LEHMER'S PROBLEM AND ALGEBRAIC POINTS OF WEIERSTRASS SIGMA FUNCTIONS

By

Gorekh Prasad Sena

Enrolment No. MATH11201704005

National Institute of Science Education and Research, Bhubaneswar

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

April, 2023

Homi Bhaba 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 **Gorekh Prasad Sena** entitled **"Lehmer's problem and algebraic points of Weierstrass sigma functions"** and recommend that it may be accepted as fulfilling the thesis requirement for the award of Degree of Doctor of Philosophy.

Chairman - Prof. Brundaban Sahu	31.08.2023
Guide / Convener - Dr. K. Senthil Kumar	31/08/2023
Co-guide - None	
Examiner - Prof. Purusottam Rath	
Member 1 - Dr. Binod Kumar Sahoo	
Member 2 - Dr. Jaban Meher	31/08/23
Member 3 - Prof. G. Kasi Viswanadham	31/08/23

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

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

Date : 31/08/23

Place : NISER, JATNI

Signature
Co-guide (if any)

31/08/2023
Signature
Guide

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 judgment the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

Gorekh Prasad Sena

Gorekh Prasad Sena

DECLARATION

I hereby declare that I am the sole author of this thesis in partial fulfillment of the requirements for a postgraduate degree from National Institute of Science Education and Research (NISER). I authorize NISER to lend this thesis to other institutions or individuals for the purpose of scholarly research.

Gorekh Prasad Sena

Gorekh Prasad Sena

List of Publications arising from the thesis

Journal

1. Gorekh Prasad Sena and K. Senthil Kumar, *On the number of algebraic points on the graph of the Weierstrass sigma functions*. Accepted in **Bull. Aust. Math. Soc.**

2. Gorekh Prasad Sena and K. Senthil Kumar, *Lehmer's problem and splitting of rational primes in number fields*. **Acta Math. Hungar.**, 169 (2) (2023), 349-358.

3. Gorekh Prasad Sena, *Height of algebraic units under splitting conditions*. Accepted in **Proc. Indian Acad. Sci. Math. Sci.**

Preprint

1. Gorekh Prasad Sena and K. Senthil Kumar, *Lehmer's problem and Reciprocal numbers*. (Submitted).

Gorekh Prasad Sena
Gorekh Prasad Sena

Dedicated

To

BABA and MAA

ACKNOWLEDGEMENTS

First and foremost, I would like to convey my sincere gratitude to my advisor, Dr. K. Senthil Kumar, for exposing me to various research topics, the result of which is this thesis. I am also grateful for his wise advice and his patience in rectifying my many grammatical mistakes during my Ph.D career.

I thank the members of my doctoral committee, Prof. B. Sahu, Dr. J. Meher, Dr. B. K. Sahoo and Dr. G. K. Viswanadham for giving critical suggestions periodically over the years. I also thank the faculty members of NISER for sharing their ideas and knowledge during various periods of my Ph.D.

During my M.Sc, I had the privilege of attending courses taught by Prof. R. Tandon, Prof. V. Kannan and Dr. T. Sengupta. Their teaching has a significant impact on me and tremendously motivates my studies. In future, I only wish to teach like them.

I thank Veekesh bhaiya with whom I had many fruitful discussions regarding various research problems. I also thank Diptesh, Mrityunjay, Nilkantha bhaiya, Rajeeb bhai, Shivansh with whom I had many fun time at NISER.

Last, but not the least, without the support of my friends, Gopi and Panda, this journey of my Ph.D would not be this much smoother.

ABSTRACT

Mahler measure of an algebraic integer α, denoted by $M(\alpha)$, is the product of all the conjugates of α that lies outside the unit circle of the complex plane. One of the longstanding open problem related to the Mahler measure is the *Lehmer problem* which asks for an absolute constant $c > 1$ such that $M(\alpha) \geq c$ for any nonzero algebraic integer α which is not a root of unity. Though this problem has been verified for various classes of algebraic integers, including the class of nonreciprocal algebraic integers, the general case remains open. In this thesis, we study the relationship between the lower bounds of the Mahler measure and the splitting of primes in number fields. As a consequence of our results, we answer the Lehmer problem affirmatively for various classes of algebraic integers. For example, one of our results imply that if all the residual degrees of primes in $\mathcal{O}_{\mathbb{Q}(\alpha)}$ which lie above 2 are any fixed positive integer n, then either $M(\alpha) = 1$ or $M(\alpha) \geq 2^{\frac{1}{4(2^n-1)}}$. In another direction, we obtain a lower bound for the Mahler measure for a class of reciprocal algebraic integers, which improves the best unconditional lower bound given by Dobrowolski for this class. We also study in this thesis some upper bounds for the number of algebraic points of bounded degrees and bounded Mahler measures on the Weierstrass sigma function $\sigma(z)$. Recently, Boxall *et al.* gave such bounds for the number of algebraic points on $\sigma(z)$ under some conditions on the imaginary part of the quotient $\tau = \omega_2/\omega_1$ of an order $\mathbb{Z}$-basis $\{\omega_1, \omega_2\}$ for the lattice associated to $\sigma(z)$. Our results are based on the quasi-periods of the Weierstrass zeta function $\zeta(z)$ associated to $\sigma(z)$.

Contents

References 67

Summary

A longstanding open problem related to the Mahler measure asks for an absolute constant $c > 1$ such that for any nonzero algebraic integer α which is not a root of unity, the Mahler measure of α, denoted by $M(\alpha)$, is at least c. This problem is due to Lehmer, and is commonly called the Lehmer problem. Though this problem is still open, it has been solved for various classes of algebraic integers. For example, Smyth [43] proved it for the class of nonreciprocal algebraic integers. In [4], Amoroso and Dvornicich proved it for elements which lie in an abelian extension of $\mathbb{Q}$. In [2], Amoroso and David proved it for the generators of any Galois extension. In [12], Borwein, Dobrowolski and Mossinghoff proved it for the class of algebraic integers whose minimal polynomial over $\mathbb{Q}$ having odd integers. The best unconditional lower bound for the Mahler measure, upto a constant, is due to Dobrowolski [17]. In this thesis, we obtain a lower bound for the Mahler measure for a class of reciprocal algebraic integers, which improves the best unconditional lower bound given by Dobrowolski for this class. In another direction, we study the relationship between the lower bounds of the Mahler measure and the splitting of primes in number fields. Consequently, we answer Lehmer's problem affirmatively for various classes of algebraic integers. For example, we prove that if all the residual degrees of primes in $\mathcal{O}_{\mathbb{Q}(\alpha)}$ which lie above 2 are any fixed positive integer n, then either $M(\alpha) = 1$ or $M(\alpha) \geq 2^{\frac{1}{4(2^n-1)}}$.

The problem of counting integral points on graphs of different kinds of functions can be traced back to the work of Jarnik [24]. In 2011, Masser [30] proved the following upper bound for the Riemann zeta function: For any integer $H \geq 3$, the number of rational q with $q \in (2,3)$ such that both q and $\zeta(q)$ have denominator at most H is at most $C\left(\log H / \log\log H\right)^2$, for some effective absolute constant $C > 0$. In the same paper, Masser suggested to extend his method to other classes of functions. Based on his sug-

gestion, several mathematicians have extended his method to various classes of functions. For example, Jones and Thomas [25] gave a bound for the algebraic points of bounded degrees and bounded Weil heights on the graph of Weierstrass zeta function. Boxall and Jones [14] gave such bounds for the entire functions with finite order and positive lower order. Recently, Boxall, Chalebgwa and Jones [13] proved various such upper bounds for the Weierstrass sigma function $\sigma_\Omega(z)$ under some conditions on the imaginary part of the quotient $\tau = \omega_2/\omega_1$ of an $\mathbb{Z}$-basis $\{\omega_1, \omega_2\}$ for the lattice Ω associated to the Weierstrass sigma function. In this thesis, we extend the main results of [13] under the assumption that $\rho = \eta_2/\eta_1$ is a nonzero real number, where $\eta_i = \zeta_\Omega(\omega_i/2)$ is the quasi-period of the Weierstrass zeta function $\zeta_\Omega(z)$ associated to ω_i $(i = 1, 2)$. With this assumption, we are able to count the algebraic points of $\sigma_\Omega(z)$ of bounded degrees and bounded Weil heights in some unbounded subset of $\mathbb{C}$ under three conditions: (i) lattice points are algebraic; (ii) invariants associated to lattice are algebraic; (iii) algebraic points are away from lattice points.

Chapter 1

Introduction to Lehmer's problem

In this chapter, we give an overview on the state of the art of Lehmer's problem.

1.1 History of Lehmer's problem

We start with the following definition.

Definition 1.1. For a nonzero polynomial $f(x) = a_d x^d + \cdots + a_0 \in \mathbb{C}[x]$, its *Mahler measure* is defined by

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

where $\alpha_1, \ldots, \alpha_d$ are the roots of f in $\mathbb{C}$. Mahler measure of an algebraic number α, denoted by $M(\alpha)$, is defined by the Mahler measure of the minimal polynomial of α over $\mathbb{Z}$.

In the above definition, an empty product is assumed to be 1.

Definition 1.2. For an algebraic number α of degree d over $\mathbb{Q}$, its *Weil height*, also known as *absolute logarithmic height*, is defined by

$$h(\alpha) = \frac{1}{d} \log M(\alpha). \tag{1.1}$$

In 1933, D. H. Lehmer [28] gave a factorization method to produce large prime numbers. His method was to define a sequence

$$\triangle_n(f) = \prod_{i=1}^{d} (\alpha_i^n - 1), \ (n \in \mathbb{N})$$

where f is a monic integer polynomial with $\alpha_1, \ldots, \alpha_d$ are its roots. By choosing the polynomial $f(x) = x - 2$, we get $\triangle_n(f) = 2^n - 1$, which are Mersenne numbers. Note that

whether or not there are infinitely many primes of the form $2^n - 1$ is an open problem. So, the motivation to define such a sequence might be to generalize the notion of Mersenne numbers. Lehmer was able to produce some large prime number as values of $\triangle_n(f)$ for suitable f and n. For example, if $f(x) = x^3 - x - 1$, then Lehmer showed that

$$\triangle_{113}(f) = 63088004325217$$

and

$$\triangle_{127}(f) = 3233514251032733$$

are prime numbers. He measured the growth of this sequence and observed that the sequence $(\triangle_n(f))_{n\in\mathbb{N}}$ is more likely to produce large prime numbers if it does not grow too quickly. He proved the following.

Theorem 1.3 ([28]). *Let $f(x)$ be a monic integer polynomial with no roots on the unit circle. Then*

$$\lim_{n\to\infty} \left| \frac{\triangle_{n+1}(f)}{\triangle_n(f)} \right| = \prod_{i=1}^{d} \max\{1, |\alpha_i|\},$$

where $\alpha_1, \ldots, \alpha_d$ are the roots of f.

Motivated by the above theorem, Lehmer searched for algebraic integers with small Mahler measure. He found that the polynomial

$$x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$$

has Mahler measure $1.176\ldots$ and he was not able to find any other polynomial whose Mahler measure smaller than $1.176\ldots$. At this juncture, he asked the following question.

Lehmer's problem. *Does there exists a constant $c > 1$ such that $M(\alpha) \geq c$, for any nonzero algebraic integer α which is not a root of unity?*

In terms of Weil height, it reads as follows.

Lehmer's problem (In terms of Weil height). *Does there exists a constant $c > 0$ such that $h(\alpha) \geq c/d$, for any nonzero algebraic integer α of degree d which is not a root of unity?*

Till now, we are not able to find any algebraic integer whose Mahler measure is less than $1.176\ldots$. So, Lehmer's problem remains open.

1.2 Properties of Mahler measure

Theorem 1.4. *For any fixed $D \geq 1$ and $M \geq 1$, the set*

$$S(M, D) = \left\{\alpha \in \overline{\mathbb{Q}} : [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq D \text{ and } M(\alpha) \leq M\right\}$$

is finite, where $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$.

Proof. For simplicity, let $S = S(M, D)$. Let $\alpha \in S$ and $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ be the minimal polynomial of α over $\mathbb{Z}$. Let $\alpha_1 = \alpha, \ldots, \alpha_d$ be the roots of $f(x)$ in $\mathbb{C}$. The factorization of $f(x)$ in terms of its roots gives

$$\frac{a_{d-k}}{a_d} = (-1)^k \sum_{1 \leq i_1 < \cdots < i_k \leq d} \alpha_{i_1} \cdots \alpha_{i_k}, \quad (k = 1, \ldots, d).$$

So, we obtain $|a_{d-k}| \leq \binom{d}{k} M(\alpha)$. Also, $|a_d| \leq M(\alpha) \leq M$. Since $d \leq D$ and $M(\alpha) \leq M$, there are only finitely many possible choices for the minimal polynomials of elements of S. Therefore, the set S is finite. □

The following result is due to Kronecker [26].

Theorem 1.5. *Let α be a nonzero algebraic integer. Then $M(\alpha) = 1$ if and only if α is a root of unity.*

Proof. Let $M(\alpha) = 1$. Then $M(\alpha^n) = 1$ for all $n \in \mathbb{N}$. Since for all $n \in \mathbb{N}$, $[\mathbb{Q}(\alpha^n) : \mathbb{Q}] \leq [\mathbb{Q}(\alpha) : \mathbb{Q}]$ and $M(\alpha^n) = 1$, by Theorem 1.4, the sequence $(\alpha^n)_{n\in\mathbb{N}}$ contains only

finitely many elements. So $\alpha^i = \alpha^j$, for some $i \neq j$. Thus α is a root of unity. Conversely, if α is a root of unity, then all the conjugates of α have absolute value equal to 1. Thus $M(\alpha) = 1$. □

Next, we prove an integral representation for the Mahler measure. First, we start with the following.

Proposition 1.6. *For $0 \neq f(x) \in \mathbb{C}[x]$, put*

$$M^*(f) = \exp\left(\int_0^1 \log\left|f(e^{2\pi it})\right| dt\right).$$

Then for any $f, g \in \mathbb{C}[x]$ and $\alpha \in \mathbb{C} \setminus \{0\}$, we have

(i) $M^*(fg) = M^*(f)M^*(g)$.

(ii) $M^*(\alpha) = |\alpha|$.

(iii) $M^*(x - \alpha) = \max\{1, |\alpha|\}$.

Proof. First two relations follows from the definition of M^*. Third relation follows from the fact that the function $\log|z - \alpha|$ (*resp.* $\log|1 - z\overline{\alpha}|$) is harmonic in the unit disk if $|\alpha| > 1$ (*resp.* $|\alpha| < 1$). Finally, the case $|\alpha| = 1$ is deduced by continuity. For more details, see [9, p. 23]. □

From Proposition 1.6, both M and M^* multiplicative on $\mathbb{Z}[x] \setminus \{0\}$ and they agree on polynomials of degree ≤ 1. Hence, we obtain the following.

Theorem 1.7. *Let α be a nonzero algebraic number. Then*

$$M(\alpha) = \exp\left(\int_0^1 \log\left|f(e^{2\pi it})\right| dt\right),$$

where f is the minimal polynomial of α over $\mathbb{Z}$.

1.3 Unconditional lower bounds

In 1965, Schinzel and Zaassenhaus gave the following first unconditional lower bound in the direction of Lehmer's problem.

Theorem 1.8 ([41]). *Let α be an algebraic integer of degree d, which is neither zero nor a root of unity. Then there exists a constant $c > 0$, which is independent of α, such that*

$$M(\alpha) > 1 + \frac{c}{2^d}. \tag{1.2}$$

In 1971, using methods from Fourier analysis, Blanksby and Montgomery drastically improved the lower bound (1.2) and proved the following.

Theorem 1.9 ([8]). *If α is an algebraic integer of degree d, which is neither zero nor a root of unity, then*

$$M(\alpha) > 1 + \frac{1}{52d\log(6d)}. \tag{1.3}$$

In 1978, using techniques from transcendental number theory, Stewart obtained the following lower bound.

Theorem 1.10 ([44]). *If α is an algebraic integer of degree $d > 1$, which is neither zero nor a root of unity, then*

$$M(\alpha) > 1 + \frac{1}{10^4 d\log d}. \tag{1.4}$$

Though the lower bound (1.4) is slightly weaker than the lower bound (1.3), the method of the proof is entirely different. Stimulated by the method of Stewart, Dobrowolski successfully extended his argument to prove the following lower bound.

Theorem 1.11 ([17]). *If α is an algebraic integer of degree $d > 2$, which is neither zero nor a root of unity, then*

$$M(\alpha) \geq 1 + \frac{1}{1200}\left(\frac{\log\log d}{\log d}\right)^3. \tag{1.5}$$

Later, Voutier [45] improved the lower bound (1.5) by a constant, which is the best unconditional lower bound in the direction of Lehmer's problem till now.

Theorem 1.12 ([45]). *If α is an algebraic integer of degree $d > 2$ which is neither zero nor a root of unity, then*

$$M(\alpha) \geq 1 + \frac{1}{4}\left(\frac{\log\log d}{\log d}\right)^3.$$

1.4 Conditional lower bounds

Though, the Lehmer's problem remains open, it has been solved for various classes of algebraic integers. Recall that an algebraic number α is said to be reciprocal if α^{-1} is also a conjugate of α over $\mathbb{Q}$. Otherwise, it is called nonreciprocal. In 1951, Breusch [15] proved the following lower bound of the Mahler measure for the class of nonreciprocal algebraic integers.

Theorem 1.13 ([15]). *Let α be an algebraic integer which is neither zero nor a root of unity. Suppose α is nonreciprocal. Then*

$$M(\alpha) \geq M(x^3 - x^2 - 1/4) = 1.1796\ldots. \tag{1.6}$$

In [43], Smyth improved the lower bound (1.6), which is the best possible lower bound for all nonreciprocal algebraic integers.

Theorem 1.14 ([43]). *If α is a nonreciprocal algebraic integer which is neither zero nor a root of unity, then $M(\alpha) \geq M(x^3 - x - 1) = 1.3247\ldots$.*

In 1999, Amoroso and David [2] proved the following lower bound for the generators of Galois extensions.

Theorem 1.15 ([2]). *There exists an absolute constant $c > 1$ such that the following holds: Let α be an algebraic integer which is neither zero nor a root of unity. Suppose $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois. Then $M(\alpha) > c$.*

In 2016, Amoroso and Masser [5] proved the following better result for the generator of the Galois extension.

Theorem 1.16 ([5]). *Let α be an algebraic integer which is neither zero nor a root of unity. For any $\varepsilon > 0$, there exists $c(\varepsilon) > 0$ such that if $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois, then $h(\alpha) \geq \frac{c(\varepsilon)}{d^{\varepsilon}}$.*

Amoroso and Dvornicich [4] proved the following strong result by putting some additional conditions on the Galois extension.

Theorem 1.17 ([4]). *Assume α is an algebraic integer which lies in an abelian extension of $\mathbb{Q}$ and is neither zero nor a root of unity. Then*

$$M(\alpha) > 5^{d/12} \approx 1.1435^{d}, \text{ where } d = [\mathbb{Q}(\alpha) : \mathbb{Q}]. \tag{1.7}$$

Also, the authors of [4] shown that $\sqrt[12]{5}$ on the right hand side of (1.7) cannot be replaced by any number greater than $\sqrt[12]{7}$. Later, the lower bound (1.7) was improved to $(1.1677)^{d}$ by Ishak, Mossinghoff, Pinner and Wiles [23].

In [6], Amoroso and Zannier proved the following general lower bound for the Weil height of elements of an abelian extension of K in terms of $[K : \mathbb{Q}]$.

Theorem 1.18 ([6]). *Let K be a number field of degree D over $\mathbb{Q}$. Suppose L/K is abelian. Then for any $\alpha \in L$ which is neither zero nor a root of unity, $h(\alpha) \geq \frac{1}{3^{D^2+2D+6}}$.*

In [40], Schinzel proved the following result for the totally real algebraic integers.

Theorem 1.19 ([40]). *If $\alpha \neq \pm 1$ is an algebraic integer such that all the conjugates of α over $\mathbb{Q}$ are real, then $M(\alpha) \geq \left(\frac{1+\sqrt{5}}{2}\right)^{d/2}$, where $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$.*

In [20], Garza generalized the above result.

Theorem 1.20 ([20]). *Let α be an algebraic number of degree d and S be the set of all real conjugates of α and suppose that $|S| \neq 0$. Let $\beta = (|S| - d)/|S|$. Then either*

$$M(\alpha) = 1 \text{ or } M(\alpha) \geq \left(\frac{2^{\beta} + \sqrt{4^{\beta} + 4}}{2}\right)^{|S|/2}.$$

For more results on Lehmer's problem, we refer the interested readers to the excellent survey article by Smyth [42].

1.5 Absolute values

In this section, we recall some theory of absolute values on number fields. These are required to give an equivalent definition of the Mahler measure in terms of absolute values on number fields.

1.5.1 Definition and Examples

Definition 1.21. An absolute value on a field K is a function

$$|\cdot| \ : \ K \to [0, \infty)$$

which satisfies the following three conditions:

1. $|\alpha| = 0$ if and only if $\alpha = 0$.
2. $|\alpha\beta| = |\alpha|\,|\beta|$ for all $\alpha, \beta \in K$.
3. $|\alpha + \beta| \leq |\alpha| + |\beta|$ for all $\alpha, \beta \in K$.

An absolute value is said to be nonarchimedean if it satisfy the stronger inequality

$$|\alpha + \beta| \leq \max\{|\alpha|\,, |\beta|\} \text{ for all } \alpha, \beta \in K.$$

Otherwise, it is called archimedean absolute value.

Example 1.22. For any field K, define $|0| = 0$ and $|\alpha| = 1$ for all $\alpha \in K \setminus \{0\}$. It is clearly an absolute value on K and is called the trivial absolute value.

Example 1.23. Consider $K = \mathbb{Q}$. One can easily prove that for $q \in \mathbb{Q}$, $|q|_\infty = \max\{q, -q\}$ is an absolute value on $\mathbb{Q}$. Similarly, for any fixed prime $p \in \mathbb{N}$ and $q \in \mathbb{Q}$, write $q = p^m \frac{a}{b}$,

where $a, b \in \mathbb{Z}$ and $p \nmid ab$. Put $|q|_p = p^{-m}$. Then for each prime p, $|\cdot|_p$ is an absolute value on $\mathbb{Q}$ and is called the p-adic absolute value on $\mathbb{Q}$.

Lemma 1.24. *An absolute value $|\cdot|$ on a field K is nonarchimedean if and only if $|n| \leq 1$ for all $n \in \mathbb{N}$.*

Proof. If $|\cdot|$ is nonarchimedean, then $|n| \leq |1| = 1$ for all $n \in \mathbb{N}$. Conversely, suppose $|n| \leq 1$ for all $n \in \mathbb{N}$. So, for $\alpha \in K$, $|n\alpha| = |n||\alpha| \leq |\alpha|$. Now for $\alpha, \beta \in K$,

$$|\alpha + \beta|^n = \left| \sum_{k=0}^{n} \binom{n}{k} \alpha^k \beta^{n-k} \right| \leq \sum_{k=0}^{n} |\alpha|^k |\beta|^{n-k} \leq (n+1)s^n,$$

where $s = \max\left\{|\alpha|, |\beta|\right\}$. Taking n^{th} root and allowing $n \to \infty$, we obtain

$$|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}.$$

This completes the proof of the lemma. □

An immediate consequence is the following.

Corollary 1.25. *Any absolute value in a field of positive characteristic is nonarchimedean. Moreover, in the case of finite field, there is only one absolute value, namely, the trivial one.*

Let K be any field with a nontrivial absolute value $|\cdot|$. Then for $\alpha, \beta \in K$,

$$d(\alpha, \beta) = |\alpha - \beta|$$

defines a metric on K. Therefore, it induces a topology on K. Two absolute values on K are said to be equivalent if they induce the same tolopolgy on K.

Proposition 1.26 ([39, p. 10])**.** *Two absolute values $|\cdot|_1$ and $|\cdot|_2$ are said to be equivalent if and only if there exists an $\eta > 0$ such that for all $\alpha \in K$*

$$|\alpha|_1 = |\alpha|_2^{\eta}.$$

In particular, a nontrivial absolute value is not equivalent to the trivial absolute value.

A natural question is that if $|\cdot|$ is an absolute value, then which powers of $|\cdot|$ is also an absolute value. The next lemma gives the answer.

Lemma 1.27 ([39, p. 10]). *Let $|\cdot|$ is an absolute value on K. Consider*

$$S = \left\{\eta > 0 : |\cdot|^\eta \text{ is an absolute value}\right\}.$$

Then S is either $(0, \infty)$ or $(0, r]$ with $r \geq 1$.

Remark 1.28. Consider the ordinary absolute value $|\cdot|$ on $\mathbb{R}$. Then $|\cdot|^\eta$ is an absolute value if and only if $0 < \eta \leq 1$. Indeed, if $\eta > 1$, then $(1+1)^\eta > 1+1$. So the triangle inequality fails if $\eta > 1$. The same holds for $\mathbb{C}$.

Remark 1.29. Suppose $|\cdot|$ is a p-adic absolute value on $\mathbb{Q}$. Then for any $\eta > 0$,

$$|\alpha + \beta|^\eta \leq \big(\max\{|\alpha|, |\beta|\}\big)^\eta \leq \max\{|\alpha|^\eta, |\beta|^\eta\}, \text{ for all } \alpha, \beta \in \mathbb{Q}.$$

Thus, for all $\eta > 0$, $|\cdot|^\eta$ is also an absolute value.

The following proposition classifies all absolute values on $\mathbb{Q}$ upto equivalence. For the proof, see [39, Theorem 1].

Proposition 1.30. *Every absolute value on $\mathbb{Q}$ is equivalent to either $|\cdot|_\infty$ or $|\cdot|_p$, for some prime number p.*

1.5.2 Completion

Let K be a field with a nontrivial absolute value $|\cdot|$. A sequence $\{\alpha_n\}_{n\in\mathbb{N}}$ of elements of K is said to be Cauchy if for any $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that for all $n, m \geq N$,

$$|\alpha_n - \alpha_m| < \varepsilon.$$

We say that K is complete if every Cauchy sequence in K converges in K.

The following results give information on completion of a number field with respect to an absolute value.

Proposition 1.31 ([27, Ch. 12, Proposition 2.1]). *Let K be a field with a nontrivial absolute value $|\cdot|$. Then there exists a pair (L, σ), consisting of a field L which is complete with respect to an absolute value $|\cdot|_1$ and an embedding $\sigma : K \to L$ such that $\sigma(K)$ is dense in L and $|\alpha| = |\sigma(\alpha)|_1$ for all $\alpha \in K$. Moreover, if (L', σ') is another pair, then there exists a unique isomorphism $\phi : L \to L'$ which preserves the absolute value and $\phi \circ \sigma = \sigma'$.*

Proposition 1.32 ([27, Ch. 12, Proposition 2.5]). *Let K be a field which is complete with respect to a nontrivial absolute value $|\cdot|$. If L is a finite and separable extension of K, then there exists a unique absolute value $|\cdot|_1$ on L which extends the absolute value $|\cdot|$ on K and L is complete with respect to $|\cdot|_1$.*

1.5.3 Absolute values on number fields

Let K be a number field and $\mathcal{O}_K$ be the ring of integers of K. For any embeddding σ of K into $\mathbb{C}$, $|\alpha|_\sigma = |\sigma(\alpha)|_\infty$ defines an archimedean absolute value on K, where $|\cdot|_\infty$ is the usual absolute value on $\mathbb{C}$. The following theorem classifies all archimedean absolute values on K; see [22, Proposition B.1.3] for the proof.

Theorem 1.33. *Let K be a number field of degree n over $\mathbb{Q}$. Let $\sigma_1, \ldots, \sigma_{r_1}$ be the real embeddings of K and $(\tau_1, \overline{\tau}_1), \ldots, (\tau_{r_2}, \overline{\tau}_{r_2})$ be the r_2 pairs of complex embeddings of K, where $r_1 + 2r_2 = n$. If $|\cdot|$ is an archimedean absolute value on K, then $|\cdot|$ is equivalent to $|\cdot|_\sigma$ for some $\sigma \in \{\sigma_1, \sigma_2, \ldots, \sigma_{r_1}, \tau_1, \tau_2, \ldots, \tau_{r_2}\}$.*

For a prime ideal $\mathcal{P}$ in $\mathcal{O}_K$ and $\alpha \in K$, $e_\mathcal{P}(\alpha)$ denotes the exponent of $\mathcal{P}$ in the prime factorization of $\alpha\mathcal{O}_K$. If

$$\alpha\mathcal{O}_K = \prod_{\mathcal{P}} \mathcal{P}^{e_\mathcal{P}(\alpha)},$$

then

$$|\alpha|_\mathcal{P} = p^{\frac{-e_\mathcal{P}(\alpha)}{e_\mathcal{P}(p)}}$$

defines a nonarchimedean absolute value on K, where $\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$. So $|p|_{\mathcal{P}} = 1/p$. The following theorem classifies all nonarchimedean absolute values on K; see [22, Proposition B.1.3] for the proof.

Theorem 1.34. *Let K be a number field and $|\cdot|$ be a nonarchimedean absolute value on K. Then there exists a prime ideal $\mathcal{P}$ of $\mathcal{O}_K$ such that $|\cdot|$ is equivalent to $|\cdot|_{\mathcal{P}}$.*

In each equivalence class v of nontrivial absolute values on a number field K, we choose the representative $|\cdot|_v$ which is *normalized* by

$$\begin{cases} |x|_v = x & \text{if } x \in \mathbb{Q}, x > 0, \text{ and } v \text{ is archimedean,} \\ |p|_v = 1/p & \text{if } v \text{ extends the } p\text{-adic absolute value on } \mathbb{Q}. \end{cases}$$

Let M_K be the set of all nontrivial normalized absolute values on K and $M_K^\infty \subseteq M_K$ be the set of all archimedean absolute values on K. For $v \in M_K$, K_v denotes the completion of K with respect to the absolute value $|\cdot|_v$. For a finite extension L over K and $w \in M_L$, we denote $w \mid v$ if w is an extension of v. The local and global degrees of an extension is related by the following degree formula; see [27, Ch. 12, Proposition 3.3] for the proof.

Proposition 1.35. *Let L/K be a separable extension and $v \in M_K$. Then*

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

We have the following product formula; see [22, Proposition B.1.2] for the proof.

Proposition 1.36. *Let α be a nonzero element of a number field K. Then*

$$\prod_{v \in M_K} |\alpha|_v^{[K_v : \mathbb{Q}_v]} = 1,$$

where $\mathbb{Q}_v$ is the completion of $\mathbb{Q}$ at the restriction of v to $\mathbb{Q}$.

1.6 Relation of Absolute values with Mahler measure

In this section, we prove an equivalent definition of the Mahler measure in terms of absolute values on number fields. For $v \in M_K$, denote $d_v = [K_v : \mathbb{Q}_v]$. First, we need the following lemma; see [47, Lemma 3.1] for the proof.

Lemma 1.37. *Let K be a number field and $p \in \mathbb{N}$ a prime number. Let $\alpha \in K$ be an algebraic number of degree d over $\mathbb{Q}$ with leading coefficient a_d. Then*

$$|a_d|_p \prod_{v \in M_K, v|p} \max\left\{1, |\alpha|_v\right\}^{d_v} = 1.$$

The following is an equivalent definition of the Mahler measure in terms of absolute values on number fields.

Proposition 1.38. *Let α be an algebraic number. Then*

$$M(\alpha) = \prod_{v \in M_{\mathbb{Q}(\alpha)}} \max\{1, |\alpha|_v\}^{d_v}.$$

Proof. Let $K = \mathbb{Q}(\alpha)$. If $v \in M_K^\infty$ corresponds to a real embedding, then $d_v = [K_v : \mathbb{Q}_v] = 1$. If $v \in M_K^\infty$ corresponds to a complex embedding, then $d_v = [K_v : \mathbb{Q}_v] = 2$. Using this and the definition of the Mahler measure, we get

$$M(\alpha) = |a_d| \prod_{v \in M_K^\infty} \max\{1, |\alpha|_v\}^{d_v}.$$

By the product formula, $|a_d| = \prod_p |a_d|_p^{-1}$. So

$$M(\alpha) = \prod_p |a_d|_p^{-1} \prod_{v \in M_K^\infty} \max\{1, |\alpha|_v\}^{d_v}.$$

By Lemma 1.37,

$$|a_d|_p^{-1} = \prod_{v \in M_K, v|p} \max\{1, |\alpha|_v\}^{d_v}.$$

Hence

$$\begin{aligned} M(\alpha) &= \prod_{v \in M_K \setminus M_K^\infty} \max\{1, |\alpha|_v\}^{d_v} \prod_{v \in M_K^\infty} \max\{1, |\alpha|_v\}^{d_v} \\ &= \prod_{v \in M_K} \max\{1, |\alpha|_v\}^{d_v}. \end{aligned}$$

This completes the proof of the proposition. □

Proposition 1.39. *Let K be any number field containing an algebraic number α. Then*

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

Proof. This follows from Proposition 1.38 and (1.1). □

Remark 1.40. The Weil height of an algebraic number α is independent of any number field K containing α. It follows from [22, Lemma B.2.1 (c)].

Chapter 2

Lower bound for the Mahler measure

2.1 Introduction

As mentioned in Chapter 1, Lehmer's problem has been solved for various classes of algebraic integers; however, the general case remains open. As seen in Theorem 1.12, the best unconditional lower bound for the Mahler measure is given by

$$M(\alpha) \geq 1 + \frac{1}{4}\left(\frac{\log\log d}{\log d}\right)^3, \tag{2.1}$$

where d is the degree of α. Notice that if the answer to the Lehmer problem is yes, then we can replace the quantity $\frac{1}{4}\left(\frac{\log\log d}{\log d}\right)^3$ on the right hand side of (2.1) by a constant $c > 0$, which is independent of α and d. In this direction, one may ask the following: Can we replace the term $\left(\frac{\log\log d}{\log d}\right)^3$ in (2.1) by a function f of d such that $\left(\frac{\log\log d}{\log d}\right)^3 / f(d) \to 0$ as $d \to \infty$? In this chapter, we show the existence of such an f for a class of algebraic integers. We need the following definition to state our theorem. For any algebraic integer α of degree d, define

$$A_\alpha = \left\{ z \in \mathbb{C} : \operatorname{dist}\left(\frac{k}{\pi}\arg(z/\alpha), \mathbb{Z}\right) < \frac{\log(13/5)}{14\pi}, \text{ for all } k \in \{1, \ldots, \lfloor 19600 \log d \rfloor\} \right\}$$

and

$$A'_\alpha = \left\{ z \in \mathbb{C} : \operatorname{dist}\left(\frac{k}{\pi}\arg(z\alpha), \mathbb{Z}\right) < \frac{\log(13/5)}{14\pi}, \text{ for all } k \in \{1, \ldots, \lfloor 19600 \log d \rfloor\} \right\},$$

where for any real number $r \in \mathbb{R}$, $\operatorname{dist}(r, \mathbb{Z}) := \min_{n\in\mathbb{Z}} |r - n|$.

Since for $n \geq 1$, $\arg(z^n) = n\arg(z) \pm 2\pi l$ with $l \in \mathbb{N}$, we obtain

$$A_\alpha = \left\{ z \in \mathbb{C} : \left|\arg(z^{2k}) - \arg(\alpha^{2k})\right| < \frac{\log(13/5)}{7}, \text{ for all } k \in \{1, \ldots, \lfloor 19600 \log d \rfloor\} \right\}$$

and

$$A'_\alpha = \left\{ z \in \mathbb{C} : \left| \arg(z^{2k}) + \arg(\alpha^{2k}) \right| < \frac{\log(13/5)}{7}, \text{ for all } k \in \{1, \ldots, \lfloor 19600 \log d \rfloor\} \right\}.$$

Indeed, suppose $z \in \mathbb{C}$ be such that $\left|\arg(z^{2k}) - \arg(\alpha^{2k})\right| < \frac{\log(13/5)}{7}$, for all $k \in \mathbb{N}$. Then for some $l_1, l_2 \in \mathbb{N}$,

$$\left|2k \arg(z) \pm 2\pi l_1 - 2k \arg(\alpha) \pm 2\pi l_2\right| < \frac{\log(13/5)}{7}.$$

So,

$$\left| \frac{k}{\pi}(\arg(z) - \arg(\alpha)) \pm l_1 \pm l_2 \right| < \frac{\log(13/5)}{14\pi},$$

which implies

$$\left| \frac{k}{\pi} \arg(z/\alpha) \pm 2kl_3 \pm l_1 \pm l_2 \right| < \frac{\log(13/5)}{14\pi}, \text{ for some } l_3 \in \mathbb{N}.$$

Thus, for any $k \in \mathbb{N}$,

$$\operatorname{dist}\left(\frac{k}{\pi} \arg(z/\alpha), \mathbb{Z} \right) \leq \left| \frac{k}{\pi} \arg(z/\alpha) \pm 2kl_3 \pm l_1 \pm l_2 \right| < \frac{\log(13/5)}{14\pi}.$$

Similarly, the other implication also follows.

We prove the following result.

Theorem 2.1 ([36]). *Let α be an algebraic integer of degree d which is neither zero nor a root of unity, and let $\alpha_1 = \alpha, \ldots, \alpha_d$ be the conjugates of α over $\mathbb{Q}$. Suppose $\alpha_i \in \mathbb{R} \cup A_\alpha \cup A'_\alpha$, for all $i \in \{1, \ldots, d\}$. Then $M(\alpha) \geq 1 + \frac{1}{407000 \log d}$.*

2.2 Auxiliary lemmas

For the proof of Theorem 2.1, we need the following lemmas.

Lemma 2.2 ([44]). *Let $\sigma_1, \ldots, \sigma_d$ denote the embeddings of a number field K into $\mathbb{C}$, where $d = [K : \mathbb{Q}]$. Let $b_{i,j}$ $(1 \leq i \leq N; 1 \leq j \leq M)$ be algebraic integers in the field K, with at*

least one of them is nonzero. Let

$$U = \max_{1\le j\le M} \prod_{k=1}^{d} \left(\max_{1\le i\le N} |\sigma_k(b_{i,j})| \right).$$

If $N \ge 2dM$, *then the system of equations*

$$\sum_{i=1}^{N} b_{i,j} x_i = 0 \qquad (1 \le j \le M),$$

has a nontrivial solution in rational integers $x_1, \dots, x_N$ *with* $\max_{1\le i\le N} |x_i| \le \sqrt{2} N U^{1/d}$.

Lemma 2.3 ([46]). *Let* r_1, r_2 *be two positive real numbers with* $r_1 < r_2$. *Suppose* f *is a nonzero analytic function in the open disc* $|z| < r_2$ *and continuous in the closed disc* $|z| \le r_2$. *Then*

$$|f|_{r_1} \le |f|_{r_2} \left(\frac{r_1^2 + r_2^2}{2 r_1 r_2} \right)^{-\mathcal{N}},$$

where $|f|_r = \max_{|z|=r} |f(z)|$ *and* $\mathcal{N}$ *is the number of zeros (counting multiplicities) of* f *in* $|z| \le r_1$.

Lemma 2.4. *Let* K *be a subfield of* $\mathbb{C}$ *and* $u \in K^*$. *Assume that there exists a nonzero polynomial* $F \in K[X, Y]$ *with* $\deg_X \le d_0$ *and* $\deg_Y \le d_1$ *such that* $F(n, u^n) = 0$ *for all* $n \in \mathbb{N} \cup \{0\}$, *then* u *is a root of unity.*

Proof. This is an application of Philippon's zeros estimate to the algebraic group $G = \mathbb{G}_a \times \mathbb{G}_m$ where $\mathbb{G}_a, \mathbb{G}_m$ respectively the additive and multiplicative groups of complex numbers, see [47, Theorem 5.1] for more details. Note that the only proper connected algebraic subgroups G are

$$(0), \quad (0) \times \mathbb{G}_m, \quad \mathbb{G}_a \times (0).$$

Let S be any positive integer and let

$$\sum = \{(n, \alpha^n) : \ n \in \mathbb{N} \cup \{0\}, \ n \le S\}.$$

Also, let

$$\sum[2] = \{(n, \alpha^n) : n \in \mathbb{N} \cup \{0\},\ n \leq 2S\}.$$

Since the polynomial $F(X, Y)$ vanishes on $\sum[2]$, by [47, Theorem 5.1], for any proper connected algebraic subgroup G^* of G, at least one of the following holds:

(i) $\text{card}\left(\frac{\sum+G^*}{G^*}\right) \leq 4d_0d_1$ if $G^* = (0)$;

(ii) $\text{card}\left(\frac{\sum+G^*}{G^*}\right) \leq 2d_0$ if $G^* = (0) \times \mathbb{G}_m$;

(iii) $\text{card}\left(\frac{\sum+G^*}{G^*}\right) \leq 4d_1$ if $G^* = \mathbb{G}_a \times (0)$.

If (i) holds then $\text{card}\left(\frac{\sum+G^*}{G^*}\right) \geq 2S$. But S can be any natural number. Hence (i) cannot hold. Similarly, if (ii) holds then in this case also $\text{card}\left(\frac{\sum+G^*}{G^*}\right) \geq 2S$. Therefore, (iii) must hold. This means not all the integral powers of α are distinct.This proves that α is a root of unity, and the proof is complete. □

Lemma 2.5. *The function $f(n) = \frac{\log(5n+5)}{n}$ is a strictly decreasing function of positive integers.*

Proof. Let $n \in \mathbb{N}$. Since

$$\begin{aligned}\left(1 + \frac{1}{n+1}\right)^n &= 1 + \frac{n}{n+1} + \frac{n(n-1)}{2!}\frac{1}{(n+1)^2} + \cdots + \frac{1}{(n+1)^n} \\ &< 1 + n < 5n + 5,\end{aligned}$$

we have

$$\left(\frac{5n+10}{5n+5}\right)^n < 5n + 5.$$

This implies

$$n \log(5n + 10) < (n + 1) \log(5n + 5).$$

Thus we get

$$\frac{\log(5n+10)}{n+1} < \frac{\log(5n+5)}{n},$$

the lemma follows. □

2.3 Proof of Theorem 2.1

Throughout this section, we choose the branch of the logarithm such that $-\pi < \mathrm{Im}(\log x) \leq \pi$, where $\mathrm{Im}(z)$ denotes the imaginary part of z. For a real number x, $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x. Let G be the set of all embeddings of $\mathbb{Q}(\alpha)$ into $\mathbb{C}$ over $\mathbb{Q}$. If $\sigma(\alpha) \in \mathbb{R}$ for all $\sigma \in G$ then by Theorem 1.19, the theorem follows. So, we assume that there exists $\sigma \in G$ such that $\sigma(\alpha) \notin \mathbb{R}$. Without loss of generality, we take $\sigma = Id$. Also, by Theorem 1.14, we may assume that α is reciprocal.

We prove Theorem 2.1 by contradiction. We can assume $d \geq 50000$. Indeed, if $d < 50000$, then

$$M(\alpha) - 1 \leq \frac{1}{407000 \log d} < \frac{1}{4}\left(\frac{\log\log d}{\log d}\right)^3,$$

and hence by Theorem 1.12, α is a root of unity.

Put

$$K_2 = \left\lfloor \frac{d}{80 \log d} \right\rfloor, \; K_3 = \lfloor 80 \log d \rfloor, \; K_4 = d + \frac{490 U K_3}{d} + 1,$$

and

$$U = \left\lfloor \frac{K_2 K_3}{2} \right\rfloor.$$

Let $r_1, r_2, \ldots, r_{K_3}$ be K_3 positive integers with

$$1 \leq r_1 < r_2 < \cdots < r_{K_3} \leq 245 K_3$$

and

$$\max_{1 \leq s \leq t \leq K_3} \left| \arg\left(\alpha^{2r_s}\right) - \arg\left(\alpha^{2r_t}\right) \right| \leq \frac{2\pi}{245}.$$

Note that by the pigeon-hole principle such a list of integers always exist. Put

$$\theta_1 = \min_{1 \leq k \leq K_3} \arg\left(\alpha^{2r_k}\right) \qquad \text{and} \qquad \theta = \theta_1 + \frac{\pi}{245}.$$

Thus

$$\max_{1 \leq k \leq K_3} \left| \arg\left(\alpha^{2r_k}\right) - \theta \right| \leq \frac{\pi}{245}. \tag{2.2}$$

If for some $\sigma \in G$, $\sigma(\alpha) \in A_\alpha \cup A'_\alpha$, then using (2.2), we have

$$\begin{aligned}\left|\arg\left(\sigma(\alpha)^{2r_k}\right) \pm \theta\right| &= \left|\arg\left(\sigma(\alpha)^{2r_k}\right) - \arg\left(\alpha^{2r_k}\right) + \arg\left(\alpha^{2r_k}\right) \pm \theta\right| \\ &\leq \frac{\log(13/5)}{7} + \frac{\pi}{245} \leq \frac{\pi}{21}. \end{aligned} \tag{2.3}$$

The proof of Theorem 2.1 now proceeds by several lemmas.

Lemma 2.6. *There exist integers*

$$a_{i,j,k}\ (1 \leq i \leq d; 1 \leq j \leq K_2; 1 \leq k \leq K_3)$$

such that the function

$$f^*(z) = \sum_{i=1}^{d} \sum_{j=1}^{K_2} \sum_{k=1}^{K_3} a_{i,j,k} \alpha^i z^j \exp\left(z \log \alpha^{2r_k}\right)$$

satisfy

$$f^*(n) = 0 \tag{2.4}$$

for all $n = 1, \ldots, U$ *with*

$$0 < \max_{i,j,k} \left|a_{i,j,k}\right| \leq \sqrt{2}(dK_2K_3) M(\alpha)^{1+\frac{490UK_3}{d}} U^{K_2}.$$

Proof. The system of equations (2.4) is equivalent to

$$\sum_{i=1}^{d} \sum_{j=1}^{K_2} \sum_{k=1}^{K_3} a_{i,j,k} \alpha^{i+2nr_k} n^j = 0 \quad (n = 1, \ldots, U) \tag{2.5}$$

with unknowns $a_{i,j,k}$. This is a system of $U \leq K_2K_3/2$ equations in dK_2K_3 unknowns $a_{i,j,k}$. Note that

$$\begin{aligned}\max_{1\leq n\leq U} \prod_{\sigma\in G} \left(\max_{i,j,k} \left|\sigma(\alpha^{i+2nr_k} n^j)\right|\right) &\leq \max_{1\leq n\leq U} \prod_{\sigma\in G} \left(\max_{i,j,k} \left(n^j \max\left\{1, \left|\sigma(\alpha)\right|\right\}^{i+2nr_k}\right)\right) \\ &\leq \max_{1\leq n\leq U} \left(n^{K_2 d} \left(\prod_{\sigma\in G} \max\left\{1, \left|\sigma(\alpha)\right|\right\}\right)^{d+490nK_3}\right) \\ &\leq U^{K_2 d} M(\alpha)^{d+490UK_3}. \end{aligned}$$

Hence, by Lemma 2.2, there exist integers $a_{i,j,k}$ with

$$\begin{aligned} 0 < \max_{i,j,k} \left|a_{i,j,k}\right| \leq & \sqrt{2} dK_2K_3 \left(U^{K_2 d} M(\alpha)^{d+490UK_3}\right)^{1/d} \\ = & \sqrt{2}(dK_2K_3) M(\alpha)^{1+\frac{490UK_3}{d}} U^{K_2}, \end{aligned}$$

such that (2.5) holds for all $n = 1, \ldots, U$. This completes the proof of the lemma. □

For each $\sigma \in G$, define

$$f_\sigma^*(z) = \sum_{i=1}^{d} \sum_{j=1}^{K_2} \sum_{k=1}^{K_3} a_{i,j,k} \sigma(\alpha)^i z^j \exp\left(z \log \sigma(\alpha)^{2r_k}\right).$$

That is, f_σ^* is obtained from f^* by replacing α with $\sigma(\alpha)$. Note that $f_{Id}^*(z) = f^*(z)$.

Next we show that f_σ^* also vanishes on $\{1, 2, \ldots, U\}$ for all $\sigma \in G$.

Lemma 2.7. *For all $\sigma \in G$, we have $f_\sigma^*(n) = 0$, for all $n \in \{1, \ldots, U\}$.*

Proof. Let $\sigma \in G$. By Lemma 2.6, we have

$$\sum_{i=1}^{d} \sum_{j=1}^{K_2} \sum_{k=1}^{K_3} a_{i,j,k} \alpha^{i+2nr_k} n^j = 0$$

for all $n \in \{1, \ldots, U\}$. Applying σ on both sides, we get

$$\sum_{i=1}^{d} \sum_{j=1}^{K_2} \sum_{k=1}^{K_3} a_{i,j,k} \sigma(\alpha)^{i+2nr_k} n^j = 0$$

for all $n \in \{1, \ldots, U\}$. From this we easily get that $f_\sigma^*(n) = 0$, for all $n \in \{1, \ldots, U\}$. □

To obtain a required contradiction, we need to slightly change the function f_σ^*. For each $\sigma \in G$, we define

$$f_\sigma(z) = \begin{cases} \exp(-i\theta z) f_\sigma^*(z) & \text{if } \sigma(\alpha) \in A_\alpha, \\ \exp(i\theta z) f_\sigma^*(z) & \text{if } \sigma(\alpha) \in A'_\alpha, \\ f_\sigma^*(z) & \text{if } \sigma(\alpha) \in \mathbb{R}. \end{cases}$$

Note that if $\sigma = Id$, then $f_{Id}(z) = \exp(-i\theta z) f^*(z)$. From Lemma 2.7, we see that $f_\sigma(n) = 0$, for $n = 1, \ldots, U$ and for all $\sigma \in G$.

Lemma 2.8. *Let $\sigma \in G$. Suppose for an integer $J \geq U$, we have $f_\sigma(n) = 0$ for all $n \leq J$. Then $|f_\sigma(J+1)| \leq \sqrt{2}(dK_2K_3)^2 M(\alpha)^{K_4} U^{K_2} (5J+5)^{K_2} \exp(-J(0.056))$.*

Proof. Since $f_\sigma(z)$ has at least J zeros in the region $|z| \leq J+1$, applying Lemma 2.3 to the function f_σ with $r = J+1$ and $R = 5(J+1)$, we get

$$\left|f_\sigma(J+1)\right| \leq |f_\sigma|_{J+1} \leq |f_\sigma|_{5J+5} \frac{1}{(13/5)^J}.$$

Next, we calculate an upper bound for $|f_\sigma|_{5J+5}$. Using Lemma 2.6 and $|\alpha| \leq M(\alpha)$, we obtain

$$|f_\sigma|_{5J+5} \leq \sqrt{2}(dK_2K_3)^2 M(\alpha)^{K_4} U^{K_2} (5J+5)^{K_2} \exp\left((5J+5)\left(\log \sigma(\alpha)^{2r_{k_3}} + i\theta_0\right)\right),$$

where

$$\theta_0 = \begin{cases} -\theta & \text{if } \sigma(\alpha) \in A_\alpha, \\ +\theta & \text{if } \sigma(\alpha) \in A'_\alpha, \\ 0 & \text{if } \sigma(\alpha) \in \mathbb{R}. \end{cases}$$

So

$$|f_\sigma|_{5J+5} \leq \sqrt{2}(dK_2K_3)^2 M(\alpha)^{K_4} U^{K_2} (5J+5)^{K_2} \exp\left((5J+5)\triangle\right),$$

where

$$\triangle = \max_{1\leq k\leq K_3} \left|\log \sigma(\alpha)^{2r_k} + i\theta_0\right| \leq \max_{1\leq k\leq K_3} \left|490K_3 \log\left|\sigma(\alpha)\right| + i\left(\arg\left(\sigma(\alpha)^{2r_k}\right) + \theta_0\right)\right|.$$

If for some $\sigma \in G$, $|\sigma(\alpha)| \geq 1$ then $\log|\sigma(\alpha)| \leq \log M(\alpha)$. Otherwise, if $|\sigma(\alpha)| < 1$ then since α is reciprocal, both $\sigma(\alpha)$ and $\sigma(\alpha)^{-1}$ are conjugates of α over $\mathbb{Q}$. Therefore, $\frac{1}{|\sigma(\alpha)|} \geq 1$ and

$$|\log|\sigma(\alpha)|| = -\log|\sigma(\alpha)| = \log\frac{1}{|\sigma(\alpha)|} \leq \log M(\alpha).$$

Therefore,

$$\triangle \leq \max_{1\leq k\leq K_3} \left|490K_3 \log M(\alpha) + i\left(\arg\left(\sigma(\alpha)^{2r_k}\right) + \theta_0\right)\right|.$$

If $\sigma(\alpha) \in A_\alpha \cup A'_\alpha$, then using (2.3), we get

$$\triangle \leq \max_{1\leq k\leq K_3} \left|490K_3 \log M(\alpha) + i(\pi/21)\right|.$$

Using $K_3 \leq 80 \log d$ and $\log M(\alpha) \leq 1/(407000 \log d)$, we get $490K_3 \log M(\alpha) < 0.0964$. So

$$\triangle \leq \sqrt{0.0964^2 + (\pi/21)^2} \leq 0.17797,$$

whence

$$(13/5)^{-J} \exp((5J+5)\triangle) \leq (13/5)^{-J} \exp((5J+5)0.17797) \leq \exp(-J(0.056)).$$

Thus,

$$\left|f_\sigma(J+1)\right| \leq |f_\sigma|_{5J+5} (13/5)^{-J} \leq \sqrt{2}(dK_2K_3)^2 M(\alpha)^{K_4} U^{K_2} (5J+5)^{K_2} \exp(-J(0.056)).$$

If $\sigma(\alpha) \in \mathbb{R}$, then for any $k \in \{1, \ldots, K_3\}$, $\arg\left(\sigma(\alpha)^{2r_k}\right) = 0$. Therefore,

$$\triangle \leq 490K_3 \log M(\alpha) < 0.0964.$$

Finally, we have

$$(13/5)^{-J} \exp((5J+5)\triangle) \leq (13/5)^{-J} \exp((5J+5)0.0964) \leq \exp(-J(0.056)),$$

whence

$$\left|f_\sigma(J+1)\right| \leq |f_\sigma|_{5J+5} (13/5)^{-J} \leq \sqrt{2}(dK_2K_3)^2 M(\alpha)^{K_4} U^{K_2} (5J+5)^{K_2} \exp(-J(0.056)).$$

This completes the proof of the lemma. □

Lemma 2.9. *Let $\sigma \in G$ and let $J \geq U$ be an integer. Suppose $f_\sigma(n) = 0$ for all $n \leq J$. Then we have $|f_\sigma(J+1)| < 1$.*

Proof. We prove by contradiction. Suppose $\left|f_\sigma(J+1)\right| \geq 1$. Then from Lemma 2.8, we have

$$1 \leq \left|f_\sigma(J+1)\right| \leq \sqrt{2}(dK_2K_3)^2 M(\alpha)^{K_4} U^{K_2} (5J+5)^{K_2} \exp(-J(0.056)).$$

Taking logarithm both sides, we have

$$(0.056)J \leq \log\sqrt{2} + 2\log(dK_2K_3) + K_4 \log M(\alpha) + K_2 \log U + K_2 \log(5J+5),$$

which implies

$$0.056 \leq \frac{\log\sqrt{2}}{J} + \frac{2\log(dK_2K_3)}{J} + \frac{K_4}{J}\log M(\alpha) + \frac{K_2}{J}\log U + \frac{K_2}{J}\log(5J+5).$$

Since $J \geq U$, by Lemma 2.5, we have

$$\frac{\log(5J+5)}{J} \leq \frac{\log(5U+5)}{U}.$$

So

$$0.056 \leq \frac{\log\sqrt{2}}{U} + \frac{2\log(dK_2K_3)}{U} + \frac{K_4}{U}\log M(\alpha) + \frac{K_2}{U}\log U + \frac{K_2}{U}\log(5U+5). \quad (2.6)$$

Since $d \geq 50000$, we have

$$\frac{\log\sqrt{2}}{U} < 0.00001387,\ \frac{2\log(dK_2K_3)}{U} < 0.001732,\ \frac{K_4}{U}\log M(\alpha) < 0.0000026595,$$

and

$$\frac{K_2}{U}\log U < 0.025,\ \frac{K_2}{U}\log(5U+5) < 0.02500554.$$

Hence, the right hand side of (2.6) is at most 0.0518. And this contradiction proves that $\left|f_\sigma(J+1)\right| < 1$. This completes the proof of the lemma. □

Lemma 2.10. *For all $n \in \mathbb{N}$, we have $f_{Id}(n) = 0$.*

Proof. We prove this by induction on n. By Lemma 2.7, we assume that for some integer $J \geq U$, $f_{Id}(n) = 0$ for all $n = 1, \ldots, J$, and then we will prove that $f_{Id}(J+1) = 0$. This will then complete the induction step. From Lemma 2.9, we have $\left|f_\sigma^*(J+1)\right| = \left|f_\sigma(J+1)\right| < 1$ for all $\sigma \in G$. However, all the conjugates of the algebraic integer $f^*(J+1)$ over $\mathbb{Q}$ are of the form $f_\sigma^*(J+1)$ with $\sigma \in G$. Therefore, by Theorem 1.5, $f^*(J+1)$ is either a root of unity or zero. But since $\left|f^*(J+1)\right| < 1$, we must have $f^*(J+1) = 0$. So $f_{Id}(J+1) = 0$. The proof of lemma is complete. □

Proof of Theorem 2.1. Let $A_{j,k} = \sum_{i=1}^{d} a_{i,j,k}\alpha^i$. Since α has degree d, at least one $A_{j,k}$ is nonzero. So,

$$A(X,Y) = \sum_{j=1}^{K_2}\sum_{k=1}^{K_3} A_{j,k}X^jY^{2r_k}$$

is a nonzero polynomial. Using Lemma 2.10, we get

$$A(n,\alpha^n) = f^*(n) = f_{Id}(n)\exp(i\theta n) = 0$$

for all $n \in \mathbb{N}\cup\{0\}$. Applying Lemma 2.4 , we see that α is a root of unity. This completes the proof of Theorem 2.1.

□

2.4 Construction of reciprocal algebraic integers

In this section, we construct examples of reciprocal algebraic integers satisfying the conditions of Theorem 2.1. More precisely, we prove the following.

Theorem 2.11. *There exist infinitely many reciprocal algebraic integers $(\delta_n)_{n\in\mathbb{N}}$ of unbounded degrees over $\mathbb{Q}$ satisfying the hypothesis of Theorem 2.1.*

We need some definitions. For subfields K and L of $\mathbb{C}$, we say that K is *linearly disjoint from* L over $\mathbb{Q}$ if for any finite set of elements of K which is linearly independent over $\mathbb{Q}$

is still linearly independent over L. Let $n \in \mathbb{N}$. A set of complex numbers $\beta_1, \beta_2, \ldots, \beta_n$ are said to be *linearly disjoint* over $\mathbb{Q}$ if for each j with $1 \leq j \leq n$, the field $\mathbb{Q}(\beta_j)$ is linearly disjoint from $\mathbb{Q}(\beta_1, \beta_2, \ldots, \beta_{j-1}, \beta_{j+1}, \ldots, \beta_n)$ over $\mathbb{Q}$. Note that if $\beta_1, \beta_2, \ldots, \beta_n$ are linearly disjoint over $\mathbb{Q}$ then $\beta_j \notin \mathbb{Q}$ for $1 \leq j \leq n$.

We first prove the following lemma.

Lemma 2.12. *Let α and β be two reciprocal algebraic integers with conjugates $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ respectively over $\mathbb{Q}$. Assume that $-\alpha \notin \{\alpha_1, \ldots, \alpha_n\}$. Further, suppose that the fields $\mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ and $\mathbb{Q}(\beta_1, \ldots, \beta_n)$ are linearly disjoint over $\mathbb{Q}$. Then $\alpha\beta$ is reciprocal algebraic integer of degree mn over $\mathbb{Q}$.*

Proof. First we show that $\alpha\beta$ has degree mn over $\mathbb{Q}$. That is, we need to show that for integers i, j, k, ℓ with $1 \leq i, k \leq m$, $1 \leq j, \ell \leq n$ we have

$$\alpha_i \beta_j = \alpha_k \beta_\ell$$

if and only if $i = k, j = \ell$. To see this, suppose $\alpha_i\beta_j = \alpha_k\beta_\ell$ for some integers i, j, k, ℓ in the above range. This means, the set $\{\alpha_i, \alpha_k\}$ is linearly disjoint over $\mathbb{Q}(\beta_1, \ldots, \beta_n)$. Hence, we must have

$$a\alpha_i = b\alpha_k$$

for some nonzero integers a, b. Taking norm on both sides, we deduce $a^m = b^m$. So, $a = \pm b$ and thus $\alpha_i = \pm\alpha_k$. If $\alpha_i = \alpha_k$, then we are done. Otherwise, we must have $-\alpha \in \{\alpha_1, \ldots, \alpha_n\}$. This is a contradiction to one of our assumptions on α. Hence $\alpha\beta$ must be of degree mn over $\mathbb{Q}$.

Finally, since

$$\frac{1}{\alpha\beta} \in \{\alpha_i\beta_j : \quad 1 \leq i \leq m,\ 1 \leq j \leq n\},$$

we see that $\alpha\beta$ is a reciprocal algebraic integer of degree mn over $\mathbb{Q}$. This completes the proof of the lemma. □

Corollary 2.13. *Let α be a reciprocal algebraic integer such that $-\alpha$ is not a conjugate of α over $\mathbb{Q}$. Then there exist an injective sequence $(\gamma_n)_{n\geq 1}$ of totally positive reciprocal algebraic integers such that for $n \geq 1$, we have* $\deg(\gamma_n) > n$, *$\alpha\gamma_n$ reciprocal,* $\deg(\alpha\gamma_n) = \deg(\alpha)\deg(\gamma_n)$ *and* $\arg(\alpha\gamma_n) = \arg(\alpha)$.

Proof. For simplicity, for an algebraic number α, let $\mathbb{Q}_{\mathfrak{n}}(\alpha)$ denotes the normal closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ in $\mathbb{C}$. Let $\mathcal{B}_\alpha$ be the collection of totally positive reciprocal algebraic integers with the following three properties.

(i) For each $\beta \in \mathcal{B}_\alpha$, we have all the conjugates of β are totally positive.

(ii) For each $\beta \in \mathcal{B}_\alpha$, we have $\mathbb{Q}_{\mathfrak{n}}(\beta)$ is linearly disjoint to $\mathbb{Q}_{\mathfrak{n}}(\alpha)$ over $\mathbb{Q}$.

(iii) For any two distinct elements $\beta, \beta' \in \mathcal{B}_\alpha$, we have $\mathbb{Q}_{\mathfrak{n}}(\beta)$ and $\mathbb{Q}_{\mathfrak{n}}(\beta')$ are linearly disjoint over $\mathbb{Q}$.

The set $\mathcal{B}_\alpha$ is infinite. Indeed, there exist infinitely many prime integers p such that the extensions $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$'s are pairwise linearly disjoint over $\mathbb{Q}$ and linearly disjoint to $\mathbb{Q}_{\mathfrak{n}}(\alpha)$ over $\mathbb{Q}$. For each such prime p, let $a \in \mathbb{N}$ be such that the equation $pX^2 - a^2 + 1 = 0$ has a solution in $\mathbb{Z}$. Then the largest root, $\delta_p = a + \sqrt{a^2 - 1}$, of the polynomial $X^2 - 2aX + 1$ belongs to $\mathcal{B}_\alpha$.

Choose an infinite sequence $(\beta_n)_{n\geq 1}$ of elements of $\mathcal{B}_\alpha$ such that for all $n \geq 1$ we have

(iv) $\beta_1 \cdots \beta_n$ is reciprocal;

(v) $\mathbb{Q}_{\mathfrak{n}}(\beta_1 \cdots \beta_{n-1}\alpha)$ is linearly disjoint to $\mathbb{Q}_{\mathfrak{n}}(\beta_n)$ over $\mathbb{Q}$;

(vi) $-\beta_1 \cdots \beta_{n-1}\alpha$ is not conjugate to $\beta_1 \cdots \beta_{n-1}\alpha$; and

(vii) $[\mathbb{Q}(\beta_1 \cdots \beta_n) : \mathbb{Q}] \geq n$.

Such a sequence exists. Because for distinct prime integers $p_1, \ldots, p_\ell$ $(\ell \geq 1)$, we have

$$[\mathbb{Q}(\delta_{p_1} \cdots \delta_{p_\ell}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_\ell}) : \mathbb{Q}] = 2^\ell.$$

Hence one can inductively construct an injective sequence of prime integers $(p_n)_{n\geq 1}$ such that the associated sequence $(\delta_{p_n})_{n\geq 1}$ have all the properties $(iv) - (vii)$.

Now setting $\gamma_n = \beta_1 \cdots \beta_n$ $(n \geq 1)$ we see from Lemma 2.12 that $\alpha\gamma_n$ is reciprocal, $\deg(\alpha\gamma_n) = \deg(\alpha)\deg(\gamma_n) > n$ and $\arg(\alpha\gamma_n) = \arg(\alpha)$. Hence the sequence $(\gamma_n)_{n\geq 1}$ have all the properties stated in the corollary, and this completes the proof of the corollary. □

Now we prove Theorem 2.11. Let α be any nonzero reciprocal algebraic integer satisfying the hypothesis of Theorem 2.1. (For example, we can take α to be any one of the complex roots of $f(x) = x^8 + 7x^4 + 1$. This polynomial is irreducible over $\mathbb{Q}$. By using WolframAlpha software we see that all the roots of this polynomial have arguments $\pm\theta, \pm\theta \mp \pi$ such that $0 < \theta < \pi/2$.) By Corollary 2.13, we obtain an injective sequence $(\gamma_n)_{n\geq 1}$ of totally positive reciprocal algebraic integers with $(\deg(\gamma_n))_{n\geq 1}$ such that for all $n \geq 1$ we have $\alpha\gamma_n$ is reciprocal, $\deg(\alpha\gamma_n) \geq n$, and $\arg(\alpha\gamma_n) = \arg(\alpha)$. Then the sequence $(\alpha\gamma_n)_{n\geq 1}$ is an injective sequence of reciprocal algebraic integers with the properties that $\deg(\alpha\gamma_n) \geq n$ and the conjugates of $\alpha\gamma_n$ have arguments lie in $\{\pm\theta, \pm\theta \mp \pi\}$. Define $\delta_n = \alpha\gamma_n$. Then all the conjugates of δ_n lie in either A_{δ_n} or A'_{δ_n}. This completes the proof of Theorem 2.11.

Chapter 3

Splitting of primes and Absolute Weil height

3.1 Introduction

As mentioned in Chapter 1, an equivalent definition of Weil height in terms of absolute values in number fields is given by

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

where K is any number field containing α. Since nonarchimedean absolute values on K correspond to the prime ideals in $\mathcal{O}_K$, one may expect connection between lower bounds for the Weil height and splitting of primes in number fields. This has been explored by several Mathematicians. For example, Bombieri and Zannier [11] studied for totally p-adic algebraic numbers. Recall that, for a rational prime p, an algebraic number α is said to be totally p-adic if p splits into $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ distinct prime ideals in $\mathcal{O}_{\mathbb{Q}(\alpha)}$. For each rational prime p, define

$$\sigma(p, \mathbb{Q}) = \inf\left\{h(\alpha) : \alpha \text{ is totally } p\text{-adic and } h(\alpha) > 0\right\}.$$

Bombieri and Zannier [11] showed that for each prime p,

$$\sigma(p, \mathbb{Q}) \geq \frac{\log p}{2(p+1)}. \tag{3.1}$$

The lower bound for $\sigma(p, \mathbb{Q})$ in (3.1) was slightly improved by Fili and Petsche [19] to $\frac{p \log p}{2(p^2-1)}$, and significantly improved by Pottmeyer [34] to $\frac{\log(p/2)}{p+1}$.

For each rational prime p, define

$$\tau(p, \mathbb{Q}) = \inf\left\{h(\alpha) : \alpha \text{ is totally } p\text{-adic algebraic unit and } h(\alpha) > 0\right\}.$$

Recall that an algebraic integer α is said to be a unit if α^{-1} is also an algebraic integer. Petsche [32] drastically improved the lower bound (3.1) for algebraic units and proved that

$$\tau(p, \mathbb{Q}) \geq \frac{\log(p/2)}{p-1}. \tag{3.2}$$

Later, the lower bound for $\tau(p, \mathbb{Q})$ in (3.2) was slightly improved by Dubickas and Mossinghoff [18, Theorem 4.2].

For unramified primes, Mignotte [31] proved the following lower bound for $M(\alpha)$.

Theorem 3.1 ([31]). *Let α be an algebraic integer of degree d which is neither zero nor a root of unity. If there exists a rational prime $p < d \log d$ which is unramified in $\mathbb{Q}(\alpha)$, then $M(\alpha) \geq 1.2$. In particular, by taking $d \geq 3$, if 2 is unramified in $\mathbb{Q}(\alpha)$, then $M(\alpha) \geq 1.2$.*

In [21], Garza proved a natural counterpart to Mignotte's result for the case of total ramification. He proved the following.

Theorem 3.2 ([21]). *Let α be an algebraic integer of degree d which is neither zero nor a root of unity. If 2 is totally ramified in $\mathbb{Q}(\alpha)$, then $M(\alpha) \geq \sqrt[4]{2}$. Further, if there exists a rational prime $p > [\mathbb{Q}(\alpha) : \mathbb{Q}]$ which is totally ramified in $\mathbb{Q}(\alpha)$, then $M(\alpha) \geq \sqrt{5} - 1$.*

Looking at the above results, a natural question is what can we say about $M(\alpha)$ if 2 is neither unramified nor totally ramified in $\mathbb{Q}(\alpha)$? In the next section, we shall explore this case and provide some lower bound for $M(\alpha)$ in this direction.

3.2 Lower bound under prime factorization of 2

Let K be a number field. For a prime ideal $\mathcal{P}$ in $\mathcal{O}_K$, define $f_{\mathcal{P}} := [\mathcal{O}_K/\mathcal{P} : \mathbb{Z}/p\mathbb{Z}]$, where $p\mathbb{Z} = \mathcal{P} \cap \mathbb{Z}$. The following theorem proves a lower bound for $M(\alpha)$ under the prime factorization of $2\mathcal{O}_{\mathbb{Q}(\alpha)}$.

Theorem 3.3 ([38]). *Let $n \in \mathbb{N}$ and let*

$$S = \left\{ \alpha \in \overline{\mathbb{Q}} : 2\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\cdots\mathcal{P}_r^{e_r} \text{ with } f_{\mathcal{P}_i} = n, \text{ for all } i = 1, \ldots, r \right\}.$$

Then for all $\alpha \in S$, either $M(\alpha) \geq 2^{\frac{1}{4(2^n-1)}}$ or $M(\alpha) = 1$.

An immediate consequence of Theorem 3.3 for $n = 1$ is the following.

Corollary 3.4. *Let α be an algebraic integer of degree d which is neither zero nor a root of unity. Suppose $2\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\cdots\mathcal{P}_r^{e_r}$, where $\mathcal{P}_1, \ldots, \mathcal{P}_r$ are distinct prime ideals of $\mathcal{O}_{\mathbb{Q}(\alpha)}$, with $e_1 + e_2 + \cdots + e_r = d$. Then $M(\alpha) \geq \sqrt[4]{2} = 1.189\ldots$.*

Note that the case $r = 1$ in Corollary 3.4 corresponds to the first part of Theorem 3.2.

Remark 3.5. The lower bound $\sqrt[4]{2}$ in the Corollary 3.4 cannot be attained by any algebraic integer, i.e. there does not exist any algebraic integer α which satisfy the conditions of Theorem 3.3 such that $M(\alpha) = \sqrt[4]{2}$. Indeed, since $M(\alpha) = \pm a_d \prod_{|\alpha_i|>1} \alpha_i$, where a_d is the leading coefficient of the minimal polynomial of α over $\mathbb{Z}$ and α_i are its conjugates, Mahler measure of any algebraic number is always a Perron number. (Recall that a positive real number α is said to be a Perron number if $|\alpha_n| < \alpha$ for any conjugate $\alpha_n \neq \alpha$ of α). This was first observed by Adler and Marcus [1]. However, $\sqrt[4]{2}$ is not a Perron number and therefore $\sqrt[4]{2} \neq M(\alpha)$ for any algebraic integer α.

Proof of Theorem 3.3. Let n, S be in Theorem 3.3. Suppose $M(\alpha) \neq 1$. By Theorem 1.14, we can assume that α is a reciprocal algebraic integer, because if α is nonreciprocal, then $M(\alpha) \geq M(x^3 - x - 1) = 1.3247\ldots > \sqrt[4]{2}$. So $1/\alpha$ is also an algebraic integer. Thus α is a unit in $\mathcal{O}_K$. Put $K = \mathbb{Q}(\alpha)$. By our assumption

$$2\mathcal{O}_K = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\cdots\mathcal{P}_r^{e_r}$$

with $f_{\mathcal{P}_i} = n$ for all $i = 1, \ldots, r$. Since $n = [\mathcal{O}_K/\mathcal{P}_i : \mathbb{Z}/2\mathbb{Z}]$, we have $\left|\mathcal{O}_K/\mathcal{P}_i\right| = 2^n$ for all $i \in \{1, \ldots, r\}$. So $\alpha^{2^n} - \alpha \in \mathcal{P}_i$ for all $i \in \{1, \ldots, r\}$. Since α is a unit, we have $\alpha^{2^n-1} - 1 \in \mathcal{P}_i$ for all $i \in \{1, \ldots, r\}$.

For each $i \in \{1, \ldots, r\}$, choose s_i minimal such that $2^{s_i} \geq e_i$. For any fixed i, by the minimality of s_i, we have $2^m \leq e_i$, for all $m = 0, 1, \ldots, s_i - 1$. Since $2\mathcal{O}_K = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\cdots\mathcal{P}_r^{e_r} \subseteq \mathcal{P}_i^{e_i} \subseteq \mathcal{P}_i^{2^m}$ for all $m = 0, 1, \ldots, s_i - 1$, we have $2 \in \mathcal{P}_i^{2^m}$ for all $m = 0, 1, \ldots, s_i - 1$. Since $2 \in \mathcal{P}_i$ and $\alpha^{2^n-1} - 1 \in \mathcal{P}_i$, we have $\alpha^{2^n-1} - 1 + 2 = \alpha^{2^n-1} + 1 \in \mathcal{P}_i$; whence $\alpha^{2(2^n-1)} - 1 \in \mathcal{P}_i^2$. Since $2 \in \mathcal{P}_i^{2^m}$ for all $m = 0, 1, \ldots, s_i - 1$, repeating this argument, we get $\alpha^{2^{s_i}(2^n-1)} - 1 \in \mathcal{P}_i^{2^{s_i}} \subseteq \mathcal{P}_i^{e_i}$. Since $2 \in \mathcal{P}_i^{e_i}$, we have $\alpha^{2^{s_i}(2^n-1)} - 1 + 2 = \alpha^{2^{s_i}(2^n-1)} + 1 \in \mathcal{P}_i^{e_i}$. Thus, for all $i \in \{1, \ldots, r\}$,

$$\alpha^{2^{s_i+1}(2^n-1)} - 1 \in \mathcal{P}_i^{2e_i}.$$

Define $s = \max\{s_1, s_2, \ldots, s_r\}$. Without loss of generality, assume $s = s_1$. So,

$$\alpha^{2^{s+1}(2^n-1)} - 1 \in \mathcal{P}_1^{2e_1}.$$

Take any $i \neq 1$. Then $\alpha^{2^{s_i+1}(2^n-1)} - 1 \in \mathcal{P}_i^{2e_i}$. Since $2 \in \mathcal{P}_i$ and $\alpha^{2^{s_i+1}(2^n-1)} - 1 \in \mathcal{P}_i$, we get $\alpha^{2^{s_i+1}(2^n-1)} + 1 \in \mathcal{P}_i$; whence $\alpha^{2^{s_i+2}(2^n-1)} - 1 \in \mathcal{P}_i^{2e_i+1}$. Applying the same method inductively, we get $\alpha^{2^{s_i+s-s_i+1}(2^n-1)} - 1 \in \mathcal{P}_i^{2e_i+s-s_i}$. Thus $\alpha^{2^{s+1}(2^n-1)} - 1 \in \mathcal{P}_i^{2e_i+s-s_i} \subseteq \mathcal{P}_i^{2e_i}$. So, for all $i \in \{1, \ldots, r\}$ we have

$$\left|\alpha^{2^{s+1}(2^n-1)} - 1\right|_{\mathcal{P}_i} \leq 2^{\frac{-2e_i}{e_i}} = \frac{1}{4} \leq \frac{1}{4}\max\{1, |\alpha|_{\mathcal{P}_i}\}^{2^{s+1}(2^n-1)}.$$

If $v \mid \infty$, then $\left|\alpha^{2^{s+1}(2^n-1)} - 1\right|_v \leq |\alpha|_v^{2^{s+1}(2^n-1)} + 1 \leq 2\max\{1, |\alpha|_v^{2^{s+1}(2^n-1)}\}$.
Thus, we have

$$\left|\alpha^{2^{s+1}(2^n-1)} - 1\right|_v \leq \begin{cases} \frac{1}{4}\max\{1, |\alpha|_v\}^{2^{s+1}(2^n-1)} & \text{if } v \mid 2, \\ \max\{1, |\alpha|_v\}^{2^{s+1}(2^n-1)} & \text{if } v \nmid 2, v \nmid \infty, \\ 2\max\{1, |\alpha|_v\}^{2^{s+1}(2^n-1)} & \text{if } v \mid \infty. \end{cases} \tag{3.3}$$

Since α is not a root of unity, $\alpha^{2^{s+1}(2^n-1)} - 1 \neq 0$. Applying the product formula (1.36) to

the element $\alpha^{2^{s+1}(2^n-1)}-1$ and using (3.3), we get

$$\begin{aligned}
0 &= \sum_{v\in M_K}[K_v:\mathbb{Q}_v]\log\left|\alpha^{2^{s+1}(2^n-1)}-1\right|_v \\
&\leq \sum_{v|2}[K_v:\mathbb{Q}_v]\{-\log 4+2^{s+1}(2^n-1)\max\{0,\log|\alpha|_v\}\}+ \\
&\quad \sum_{v\nmid 2,v\nmid\infty}[K_v:\mathbb{Q}_v]\{2^{s+1}(2^n-1)\max\{0,\log|\alpha|_v\}\}+ \\
&\quad \sum_{v|\infty}[K_v:\mathbb{Q}_v]\{\log 2+2^{s+1}(2^n-1)\max\{0,\log|\alpha|_v\}\} \\
&= \sum_{v|2}-[K_v:\mathbb{Q}_v]\log 4+\sum_{v|\infty}[K_v:\mathbb{Q}_v]\log 2+ \\
&\quad \sum_{v\in M_K}2^{s+1}(2^n-1)\max\{0,\log|\alpha|_v\}[K_v:\mathbb{Q}_v].
\end{aligned}$$

By (1.35), we have

$$\sum_{v|2}[K_v:\mathbb{Q}_v]=[K:\mathbb{Q}] \quad \text{and} \quad \sum_{v|\infty}[K_v:\mathbb{Q}_v]=[K:\mathbb{Q}].$$

By (1.39), we have

$$\sum_{v\in M_K}[K_v:\mathbb{Q}_v]\max\{0,\log|\alpha|_v\}=[K:\mathbb{Q}]h(\alpha).$$

Therefore,

$$0\leq -[K:\mathbb{Q}]\log 4+[K:\mathbb{Q}]\log 2+2^{s+1}(2^n-1)[K:\mathbb{Q}]h(\alpha),$$

which implies

$$h(\alpha)\geq\frac{\log 2}{2^{s+1}(2^n-1)}.$$

Using the minimality of s, we have $2^{s+1}<4e_1\leq 4[\mathbb{Q}(\alpha):\mathbb{Q}]$. So

$$\frac{\log M(\alpha)}{[\mathbb{Q}(\alpha):\mathbb{Q}]}\geq\frac{\log 2}{4[\mathbb{Q}(\alpha):\mathbb{Q}](2^n-1)}.$$

Thus, we have $M(\alpha)\geq 2^{\frac{1}{4(2^n-1)}}$. This completes the proof of Theorem 3.3. □

3.3 Lower bound under prime factorization of odd rational prime

In the previous section, we prove a lower bound for $M(\alpha)$ subject to the prime factorization of $2\mathcal{O}_{\mathbb{Q}(\alpha)}$. So, it is natural to ask a lower bound for $M(\alpha)$ in terms of the prime factorization of an odd rational prime p in $\mathcal{O}_{\mathbb{Q}(\alpha)}$. We prove two results in this direction. The first one is the following.

Theorem 3.6 ([38]). *Let α be an algebraic integer of degree d which is neither zero nor a root of unity. If there exists an odd rational prime p such that $p\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\cdots\mathcal{P}_r^{e_r}$, where $\mathcal{P}_1,\ldots,\mathcal{P}_r$ are distinct prime ideals of $\mathcal{O}_{\mathbb{Q}(\alpha)}$, with $\max_{1\le i\le r}\{e_i\} \le p$ and $\sum_{i=1}^{r} e_i = d$, then*

$$h(\alpha) \ge \frac{\log(p/2)}{p(p-1)}.$$

Moreover, if $p \le \sqrt{d\log d}$, we have $M(\alpha) \ge c_1$, for some $c_1 > 1$.

We first proved the last part of Theorem 3.6 by assuming only $p \le \sqrt{d}$. During a discussion with Prof. M. Waldschmidt, he pointed out that the same conclusion holds for $p \le \sqrt{d\log d}$.

An immediate consequence of Theorem 3.6 is the following.

Corollary 3.7. *Let α be an algebraic integer of degree d such that $1 < M(\alpha) < c_1$. Consider any rational prime p with $2 < p \le \sqrt{d\log d}$. If*

$$p\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\cdots\mathcal{P}_r^{e_r},$$

then either

$$e_i > p, \text{ for some } i \in \{1,\ldots,r\}$$

or

$$[\mathcal{O}_{\mathbb{Q}(\alpha)}/\mathcal{P}_j : \mathbb{Z}/p\mathbb{Z}] > 1, \text{ for some } j \in \{1,\ldots,r\}.$$

Proof of Theorem 3.6. As in the proof of Theorem 3.3, we assume that α is a unit. Put $K = \mathbb{Q}(\alpha)$. Given that there exists an odd prime p such that

$$p\mathcal{O}_K = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\cdots\mathcal{P}_r^{e_r},$$

where $\max_{1\leq i\leq r}\{e_i\} \leq p$ and $\sum_{i=1}^{r} e_i = d$. Since $\sum_{i=1}^{r} e_i = d$, we have

$$f_{\mathcal{P}_i} = [\mathcal{O}_K/\mathcal{P}_i : \mathbb{Z}/p\mathbb{Z}] = 1, \text{ for all } i \in \{1,\ldots,r\}.$$

So $\left|\mathcal{O}_K/\mathcal{P}_i\right| = p$, for all $i \in \{1,\ldots,r\}$. Thus $\alpha^p - \alpha \in \mathcal{P}_i$ for all $i \in \{1,\ldots,r\}$. Since α is a unit, we have $\alpha^{p-1} - 1 \in \mathcal{P}_i$ for all $i \in \{1,\ldots,r\}$. So $\left(\alpha^{p-1}-1\right)^p \in \mathcal{P}_i^p \subseteq \mathcal{P}_i^{e_i}$. Hence by binomial theorem, we get $\alpha^{p(p-1)} - 1 \in \mathcal{P}_i^{e_i}$, for all $i = 1,\ldots,r$. So

$$\left|\alpha^{p(p-1)} - 1\right|_{\mathcal{P}_i} \leq p^{\frac{-e_i}{e_i}} = \frac{1}{p} \leq \frac{1}{p}\max\{1, |\alpha|_{\mathcal{P}_i}\}^{p(p-1)}.$$

If $v \mid \infty$, then $\left|\alpha^{p(p-1)} - 1\right|_v \leq |\alpha|_v^{p(p-1)} + 1 \leq 2\max\{1, |\alpha|_v^{p(p-1)}\}$.

Thus, we have

$$\left|\alpha^{p(p-1)} - 1\right|_v \leq \begin{cases} \frac{1}{p}\max\{1, |\alpha|_v\}^{p(p-1)} & \text{if } v \mid p, \\ \max\{1, |\alpha|_v\}^{p(p-1)} & \text{if } v \nmid p, v \nmid \infty, \\ 2\max\{1, |\alpha|_v\}^{p(p-1)} & \text{if } v \mid \infty. \end{cases} \tag{3.4}$$

Since α is not a root of unity, $\alpha^{p(p-1)} - 1 \neq 0$. Applying the product formula (1.36) to the element $\alpha^{p(p-1)} - 1$ and using (3.4), we get

$$\begin{aligned} 0 &= \sum_{v\in M_K} [K_v : \mathbb{Q}_v] \log \left|\alpha^{p(p-1)} - 1\right|_v \\ &\leq \sum_{v\mid p} [K_v : \mathbb{Q}_v]\{-\log p + p(p-1)\max\{0, \log|\alpha|_v\}\} + \\ &\quad \sum_{v\nmid p, v\nmid\infty} [K_v : \mathbb{Q}_v]\{p(p-1)\max\{0, \log|\alpha|_v\}\} + \\ &\quad \sum_{v\mid\infty} [K_v : \mathbb{Q}_v]\{\log 2 + p(p-1)\max\{0, \log|\alpha|_v\}\} \\ &= -\sum_{v\mid p} [K_v : \mathbb{Q}_v]\log p + \sum_{v\mid\infty} [K_v : \mathbb{Q}_v]\log 2 + \sum_{v\in M_K} p(p-1)\max\{0, \log|\alpha|_v\}[K_v : \mathbb{Q}_v]. \end{aligned}$$

By (1.35), we have

$$\sum_{v|p}[K_v:\mathbb{Q}_v]=[K:\mathbb{Q}] \quad \text{and} \quad \sum_{v|\infty}[K_v:\mathbb{Q}_v]=[K:\mathbb{Q}].$$

By (1.39), we have

$$\sum_{v\in M_K}[K_v:\mathbb{Q}_v]\max\{0,\log|\alpha|_v\}=[K:\mathbb{Q}]h(\alpha).$$

Therefore,

$$0\leq -[K:\mathbb{Q}]\log p+[K:\mathbb{Q}]\log 2+p(p-1)[K:\mathbb{Q}]h(\alpha),$$

which implies

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

This completes the proof of the first part of Theorem 3.6.

For the last part, if $p\leq\sqrt{d}$, then $p(p-1)\leq d$. So $\frac{\log(p/2)}{p(p-1)}\geq\frac{\log(p/2)}{d}$. Thus, we have $M(\alpha)\geq p/2$. If $\sqrt{d}<p\leq\sqrt{d\log d}$, then for $d\geq 16$,

$$\frac{\log(p/2)}{p(p-1)}\geq\frac{\log(\sqrt{d}/2)}{d\log d}\geq\frac{1}{4d}.$$

Thus, $M(\alpha)\geq\sqrt[4]{e}$. This completes the last part of the proof. □

The second result for odd rational prime is the following.

Theorem 3.8 ([38]). *Let α be an algebraic integer of degree d which is neither zero nor a root of unity. If there exists an odd rational prime p such that $p\mathcal{O}_{\mathbb{Q}(\alpha)}=\mathcal{P}_1\mathcal{P}_2\cdots\mathcal{P}_d$, where $\mathcal{P}_1,\ldots,\mathcal{P}_d$ are distinct prime ideals of $\mathcal{O}_{\mathbb{Q}(\alpha)}$, then*

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

Moreover, if $p\leq d\log d$, we have $M(\alpha)\geq c_2$, for some constant $c_2>1$.

We first proved the last part of Theorem 3.8 by assuming only $p \leq d$. During a discussion with Prof. M. Waldschmidt, he pointed out that the same conclusion holds for $p \leq d \log d$.

As mentioned in the introduction, Pottmeyer [34, Theorem 1.1] also proved the first part of Theorem 3.8, but our method of proof is simple and different.

Proof. As in the proof of Theorem 3.3, we assume that α is a unit. Put $K = \mathbb{Q}(\alpha)$. Given that there exists an odd prime number p such that

$$p\mathcal{O}_K = \mathcal{P}_1\mathcal{P}_2 \cdots \mathcal{P}_d,$$

Since p splits completely in K, we have $[\mathcal{O}_K/\mathcal{P}_i : \mathbb{Z}/p\mathbb{Z}] = 1$ for all $i \in \{1, \ldots, d\}$. Thus $\left|\mathcal{O}_K/\mathcal{P}_i\right| = p$ for all $i \in \{1, \ldots, d\}$. Thus $\alpha^p - \alpha \in \mathcal{P}_i$ for all $i \in \{1, \ldots, d\}$. Since α is a unit, we have $\alpha^{p-1} - 1 \in \mathcal{P}_i$ for all $i \in \{1, \ldots, d\}$. So

$$\left|\alpha^{p-1} - 1\right|_{\mathcal{P}_i} \leq \frac{1}{p} \leq \frac{1}{p} \max\{1, |\alpha|_{\mathcal{P}_i}\}^{p-1}.$$

If $v \mid \infty$, then $\left|\alpha^{p-1} - 1\right|_v \leq |\alpha|_v^{p-1} + 1 \leq 2\max\{1, |\alpha|_v^{p-1}\}$.

Thus we have

$$\left|\alpha^{p-1} - 1\right|_v \leq \begin{cases} \frac{1}{p}\max\{1, |\alpha|_v\}^{p-1} & \text{if } v \mid p, \\ \max\{1, |\alpha|_v\}^{p-1} & \text{if } v \nmid p, v \nmid \infty, \\ 2\max\{1, |\alpha|_v\}^{p-1} & \text{if } v \mid \infty. \end{cases} \tag{3.5}$$

Since α is not a root of unity, $\alpha^{p-1} - 1 \neq 0$. Applying the product formula (1.36) to the

element $\alpha^{p-1}-1$ and using (3.5), we get

$$\begin{aligned}
0 &= \sum_{v\in M_K}[K_v:\mathbb{Q}_v]\log\left|\alpha^{p-1}-1\right|_v \\
&\le \sum_{v|p}[K_v:\mathbb{Q}_v]\{-\log p+(p-1)\max\{0,\log|\alpha|_v\}\}+ \\
&\quad \sum_{v\nmid p,v\nmid\infty}[K_v:\mathbb{Q}_v]\{(p-1)\max\{0,\log|\alpha|_v\}\}+ \\
&\quad \sum_{v|\infty}[K_v:\mathbb{Q}_v]\{\log 2+(p-1)\max\{0,\log|\alpha|_v\}\} \\
&= -\sum_{v|p}[K_v:\mathbb{Q}_v]\log p+\sum_{v|\infty}[K_v:\mathbb{Q}_v]\log 2+\sum_{v\in M_K}(p-1)\max\{0,\log|\alpha|_v\}[K_v:\mathbb{Q}_v].
\end{aligned}$$

By (1.35), we have

$$\sum_{v|p}[K_v:\mathbb{Q}_v]=[K:\mathbb{Q}] \quad \text{and} \quad \sum_{v|\infty}[K_v:\mathbb{Q}_v]=[K:\mathbb{Q}].$$

Also, by (1.39), we have

$$\sum_{v\in M_K}[K_v:\mathbb{Q}_v]\max\{0,\log|\alpha|_v\}=[K:\mathbb{Q}]h(\alpha).$$

Therefore,

$$0\le -[K:\mathbb{Q}]\log p+[K:\mathbb{Q}]\log 2+(p-1)[K:\mathbb{Q}]h(\alpha),$$

which implies

$$h(\alpha)\ge\frac{\log(p/2)}{p-1}.$$

This completes the proof of the first part of Theorem 3.8.

For the last part, if $p\le d$, then $\frac{\log M(\alpha)}{d}\ge\frac{\log(p/2)}{p-1}\ge\frac{\log(p/2)}{d}$. Thus, $M(\alpha)\ge p/2$.

If $d<p\le d\log d$, then for $d\ge 4$,

$$\frac{\log(p/2)}{p-1}\ge\frac{\log(d/2)}{d\log d}\ge\frac{1}{2d}.$$

Thus, $M(\alpha)\ge\sqrt{e}$. This completes the last part of the proof. □

An immediate corollary of Theorem 3.8 is the following.

Corollary 3.9. *Let α be an algebraic integer of degree d such that $1 < M(\alpha) < c_2$. Then there are no odd rational prime p with $p \leq d \log d$ that splits completely in $\mathbb{Q}(\alpha)$.*

3.4 Base field is a number field

In this section, we generalize the results of Section 3.2 and Section 3.3 to number fields K. Here, our results are based on how primes in $\mathcal{O}_K$ splits in $\mathcal{O}_{K(\alpha)}$.

First, we need to generalize the definition of totally p-adic algebraic unit to a number field K. For any prime ideal $\mathcal{P} \in \mathcal{O}_K$ and any $\alpha \in \overline{\mathbb{Q}} \setminus \{0\}$, we say that α is totally $\mathcal{P}$-adic, if $\mathcal{P}$ splits into $[K(\alpha) : K]$ distinct prime ideals in $\mathcal{O}_{K(\alpha)}$. Define

$$\tau(\mathcal{P}, K) = \inf\Big\{h(\alpha) : \alpha \in \overline{\mathbb{Q}} \text{ is totally } \mathcal{P}\text{-adic algebraic unit and } h(\alpha) > 0\Big\}.$$

Petsche [32] proved that

$$\tau(\mathcal{P}, K) \geq \frac{\log\left(||P||/2^{[K:\mathbb{Q}]}\right)}{(||P|| - 1)[K : \mathbb{Q}]}, \tag{3.6}$$

where $||P||$ is the absolute norm of $\mathcal{P}$. Note that the lower bound (3.6) is only nontrivial when $||P|| > 2^{[K:\mathbb{Q}]}$. A natural question is whether or not we can give a similar lower bound for $h(\alpha)$ for other classes of algebraic units. We prove two results regarding this question. The first result is the following.

Theorem 3.10 ([35])**.** *Let α be an algebraic unit which is not a root of unity. Let $\mathcal{P}$ be a prime ideal, which lies above a rational odd prime p, of the ring of integer $\mathcal{O}_K$ of a number field K of degree d over $\mathbb{Q}$. Suppose*

$$\mathcal{P}\mathcal{O}_{K(\alpha)} = \mathscr{P}_1^{e_1}\mathscr{P}_2^{e_2}\cdots\mathscr{P}_r^{e_r},$$

where $\mathscr{P}_1, \ldots, \mathscr{P}_r$ are distinct prime ideals of $\mathcal{O}_{K(\alpha)}$ with $e_1 + \cdots + e_r = [K(\alpha) : K]$ and $\max_{1\leq i\leq r}\{e_i\} \leq p$. Then $h(\alpha) \geq c$, where $c > 0$ is a constant depending only on p and $[K : \mathbb{Q}] = d$.

Note that when $e_i = 1$ for all $i = 1, \ldots, r$ in Theorem 3.10, we get $\tau(\mathcal{P}, K) \geq c$, where $c > 0$ is a constant which depends only p and $[K : \mathbb{Q}]$. Hence, in this case, our lower bound is always nontrivial, unlike (3.6).

Our second result is the following.

Theorem 3.11 ([35]). *Let α be an algebraic unit which is not a root of unity. Let $\mathcal{P}$ be a prime ideal, which lies above 2, of the ring of integer $\mathcal{O}_K$ of a number field K of degree d over $\mathbb{Q}$. Suppose*

$$\mathcal{P}\mathcal{O}_{K(\alpha)} = \mathscr{P}_1^{e_1}\mathscr{P}_2^{e_2}\cdots\mathscr{P}_r^{e_r},$$

where $\mathscr{P}_1, \ldots, \mathscr{P}_r$ are distinct prime ideals of $\mathcal{O}_{K(\alpha)}$ with $e_1 + \cdots + e_r = [K(\alpha) : K]$. Then $M(\alpha) \geq C(K)$, where $C(K) > 1$ is a constant which depends only on $[K : \mathbb{Q}] = d$.

3.4.1 Prime factorization of primes lying above odd rational prime

In this section, we prove Theorem 3.10. First, we prove the following auxiliary lemma. It is a slight generalization of [3, Lemma 2.1]. The proof follows their technique.

Lemma 3.12. *Let K be a number field and $\beta_1, \beta_2 \in \mathcal{O}_K$. Let S be a finite set of places of K which lies over a rational prime p. Suppose $\eta > 0$ be such that for all $v \in S$*

$$|\beta_1 - \beta_2|_v \leq p^{-\eta}. \tag{3.7}$$

Then for any $n \in \mathbb{N}$, there exists a positive real number $s_{p,\eta}(n)$, such that for all $v \in S$

$$\left|\beta_1^{p^n} - \beta_2^{p^n}\right|_v \leq p^{-s_{p,\eta}(n)}$$

with $s_{p,\eta}(n) \to \infty$ as $n \to \infty$.

Proof. Let $v \in S$. For any $n \in \mathbb{N}$, ζ_{p^n} denotes a primitive root of unity of order p^n. We denote the only valuation of $K(\zeta_{p^n})$ extending v by the same letter v. For any $j \in \mathbb{N}$, since

p is totally ramified in $\mathbb{Q}(\zeta_{p^j})$, we have $|1-\zeta_{p^j}|_v = p^{-1/p^{j-1}(p-1)}$. Also, since $\beta_2 \in \mathcal{O}_K$ and v is a nonarchimedean absolute value, $|\beta_2|_v \leq 1$. Using this and (3.7), we obtain

$$\begin{aligned}\left|\beta_1 - \zeta_{p^j}\beta_2\right|_v &= \left|\beta_1 - \beta_2 + (1-\zeta_{p^j})\beta_2\right|_v \\ &\leq \max\left\{p^{-\eta}, p^{-1/p^{j-1}(p-1)}\right\} \\ &= p^{\frac{-\min\left\{p^{j-1}(p-1)\eta,1\right\}}{p^{j-1}(p-1)}}.\end{aligned}$$

Since

$$\beta_1^{p^n} - \beta_2^{p^n} = (\beta_1-\beta_2)\prod_{j=1}^{n}\prod_{\zeta_{p^j}}(\beta_1 - \zeta_{p^j}\beta_2),$$

where the second product is taken over all the roots of unity ζ_{p^j} of order p^j, we obtain

$$\begin{aligned}\left|\beta_1^{p^n} - \beta_2^{p^n}\right|_v &= |\beta_1-\beta_2|_v \prod_{j=1}^{n}\prod_{\zeta_{p^j}}\left|(\beta_1 - \zeta_{p^j}\beta_2)\right|_v \\ &\leq p^{-\eta}\prod_{j=1}^{n} p^{-\min\{p^{j-1}(p-1)\eta,1\}} \\ &= p^{-\eta}p^{-\sum_{j=1}^{n}\min\{p^{j-1}(p-1)\eta,1\}} \\ &= p^{-s},\end{aligned}$$

where

$$s = \eta + \sum_{j=1}^{n}\min\{p^{j-1}(p-1)\eta, 1\}.$$

Define an integer $k = k_{p,\eta}$ by $k = 0$ if $(p-1)\eta > 1$ and by

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

otherwise. Then

$$s = \eta + \sum_{j=1}^{k} p^{j-1}(p-1)\eta + \sum_{j=k+1}^{n} 1 = p^k\eta + \max\{0, n-k\}.$$

By taking

$$s_{p,\eta}(n) = p^k\eta + \max\{0, n-k\}$$

completes the proof of the lemma. □

Proof of Theorem 3.10. Put $L = K(\alpha)$. Given that $\mathcal{P}$ is a prime ideal in $\mathcal{O}_K$ such that $\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$ and

$$\mathcal{P}\mathcal{O}_L = \mathscr{P}_1^{e_1}\mathscr{P}_2^{e_2}\cdots\mathscr{P}_r^{e_r},$$

where $\max_{1\le i\le r}\{e_i\} \le p$ and $\sum_{i=1}^{r} e_i = [L:K]$. Since $\sum_{i=1}^{r} e_i = [L:K]$, we have

$$[\mathcal{O}_L/\mathscr{P}_i : \mathcal{O}_K/\mathcal{P}] = 1, \text{ for all } i \in \{1,\dots,r\}.$$

Let f be the inertia degree of $\mathcal{P}$ over p. So $\left|\mathcal{O}_L/\mathscr{P}_i\right| = \left|\mathcal{O}_K/\mathcal{P}\right| = p^f$, for all $i \in \{1,\dots,r\}$. Thus $\alpha^{p^f} - \alpha \in \mathscr{P}_i$ for all $i \in \{1,\dots,r\}$. Since α is a unit, we have $\alpha^{p^f-1} - 1 \in \mathscr{P}_i$ for all $i \in \{1,\dots,r\}$. So $\left(\alpha^{p^f-1}-1\right)^p \in \mathscr{P}_i^p \subseteq \mathscr{P}_i^{e_i}$. Hence by binomial theorem, we get $\alpha^{p(p^f-1)} - 1 \in \mathscr{P}_i^{e_i}$, for all $i = 1,\dots,r$. So for all $i = 1,\dots,r$

$$\left|\alpha^{p(p^f-1)} - 1\right|_{\mathscr{P}_i} \le p^{\frac{-e_i}{e_i e}} = p^{-1/e} \le p^{-1/d},$$

where e is the ramification degree of $\mathcal{P}$ over p. Applying Lemma 3.12, we deduce that there exists a λ which depends only on p and d such that

$$\left|\alpha^{p(p^f-1)p^\lambda} - 1\right|_{\mathscr{P}_i} \le p^{-d}, \text{ for all } i = 1,\dots,r.$$

If $v \mid \infty$, then $\left|\alpha^{p(p^f-1)p^\lambda} - 1\right|_v \le |\alpha|_v^{p(p^f-1)p^\lambda} + 1 \le 2\max\{1,|\alpha|_v\}^{p(p^f-1)p^\lambda}$.
Thus we have

$$\left|\alpha^{p(p^f-1)p^\lambda} - 1\right|_v \le \begin{cases} p^{-d}\max\{1,|\alpha|_v\}^{p(p^f-1)p^\lambda} & \text{if } v \mid \mathcal{P}, \\ \max\{1,|\alpha|_v\}^{p(p^f-1)p^\lambda} & \text{if } v \nmid \mathcal{P}, v \nmid \infty, \\ 2\max\{1,|\alpha|_v\}^{p(p^f-1)p^\lambda} & \text{if } v \mid \infty. \end{cases} \tag{3.8}$$

Since α is not a root of unity, $\alpha^{p(p^f-1)p^\lambda} - 1 \neq 0$. Applying the product formula (1.36) to

the element $\alpha^{p(p^f-1)p^\lambda}-1$ and using (3.8), we obtain

$$\begin{aligned}
0 &= \sum_{v\in M_L}[L_v:\mathbb{Q}_v]\log\left|\alpha^{p(p^f-1)p^\lambda}-1\right|_v \\
&\le \sum_{v|\mathcal{P}}[L_v:\mathbb{Q}_v]\{-d\log p + p(p^f-1)p^\lambda\max\{0,\log|\alpha|_v\}\}+ \\
&\quad \sum_{v\nmid\mathcal{P},v\nmid\infty}[L_v:\mathbb{Q}_v]\{p(p^f-1)p^\lambda\max\{0,\log|\alpha|_v\}\}+ \\
&\quad \sum_{v|\infty}[L_v:\mathbb{Q}_v]\{\log 2 + p(p^f-1)p^\lambda\max\{0,\log|\alpha|_v\}\} \\
&= \sum_{v|\mathcal{P}}-[L_v:\mathbb{Q}_v]d\log p + \sum_{v|\infty}[L_v:\mathbb{Q}_v]\log 2+ \\
&\quad \sum_{v\in M_L}p(p^f-1)p^\lambda[L_v:\mathbb{Q}_v]\max\{0,\log|\alpha|_v\}.
\end{aligned}$$

By (1.39), we have

$$\sum_{v\in M_L}[L_v:\mathbb{Q}_v]\max\{0,\log|\alpha|_v\} = [L:\mathbb{Q}]h(\alpha),$$

and by (1.35), we have

$$\sum_{v|\infty}[L_v:\mathbb{Q}_v] = [L:\mathbb{Q}].$$

Therefore,

$$0 \le -d\log p\sum_{v|\mathcal{P}}[L_v:K_\mathcal{P}][K_\mathcal{P}:\mathbb{Q}_p] + [L:\mathbb{Q}]\log 2 + p(p^f-1)p^\lambda[L:\mathbb{Q}]h(\alpha).$$

Since

$$\sum_{v|\mathcal{P}}[L_v:K_\mathcal{P}] = [L:K],$$

we have

$$0 \le -d\log p\frac{[K_\mathcal{P}:\mathbb{Q}_p][L:\mathbb{Q}]}{[K:\mathbb{Q}]} + [L:\mathbb{Q}]\log 2 + p(p^f-1)p^\lambda[L:\mathbb{Q}]h(\alpha).$$

So

$$h(\alpha) \ge \frac{[K_\mathcal{P}:\mathbb{Q}_p]\log p - \log 2}{p(p^f-1)p^\lambda} \ge \frac{\log(p/2)}{p(p^f-1)p^\lambda} \ge \frac{\log(p/2)}{p(p^d-1)p^\lambda}.$$

Since λ is only a function of p and d, this completes the proof of Theorem 3.10. □

3.4.2 Prime factorization of primes lying above 2

In this section, we prove Theorem 3.11.

Proof of Theorem 3.11. Put $L = K(\alpha)$. Given $\mathcal{P}\mathcal{O}_L = \mathscr{P}_1^{e_1}\mathscr{P}_2^{e_2}\cdots\mathscr{P}_r^{e_r}$, where $e_1 + e_2 + \cdots + e_r = [L : K]$. So, $[\mathcal{O}_L/\mathscr{P}_i : \mathcal{O}_K/\mathcal{P}] = 1$, for all $i \in \{1, \ldots, r\}$. Let f be the inertia degree of $\mathcal{P}$ over 2. So $\left|\mathcal{O}_L/\mathscr{P}_i\right| = \left|\mathcal{O}_K/\mathcal{P}\right| = 2^f$ for all $i \in \{1, \ldots, r\}$. Thus

$$\alpha^{2^f} - \alpha \in \mathscr{P}_i \text{ for all } i \in \{1, \ldots, r\}.$$

Since α is a unit, we have

$$\alpha^{2^f-1} - 1 \in \mathscr{P}_i \text{ for all } i \in \{1, \ldots, r\}.$$

For each $i \in \{1, \ldots, r\}$, choose s_i minimal such that $2^{s_i} \geq e_i$. For any fixed i, by the minimality of s_i, we have $2^n < e_i$, for all $n = 0, 1, \ldots, s_i - 1$. Since

$$\mathcal{P}\mathcal{O}_L = \mathscr{P}_1^{e_1}\mathscr{P}_2^{e_2}\cdots\mathscr{P}_r^{e_r} \subseteq \mathscr{P}_i^{e_i} \subseteq \mathscr{P}_i^{2^n}$$

for all $n = 0, 1, \ldots, s_i - 1$, we have $2 \in \mathscr{P}_i^{2^n}$ for all $n = 0, 1, \ldots, s_i - 1$. Since $2 \in \mathscr{P}_i$ and $\alpha^{2^f-1} - 1 \in \mathscr{P}_i$, we have $\alpha^{2^f-1} - 1 + 2 = \alpha^{2^f-1} + 1 \in \mathscr{P}_i$; whence $\alpha^{2^{f+1}-2} - 1 \in \mathscr{P}_i^2$. Using $2 \in \mathscr{P}_i^{2^n}$ for all $n = 0, 1, \ldots, s_i - 1$ and applying the same method inductively, we get

$$\alpha^{2^{f+s_i}-2^{s_i}} - 1 \in \mathscr{P}_i^{2^{s_i}} \subseteq \mathcal{P}_i^{e_i}.$$

Define $s = \max\{s_1, s_2, \ldots, s_r\}$. Without loss of generality, assume $s = s_1$. So, $\alpha^{2^{f+s}-2^s} - 1 \in \mathscr{P}_1^{e_1}$. Take any $i \neq 1$. Then $\alpha^{2^{f+s_i}-2^{s_i}} - 1 \in \mathscr{P}_i^{e_i}$. Since $2 \in \mathcal{P}_i$ and $\alpha^{2^{f+s_i}-2^{s_i}} - 1 \in \mathscr{P}_i$, we get $\alpha^{2^{f+s_i}-2^{s_i}} + 1 \in \mathscr{P}_i$; whence $\alpha^{2^{f+s_i+1}-2^{s_i+1}} - 1 \in \mathscr{P}_i^{e_i+1}$. Applying the same method inductively, we get $\alpha^{2^{f+s_i+s-s_i}-2^{s_i+s-s_i}} - 1 \in \mathscr{P}_i^{e_i+s-s_i}$. Thus $\alpha^{2^{f+s}-2^s} - 1 \in \mathscr{P}_i^{e_i+s-s_i} \subseteq \mathscr{P}_i^{e_i}$. So, for all $i \in \{1, \ldots, r\}$ we have

$$\left|\alpha^{2^{f+s}-2^s} - 1\right|_{\mathscr{P}_i} \leq 2^{\frac{-e_i}{e_i e}} = 2^{\frac{-1}{e}} \leq 2^{\frac{-1}{d}},$$

where e is the ramification degree of $\mathcal{P}$ over 2. Applying Lemma 3.12, we deduce that there exists a λ which depends only on d such that

$$\left|\alpha^{(2^{f+s}-2^s)2^\lambda}-1\right|_{\mathscr{P}_i}\leq 2^{-2d},\quad \text{for all } i=1,\dots,r.$$

If $v\mid\infty$, then $\left|\alpha^{(2^{f+s}-2^s)2^\lambda}-1\right|_v\leq|\alpha|_v^{(2^{f+s}-2^s)2^\lambda}+1\leq 2\max\{1,|\alpha|_v\}^{(2^{f+s}-2^s)2^\lambda}$.
Thus we have

$$\left|\alpha^{(2^{f+s}-2^s)2^\lambda}-1\right|_v\leq\begin{cases}2^{-2d}\max\{1,|\alpha|_v\}^{(2^{f+s}-2^s)2^\lambda} & \text{if } v\mid\mathcal{P},\\ \max\{1,|\alpha|_v\}^{(2^{f+s}-2^s)2^\lambda} & \text{if } v\nmid\mathcal{P},v\nmid\infty,\\ 2\max\{1,|\alpha|_v\}^{(2^{f+s}-2^s)2^\lambda} & \text{if } v\mid\infty.\end{cases}\tag{3.9}$$

Since α is not a root of unity, $\alpha^{(2^{f+s}-2^s)2^\lambda}-1\neq 0$. Applying the product formula (1.36) to the element $\alpha^{(2^{f+s}-2^s)2^\lambda}-1$ and using (3.9), we obtain

$$\begin{aligned}0&=\sum_{v\in M_L}[L_v:\mathbb{Q}_v]\log\left|\alpha^{(2^{f+s}-2^s)2^\lambda}-1\right|_v\\&\leq\sum_{v\mid\mathcal{P}}[L_v:\mathbb{Q}_v]\{-2d\log 2+(2^{f+s}-2^s)2^\lambda\max\{0,\log|\alpha|_v\}\}+\\&\quad\sum_{v\nmid\mathcal{P},v\nmid\infty}[L_v:\mathbb{Q}_v]\{(2^{f+s}-2^s)2^\lambda\max\{0,\log|\alpha|_v\}\}+\\&\quad\sum_{v\mid\infty}[L_v:\mathbb{Q}_v]\{\log 2+(2^{f+s}-2^s)2^\lambda\max\{0,\log|\alpha|_v\}\}\\&=\sum_{v\mid\mathcal{P}}-[L_v:\mathbb{Q}_v]2d\log 2+\sum_{v\mid\infty}[L_v:\mathbb{Q}_v]\log 2+\\&\quad\sum_{v\in M_L}(2^{f+s}-2^s)2^\lambda[L_v:\mathbb{Q}_v]\max\{0,\log|\alpha|_v\}.\end{aligned}$$

Since

$$\sum_{v\in M_L}[L_v:\mathbb{Q}_v]\max\{0,\log|\alpha|_v\}=[L:\mathbb{Q}]h(\alpha)$$

and

$$\sum_{v\mid\infty}[L_v:\mathbb{Q}_v]=[L:\mathbb{Q}],$$

we get

$$0 \leq -2d \log 2 \sum_{v|\mathcal{P}} [L_v : K_{\mathcal{P}}][K_{\mathcal{P}} : \mathbb{Q}_2] + [L : \mathbb{Q}] \log 2 + (2^{f+s} - 2^s)2^{\lambda}[L : \mathbb{Q}]h(\alpha).$$

Using

$$\sum_{v|\mathcal{P}} [L_v : K_{\mathcal{P}}] = [L : K],$$

we have

$$0 \leq -2d \log 2 \frac{[K_{\mathcal{P}} : \mathbb{Q}_2][L : \mathbb{Q}]}{[K : \mathbb{Q}]} + [L : \mathbb{Q}] \log 2 + (2^{f+s} - 2^s)2^{\lambda}[L : \mathbb{Q}]h(\alpha).$$

Thus

$$h(\alpha) \geq \frac{[K_{\mathcal{P}} : \mathbb{Q}_2] \log 4 - \log 2}{(2^{f+s} - 2^s)2^{\lambda}} \geq \frac{\log 2}{2^s(2^f - 1)2^{\lambda}}.$$

Using the minimality of s, we have $2^s < 2e_1 \leq 2[K(\alpha) : K] \leq 2[\mathbb{Q}(\alpha) : \mathbb{Q}]$. Also, since $f \leq d$, we get

$$\frac{\log M(\alpha)}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} \geq \frac{\log 2}{2[\mathbb{Q}(\alpha) : \mathbb{Q}](2^d - 1)2^{\lambda}}.$$

Thus, we have

$$M(\alpha) \geq 1 + \frac{\log 2}{2^{\lambda+1}(2^d - 1)}.$$

Since λ is only a function of d, this completes the proof of Theorem 3.11. □

Chapter 4

Algebraic points of Weierstrass sigma functions

4.1 Introduction

The problem of counting integral points on graphs of different kinds of functions can be traced back to the work of Jarnik [24]: he proved that a strictly convex arc $y = f(x)$ of length l contains at most

$$3(4\pi)^{-1/3}l^{2/3} + O(l^{1/3}) \tag{4.1}$$

integral points. Recall that $f(x) = O(g(x))$ if there exists a real number $M > 0$ and a real number x_0 such that $|f(x)| \leq Mg(x)$ for all $x \geq x_0$. In (4.1), the exponents and the constants are best possible. In the seminal paper of Bombieri and Pila [10], along with several other results, they proved an upper bound for the number of integral points on the homothetic dilation of transcendental real analytic functions. If Γ is the graph of f, then the homothetic dilation of Γ by a real number $t > 0$, denoted by $t\Gamma$, is defined by

$$t\Gamma = \left\{(tx, tf(x)) : (x, f(x)) \in \Gamma\right\}.$$

Theorem 4.1 ([10]). *Let Γ be the graph of a real analytic transcendental function f on a closed and bounded interval I of $\mathbb{R}$. For any $\varepsilon > 0$, there exists a constant $C_1(f, \varepsilon)$ such that, for all $t \geq 1$,*

$$\left|t\Gamma \cap \mathbb{Z}^2\right| \leq C_1(f, \varepsilon)t^{\varepsilon}.$$

Note that, if $t = H$ is an positive integer, then the number of rational points on Γ of denominator H is same as the number of integral points on $H\Gamma$ and therefore, there are at

most $C_1(f,\varepsilon)H^{\varepsilon}$ such points. Later, Pila [33] generalized this theorem by counting rational points whose absolute values of both numerator and denominator at most H on Γ. He proved the following.

Theorem 4.2 ([33]). *Let Γ be the graph of a real analytic transcendental function f on a closed and bounded interval I of $\mathbb{R}$. Let $\varepsilon > 0$. Then there exists a constant $C_2(f,\varepsilon)$ such that, for any $H \in \mathbb{N}$, the number of rational points whose numerator and denominator have absolute values at most H on Γ is at most $C_2(f,\varepsilon)H^{\varepsilon}$.*

It is also shown in [10] that these bounds are best possible in general. However, for some special functions, the upper bound could be improved to one of the form $c(\log H)^{\eta}$, for some $c, \eta > 0$. For example, Masser [30] proved such bound for the Riemann ζ-function.

Theorem 4.3 ([30]). *There exists an absolute constant $C_3 > 0$ such that for any integer $H \geq 3$, the number of rational q with $q \in (2,3)$ such that both q and $\zeta(q)$ have denominator at most H is at most $C_3 \left(\log H / \log\log H\right)^2$.*

In the same paper, Masser suggested to prove analogue of his theorem for other functions; namely, the Weierstrass zeta function, Euler Gamma function, Weierstrass sigma function and so on.

For a lattice $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ in $\mathbb{C}$, the corresponding Weierstrass sigma function is defined by

$$\sigma_{\Omega}(z) = z \prod_{\omega \in \Omega \setminus \{0\}} \left(1 - \frac{z}{\omega}\right) \exp\left(\frac{z}{\omega} + \frac{z^2}{2\omega^2}\right),$$

while the associated Weierstrass zeta function is defined by

$$\zeta_{\Omega}(z) = \frac{\sigma'_{\Omega}(z)}{\sigma_{\Omega}(z)}.$$

For an algebraic number α of degree d, its *multiplicative height* is defined by $H(\alpha) = \left(M(\alpha)\right)^{1/d}$, where $M(\alpha)$ is its Mahler measure. For a pair α, β of algebraic numbers, we

put $H(\alpha,\beta)=\max\{H(\alpha),H(\beta)\}$. Following the suggestion of Masser, Jones and Thomas [25] proved the following density result for the Weierstrass zeta function along with several other results.

Theorem 4.4 ([25]). *Let $\Omega=\mathbb{Z}\omega_1+\mathbb{Z}\omega_2$ be a lattice in $\mathbb{C}$ and $\zeta_\Omega(z)$ be the corresponding Weierstrass ζ-function. Then there exist constants $R=R(\Omega)>0$ and $C_4=C_4(d,\Omega)>0$ such that there are at most $C_4(\log H)^{15}$ algebraic points z which satisfy $[\mathbb{Q}(z,\zeta_\Omega(z)):\mathbb{Q}]\leq d$ and $H(z,\zeta_\Omega(z))\leq H$ and $\left|z-\frac{\omega_1+\omega_2}{4}\right|\leq R$.*

In [14], Boxall and Jones proved an upper bound by putting order condition on entire functions. Recall that the order of an entire function f is defined by

$$\rho=\limsup_{r\to\infty}\frac{\log\log M_f(r)}{\log r},$$

while its lower order is defined by

$$\lambda=\liminf_{r\to\infty}\frac{\log\log M_f(r)}{\log r},$$

where $M_f(r)=\max_{|z|\leq r}|f(z)|$.

Theorem 4.5 ([14]). *Let f be a nonconstant entire function having ρ as its finite order and λ as its positive lower order. Suppose $r>0$ be a real number. Then there exist positive constants $C_5=C_5(f,r)$ and $n=n(\rho,\lambda)$ such that for $H>e$, there are at most $C_5(\log H)^n$ rational numbers $q\in[-r,r]$ such that both q and $f(q)$ have height at most H.*

To state some results, we need following definitions. Let $d\geq 1, H\geq 1$ be real numbers. For any function f and any subset $\mathcal{Z}\subseteq\mathbb{C}$, define

$$S_f(\mathcal{Z},d,H)=\left\{z\in\overline{\mathbb{Q}}:z\in\mathcal{Z},[\mathbb{Q}(z,f(z)):\mathbb{Q}]\leq d,H(z,f(z))\leq H\right\}$$

and

$$S_f(d,H)=\left\{z\in\overline{\mathbb{Q}}:[\mathbb{Q}(z,f(z)):\mathbb{Q}]\leq d,H(z,f(z))\leq H\right\}.$$

Besson [7] was the first to study the number of algebraic points of bounded degrees and bounded heights on the graph of Weierstrass σ-function. He proved the following.

Theorem 4.6 ([7]). *For $R \geq 2$, define $\mathcal{Z}_R = \{z \in \overline{\mathbb{Q}} : |z| \leq R\}$. Then for all $d \geq 1,\ H \geq 3$*

$$\left|S_{\sigma_\Omega}(\mathcal{Z}_R, d, H)\right| \leq C_6 R^{10} \log R \frac{d^4 (\log H)^2}{\log(d \log H)},$$

for some effective constant $C_6 = C_6(\Omega) > 0$.

In this result, Besson counts algebraic points on a bounded domain. Recently, Boxall *et al.* [13], by putting some additional conditions on the Weierstrass σ-function, proves an upper bound for the number of algebraic points of bounded degree and bounded height on the entire graph of the Weierstrass σ-function. They proved two such results. Let $\mathrm{Re}(z)$ and $\mathrm{Im}(z)$ denote the real and imaginary part of a complex number z, respectively. The first result is the following.

Theorem 4.7 ([13]). *Suppose $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice with ω_1, ω_2 both algebraic and $\mathrm{Im}(\omega_2/\omega_1) \leq 1.9$. Then there exists a constant $C_7 = C_7(\Omega) > 0$ such that for all $d \geq e$ and $H \geq e^e$,*

$$\left|S_{\sigma_\Omega}(d, H)\right| \leq C_7 d^6 (\log d)(\log H)^2 \log\log H.$$

For the second result, consider the invariants

$$g_2 = 60 \sum_{\omega \in \Omega \setminus \{0\}} \omega^{-4}, \quad g_3 = 140 \sum_{\omega \in \Omega \setminus \{0\}} \omega^{-6}$$

associated to Ω.

Theorem 4.8 ([13]). *Suppose $\mathrm{Im}(\omega_2/\omega_1) \leq 1.9$ and g_2 and g_3 are both algebraic. Then there exists a constant $C_8 = C_8(\Omega) > 0$ such that for all $d \geq e$ and $H \geq e^e$,*

$$\left|S_{\sigma_\Omega}(d, H)\right| \leq C_8 d^{20} (\log d)^5 (\log H)^2 \log\log H.$$

One of the main constrain of the above two results is that they hold for a restrictive range of ω_2/ω_1. Our aim is to remove this constrain and extend these two results of [13] for a general $\omega_2/\omega_1 \in \mathbb{H}$ under the assumption that $\rho = \eta_2/\eta_1$ is a nonzero real number, where $\eta_i = 2\zeta_\Omega(\omega_i/2)$ is the quasi-period associated to ω_i $(i = 1, 2)$. With this assumption, we are able to count the algebraic points of $\sigma_\Omega(z)$ in an unbounded subset $\mathcal{A}_\rho$ of $\mathbb{C}$ defined by

$$\mathcal{A}_\rho = \begin{cases} z = x + iy \in \mathbb{C} : xy > 0 & \text{if } \rho > 0, \\ z = x + iy \in \mathbb{C} : xy < 0 & \text{if } \rho < 0. \end{cases}$$

Our first result is an analogue of [13, Theorem 1.1] (see Section 4.4 for the proof).

Theorem 4.9 ([37]). *Let $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice in $\mathbb{C}$ such that ω_1 and ω_2 both algebraic. Assume that $\rho = \eta_2/\eta_1$ a nonzero real number. Then there exists a constant $C_9 = C_9(\Omega) > 0$ such that for all $d \geq e$ and $H \geq e^e$,*

$$\left|S_{\sigma_\Omega}(A_\rho, d, H)\right| \leq C_9 d^6 (\log d)(\log H)^2 \log\log H.$$

Our second result deals with the case that g_2, g_3 are algebraic. It is analogues to [13, Theorem 1.2] (see Section 4.5 for the proof).

Theorem 4.10 ([37]). *Let $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice in $\mathbb{C}$ such that g_2 and g_3 both algebraic. Assume that $\rho = \eta_2/\eta_1$ a nonzero real number. Then there exists a constant $C_{10} = C_{10}(\Omega) > 0$ such that for all $d \geq e$ and $H \geq e^e$,*

$$\left|S_{\sigma_\Omega}(A_\rho, d, H)\right| \leq C_{10} d^{20} (\log d)^5 (\log H)^2 \log\log H.$$

We also prove the following more general result with no assumptions on the quantities ω_1, ω_2, g_2 and g_3. In this case, we are only able to count the algebraic points of $\sigma_\Omega(z)$ which are not close to the lattice points. The proof is given in Section 4.6.

Theorem 4.11 ([37]). *Let $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice in $\mathbb{C}$. Assume that $\rho = \eta_2/\eta_1$ a nonzero real number. Let $0 < \delta < \min\{1, |\omega_1 + \omega_2|/2, |\omega_1 - \omega_2|/2\}$. Then there exists a*

constant $C_{11} = C_{11}(\delta, \Omega) > 0$ *such that for all* $d \geq e$ *and* $H \geq e^e$,

$$\left|S_{\sigma_\Omega}(A_\rho, d, H) \cap \{z \in A_\rho : \mathit{dist}(z, \Omega) \geq \delta\}\right| \leq C_{11} d^4 (\log d)(\log H)^2 \log\log H,$$

where $\mathit{dist}(z, \Omega) = \min_{w \in \Omega} |z - w|$.

Throughout this chapter, we fix an $\mathbb{Z}$-basis $\{\omega_1, \omega_2\}$ of Ω such that $\tau = \omega_2/\omega_1$ lies in the upper half plane $\mathbb{H}$ of $\mathbb{C}$ with $|\tau| \geq 1$ and the real part of τ lies in the interval $\left[-\frac{1}{2}, \frac{1}{2}\right]$. Note that such a basis always exists.

4.2 Zero estimate and existence of nonzero polynomial

In this section, we state two results which are required for our proofs. The first is the zero estimate for the Weierstrass σ-function.

Proposition 4.12 ([7, Théorème 1.2]). *Let* $T \geq 1$ *be an integer and* $R \geq 2$ *be a real number. Consider any nonzero polynomial* $P(X, Y) \in \mathbb{C}[X, Y]$ *of degree at most* T *in each variable. Then there exists an effective constant* $C_{12} = C_{12}(\Omega) > 0$ *such that the function* $P(z, \sigma_\Omega(z))$ *has at most* $C_{12} T (R + \sqrt{T})^2 \log(R + T)$ *zeros in* $|z| \leq R$.

Proposition 4.13 ([30, Proposition 2]). *Let* A, Z, M *and* H *with* $H \geq 1$ *be positive real numbers. Let* $d \in \mathbb{N}$ *and* $T \geq \sqrt{8d}$. *Assume* f, g *be two analytic functions on* $|z| < 2Z$ *and continuous on* $|z| \leq 2Z$. *Suppose that for all* $|z| \leq 2Z$, $|f(z)| \leq M, \left|g(z)\right| \leq M$. *Let* $S \subseteq \mathbb{C}$ *be finite set such that for all* $z_1, z_2 \in S$,

1. $|z_1| \leq Z$,
2. $|z_1 - z_2| \leq 1/A$,
3. $[\mathbb{Q}(f(z_1), g(z_2)) : \mathbb{Q}] \leq d$,
4. $H\left(f(z_1), g(z_2)\right) \leq H$.

If

$$(AZ)^T > (4T)^{96d^2/T}(M+1)^{16d}H^{48d^2}, \tag{4.2}$$

then there exists a polynomial $P \in \mathbb{Z}[X,Y] \setminus \{0\}$ *of total degree at most* T *such that*

$$P\left(f(z), g(z)\right) = 0 \text{ for all } z \in S.$$

4.3 Growth conditions

In this section, we prove an important growth condition for $\sigma_\Omega(z)$. Let P be the fundamental parallelogram for the lattice $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ enclosed with vertices $\frac{\pm\omega_1 \pm \omega_2}{2}$.

Proposition 4.14. *Let* $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ *be a lattice in* $\mathbb{C}$ *with* $\rho = \eta_2/\eta_1$ *is a nonzero real number. Then there exist positive constants* r *and* C *depending only on* Ω *such that for all* $z \in \mathcal{A}_\rho$ *with* $|z| \geq r$*, there exists* $z_0 \in P$ *with*

$$\left|\sigma_\Omega(z)\right| \geq \left|\sigma_\Omega(z_0)\right| e^{C|z|^2}.$$

Proof. As in the proof of [13, Proposition 2.1], we may assume that $\Omega = \mathbb{Z} + \mathbb{Z}\tau$ with $\tau \in \mathbb{H}$. Let $z \in \mathcal{A}_\rho$ and $z_0 \in P$ be such that $z = z_0 + m + n\tau$, for some integers m and n. Then we have

$$\sigma_\Omega(z_0 + m + n\tau) = (-1)^{m+n+mn}\sigma_\Omega(z_0)e^{(m\eta_1+n\eta_2)(z_0+\frac{m}{2}+\frac{n}{2}\tau)}$$

(see [29, p. 255]). Hence,

$$|\sigma_\Omega(z_0 + m + n\tau)| = |\sigma_\Omega(z_0)|e^{R(m,n,z_0)}$$

where $R(m,n,z_0) = \mathrm{Re}[(m\eta_1 + n\eta_2)(z_0 + \frac{m}{2} + \frac{n}{2}\tau)]$. Note that

$$R(m,n,z_0) = \mathrm{Re}\left(\frac{\eta_1}{2}\right)m^2 + \mathrm{Re}\left(\frac{\eta_1\tau+\eta_2}{2}\right)mn + \mathrm{Re}\left(\frac{\eta_2\tau}{2}\right)n^2 + \mathrm{Re}\left(\eta_1 z_0\right)m + \mathrm{Re}\left(\eta_2 z_0\right)n.$$

Further, using the Legendre's relation $\eta_1\tau - \eta_2 = 2\pi i$, we obtain

$$\mathrm{Re}(\eta_1\tau) = \mathrm{Re}(\eta_2)$$

and

$$\mathrm{Re}\left(\frac{\eta_1\tau + \eta_2}{2}\right) = \mathrm{Re}(\eta_2).$$

Moreover,

$$\mathrm{Re}(\eta_2\tau) = \mathrm{Re}(\eta_1\rho\tau) = \rho\,\mathrm{Re}(\eta_1\tau) = \rho\,\mathrm{Re}(\eta_2) = \rho^2\,\mathrm{Re}(\eta_1).$$

Therefore,

$$\begin{aligned}\mathrm{Re}\left(\frac{\eta_1}{2}\right)m^2 + \mathrm{Re}\left(\frac{\eta_1\tau+\eta_2}{2}\right)mn + \mathrm{Re}\left(\frac{\eta_2\tau}{2}\right)n^2 &= \mathrm{Re}(\eta_1)\left(\frac{m^2}{2} + \rho mn + \frac{\rho^2}{2}n^2\right)\\ &= \frac{1}{2}\mathrm{Re}(\eta_1)\,(n\rho+m)^2.\end{aligned}$$

Whence,

$$\begin{aligned}R(m,n,z_0) &= \frac{1}{2}\mathrm{Re}(\eta_1)\,(n\rho+m)^2 + \mathrm{Re}(\eta_1 z_0)(n\rho+m)\\ &= (n\rho+m)\left[\frac{\mathrm{Re}(\eta_1)}{2}\,(n\rho+m) + \mathrm{Re}(\eta_1 z_0)\right]\end{aligned}$$

(Recall that by Dirichlet's theorem, there are infinitely many pairs of integers (m,n) such that either $\rho + \frac{m}{n} = 0$ or $|\rho + \frac{m}{n}| < \frac{1}{n^2}$. Because of this reason, we need to restrict the values of m, n). Also, since $\eta_2/\eta_1 = \tau - 2\pi i/\eta_1$ and η_2/η_1 is real, we have $\mathrm{Im}(\tau - 2\pi i/\eta_1) = 0$. So

$$\mathrm{Im}(\tau) = 2\pi\,\mathrm{Re}(1/\eta_1) = 2\pi\frac{\mathrm{Re}(\eta_1)}{\mathrm{Re}(\eta_1)^2 + \mathrm{Im}(\eta_1)^2}.$$

Since $\mathrm{Im}(\tau) > 0$, we have $\mathrm{Re}(\eta_1) > 0$.

Case 1. $\rho > 0$. Suppose $m > 0, n > 0$. Then there exists a positive constant $r = r(\Omega)$ such that whenever $|z| > r$, we have

$$R(m,n,z_0) \geq c_1(n\rho+m)^2 \geq c_2\max(|m|,|n|)^2,$$

for some positive constants c_1, c_2 depending only on Ω. On the other hand, we obtain

$$|z_0 + m + n\tau| \leq c_3 \max(|m|, |n|)$$

for some constant $c_3 = c_3(\Omega) > 0$. Hence, we obtain that

$$|\sigma_\Omega(z_0 + m + n\tau)| \geq |\sigma_\Omega(z_0)| e^{c_4 |z_0 + m + n\tau|^2} \tag{4.3}$$

for some constant $c_4 = c_4(\Omega) > 0$. Now, if $m < 0, n < 0$ then consider the point $-z_0 - m - n\tau$. Clearly, $-z_0 \in P$. Therefore, from (4.3) we obtain that

$$|\sigma_\Omega(-z_0 - m - n\tau)| \geq |\sigma_\Omega(-z_0)| e^{c_4 |-z_0 - m - n\tau|^2} = |\sigma_\Omega(-z_0)| e^{c_4 |z_0 + m + n\tau|^2}$$

But, since $\sigma_\Omega(z)$ is an odd function, we have

$$|\sigma_\Omega(-z_0 - m - n\tau)| = |\sigma_\Omega(z_0 + m + n\tau)|, \quad \text{and} \quad |\sigma_\Omega(-z_0) = |\sigma_\Omega(z_0)|,$$

and hence the required result follows.

Case 2. $\rho < 0$. The proof of this case is similar to Case 1, and therefore we omit it here. □

4.4 Lattice points are algebraic

In this section, we prove Theorem 4.9. Throughout this section, let r and C denote the constants from Proposition 4.14. In the following $c_5, \ldots, c_{17}$ denote positive constants depending only on Ω (and are independent of d and H). Since

$$\lim_{z \to 0} \frac{\sigma_\Omega(z)}{z} = 1,$$

there exists an ε with $0 < \varepsilon < 1/2$ such that

$$\big|\log |\sigma_\Omega(z)| - \log |z|\big| \leq 1 \tag{4.4}$$

whenever $|z| < \varepsilon$. We fix such an ε.

First, we prove several lemmas which are required for the proof of our theorem.

Lemma 4.15. *For some $d \geq e$ and $H \geq e$, suppose $z \in S_{\sigma_\Omega}(A_\rho, d, H)$ and $z_0 \in P$ be such that $z - z_0 \in \Omega$ with $|z_0| \geq \varepsilon$. Assume that $|z| \geq r$. Then $|z| \leq C_{13}\sqrt{d \log H}$, for some constant $C_{13} = C_{13}(\Omega) > 0$.*

Proof. Let $S = \{z \in P : |z| < \varepsilon\}$. Note that $P \setminus S$ is compact. Since $\sigma_\Omega(z)$ is continuous and nonzero in $P \setminus S$, for all $z \in P \setminus S$, we have $|\sigma_\Omega(z)| \geq c_5$. Since $|z_0| \geq \varepsilon$, we have $|\sigma_\Omega(z_0)| \geq c_5$. Now from Proposition 4.14, we have

$$\left|\sigma_\Omega(z)\right| \geq \left|\sigma_\Omega(z_0)\right| e^{C|z|^2}.$$

On the other hand, since $[\mathbb{Q}(\sigma_\Omega(z)) : \mathbb{Q}] \leq d$ and $H(\sigma_\Omega(z)) \leq H$, we have $|\sigma_\Omega(z)| \leq H^d$. So

$$C|z|^2 \leq \log|\sigma_\Omega(z)| - \log|\sigma_\Omega(z_0)| \leq d \log H - \log c_5 \leq c_6 d \log H,$$

and therefore, we have $|z| \leq c_7\sqrt{d \log H}$. This completes the proof of the lemma. □

Lemma 4.16. *For some $d \geq e$ and $H \geq e$, suppose $z \in S_{\sigma_\Omega}(A_\rho, d, H)$ and $z_0 \in P$ be such that $z - z_0 \in \Omega$ with $|z_0| < \varepsilon$. Assume that $|z| \geq r$. For all $B > 0$ and for all $N \geq \sqrt{d \log H}$, we have if $|z| \geq \sqrt{\frac{2+B}{C}}N$, then $\log|z_0| \leq -BN^2$.*

Proof. Let $z \in \mathcal{A}_\rho$ with $|z| \geq r$. Let $z_0 \in P$ be such that $z - z_0 \in \Omega$. From Proposition 4.14, we have

$$\left|\sigma_\Omega(z)\right| \geq \left|\sigma_\Omega(z_0)\right| e^{C|z|^2}.$$

Using $|\sigma_\Omega(z)| \leq H^d$ and $N \geq \sqrt{d \log H}$, we obtain

$$C|z|^2 + \log|\sigma_\Omega(z_0)| \leq \log|\sigma_\Omega(z)| \leq d \log H \leq N^2. \tag{4.5}$$

For any $B > 0$, put

$$A = \sqrt{\frac{2+B}{C}}.$$

If $|z| \geq AN$, then from (4.5) we deduce that $CA^2N^2 + \log|\sigma_\Omega(z_0)| \leq N^2$. So, $\log|\sigma_\Omega(z_0)| \leq (1 - CA^2)N^2$. Since $|z_0| < \varepsilon$, applying (4.4), we obtain

$$\begin{aligned}\log|z_0| \leq & \log|\sigma_\Omega(z_0)| + 1\\ \leq & (1 - CA^2)N^2 + 1\\ \leq & (2 - CA^2)N^2\\ = & -BN^2.\end{aligned}$$

Thus the result follows. □

Lemma 4.17. *Assume that ω_1 and ω_2 both algebraic. For $d \geq e$ and $H \geq e$, let $z \in S_{\sigma_\Omega}(\mathcal{A}_\rho, d, H)$ be such that $|z| \geq r$. Then there exists a constant $C_{14} = C_{14}(\Omega) > 0$ such that $|z| \leq C_{14} d\sqrt{\log H}$.*

Proof. Suppose $z \in \mathcal{A}_\rho$. Choose $z_0 \in P$ such that $z - z_0 \in \Omega$. If $|z_0| \geq \varepsilon$, then by Lemma 4.15 we have $|z| \leq c_8\sqrt{d \log H}$. So we assume that $|z_0| < \varepsilon$. Since $\omega_2/\omega_1 \notin \mathbb{R}$, if $\omega = z - z_0 = k\omega_1 + l\omega_2 \in \Omega$, then we obtain $\max(|k|, |l|) \leq c_9|\omega|$. Therefore,

$$\max(|k|, |l|) \leq c_9(|z| + |z_0|) \leq c_9(|z| + |\omega_1| + |\omega_2|) \leq c_{10}|z|.$$

On the other hand, since $H(z) \leq H$ and $[\mathbb{Q}(z) : \mathbb{Q}] \leq d$, we deduce that $|z| \leq H^d$. So $H(k) = |k| \leq c_{10}|z| \leq c_{10}H^d$ and similarly $H(l) \leq c_{10}H^d$. Now using the inequality

$$H(z_0) \leq 2H(z)H(\omega) \leq 4H(z)H(k)H(\omega_1)H(l)H(\omega_2) \leq c_{11}H^{2d+1},$$

together with the bounds

$$[\mathbb{Q}(z_0) : \mathbb{Q}] = [\mathbb{Q}(z - \omega) : \mathbb{Q}] \leq [\mathbb{Q}(\omega_1, \omega_2) : \mathbb{Q}]d \leq c_{12}d,$$

and

$$M(z_0) = M(z_0^{-1}) \geq 1/|z_0|,$$

we deduce that

$$\begin{aligned}\log|z_0| \geq \log(1/M(z_0)) &= -[\mathbb{Q}(z_0):\mathbb{Q}]\log(H(z_0)) \\ &\geq -c_{12}d((2d+1)\log H + \log c_{11}) \geq -c_{13}d^2\log H\end{aligned}$$

where $M(\alpha)$ is the Mahler measure of α. Applying Lemma 4.16 with $B = c_{13}$ and $N = d\sqrt{\log H}$, we deduce $|z| \leq c_{14}d\sqrt{\log H}$, where $c_{14} = \sqrt{\frac{2+c_{13}}{C}}$. Taking $C_{14} = \max\{c_8, c_{14}\}$, we obtain the required result. □

Finally, we need the following result to prove our theorem.

Proposition 4.18 ([29]). *There exists a constant $C_{15} = C_{15}(\Omega)$ such that for any $R \geq 1$,*

$$\left|\sigma_\Omega(z)\right| \leq C_{15}^{R^2}, \text{ for all } |z| \leq R.$$

Proof of Theorem 4.9. Define

$$\mathcal{Z}_1 = \{z \in \mathcal{A}_\rho : [\mathbb{Q}(z, \sigma_\Omega(z)) : \mathbb{Q}] \leq d,\ H(z, \sigma_\Omega(z)) \leq H\}.$$

Put

$$Z = 4C_{14}d\sqrt{\log H}, \quad A = 2/Z.$$

From Lemma 4.17, we have $|z| \leq C_{14}d\sqrt{\log H} \leq Z$ and $|z - z'| \leq 1/A$ for all $z, z' \in \mathcal{Z}_1$. On the other hand, from Proposition 4.18, there exists a constant $c_{15} \geq 1$ such that for all $z \in \mathcal{A}_\rho$, $\left|\sigma_\Omega(z)\right| \leq c_{15}^{|z|^2}$. Put $M = c_{15}^{Z^2}$. Then $|z| \leq M$ and $\left|\sigma_\Omega(z)\right| \leq M$ for all $|z| \leq 2Z$. With these choices of A, Z and M, conditions of Proposition 4.13 are satisfied. If we take $T = c_{16}d^3\log H$ for a sufficiently large $c_{16} > 0$, then (4.2) is satisfied. Hence by Proposition 4.13, there exists a nonzero polynomial $P \in \mathbb{Z}[X, Y]$ of total degree at most T such that

$$P\left(z, \sigma_\Omega(z)\right) = 0 \text{ for all } z \in \mathcal{Z}_1.$$

Finally, taking $R = C_{14}d\sqrt{\log H}$ and $T = c_{16}d^3 \log H$ in Proposition 4.12, we deduce that there are at most $c_{17}d^6(\log d)(\log H)^2 \log\log H$ zeros of $P(z, \sigma_\Omega(z))$ lie in the region $|z| \leq R$. Hence the number of elements in the set $\mathcal{Z}_1$ is at most $c_{17}d^6(\log d)(\log H)^2 \log\log H$. This completes the proof. □

4.5 Invariants are algebraic

In this section, we prove Theorem 4.10. Throughout this section, let Ω denote a lattice in $\mathbb{C}$ with algebraic invariants g_2, g_3. In this section, $c_{18}, \ldots, c_{27}$ denote various constants which depend only on Ω. We first state the following transcendence measure for the nonzero elements of Ω, due to David and Hirata-Kohno.

Lemma 4.19 ([16]). *Let Ω be a lattice in $\mathbb{C}$. Let $d \geq 1$ and $H \geq 3$ be real numbers. Let α be an algebraic number with $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq d$ and $H(\alpha) \leq H$. Then there exists a constant $C_{16} = C_{16}(\Omega) > 0$ such that*

$$\log|\alpha - \omega| \geq -C_{16}d^4(\log d)^2(\log H)|\omega|^2(1 + \max\{0, \log|\omega|\})^3$$

for all $\omega \in \Omega \setminus \{0\}$.

The following is an analogue of [13, Proposition 4.2].

Lemma 4.20. *Assume that $\rho = \eta_2/\eta_1$ is a nonzero real number. Let $d \geq 1, H \geq 3$ be real numbers. There exist positive constants C_{17}, C_{18} depending only on Ω such that the following holds. If $z, z' \in \mathcal{A}_\rho$ be such that $[\mathbb{Q}(z, \sigma_\Omega(z)) : \mathbb{Q}] \leq d$, $[\mathbb{Q}(z', \sigma_\Omega(z')) : \mathbb{Q}] \leq d$, $H(z, \sigma_\Omega(z)) \leq H$ and $H(z', \sigma_\Omega(z')) \leq H$, then*

$$\min\{|z|, |z'|\} \leq C_{17}\sqrt{d^9(\log d)^2 \log H}$$

or there exists $\omega, \omega' \in \Omega$ such that

$$\max\{\log|z - \omega|, \log|z' - \omega'|\} \leq -C_{18}d^9(\log d)^2 \log H$$

with $z'/z = \omega'/\omega \in \mathbb{Q}$.

Proof. The proof follows along the same line of argument as in [13, Proposition 4.2], so we omit it here. □

Lemma 4.21. *Assume that* $\rho = \eta_2/\eta_1$ *is a nonzero real number and* g_2, g_3 *both algebraic. Let* $d \geq 1, H \geq 3$ *be real numbers. Let* r *be from Proposition 4.14 and* C_{17} *be from Lemma 4.20. Consider the set*

$$S = \Big\{ z \in \mathcal{A}_\rho : [\mathbb{Q}(z, \sigma_\Omega(z)) : \mathbb{Q}] \leq d, H(z, \sigma_\Omega(z)) \leq H \text{ and } |z| > \max\Big\{ r, C_{17}\sqrt{d^9(\log d)^2 \log H} \Big\} \Big\}.$$

Then there exists a positive constant $C_{19} = C_{19}(\Omega)$ *such that* S *has at most*

$$C_{19}\sqrt{d^5(\log d)^2(\log H)(1 + d\log H)^3}$$

many elements.

Proof. We follow the strategy given in [13]. Suppose $z, z' \in S$. Then

$$\min\{|z|, |z'|\} > C_{17}\sqrt{d^9(\log d)^2 \log H}.$$

So by Lemma 4.20, there exists $\omega, \omega' \in \Omega$ such that

$$\max\{\log|z - \omega|, \log|z' - \omega'|\} \leq -C_{18}d^9(\log d)^2 \log H$$

with $z'/z = \omega'/\omega \in \mathbb{Q}$. This implies z, z' are not periods of Ω.

Put $\omega'/\omega = q$. Let $\omega^* \in \Omega \setminus \{0\}$ be of minimum modulus which lie on the line joining 0 and ω. So $\omega = m\omega^*$ for some nonzero integer m. Let $z^* = z/m$. Note that $z^* \in \mathcal{A}_\rho$. Also since ω' and ω lie on the same line, we have $\omega' = m_1\omega^*$ for some $m_1 \in \mathbb{Z}$. So $qm\omega^* = m_1\omega^*$. Hence $qm = m_1$. Now $z' = qz = qmz^* = m_1z^*$. So z' is an integer multiple of z^*. Thus if we show that whenever $nz^* \in S$ for some $n \in \mathbb{Z}$ implies

$$n^2 \leq c_{18}d^5(\log d)^2(\log H)(1 + d\log H)^3,$$

then we are done. Because, just now we have seen that if $z' \in S$ then $z' = nz^*$ for some $n \in \mathbb{N}$. Accordingly, we assume $nz^* \in S$ for some $n \in \mathbb{Z}$. Put $nz^* = z''$. Thus, we have $z'' \in \mathcal{A}_\rho$. Let $z_0 \in P$ be such that $z'' - z_0 = \omega'' \in \Omega$. Since both z'' and z belong to S, we have $z''/z = \omega''/\omega$. Hence, $nz^*/mz^* = \omega''/m\omega^*$, or equivalently we obtain that $\omega'' = n\omega^*$. Now $z'' \in \mathcal{A}_\rho$, from Proposition 4.14 we obtain

$$\log|\sigma_\Omega(z'')| \geq \log|\sigma_\Omega(z_0)| + C|z''|^2.$$

Note that $z_0 \neq 0$. Therefore, $|\sigma_\Omega(z_0)/z_0| > e^{c_{18}}$. Hence, we obtain

$$\begin{aligned}
\log|\sigma_\Omega(z'')| &\geq \log|z_0| + c_{19} + C|z''|^2 \\
&= \log|z'' - \omega''| + c_{19} + C|z''|^2 \\
&\geq \log|nz^* - n\omega^*| + c_{19} + Cn^2|z^*|^2 \\
&\geq \log|z^* - \omega^*| + c_{19} + Cn^2|z^*|^2.
\end{aligned}$$

Write $\omega = k\omega_1 + l\omega_2$ with integers k, l. As we have seen earlier in the proof of Lemma 4.17, $\max(|k|, |l|) \leq c_{20}|z| \leq c_{20}H^d$. Further, since $\omega = m\omega^*$, we obtain that m divides both k, l. We deduce that $|m| \leq c_{20}H^d$. So, $\log H(z^*) = \log H(z/m) \leq c_{21}d \log H$. Since $z^* = z/m$ is algebraic, by Lemma 4.19, we deduce that

$$\begin{aligned}
\log|z^* - \omega^*| &\geq -c_{22}d^4(\log d)^2 d(\log H)|\omega^*|^2 \left(1 + \max\{0, \log|\omega^*|\}\right)^3 \\
&\geq -c_{23}d^5(\log d)^2(\log H)|z^*|^2 \left(1 + \max\{0, \log|z^*|\}\right)^3.
\end{aligned}$$

So,

$$\begin{aligned}
-c_{23}d^5(\log d)^2(\log H)|z^*|^2 \left(1 + \max\{0, \log|z^*|\}\right)^3 + c_{19} + Cn^2|z^*|^2 \leq \log|\sigma_\Omega(z'')| \\
\leq d \log H.
\end{aligned}$$

In other words,

$$n^2 \leq c_{24}d^5(\log d)^2(\log H)(1 + d\log H)^3.$$

This completes the proof of the lemma. □

Proof of Theorem 4.10. In order to prove Theorem 4.10, by Lemma 4.21, we only need to count the number of elements in the set

$$\mathcal{Z}_2 = \Big\{ z \in \mathcal{A}_\rho : [\mathbb{Q}(z, \sigma_\Omega(z)) : \mathbb{Q}] \le d,\ H(z, \sigma_\Omega(z)) \le H \text{ and } |z| \le C_{17}\sqrt{d^9 (\log d)^2 \log H} \Big\}.$$

Put

$$Z = 4C_{17}\sqrt{d^9 (\log d)^2 \log H}, \quad A = 2/Z.$$

Then $|z| \le Z$ and $|z - z'| \le 1/A$ for all $z, z' \in \mathcal{Z}_2$.

By Proposition 4.18, for all $z \in \mathcal{A}_\rho$, we have $\big|\sigma_\Omega(z)\big| \le c_{25}^{|z|^2}$. Put $M = c_{25}^{Z^2}$. Then $|z| \le M$ and $\big|\sigma_\Omega(z)\big| \le M$ for all $|z| \le 2Z$. With these choices of A, Z and M, conditions of Proposition 4.13 are satisfied. If we take $T = c_{26} d^{10} (\log d)^2 \log H$ for a sufficiently large $c_{26} > 0$, then (4.2) is satisfied. Thus by Proposition 4.13, we deduce that there exists a nonzero polynomial $P \in \mathbb{Z}[X, Y]$ of total degree at most T such that

$$P\big(z, \sigma_\Omega(z)\big) = 0 \text{ for all } z \in \mathcal{Z}_2.$$

Finally, taking $R = C_{17}\sqrt{d^9 (\log d)^2 \log H}$ and $T = c_{26} d^{10} (\log d)^2 \log H$ in Proposition 4.12, we deduce that there are at most $c_{27} d^{20} (\log d)^5 (\log H)^2 \log\log H$ number of zeros of $P(z, \sigma_\Omega(z))$ lie in the region $|z| \le R$. Hence the number of element in the set $\mathcal{Z}_2$ is at most $c_{27} d^{20} (\log d)^5 (\log H)^2 \log\log H$. Since

$$\sqrt{c_{24} d^5 (\log d)^2 (\log H)(1 + d \log H)^3} \le c_{27} d^{20} (\log d)^5 (\log H)^2 \log\log H,$$

from Lemma 4.21 we obtain

$$\big|S_{\sigma_\Omega}(A_\rho, d, H)\big| \le 2c_{27} d^{20} (\log d)^5 (\log H)^2 \log\log H.$$

This completes the proof of the theorem. □

4.6 Algebraic points away from lattice points

In this section, we prove Theorem 4.11. Throughout this section, let δ, r denote constants from the statement of Theorem 4.11 and Proposition 4.14, respectively.

Lemma 4.22. *Let $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice in $\mathbb{C}$ with $\rho = \eta_2/\eta_1$ is a nonzero real number. For $d \geq e$ and $H \geq e$, let $z \in S_{\sigma_\Omega}(A_\rho, d, H)$ be such that $|z| \geq r$ and dist$(z, \Omega) \geq \delta$. Then there exists a constant $C_{20} = C_{20}(\delta, \Omega)$ such that $|z| \leq C_{20}\sqrt{d \log H}$.*

Proof. Let $z \in \mathcal{A}_\rho$ and $z_0 \in P$ be such that $z - z_0 = m_1\omega_1 + n_1\omega_2 \in \Omega$. Since dist$(z, \Omega) \geq \delta$, we have $|z_0| = |z - m_1\omega_1 - n_1\omega_2| \geq \delta$. Let ε denote the constant from Lemma 4.15.

Case 1. $\delta \geq \varepsilon$. Since $|z_0| \geq \delta$, we have $|z_0| \geq \varepsilon$. So by Lemma 4.15, there exists a constant $c_{28} = c_{28}(\Omega)$ such that $|z| \leq c_{28}\sqrt{d \log H}$. Hence the lemma is proved.

Case 2. $\delta < \varepsilon$. Suppose $\delta \leq$ dist$(z, \Omega) < \varepsilon$. So $\delta \leq |z_0| < \varepsilon$. Hence

$$|z_0| \geq e^{-\log 1/\delta} \geq e^{-d \log H \log 1/\delta} = e^{-BN^2},$$

where $B = \log 1/\delta$ and $N = \sqrt{d \log H}$. Since $|z_0| < \varepsilon$, applying Lemma 4.16, we obtain

$$|z| \leq \sqrt{\frac{2 + \log 1/\delta}{C}}\sqrt{d \log H},$$

where C be as in Lemma 4.16.

Now suppose dist$(z, \Omega) \geq \varepsilon$. So $|z_0| \geq \varepsilon$. Then as in Case 1, we get $|z| \leq c_{28}\sqrt{d \log H}$. Taking $C_{20} = \max\left(c_{28}, \sqrt{\frac{2+\log 1/\delta}{C}}\right)$, we get the required result. □

Proof of Theorem 4.11. Define

$$\mathcal{Z}_3 = \{z \in \mathcal{A}_\rho : \text{dist}(z, \Omega) \geq \delta, [\mathbb{Q}(z, \sigma_\Omega(z)) : \mathbb{Q}] \leq d \text{ and } H(z, \sigma_\Omega(z)) \leq H\}.$$

Put

$$Z = 4C_{20}\sqrt{d \log H}, \quad A = 2/Z.$$

From Lemma 4.22, we have $|z| \leq C_{20}\sqrt{d \log H} \leq Z$ and $|z - z'| \leq 1/A$ for all $z, z' \in \mathcal{Z}_3$. By Proposition 4.18, $\left|\sigma_\Omega(z)\right| \leq c_{29}^{|z|^2}$. Put $M = c_{29}^{Z^2}$. Then $|z| \leq M$ and $\left|\sigma_\Omega(z)\right| \leq M$ for all $|z| \leq 2Z$. With these choices of A, Z and M, conditions of Proposition 4.13 are satisfied. If we take $T = c_{30}d^2 \log H$ for some sufficiently large constant $c_{30} = c_{30}(\delta, \Omega)$, then (4.2) is satisfied. Thus by applying Proposition 4.13, there exists a nonzero polynomial $P \in \mathbb{Z}[X, Y]$ of total degree at most T such that

$$P\left(z, \sigma_\Omega(z)\right) = 0 \text{ for all } z \in \mathcal{Z}_3.$$

Finally, taking $R = C_{20}\sqrt{d \log H}$ and $T = c_{30}d^2 \log H$ in Proposition 4.12, we deduce that there are at most $c_{31}d^4(\log d)(\log H)^2 \log\log H$ zeros of $P(z, \sigma_\Omega(z))$ lie in the region $|z| \leq R$, for some constant $c_{31} = c_{31}(\delta, \Omega) > 0$. Hence the number of elements in the set $\mathcal{Z}_3$ is at most $c_{31}d^4(\log d)(\log H)^2 \log\log H$. This completes the proof of the theorem. □

4.7 Concluding remarks

One of the general methods to prove an upper bound for the number of algebraic points of bounded degrees and bounded heights on graphs of functions is to find a nonzero polynomial (depending upon the original function considered) with certain conditions that vanishes at certain points. Then we need to prove a zero estimate for the original function to conclude the required upper bound. For the Weierstrass sigma function $\sigma(z)$, to produce the required nonzero polynomial, we first proved a growth estimate for $\sigma(z)$ (Proposition 4.14). To prove this estimate, we used the functional equation for $\sigma(z)$ and calculated a lower bound for a quadratic form. Then we applied [30, Proposition 2] to produce the required nonzero polynomial. After this, we applied the zero estimate of $\sigma(z)$, proved by Besson (Proposition 4.12), to prove our results. In order to use this method to prove similar upper bounds for other functions, for example $\sin(z)$, we need a zero estimate for $\sin(z)$ - which I currently do not have.

References

[1] Adler, R. L. and Marcus, B. Topological entropy and equivalence of dynamical systems. *Mem. Amer. Math. Soc.* **20**, 219 (1979), iv+84 pp.

[2] Amoroso, F. and David, S. Le problème de Lehmer en dimension supérieure. *J. Reine Angew. Math.* **513** (1999), 145–179.

[3] Amoroso, F., David, S. and Zannier, U. On fields with Property (B). *Proc. Amer. Math. Soc.* **142**, 6 (2014), 1893–1910.

[4] Amoroso, F. and Dvornicich, R. A lower bound for the height in abelian extensions. *J. Number Theory* **80**, 2 (2000), 260–272.

[5] Amoroso, F. and Masser, D. Lower bounds for the height in Galois extensions. *Bull. Lond. Math. Soc.* **48**, 6 (2016), 1008–1012.

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

[7] Besson, E. Points algébriques de la fonction sigma de weierstrass. *Preprint (2015)* (https://rivoal.perso.math.cnrs.fr/sigma.pdf).

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

[9] Bombieri, E. and Gubler, W. *Heights in Diophantine geometry*, vol. 4 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2006.

[10] Bombieri, E. and Pila, J. The number of integral points on arcs and ovals. *Duke Math. J.* **59**, 2 (1989), 337–357.

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

[12] Borwein, P., Hare, K. G. and Mossinghoff, M. J. The Mahler measure of polynomials with odd coefficients. *Bull. London Math. Soc.* **36**, 3 (2004), 332–338.

[13] Boxall, G., Chalebgwa, T. and Jones, G. On algebraic values of Weierstrass σ-functions. *Atti Accad. Naz. Lincei Rend. Lincei Mat. Appl.* **32**, 4 (2021), 819–833.

[14] Boxall, G. and Jones, G. Rational values of entire functions of finite order. *Int. Math. Res. Not. IMRN*, 22 (2015), 12251–12264.

[15] Breusch, R. On the distribution of the roots of a polynomial with integral coefficients. *Proc. Amer. Math. Soc.* **2** (1951), 939–941.

[16] David, S. and Hirata-Kohno, N. Linear forms in elliptic logarithms. *J. Reine Angew. Math.* **628** (2009), 37–89.

[17] Dobrowolski, E. On a question of Lehmer and the number of irreducible factors of a polynomial. *Acta Arith.* **34**, 4 (1979), 391–401.

[18] Dubickas, A. and Mossinghoff, M. J. Auxiliary polynomials for some problems regarding Mahler's measure. *Acta Arith.* **119**, 1 (2005), 65–79.

[19] Fili, P. and Petsche, C. Energy integrals over local fields and global height bounds. *Int. Math. Res. Not. IMRN*, 5 (2015), 1278–1294.

[20] Garza, J. On the height of algebraic numbers with real conjugates. *Acta Arith.* **128**, 4 (2007), 385–389.

[21] Garza, J. The Lehmer strength bounds for total ramification. *Acta Arith.* **137**, 2 (2009), 171–176.

[22] Hindry, M. and Silverman, J. H. *Diophantine geometry*, vol. 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[23] Ishak, M. I. M., Mossinghoff, M. J., Pinner, C. and Wiles, B. Lower bounds for heights in cyclotomic extensions. *J. Number Theory* **130**, 6 (2010), 1408–1424.

[24] Jarník, V. Über die Gitterpunkte auf konvexen Kurven. *Math. Z.* **24**, 1 (1926), 500–518.

[25] Jones, G. O. and Thomas, M. E. M. Rational values of Weierstrass zeta functions. *Proc. Edinb. Math. Soc. (2)* **59**, 4 (2016), 945–958.

[26] Kronecker, L. Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten. *J. Reine Angew. Math.* **53** (1857), 173–175.

[27] Lang, S. *Algebra*, third ed., vol. 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[28] Lehmer, D. H. Factorization of certain cyclotomic functions. *Ann. of Math. (2)* **34**, 3 (1933), 461–479.

[29] Masser, D. *Elliptic functions and transcendence*, vol. 437 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin-New York, 1975.

[30] Masser, D. Rational values of the Riemann zeta function. *J. Number Theory* **131**, 11 (2011), 2037–2046.

[31] Mignotte, M. Entiers algébriques dont les conjugués sont proches du cercle unité. In *Séminaire Delange-Pisot-Poitou, 19e année: 1977/78, Théorie des nombres, Fasc. 2*. Secrétariat Math., Paris, 1978, pp. Exp. No. 39, 6.

[32] Petsche, C. J. The height of algebraic units in local fields. *Preprint (2003)* (https://drive.google.com/file/d/1S9dqPOyWcqgruNesAkJdPk1SVwViD7Qg/view).

[33] Pila, J. Geometric postulation of a smooth function and the number of rational points. *Duke Math. J.* **63**, 2 (1991), 449–463.

[34] Pottmeyer, L. Small totally p-adic algebraic numbers. *Int. J. Number Theory* **14**, 10 (2018), 2687–2697.

[35] Prasad, G. Height of algebraic units under splitting conditions. *Accepted in Proc. Indian Acad. Sci. Math. Sci*.

[36] Prasad, G. and Senthil Kumar, K. Lehmer's problem and reciprocal numbers. *(Submitted)*.

[37] Prasad, G. and Senthil Kumar, K. On the number of algebraic points on the graph of the weierstrass sigma functions. *Accepted in Bull. Aust. Math. Soc*.

[38] Prasad, G. and Senthil Kumar, K. Lehmer's problem and splitting of rational primes in number fields. *Acta Math. Hungar.* **169**, 2 (2023), 349–358.

[39] Ribenboim, P. *The theory of classical valuations*. Springer Monographs in Mathematics. Springer-Verlag, New York, 1999.

[40] Schinzel, A. On the product of the conjugates outside the unit circle of an algebraic number. *Acta Arith.* **24** (1973), 385–399.

[41] Schinzel, A. and Zassenhaus, H. A refinement of two theorems of Kronecker. *Michigan Math. J.* **12** (1965), 81–85.

[42] Smyth, C. The Mahler measure of algebraic numbers: a survey. In *Number theory and polynomials*, vol. 352 of *London Math. Soc. Lecture Note Ser.* Cambridge Univ. Press, Cambridge, 2008, pp. 322–349.

[43] Smyth, C. J. On the product of the conjugates outside the unit circle of an algebraic integer. *Bull. London Math. Soc.* **3** (1971), 169–175.

[44] Stewart, C. L. Algebraic integers whose conjugates lie near the unit circle. *Bull. Soc. Math. France* **106**, 2 (1978), 169–176.

[45] Voutier, P. An effective lower bound for the height of algebraic numbers. *Acta Arith.* **74**, 1 (1996), 81–95.

[46] Waldschmidt, M. *Transcendence methods*, vol. 52 of *Queen's Papers in Pure and Applied Mathematics*. Queen's University, Kingston, Ont., 1979.

[47] Waldschmidt, M. *Diophantine approximation on linear algebraic groups*, vol. 326 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2000.