

Lower bound on height functions

By

Sushant

MATH10202104006

The Institute of Mathematical Sciences, Chennai

A thesis submitted to the

Board of Studies in Mathematical Sciences

In partial fulfillment of requirements

for the Degree of

DOCTOR OF PHILOSOPHY

of

HOMI BHABHA NATIONAL INSTITUTE



July, 2026

Homi Bhabha National Institute

Recommendations of the Viva Voce Committee

As members of the Viva Voce Committee, we certify that we have read the dissertation prepared by Sushant entitled “Lower bound on height functions” and recommend that it may be accepted as fulfilling the thesis requirement for the award of Degree of Doctor of Philosophy.



Chairman - Sanoli Gun

Date: July 24, 2026



Guide/Convenor - Anup B. Dixit

Date: July 24, 2026



Examiner - Narasimha Kumar

Date: July 24, 2026



Member 1 - Amritanshu Prasad

Date: July 24, 2026



Member 2 - Anirban Mukhopadhyay

Date: July 24, 2026



Member 3 - Purusottam Rath

Date: July 24, 2026

Final approval and acceptance of this thesis is contingent upon the candidate's submission of the final copies of the thesis to HBNI.

I hereby certify that I have read this thesis prepared under my direction and recommend that it may be accepted as fulfilling the thesis requirement.

Date: July 24, 2026

Place: Chennai

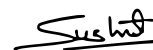


Anup B. Dixit (Guide)

CERTIFICATION ON ACADEMIC INTEGRITY

1. I, Sushant, HBNI Enrolment Number: MATH10202104006, hereby undertake that the thesis, titled “Lower bound on height functions” is prepared by me and is the original work undertaken by me.
2. I also hereby undertake that this document has been duly checked through a plagiarism detection tool and the document is found to be plagiarism free as per the guidelines of the Institute/UGC.
3. I am aware and undertake that if plagiarism is detected in my thesis at any stage in the future, suitable penalty will be imposed as per the guidelines of the Institute/UGC.

Date : July 24, 2026



Sushant

Endorsement by the thesis supervisor

I certify that the thesis written by the researcher is plagiarism free as mentioned above by the student.

Date : July 24, 2026



Anup B. Dixit

Reader F

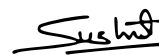
Mathematical Sciences

IMSc, Chennai

STATEMENT BY AUTHOR

This dissertation has been submitted in partial fulfillment of requirements for an advanced degree at Homi Bhabha National Institute (HBNI) and is deposited in the Library to be made available to borrowers under rules of the HBNI.

Brief quotations from this dissertation are allowable without special permission, provided that accurate acknowledgement of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the Competent Authority of HBNI when in his or her judgement the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

A handwritten signature in black ink, appearing to read 'Sushant', with a horizontal line drawn underneath it.

Sushant

DECLARATION

I hereby declare that the investigation presented in the thesis has been carried out by me. The work is original and has not been submitted earlier as a whole or in part for a degree / diploma at this or any other Institution / University.

A handwritten signature in black ink, appearing to read 'Sushant', with a horizontal line underneath it.

Sushant

List of publications arising from this thesis

Journal

1. On the height of the lowest zero of the Dedekind Zeta function, *Bulletin of the Australian Mathematical Society*, Vol. **111**, Issue 3, pp. 460 - 468, 2025.
2. A p -adic criterion for Lehmer's conjecture (with A. B. Dixit), *International Journal of Number Theory*, <https://doi.org/10.1142/S1793042126500855>, 2026.
3. On points of small height in infinite extensions (with A. B. Dixit), *Annali della Scuola Normale Superiore di Pisa*, <https://doi.org/10.2422/2036-2145.202511.008>, 2026.

Conferences

1. Lower bound on height functions, to appear in Proceedings of the International Conference on Lie Algebra and Number Theory (ICLANT - 2024), *Springer Proceedings in Mathematics & Statistics*.

Submitted

1. Lower bound on heights of algebraic numbers and low lying zeros of Dedekind zeta function (with A. B. Dixit), [arXiv:2309.15872](https://arxiv.org/abs/2309.15872), submitted.

Sushant

Other publications (not included in this thesis)

1. An estimate for incomplete mixed character sums and applications (D. Basnet, G. Kapetanakis, A. Mazumder), *Finite Fields and Their Applications*, Vol. **117**, 2027
2. On the distribution of shapes of pure quartic number fields (with S. Das, A. Mukhopadhyay, A. Ray), [arXiv:2506.23766](#), submitted.
3. Lower bound on Néron–Tate height of Abelian varieties, [arXiv:2511.17933](#), submitted.

Sushant

To my family,

for their endless love and countless sacrifices.

ACKNOWLEDGEMENTS

I would like to begin by expressing my deepest gratitude to my advisor, Dr. Anup Dixit, for his invaluable guidance from the very first day I joined him. Without his guidance, this research would not have been possible. I am especially thankful to him for his unwavering support and for constantly encouraging me to challenge myself and grow as a researcher. I am deeply indebted to Dr. Siddhi Pathak for her invaluable guidance and advice over the years. Her feedback on my talks and mathematical writing has greatly helped me develop these skills. Dr. Anup and Dr. Siddhi supported me through tough times by always motivating and uplifting me. Their support means more to me than I can express.

I am extremely grateful to Prof. Sinnou David for his availability and constant support over the last few years. He has greatly helped me in learning some of the geometric techniques used in my research and has always encouraged me. I am also grateful to him for offering courses on elliptic curves and algebraic curves at CMI and IMSc. I would also like to express my sincere gratitude to Dr. Anwesh Ray for his course on Arithmetic Dynamics at CMI, for the opportunity to work with him, and for the many mathematical discussions.

I also thank my doctoral committee members Prof. Amritanshu Prasad, Prof. Anirban Mukhopadhyay, Prof. Purusottam Rath and Prof. Sanoli Gun for their encouragement and insightful comments.

I would like to express my sincere thanks to Prof. Arno Fehm and Prof. Narasimha Kumar for carefully reading this thesis and for their comments and valuable suggestions, which have significantly improved its quality and clarity.

I am extremely grateful to Prof. Martin Widmer for hosting me at TU Graz

and for the many valuable discussions we had, both in person and remotely. I truly appreciate his kindness and support. I also want to thank Dr. Lukas Pottmeyer for his availability for discussion at Universität Duisburg–Essen, despite his busy teaching schedule. I am grateful to Prof. Aurélien Galateau for hosting me at the University of Cergy and for the many valuable discussions we had. I would also like to thank Dr. Arnaud Plessis for the countless email conversations regarding my queries and his valuable comments on some of my work. I am grateful to CNRS ReLaX Lab for providing travel support for my visit to Cergy, and especially to Prof. Pascal Weil and Prof. Sinnou David for their generous support and assistance throughout the process. I would also like to thank Prof. Michel Waldschmidt, Prof. Kumar Murty, Prof. Umberto Zannier, Prof. Ram Murty, Prof. Sara Checcoli and Prof. Arno Fehm for their valuable suggestions and encouragement.

I really enjoy the courses I took at IMSc and want to thank Prof. Amritanshu Prasad, Prof. Anirban Mukhopadhyay, Dr. Anup Dixit, Dr. Indrava Roy, Prof. Jaya Iyer, Prof. K. N. Raghavan, Prof. R. Balasubramanian, Prof. Sanoli Gun, and Prof. Vijay Kodiyalam for their wonderful teaching. Special thanks to Prof. Sanoli Gun for her guidance in my research methodology course and for organizing numerous number theory programs at IMSc—I truly benefited from them. My thanks also go to Prof. S Sunder and Dr. Rahul Gupta for the encouragement and for always being so friendly and supportive.

The CMI–IMSc Number Theory Seminar broadened my interest immensely and provided an opportunity to present my work. I am thankful to Dr. Anup Dixit and Dr. Siddhi Pathak for organizing it. I also extend my thanks to all the number theory group members from CMI and IMSc—I have learned many things, directly and indirectly, from each one of them.

I would also like to thank IMSc for providing excellent research facilities. I am particularly grateful to all the staff members of IMSc for their kindness and support.

Special thanks are due to R. Indra for her prompt assistance in various matters.

I am indebted to all my teachers, from school through my masters, especially Dr. Tapas Chatterjee, who inspired me to pursue research in number theory. I would also like to thank Prof. Sudhanshu Sekhar and Dr. Saurabh Kumar Singh for the various number theory courses they offered during my short stay at IIT Kanpur and especially, Prof. Sudhanshu Sekhar for his guidance during this period.

This journey would have been much harder without my friends, and I am deeply thankful to Tirtharaj, Suraj, Arunabha, Vishwajeet, Shaunak, Sunil, Rohit, Aritra, Gopal, Manav, and Sourav for their friendship and for making these years of graduate life enjoyable. I would also like to thank my batchmates Abhirup, Aryan, Astrid, Soumyadip, Velmurugan, and Tirtharaj, as well as my seniors Karthick, Manas, Sunil Satish, Tanmoy, Ankur, Rashi, and Neelam. A special mention goes to Dhananjay, Joseph, Aryan, and Astrid for being a source of joy and fun during the initial phase of my PhD. I am also thankful to Arup, Priyotosh, Sarbartha, Prabhat, Divyanshu, Nitin, and Ritesh for the wonderful time we shared. I am also thankful to the postdocs at IMSc, especially Sonam, Sunil and Mrityunjay, as well as many others, for fruitful discussions and help with various academic and non-academic matters. I would like to extend my thanks to my undergraduate friends from H. N. B. Garhwal University and my postgraduate friends from IIT Ropar, who made learning mathematics a shared adventure, and whose encouragement and laughter turned challenges into cherished memories. I am grateful to Dr. Suraj Singh Khurana for his support, advice, and many insightful discussions, especially during my masters. Special thanks to Priyanshu, for her constant encouragement and for being there through every challenge.

I really enjoyed playing tennis at IMSc and I am thankful to Dr. Anup, Dr. Ajit, Dr. Rahul, Prof. Sunder and others for their company. I would also like to thank Rakesh, Hitesh, Vijay, Sashikanta, Vasan, Moovendan, Pritesh, Nikhil, and many

more for all the fun we had on the cricket ground. In the last phase of my PhD, I also had the pleasure of playing table tennis with Gorekh and Sabyasachi, and I thank them for those enjoyable moments.

I owe everything to my family for their unwavering support and encouragement since my childhood. My parents have always supported my decisions throughout my academic journey, and I am deeply grateful for their patience and belief in me. I am especially indebted to my brother, Shubham, who is currently a postdoc at IMSc, for inspiring me to pursue research and for always standing by me and supporting me in every possible way. His presence at IMSc during the final phase of my PhD has been a constant source of positivity. I also thank my sister, brother-in-law, and sister-in-law for their support. Lastly, I would like to thank the little ones at home—Shreeja, Devansh, and Shivansh—who have no idea know what a thesis is, but certainly know how to make me smile.

Finally, my heartfelt thanks go to everyone who supported me along the way—whether through encouragement, advice, or simply being there when it mattered. Your kindness has not gone unnoticed.

Contents

Summary	i
Notations	iii
1 Introduction	v
1.1 Organization of thesis	vii
2 Weil height and Lehmer's conjecture	1
2.1 Introduction	1
2.2 Mahler measure	3
2.3 Height functions	5
2.3.1 Weil height of algebraic numbers	6
2.4 Lehmer's conjecture	8
3 Weil height and low-lying zeros of zeta function	11
3.1 Dedekind Zeta function	13
3.2 Lehmer's conjecture and low-lying zeros	15

3.3	Explicit formula and lower bound on discriminant	17
3.4	Lower bound on height function	22
4	Small height and p-adic distribution	26
4.1	Small height and p -adic equidistribution	27
4.2	A p -adic criterion for Lehmer's conjecture	30
4.3	A non-archimedean equidistribution theorem	36
5	Points of small height and asymptotically positive extensions	41
5.1	Bogomolov and Northcott property	42
5.2	Asymptotically positive extension	44
5.3	Bogomolov property for asymptotically positive extension	50
5.4	Relative Weil height and Mahler's inequality	57
5.5	Improved height bound for asymptotically positive extensions	60
5.6	Applications	63
6	Points of small height on Elliptic curves	66
6.1	Canonical height on elliptic curves	68
6.2	Bogomolov property for elliptic curves	69
6.3	Local heights on elliptic curves	74
6.3.1	Archimedean place	75
6.3.2	Non-archimedean place	76
6.3.3	Explicit formula for local height and Tate map	79

6.4	Lower bound on height for elliptic curves over asymptotically positive	
	extensions	82
6.5	Concluding remarks	86

Summary

In this thesis, we investigate lower bounds for heights in connection with Lehmer's conjecture, establishing new relationships between the Weil height and analytic objects such as the zeros of the Dedekind zeta function. Our results yield a novel criterion for Lehmer's conjecture under the Generalized Riemann Hypothesis. In addition, we prove a p -adic equidistribution theorem for algebraic numbers of small Weil height, thereby verifying Lehmer's conjecture for a broad class of algebraic numbers.

We further study points of small height over infinite algebraic extensions of rationals, in the spirit of the Bogomolov property introduced by Bombieri and Zannier. We formulate a new criterion for the Bogomolov property via the notion of *asymptotically positive extensions*. This criterion not only strengthens earlier results of Bombieri and Zannier but also, in contrast to previously known cases, produces a substantial class of non-Galois extensions satisfying the Bogomolov property. Moreover, we establish the Bogomolov property for points on elliptic curves defined over *asymptotically positive extensions* with respect to the Néron–Tate height.

Notations

In this thesis, we adopt the following standard notations from number theory.

$\mathbb{N}$	:	The set of natural numbers $\{1, 2, 3, \dots\}$
$\mathbb{Z}$	:	The set of integers
$\mathbb{Q}$	:	The field of rational numbers
$\mathbb{R}$	:	The field of real numbers
$\mathbb{C}$	:	The field of complex numbers
$\Re(z)$	:	The real part of $z \in \mathbb{C}$
$\Im(z)$	:	The imaginary part of $z \in \mathbb{C}$
K	:	A number field
n_K	:	The degree of $K/\mathbb{Q}$
d_K	:	The absolute discriminant of K
M_K	:	The set of places of K
M_K^∞	:	The set of infinite places of K
$\overline{\mathbb{Q}}$	:	A fixed algebraic closure of $\mathbb{Q}$
$\overline{K}$	:	The algebraic closure of K inside $\overline{\mathbb{Q}}$
μ_∞	:	The set of all roots of unity in $\overline{\mathbb{Q}}$

In addition to the above list, all other notations are defined at their first use. Furthermore, all algebraic extensions of $\mathbb{Q}$ are assumed to lie inside $\overline{\mathbb{Q}}$.

Chapter 1

Introduction

A classical theme in number theory is the study of integer and rational solutions to polynomial equations. This line of inquiry, stretching from the ancient problems of Diophantus to the monumental proof by Andrew Wiles of Fermat’s last theorem, has been a primary force in shaping the field of modern number theory. Since the last century, Diophantine geometry has emerged as a branch of mathematics that employs geometric tools to study integer or rational solutions to systems of polynomial equations by viewing them as points on algebraic varieties.

Height functions play a central role in Diophantine geometry to provide a meaningful notion of size to number-theoretic objects and serve as an important tool in proving finiteness results and addressing counting problems. A height function measures the arithmetic complexity of the underlying objects (e.g. rational solutions of a polynomial) and induces a total preorder on them. A nice height function should have only finitely many points of bounded height and degree (so that the height can be used for ‘counting’). This finiteness property, established by Northcott for the Weil height on algebraic numbers, is a cornerstone of descent techniques in Diophantine geometry. In the last century, applications of height functions have led to famous results such as the Mordell-Weil theorem (through the method of descent),

Faltings's proof of Mordell's conjecture (by introducing the Faltings height) and it also appears in the statement of the famous Birch and Swinnerton-Dyer conjecture. The Weil height function on algebraic numbers of bounded degree induces a well-founded preorder. A theorem of Kronecker classifies the roots of unity as precisely the algebraic numbers of height zero. In other words, roots of unity are the arithmetically simplest algebraic numbers. This naturally raises the question of studying algebraic numbers of small height beyond roots of unity. The arithmetic of points of small height has a deep geometric significance. For example, Bilu's theorem tells that algebraic numbers of small height become equidistributed on the unit circle. A celebrated conjecture due to Lehmer predicts a non-trivial lower bound on the heights of algebraic numbers in terms of degree. More precisely, it asserts that there exists an absolute constant $c > 0$ such that for all $\alpha \in \overline{\mathbb{Q}}^\times$ that are not roots of unity,

$$h(\alpha) > \frac{c}{[\mathbb{Q}(\alpha) : \mathbb{Q}]},$$

where h denotes the Weil height and $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is the degree of α . This conjecture has been settled in certain special cases, but remains open in general.

In 2001, inspired by the famous Bogomolov conjecture, Bombieri and Zannier introduced the notion of Bogomolov property for subsets of $\overline{\mathbb{Q}}$. More precisely, a subset $S \subseteq \overline{\mathbb{Q}}$ is said to have the **Bogomolov property** (B) if there exists an absolute constant $c > 0$ such that $h(\alpha) > c$ for all $\alpha \in S$ that are not roots of unity. It follows from **Northcott's theorem** that, for a set S to satisfy property (B) non-trivially, it must contain algebraic numbers of arbitrarily large degree. This naturally leads to the following question :

Question. *Given an infinite extension $\mathcal{L}/\mathbb{Q}$, under what conditions $\mathcal{L}$ has property (B)?*

The answer to the above question is known to be affirmative in certain cases, such

as when $\mathcal{L}/\mathbb{Q}$ is totally real (Smyth [65]), when $\mathcal{L}/\mathbb{Q}$ is abelian (Amoroso–Dvornicich [3]) and when $\mathcal{L}/\mathbb{Q}$ is Galois with finite local degree at a prime p (Bombieri–Zannier [12]).

The study of lower bounds for height on subsets of $\overline{\mathbb{Q}}^\times$ can be viewed from a geometric perspective by identifying $\mathbb{Q}^\times$ with the one-dimensional multiplicative algebraic group $\mathbb{G}_m$, which may be realized as $\mathbb{P}^1 \setminus \{0, \infty\}$ or, equivalently, as the affine curve $\{(x, y) \in \mathbb{A}^2 : xy = 1\}$. This viewpoint motivates the investigation of lower bounds for heights of points lying on varieties endowed with additional algebraic structure. The varieties of most natural interest to number theorists in this context are elliptic curves and, more generally, abelian varieties, which are projective algebraic groups with a commutative group law. The natural analogue of the Weil height in this geometric setting is the Néron–Tate height. This leads to the study of Lehmer-type and Bogomolov-type lower bounds for points on these varieties.

This thesis is divided into two principal themes. The first concerns lower bounds for the Weil height of algebraic numbers and their implications towards Lehmer’s conjecture and the Bogomolov property. The second theme focuses on geometric analogues, establishing absolute lower bounds for the Néron–Tate height on elliptic curves over certain infinite extensions.

1.1 Organization of thesis

This thesis is organized as follows.

In Chapter [2] we give a history of Lehmer’s original problem on the Mahler measure. We also review the Weil height, its properties, and its connection to the Mahler measure.

In Chapter [3](#) we establish a connection between the Weil height and the low-lying zeros of Dedekind zeta functions in the context of Lehmer’s conjecture. Classical approaches to lower bounds for heights rely on lower bounds for the discriminants of minimal polynomials. We derive lower bounds for the discriminants of number fields in terms of the low-lying zeros of Dedekind zeta functions and combine these with Mahler’s inequality to obtain lower bounds for heights. As a consequence, we establish Lehmer’s conjecture for a broad class of algebraic numbers, conditional on the Generalized Riemann Hypothesis (GRH). The main result of this chapter is Theorem [3.2.1](#) ([\[18\]](#) Theorem 1.1)]. We also present computational data for algebraic numbers of small degree in the support of Theorem [3.2.1](#).

In Chapter [4](#) we provide an effective lower bound for the Weil height of algebraic numbers satisfying certain local conditions related to non-archimedean places and formulate a non-archimedean analogue of the angular equidistribution of Galois conjugates of algebraic numbers. As a consequence, we obtain Lehmer’s conjecture for algebraic numbers whose sufficiently many conjugates lie in a given local field. The main results of this chapter are Theorem [4.2.1](#) ([\[20\]](#) Theorem 1.3)], Proposition [4.2.2](#) ([\[20\]](#) Proposition 1.4)] and Theorem [4.3.1](#) ([\[20\]](#) Theorem 1.6)].

In Chapter [5](#), we introduce the notion of asymptotically positive infinite extensions of the rationals, inspired by asymptotically exact families of number fields. For these asymptotically positive extensions, we obtain absolute lower bounds on the Weil height, thereby establishing the Bogomolov property for a wide range of infinite non-Galois extensions. We develop the theory of relative Weil height and relative Mahler’s inequality in Section [5.4](#), an essential tool for our result. Our result encompasses the famous theorem of Bombieri and Zannier on the Bogomolov property for totally p -adic extensions of type (e, f) . The main result of this chapter is Theorem [5.3.2](#) ([\[19\]](#) Theorem 1.2)].

In Chapter [6](#), we derive lower bounds for the canonical height of points on an

elliptic curve lying in an asymptotically positive extensions, thereby establishing the Bogomolov property. Our theorem provide a non-Galois framework for an earlier result of M. Baker for totally v -adic extensions of type (e, f) . The main results of this chapter are Theorem [6.2.1](#) ([\[19\]](#) Theorem 7.2]) and Corollary [6.2.3](#) ([\[19\]](#) Corollary 7.4]).

Chapter 2

Weil height and Lehmer's conjecture

2.1 Introduction

A significant part of this thesis revolve around a classical problem posed by D. H. Lehmer [42] in 1933, widely known as Lehmer's problem or Lehmer's conjecture. The origin of Lehmer's problem lies in the study of one of the most fundamental objects in number theory—the prime numbers. In the course of developing a method to generate large primes, Lehmer studied the Pierce numbers. Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial that factors over $\mathbb{C}$ as

$$f(x) = \prod_{i=1}^n (x - \alpha_i).$$

The integers $\Delta_r(f) = \prod_{i=1}^n (\alpha_i^r - 1)$ for $r \geq 1$ are known as the Pierce numbers. Lehmer was interested in the factorization of these numbers in the hope of obtaining a large prime factor of $\Delta_r(f)$ with large absolute value. It is straightforward to see that if any of the α_i is a root of unity, then the sequence $\Delta_r(f)$ has only finitely many

non-zero values and such polynomials are not useful to produce large primes. For non-cyclotomic polynomials f , Lehmer proved that

$$\lim_{r \rightarrow \infty} \frac{|\Delta_{r+1}(f)|}{|\Delta_r(f)|} = \prod_{i=1}^n \max\{|\alpha_i|, 1\},$$

and observed that if the quantity $\prod_{i=1}^n \max\{|\alpha_i|, 1\}$ is small, or equivalently if $|\Delta_r(f)|$ does not grow rapidly, then the sequence of integers $|\Delta_r(f)|$ is likely to have a large prime factor.

For a polynomial f as above, we define

$$M(f) = \prod_{i=1}^n \max\{|\alpha_i|, 1\}.$$

Note that $M(f) > 1$ for all non-cyclotomic polynomial and the smallest value of $M(f)$ Lehmer could found was

$$M(f) = 1.176280821 \dots,$$

for the polynomial $f(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$, known as ‘Lehmer’s polynomial’. Further, he posed the following problem.

Lehmer’s problem (1933): *Among the monic integer polynomials f such that $M(f) > 1$, is it possible to choose polynomials with $M(f)$ arbitrarily close to 1?*

Lehmer’s problem remains open in general but has been settled for certain cases, which we shall see at the end of this chapter. To this date, the polynomial with the smallest $M(f) > 1$ remains the Lehmer’s polynomial. Subsequently, Mahler studied the quantity $M(f)$ in 1962 to investigate the transcendence of numbers, calling it the *measure* of the polynomial f . Later, in 1979, M. Waldschmidt referred to it as the *Mahler measure*.

2.2 Mahler measure

The Mahler measure $M(f)$ of a monic integral polynomial f can also be interpreted as a measure of how far the roots of a polynomial lie from the unit circle. This notion is captured by logarithmic average of a holomorphic function on the unit circle and thus provide a way to define Mahler measure for arbitrary nonzero complex polynomials. Let $f(z) \neq 0$ be a polynomial in $\mathbb{C}[z]$. The **Mahler measure** of f is defined as

$$(2.1) \quad M(f) := \exp \left(\frac{1}{2\pi} \int_0^{2\pi} \log |f(e^{i\theta})| d\theta \right).$$

One of the main advantages of defining the Mahler measure in integral form is that it immediately gives that Mahler measure is multiplicative, i.e., if f and g are complex polynomials, then $M(fg) = M(f)M(g)$.

We now recall the Jensen's formula from complex analysis, which enables us to derive the form of the Mahler measure presented in the previous section. We use the notation D_R for the open disc of radius R centered at the origin in the complex plane, and C_R for its boundary.

Theorem 2.2.1 (Jensen's formula). *Let $\Omega \subseteq \mathbb{C}$ be an open set that contains the closure of a disc D_R and suppose that f is a holomorphic function on Ω such that $f(0) \neq 0$ and f vanishes nowhere on the circle C_R . If $z_1, \dots, z_n$ denote the zeros of f inside the disc (counted with multiplicities), then*

$$\log |f(0)| = \sum_{i=1}^n \log \left(\frac{|z_i|}{R} \right) + \frac{1}{2\pi} \int_0^{2\pi} \log |f(Re^{i\theta})| d\theta.$$

Let $f(z) = a_n z^n + a_{n-1} z^{n-1} + \dots + a_0$ be a complex polynomial such that $a_0 a_n \neq 0$ and $\alpha_1, \alpha_2, \dots, \alpha_n$ be its roots counted with multiplicities. Applying above theorem

to f yields

$$\begin{aligned}
 M(f) &= \exp \left(\int_0^1 \log |f(e^{i2\pi t})| dt \right) = \exp \left(\log |f(0)| - \sum_i \log \min\{1, |\alpha_i|\} \right) \\
 (2.2) \quad &= |a_0| \frac{1}{\prod_i \min\{1, |\alpha_i|\}} = |a_n| \prod_i \max\{1, |\alpha_i|\}.
 \end{aligned}$$

For monic polynomials with integer coefficients, this coincides precisely with the Mahler measure introduced in the previous section. Equation (2.2) provides an explicit description of the Mahler measure of a polynomial in terms of its roots and leading coefficient, which is particularly useful for arithmetic applications. Recall that the minimal polynomial of a non-zero algebraic number over integers is unique up to sign of its leading coefficient. This allow us to define the notion of the Mahler measure of a non-zero algebraic number. The **Mahler measure of a non-zero algebraic number** α is defined as

$$M(\alpha) := M(m_\alpha(x)),$$

where $m_\alpha(x)$ is minimal polynomial of α over integers. It follows from (2.2) that if a_n is the leading coefficient of $m_\alpha(x)$ and $\alpha_1, \alpha_2, \dots, \alpha_n$ are its root, then

$$M(\alpha) = |a_n| \prod_{i=1}^n \max\{1, |\alpha_i|\}.$$

We now state Lehmer's conjecture in terms of Mahler measure of algebraic numbers.

Conjecture 2.2.2 (Lehmer's problem). *There exists an absolute constant $c > 0$ such that for all non-zero algebraic numbers α , not root of unity, we have*

$$\log M(\alpha) > c.$$

In modern terms, Lehmer's conjecture is formulated using height functions. In the

next section, we introduce the notion of the Weil height and see its connection to the Mahler measure.

2.3 Height functions

The Mahler measure provides a notion of size for polynomials with integral coefficients and behaves analogously to a height function, an arithmetic invariant that quantifies the complexity of solutions to Diophantine equations. In addition to the representations given in (2.1) and (2.2), the Mahler measure admits a representation in terms of the Weil height, providing a local description. More precisely, it decomposes as a sum over all places, where each place contributes a local term, thereby expressing the measure as an aggregate of its local contributions.

One of the most basic examples of a height function is the natural height on the set of non-zero rational numbers $\mathbb{Q}^*$. Let $\frac{a}{b} \in \mathbb{Q}^*$ be in its lowest form. Then, the natural height of a/b is defined as

$$h\left(\frac{a}{b}\right) = \log \max\{|a|, |b|\}.$$

For simplicity, the height of zero is defined to be 0. It clearly follows from the definition that:

“There are only finitely many rationals with bounded natural height”.

This is called the finiteness property of height and it is often desirable for a height function to satisfy this property. There is another viewpoint for expressing the quantity $\max\{|a|, |b|\}$ as follows:

$$\log \max\{|a|, |b|\} = \sum_p \log \max\left\{1, \left|\frac{a}{b}\right|_p\right\},$$

where the sum runs over all primes p and $|\cdot|_p$ denotes the p -adic absolute value on $\mathbb{Q}$, defined for $x = p^k \frac{m}{n}$ ($p \nmid mn$) by $|x|_p = p^{-k}$ (and $|0|_p = 0$).

This shift in perspective has led André Weil to generalize the above notion of height to algebraic numbers, known as the Weil height.

2.3.1 Weil height of algebraic numbers

Let K be a number field of degree $[K : \mathbb{Q}] = d$. A *place* v of K is an equivalence class of non-trivial absolute values on K . The set of all places of K is denoted by M_K . For each place $v \in M_K$, we write K_v for the completion of K with respect to v , and $d_v = [K_v : \mathbb{Q}_w]$ for the local degree, where $w \in M_{\mathbb{Q}}$ is the place obtained by restricting v to $\mathbb{Q}$.

It follows from a well known theorem of A. Ostrowski that each place $v \in M_K$ corresponds either to a non-zero prime ideal $\mathfrak{p}_v$ in the ring of integers $\mathcal{O}_K$ of K or to an embedding $\sigma_v : K \hookrightarrow \mathbb{C}$. If v corresponds to a prime ideal, we call v a *finite* (or *non-archimedean*) place, denoted $v \nmid \infty$. If v corresponds to a complex embedding, we call v an *infinite* (or *archimedean*) place, denoted $v \mid \infty$. For each place $v \in M_K$, we choose a representative $|\cdot|_v$ normalized as follows: If v is finite and $\alpha \neq 0$, then

$$|\alpha|_v = N\mathfrak{p}_v^{-\frac{\text{ord}_{\mathfrak{p}_v}(\alpha\mathcal{O}_K)}{d_v}},$$

where $N\mathfrak{p}_v$ is the norm of $\mathfrak{p}_v$ from K to $\mathbb{Q}$, and $\text{ord}_{\mathfrak{p}_v}(\alpha\mathcal{O}_K)$ is the exponent of $\mathfrak{p}_v$ in the prime ideal factorization of the fractional ideal $\alpha\mathcal{O}_K$. Moreover, we set $|0|_v = 0$. If v is infinite, then

$$|\alpha|_v = |\sigma_v(\alpha)|.$$

The *logarithmic Weil height*, also called the *absolute height* or simply the *Weil*

height, of a non-zero $\alpha \in K$ is defined as

$$h(\alpha) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} \log \max\{1, |\alpha_v|\}.$$

It is clear from the definition of $|\cdot|_v$ that for any $\alpha \in K^*$, the equality $|\alpha|_v \neq 1$ holds for only finitely many places $v \in M_K$. Hence, all but finitely many terms in the above summation vanish. The factor $\frac{1}{[K:\mathbb{Q}]}$ in the definition of $h(\alpha)$ ensures that the definition of $h(\alpha)$ is independent of the number field K . Thus, $h(\cdot)$ defines a well-defined function on $\overline{\mathbb{Q}}^*$ and called *absolute Weil height*.

The Weil height on algebraic numbers satisfies various interesting properties.

Proposition 2.3.1. *For all $\alpha, \beta \in \overline{\mathbb{Q}}^*$ and $n \in \mathbb{Z}$, the Weil height h is a non-negative function satisfying*

$$(i) \quad h(\alpha\beta) \leq h(\alpha) + h(\beta),$$

$$(ii) \quad h(\alpha + \beta) \leq \log 2 + h(\alpha) + h(\beta),$$

$$(iii) \quad h(\alpha^n) = |n| h(\alpha),$$

$$(iv) \quad h(\sigma(\alpha)) = h(\alpha) \text{ for all } \sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).$$

Proof. See [45] Chapter 14]. □

Moreover, the following theorem due to Kronecker [38] completely classifies algebraic numbers of smallest height.

Theorem 2.3.2 (Kronecker). *$h(\alpha) = 0$ if and only if α is a root of unity.*

One the most important feature of the Weil height function gives a well-founded preorder on the set of algebraic number with bounded degree and was first observed by D. G. Northcott [50].

Theorem 2.3.3 (Northcott). *There are only finitely many algebraic numbers α with bounded degree and bounded height.*

The original motivation for Northcott to study heights and related finiteness properties was applications to algebraic dynamics. Northcott's theorem has been used extensively, especially to deduce finiteness results in Diophantine geometry and arithmetic dynamics.

2.4 Lehmer's conjecture

The Weil height is a non-negative function defined on the set of non-zero algebraic numbers which takes the value zero precisely at the roots of unity (Kronecker's theorem). A natural question, therefore, is to identify the algebraic numbers of small positive height next to the roots of unity. The example $h(2^{1/n}) = \log 2/n$ shows that there exist algebraic numbers of arbitrarily small height, with precise growth controlled by the degree. This motivates studying how the height grows with respect to degree. Although determining the precise order of growth is often difficult, lower bounds themselves are of significant interest. The formulation of Lehmer's conjecture in terms of the Weil height connects the study of lower bounds on height by predicting the precise lower bound for the height of algebraic numbers in terms of their degree.

Let K be a number field and $\alpha \in K^*$ with minimal polynomial $m_\alpha(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$. The following proposition is useful in expressing Mahler measure entirely in terms of valuations.

Proposition 2.4.1. *Let α , K , and m_α be as above. Suppose $\alpha_1, \alpha_2, \dots, \alpha_n$ are the*

complex roots of m_α . Then

$$|a_n|^{[K:\mathbb{Q}(\alpha)]} = \prod_{v \in M_K \setminus M_K^\infty} \max \{1, |\alpha|_v\}, \quad \prod_{i=1}^d \max \{1, |\alpha_i|\}^{[K:\mathbb{Q}(\alpha)]} = \prod_{v \in M_K^\infty} \max \{1, |\alpha|_v\},$$

where M_K^∞ denotes the set of archimedean places of K .

Proof. See [45] Proposition 14.4]. □

As a consequence of the above proposition, the Weil height of α is related to the Mahler measure of α by the relation

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

This allows us to formulate Lehmer's conjecture in terms of the Weil height as follows.

Conjecture 2.4.2. (*Lehmer's problem*) *There exists an absolute constant $c > 0$ such that if $\alpha \in \overline{\mathbb{Q}}$ is not a root of unity, then*

$$(2.3) \quad h(\alpha) \geq \frac{c}{[\mathbb{Q}(\alpha) : \mathbb{Q}]}.$$

As mentioned in the beginning of this chapter, the conjecture remains open but significant progress has been made in recent times. Using a sharpened version of Siegel's lemma and thereby constructing an auxiliary polynomial with small coefficients, E. Dobrowolski [21] proved that for $\alpha \in \overline{\mathbb{Q}}^*$ not a root of unity,

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

where $n = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ and $c > 0$ is an absolute constant. Subsequently, this constant c has been improved in the works of U. Rausch [56] and P. Voutier [71]. We call $\alpha \in \overline{\mathbb{Q}}$ reciprocal if α and $1/\alpha$ are conjugates. In 1971, C. Smyth [65] showed that Lehmer's

conjecture holds for all non-reciprocal algebraic numbers. This result, with a weaker constant, was also obtained by R. Breusch [13] in 1951. On another front, consider $\alpha \in \overline{\mathbb{Q}}$, not a root of unity, such that the Galois closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$, say K_α , has degree $[K_\alpha : \mathbb{Q}]$ polynomially bounded in terms of $n = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ (i.e., $[K_\alpha : \mathbb{Q}] = O(n^k)$ for some fixed $k \in \mathbb{N}$). For all such α , F. Amoroso and S. David [1] proved that Lehmer's conjecture holds. Consequently, Lehmer's conjecture holds for all α such that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a Galois extension.

A weaker version of Lehmer's conjecture was proposed by A. Schinzel and H. Zassenhaus [58], which was recently resolved by V. Dimitrov [16]. Let $\boxed{\alpha}$ denote the house of $\alpha \in \overline{\mathbb{Q}}$ defined as

$$\boxed{\alpha} = \max_i \{|\alpha_i|\},$$

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,

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

for $c = (\log 2)/4$. It is easily seen that Lehmer's conjecture implies Dimitrov's theorem, albeit for a different constant $c > 0$.

The reader may refer to the excellent survey articles [66] and [70] for a comprehensive account of Lehmer's problem.

Chapter 3

Weil height and low-lying zeros of zeta function

Classically, two main approaches have been used to obtain lower bounds for the Weil height. The first relies on the metric properties of absolute values and analyzes the local factors explicitly that appear in the definition of the Weil height. The second approach, introduced by K. Mahler, is based on deriving lower bounds for the discriminant of a polynomial. In 1964, K. Mahler [43] proved the following inequality, which since then has played a key role in proving Lehmer's conjecture for certain classes of algebraic numbers and even obtaining stronger lower bounds on the Weil height.

Theorem 3.0.1 (Mahler). *Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ be a polynomial with roots $\alpha_1, \alpha_2, \dots, \alpha_n$. 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 .

Proof. Expressing the discriminant of f in terms of the Vandermonde determinant

and using the Hadamard's inequality, we obtain

$$\begin{aligned} |D| &\leq |a_n|^{2n-2} \prod_{i=1}^n \left(\sum_{j=0}^{n-1} |\alpha_i^j|^2 \right) \\ &\leq |a_n|^{2n-2} \prod_{i=1}^n n \max\{1, |\alpha_i|\}^{2n-2} \leq n^n \cdot M(f)^{2n-2}. \end{aligned}$$

□

This simple-looking inequality due to Mahler turns out to be a powerful tool in deriving lower bounds on height of an algebraic number by studying the discriminant of its minimal polynomial. In a seminal paper, E. Bombieri and U. Zannier [12] used Mahler's inequality together with valuation theory to obtain absolute lower bounds on the Weil height for totally p -adic extensions of rationals. We shall discuss their results in detail in Chapter 5.

It follows from the definition of the Mahler measure that for any algebraic non-integer α , one has $M(\alpha) \geq 2$. Thus, Lehmer's conjecture holds for all algebraic non-integers. For an algebraic integer, a standard fact from algebraic number theory tells that the discriminant of its minimal polynomial and the field discriminant differ only by the index. Let α be a nonzero algebraic integer and set $K = \mathbb{Q}(\alpha)$. Let $I(\alpha) := [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ denote the index of α , let $d(\alpha)$ denote the discriminant of the minimal polynomial of α , and let d_K denote the absolute discriminant $|\text{disc}(K/\mathbb{Q})|$ of the number field K . It is well known that

$$d(\alpha) = I(\alpha)^2 d_K.$$

This relation reduces the initial problem of studying polynomial discriminant to the discriminant of number fields. For an algebraic integer α , if $K = \mathbb{Q}(\alpha)$, applying

Theorem [3.0.1](#) along with above relation, we obtain

$$2h(\alpha) \geq \frac{\log d_K}{n_K^2} - \frac{\log n_K}{n_K} + \frac{2 \log I_K}{n_K^2}.$$

As a consequence, in a family of number fields $\{K_i = \mathbb{Q}(\alpha_i)\}$ with α_i algebraic integers, if $\log d_{K_i} \geq n_{K_i} \log n_{K_i} + \epsilon n_{K_i}$, then Lehmer's conjecture holds for $\bigcup_i \{\alpha_i\}$. The classical analytic formulae suggest that the growth of the discriminant of a number field is largely governed by the splitting behavior of primes and the distribution of low-lying zeros of the associated zeta functions. In fact, in the result of Bombieri and Zannier, the totally p -adic condition can be interpreted as a situation in which prime splitting largely governs the growth of the discriminant. With this motivation, we obtain the lower bound on the height in terms of other field invariants, in particular, the low lying zeros of the Dedekind zeta function of number fields. In the next section we give a brief introduction to the Dedekind zeta function and its properties.

3.1 Dedekind Zeta function

The Dedekind zeta function associated to a number field K is defined on the half-plane $\Re(s) > 1$ as the product

$$\zeta_K(s) := \prod_{\mathfrak{p} \neq 0} \left(1 - \frac{1}{(N\mathfrak{p})^s} \right)^{-1},$$

where $\mathfrak{p}$ runs over all non-zero prime ideals of the ring of integers $\mathcal{O}_K$, and $N\mathfrak{p}$ denotes the absolute norm of $\mathfrak{p}$. The unique factorization of ideals implies that in the half-plane $\Re(s) > 1$, $\zeta_K(s)$ has a Dirichlet series expansion

$$\zeta_K(s) = \sum_{0 \neq \mathfrak{a} \subseteq \mathcal{O}_K} \frac{1}{(N\mathfrak{a})^s},$$

where the sum runs over all non-zero ideals $\mathfrak{a}$ of $\mathcal{O}_K$.

When $K = \mathbb{Q}$, one recovers $\zeta_K(s) = \zeta(s)$, thus Dedekind zeta functions generalize the Riemann zeta function. These functions first appeared in the work of R. Dedekind, and later named after him by E. Hecke. Hecke was the first to observe that $\zeta_K(s)$ admits an analytic continuation to the complex plane, except for a simple pole at $s = 1$ and satisfies a functional equation [47, Chapter 7, Theorem 7.2]

$$\zeta_K(s) = d_K^{\frac{1}{2}-s} \pi^{\frac{r_1}{2}(2s-1)} (2\pi)^{r_2(2s-1)} \frac{\Gamma\left(\frac{1-s}{2}\right)^{r_1} \Gamma(1-s)^{r_2}}{\Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma(s)^{r_2}} \zeta_K(1-s),$$

where $\Gamma(s)$ denotes the Gamma function, and r_1 and r_2 are the numbers of real embeddings and pairs of complex embeddings of the number field K , respectively. Moreover, the residue at $s = 1$ encodes important algebraic invariants of K , and is known as the analytic class number formula.

There is an analogue of the famous Riemann Hypothesis for $\zeta_K(s)$, known as the Generalized Riemann Hypothesis (GRH) (see [35, Section 5.7]).

Conjecture 3.1.1. (*Generalized Riemann Hypothesis*) *If $\zeta_K(s) = 0$ for $0 < \operatorname{Re}(s) < 1$, then $\Re(s) = 1/2$.*

The discriminant of a number field K is one of the most fundamental arithmetic invariants attached to it, and determines which rational primes are ramified in K . It also appears in several important analytic formulae, such as the functional equation of the Dedekind zeta function of K and the analytic class number formula. A theorem of C. Hermite tells that there are only finitely many number fields with bounded discriminant. Thus, the discriminant serves as a height function on the set of number fields and provides a framework for studying various distribution problems.

Discriminant bounds have numerous applications in both algebraic and analytic number theory, and there has been substantial work in this direction. Let K be

a number field of degree $n = r_1 + 2r_2$, where r_1 and r_2 denote the numbers of real embeddings and complex embeddings (up to conjugation) of K , respectively. Denote by d_K the absolute discriminant of K . During the late nineteenth century, in the course of developing a geometric approach to number-theoretic problems, H. Minkowski proved that

$$d_K^{1/2} \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^{r_2} \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^{n/2}.$$

An immediate consequence of Minkowski's bound is that if $K \neq \mathbb{Q}$, then $d_K > 1$. As a result, it follows that the only number field unramified at every rational prime is $\mathbb{Q}$. Moreover, this bound implies that $d_K \rightarrow \infty$ as $n \rightarrow \infty$. Hence, Minkowski's bound implies Hermite's finiteness theorem.

In 1974, H. Stark [67] introduced an analytic method to obtain lower bounds on discriminants by proving a variant of the explicit formula for $\log d_K$. His method provide a substantial improvement over Minkowski's bound. Later, using the explicit formula due to A. Guinand and A. Weil [51], improved lower bounds for discriminant were obtained by A. Odlyzko and G. Poitou. Interested readers may refer to the excellent survey article by Odlyzko [51] on lower bounds for discriminants and their connections with regulators, class numbers, and zeros of the Dedekind zeta function.

3.2 Lehmer's conjecture and low-lying zeros

The zeros of $\zeta_K(s)$ that lie near to the real axis in the critical strip $0 < \Re(s) < 1$ are called *low-lying zeros* of $\zeta_K(s)$. Let $N_K(T)$ denote the number of zeros of $\zeta_K(s)$ in the critical strip with $|\Im(s)| < T$ and define

$$\lambda_K(T) := \sum_{\substack{|t| < T \\ \zeta_K(\sigma+it)=0}} \frac{1}{1+t^2},$$

where t runs over the imaginary part of the non-trivial zeros of $\zeta_K(s)$. The main result [18 Theorem 1.1] of this chapter is as follows.

Theorem 3.2.1. *Let α be a non-zero algebraic integer and $K = \mathbb{Q}(\alpha)$. Under GRH*

$$2n_K h(\alpha) \geq \frac{3.67}{n_K} \left(\lambda_K(2) - \frac{1}{5} N_K(2) \right) - \log n_K + O(1),$$

where the implied constant is absolute.

$m_\alpha(x)$	$3.67 \left(\lambda_K(2) - \frac{1}{5} N_K(2) \right)$	$n_K \left(\log n_K + \frac{1}{1000} \right)$	$N_K(2)$
$x^3 + 2x^2 + 28$	3.72540010277642	3.29883686600433	2
$x^3 + 20x + 20$	4.51802933608664	3.29883686600433	2
$x^4 + 21x^2 + 1$	5.61114340905622	5.54917744447956	4
$x^4 + 28x^2 + 14x + 1$	5.64396152749838	5.54917744447956	4
$x^4 + x + 23$	6.38880039028607	5.54917744447956	4
$x^4 + 91x^2 + 1$	8.78557905852989	5.54917744447956	4
$x^5 + 21x^2 + 1$	9.43790681492255	8.05218956217050	6

Table 3.1: Computational data in support of Theorem 3.2.1

The above theorem implies that for a number field $K = \mathbb{Q}(\alpha)$ generated by an algebraic integer α , if

$$3.67 \left(\lambda_K(2) - \frac{1}{5} N_K(2) \right) \geq n_K \left(\log n_K + \frac{1}{1000} \right),$$

then $h(\alpha) \geq \frac{0.0005}{n_K}$, and hence Lehmer's conjecture holds for such α . Table 3.1, computed using SageMath, provides evidence for the existence of number fields satisfying this hypothesis. The constant $1/1000$ is chosen arbitrarily, and the low-lying zeros term is by no means optimal. A more suitable test function in the explicit formula would yield a sharper estimate.

In the following section, we discuss the explicit formula due to Guinand and Weil, which we shall use to obtain a lower bound on the discriminant in terms of low-lying zeros of the Dedekind zeta function. We provide the proof of Theorem [3.2.1](#) in the last section as a consequence of a more general result (Theorem [3.3.5](#)) that gives a lower bound on discriminant in terms of low-lying zeros of Dedekind zeta function.

3.3 Explicit formula and lower bound on discriminant

In this section, we state and develop the necessary ingredients towards the proof of our results.

Explicit formulae in number theory serve as a bridge between algebraic and analytic number theory. They provide information about arithmetic properties of number fields (such as discriminant bounds and the splitting behavior of primes) in terms of purely analytic objects, such as the zeros of $\zeta_K(s)$, and vice versa. An important role in the proof of Theorem [3.2.1](#) is played by Weil's explicit formula.

Let F be a real valued even function satisfying the following conditions :

- (i) F is continuously differentiable on $\mathbb{R}$ except at a finite number of points a_i where $F(x)$ and its derivative $F'(x)$ has only discontinuities of the first kind for which F satisfies the mean condition, i.e.

$$F(a_i) = \frac{1}{2} (F(a_i + 0) + F(a_i - 0)).$$

- (ii) There exists $b > 0$ such that $F(x)$ and $F'(x)$ are $O(e^{-(1/2+b)|x|})$ in the vicinity of ∞ .

Then, we have the following explicit formula due to Weil (formulated by Poitou [54]).

Theorem 3.3.1 (Weil's explicit formula). *Let $F(x)$ be an even positive function defined on the whole real line $\mathbb{R}$ satisfying (i) and (ii) such that $F(0) = 1$. Define*

$$\phi(s) := \int_{-\infty}^{\infty} F(x) e^{(s-1/2)x} dx.$$

Let K be a number field. Denote by n_K and d_K the degree and absolute discriminant of K over $\mathbb{Q}$. Let r_1 and r_2 denote the number of real and complex embedding (upto conjugation) of K . Then, we have

$$\begin{aligned} \log d_K = & r_1 \frac{\pi}{2} + n_K(\gamma + \log 8\pi) - n_K \int_0^{\infty} \frac{1-F(x)}{2 \sinh x/2} dx - r_1 \int_0^{\infty} \frac{1-F(x)}{2 \cosh x/2} dx \\ & - 4 \int_0^{\infty} F(x) \cosh x/2 dx + \sum_{\rho}' \phi(\rho) + 2 \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} N(\mathfrak{p})^{-m/2} F(m \log N(\mathfrak{p})) \log N(\mathfrak{p}), \end{aligned}$$

where in the first sum ρ runs over all zeros of the Dedekind zeta function $\zeta_K(s)$ in the critical strip, where ρ and $\bar{\rho}$ are grouped together, $\mathfrak{p}$ runs over the prime ideals of K and $N(\mathfrak{p})$ denotes the norm of $\mathfrak{p}$. Here, γ is the Euler–Mascheroni constant.

The above formula establishes a relation between the complex zeros of the Dedekind zeta function, which constitute of analytic data, and the sum over prime powers, which represents arithmetic data. Choosing an appropriate test function $F(x)$ allows us to bound one term while making the other arbitrarily large. We use this observation to prove the following lemma.

Lemma 3.3.2. *Let K be a number field of degree n_K and absolute discriminant d_K . Then under GRH*

$$\log d_K = \left(2 - \frac{\pi}{2}\right) r_1 + (\gamma + \log 8\pi - 2) n_K - \frac{16}{3} + \sum_t \frac{2}{1+t^2} + 2 \sum_q N_K(q) \frac{\log q}{q^{3/2}},$$

where t runs over imaginary parts of non-trivial zeros of $\zeta_K(s)$ and q over all prime

powers.

Proof. Applying the explicit formula in Theorem [3.3.1](#) with $F(x) = e^{-|x|}$, we obtain

$$(3.1) \quad \log d_K = r_1 \frac{\pi}{2} + n_K(\gamma + \log 8\pi) - n_K \int_0^\infty \frac{1 - e^{-|x|}}{2 \sinh x/2} dx - r_1 \int_0^\infty \frac{1 - e^{-|x|}}{2 \cosh x/2} dx \\ - 4 \int_0^\infty e^{-|x|} \cosh x/2 dx + 2 \sum_{\mathfrak{p}} \sum_{m=1}^\infty N(\mathfrak{p})^{-m/2} e^{-|m \log N(\mathfrak{p})|} \log N(\mathfrak{p}) \\ + \sum_{\rho} \phi(\rho),$$

where $\phi(\rho) = \int_{-\infty}^\infty e^{-|x|} \cdot e^{(\rho-1/2)x} dx$

Assuming the GRH, every non-trivial zero ρ of $\zeta_K(s)$ is of the form $1/2 + it$. Therefore

$$\sum_{\rho} \phi(\rho) = \operatorname{Re} \sum_t \int_{-\infty}^\infty e^{itx - |x|} dx,$$

where the sum runs over the imaginary parts t of the non-trivial zeros $\rho = \frac{1}{2} + it$ of $\zeta_K(s)$.

Substituting this into [\(3.1\)](#) and evaluating the integrals gives

$$\log d_K = r_1 \frac{\pi}{2} + n_K(\gamma + \log 8\pi) - 2n_K - (\pi - 2)r_1 - \frac{16}{3} + \sum_t \frac{2}{1+t^2} \\ + 2 \sum_q N_K(q) \sum_{m=1}^\infty \frac{\log q}{q^{m/2}} e^{-m \log q} \\ = \left(2 - \frac{\pi}{2}\right) r_1 + (\gamma + \log 8\pi - 2)n_K - \frac{16}{3} + \sum_t \frac{2}{1+t^2} + 2 \sum_q N_K(q) \frac{\log q}{q^{\frac{3}{2}}}.$$

as required. □

To estimate the sum over the zeros of $\zeta_K(s)$ in the above lemma, we require the following result due to Ehsan Hasanalizade, Qingyu Shen, and P. J. Wong [\[31\]](#), Corollary 1.2], which provides an explicit bound for $N_K(T)$.

Theorem 3.3.3 (Hasanalizade-Shen-Wong). *Let K be a number field and $N_K(T)$ be the number of zeroes ρ of $\zeta_K(s)$ in the critical strip with $|\operatorname{Im}(\rho)| \leq T$. Then,*

$$\left| N_K(T) - \frac{T}{\pi} \log \frac{d_K T^{n_K}}{(2\pi e)^{n_K}} \right| \leq 0.228 (\log d_K + n_K \log T) + 23.108 n_K + 4.520$$

for $T \geq 1$, where d_K and n_K are absolute discriminant and degree of K , respectively.

We now estimate the sum over the zeros of $\zeta_K(s)$ in Lemma 3.3.2 as follows.

Lemma 3.3.4. *Under GRH*

$$\sum_t \frac{2}{1+t^2} = 2 \sum_{|t| \leq 2} \left(\frac{1}{1+t^2} - \frac{1}{5} \right) + (0.548 + c_1) \log d_K + (0.309 + c_2) n_K + O(1),$$

where t runs over the imaginary part of all the non-trivial zeros of $\zeta_K(s)$ and $|c_1| \leq 0.0912$ and $|c_2| \leq 9.3572$.

Proof. If $N_K(T)$ is the number of zeros of $\zeta_K(s)$ with imaginary part $|t| \leq T$, then Theorem 3.3.3 gives

$$(3.2) \quad \left| N_K(T) - \frac{T}{\pi} \log \frac{d_K T^{n_K}}{(2\pi e)^{n_K}} \right| \leq 0.228 \log d_K + 0.228 n_K \log T + 23.108 n_K + 4.520.$$

Since the zeros of $\zeta_K(s)$ are symmetric about the real line, for $T > 2$,

$$\sum_{|t| \leq T} \frac{2}{1+t^2} = \sum_{|t| \leq 2} \frac{2}{1+t^2} + 2 \sum_{2 < t \leq T} \frac{2}{1+t^2}.$$

Assume the GRH. As $T \rightarrow \infty$, using partial summation, we obtain

$$(3.3) \quad \sum_t \frac{2}{1+t^2} = \sum_{|t| \leq 2} \frac{2}{1+t^2} - \frac{2}{5} N_K(2) + 4 \int_2^\infty \frac{t}{(1+t^2)^2} N_K(t) dt.$$

Using (3.2), a standard computation shows that the contribution of the main term

in (3.2) to the above integral is

$$\begin{aligned}
& 4 \int_2^\infty \frac{t}{(1+t^2)^2} \left(\frac{t}{\pi} \log \frac{d_K t^{n_K}}{(2\pi e)^{n_K}} \right) dt \\
&= \frac{4}{\pi} \left(\log d_K - n_K \log(2\pi e) \right) \int_2^\infty \frac{t^2}{(1+t^2)^2} dt + \frac{4n_K}{\pi} \int_2^\infty \frac{t^2 \log t}{(1+t^2)^2} dt \\
&= \frac{4}{\pi} \left(\log d_K - n_K \log(2\pi e) \right) (0.431) + \frac{4n_K}{\pi} (0.774) \\
&= 0.548 \log d_K + 0.309 n_K.
\end{aligned}$$

Moreover, the contribution of the rest of the terms in (3.2) to the integral in (3.3) is at most

$$\begin{aligned}
& 4(0.228 \log d_K + 23.108 n_K + 4.520) \int_2^\infty \frac{t}{(1+t^2)^2} dt + 0.228 n_K \int_2^\infty \frac{t \log t}{(1+t^2)^2} dt \\
&= 0.0912 \log d_K + 9.3572 n_K + 1.808.
\end{aligned}$$

Putting these together, we obtain the lemma. $\square$

In [18], we obtain the following lower bound on the discriminant in terms of low lying zeros of the Dedekind zeta function, conditionally on GRH.

Theorem 3.3.5. *Let K be a number field of degree n_K and absolute discriminant d_K . Then, under GRH*

$$\log d_K \geq 3.67 \sum_{|t| \leq 2} \left(\frac{1}{1+t^2} - \frac{1}{5} \right) + O(n_K),$$

where the implied constant in $O(n_K)$ is absolute.

Proof. From Lemma 3.3.2 and Lemma 3.3.4, we have

$$\begin{aligned}\log d_K &= 2 \sum_{|t| \leq 2} \left(\frac{1}{1+t^2} - \frac{1}{5} \right) + (0.548 + c_1) \log d_K + O(n_K) \\ &\geq 2 \sum_{|t| \leq 2} \left(\frac{1}{1+t^2} - \frac{1}{5} \right) + 0.456 \log d_K + O(n_K).\end{aligned}$$

Therefore

$$(3.4) \quad \log d_K \geq 3.67 \sum_{|t| \leq 2} \left(\frac{1}{1+t^2} - \frac{1}{5} \right) + O(n_K).$$

□

3.4 Lower bound on height function

We now illustrate application of Theorem 3.3.5 towards the proof of Theorem 3.2.1.

Proof of Theorem 3.2.1. Let $K = \mathbb{Q}(\alpha)$ and $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α . From Theorem 3.0.1

$$\log |D(f)| \leq n_K \log n_K + 2(n_K - 1)n_K h(\alpha).$$

Since α is an algebraic integer, we have

$$|D(f)| = I(\alpha)^2 |d_K| \geq |d_K|,$$

where $I(\alpha)$ is the index of α which is always ≥ 1 . Hence, by (3.4),

$$2(n_K - 1)n_K h(\alpha) + n_K \log n_K \geq \log d_K \geq 3.67 \sum_{|t| \leq 2} \left(\frac{1}{1+t^2} - \frac{1}{5} \right) + O(n_K).$$

Dividing both sides by n_K , we obtain

$$2n_K h(\alpha) \geq \frac{3.67}{n_K} \left(\lambda_K(2) - \frac{1}{5} N_K(2) \right) - \log n_K + O(1),$$

as required. $\square$

Recall from Section [3.2](#) that for $K = \mathbb{Q}(\alpha)$, if

$$(3.5) \quad 3.67 \left(\lambda_K(2) - \frac{1}{5} N_K(2) \right) \geq n_K \left(\log n_K + \frac{1}{1000} \right),$$

then Lehmer's conjecture holds for such α . It follows from Theorem [3.3.3](#) that the discriminant d_K of a number field can be bounded below by number of low-lying zeros up to height 2 as

$$\log d_K \geq 1.156 N_K(2) - 25.317 n_K - 5.226.$$

As a consequence of the above inequality, for

$$N_K(2) > 0.865 \left(n_K \log n_K + \frac{1}{1000} \right),$$

we obtain $h(\alpha) \geq \frac{0.005}{n_K}$. However, it is crucial to note that Theorem [3.3.3](#) along with Mahler's inequality does not provide a Lehmer type bound when $N_K(2) < 0.865 n_K \log n_K$. In the following table, computed using SageMath, we present examples of number fields satisfying condition [\(3.5\)](#). These data show that condition [\(3.5\)](#) yields a Lehmer-type bound even when $N_K(2) < 0.865 n_K \log n_K$.

The above table indicates that the quantity $3.67 \left(\lambda_K(2) - \frac{1}{5} N_K(2) \right)$ can become significantly larger than $N_K(2)$ in certain cases. This is because it can be interpreted as a weighted sum over the non-trivial zeros $1/2 + it$ of $\zeta_K(s)$ up to $|t| \leq 2$, with

$m_\alpha(x)$	$3.67 \times (\lambda_K(2) - \frac{1}{5}N_K(2))$	$n_K(\log n_K + \frac{1}{1000})$	$N_K(2)$	$0.865 \times n_K \log n_K$
$x^3 + 2x^2 + 28$	3.72540	3.29883	2	2.85349
$x^3 + 20x + 20$	4.51802	3.29883	2	2.85349
$x^4 + 21x^2 + 1$	5.61114	5.54917	4	4.80003
$x^4 + 28x^2 + 14x + 1$	5.64396	5.54917	4	4.80003
$x^4 + x + 23$	6.38880	5.54917	4	4.80003
$x^4 + 91x^2 + 1$	8.78557	5.54917	4	4.80003
$x^5 + 21x^2 + 1$	9.43790	8.05218	6	6.96514

Table 3.2: Computational data in support of Theorem [3.2.1](#)

weights $3.67 \left(\frac{1}{1+t^2} - \frac{1}{5} \right)$. When zeros lie close to the real line, the weighted sum tends to dominate the zero count $N_K(2)$, and consequently, a lower bound on this sum is less restrictive than a corresponding bound on $N_K(2)$.

Since $\frac{1}{1+t^2} - \frac{1}{5}$ tends to zero as t approaches ± 2 , the quantity $\sum_{|t| \leq 2} \left(\frac{1}{1+t^2} - \frac{1}{5} \right)$ becomes larger when the imaginary parts of the zeros are more concentrated near the origin. In particular, if we restrict attention to zeros whose imaginary parts lie in $[-1, 1]$, then

$$\lambda_K(2) - \frac{1}{5}N_K(2) \geq \lambda_K(1) - \frac{1}{5}N_K(1) \geq \frac{3}{10}N_K(1).$$

Consequently, the following corollary can be deduced from Theorem [3.2.1](#).

Corollary 3.4.1. *Under GRH, every algebraic integer $\alpha \in \overline{\mathbb{Q}}$ with $N_K(1) \geq n_K \log n_K$, where $K = \mathbb{Q}(\alpha)$, satisfies*

$$h(\alpha) \geq 0.55 \frac{\log n_K}{n_K} + o(1).$$

Consequently, Lehmer's conjecture holds for all such α under GRH.

Moreover, for the set of α with $N_K(1) \geq n_K^2$, our Theorem [3.2.1](#) provides an absolute lower bounds on height, i.e., independent of the degree. In other words, abundance of low-lying zeros of the Dedekind zeta-function leads to stronger lower bounds on height of algebraic integers. Consistent with this, in [\[18\]](#) Theorem 2.3] we also demonstrates that for a Galois monogenic number field K of large degree with a completely split prime p , one has $N_K(1) \gg_p n_K^2$ under GRH.

Chapter 4

Small height and p-adic distribution

We start this chapter by recalling the example $h(2^{1/n}) = \log 2/n$, which implies that the lower bound in the Conjecture [2.3](#) is optimal up to the choice of an absolute constant. It turns out that if we restrict ourselves to certain families of algebraic numbers, it is possible to obtain significantly stronger lower bounds on the height. For instance, consider the class of totally real algebraic numbers—those whose Galois conjugates all lie in $\mathbb{R}$ under any choice of embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. For such numbers Schinzel [\[59\]](#) proved in 1973 that the height is bounded below by an absolute constant independent of the degree,

$$(4.1) \quad h(\alpha) \geq \frac{1}{2} \log \left(\frac{1 + \sqrt{5}}{2} \right),$$

for all $\alpha \neq 0, \pm 1$ that are totally real. Sets of algebraic numbers for which height is bounded below by an absolute positive constant are of great interest and they will be discussed in detail in the next chapter.

The lower bound in [\(4.1\)](#) reflects a deeper geometric rigidity: totally real alge-

braic integers cannot have all their conjugates very close to ± 1 . More generally, one can establish lower bounds on the height of algebraic numbers, whose conjugates are restricted to a certain region of the complex plane. The following result due to Mignotte [46] quantitatively captures how the angular distribution of the conjugates relates to the height.

Theorem ([45], Theorem 15.2). *For $\alpha \in \overline{\mathbb{Q}}$, let $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. For any θ with $0 \leq \theta \leq 2\pi$ the number n of conjugates of α in any fixed sector, based at the origin, of angle θ satisfies*

$$(4.2) \quad \left| n - \frac{\theta}{2\pi} d \right| \leq 24 \left(d^{2/3} (\log 2d)^{1/3} + dh(\alpha)^{1/3} \right).$$

This result can be viewed as a quantitative refinement of a classical theorem due to Erdős and Turán [22] on the distribution of roots of complex polynomials. They showed that if $f(z) \in \mathbb{C}[z]$ has small maximum modulus on the unit circle $|z| = 1$, its roots are concentrated near the unit circle and exhibit near-uniform angular distribution.

In 1997, Bilu [10] proved a stronger equidistribution result for Galois conjugates in the complex plane associated with points of small height. More precisely, if α is an algebraic number of height close to zero, then the Galois conjugates of α are equidistributed along the unit circle in the sense of weak convergence.

4.1 Small height and p-adic equidistribution

In 2001, Bombieri and Zannier formulated and studied certain properties (Bogomolov and Northcott property) concerning points of small height in infinite extensions of $\mathbb{Q}$, which is the theme of our next chapter. Their paper establishes a non-archimedean analogue of Bilu's result as follows.

Theorem 4.1.1 ([12], Theorem 3). *Let L be a finite Galois extension of $\mathbb{Q}$ and for each rational prime p let f_p and e_p be the residual degree and ramification index of p in L . Let also $\mathfrak{p}$ a prime ideal of L dividing (p) and write $q := p^{f_p}$. Let $\alpha \in L^*$ be of degree m and let $V_p(\alpha; L)$ be the normalized variance*

$$V_p(\alpha; L) := \frac{1}{m^2} \sum_{x \in \mathbb{F}_q \cup \{\infty\}} \left(N_x - \frac{m}{q+1} \right)^2,$$

where, for $x \in \mathbb{F}_q$, N_x is the number of conjugates of α with reduction x modulo $\mathfrak{p}$ and N_∞ is the number of conjugates of α which are not integers in L_p . This variance does not depend on the choice of $\mathfrak{p} \mid p$. Then we have

$$h(\alpha) \geq -\frac{\log m}{2m-2} + \frac{m}{2m-2} \sum_{q < m} \frac{1}{e_p} \left(V_p(\alpha; L) + \frac{1}{q+1} - \frac{1}{m} \right) \log p.$$

The above theorem implies a non-archimedean equidistribution for algebraic numbers with height tending to 0. In particular, for any sequence $\{\alpha_n\}_{n \geq 1}$ of algebraic numbers such that $h(\alpha_n) \rightarrow 0$ as $n \rightarrow \infty$, we have that if p is unramified in the Galois closure of α_n then $q_n := p^{f_{p,n}} \rightarrow \infty$, where $f_{p,n}$ denotes the inertia degree of p in the Galois closure of α_n . Moreover,

$$\frac{1}{\deg(\alpha_n)^2} \sum_{x \in \mathbb{F}_{q_n} \cup \{\infty\}} \left(N_x - \frac{\deg(\alpha_n)}{q_n+1} \right)^2 \log p \rightarrow 0.$$

Subsequently, a quantitative version of Bilu's theorem was established by Petsche [52], and generalized by Favre and Rivera-Letelier [23] (see also the corrigendum [24]).

In this chapter, we establish a refined non-archimedean equidistribution phenomenon analogous to Theorem 4.1.1 in the non-Galois setting, where the conjugates of algebraic numbers are distributed over small local fields. Let p be a rational prime. Denote by $\mathbb{Q}_p$ the field of p -adic numbers. We fix an algebraic closure $\overline{\mathbb{Q}_p}$

over $\mathbb{Q}_p$ and shall assume that all the algebraic extensions of $\mathbb{Q}_p$ are subfields of $\overline{\mathbb{Q}_p}$. Further, for each prime p , we fix an embedding $i_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$. We say an algebraic number $\alpha \in \overline{\mathbb{Q}}$ *lies in an extension K of $\mathbb{Q}_p$* if $i_p(\alpha) \in K$. For ease of notation, we shall identify $i_p(\alpha)$ and α , when $\alpha \in K$. Viewing $\mathbb{R}$ as the completion of $\mathbb{Q}$ at the archimedean place, one can define a non-archimedean analogue of totally real numbers, called the totally p -adic numbers. An algebraic number α is said to be *totally p -adic* if its image lies in $\mathbb{Q}_p$ for any embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$, where $\mathbb{C}_p$ denotes the completion of $\overline{\mathbb{Q}_p}$.

A recent theorem of Pottmeyer [55] provides a p -adic analogue of Schinzel's result for totally real numbers. He showed that if α is a non-zero totally p -adic number that is not a $(p-1)$ -th root of unity,

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

More generally, let $K/\mathbb{Q}_p$ be a finite extension with ramification index e and inertia degree f . Let S be the set of algebraic numbers all of whose Galois conjugates lie in K . Then, a result of Bombieri and Zannier [12 Theorem 2] implies that

$$\liminf_{\alpha \in S} h(\alpha) \geq \frac{\log p}{2e(p^f + 1)}.$$

A generalized equidistribution theorem due to Baker and Rumely [8, Theorem 2.3] provides a non-Archimedean analogue of Bilu's equidistribution theorem, formulated using the framework of Berkovich spaces. It is important to note that the aforementioned result requires all the Galois conjugates to lie in a fixed local field. Therefore, it is natural to study the case when a subset of the conjugates lies in a fixed local field.

4.2 A p -adic criterion for Lehmer's conjecture

From the inequality (4.2), we can conclude that algebraic numbers of large degree, whose conjugates are not angularly equidistributed in the complex plane, are forced to have height away from zero. In other words, for all $\alpha \in \overline{\mathbb{Q}}$ satisfying

$$\left| n - \frac{\theta}{2\pi} d \right| \gg (d^2 \log d)^{1/3},$$

with the implied constant > 24 , Lehmer's conjecture holds. The main goal of this section is to establish a p -adic analogue of the above phenomenon. In particular, we prove Lehmer's conjecture for a class of algebraic numbers by quantifying how many conjugates must lie in a fixed local field.

We now set up the notation necessary to state our results. Let K be a finite extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}_q$. Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic number of degree d , and $\alpha_1, \alpha_2, \dots, \alpha_d$ be the Galois conjugates of α in $\overline{\mathbb{Q}}$. Define

$$\mathcal{S}_K(\alpha) = \{ \alpha_i \mid \alpha_i \in K, 1 \leq i \leq d \}.$$

In [20, Theorem 1.3], we obtain the following result.

Theorem 4.2.1. *Let K be as above. Then, for any $\alpha \in \overline{\mathbb{Q}}$*

$$h(\alpha) \geq \frac{1}{2[K : \mathbb{Q}_p]} \left(\frac{|\mathcal{S}_K(\alpha)|}{d} \right)^2 \frac{\log q}{q+1} + o_d(1),$$

where $o_d(1)$ tends to 0 as d tends to infinity.

An archimedean analog of similar nature to (4.2.1) with a condition on the number of real conjugates of α was obtained by Garza in [28] using Schinzel's method. Our proof is inspired by the proof of [12, Theorem 2] due to Bombieri and Zannier.

Proof of Theorem 4.2.1. Let K be a finite extension of $\mathbb{Q}_p$ with ramification index e and inertia degree f . Let $\mathbb{F}_q$ denote the residue field of K , where $q = p^f$. We define ν to be the unique valuation on K extending the usual p -adic valuation on $\mathbb{Q}_p$. Let $\alpha \in \overline{\mathbb{Q}}$ be a non-zero algebraic number of degree d , and α_i 's be the Galois conjugates of α in $\overline{\mathbb{Q}}$. Recall that

$$\mathcal{S}_K(\alpha) = \{ \alpha_i \mid \alpha_i \in K, 1 \leq i \leq d \}.$$

Let $m_\alpha(x)$ be the minimal polynomial of α in $\mathbb{Z}[x]$. Consider L to be the splitting field of $m_\alpha(x)$ over K and ω be the unique valuation on L extending ν on K . Rearrange the conjugates α_i of α such that

$$\omega(\alpha_1) \geq \cdots \geq \omega(\alpha_r) \geq 0 > \omega(\alpha_{r+1}) \geq \cdots \geq \omega(\alpha_d).$$

The discriminant of $m_\alpha(x)$ is given by

$$D(m_\alpha) = a_d^{2d-2} \prod_{i < j} (\alpha_i - \alpha_j)^2.$$

The contribution to the valuation of $D(m_\alpha)$ from the terms in the product for which $\omega(\alpha_j) < 0$ can be bounded from below by

$$\omega \left(\prod_{j=r+1}^d \prod_{i=1}^{j-1} (\alpha_j - \alpha_i) \right) \geq \sum_{j=r+1}^d (j-1) \omega(\alpha_j).$$

Further, it follows from the Gauss's lemma that $\omega(a_d) = -\sum_{i=r+1}^d \omega(\alpha_i)$. Hence, we

obtain

$$\begin{aligned}
\omega(D(m_\alpha)) &\geq (2d-2)\omega(a_d) + 2 \sum_{0 < i < j \leq r} \omega(\alpha_j - \alpha_i) + 2 \sum_{j=r+1}^d (j-1)\omega(\alpha_j) \\
(4.3) \quad &\geq 2 \sum_{i < j \leq r} \omega(\alpha_j - \alpha_i) - 2 \sum_{j=r+1}^d (d-j)\omega(\alpha_j).
\end{aligned}$$

Since $\omega(\alpha_j) < 0$ for $r+1 \leq j \leq d$, and $\omega(\alpha_1), \omega(\alpha_2), \dots, \omega(\alpha_r) \geq 0$, omitting a few non-negative terms if necessary, we have the following inequality

$$\begin{aligned}
\omega(D(m_\alpha)) &\geq 2 \sum_{i < j \leq r} \omega(\alpha_j - \alpha_i) - 2 \sum_{j=r+1}^d (d-j)\omega(\alpha_j) \\
(4.4) \quad &\geq 2 \sum_{\substack{i < j \leq r \\ \alpha_i, \alpha_j \in \mathcal{S}_K(\alpha)}} \nu(\alpha_j - \alpha_i) - 2 \sum_{\substack{r < j \leq d \\ \alpha_j \in \mathcal{S}_K(\alpha)}} (d-j)\nu(\alpha_j).
\end{aligned}$$

For each $x \in \mathbb{F}_q$, let N_x denote the number of conjugates of $\alpha_t \in \mathcal{S}_K(\alpha)$ with $1 \leq t \leq r$, which lie in the residue class $x \bmod \nu$. If $\alpha_i, \alpha_j \in \mathcal{S}_K(\alpha)$ lie in the same residue class modulo ν , then $\nu(\alpha_i - \alpha_j) \geq \frac{1}{e}$. Hence,

$$\sum_{\substack{i < j \leq r \\ \alpha_i, \alpha_j \in \mathcal{S}_K(\alpha)}} \nu(\alpha_j - \alpha_i) \geq \frac{1}{e} \sum_{x \in \mathbb{F}_q} \frac{N_x(N_x - 1)}{2},$$

where $q = p^f$.

Let r' be the number of ν -integral conjugates of α lying in K . Since there are $|\mathcal{S}_K(\alpha)|$ many conjugates of α lying in K , there are exactly $|\mathcal{S}_K(\alpha)| - r'$ non-integral conjugates of α in K . Therefore the second summation in (4.4) runs over all $|\mathcal{S}_K(\alpha)| - r'$ non-integral conjugates of α in K . As $d-j$ are all distinct positive

integers, we have

$$\sum_{\substack{r < j \leq d \\ \alpha_j \in \mathcal{S}_K(\alpha)}} (d-j) \geq \frac{(|\mathcal{S}_K(\alpha)| - r')(|\mathcal{S}_K(\alpha)| - r' - 1)}{2}.$$

Note that, for $r < i \leq d$, $\nu(\alpha_i) \leq -\frac{1}{e}$ and therefore, (4.4) implies that

$$\text{ord}_p(D(m_\alpha)) \geq \frac{1}{e} \left((|\mathcal{S}_K(\alpha)| - r')(|\mathcal{S}_K(\alpha)| - r' - 1) + \sum_{x \in \mathbb{F}_q} N_x(N_x - 1) \right),$$

where $\text{ord}_p(D(m_\alpha))$ is the usual p -adic valuation of $D(m_\alpha)$.

Since $(|\mathcal{S}_K(\alpha)| - r') + \sum_{x \in \mathbb{F}_q} N_x = |\mathcal{S}_K(\alpha)|$, applying Cauchy-Schwarz inequality, we obtain

$$\begin{aligned} \text{ord}_p(D(m_\alpha)) &\geq \frac{1}{e} \left((|\mathcal{S}_K(\alpha)| - r')(|\mathcal{S}_K(\alpha)| - r' - 1) + \sum_{x \in \mathbb{F}_q} N_x(N_x - 1) \right) \\ &= \frac{1}{e} \left((|\mathcal{S}_K(\alpha)| - r')^2 + \sum_{x \in \mathbb{F}_q} N_x^2 + O(d) \right) \\ &\geq \frac{1}{e} \left(\frac{|\mathcal{S}_K(\alpha)|^2}{q+1} + O(d) \right), \end{aligned}$$

where the implied constant has absolute value ≤ 1 . Therefore,

$$\begin{aligned} \log |D(m_\alpha)| &\geq \frac{1}{e} |\mathcal{S}_K(\alpha)|^2 \left(\frac{\log p}{q+1} \right) + O \left(d \frac{\log p}{e} \right) \\ &\geq \frac{1}{[K : \mathbb{Q}_p]} |\mathcal{S}_K(\alpha)|^2 \left(\frac{\log q}{q+1} \right) + O \left(d \frac{\log q}{[K : \mathbb{Q}_p]} \right). \end{aligned}$$

Applying Mahler's inequality (Theorem 3.0.1), we deduce that

$$\begin{aligned} (4.5) \quad d h(\alpha) = \log M(\alpha) &\geq \frac{\log |D(m_\alpha)|}{2d} - \frac{\log d}{2} \\ &\geq \frac{1}{2[K : \mathbb{Q}_p]} \left(\frac{|\mathcal{S}_K(\alpha)|^2}{d} \right) \frac{\log q}{(q+1)} + O \left(\frac{\log q}{[K : \mathbb{Q}_p]} \right) - \frac{\log d}{2}, \end{aligned}$$

where the implied constant in the O -term has absolute value $\leq 1/2$. Dividing both side of above inequality by d completes the proof of Theorem [4.2.1](#). $\square$

In Theorem [4.1.1](#) L is a Galois extension with finite local degree $e_p f_p$ at p . This implies that for any $\alpha \in L^*$, all the conjugates of α lie in a fixed finite extension L_p of $\mathbb{Q}_p$ such that $[L_p : \mathbb{Q}_p] = e_p f_p$. Applying Theorem [4.2.1](#) to this case, we obtain

$$h(\alpha) \geq \frac{1}{2e_p} \frac{\log p}{p^{f_p} + 1} + o_d(1).$$

This lower bound is essentially the contribution from $q = p^{f_p}$ in the right hand summation in Theorem [4.1.1](#). The rest of the terms in the sum can be bounded above by $O(\log p / e_p (p^{f_p} + 1))$. Hence, we retrieve the main term of Theorem [4.1.1](#). But, Theorem [4.2.1](#) gives more freedom in the choice of α 's, since we only require a positive proportion of the conjugates of α to lie in a finite extension of $\mathbb{Q}_p$. On the other hand, Theorem [4.1.1](#) only applies when all the conjugates of α lie in a finite extension of $\mathbb{Q}_p$. It is not difficult to construct a sequence of algebraic numbers α_n such that the local degree of the Galois closure of $\mathbb{Q}(\alpha_n)$ at p tends to infinity, but a positive proportion of the conjugates of α_n lie in $\mathbb{Q}_p$. If α is a totally p -adic number of degree d , then the above theorem implies that

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

This recovers Pottmeyer's bound up to the $o_{d,p}(1)$ term. The method of proof of Theorem [4.2.1](#) can be used to derive the following consequences.

Proposition 4.2.2. *Let K be as above. For $c > 0$, consider the set*

$$S := \left\{ \alpha \in \overline{\mathbb{Q}}^\times : |\mathcal{S}_K(\alpha)| \geq \sqrt{\left(\frac{2(q+1)[K:\mathbb{Q}_p]}{\log q} d \right) \left(c + \frac{\log(qd)}{2} \right)} \right\}.$$

Then, $h(\alpha) \geq \frac{c}{d}$ for all $\alpha \in S$ and hence Lehmer's conjecture holds for S .

Proof of Proposition 4.2.2 From (4.5), we deduce that if

$$|\mathcal{S}_K(\alpha)| \geq \sqrt{\left(\frac{2(q+1)[K:\mathbb{Q}_p]d}{\log q}\right) \left(c + \frac{\log(qd)}{2}\right)}$$

then

$$dh(\alpha) \geq c + \frac{\log q}{2} + O\left(\frac{\log q}{[K:\mathbb{Q}_p]}\right).$$

Since the absolute value of the implied constant of the O -term is bounded above by $1/2$, we conclude that

$$h(\alpha) \geq \frac{c}{d}.$$

□

The above proposition proves that a condition much weaker than “positive proportion” of conjugates in K is sufficient to establish Lehmer’s conjecture. In particular, it is enough to show that $\gg \sqrt{d \log d}$ many conjugates of α lie in a fixed local field, with a suitable implied constant. This is stated in the following corollary as a straightforward consequence of the above proposition.

Corollary 4.2.3. *Let K be as above, and define*

$$S := \left\{ \alpha \in \overline{\mathbb{Q}}^\times : |\mathcal{S}_K(\alpha)| \geq \sqrt{q^3[K:\mathbb{Q}_p]d \log d} \right\}.$$

Then, Lehmer’s conjecture holds for S . Moreover, $d \cdot h(\alpha) \rightarrow \infty$ as $d \rightarrow \infty$.

Proof of Corollary 4.2.3. Taking $|\mathcal{S}_K(\alpha)| \geq (q^3[K:\mathbb{Q}_p]d \log d)^{1/2}$ in (4.5), we obtain

$$(4.6) \quad dh(\alpha) \geq \left(\frac{q^3 \log q - q - 1}{2(q+1)}\right) \log d + O\left(\frac{\log q}{[K:\mathbb{Q}_p]}\right).$$

Note that for any real number $x \geq 2$,

$$\frac{x^3 \log x - x - 1}{2(x+1)} \geq \frac{2}{5}.$$

This is because the function in the LHS is increasing for $x \geq 2$ and the inequality holds for $x = 2$. Applying this to (4.6), we obtain

$$dh(\alpha) \geq \frac{2}{5} \log d + O\left(\frac{\log q}{[K : \mathbb{Q}_p]}\right).$$

Therefore, as $d \rightarrow \infty$, the Mahler measure $M(\alpha) = dh(\alpha)$ also tends to infinity as required. $\square$

An archimedean analogue of Theorem 4.2.1, due to Garza [28], states that if R_α denotes the proportion of conjugates of a non-zero algebraic number $\alpha \neq \pm 1$ that lie on the real line, then

$$(4.7) \quad h(\alpha) \geq \frac{R_\alpha}{2} \log \left(\frac{2^{1-1/R_\alpha} + \sqrt{4^{1-1/R_\alpha} + 4}}{2} \right).$$

If d is the degree of α , then (4.7) yields a Lehmer-type bound only when a proportion of at least $O\left(\frac{1}{\log d}\right)$ of the conjugates lie in $\mathbb{R}$. In contrast, on the non-Archimedean side, Theorem 4.2.1 provides a Lehmer-type bound when a proportion of at least $O\left(\frac{\log d}{\sqrt{d}}\right)$ conjugates lie in a given local field.

4.3 A non-archimedean equidistribution theorem

We now generalize our setup from the previous section to capture the behaviour of conjugates spread across multiple local fields over several primes. The results in this section are proved for algebraic integers but can be extended to algebraic numbers at the cost of slightly weaker lower bounds. Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic integer of degree d , and $\alpha_1, \alpha_2, \dots, \alpha_d$ be the Galois conjugates of α in $\overline{\mathbb{Q}}$. We consider a partition $\mathcal{P}_{p,\alpha}$ of the conjugates of α by defining the following equivalence relation:

$$\alpha_i \sim \alpha_j \quad \text{if} \quad \mathbb{Q}_p(\alpha_i) = \mathbb{Q}_p(\alpha_j).$$

Each equivalence class $P \in \mathcal{P}_{p,\alpha}$ obtained in this way corresponds to a finite extension K_P of $\mathbb{Q}_p$. For each K_P , denote by e_P and f_P the ramification index and inertia degree of K_P , respectively, $n_P = [K_P : \mathbb{Q}_p]$ and $\mathbb{F}_{q_P}$ the residue field. The intersection of these fields might contain some conjugates of α non-trivially, but the corresponding equivalence classes are pairwise disjoint. Since we are dealing with algebraic integers, we can ignore the contribution to the discriminant coming from the terms $\alpha_i - \alpha_j$ where α_i and α_j lie in different classes of the partition. This yields

$$(4.8) \quad \text{ord}_p(D(m_\alpha)) \geq \sum_{P \in \mathcal{P}_{p,\alpha}} v_P \left(\prod_{\substack{\alpha_i, \alpha_j \in P \\ \alpha_i \neq \alpha_j}} (\alpha_i - \alpha_j) \right),$$

where ν_P is the unique valuation on K_P extending the usual p -adic valuation on $\mathbb{Q}_p$. In [20 Theorem 1.7], we obtain the following result.

Theorem 4.3.1. *Let $\alpha \in \overline{\mathbb{Q}}$ be a non-zero algebraic integer. Let $\mathcal{P}_{p,\alpha}$ be the partition of conjugates of α defined above. For $P \in \mathcal{P}_{p,\alpha}$, let K_P be the corresponding extension of $\mathbb{Q}_p$. Then,*

$$h(\alpha) \geq \frac{1}{2} \sum_p \max \left\{ 0, \left(\frac{1}{\sum_{P \in \mathcal{P}_{p,\alpha}} e_P q_P} - \frac{1}{d^2} \sum_{P \in \mathcal{P}_{p,\alpha}} \frac{|P|}{e_P} \right) \right\} \log p - \frac{\log d}{2d}.$$

Proof. Let $\alpha \in \overline{\mathbb{Q}}$ be a non-zero algebraic integer. For $P \in \mathcal{P}_{p,\alpha}$ and $x \in \mathbb{F}_{q_P}$, define

$$N_{K_P, x} = \# \{ \alpha_i \in P : \alpha_i \equiv x \text{ in } \mathbb{F}_{q_P} \}.$$

We can write

$$|D(m_\alpha)| = \prod_p p^{\text{ord}_p(D(m_\alpha))}.$$

Taking the logarithm and using the lower bound in (4.8), we obtain

$$\log |D(m_\alpha)| \geq \sum_p \sum_{P \in \mathcal{P}_{p,\alpha}} v_P \left(\prod_{\substack{\alpha_i, \alpha_j \in P \\ \alpha_i \neq \alpha_j}} (\alpha_i - \alpha_j) \right).$$

Thus, we have

$$\begin{aligned}
\log |D(m_\alpha)| &\geq \sum_p \sum_{P \in \mathcal{P}_{p,\alpha}} \left(\sum_{x \in \mathbb{F}_{q_P}} N_{K_P,x} (N_{K_P,x} - 1) \right) \frac{\log p}{e_P} \\
(4.9) \quad &\geq \sum_p \left(\sum_{P \in \mathcal{P}_{p,\alpha}} \frac{1}{e_P} \sum_{x \in \mathbb{F}_{q_P}} N_{K_P,x} (N_{K_P,x} - 1) \right) \log p.
\end{aligned}$$

Each term $N_{K,x}(N_{K,x} - 1)$ in the above inequality is non-negative. Therefore,

$$(4.10) \quad \log |D(m_\alpha)| \geq \sum_p \max \left\{ 0, \sum_{P \in \mathcal{P}_{p,\alpha}} \frac{1}{e_P} \sum_{x \in \mathbb{F}_{q_P}} N_{K,x} (N_{K,x} - 1) \right\} \log p.$$

Since $\sum_{x \in \mathbb{F}_{q_P}} N_{K_P,x} = |P|$, using the Cauchy-Schwarz inequality, we obtain

$$\sum_{P \in \mathcal{P}_{p,\alpha}} \frac{1}{e_P} \sum_{x \in \mathbb{F}_{q_P}} N_{K_P,x}^2 \geq \sum_{P \in \mathcal{P}_{p,\alpha}} \frac{1}{e_P q_P} |P|^2.$$

As $\sum_{P \in \mathcal{P}_{p,\alpha}} |P| = d$, using the Cauchy-Schwarz inequality, we get

$$\sum_{P \in \mathcal{P}_{p,\alpha}} \frac{1}{e_P q_P} |P|^2 \geq \frac{d^2}{\sum_{P \in \mathcal{P}_{p,\alpha}} e_P q_P}$$

and hence,

$$(4.11) \quad \sum_{P \in \mathcal{P}_{p,\alpha}} \frac{1}{e_P} \sum_{x \in \mathbb{F}_{q_P}} N_{K_P,x}^2 \geq \frac{d^2}{\sum_{P \in \mathcal{P}_{p,\alpha}} e_P q_P}.$$

On the other hand

$$(4.12) \quad \sum_{P \in \mathcal{P}_{p,\alpha}} \frac{1}{e_P} \sum_{x \in \mathbb{F}_{q_P}} N_{K_P,x} = \sum_{P \in \mathcal{P}_{p,\alpha}} \frac{|P|}{e_P}.$$

Combining (4.11) and (4.12) in (4.10), we get

$$\log |D(m_\alpha)| \geq d^2 \sum_p \left(\frac{1}{\sum_{P \in \mathcal{P}_{p,\alpha}} e_P q_P} - \frac{1}{d^2} \sum_{P \in \mathcal{P}_{p,\alpha}} \frac{|P|}{e_P} \right) \log p.$$

Finally, applying Mahler's inequality (Theorem 3.0.1), we conclude the theorem. $\square$

The above theorem does not require any preassigned local field as in Theorem 4.1.1 and Theorem 4.2.1. Another important feature here is that the contribution of the inertia degree is additive. This contrasts with the situation when one considers all conjugates in a single local field, where the degree of the compositum often grows multiplicatively. To illustrate this, consider the case when the set $\mathcal{P}_{p,\alpha}$ consists of only two elements, K and K' , both unramified at p and having inertia degrees 2 and 3, respectively. In this case, the Theorem 4.3.1 gives

$$h(\alpha) \geq \frac{1}{2} \frac{\log p}{p^2(p+1)} + o_d(1).$$

Meanwhile, since the compositum KK' is the smallest local field containing the Galois closure of $\mathbb{Q}(\alpha)$. Hence, Theorem 4.1.1 gives a weaker lower bound

$$h(\alpha) \geq \frac{1}{2} \frac{\log p}{p^6 + 1} + o_d(1).$$

As a consequence of above theorem, we obtain the following corollary.

Corollary 4.3.2. *Let $\alpha \in \overline{\mathbb{Q}}$ be a non-zero algebraic integer. Let $\mathcal{P}_{p,\alpha}$ be the partition of conjugates of α defined above. For $P \in \mathcal{P}_{p,\alpha}$, let K_P be the corresponding extension of $\mathbb{Q}_p$. Then*

$$h(\alpha) \geq \frac{1}{2} \sum_p \max \left\{ 0, \frac{1}{d^2} \sum_{P \in \mathcal{P}_{p,\alpha}} \left(\frac{|P|^2}{q_P} - |P| \right) \frac{\log q_P}{n_P} \right\} - \frac{\log d}{2d}.$$

Proof. By (4.10), we have the inequality

$$\log |D(m_\alpha)| \geq \sum_p \max \left\{ 0, \sum_{P \in \mathcal{P}_{p,\alpha}} \sum_{x \in \mathbb{F}_{q_P}} N_{K_P,x} (N_{K_P,x} - 1) \frac{\log q_P}{n_P} \right\}.$$

For $P \in \mathcal{P}_{p,\alpha}$, since $\sum_{x \in \mathbb{F}_{q_P}} N_{K_P,x} = |P|$ is the total number of conjugates of α in P , using the Cauchy-Schwarz inequality, we obtain

$$\begin{aligned} \log |D(m_\alpha)| &\geq \sum_p \max \left\{ 0, \sum_{P \in \mathcal{P}_{p,\alpha}} \frac{\log q_P}{n_P} \sum_{x \in \mathbb{F}_{q_P}} N_{K_P,x} (N_{K_P,x} - 1) \right\} \\ &\geq \sum_p \max \left\{ 0, \sum_{P \in \mathcal{P}_{p,\alpha}} \left(\frac{|P|^2}{q_P} - |P| \right) \frac{\log q_P}{n_P} \right\}. \end{aligned}$$

The proof now follows by applying Mahler's inequality (Theorem 3.0.1). $\square$

This corollary can be seen as a refinement of Theorem 4.1.1 in the non-Galois setting and thus gives a **non-archimedean equidistribution theorem** similar to Bombieri and Zannier (see the first remark after Theorem 4.1.1). Here, the lower bound captures the contribution from all the small local fields containing the conjugates of α . In other words, if conjugates of α lie in several local fields K with small inertia degree, then we obtain a meaningful lower bound for $h(\alpha)$.

For a totally p -adic algebraic integer, Corollary 4.3.2 implies that

$$h(\alpha) \geq \frac{\log p}{2p} \max \left\{ 0, \left(1 - \frac{p}{d} \right) \right\} - \frac{\log d}{2d}.$$

Hence, by Northcott's theorem

$$\liminf_{\alpha \in \mathcal{O}_{\mathbb{Q}^{tp}}} h(\alpha) \geq \frac{\log p}{2p},$$

where $\mathbb{Q}^{tp}$ is the maximal totally p -adic field over $\mathbb{Q}$ and $\mathcal{O}_{\mathbb{Q}^{tp}}$ its ring of integers.

This can be realized as a weaker version of Pottmeyer's result.

Chapter 5

Points of small height and asymptotically positive extensions

In the preceding chapters, our motivation for studying points of small height arose from Lehmer's conjecture. While Lehmer's conjecture concerns the minimal rate at which the Weil height grows with respect to the degree, A. Schinzel [59] showed in 1973 that for totally real algebraic numbers $\alpha \in \mathbb{Q}^{\text{tr}} \setminus \{\pm 1\}$,

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

This result shows that when one restricts to certain subsets of algebraic numbers, one obtains much stronger lower bounds for the height than those predicted by Lehmer's conjecture. In particular, it implies that algebraic numbers of small height lie in $\overline{\mathbb{Q}} \setminus \mathbb{Q}^{\text{tr}}$. This perspective motivates the study of the location and distribution of points of small height among algebraic numbers.

The goal of this chapter is to study a property concerning points of small height, known as the Bogomolov property, which asks whether the values taken by the height function admit a gap near the origin on the real line, i.e., whether the height

is bounded away from zero by a positive constant. The origins of this property lie in the Bogomolov Conjecture (now the Ullmo–Zhang Theorem), which characterizes the distribution of points of small height on abelian varieties. In the classical setting, this property distinguishes between sets in which points of small height are isolated and those in which they are dense.

5.1 Bogomolov and Northcott property

In 2001, E. Bombieri and U. Zannier [12] defined two properties for subsets of $\overline{\mathbb{Q}}$, namely Bogomolov (B) and Northcott (N), concerning points of small height. A subset $S \subseteq \overline{\mathbb{Q}}$ is said to have the *Northcott property* (N) if for any $c > 0$, the set

$$\{\alpha \in S \mid \alpha \neq 0 \text{ and } h(\alpha) < c\}$$

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

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

is empty. Equivalently, S satisfies property (B) (resp. property (N)) if

$$\liminf_{\alpha \in S \setminus \mu_\infty} h(\alpha) > 0 \quad \left(\text{resp. } \liminf_{\alpha \in S} h(\alpha) = \infty \right).$$

Clearly, if S satisfies (N), it also satisfies (B). It follows immediately from Northcott’s theorem that number fields, as well as sets of algebraic numbers of bounded degree, satisfy property (N). As a consequence, if a sequence of algebraic numbers α_n satisfies $h(\alpha_n) \rightarrow 0$, then necessarily $\deg(\alpha_n) \rightarrow \infty$. This shows that the only interesting subsets of $\overline{\mathbb{Q}}$ that satisfy property (B) or (N) in a non-trivial way must

contain algebraic numbers of arbitrarily large degree. In particular, one can ask whether an infinite algebraic extension of $\mathbb{Q}$ satisfies property (B).

One such infinite extension is $\mathbb{Q}^{tr}$, the maximal totally real extension of $\mathbb{Q}$, which satisfies property (B) as a consequence of Schinzel's bound. In [3], 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,

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

This was generalized to K^{ab} by F. Amoroso and U. Zannier [4] for any number field K . Earlier, in 1973, A. Schinzel [59] 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 [12].

Theorem 5.1.1 (Bombieri-Zannier). *Let $\mathcal{L}$ over $\mathbb{Q}$ be an infinite Galois extension.*

Define

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

Then

$$(5.1) \quad \liminf_{\alpha \in \mathcal{L}} h(\alpha) \geq \frac{1}{2} \sum_{p \in S(\mathcal{L})} \frac{\log p}{e_p (p^{f_p} + 1)},$$

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 (5.1) diverges, then $\mathcal{L}$ satisfies property (N). An explicit example where the RHS diverges can be found in S. Checcoli and A. Fehm [15]. 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 5.1.1 in recent times. In 2015, P. Fili and C. Petsche [26] 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 [27] 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 $\mathbb{Q}$. The goal of this chapter is to 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 (5.1). 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. Vlăduț [69].

5.2 Asymptotically positive extension

For a number field K 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 an infinite tower

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

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

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

We shall show that this limit exists and is well-defined, i.e., independent of the tower $\{L_i\}$ 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 $f > 1$.

We now show that the limit above is well-defined and in fact the following lemma proves a stronger result.

Lemma 5.2.1. *Let L/K be an extension of number fields. Then, for any positive real number $x > 1$,*

$$\sum_{q \leq x} \frac{\mathcal{N}_q(K) \log q}{[K : \mathbb{Q}]} \geq \sum_{q \leq x} \frac{\mathcal{N}_q(L) \log q}{[L : \mathbb{Q}]},$$

where q runs over all prime powers.

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 $\{\mathfrak{q}_1, \mathfrak{q}_2, \dots, \mathfrak{q}_r\}$ in L . Then,

$$\prod_i N(\mathfrak{q}_i) \leq N(\mathfrak{p})^{[L:K]}.$$

Therefore,

$$\sum_{k=1}^{\lfloor \frac{\log x}{\log p} \rfloor} k \mathcal{N}_{p^k}(L) \leq [L:K] \sum_{k=1}^{\lfloor \frac{\log x}{\log p} \rfloor} k \mathcal{N}_{p^k}(K).$$

Mutlplying by $\log p$ and dividing by $[L : \mathbb{Q}]$, we obtain for any prime p

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

Summing over all primes $p \leq x$, we obtain the lemma. □

Hence, we deduce that for any tower $\mathcal{L} = \{L_i\}$ and any $x > 1$, the limit

$$\lim_{i \rightarrow \infty} \sum_{q \leq x, q \neq p^k} \frac{\mathcal{N}_q(L_i) \log q}{[L_i : \mathbb{Q}]}$$

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

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

is well-defined for all prime powers q and takes value between 0 and 1.

Definition 5.2.2. *We say that an infinite extension $\mathcal{L}/\mathbb{Q}$ is **asymptotically positive** if $\psi_q > 0$ for some prime power q .*

Under this notation, for an infinite Galois extension $\mathcal{L}/\mathbb{Q}$, the RHS of (5.1.1) can be written as

$$(5.2) \quad \frac{1}{2} \sum_{p \in S(\mathcal{L})} \frac{\log p}{e_p (p^{f_p} + 1)} = \frac{1}{2} \sum_q \psi_q \frac{\log q}{q + 1},$$

where q runs over all prime powers. This interpretation offers a remarkable advantage as it allows us to define analogous quantities for non-Galois extensions. Moreover, the condition $S(\mathcal{L})$ being non-empty is equivalent to $\mathcal{L}/\mathbb{Q}$ being asymptotically positive.

Proposition 5.2.3. *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,*

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

Proof. Let $\psi_q := \lim_{i \rightarrow \infty} \frac{\mathcal{N}_q(K_i)}{n_{K_i}}$ and $\psi'_q := \lim_{i \rightarrow \infty} \frac{\mathcal{N}_q(L_i)}{n_{L_i}}$ 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

5.2.1, 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 . $\square$

Definition 5.2.4. 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 $t \rightarrow \infty$.

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 5.2.5. 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 $j \rightarrow \infty$. Thus,

$$(5.3) \quad \mathcal{N}_{p^m}(L_j) = [L_j : L_i] \mathcal{N}_{p^m}(L_i) + o(n_{L_j}).$$

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 (5.3), 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 $j \rightarrow \infty$. 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 5.2.1 gives

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

where q runs over all the powers of p . 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 5.2.1 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. $\square$

Lemma 5.2.6. *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 $\mathcal{L}F = \{L_i F\}_{i \geq 0}$. By definition, we have

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

It follows that

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

Dividing both sides by $n_{L_i F}$ and taking the limit as $i \rightarrow \infty$, we obtain

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

Therefore, there exists some $k \in \{1, 2, \dots, d\}$ 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. $\square$

5.3 Bogomolov property for asymptotically positive extension

Inspired by Theorem [5.1.1](#) we proposed the following conjecture in [\[18\]](#) Conjecture 2.2].

Conjecture 5.3.1. *Let $\mathcal{L}/\mathbb{Q}$ be an infinite algebraic extension. Then,*

$$(5.4) \quad \liminf_{\alpha \in \mathcal{K}} h(\alpha) \geq \frac{1}{2} \sum_q \psi_q \frac{\log q}{q+1},$$

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 [\(5.4\)](#) is same as the RHS in [\(5.1\)](#). 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 [5.1.1](#) for infinite non-Galois extensions. For totally p -adic fields, Bombieri and Zannier [\[12\]](#) Example 3] demonstrated that [\(5.1\)](#) 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 [5.3.1](#) to be close to optimal.

In [\[19\]](#) Theorem 1.2], we partially resolve this conjecture as follows.

Theorem 5.3.2. *Let $\mathcal{L}/\mathbb{Q}$ be an infinite extension, 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 positive integer λ , depending on p , q 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 [5.3.1](#) still remains open, the bound in Theorem [5.3.2](#) (a) establishes it for algebraic integers. For algebraic non-integers, we obtain a weaker lower bound in Theorem [5.3.2](#) (b). Nevertheless, this proves property (B) for asymptotically positive extensions.

We emphasize that Theorem [5.3.2](#) (a) is not a straightforward generalization of Theorem [5.1.1](#). 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 [5.1.1](#) 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 $p \notin S(\tilde{\mathcal{L}})$, where $\tilde{\mathcal{L}}$ is the Galois closure of $\mathcal{L}$ over $\mathbb{Q}$. Thus, Theorem [5.1.1](#) is not applicable to $\tilde{\mathcal{L}}$, where as Theorem [5.3.2](#) gives property (B) for $\mathcal{O}_{\mathcal{L}}$. Let $K/\mathbb{Q}$ be a number field with distinct prime ideals $P_1, P_2, \dots, P_s$ and $Q_1, Q_2, \dots, Q_t$. For

any integer $n \geq 2$, there exists a degree n extension L of K such that $P_1, P_2, \dots, P_s$ split completely and $Q_1, Q_2, \dots, Q_t$ totally ramify over L . It is clear that such an L exists, for instance, by solving the congruence system

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

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 [12, 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

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

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, $p \notin S(\tilde{\mathcal{L}})$.

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.

The proof of Theorem 5.3.2 (a) requires developing the theory of relative height which will be discussed in the later sections. Towards the proof of Theorem 5.3.2 (b), we use metric properties of non-archimedean places as in Amoroso–David–Zannier [2]. Unfortunately, this method yields a significantly weaker lower bound as compared to Theorem 5.3.2 (a).

We need the following acceleration lemma from [2 Lemma 2.1].

Lemma 5.3.3. *Let L be a number field, v be a finite place of L 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 $s_{p,\rho}(\lambda) \rightarrow +\infty$ for $\lambda \rightarrow +\infty$. 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

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

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

$$(5.5) \quad |\alpha^q - \alpha|_v \leq c(v) \max(1, |\alpha|_v)^{q+1},$$

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

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

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

$$(5.6) \quad \liminf_{\alpha \in \mathcal{L} \setminus \mu_\infty} h(\alpha) \geq \frac{1}{q+1} (\psi_q(\mathcal{L}) \log q - \log 2).$$

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 [5.3.3](#) with $\rho = 1/e_v$. Proceeding similarly to [\(5.5\)](#), we obtain

$$(5.7) \quad \left| \alpha^{p^{f_v+\lambda}} - \alpha^{p^\lambda} \right|_v \leq c'(v) \max(1, |\alpha|_v)^{p^{(f_v+\lambda)+p^\lambda}},$$

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

Proof of Theorem [5.3.2](#) (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 [\(5.7\)](#), 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

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

and hence,

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

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, $\epsilon_i \rightarrow 0$ as $i \rightarrow \infty$. 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 $|\alpha^{p^\lambda+q} - \alpha^{p^\lambda}|_v$ obtained in [\(5.7\)](#), 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 $\epsilon_i \rightarrow 0$ as $i \rightarrow \infty$, we conclude that

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

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

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

This proves the theorem. □

5.4 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 3.0.1), which shall play a crucial role in the proof of Theorems 5.3.2 (a).

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

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

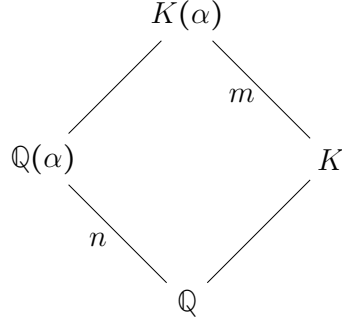
be the minimal polynomial of α over $\mathbb{Q}$. Let $f_K(x) = x^m + b_{m-1}x^{m-1} + \dots + b_0$ be the minimal polynomial of α over O_K of degree $m = [K(\alpha) : K]$ and $\alpha_1, \alpha_2, \dots, \alpha_m$ be its roots in the algebraic closure of K . We define the *relative Mahler measure* of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

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

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

$$(5.8) \quad f(x)^{[K(\alpha) : \mathbb{Q}(\alpha)]} = \prod_{\sigma} \sigma(f_K(x)),$$

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 (5.8) we have

$$(5.9) \quad h(\alpha) = \frac{1}{[K : \mathbb{Q}]} \sum_{\sigma} h_{\sigma(K)}(\alpha).$$

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

Mahler's inequality for relative height

Let α and f_K be as above. The discriminant of f_K is given as

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

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

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

We now proceed as in the proof of Mahler's inequality [43]. The product in the last equality is square of absolute value of a Vandermonde determinant. Thus applying Hadamard's inequality, we obtain

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

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

Lemma 5.4.1. *Let $\alpha \in \overline{\mathbb{Q}} \setminus K$ be an algebraic integer, 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 (5.9), we deduce that

$$(5.10) \quad h(\alpha) \geq \frac{1}{2[K:\mathbb{Q}]} \left(\frac{\log (|N_{K/\mathbb{Q}}(D(f_K))|)}{m^2} \right) - \frac{\log m}{m}.$$

It is sometimes advantageous to work with the norm of the discriminant over a number field K , as opposed to considering the discriminant over $\mathbb{Q}$. For example, in the special case where $K \subseteq \mathbb{Q}(\alpha)$, we have

$$|D(f)| \geq |\text{disc}(K/\mathbb{Q})|^{[\mathbb{Q}(\alpha):K]} |N_{K/\mathbb{Q}}(D(f_K))|,$$

where f and f_K are the minimal polynomials of an algebraic integer α over $\mathbb{Q}$ and K respectively, and $\text{disc}(K/\mathbb{Q})$ 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 (5.10) can be compared with a related result due to Silverman [61, Theorem 2], which states that

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

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 (5.10) 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.*

5.5 Improved height bound for asymptotically positive extensions

The outline of the proof of Theorems (5.3.2) (a) is inspired by the argument of Bombieri-Zannier in [12]. The new idea is to incorporate relative Mahler's inequality as developed in Section (5.4).

We also recall the following well known lemma from algebraic number theory (see [49, Prop. II. 8.2])

Lemma 5.5.1. *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 $\deg f_j(x) = e_j f_j$.

Proof of Theorem 5.3.2 (a). Let $\mathcal{L}/\mathbb{Q}$ be an infinite algebraic 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 5.2.5, 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 contained in $\mathcal{L}$ 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 and L_v be the completion of L at the non-archimedean place v corresponding to $\mathfrak{p}$. Since $\mathfrak{p}$ is almost totally split in $\mathcal{L}$ and $L(\alpha) \subseteq \mathcal{L}$, by Lemma 5.5.1, the polynomial f_L factors over L_v as

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

where $t = n + o(n)$.

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

$$\begin{aligned} v(D(f_L)) &\geq \sum_{x \in \mathbb{F}_q} N_x(N_x - 1) \\ (5.11) \quad &\geq \frac{n^2}{q} + o(n^2). \end{aligned}$$

Here $n = [L(\alpha) : L]$ and error term is $o(n^2)$ as $n \rightarrow \infty$. Taking the sum in equation

(5.11) over all places $v \in M_L$ with norm $\leq X$, we obtain

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

where q runs over all prime powers $\leq X$. Using this in the relative Mahler's inequality

(5.10), 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 $i \rightarrow \infty$ followed by $X \rightarrow \infty$, we obtain Theorem (5.3.2) (a). $\square$

5.6 Applications

We start by recalling that a subset $S \subseteq \overline{\mathbb{Q}}$ has Bogomolov property (B) if

$$\liminf_{\alpha \in S \setminus \mu_{\infty}} h(\alpha) > 0.$$

The exclusion of roots of unity is natural, since they are precisely the algebraic numbers of height zero. The necessity of this exclusion is supported by the extension $\mathbb{Q}^{ab}$, which contains all the roots of unity yet has heights bounded away from 0 on $\mathbb{Q}^{ab} \setminus \mu_\infty$. Among the other known cases of property (B) are $\mathbb{Q}^{tr}$ the maximal totally real extension of $\mathbb{Q}$ and $\mathbb{Q}^{tp}$ the maximal algebraic extension of $\mathbb{Q}$ at which p is totally split. The former has only ± 1 as roots of unity and the latter has only finitely many roots of unity, as implied by Theorem [5.1.1](#).

To distinguish the condition of finiteness of roots of unity from the Bogomolov property, the notion of the strong Bogomolov property has been introduced in the literature. We say a subset $S \subseteq \overline{\mathbb{Q}}$ has **strong Bogomolov property** if it has property (B) and contains only finitely many roots of unity, in other words

$$\liminf_{\alpha \in S} h(\alpha) > 0.$$

It follows immediately from Theorem [5.3.2](#) (a) that an asymptotically positive extension contains finitely many roots of unity. This fact together with Theorem [5.3.2](#) (b) implies the following corollary.

Corollary 5.6.1. *Let $\mathcal{K}/\mathbb{Q}$ be an asymptotically positive extension, then $\mathcal{K}$ has strong Bogomolov property.*

Alternatively, one can see the finiteness of roots of unity in an asymptotically positive extension 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 $p^f \equiv 1 \pmod{n_i}$ for all large enough i , which is a contradiction.

A *discrete norm* on an Abelian group A is a non-negative function $\|\cdot\| : A \rightarrow \mathbb{R}$ which satisfies the triangle inequality, is homogenous with respect to scaling of A

by $\mathbb{Z}$, and is bounded away from 0 on $A \setminus \{e\}$. Here e is the identity element of A . It follows from a result of Zorzitto [73] that a countable abelian group is discretely normed iff it is a free abelian group.

One can ask for which fields $F \subseteq \overline{\mathbb{Q}}$ the multiplicative group $F^\times$ is free modulo torsion part. It follows from the unique factorization property $\mathbb{Z}$ that $\mathbb{Q}^\times/\{\pm 1\}$ is a free abelian group. More generally, for a number field K the unique factorization of ideals and Dirichlet's unit theorem implies that $K^\times$ is free modulo torsion. It is an interesting question to investigate the similar question for infinite algebraic extensions of $\mathbb{Q}$. In 1953, Iwasawa [36] proved that $(K^{ab})^\times$ is free modulo torsion. Some years later Schenkman [57] showed that $(\mathbb{Q}^{(d)})^\times$ is free modulo torsion for all positive integers d , where $\mathbb{Q}^{(d)}$ is the compositum of all number fields of degree at most d .

Denote by $(F^\times)_{\text{tor}}$ the torsion subgroup of $F^\times$. It follows from the properties of Weil height that for any field F , the function $h : F^\times/(F^\times)_{\text{tor}} \rightarrow [0, \infty)$ is a norm. Moreover, if F satisfy property (B) then h is a discrete norm. As a consequence of Theorem 5.3.2 we have the following result.

Corollary 5.6.2. *Let $\mathcal{K}/\mathbb{Q}$ be an asymptotically positive extension, then $\mathcal{K}^\times/(\mathcal{K}^\times)_{\text{tor}}$ is a free abelian group.*

Hence for an asymptotically positive extension $\mathcal{K}$, combining both the corollaries above we deduce that

$$\mathcal{K}^\times \cong (\mathcal{K}^\times)_{\text{tor}} \times \bigoplus_{\mathbb{N}} \mathbb{Z},$$

where $(\mathcal{K}^\times)_{\text{tor}}$ is the finite torsion part.

Chapter 6

Points of small height on Elliptic curves

The study of lower bounds for height on subsets of $\overline{\mathbb{Q}}^\times$ can be viewed from a geometric perspective by identifying $\mathbb{Q}^\times$ with the one-dimensional multiplicative algebraic group $\mathbb{G}_m$, which can be realized as $\mathbb{P}^1 \setminus \{0, \infty\}$ or, equivalently, as the affine curve defined by the set $\{(x, y) \in \mathbb{A}^2 : xy = 1\}$. This viewpoint motivates the investigation of lower bounds for heights of points lying on varieties endowed with additional algebraic structure. The varieties of interest to number theorists in this context are elliptic curves and, more generally, abelian varieties, which are projective algebraic groups with a commutative group law. In this chapter, we study questions concerning lower bounds for heights of points on elliptic curves.

Let E be an elliptic curve defined over a number field K i.e. a smooth, projective, and non-singular curve of dimension one over K with a rational point. It is well known that (see [\[62\]](#), III. 1.) every elliptic curve E/K can be described in the form of a Weierstrass equation

$$y^2 = x^3 + Ax + B,$$

where $A, B \in K$ and $-16(4A^3 + 27B^2) \neq 0$. The quantity $-16(4A^3 + 27B^2)$ is called the discriminant of an elliptic curve and is denoted by Δ . The condition $\Delta \neq 0$ is equivalent to the non-singularity of E .

For an extension L/K , we denote by $E(L)$ the set of points $P = (x, y) \in E(\overline{K})$ such that $x, y \in L$. The set $E(L)$ along with an additional point $\mathcal{O}$, point at infinity, forms an abelian group, called the Mordell–Weil group. One of the major applications of height functions in the context of elliptic curves is the famous **Mordell–Weil theorem** which asserts that if L/K is a finite extension, then the Mordell–Weil group $E(L)$ is a finitely generated abelian group.

One can naively define a height function on an elliptic curve as follows: for a point $P = (x, y) \in E(\overline{K}) \setminus \{\mathcal{O}\}$, set $h(P) := h(x(P))$, where $h(x(P))$ denotes the (logarithmic) Weil height of the x -coordinate of P . This height function is called the *naive height* in the literature. A height function defined in this manner satisfies a finiteness property (Northcott’s theorem) and thus induces a well-founded preorder on $E(L)$ for finite extensions L/K . Recall that the Weil height on the multiplicative group $\overline{\mathbb{Q}}^\times$ characterizes roots of unity as those of height zero and is compatible with the group structure, in the sense that $h(\alpha^n) = |n|h(\alpha)$. In contrast, the above defined height function on an elliptic curve does not enjoy such compatibility with the group law. This issue was resolved independently by Néron and Tate through the introduction of a new notion of height, known as the canonical height or Néron–Tate height.

6.1 Canonical height on elliptic curves

Let E be an elliptic curve defined over a number field K . The canonical height of a point $P \in E(\overline{K}) \setminus \{\mathcal{O}\}$ is defined by the following limit process, due to Tate:

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

where h denotes the naive height. The canonical height $\widehat{h}$ is a quadratic form on $E(\overline{K})$ and satisfies the following properties (see [48] or [39, 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) $\widehat{h}(P_1 + P_2) + \widehat{h}(P_1 - P_2) = 2\widehat{h}(P_1) + 2\widehat{h}(P_2)$.

The canonical height is the unique function satisfying the properties described above. Moreover, there is an analogue of Lehmer's problem for elliptic curves, due to Anderson and Masser [5], which predicts a uniform lower bound for the canonical height of non-torsion points.

Conjecture 6.1.1 (Lehmer's problem). *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 $D =$

$[K(P) : K]$ the degree of the field of definition of P over K . Some classical results towards Lehmer's conjecture are listed below.

$\widehat{h}(P) \geq$	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) [41]
$cD^{-3}(\log D)^{-2}$	none	Masser (1989) [44]
$cD^{-2}(\log D)^{-2}$	j non-integral	Hindry-Silverman (1990) [33]

Table 6.1: Bounds on $\widehat{h}$ for $E(\overline{K})$

6.2 Bogomolov property for elliptic curves

The notion of the Bogomolov property introduced in Chapter 5 has a natural extension to elliptic curves. Analogous to the earlier definition, for an elliptic curve E over K and a subset $S \subseteq \overline{K}$, the group $E(S)$ is said to have the *Bogomolov property* (B) if there exists a positive constant $C(E, K)$ such that $\widehat{h}(P) > C(E, K)$ for all non-torsion points $P \in E(S)$. It is natural to expect that if property (B) holds for an infinite extension $\mathcal{L}/\mathbb{Q}$, it should also hold for $E(\mathcal{L})$. In fact, for most of the known results, this is the case.

Let $\mathcal{L}/\mathbb{Q}$ be an infinite algebraic extension satisfying property (B) with respect to the Weil height. We are interested in the question of whether $E(\mathcal{L})$ satisfies property (B) with respect to the canonical height. The first result of this kind is due to S. Zhang [72], 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 [59] for $\mathbb{Q}^{tr}$. An elliptic curve E is called CM (*complex multiplication*) if it has endomorphisms other than the ones given by multiplication by integers. The j -invariant of an elliptic curve $y^2 = x^3 + Ax + B$ is defined as

$$j_E = -1728 \frac{(4A)^3}{16(4A^3 + 27B^2)}$$

The significance of the j -invariant lies in the fact that two elliptic curves defined over a number field K are isomorphic over $\overline{K}$ if and only if they have the same j -invariant (see [62] III. 1. 4.). It turns out that for an elliptic curve with complex multiplication, j_E is an algebraic integer. In 2002, M. Baker proved property (B) for $E(K^{ab})$ when E is either CM or has non-integral j -invariant. This is the analog of the theorem of Amoroso-Zannier [4], where they showed property (B) for K^{ab} . Moreover, Baker's bound only depends on the j -invariant of E and is effectively computable. Later, Silverman [64] 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.

$\widehat{h}(P) \geq$	Restriction on E	Reference
cD^{-2}	none	Silverman (1981) [60]
$cD^{-1}(\log D)^{-2}$	none	Masser (1989) [44]
$cD^{-2/3}$	j non-integral	Hindry-Silverman (1990) [33]
c	j non-integral or CM	Baker (2003) [6]
c	none	Silverman (2003) [64]

Table 6.2: 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 5.1.1. 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 $\mathbb{Q}(E_{\text{tor}})$ denote the field generated by all torsion points of E in $\overline{\mathbb{Q}}$. In 2013, Habegger [30] showed that both $\mathbb{Q}(E_{\text{tor}})$ and $E(\mathbb{Q}(E_{\text{tor}}))$ 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 $\mathbb{Q}(E_{\text{tor}})$ 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 5.3.2 we know that $\mathcal{L}$ satisfies property (B). The goal of this chapter is to establish property (B) for $E(\mathcal{L})$ for every elliptic curve E as proved in [19]. 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

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

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 the compositum $L \cdot \mathcal{L} = \bigcup_{i=1}^{\infty} LL_i$ is also an asymptotically positive extension. Since E/L has semistable reduction over all

non-archimedean primes, we have, for all primes powers q ,

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

Example. Note that, in the above paragraph, the desired reduction property of the elliptic curve E holds for $L \cdot \mathcal{L}$, 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 $\mathcal{L}' = L \cdot \mathcal{L}$, 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 result, as established in [19, Theorem 7.2], is as follows.

Theorem 6.2.1. *Let E/K be an elliptic curve and $\mathcal{L} = \bigcup_i L_i$ be an infinite algebraic extension of 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 [25] 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 [6.2.1](#) and Lemma [5.2.6](#), we deduce the following.

Corollary 6.2.2. *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 [5.2.6](#) implies that $L \cdot \mathcal{L}$ is also an asymptotically positive extension and

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

for some prime power q . Now, Theorem [6.2.1](#), implies that $E(L \cdot \mathcal{L})$ satisfies property (B) and hence, $E(\mathcal{L})$ satisfies property (B). $\square$

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 6.2.3. *Let $E/\mathbb{Q}$ be an elliptic curve and $\mathcal{L}$ be an infinite algebraic 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 $\sum'_q$ 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 [6.2.3](#) 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 [\[39\]](#) 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 and every non-torsion point $P \in E(K)$,

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

where Δ is the discriminant of E over K .

In the subsequent sections, we develop the necessary tools for the proof of Theorem [6.2.1](#) and conclude the proof in the final section.

6.3 Local heights on elliptic curves

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 $\mathcal{O}$. Similar to Weil height, the canonical height $\widehat{h}$ on E has a decomposition into local height functions $\lambda_v : E(K_v) \rightarrow \mathbb{R}$ (called Néron local heights) for each place v in M_K (see [\[63\]](#) Chapter VI, Theorem 1.1]). For any $P \in E(K) \setminus \{\mathcal{O}\}$, we have

$$(6.1) \quad \widehat{h}(P) = \sum_{v \in M_K} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \lambda_v(P).$$

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.

6.3.1 Archimedean place

Let v be an Archimedean place of K . Then, the completion K_v of K at 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

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

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

$$\lambda_v : E(\mathbb{C}) \setminus \{O\} \rightarrow \mathbb{R}$$

is given by

$$(6.2) \quad \lambda_v(P) = -\frac{1}{2}B_2\left(\frac{\text{Im}(z)}{\text{Im}(\tau)}\right) \log |q_\tau| - \log |1 - u| - \sum_{n \geq 1} \log |(1 - q_\tau^n u)(1 - q_\tau^n u^{-1})|,$$

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. $\mathbb{C}^*/q_\tau^{\mathbb{Z}}$). 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 $\text{Im}(\tau) > 0$. The following proposition gives a lower bound on the discrepancy of archimedean local heights and will be useful in controlling the contribution from the archimedean places in our main theorem.

Proposition 6.3.1. *Let $P_1, P_2, \dots, P_N \in E(\mathbb{C}) \setminus \{O\}$ be N distinct points. Then,*

there is a constant $b(E) > 0$ depending on E such that

$$(6.3) \quad \sum_{\substack{1 \leq i, j \leq N \\ i \neq j}} \lambda_v(P_i - P_j) \geq -\frac{1}{2} N \log N - b(E) N.$$

This proposition follows from a result of Elkies, slightly different proof of which is given in [34 pp. 218] and [40, Chapter VI, Theorem 5.1]. An explicit version using results from Fourier analysis can be found in [7, Proposition 4].

6.3.2 Non-archimedean place

For a non-archimedean place $v \in M_K$, 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 . Let $|\cdot|_v$ be the absolute value corresponding to the place v . Throughout this chapter we fix the associated normalized valuation v on K_v defined as $v(x) = -\log|x|_v$ for all non-zero elements $x \in K_v$. Consider, the minimal Weierstrass equation

$$(6.4) \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

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

$$E_0(K_v) = \{P \in E(K_v) \mid \tilde{E} \text{ is smooth at } \overline{P}\},$$

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 [63, Chap. VI, Theorem 4.1].

Proposition 6.3.2. *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*

$$(6.5) \quad \lambda_v(P) = \frac{1}{2} \max \{v(x(P)^{-1}), 0\} + \frac{1}{12}v(\Delta)$$

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 (6.5) 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 briefly case by case. We refer the reader to [63] Chapter VI, Section 4] for further details. For the minimal Weierstrass equation (6.4), following [62] pp. 42], define

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

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

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

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

$$(6.6) \quad \lambda_v(P) = \frac{1}{2}B_2(\alpha(P))v(\Delta).$$

Good reduction ($v(\Delta) = 0$) :

In this case, we have $E_0(K_v) = E(K_v)$ and $v(\Delta) = 0$. Therefore, by [\[6.5\]](#), we get

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

for all $P \in E(K_v) \setminus \{O\}$. Further, it follows from [\[53\]](#) eq. (20) on p. 357] that

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

Therefore, in the good reduction case

$$(6.7) \quad \lambda_v(P) = \max \left\{ v \left(\frac{x(P)}{y(P)} \right), 0 \right\}.$$

6.3.3 Explicit formula for local height and Tate map

Similar to the uniformization theorem for complex elliptic curves, Tate provides a way to parametrize elliptic curves over non-archimedean complete fields ([63, See V.5]) known as Tate parametrization. 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 (6.2) in the non-archimedean case as follows (see [63, Chapter V, Theorem 4.2]).

Theorem A (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*

$$\lambda_v : E(K_v) \setminus \{O\} \longrightarrow \mathbb{R}$$

is given by the formula

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

(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

$$(6.8) \quad r(P) = \frac{\log |u(P)|_v}{\log |q_E|_v}.$$

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 [6.3.1](#). For a non-archimedean place v of a number field K , we denote by $\mathbb{C}_v$ the algebraic closure of the completion K_v .

Proposition 6.3.3. *Let $P_1, P_2, \dots, P_N \in E(\mathbb{C}_v) \setminus \{O\}$ be N distinct points, where v is a non-archimedean place. Then,*

$$(6.9) \quad \sum_{\substack{1 \leq i, j \leq N \\ i \neq j}} \lambda_v(P_i - P_j) \geq -\frac{N}{12}v(\Delta).$$

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 [6.3.3](#) for the multiplicative reduction case. We need the following result from Fourier analysis for the proof of Proposition [6.3.3](#) (see [\[11\]](#) or [\[63\]](#) Exercise 6.11(b)).

Lemma 6.3.4. *Let $t_1, \dots, t_N \in \mathbb{R}$ 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,

$$\begin{aligned} \sum_{\substack{1 \leq i, j \leq N \\ i \neq j}} B_2(t_i - t_j) &= \frac{1}{2\pi^2} \sum_{n \in \mathbb{Z}, n \neq 0} \frac{1}{n^2} \sum_{\substack{1 \leq i, j \leq N \\ i \neq j}} e^{2\pi i n (t_i - t_j)} \\ &= \frac{1}{2\pi^2} \sum_{n \in \mathbb{Z}, n \neq 0} \frac{1}{n^2} \left(\left| \sum_{1 \leq i \leq N} e^{2\pi i n t_i} \right|^2 - N \right) \\ &\geq -\frac{N}{6}. \end{aligned}$$

□

From Lemma 6.3.4, we can easily deduce Proposition 6.3.3 as follows.

Proof of Proposition 6.3.3 Let K_v be a finite extension of $\mathbb{Q}_p$ such that $P_1, P_2, \dots, P_N \in E(K_v) \setminus \{O\}$, and E/K_v has multiplicative reduction. It follows from Theorem A (ii) and the retraction map (6.8) that

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

Applying Lemma 6.3.4 with $t_i = r(P_i)$, we have the proposition. □

6.4 Lower bound on height for elliptic curves over asymptotically positive extensions

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

$$\begin{aligned} \widehat{h}(Z) &\geq \frac{1}{4N(N-1)} \sum_{\substack{1 \leq i, j \leq N \\ i \neq j}} \widehat{h}(P_i - P_j) \\ (6.10) \quad &\geq \frac{1}{4N(N-1)} \sum_{v \in M_L} \frac{[L_v : \mathbb{Q}_v]}{[L : \mathbb{Q}]} \sum_{\substack{1 \leq i, j \leq N \\ i \neq j}} \lambda_v(P_i - P_j). \end{aligned}$$

Now we begin the proof of Theorem [6.2.1](#). 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 [\(6.10\)](#) 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 [6.2.1](#) Let L/K be a number field contained in $\mathcal{L}$, and let $Z = \{P_1, P_2, \dots, P_n\} \subseteq E(L)$ be a finite set of points as above. For an archimedean place $v \in M_L^\infty$, it follows from [\(6.3\)](#) that

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

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

$$(6.11) \quad \sum_{v \in M_L^\infty} \frac{[L_v : \mathbb{Q}_v]}{[L : \mathbb{Q}]} \sum_{\substack{1 \leq i, j \leq N \\ i \neq j}} \lambda_v(P_i - P_j) \geq -\frac{1}{2} N \log N - b(E)N.$$

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 (6.7), we have

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

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

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

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

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

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

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

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

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

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

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

Hence,

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

Therefore,

$$(6.12) \quad \sum'_{v \in M_L} \frac{[L_v : \mathbb{Q}_p]}{[L : \mathbb{Q}]} \sum_{\substack{1 \leq i, j \leq N \\ i \neq j}} \lambda_v(P_i - P_j) \geq \frac{N^2}{2} \sum_q \frac{G_q(L)}{[L : \mathbb{Q}]} \left(\frac{1}{q+1+2\sqrt{q}} - \frac{1}{N} \right) \log q,$$

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 $k_v = -\text{ord}_v(j_E) \geq 1$. Recall that the retraction homomorphism $r : E(K_v) \rightarrow \mathbb{R}/\mathbb{Z}$ 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 $u \mapsto \frac{\log |u|_v}{\log |q_E|_v}$. Note that $\text{Im}(r) = \langle 1/k_v \rangle \subseteq \mathbb{R}/\mathbb{Z}$, 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 [A](#) (ii), we obtain

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

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

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

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,

$$\begin{aligned} \sum_{v \in M_L}'' \frac{[L_v : \mathbb{Q}_p]}{[L : \mathbb{Q}]} \sum_{\substack{1 \leq i, j \leq N \\ i \neq j}} \lambda_v(P_i - P_j) &\geq \sum_{v \in M_L}'' \frac{[L_v : \mathbb{Q}_p]}{[L : \mathbb{Q}]} \left(\frac{\log p}{12 k_v} N(N-1) + O(N) \right) \\ &\geq c_E \sum_{v \in M_L}'' \frac{[L_v : \mathbb{Q}_p]}{[L : \mathbb{Q}]} \left(\frac{\log p}{12 e_v} N(N-1) + O(N) \right) \\ (6.13) \quad &\geq c_E N(N-1) \sum_q \frac{B_q(L)}{[L : \mathbb{Q}]} \frac{\log q}{12} + O(N), \end{aligned}$$

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 (6.11), (6.12) and (6.13) in (6.10), we obtain

$$\begin{aligned} \widehat{h}(Z) &\geq \frac{1}{4N(N-1)} \left(-\frac{1}{2} N \log N - b(E)N + \frac{N^2}{2} \sum_q \frac{G_q(L)}{[L : \mathbb{Q}]} \left(\frac{1}{q+1+2\sqrt{q}} - \frac{1}{N} \right) \log q \right. \\ (6.14) \quad &\quad \left. + N(N-1) \sum_q \frac{B_q(L)}{[L : \mathbb{Q}]} \frac{\log q}{12} + O(N) \right). \end{aligned}$$

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

Taking N large, (6.14) 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. $\square$

6.5 Concluding remarks

The problem of obtaining lower bound on canonical height can be formulated in a more general setting of abelian varieties. An abelian variety over a number field K is a projective group variety such that the morphisms corresponding to the group operations are defined over K . Elliptic curves are precisely abelian varieties of dimension one. A very ample line bundle $\mathfrak{L}$ on an abelian variety A allows one to realize A as a subvariety of projective space. Consequently, the Weil height on A with respect to $\mathfrak{L}$ is defined using the corresponding projective embedding. Applying Tate's limiting process to this Weil height then yields the canonical height $\hat{h}_{\mathfrak{L}}$. Thus, a natural question is to ask for which infinite extensions $\mathcal{K}/K$, the group of points $A(\mathcal{K})$ has the Bogomolov property with respect to $\hat{h}_{\mathfrak{L}}$.

It is known that for an abelian variety $A/\mathbb{Q}$, the group of totally real points $A(\mathbb{Q}^{tr})$ satisfies the Bogomolov property ([72]). For a number field K and an abelian variety A/K , the group of abelian points $A(K^{ab})$ also satisfies the Bogomolov property ([9]). In this chapter, we have seen that for an elliptic curve $E/\mathbb{Q}$, the set $E(\mathbb{Q}^{tp})$ satisfies property (B) with respect to the canonical height. Hence one can ask the following question in the context of abelian varieties.

Question. Let $A/\mathbb{Q}$ be an abelian variety and $\mathfrak{L}$ be a very ample line bundle on A . Does $A(\mathbb{Q}^{tp})$ satisfy property (B) with respect to $\hat{h}_{\mathfrak{L}}$?

When A has bad reduction at a prime p , a tropical equidistribution theorem due to Gubler [29] answers the above question in affirmative. On the other hand, when A has good reduction at p , a non-archimedean equidistribution theorem of Chambert-Loir's [14] establishes property (B) for a dense Zariski open subset of $A(\mathbb{Q}^{tp})$. Despite these progress, it remains an open problem whether $A(\mathbb{Q}^{tp})$ satisfies the Bogomolov property in the good reduction case. In fact, this question was explicitly raised by Vesselin Dimitrov (<https://mathoverflow.net/questions/123096>) around 2013.

We address the above question in a recent work [37] and establish Bogomolov property for $A(\mathbb{Q}^{tp})$ for all but finitely many primes p . However, proving this for all primes remains an open problem. More generally, one could also consider the above question for semi-abelian varieties and for points over asymptotically positive extensions. This opens the door to several promising directions for future research.

Bibliography

- [1] F. Amoroso, S. David, Le Problème de Lehmer en Dimension Supérieure, *J. Reine Angew. Math.*, **513**, pp. 145-179, (1999).
- [2] F. Amoroso, S. David, U. Zannier, On fields with Property (B), *Proc. Amer. Math. Soc.*, **142**, no. 6, 1893–1910, (2014).
- [3] F. Amoroso, R. Dvornicich, A Lower Bound for the Height in Abelian Extensions, *Journal of Number Theory*, **80**, pp. 260-272, (2000).
- [4] F. Amoroso, U. Zannier, A relative Dobrowolski lower bound over abelian extensions, *Ann. Sc. Norm. Super. Pisa Cl. Sci.*, **29(4)**, pp. 711–727, (2000).
- [5] M. Anderson, D. Masser, Lower bound for heights on elliptic curves, *Math. Z.*, **174**, pp. 23–34, (1980).
- [6] M. Baker, Lower bounds for the canonical height on elliptic curve over abelian extensions, *IMRN*, **29**, pp. 1571-1582, (2003).
- [7] M. Baker, C. Petsche, Global discrepancy and small points on elliptic curves, *Int. Math. Res. Not. IMRN*, **61**, pp. 3791-3834, (2005).
- [8] M. Baker, R. Rumely, Equidistribution of small points, rational dynamics, and potential theory, *Ann. Inst. Fourier*, **56**, no.3, pp. 625–688 (2006).
- [9] M. H. Baker, J.H. Silverman, A lower bound for the canonical height on abelian varieties over abelian extensions, *Math. Res. Lett.*, **11**, pp. 377-396, (2004).

- [10] Y. Bilu, Limit distribution of small points on algebraic tori, *Duke Math. J.*, **89**(3), pp. 465-476, (1997).
- [11] P. E. Blanksby, H. L. Montgomery, Algebraic integers near the unit circle, *Acta Arith.*, **18**, pp. 355-369, (1971).
- [12] E. Bombieri, U. Zannier, A note on heights in certain infinite extensions of $\mathbb{Q}$, *Rendiconti Lincei Matematica E Applicazioni*, series 9, **12**, no. 1, pp. 5-14, (2001).
- [13] R. Breusch, On the distribution of the roots of a polynomial with integral coefficients, *Proc. Amer. Math. Soc.*, **2**, 939-941, (1951).
- [14] A. Chambert-Loir, Mesures et Équidistribution sur les espaces de Berkovich, *J. Reine Angew. Math.*, **595**, pp. 215–235, (2006).
- [15] S. Checcoli, A. Fehm, On the Northcott property and local degrees, *Proc. Amer. Math. Soc.*, **149**, pp. 2403–2414, (2021).
- [16] V. Dimitrov, A proof of the Schinzel-Zassenhaus conjecture on polynomials, *arXiv:1912.12545 [math.NT]*, (2019).
- [17] V. Dimitrov, <https://mathoverflow.net/questions/123096> (2013).
- [18] A. B. Dixit, S. Kala, Lower bound on height of algebraic numbers and low lying zeros of the Dedekind zeta-function, *arXiv:2309.15872 [math.NT]*, (2023).
- [19] A. B. Dixit, S. Kala, Bogomolov property for certain infinite non-Galois extensions, to appear in *Ann. Scuola Norm. Sup. Pisa Cl. Sci.*, (2026).
- [20] A. B. Dixit, S. Kala, A p -adic criterion for Lehmer’s conjecture, <https://doi.org/10.1142/S1793042126500855>, to appear in *Int. J. Number Theory*, (2026).

- [21] E. Dobrowolski, On a question of Lehmer and the number of irreducible factors of a polynomial, *Acta Arithmetica*, **34**, pp. 391-401, (1979).
- [22] P. Erdős, P. Turán, On the distribution of roots of polynomials, *Annals of Math.*, **51**, pp. 105-119, (1950).
- [23] C. Favre, J. Rivera-Letelier, Équidistribution quantitative des points de petite hauteur sur la droite projective *Math. Ann.*, **335**(2), pp. 311–361, (2006).
- [24] C. Favre, J. Rivera-Letelier, Corrigendum to: Équidistribution quantitative des points de petite hauteur sur la droite projective [*Math. Ann.*, **335**(2), pp. 311–361, (2006)], *Math. Ann.*, **339**(4), pp. 799–801, (2007).
- [25] P. Fili, Z. Miner, Equidistribution and the heights of totally real and totally p-adic numbers, *Acta Arith.*, **170**, no. 1, 15–25, (2015).
- [26] P. Fili and C. Petsche, Energy integrals over local fields and global height bounds, *Int. Math. Res. Not. IMRN*, **5**, pp. 1278–1294, (2015).
- [27] P. Fili, I. Pritsker, Height bounds for algebraic numbers satisfying splitting conditions, *J. Number Theory*, **175**, pp. 250-264, (2017).
- [28] J. Garza, On the height of algebraic numbers with real conjugates, *Acta Arith.*, **128**, no. 4, 385–389, (2007).
- [29] W. Gubler, The Bogomolov conjecture for totally degenerate abelian varieties, *Invent. math.*, **169**, pp. 377–400, (2007).
- [30] P. Habegger, Small height and infinite nonabelian extensions, *Duke Math. J.*, **162**(11), pp. 2027–2076, (2013).
- [31] E. Hasanlizada, Q. Shen, P. Wong, Counting zeros of Dedekind zeta functions, *Mathematics of Computation*, **91**, pp. 277-293, (2021).

- [32] M. Hindry, J. H. Silverman, The canonical height and integral points on elliptic curves, *Invent. Math.*, **93**, pp. 419-450, (1988).
- [33] M. Hindry, J. H. Silverman, On Lehmer's conjecture for elliptic curves, in *Séminaire de Théorie des Nombres, Paris (1988-1989)*, *Progr. Math.*, **91**, Birkhäuser Boston, Boston, MA, pp. 103-116, (1990).
- [34] P. Hriljac, Splitting fields of principal homogeneous spaces, *Lecture Notes in Math.*, **1240**, Number theory (New York), 1984-1985, pp. 214-229, (1987).
- [35] H. Iwaniec and E. Kowalski, Analytic number theory, *Amer. Math. Soc. Colloq. Publ.*, **53**, (2004).
- [36] K. Iwasawa, A note on Kummer extensions, *J. Math. Soc. Japan*, **5**, pp. 253-262, (1953).
- [37] S. Kala, Lower bound for the canonical on Abelian varieties over totally p -adic extensions, *arXiv:2511.17933 [math.NT]*, (2026).
- [38] L. Kronecker, Zwei Sätze über Gleichungen mit Ganzzahligen Coefficienten, *J. Reine Angew. Math.*, **53**, pp. 173–175, (1857).
- [39] S. Lang, Elliptic Curves : Diophantine Analysis, *Grundlehren der Mathematischen Wissenschaften*, **231**, Springer-Verlag, Berlin, (1978).
- [40] S. Lang, Introduction to Arakelov theory, *Springer-Verlag, New York*, (1988).
- [41] M. Laurent, Minoration de la hauteur de Néron–Tate, *Séminaire de théorie des nombres de Paris 1981-1982*, *Progr. Math.*, Birkhäuser, Boston-Basel-Stuttgart, pp. 137-152, (1983).
- [42] D. H. Lehmer, Factorization of certain cyclotomic functions, *Ann. Math. 2.*, **34**, (3), 461–479, (1933).

- [43] K. Mahler, An inequality for the discriminant of a polynomial, *Michigan Math. J.*, **11**, pp. 257-262, (1964).
- [44] D. Masser, Counting points of small height on elliptic curves, *Bull. Soc. Math. France*, **117**, pp. 247-265, (1989).
- [45] D. Masser, Auxiliary polynomials in number theory, *Cambridge Tracts in Math.*, **207**, Cambridge University Press, Cambridge, 2016.
- [46] M. Mignotte, Entiers Algébriques dont les Conjugués sont Proches du Cercle Unité, *Séminaire Delange-Pisot-Poitou, 19e année: 1977/78, Théorie des Nombres, Fasc. 2*, Exp. No. **39**, pp. 1-6, Paris, (1978).
- [47] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, *Springer Monographs in Mathematics*, Springer-Verlag Berlin, (2004).
- [48] A. Néron, Quasi-fonctions et Hauteurs sur les Variétés Abéliennes. *Ann. of Math. (2)*, **82**, pp. 249–331, (1965).
- [49] J. Neukirch, Algebraic number theory, *Grundlehren der mathematischen Wissenschaften*, Springer-Verlag Berlin, (1999).
- [50] D. G. Northcott, An inequality on the theory of arithmetic on algebraic varieties, *Proceedings of Cambridge Philosophical Soc.*, **45**, pp. 502-509, (1949).
- [51] A. M. Odlyzko, Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results, *Séminaire de Théorie des Nombres de Bordeaux*, **2**, no. 1, p. 119-141, (1990).
- [52] C. Petsche, A quantitative version of Bilu’s equidistribution theorem, *Int. J. Number Theory*, **1**, no. 2, pp. 281–291, (2005).
- [53] C. Petsche, Nonarchimedean equidistribution on elliptic curves with global applications, *Pacific J. Math.*, **242**, no. 2, pp. 345–375, (2009).

- [54] G. Poitou, Sur les petits discriminants, Séminaire Delange-Pisot-Poitou, 18e année:1976/77, Théorie des nombres, Fasc. 1, Exp. No. 6, 18, Secrétariat Math., Paris, 1977.
- [55] L. Pottmeyer, Small totally p -adic algebraic numbers, *Int. J. Number theory*, **14**, no. 10, pp. 2687-2697, (2018).
- [56] U. Rausch, On a theorem of Dobrowolski about the product of conjugate numbers, *Colloquium Mathematicum*, **50**, Issue. 1, pp. 137-142, (1985).
- [57] E. Schenkman, On the multiplicative group of a field, *Arch. Math. (Basel)*, **15**, pp. 282-285, (1964).
- [58] A. Schinzel, H. Zassenhaus, A refinement of two theorems of Kronecker, *Michigan Math J.*, **12**, pp. 81-85, (1965).
- [59] A. Schinzel, On the product of the conjugates outside the unit circle of an algebraic number, *Acta Arith.*, **24**, 4, pp. 385-399, (1973).
- [60] J. H. Silverman, Lower bound for the canonical height on elliptic curves, *Duke Math. J.*, **48**(3), pp. 633-648, (1981).
- [61] J. H. Silverman, Lower bounds for height functions, *Duke Math. J.*, **51**(2), pp. 395 - 403, (1984).
- [62] J. H. Silverman, The arithmetic of elliptic curves, *Grad. Texts in Math.*, Springer, GTM **106**, (1986).
- [63] J. H. Silverman, Advanced topics in the arithmetic of elliptic curves, *Grad. Texts in Math.*, Springer, **151**, (1994).
- [64] J. H. Silverman, A lower bound for the canonical height on elliptic curves over abelian extensions, *J. Number Theory*, **104**, pp. 353-372, (2004).

- [65] C. J. Smyth, On the product of the conjugates outside the unit circle of an algebraic integer, *Bulletin of London Mathematical Society*, **3**, no. 2, pp. 169-175, (1971).
- [66] C. J. Smyth, Mahler measure of one-variable polynomials: a survey, Conference proceedings, University of Bristol, 3-7 April 2006, LMS Lecture Note Series **352**, Cambridge University Press, Cambridge, pp. 322-349, (2008).
- [67] H. M. Stark, Some effective cases of the Brauer-Siegel theorem, *Invent. Math.*, **23**, pp. 135-152, (1974).
- [68] L. Szpiro, E. Ullmo, and S. W. Zhang, Équirépartition des petits points, *Invent. Math.*, **127**, no. 2, pp. 337-347, (1997).
- [69] M. A. Tsfasman, S. G. Vlăduţ, Infinite global fields and the generalized Brauer-Siegel theorem, *Mosc. Math. J.*, **2**, Num. 2, pp. 329-402, (2002).
- [70] J. Verger-Gaugry, A Survey on the Conjecture of Lehmer and the Conjecture of Schinzel-Zassenhaus, HAL-02315014, (2019).
- [71] P. Voutier, An effective lower bound for the height of algebraic numbers, *Acta Arith.*, **74**, 81-95, (1996).
- [72] S. Zhang, Equidistribution of small points on abelian varieties, *Ann. of Math.* (2), **147**, No.1, pp. 159-165, (1998).
- [73] F. Zorzitto, Discretely normed abelian groups, *Aequationes Math.*, **29**, no. 2-3, pp. 172-174, (1985).