ON POINTS OF SMALL HEIGHT IN INFINITE EXTENSIONS

ANUP B. DIXIT AND SUSHANT KALA

Abstract. In this paper, we introduce the notion of asymptotically positive infinite extensions of $\mathbb{Q}$, in the spirit of the Tsfasman-Vlăduţ theory of asymptotically exact families of number fields. For asymptotically positive extensions, we obtain lower bounds on the logarithmic Weil height, establishing the Bogomolov property for a wide range of infinite non-Galois extensions. Our result is in the spirit of the famous theorem of E. Bombieri and U. Zannier on Bogomolov property for totally p-adic extensions of type (e, f). Additionally, our theorem can be interpreted as a p-adic equidistribution result on conjugates of α, resonating with the archimedean equidistribution theorem à la F. Amoroso–M. Mignotte and Y. Bilu. In the parallel setting of elliptic curves, we derive lower bounds on the canonical height for points on an elliptic curve over asymptotically positive extensions, without any restriction on its reduction type. In particular, this extends a result of M. Baker and C. Petsche in the context of totally v-adic extensions.

1. Introduction

The logarithmic Weil height $h : \overline{\mathbb{Q}} \setminus \{0\} \to \mathbb{R}^+ \cup \{0\}$ plays a central role in understanding the arithmetic complexity of algebraic numbers and also induces a partial ordering on algebraic numbers with bounded degree. A well-known theorem of Kronecker characterizes the algebraic numbers α with $h(\alpha) = 0$ as precisely the roots of unity. For $\alpha \in \overline{\mathbb{Q}} \setminus \{0\}$ not a root of unity, Lehmer famously conjectured that

$$h(\alpha) > \frac{c}{\deg(\alpha)}$$

for an absolute constant $c > 0$. This remains an important open problem in number theory. The fact that $h(2^{1/n}) = (\log 2)/n$ shows that this expected lower bound of order $1/\deg(\alpha)$ for $h(\alpha)$ is sharp. Consequently, a crucial avenue of inquiry is to determine interesting subsets of $\overline{\mathbb{Q}}$, on which the height is uniformly bounded below.

A subset $S \subseteq \overline{\mathbb{Q}}$ is said to have the *Northcott property (N)* if for any $c > 0$, the set

$$\left\{\alpha \in S \,|\, \alpha \neq 0 \text{ and } h(\alpha) < c\right\}$$

is finite. Closely related is the *Bogomolov property (B)*. We say that a set $S \subset \overline{\mathbb{Q}}$ satisfies the property (B) if there exists a constant $c > 0$ such that

$$\left\{\alpha \in S \,|\, \alpha \neq 0, \alpha \text{ not a root of unity and } h(\alpha) < c\right\}$$

is empty. Clearly, if S satisfies (N), it also satisfies (B).

In [2], F. Amoroso and R. Dvornicich proved that $\mathbb{Q}^{ab}$, the maximal abelian extension of $\mathbb{Q}$, satisfies property (B). They showed that for non-zero $\alpha \in \mathbb{Q}^{ab}$, not a root of unity,

$$h(\alpha) > \frac{\log 5}{12}.$$

2020 *Mathematics Subject Classification.* 11G50, 11R04, 11R06, 11G05 .

Key words and phrases. Asymptotically positive extension, Weil height, Bogomolov property, Northcott property, Lehmer's conjecture, Canonical height of elliptic curves.

This was generalized to K^{ab} by F. Amoroso and U. Zannier [4] for any number field K. Earlier, in 1973, A. Schinzel [34] obtained property (B) for the set $\mathbb{Q}^{tr}$ of totally real numbers. More precisely, for $\alpha \in \mathbb{Q}^{tr} \setminus \{\pm 1\}$, he proved that

$$h(\alpha) \geq \frac{1}{2}\log\left(\frac{1+\sqrt{5}}{2}\right).$$

Another family of infinite extensions of $\mathbb{Q}$ for which we know property (B) are totally p-adic fields of type (e, f), i.e., infinite Galois extensions of $\mathbb{Q}$ with finite local degree over a prime p. This is the famous theorem of E. Bombieri and U. Zannier [10].

Theorem A (Bombieri-Zannier)**.** *Let $\mathcal{L}$ over $\mathbb{Q}$ be an infinite Galois extension. Define*

$$S(\mathcal{L}) := \left\{ p \ \text{prime} \,\middle|\, [\mathcal{L}_v : \mathbb{Q}_p] < \infty \ \text{for some } v \ \text{above } p \right\}.$$

Then

$$\liminf_{\alpha \in \mathcal{L}} \ h(\alpha) \ \geq \frac{1}{2} \sum_{p \in S(\mathcal{L})} \frac{\log p}{e_p \left(p^{f_p}+1\right)}, \tag{1}$$

where e_p is the ramification index and f_p is the residual degree of $\mathcal{L}_v/\mathbb{Q}_p$.

Thus, if $S(\mathcal{L})$ is non-empty, then $\mathcal{L}$ satisfies property (B). Furthermore, if the right-hand side in (1) diverges, then $\mathcal{L}$ satisfies property (N). An explicit example where the RHS diverges can be found in S. Checcoli and A. Fehm [11]. Note that if $p \in S(\mathcal{L})$, then for any $\alpha \in \mathcal{L}$, all the conjugates of α lie in a finite extension L_v of $\mathbb{Q}_p$. This can be considered as a non-archimedean analog of Schinzel's result on $\mathbb{Q}^{tr}$. There have been refinements of Theorem A in recent times. In 2015, P. Fili and C. Petsche [16] used methods of potential theory to obtain lower bounds on the height of algebraic numbers, all whose conjugates lie in certain local fields. This was later extended by P. Fili and I. Pritsker [17] to obtain new lower bounds for height of algebraic numbers all of whose conjugates lie in real intervals and p-adic discs.

All the above results give property (B) for infinite Galois extensions of $\mathbb{Q}$. In this paper, we establish property (B) for certain infinite extensions of $\mathbb{Q}$, which are not necessarily Galois. This is a rare instance where property (B) is proved for infinite non-Galois extensions. One of the main challenges in non-Galois extensions is the absence of natural invariants such as e_p and f_p, which were crucial in (1). To overcome this, we introduce the theory of asymptotically positive extensions, inspired by the study of asymptotically exact families by M. A. Tsfasman and S. G. Vlăduţ [42].

For a number field $K/\mathbb{Q}$ and a rational prime power $q = p^f$, define

$$\mathcal{N}_q(K) := \text{ the number of prime ideals of } K \text{ with norm } q.$$

An infinite extension $\mathcal{L}/\mathbb{Q}$ can be written as a tower of number fields

$$\mathcal{L} \supsetneq \cdots \supsetneq L_m \supsetneq L_{m-1} \supsetneq \cdots \supsetneq L_1 = \mathbb{Q},$$

where $L_i/\mathbb{Q}$ are finite extensions. Define

$$\psi_q(\mathcal{L}) = \psi_q := \lim_{i \to \infty} \frac{\mathcal{N}_q(L_i)}{[L_i : \mathbb{Q}]}.$$

This limit exists and is well-defined, i.e., independent of the tower $\{L_i\}$ (as shown in Proposition 4.2) and $0 \leq \psi_q \leq 1$. For instance, if a prime p splits completely in $\mathcal{L}$, then $\psi_p = 1$ and $\psi_{p^f} = 0$ for all $f > 1$. If $\psi_q > 0$ for some prime power q, we call the extension $\mathcal{L}$ to be *asymptotically positive*.

Inspired by Theorem A, the authors proposed the following conjecture in [13, Conjecture 2.2].

Conjecture 1.1. *Let $\mathcal{L}/\mathbb{Q}$ be an infinite extension of $\mathbb{Q}$. Then,*

$$\liminf_{\alpha\in\mathcal{K}} h(\alpha) \geq \frac{1}{2}\sum_{q} \psi_q \frac{\log q}{q+1}, \tag{2}$$

where q runs over all prime powers. Hence, if $\mathcal{L}$ is asymptotically positive, then $\mathcal{L}$ has property (B).

For infinite Galois extensions, the RHS in (2) is same as the RHS in (1). Indeed, let $\mathcal{L}/\mathbb{Q}$ be an infinite Galois extension and $p \in S(\mathcal{L})$, then

$$\frac{\log p}{e_p(p^{f_p}+1)} = \frac{\log p^{f_p}}{e_p f_p(p^{f_p}+1)} = \psi_{p^{f_p}}\left(\frac{\log p^{f_p}}{p^{f_p}+1}\right),$$

with e_p and f_p as before. The advantage of this formulation in terms of ψ_q's enables us to conjecture the analog of Theorem A for infinite non-Galois extensions. For totally p-adic fields, Bombieri and Zannier [10, Example 3] demonstrated that (1) is close to being optimal. More precisely, let S be a finite set of primes and $\mathcal{L}$ be the field of all totally p-adic algebraic numbers for $p \in S$. Then, they showed that

$$\sum_{p\in S}\frac{\log p}{p-1} \geq \liminf_{\alpha\in\mathcal{L}} h(\alpha) \geq \frac{1}{2}\sum_{p\in S}\frac{\log p}{p+1}.$$

Therefore, we also expect the lower bound in Conjecture 1.1 to be close to optimal.

In this paper, we partially resolve this conjecture as follows.

Theorem 1.2. *Let $\mathcal{L}/\mathbb{Q}$ be an infinite extension of $\mathbb{Q}$, and let $\mathcal{O}_\mathcal{L}$ be the ring of algebraic integers of $\mathcal{L}$.*

(a) The following inequality holds:

$$\liminf_{\alpha\in\mathcal{O}_\mathcal{L}} h(\alpha) \geq \frac{1}{2}\sum_{q} \psi_q \frac{\log q}{q},$$

where q runs over all prime powers.

(b) If $\psi_q(\mathcal{L}) > 0$ for $q = p^f$, there exists a λ, depending on p and $\mathcal{L}$, such that

$$\liminf_{\alpha\in\mathcal{L}\setminus\mu_\infty} h(\alpha) \geq \frac{\log q}{p^\lambda(q+1)}.$$

Therefore, if $\mathcal{L}$ is asymptotically positive, then $\mathcal{L}$ has property (B). Moreover, if the sum in (a) diverges, then $\mathcal{O}_\mathcal{L}$ has property (N).

Although Conjecture 1.1 still remains open, the bound in Theorem 1.2 (a) establishes it for algebraic integers. For algebraic non-integers, we obtain a weaker lower bound in Theorem 1.2 (b). Nevertheless, this proves property (B) for asymptotically positive extensions.

Remark. *It is important to note that asymptotically positive extensions contain finitely many roots of unity. This follows immediately from Theorem 1.2 (a). Alternatively, one can see this as follows. Let $\mathcal{L}$ be an asymptotically positive extension with $\psi_{p^f}(\mathcal{L}) > 0$. Suppose there exists an infinite tower of cyclotomic subfields of $\mathcal{L}$, say $\mathcal{K} = \bigcup_{i=1}^{\infty} K_i$ with $K_i = \mathbb{Q}(\zeta_{n_i})$. Clearly, $\psi_{p^f}(\mathcal{K}) > 0$. For sufficiently large i, the inertia degree of p in K_i must equal f. This implies that $p^f \equiv 1 \bmod n_i$ for all large enough i, which is a contradiction.*

We emphasize that Theorem 1.2 (a) is not a straightforward generalization of Theorem A. When $\mathcal{L}/\mathbb{Q}$ is Galois, the condition $[\mathcal{L}_v : \mathbb{Q}_p] < \infty$ is equivalent to the existence of a finite Galois extension $L/\mathbb{Q}$ with $L \subset \mathcal{L}$ such that all the prime ideals above p in L split completely in $\mathcal{L}$. However, if $\mathcal{L}/\mathbb{Q}$ is not Galois, one may not have such eventual complete splitting, yet it is still possible to have $\psi_q(\mathcal{L}) > 0$ for some prime power q. In this case, applying Theorem A to the Galois closure of $\mathcal{L}/\mathbb{Q}$ would lead to poor bounds on $h(\alpha)$. We illustrate this with an example below.

Example. Fix a rational prime p. We construct an infinite extension $\mathcal{L}/\mathbb{Q}$ such that $\psi_p > 0$, but $p \notin S(\widetilde{\mathcal{L}})$, where $\widetilde{\mathcal{L}}$ is the Galois closure of $\mathcal{L}$ over $\mathbb{Q}$. Thus, Theorem A is not applicable to $\widetilde{\mathcal{L}}$, where as Theorem 1.2 gives property (B) for $\mathcal{O}_{\mathcal{L}}$.

Let $K/\mathbb{Q}$ be a number field with distinct prime ideals $P_1, P_2, ..., P_s$ and $Q_1, Q_2, ..., Q_t$. For any integer $n \geq 2$, there exists a degree n extension L of K such that $P_1, P_2, ..., P_s$ split completely and $Q_1, Q_2, ..., Q_t$ totally ramify over L. It is clear that such an L exists, for instance, by solving the congruence system

$$\begin{aligned} f(x) &\equiv (x-1)(x-2)\cdots(x-n) && \pmod{P_j^m} \quad \text{for} \quad j = 1, 2, \ldots, s, \\ f(x) &\equiv x^n - b_i && \pmod{Q_i^2} \quad \text{for} \quad i = 1, 2, \ldots, t, \end{aligned}$$

where m is sufficiently large and $b_i \in Q_i \setminus Q_i^2$. As an application of the Chinese Remainder Theorem, we obtain a polynomial $f(x) \in \mathcal{O}_K[x]$ satisfying the above system of congruences. The congruence conditions and the choices of b_i ensure that $f(x)$ is an Eisenstein polynomial at each Q_i. Hence, $f(x)$ is irreducible, and each Q_i totally ramifies in the number field L obtained by adjoining a root of $f(x)$. In order to show that P_j splits completely in L, it suffices to prove that $f(x)$ splits into distinct linear factors over K_{P_j}, the completion of K at P_j. It follows from Hensel's lemma or the Newton approximation scheme [10, Lemma 1] that each integer $1 \leq i \leq n$ can be lifted to a unique root of $f(x)$ in K_{P_j} when m is sufficiently large. Thus, $f(x)$ splits into linear factors over K_{P_j}.

With the above observation, we now illustrate an example. Let $L_1/\mathbb{Q}$ be a degree 4 extension where p splits completely into $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$. Construct L_2/L_1 a degree 9 extension such that $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ split completely and $\mathfrak{p}_4$ ramifies, but not totally in L_2. This is achieved by first constructing L_2'/L_1 of degree 3 such that $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ split completely and $\mathfrak{p}_4$ ramifies completely. Then, we construct L_2/L_2' where all primes in L_2' above $\mathfrak{p}_1, \mathfrak{p}_2$ and $\mathfrak{p}_3$ split completely and the prime above $\mathfrak{p}_4$ also splits completely. Inductively construct L_{i+1}/L_i, an extension of degree p_{i+1}^2, where p_i is the i-th prime number, such that $\mathcal{N}_p(L_i) - \frac{\mathcal{N}_p(L_i)}{{p_i}^2}$ of the prime ideals of L_i with norm p split completely in L_{i+1} and the remaining prime ideals with norm p ramify in L_{i+1}, but not completely. For this tower $\mathcal{L} = \{L_i\}$, note that

$$\psi_p = \lim_{i \to \infty} \frac{\mathcal{N}_p(L_i)}{[L_i : \mathbb{Q}]} \geq \prod_{p_i} \left(1 - \frac{1}{{p_i}^2}\right) = \frac{1}{\zeta(2)},$$

where the product above runs over all rational primes p_i. Thus, we have $\psi_p > 0$. However, since the ramification degree of p is unbounded, $p \notin S(\widetilde{\mathcal{L}})$.

The maximal totally v-adic extensions of number fields are extreme examples of asymptotically positive extensions. For a random infinite extension $\mathcal{K}$ with $\psi_q > 0$, it is highly unlikely to expect $\mathcal{K}$ to be Galois or a maximal totally v-adic extension of a number field. The asymptotically positive condition is much weaker, as it is a density condition rather than a structural one. In particular, it does not require complete splitting, bounded local degrees at all places above a prime, or uniform Frobenius distribution.

In special cases, where there is minimal ramification of a prime in the infinite extension, it is feasible to obtain finer lower bounds, which could potentially surpass Theorem 1.2 (a). In this context, we define an infinite extension $\mathcal{L}/\mathbb{Q}$ to be *almost totally split at a prime p* if $\psi_p = 1$ and *almost unramified asymptotically positive at a prime p* if

$$\sum_{f\geq 1} f\,\psi_{p^f} = 1.$$

For such extensions, we obtain the following.

Proposition 1.3. *Let S denote a set of rational primes. Let $\mathcal{L}/\mathbb{Q}$ be an infinite extension which is almost totally split at all primes $p \in S$. Then*

$$\liminf_{\alpha\in\mathcal{L}} h(\alpha) \geq \frac{1}{2}\sum_{p\in S}\frac{\log p}{p+1}.$$

In other words, for the almost totally split case, we obtain Theorem 1.2 (a) over all algebraic numbers and not just algebraic integers. In the special case of the totally p-adic extension $\mathcal{L}/\mathbb{Q}$, which is the maximal extension of $\mathbb{Q}$ where p splits completely, Proposition 1.3 gives a slightly weaker result than the best known result obtained by L. Pottmeyer in [33]. He showed that if α is totally p-adic and not a $(p-1)$-th root of unity, then

$$h(\alpha) \geq \frac{\log(p/2)}{p+1}. \tag{3}$$

However, if more than one prime split completely in $\mathcal{L}$, then Pottmeyer's method may yield weaker bounds than Proposition 1.3.

We also establish a refined lower bound for almost unramified asymptotically positive extensions.

Theorem 1.4. *Let $\mathcal{L}/\mathbb{Q}$ be an infinite extension which is almost unramified asymptotically positive at a prime p. Then*

$$\liminf_{\alpha\in\mathcal{L}} h(\alpha) \geq \frac{1}{2}\sum_{f\geq 1} f^3\left(\psi_{p^f}\right)^2\frac{\log p}{p^f}.$$

Remark. *Using the same method, Proposition 1.3 and Theorem 1.4 can be extended to the infinite extensions $\mathcal{L}/K$, where K has class number one. In this case, let S be the set of prime ideals $\mathfrak{p}$ in $\mathcal{O}_K$ which almost totally splits in $\mathcal{L}$. Then*

$$\liminf_{\alpha\in\mathcal{L}} h(\alpha) \geq \frac{1}{2}\sum_{\mathfrak{p}\in\mathcal{O}_K}\frac{\log \mathrm{Norm}(\mathfrak{p})}{\mathrm{Norm}(\mathfrak{p})+1}.$$

Equivalently, let $\mathfrak{p}$ be a prime ideal in K which is almost unramified in $\mathcal{L}$, a similar statement as Theorem 1.4 can be deduced.

It is worth highlighting that the proof of Theorem A by Bombieri-Zannier involves obtaining lower bounds on the discriminant of the minimal polynomial of α and using Mahler's inequality (see Theorem 2.1). Applying the same method directly fails to give any meaningful result in the non-Galois setting. The novelty in our proof is building the theory of relative heights and establishing a relative Mahler's inequality, which helps in circumventing the obstructions that are encountered otherwise.

Another family of algebraic numbers satisfying property (B) can be obtained from the angular equidistribution theorem by Amoroso-Mignotte [3] (also see M. Mignotte [29] and Y. Bilu [9]).

Theorem B ([27], Theorem 15.2)**.** *For $\alpha \in \overline{\mathbb{Q}}$, let $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. For any θ with $0 \le \theta \le 2\pi$ the number n of conjugates of α in any fixed sector, based at the origin, of angle θ satisfies*

$$\left| n - \frac{\theta}{2\pi} d \right| \le 24 \left(d^{2/3} (\log 2d)^{1/3} + dh(\alpha)^{1/3} \right).$$

In other words, the set of all α whose conjugates do not have angular equidistribution satisfies property (B). If $\mathcal{L}$ is asymptotically positive, for all but finitely many $\alpha \in \mathcal{L}$, a positive proportion of their conjugates lie in a finite local extension $L_v/\mathbb{Q}_p$. Hence, Theorem 1.2 can be regarded as a p-adic equidistribution result in the spirit of Theorem B.

1.1. **Lower bound for canonical height of points on elliptic curves.** Let E be an elliptic curve defined over a number field K given by the Weierstrass equation $y^2 = x^3 + Ax + B$, where $A, B \in K$. For any extension L/K, denote by $E(L)$ the set of points $P \in E(\overline{K})$ such that $x(P), y(P) \in L$. Define the logarithmic Weil height of P as

$$h(P) := h(x(P)).$$

Although the logarithmic Weil height is easy to define, it is not compatible with respect to the group operation on elliptic curves. With this in mind, Néron and Tate introduced a height function, namely the canonical height, defined as

$$\widehat{h}(P) = \lim_{n \to \infty} \frac{h([2^n] \cdot P)}{4^n}.$$

The canonical height $\widehat{h}$ is a quadratic form on $E(\overline{K})$.

In the case of elliptic curves, torsion points can be thought of as analogs of roots of unity. Furthermore, $\widehat{h}(P) = 0$ if and only if P is a torsion point. Thus the analog of Kronecker's theorem holds for canonical height. It is then natural to consider lower bounds on $\widehat{h}$ for non-torsion points on elliptic curves. In this aspect, Lehmer's conjecture has been formulated in [5].

A set S of points in $E(\overline{K})$ is said to have the Bogomolov property (B) if there exists a constant $c > 0$ such that for all non-torsion points $P \in S$

$$\widehat{h}(P) \ge c.$$

Let $\mathcal{L}/\mathbb{Q}$ be an asymptotically positive infinite extension. By Theorem 1.2, we know that $\mathcal{L}$ satisfies property (B). It is natural to ask whether the same holds in the case of $E(\mathcal{L})$ when $K \subset \mathcal{L}$. We answer this in the affirmative below.

Theorem 1.5. *Let E/K be an elliptic curve. Let $\mathcal{L}/\mathbb{Q}$ be an asymptotically positive extension containing K. Then $E(\mathcal{L})$ satisfies property (B).*

For a totally p-adic extension $\mathcal{L}$ of type (e, f), M. Baker and C. Petsche [7] established property (B) for $E(\mathcal{L})$ under the condition that E has semi-stable reduction at the prime p. We establish property (B) for $E(\mathcal{L})$ over asymptotically positive extensions independent of the reduction type of E at p.

This theme of lower bounds on canonical height of elliptic curves is discussed in Section 7 and an explicit lower bound for $\widehat{h}(P)$ is obtained in Theorem 7.2.

Organization. This paper is organized as follows. In Section 2, we recall basic definition and some necessary results towards the proof of our main theorems. We develop the theory of relative height and deduce a relative Mahler's inequality in Section 3. Basic properties of asymptotically positive extensions are obtained in Section 4 and we prove Theorem 1.2 in Section 5. In Section 6, we prove Proposition 1.3 and Theorem 1.4. We describe the analog of this problem for elliptic curves in Section 7. Developing the necessary tools for local heights in Section 8, we prove Theorem 7.2 and hence Theorem 1.5 in Section 9.

Acknowledgments. We thank the referee for helpful comments and suggestions which significantly improved the earlier version of this manuscript. We are grateful to Prof. Sinnou David for several insightful comments, which simplified our proof of Theorem 7.2 avoiding the theory of discrepancies. We are thankful to Prof. Martin Widmer, Prof. Lukas Pottmeyer and Prof. Michel Waldschmidt for fruitful discussions and encouragement. We thank Prof. Sara Checcoli and Prof. Arno Fehm for their comments on an earlier version of this paper. We thank Prof. V. Kumar Murty, Prof. M. Ram Murty, Prof. Arnaud Plessis, Prof. Ananth Shankar, Prof. Siddhi Pathak and Jenvrin Jonathan for several helpful suggestions.

2. **Preliminaries**

Let $K/\mathbb{Q}$ be a number field. For $\alpha \in K^*$, the absolute logarithmic height or logarithmic Weil height is defined as

$$h(\alpha) = \sum_{v \in M_K} \log^+ |\alpha|_v,$$

where M_K is the set of all places of K, $\log^+ x = \max(0, \log x)$ and $|\alpha|_v$ is the normalized valuation on α defined as:

$$|\alpha|_v := \begin{cases} (N\mathfrak{p})^{-\frac{ord_{\mathfrak{p}}(\alpha)}{[K:\mathbb{Q}]}}, & \text{if } v \text{ is non-archimedean corresponding to the prime ideal } \mathfrak{p}, \\ |\sigma(\alpha)|^{\frac{[K_v:\mathbb{R}]}{[K:\mathbb{Q}]}}, & \text{if } v \text{ is archimedean corresponding to the embedding } \sigma \text{ of } K. \end{cases}$$

One can also define the logarithmic Weil height through the Mahler measure. Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ be the minimal polynomial of α. Then, its Mahler measure is defined as

$$M(\alpha) := |a_n| \prod_i \max(1, |\alpha_i|),$$

where α_i's denote the Galois conjugates of α. Mahler measure is connected to the height of α by the relation

$$\log M(\alpha) = h(\alpha)\,[\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Thus, Lehmer's conjecture can be stated as

$$\log M(\alpha) \geq c$$

for all non-zero $\alpha \in \overline{\mathbb{Q}}$ that are not roots of unity, where $c > 0$ is an absolute constant.

While this conjecture remains unresolved, there has been significant progress in recent times. The interested reader may refer to the excellent survey articles [41], [43] and the book by D. Masser [27] for a comprehensive account of this problem.

We now recall the classical Mahler's inequality [26].

Theorem 2.1 (Mahler)**.** *Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ be a polynomial with roots $\alpha_1, \alpha_2, \cdots, \alpha_n$. Let*

$$D := a_n^{2n-2} \prod_{i>j} (\alpha_i - \alpha_j)^2$$

be its discriminant. Then,

$$|D| \leq n^n M(f)^{2n-2},$$

where $M(f)$ denotes the Mahler measure of f, given by $M(f) := |a_n| \prod_i \max(1, |\alpha_i|)$.

We also recall the following well known lemma from algebraic number theory (see [31, Prop. II. 8.2])

Lemma 2.2. *Let K be a number field. Suppose $L = K(\alpha)$ and $f_K(x) \in \mathcal{O}_K[x]$ be the minimal polynomial of α over K. For a prime ideal $\mathfrak{p} \in K$, if*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \mathfrak{q}_2^{e_2} \cdots \mathfrak{q}_g^{e_g}$$

and $f_K(x)$ factors in K_v, the local field corresponding to $\mathfrak{p}$, as

$$f_K(x) = f_1(x) f_2(x) \cdots f_G(x),$$

then $g = G$ and up to ordering, $\deg f_j(x) = e_j f_j$, where e_j and f_j are the ramification index and the residue class degree of $\mathfrak{q}_j$ respectively.

In particular, let $L = \mathbb{Q}(\alpha)$ and $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α. If $p\mathcal{O}_L = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_g^{e_g}$ and $f(x)$ factors in $\mathbb{Q}_p$ as $f(x) = f_1(x) f_2(x) \cdots f_G(x)$, then $g = G$ and up to ordering $\deg f_j(x) = e_j f_j$.

We also need the following acceleration lemma as in [1, Lemma 2.1].

Lemma 2.3. *Let L be a number field, v be a finite place of K over a rational prime p and let $\rho > 0$. Let $\gamma_1, \gamma_2 \in \mathcal{O}_L$ such that $|\gamma_1 - \gamma_2|_v \leq p^{-\rho}$. Then for any non-negative integer λ we have $\left|\gamma_1^{p^\lambda} - \gamma_2^{p^\lambda}\right|_v \leq p^{-s_{p,\rho}(\lambda)}$ with $s_{p,\rho}(\lambda) \to +\infty$ for $\lambda \to +\infty$. More precisely, let us define an integer $k = k_{p,\rho}$ by $k = 0$ if $(p-1)\rho > 1$ and by*

$$p^{k-1}(p-1)\rho \leq 1 < p^k (p-1)\rho$$

otherwise. Then we can take

$$s_{p,\rho}(\lambda) = p^k \rho + \max(0, \lambda - k).$$

3. **Relative Weil height and Mahler's inequality**

In this section, we develop the theory of relative Weil height and prove an analog of Mahler's inequality (Theorem 2.1), which shall play a crucial role in the proof of Theorems 1.2 and 1.4.

Let K be a number field and $\alpha \in \overline{\mathbb{Q}} \setminus K$ be an algebraic integer of degree $n = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Let

$$f(x) = x^n + a_{n-1} x^{n-1} + \ldots + a_0$$

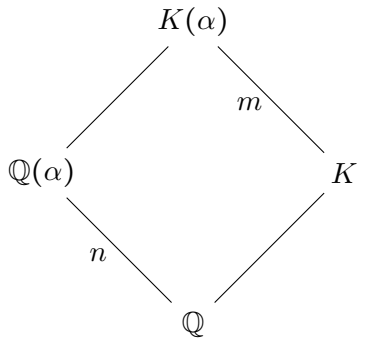
be the minimal polynomial of α over $\mathbb{Q}$ and $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the distinct complex roots of f. Let $f_K(x) = x^m + b_{m-1} x^{m-1} + \ldots + b_0$ be the minimal polynomial of α over O_K of degree $m = [K(\alpha) : K]$ and α_j's be its roots in the algebraic closure of K. We define the *relative Mahler measure* of α with respect to an embedding $\sigma : K \hookrightarrow \mathbb{C}$ as

$$M_{\sigma(K)}(\alpha) = \prod_{i=1}^{m} \max\left\{1, |\alpha_j^{\sigma}|\right\},$$

where $\left\{\alpha_j^{\sigma} : 1 \le j \le m\right\}$ are the complex roots of $\sigma(f_K(x))$. Counting all the roots with multiplicity, one obtains

$$f_K(x)^{[K(\alpha):\mathbb{Q}(\alpha)]} = \prod_{\sigma} \sigma(f_K(x)), \tag{4}$$

where σ runs over all the embeddings of K.



Thus, a natural way to define the *relative height* of α with respect to an embedding $\sigma : K \hookrightarrow \mathbb{C}$ is

$$h_{\sigma(K)}(\alpha) = \frac{\log M_{\sigma(K)}(\alpha)}{[K(\alpha) : K]} = \frac{\log M_{\sigma(K)}(\alpha)}{m}.$$

Using the multiplicativity of Mahler measure, from (4) we have

$$h(\alpha) = \frac{1}{[K : \mathbb{Q}]} \sum_{\sigma} h_{\sigma(K)}(\alpha). \tag{5}$$

In other words, the logarithmic Weil height is the average of relative heights with respect to all the embeddings.

3.1. **Mahler's inequality for relative height.** Let α and f_K be as above. The discriminant of f_K is given as

$$D(f_K) = \prod_{i<j\le m} (\alpha_i - \alpha_j)^2.$$

Thus for an embedding $\sigma : K \hookrightarrow \mathbb{C}$, we have

$$|\sigma(D(f_K))| = \prod_{i<j\le m} |\sigma(\alpha_i) - \sigma(\alpha_j)|^2.$$

We now proceed as in the proof of Mahler's inequality [26]. The product in the last equality is square of absolute value of a Vandermonde determinant. Thus applying Hadamard's inequality, we obtain

$$\begin{aligned} |\sigma(D(f_K))| &\le \prod_{i=1}^{m} \left(\sum_{j=0}^{m-1} |\sigma(\alpha_i)^j|^2 \right) \\ &\le \prod_{i=1}^{m} m \max\{1, |\sigma(\alpha_i)|^{2m-2}\} \\ &= m^m M_{\sigma(K)}(\alpha). \end{aligned}$$

Taking the logarithm, we deduce Mahler's inequality for relative height as below.

Lemma 3.1. *Let $\alpha \in \overline{\mathbb{Q}} \setminus K$ be an algebraic number, with minimal polynomial $f_K(x)$ over K of degree m. Then, for any embedding $\sigma : K \hookrightarrow \mathbb{C}$, we have*

$$\log|\sigma(D(f_K)| \ \leq \ m\log m + (2m-2)\log M_{\sigma(K)}(\alpha).$$

In other words, for relative height

$$h_{\sigma(K)}(\alpha) \geq \frac{1}{2}\left(\frac{\log|\sigma(D(f_K)|}{m^2} - \frac{\log m}{m}\right).$$

Summing over all embeddings of K and using (5), we deduce that

$$h(\alpha) \geq \frac{1}{2\,[K:\mathbb{Q}]}\left(\frac{\log\left(|N_{K/\mathbb{Q}}\,(D(f_K))\,|\right)}{m^2}\right) - \frac{\log m}{m}\,. \tag{6}$$

It is sometimes advantageous to work with the norm of the discriminant over a number field K, as opposed to considering the discriminant over $\mathbb{Q}$. This is mainly because of the identity

$$D(f) = |disc(K/\mathbb{Q})|^2\, N_{K/\mathbb{Q}}(D(f_K)),$$

where f and f_K are the minimal polynomials of an algebraic number α over $\mathbb{Q}$ and K respectively, and $disc(K/\mathbb{Q})$ is the discriminant of $K/\mathbb{Q}$. Thus $|N_{K/\mathbb{Q}}(D(f_K))|$ is smaller than $|D(f)|$ and hence, it is more feasible to obtain upper bounds for this norm.

The lower bound in (6) can be compared with a related result due to Silverman [37, Theorem 2], which states that

$$h(\alpha) \geq \frac{1}{2m-2}\left(\frac{1}{m}\log|N_{K/\mathbb{Q}}\left(\Delta_{K(\alpha)/K}\right)| - [K:\mathbb{Q}]\log m\right),$$

where $\Delta_{K(\alpha)/K}$ denotes the discriminant ideal. Notably, when $K = \mathbb{Q}$ and α is an algebraic integer, the relation $|D_f| = [\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]]^2|\Delta_{\mathbb{Q}(\alpha)}|$ demonstrates that (6) provides a sharper lower bound.

Remark. *The natural obstruction to extending the theory of relative Weil height to algebraic numbers is that the ring of integers of a general number field is not necessarily a principal ideal domain (PID). Consequently, there is no canonical choice for the minimal polynomial of an element $\alpha \in L \setminus K$ over $\mathcal{O}_K$. One can still extend the theory to the case when the number field K has class number one.*

4. **Asymptotically positive extensions**

In this section, we state and prove some basic properties of asymptotically positive extensions and the invariant ψ_q.

Lemma 4.1. *Let L/K be an extension of number fields and p be a rational prime. Then,*

$$\sum_{p^k \leq x} \frac{\mathcal{N}_{p^k}(K)\,\log p^k}{[K:\mathbb{Q}]} \geq \sum_{p^k \leq x} \frac{\mathcal{N}_{p^k}(L)\,\log p^k}{[L:\mathbb{Q}]}.$$

Proof. If a prime ideal $\mathfrak{q}$ in L has norm $\leq x$, then the prime ideal below, $\mathfrak{p} = \mathfrak{q} \cap K$ also has norm $\leq x$. Suppose a prime ideal $\mathfrak{p}$ in K splits into $\{\mathfrak{q}_1, \mathfrak{q}_2, \cdots, \mathfrak{q}_r\}$ in L. Then,

$$\prod_{i \leq r} N(\mathfrak{q}_i) = N(\mathfrak{p})^{[L:K]}.$$

Taking log on both sides

$$\sum_{m=1}^{n} \mathcal{N}_{p^m}(L) \log p^m \leq [L:K] \sum_{m=1}^{n} \mathcal{N}_{p^m}(K) \log p^m.$$

Dividing by $[L:\mathbb{Q}]$, we obtain the lemma.

□

Throughout this paper, for a number field $L/\mathbb{Q}$, denote by $n_L := [L:\mathbb{Q}]$. From Lemma 4.1, we deduce that for any tower $\mathcal{L} = \{L_i\}$ and any $x > 1$, the limit

$$\lim_{i \to \infty} \sum_{p^k \leq x} \frac{\mathcal{N}_{p^k}(L_i) \log p^k}{n_{L_i}}$$

exists. Therefore, inductively, we can conclude that the limit

$$\psi_q = \lim_{i \to \infty} \frac{\mathcal{N}_q(L_i)}{n_{L_i}}$$

exists for all prime powers q and takes value between 0 and 1. We now show that this invariant is independent of the choice of tower and hence, is well-defined.

Proposition 4.2. *Let $\mathcal{L}/\mathbb{Q}$ be an infinite extension and q be a rational prime power. Suppose $\{L_i\}$ and $\{K_i\}$ are two towers of number fields such that $\mathcal{L} = \bigcup_i K_i = \bigcup_i L_i$. Then,*

$$\lim_{i \to \infty} \frac{\mathcal{N}_q(L_i)}{n_{L_i}} = \lim_{i \to \infty} \frac{\mathcal{N}_q(K_i)}{n_{K_i}}.$$

Proof. Let $\psi_q := \lim_{i \to \infty} \frac{\mathcal{N}_q(K_i)}{n_{K_i}}$ and $\psi'_q := \lim_{i \to \infty} \frac{\mathcal{N}_q(L_i)}{n_{L_i}}$ for a prime power $q = p^m$. Suppose $K_i = \mathbb{Q}(\alpha)$. Since $K_i \subset \mathcal{L} = \bigcup_j L_j$, there exists L_j such that $\alpha \in L_j$. Hence, $K_i \subset L_j$ for some j. Similarly, every $L_j \subset K_l$ for some l. Therefore, applying Lemma 4.1, for every i, there exists j and l such that using

$$\sum_{p^k \leq x} \frac{\mathcal{N}_{p^k}(K_i) \log p^k}{n_{K_i}} \geq \sum_{p^k \leq x} \frac{\mathcal{N}_{p^k}(L_j) \log p^k}{n_{L_j}} \geq \sum_{p^k \leq x} \frac{\mathcal{N}_{p^k}(K_l) \log p^k}{n_{K_l}}.$$

Since ψ_q and ψ'_q exist for all prime powers, taking i to infinity, we conclude that for all $x > 1$,

$$\sum_{q \leq x} \psi_q \log q \geq \sum_{q \leq x} \psi'_q \log q \geq \sum_{q \leq x} \psi_q \log q.$$

Hence, $\psi_q = \psi'_q$ for all prime powers q. □

For an infinite extension $\mathcal{L} = \bigcup_i L_i$ over $\mathbb{Q}$, we say that a prime ideal $\mathfrak{p} \in L_j$ almost totally splits in $\mathcal{L}$ if the number of prime ideals above $\mathfrak{p}$ in L_t is $[L_t : L_j] + o(n_{L_t})$ for $t > j$ as $t \to \infty$. If $\psi_q > 0$ for some prime power q, then over any tower $\mathcal{L} = \bigcup_i L_i$, there exists an L_j such that all the primes above p in L_j with norm q almost totally split in $\mathcal{L}$. More precisely, we have the following.

Proposition 4.3. *Let $\mathcal{L} = \{L_i\}$ be an infinite extension of $\mathbb{Q}$ and p be a fixed rational prime. Suppose $\psi_{p^m} > 0$. Then there exists an integer N such that all prime ideals $\mathfrak{p} \in L_N$ with norm p^m almost totally split in $\mathcal{L}$. Furthermore, for any $\epsilon > 0$, there exists an M such that except at most ϵn_{L_M}, all prime ideals above p in L_M almost totally split in $\mathcal{L}$.*

Proof. To begin with, ψ_{p^m} is well-defined. Therefore, there exists an N_0 such that for all $i \geq N_0$, and $j > i$,

$$\frac{\mathcal{N}_{p^m}(L_j)}{n_{L_j}} - \frac{\mathcal{N}_{p^m}(L_i)}{n_{L_i}} = o(1),$$

as $j \to \infty$. Thus,

$$\mathcal{N}_{p^m}(L_j) = [L_j : L_i]\mathcal{N}_{p^m}(L_i) + o(n_{L_j}). \tag{7}$$

Let m be the smallest positive integer such that $\psi_{p^m} > 0$. Since $\psi_{p^t} = 0$ for all $t < m$, the number of prime ideals in L_i with norm $< p^m$ is $o(n_{L_i})$. Thus, almost all the prime ideals in L_j with norm p^m lie above the prime ideals in L_i with norm p^m. By equation (7), we deduce that above every $\mathfrak{p}$ in L_i with norm p^m, there are $[L_j : L_i] + o(n_{L_j})$ prime ideals in L_j, which implies that $\mathfrak{p}$ almost totally splits in $\mathcal{L}$.

Now suppose $m_1 > m$ is the smallest positive integer with $\psi_{p^{m_1}} > 0$. As $\psi_{p^{m_1}}$ is well-defined, we get that there exists an N_1 such that for all $i \geq \max(N_0, N_1)$ and $j > i$,

$$\mathcal{N}_{p^{m_1}}(L_j) = [L_j : L_i]\mathcal{N}_{p^{m_1}}(L_i) + o(n_{L_j})$$

as $j \to \infty$. Note that all prime ideals with norm p^m almost totally split in $\mathcal{L}$. Also, since $\psi_q = 0$ for all prime ideals with norm $\in (p^m, p^{m_1})$, the number of prime ideals in L_i with norm $\in (p^m, p^{m_1})$ is $o(n_{L_i})$. Therefore, we deduce that $[L_j : L_i]\mathcal{N}_{p^{m_1}}(L_i) + o(n_{L_j})$ prime ideals in L_j with norm p^{m_1} lie above $\mathcal{N}_{p^{m_1}}(L_i)$ prime ideals in L_i with norm p^{m_1}. Hence, every prime $\mathfrak{p}$ in L_i with norm p^{m_1} almost totally split in $\mathcal{L}$. Inductively, for any $X > 1$, there exists a N such that all prime ideals with norm $p^m \leq X$ in L_N almost totally split in $\mathcal{L}$ if $\psi_{p^m} > 0$.

To prove the second statement, taking $K = \mathbb{Q}$ in Lemma 4.1 gives

$$\sum_q \psi_q \log q \leq \log p,$$

where q runs over all the powers of p. Thus, $\sum_{m=1}^{\infty} \psi_{p^m}$ is bounded. Therefore, $\sum_m \psi_{p^m}$ is bounded and for every $\epsilon > 0$, there exists $X > 1$ such that

$$\sum_{p^m > X} \psi_{p^m} < \frac{\epsilon}{2}.$$

Using Lemma 4.1, one can find an M uniformly such that for all $i \geq M$,

$$\sum_{p^k \geq X} \frac{\mathcal{N}_{p^k}(L_i) \log p^k}{n_{L_i}} < \epsilon.$$

In other words, the number of prime ideals in L_i with norm $p^m > X$ is at most ϵn_{L_i} for $i \geq M$. This proves the proposition. □

Lemma 4.4. *Let $\mathcal{L}$ be an asymptotically positive extension and F be a number field. Then the compositum $\mathcal{L}F$ is also an asymptotically positive extension.*

Proof. Let $\mathcal{L} = \{L_i\}_{i\geq 0}$ be a tower of number fields. Since $\mathcal{L}$ is asymptotically positive, there exists a prime power $q = p^f$ such that $\psi_q(\mathcal{L}) > 0$. Let F be a number field of degree d, and define the tower $\mathcal{L}F = \{L_iF\}_{i\geq 0}$.

By definition, we have

$$N_q(L_i) = \psi_q(\mathcal{L})\, n_{L_i} + o(n_{L_i}).$$

It follows that

$$\sum_{k=1}^{d} N_{q^k}(L_iF) \geq \psi_q(\mathcal{L})\, n_{L_i} + o(n_{L_i}).$$

Dividing both sides by n_{L_iF} and taking the limit as $i \to \infty$, we obtain

$$\sum_{k=1}^{d} \psi_{q^k}(\mathcal{L}F) \geq \frac{\psi_q(\mathcal{L})}{d}.$$

Therefore, there exists some $k \in \{1, 2, \ldots, d\}$ such that for $q' = q^k$,

$$\psi_{q'}(\mathcal{L}F) \geq \frac{\psi_q(\mathcal{L})}{d^2} > 0.$$

Hence $\mathcal{L}F$ is asymptotically positive. □

5. **Proof of Theorem 1.2**

The outline of the proof of Theorems 1.2 (a) is inspired by the argument of Bombieri-Zannier in [10]. The new idea is to incorporate relative Mahler's inequality as developed in Section 3. The proof of Theorem 1.2 (b) involves the use of metric property of height and acceleration lemma.

Proof of Theorem 1.2 (a). Let $\mathcal{L}/\mathbb{Q}$ be an infinite extension. For any number field $L \subset \mathcal{L}$, by Northcott's theorem, there are finitely many $\alpha \in \mathcal{L}$ with degree $\leq n_L$ such that $h(\alpha) \leq \sum_q \psi_q(\mathcal{L}) \frac{\log q}{q+1}$, provided this sum converges.

For any $X > 1$, by Proposition 4.3, there exists a number field $L \subset \mathcal{L}$ such that for all prime powers $q \leq X$ with $\psi_q(\mathcal{L}) > 0$, all prime ideals of norm q in any finite extension of L almost totally split in $\mathcal{L}$.

For any $\alpha \in \mathcal{O}_{\mathcal{L}} \setminus L$, let $f_L(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be its minimal polynomial over $\mathcal{O}_L$. Let $q \leq X$ be such that $\psi_q(\mathcal{L}) > 0$ with $q = p^m$. Let $\mathfrak{p} \subset \mathcal{O}_L$ be a prime ideal with norm q. Since $\mathfrak{p}$ is almost totally split in $L(\alpha)$, by Lemma 2.2, we can write

$$f_L(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_t)\, g(x),$$

where $t = n + o(n)$. If L_v is the completion of L with respect to v, corresponding to the prime ideal $\mathfrak{p}$, then we have $\alpha_1, \alpha_2, \cdots, \alpha_t \in L_v$. Hence, the valuation v can be applied to all α_i's for $i \leq t$.

Let P_w be the splitting field of $f_L(x)$ over L_v with the unique valuation w extending v. Write

$$f_L(x) = (x - \beta_1)(x - \beta_2)\cdots(x - \beta_n).$$

The discriminant of f_L is given by

$$D(f_L) = \prod_{i<j} (\beta_i - \beta_j)^2.$$

Therefore,

$$w(D(f_L)) \geq 2 \sum_{i<j\leq n} w(\beta_j - \beta_i)$$

Restricting to β_j's which lie in L_v gives

$$v(D(f_L)) \geq 2 \sum_{\substack{i<j\leq n \\ \beta_i, \beta_j \in L_v}} v(\beta_j - \beta_i).$$

The number of $\beta_j \in L_v$ is $n + o(n)$. Let $\mathbb{F}_q := \mathcal{O}_L/\mathfrak{p}$ be the residue field at $\mathfrak{p}$. For each $x \in \mathbb{F}_q$, let N_x denote the number of roots β_j of f_L in L_v which lie in the residue class $x \bmod \mathfrak{p}$. Then, we have the lower bound

$$v(D(f_L) \geq \sum_{x \in \mathbb{F}_q} N_x(N_x - 1).$$

Since $\sum_{x\in\mathbb{F}_q} N_x = n + o(n)$, applying Cauchy-Schwarz inequality, we obtain

$$\begin{aligned} v(D(f_L)) &\geq \sum_{x\in\mathbb{F}_q} N_x(N_x-1) \\ &\geq \frac{n^2}{q} + o(n^2). \end{aligned} \tag{8}$$

Here $n = [L(\alpha) : L]$ and error term is $o(n^2)$ as $n \to \infty$. Taking the sum in equation (8) over all places $v \in M_L$ with norm $\leq X$, we obtain

$$\begin{aligned} \log N_{L/\mathbb{Q}}(D(f_L)) &= \sum_{v\in M_L} v(D(f_L)) \log(\mathrm{Norm}(v)) \\ &\geq \sum_{\substack{v\in M_L \\ \mathrm{Norm}(v)\leq X}} v(D(f_L))\, \log(\mathrm{Norm}(v)) \\ &= \left(\sum_{q\leq X} \mathcal{N}_q(L)\, \frac{\log q}{q} \right) n^2 + o(n^2), \end{aligned}$$

where q runs over all prime powers $\leq X$. Using this in the relative Mahler's inequality (6), we deduce that

$$h(\alpha) \geq \frac{1}{2[L:\mathbb{Q}]} \left(\sum_{q\leq X} \mathcal{N}_q(L)\, \frac{\log q}{q} \right) + o(1).$$

Hence,

$$\liminf_{\alpha\in\mathcal{O}_{\mathcal{L}}} h(\alpha) \geq \frac{1}{2} \sum_{q\leq X} \frac{\mathcal{N}_q(L)}{[L:\mathbb{Q}]}\, \frac{\log q}{q}.$$

Since $L \subseteq L_i$ for all large enough i and every extension of L has the property that all the ideal of norm q almost totally split in $\mathcal{L}$, thus

$$\liminf_{\alpha\in\mathcal{O}_{\mathcal{L}}} h(\alpha) \geq \frac{1}{2} \sum_{q\leq X} \frac{\mathcal{N}_q(L_i)}{[L_i:\mathbb{Q}]}\, \frac{\log q}{q}$$

for all but finitely many L_i. Taking the limit as $i \to \infty$ followed by $X \to \infty$, we obtain Theorem 1.2 (a). □

Towards the proof of Theorem 1.2 (b) we use metric inequalities as in Amoroso–David–Zannier [1]. This consequently proves the property (B) for asymptotically positive extensions. Unfortunately, this method yields a significantly weaker lower bound as compared to Theorem 1.2 (a).

Let $L/\mathbb{Q}$ be a number field and $\alpha \in L^\times$ not a root of unity. For a non-archimedean place v of L above p, denote by e_v and f_v the ramification index and inertia degree of v respectively. Since the residue field corresponding to v has order $q = p^{f_v}$, if α is v-integral, we have

$$|\alpha^q - \alpha|_v \leq p^{-1/e_v}.$$

On the other hand, if α fails to be v-integral, then its reciprocal α^{-1} must be v-integral, and consequently

$$|\alpha^{-q}(\alpha^q-\alpha)|_v = |\alpha|_v\ |\alpha^{-q}-\alpha^{-1}|_v \leq p^{-1/e_v}\ |\alpha|_v \implies |\alpha^q-\alpha|_v \leq p^{-1/e_v}\ |\alpha|_v^{q+1}$$

Therefore, for non-archimedean places $v \mid p$ of norm q, we get

$$|\alpha^q - \alpha|_v \leq c(v) \max\left(1, |\alpha|_v\right)^{q+1}, \tag{9}$$

where $c(v) = p^{-1/e_v}$. For all other places $w \in M_L$,

$$|\alpha^q - \alpha|_w \leq c(w) \max(1, |\alpha|_w)^{q+1},$$

where

$$c(w) = \begin{cases} 1, & \text{if } w \nmid \infty,\ N(w) \neq q; \\ 2, & \text{if } w \mid \infty. \end{cases}$$

Since α is not a root of unity, $\alpha^q - \alpha \neq 0$. Hence, the product formula gives

$$\begin{aligned} 0 &= \sum_{w \in M_L} \frac{[L_w : \mathbb{Q}_w]}{[L : \mathbb{Q}]} \log |\alpha^q - \alpha|_w \\ &\leq \sum_{w \in M_L} \frac{[L_w : \mathbb{Q}_w]}{[L : \mathbb{Q}]} \left(\log c(w) + (q+1) \log \max\{1, |\alpha|_w\}\right) \\ &= \left(\sum_{w \mid \infty} \frac{[L_w : \mathbb{Q}_w]}{[L : \mathbb{Q}]} \right) \log 2 - \left(\sum_{w \mid p, N(w) = q} \frac{[L_w : \mathbb{Q}_w]}{[L : \mathbb{Q}]} \right) \frac{\log p}{e_w} + (q+1) h(\alpha) \\ &= \log 2 - \frac{\mathcal{N}_q(L)}{[L : \mathbb{Q}]} \log q + (q+1) h(\alpha). \end{aligned}$$

So, we immediately deduce that

$$h(\alpha) \geq \frac{1}{q+1} \left(\frac{\mathcal{N}_q(L)}{[L : \mathbb{Q}]} \log q - \log 2 \right).$$

Suppose $\mathcal{L} = \bigcup_i L_i$. Taking liminf, we get

$$\liminf_{\alpha \in \mathcal{L} \setminus \mu_\infty} h(\alpha) \geq \frac{1}{q+1} \left(\psi_q(\mathcal{L}) \log q - \log 2 \right). \tag{10}$$

This bound is meaningful only if

$$\psi_q(\mathcal{L}) > \frac{2}{\log q},$$

which may not hold, as ψ_q can take arbitrarily small positive values. To overcome this limitation, we use the Lemma 2.3 with $\rho = 1/e_v$. Proceeding similarly to (9), we obtain

$$\left| \alpha^{p^{f_v + \lambda}} - \alpha^{p^\lambda} \right|_v \leq c'(v) \max(1, |\alpha|_v)^{p^{(f_v + \lambda)} + p^\lambda}, \tag{11}$$

where $c'(v) = p^{-s_{p,\rho}(\lambda)}$.

Proof of Theorem 1.2 (b). Suppose $\mathcal{L}/\mathbb{Q}$ is an asymptotically positive extension with $\psi_q(\mathcal{L}) > 0$ for $q = p^f$. Write $\mathcal{L} = \bigcup_{i=1}^{\infty} L_i$ as a tower of number fields.

In order to apply (11), note that $s_{p,\rho}(\lambda)$ depends on both λ and the place v. For our application, we first show that we can choose λ depending only on p such that the $s_{p,\rho}(\lambda)$ is bounded below uniformly, for a positive proportion of places above p. Indeed

$$\mathcal{N}_q(L_i) \leq \sum_{\substack{v \mid p, \\ N(v) = q}} e_v \leq [L_i : \mathbb{Q}]$$

and hence,

$$\frac{1}{\mathcal{N}_q(L_i)} \sum_{\substack{v \mid p, \\ N(v) = q}} e_v \leq \frac{[L_i : \mathbb{Q}]}{\mathcal{N}_q(L_i)}.$$

For sufficiently large i, let ϵ_i be such that the number of $v \mid p$, with $N(v) = q$ and $e_v \leq \frac{2}{\psi_q(\mathcal{L})}$ is given by $(1-\epsilon_i)\psi_q(\mathcal{L})[L_i:\mathbb{Q}]$. Clearly, $\epsilon_i \to 0$ as $i \to \infty$. For all such places with $e_v \leq \frac{2}{\psi_q(\mathcal{L})}$, the value of $\rho = \frac{1}{e_v}$ is uniformly bounded below. Therefore, for all such places, λ can be chosen so that $s_{p,\rho}(\lambda)$ is bounded below uniformly.

Using metric estimates for $\left|\alpha^{p^{\lambda}+q} - \alpha^{p^{\lambda}}\right|_v$ obtained in (11), we deduce that

$$\begin{aligned} p^{\lambda}(q+1)\ h(\alpha) &\geq \left(\sum_{\substack{v|p,\ N(v)=q \\ e_v \leq \frac{2}{\psi_q(\mathcal{L})}}} \frac{[(L_i)_v:\mathbb{Q}_p]}{[L_i:\mathbb{Q}]} \right) s_{p,\rho}(\lambda)\log p - \log 2 \\ &\geq s_{p,\rho}(\lambda)(1-\epsilon_i)\,\psi_q(\mathcal{L})\,\log q - \log 2, \end{aligned}$$

Since $\epsilon_i \to 0$ as $i \to \infty$, we conclude that

$$\liminf_{\alpha \in \mathcal{L}\setminus\mu^{\infty}} \quad h(\alpha) \geq \frac{1}{p^{\lambda}(q+1)} \left(s_{p,\rho}(\lambda)\ \psi_q(\mathcal{L})\log q - \log 2 \right).$$

Now choosing λ large enough so that $s_{p,\rho}(\lambda) > 2/\psi_q(\mathcal{L})$, we deduce that

$$\liminf_{\alpha \in \mathcal{L}\setminus\mu^{\infty}} \quad h(\alpha) > \frac{\log q}{p^{\lambda}(q+1)}.$$

This proves the theorem. □

6. **Proof of Proposition 1.3 and Theorem 1.4**

The central ideas in the proof of Proposition 1.3 and Theorem 1.4 are similar to those used in Theorem 1.2 (a), though a more careful analysis is required. For almost totally split extensions, unlike in the proof of Theorem 1.2 (a), we do not restrict ourselves to algebraic integers, as over the base field $\mathbb{Q}$ the relative Mahler measure coincides with the usual Mahler measure.

Proof of Proposition 1.3. Let $\mathcal{L}$ be an infinite extension and S be a set of rational primes such that $\mathcal{L}$ is almost totally split at each $p \in S$.

For any $\alpha \in \mathcal{L}$, let $L = \mathbb{Q}(\alpha)$ and $f(x) \in \mathbb{Z}[x]$ be its minimal polynomial of degree n. By Lemma 2.2, the minimal polynomial f factorizes over $\mathbb{Q}_p$ as

$$f(x) = a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_t)g(x),$$

where $t = n + o(n)$ and $\deg(g(x)) = o(n)$ as n goes to infinity. Thus the p-adic valuation v on $\mathbb{Q}_p$ can be applied to $\alpha_1, \cdots, \alpha_t$. Let L_w be the splitting field of $f(x)$ over $\mathbb{Q}_p$ with valuation w. Write

$$f(x) = a_n(x-\beta_1)(x-\beta_2)\cdots(x-\beta_n),$$

where $\beta_i \in L_w$ satisfying

$$w(\beta_1) \geq \cdots \geq w(\beta_r) \geq 0 > w(\beta_{r+1}) \geq \cdots \geq w(\beta_n).$$

Note that except for $o(n)$ many β_i's, the rest are same as α_i's up to ordering. Consider the discriminant

$$D(f) = a_n^{2n-2} \prod_{i<j} (\beta_i - \beta_j)^2.$$

The contribution in the product where at least one $w(\beta_j) < 0$ can be bounded by

$$w\left(\prod_{j=r+1}^{n}\prod_{i=1}^{j-1}(\beta_j-\beta_i)\right) \geq \sum_{j=r+1}^{n}(j-1)\,w(\beta_j).$$

Hence, we obtain

$$\begin{aligned} w(D(f)) &\geq (2n-2)w(a_n) + 2\sum_{0<i<j\leq r} w(\beta_j-\beta_i) \;+\; 2\sum_{j=r+1}^{n}(j-1)\,w(\beta_j) \\ &\geq 2\sum_{i<j\leq r} w(\beta_j-\beta_i) \;-\; 2\sum_{j=r+1}^{n}(n-j)\,w(\beta_j). \end{aligned} \tag{12}$$

Recall that $f(x)$ has $n+o(n)$ roots in $\mathbb{Q}_p$. Let e_w be the ramification index of $L_w/\mathbb{Q}_p$. For $\beta \in \mathbb{Q}_p$, we have $w(\beta) = v(\beta)\,e_w$. Since all terms in the RHS of (12) are positive, we can write

$$\begin{aligned} v(D(f)) = \frac{w(D(f))}{e_w} &\geq \frac{2}{e_w}\sum_{i<j\leq r} w(\beta_j-\beta_i) \;-\; \frac{2}{e_w}\sum_{j=r+1}^{n}(n-j)\,w(\beta_j) \\ &\geq 2\sum_{\substack{i<j\leq r\\ \beta_i,\beta_j\in\mathbb{Q}_p}} v(\beta_j-\beta_i) \;-\; 2\sum_{\substack{r<j\leq n\\ \beta_j\in\mathbb{Q}_p}}(n-j)\,v(\beta_j). \end{aligned} \tag{13}$$

Let N_x denote the number of v-integral roots β_j of the polynomial f in $\mathbb{Q}_p$, which lie in the residue class $x \bmod p$. If $\beta_i, \beta_j \in \mathbb{Q}_p$ lie in the same residue class modulo p, then $v(\beta_i-\beta_j) \geq 1$. Hence,

$$\sum_{\substack{i<j\leq r\\ \beta_i,\beta_j\in\mathbb{Q}_p}} v(\beta_j-\beta_i) \geq \sum_{x\in\mathbb{F}_p}\frac{N_x(N_x-1)}{2}.$$

Therefore, by (13), we have the lower bound

$$v(D(f)) \geq \sum_{x\in\mathbb{F}_p} N_x(N_x-1) + (n-r)(n-r-1).$$

Since the number of roots of $f(x)$ in $\mathbb{Q}_p$ is $n-r+\sum_{x\in\mathbb{F}_p}N_x = n+o(n)$, applying Cauchy-Schwarz inequality, we obtain

$$v(D(f)) \geq \frac{n^2+o(n^2)}{p+1}.$$

Summing over all primes $p \in S$ with $p \leq X$, we obtain

$$\log D(f) \geq \left(\sum_{p\in S,\,p\leq X}\frac{\log p}{p+1}\right)\left(n^2+o(n^2)\right).$$

Now, applying Theorem 2.1, we deduce

$$\begin{aligned} h(\alpha) = \frac{\log M(\alpha)}{n} &\geq \frac{(n-1)\log M(f)}{n^2} \geq \frac{\log D(f)}{2n^2} - \frac{\log n}{n} \\ &\geq \frac{1}{2}\left(\sum_{p\in S,\,p\leq X}\frac{\log p}{p+1}\right)(1+o(1)) - \frac{\log n}{n}. \end{aligned}$$

As $n \to \infty$, we have

$$\liminf_{\alpha\in\mathcal{L}} h(\alpha) \geq \frac{1}{2}\sum_{p\in S,\,p\leq X}\frac{\log p}{p+1}.$$

Finally, taking $X \to \infty$ proves Proposition 1.3.

□

Remark. *Let $\mathcal{L}$ be an extension which is almost totally split at a rational prime p. Then, for any $\alpha \in \mathcal{L}$ that is not a root of unity, it follows from* (10) *that*

$$h(\alpha) \geq \frac{\log(p/2)}{p+1} + o(1),$$

where $o(1)$ tends to zero as $\deg(\alpha) \to \infty$. In the totally p-adic case, this error term vanishes, yielding Pottmeyer's bound in (3) *exactly.*

We now establish lower bounds for logarithmic Weil heights of elements in an almost unramified asymptotically positive extension. Recall that an infinite extension $\mathcal{L}/\mathbb{Q}$ is said be almost unramified asymptotically positive at a prime p if

$$\sum_{f\geq 1} f\,\psi_{p^f} = 1.$$

In other words, if $\mathcal{L} = \bigcup_i L_i$,

$$\sum_{f=1}^{\infty} f\,\mathcal{N}_{p^f}(L_i) = n_{L_i} + o(n_{L_i}).$$

Proof of Theorem 1.4. We first note that for $L \subset \mathcal{L}$, the number of prime ideals in L with ramification index ≥ 2 is $o(n_L)$. Indeed, suppose $p\mathcal{O}_L = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}$. Because $\mathcal{L}$ is almost unramified asymptotically positive, we have

$$n_L = \sum_{f=1}^{\infty} f\,\mathcal{N}_{p^f}(L) + o(n_L) = \sum_{j\leq g} f_j + o(n_L),$$

where f_j is the residue class index of $\mathfrak{p}_j$. As $n_L = \sum_j e_j f_j$, we deduce that $e_j \geq 2$ for at most $o(n_L)$ prime ideals above p.

Since $\mathcal{L}$ is almost unramified asymptotically positive at p, for a given $\epsilon > 0$, there exists an integer N such that

$$1 - \epsilon \leq \sum_{f=1}^{N} f\,\psi_{p^f} \leq 1.$$

Thus for $\alpha \in \mathcal{L}$ and $L = \mathbb{Q}(\alpha)$ with $[L:\mathbb{Q}]$ large enough,

$$(1-\epsilon)\,n_L \leq \sum_{f=1}^{N} f\,\mathcal{N}_{p^f}(L) \leq n_L.$$

Let $f(x) = a_{n_L}x^{n_L} + a_{n_{L-1}}x^{n_{L-1}} + \cdots + a_0$ be the minimal polynomial of α over $\mathbb{Q}$ and $\widetilde{L}_\omega$ be the splitting field of $f(x)$ over $\mathbb{Q}_p$. Suppose the conjugates of α given by $\alpha_1, \alpha_2, \cdots, \alpha_{n_L}$ be ordered such that

$$\omega(\alpha_1) \geq \omega(\alpha_2) \geq \ldots \geq \omega(\alpha_r) \geq 0 > \omega(\alpha_{r+1}) \geq \ldots \geq \omega(\alpha_{n_L}).$$

Let $S_1, S_2, \ldots, S_N$ denote the set of unramified prime ideals in L above p, with norm $p, p^2, \ldots, p^N$ respectively. Thus, for each place ν_k in S_k, L_{ν_k} is an unramified extension of $\mathbb{Q}_p$ of degree k. By the uniqueness of the unramified extensions of $\mathbb{Q}_p$ of a given degree and the fact that $\widetilde{L}_\omega$ is the splitting field of $f(x)$, it follows that $L_{\nu_k} \subseteq \widetilde{L}_\omega$, for $1 \leq k \leq N$. Moreover, each L_{ν_k} has exaclty

$|S_k|$ many roots of $f(x)$ that generate L_{ν_k}. Hence, the roots of $f(x) \in \widetilde{L}_\omega$ that generate L_{ν_k} are in one to one correspondence with S_k.

For $1 \le k \le N$, let $\alpha_{1,k}, \alpha_{2,k}, \ldots, \alpha_{|S_k|,k}$ be the roots of $f(x)$ that generate L_{ν_k}. Grouping these roots together, we can write

$$\begin{aligned} f(x) = \; a_{n_L} & (x-\alpha_{1,1})(x-\alpha_{2,1}) \ldots (x-\alpha_{|S_1|,1}) \\ & (x-\alpha_{1,2})(x-\alpha_{2,2}) \ldots (x-\alpha_{|S_2|,2}) \\ & \vdots \qquad\quad \vdots \qquad\quad\quad \vdots \\ & (x-\alpha_{1,N})(x-\alpha_{2,N}) \ldots (x-\alpha_{|S_N|,N})\; g(x) \end{aligned}$$

where $g(x)$ has degree $o(n_L)$. The roots are ordered such that for a fixed k,

$$\omega(\alpha_{1,k}) \ge \omega(\alpha_{2,k}) \ge \ldots \ge \omega(\alpha_{r_k,k}) \ge 0 > \omega(\alpha_{r_k+1,k}) \ge \omega(\alpha_{|S_k|,k}).$$

Let $D(f)$ be the discriminant of $f(x)$. Then, we have

$$\begin{aligned} \omega(D(f)) \;&\ge\; 2 \sum_{1 \le i < j \le r} \omega(\alpha_i - \alpha_j) - 2 \sum_{j=r+1}^{n_L} (n_L - j)\, \omega(\alpha_j) \\ &\ge\; 2 \sum_{k=1}^{N} \left(\sum_{i<j\le r_k} \omega(\alpha_{i,k} - \alpha_{j,k}) - \sum_{j=r_k+1}^{|S_k|} (n_L - t_{j,k})\; \omega(\alpha_{j,k}) \right), \end{aligned} \tag{14}$$

where $t_{j,k}$ is the integer such that $\alpha_{t_{j,k}} = \alpha_{j,k}$. The last inequality follows from the fact that each term on the RHS of (14) is non-negative and we are considering only those roots that generate L_{ν_k}, for $1 \le k \le N$.

Let ν denote the usual p–adic valuation on $\mathbb{Q}_p$. Since ω and ν_k are the unique extensions of ν to $\widetilde{L}_\omega$ and L_{ν_k} respectively, we have

$$\begin{aligned} \omega(D(f)) &= \nu(D(f))\, e(\widetilde{L}_\omega | \mathbb{Q}_p), \\ \omega(\alpha_i - \alpha_j) &= \nu_k(\alpha_{i,l} - \alpha_{j,k})\, e(\widetilde{L}_\omega | L_{\nu_k}) \quad \text{and} \\ \omega(\alpha_j) &= \nu_k(\alpha_i)\, e(\widetilde{L}_\omega | L_{\nu_k}). \end{aligned}$$

Furthermore, $L_{\nu_k}/\mathbb{Q}_p$ is unramified and hence, $e(\widetilde{L}_\omega | L_{\nu_k}) = e(\widetilde{L}_\omega | \mathbb{Q}_p)$. Thus,

$$\nu(D(f)) \ge \; 2 \sum_{k=1}^{N} \left(\sum_{i<j\le r_k} \nu_k(\alpha_{i,k} - \alpha_{j,k}) - \sum_{j=r_k+1}^{|S_k|} (n_L - t_{j,k})\; \nu_k(\alpha_{j,k}) \right).$$

The roots $\alpha_{1,k}, \alpha_{2,k}, \ldots, \alpha_{r_k,k}$ lie in L_{ν_k}. Since the residue field of L_{ν_k} is $\mathbb{F}_{p^k}$, for each $x \in \mathbb{F}_{p^k}$, let $N_{x,k}$ denote the number of ν-integral $\alpha_{i,k}$'s that lie in the residue class $x \mod p^k$. Also, note that the numbers $(n_L - t_{j,k})$ appearing in (14) are distinct elements from the set $\{n_L - j : r_k + 1 \le j \le n_L\}$ and hence, form a set of distinct non-negative integers. Thus, we have the trivial bound

$$-\sum_{j=r_k+1}^{|S_k|} (n_L - t_{j,k})\; \nu_k(\alpha_{j,k}) \;\ge\; \sum_{j=0}^{|S_k|-r_k-1} j \;=\; \frac{(|S_k| - r_k - 1)\,(|S_k| - r_k)}{2}.$$

Therefore

$$\begin{aligned}\nu(D(f)) &\geq \sum_{k=1}^{N}\left(\sum_{x\in\mathbb{F}_{p^k}} N_{x,k}\left(N_{x,k}-1\right)+\left(|S_k|-r_k-1\right)\left(|S_k|-r_k\right)\right)\\ &\geq \sum_{k=1}^{N}\left(\sum_{x\in\mathbb{F}_{p^k}} {N_{x,k}}^2+\left(|S_k|-r_k\right)^2\right)+O(n_L).\end{aligned}$$

Since $(|S_k|-r_k)+\sum_{x\in\mathbb{F}_{p^k}} N_{x,k}=|S_k|$, by Cauchy-Schwarz inequality, we obtain

$$\nu_k(D(f)) \geq \sum_{k=1}^{N}\left(\frac{|S_k|^2}{p^k+1}\right)+O(n_L).$$

As $|S_k|=k\mathcal{N}_{p^k}(L)+o(n_L)$, we deduce that

$$\nu(D(f)) \geq \sum_{k=1}^{N}\left(\frac{k^2\mathcal{N}_{p^k}(L)^2}{p^k+1}\right)+O(n_L) \geq {n_L}^2\sum_{k=1}^{N}\frac{k^2}{p^k+1}\left(\frac{\mathcal{N}_{p^k}(L)}{n_L}\right)^2+o({n_L}^2).$$

Therefore,

$$\log D(f) \geq {n_L}^2\sum_{k=1}^{N}\frac{k^2}{p^k+1}\left(\frac{\mathcal{N}_{p^k}(L)}{n_L}\right)^2\log q+o({n_L}^2).$$

Now, using Theorem 2.1 and taking $N\to\infty$, we conclude that

$$\liminf_{\alpha\in\mathcal{L}} h(\alpha)\geq\sum_{k\geq 1}k^3\left(\psi_{p^k}\right)^2\frac{\log p}{2\left(p^k+1\right)}.$$

□

7. **Canonical height on elliptic curves**

Let E be an elliptic curve defined over a number field K. Recall that the canonical height of a point $P\in E(\overline{K})$ is given by

$$\widehat{h}(P):=\lim_{n\to\infty}\frac{h([2^n]\cdot P)}{4^n},$$

where h is the Weil height. The canonical height $\widehat{h}$ is a quadratic form on $E(\overline{K})$ and satisfies the following properties (see [30] or [22, Chapter IV, §3]) :

(a) $\widehat{h}(P)\geq 0$ for all $P\in E(\overline{K})$, and $\widehat{h}(P)=0$ iff P is a torsion point.

(b) $\widehat{h}([n]\cdot P)=n^2\widehat{h}(P)$ for all $n\in\mathbb{Z}$.

(c) $\widehat{h}(P_1+P_2)+\widehat{h}(P_1-P_2)=2\widehat{h}(P_1)+2\widehat{h}(P_2)$.

Lehmer's conjecture for elliptic curves, as formulated in [5] can be stated as follows.

Conjecture 7.1. *Let E be an elliptic curve over a number field K. For any $P \in E(\overline{K})$, let $K(P)$ denote the field obtained by adjoining the coordinates of P to K. Then, there exists a constant $C(E,K)$ depending only on E and K such that*

$$\widehat{h}(P) > \frac{C(E,K)}{[K(P):K]},$$

for all non-torsion points $P \in E(\overline{K})$.

This remains open but weaker lower bounds have been obtained in special cases. For a fixed number field K and a non-torsion point $P \in E(\overline{K})$, denote by $D = [K(P):K]$. Some classical results are listed below.

$\widehat{h}(P) \geqslant$	Restriction on E	Reference
$cD^{-10}(\log D)^{-6}$	none	Anderson-Masser (1980) [5]
$cD^{-1}\left(\frac{\log\log(D)}{\log(D)}\right)^3$	CM	Laurent (1983) [24]
$cD^{-3}(\log D)^{-2}$	none	Masser (1989) [28]
$cD^{-2}(\log D)^{-2}$	j non-integral	Hindry-Silverman (1990) [19]

TABLE 1. Bounds on $\widehat{h}$ for $E(\overline{K})$

Analogous to the case of algebraic numbers, for an elliptic curve E over K and $S \subseteq \overline{K}$, $E(S)$ is said to have *Bogomolov* property (B) if there exists a constant $C(E,K) > 0$, such that $\widehat{h}(P) > C(E,K)$, for all non-torsion points $P \in E(S)$.

Let $\mathcal{L}/\mathbb{Q}$ be an infinite extension satisfying property (B) with respect to the Weil height. Our objective is to understand if $E(\mathcal{L})$ satisfies property (B) with respect to the canonical height. The first result of this kind is due to S. Zhang [44], who showed that for an elliptic curve $E/\mathbb{Q}$, the set of totally real points $E(\mathbb{Q}^{tr})$ satisfies property (B). This can be thought of as the analog of Schinzel's result [34] for $\mathbb{Q}^{tr}$. In 2002, M. Baker proved property (B) for $E(K^{ab})$ when E is CM or has non-integral j-invariant. This is the analog of the theorem of Amoroso-Zannier [4] for K^{ab}. Moreover, Baker's bound only depends on the j–invariant of E and is effectively computable. Later, Silverman [40] proved property (B) for $E(K^{ab})$ when E is non-CM with the constant being ineffective. Some known bounds on $\widehat{h}$ over infinite extensions are summarized in the table below.

$\widehat{h}(P) \geqslant$	Restriction on E	Reference
cD^{-2}	none	Silverman (1981) [36]
$cD^{-1}(\log D)^{-2}$	none	Masser (1989) [28]
$cD^{-2/3}$	j non-integral	Hindry-Silverman (1990) [19]
c	j non-integral or CM	Baker (2003) [6]
c	none	Silverman (2003) [40]

TABLE 2. Bounds on $\widehat{h}$ for $E(K^{ab})$

Recall that a subfield $\mathcal{L}$ of $\overline{\mathbb{Q}}$ is said to be totally p-adic of type (e,f) if for any place v in $\mathcal{L}$ above p, $\mathcal{L}_v/\mathbb{Q}_p$ is a finite extension with ramification index and residue class degree bounded above by e and f respectively. Let E/K be an elliptic curve with semistable reduction at all places above $p \neq 2$. In 2005, M. Baker and C. Petsche [7] showed that if $\mathcal{L}/K$ is a totally p-adic field of type (e,f) for a prime p, then $E(\mathcal{L})$ has property (B). This can be regarded as the elliptic analog of Bombieri-Zannier's result Theorem A. In this case, they also gave an effective upper bound for the number of torsion points in $E(\mathcal{L})$. Let $E/\mathbb{Q}$ be an elliptic curve and $\mathbb{Q}(E_{tor})$

denote the field generated by all torsion points of E in $\overline{\mathbb{Q}}$. In 2013, Habegger [18] showed that both $\mathbb{Q}(E_{tor})$ and $E(\mathbb{Q}(E_{tor}))$ have property (B) with respect to the Weil and the canonical height respectively. Note that the Kronecker-Weber theorem implies that $\mathbb{Q}^{ab}$ is generated by all the roots of unity in $\overline{\mathbb{Q}}$. Therefore, the field $\mathbb{Q}(E_{tor})$ can be thought of as the elliptic analog of $\mathbb{Q}^{ab}$.

Let $\mathcal{L}/\mathbb{Q}$ be an asymptotically positive infinite extension. By Theorem 1.2, we know that $\mathcal{L}$ satisfies property (B). Our goal is to prove that $E(\mathcal{L})$ satisfies property (B) for any elliptic curve E. Towards this, we introduce some notation.

Consider an elliptic curve E/K and a tower $\mathcal{L} = \{L_i\}_{i\geq 0}$ containing K. For any rational prime power $q = p^k$, denote by $G_q(L_i)$ and $B_q(L_i)$ the number of prime ideals in L_i of norm q with good reduction and split multiplicative reduction at E/L_i respectively. Define

$$\xi_q(\mathcal{L}) := \lim_{i\to\infty} \frac{G_q(L_i)}{[L_i:\mathbb{Q}]} \quad \text{and} \quad \chi_q(\mathcal{L}) := \lim_{i\to\infty} \frac{B_q(L_i)}{[L_i:\mathbb{Q}]}.$$

Since every prime of bad reduction attains split multiplicative reduction after a finite base change, there exists a number field L/K such that E/L has semistable reduction i.e. either good or split multiplicative reduction at every non-archimedean place in L. Suppose $\mathcal{L} = \bigcup_{i=1}^{\infty} L_i$ be an asymptotically positive extension and $L \subset \mathcal{L}$, then clearly

$$\psi_q(\mathcal{L}) = \xi_q(\mathcal{L}) + \chi_q(\mathcal{L}).$$

On the other hand, if $L \notin \mathcal{L}$, then note that $\mathcal{L} \otimes_K L = \bigcup_{i=1}^{\infty} L_i \otimes_K L$ is also an asymptotically positive extension. Since E/L has semistable reduction over all non-archimedean primes, we have, for all primes powers q,

$$\psi_q(\mathcal{L} \otimes_K L) = \xi_q(\mathcal{L} \otimes_K L) + \chi_q(\mathcal{L} \otimes_K L).$$

Example. Note that, in the above paragraph, the desired reduction property of the elliptic curve E holds for $\mathcal{L}' := \mathcal{L} \otimes_K L$, but not necessarily for $\mathcal{L}$. For instance, let $E/\mathbb{Q}$ be the elliptic curve given by $y^2 = x^3 + 7x$ and let $\mathcal{L} := \mathbb{Q}^{t_7}$, the maximal totally 7-adic extension of $\mathbb{Q}$. Then, $\mathcal{L}$ is asymptotically positive with $\psi_7(\mathcal{L}) = 1$ and for any $L_i \subset \mathcal{L}$, E/L_i has additive reduction at all the places of L_i above 7. However, in $L = \mathbb{Q}(\sqrt{-1})$, the prime 7 remains inert and E has split multiplicative reduction over the unique prime above 7 in L. Now, considering the infinite extension $\mathcal{L}' = \mathcal{L} \otimes_{\mathbb{Q}} L$, we note that $\mathcal{L}'$ is asymptotically positive with $\psi_{49}(\mathcal{L}') > 0$ and E has semistable reduction over all the primes above 7 in $\mathcal{L}'$.

Our main theorem is as follows.

Theorem 7.2. *Let E/K be an elliptic curve and $\mathcal{L} = \bigcup_i L_i$ be an infinite extension over K. Then,*

$$\liminf_{P\in E(\mathcal{L})} \widehat{h}(P) \geq \frac{1}{48} \sum_q \left(6 \left(\frac{q+1}{q+1+2\sqrt{q}} \right) \xi_q(\mathcal{L}) + (q+1)\, c_E\, \chi_q(\mathcal{L}) \right) \frac{\log q}{q+1},$$

where the sum runs over all prime powers q and c_E is a positive constant depending on E and K.

This answers a question raised by P. Fili and Z. Miner [15] about obtaining a quantitative lower bound for canonical height of points on elliptic curves over totally p-adic extensions. This question appears in the pre-print version of the paper (see page 4 of `https://math.okstate.edu/people/fili/equi-splitting.pdf`).

As an immediate corollary to Theorem 7.2 and Lemma 4.4, we deduce Theorem 1.5 as stated in the introduction.

Corollary 7.3. *Let E/K be an elliptic curve. Let $\mathcal{L}/\mathbb{Q}$ be an asymptotically positive extension containing K. Then $E(\mathcal{L})$ satisfies property (B).*

Proof. Let L/K be a finite extension such that E/L has good reduction or split multiplicative reduction over all non-archimedean places in L. Since $\mathcal{L}/\mathbb{Q}$ is asymptotically positive, Lemma 4.4 implies that $\mathcal{L} \otimes_K L$ is also an asymptotically positive extension and

$$\psi_q(\mathcal{L} \otimes_K L) = \xi_q(\mathcal{L} \otimes_K L) + \chi_q(\mathcal{L} \otimes_K L) > 0$$

for some prime power q. Now, Theorem 7.2, implies that $E(\mathcal{L} \otimes_K L)$ satisfies property (B) and hence, $E(\mathcal{L})$ satisfies property (B). □

Let $E/\mathbb{Q}$ be an elliptic curve with good reduction at p. For $q = p^m$ and any infinite extension $\mathcal{L}/\mathbb{Q}$, by definition $\psi_q(\mathcal{L}) = \xi_q(\mathcal{L})$. Hence, we have the following corollary.

Corollary 7.4. *Let $E/\mathbb{Q}$ be an elliptic curve and $\mathcal{L}$ be an infinite extension of $\mathbb{Q}$. Then,*

$$\liminf_{P \in E(\mathcal{L})} \widehat{h}(P) \geq \frac{1}{8} \sum_q{}' \psi_q(\mathcal{L}) \frac{\log q}{q + 1 + 2\sqrt{q}},$$

where $\sum'$ runs over all prime powers $q = p^m$ such that E has good reduction at p. In particular, if $\psi_{p^m} > 0$ and E has good reduction at p, then $E(\mathcal{L})$ satisfies property (B).

The condition in the corollary above can be relaxed from primes of good reduction to primes of potentially good reduction for E. This is because if $E/\mathbb{Q}$ has potentially good reduction at p, then there exists a finite extension $K/\mathbb{Q}$ such that E/K has good reduction at all places of K lying above p.

Note that the lower bound in the above corollary is independent of the elliptic curve. By Corollary 7.4, one may vary over all elliptic curves $E/\mathbb{Q}$ with good reduction at p and still obtain a uniform lower bound on $\widehat{h}$. It is worthwhile comparing this to Lang's conjecture [22, p. 92], which states that for a fixed number field $K/\mathbb{Q}$, there exist constants C_1 and C_2 depending only on K such that for any elliptic curve E/K

$$\widehat{h}(P) \geq C_1 \log N_{K/\mathbb{Q}} \Delta - C_2,$$

where Δ is the discriminant of E over K.

8. **A lower bound on local height**

Let K be a number field. Denote by M_K and M_K^∞ the set of all places and the set of archimedean places of K respectively. Suppose that $v \in M_K \setminus M_K^\infty$ be a non-archimedean place corresponding to a prime ideal $\mathfrak{p}$ in K above p. Denote by $|\cdot|_v$ the unique absolute value on K_v which extends the usual p-adic absolute value on $\mathbb{Q}_p$.

Let E/K be an elliptic curve with point of infinity O. Similar to Weil height, the canonical height $\widehat{h}$ on E has a decomposition into local height functions $\lambda_v : E(K_v) \to \mathbb{R}$ (called Néron local heights) for each place v in M_K (see [38, Chapter VI, Theorem 1.1]). For any $P \in E(K) \setminus \{O\}$, we have

$$\widehat{h}(P) = \sum_{v \in M_K} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \lambda_v(P). \tag{15}$$

Unlike the canonical height $\widehat{h}$, the local height λ_v can take negative values, but such places are only finitely many. We start by discussing explicit formula for λ_v and some lower bounds on λ_v for both archimedean and non-archimedean places.

8.1. **Archimedean place.** Let v be an Archimedean place of K. Then, the $v-$adic completion of K, K_v is either $\mathbb{R}$ or $\mathbb{C}$. Thus, we can assume E to be defined over $\mathbb{C}$. By uniformization theorem for elliptic curves over $\mathbb{C}$, we get the following isomorphism

$$E(\mathbb{C}) \quad \cong \quad \mathbb{C}/\Lambda_\tau \quad \xrightarrow[z\mapsto u=e^{2\pi i z}]{\cong} \quad \mathbb{C}^*\big/q_\tau^{\mathbb{Z}},$$

where Λ_τ is the lattice $\mathbb{Z}+\tau\mathbb{Z}$ in $\mathbb{C}$ for some τ in the upper half plane and $q_\tau = e^{2\pi i\tau}$. Then, the local height function

$$\lambda_v : E(\mathbb{C}) \smallsetminus \{O\} \to \mathbb{R}$$

is given by

$$\lambda_v(P) = -\frac{1}{2}B_2\left(\frac{\mathrm{Im}(z)}{\mathrm{Im}(\tau)}\right)\log|q_\tau| - \log|1-u| - \sum_{n\geq 1}\log\left|(1-{q_\tau}^n u)(1-{q_\tau}^n u^{-1})\right|, \tag{16}$$

where $B_2(T) = T^2 - T + \frac{1}{6}$ is the second Bernoulli polynomial for $0 \leq T \leq 1$, extended to $\mathbb{R}$ periodically and z (resp. u) is the image of P in $\mathbb{C}/\Lambda_\tau$ (resp. $\mathbb{C}^*\big/q_\tau^{\mathbb{Z}}$). The periodicity of $B_2(T)$ ensures that the definition of $\lambda_v(P)$ is independent of the representative z in $\mathbb{C}/\Lambda_\tau$. Further, the convergence of the series is guaranteed by the fact that $\mathrm{Im}(\tau) > 0$.

Proposition 8.1. *Let $P_1, P_2, \ldots, P_N \in E(\mathbb{C})\smallsetminus\{O\}$ be N distinct points. Then, there is a constant $b(E) > 0$ depending on E such that*

$$\sum_{\substack{1\leq i,\, j\leq N\\ i\neq j}} \lambda_v(P_i - P_j) \geq -\frac{1}{2}N\log N - b(E)\,N. \tag{17}$$

This proposition follows from a result of Elkies, slightly different proof of which is given in [20, pp. 218] and [23, Chapter VI, Theorem 5.1]. An explicit version using results from Fourier analysis can be found in [7, Proposition 4].

8.2. **Non-archimedean place.** For a non-archimedean place v, let K_v be the completion of K. Thus, E/K can be seen as an elliptic curve over K_v. Denote by Δ the discriminant of a Weierstrass equation of E. Consider, the minimal Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a^6 \tag{18}$$

of E corresponding to v, i.e., $v(\Delta)$ is minimal, subject to the condition that the coefficients are v-integral. Let $\widetilde{E}$ be the curve obtained by reduction of Weierstrass equation of E at v. Define,

$$E_0(K_v) = \left\{P \in E(K_v)\,|\,\widetilde{E} \text{ is smooth at } \overline{P}\right\},$$

where $\overline{P}$ is the reduction of P at v. Thus, $E_0(K_v)$ consists of all the points of $E(K_v)$ that reduce to a non-singular point after reducing modulo v. An explicit formula for λ_v at these points is given as follows [38, Chap. VI, Theorem 4.1].

Proposition 8.2. *Let E/K_v be an elliptic curve and v be non-archimedean place of K. Let Δ be the discriminant of a Weierstrass equation of E with $v-$integral coefficients. Then the local height function*

$$\lambda_v(P) = \frac{1}{2}\max\left\{v(x(P)^{-1}), 0\right\} + \frac{1}{12}v(\Delta) \tag{19}$$

for all $P \in E_0(K_v)\setminus\{O\}$.

The above formula for local height does not depend on the choice of the Weierstrass equation. However, it only holds for points in $E_0(K_v)$, which depends on the choice of Weierstrass equation, and hence, for two different Weierstrass equation, the formula coincides on the intersection.

Moreover, equation (19) is valid only for points that are non-singular modulo v. The explicit description of λ_v on $E(K_v)\setminus E_0(K_v)$ depends on the nature of reduction type of $E(K_v)$ and is

discussed below case by case. For the minimal Weierstrass equation (18), following [39, pp. 42], define

$$b_2 = {a_1}^2 + 4a_4,\ b_4 = 2a_4 + a_1a_3,\ b_6 = {a_3}^2 + 4a_6 \text{ and } c_4 = {b_2}^2 - 24b_4.$$

8.2.1. **Additive reduction** $(v(\Delta) > 0,\ v(c_4) > 0)$ **:**

Let $f(x) \in K_v[x]$ be a polynomial. For $P \in E(K_v) \setminus \{O\}$, denote $f(x(P))$ by $f(P)$.

Consider the polynomials :

$$F(x) := 4x^3 + b_2x^2 + 2b_4x + b_6,$$
$$G(x) := (3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8)^2.$$

Then, for $P \in E(K_v) \setminus E_0(K_v)$, we have

$$\lambda_v(P) = \begin{cases} -\frac{1}{6}v(F(P)) + \frac{1}{12}v(\Delta) & \text{if } v(G(P)) \geq 3v(F(P)), \\ -\frac{1}{16}v(G(P)) + \frac{1}{12}. \end{cases}$$

8.2.2. **Multiplicative reduction** $(v(\Delta) > 0, v(c_4) = 0)$ **:**

Let

$$\alpha(P) = \min\left\{\frac{v((2y + a_1x + a_3)P)}{v(\Delta)}, \frac{1}{2}\right\}.$$

Then, for $P \in E(K_v) \setminus E_0(K_v)$, the local height is given by

$$\lambda_v(P) = \frac{1}{2}B_2(\alpha(P))v(\Delta). \tag{20}$$

8.2.3. **Good reduction** $(v(\Delta) = 0)$ **:**

In this case, we have $E_0(K_v) = E(K_v)$ and $v(\Delta) = 0$. Therefore, by (19), we get

$$\lambda_v(P) = \frac{1}{2}\max\left\{v(x(P)^{-1}), 0\right\}$$

for all $P \in E(K_v) \setminus \{O\}$. Further, the integrality of coefficients of (18) implies that

$$v(x(P)^{-1}) < 0 \iff v(x(P)/y(P)) < 0.$$

Using this along with the fact that $\min\{3\,v(x(P)), 0\} = \min\{2\,v(y(P)), 0\}$, we obtain

$$\frac{1}{2}\max\{v(x(P)^{-1}), 0\} = v(x(P)/y(P)).$$

Therefore, in the good reduction case

$$\lambda_v(P) = \max\left\{v\left(\frac{x(P)}{y(P)}\right), 0\right\}. \tag{21}$$

8.3. **Explicit formula for local height and Tate map.** Similar to the uniformization theorem for complex elliptic curves, the Tate parametrization offers a way to parametrize elliptic curves over non-archimedean complete fields ([38, See V.5]). Therefore, for an elliptic curve E/K_v, which has multiplicative reduction at v, there exists $q_E \in K_v^\times$ such that $|q_E|_v < 1$ and the corresponding parametrization (Tate map) is given by the isomorphism

$$\phi : K_v^\times / q_E^{\mathbb{Z}} \xrightarrow{\cong} E(K_v).$$

The Tate parametrization provides an analog of explicit formula for the local height function (16) in the non-archimedean case as follows (see [38, Chapter V, Theorem 4.2]).

Theorem C (Tate)**.** *Let $K_v/\mathbb{Q}_p$ be a finite extension and E/K_v be an elliptic curve with multiplicative reduction at v. Let ϕ be the Tate map of E/K_v discussed above. Then,*

(i) the Néron local height function

$$\lambda_v \circ \phi : E(K_v)\backslash\{O\} \longrightarrow \mathbb{R}$$

is given by the formula

$$\lambda_v(\phi(u)) = \frac{1}{2}B_2\left(\frac{v(u)}{v(q_E)}\right)v(q_E) + v(1-u) + \sum_{n\geq 1} v\left((1-q_E^n u)\left(1-q_E^n u^{-1}\right)\right).$$

(ii) If we choose u (by periodicity) to satisfy

$$0 \leq v(u) < v(q_E),$$

then

$$\lambda_v(\phi(u)) = \begin{cases} \frac{1}{2}B_2\left(\frac{v(u)}{v(q_E)}\right)v(q_E), & \text{if } 0 < v(u) < v(q_E), \\ v(1-u) + \frac{1}{12}v(q_E), & \text{if } v(u) = 0. \end{cases}$$

Remark. Suppose that E has multiplicative reduction. If $P \in E(K_v)$, we write $u(P)$ for the image of P in $K_v^\times/q_E^{\mathbb{Z}}$ under the Tate map $E(K_v) \simeq K_v^\times/q_E^{\mathbb{Z}}$. Consider, the retraction homomorphism $r : E(K_v) \longrightarrow \mathbb{R}/\mathbb{Z}$ defined as

$$r(P) = \frac{\log|u(P)|_v}{\log|q_E|_v}.$$

Since $\{\,|x|_v \mid x \in K_v^\times\,\} \subseteq p^{\mathbb{Q}}$, the image of r is actually contained in the subgroup $\mathbb{Q}/\mathbb{Z}$ of $\mathbb{R}/\mathbb{Z}$.

We end this section with the following non-archimedean analog of Proposition 8.1.

Proposition 8.3. *Let $P_1, P_2, \ldots, P_N \in E(\mathbb{C}_v) \smallsetminus \{O\}$ be N distinct points, where v is a non-archimedean place. Then,*

$$\sum_{\substack{1\leq i,\, j\leq N \\ i\neq j}} \lambda_v(P_i - P_j) \geq -\frac{N}{12}v(\Delta). \tag{22}$$

Above proposition holds trivially in the good reduction case, so it is enough to consider additive and multiplicative reduction case. Since the local height is invariant under base change to a higher extension, there always exists a finite extension of K_v such that E has either good reduction or multiplicative reduction at v. Therefore, it is enough to prove Proposition 8.3 for the multiplicative reduction case. We need the following result from Fourier analysis for the proof of Proposition 8.3 (see [8] or [38, Excercise 6.11(b)]).

Lemma 8.4. *Let $t_1, \ldots, t_N \in \mathbb{R}$ and $B_2(t) = (t-[t])^2 - (t-[t]) + \frac{1}{6}$ be the periodic extension of second Bernoulli polynomial on the interval $[0,1]$. Then,*

$$\sum_{\substack{1\leq i,j\leq N \\ i\neq j}} B_2(t_i - t_j) \geq -\frac{N}{6}.$$

Proof. The Fourier expansion of $B_2(t)$ is given by

$$B_2(t) = \frac{1}{2\pi^2}\sum_{n\in\mathbb{Z},n\neq 0}\frac{e^{2\pi i n t}}{n^2}.$$

Therefore,

$$\begin{aligned}\sum_{\substack{1\le i,j\le N\\ i\neq j}} B_2(t_i-t_j) &= \frac{1}{2\pi^2}\sum_{n\in\mathbb{Z},n\neq 0}\frac{1}{n^2}\sum_{\substack{1\le i,j\le N\\ i\neq j}} e^{2\pi i n(t_i-t_j)}\\ &= \frac{1}{2\pi^2}\sum_{n\in\mathbb{Z},n\neq 0}\frac{1}{n^2}\left(\left|\sum_{1\le i,j\le N} e^{2\pi i n t_i}\right|^2 - N\right)\\ &\ge -\frac{N}{12}.\end{aligned}$$

□

Proof of Proposition 8.3. Since E/K_v has multiplicative reduction, by (20),

$$\sum_{\substack{1\le i,\,j\le N\\ i\neq j}} \lambda_v(P_i-P_j) = \frac{v(\Delta)}{2}\sum_{\substack{1\le i,\,j\le N\\ i\neq j}} B_2(\alpha(P_i-P_j)).$$

Applying Lemma 8.4, we have the proposition. □

9. **Proof of Theorem 7.2**

Let E/K be an elliptic curve over a number field K and $\mathcal{L}=\bigcup_i L_i$ be an asymptotically positive tower over K. Let $L\subseteq\mathcal{L}$ be a finite extension of K. For a finite set $Z=\{P_1,P_2,\dots,P_N\}\subseteq E(L)$, define

$$\widehat{h}(Z) = \frac{1}{|Z|}\sum_{P\in Z}\widehat{h}(P)$$

to be the average of canonical heights. Using the parallelogram property of canonical height, we obtain

$$\begin{aligned}\widehat{h}(Z) &\ge \frac{1}{4N(N-1)}\sum_{\substack{1\le i,\,j\le N\\ i\neq j}}\widehat{h}(P_i-P_j)\\ &\ge \frac{1}{4N(N-1)}\sum_{v\in M_L}\frac{[L_v:\mathbb{Q}_v]}{[L:\mathbb{Q}]}\sum_{\substack{1\le i,\,j\le N\\ i\neq j}}\lambda_v(P_i-P_j).\end{aligned}\tag{23}$$

Now we begin the proof of Theorem 7.2. Throughout the proof, we assume that E/L has either good or split multiplicative reduction at any non-archimedean place $v\in M_L$. If not, this can be ensured by a finite base change. The proof consists of three parts: obtaining lower bound of the contribution in (23) due to archimedean places, places of good reduction, and places of split multiplicative reduction. The lower bound for the split multiplicative case is inspired by [7, Theorem 20].

Proof of Theorem 7.2. For an archimedean place $v\in M_L^\infty$, from (17) we know that

$$\sum_{\substack{1\le i,\,j\le N\\ i\neq j}}\lambda_v(P_i-P_j)\ge -\frac{1}{2}N\log N - b(E)N.$$

Since $\sum_{v\in M_L^\infty}[L_v:\mathbb{Q}_v]/[L:\mathbb{Q}]=1$, we can write

$$\sum_{v\in M_L^\infty}\frac{[L_v:\mathbb{Q}_v]}{[L:\mathbb{Q}]}\sum_{\substack{1\le i,\,j\le N\\ i\neq j}}\lambda_v(P_i-P_j)\ge -\frac{1}{2}N\log N - b(E)N.\tag{24}$$

Suppose E has good reduction at $v \in M_L \setminus M_L^\infty$, a non-archimedean place lying above the rational prime p. By (21), we have

$$\sum_{\substack{1\le i,j\le N\\ i\neq j}} \lambda_v(P_i - P_j) \ge \frac{1}{2} \sum_{\substack{1\le i,j\le N\\ i\neq j}} \max\left\{ v\left(\frac{x(P_i-P_j)}{y(P_i-P_j)}\right), 0\right\}.$$

Let $\mathbb{F}_q$ be the residue field of $L_v/\mathbb{Q}_p$ and $\widetilde{E}$ be the reduction of E at v. Suppose

$$\widetilde{E}(\mathbb{F}_q) = \{T_1, T_2, \dots, T_m\}.$$

For $1 \le l \le m$, define

$$A_l := |\{ P_i \in Z \,|\, P_i \equiv T_l \pmod{v}\}|.$$

Clearly, $\sum_{i=1}^m A_i = N$. Note that if $P_i \equiv P_j \pmod{v}$, then

$$v\left(\frac{x(P_i-P_j)}{y(P_i-P_j)}\right) \ge \frac{\log p}{e_v},$$

where p is the rational prime dividing v and e_v is ramification index of v. Therefore,

$$\begin{aligned}\sum_{\substack{1\le i,j\le N\\ i\neq j}} \lambda_v(P_i - P_j) &\ge \frac{1}{2}\frac{\log p}{e_v}\left(\sum_{l=1}^m A_l\,(A_l - 1)\right)\\ &\ge \frac{1}{2}\frac{\log p}{e_v}\left(\frac{N^2}{m} - N\right),\end{aligned}$$

where the last step follows from the Cauchy-Schwartz inequality. By Hasse's inequality,

$$m \le q + 1 + 2\sqrt{q}.$$

Hence,

$$\sum_{\substack{1\le i,j\le N\\ i\neq j}} \lambda_v(P_i - P_j) \ge \frac{1}{2[L_v:\mathbb{Q}_p]}\left(\frac{N^2}{q+1+2\sqrt{q}} - N\right)\log q.$$

Therefore,

$$\sum_{v\in M_L}{}' \frac{[L_v:\mathbb{Q}_p]}{[L:\mathbb{Q}]} \sum_{\substack{1\le i,j\le N\\ i\neq j}} \lambda_v(P_i - P_j) \ge \frac{N^2}{2}\sum_q \frac{G_q(L)}{[L:\mathbb{Q}]}\left(\frac{1}{q+1+2\sqrt{q}} - \frac{1}{N}\right)\log q, \tag{25}$$

where $\sum'$ runs over all non-archimedean $v \in M_L$ at which E has good reduction.

Finally, suppose E has split multiplicative reduction at $v \in M_L \setminus M_L^\infty$, a non-archimedean place with norm q. Let $k_v = -\operatorname{ord}_v(j_E) \ge 1$. Recall that the retraction homomorphism $r : E(K_v) \to \mathbb{R}/\mathbb{Z}$ factors as

$$E(K_v) \longrightarrow K_v^\times/q_E^{\mathbb{Z}} \longrightarrow \mathbb{R}/\mathbb{Z},$$

where $q_E \in K_v^\times$ with $|q_E|_v = |1/j_E|_v$. Here the first map is the Tate parametrization and the second map is given by $u \mapsto \frac{\log|u|_v}{\log|q|_v}$. Note that $\mathrm{Im}(r) = \langle 1/k_v\rangle \subseteq \mathbb{R}/\mathbb{Z}$, and therefore $e^{2\pi i n r(P_j)} = 1$ whenever

$k_v \mid n$. Since $P_i \neq P_j$ for $i \neq j$, using Theorem C (ii), we obtain

$$\begin{aligned}
\sum_{\substack{1\le i,\, j\le N\\ i\neq j}} \lambda_v(P_i - P_j) &\geq \frac{1}{2}\, v(q_E) \sum_{\substack{1\le i,\, j\le N\\ i\neq j}} B_2\left(\frac{v(u(P_i)) - v(u(P_j))}{v(q_E)}\right)\\
&\geq \frac{1}{2}\, v(q_E)\left(\frac{1}{2\pi^2}\sum_{n\in\mathbb{Z},\ n\neq 0}\frac{1}{n^2}\sum_{\substack{1\le i,j\le N\\ i\neq j}} e^{2\pi i n\left(\frac{v(u(P_i))-v(u(P_j))}{v(q_E)}\right)}\right)\\
&\geq \frac{1}{4\pi^2}\, v(q_E)\left(N(N-1)\sum_{n\in k_v\mathbb{Z},\ n\neq 0}\frac{1}{n^2} + \sum_{n\in\mathbb{Z}\setminus k_v\mathbb{Z}}\frac{1}{n^2}\sum_{\substack{1\le i,j\le N\\ i\neq j}} e^{2\pi i n\left(\frac{v(u(P_i))-v(u(P_j))}{v(q_E)}\right)}\right)\\
&\geq \frac{1}{4\pi^2}\, v(q_E)\left(N(N-1)\sum_{n\in k_v\mathbb{Z},\ n\neq 0}\frac{1}{n^2} + \sum_{n\in\mathbb{Z}\setminus k_v\mathbb{Z}}\frac{1}{n^2}\left(\left|\sum_{1\le i\le N} e^{2\pi i n\left(\frac{v(u(P_i))}{v(q_E)}\right)}\right|^2 - N\right)\right)\\
&\geq N(N-1)\frac{\log|j_E|_v}{4\pi^2}\sum_{n\in k_v\mathbb{Z}\setminus\{0\}}\frac{1}{n^2} + O(N)
\end{aligned}$$

As $\zeta(2) = \sum_{n\geq 1}\frac{1}{n^2} = \frac{\pi^2}{6}$, we deduce that

$$\begin{aligned}
\sum_{\substack{1\le i,\, j\le N\\ i\neq j}} \lambda_v(P_i - P_j) &\geq N(N-1)\frac{\log|j_E|_v}{12\, {k_v}^2} + O(N)\\
&\geq N(N-1)\frac{\log p}{12\, k_v} + O(N).
\end{aligned}$$

Since j_E is fixed, there exists a constant $c_E > 0$ only dependent on E such that

$$k_v \leq \frac{e_v}{c_E},$$

where e_v is the ramification index of $L_v/\mathbb{Q}_p$. Therefore,

$$\begin{aligned}
\sum_{v\in M_L}{}'' \frac{[L_v:\mathbb{Q}_p]}{[L:\mathbb{Q}]}\sum_{\substack{1\le i,\, j\le N\\ i\neq j}} \lambda_v(P_i - P_j) &\geq \sum_{v\in M_L}{}'' \frac{[L_v:\mathbb{Q}_p]}{[L:\mathbb{Q}]}\left(\frac{\log p}{12\, k_v}N(N-1) + O(N)\right)\\
&\geq c_E \sum_{v\in M_L}{}'' \frac{[L_v:\mathbb{Q}_p]}{[L:\mathbb{Q}]}\left(\frac{\log p}{12\, e_v}N(N-1) + O(N)\right)\\
&\geq c_E\, N(N-1)\sum_q \frac{B_q(L)}{[L:\mathbb{Q}]}\frac{\log q}{12} + O(N), \qquad (26)
\end{aligned}$$

where $\sum''$ runs over all non-archimedean $v \in M_L$ at which E/L has split multiplicative reduction and q runs over all prime powers. Combining (24), (25) and (26) in (23), we obtain

$$\begin{aligned}
\widehat{h}(Z) \geq \frac{1}{4\,N(N-1)}\Bigg(&-\frac{1}{2}N\log N - b(E)N + \frac{N^2}{2}\sum_q \frac{G_q(L)}{[L:\mathbb{Q}]}\left(\frac{1}{q+1+2\sqrt{q}} - \frac{1}{N}\right)\log q\\
&+ N(N-1)\sum_q \frac{B_q(L)}{[L:\mathbb{Q}]}\frac{\log q}{12} + O(N)\Bigg). \qquad (27)
\end{aligned}$$

For any N, the above inequality holds for all possible N-points $\{P_1, P_2, \cdots, P_N\} \subset E(L)$. Considering an infinite sequence $\{P_n\}_{n\geq 1}$ in $E(\mathcal{L})$ such that $\lim \hat{h}(P_n) = \liminf_{P\in E(\mathcal{L})} \hat{h}(P)$. Thus

$\lim \hat{h}(Z_N) = \liminf_{P\in E(\mathcal{L})} \hat{h}(P)$, where $Z_N = \{P_1, P_2, \ldots, P_N\}$. Taking N large, (27) implies that

$$\liminf_{P\in E(\mathcal{L})} \widehat{h}(P) \geq \frac{1}{8}\sum_q \xi_q(\mathcal{L})\,\frac{\log q}{q+1+2\sqrt{q}} + \frac{c_E}{48}\sum_q \chi_q(\mathcal{L})\,\log q$$

as required. □

10. **Concluding remarks**

The notion of relative height as discussed in Section 3 leads to several interesting questions. For instance, one can formulate a stronger Schinzel-Zassenhaus conjecture in this context. In [35], A. Schinzel and H. Zassenhaus proposed a weaker version of Lehmer's conjecture, which was recently resolved by V. Dimitrov [12]. Let $\left|\alpha\right|$ denote the house of $\alpha \in \overline{\mathbb{Q}}$ defined as

$$\left|\alpha\right| = \max_i\{|\alpha_i|\},$$

where α_i's are the conjugates of α. Then Dimitrov's theorem states that for any non-zero $\alpha \in \overline{\mathbb{Q}}$ not a root of unity,

$$\log\left|\alpha\right| > \frac{c}{[\mathbb{Q}(\alpha):\mathbb{Q}]}$$

for $c = (\log 2)/4$. In the context of relative heights, it is possible to formulate a generalization of this conjecture in the following way. Let m be a fixed positive integer. For any algebraic integer $\alpha \in \overline{\mathbb{Q}}$ define

$$\left|\alpha\right|_m := \max_{\substack{[\mathbb{Q}(\alpha):K]\leq m \\ \sigma:K\hookrightarrow\mathbb{C}}} M_{\sigma(K)}(\alpha).$$

When $m = 1$, it is clear that $\left|\alpha\right|_1 = \left|\alpha\right|$. Thus, it is reasonable to make the following conjecture, in the spirit of Dimitrov's theorem.

Conjecture 10.1. *Let m be a fixed positive integer. For all non-zero algebraic integer $\alpha \in \overline{\mathbb{Q}}$, which are not roots of unity,*

$$\log\left|\alpha\right|_m > \frac{c}{[\mathbb{Q}(\alpha):\mathbb{Q}]},$$

for an absolute constant $c > 0$.

References

[1] F. Amoroso, S. David and U. Zannier, *On fields with 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 **80** (2000), 260-272.

[3] F. Amoroso and M. Mignotte, *On the distribution of the roots of polynomials*, Ann. Inst. Fourier (Grenoble) **46** (1996), 1275-1291.

[4] F. Amoroso and U. Zannier, *A relative Dobrowolski lower bound over abelian extensions*, Ann. Sc. Norm. Super. Pisa Cl. Sci. **29** (2000), 711–727.

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

[6] M. Baker, *Lower bounds for the canonical height on elliptic curve over abelian extensions*, Int. Math. Res. Not. IMRN **29** (2003), 1571-1582.

[7] M. Baker and C. Petsche, *Global discrepancy and small points on elliptic curves*, Int. Math. Res. Not. IMRN **61** (2005), 3791-3834.

[8] P. E. Blanksby and H. L. Montgomery, *Algebraic integers near the unit circle*, Acta Arith. **18** (1971), 355-369.

[9] Y. Bilu, *Limit distribution of small points on algebraic tori*, Duke Math. J. **89** (1997), 465-476.

[10] E. Bombieri and U. Zannier, *A note on heights in certain infinite extensions of* $\mathbb{Q}$, Atti. Acad. Naz. Lincei Cl. Sci. Mat. Fis. Natur. Rend. Lincei (9) Mat. Appl. **12** (2001), 5-14.

[11] S. Checcoli and A. Fehm, *On the Northcott property and local degrees*, Proc. Amer. Math. Soc. **149** (2021), 2403–2414.
[12] V. Dimitrov, *A proof of the Schinzel-Zassenhaus conjecture on polynomials*, arXiv:1912.12545 (2019).
[13] A. B. Dixit and S. Kala, *Lower bound on height of algebraic numbers and low lying zeros of the Dedekind zeta-function*, arXiv:2309.15872 (2023).
[14] G. Faltings, *Calculus on arithmetic surfaces*, Ann. of Math. (2) **119** (1984), 387-424.
[15] P. Fili and Z. Miner, *Equidistribution and the heights of totally real and totally p-adic numbers*, Acta Arith. **170** (2015), 15–25.
[16] P. Fili and C. Petsche, *Energy integrals over local fields and global height bounds*, Int. Math. Res. Not. IMRN **5** (2015), 1278–1294.
[17] P. Fili and I. Pritsker, *Height bounds for algebraic numbers satisfying splitting conditions*, J. Number Theory **175** (2017), 250-264.
[18] P. Habegger, *Small height and infinite nonabelian extensions*, Duke Math. J. **162** (2013), 2027–2076.
[19] M. Hindry and J. H. Silverman, *On Lehmer's conjecture for elliptic curves*, In: "Séminaire de Théorie des Nombres, Paris (1988-1989)", Progr. Math. **91** (1990), Birkhäuser Boston, Boston, MA, 103-116.
[20] P. Hriljac, Splitting fields of principal homogeneous spaces, *Lecture Notes in Math.* **1240** (1987), Springer-Verlag, Berlin, 214-229.
[21] L. Kronecker, *Zwei Sätze über Gleichungen mit Ganzzahligen Coefficienten*, J. Reine Angew. Math. **53** (1857), 173–175.
[22] S. Lang, *Elliptic Curves : Diophantine Analysis*, Grundlehren der Mathematischen Wissenschaften **231**, Springer-Verlag, Berlin (1978).
[23] S. Lang, *Introduction to Arakelov theory*, Springer-Verlag, New York (1988).
[24] M. Laurent, *Minoration de la hauteur de Néron–Tate*, In : "Séminaire de théorie des nombres de Paris (1981-1982)", Progr. Math. **38** (1983), Birkhäuser, Boston-Basel-Stuttgart, 137-151.
[25] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. (2) **34** (1933), 461–479.
[26] K. Mahler, *An inequality for the discriminant of a polynomial*, Michigan Math. J. **11** (1964), 257-262.
[27] D. Masser, *Auxiliary polynomials in number theory*, Cambridge Tracts in Math. **207** (2016), Cambridge University Press, Cambridge.
[28] D. Masser, *Counting points of small height on elliptic curves*, Bull. Soc. Math. France **117** (1989), 247-265.
[29] M. Mignotte, *Entiers Alǵebriques dont les Conjugúes sont Proches du Cercle Unité*, In : "Séminaire Delange-Pisot-Poitou, 19e année: 1977/78", Théorie des Nombres, Fasc. 2, Exp. No. **39** (1978), Paris, 1-6.
[30] A. Néron, *Quasi-fonctions et Hauteurs sur les Variétés Abéliennes*, Ann. of Math. (2) **82** (1965), 249–331.
[31] J. Neukirch, *Algebraic number theory*, Springer-Verlag, Berlin (1999).
[32] D. G. Northcott, *An inequality on the theory of arithmetic on algebraic varieties*, Proc. Cambridge Philos. Soc. **45** (1949), 502-509.
[33] L. Pottmeyer, *Small totally p-adic algebraic numbers*, Int. J. Number theory **14** (2018), 2687-2697.
[34] A. Schinzel, *On the product of the conjugates outside the unit circle of an algebraic number*, Acta Arith. **24** (1973), 385-399.
[35] A. Schinzel and H. Zassenhaus, *A refinement of two theorems of Kronecker*, Michigan Math. J. **12** (1965), 81-85.
[36] J. H. Silverman, *Lower bound for the canonical height on elliptic curves*, Duke Math. J. **48** (1981), 633–648.
[37] J. H. Silverman, *Lower bounds for height functions*, Duke Math. J. **51** (1984), 395-403.
[38] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts in Math., Springer, **151** (1994).
[39] J. H. Silverman, *The arithmetic of elliptic curves*, Grad. Texts in Math., Springer, **106** (1986).
[40] J. H. Silverman, *A lower bound for the canonical height on elliptic curves over abelian extensions*, J. Number Theory **104** (2004), 353-372.
[41] C. J. Smyth, *The Mahler Measure of Algebraic Numbers: A Survey*, Number Theory and Polynomials, London Math. Soc. Lecture Note Ser. **352** (2008), Cambridge Univ. Press, 322–349.
[42] M. A. Tsfasman and S. G. Vlăduţ, *Infinite global fields and the generalized Brauer-Siegel theorem*, Mosc. Math. J. **2** (2002), 329-402.
[43] J. Verger-Gaugry, *A Survey on the Conjecture of Lehmer and the Conjecture of Schinzel-Zassenhaus*, HAL-02315014 (2019).
[44] S. Zhang, *Equidistribution of small points on abelian varieties*, Ann. of Math. (2) **147** (1998), 159-165.

Institute of Mathematical Sciences (A CI of Homi Bhabha National Institute), CIT Campus, IV Cross Road, Chennai, India-600113

Email address: anupdixit@imsc.res.in

Institute of Mathematical Sciences (A CI of Homi Bhabha National Institute), CIT Campus, IV Cross Road, Chennai, India-600113

Email address: sushant@imsc.res.in