On Weber's Class Number Problem

ウェーバーの類数問題について

February 2012

Waseda University
Graduate School of Fundamental Science and Engineering
Major in Pure and Applied Mathematics
Research on Number Theory

Takayuki MORISAWA

Acknowledgements

I would like to express sincere gratitude to Professor Keiichi Komatsu who guided me to the number theory and has given constant encouragement and fruitful suggestions since I was an undergraduate student.

I would like to thank Professor Takashi Fukuda for his helpful comments around the computational work in Chapter 7 and Chapter 8.

I would also like to thank Professor Ryotaro Okazaki for crucial observation and profitable discussions. The contents in Chapter 2, Chapter 3 and Chapter 4 are parts of the joint works with him.

Further, I would like to express my thanks to Professor Norio Adachi, Professor Kiichiro Hashimoto, Professor Katsuya Miyake, Professor Manabu Ozaki and Professor Atsuki Umegaki for interesting and helpful conversations and all other members of the number theory seminars at Waseda University for giving me a favorable environment.

I would like to mention that part of the work in this thesis is supported by JSPS Research Fellowships for Young Scientists.

Finally, I wish to be grateful to my parents, Masaharu and Michiko, and my friends.

Takayuki MORISAWA
Major in Pure and Applied Mathematics
Graduate School of Fundamental Science and Engineering
Waseda University
3-4-1, Ohkubo, Shinjuku, Tokyo, 169-8555, JAPAN

Introduction

In algebraic number theory, the class number of an algebraic number field is one of the most important objects. Two hundred years ago, Gauss conjectured that there exist infinitely many real quadratic fields with class number one. This conjecture is still open. Far from that, it is not yet known whether there exist infinitely many algebraic number fields with class number one. In order to approach this conjecture, we focus on Weber's work.

Let p be a prime number and μ_m the group of all m-th roots of unity. We denote by $\mathbb{B}_{p,n}$ the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension of the rational number field $\mathbb{Q}$. We are interested in the class number $h_{p,n}$ of $\mathbb{B}_{p,n}$. In the case $p = 2$, Weber [31] showed that 2 does not divide $h_{2,n}$ for any non-negative integer n and he also showed $h_{2,1} = h_{2,2} = h_{2,3} = 1$. Based on these results, Weber asked whether $h_{2,n} = 1$ for any non-negative integer n. Then we consider a generalized version of his problem:

Weber's Class Number Problem. Is the class number $h_{p,n}$ equal to one for any positive integer n?

This problem has been studied by Bauer [2], Cohn [3], Masley [23], who showed $h_{2,4} = 1$. Later, van der Linden [21] showed $h_{2,5} = 1$ or 97. However, Komatsu and Fukuda [6] showed that 97 does not divide $h_{2,n}$ for any positive integer n. Hence we have $h_{2,5} = 1$. In [2] and [21], we know that $h_{p,n} = 1$ for $(p, n) \in \{(3, 1), (3, 2), (3, 3), (5, 1), (7, 1)\}$. Linden also showed that $h_{p,n} = 1$ for $(p, n) \in \{(2, 6), (3, 4), (5, 2), (11, 1), (13, 1)\}$ under the generalized Riemann hypothesis.

However, direct calculation of $h_{p,n}$ is extremely difficult for large p^n. Therefore, in order to break the wall of the computational complexity, we

study the ℓ-indivisibility of $h_{p,n}$ for a prime number ℓ and for all positive integer n:

Problem. Does a prime number ℓ divide $h_{p,n}$ for any positive integer n?

In the case $\ell = p$, Iwasawa [19] proved that p does not divide $h_{p,n}$ for any positive integer n. Thus we study the non-p-part of $h_{p,n}$. Washington [29] showed that the ℓ-part of $h_{p,n}$ is bounded as n tends to ∞ for each prime number ℓ different from p.

K. Horie [10, 11, 12, 13] and K. Horie and M. Horie [14, 15, 16, 17] developed a method for proving the ℓ-indivisibility of $h_{p,n}$:

Theorem 0.1 (K. Horie - M. Horie [14])**.** *Let p be a prime number, ℓ a prime number different from p, f the inertia degree of ℓ in $\mathbb{Q}(\mu_{2p})/\mathbb{Q}$ and p^s the exact power of p dividing $\ell^{\,f} - 1$. Then there exists an explicit positive constant $H(p, s, f)$ such that ℓ does not divide $h_{p,n}$ for any positive integer n if ℓ does not divide $h_{p,s-1}$ and is greater than $H(p, s, f)$.*

From Theorem 0.1 and numerical calculation, K. Horie and M. Horie showed several results. For example, they showed that ℓ does not divide $h_{p,n}$ for any positive integer n if $3 \leq p \leq 23$ and ℓ is a primitive root modulo p^2. In the case $p = 2$, K. Horie showed that ℓ does not divide $h_{2,n}$ for any positive integer n if $\ell \not\equiv \pm 1 \pmod 8$. Fukuda and Komatsu [6, 7, 8] proved that ℓ does not divide $h_{2,n}$ for any positive integer n if $\ell < 10^9$ or $\ell \not\equiv \pm 1 \pmod{32}$. And Okazaki [25] proved that ℓ does not divide $h_{2,n}$ for any positive integer n if ℓ satisfies $\ell > (a^c \cdot c!)^{1/f}$ where f is the inertia degree of ℓ in $\mathbb{Q}(\sqrt{-1})$, 2^s is the exact power of 2 dividing $\ell^{\,f} - 1$, $c = 2^{s-1}$ and a is the constant nearly equal to 0.8079.

In this thesis, based on the above point of view, we shall treat the case p is an odd prime number and study the ℓ-indivisibility of the class number $h_{p,n}$ of the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension of the rational number field $\mathbb{Q}$ for any non-negative integer n.

In chapter 1, we shall recall the main objects of this thesis, that is, the class number, the cyclotomic $\mathbb{Z}_p$-extension, Horie's lemma and the Mahler measure.

In chapter 2, we shall calculate the upper bound of the Mahler measure of the Horie unit and define a constant $G_1(p, s, f)$ where s and f depend on the decomposition field of a prime number ℓ in $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}$. By using Schinzel's inequality and applying Minkowski convex body theorem, we shall prove that a prime number ℓ does not divide $h_{p,n}$ for any non-negative integer n if ℓ is greater than $G_1(p, s, f)$.

In chapter 3, we shall study the new convex body which is more suitable to use Horie's lemma. The results in this chapter play an important role in the next chapter.

In chapter 4, based on the results in the previous chapter, we shall define a constant $G_{cyclo}(p, s, f)$ which is smaller than $G_1(p, s, f)$. From the same argument as in Chapter 2, we shall prove that a prime number ℓ does not divide $h_{p,n}$ for any non-negative integer n if ℓ is greater than $G_{cyclo}(p, s, f)$.

From chapter 5, we shall treat the case $p = 3$ and study the *ell*-indivisibility problem more precisely.

In chapter 5, we shall give a better upper bound of the Mahler measure of Horie unit and a better lower bound of the Mahler measure of relative units. From the same argument as in Chapter 2, we shall prove that a prime number ℓ does not divide $h_{3,n}$ for any non-negative integer n if ℓ^f is greater than $2^{c/2} \cdot c!$ where c/f is the degree of the decomposition field of ℓ in $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}$.

In chapter 6, we shall give the explicit bound of Washington's theorem for the cyclotomic $\mathbb{Z}_3$-extension of the rational number field $\mathbb{Q}$.

In chapter 7, we shall give the algorithm to compute the ℓ-indivisibility of the class number $h_{3,n}$ by using the result in Chapter 6.

In chapter 8, based on the previous algorithm, we shall give the computational results for the ℓ-indivisibility of the class number $h_{3,n}$. By compositing these results and the theorem in Chapter 5, we obtain that, for example, a prime number ℓ does not divide the class number $h_{3,n}$ for any non-negative integer n if ℓ is not congruent to $+1$ or -1 modulo 27.

Contents

Chapter 1

Horie's Lemma and Mahler Measure

In this chapter, we recall the properties of the ideal class group and the definition of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Next, we shall show Horie's method for ℓ-indivisibility of class numbers in the cyclotomic $\mathbb{Z}_p$-extension of the rational number field $\mathbb{Q}$. Finally, we will introduce the Mahler measure of algebraic numbers and its properties.

1.1 Ideal Class Group of Algebraic Number Fields

Let K be an algebraic number field (with finite degree over $\mathbb{Q}$). We denote by $Cl(K)$ and $h(K)$ the ideal class group of K and its order. We call $h(K)$ the class number of K. Let ℓ be a prime number. We also denote by $A(K)$ the ℓ-Sylow subgroup of $Cl(K)$.

Then we have the following:

Lemma 1.1. *Let L/K be an extension of algebraic number fields such that there is no nontrivial unramified abelian subextension. Then the norm map $Cl(L) \longrightarrow Cl(K)$ is surjective for any prime number ℓ.*

Proof. We denote by H_L and H_K maximal unramified abelian extension over L and K, respectively. From class field theory, we have a commutative

diagram

$$\begin{array}{ccc} \mathrm{Gal}(H_L/L) & \xrightarrow{\sim} & Cl(L) \\ \text{restriction}\big\downarrow & & \big\downarrow\text{norm} \\ \mathrm{Gal}(H_K/K) & \xrightarrow{\sim} & Cl(K) \end{array} \tag{1.1.1}$$

Since LH_K/L is an unramified abelian extension, we have $LH_K \subseteq H_L$. Hence the restriction map $\mathrm{Gal}(H_L/L) \longrightarrow \mathrm{Gal}(H_K/K)$ is surjective. By (1.1.1), we obtain that the norm map $Cl(L) \longrightarrow Cl(K)$ is surjective. □

Lemma 1.2. *Let ℓ be a prime number and L/K an extension of algebraic number fields of degree prime to ℓ. Then the natural map $A(K) \longrightarrow A(L)$ is injective. In particular, we have $A(L) = A(K) \oplus D(L/K)$, where $D(L/K)$ is the kernel of the norm map $A(L) \longrightarrow A(K)$.*

Proof. Let $\mathrm{Nr}_{L/K}$ be the norm map $A(L) \longrightarrow A(K)$. We put $m = [L : K]$. Since ℓ does not divide m and $A(K)$ is an ℓ-group, $m^{-1} : A(K) \longrightarrow A(K)$ is isomorphism and the composition

$$A(K) \xrightarrow{m^{-1}} A(K) \longrightarrow A(L) \xrightarrow{\mathrm{Nr}_{L/K}} A(K)$$

is the identity. Hence we have the exact sequence

$$1 \longrightarrow D(L/K) \longrightarrow A(L) \xrightarrow{\mathrm{Nr}_{L/K}} A(K) \longrightarrow 1$$

splits. This completes the proof. □

1.2 Cyclotomic $\mathbb{Z}_p$-extension

Let p be a prime number and μ_m the group of all m-th root of unity. We denote by $\mathbb{B}_{p,n}$ the unique real subfield of $\mathbb{Q}(\mu_{2p^{n+1}})$ which is cyclic of degree p^n over $\mathbb{Q}$ for any non-negative integer n. We put $\mathbb{B}_{p,\infty} = \bigcup_{n\geq 0} \mathbb{B}_{p,n}$. We know that Galois group $\mathrm{Gal}(\mathbb{B}_{p,\infty}/\mathbb{Q})$ is topologically isomorphic to the p-adic integer ring $\mathbb{Z}_p$ as additive group. Then we call $\mathbb{B}_{p,\infty}$ the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ and $\mathbb{B}_{p,n}$ the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. We denote by $h_{p,n}$ the class number of $\mathbb{B}_{p,n}$ and consider the ℓ-indivisibility

of $h_{p,n}$ for a prime number ℓ and any non-negative integer n. In the case $\ell = p$, Iwasawa [19] showed the following:

Theorem 1.3 (Iwasawa)**.** *A prime number p does not divide $h_{p,n}$ for any non-negative integer n.*

Then we study non-p-part of $h_{p,n}$. In the case $\ell \neq p$, Washington [29] showed the following:

Theorem 1.4 (Washington)**.** *Let ℓ be a prime number different from p and ℓ^{e_n} the exact power of ℓ dividing $h_{p,n}$. Then e_n is bounded as n tends to ∞.*

1.3 Horie Unit and Horie's Lemma

Let p be an odd prime number. We put $\zeta_n = \exp(2\pi\sqrt{-1}/p^n)$ a primitive p^n-th root of unity with $\zeta_{n+1}^p = \zeta_n$. Given $k \in \mathbb{Z}$ which is prime to p, there exist a unique $p-1$-th root of unity $\omega_p(k) \in \mathbb{Z}_p$ such that

$$k \equiv \omega_p(k) \pmod{p}.$$

We call ω_p the Teichmüller character modulo p. For each $b \in \mathbb{Z}_p \setminus p^{n+1}\mathbb{Z}_p$, we put

$$\delta_{p,n}(b) = \frac{\zeta_1^b \zeta_{n+1}^b - \zeta_1^{-b}\zeta_{n+1}^{-b}}{\zeta_{n+1}^b - \zeta_{n+1}^{-b}},$$

a cyclotomic unit in $\mathbb{Q}(\zeta_{n+1} + \zeta_{n+1}^{-1})$. It can be rewritten as

$$\delta_{p,n}(b) = \frac{\sin(2b(1+p^n)\pi/p^{n+1})}{\sin(2b\pi/p^{n+1})}.$$

We define the n-th Horie unit

$$\eta_{p,n} = \prod_{k=1}^{(p-1)/2} \delta_{p,n}(\omega_p(k))$$

as a cyclotomic unit in $\mathbb{B}_{p,n}$.

Remark 1.5. The n-th Horie unit is a norm of $\delta(1)$ from $\mathbb{Q}(\zeta_{n+1}+\zeta_{n+1}^{-1})$ to $\mathbb{B}_{p,n}$.

Remark 1.6. Note that $\delta_{p,n}(\omega(p-k))=\delta_{p,n}(\omega(k))$, we have

$$\eta_{p,n}=\prod_{k=(p+1)/2}^{p-1}\delta_{p,n}(\omega_p(k)).$$

Next, let $E_{p,n}$ be the unit group of $\mathbb{B}_{p,n}$, σ a generator of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{n+1})/\mathbb{Q}(\zeta_1))$ and we put $\tau=\sigma^{p^{n-1}}$. Then τ generates the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{n+1})/\mathbb{Q}(\zeta_n))$. An element α in $\mathbb{Z}[\zeta_n]$ is uniquely expressed in the form

$$\alpha=\sum_{i=0}^{(p-1)p^{n-1}-1}a_i\zeta_n^i\quad(a_i\in\mathbb{Z}).$$

For each such α, we associate the element α_σ in the group ring $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_{n+1})/\mathbb{Q}(\zeta_1))]$ by

$$\alpha_\sigma=\sum_{i=0}^{(p-1)p^{n-1}-1}a_i\sigma^i.$$

Since

$$\begin{array}{rcl}\mathbb{Z}[\zeta_n] & \cong & \mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_{n+1})/\mathbb{Q}(\zeta_1))]/(1+\tau+\cdots+\tau^{p-1})\\ \alpha & \longmapsto & \alpha_\sigma\end{array}$$

and $(1-\tau)(1+\tau+\cdots+\tau^{p-1})=0$, the group ring $\mathbb{Z}[\zeta_n]$ acts on $(\mathbb{B}_{p,n}^\times)^{1-\tau}$. Horie [11] proved the following:

Lemma 1.7 (K. Horie)**.** *Let ℓ be a prime number different from p and F an extension in $\mathbb{Q}(\zeta_n)$ of the decomposition field of ℓ for $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Then ℓ divides the integer $h_{p,n}/h_{p,n-1}$ if and only if there exists a prime ideal $\mathfrak{L}$ of F dividing ℓ such that $\eta_{p,n}^{\alpha_\sigma}$ is an ℓ-th power in $E_{p,n}$ for any element α of the integral ideal $\ell\mathfrak{L}^{-1}$ of F.*

Proof. We denote by $C_{p,n}$ the group of circular units in $\mathbb{B}_{p,n}$ (see [27]). Then we know that $h_{p,n}=(E_{p,n}:C_{p,n})$ and $\eta_{p,n}^{1-\sigma}$ generates $C_{p,n}^{1-\tau}$ as $\mathbb{Z}[\zeta_n]$-module

(see [12]). From Theorem 1.3, we obtain that

$$1 \longrightarrow E_{p,n}/C_{p,n} \longrightarrow E_{p,n}/C_{p,n} \longrightarrow E_{p,n}^{1-\tau}/C_{p,n}^{1-\tau} \longrightarrow 1$$

is an exact sequence. Hence we have $h_{p,n}/h_{p,n-1} = (E_{p,n}^{1-\tau} : C_{p,n}^{1-\tau})$.

Let ϵ be an element in $E_{p,n}$ and α an element in $\mathbb{Z}[\zeta_n]$. We assume that $\epsilon^{(1-\tau)\alpha} = 1$. Since there exists an element $\alpha' \in \mathbb{Z}[\zeta_n]$ such that $\alpha\alpha' = m$ is a rational integer, we have $\epsilon^{(1-\tau)m} = 1$. Hence we obtain $\epsilon^{1-\tau} = 1$. This implies that $E_{p,n}^{1-\tau}$ is a torsion-free $\mathbb{Z}[\zeta_n]$-module. Since

$$1 \longrightarrow E_{p,n-1} \longrightarrow E_{p,n} \xrightarrow{1-\tau} E_{p,n}^{1-\tau} \longrightarrow 1$$

is an exact sequence, $E_{p,n}^{1-\tau}$ is a free abelian group of rank $(p-1)p^{n-1} = [\mathbb{Q}(\zeta_n)/\mathbb{Q}]$. From [20] Chapter 1, Proposition 27, there exists an integral ideal $\mathfrak{a}$ of $\mathbb{Q}(\zeta_n)$ such that

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C_{p,n}^{1-\tau} & \longrightarrow & E_{p,n}^{1-\tau} & \longrightarrow & E_{p,n}^{1-\tau}/C_{p,n}^{1-\tau} & \longrightarrow & 1 \\ & & \wr\downarrow & & \wr\downarrow & & \wr\downarrow & & \\ 0 & \longrightarrow & \mathbb{Z}[\zeta_n] & \longrightarrow & \mathfrak{a}^{-1} & \longrightarrow & \mathbb{Z}[\zeta_n]/\mathfrak{a} & \longrightarrow & 0 \end{array}$$

is an exact commutative diagram of $\mathbb{Z}[\zeta_n]$-modules.

If ℓ divides $h_{p,n}/h_{p,n-1} = (E_{p,n}^{1-\tau} : C_{p,n}^{1-\tau})$, then there exists a prime ideal $\mathfrak{L}$ of F dividing ℓ such that $\mathfrak{L}$ divides $\mathfrak{a}$. For any element $\alpha \in \ell\mathfrak{L}^{-1}$, we have $\alpha \in \ell\mathfrak{a}^{-1}$. Therefore, we obtain $\eta_{p,n}^{(1-\sigma)\alpha_\sigma} \in E_{p,n}^{(1-\tau)\ell}$ from above diagram. In particular, we have $\eta_{p,n}^{(1-\sigma)\alpha_\sigma} \in E_{p,n}^{\ell}$. Note that $\sum_{k=0}^{p-1}(1-\tau^k) = p - (1 + \tau + \cdots \tau^{p-1})$ and $1-\sigma$ divides $1-\tau$, we have $\eta_{p,n}^{p\alpha_\sigma} \in E_{p,n}^{\ell}$. Since p is an odd prime number and different from ℓ, we obtain $\eta_{p,n}^{\alpha_\sigma} \in E_{p,n}^{\ell}$.

Conversely, if there exists a prime ideal $\mathfrak{L}$ of F dividing ℓ such that $\eta_{p,n}^{\alpha_\sigma}$ is an ℓ-th power in $E_{p,n}$ for every element $\alpha \in \ell\mathfrak{L}^{-1}$, then we have $\ell\mathfrak{L}^{-1} \subseteq \ell\mathfrak{a}$. Hence $\mathfrak{L}$ divides $\mathfrak{a}$. Therefore, ℓ divides $(E_{p,n}^{1-\tau} : C_{p,n}^{1-\tau}) = h_{p,n}/h_{p,n-1}$.

□

1.4 Mahler Measure and Schinzel's Inequality

Let α be an algebraic number. Denote by $\deg \alpha$ its degree over $\mathbb{Q}$. Suppose the minimal polynomial of α in $\mathbb{Z}[X]$ factors as

$$a(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_{\deg\alpha})$$

over $\mathbb{C}$. The Mahler measure $M(\alpha)$ of α is defined by

$$M(\alpha) = |a| \prod_{j=1}^{\deg\alpha} \max\{1, |\alpha_j|\}.$$

It satisfies the following:

Proposition 1.8. *Let α, β be algebraic integers. Then we have the following:*

1. *Let r be a positive integer. If $\deg \alpha^r = \deg \alpha$, then we have $M(\alpha^r) = M(\alpha)^r$.*
2. *If $\deg \alpha\beta \leq \deg \alpha$ and $\deg \alpha\beta \leq \deg \beta$, then we have $M(\alpha\beta) \leq M(\alpha)M(\beta)$.*
3. *If σ is an automorphism of $\mathbb{Q}(\alpha)$, then we have $M(\alpha^\sigma) = M(\alpha)$.*
4. *If α is a unit, then we have $M(\alpha^{-1}) = M(\alpha)$.*

Let $F(x)$ be a minimal polynomial of a unit in $\mathbb{B}_{p,n}$. We pay attention to Remark 1.16 in [4] and notice that $F(1)F(-1)$ has an exponential lower bound in the degree of $\mathbb{B}_{p,n}$. Now we can show the following inequality by tracing the proof of Theorem 1.14 in [4].

Theorem 1.9 (Schinzel's Inequality)**.** *Let ϵ be a totally real unit different from ± 1 Let $\mathfrak{M}$ be an ideal of $\mathbb{Q}(\epsilon)$ containing $\epsilon^2 - 1$. Then we have*

$$M(\epsilon) \geq \left(\frac{C^{1/d} + \sqrt{C^{2/d}+4}}{2} \right)^{d/2}$$

where $d = \deg \epsilon$ and C is the absolute norm of $\mathfrak{M}$. In particular, we have

$$M(\epsilon) \geq \left(\frac{1+\sqrt{5}}{2} \right)^{d/2}.$$

Proof. Let ϵ be a unit of degree d over $\mathbb{Q}$ other than ± 1 with minimal polynomial

$$(X - \epsilon_1) \cdots (X - \epsilon_d) \in \mathbb{Z}[X].$$

Put $M = M(\epsilon)$ and $A = |F(1)F(-1)|$. We have $M^2 = \prod_{\epsilon_i^2 \geq 1} \epsilon_i^2$, and

$$A = \frac{1}{M^2} \prod_{\epsilon_i^2 \geq 1} |\epsilon_i^2 - 1| \cdot \prod_{\epsilon_i^2 < 1} |\epsilon_i^{-2} - 1|.$$

In order to prove Theorem 1.9, we use the following lemma:

Lemma 1.10. *Let $y_i > 1$ be real numbers, for $1 \leq i \leq m$. Then,*

$$(y_1 - 1) \cdots (y_m - 1) \leq ((y_1 \cdots y_m)^{1/m} - 1)^m.$$

We apply the above lemma,

$$A \leq \frac{1}{M^2} \left(\left(\prod_{\epsilon_i^2 \geq 1} \epsilon_i^2 \cdot \prod_{\epsilon_i^2 < 1} \epsilon_i^{-2} \right)^{1/d} - 1 \right)^d.$$

Since $M^4 = \prod_{\epsilon_i^2 \geq 1} \epsilon_i^2 \cdot \prod_{\epsilon_i^2 < 1} \epsilon_i^{-2}$, we have

$$A \leq \left(M^{2/d} - \frac{1}{M^{2/d}} \right)^d.$$

Hence we have

$$M^{2/d} \geq \frac{A^{1/d} + \sqrt{A^{2/d} + 4}}{2}.$$

This implies

$$M \geq \left(\frac{A^{1/d} + \sqrt{A^{2/d} + 4}}{2} \right)^{d/2}.$$

Since $A \geq C$, we have

$$M(\epsilon) \geq \left(\frac{C^{1/d} + \sqrt{C^{2/d}+4}}{2} \right)^{d/2}.$$

□

Let $\mathfrak{P}$ be a prime ideal in $\mathbb{Q}(\zeta_{n+1})$ dividing p and $\mathrm{ord}_{\mathfrak{P}}(x)$ the normalized additive $\mathfrak{P}$-adic valuation of x. Moreover, we let $\mathfrak{p}$ be a prime ideal in $\mathbb{B}_{p,n}$ dividing p and $\mathrm{ord}_{\mathfrak{p}}(x)$ the normalized additive $\mathfrak{p}$-adic valuation of x. Then we have $\mathrm{ord}_{\mathfrak{p}}(x) = (p-1) \cdot \mathrm{ord}_{\mathfrak{P}}(x)$ for all x in $\mathbb{B}_n$. If ϵ is a unit in $\mathbb{B}_{p,n}$, then we have the following:

Lemma 1.11. *Let ϵ be a unit in $\mathbb{B}_{p,n}$. If $Nr_{\mathbb{B}_{p,n}/\mathbb{B}_{p,n-1}}(\epsilon) = 1$ and $\epsilon \neq 1$, then we have*

$$\mathrm{ord}_{\mathfrak{p}}(\epsilon - 1) \geq \frac{N-1}{p-1},$$

where $N = p^n$.

Proof. There exists an element x in $\mathbb{Z}[\zeta_{n+1}]$ such that $\epsilon = x^{1-\tau}$ by the Hilbert's theorem 90. Since $\mathfrak{P}^p = (1-\zeta_{n+1}^p)$ and $(1-\zeta_{n+1}^p)^\tau = 1-\zeta_{n+1}^p$, we may assume $\mathrm{ord}_{\mathfrak{P}}(x) = 0, 1 \ldots p-1$. Note that if α is an element of $\mathbb{Z}[\zeta]$ then we have $\mathrm{ord}_{\mathfrak{P}}(\alpha - \alpha^\tau) \geq N$. Hence we have

$$\mathrm{ord}_{\mathfrak{P}}(\epsilon - 1) = \mathrm{ord}_{\mathfrak{P}} \left(\frac{x - x^\tau}{x^\tau} \right) \geq N - p + 1,$$

that is, $(p-1)\mathrm{ord}_{\mathfrak{p}}(\epsilon - 1) \geq N - p + 1$. Since $\mathrm{ord}_{\mathfrak{p}}(\epsilon - 1)$ is a rational integer, we have

$$\mathrm{ord}_{\mathfrak{p}}(\epsilon - 1) \geq \frac{N-1}{p-1}.$$

□

Note that the absolute norm of $\mathfrak{p}$ is equal to p. From Theorem 1.9 and Lemma 1.11, we get the following:

Lemma 1.12. *Let ϵ be a unit in $\mathbb{B}_{p,n}$ with $Nr_{\mathbb{B}_{p,n}/\mathbb{B}_{p,n-1}}(\epsilon) = 1$ and put $N = p^n$. Then we have*

$$M(\epsilon) \geq \left(\frac{p^{(N-1)/(p-1)N} + \sqrt{p^{2(N-1)/(p-1)N} + 4}}{2} \right)^{N/2}.$$

Chapter 2

Inequality for Odd Prime Number

Let p be an odd prime number. We denote by $h_{p,n}$ the class number of the n-th layer $\mathbb{B}_{p,n}$ of the cyclotomic $\mathbb{Z}_p$-extension of the rational number field $\mathbb{Q}$. In this chapter, we shall consider the ℓ-indivisibility of $h_{p,n}$ for any prime number ℓ different from p. First, we shall give an upper bound of the Mahler measure of Horie unit. Next, we shall apply Minkoski convex body theorem to the ideal $\ell\mathfrak{L}^{-1}$ in Lemma 1.7. Then, based on Lemma 1.7, we can get the following by combining these results and Schinzel's inequality:

Theorem 2.1. *Let p be an odd prime number, ℓ a prime number different from p and n a positive integer.*
Choose s so that p^s the exact power of p dividing $\ell^{p-1}-1$. We put $r = \min\{n, s\}$, $q(m) = p^{m-1}$ and $c(m) = (p-1)\cdot q(m)$. We denote by f the inertia degree of ℓ in $\mathbb{Q}(\mu_p)/\mathbb{Q}$. We also put

$$G_1(p,r,f) = \left(\left(\frac{\sqrt{6}p}{2}\right)^{c(r)} \cdot c(r)!\right)^{1/f}.$$

If ℓ satisfies $\ell > G_1(p,r,f)$, then ℓ does not divide $h_{p,n}$.

2.1 Upper Bound of Mahler Measure of Horie Unit

In this section, we study an upper bound of Mahler measure of Horie unit.

Lemma 2.2. *Let ν be a positive integer. Assume sequences $\{a_i\}_{i=1}^{\nu}$ and $\{b_i\}_{i=1}^{\nu}$ satisfy $a_1 \geq a_2 \geq \cdots \geq a_\nu > 0$ and $0 < b_1 \leq b_2 \leq \cdots \leq b_\nu$ respectively. Let λ be the largest number such that $a_\lambda \geq b_\lambda$ if $a_1 \geq b_1$ or 0 otherwise. Let ϕ and ψ be injections from $\{1, 2, \cdots, \mu\}$ to $\{1, 2, \cdots, \nu\}$ for $0 \leq \mu \leq \nu$. Then we have*

$$\prod_{i=1}^{\mu} \frac{a_{\phi(i)}}{b_{\psi(i)}} \leq \prod_{i=1}^{\lambda} \frac{a_i}{b_i},$$

where the left hand side reads 1 if it is an empty product.

Proof. Obviously, we have

$$\prod_{i=1}^{\mu} a_{\phi(i)} \leq \prod_{i=1}^{\mu} a_i, \prod_{i=1}^{\mu} b_{\phi(i)} \geq \prod_{i=1}^{\mu} b_i.$$

Hence we have

$$\prod_{i=1}^{\mu} \frac{a_{\phi(i)}}{b_{\psi(i)}} \leq \prod_{i=1}^{\mu} \frac{a_i}{b_i}.$$

On the other hand, the function

$$\mu \longmapsto \prod_{i=1}^{\mu} \frac{a_i}{b_i}$$

takes its maximum at $\mu = \lambda$. □

We put $N = p^n$ and $\Theta = \pi/2pN$. Recalling the n-th Horie unit

$$\eta_{p,n} = \prod_{k=1}^{(p-1)/2} \delta_{p,n}(\omega_p(k)) = \prod_{k=(p+1)/2}^{p-1} \delta_{p,n}(\omega_p(k)),$$

the definition of Mahler measure implies

$$M(\eta_{p,n}) \leq \prod_{j=1}^{(pN-1)/2} \max\{1, |\delta_{p,n}(j)|\}.$$

We put $S = \{|\sin(4j\Theta)|\}_{j=1}^{(pN-1)/2}$. Since $\delta_{p,n}(j) = |\sin(4j(1+N)\Theta)|/|\sin(4j\Theta)|$, the numerator and the denominator of $\delta_{p,n}(j)$ are in S. Since $\sin(4j\Theta) = \sin(2(pN-2j)\Theta)$, we have

$$S = \left\{ \sin(2j\Theta) \;\middle|\; j = 1, 2, \cdots, \frac{pN-1}{2} \right\}.$$

Then we have

$$M(\eta_{p,n}) \leq \prod_{j=1}^{\lfloor (pN-1)/4 \rfloor} \frac{\sin((pN+1-2j)\Theta)}{\sin(2j\Theta)}$$

from Lemma 2.2. Since

$$\sin((pN+1-2j)\Theta) = \cos((2j-1)\Theta),$$

we have

$$\begin{aligned} M(\eta_{p,n}) &\leq \prod_{j=1}^{\lfloor (pN-1)/4 \rfloor} \frac{\cos((2j-1)\Theta)}{\sin((2j-1)\Theta)} \\ &= \prod_{j=1}^{\lfloor (pN-1)/4 \rfloor} \cot((2j-1)\Theta). \end{aligned}$$

We will estimate the logarithm of the right hand side by using integral. For this purpose, we verify convexity of the function $\log\cot\theta$ on the interval $0 < \theta < \pi/4$. Indeed, we have

$$\frac{d}{d\theta} \log\cot\theta = -\frac{1}{\sin\theta\cos\theta} < 0$$

and

$$\frac{d^2}{d\theta^2} \log\cot\theta = \frac{\cos 2\theta}{(\sin\theta\cos\theta)^2} > 0.$$

Therefore, we have

$$\frac{\pi}{pN}\sum_{j=1}^{\lfloor (pN-1)/4\rfloor}\log\cot((2j-1)\Theta) < \int_0^{\pi/4}\log\cot t\ dt.$$

This implies

$$M(\eta_{p,n}) < \exp\left(\frac{pN}{\pi}\int_0^{\pi/4}\log\cot t\ dt\right).$$

Here, we put

$$L(\theta) = \int_0^{\theta}\log\cot t\ dt$$

for $0 \leq \theta < \pi/2$. Recall the Lobachevsky function ([9],[22]) to see:

Lemma 2.3. *We have*

$$L(\theta) = \sum_{m=0}^{\infty}\frac{1}{(2m+1)^2}\sin(2(2m+1)\theta).$$

By the above lemma, we have

$$L\left(\frac{\pi}{4}\right) = \sum_{m=0}^{\infty}\frac{(-1)^m}{(2m+1)^2}.$$

The right hand side is called Catalan's constant. Its value is evaluated as follows

$$L\left(\frac{\pi}{4}\right) = 0.915965594\cdots.$$

Hence we have

$$\frac{pN}{\pi}L\left(\frac{\pi}{4}\right) < 0.291560904\cdot pN.$$

We now conclude the following:

Lemma 2.4. *We have*

$$M(\eta_{p,n}) < \exp(0.291560904\cdot pN).$$

2.2 Minkowski Convex Body Theorem for Theorem 2.1

Let ℓ be a prime number different from p, n a positive integer and p^s the exact power of p dividing $\ell^{p-1}-1$. We put $r=\min\{n,s\}$, $q=p^{r-1}$ and $c=(p-1)q$. In this section, we consider the mapping:

$$\mu : \mathbb{Q}(\zeta_r) \longrightarrow \mathbb{C}^c; \quad \alpha \longmapsto \overrightarrow{\alpha} := (\alpha^\rho)_{\rho\in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})} \tag{2.2.1}$$

and the $\mathbb{R}$-vector space:

$$W = \mathbb{R}\overrightarrow{1}+\mathbb{R}\overrightarrow{\zeta_r}+\cdots+\mathbb{R}\overrightarrow{\zeta_r^{c-1}} \cong \mathbb{R}^c; \quad \sum_{j=0}^{c-1} a_j \overrightarrow{\zeta^j} \longmapsto (a_0,a_1,\ldots,a_{c-1}). \tag{2.2.2}$$

We put

$$X_1 = \left\{ \sum_{i=0}^{c-1} a_i \overrightarrow{\zeta_r^i} \in W \;\middle|\; a_0,\cdots,a_{c-1}\in\mathbb{R},\ |a_0|+|a_1|+\cdots+|a_{c-1}| \le \frac{2\ell}{\sqrt{6}p} \right\}$$

and define $|\cdot|_1$ on $\mathbb{Z}[\zeta_r]$ such that

$$|a_0+a_1\zeta_r+\cdots+a_{c-1}\zeta_r^{c-1}|_1 = |a_0|+|a_1|+\cdots|a_{c-1}|.$$

Now we apply Minkowski convex body theorem with respect to the volume on W induced by the standard volume on $\mathbb{R}^c$ by (2.2.2) to see:

Lemma 2.5. *Let ℓ, n, s, r, c and X_1 be as above and $\mathfrak{L}$ a prime ideal of $\mathbb{Q}(\zeta_r)$ dividing ℓ. We denote by f the inertia degree of $\mathfrak{L}$ in $\mathbb{Q}(\zeta_r)/\mathbb{Q}$. If ℓ satisfies $\ell^f > (\sqrt{6}p/2)^c\cdot c!$, then there exists a non-zero element $\overrightarrow{\alpha}$ in $X_1\cap\mu(\ell\mathfrak{L}^{-1})$. Then α lies in $\ell\mathfrak{L}^{-1}$ and satisfies $|\alpha|_1 \le 2\ell/\sqrt{6}p$.*

2.3 Proof of Theorem 2.1

Let ℓ be a prime number different form p, p^s the exact power of p dividing $\ell^{p-1}-1$ and n a positive integer. We put $N=p^n$, $r=\min\{n,s\}$ and $c=(p-1)\cdot p^{r-1}$. We denote by f the inertia degree of ℓ in $\mathbb{Q}(\zeta_r)/\mathbb{Q}$. Assume

that ℓ satisfies $\ell^f > (\sqrt{6}p/2)^c \cdot c!$. We also assume that ℓ divides $h_{p,n}/h_{p,n-1}$. By Lemma 1.7 and Lemma 2.5, there exist a prime ideal $\mathfrak{L}$ in $\mathbb{Q}(\zeta_r)$ lying above ℓ, an element α in $\ell\mathfrak{L}^{-1}$ and a unit ϵ in $E_{p,n}$ such that

$$\eta_{p,n}^{\alpha_\sigma} = \epsilon^\ell \tag{2.3.1}$$

and

$$|\alpha|_1 < \frac{2\ell}{\sqrt{6}p}. \tag{2.3.2}$$

By Theorem 1.9, we have

$$M(\epsilon) \geq \left(\frac{1+\sqrt{5}}{2}\right)^{N/2} > \exp(0.240605912 \cdot N). \tag{2.3.3}$$

Since $\deg \epsilon^\ell = \deg \epsilon$ and $\deg \eta_{p,n}^{\alpha_\sigma} \leq \deg \eta_{p,n}$, we have

$$M(\epsilon^\ell) = M(\epsilon)^\ell \tag{2.3.4}$$

and

$$M(\eta_{p,n}^{\alpha_\sigma}) \leq M(\eta_{p,n})^{|\alpha|_1}. \tag{2.3.5}$$

By (2.3.1), (2.3.2), (2.3.3), (2.3.4), (2.3.5) and Lemma 2.4, we have

$$\begin{aligned} \exp(0.240605912 \cdot N\ell) &\leq M(\epsilon)^\ell = M(\epsilon^\ell) = M(\eta_{p,n}^{\alpha_\sigma}) \\ &\leq M(\eta_{p,n})^{|\alpha|_1} \\ &< \exp\left(0.291560904 \cdot pN \cdot \frac{2\ell}{\sqrt{6}p}\right). \end{aligned}$$

Hence we have

$$0.240605912 < 0.291560904 \cdot \frac{2}{\sqrt{6}} = 0.238058481\cdots.$$

Contradiction established Theorem 2.1.

Chapter 3

Volume of a Certain Convex Body

For proving Theorem 4.1 in the next chapter, we consider another convex body.

Let p be an odd prime number and r a positive integer. Put $q = p^{r-1}$, $c = (p-1)q$, $\zeta = \zeta_r$ and $\omega = \zeta_1$. We also put

$$\mathfrak{B} = \left\{ \sum_{i=0}^{pq-1} s_i t_i \overrightarrow{\zeta^i} \;\middle|\; s_i \in \{+1, -1\}, 0 \leq t_i \leq 1, (i = 0, 1, \ldots, pq-1), \sum_{i=0}^{pq-1} t_i \leq 1 \right\}$$

where $\overrightarrow{\zeta^i}$ is defined in Section 4.1. In this chapter, we shall calculate the volume of $\mathfrak{B}$.

3.1 Convex Hull of Standard Vectors

We consider more general situations. Let $2 \leq \nu \in \mathbb{Z}$ and V the linear space

$$V = \mathbb{R}^\nu.$$

Denote by $\boldsymbol{e}_1, \boldsymbol{e}_2 \ldots, \boldsymbol{e}_\nu$ the standard basis for V and set

$$\boldsymbol{d} = \boldsymbol{e}_1 + \boldsymbol{e}_2 + \cdots + \boldsymbol{e}_\nu$$

For any set $\mathfrak{M}$ in V, we denote by $\hat{\mathfrak{M}}$ the convex hull of $\mathfrak{M}$. We also set $\mathfrak{N} = \{1, 2, \ldots, \nu\}$.

We consider the symmetric convex hull $\mathfrak{B}_\nu$ of the set

$$\mathfrak{R} = \{\boldsymbol{d}, -\boldsymbol{d}, +\boldsymbol{e}_i, -\boldsymbol{e}_i \mid i \in \mathfrak{N}\} :$$

$$\begin{aligned} \mathfrak{B}_\nu &= \hat{\mathfrak{R}} \\ &= \left\{ s_0 t_0 \boldsymbol{d} + \sum_{i=1}^{\nu} s_i t_i \boldsymbol{e}_i \;\middle|\; s_j \in \{+1, -1\}, 0 \leq t_j \leq 1, (j = 0, 1, \ldots, \nu), \sum_{i=0}^{\nu} t_i \leq 1 \right\}. \end{aligned}$$

We will calculate its volume $\mathrm{vol}(\mathfrak{B}_\nu)$, where vol denotes the Lebesgue measure on V.

Define the norm $|\bullet|_{\mathrm{cyclo}}$ on V by

$$|\boldsymbol{v}|_{\mathrm{cyclo}} = \inf\{r \in \mathbb{R}_{\geq 0} \mid \boldsymbol{v} \in r\mathfrak{B}_\nu\}.$$

Then, for $\boldsymbol{v} \in V$, we have

$$|\boldsymbol{v}|_{\mathrm{cyclo}} = \min\{r \in \mathbb{R}_{\geq 0} \mid \boldsymbol{v} \in r\mathfrak{B}_\nu\} < +\infty.$$

We also denote by $|\bullet|_{\mathrm{cyclo}}$ the norm on V^K defined by

$$|(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_K)|_{\mathrm{cyclo}} = \sum_{i=1}^{K} |\boldsymbol{v}|_{\mathrm{cyclo}}$$

Let

$$\mathfrak{B}_\nu^{(K)} = \{(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_K) \in V^K \mid |(\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_K)|_{\mathrm{cyclo}} \leq 1\}.$$

We will calculate its volume $\mathrm{vol}^{(K)}(\mathfrak{B}_\nu^{(K)})$, where $\mathrm{vol}^{(K)}$ denotes the Lebesgue measure on V^K.

3.2 Decomposition into Simplices

The symmetric convex body $\mathfrak{B}_\nu$ contains the convex hull $\mathfrak{C}_\nu$ of the set

$$\mathfrak{Q} = \{+\boldsymbol{e}_i, -\boldsymbol{e}_i \mid i \in \mathfrak{N}\} :$$

$$\mathfrak{C}_\nu = \left\{ \sum_{i=1}^{\nu} s_i t_i \boldsymbol{e}_i \;\middle|\; s_j \in \{+1,-1\}, 0 \le t_j \le 1, (j \in \mathfrak{N}); \sum_{i=1}^{\nu} t_i \le 1 \right\}.$$

For an arbitrary subset I of $\{1, 2, \ldots, \nu\}$, we define

$$\mathfrak{V}_I = \{+\boldsymbol{e}_i, -\boldsymbol{e}_j \mid i \in I, j \notin I\}; \quad \mathfrak{F}_I = \widehat{\mathfrak{V}_I}.$$

Then, $\mathfrak{F}_I$ with $I \subset \{1, 2, ..., \nu\}$ form the facets of $\mathfrak{C}_\nu$. We set

$$\mathfrak{S}_I(P) = \widehat{\{P\} \cup \mathfrak{F}_I}.$$

Obviously, $\mathfrak{S}_I(P)$ is a simplex of ν-dimension.

The symmetric convex body $\mathfrak{C}_\nu$ has the following decomposition in to simplices:

$$\mathfrak{C}_\nu = \bigcup_{I \subset \mathfrak{N}} \mathfrak{S}_I(\boldsymbol{o}),$$

where $\boldsymbol{o} = (0, 0, ..., 0)$ is the origin of V.

Lemma 3.1. *The symmetric convex body $\mathfrak{B}_\nu$ is decomposed into a non-overlapping union of ν-dimensional closed simplices as follows:*

$$\mathfrak{B}_\nu = \bigcup_{I \subset \mathfrak{N}} \mathfrak{S}_I(\boldsymbol{o}) \cup \bigcup_{I \subset \mathfrak{N};\, 2|I| > \nu} \mathfrak{S}_I(+\boldsymbol{d}) \cup \bigcup_{I \subset \mathfrak{N};\, 2|I| < \nu} \mathfrak{S}_I(-\boldsymbol{d}).$$

Proof. Obviously, $\mathfrak{B}_\nu$ contains the right hand side. It suffice to prove that $\mathfrak{B}_\nu$ is contained in the right hand side.

Let $P \in \mathfrak{B}_\nu \setminus \mathfrak{C}_\nu$. Then, there exists $x, y, z \in [0, 1]$ and $Q \in \mathfrak{C}_\nu$ such that $P = xQ + y(+\boldsymbol{d}) + z(-\boldsymbol{d})$ and $x + y + z = 1$. Let $s = +1$ or -1 according as $y \ge z$ or not. Then, we have $P = |y - z|(s\boldsymbol{d}) + (xQ + (y + z - |y - z|)\boldsymbol{o})$. Thus, P lies on the segment $\mathfrak{L}$ connecting one of $\pm\boldsymbol{d}$ to some point Q' of $\mathfrak{C}_\nu$. Since $\mathfrak{B}_\nu$ is a symmetric convex body, we may assume the sign of $\boldsymbol{d}$ here is positive. The closest point Q'' in $\mathfrak{L} \cap \mathfrak{C}_\nu$ is uniquely determined since $\mathfrak{C}_\nu$ is topologically closed while $Q' \in \mathfrak{C}_\nu$, $\boldsymbol{d} \notin \mathfrak{C}_\nu$. By convexity of $\mathfrak{C}_\nu$, the segment connecting Q' to Q'' is contained in $\mathfrak{C}_\nu$. Thus, the point P lies on the segment connecting $\boldsymbol{d}$ to Q''.

Write $Q'' = (x_1, x_2, \ldots, x_\nu)$. Then, we have

$$-1 \leq x_i \leq +1, \quad (i \in \mathfrak{N}); \quad \sum_{i=1}^{\nu} |x_i| = 1.$$

By symmetry of the set $\mathfrak{B}_\nu$ with respect to permutation of the coordinates, we may assume

$$+1 \geq x_1 \geq x_2 \geq \cdots \geq x_m \geq 0 > x_{m+1} \geq x_{m+2} \geq \cdots x_{m+n} \geq -1,$$

where $m + n = \nu$. An arbitrary point $Y = (y_1, y_2, \ddots, y_\nu)$ on the segment connecting $\boldsymbol{d}$ to Q'' is written as

$$Y = t\boldsymbol{d} + (1-t)(x_1, x_2, \ldots, x_\nu), \quad 0 \leq t \leq 1.$$

For sufficiently small positive t, we have

$$\begin{aligned} |y_1| + |y_2| + \cdots + |y_\nu| &= \sum_{i=1}^{m} (t + (1-t)\,|x_i|) + \sum_{j=1}^{n} (-t + (1-t)\,|x_{m+j}|) \\ &= t\,(m-n) + (1-t) \sum_{k=1}^{\nu} |x_k| \\ &= t(m-n-1) + 1. \end{aligned}$$

Here, by the choice of Q'', the left hand side is larger than 1. Therefore, we have $m > n$.

Set $I = \{1, 2, \ldots, m\}$. Then, $(x_1, x_2, \ldots, x_\nu) \in \mathfrak{F}_I$ with $2|I| > \nu$. We now see $P \in \mathfrak{S}_I(+\boldsymbol{d})$.

Ambiguity in choice of I such that $(x_1, x_2, \ldots, x_\nu) \in \mathfrak{F}_I$ only occurs if $x_k = 0$ for some k. In this case P belongs to the convex hull of the set $\{\boldsymbol{d}, +\boldsymbol{e}_i, \boldsymbol{e}_j \mid x_i > 0; x_j < 0\}$ consisting less than $\nu + 1$ points. This convex hull has smaller dimension than ν. We now see that our union of the Lemma is non-overlapping.

3.3 Decomposition into Simplices

The symmetric convex body $\mathfrak{B}_\nu$ contains the convex hull $\mathfrak{C}_\nu$ of the set

$$\mathfrak{Q} = \{+\boldsymbol{e}_i, -\boldsymbol{e}_i \mid i \in \mathfrak{N}\} :$$

$$\mathfrak{C}_\nu = \left\{ \sum_{i=1}^{\nu} s_i t_i \boldsymbol{e}_i \;\middle|\; s_j \in \{+1,-1\}, 0 \le t_j \le 1, (j \in \mathfrak{N}); \sum_{i=1}^{\nu} t_i \le 1 \right\}.$$

For an arbitrary subset I of $\{1,2,\ldots,\nu\}$, we define

$$\mathfrak{V}_I = \{+\boldsymbol{e}_i, -\boldsymbol{e}_j \mid i \in I, j \notin I\}; \quad \mathfrak{F}_I = \widehat{\mathfrak{V}_I}.$$

Then, $\mathfrak{F}_I$ with $I \subset \{1,2,...,\nu\}$ form the facets of $\mathfrak{C}_\nu$. We set

$$\mathfrak{S}_I(P) = \widehat{\{P\} \cup \mathfrak{F}_I}.$$

Obviously, $\mathfrak{S}_I(P)$ is a simplex of ν-dimension.

The symmetric convex body $\mathfrak{C}_\nu$ has the following decomposition in to simplices:

$$\mathfrak{C}_\nu = \bigcup_{I \subset \mathfrak{N}} \mathfrak{S}_I(\boldsymbol{o}),$$

where $\boldsymbol{o} = (0,0,...,0)$ is the origin of V.

Lemma 3.2. *The symmetric convex body $\mathfrak{B}_\nu$ is decomposed into a non-overlapping union of ν-dimensional closed simplices as follows:*

$$\mathfrak{B}_\nu = \bigcup_{I \subset \mathfrak{N}} \mathfrak{S}_I(\boldsymbol{o}) \cup \bigcup_{I \subset \mathfrak{N};\, 2|I| > \nu} \mathfrak{S}_I(+\boldsymbol{d}) \cup \bigcup_{I \subset \mathfrak{N};\, 2|I| < \nu} \mathfrak{S}_I(-\boldsymbol{d}).$$

Proof. Obviously, $\mathfrak{B}_\nu$ contains the right hand side. It suffice to prove that $\mathfrak{B}_\nu$ is contained in the right hand side.

Let $P \in \mathfrak{B}_\nu \setminus \mathfrak{C}_\nu$. Then, there exists $x, y, z \in [0,1]$ and $Q \in \mathfrak{C}_\nu$ such that $P = xQ + y(+\boldsymbol{d}) + z(-\boldsymbol{d})$ and $x + y + z = 1$. Let $s = +1$ or -1 according as $y \ge z$ or not. Then, we have $P = |y-z|(s\boldsymbol{d}) + (xQ + (y + z - |y-z|)\boldsymbol{o})$. Thus, P lies on the segment $\mathfrak{L}$ connecting one of $\pm\boldsymbol{d}$ to some point Q' of $\mathfrak{C}_\nu$. Since $\mathfrak{B}_\nu$ is a symmetric convex body, we may assume the sign of $\boldsymbol{d}$ here is positive. The closest point Q'' in $\mathfrak{L} \cap \mathfrak{C}_\nu$ is uniquely determined since $\mathfrak{C}_\nu$ is topologically closed while $Q' \in \mathfrak{C}_\nu$, $\boldsymbol{d} \notin \mathfrak{C}_\nu$. By convexity of $\mathfrak{C}_\nu$, the segment connecting Q' to Q'' is contained in $\mathfrak{C}_\nu$. Thus, the point P lies on the segment connecting $\boldsymbol{d}$ to Q''.

Write $Q'' = (x_1, x_2, \ldots, x_\nu)$. Then, we have

$$-1 \leq x_i \leq +1, \quad (i \in \mathfrak{N}); \quad \sum_{i=1}^{\nu} |x_i| = 1.$$

By symmetry of the set $\mathfrak{B}_\nu$ with respect to permutation of the coordinates, we may assume

$$+1 \geq x_1 \geq x_2 \geq \cdots \geq x_m \geq 0 > x_{m+1} \geq x_{m+2} \geq \cdots x_{m+n} \geq -1,$$

where $m + n = \nu$. An arbitrary point $Y = (y_1, y_2, \ddots, y_\nu)$ on the segment connecting $\boldsymbol{d}$ to Q'' is written as

$$Y = t\boldsymbol{d} + (1-t)(x_1, x_2, \ldots, x_\nu), \quad 0 \leq t \leq 1.$$

For sufficiently small positive t, we have

$$\begin{aligned} |y_1| + |y_2| + \cdots + |y_\nu| &= \sum_{i=1}^{m} (t + (1-t)\,|x_i|) + \sum_{j=1}^{n} (-t + (1-t)\,|x_{m+j}|) \\ &= t\,(m-n) + (1-t) \sum_{k=1}^{\nu} |x_k| \\ &= t(m-n-1) + 1. \end{aligned}$$

Here, by the choice of Q'', the left hand side is larger than 1. Therefore, we have $m > n$.

Set $I = \{1, 2, \ldots, m\}$. Then, $(x_1, x_2, \ldots, x_\nu) \in \mathfrak{F}_I$ with $2|I| > \nu$. We now see $P \in \mathfrak{S}_I(+\boldsymbol{d})$.

Ambiguity in choice of I such that $(x_1, x_2, \ldots, x_\nu) \in \mathfrak{F}_I$ only occurs if $x_k = 0$ for some k. In this case P belongs to the convex hull of the set $\{\boldsymbol{d}, +\boldsymbol{e}_i, \boldsymbol{e}_j \mid x_i > 0; x_j < 0\}$ consisting less than $\nu + 1$ points. This convex hull has smaller dimension than ν. We now see that our union of the Lemma is non-overlapping.

3.4 Volume of each Simplex

By decomposing into simplices and evaluating the volume of each simplex, we show the following:

Proposition 3.3. *Put* $M_n = \sum_{k=0}^{2k<n} \binom{n}{k} (n-2k-1) + 2^{n-1}$. *Then we have*

$$\mathrm{vol}(\mathfrak{B}_\nu) = \frac{2}{\nu!} M_\nu.$$

In Proposition 3.4, we evaluate this combinatorial sum. And we rewrite Proposition 3.3 into a useful form in Proposition 3.5.

Proof. Let column vectors $\boldsymbol{e}'_1$, $\boldsymbol{e}'_2$, $\ldots$, $\boldsymbol{e}'_{\nu+1}$ be the standard basis of $\mathbb{R}^{\nu+1}$. Let $\boldsymbol{v} \in V \longrightarrow \tilde{\boldsymbol{v}} \in \mathbb{R}^{\nu+1}$ be the map

$$(z_1, z_2, \ldots, z_\nu) \longmapsto {}^t(z_1, z_2, \ldots, z_\nu, 1).$$

Then, we have

$$\mathrm{vol}(\mathfrak{S}_I(\boldsymbol{v})) = \frac{1}{\nu!} \left|\det\left(\widetilde{s_1\boldsymbol{e}}_1, \widetilde{s_2\boldsymbol{e}}_2, \ldots, \widetilde{s_\nu\boldsymbol{e}}_\nu, \tilde{\boldsymbol{v}}\right)\right|,$$

where $s_i = +1$ or -1 according as $i \in I$ or not. In particular,

$$\mathrm{vol}(\mathfrak{S}_I(\boldsymbol{d})) = \frac{1}{\nu!} \left|\det\left(\widetilde{s_1\boldsymbol{e}}_1, \widetilde{s_2\boldsymbol{e}}_2, \ldots, \widetilde{s_\nu\boldsymbol{e}}_\nu, \widetilde{\boldsymbol{d}}\right)\right|,$$

We perform column operation on the matrix: subtract $s_i\widetilde{s_i\boldsymbol{e}}_i$ $(i \in \mathfrak{N})$ from the last column. Then, we get

$$\mathrm{vol}(\mathfrak{S}_I(\boldsymbol{d})) = \frac{1}{\nu!} \left|\det\left(\widetilde{s_1\boldsymbol{e}}_1, \widetilde{s_2\boldsymbol{e}}_2, \ldots, \widetilde{s_\nu\boldsymbol{e}}_\nu, (\nu+1-2|I|)\widetilde{\boldsymbol{o}}\right)\right| = \frac{2|I|-\nu-1}{\nu!},$$

provided $2|I| > \nu$. By symmetry, we also get

$$\mathrm{vol}(\mathfrak{S}_I(\boldsymbol{d})) = \frac{2(\nu-|I|)-\nu-1}{\nu!} = \frac{\nu-2|I|-1}{\nu!}$$

provided $2|I| < \nu$. We now see

$$\mathrm{vol}(\mathfrak{B}_\nu) = \frac{2}{\nu!}\left(\sum_{k=0}^{2k<\nu} \binom{\nu}{k} (\nu-2k-1) + 2^{\nu-1}\right) = \frac{2}{\nu!} M_\nu.$$

□

The combinatorial sum in Proposition 3.3 is evaluated by the following:

Proposition 3.4. *We have*

$$M_{2n} = \frac{2n+1}{2}\binom{2n}{n}, \quad M_{2n+1} = (2n+1)\binom{2n}{n}.$$

With permission from Hacene Belbachir, we include his proof of Proposition 3.4.

Proof of Proposition 3.4. We put $S_n = \sum_{k=0}^{2k<n} \binom{n}{k}$ and $T_n = \sum_{k=0}^{2k<n} k\binom{n}{k}$. Using the fact that

$$k\binom{n}{k} = n\binom{n-1}{k-1},$$

we have

$$T_n = n \sum_{k=0}^{2k<n-2} \binom{n-1}{k}.$$

Now using the symmetry of binomial coefficient, we have

$$S_{2n} = 2^{2n-1} - \frac{1}{2}\binom{2n}{n}, \quad S_{2n+1} = 2^{2n}$$

and

$$T_{2n} = n2^{2n-1} - n\binom{2n}{n}, \quad T_{2n+1} = (2n+1)2^{2n-1} - \frac{2n+1}{2}\binom{2n}{n}.$$

Since $M_n = (n-1)S_n - 2T_n + 2^{n-1}$, we have

$$M_{2n} = \frac{2n+1}{2}\binom{2n}{n}, \quad M_{2n+1} = (2n+1)\binom{2n}{n}.$$

□

Form the Proposition 3.3 and Proposition 3.4, we obtain the following:

Proposition 3.5. *We have*

$$\mathrm{vol}(\mathfrak{B}_\nu) = \begin{cases} \dfrac{2}{(m!)^2} & \text{if} \quad \nu = 2m+1; \\ \dfrac{2m+1}{(m!)^2} & \text{if} \quad \nu = 2m. \end{cases} \tag{3.4.1}$$

We can make up (3.4.1) in the following formula which looks simpler on the surface:

$$\mathrm{vol}(\mathfrak{B}_\nu) = \frac{2^\nu}{\nu!} B_m = \mathrm{vol}(\widehat{\mathfrak{M}}) B_m,$$

where we put ,

$$B_m = \frac{(2m+1)!}{2^{2m} m!^2}, \quad m = \left\lfloor \frac{\nu}{2} \right\rfloor \tag{3.4.2}$$

$$\mathrm{vol}(\widehat{\mathfrak{M}}_\nu) = \frac{2^\nu}{\nu!}, \quad \mathfrak{M}_\nu = \{\boldsymbol{e}_i, -\boldsymbol{e}_i \mid 1 \leq i \leq \nu\}.$$

3.5 Calculation of $\mathrm{vol}(\mathfrak{B}_\nu^{(K)})$

In (3.4.1), we have

$$\mathrm{vol}(\mathfrak{B}_\nu^{(1)}) = \mathrm{vol}(\mathfrak{B}_\nu) = \begin{cases} \dfrac{2}{(m!)^2} & \text{if} \quad \nu = 2m+1; \\ \dfrac{2m+1}{(m!)^2} & \text{if} \quad \nu = 2m. \end{cases} \tag{3.5.1}$$

Let $K \geq 2$. The set $\mathfrak{B}_\nu^K$ is not the direct product (e.g., of $\mathfrak{B}_\nu$ and $\mathfrak{B}_\nu^{(K-1)}$). However, it is a fiber product:

$$\mathfrak{B}_\nu^{(K)} = \bigcup_{\boldsymbol{v} \in \mathfrak{B}_\nu} \left(\{\boldsymbol{v}\} \times \left(1 - |\boldsymbol{v}|_{\mathrm{cyclo}}\right) \mathfrak{B}_\nu^{(K-1)} \right).$$

Therefore, we have

$$\begin{aligned} \mathrm{vol}(\mathfrak{B}_\nu^{(K)}) &= \int_{\boldsymbol{v} \in \mathfrak{B}_\nu} \mathrm{vol}^{(K-1)} \left(\left(1 - |\boldsymbol{v}|_{\mathrm{cyclo}}\right) \mathfrak{B}_\nu^{(K-1)} \right) d\mathrm{vol}(\boldsymbol{v}) \\ &= \int_0^1 \mathrm{vol}^{(K-1)} \left((1-r)\, \mathfrak{B}_\nu^{(K-1)} \right) d\mathrm{vol}(r\mathfrak{B}_\nu), \end{aligned}$$

where the right hand side is the Stieltjes integral. Thus, we can calculate

$$\begin{aligned} \mathrm{vol}(\mathfrak{B}_\nu^{(K)}) &= \int_0^1 (1-r)^{(K-1)\nu} \mathrm{vol}^{(K-1)} \left(\mathfrak{B}_\nu^{(K-1)} \right) dr^\nu \mathrm{vol}(\mathfrak{B}_\nu) \\ &= \int_0^1 (1-r)^{(K-1)\nu} \, dr^\nu \cdot \mathrm{vol}(\mathfrak{B}_\nu) \cdot \mathrm{vol}^{(K-1)} \left(\mathfrak{B}_\nu^{(K-1)} \right). \end{aligned}$$

Hence we have

$$\mathrm{vol}(\mathfrak{B}_\nu^{(K)}) = \nu \int_0^1 (1-r)^{(K-1)\nu}\, r^{\nu-1} dr \cdot \mathrm{vol}(\mathfrak{B}_\nu) \cdot \mathrm{vol}^{(K-1)}\left(\mathfrak{B}_\nu^{(K-1)}\right). \quad (3.5.2)$$

As

$$\begin{aligned}\int_0^1 (1-r)^a r^b dr &= \left[-\frac{1}{a+1}(1-r)^{a+1} r^b\right]_{r=0}^{r=1} + \int_0^1 \frac{1}{a+1}(1-r)^{a+1} \cdot b r^{b-1} dr \\ &= \frac{b}{a+1}\int_0^1 (1-r)^{a+1} r^{b-1} dr,\end{aligned}$$

we have

$$\begin{aligned}&\int_0^1 (1-r)^{(K-1)\nu}\, r^{\nu-1} dr \\ =\ & \frac{\nu-1}{(K-1)\nu+1} \cdot \frac{\nu-2}{(K-1)\nu+2} \cdots \frac{\nu-(\nu-1)}{(K-1)\nu+(\nu-1)} \int_0^1 (1-r)^{(K-1)\nu+(\nu-1)}\, dr \\ =\ & \frac{\nu-1}{(K-1)\nu+1} \cdot \frac{\nu-2}{(K-1)\nu+2} \cdots \frac{\nu-(\nu-1)}{(K-1)\nu+(\nu-1)} \cdot \frac{1}{(K-1)\nu+\nu} \\ =\ & \frac{(\nu-1)!(K\nu-\nu)!}{(K\nu)!}\end{aligned}$$

Substituting this in (3.5.2), we deduce the recursion:

$$\mathrm{vol}(\mathfrak{B}_\nu^{(K)}) = \frac{\nu!(K\nu-\nu)!}{(K\nu)!} \cdot \mathrm{vol}(\mathfrak{B}_\nu) \cdot \mathrm{vol}^{(K-1)}\left(\mathfrak{B}_\nu^{(K-1)}\right).$$

This implies

$$\mathrm{vol}(\mathfrak{B}_\nu^{(K)}) = \frac{\nu!^K}{(K\nu)!}\, \mathrm{vol}(\mathfrak{B}_\nu)^K.$$

By substituting (3.5.1) in the right hand side, we arrive at

$$\mathrm{vol}(\mathfrak{B}_\nu^{(K)}) = \frac{\nu!^K}{(K\nu)!}\, \mathrm{vol}(\mathfrak{B}_\nu)^K = \begin{cases} \dfrac{\nu!^K}{(K\nu)!}\, \dfrac{2^K}{(m!)^{2K}} & \text{if} \quad \nu = 2m+1; \\ \dfrac{\nu!^K}{(K\nu)!}\, \dfrac{(2m+1)^K}{(m!)^{2K}} & \text{if} \quad \nu = 2m. \end{cases}$$

Then we have the following:

Lemma 3.6. *Let $2 \leq \nu \in \mathbb{Z}$ and $1 \leq K \in \mathbb{Z}$. We have*

$$\mathrm{vol}(\mathfrak{B}_{\nu}^{(K)}) = \begin{cases} \dfrac{\nu!^K}{(K\nu)!}\dfrac{2^K}{(m!)^{2K}} & \text{if} \quad \nu = 2m+1; \\ \dfrac{\nu!^K}{(K\nu)!}\dfrac{(2m+1)^K}{(m!)^{2K}} & \text{if} \quad \nu = 2m. \end{cases}$$

We can make this up in the following formula which looks simpler on the surface.

$$\mathrm{vol}(\mathfrak{B}_{\nu}^{(K)}) = \frac{2^{K(\nu-2m)}}{(K\nu)!}\frac{(2m+1)!^K}{(m!)^{2K}} = \frac{2^{K\nu}}{(K\nu)!}B_m^K,$$

where we put $m = \lfloor \nu/2 \rfloor$ and B_m is defined by (3.4.2).

3.6 Volume of $\mathfrak{B}$

In the case $\nu = p-1$ and $K = q$, we have $\mathfrak{B}_{p-1}^{(q)} = \mathfrak{B}$. From Lemma 3.6, we get the following:

Lemma 3.7. *We have*

$$\mathrm{vol}(\mathfrak{B}) = \frac{(p-1)!^q}{(q(p-1))!}\frac{p^q}{((p-1)/2)!^{2q}}.$$

Chapter 4

Smaller Bound for Odd Prime Numbers

Let p be an odd prime number. In the previous chapter, we have focused on the new convex body $\mathfrak{B}$ and calculated the volume of it. In this chapter, based on the results in chapter 3, we obtain further improvement of Theorem 2.1:

Theorem 4.1. *Let p, ℓ, n, s, r, $q(m)$ and $c(m)$ and f be the same as in Theorem 2.1. We put*

$$G_{cyclo}(p,r,f) = \left(\sqrt{6}^{c(r)}\left(\frac{p^{p-2}((p-1)/2)!^2}{(p-1)!}\right)^{q(r)} c(r)!\right)^{1/f}.$$

If ℓ satisfies $\ell > G_{cyclo}(p,r,f)$, then ℓ does not divide $h_{p,n}$ for any positive integer n.

4.1 Minkowski Convex Body Theorem for Theorem 4.1

Let ℓ be a prime number different from p, n a positive integer and p^s the exact power of p dividing $\ell^{p-1}-1$. We put $r = \min\{n, s\}$, $q = p^{r-1}$, $c = (p-1)q$ and $\omega = \zeta_1$. Recall the mapping μ in section 2.2 (2.2.1):

$$\mu : \mathbb{Q}(\zeta_r) \longrightarrow \mathbb{C}^c; \quad \alpha \longmapsto \overrightarrow{\alpha} := (\alpha^\rho)_{\rho \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})}$$

and the $\mathbb{R}$-vector space:

$$W = \mathbb{R}\overrightarrow{1} + \mathbb{R}\overrightarrow{\zeta_r} + \cdots + \mathbb{R}\overrightarrow{\zeta_r^{c-1}}.$$

We put

$$W_i = \mathbb{R}\overrightarrow{\zeta_r^i} + \mathbb{R}\overrightarrow{\zeta_r^i\omega} + \cdots + \mathbb{R}\overrightarrow{\zeta_r^i\omega^{p-2}}.$$

Then we have

$$W \cong \mathbb{R}^c; \quad \sum_{j=0}^{c-1} a_j \overrightarrow{\zeta_r^j} \longmapsto (a_0, a_1, \ldots, a_{c-1}), \tag{4.1.1}$$

$$W_i \cong \mathbb{R}^{p-1}; \quad \sum_{j=0}^{p-2} a_{i+qj}\overrightarrow{\zeta_r^i\omega^j} \longmapsto (a_i, a_{i+q}, \ldots, a_{i+q(p-2)})$$

and

$$W = W_0 + W_1 + \cdots W_{q-1}.$$

By the isomorphism above, we identify W with $\mathbb{R}^c$ and W_i with $\mathbb{R}^{p-1}$. Then $\overrightarrow{\zeta^i\omega^{p-1}}$ is $(-1, \ldots, -1)$ in W_i. We define $|\bullet|_{\mathrm{cyclo}}$ on W which is the same as in 3.1 for $\nu = p-1$ and $K = q$. Let

$$\mathfrak{B} = \left\{ \sum_{i=0}^{pq-1} s_i t_i \overrightarrow{\zeta^i} \;\middle|\; s_i \in \{+1, -1\}, 0 \leq t_i \leq 1, (i = 0, 1, \ldots, pq-1), \sum_{i=0}^{pq-1} t_i \leq 1 \right\}$$

and

$$X_{cyclo} = \frac{2\ell}{\sqrt{6}p}\mathfrak{B}.$$

From Lemma 3.7 and Minkowski convex body theorem with respect to the volume on W induced by the standard volume on $\mathbb{R}^c$ by (4.1.1), we have:

Lemma 4.2. *Let ℓ, n, s, r, q, c and X_{cyclo} be as above and $\mathfrak{L}$ a prime ideal of $\mathbb{Q}(\zeta_r)$ dividing ℓ. We denote by f the inertia degree of $\mathfrak{L}$ in $\mathbb{Q}(\zeta_r)/\mathbb{Q}$. If ℓ satisfies*

$$\ell^f > \sqrt{6}^c \left(\frac{p^{p-2}((p-1)/2)!^2}{(p-1)!} \right)^q c!,$$

then there exists a non-zero element $\overrightarrow{\alpha}$ in $X_{cyclo} \cap \mu(\ell\mathfrak{L}^{-1})$. Then α lies in $\ell\mathfrak{L}^{-1}$ and satisfies $|\mu(\alpha)|_{cyclo} \leq 2\ell/\sqrt{6}p$.

4.2 Proof of Theorem 4.1

Let ℓ be a prime number different form p, p^s the exact power of p dividing $\ell^{p-1}-1$ and n a positive integer. We put $N=p^n$, $r=\min\{n,s\}$, $q=p^{r-1}$, $c=(p-1)q$ and $\omega=\zeta_1$. We denote by f the inertia degree of ℓ in $\mathbb{Q}(\zeta_r)/\mathbb{Q}$. Assume that ℓ satisfies

$$\ell^f > \sqrt{6}^c \left(\frac{p^{p-2}((p-1)/2)!^2}{(p-1)!}\right)^q c!.$$

We also assume that ℓ divides $h_{p,n}/h_{p,n-1}$. By Lemma 1.7 and Lemma 4.2, there exist a prime ideal $\mathfrak{L}$ in $\mathbb{Q}(\zeta_r)$ lying above ℓ, an element α in $\ell\mathfrak{L}^{-1}$ and a unit ϵ in $E_{p,n}$ such that

$$\eta_{p,n}^{\alpha_\sigma} = \epsilon^\ell \tag{4.2.1}$$

and

$$|\mu(\alpha)|_{\mathrm{cyclo}} < \frac{2\ell}{\sqrt{6}p}. \tag{4.2.2}$$

By Theorem 1.9, we have

$$M(\epsilon) \geq \left(\frac{1+\sqrt{5}}{2}\right)^{N/2} > \exp(0.240605912\cdot N). \tag{4.2.3}$$

Since $\deg \epsilon^\ell = \deg \epsilon$, $\deg \eta_{p,n}^{\alpha_\sigma} \leq \deg \eta_{p,n}$ and $1+\omega+\cdots\omega^{p-1}=0$, we have

$$M(\epsilon^\ell) = M(\epsilon)^\ell \tag{4.2.4}$$

and

$$M(\eta_{p,n}^{\alpha_\sigma}) \leq M(\eta_{p,n})^{|\mu(\alpha)|\mathrm{cyclo}}. \tag{4.2.5}$$

By (4.2.1) — (4.2.5) and Lemma 2.4, we have

$$\begin{aligned}
\exp(0.240605912\cdot N\ell) &\leq M(\epsilon)^\ell = M(\epsilon^\ell) = M(\eta_{p,n}^{\alpha_\sigma}) \\
&\leq M(\eta_{p,n})^{|\mu(\alpha)|_{cyclo}} \\
&< \exp\left(0.291560904\cdot pN\cdot\frac{2\ell}{\sqrt{6}p}\right).
\end{aligned}$$

Hence we have

$$0.240605912 < 0.291560904 \cdot \frac{2}{\sqrt{6}} = 0.238058481 \cdots .$$

This is a contradiction.

Chapter 5

Inequality for $p = 3$

From this chapter, we consider the case $p = 3$. We put $\mathbb{B}_n = \mathbb{B}_{3,n}$, $h_n = h_{3,n}$, $\eta_n = \eta_{3,n}$, $\zeta = \zeta_{n+1}$ and $\omega = \zeta_1$ for the ease of notation. Then we have

$$\mathbb{B}_n = \mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}\left(2\cos\frac{2\pi\sqrt{-1}}{3^{n+1}}\right).$$

In this chapter, we shall calculate an upper bound of the Mahler measure of Horie unit more precisely than Lemma 2.4. And we shall also give a better lower bound of Mahler measure of relative units of $\mathbb{B}_n/\mathbb{B}_{n-1}$ by using Hilbert's theorem 90. From these results, we can get a smaller bound for a prime number ℓ in Theorem 2.1 and Theorem 4.1:

Theorem 5.1. *Let $\ell \geq 5$ be a prime number, n a positive integer and 3^s the exact power of 3 dividing $\ell^2 - 1$. We put $r = \min\{n, s\}$ and $c = 2 \cdot 3^{r-1}$. We denote by f the inertia degree of ℓ in $\mathbb{Q}(\zeta_r)/\mathbb{Q}$. If ℓ satisfies $\ell^f > 2^{c/2} \cdot c!$, then ℓ does not divide h_n/h_{n-1}.*

By using this theorem, we get Theorem 8.2 and Theorem 8.4 in Chapter 8. They can not be proven by using Theorem 0.1.

5.1 Lower Bound of Mahler Measure of Relative Units for $p = 3$

Let $\mathfrak{P}$ be a prime ideal in $\mathbb{Q}(\zeta)$ dividing 3 and $\mathrm{ord}_{\mathfrak{P}}(x)$ the normalized additive $\mathfrak{P}$-adic valuation of x. Moreover, we let $\mathfrak{p}$ be a prime ideal in $\mathbb{B}_n$ dividing 3 and $\mathrm{ord}_{\mathfrak{p}}(x)$ the normalized additive $\mathfrak{p}$-adic valuation of x. Then we have $\mathrm{ord}_{\mathfrak{p}}(x) = 2 \cdot \mathrm{ord}_{\mathfrak{P}}(x)$ for all x in $\mathbb{B}_n$. We denote by τ a generator of $\mathrm{Gal}(\mathbb{B}_n/\mathbb{B}_{n-1})$ which satisfies $\zeta^\tau = \zeta^{3^n+1}$. From Lemma 1.11, we have the following:

Lemma 5.2. *Let ϵ be a unit in $\mathbb{B}_n$. If $\mathrm{Nr}_{\mathbb{B}_n/\mathbb{B}_{n-1}}(\epsilon) = 1$, then we have*

$$\mathrm{ord}_{\mathfrak{p}}(\epsilon - 1) \geq \frac{3^n - 1}{2}.$$

Remark 5.3. We put $\omega = \zeta^{3^n}$ and recall the n-th Horie unit

$$\eta_n = \frac{\zeta - \zeta^{-1}}{\omega\zeta - \omega^{-1}\zeta^{-1}}.$$

We have $\mathrm{Nr}_{\mathbb{B}_n/\mathbb{B}_{n-1}}(\eta_n) = 1$ and

$$\begin{aligned}
\eta_n^{-1} - 1 &= \frac{\omega\zeta - \omega^{-1}\zeta^{-1} - \zeta + \zeta^{-1}}{\zeta - \zeta^{-1}} \\
&= \frac{\omega\zeta^2 - \omega^2 - \zeta^2 + 1}{\zeta^2 - 1} \\
&= \frac{(\omega - 1)\zeta^2 - (\omega - 1)(\omega + 1)}{\zeta^2 - 1} \\
&= \frac{\omega - 1}{\zeta^2 - 1}(\zeta^2 + \omega^2).
\end{aligned}$$

Since $(\zeta^2 - 1) = \mathfrak{P}$, $(\omega - 1) = \mathfrak{P}^{3^n}$ and $\zeta^2 + \omega^2$ is a unit in $\mathbb{Q}(\zeta)$, we have $(\eta_n - 1) = \mathfrak{P}^{3^n-1}$ in $\mathbb{Q}(\zeta)$. Hence we have $(\eta_n - 1) = \mathfrak{p}^{(3^n-1)/2}$, that is, the inequality in Lemma 5.2 is best possible.

On the other hand, we have

$$\begin{aligned}\eta_n^{-1}+1 &= \frac{\omega\zeta-\omega^{-1}\zeta^{-1}+\zeta-\zeta^{-1}}{\zeta-\zeta^{-1}}\\ &= \frac{\omega\zeta^2-\omega^2+\zeta^2-1}{\zeta^2-1}\\ &= \frac{(\omega+1)\zeta^2-(\omega^2+1)}{\zeta^2-1}\\ &= \frac{-\omega^2\zeta^2+\omega}{\zeta^2-1}\\ &= -\omega\frac{\omega\zeta^2-1}{\zeta^2-1}.\end{aligned}$$

Hence we have $\eta_n^{-1}+1$ is a unit, that is, η_n+1 is a unit.

Note that the absolute norm of $\mathfrak{p}$ is equal to 3. From Theorem 1.9 and Lemma 5.2, we conclude the following:

Lemma 5.4. *Let ϵ be a unit in $\mathbb{B}_n$ with $\mathrm{Nr}_{\mathbb{B}_n/\mathbb{B}_{n-1}}\epsilon = 1$ and put $N = 3^n$. Then we have*

$$M(\epsilon) \geq \left(\frac{3^{(N-1)/2N}+\sqrt{3^{(N-1)/N}+4}}{2}\right)^{N/2}.$$

In particular, if $n \geq 4$, then we have

$$M(\epsilon) \geq \left(\frac{3^{40/81}+\sqrt{3^{80/81}+4}}{2}\right)^{N/2}.$$

5.2 Upper Bound of Mahler Measure of Horie Unit for $p = 3$

We put $N = 3^n$ and $\Theta = \pi/6N$. Note the n-th Horie unit can be written in terms of real trigonometric function as follows:

$$\eta_n = \frac{\zeta-\zeta^{-1}}{\omega\zeta-\omega^{-1}\zeta^{-1}} = \frac{\sin(4\Theta)}{\sin(4(1+N)\Theta)}.$$

Let σ be a generator of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{n+1})/\mathbb{Q}(\zeta_1))$ with $\zeta_{n+1}^{\sigma} = \zeta_{n+1}^4$. We have

$$\begin{aligned}
M(\eta_n) &= \prod_{i=0}^{N-1} \max\{1, |\eta_n^{\sigma^i}|\} \\
&= \prod_{\substack{0 \le j < 3N \\ j \equiv 1 \pmod 3}} \max\left\{1, \left|\frac{\sin(4j\Theta)}{\sin(4(j+N)\Theta)}\right|\right\} \\
&= \prod_{\substack{0 \le j < 3N \\ j \equiv 1 \pmod 3}} \max\left\{1, \left|\frac{\sin(4((2N-j)+N)\Theta)}{\sin(4(2N-j)\Theta)}\right|\right\} \\
&= \prod_{\substack{0 \le j < 3N \\ j \equiv -1 \pmod 3}} \max\left\{1, \left|\frac{\sin(4(j+N)\Theta)}{\sin(4j\Theta)}\right|\right\}.
\end{aligned}$$

Since $M(\eta_n) = M(\eta_n^{-1})$, we have

$$\begin{aligned}
M(\eta_n) &= M(\eta_n^{-1}) \\
&= \prod_{i=0}^{N-1} \max\{1, |(\eta_n^{-1})^{\sigma^i}|\} \\
&= \prod_{\substack{0 \le j < 3N \\ j \equiv 1 \pmod 3}} \max\left\{1, \left|\frac{\sin(4(j+N)\Theta)}{\sin(4j\Theta)}\right|\right\}.
\end{aligned}$$

Hence we have

$$\begin{aligned}
M(\eta_n)^2 &= \prod_{0 \le j < 3N}^{*} \max\left\{1, \left|\frac{\sin(4(j+N)\Theta)}{\sin(4j\Theta)}\right|\right\} \\
&= \prod_{0 \le j < N}^{*} \prod_{0 \le i < 3} \max\left\{1, \left|\frac{\sin(4(j+(i+1)N)\Theta)}{\sin(4(j+iN)\Theta)}\right|\right\},
\end{aligned}$$

where $\overset{*}{\prod}$ denotes the product over indices coprime with 3. Write $\{|\sin(4(j+iN)\Theta) \mid i=0,1,2\} = \{s_0, s_1, s_2\}$ with $s_0 < s_1, s_2$. Then,

$$\begin{aligned}
& \prod_{0 \le i < 3} \max\left\{1, \left|\frac{\sin(4(j+(i+1)N)\Theta)}{\sin(4(j+iN)\Theta)}\right|\right\} \\
= & \begin{cases} \dfrac{s_2}{s_0} & \text{if} \quad s_1 < s_2 \\ \dfrac{s_1}{s_0} & \text{if} \quad s_1 > s_2 \end{cases} \\
= & \frac{\max\{s_0, s_1, s_2\}}{\min\{s_0, s_1, s_2\}}.
\end{aligned}$$

The maximum in the right hand side can be found by considering the inequality

$$|\sin(4j\Theta + 4Ni\Theta)| \ge |\sin(4j\Theta + 4N(i+1)\Theta)|, |\sin(4j\Theta + 4N(i-1)\Theta)|.$$

Hence, the maximum is obtained at i with

$$4j\Theta + 4Ni\Theta \in \left(\frac{\pi}{3}, \frac{2\pi}{3}\right) \cup \left(\frac{4\pi}{3}, \frac{5\pi}{3}\right)$$

or equivalently

$$j + iN \in \left(\frac{N}{2}, N\right) \cup \left(2N, \frac{5N}{2}\right).$$

Similarly, the minimum is obtained at i with

$$4j\Theta + 4Ni\Theta \in \left(-\frac{\pi}{6}, \frac{\pi}{6}\right) \cup \left(\frac{5\pi}{6}, \frac{7\pi}{6}\right)$$

or equivalently

$$j + iN \in \left(-\frac{N}{4}, \frac{N}{4}\right) \cup \left(\frac{5N}{4}, \frac{7N}{4}\right).$$

Therefore, we have

$$M(\eta_n)^2 = \frac{\overset{*}{\prod\limits_{N/2<j<N}} |\sin(4j\Theta)| \cdot \overset{*}{\prod\limits_{2N<j<5N/2}} |\sin(4j\Theta)|}{\overset{*}{\prod\limits_{-N/4<j<N/4}} |\sin(4j\Theta)| \cdot \overset{*}{\prod\limits_{5N/4<j<7N/4}} |\sin(4j\Theta)|}.$$

Thus, we get

$$
\begin{aligned}
M(\eta_n) &= \frac{\overset{*}{\prod\limits_{N/2<j<N}} \sin(4j\Theta)}{\overset{*}{\prod\limits_{0<j<N/4}} \sin(4j\Theta) \cdot \overset{*}{\prod\limits_{5N/4<j<3N/2}} \sin(4j\Theta)} \\
&= \frac{\overset{*}{\prod\limits_{N/2<j<N}} \cos((4j-3N)\Theta)}{\overset{*}{\prod\limits_{0<j<N/4}} \sin(4j\Theta) \cdot \overset{*}{\prod\limits_{5N/4<j<3N/2}} \sin((6N-4j)\Theta)} \\
&= \frac{\overset{*}{\prod\limits_{-N<4j-3N<N}} \cos((4j-3N)\Theta)}{\overset{*}{\prod\limits_{0<j<N/4}} \sin(4j\Theta) \cdot \overset{*}{\prod\limits_{0<3N-2j<N/2}} \sin((6N-4j)\Theta)} \\
&= \frac{\overset{*}{\prod\limits_{0<3N-4j<N}} \cos((3N-4j)\Theta) \cdot \overset{*}{\prod\limits_{0<4j-3N<N}} \cos((4j-3N)\Theta)}{\overset{*}{\prod\limits_{0<4j<N}} \sin(4j\Theta) \cdot \overset{*}{\prod\limits_{0<6N-4j<N}} \sin((6N-4j)\Theta)}.
\end{aligned}
$$

Noting that the ranges of the products are

$$
\left\{k \in \mathbb{Z} \;\middle|\; k \equiv +3N \pmod 4, k \not\equiv 0 \pmod 3\right\} \cap \left(0, \frac{\pi}{3}\right),
$$

$$
\left\{k \in \mathbb{Z} \;\middle|\; k \equiv -3N \pmod 4, k \not\equiv 0 \pmod 3\right\} \cap \left(0, \frac{\pi}{3}\right),
$$

$$
\left\{k \in \mathbb{Z} \;\middle|\; k \equiv 0 \pmod 4, k \not\equiv 0 \pmod 3\right\} \cap \left(0, \frac{\pi}{3}\right),
$$

$$
\left\{k \in \mathbb{Z} \;\middle|\; k \equiv 2 \pmod 4, k \not\equiv 0 \pmod 3\right\} \cap \left(0, \frac{\pi}{3}\right),
$$

we get

$$M(\eta_n) = \frac{\overset{*}{\prod_{0<k<N,\ 2\nmid k}} \cos(k\Theta)}{\overset{*}{\prod_{0<k<N,\ 2|k}} \sin(k\Theta)}.$$

Then we have

$$M(\eta_n) = \frac{\cos((N-2)\Theta)}{\sin((N-1)\Theta)} \cdot \prod_{0<3K<N,\ 2\nmid K} \frac{\cos((3K-2)\Theta)\cdot\cos((3K+2)\Theta)}{\sin((3K-1)\Theta)\cdot\sin((3K+1)\Theta)}. \tag{5.2.1}$$

For $(t,v) \in \mathbb{R}^2$ such that $0 < t-v \le t \le t+v < \pi/4$, we have

$$\frac{\partial}{\partial v} \log \frac{\cos(t-v)}{\sin(t+v)} = \tan(t-v) - \cot(t+v) < 0.$$

Thus we have

$$\cot \frac{(2N-3)\Theta}{2} > \frac{\cos((N-2)\Theta)}{\sin((N-1)\Theta)}.$$

For $(t,u,v) \in \mathbb{R}^3$ such that $0 < t-u-v \le t-u+v \le t \le t+u-v \le t+u+v < \pi/4$, put

$$g(t,u,v) = \log \frac{\cos(t-u-v)\cos(t+u+v)}{\sin(t-u+v)\sin(t+u-v)}.$$

Then we have

$$\frac{\partial}{\partial v} g(t,u,v) = \tan(t-u-v) - \tan(t+u+v) - \cot(t-u+v) + \cot(t+u-v).$$

Since

$$\tan(t-u-v) \le \tan t \le \tan(t+u+v), \quad \cot(t-u+v) \ge \cot t \ge \cot(t+u-v),$$

this implies

$$\frac{\partial}{\partial v} g(t,u,v) \le 0.$$

Hence we see

$$g(t,u,v) \le g(t,u,0).$$

Therefore, the factor in the product of (5.2.1) is estimated by the following:

$$\frac{\cos((3K-2)\Theta)\cdot\cos((3K+2)\Theta)}{\sin((3K-1)\Theta)\cdot\sin((3K+1)\Theta)} \le \cot\frac{(6K-3)\Theta}{2}\cdot\cot\frac{(6K+3)\Theta}{2}.$$

Summing up, we get

$$\begin{aligned} M(\eta_n) &\le \cot\frac{(2N-3)\Theta}{2}\cdot\prod_{0<3K<N,\ 2\nmid K}\left(\cot\frac{(6K-3)\Theta}{2}\cdot\cot\frac{(6K+3)\Theta}{2}\right) \\ &= \prod_{0<J<2N/3,\ 2\nmid J}\cot\frac{J\pi}{4N}. \end{aligned}$$

Since

$$\frac{d^2}{dt^2}\log\cot t = -\frac{d}{dt}\frac{1}{\sin t\cos t} = -\frac{d}{dt}\frac{2}{\sin 2t} = \frac{4\cos t}{(\sin 2t)^2} > 0$$

holds for $0 < t < \pi/4$, we have

$$\sum_{0<J<2N/3,\ 2\nmid J}\log\cot\frac{J\pi}{4N} \le \frac{2N}{\pi}\int_0^{\pi/6}\log\cot t\ dt.$$

Recall the Lobachevsky function ([9], [22])

$$-\int_0^\theta \log\cos t\ dt = \theta\log 2 + \sum_{m=1}^{\infty}\frac{(-1)^m}{2m^2}\sin 2m\theta$$

and its companion function

$$-\int_0^\theta \log\sin t\ dt = \theta\log 2 + \sum_{m=1}^{\infty}\frac{1}{2m^2}\sin 2m\theta$$

for $0 \le \theta < \pi/2$. Subtracting the both sides, we get

$$\int_0^\theta \log\cot t\ dt = \sum_{m=0}^{\infty}\frac{1}{(2m+1)^2}\sin(2(2m+1)\theta).$$

Substituting $\theta = \pi/6$, we get

$$\begin{aligned}\int_0^{\pi/6} \log\cot t \; dt &= \sum_{m=0}^{\infty} \frac{1}{(2m+1)^2} \sin\frac{(2m+1)\pi}{3} \\ &= \frac{\sqrt{3}}{2}\left(1 - \sum_{m=1}^{\infty}\left(\frac{1}{(6m-1)^2} - \frac{1}{(6m+1)^2}\right)\right).\end{aligned}$$

Since

$$\frac{1}{(6m-1)^2} - \frac{1}{(6m+1)^2} > 0,$$

we obtain

$$\begin{aligned}&\frac{\sqrt{3}}{2}\left(1 - \sum_{m=1}^{\infty}\left(\frac{1}{(6m-1)^2} - \frac{1}{(6m+1)^2}\right)\right) \\ <\ &\frac{\sqrt{3}}{2}\left(1 - \sum_{m=1}^{1000}\left(\frac{1}{(6m-1)^2} - \frac{1}{(6m+1)^2}\right)\right) \\ <\ &0.845785\end{aligned}$$

and

$$\frac{2}{\pi} \times 0.845785 < 0.53845.$$

Now we conclude the following:

Lemma 5.5. *Let $N = 3^n$, then we have*

$$M(\eta_n) \leq \exp(0.53845 \cdot N).$$

5.3 Minkowski Convex Body Theorem for $p = 3$

Let $\ell \geq 5$ be a prime number, n a positive integer and 3^s the exact power of 3 dividing $\ell^2 - 1$. We put $r = \min\{n, s\}$ and $c = 2 \cdot 3^{r-1}$. In this section, we consider the mapping:

$$\mu : \mathbb{Q}(\zeta_r) \longrightarrow \mathbb{C}^c, \quad \alpha \longmapsto \overrightarrow{\alpha} := (\alpha^\rho)_{\rho \in \mathrm{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q})}$$

and the $\mathbb{R}$-vector space:

$$V = \mathbb{R}\overrightarrow{1} + \mathbb{R}\overrightarrow{\zeta_r} + \cdots + \mathbb{R}\overrightarrow{\zeta_r^{c-1}} \cong \mathbb{R}^c. \tag{5.3.1}$$

We put

$$X = \left\{ \sum_{i=0}^{c-1} a_i \overrightarrow{\zeta_r^i} \in V \;\middle|\; |a_0| + |a_1| + \cdots |a_{c-1}| \leq \frac{\ell}{\sqrt{2}} \right\}$$

and define $|\cdot|_1$ on $\mathbb{Z}[\zeta_r]$ such that

$$|a_0 + a_1\zeta_r + \cdots + a_{c-1}\zeta_r^{c-1}|_1 = |a_0| + |a_1| + \cdots + |a_{c-1}|.$$

We consider the volume $\mathrm{vol}(\cdot)$ on V induced by the standard volume on $\mathbb{R}^c$ by (5.3.1). For an ideal $\mathfrak{a}$ of $\mathbb{Q}(\zeta_r)$, we also denote by $\mathrm{vol}(\mathfrak{a})$ the volume of the fundamental domain of the lattice $\mu(\mathfrak{a})$. Then we have

$$\mathrm{vol}(X) = \frac{\left(\sqrt{2}\ell\right)^c}{c!}$$

and

$$\mathrm{vol}(\ell\mathfrak{L}^{-1}) = \ell^{c-f}$$

where $\mathfrak{L}$ is a prime ideal of $\mathbb{Q}(\zeta_r)$ dividing ℓ and f is the inertia degree of $\mathfrak{L}$ in $\mathbb{Q}(\zeta_r)/\mathbb{Q}$. Now we apply Minkowski convex body theorem to see:

Lemma 5.6. *Let ℓ, n, s, r, c and X be as above and $\mathfrak{L}$ a prime ideal of $\mathbb{Q}(\zeta_r)$ dividing ℓ. We denote by f the inertia degree of $\mathfrak{L}$ in $\mathbb{Q}(\zeta_r)/\mathbb{Q}$. If ℓ satisfies $\ell^f > 2^{c/2} \cdot c!$, then there exists a non-zero element α in $X \cap \mu(\ell\mathfrak{L}^{-1})$. Therefore, if ℓ satisfies $\ell^f > 2^{c/2} \cdot c!$, then there exists a non-zero element α in $\ell\mathfrak{L}^{-1}$ such that $|\alpha|_1 \leq \ell/\sqrt{2}$.*

Proof. Since $\ell^f > 2^{c/2} \cdot c!$, we have

$$\mathrm{vol}(X) > 2^c \mathrm{vol}(\ell\mathfrak{L}^{-1}).$$

□

5.4 Proof of Theorem 5.1

Let $\ell \geq 5$ be a prime number, 3^s the exact power of 3 dividing $\ell^2 - 1$ and n a positive integer. Since $h_0 = h_1 = h_2 = h_3 = 1$, we may assume $n \geq 4$. We put $N = 3^n$, $r = \min\{n, s\}$ and $c = 2 \cdot 3^{r-1}$. We denote by f the inertia degree of ℓ in $\mathbb{Q}(\zeta_r)/\mathbb{Q}$. Assume that ℓ satisfies $\ell^f > 2^{c/2} \cdot c!$. We also assume that ℓ divides h_n/h_{n-1}. By Lemma 1.7 and Lemma 5.6, there exist an element α in $\ell\mathfrak{L}^{-1}$ and a unit ϵ in $\mathbb{B}_n$ such that

$$\eta_n^{\alpha_\sigma} = \epsilon^\ell \tag{5.4.1}$$

and

$$|\alpha|_1 < \frac{\ell}{\sqrt{2}}, \tag{5.4.2}$$

where $\mathfrak{L}$ is a prime ideal in $\mathbb{Q}(\zeta_r)$ dividing ℓ. Since $\mathrm{Nr}_{\mathbb{B}_n/\mathbb{B}_{n-1}}(\eta_n) = 1$, we have $\mathrm{Nr}_{\mathbb{B}_n/\mathbb{B}_{n-1}}(\epsilon) = 1$. By Lemma 5.4,

$$M(\epsilon) \geq \left(\frac{3^{40/81} + \sqrt{3^{80/81} + 4}}{2} \right)^{N/2}. \tag{5.4.3}$$

By taking the logarithm, we have

$$\begin{aligned} \log \left(\frac{3^{40/81} + \sqrt{3^{80/81} + 4}}{2} \right) &> \log \left(\frac{\sqrt{3} + \sqrt{7}}{2} \right) - \frac{1}{162} \log 3 \\ &> 0.77661. \end{aligned}$$

Hence we obtain

$$M(\epsilon) > \exp(0.77661 \cdot N/2) \tag{5.4.4}$$

Since $\deg \epsilon^\ell = \deg \epsilon$ and $\deg \eta_n^{\alpha_\sigma} \leq \deg \eta_n$, we have

$$M(\epsilon^\ell) = M(\epsilon)^\ell \tag{5.4.5}$$

and

$$M(\eta_n^{\alpha_\sigma}) \leq M(\eta_n)^{|\alpha|_1}. \tag{5.4.6}$$

By (5.4.1), (5.4.2), (5.4.3), (5.4.4), (5.4.5), (5.4.6) and Lemma 5.5, we obtain

$$\begin{aligned} \exp(0.77661 \cdot \ell \cdot N/2) &< M(\epsilon^{\ell}) = M(\eta_n^{\alpha_\sigma}) \\ &\leq M(\eta_n)^{|\alpha|_1} \\ &\leq \exp(0.53845 \cdot N \cdot \ell/\sqrt{2}). \end{aligned}$$

Hence we must have

$$0.77661 \leq 0.53845 \cdot \sqrt{2} = 0.761483\ldots.$$

This is a contradiction.

Chapter 6

Explicit Bound of ℓ-indivisibility for $p = 3$

In this chapter, we shall give three explicit bounds of the growth of the ℓ-part of class numbers in the cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}$. The third bound is the smallest. However, we use different methods to prove them. Hence we shall write and prove all of them.

We denote by $\lfloor x \rfloor$ the greatest integer not exceeding a real number x. We show the following:

Theorem 6.1 (First Bound)**.** *Let $\ell \geqq 5$ be a prime number and 3^s the exact power of 3 dividing $\ell^2 - 1$. Put*

$$m_{\ell,1} = 3s + 2 + \lfloor \log_3(\ell - 1) \rfloor + \left\lfloor \log_3 \frac{\ell - 1}{2} \right\rfloor + \lfloor \log_3(2s + 1 + \lfloor \log_3(\ell - 1) \rfloor) \rfloor.$$

If ℓ does not divide $h_{m_{\ell,1}}$, then ℓ does not divide h_n for any positive integer n.

Theorem 6.2 (Second Bound)**.** *Let $\ell \geq 5$ be a prime number and 3^s the exact power of 3 dividing $\ell^2 - 1$. Put*

$$m_{\ell,2} = 2s - 1 + \lfloor \log_3 \ell \rfloor.$$

If ℓ does not divide $h_{m_{\ell,2}}$, then ℓ does not divide h_n for any positive integer n.

Theorem 6.3 (Third Bound)**.** *Let $\ell \geq 5$ be a prime number and 3^s the exact power of 3 dividing $\ell^2 - 1$. Put*

$$m_{\ell,3} = 2s + \left\lfloor \frac{1}{2}\log_3(\ell - 1) + \frac{1}{2} \right\rfloor.$$

If ℓ does not divide $h_{m_{\ell,3}}$, then ℓ does not divide h_n for any positive integer n.

Remark 6.4. Friedman-Sands [5] made explicit bound of the stabilization on the ℓ-part of the minus part of class groups in the cyclotomic $\mathbb{Z}_3$-extension over imaginary abelian fields.

6.1 First Bound

Let n be a positive integer, ℓ a prime number with $\ell \geqq 5$, χ a character mod ℓ with $\chi(-1) = -1$ and ψ_n an even character mod 3^{n+1} whose order is 3^n. Then the generalized Bernoulli number is defined by

$$B_{1,\chi\psi_n} = \frac{1}{3^{n+1}\ell} \sum_{b=1}^{3^{n+1}\ell} b\chi\psi_n(b).$$

Let s be as in Theorem 6.1 and ζ_{ψ_n} such a primitive 3^{n+1}-th root of unity as

$$\zeta_{\psi_n}^{3^{n+1-s}} = \psi_n(1 + 3^{n+1-s}).$$

We define a rational function $f_{1,\chi}(T)$ in the rational function field $\mathbb{Q}_\ell(T)$ by

$$f_{1,\chi}(T) = \left(\sum_{\substack{b \equiv 1 \pmod{3^s} \\ 0 < b < 3^s\ell}} \chi(b)T^b \right) (T^{3^s\ell} - 1)^{-1}.$$

We put $d = s + 1 + \lfloor \log_3(\ell - 1) \rfloor$. We also put $\mathbb{B}'_n = \mathbb{B}_n(\mu_\ell)$. Let h'^-_n be the relative class number of $\mathbb{B}'_n$. Then we have the following result by [30] p.387:

Lemma 6.5. *Let χ, ψ_n be as above and $n \geqq 2s-1$. If $B_{1,\chi\psi_n} \equiv 0 \pmod{\overline{\ell}}$ in $\mathbb{Z}_\ell[\zeta_{\psi_n}]$, then $f_{1,\chi}(\zeta_{\psi_n}) \equiv 0 \pmod{\overline{\ell}}$ in $\mathbb{Z}_\ell[\zeta_{\psi_n}]$, where $\overline{\ell}$ is the ideal of $\mathbb{Z}_\ell[\zeta_{\psi_n}]$ generated by ℓ.*

Lemma 6.6. *If $d + s - 1 \leqq n$, then the prime number ℓ does not divide h'^-_n / h'^-_{d+s-1}.*

Proof. Assume that $d + s - 1 \leqq n$. We put

$$g(T) = \frac{(T^{3^s\ell} - 1) f_{1,\chi}(T)}{T}.$$

Since

$$g(T) = \sum_{\substack{b \equiv 1 \pmod{3^s} \\ 0 < b \leqq 1 + 3^s(\ell-1)}} \chi(b) T^{b-1},$$

we have $\deg g(T) \leqq 3^s(\ell - 1)$ where $\deg g(T)$ means the degree of the polynomial $g(T)$. Since

$$[\mathbb{Q}_\ell(\zeta) : \mathbb{Q}_\ell] \geqq 3^{n+1-s} \geqq 3^d > 3^s(\ell - 1) \geqq \deg g(T)$$

for a primitive 3^{n+1}-th root of unity $\zeta \in \overline{\mathbb{Q}_\ell}$, we have

$$g(\zeta) \not\equiv 0 \pmod{\overline{\ell}},$$

and hence

$$f_{1,\chi}(\zeta) \not\equiv 0 \pmod{\overline{\ell}}.$$

In particular, we obtain $f_{1,\chi}(\zeta_{\psi_n}) \not\equiv 0 \pmod{\overline{\ell}}$. From Lemma 6.5, we see $B_{1,\chi\psi_n} \not\equiv 0 \pmod{\overline{\ell}}$. Hence we obtain

$$\frac{h'^-_n}{h'^-_{d+s-1}} \not\equiv \ 0 \pmod{\overline{\ell}}$$

from the class number formula

$$h_n'^- = 2\ell Q_{n,\ell} \prod_{\chi} \prod_{b=1}^{3^n} \left(-\frac{1}{2} B_{1,\chi\psi_n^b} \right),$$

where $Q_{n,\ell} = 1$ or 2 and χ runs over all characters mod ℓ with $\chi(-1) = -1$. □

We denote the plus part and the minus part of the ideal class group of $\mathbb{B}_n'$ by $Cl^+(\mathbb{B}_n')$ and by $Cl^-(\mathbb{B}_n')$ respectively. We also denote the ℓ-rank of $Cl^+(\mathbb{B}_n')$ and $Cl^-(\mathbb{B}_n')$ by $r_n'^+$ and by $r_n'^-$ respectively. Then Theorem 10.11 in [30] implies

$$r_n'^+ \leqq r_n'^-.$$

Lemma 6.7. *Suppose $s+1 \leqq n$. If ℓ divides h_n and if ℓ does not divide h_{n-1}, then $3^{n-s-1} < r_n'^-$.*

Proof. Let r_n be the ℓ-rank of the ideal class group of $\mathbb{B}_n$. By Theorem 10.8 in [30], we have $r_n \geqq 3^{n-s}$ if $\ell \equiv 1 \pmod 3$ and $r_n \geqq 2 \cdot 3^{n-s}$ if $\ell \equiv 2 \pmod 3$. Since $r_n \leqq r_n'^+$, we have $3^{n-s-1} < r_n'^-$. □

Now we prove Theorem 6.1.

Since $|B_{1,\chi\psi_n^b}| \leqq 3^{n+1}\ell$, we have

$$\begin{aligned} h_n'^- &\leqq 2 \cdot 2 \cdot \ell \left(\frac{1}{2} 3^{n+1} \ell \right)^{\frac{\ell-1}{2} 3^n} \\ &< \ell^{3^n (n+1) \frac{\ell-1}{2} + 2}. \end{aligned}$$

Hence we obtain

$$r_n'^- < 3^n (n+1) \frac{\ell - 1}{2} + 2,$$

and then

$$r_n'^- < 3^{d+s-1} (d+s) \frac{\ell - 1}{2} + 2 \tag{6.1.1}$$

by Lemma 6.6.

Let $m_{\ell,1}$ be as in Theorem 6.1 and assume that ℓ does not divide $h_{m_{\ell,1}}$. We also assume that there exists a positive integer n such that ℓ divides h_n but does not divide h_{n-1}. Then we have $m_\ell < n$. By Lemma 6.7 and (6.1.1), we obtain

$$3^{n-s-1} \leqq 3^{d+s-1}(d+s)\frac{\ell-1}{2}.$$

Hence we have

$$n - s - 1 \leqq d + s - 1 + \log_3(d+s) + \log_3 \frac{\ell-1}{2};$$

this implies

$$n \leqq 3s + 1 + \lfloor \log_3(\ell-1) \rfloor + \log_3(d+s) + \log_3 \frac{\ell-1}{2}.$$

Therefore we have

$$n \leqq 3s+2+\lfloor \log_3(\ell-1)\rfloor + \left\lfloor \log_3 \frac{\ell-1}{2} \right\rfloor + \lfloor \log_3(2s+1+\rfloor \log_3(\ell-1)\rfloor)\rfloor = m_\ell.$$

This is a contradiction.

6.2 Second Bound

We prove Theorem 6.2 by using K. Horie's method in [12]. K. Horie [10] proved the following:

Lemma 6.8 (K. Horie)**.** *Let $\ell \geq 5$ be a prime number φ the Frobenius automorphism of ℓ in $\mathbb{Q}(\zeta_{n+1})/\mathbb{Q}$. If an element β in $\mathbb{Z}[\zeta_{n+1}]$ is an ℓ-th power in $\mathbb{Z}[\zeta_{n+1}]$, then $\beta^\varphi - \beta^\ell \in \ell^2\mathbb{Z}[\zeta_{n+1}]$.*

Moreover, we use the following lemma:

Lemma 6.9. *Let a_i be elements in $\mathbb{Z}$ and ζ a primitive 3^{n+1}-th root of unity. If*

$$\sum_{i=0}^{2\cdot 3^{n-1}-1} a_i\zeta^i \equiv 0 \pmod{\ell},$$

then $a_j \in \ell\mathbb{Z}$ for $0 \leq j \leq 2\cdot 3^{n-1}-1$.

Let ℓ and φ be as in Lemma 6.8, $\zeta = \zeta_{n+1}^2$ a primitive 3^{n+1}-th root of unity, $\omega = \zeta_1^2$, σ a generator of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\omega))$ and recall $\eta = \dfrac{1}{\omega} \cdot \dfrac{\zeta - 1}{\omega\zeta - 1}$ the n-th Horie unit. Let s be as in Theorem 6.2 and we choose $\mathbb{Q}(\zeta_s)$ as F. We assume $n \geq s$ and ℓ divides h_n/h_{n-1}. Then, by Lemma 1.7, there exists a prime ideal $\mathfrak{L}$ in $\mathbb{Q}(\zeta_s)$ dividing ℓ such that η^{α_σ} is an ℓ-th power of a unit in $\mathbb{B}_n$ for any element α of the ideal $\ell\mathfrak{L}^{-1}$ of $\mathbb{Q}(\zeta_s)$. Let

$$\alpha = \sum_{i=0}^{2\cdot 3^{s-1}-1} a_i (\zeta_n^{3^{n-s}})^i$$

be an element in $\ell\mathfrak{L}^{-1}$ with $a_i \in \mathbb{Z}$ and we put $\tau = \sigma^{3^{n-s}}$. Then $\alpha_\sigma = \sum_{i=0}^{2\cdot 3^{s-1}-1} a_i \tau^i$. Noting that

$$\begin{aligned}(\beta+\gamma)^{a\ell} &= \left(\beta^\ell + \gamma^\ell + \sum_{k=1}^{\ell-1} \binom{\ell}{k} \beta^k \gamma^{\ell-k}\right)^a \\ &\equiv (\beta^\ell + \gamma^\ell)^a + a(\beta^\ell + \gamma^\ell)^{a-1} \sum_{k=1}^{\ell-1} \binom{\ell}{k} \beta^k \gamma^{\ell-k} \pmod{\ell^2}\end{aligned}$$

for β, $\gamma \in \mathbb{Z}[\zeta]$ and for $a \in \mathbb{Z}$, it follows that

$$(\zeta^{\tau^i} - 1)^{\ell a_i} \equiv (\zeta^{\ell\tau^i} - 1)^{a_i} + a_i(\zeta^{\ell\tau^i} - 1)^{a_i - 1} \sum_{k=1}^{\ell-1} \binom{\ell}{k} \zeta^{k\tau^i} (-1)^{\ell-k} \pmod{\ell^2},$$

$$(\omega\zeta^{\tau^i} - 1)^{-\ell a_i} \equiv (\omega^\ell \zeta^{\ell\tau^i} - 1)^{-a_i} - a_i(\omega^\ell\zeta^{\ell\tau^i} - 1)^{-a_i - 1} \sum_{k=1}^{\ell-1} \binom{\ell}{k} \omega^k \zeta^{k\tau^i} (-1)^{\ell-k} \pmod{\ell^2}.$$

From these congruence relations and a consequence

$$\begin{aligned}\frac{(\eta^{\alpha_\sigma})^\ell - (\eta^{\alpha_\sigma})^\varphi}{\omega^{-\ell\alpha_\sigma}} &= \prod_{i=0}^{2\cdot 3^{s-1}-1} \frac{(\zeta^{\tau^i} - 1)^{\ell a_i}}{(\omega\zeta^{\tau^i} - 1)^{\ell a_i}} - \prod_{i=0}^{2\cdot 3^{s-1}-1} \frac{(\zeta^{\ell\tau^i} - 1)^{a_i}}{(\omega^\ell\zeta^{\ell\tau^i} - 1)^{a_i}} \\ &\equiv 0 \pmod{\ell^2}\end{aligned}$$

of Lemma 1.7 and 6.8, we obtain

$$\sum_{i=0}^{2\cdot 3^{s-1}-1} \left(\frac{a_i}{\zeta^{\ell\tau^i} - 1} \sum_{k=1}^{\ell-1} \binom{\ell}{k} \zeta^{k\tau^i} (-1)^{\ell-k} - \frac{a_i}{\omega^\ell\zeta^{\ell\tau^i} - 1} \sum_{k=1}^{\ell-1} \binom{\ell}{k} \omega^k \zeta^{k\tau^i} (-1)^{\ell-k} \right) \equiv 0 \pmod{\ell^2},$$

since $\zeta^{\ell\tau^i}-1$ are prime to ℓ. By the congruence

$$\left(\begin{array}{c}\ell\\ k\end{array}\right) \equiv \frac{\ell(-1)^{k-1}}{k} \pmod{\ell^2} \quad (1 \le k \le \ell-1),$$

we have

$$\sum_{i=0}^{2\cdot 3^{s-1}-1}\left(\frac{a_i}{\zeta^{\ell\tau^i}-1}\sum_{k=1}^{\ell-1}\frac{\ell}{k}\zeta^{k\tau^i} - \frac{a_i}{\omega^\ell\zeta^{\ell\tau^i}-1}\sum_{k=1}^{\ell-1}\frac{\ell}{k}\omega^k\zeta^{k\tau^i}\right) \equiv 0 \pmod{\ell^2}.$$

Hence we obtain

$$\sum_{i=0}^{2\cdot 3^{s-1}-1} a_i \sum_{k=1}^{\ell-1}\frac{1}{k}\left(\frac{1}{\zeta^{\ell\tau^i}-1} - \frac{\omega^k}{\omega^\ell\zeta^{\ell\tau^i}-1}\right)\zeta^{k\tau^i} \equiv 0 \pmod{\ell}.$$

By substituting $(\zeta^{3^s})^{\tau^i} = \zeta^{3^s}$, we obtain

$$\begin{aligned} 0 &\equiv \sum_{i=0}^{2\cdot 3^{s-1}-1} a_i \sum_{k=1}^{\ell-1}\frac{1}{k}\left(\sum_{j=0}^{3^s-1}(\zeta^{\ell\tau^i})^j - \omega^k\sum_{j=0}^{3^s-1}(\omega^\ell\zeta^{\ell\tau^i})^j\right)\zeta^{k\tau^i} \\ &\equiv \sum_{i=0}^{2\cdot 3^{s-1}-1} a_i \sum_{k=1}^{\ell-1}\sum_{j=0}^{3^s-1}\frac{1-\omega^{\ell j+k}}{k}\zeta^{(\ell j+k)\tau^i} \pmod{\ell}. \end{aligned}$$

Now we have the following:

Lemma 6.10. *Let α be as in Lemma 1.7 and*

$$\alpha = \sum_{i=0}^{2\cdot 3^{s-1}-1} a_i(\zeta_n^{3^{n-s}})^i \tag{6.2.1}$$

with $a_i \in \mathbb{Z}$. If ℓ divides h_n/h_{n-1}, then

$$\sum_{i=0}^{2\cdot 3^{s-1}-1} a_i \sum_{k=1}^{\ell-1}\sum_{j=0}^{3^s-1}\frac{1-\omega^{\ell j+k}}{k}\zeta^{(\ell j+k)\tau^i} \equiv 0 \pmod{\ell}.$$

We put

$$S = \{b_0 3^{n-s+1} + b_1 3^{n-s+2} + \cdots + b_{s-1}3^n \mid b_j = 0,1,2 \text{ for } 0 \le j \le s-1\}$$

and define the subset S' of S by

$$S' = \bigcup_{i=0}^{2\cdot 3^{s-1}-1}\{r \in S\zeta^{\tau^{\mathtt{i}}-\mathtt{1}} = \zeta^{\mathtt{r}}\}.$$

Lemma 6.11. *Let j and k be rational integers with $0 \leq j \leq 3^s - 1$, $1 \leq k \leq \ell - 1$ and $r \in S'$. Let ℓ be a prime number with $5 \leq \ell < 3^{n-2s+1}$. If $(r+1)(\ell j + k) \equiv 2 \cdot 3^{s-1}\ell - 1 \pmod{3^n}$, then we have $j = 2 \cdot 3^{s-1} - 1$, $k = \ell - 1$ and $r = 0$ or 3^n.*

Proof. We have

$$-3^{n-s+1} < (2 \cdot 3^{s-1} - j)\ell - k - 1 < 3^{n-s+1}$$

because of $0 \leq j \leq 3^s - 1$, $1 \leq k \leq \ell - 1$ and $\ell < 3^{n-2s+1}$.
Since $(2 \cdot 3^{s-1} - j)\ell - k - 1 \equiv 0 \pmod{3^{n-s+1}}$, we have $(2 \cdot 3^{s-1} - j)\ell - k - 1 = 0$. Since $2 \leq k + 1 = (2 \cdot 3^{s-1} - j)\ell \leq \ell$, we have $k = \ell - 1$ and $j = 2 \cdot 3^{s-1} - 1$, which implies $r \equiv 0 \pmod{3^n}$. Hence $r = 0$, $r = 3^n$ or $r = 2 \cdot 3^n$. Since $r \in S'$, we have $r = 0$ or $r = 3^n$. □

Proof of Theorem 6.2. The assertion of Theorem 6.2 is trivial when $n = m_\ell$. So we assume that there exists an integer $n > m_\ell$ such that ℓ divides h_n/h_{n-1}. Then ℓ satisfies $\ell < 3^{n-2s+1}$ and Lemma 6.10 yields

$$\sum_{i=0}^{2 \cdot 3^{s-1}-1} a_i \sum_{k=1}^{\ell-1} \sum_{j=0}^{3^s-1} \frac{1 - \omega^{\ell j + k}}{k} \zeta^{(\ell j + k)\tau^i} \equiv 0 \pmod{\ell} \tag{6.2.2}$$

where a_i is the rational integer defined by (6.2.1). Since $\zeta_n^{3^{n-s}}$ is a unit, we may assume $a_0 \not\equiv 0 \pmod{\ell}$. From Lemma 6.9, Lemma 6.11 and (6.2.2), we have

$$a_0 \frac{1 - \omega^2}{\ell - 1} \zeta^{2 \cdot 3^{s-1}\ell - 1} + a_{3^{s-1}} \frac{1 - \omega^2}{\ell - 1} \zeta^{(2 \cdot 3^{s-1}\ell - 1)(3^n + 1)} \equiv 0 \pmod{\ell}.$$

Hence we have $a_0 \equiv 0 \pmod{\ell}$. This is a contradiction. □

6.3 Third Bound

Let $\ell \geq 5$ be a prime number and put $\mathbb{B}'_n = \mathbb{B}_n(\mu_\ell)$. We also put $\Delta_n = \mathrm{Gal}(\mathbb{B}'_n/\mathbb{B}_n)$ and $\omega_\ell : \Delta_n \longrightarrow \mathbb{Z}_\ell^\times$ such that $z^{\omega_\ell(\rho)} = z^\rho$ for all $z \in \mu_\ell$ and $\rho \in \Delta_n$.

Let 3^s be the exact power of 3 dividing ℓ^2-1 and put

$$m_{\ell,3} = 2s + \left\lfloor \frac{1}{2}\log_3(\ell-1) + \frac{1}{2} \right\rfloor.$$

We denote by v_ℓ the additive ℓ-adic valuation normalized by $v_\ell(\ell)=1$. Then we have the following:

Lemma 6.12. *If $n \geq m_{\ell,3}$, then we have $v_\ell\left(B_{1,\omega_\ell^{-1}\psi_n^{-1}}\right) = 0$ for all even characters ψ_n modulo 3^{n+1} with order 3^n.*

Proof. From Lemma 6.5, $B_{1,\omega_\ell^{-1}\psi_n^{-1}} \not\equiv 0 \pmod{\ell}$ if $2s + \lfloor \log_3(\ell-1) \rfloor \leq n$.

From now on, we assume $m_{\ell,3} \leq n \leq 2s + [\log_3(\ell-1)] - 1$. We recall a rational function

$$f_{1,\omega_\ell^{-1}}(T) = \left(\sum_{\substack{b \equiv 1 \pmod{3^s} \\ 0<b<3^s\ell}} \omega_\ell^{-1}(b) T^b \right) (T^{3^s\ell}-1)^{-1}$$

for $\chi = \omega_\ell^{-1}$. We put $g(T) = \sum_{b=0}^{\ell-1} \omega_\ell^{-1}(1+3^s b) T^{3^s b}$ and $h(T) = \sum_{b=0}^{\ell-1} \omega_\ell^{-1}(1+3^s b) T^b$ Then we have

$$T^{-1}(T^{3^s\ell}-1) f_{1,\omega_\ell^{-1}}(T) = g(T) = h(T^{3^s}) \tag{6.3.1}$$

Let ζ be a primitive 3^{n+1}-th root of unity in $\overline{\mathbb{Q}}_\ell$, and we put $u = n-2s+1$, $\theta = \zeta^{3^{u+s}}$, $e = [(\ell-1)/3^u]$ and

$$a_{i,j} = \begin{cases} \omega_\ell^{-1}(1+3^s(i+3^u j)) & \text{if } i+3^u j < \ell, \\ 0 & \text{if } i+3^u j \geq \ell. \end{cases}$$

Then $T^{3^u} - \theta \bmod \ell$ is irreducible over $\mathbb{Z}_\ell[\theta]/\ell\mathbb{Z}_\ell[\theta]$. Since $n \leq 2s + [\log_3(\ell-1)] - 1$, we have $u \leq [\log_3(\ell-1)]$ and $e \geq 1$. We also put $s_i(\theta) = \sum_{j=0}^{e} a_{i,j}\theta^j$ and $r(T) = \sum_{i=0}^{3^u-1} s_i(\theta) T^i$. Then there exists a polynomial $q(T)$ in $\mathbb{Z}_\ell[\theta][T]$ such that

$$h(T) = (T^{3^u} - \theta) q(T) + r(T). \tag{6.3.2}$$

In [6], Fukuda-Komatsu showed the following:

Lemma 6.13. *Let α, β, γ be nonzero elements in $\overline{\mathbb{F}}_\ell$ and let ν_i, μ_j positive integers with $\nu_1 < \nu_2 < \cdots < \nu_k < \ell$ and $\mu_1 < \mu_2 < \cdots < \mu_k < \ell$. Let*

$$S = \begin{pmatrix} \dfrac{1}{\alpha} & \dfrac{1}{\alpha+\beta\mu_1} & \cdots & \dfrac{1}{\alpha+\beta\mu_k} \\ \dfrac{1}{\alpha+\gamma\nu_1} & \dfrac{1}{\alpha+\beta\mu_1+\gamma\nu_1} & \cdots & \dfrac{1}{\alpha+\beta\mu_k+\gamma\nu_1} \\ \vdots & \vdots & \ddots & \vdots \\ \dfrac{1}{\alpha+\gamma\nu_k} & \dfrac{1}{\alpha+\beta\mu_1+\gamma\nu_k} & \cdots & \dfrac{1}{\alpha+\beta\mu_k+\gamma\nu_k} \end{pmatrix}$$

be a matrix of degree $k+1$. We assume that none of the denominators of entries of S are zero. Then the determinant $|S|$ is not zero.

Corollary 6.14. *We put*

$$R = \begin{pmatrix} \overline{a}_{0,0} & \cdots & \overline{a}_{0,e} \\ \overline{a}_{1,0} & \cdots & \overline{a}_{1,e} \\ \vdots & \ddots & \vdots \\ \overline{a}_{3^u-1,0} & \cdots & \overline{a}_{3^u-1,e} \end{pmatrix}$$

with $\overline{a}_{i,j} = a_{i,j} + \ell\mathbb{Z}_\ell[\theta]$ in $\mathbb{Z}_\ell[\theta]/\ell\mathbb{Z}_\ell[\theta]$. If $3^u > e$, then the rank of R is greater than or equal to e.

We assume $f_{1,\omega_\ell^{-1}}(\zeta) \equiv 0 \pmod{\ell}$. Then we have $h(\zeta^{3^s}) \equiv 0 \pmod{\ell}$ by (6.3.1). Hence we have $r(\zeta^{3^s}) \equiv 0 \pmod{\ell}$ by (6.3.2). Since $T^{3^u} - \theta \bmod \ell$ is irreducible over $\mathbb{Z}_\ell[\theta]/\ell\mathbb{Z}_\ell[\theta]$, we have

$$s_i(\theta) \equiv 0 \pmod{\ell} \quad (0 \le i \le 3^u - 1). \tag{6.3.3}$$

From the condition $m_3 \le n$, it follows that $3^{2u-1} > \ell - 1$, which implies $3^{u-1} > (\ell-1)/3^u \ge e$. Let R be the matrix in Lemma 6.13 and we put $f = \ell - 1 - 3^u e$.

First suppose $f \ge 3^{u-1}$, which implies $f > e$. We put

$$R_1 = \begin{pmatrix} \overline{a}_{0,0} & \cdots & \overline{a}_{0,e} \\ \overline{a}_{1,0} & \cdots & \overline{a}_{1,e} \\ \vdots & \ddots & \vdots \\ \overline{a}_{e+1,0} & \cdots & \overline{a}_{e+1,e} \end{pmatrix}.$$

By Lemma 6.13, the rank of R_1 is equal to $e+1$. Hence we have $\theta \equiv 0 \pmod{\ell}$ by (6.3.3), which is a contradiction. Next suppose $f < 3^{u-1}$, which implies $3^u - f > e+1$. We put

$$R_2 = \begin{pmatrix} \overline{a}_{f,0} & \cdots & \overline{a}_{f,e} \\ \overline{a}_{f+1,0} & \cdots & \overline{a}_{f+1,e} \\ \vdots & \ddots & \vdots \\ \overline{a}_{f+e+1,0} & \cdots & \overline{a}_{f+e+1,e} \end{pmatrix}.$$

From the definition of $a_{i,j}$, we have $\overline{a}_{f+1,e} = \cdots = \overline{a}_{f+e+1,e} = 0$. By Lemma 6.13, the rank of R_2 is equal to $e+1$ if $\overline{a}_{f,e} \neq 0$ or e if $\overline{a}_{f,e} = 0$. In both cases, we have $\theta \equiv 0 \pmod{\ell}$ by (6.3.3), which is a contradiction. Hence $f_{1,\omega_\ell^{-1}}(\zeta) \not\equiv 0 \pmod{\ell}$ and Lemma 6.5 yields the conclusion. □

We denote by A_n and A'_n the ℓ-Sylow subgroup of the ideal class group of $\mathbb{B}_n$ and $\mathbb{B}'_n$, respectively. We also put $\Gamma'_n = \mathrm{Gal}(\mathbb{B}'_n/\mathbb{B}'_0)$ and $G_n = \mathrm{Gal}(\mathbb{B}'_n/\mathbb{Q})$. Then we have $G_n \cong \Delta_n \times \Gamma'_n$.

We define idempotent ε_i in the group ring $\mathbb{Z}_\ell[\Delta_n]$

$$\varepsilon_i = \frac{1}{\ell - 1} \sum_{\rho \in \Delta_n} \omega_\ell^{-i}(\rho)\rho$$

for $0 \leq i \leq \ell - 2$. From [24], we have the following:

Theorem 6.15 (Mazur-Wiles)**.** *We have*

$$v_\ell\left(B_{1,\omega_\ell^{-1}\psi_n^{-j}}\right) \geq 0$$

and

$$v_\ell(|\varepsilon_1 A'_n|) - v_\ell(|\varepsilon_1 A'_{n-1}|) = \sum_{\substack{j=1 \\ (j,3)=1}}^{3^n-1} v_\ell\left(B_{1,\omega_\ell^{-1}\psi_n^{-j}}\right)$$

From Lemma 6.12 and Theorem 6.15, we obtain the following:

Lemma 6.16. *If $n \geq m_{\ell,3}$, then we have $\varepsilon_1 A'_n = \varepsilon_1 A'_{n-1}$.*

Since the natural map $A'_{n-1} \longrightarrow A'_n$ is injective by Lemma 1.2, we regard A'_{n-1} as G_n-submodule of A'_n. Let D_n and D'_n be the kernel of the norm map $A_n \longrightarrow A_{n-1}$ and $A'_n \longrightarrow A'_{n-1}$, respectively. Then we have $A_n = A_{n-1} \oplus D_n$ and $A'_n = A'_{n-1} \oplus D'_n$ again from Lemma 1.2. Let L'_n be the maximal unramified elementary abelian ℓ-extension of $\mathbb{B}'_n$. Since $L'_n/\mathbb{Q}$ is a Galois extension and the Galois group $\mathrm{Gal}(L'_n/\mathbb{B}'_n)$ is a normal abelian subgroup of $\mathrm{Gal}(L'_n/\mathbb{Q})$, G_n can act on $\mathrm{Gal}(L'_n/\mathbb{B}'_n)$. Hence $\mathrm{Gal}(L'_n/\mathbb{B}'_n)$ is isomorphic to $A'_n/\ell A'_n$ as G_n-module by Artin map, which shows $\mathrm{Gal}(L'_n/L'_{n-1}\mathbb{B}'_n) \cong D'_n/\ell D'_n$ from class field theory. Since

$$\mathrm{Gal}(L'_n/\mathbb{B}'_n) \cong A'_{n-1}/\ell A'_{n-1} \oplus D'_n/\ell D'_n,$$

there exists a subextension K'_n of $L'_n/\mathbb{B}'_n$ such that $\mathrm{Gal}(L'_n/K'_n) \cong A'_{n-1}/\ell A'_{n-1}$. Hence we have the following:

Proposition 6.17. *1.* $L'_n = K'_n L'_{n-1}$.

2. $L'_{n-1}\mathbb{B}'_n \cap K'_n = \mathbb{B}_n$.

3. $\mathrm{Gal}(K'_n/\mathbb{B}'_n) \cong D'_n/\ell D'_n$.

4. $K'_n/\mathbb{Q}$ *is a Galois extension of* $\mathbb{Q}$.

Since $\mu_\ell \subseteq \mathbb{B}'_n$ and since $K'_n/\mathbb{B}'_n$ is a Kummer extension, there exists a subgroup $\mathfrak{V} \subseteq \mathbb{B}'^{\times}_n/(\mathbb{B}'^{\times}_n)^\ell$ such that $K'_n = \mathbb{B}'_n(\sqrt[\ell]{\mathfrak{V}})$ in the obvious notations. Then there is a non-degenerate pairing

$$\begin{array}{rcl} \mathrm{Gal}(K'_n/\mathbb{B}'_n) \times \mathfrak{V} & \longrightarrow & \mu_\ell \\ (h, \tilde{b}) & \longmapsto & \langle h, \tilde{b} \rangle \end{array}$$

which is defined by

$$\langle h, \tilde{b} \rangle = \frac{h(\sqrt[\ell]{b})}{\sqrt[\ell]{b}},\ \tilde{b} = b(\mathbb{B}'^{\times}_n)^\ell$$

and satisfies

$$\langle h^g, \tilde{b}^g \rangle = \langle h, \tilde{b} \rangle^g$$

for any $g \in G_n$. Then the reflection theorem says $\varepsilon_j\mathfrak{V} \cong \varepsilon_i \mathrm{Gal}(K'_n/\mathbb{B}'_n)$ with $i + j \equiv 1 \pmod{\ell - 1}$. Hence we have

$$\begin{aligned}
\varepsilon_1\mathfrak{V} &\cong \varepsilon_0 \mathrm{Gal}(K'_n/\mathbb{B}'_n) \\
&\cong \varepsilon_0(D'_n/\ell D'_n) \\
&= D_n/\ell D_n \\
&\cong (A_n/A_{n-1})/\ell(A_n/A_{n-1})
\end{aligned}$$

from Lemma 1.1. Now we prove the following:

Lemma 6.18. *If $\varepsilon_1 A'_n = \varepsilon_1 A'_{n-1}$, then we have $A_n = A_{n-1}$.*

Proof. Suppose that A_n/A_{n-1} is non-trivial. Then $\varepsilon_1\mathfrak{V}$ is non-trivial. This implies that there exists an element $b(\mathbb{B}'^{\times}_n)^{\ell} \in \varepsilon_1\mathfrak{V}$ with $\mathbb{B}'_n(\sqrt[\ell]{b}) \supsetneq \mathbb{B}'_n$. Since K'_n
$supseteq \mathbb{B}'_n(\sqrt[\ell]{b})$, we have $\mathbb{B}'_n(\sqrt[\ell]{b}) \cap L'_{n-1}\mathbb{B}'_n = \mathbb{B}'_n$ from Proposition 6.17 (2). Then there exists an ideal $\mathfrak{b}$ of $\mathbb{B}'_n$ whose ideal class $\mathrm{cl}(\mathfrak{b})$ belongs to $\varepsilon_1 A'_n$ and whose ℓ-th power is (b). Since $\varepsilon_1(A'_n/A'_{n-1}) \cong \varepsilon_1 A'_n/\varepsilon_1 A'_{n-1}$, there exists an element d in $\mathbb{B}'_{n-1}$ with $\mathfrak{b} = (d)$. Hence there exists a unit u of $\mathbb{B}'_n$ with $b = du$. This implies that

$$b(\mathbb{B}'^{\times}_n)^{\ell} = \varepsilon_1 b(\mathbb{B}'^{\times}_n)^{\ell} = (\varepsilon_1 d(\mathbb{B}'^{\times}_n)^{\ell})(\varepsilon_1 u(\mathbb{B}'^{\times}_n)^{\ell}).$$

Since $\varepsilon_1 u(\mathbb{B}'^{\times}_n)^{\ell} = z(\mathbb{B}'^{\times}_n)^{\ell}$ for some $z \in \mu_{2\ell}$, we have $\mathbb{B}'_n(\sqrt[\ell]{b}) \subseteq L'_{n-1}$. This is a contradiction. □

From Lemma 6.16 and Lemma 6.18, we obtain Theorem 6.3.

Chapter 7

Algorithm for $p = 3$

In this chapter, we give the algorithm to calculate the ℓ-indivisibility of the class number of the n-th layer of the cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}$.

Let $\Gamma_n = \mathrm{Gal}(\mathbb{B}_n/\mathbb{Q})$ be the Galois group of $\mathbb{B}_n$ over $\mathbb{Q}$ and A_n the ℓ-part of the ideal class group of $\mathbb{B}_n$.

For a character $\chi : \Gamma_n \longrightarrow \overline{\mathbb{Q}}_\ell$, we define e_χ by

$$e_\chi = \frac{1}{|\Gamma_n|} \sum_{\sigma \in \Gamma_n} \mathrm{Tr}(\chi^{-1}(\sigma))\sigma \in \mathbb{Z}_\ell[\Gamma_n],$$

where Tr is the trace map of $\mathbb{Q}_\ell(\chi(\Gamma_n))/\mathbb{Q}_\ell$. We denote by $A_{n,\chi}$ the χ-part $e_\chi A_n$ of A_n. Then we have $A_n = \bigoplus_\chi A_{n,\chi}$ where χ runs over all representatives of $\mathbb{Q}_\ell$-conjugacy classes of characters of Γ_n.

In order to prove that ℓ does not divide h_n, it is sufficient to prove that ℓ does not divide the order of $A_{n,\chi}$ for each χ. If χ is not injective, then there exists a positive integer k such that $\mathbb{B}_k = \mathbb{B}_n^{\mathrm{Ker}\chi}$ and $A_{n,\chi} \cong A_{k,\chi}$. Therefore we may assume χ is injective.

Now, for $n \geqq 1$, let ζ_n denote a primitive 3^n-th root of unity in $\mathbb{C}$ and put

$$\xi_n = (\zeta_{n+1} - 1)(\zeta_{n+1}^{-1} - 1) = 2 - (\zeta_{n+1} + \zeta_{n+1}^{-1}) \ \in \ \mathbb{B}_n.$$

We fix a truncation $e_{\chi,\ell} \in \mathbb{Z}[\Gamma_n]$ of e_χ satisfying

$$e_{\chi,\ell} \equiv e_\chi \pmod{\ell}$$

in order to consider an action on ξ_n. The following lemma is a special case of Lemma 1 in [1].

Lemma 7.1. *If there exists a prime number q which is congruent to 1 modulo $3^{n+1}\ell$ and satisfies*

$$(\xi_n^{e_{\chi,\ell}})^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{\mathfrak{q}}$$

for some prime ideal $\mathfrak{q}$ of $\mathbb{B}_n$ lying above q, then we have $|A_{n,\chi}| = 1$, where $|A_{n,\chi}|$ denotes the order of $A_{n,\chi}$.

Owing to Lemma 7.1 , we may regard χ as a character of Γ_n into $\overline{\mathbb{F}}_\ell$ and define e_χ to be an element of $\mathbb{F}_\ell[\Gamma_n]$ where $\overline{\mathbb{F}}_\ell$ is an algebraic closure of the finite field $\mathbb{F}_\ell = \mathbb{Z}/\ell\mathbb{Z}$. Let $\overline{\zeta}_n$ be a primitive 3^n-th root of unity in $\overline{\mathbb{F}}_\ell$ and put $K = \mathbb{F}_\ell(\overline{\zeta}_n)$. Let ρ be the generator of Γ_n determined by $\zeta_{n+1} \longmapsto \zeta_{n+1}^4$ and χ the character of Γ_n defined by $\chi(\rho) = \overline{\zeta}_n^{-1}$. Then

$$e_{\chi^j} = \frac{1}{3^n}\sum_{i=0}^{3^n-1} \mathrm{Tr}_{K/\mathbb{F}_\ell}(\overline{\zeta}_n^{ij})\rho^i.$$

Let q be a prime number congruent to 1 modulo $3^{n+1}\ell$ and g_q a primitive root of q. Then

$$\zeta_{n+1} \equiv g_q^{\frac{q-1}{3^{n+1}}} \pmod{\mathfrak{q}}$$

for some prime ideal $\mathfrak{q}$ of $\mathbb{B}_n$ lying above q.
Therefore, if $e_{\chi^j} = \sum_i a_{ij}\rho^i$, then we have

$$\begin{aligned}
\xi_n^{e_{\chi^j}} &= \prod_{i=0}^{3^n-1}(2 - \zeta_{n+1} - \zeta_{n+1}^{-1})^{a_{ij}\rho^i} \\
&= \prod_{i=0}^{3^n-1}(2 - \zeta_{n+1}^{4^i} - \zeta_{n+1}^{-4^i})^{a_{ij}} \\
&\equiv \prod_{i=0}^{3^n-1}(2 - g_q^{\frac{q-1}{3^{n+1}}4^i} - g_q^{-\frac{q-1}{3^{n+1}}4^i})^{a_{ij}} \pmod{\mathfrak{q}}.
\end{aligned}$$

The last product should be calculated modulo q. We fix positive integers z_1

and z_2 satisfying

$$\begin{aligned} z_1 &\equiv g_q^{\frac{q-1}{3^{n+1}}} \pmod{q} \\ z_2 &\equiv z_1^{-1} \pmod{q}. \end{aligned}$$

7.1 The case $\ell \equiv 1 \pmod 3$ and $2 \leqq n \leqq s$.

Since $\overline{\zeta}_n \in \mathbb{F}_\ell$, we have $\mathrm{Tr}_{K/\mathbb{F}_\ell}(\overline{\zeta}_n) = \overline{\zeta}_n$ and

$$e_{\chi^j} = \frac{1}{3^n} \sum_{i=0}^{3^n-1} \overline{\zeta}_n^{ij} \rho^i.$$

Let g_ℓ be a primitive root of ℓ and fix integers a_{ij} satisfying

$$a_{ij} \equiv g_\ell^{\frac{\ell-1}{3^n} ij} \pmod{\ell}.$$

There are $2 \cdot 3^{n-1}$ injective characters of Γ_n and none of them is conjugate over $\mathbb{F}_\ell$. If we put

$$X = \{j \in \mathbb{Z} \mid 1 \leqq j < 3^n, (j,3) = 1\},$$

then $\{\chi^j \mid j \in X\}$ is the set of all injective characters of Γ_n. Then Lemma 7.1 implies the following criterion.

Criterion 7.2. Put $b = 4$. If there exists a prime number q which is congruent to 1 modulo $3^{n+1}\ell$ and satisfies

$$\Big(\prod_{i=0}^{3^n-1} (2 - z_1^{b^i} - z_2^{b^i})^{a_{ij}}\Big)^{\frac{q-1}{\ell}} \not\equiv 1 \pmod{q} \quad \text{for each } j \in X,$$

then ℓ does not divide h_n/h_{n-1}.

7.2 The case $\ell \equiv 1 \pmod 3$ and $s+1 \leqq n$.

We have $[K : \mathbb{F}_\ell] = 3^{n-s}$. The minimal polynomial of $\overline{\zeta}_n$ over $\mathbb{F}_\ell$ is

$$T^{3^{n-s}} - \overline{\zeta}_n^{3^{n-s}}.$$

Therefore $\mathrm{Tr}_{K/\mathbb{F}_\ell}(\overline{\zeta}_n^i) = 0$ if i is not divisible by 3^{n-s}. Hence we have

$$\begin{aligned} e_{\chi^j} &= \frac{1}{3^n}\sum_{i=0}^{3^s-1} \mathrm{Tr}_{K/\mathbb{F}_\ell}(\overline{\zeta}_n^{3^{n-s}ij})\rho^{3^{n-s}i} \\ &= \frac{1}{3^s}\sum_{i=0}^{3^s-1} \overline{\zeta}_s^{ij}\rho^{3^{n-s}i}. \end{aligned}$$

Since there are $2\cdot 3^{s-1}$ non-conjugate primitive 3^n-th roots of unity in $\overline{\mathbb{F}}_\ell$, there are the same number of $\mathbb{F}_\ell$-conjugacy classes of injective characters of Γ_n. In this case, we put

$$X = \{j \in \mathbb{Z} \mid 1 \leqq j < 3^s, (j,3) = 1\}.$$

Then $\{\chi^j \mid j \in X\}$ is a set of representatives of $\mathbb{F}_\ell$-conjugacy classes of injective characters of Γ_n.

Let g_ℓ be a primitive root of ℓ and fix integers a_{ij} satisfying

$$a_{ij} \equiv g_\ell^{\frac{\ell-1}{3^s}ij} \pmod{\ell}.$$

Criterion 7.3. Put $b = 4^{3^{n-s}}$. If there exists a prime number q which is congruent to 1 modulo $3^{n+1}\ell$ and satisfies

$$(\prod_{i=0}^{3^s-1}(2 - z_1^{b^i} - z_2^{b^i})^{a_{ij}})^{\frac{q-1}{\ell}} \not\equiv 1 \pmod{q} \quad \text{for each } j \in X,$$

then ℓ does not divide h_n/h_{n-1}.

7.3 The case $\ell \equiv -1 \pmod 3$ and $2 \leqq n \leqq s$.

We have $[K : \mathbb{F}_\ell] = 2$. Since there are 3^{n-1} non-conjugate primitive 3^n-th roots of unity in $\overline{\mathbb{F}}_\ell$, there are the same number of $\mathbb{F}_\ell$-conjugacy classes of injective characters of Γ_n. In this case, we put

$$X = \left\{ j \in \mathbb{Z} \;\middle|\; 1 \leqq j \leqq \frac{3^n-1}{2}, (j,3) = 1 \right\}.$$

Then $\{\chi^j \mid j \in X\}$ is a set of representatives of $\mathbb{F}_\ell$-conjugacy classes of injective characters of Γ_n.

In this case, we have

$$\begin{aligned} e_{\chi^j} &= \frac{1}{3^n}\sum_{i=0}^{3^n-1} \mathrm{Tr}_{K/\mathbb{F}_\ell}(\overline{\zeta}_n^{ij})\rho^i \\ &= \frac{1}{3^n}\sum_{i=0}^{3^n-1} \mathrm{Tr}_{\mathbb{F}_\ell(\overline{\zeta}_s)/\mathbb{F}_\ell}(\overline{\zeta}_s^{3^{s-n}ij})\rho^i. \end{aligned}$$

Fix integers a_{ij} satisfying

$$a_{ij} \equiv t_{3^{s-n}ij} \pmod{\ell},$$

where t_i is the element of $\mathbb{F}_\ell$ defined by (7.4.1) in 7.4.

Criterion 7.4. Put $b = 4$. If there exists a prime number q which is congruent to 1 modulo $3^{n+1}\ell$ and satisfies

$$\Big(\prod_{i=0}^{3^n-1}(2 - z_1^{b^i} - z_2^{b^i})^{a_{ij}}\Big)^{\frac{q-1}{\ell}} \not\equiv 1 \pmod{q} \quad \text{for each } j \in X,$$

then ℓ does not divide h_n/h_{n-1}.

7.4 The case $\ell \equiv -1 \pmod 3$ and $s+1 \leqq n$.

We have $[K : \mathbb{F}_\ell] = 2 \cdot 3^{n-s}$. Let

$$T^2 - aT + 1$$

be the minimal polynomial of $\overline{\zeta}_s$ over $\mathbb{F}_\ell$. Then the minimal polynomial of $\overline{\zeta}_n$ over $\mathbb{F}_\ell$ is

$$T^{2\cdot 3^{n-s}} - aT^{3^{n-s}} + 1.$$

therefore $\mathrm{Tr}_{K/\mathbb{F}_\ell}(\overline{\zeta}_n^i) = 0$ if i is not divisible by 3^{n-s}. Hence we have

$$\begin{aligned} e_{\chi^j} &= \frac{1}{3^n}\sum_{i=0}^{3^s-1} \mathrm{Tr}_{K/\mathbb{F}_\ell}(\overline{\zeta}_n^{3^{n-s}ij})\rho^{3^{n-s}i} \\ &= \frac{1}{3^s}\sum_{i=0}^{3^s-1} \mathrm{Tr}_{\mathbb{F}_\ell(\overline{\zeta}_s)/\mathbb{F}_\ell}(\overline{\zeta}_s^{ij})\rho^{3^{n-s}i}. \end{aligned}$$

We need to calculate

$$t_i = \mathrm{Tr}_{\mathbb{F}_\ell(\overline{\zeta}_s)/\mathbb{F}_\ell}(\overline{\zeta}_s^i). \tag{7.4.1}$$

We start from $t_1 = \overline{\zeta}_s + \overline{\zeta}_s^{-1}$ and proceed to

$$\begin{aligned} t_3 &= \overline{\zeta}_s^3 + \overline{\zeta}_s^{3\ell} = (\overline{\zeta}_s + \overline{\zeta}_s^\ell)^3 - 3\overline{\zeta}_s^{(\ell+1)}(\overline{\zeta}_s + \overline{\zeta}_s^\ell) = t_1^3 - 3t_1 \\ t_{3^2} &= \overline{\zeta}_s^{3^2} + \overline{\zeta}_s^{3^2\ell} = (\overline{\zeta}_s^3 + \overline{\zeta}_s^{3\ell})^3 - 3\overline{\zeta}_s^{3(\ell+1)}(\overline{\zeta}_s^3 + \overline{\zeta}_s^{3\ell}) = t_3^3 - 3t_3 \\ &\vdots \\ t_{3^{s-1}} &= \overline{\zeta}_s^{3^{s-1}} + \overline{\zeta}_s^{3^{s-1}\ell} = t_{3^{s-2}}^3 - 3t_{3^{s-2}} = -1, \end{aligned}$$

noting $\overline{\zeta}_s^{\ell+1} = 1$. Reversing this procedure, we obtain t_1 recursively.

Lemma 7.5. *Let $b_1 = -1 \in \mathbb{F}_\ell$. If $s \geqq 2$, we choose $b_i \in \mathbb{F}_\ell$ $(2 \leqq i \leqq s)$ by*

$$b_{i+1}^3 - 3b_{i+1} = b_i.$$

Then we have $t_1 = b_s$.

Remark 7.6. For each step, we have three roots. Hence we have just 3^{s-1} t_1 which correspond to 3^{s-1} non-conjugate primitive 3^s-th roots of unity in $\overline{\mathbb{F}}_\ell$. We fix arbitrary one.

We obtain t_i $(2 \leqq i \leqq 3^s - 1)$ from $t_0 = 2$ and t_1 using the following recurrence formula.

Lemma 7.7. *There holds $t_{i+2} = t_{i+1}t_1 - t_i$.*

Proof. We have

$$\begin{aligned} t_1 t_{i+1} &= (\overline{\zeta}_s + \overline{\zeta}_s^\ell)(\overline{\zeta}_s^{i+1} + \overline{\zeta}_s^{(i+1)\ell}) \\ &= \overline{\zeta}_s^{i+2} + \overline{\zeta}_s^{(i+2)\ell} + \overline{\zeta}_s^{i+\ell+1} + \overline{\zeta}_s^{i\ell+\ell+1} \\ &= (\overline{\zeta}_s^{i+2} + \overline{\zeta}_s^{(i+2)\ell}) + \overline{\zeta}_s^{\ell+1}(\overline{\zeta}_s^i + \overline{\zeta}_s^{i\ell}) \\ &= t_{i+2} + t_i. \end{aligned}$$

□

Since there are 3^{s-1} non-conjugate primitive 3^n-th roots of unity in $\overline{\mathbb{F}}_\ell$, there are the same number of $\mathbb{F}_\ell$-conjugacy classes of injective characters of Γ_n. In this case, we put

$$X = \left\{ j \in \mathbb{Z} \;\middle|\; 1 \leqq j \leqq \frac{3^s - 1}{2}, (j, 3) = 1 \right\}.$$

Then $\{\chi^j \mid j \in X\}$ is a set of representatives of $\mathbb{F}_\ell$-conjugacy classes of injective characters of Γ_n. We fix integers a_{ij} satisfying

$$a_{ij} \equiv t_{ij} \pmod{\ell}.$$

Note that ij in the left hand side is a subscript with two indices and that in the right is the product of i and j.

Criterion 7.8. Put $b = 4^{3^{n-s}}$. If there exists a prime number q which is congruent to 1 modulo $3^{n+1}\ell$ and satisfies

$$\Big(\prod_{i=0}^{3^s-1} (2 - z_1^{b^i} - z_2^{b^i})^{a_{ij}}\Big)^{\frac{q-1}{\ell}} \not\equiv 1 \pmod{q} \quad \text{for each } j \in X,$$

then ℓ does not divide h_n/h_{n-1}.

Chapter 8

Computational Results for $p = 3$

In this chapter, we shall give computational results for the ℓ-indivisibility of $h_{3,n}$. By using Theorem 6.3 and the algorithm in Chapter 7, we obtain the following:

Theorem 8.1. *Let ℓ be a prime number. If ℓ satisfies $\ell < 400000$, then ℓ does not divide h_n for any non-negative integer n.*

Let ℓ be a prime number with $\ell \not\equiv \pm 1 \pmod{27}$. Then $s = 1$ or 2 and $f = 1$ or 2 where s and f is the same as in Theorem 5.1. We put $c = 2 \cdot 3^{s-1}$. Then we have $(2^{c/2} \cdot c!)^{1/f} \leq 5760$. From Theorem 5.1 and Theorem 8.1, we obtain the following.

Theorem 8.2. *Let ℓ be a prime number. If ℓ satisfies $\ell \not\equiv \pm 1 \pmod{27}$, then ℓ does not divide h_n for any non-negative integer n.*

Next, we restrict our attention to a prime number ℓ with $\ell \equiv 26,\ 53 \pmod{81}$. Then we again have the following:

Theorem 8.3. *Let ℓ be a prime number with $\ell \equiv 26$ or $53 \pmod{81}$. If ℓ satisfies $\ell < 1.82 \times 10^9$, then ℓ does not divide h_n for any non-negative integer n.*

If ℓ is a prime number with $\ell \equiv 26$ or $53 \pmod{81}$, then $s = 3$ and $f = 2$ where s and f is the same as in Theorem 5.1. We put $c = 2 \cdot 3^{s-1}$. Then

we have $(2^{c/2} \cdot c!)^{1/f} < 1.82 \times 10^9$. From Theorem 5.1 and Theorem 8.3, we obtain the following.

Theorem 8.4. *Let ℓ be a prime number. If ℓ satisfies $\ell \equiv 26$ or $53 \pmod{81}$, then ℓ does not divide h_n for any non-negative integer n.*

Bibliography

[1] M. Aoki and T. Fukuda, *An Algorithm for Computing p-Class Groups of Abelian Number Fields*, Algorithmic Number Theory,56-71,Lecture Notes in Computer Science, vol.4076, Springer, Berlin, 2006.

[2] H. Bauer, *Numeriche Bestimmung con Klassenzahlen reeler zyklischer Zahlkörper*, J. Number Th., **1** (1969), 161-162.

[3] H. Cohn, *A Numerical Study of Weber's Real Class Number Calculation I*, Numer. Math. 2, **2** (1960), 347-362.

[4] G. Everest and T. Ward, *Heights of Polynomials and Entropy in Algebraic Dynamics*, Universitext, Springer-Verlag London, Ltd., London, 1999.

[5] E. Friedman and J. W. Sands (with an appendix by L. C. Washington), *On the ℓ-adic Iwasawa λ-invariant in a p-extension*, Math. of Comp. **64**-212 (1995), 1659-1674.

[6] T. Fukuda and K. Komatsu, *Weber's Class Number Problem in the Cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$*, Experiment. Math. **18**-2 (2009), 213-222.

[7] T. Fukuda and K. Komatsu, *Weber's Class Number Problem in the Cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$,* II, J. Théor. Nombres Bordeaux, **22**-2 (2010), 359-368.

[8] T. Fukuda and K. Komatsu, *Weber's Class Number Problem in the Cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$,* III, Int. J. of Number Theory, **7**-6 (2011), 1627-1635.

[9] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, Academic Press (1965).

[10] K. Horie, *Ideal Class Groups of Iwasawa-theoretical Abelian Extensions over the Rational Field*, J. London Math. Soc. **66** (2002), 257-275.

[11] K. Horie, *Primary Components of the Ideal Class Group of the $\mathbb{Z}_p$-extension over $\mathbb{Q}$ for Typical Inert Primes*, Proc. Japan Acad. Ser. A Math. Sci., **81** (2005), no.3, 40-43.

[12] K. Horie, *The Ideal Class Group of the Basic $\mathbb{Z}_p$-extension over an Imaginary Quadratic Field*, Tohoku Math. J., **57** (2005), 375-394.

[13] K. Horie, *Certain Primary Components of the Ideal Class Group of the $\mathbb{Z}_p$-extension over the Rationals*, Tohoku Math. J., **59** (2007), 259-291.

[14] K. Horie and M. Horie, *The Narrow Class Groups of Some $\mathbb{Z}_p$-extensions over the Rationals*, Acta Arith., **135** (2008), no.2, 159-180.

[15] K. Horie and M. Horie, *The Ideal Class Group of the $\mathbb{Z}_p$-extension over the Rationals*, Tohoku Math. J., **61** (2009), 551-570.

[16] K. Horie and M. Horie, *The Ideal Class Group of the $\mathbb{Z}_{23}$-extension over the Rational Field*, Proc. Japan Acad., **85** (2009), Ser. A, 155-159.

[17] K. Horie and M. Horie, *The Narrow Class Groups of the $\mathbb{Z}_{17}$- and $\mathbb{Z}_{19}$-extensions over the Rational Field*, Abh. Math. Sem. Univ. Hamburg., **80**-1 (2010), 47-57.

[18] H. Ichimura and S. Nakajima, *On the 2-part of the Ideal Class Group of the Cyclotomic $\mathbb{Z}_p$-extension over the Rationals*, Abh. Math. Sem. Univ. Hamburg., **80**-2 (2010), 175-182.

[19] K. Iwasawa, *A Note on Class Numbers of Algebraic Number Fields*, Abh. Math. Sem. Univ. Hamburg **20** (1956), 257-258.

[20] S. Lang, *Algebraic Number Theory*, 2nd edition, Graduate Texts in Math., **110**, Springer-Verlag, New York, Heidelberg, Berlin, (1994).

[21] F. J. van der Linden, *Class Number Computations of Real Abelian Number Fields*, Math. Comp. **39** (1982), 693-707.

[22] N. I. Lobachevsky, *Complete Works*, I, III, V, Gostekhizdat, Moscow and Leningrad (1946–1951).

[23] J. M. Masley, *Class Numbers of Real cyclic number fields with small conductor*, Compositio math. **37** (1978), 297-319.

[24] B. Mazur and A. Wiles, *Class Fields of Abelian Extensions of* $\mathbb{Q}$, Inv. Math. **76** (1984), 179-330.

[25] R. Okazaki, *On a Lower Bound for Relative Units, Schinzel's Lower Bound and Weber's Class Number Problem*, preprint.

[26] A. Schinzel, *On the Product of the Conjugates outside the Unit Circle of an Algebraic Integer*, Acta Arith. **24** (1973), 385-399.

[27] W. Sinnott, *On the Stickelberger Ideal and the Circular Units of an Abelian Field*, Inv. Math., **62** (1980), 181-234.

[28] L. C. Washington, *Class Numbers and Cyclotomic* $\mathbb{Z}_p$*-extensions*, Inv. Math. **49** (1978), 87-97.

[29] L. C. Washington, *The Non-p-part of the Class Number in a Cyclotomic* $\mathbb{Z}_p$*-extension*, Inv. Math. **49** (1978), 87-97.

[30] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd edition, Graduate Texts in Math.,83, Springer-Verlag, New York, Heidelberg, Berlin, 1997.

[31] H. Weber, *Theorie der Abel'schen Zahlkörper*, Acta Math., **8** (1886), 193-263.

List of Papers by Takayuki MORISAWA

1. T. Morisawa, *A Class Number Problem in the Cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}$*, Tokyo J. Math. **32** (2009), 549-558.

2. T. Morisawa, *Mahler Measure of the Horie Unit and Weber's Class Number Problem in the Cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}$*, to appear in Acta Arith..

3. T. Fukuda, K. Komatsu and T. Morisawa, *On λ-invariants of $\mathbb{Z}_\ell$-extensions over Real Abelian Number Fields of Prime Power Conductors*, to appear in Funct. Approx. Comment. Math..