., Publications de l'Université de Nancago VIII, Hermann, Paris, 1968.
[30] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), 259–331.
[31] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, New York, 1994.
[32] J. H. Silverman, *A lower bound for the canonical height on elliptic curves over abelian extensions*, J. Number Theory 104 (2004), 353–372.
[33] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math. 106, Springer, Dordrecht, 2009.
[34] S. Zhang, *Equidistribution of small points on abelian varieties*, Ann. of Math. 147 (1998), 159–165.

Arnaud Plessis
Beijing Institute of Mathematical Sciences and Applications
101408, Beijing, P.R. China
E-mail: plessis@bimsa.cn