UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

Ricardo Silva Toso

A lower bound for the canonical height on elliptic curves over abelian extensions

Rio de Janeiro
2014

Ricardo Silva Toso

A lower bound for the canonical height on elliptic curves over abelian extensions

Dissertação de Mestrado submetida ao Programa de Pós-graduação do Instituto de Matemática da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Orientador: Amílcar Pacheco

Rio de Janeiro

2014

T714l Toso, Ricardo Silva
A lower bound for the canonical height on elliptic curves over abelian extensions / Ricardo Silva Toso. – Rio de Janeiro, 2014.
51 f. : il.; 30 cm.

Orientador: Amílcar Pacheco

Dissertação (mestrado) – UFRJ / Instituto de Matemática, Programa de Pós-graduação em Matemática, 2014.
Referências: f. 44-46

1. Curves, Elliptic – Thesis 2. Algebraic Geometry 3. Algebraic Number Theory I. Pacheco, Amílcar (Orient.). II. Universidade Federal do Rio de Janeiro, Instituto de Matemática, Programa de Pós-graduação em Matemática. III. Título.

CDD 512

A lower bound for the canonical height on elliptic curves over abelian extensions

de

Ricardo Silva Toso

Orientador: Amílcar Pacheco

Dissertação de Mestrado submetida ao Programa de Pós-graduação do Instituto de Matemática da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Aprovada em 4 de Abril de 2014, por:

____

Presidente, Professor Amílcar Pacheco, IM-UFRJ

____

Professor Aftab Pande, IM-UFRJ

____

Professora Cecília Salgado Guimarães da Silva, IM-UFRJ

____

Professor Rodrigo Salomão, IM-UFF

____

Suplente, Professor Ilir Snopche, IM-UFRJ

Rio de Janeiro

2014

Agradecimentos

À minha família e amigos por todo apoio e incentivo.

Ao meu professor orientador Amílcar pela excelente orientação.

Aos professores da banca pela dedicação e paciência de ler meu trabalho.

À professora Victoria pelo empenho na revisão do inglês.

Ao CNPq e à FAPERJ pelo apoio financeiro.

Abstract

Let $K/\mathbb{Q}$ be a number field and let K^{ab} be the maximal abelian extension of K. Let E/K be an elliptic curve and let $\hat{h} : E(\bar{K}) \to \mathbb{R}$ be the canonical height on E. In this dissertation we prove the existence of a constant $C = C(E/K) > 0$ such that $\hat{h}(P) \geq C$ for all nontorsion $P \in E(K^{ab})$.

Keywords: Elliptic Curve, Number Field, Canonical Height, Lehmer's Conjecture.

Resumo

Seja $K/\mathbb{Q}$ um corpo de números e K^{ab} a extensão abeliana maximal de K. Seja E/K uma curva elítica e $\hat{h} : E(\bar{K}) \to \mathbb{R}$ a altura canônica em E. Nesta dissertação prova-se a existência de uma constante $C = C(E/K) > 0$ tal que $\hat{h}(P) \geq C$ para todos os pontos $P \in E(K^{ab})$ que não são de torção.

Palavras-chave: Curva Elítica, Corpo de Números, Altura Canônica, Conjectura de Lehmer.

Contents

1 Introduction

The main objective of this text is to present an article due to Joseph H. Silverman [Si04], where he extends the work of Baker [Ba03], proving a lower bound for the canonical height (on elliptic curves over number fields) restricted to nontorsion points in the maximal abelian extension. In this section we are going to, from a pedestrian point of view, briefly discuss some of the contents and ideas that will appear throughout this dissertation.

One of the central objects here is the canonical height on elliptic curves (also known as the Néron-Tate height). Roughly speaking, a height is a function which measures the arithmetic complexity of a point in a set with an arithmetic structure. For example, in some sense the rational numbers

$$\frac{1}{3} \qquad \text{and} \qquad \frac{100000}{300001}$$

are very "close" to one another, however, the second is much more arithmetically complicated than the first, so a height function over $\mathbb{Q}$ would attain a much higher value when computed on the second point than on the first one. Note that in mathematics, what is known as height may change according to the subject and there is no precise definition of what is called a height function. However, usually the guiding principles for calling something a height, besides the arithmetic complexity measurement, are the concepts of geometric relations leading to height relations and the existence of only finitely many points of bounded height.

Now that we have briefly introduced what a height is, to contextualize the main problem of this text we shall briefly discuss the conjecture which in some sense is the origin of such a problem, namely: the classical Lehmer conjecture. It states that there exists a constant $C > 0$ such that the absolute logarithmic height h on $\bar{\mathbb{Q}}^*$ satisfies $h(\alpha) \geq C/[\mathbb{Q}(\alpha) : \mathbb{Q}]$ for every $\alpha \in \bar{\mathbb{Q}}^*$ that is not a root of unity, i.e., roughly, it is asserting that every nonroot of unity element of $\bar{\mathbb{Q}}^*$ has at least a certain minimal arithmetic complexity which depends only on the degree of such an element over $\mathbb{Q}$.

This problem has revealed itself to be very difficult and survived for over 80 years. It was first proposed in one of its earliest forms by Derrick H. Lehmer in 1933 [Le33] and up to now it has still not been solved. Currently, the best known result in the direction of this conjecture is Dobrowolski's estimate [Do79],

$$h(\alpha) \geq \frac{C}{D}\left(\frac{\log\log D}{\log D}\right)^3,$$

where $D := [\mathbb{Q}(\alpha) : \mathbb{Q}]$ and α runs over all the elements of $\bar{\mathbb{Q}}^*$ which are not roots of unity.

Now getting back to our subject, as the reader may already be aware, every elliptic curve has a group structure attached to it, and so it makes sense to talk about the arithmetic of an elliptic curve (relative to such a group structure). The canonical height on elliptic curves, that we have briefly mentioned at the beginning and that we shall always denote by $\hat{h}$, is in some sense the most outstanding height to measure such arithmetic complexity. It is derived from the ordinary height h for elliptic curves, which for a number field K and an elliptic curve E/K, can be computed for any $P \in E(\bar{K})$ by

$$h(P) := \frac{1}{2[L:\mathbb{Q}]} \sum_{w \in M_L} \max\{-[L_w : \mathbb{Q}_w] w(x(P)), 0\},$$

where L/K is any finite extension such that $P \in E(L)$, and M_L as usual is the set of normalized representatives for the places of L. With these settings, the canonical height $\hat{h}$ is then a certain limiting process of these ordinary heights, precisely

$$\hat{h}(P) := \lim_{n\to\infty} \frac{1}{n^2} h([n]P).$$

As was mentioned earlier, this height will be a central object in this dissertation. Throughout this text, whenever we require some of its properties, we will always try to provide further references and clarifications, therefore in this section we won't go any further. For a much more specific description and construction one can refer to [Si09, VIII].

Keeping the canonical height in mind, we may turn back to the Lehmer conjecture and try to contrast our elliptic settings with the classical number theoretical settings, and so as the reader may have already guessed, what we define as the elliptic Lehmer conjecture is the "translation" of the classical Lehmer conjecture to the case of elliptic curves. In summary, it asserts that every nontorsion point in an elliptic curve has at least a certain minimal arithmetic complexity, which depends on the curve and the degree of such a point over the field of definition of the curve. Formally, the elliptic analogue of the classical Lehmer conjecture states:

Conjecture 1.1. *Let E/K be an elliptic curve defined over a number field K and let $\hat{h}$ be the canonical height on E. For any $P \in E(\bar{K})$, denote by $K(P)$ its minimal field of definition over K and set $D(P) := [K(P) : K]$. Then, there exists a constant $C = C(E/K) > 0$ such that*

$$\hat{h}(P) \geq \frac{C}{D(P)} \quad \textit{for all nontorsion points } P \in E(\bar{K}).$$

(The "$C = C(E/K)$" is just to reflect the fact that C depends on E/K.)

Even though much progress has been made in the direction of this conjecture, up to now it remains unsolved. The next table provides a small list of some of the most relevant recent improvements toward it.

History of lower bounds for $\hat{h}$ in $E(\bar{K}) \setminus \{tors\}$. ($D := [K(P) : K]$)

$\hat{h}(P) \geq$	Restriction on E	Reference
$C/(D^{10}(\log D)^6)$	none	Anderson-Masser [AnMa80]
$C/(D(\frac{\log D}{\log\log D})^3)$	CM	Laurent [La83]
$C/(D^3(\log D)^2)$	none	Masser [Ma89]
$C/(D^2(\log D)^2)$	$j(E)$ nonintegral	Hindry-Silverman [HiSi90]

Besides the classical settings and the configuration for elliptic curves over number fields that we just mentioned, the Lehmer conjecture can also be considered for many other subjects, for instance, abelian varieties. Indeed, we point out that Masser [Ma84] could prove a very strong bound in the direction of the abelian varieties analogue of Lehmer's conjecture. Furthermore, assuming complex multiplication, David and Hindry [DaHi00] could generalize the Dobrowolski-type estimate for the elliptic case (given by Laurent, see table above) to the abelian variety case.

As the reader may have already noticed at this point, the kind of problem presented by Lehmer's conjecture gives rise to a very rich field of questions and problems going much beyond just number theory. In this dissertation we shall work solely toward the elliptic Lehmer conjecture over number fields, and indeed we will end up proving it for points that are defined over the maximal abelian extension. But note that in a general sense, what we are doing here is just scratching the surface of this vast and elegant question.

Now to contrast what we are going to handle ahead we turn back once more to the classical Lehmer conjecture, for even though this conjecture in the general settings remains open, a natural approach would be to consider it with some restrictions. A very peculiar case is the one occurring when we restrict the conjecture to the maximal abelian extension. In such a case, Amoroso and Dvornicich [AmDv00] produced a lower bound that is even stronger than the one proposed by the general conjecture (but which of course is restricted only to points in the maximal abelian extension). Precisely, they proved the existence of a constant $C > 0$ such that the absolute logarithmic height h on $\bar{\mathbb{Q}}^*$ satisfies

$$h(\alpha) \geq C \quad \text{for all nonroot of unity } \alpha \in \mathbb{Q}^{ab^*}.$$

With this approach to the classical Lehmer conjecture in mind, the natural question when looking back at the elliptic Lehmer conjecture would be to ask if some better estimates could also be produced for the elliptic case if we restrict the conjecture just to points defined over the maximal abelian extension of our field of definition. In the last 30 years, much progress has been made in this direction, culminating in Silverman's article [Si04] where, making use of Baker [Ba03], he finally was able to prove that in the elliptic case it is also possible to bound with a constant. The following table provides some of the history concerning the progress made in this variant of the conjecture, i.e., the elliptic Lehmer conjecture (over number fields) restricted to points defined over the maximal abelian extension of the field of definition.

History of lower bounds for $\hat{h}$ in $E(K^{ab}) \setminus \{tors\}$. $(D := [K(P) : K])$

$\hat{h}(P) \geq$	Restriction on E	Reference
$C/(D^2)$	none	Silverman [Si81]
$C/(D(\log D)^2)$	none	Masser [Ma89]
$C/(D^{2/3})$	$j(E)$ nonintegral	Hindry-Silverman [HiSi90]
C	CM or $j(E)$ nonintegral	Baker [Ba03]
C	none	Silverman [Si04]

This last article [Si04] in the table above will be what we work on here in this text. So, we formally state once and for all the main objective of this dissertation:

Theorem 1.2. *Let K be a number field, let E/K be an elliptic curve, and let $\hat{h} : E(\bar{K}) \to \mathbb{R}$ be the canonical height on E. Then there exists a constant $C = C(E/K) > 0$ such that*

$$\hat{h}(P) \geq C \ \text{ for all nontorsion } P \in E(K^{ab}).$$

In addition, it is relevant to point out that after establishing this result, Silverman and Baker worked together to prove the abelian varieties analogue of this same result, which was published in [BaSi04]. Furthermore, the same kind of problem presented in Theorem 1.2 has also been considered for Drinfeld modules of arbitrary rank, and indeed, this configuration of the problem has already been solved by David and Pacheco in [DaPa08].

Now that our main problem has been introduced, we will provide a brief sketch of the method of the proof, so the reader can be somewhat aware of why we are building theorems in a certain way during each one of the sections ahead.

Sketch:

Since the case in which the elliptic curve E has complex multiplication has already been proved by Baker [Ba03], we may assume that our curve E does not have CM, i.e., $\mathrm{End}(E) \equiv \mathbb{Z}$. So with this additional assumption in hand, we fix a prime $\mathfrak{p}$ of K, which we take satisfying some very useful properties and whose existence is guaranteed due to our section 4. Next for a given generic nontorsion $P \in E(K^{ab})$, we define $L := K(P)$ (i.e., the minimal field of definition for P over K), thus we know that L/K is Galois, and therefore the ramification index of all the primes of L lying over $\mathfrak{p}$ is the same. The demonstration then proceeds by splitting in two cases according to this ramification index:

— The first one is when our prime $\mathfrak{p}$ does not ramify in the extension L/K. In this case we can use the results we are going to build in section 5 to prove the existence of a certain point $(\Phi_{\mathfrak{p}}(\sigma)P)$ that has a lot of useful properties. With this new point and its properties in hand, we then use our results from section 3 to produce a lower bound for the (global) canonical height of this point $(\Phi_{\mathfrak{p}}(\sigma)P)$, and thus finally, using this last bound, we produce a lower bound for the (global) canonical height of P.

— The second case is when our prime $\mathfrak{p}$ does ramify in the extension L/K. Here we can use the results we are going to build in section 6 to prove the existence of another certain point $([p]((\tau-1)^2P))$ that also has a lot of useful properties. So with this new point and its properties in hand, we proceed in a similar way as in the previous case. i.e., we use our results from section 3 to produce a lower bound for the (global) canonical height of this new point $([p]((\tau-1)^2P))$, and then finally, using this last bound, we produce a lower bound for the (global) canonical height of P.

2 Notation and Preliminaries

In this section we recall some well known results concerning algebraic number theory and elliptic curves that will be used over and over throughout this dissertation. This is also the section where we set notation, and indeed, we start by doing that. We set the following notation:

$K/\mathbb{Q}$ a number field.

$\mathcal{O}_K$ the ring of integers of K.

$\bar{K}$ the algebraic closure of K.

K^{ab} the maximal abelian extension of K.

K_v the completion of K with respect to a valuation v.

$K_\mathfrak{p}$ the completion of K with respect to a valuation $v_\mathfrak{p}$ of a prime $\mathfrak{p}$.

E/K an elliptic curve defined over K.

$\hat{h} : E(\bar{K}) \to \mathbb{R}$ the canonical height on E.

$\hat{\lambda}_v : E(\bar{K}) \smallsetminus \{O\} \to \mathbb{R}$ the local canonical height on E associated to a place v of K, and normalized as described in [Si94, VI 1.1].

Note that unless otherwise specified, we shall always consider this notation as fixed. Even though, whenever we enunciate a theorem or any kind of formal statement, we will always try to be very specific and precise, therefore we will naturally end up rewriting some of this notation. The only exceptions to this are the two heights above, which we will always consider as being the ones relative to the elliptic curve we are handling without further ado (since there is always going to be only one curve, this won't cause any problem at all). Also note that, although we have set all of the above notation for a fixed number field K, whenever we are handling another number field, say F, we will use the same notation for the objects attached to F in the very obvious way, for instance: $\bar{F}$ for the algebraic closure, $\mathcal{O}_F$ for the ring of integers, and so on.

Next, for a generic number field $F/\mathbb{Q}$, we denote by M_F the set of absolute values on F extending the usual absolute values on $\mathbb{Q}$. And just to clarify, by "usual absolute values on $\mathbb{Q}$" we mean the $|\,.\,|_p$'s defined by

$$\left|p^n \frac{a}{b}\right|_p := p^{-n} \quad \text{for } a, b \in \mathbb{Z} \text{ satisfying } p \nmid ab,$$

together with the $|\,.\,|_\infty$ defined by $|x|_\infty := \max\{x, -x\}$.

For any absolute value $|\,.\,|_v \in M_F$, we write $v(\,.\,) := -\log|\,.\,|_v$, and from now on through this correspondence we make the standard abuse of considering M_F also as the set of such functions. Note that this way the representatives we are taking for the equivalence classes of valuations are normalized in a manner slightly different from the usual, since for a finite place associated to a prime $\mathfrak{p}$ of F, it is standard to set the representative for the associated equivalence class of valuations as being the function $v_{\mathfrak{p}}(x) := Ord_{\mathfrak{p}}(x)$, and so one has $v_{\mathfrak{p}}(F^*) = \mathbb{Z}$. On the other hand, here we are taking the representatives defined by $v(x) := -\log|x|_v$, so we won't have $v(F) = \mathbb{Z}$. The reason for us to take the representatives normalized in this unusual way is to be in agreement with [Si94, VI], which makes this assumption to conclude many formulas and theorems that are of great relevance to this dissertation. (Also note that this choice provides that on a finite extension L/K, if $w \in M_L$ lies over $v \in M_K$, then $w(\alpha) = v(\alpha)$ for any $\alpha \in K$, which can ease many calculations.)

Now that we have set notation, we start to recall some basic results from algebraic number theory that will be used frequently, and so they are restated here for the convenience of the reader.

The first one is the product formula [La94, V §1], which if we assume that the set of valuations M_K is normalized as above, then it may be rewritten as the standard summation

$$\sum_{v \in M_K} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} v(\alpha) = 0 \quad \forall \alpha \in K^*. \tag{2.1}$$

Further, for a finite extension L/K, we recall the extension formula [La94, II §1 Corollary 1],

$$\sum_{w \in M_L, w|v} [L_w : K_v] = [L : K]. \tag{2.2}$$

Finally, we note that since we are assuming $v\,(\,.\,) := -\log|\,.\,|_v$ and the absolute values we are considering are the ones extending the usual ones from $\mathbb{Q}$, if we denote by $v_{\mathfrak{p}}$ the valuation associated to a prime $\mathfrak{p}$ of K, then $v_{\mathfrak{p}}$ is discrete and its smallest positive value is $(\log p)/e(\mathfrak{p}/K/\mathbb{Q})$, i.e.,

$$\inf\{v_{\mathfrak{p}}(\alpha)\ ;\ \alpha \in K^* \text{ and } v_{\mathfrak{p}}(\alpha) > 0\} = \frac{\log p}{e(\mathfrak{p}, K/\mathbb{Q})}, \tag{2.3}$$

where $e(\mathfrak{p}, K/\mathbb{Q})$ denotes the ramification index of $\mathfrak{p}$ in the extension $K/\mathbb{Q}$, or equivalently, of $\mathfrak{p}$ over p. And just to clarify why the above statement is true: if we set $e := e(\mathfrak{p}, K/\mathbb{Q})$ and take any uniformizer $\pi \in K_{\mathfrak{p}}$ for $\mathfrak{p}$, then locally we have $(p) = (\pi)^e$, thus $v_{\mathfrak{p}}(\pi) = v_{\mathfrak{p}}(p)/e = (\log p)/e$.

Now again for the convenience of the reader, we shall also restate two key results about the canonical height that are crucial to this work.

The first one is [Si94, VI 2.1], which asserts that for any finite extension L/K of our field of definition K, the canonical height on E can be written as a certain summation over the local canonical heights of the places from L. Precisely, it states

$$\hat{h}(P) = \sum_{w \in M_L} \frac{[L_w : \mathbb{Q}_w]}{[L : \mathbb{Q}]} \hat{\lambda}_w(P) \quad \forall P \in E(L) \smallsetminus \{O\}. \tag{2.4}$$

Next we have [Si94, VI 1.1], which provides that if E/L_w is an elliptic curve defined over a field L_w that is complete with respect to a nonarchimedean valuation w, then for any w-integral Weierstrass equation for E we have

$$\hat{\lambda}_w(P) = \frac{1}{12}w(\Delta) + \frac{1}{2}\max\{w(x(P)^{-1}), 0\} \quad \forall P \in E_0(L_w) \smallsetminus \{O\}, \qquad (2.5)$$

where Δ is the discriminant of the Weierstrass equation, and $E_0(L_w)$ is the set of points in $E(L_w)$ with nonsingular reduction modulo w.

This identity (2.5) will be of such major importance to this work that we shall once and for all reformulate it into the format it will be used throughout this dissertation. This reformulation is our first lemma, even though in some sense it is just a corollary of (2.5).

Lemma 2.1. *Let K be a number field, let E/K be an elliptic curve, let $v \in M_K$ be a finite place of good reduction for E and fix a minimal Weierstrass equation for E at v, say*

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

Let L/K be any finite extension and let $w \in M_L$ be a place of L lying over v. Then for all points $P \in E(L) \smallsetminus \{O\}$ such that $w(x(P)) < 0$ or $w(y(P)) < 0$, we have

$$\hat{\lambda}_w(P) = w(x(P)/y(P)) > 0.$$

Proof. Since we are assuming that E has good reduction at v (therefore also at w) and fixing a Weierstrass which is minimal, we have $w(\Delta) = 0$ and $E_0(L_w) = E(L_w)$. Thus (2.5) gives us

$$\hat{\lambda}_w(P) = \max\{\frac{1}{2}w(x(P)^{-1}), 0\} \quad \forall P \in E(L) \smallsetminus \{O\}.$$

Furthermore, due to the integrality of the minimal Weierstrass equation, one has

$$w(x) < 0 \iff w(y) < 0,$$

and in this case, from a standard computation with the equation we get $w(y^2) = w(x^3)$, which implies that $w(x^{-1}) = 2w(x/y)$. Hence, for any point $P \in E(L) \smallsetminus \{O\}$ we have

$$w(x(P)) < 0 \text{ or } w(y(P)) < 0 \implies \frac{1}{2}w(x(P)^{-1}) = w(x(P)/y(P)) > 0.$$

Thus from the previous identity for $\hat{\lambda}_w(P)$, we see that if $P \in E(L) \smallsetminus \{O\}$ satisfies $w(x(P)) < 0$ or $w(y(P)) < 0$, then

$$\hat{\lambda}_w(P) = \frac{1}{2}w(x(P)^{-1}) = w(x(P)/y(P)) > 0.$$

□

3 Some Useful Lower Bounds

The main objective of this section is to build results in a way that allows us to translate some lower bounds for a particular set of local canonical heights of a point, into a lower bound for the (global) canonical height of this same point. In order to do that we must first prove a key lemma. Once this lemma is established, the theorem that is the main result of this section will follow as a corollary.

Lemma 3.1. *If E/K is an elliptic curve defined over a number field K, then there exists a constant $C_0 = C_0(E/K) \geq 0$ such that for any finite extension L/K we have*

$$\sum_{w \in M_L} \frac{[L_w : \mathbb{Q}_w]}{[L : \mathbb{Q}]} \min\{\hat{\lambda}_w(P), 0\} \geq -C_0 \quad \forall P \in E(L) \smallsetminus \{O\}.$$

Proof. We begin by decomposing the above sum into three sums, each one over a certain subset of M_L. Namely, we split M_L into the three following sets:

M_L^{good}	the set of finite good reduction places for E.
M_L^{bad}	the set of finite bad reduction places for E.
M_L^{∞}	the set of archimedean places (infinite places).

First we handle the summation over M_L^{good} which is the easiest of all three, for if $w \in M_L^{good}$, then $E_0(L_w) = E(L_w)$ and the discriminant Δ of any minimal Weierstrass equation for E at w satisfies $w(\Delta) = 0$, so for any point $P \in E(L) \smallsetminus \{O\}$ the formula (2.5) mentioned in the previous section immediately gives us $\hat{\lambda}_w(P) \geq 0$, and thus $\min\{\hat{\lambda}_w(P), 0\} = 0$ for all such places $w \in M_L^{good}$. Therefore we have just proven a "bound" for our first partial sum

$$\sum_{w \in M_L^{good}} \frac{[L_w : \mathbb{Q}_w]}{[K : \mathbb{Q}]} \min\{\hat{\lambda}_w(P), 0\} = 0 \quad \forall P \in E(L) \smallsetminus \{O\}.$$

Second, we deal with the summation over M_L^{bad}. We start by taking a generic $w \in M_L^{bad}$, then we consider the place $v \in M_K^{bad}$ lying below w and proceed according to how the bad reduction of E at v behaves. If E has split multiplicative reduction at v, then [Si09, VII 5.5] guarantees $|j(E)|_v > 1$, thus we know that E can be identified (over K_v) to a certain Tate curve E_{q_v}/K_v ($|q_v|_v < 1$, see [Si94, V 5.3(b)]). On the other hand, we may also consider this curve E_{q_v} as a Tate curve defined over L_w (since $K_v \subset L_w$ and $w_{|K} = v$), so we can write the usual Tate parametrization for it over L_w, i.e.,

$$\phi : L_w^*/q_v^{\mathbb{Z}} \xrightarrow{\sim} E_{q_v}(L_w).$$

This way we are able to evoke [Si94, VI 4.2.b] for E_{q_v}/L_w, which asserts that in this parametrization, if we choose the representatives modulo $q_v^{\mathbb{Z}}$ for $u(P) := \phi^{-1}(P)$ to satisfy

$$0 \leq w(u(P)) < w(q_v),$$

then the local canonical height $\hat{\lambda}_w$ on $E_{q_v}(L_w)$ is given by the explicit formula

$$\hat{\lambda}_w(P) = \begin{cases} \frac{1}{2}\mathbb{B}_2\left(\frac{w(u)}{w(q_v)}\right) w(q_v) & \text{if } 0 < w(u) < w(q_v) \\ \frac{1}{12} w(q_v) + w(1-u) & \text{if } w(u) = 0 \end{cases}$$

where $u = u(P) = \phi^{-1}(P)$ and $\mathbb{B}_2(t)$ is the second Bernoulli polynomial (i.e., $t^2 - t + \frac{1}{6}$) for $0 \leq t \leq 1$ extended periodically to $\mathbb{R}/\mathbb{Z}$.

So, using the fact that $\mathbb{B}_2(t)$ has a minimum at $t = 1/2$ and $\mathbb{B}_2(1/2) = -1/12$, we can compute

$$\hat{\lambda}_w(P) = \frac{1}{2}\mathbb{B}_2\left(\frac{w(u(P))}{w(q_v)}\right)w(q_v) \geq -\frac{1}{24}w(q_v) = \frac{1}{24}\log|q_v|_v$$

$$\forall P \in E_{q_v}(L_w) \smallsetminus \{O\}.$$

Therefore, as $|q_v|_v < 1$, for an appropriate constant $C_v > 0$ we may write

$$\hat{\lambda}_w(P) > -C_v \quad \forall P \in E_{q_v}(L_w) \smallsetminus \{O\}.$$

Thus, since $E_{q_v} \cong E$ (over K_v), we get

$$\hat{\lambda}_w(P) > -C_v \quad \forall P \in E(L_w) \smallsetminus \{O\},$$

which is a suitable enough lower bound for $\hat{\lambda}_w$ that we have produced assuming the bad reduction of E at v is split multiplicative. (Note that this constant C_v depends on the place v lying below w, but not on w itself, therefore C_v depends on K, but not on L. This is the reason why we were working with v instead of directly with w, for otherwise our constant would end up depending on L.)

On the other hand, if the bad reduction of E at the v lying below w is not split multiplicative, then it must be additive or nonsplit multiplicative, and in these cases, we may take a tower of finite extensions $L'_{w'}/K'_{v'}/K_v$ (with $L_w \subset L'_{w'}$) such that E has good reduction or split multiplicative reduction at v'. So we can again use the same arguments as above (just replacing L_w/K_v by $L'_{w'}/K'_{v'}$) to conclude that for any $w \in M_L^{bad}$ we can produce a constant $C_v > 0$ such that

$$\hat{\lambda}_w(P) > -C_v \quad \forall P \in E(L) \smallsetminus \{O\}.$$

This way, since the number of bad reduction places for any elliptic curve is finite, we may set C_1 as the greatest of all the constants C_v with w running all over M_L^{bad} to get

$$\hat{\lambda}_w(P) \geq -C_1 \quad \forall w \in M_L^{bad} \ \forall P \in E(L) \smallsetminus \{O\}.$$

Hence, for any $P \in E(L) \smallsetminus \{O\}$ we have

$$\begin{aligned}
&\sum_{w \in M_L^{bad}} \frac{[L_w : \mathbb{Q}_w]}{[L : \mathbb{Q}]} \min\{\hat{\lambda}_w(P), 0\} \\
&\qquad\qquad \geq \sum_{w \in M_L^{bad}} \frac{[L_w : \mathbb{Q}_w]}{[L : \mathbb{Q}]}(-C_1) \\
&\qquad\qquad \geq \sum_{v \in M_K^{bad}} \sum_{w|v} \frac{[L_w : \mathbb{Q}_w]}{[L : \mathbb{Q}]}(-C_1) \\
&\qquad\qquad = \sum_{v \in M_K^{bad}} (-C_1) \quad \text{(from the extension formula (2.2))} \\
&\qquad\qquad = -C_1(\# M_K^{bad}) = -C_2,
\end{aligned}$$

and so we have proven the desired lower bound for the summation over M_L^{bad}.

Now finally, we handle the archimedean places. For convenience, here we work on M_K^∞ instead of M_L^∞, and later we extend our conclusions to M_L^∞. We start by taking a generic $v \in M_K^\infty$ and fixing an isomorphism chain $E(\bar{K}_v) \cong E(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z} + \tau_v\mathbb{Z}) \cong \mathbb{C}^*/q_v^{\mathbb{Z}}$ with $0 < |q_v|_v < e^{-\pi}$ as in [Si94, VI 3.4]. (To clarify a bit, this whole chain is given by the map $P \mapsto u(P)$, where u is the function from [Si94, I §6], i.e., it is defined by $u(P) = e^{2\pi i z}$ where the $z = z(P)$ is the one related to P by the Weierstrass $\wp$-function, in other words $P = (\wp(z), \wp'(z))$. For a precise description and construction of this chain one can refer to [Si09, VI] and [Si94, I], in the following we shall just briefly use it for the next formula, which makes use of it but overall doesn't really concern its rich construction very deeply.) With this chain of isomorphisms fixed, we may evoke [Si94, VI 3.4] which asserts that the local canonical height $\hat{\lambda}_v$ over $E(\bar{K}_v) \smallsetminus \{O\}$ is given by the explicit formula

$$\hat{\lambda}_v(P) = \frac{1}{2}\mathbb{B}_2\left(\frac{\log|u|_v}{\log|q_v|_v}\right)\log|q_v^{-1}|_v - \log|1-u|_v - \sum_{n\geq 1}\log|(1-q_v^n u)(1-q_v^n/u)|_v, \tag{3.1}$$

where $u = u(P) = e^{2\pi i z(P)} \in \mathbb{C}^*/q_v^{\mathbb{Z}}$, $\mathbb{B}_2(t)$ is the second Bernoulli polynomial for $0 \leq t \leq 1$ extended periodically to $\mathbb{R}/\mathbb{Z}$, and we are computing $|\,.\,|_v$ on $\mathbb{C}$ through the isomorphism $\mathbb{C} \cong \bar{K}_v$. Again the reader can refer to the proof of this formula in [Si94, VI 3.4] for more precise clarifications, here we just point out that by construction this equation is well defined, i.e., the value of $\hat{\lambda}_v(P)$ is independent of the chosen representative for the equivalence class of $u \in \mathbb{C}^*/q_v^{\mathbb{Z}}$ which we take during the computation of the absolute values above, as long we use the same representative in the whole formula.

With the above explicit formula for $\hat{\lambda}_v$ in mind, we define the compact set

$$B := \{\alpha \in \mathbb{C} : |q_v|_v \leq |\alpha|_v \leq |q_v|_v^{-1}\},$$

which by construction contains at least one representative for each equivalence class of $\mathbb{C}^*/q_v^{\mathbb{Z}}$. Thus, for any $P \in E(\bar{K}_v)$, when using formula (3.1) we can take the representative for $u(P)$ always inside B, and so from now on we consider them to be always taken in this way.

One immediate consequence of this particular choice of representatives is that since B is compact we can easily see

$$\log|1-u(P)|_v < C_{1,v} \quad \forall P \in E(\bar{K}_v),$$

for an appropriate constant $C_{1,v} > 0$.

Next, we split the summation in formula (3.1) as

$$\sum_{n\geq 1}\log|(1-q_v^n u)(1-q_v^n/u)|_v = \log\prod_{n\geq 1}|(1-q_v^n u)(1-q_v^n/u)|_v$$

$$= \log|\prod_{n\geq 1}(1-q_v^n u)|_v + \log|\prod_{n\geq 1}(1-q_v^n/u)|_v,$$

and to handle these infinite products we consider the set

$$\Omega := \{\alpha \in \mathbb{C} : |q_v|_v^2 < |\alpha| < |q_v|_v^{-2}\},$$

which is an open subset of $\mathbb{C}$, so we can use the standard complex analysis result [StSh03, V 3.2] to guarantee that the products

$$\prod_{n\geq 1}(1-q_v^n u) \quad \text{and} \quad \prod_{n\geq 1}(1-q_v^n/u)$$

define holomorphic functions of u on Ω. Thus, the fact that B is a compact subset of Ω implies that these products are bounded in B. In other words, we have just proven that there is another positive constant $C_{2,v}$ such that

$$\sum_{n\geq 1}\log|(1-q_v^n u)(1-q_v^n/u)|_v \leq C_{2,v} \quad \forall u \in B.$$

Hence, since we are taking the representatives for $u(P)$ always inside B, we have

$$\sum_{n\geq 1}\log|(1-q_v^n u(P))(1-q_v^n/u(P))|_v \leq C_{2,v} \quad \forall P \in E(\bar{K}_v).$$

So, formula (3.1) gives us

$$\hat{\lambda}_v(P) \geq \frac{1}{2}\mathbb{B}_2\left(\frac{\log|u|_v}{\log|q_v|_v}\right)\log|q_v^{-1}|_v - C_{1,v} - C_{2,v} \quad \forall P \in E(\bar{K}_v) \smallsetminus \{O\}.$$

Furthermore, using the fact that the second Bernoulli polynomial $t^2 - t + \frac{1}{6}$ has a minimum at $t = 1/2$ and $\mathbb{B}_2(1/2) = -1/12$, for an appropriate positive constant $C_{3,v}$ we can see that

$$\hat{\lambda}_v(P) \geq -\frac{1}{24}\log|q_v^{-1}|_v - C_{1,v} - C_{2,v} \geq -C_{3,v} \quad \forall P \in E(\bar{K}_v) \smallsetminus \{O\}.$$

Thus, since the number of archimedean places $v \in M_K$ is finite, we may set C_4 as the greatest of all the constants $C_{3,v}$ with v running over M_K^∞ to conclude

$$\hat{\lambda}_v(P) \geq -C_4 \quad \forall v \in M_K^\infty, \ \forall P \in E(\bar{K}_v) \smallsetminus \{O\}.$$

On the other hand, we know that every $w \in M_L^\infty$ lies over a $v \in M_K^\infty$ and for such pair we have $\bar{L}_w = \bar{K}_v$, so we can compute $\hat{\lambda}_w$ on $E(L)$ using the height $\hat{\lambda}_v$ and the inclusion $E(L) \subset E(\bar{K}_v)$. Therefore, from the above lower bound we get

$$\hat{\lambda}_w(P) \geq -C_4 \quad \forall w \in M_L^\infty, \ \forall P \in E(L) \smallsetminus \{O\}.$$

Hence, making use of the extension formula (2.2) for $L/\mathbb{Q}$, one can conclude

$$\sum_{w \in M_L^\infty} \frac{[L_w : \mathbb{Q}_w]}{[L : \mathbb{Q}]} \min\{\hat{\lambda}_w(P), 0\} \geq \sum_{w \in M_L^\infty} \frac{[L_w : \mathbb{Q}_w]}{[L : \mathbb{Q}]}(-C_4) = -C_4.$$

And this accomplishes the result for the summation over the archimedean places.

In summary, we have constructed lower bounds for the summations over each one of the three subsets of M_L that we mentioned at the beginning. So, adding up these three summations and taking $C_0 := C_2 + C_4$ gives us

$$\sum_{w \in M_L} \frac{[L_w : \mathbb{Q}_w]}{[L : \mathbb{Q}]} \min\{\hat{\lambda}_w(P), 0\} \geq -(0 + C_2 + C_4) = -C_0 \quad \forall P \in E(L) \smallsetminus \{O\},$$

which concludes the proof since all the constants here were constructed depending only on K and E, but never on P or L.

□

Remark: During the above demonstration, we were not very careful about keeping track of the constants we were building, so we have only proved the existence of a constant $C_0 > 0$ for which the result holds even though we don't really know how this constant looks like. It is interesting to note that a more precise approach could be taken to the above constructions. Indeed, using the explicit formulas for the local canonical heights, it is possible to give an estimate for the constant C_0 in terms of the j-invariant and minimal discriminant $\mathfrak{D}_{E/K}$ of E/K. Roughly, we can prove the existence of an absolute constant $C_0' > 0$ such that we can take our $C_0 = C_0(E/K)$ in the above lemma as

$$C_0 := C_0' \max\{1, h(j), \log N_{K/\mathbb{Q}}\mathfrak{D}_{E/K}\}.$$

For further computations of the explicit constants associated to the local canonical heights one can refer to [Si90].

Now that we have proven the above key lemma, we can produce our first theorem, which translates certain lower bounds for some local canonical heights of a point into a lower bound for the (global) canonical height of this same point. In the later sections, we will show that for any nontorsion point $P \in E(K^{ab})$, we can produce another point related to the first one, whose local canonical heights are bounded in the manner required by this theorem. Actually, this fact will play a major role during the proof of our main result in the last section.

Theorem 3.2. *Let E/K be an elliptic curve defined over a number field K, let $\mathfrak{p}$ be a degree 1 unramified prime of K (over $\mathbb{Q}$) and denote by p its residual characteristic. Let L/K be a finite extension and assume there is a nontrivial point $Q \in E(L)$ such that*

$$\hat{\lambda}_{\mathfrak{P}}(Q) \geq \log p \quad \textit{for all primes } \mathfrak{P} \textit{ of } L \textit{ lying over } \mathfrak{p}.$$

Then, this point satisfies

$$\hat{h}(Q) \geq \frac{\log p}{[K:\mathbb{Q}]} - C_0,$$

where $C_0 = C_0(E/K)$ is the constant from the previous lemma.

Proof. The idea here is to use the decomposition (2.4) of the canonical height into a summation over the local heights. As usual, we denote by $v_{\mathfrak{p}}$ the valuation on K associated to $\mathfrak{p}$, and then we first compute a lower bound for the contribution related to the valuations $w \in M_L$ lying over $v_{\mathfrak{p}}$ to the summation (2.4). We proceed as follows,

$$\sum_{w \in M_L, w | v_{\mathfrak{p}}} \frac{[L_w : \mathbb{Q}_w]}{[L : \mathbb{Q}]} \hat{\lambda}_w(Q) =$$

$$= \sum_{w \in M_L, w | v_{\mathfrak{p}}} \frac{[L_w : K_{v_{\mathfrak{p}}}]}{[L : K][K : \mathbb{Q}]} \hat{\lambda}_w(Q) \quad \text{(since } \mathfrak{p} \text{ is unramif. of deg. 1, so } K_{v_{\mathfrak{p}}} = \mathbb{Q}_{v_{\mathfrak{p}}} = \mathbb{Q}_w\text{)}$$

$$= \frac{1}{[K : \mathbb{Q}]} \sum_{\mathfrak{P} | \mathfrak{p}} \frac{[L_{\mathfrak{P}} : K_{\mathfrak{p}}]}{[L : K]} \hat{\lambda}_{\mathfrak{P}}(Q) \qquad \text{(here we translated into prime ideal notation)}$$

$$\geq \frac{1}{[K : \mathbb{Q}]} \sum_{\mathfrak{P} | \mathfrak{p}} \frac{[L_{\mathfrak{P}} : K_{\mathfrak{p}}]}{[L : K]} \log p \qquad \text{(since we are assuming } \hat{\lambda}_{\mathfrak{P}}(Q) \geq \log p \ \forall \mathfrak{P} | \mathfrak{p}\text{)}$$

$$= \frac{\log p}{[K : \mathbb{Q}]}. \qquad \text{(due to the extension formula (2.2))}$$

Now that we have established this lower bound, we use it together with (2.4) to compute

$$\begin{aligned}
\hat{h}(Q) &= \sum_{w\in M_L} \frac{[L_w : \mathbb{Q}_w]}{[L : \mathbb{Q}]} \hat{\lambda}_w(P) \quad \text{(this is (2.4))} \\
&\geq \frac{\log p}{[K : \mathbb{Q}]} + \sum_{w\in M_L, w\nmid v_{\mathfrak{p}}} \frac{[L_w : \mathbb{Q}_w]}{[L : \mathbb{Q}]} \hat{\lambda}_w(Q) \quad \text{(from the above lower bound)} \\
&\geq \frac{\log p}{[K : \mathbb{Q}]} + \sum_{w\in M_L, w\nmid v_{\mathfrak{p}}} \frac{[L_w : \mathbb{Q}_w]}{[L : \mathbb{Q}]} \min\{\hat{\lambda}_w(Q), 0\} \\
&\geq \frac{\log p}{[K : \mathbb{Q}]} + \sum_{w\in M_L} \frac{[L_w : \mathbb{Q}_w]}{[L : \mathbb{Q}]} \min\{\hat{\lambda}_w(Q), 0\} \\
&\geq \frac{\log p}{[K : \mathbb{Q}]} - C_0. \quad \text{(due to the previous lemma)}
\end{aligned}$$

□

4 Torsion in Abelian Extensions

In this small section we will use a deep result due to Serre to guarantee that the ℓ-torsion in $E(K^{ab})$ is trivial except for a finite number of primes $\ell \in \mathbb{Z}$. This will be required during the proof of our main theorem to ensure the existence of a certain prime that has some useful properties.

Theorem 4.1. *Let K be a number field and let E/K be an elliptic curve without complex multiplication (i.e., End$(E) \cong \mathbb{Z}$). Then there is a finite set of primes $S \subset \mathbb{Z}$ such that*

$$E(K^{ab})[\ell] = \{O\} \quad \textit{for all primes } \ell \notin S.$$

Proof. Recall that for any given integer $m \geq 2$, $\mathrm{Gal}(\bar{K}/K)$ acts naturally on $E[m]$ (since if $[m]P = O$, then $[m](P^\sigma) = ([m]P)^\sigma = O$), therefore we have the natural representation

$$\rho_m : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(E[m]) \cong GL_2\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right),$$

where the above isomorphism takes place because of the well known statement [Si09, III 6.4] which asserts that $Char(K) = 0$ implies

$$E[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}. \tag{4.1}$$

With this brief review in mind, we evoke the outstanding result due to Serre [Se72] that guarantees the above representation is surjective for all but finitely many primes, i.e., there exists a finite set of primes $S \subset \mathbb{Z}$ such that for all $\ell \notin S$ the Galois representation

$$\rho_\ell : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(E[\ell]) \cong GL_2(\mathbb{F}_\ell) \tag{4.2}$$

is surjective. This way, for any fixed $\ell \notin S$ and any given $T \in E(K^{ab})[\ell] \smallsetminus \{O\}$, we can use the isomorphism (4.1) to consider T also as an element of

$\mathbb{F}_\ell^2$, and since the group $GL_2(\mathbb{F}_\ell)$ acts transitively on the nonzero vectors of $\mathbb{F}_\ell^2$, from the surjectivity of (4.2) we see that the Galois orbit of T is the whole $\mathbb{F}_\ell^2 \smallsetminus \{(0,0)\}$ (i.e., the whole $E[\ell]) \smallsetminus \{O\}$). Meanwhile, we know that all Galois conjugates of T are also defined over K^{ab}, and so we may conclude $E[\ell] \subset E(K^{ab})$. Furthermore, since any $\sigma \in \mathrm{Gal}(\bar{K}/K)$ when restricted to K^{ab} can be seen as an element of $\mathrm{Gal}(K^{ab}/K)$ (for K^{ab}/K is Galois), the fact that $E[\ell] \subset E(K^{ab})$ implies that our representation (4.2) can be decomposed as

$$\mathrm{Gal}(\bar{K}/K) \to \mathrm{Gal}(K^{ab}/K) \to \mathrm{Aut}(E[\ell]) \cong GL_2(\mathbb{F}_\ell),$$

where the first arrow is the restriction to K^{ab} (in other words, ρ_ℓ factors through $\mathrm{Gal}(K^{ab}/K)$).

On the other hand, the surjectivity of (4.2) also implies

$$\mathrm{Im}(\rho_\ell) = \mathrm{Aut}(E[\ell]) \cong GL_2(\mathbb{F}_\ell),$$

but these groups are nonabelian, and so one has a contradiction with the fact that ρ_ℓ factors through the abelian group $\mathrm{Gal}(K^{ab}/K)$. Thus we must have $E(K^{ab})[\ell] \smallsetminus \{O\} = \varnothing$, which concludes our demonstration.

□

Remark: This result as it is stated above will be enough for our purposes later on, nevertheless, it is good to point out that we could strengthen it even more, since also due to Serre (this time [Se98]), the image of $\mathrm{Gal}(\bar{K}/K)$ in $\mathrm{Aut}(T_\ell(E))$ is open, and thus has finite index. Therefore, we could proceed with a similar argument as the above to prove that for any $\ell \in S$, the ℓ-power torsion in $E(K^{ab})$ is finite, and hence conclude that $E(K^{ab})_{tors}$ is finite under the same hypothesis.

5 Tools for the Unramified Case

In this section we will use some reduction techniques, and therefore we will end up working with elliptic curves defined over finite fields. So for this purpose, we shall briefly recall here some key facts about elliptic curves over finite fields that will be required ahead.

Before anything else, for a generic elliptic curve $E'/\mathbb{F}_q$ (the prime " $'$ " here is just to make a clear distinction from our fixed curve E/K), remember we have the q-power Frobenius endomorphism

$$f_q : E' \to E', \quad (x, y) \mapsto (x^q, y^q),$$

which provides some very useful tools:

The first tool is the well known bound due to Hasse for the number of points in $E'(\mathbb{F}_q)$ (see [Si09, V 1.1]). It asserts that

$$|q + 1 - \#E'(\mathbb{F}_q)| \leq 2\sqrt{q}, \tag{5.1}$$

and for convenience we set $a_q = a_q(E'/\mathbb{F}_q) := q + 1 - \#E'(\mathbb{F}_q)$.

The second one is [Si09, V 2.3.1], which ensures that the roots of the polynomial $X^2 - a_q X + q$ have absolute value $\sqrt{q}$ and that this polynomial evaluated at f_q is the zero map, i.e.,

$$f_q^2 - a_q f_q + q = 0 \text{ in } \mathrm{End}(E'). \tag{5.2}$$

Now with these two results on hand, we are ready to enunciate and prove the following theorem, which provides all the machinery required to handle the unramified case during the proof of our main theorem. It is also good to note that this next theorem makes no assumptions about being or not in the unramified case, and therefore is much more general. However, it is under the hypothesis that we are in the unramified case that it will be useful during the proof of our main theorem, since in this case, the (c) ahead will provide a lower bound that is exactly what we need.

Theorem 5.1. *Let $K/\mathbb{Q}$ be a number field and let L/K be a finite Galois extension. Let $\mathfrak{p}$ be a prime of K, let $\mathfrak{P}$ be a prime of L lying over $\mathfrak{p}$ and let $\sigma \in Gal(L/K)$ be a Frobenius element associated to $\mathfrak{P}$ (i.e., $\sigma(x) \equiv x^q \,(mod \mathfrak{P})$). Let $\kappa := \mathcal{O}_K/\mathfrak{p}$, $p := Char(\kappa)$ and $q := \#\kappa$. Finally, let E/K be an elliptic curve with good reduction at $\mathfrak{p}$ (therefore also at $\mathfrak{P}$) and set*

$$\Phi_{\mathfrak{p}}(X) := X^2 - a_q X + q \ \in \mathbb{Z}[X] \ \ \textit{(the polynomial from } (5.2)\textit{)}.$$

Then, for any given $P \in E(L)$ we have:

(a) $\Phi_{\mathfrak{p}}(\sigma)P$ is in the kernel of the reduction modulo $\mathfrak{P}$.

(b) If $\Phi_{\mathfrak{p}}(\sigma)P = O$, then P is a torsion point.

(c) If P is a nontorsion point, then

$$\hat{\lambda}_{\mathfrak{P}}(\Phi_{\mathfrak{p}}(\sigma)P) \geq \frac{\log p}{e(\mathfrak{P}, L/\mathbb{Q})}$$

(where as usual $e(\mathfrak{P}, L/\mathbb{Q})$ denotes the ramification index of $\mathfrak{P}$ in the extension $L/\mathbb{Q}$, i.e., the ramification index of $\mathfrak{P}$ over p).

Proof. Through this demonstration a tilde will always denote reduction modulo $\mathfrak{P}$.

(a) We begin by fixing a minimal Weierstrass equation for E at $\mathfrak{p}$, which since the reduction is good, also has to be minimal at $\mathfrak{P}$.

Now remember we have the natural embedding

$$\kappa = \frac{\mathcal{O}_K}{\mathfrak{p}} \hookrightarrow \frac{\mathcal{O}_L}{\mathfrak{P}}$$

that allows us to see κ as if it were a subfield of $\mathcal{O}_L/\mathfrak{P}$. But since E is defined over K and our fixed Weierstrass equation was taken as minimal at $\mathfrak{p}$, we know that all of its coefficients are in $\mathcal{O}_K$. Thus, when we reduce this equation modulo $\mathfrak{P}$, all of its coefficients will lie in the image of the above embedding, and therefore we may regard $\tilde{E}$ as defined over κ, and not merely over $\mathcal{O}_L/\mathfrak{P}$ as we would normally expect. But as $\#\kappa = q$, we have just proven that $\tilde{E}$ is defined over a field with q elements, and for such a case we can use (5.2) to conclude that the q-power Frobenius endomorphism $f_q \in \mathrm{End}(\tilde{E})$ satisfies

$$\Phi_{\mathfrak{p}}(f_q) = 0 \text{ in } \mathrm{End}(\tilde{E}).$$

On the other hand, since σ was defined as a Frobenius element for $\mathfrak{P}$, when reduced modulo $\mathfrak{P}$, it acts over $\tilde{E}$ as if it were the q-power Frobenius endomorphism $f_q \in \mathrm{End}(\tilde{E})$, i.e.,

$$\sigma = f_q \text{ in } \mathrm{End}(\tilde{E}).$$

So, we may use the fact that the Galois action commutes with the reduction to compute

$$\widetilde{\Phi_{\mathfrak{p}}(\sigma)P} = \Phi_{\mathfrak{p}}(f_q)\tilde{P} = \tilde{O}.$$

(b) Assume P satisfies $\Phi_{\mathfrak{p}}(\sigma)P = O$ and define $m := [L : K]$. Now note that the roots of $X^m - 1$ have absolute value 1, and as mentioned at the beginning of this section, the roots of $\Phi_{\mathfrak{p}}(X)$ have absolute value $\sqrt{q}$, thus, as elements of $\mathbb{Q}[X]$ these two polynomials have no common factors, and therefore their GCD is 1. So, since $\mathbb{Q}[X]$ is a Euclidean domain, we may use the extended euclidean algorithm to guarantee the existence of two polynomial $a(X)$, $b(X) \in \mathbb{Q}[X]$ such that

$$a(X)\Phi_{\mathfrak{p}}(X) + b(X)(X^m - 1) = 1.$$

Further, multiplying the above equation by an appropriate constant $r \in \mathbb{Z}$ that cancels out all the denominators of the coefficients of $a(X)$ and $b(X)$, we end up with two polynomials $A(X)$ and $B(X) \in \mathbb{Z}[X]$ such that

$$A(X)\Phi_{\mathfrak{p}}(X) + B(X)(X^m - 1) = r.$$

Thus, since this above equation is taking place in $\mathbb{Z}[X]$, we may replace X by σ and consider it as an identity in the group ring $\mathbb{Z}[\mathrm{Gal}(L/K)]$, i.e.,

$$A(\sigma)\Phi_{\mathfrak{p}}(\sigma) + B(\sigma)(\sigma^m - 1) = r \quad \text{in } \mathbb{Z}[\mathrm{Gal}(L/K)].$$

Therefore we have

$$\begin{aligned}[r]P &= (A(\sigma)\Phi_{\mathfrak{p}}(\sigma) + B(\sigma)(\sigma^m - 1))P \\ &= A(\sigma)(\Phi_{\mathfrak{p}}(\sigma)P) + B(\sigma)((\sigma^m - 1)P) \\ &= O. \quad \text{(since we are assuming } \Phi_{\mathfrak{p}}(\sigma)P = O \text{ and } m = [L:K])\end{aligned}$$

Hence P is a torsion point as we wanted to prove.

(c) Assume P is a nontorsion point, denote by $w_{\mathfrak{P}}$ the valuation on L associated to $\mathfrak{P}$, and to ease notation set $Q := \Phi_{\mathfrak{p}}(\sigma)P$. This way, since P is nontorsion, we can use the item (b) above to guarantee $Q \neq O$. On the other hand, (a) tells us that Q is in the kernel of the reduction modulo $\mathfrak{P}$, so we must have $w_{\mathfrak{P}}(y(Q)^{-1}) > 0$ (where as usual x and y are the ones relative to a fixed minimal Weierstrass equation for E at $\mathfrak{p}$, which therefore is also minimal at $\mathfrak{P}$). But in this case, we can apply Lemma 2.1 to conclude

$$\hat{\lambda}_{\mathfrak{P}}(Q) = w_{\mathfrak{P}}(x(Q)/y(Q)) > 0,$$

and furthermore, due to (2.3) we have

$$w_{\mathfrak{P}}(x(Q)/y(Q)) \geq \frac{\log p}{e(\mathfrak{P}, L/\mathbb{Q})}.$$

Thus, our proof is complete.

□

6 Tools for the Ramified Case

In the previous section, we proved under some hypotheses that for any point $P \in E(L)$ (L/K finite and Galois), we could produce a certain key point $\Phi_{\mathfrak{p}}(\sigma)P$ that have lots of useful properties. These key points will be used to handle the unramified case during the proof of our main theorem. To deal with the ramified case, we will need to produce other points that also have some amazing properties similar to these key points we just mentioned, but which are suitable for the ramified case. Roughly speaking, these new key points will be the points $[p]((\tau-1)^2 P)$ where τ is a very peculiar element from $\mathrm{Gal}(L/K)$ as we shall see ahead.

Remember that for an abelian extension L/K, if we fix any prime $\mathfrak{p}$ of K, then all primes $\mathfrak{P}$ of L lying over $\mathfrak{p}$ have the same inertia group. So, in situations like this, as usual we denote by $I_{\mathfrak{p}}(L/K)$ the subgroup of $\mathrm{Gal}(L/K)$ that is simultaneously the inertia group of all the primes of L lying over $\mathfrak{p}$.

In the following, we shall need some number theoretical results that are mainly due to Amoroso and Dvornicich. For the sake of convenience, here we glue all these results into a single statement (the next lemma) that is exactly what is required ahead. Specifically, the following lemma is modeled after [AmDv00, §2, Lemma 2].

Lemma 6.1. *Let K be a number field, let $\mathfrak{p}$ be a degree 1 unramified prime of K (over $\mathbb{Q}$) with residual characteristic p, and let L/K be a finite abelian extension that is ramified at $\mathfrak{p}$. Then there exists a nontrivial element $\tau \in I_{\mathfrak{p}}(L/K)$ such that for any prime $\mathfrak{P}$ of L lying over $\mathfrak{p}$ we have:*

$$(\tau\alpha)^p \equiv \alpha^p \pmod{p\mathcal{O}_{L_{\mathfrak{P}}}} \quad \forall \alpha \in \mathcal{O}_{L_{\mathfrak{P}}},$$

where $\mathcal{O}_{L_{\mathfrak{P}}}$ denotes the ring of integers of $L_{\mathfrak{P}}$ (i.e., the valuation ring of $L_{\mathfrak{P}}$).

Proof. We begin by fixing a prime $\mathfrak{P}$ of L lying over $\mathfrak{p}$, and first we will prove the result just for this fixed prime, i.e., we will produce a $\tau \in I_{\mathfrak{p}}(L/K)$ that *a priori* has the stated property just for this fixed prime $\mathfrak{P}$. Later we shall make a simple argument to guarantee that this same τ also works for all the other primes of L lying over $\mathfrak{p}$.

As by hypothesis $\mathfrak{p}$ is unramified of degree 1, the local fundamental equation gives us $[K_{\mathfrak{p}} : \mathbb{Q}_p] = 1$, therefore we must have $K_{\mathfrak{p}} = \mathbb{Q}_p$. Hence, the fact that L/K is abelian implies that $L_{\mathfrak{P}}$ is an abelian extension of $\mathbb{Q}_p$. Thus, by the local Kronecker-Weber theorem, there is an integer (which we take as being minimal) $m \geq 1$ such that $L_{\mathfrak{P}} \subset \mathbb{Q}_p(\zeta_m)$, where ζ_m denotes a primitive m^{th} root of unity. Meanwhile, recall that if gcd(m,p)=1, then $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ is unramified (this is [Ne99, II 7.12]). So, since by our assumptions $L_{\mathfrak{P}}/\mathbb{Q}_p$ is ramified, we must have $p|m$, and consequently, it makes sense to write $\zeta_{m/p} := \zeta_m^p$.

Now with the above discussion in mind, we take τ as being a generator for the cyclic group $\text{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p(\zeta_{m/p}))$. This way, the minimality of m implies that $L_{\mathfrak{P}} \not\subset \mathbb{Q}_p(\zeta_{m/p})$, and thus τ restricted to $L_{\mathfrak{P}}$ is a nontrivial element of $\text{Gal}(L_{\mathfrak{P}}/\mathbb{Q}_p)$. But since τ fixes $\zeta_{m/p} = \zeta_m^p$, we must have

$$\tau(\zeta_m) = \omega\zeta_m,$$

where ω is a certain p^{th} root of unity. Further, for any $\alpha \in \mathcal{O}_{L_{\mathfrak{P}}}$, due to the inclusion $\mathcal{O}_{L_{\mathfrak{P}}} \subset \mathcal{O}_{\mathbb{Q}_p(\zeta_m)} = \mathbb{Z}_p[\zeta_m]$, we can see that $\alpha = f(\zeta_m)$ for some polynomial $f(x) \in \mathbb{Z}_p[x]$, hence

$$\tau(\alpha) = \tau(f(\zeta_m)) = f(\tau(\zeta_m)) = f(\omega\zeta_m).$$

Thus we can take the p^{th} power to yield

$$\begin{aligned}(\tau\alpha)^p &= (f(\omega\zeta_m))^p \\ &\equiv f((\omega\zeta_m)^p) \pmod{p\mathbb{Z}_p[\zeta_m]} \\ &= f(\zeta_m^p) \\ &\equiv (f(\zeta_m))^p \pmod{p\mathbb{Z}_p[\zeta_m]} \\ &= \alpha^p,\end{aligned}$$

i.e., in summary we have just proven: if $\alpha \in \mathcal{O}_{L_\mathfrak{P}}$, then

$$(\tau\alpha)^p - \alpha^p \in p\mathbb{Z}_p[\zeta_m].$$

But on the other hand, $\alpha \in \mathcal{O}_{L_\mathfrak{P}} \subset L_\mathfrak{P}$ naturally implies

$$(\tau\alpha)^p - \alpha^p \in L_\mathfrak{P}.$$

So taking the intersection,

$$\alpha \in \mathcal{O}_{L_\mathfrak{P}} \;\Rightarrow\; (\tau\alpha)^p - \alpha^p \in L_\mathfrak{P} \cap p\mathbb{Z}_p[\zeta_m] = p\mathcal{O}_{L_\mathfrak{P}}.$$

In other words,

$$(\tau\alpha)^p \equiv \alpha^p \pmod{p\mathcal{O}_{L_\mathfrak{P}}} \quad \forall\alpha \in \mathcal{O}_{L_\mathfrak{P}}.$$

Next, to see that τ restricted to $L_\mathfrak{P}$ is indeed an element of $I(L_\mathfrak{P}/K_\mathfrak{p}) = I_\mathfrak{p}(L/K)$, we again take a generic $\alpha \in \mathcal{O}_{L_\mathfrak{P}}$ and use what we have already proved for τ to compute

$$(\tau(\alpha) - \alpha)^p \equiv \tau(\alpha)^p - \alpha^p \equiv 0 \pmod{p\mathcal{O}_{L_\mathfrak{P}}},$$

hence

$$(\tau(\alpha) - \alpha)^p \in p\mathcal{O}_{L_\mathfrak{P}} \subset \mathfrak{P}\mathcal{O}_{L_\mathfrak{P}},$$

and thus, since $\mathfrak{P}\mathcal{O}_{L_{\mathfrak{P}}}$ is a prime ideal, we must have $(\tau(\alpha)-\alpha)\in\mathfrak{P}\mathcal{O}_{L_{\mathfrak{P}}}$, therefore

$$\tau(\alpha)\equiv\alpha \pmod{\mathfrak{P}\mathcal{O}_{L_{\mathfrak{P}}}}.$$

But it means $\tau\in I(L_{\mathfrak{P}}/K\mathfrak{p})$, and so the result is proven for our fixed $\mathfrak{P}$.

Now in order to prove that the same τ also works for any other prime $\mathfrak{P}'$ of L lying over $\mathfrak{p}$, we proceed as follows:

Since all primes of L lying over the same prime of K are Galois conjugates, we know there is a $g\in\mathrm{Gal}(L/K)$ such that $g(\mathfrak{P})=\mathfrak{P}'$. So for any $\alpha\in\mathcal{O}_{L_{\mathfrak{P}'}}$ we have $g^{-1}(\alpha)\in\mathcal{O}_{L_{\mathfrak{P}}}$, and then we may compute

$$\begin{aligned}\tau(\alpha)^p &= \tau(g(g^{-1}(\alpha)))^p\\ &= g(\tau(g^{-1}(\alpha))^p) \quad \text{(since } L/K \text{ is abelian.)}\\ &\equiv g(g^{-1}(\alpha)^p) \pmod{g(p\mathcal{O}_{L_{\mathfrak{P}}})}\\ &= \alpha^p,\end{aligned}$$

but $g(p\mathcal{O}_{L_{\mathfrak{P}}})=p\mathcal{O}_{L_{\mathfrak{P}'}}$, therefore we have proven

$$\tau(\alpha)^p=\alpha^p \pmod{p\mathcal{O}_{L_{\mathfrak{P}'}}} \quad \forall\,\alpha\in\mathcal{O}_{L_{\mathfrak{P}'}}.$$

□

Next we make use of some of the basic properties of formal groups to compute the following inclusion that will be used later in this section.

Lemma 6.2. *Let R be a ring, let $F(x,y)\in R[[x,y]]$ be a formal group over R, and let $p\in\mathbb{Z}$ be a prime. Let $\iota(t)\in R[[t]]$ be the inversion series for F and let $M_p(t)\in R[[t]]$ be the multiplication-by-p series for F. Then,*

$$M_p(F(x,\iota(y)))\in(x^p-y^p)R[[x,y]]+pR[[x,y]].$$

Proof. Due to the standard result concerning formal groups [Si09, IV 4.4], we know that there are two power series $A(t)$, $B(t) \in R[[t]]$ such that

$$A(0) = B(0) = 0 \quad \text{and} \quad M_p(t) = A(t^p) + pB(t).$$

On the other hand, by the definition of ι, we have $F(t, \iota(t)) \equiv 0$, thus $F(x, \iota(y))$ must be divisible by $x - y$ (since it vanishes at $x = y$). Hence there exists a $G(x, y) \in R[[x, y]]$ such that

$$F(x, \iota(y)) = (x - y)G(x, y).$$

Therefore,

$$\begin{aligned} M_p(F(x, \iota(y))) &= A(F(x, \iota(y))^p) + pB(F(x, \iota(y))) \\ &= A((x - y)^p G(x, y)^p) + pB(F(x, \iota(y))) \\ &\in A((x - y)^p G(x, y)^p) + pR[[x, y]], \end{aligned}$$

but since $A(0) = 0$, the constant term of $A(t)$ must be 0, so we have

$$A((x - y)^p G(x, y)^p) + pR[[x, y]] \subset (x - y)^p R[[x, y]] + pR[[x, y]].$$

Further, except for x^p and y^p, all the other terms of $(x - y)^p$ have coefficients that are multiples of p, and thus they lie in $pR[[x, y]]$. This way we can see

$$(x - y)^p R[[x, y]] + pR[[x, y]] \subset (x^p - y^p)R[[x, y]] + pR[[x, y]].$$

Finally, fitting together all these inclusions yields

$$M_p(F(x, \iota(y))) \in (x^p - y^p)R[[x, y]] + pR[[x, y]].$$

□

Next, we note the following corollary of this lemma.

Corollary 6.3. *Let L/K be a finite Galois extension of number fields that ramifies at a prime $\mathfrak{p}$ of K, let E/K be an elliptic curve with good reduction at $\mathfrak{p}$ and let $z := -x/y$ be the parameter for the formal group $\hat{E}$ associated to a fixed minimal Weierstrass equation for E at $\mathfrak{p}$. Then, for any prime $\mathfrak{P}$ of L lying over $\mathfrak{p}$ and any $\tau \in I(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ we have:*

(a) $(\tau - 1)P \in E_1(L_{\mathfrak{P}}) \quad \forall P \in E(L_{\mathfrak{P}})$.

(b) $z([p](\tau-1)Q) \in (\tau z(Q)^p - z(Q)^p)\mathcal{O}_{L_{\mathfrak{P}}} + p\mathcal{O}_{L_{\mathfrak{P}}} \quad \forall Q \in E_1(L_{\mathfrak{P}})$.

(Where as usual $E_1(L_{\mathfrak{P}})$ denotes the kernel of the reduction modulo $\mathfrak{P}\mathcal{O}_{L_{\mathfrak{P}}}$, so we have the very useful isomorphism $E_1(L_{\mathfrak{P}}) \cong \hat{E}(\mathfrak{P}\mathcal{O}_{L_{\mathfrak{P}}})$. See [Si09, VII 2.2].)

Proof. (a) By definition of the inertia group, any of its elements fixes everything modulo $\mathfrak{P}\mathcal{O}_{L_{\mathfrak{P}}}$, so we have $\tau P - P \equiv P - P \equiv O \pmod{\mathfrak{P}\mathcal{O}_{L_{\mathfrak{P}}}}$, thus $\tau P - P$ lies in the kernel of the reduction.

(b) This is immediate from the isomorphism $E_1(L_{\mathfrak{P}}) \cong \hat{E}(\mathfrak{P}\mathcal{O}_{L_{\mathfrak{P}}})$, which we can apply in the previous lemma with $x = \tau z(Q)$ and $y = z(Q)$ to conclude what we desired to prove.

□

Now that we have produced all the above machinery, we can finally state and prove the central result of this section. As mentioned before, it ensures some properties for a certain point in a similar way as Theorem 5.1 did for the point $\Phi_{\mathfrak{p}}(\sigma)P$.

Theorem 6.4. *Let K be a number field, let E/K be an elliptic curve with good reduction at an unramified degree 1 prime $\mathfrak{p}$ of K (over $\mathbb{Q}$), and denote by p the residual characteristic of $\mathfrak{p}$. For a fixed $P \in E(K^{ab})$, let $L := K(P)$ be its minimal field of definition and assume $\mathfrak{p}$ ramifies in L. Finally, take a nontrivial $\tau \in I_{\mathfrak{p}}(L/K)$ such that*

$$(\tau\alpha)^p \equiv \alpha^p \pmod{p\mathcal{O}_{L_{\mathfrak{P}}}} \quad \forall\alpha \in \mathcal{O}_{L_{\mathfrak{P}}} \ \ \forall\,\mathfrak{P}|\mathfrak{p},$$

whose existence is guaranteed by Lemma 6.1, and define

$$P' := [p]((\tau - 1)^2 P).$$

Then we have

- *(a)* $\hat{\lambda}_{\mathfrak{P}}(P') \geq \log p$ *for all primes* $\mathfrak{P}$ *of* L *lying over* $\mathfrak{p}$.
- *(b)* *If* P *is a nontorsion point and* $E(K^{ab})[p] = \{O\}$, *then* $P' \neq O$.

Proof. (a) Note that even though $\hat{\lambda}_{\mathfrak{P}}$ is not naturally defined on O, here as usual we evaluate it on O according to the extended definition $\hat{\lambda}_{\mathfrak{P}}(O) := \infty$, thus the desired result is trivially true if $P' = O$. Therefore, from now on we may assume $P' \neq O$ without any loss of generality.

We begin by taking a generic $\mathfrak{P}$ of L lying over $\mathfrak{p}$ and fixing once and for all a minimal Weierstrass equation for E at $\mathfrak{P}$, say

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

As in the following we will work with the formal group of E, here we also make the standard change of variables

$$z := -\frac{x}{y} \qquad w := -\frac{1}{y},$$

this way z is a parameter for the formal group and we have $(z(O), w(O)) = (0, 0)$ (see [Si09, IV §1]).

Keeping the above discussion in mind, we define $Q := (\tau - 1)P$, so by Corollary 6.3.a, Q is in the kernel of the reduction modulo $\mathfrak{P}\mathcal{O}_{L_{\mathfrak{P}}}$. Thus, since $P' = [p](\tau - 1)Q$, we can use Corollary 6.3.b to obtain

$$z(P') \in ((\tau z(Q))^p - z(Q)^p)\mathcal{O}_{L_{\mathfrak{P}}} + p\mathcal{O}_{L_{\mathfrak{P}}}. \tag{6.1}$$

But on the other hand, we may also use the fact that Q lies in the kernel of the reduction modulo $\mathfrak{P}\mathcal{O}_{L_{\mathfrak{P}}}$ to see

$$(\widetilde{z(Q)}, \widetilde{w(Q)}) = (\tilde{0}, \tilde{0}),$$

hence we can conclude $z(Q) \in \mathcal{O}_{L_{\mathfrak{P}}}$. Therefore, from our choice of τ we get $\tau z(Q)^p \equiv z(Q)^p \pmod{p\mathcal{O}_{L_{\mathfrak{P}}}}$. Thus $\tau z(Q)^p - z(Q)^p \in p\mathcal{O}_{L_{\mathfrak{P}}}$, and then (6.1)

$$z(P') \in p\mathcal{O}_{L_{\mathfrak{P}}}. \tag{6.2}$$

Meanwhile, one can write $P' = (\tau - 1)([p]Q)$, so Corollary 6.3.a also guarantees P' is in the kernel of the reduction modulo $\mathfrak{P}\mathcal{O}_{L_{\mathfrak{P}}}$. Thus for P' as well we have

$$(\widetilde{z(P')}, \widetilde{w(P')}) = (\tilde{0}, \tilde{0}),$$

hence

$$w_{\mathfrak{P}}(y(P')^{-1}) = w_{\mathfrak{P}}(w(P')) > 0$$

(note here $w_{\mathfrak{P}}$ is the valuation on L associated to $\mathfrak{P}$, and so it has nothing to do with the variable $w = -1/y$ above).

Therefore, we may use Lemma 2.1 to compute

$$\begin{aligned}\hat{\lambda}_{\mathfrak{P}}(P') &= w_{\mathfrak{P}}(x(P')/y(P')) \\ &= w_{\mathfrak{P}}(z(P')) \\ &\geq w_{\mathfrak{P}}(p) \quad \text{(from (6.2))} \\ &= -\log |p|_{w_{\mathfrak{P}}} \\ &= \log p.\end{aligned}$$

(b) Here we proceed by *reductio ad absurdum.* So, assume we have $P' = O$.

We begin by setting $m := o(\tau)$ (the order of τ as element of $\mathrm{Gal}(L/K)$), and then we note that the resultant of the polynomials $(X-1)$ and $(\sum_{i=0}^{m-1} X^i)$ is m, so we know there exist two polynomials $A(X)$, $B(X) \in \mathbb{Z}[X]$ such that

$$A(X)(X-1) + B(X)\sum_{i=0}^{m-1} X^i = m.$$

Next, multiplying both sides of this equation by $p(X-1)$ provides

$$pA(X)(X-1)^2 + pB(X)(X^m - 1) = mp(X-1).$$

So, keeping in mind that m was taken as the order of τ, we evaluate this identity at $X = \tau$ and apply it to the point P. This way we can see

$$[p]A(\tau)(\tau-1)^2 P + [p]B(\tau)(1-1)P = [mp](\tau-1)P.$$

But, since we are under the hypothesis $[p](\tau-1)^2 P = P' = O$, the left side above is clearly O, hence we have just proven

$$[mp](\tau-1)P = O,$$

and so

$$(\tau-1)P \in E(L)_{tors}$$

On the other hand, we know from Corollary 6.3.a that for any prime $\mathfrak{P}$ of L lying over $\mathfrak{p}$, $(\tau - 1)P$ is in the kernel of the reduction modulo $\mathfrak{P}\mathcal{O}_{L_{\mathfrak{P}}}$, therefore (due to the isomorphism $E_1(L_{\mathfrak{P}}) \cong \hat{E}(\mathfrak{P}\mathcal{O}_{L_{\mathfrak{P}}})$ [Si09, VII 2.2]) we can regard $(\tau - 1)P$ as an element of the formal group $\hat{E}(\mathfrak{P}\mathcal{O}_{L_{\mathfrak{P}}})$. Then we evoke the result concerning formal groups [Si09, IV 3.2.b], which states that any finite order element of the formal group $\hat{E}(\mathfrak{P}\mathcal{O}_{L_{\mathfrak{P}}})$ has an order that is a p-power, to conclude that, since $(\tau - 1)P \in E(L)_{tors}$, there must exist a $n \in \mathbb{Z}_{>0}$ such that

$$[p^n](\tau - 1)P = O.$$

Hence, as we are assuming $E(K^{ab})[p] = \{O\}$, we must have $(\tau - 1)P = O$, and thus

$$\tau(P) = P.$$

Therefore $P \in L^{\tau}$ (the fixed field of τ). However, as L/K is Galois and τ is nontrivial, we know that L^{τ} is a proper subfield of L, and so we have a contradiction to the fact that L was taken as the minimal field of definition of P.

□

7 The Main Theorem

In this section we shall use the theorems previously constructed to finally prove our main theorem.

Theorem 7.1. *Let K be a number field, let E/K be an elliptic curve, and let $\hat{h} : E(\bar{K}) \to \mathbb{R}$ be the canonical height on E. Then there exists a constant $C = C(E/K) > 0$ such that*

$$\hat{h}(P) \geq C \ \textit{ for all nontorsion } P \in E(K^{ab}).$$

Proof. As mentioned in the introductory section, the approach here will be to prove this theorem just for the case when our elliptic curve does not have complex multiplication (i.e., when $\mathrm{End}(E) = \mathbb{Z}$), since due to Baker [Ba03] this result already is established for the CM case. Therefore, keep in mind that throughout this whole demonstration we will be under the additional hypothesis that $\mathrm{End}(E) = \mathbb{Z}$. (Note that Baker in [Ba03] could also prove this theorem for the case when $j(E)$ is nonintegral, but we won't use this fact here.)

The central key for our proof is a certain prime $\mathfrak{p}$ of K, which we fix through the course of this demonstration, and consider it to have been chosen with the following properties:

$(p.1)$ $\mathfrak{p}$ is unramified of degree 1 (over $\mathbb{Q}$).

$(p.2)$ E has good reduction at $\mathfrak{p}$.

$(p.3)$ $p \geq \exp([K : \mathbb{Q}](1 + C_0))$.

$(p.4)$ $E(K^{ab})[p] = \{O\}$.

(here as usual we are denoting by p the residual characteristic of $\mathfrak{p}$, and $C_0 = C_0(E/K)$ is the constant from Theorem 3.2.) To clarify why we can guarantee the existence of such a prime with these properties: from standard algebraic number theory, we know that the set of unramified degree 1 primes of K is infinite (see [Ne99, VII §13]). On the other hand, (p.2) and (p.3) eliminate only finitely many primes, and since we are under the hypothesis $\mathrm{End}(E) = \mathbb{Z}$, we may use Theorem 4.1 to conclude that (p.4) also excludes only a finite number of primes. (Note that it is here where we are making use of the assumption that E does not have complex multiplication, for otherwise we could not evoke Theorem 4.1 to conclude this last step.)

Now with this (fixed) prime $\mathfrak{p}$ on hand, we can begin our demonstration. We start by taking a generic nontorsion point $P \in E(K^{ab})$ and defining L as its minimal field of definition (i.e., $L := K(P)$). This way, since P was taken in $E(K^{ab})$, we know that L/K is abelian, and therefore all the primes of L lying over $\mathfrak{p}$ have the same ramification index. Henceforth, we split our proof according to such ramification index.

First, assume $\mathfrak{p}$ is unramified at L/K. In this case, we know that the Frobenius elements associated to each prime $\mathfrak{P}$ of L lying over $\mathfrak{p}$ are also all the same element, which we shall denote from now on by σ. Under these circumstances, we take the polynomial

$$\Phi_{\mathfrak{p}}(X) := X^2 - a_p X + p \ \in \mathbb{Z}[X]$$

from Theorem 5.1 (here $q = p$ because $\mathfrak{p}$ has degree 1). So, as P is a nontorsion point and $\mathfrak{p}$ is an unramifed prime that does not ramify at L/K, Theorem 5.1 assures $\Phi_{\mathfrak{p}}(\sigma)P \neq O$ and

$$\hat{\lambda}_{\mathfrak{P}}(\Phi_{\mathfrak{p}}(\sigma)P) \geq \log p \quad \forall\, \mathfrak{P}|\mathfrak{p}.$$

But then, Theorem 3.2 together with our hypothesis (p.3) gives us:

$$\hat{h}(\Phi_{\mathfrak{p}}(\sigma)P) \geq \frac{\log p}{[K : \mathbb{Q}]} - C_0 \geq 1.$$

On the other hand, we can use the fact that $\hat{h}$ is a Galois invariant positive semidefinite quadratic form (see [Si09, VIII 5.10 & 9.3]), to produce a lower bound for $\hat{h}(P)$ in terms of $\hat{h}(\Phi_{\mathfrak{p}}(\sigma)P)$. Precisely, we compute

$$\begin{aligned}\hat{h}(\Phi_{\mathfrak{p}}(\sigma)P) &= \hat{h}(\sigma^2 P - [a_p]\sigma P + [p]P)\\ &\leq 3(\hat{h}(\sigma^2 P) + \hat{h}([a_p]\sigma P) + \hat{h}([p]P))\\ &= 3(\hat{h}(P) + a_p^2\hat{h}(P) + p^2\hat{h}(P))\\ &\leq 3(1+4p+p^2)\hat{h}(P). \quad (\text{since } |a_p| \leq 2\sqrt{p})\end{aligned}$$

Therefore

$$\hat{h}(P) \geq \frac{\hat{h}(\Phi_{\mathfrak{p}}(\sigma)P)}{3(1+4p+p^2)} \geq \frac{1}{3(1+4p+p^2)},$$

and as the primes $\mathfrak{p}$ and p were taken depending only on E and K, this is the desired lower bound for the case when L/K is unramified at $\mathfrak{p}$.

Now let us suppose L/K ramifies at $\mathfrak{p}$ (remember $L := K(P)$ where P is a given generic nontorsion point of $E(K^{ab})$). In this case, we can take $\tau \in I_{\mathfrak{p}}(L/K)$ according to Lemma 6.1 and use Theorem 6.4.a to guarantee that the point $P' := [p]((\tau - 1)^2 P)$ satisfies

$$\hat{\lambda}_{\mathfrak{P}}(P') \geq \log p \quad \forall\, \mathfrak{P}|\mathfrak{p}.$$

Further, due to our hypothesis (p.4), we may use Theorem 6.4.b to conclude $P' \neq O$. So, from Theorem 3.2 together with our assumption (p.3), we get

$$\hat{h}(P') \geq \frac{\log p}{[K:\mathbb{Q}]} - C_0 \geq 1.$$

On the other hand, we may again use the fact that $\hat{h}$ is a Galois invariant positive semidefinite quadratic form to argue in a similar way as we did for the previous case. We proceed as follows

$$\begin{aligned}
\hat{h}(P') &= \hat{h}([p](\tau - 1)^2 P) \\
&= p^2 \hat{h}(\tau^2 P - [2]\tau P + P) \\
&\leq 3p^2(\hat{h}(\tau^2 P) + 4\hat{h}(\tau P) + \hat{h}(P)) \\
&= 18p^2 \hat{h}(P).
\end{aligned}$$

Hence

$$\hat{h}(P) \geq \frac{\hat{h}(P')}{18p^2} \geq \frac{1}{18p^2}.$$

And so, as the primes $\mathfrak{p}$ and p were taken depending only on E and K, the proof is also complete for the case when $\mathfrak{p}$ ramifies at L/K.

□

References

[AmDv00] F. Amoroso, R. Dvornicich, *A lower bound for the height in abelian extensions*, J. Number Theory 80 (2000), 260-272.

[AnMa80] M. Anderson, D. Masser, *Lower bound for heights on elliptic curves*, Math. Zeit. 174 (1980), 23–34.

[Ba03] M. Baker, *Lower bounds for the canonical height on elliptic curves over abelian extensions*, IMRN 29 (2003), 1571-1582.

[BaSi04] M. Baker, J. H. Silverman, *A lower bound for the canonical height on abelian varieties over abelian extensions*, Math. Res. Letters 11 (2004), 377-396.

[DaHi00] S. David, M. Hindry, *Minoration de la hauteur de Néron-Tate sur les variétés abéliennes de type C.M*, J. Reine Angew. Math. 529 (2000), 1–74.

[DaPa08] S. David, A. Pacheco, *Le problème de Lehmer abélien pour un module de Drinfeld*, Int. J. Number Theory 4 (2008), 1043-1067.

[Do79] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Airth. 34 (1979), 391-401.

[FrTa93] A. Frölich, M. J. Taylor, *Algebraic Number Theory*, Cambridge University Press, 1993.

[HiSi90] M. Hindry, J. H. Silverman, *On Lehmer's conjecture for elliptic curves*, in Séminaire de Théorie des Nombres, Paris (1988–1989), Progress in Mathematics, Vol. 91, Birkhäuser, Boston, MA, 1990, pp. 103–116.

[La94] S. Lang, *Algebraic Number Theory*, Springer-Verlag, 2nd edition, 1994.

[La83] M. Laurent, *Minoration de la hauteur de Néron-Tate*, in Séminaire de Théorie des Nombres, Paris (1981–1982), Vol. 38, Birkhäuser, Boston, Basil, Stuttgart, 1983, pp. 137–152.

[Le33] D. H. Lehmer, *Factorization of Certain Cyclotomic Functions*, Ann. Math. 34 (1933), 461-469.

[Ma84] D. Masser, *Small values of the quadratic part of the Néron-Tate height on an abelian variety*, Compositio Math. 53 (1984), 153-170.

[Ma89] D. Masser, *Counting points of small height on elliptic curves*, Bull. Soc. Math. France 117 (1989), 247–265.

[Ne99] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, 1999 (Tanslation of 1992 German).

[Se72] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones Math. 15 (1972), 259-331.

[Se98] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves (revised reprint of the 1968 original).*, Research Notes in Mathematics, Vol. 7, A K Peters Ltd. (1998).

[Si81] J. H. Silverman, *Lower bound for the canonical height on elliptic curves*, Duke Math. J. 48 (1981), 633–648.

[Si90] J. S. Silverman, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. 55 (1990), 723-743.

[Si94] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, 1994.

[Si04] J. H. Silverman, *A lower bound for the canonical height on elliptic curves over abelian extensions*, J. Number Theory 104 (2004), 353-372.

[Si09] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 2nd edition, 2009.

[StSh03] E. M. Stein, R. Shakarchi, *Complex Analysis*, Princeton University Press, 2003.