이학박사 학위논문

The Gauss class number problem and the conjecture of Birch and Swinnerton-Dyer

(가우스 류수 문제와 버츠와 스위너튼 다이어의 추측)

2020년 2월

서울대학교 대학원

수리과학부

김 지 구

The Gauss class number problem and the conjecture of Birch and Swinnerton-Dyer

(가우스 류수 문제와 버츠와 스위너튼 다이어의 추측)

지도교수 변 동 호

이 논문을 이학박사 학위논문으로 제출함

2019년 10월

서울대학교 대학원

수리과학부

김 지 구

김 지 구의 이학박사 학위논문을 인준함

2019년 12월

위 원 장	____________________	(인)
부 위 원 장	____________________	(인)
위 원	____________________	(인)
위 원	____________________	(인)
위 원	____________________	(인)

The Gauss class number problem and the conjecture of Birch and Swinnerton-Dyer

A dissertation
submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
to the faculty of the Graduate School of
Seoul National University

by

Jigu Kim

Dissertation Director : Professor Dongho Byeon

Department of Mathematical Science
Seoul National University

February 2020

Abstract

The Gauss class number problem and the conjecture of Birch and Swinnerton-Dyer

Jigu Kim

Department of Mathematical Sciences
The Graduate School
Seoul National University

The Gauss class number problem is to determine a complete list of quadratic number fields for any given class number. It follows from Siegel's theorem that for each class number there are only finitely many imaginary quadratic fields and real quadratic fields of Richaud-Degert type. Since Siegel's theorem is ineffective, it cannot provide a solution for the Gauss class number problem.

Goldfeld discovered an effective method, which concerns arithmetic of an elliptic curve, to solve the class number problem for imaginary quadratic fields and real quadratic fields of Richaud-Degert type. In the imaginary case only Oesterlé simplified Goldfeld's proof and made an explicit result, which led him to solve the class number three problem for imaginary quadratic fields.

We find explicit constants in Goldfeld's method and apply the results to the class number problem for real quadratic fields of Richaud-Degert type.

Key words: class numbers, quadratic fields, elliptic curves.
Student Number: 2014-21201

Contents

Chapter 1

Introduction

In his 1801 Disquisitiones Arithmeticae [Gau], Gauss posed his class number conjectures in the language of binary quadratic forms (for even discriminant only). Since Dedekind's time, the conjectures have been rephrased in the language of quadratic fields, which is how we will state.

Let K be a quadratic field, i.e. an extension of $\mathbb{Q}$ of degree 2. There is a unique square-free integer $D \neq 1$ such that $K = \mathbb{Q}(\sqrt{D})$. We call D the fundamental radicand. Let $d = 4D/\sigma^2$, where $\sigma = 2$ if $D \equiv 1 \pmod 4$ and $\sigma = 1$ otherwise. The value d is called the fundamental discriminant. We denote by $h(d)$ the class number of K.

Gauss surmised that $h(d) \to \infty$ as $K = \mathbb{Q}(\sqrt{d})$ runs through the imaginary quadratic fields (i.e., $d < 0$ and $d \to -\infty$). Landau [Lan18] published Hecke's work, which stated that the conjecture is true under the assumption that the Generalized Riemann hypothesis (GRH for short) was true. Unexpectedly, the falsity of the GRH also implies the right answer by a series of papers of Deuring [Deu33], Mordell [Mor34] and Heilbronn [Hei34] in the 1930's. So they gave an unconditional proof.

For positive discriminants, Gauss predicted completely different behavior of the class numbers and surmised that there are infinitely many real quadratic fields with class number one, which is still unproved. Unlike an imaginary quadratic field, a real quadratic field has infinitely many units and its unit group U_K is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. Let $\varepsilon_d > 1$ be the fundamental unit such that $U_K = \{\pm 1\} \times \langle \varepsilon_d \rangle$ and let $R(d) = \log(\varepsilon_d)$ be the regulator of $\mathbb{Q}(\sqrt{d})$ for $d > 0$.

Disquisitiones Arithmeticae [Gau] also gave the tables of imaginary quadratic fields with low class numbers and Gauss conjectured that there are no more. For this class number problem and other purposes, a lower bound of $h(d)$ for $d < 0$ and that of $h(d) \times R(d)$ for $d > 0$, have been studied by Landau [Lan35], Siegel [Sie35], Tatuzawa [Tat51], etc. However, their results are not effective. For example, it follows that there is at most one fundamental discriminant $d_{10} < 0$ with class number one, beyond that 9 already known to Gauss. So different methods were required to solve the class number one problem for imaginary quadratic fields. In the late 1960's, both nonexistence of $d_{10} < 0$ with class number one and that of $d_{19} < 0$ with class number two were proved by two different methods: one is Baker's effective transcendence method [Bak69, Bak71] and the other is Stark's [Sta67, Sta69, Sta71]. However, neither Baker's method nor Strark's applied to the class number three problem.

In 1976, Goldfeld [Gol76] made a startling discovery: The existence of an elliptic curve E over $\mathbb{Q}$ with high analytic rank g implies that for any fundamental discriminant $d < 0$ and any small $\epsilon > 0$

$$h(d) > c_E \times \begin{cases} (\log d)^{g-2-\epsilon} & \text{if } \chi_d(-N) = (-1)^{g-1}, \\ (\log d)^{g-3-\epsilon} & \text{if } \chi_d(-N) = (-1)^{g-2}, \end{cases}$$

and the constant c_E can be effectively computed. The inequality holds with a factor $R(d)$ on the left-hand side if $d > 0$.

In 1983, Gross and Zagier [GZ83] were able to find a Weil curve E with analytic rank 3, which satisfies all of Goldfeld's hypotheses. The corresponding constant c_E of a slightly different form, was computed by Oesterlé [Oes85, Oes88]: For any $d < 0$,

$$h(d) > \begin{cases} \frac{1}{55} \log|d| \cdot \theta(d) & \text{if } (d, 5077) = 1, \\ \frac{1}{7000} \log|d| \cdot \theta(d) \end{cases}$$

where $\theta(d) = \prod_{p \in P(d)} \left(1 - \frac{\lfloor 2\sqrt{p} \rfloor}{p+1}\right)$ and $P(d)$ is the set of prime divisors of d except maximal one. The first inequality is calculated from Gross and Zagier's elliptic curve

$$y^2 + y = x^3 - 7x + 6, \quad N = 5077,$$

and the other one is from the twisted elliptic curve

$$-139y^2 = x^3 + 10x^2 - 20x + 8, \quad N = 37 \cdot 139^2.$$

Oesterlé's method, however, works for imaginary quadratic fields only.

For sake of application to real quadratic fields of narrow Richaud-Degert type (i.e., $D = n^2 \pm 1$ or $n^2 \pm 4$) whose regulators are the smallest size as a function of d, we will largely follow Goldfeld's paper [Gol76] and calculate all constants in questions. The constant c_E will be provided by the following two different methods: The Grössencharakter for an elliptic curve with complex multiplication, and Goldfeld-Hoffstein-Lieman method for an elliptic modular form which is not a lift from GL(1) (cf. [GHL94] and [Wak]).

As a preliminary part, part I consists of chapter 2 and chapter 3. In chapter 2, we will review Dirichlet's class number formula and list ineffective results about lower bounds for $L(1, \chi)$. In chapter 3, we will recall the definition of the Hasse-Weil L-function attached to an elliptic curve and the conjecture of Birch and Swinnerton-Dyer. We will also introduce some materials to be used to compute c_E.

Part II consists of chapter 4 and chapter 5. Chapter 4 contains main results and explicit constants in Goldfeld's method. Chapter 5 provides applications to a certain family of real quadratic fields of narrow Richaud-Degert type as well as two different proofs for Lemma 4.3.3.

Part I

Preliminary

Chapter 2

Special values of the Dirichlet L-functions

2.1 Dirichlet's class number formula

Definition 2.1.1. For a positive integer q, a Dirichlet character $\pmod{q}$ is a homomorphism from $(\mathbb{Z}/q\mathbb{Z})^*$ to the unit circle $S^1 \subset \mathbb{C}$, extended by zero to a function on $\mathbb{Z}/q\mathbb{Z}$ and lifted to $\mathbb{Z}$.

Definition 2.1.2. The principal character $\chi_0 \pmod{q}$ is defined by $\chi_0(n) = 1$ if $(n, q) = 1$ and $\chi_0(n) = 0$ otherwise. A Dirichlet character $\chi \pmod{q}$ that cannot be obtained by $\chi = \chi_0\chi'$ with $\chi_0 \pmod{q}$ and any character χ' modulo a proper factor $q' \mid q$, is called primitive. Any Dirichlet character χ comes from a unique primitive character χ' and the modulus of this χ' is called the conductor of χ.

Proposition 2.1.3. We denote a rational prime by p. For any Dirichlet charater the following holds.

(1) Since $\chi(-1)^2 = \chi(1) = 1$, $\chi(-1) = \pm 1$.

(2) The number of primitive Dirichlet characters (mod q) is $q\prod_{p|q}\alpha_p$, where $\alpha_p = ((p-1)/p)^2$ if $p^2 \mid q$ and $(p-2)/p$ if $p \parallel q$.

(3) Every real Dirichlet character is of the form $\chi_0\psi\prod_{l\in S}\left(\frac{\cdot}{l}\right)$, where χ_0 is the principal character, $\psi = \chi_4^{\epsilon_4}\chi_8^{\epsilon_8}$ for some $\epsilon_4, \epsilon_8 \in \{0,1\}$, S is a finite set of odd primes, and $\left(\frac{\cdot}{l}\right)$ is the Legendre symbol.

(4) Every real primitive Dirichlet character χ (mod q) can be defined, using the Kronecker symbol, to be

$$\chi(n) = \chi_d(n) = \left(\frac{d}{n}\right),$$

which is attached to the quadratic field $\mathbb{Q}(\sqrt{d})$ and the fundamental discriminant is given by $d = \chi(-1)q$.

Let $\nu = \nu(\chi) = \frac{1-\chi(-1)}{2}$.

Definition 2.1.4. The function

$$L(s,\chi) = \sum_{n=1}^{\infty}\chi(n)n^{-s} = \prod_p(1-\chi(p)p^{-s})^{-1}$$

is called the Dirichlet L-function and

$$\Lambda(s,\chi) = \left(\frac{\pi}{q}\right)^{-\frac{s+\nu}{2}}\Gamma\left(\frac{s+\nu}{2}\right)L(s,\chi)$$

is called the completed Dirichlet L-function.

Theorem 2.1.5. The completed Dirichlet L-function of a primitive character χ modulo q has an analytic continuation to the whole complex plane as an entire function and satisfies the functional equation

$$\Lambda(s,\chi) = \frac{\tau(\chi)}{i^{\nu}\sqrt{q}}\Lambda(1-s,\overline{\chi}),$$

where $\tau(\chi) = \sum_{m=1}^{q} \chi(m) \exp(m/q)$.

Theorem 2.1.6 (Dirichlet's class number formula). The following identity holds for any number field K.

$$h_K = \frac{w_K |d_K|^{1/2}}{2^{r_1(K)+r_2(K)} \pi^{r_2(K)} R_K} \lim_{s\to 1} \frac{\zeta_K(s)}{\zeta(s)},$$

where h_K is the class number, w_K the number of units of finite order of $\mathcal{O}_K$, d_K the fundamental discriminant, r_1 the number of real embeddings, $2r_2$ the number of complex embeddings, R_K the regulator, and $\zeta_K(s)$ the Dedekind zeta function of K.

Remark 2.1.7. If $K = \mathbb{Q}$ or an imaginary quadratic field, $R_K = 1$ by convention.

When K is a quadratic field, $\zeta_K(s) = \zeta(s) L(s, \chi_d)$ with the real primitive Dirichlet character χ_d attached to $\mathbb{Q}(\sqrt{d})$.

Theorem 2.1.8 (Class number formula for quadratic fields). For any quadratic field $\mathbb{Q}(\sqrt{d})$,

$$h(d) = \begin{cases} \frac{\sqrt{|d|}}{\pi} L(1, \chi_d) & \text{if } d < -4, \\ \frac{\sqrt{d}}{2R(d)} L(1, \chi_d) & \text{if } d > 1. \end{cases}$$

The value of Dirichlet L-function at $s = 1$, $L(1, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-1}$ is of main interest. Dirichlet [Dir], who first faced this problem in his work on primes in arithmetic progressions, proved that

$$L(1, \chi_d) > \begin{cases} \pi |d|^{-\frac{1}{2}} & \text{if } d < -4, \\ 2 \log\left(\frac{1}{2}(\sqrt{d-4} + \sqrt{d})\right) d^{-\frac{1}{2}} & \text{if } d > 5, \end{cases}$$

which is immediately followed from Theorem 2.1.8 and $h \geq 1$.

2.2 An upper bound and regulators

Proposition 2.2.1. [Ove14, Proposition 5.3] Let χ and χ_0 be a nonprincipal and principal Dirichlet character modulo q respectively. For $\sigma \geq 1/4$,

$$|L(s,\chi)| \leq 2q(|t|+4)$$

and

$$\left| L(s,\chi_0) - \frac{\phi(q)}{q}\frac{1}{s-1} \right| \leq 2q(|t|+4).$$

This proposition will be used to show Siegel's Theorem 2.4.1. The next result provides better estimates for the special value of $L(s,\chi)$ at $s=1$.

Theorem 2.2.2. For a non-principal Dirichlet character χ modulo $q \geq 3$

$$|L(1,\chi)| \leq \begin{cases} \frac{3}{2}\log q & \text{for a primitive character } \chi, \\ \left(\frac{1}{2}+\sqrt{\frac{8}{3}}\right)\log q & \text{for a non-primitive character } \chi. \end{cases}$$

Proof. Let $A_q(x) = \sum_{n \leq x} \chi(n)$. By Pólya-Vinogradov inequality (cf. [Ove14, Proposition 3.24]),

$$|A_q(x)| < c\sqrt{q}\log q,$$

where $c = 1$ if χ is primitive and $c = \sqrt{8/3}$ otherwise. By partial summation, we have

$$\begin{aligned} L(1,\chi) &= \lim_{x\to\infty} \sum_{n \leq x} \frac{A_q(n)}{n} \\ &= \lim_{x\to\infty} \left(\frac{A_q(x)}{x} + \int_1^x A_q(u)u^{-2} \right) du \\ &= \int_1^\infty A_q(u)u^{-2}du. \end{aligned}$$

Hence we have

$$\begin{aligned}|L(1,\chi)| &\le \int_1^b |A_q(u)|u^{-2}du + \int_b^\infty |A_q(u)|u^{-2}du \\ &\le \int_1^b uu^{-2}du + \int_b^\infty c\sqrt{q}(\log q)u^{-2}du.\end{aligned}$$

If we choose $b = \sqrt{q}$, then $|L(1,\chi)| \le \log\sqrt{q} + c\log q = \left(\frac{1}{2}+c\right)\log q$. $\square$

Corollary 2.2.3. For the regulator $R(d)$ of a real quadratic field $\mathbb{Q}(\sqrt{d})$,

$$R(d) \le \frac{3\sqrt{d}}{4}\log d.$$

In other words, the fundamental unit ε_d has the following upper bound.

$$\varepsilon_d \le \exp\left(3\sqrt{d}/4\right)d.$$

Proof. $R(d) \le h(d)R(d) = \frac{\sqrt{d}}{2}L(1,\chi_d) \le \frac{3\sqrt{d}}{4}\log d$. $\square$

It is natural to ask what are optimal bounds of $L(1,\chi_d)$ and $R(d)$. Under the GRH, Littlewood deduced the following bounds.

Theorem 2.2.4. [Lit28, Theorem 1 and Theorem 2] Assume $L(s,\chi)$ has no zeros in $\sigma > 1/2$.

(1) If χ is a real non-principal character χ modulus q, then as $q \to \infty$

$$\{1+o(1)\}\frac{\pi^2}{12e^\gamma}(\log\log|q|)^{-1} < L(1,\chi) < \{1+o(1)\}2e^\gamma\log\log|q|,$$

where γ is Euler's constant. The right-hand inequality is true also for a complex character if one replaces $L(1,\chi)$ by $|L(1,\chi)|$.

(2) There are infinitely many d such that for χ_d

$$L(1,\chi_d) > \{1+o(1)\}e^\gamma\log\log|d|.$$

(3) There are infinitely many d such that for χ_d

$$L(1,\chi_d) < \{1+o(1)\}\frac{\pi^2}{6e^\gamma}(\log\log|d|)^{-1}.$$

Remark 2.2.5. However, Littlewood gave nothing about the $o(1)$, neither its sign nor the manner in which it approaches zero as a function of d. The statement (3) in Theorem 2.2.4 was later established unconditionally by Chowla [Cho48].

Therefore under the GRH, we expect that the regulator $R(d)$ of a real quadratic field $\mathbb{Q}(\sqrt{d})$ has the following upper bound.

$$R(d) < \{1+o(1)\}2e^\gamma\sqrt{d}\log\log|d|.$$

On the other hand, in view of the Cohen-Lenstra heuristics and some numerical evidence, the following is conjectured.

Conjecture 2.2.6. [JLW95] There exists an infinite set of the prime fundamental radicand $D > 0$ for which

$$R(d) \gg \frac{\sqrt{d}}{\log\log d}.$$

At present the best result of this type is that of Halter-Koch.

Theorem 2.2.7. [HK89] There exists an infinite set of discriminant $d > 0$ of an order of a real quadratic field (not necessarily a fundamental discriminant) such that

$$R(d) \gg \log^4 d.$$

2.3 Siegel zero

To introduce the definition of Siegel zero, we recall a zero-free region for $\zeta(s)$ and $L(s,\chi)$, respectively.

Theorem 2.3.1. There is a constant $c > 0$ such that if $|t| > 2$ and $\zeta(\sigma + it) = 0$ then

$$\sigma < 1 - \frac{c}{\log |t|}.$$

Theorem 2.3.2. There is a constant $c > 0$ such that if $L(\sigma + it, \chi) = 0$ for some primitive complex Dirichlet character χ mod q then

$$\sigma < 1 - \frac{c}{\log q(|t| + 2)}. \tag{2.1}$$

If χ is a real primitive character then (2.1) holds for all zeros of $L(s,\chi)$ with at most one exception. The exceptional zero, if it exists, is real and simple.

Definition 2.3.3. The exceptional zero in Theorem 2.3.2, if it exists, is called Siegel zero (or Landau-Siegel zero).

Remark 2.3.4. Since we can choose constant c arbitrary small in Theorem 2.3.2 and Definition 2.3.3, if Siegel zero exists then there must be infinitely many Siegel zeros and the corresponding $\mathbb{Q}(\sqrt{d})$. As in [HB83], the meaning of Siegel zeros is to be as follows: there is a sequence of d_j's, $|d_j| \to \infty$, and corresponding Siegel zeros β_j of $L(s, \chi_d)$ with $(1 - \beta_j) \log |d_j| \leq \epsilon_0$, for some fixed positive ϵ_0.

We expect that there is no such zero by the Generalized Riemann Hypothesis (GRH for short), which is the conjecture that each nontrivial zero of an L-series associated to a primitive Dirichlet character χ has real part $1/2$. The nonexistence of Siegel zero, though much weaker than the GRH, is not yet proved. But we can still obtain some strong restrictions on how Siegel zeros can vary with q and χ. Siegel zeros cannot occur even for characters of different moduli if we set the threshold low enough:

Theorem 2.3.5. [Lan18] There is a constant $c > 0$ such that, for any distinct primitive real characters χ_1, χ_2 to (not necessarily distinct) moduli q_1, q_2 at most one of $L(s, \chi_1)$ and $L(s, \chi_2)$ has an exceptional zero $\beta > 1 - \frac{c}{\log q_1 q_2}$. In particular, for each q there is at most one real character mod q whose L-series has an exceptional zero $\beta > 1 - (c/\log q)$.

2.4 Ineffective lower bounds

2.4.1 Siegel-Tazuzawa theorem

In this section we introduce one of the simplest proofs of Siegel's theorem due to Goldfeld [Gol74] and see what leads to a noneffective result.

Theorem 2.4.1. [Sie35] Given $0 < \epsilon < \frac{1}{2}$, there is $c(\epsilon) > 0$ which is ineffective such that

$$L(1, \chi_d) \geq c(\epsilon) \cdot |d|^{-\epsilon}.$$

Proof. Suppose that χ and χ_1 are primitive quadratic characters to distinct moduli q, q_1 respectively ($q > q_1$). Let

$$F(s) = \zeta(s) L(s, \chi_1) L(s, \chi) L(s, \chi_1 \chi) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

Since all the Dirichlet coefficients of

$$\log\left(F(s)\right) = \sum_p \sum_{k=1}^{\infty} \frac{1}{k} \left(1 + \chi_1(p^k) + \chi(p^k) + \chi_1(p^k)\chi(p^k)\right) p^{-ks}$$

are nonnegative, $a_n \geq 0$.

Let $P(s) = s(s+1)(s+2)(s+3)(s+4)(s+5)$ and let $1/2 < \alpha < 1$. By the weighted version of the Perron formula (cf. [Ove14, p. 161]),

$$\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} F(s+\alpha)\frac{x^{s+5}}{P(s)}ds = \sum_{n<x}(x-n)^5 a_n n^{-\alpha} \geq (x-1)^5.$$

By the residue theorem,

$$\begin{aligned}
& L(1,\chi_1)L(1,\chi)L(1,\chi_1\chi)\frac{x^{1-\alpha}}{P(1-\alpha)} + \frac{F(\alpha)}{120} + \frac{1}{2\pi i}\int_{-\alpha/2-i\infty}^{-\alpha/2+i\infty} F(s+\alpha)\frac{x^s}{P(s)}ds \\
= & \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} F(s+\alpha)\frac{x^s}{P(s)}ds \\
\geq & \frac{(x-1)^5}{x^5}.
\end{aligned}$$

By Proposition 2.2.1, $F(s) = O\left(q_1^2 q^2(|t|+4)^4\right)$ in the region: $\sigma \geq 1/4$ and $|s-1| > \epsilon_0 > 0$. Since the degree of the polynomial $P(s)$ is 6, we have

$$L(1,\chi_1)L(1,\chi)L(1,\chi_1\chi)\frac{x^{1-\alpha}}{P(1-\alpha)} + \frac{F(\alpha)}{120} + O\left(q_1^2 q^2 x^{-\alpha/2}\right) \geq \frac{(x-1)^5}{x^5}.$$

By Theorem 2.2.2, $L(1,\chi_1)L(1,\chi_1\chi) \ll \log q_1 (\log q_1 + \log q)$.

Now we suppose $F(\alpha) \leq 0$ for some $\chi_1 \pmod{q_1}$ and some $1-\delta < \alpha < 1$ ($\delta > 0$ will be determined later). Then for sufficiently large c defined by $x = (cq^4)^{2/\alpha}$,

$$L(1,\chi)(\log q)^2(cq^4)^{2(1-\alpha)/\alpha} \gg 1.$$

Since $0 < \frac{8(1-\alpha)}{\alpha} < \frac{8\delta}{1-\delta}$, if we choose δ sufficiently small then for any $\epsilon > 0$ we can force

$$L(1,\chi) \gg q^{-\epsilon}.$$

For an imprimitive character $\chi' \pmod{q'}$ induced by a primitive character $\chi \pmod{q}$,

$$L(1,\chi') = L(1,\chi)\prod_{p|q'}(1-\frac{\chi(p)}{p}) \gg q^{-\epsilon}\prod_{p\le q'}(1-p^{-1}).$$

By the Mertens formula (cf. [Ove14, Proposition 1.11]),

$$L(1,\chi') \gg q^{-\epsilon}\frac{1}{\log q'} \gg (q')^{-2\epsilon} = (q')^{-\epsilon'}.$$

Now it suffices to show that there are χ_1 and α such that $1-\delta < \alpha < 1$ and $F(\alpha) \le 0$. If there is no Siegel zero, we choose some arbitrary real primitive character χ_1 modulo some $q_1 \ge 3$. In this case $L(\alpha,\chi_1)$, $L(\alpha,\chi)$ and $L(\alpha,\chi_1\chi)$ are positive for any α with $1-\delta < \alpha < 1$. Since $\zeta(\alpha)$ is negative, $F(\alpha) \le 0$. In the other case there exists a real primitive character χ_1 with modulo $q_1 \ge 3$ such that $L(\beta,\chi_1) = 0$ (so $F(\beta) = 0$) for Siegel zero β with $1-\delta < \beta < 1$. We have no way to estimate this modulus q_1 and so the result of the latter case become ineffective. □

A lower bound of $L(1,\chi_d)$ can be deduced immediately from an estimate of a Siegel zero β by the following lemma due to Tatuzawa.

Lemma 2.4.2. [Tat51, Lemma 8] Let $0 < \epsilon < 1/2$. If $L(s,\chi)$ has no real zero β in the interval $1-\epsilon/4 < \beta < 1$ then

$$L(1,\chi) \ge 0.376\frac{\epsilon}{|d|^{\epsilon}}.$$

Tatuzawa used Theorem 2.3.5 and Lemma 2.4.2 to show the following theorem. The above proof of Theorem 2.4.1 was further developed by Hoffstein [Hof80] to yield a simple proof of the following theorem, too.

Theorem 2.4.3. [Tat51, Theorem 2] Let $0 < \epsilon < \frac{1}{2}$ and $|d| \ge \max\{e^{\frac{1}{\epsilon}}, e^{11.2}\}$. Then

$$L(1,\chi_d) \ge 0.655\epsilon \cdot |d|^{-\epsilon}$$

with one possible exception.

Remark 2.4.4. Hecke's conditionally effective result assuming nonexistence of Siegel zero (published by Landau [Lan18]), can be obtained by Lemma 2.4.2 with substituting ϵ with $4c/\log|d|$, where c is in Theorem 2.3.2. Also, under the assumption that there is no Siegel zero, one exception in Theorem 2.4.3 can be removed.

2.4.2 Sarnak-Zaharescu theorem

Assuming that all the zeros of the L-functions are either real or lie on the critical line (Hypothesis **H**), Sarnak and Zaharescu [SZ02] improved results on Siegel zero and established a better lower bound for $L(1,\chi_d)$. We will state Hypothesis **H** separately depending on the L-functions in questions:

(1) Hypothesis $\mathbf{H}_1$: All the zeros of $L(s,\chi_d)$ are either on the line $\mathrm{Re}(s) = 1/2$ or are real.

(2) Hypothesis $\mathbf{H}_2$: Not only $\mathbf{H}_1$, but also all the zeros of the $L(E\otimes\chi_d, s)$ are either on the line $\mathrm{Re}(s) = 1$ or are real.

Remark 2.4.5. Hypothesis $\mathbf{H_1}$ (Hypothesis $\mathbf{H_2}$) is a weak form of the Generalized Riemann Hypothesis (Grand Riemann Hypothesis, respectively), excluding the assumption for real zeros. On the other hands, there are some reasons to accept Hypothesis **H**. For example, **H** is true for the Selberg zeta function for a lattice Γ in $\mathrm{SL}(2,\mathbb{R})$, and some authors have studied the zeros of $\zeta(s)L(s,\chi_d)$ differently according to real zeros and complex zeros.

Theorem 2.4.6. [SZ02, Theorem 1] Assume Hypothesis $\mathbf{H}_1$. Then for any $\epsilon > 0$ there exists a constant $c(\epsilon) > 0$ (ineffective) such that

$$L(1,\chi_d) \geq \frac{c(\epsilon)}{(\log|d|)^{\epsilon}}.$$

Theorem 2.4.7. [SZ02, Theorem 3] Assume Hypothesis $\mathbf{H}_2$. Given an elliptic curve E over $\mathbb{Q}$ of which the L-function has a zero of order g at $s = 1$, for any $\epsilon > 0$ there is an effective constant $c(E, \epsilon) > 0$ such that

$$L(1, \chi_d) \geq \frac{c(E, \epsilon)}{|d|^{(2+\epsilon)/(g+1)}}.$$

2.4.3 A table

We give a table of lower bounds for $L(1, \chi_d)$ in growth rate order, including Goldfeld's result and Oesterlé's which we introduced in chapter 1. The following table implies that for sufficiently large d

$$L(1, \chi_d) \geq \text{contant} \times \text{growth rate},$$

for each item.

Growth rate	Constant	Condition	Due to
$\frac{1}{(\log\|d\|)^{\epsilon_1}}$	Conditionally ineffective, $c(\epsilon_1)$	The Generalized RH except real zeros	Sarnak, Zaharescu
$\frac{1}{\log\|d\|}$	Conditionally effective, c	No Siegel zero	Hecke
$\frac{1}{\|d\|^{\epsilon_2}}$	Ineffective, $c(\epsilon_2)$		Siegel
$\frac{1}{\|d\|^{\epsilon_2}}$	$0.665\epsilon_2 \quad \|d\| \geq d(\epsilon_2)$	At most one exception	Tatuzawa
$\frac{1}{\|d\|^{(2+\epsilon_1)/(g+1)}}$	Conditionally effective, $c(E)$	The Grand RH except real zeros, ($\exists\ E/\mathbb{Q}$ s.t. $g \gg 1$)	Sarnak, Zaharescu
$\frac{(\log\|d\|)^{g-3-\epsilon_1}}{\|d\|^{1/2}}$	Effective, $c(E)$	($\exists\ E/\mathbb{Q}$ s.t. $g \gg 1$)	Goldfeld
$\frac{\log\|d\|\cdot\theta(d)}{\|d\|^{1/2}} \quad d < 0$	$\pi/55 \ \ (d, 5077) = 1$, or $1/7000$		Oesterlé
$\pi\|d\|^{-1/2} \quad d < -4$ $(\log(d-4))\, d^{-1/2} \quad d > 5$	1		Dirichlet

where any $\epsilon_1 > 0$ and $0 < \epsilon_2 < \frac{1}{2}$, $d(\epsilon_2) = \max\{e^{\frac{1}{\epsilon}}, e^{11.2}\}$, g is the analytic rank of an elliptic curve over $\mathbb{Q}$, $\theta(d) = \prod_{p \in P(d)} \left(1 - \frac{\lfloor 2\sqrt{p} \rfloor}{p+1}\right)$, and $P(d)$ is the set of prime divisors of d except maximal one.

2.5 Real quadratic fields of Richaud-Degert type

In the section 2.2, we introduced the two unsolved questions regarding the regulator $R(d)$ of $\mathbb{Q}(\sqrt{d})$ with $d > 0$:

(1) What is the largest value that $R(d)$ can attain as a function of d?

(2) How often does $R(d)$ become that large?

Now we restrict real quadratic fields to be of certain forms, so that we avoid difficulty of the regulator. Recall that for $K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{D})$, the fundamental discriminant d and the fundamental radicand D have the following relation:

$$d = 4D/\sigma^2,$$

where

$$\begin{cases} \sigma = 2 & \text{if } D \equiv 1 \pmod 4, \\ \sigma = 1 & \text{otherwise.} \end{cases}$$

Definition 2.5.1. Let $D = n^2 + r \neq 5$ be a square-free positive integer such that

$$r \mid 4n \quad \text{and} \quad -n < r \leq n.$$

The real quadratic field $K = \mathbb{Q}(\sqrt{D})$ is called a real quadratic field of Richaud-Degert (R-D for short) type. Specially, if $|r| \in \{1, 4\}$ then K is of narrow R-D type. Otherwise, it is of wide R-D type.

Theorem 2.5.2. [Deg58, Satz 1 and Satz 2] Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic field of R-D type. Then the fundamental unit ε and its norm are given as follows:

$$\begin{cases} \varepsilon = n + \sqrt{n^2 + r}, & N(\varepsilon) = -\mathrm{sgn}(r) \quad \text{if } |r| = 1, \\ \varepsilon = (n + \sqrt{n^2 + r})/2, & N(\varepsilon) = -\mathrm{sgn}(r) \quad \text{if } |r| = 4, \\ \varepsilon = (2n^2 + r)/|r| + 2n\sqrt{n^2 + r}/|r|, & N(\varepsilon) = 1 \qquad\qquad\ \ \text{if } |r| \neq 1, 4. \end{cases}$$

By theorem 2.4.3 and theorem 2.5.2, in the 1980's Mollin and Williams made a list of R-D types of various class numbers, and showed that the list is complete with one possible GRH-ruled out exception (cf. [Mol96]). Some of these lists have been unconditionally verified. In 2007, for example, Byeon, Kim, and Lee [BKL07] classified all real quadratic fields of narrow R-D types with class number one.

Chapter 3

The L-function attached to an elliptic curve

3.1 The Hasse-Weil L-function

We begin by defining the incomplete L-function, which omits the finitely many places at which E has bad reduction. Also, we introduce isogeny theorem to explain that the incomplete L-function determines E up to isogeny over K. We then define the global Hasse-Weil L-function and the complete L-function, and describe its analytic properties.

Let E be an elliptic curve over a number field K and let its Weierstrass equation

$$y^2 + c_1xy + c_3y = x^3 + c_2x^2 + c_4x + c_6,$$

with $c_i \in K$. Let S be the finite set of places of K consisting of the infinite places and the places where E has bad reduction. For all places $\nu \notin S$, there is a model of E such that the coefficients c_i lie in the local ring $\mathcal{O}_\nu$ at ν and the discriminant $\triangle_\nu$ is a unit in $\mathcal{O}_\nu$. Let π_ν be a uniformizing element in $\mathcal{O}_\nu$ and let $\mathcal{O}_\nu/\pi_\nu\mathcal{O}_\nu = \mathbb{F}_\nu$ be the residue field, of cardinality q_ν. For $\nu \notin S$, we gat an elliptic curve $\widetilde{E}_\nu$ over the residue field $\mathbb{F}_\nu$. The formal local L-factor at v with $v \notin S$, is

$$L_v(E/K, s) = L(\widetilde{E}_v/\mathbb{F}_v, q_v^{-s}) = (1 - a_v q_v^{-s} + q_v^{1-2s})^{-1},$$

where $\#\widetilde{E}_v(\mathbb{F}_v) = 1 + q_v - a_v$.

Definition 3.1.1. The incomplete L-function of E is

$$L_S(E/K, s) = \prod_{v \notin S} L_v(E/K, s). \tag{3.1}$$

Conversely, the formal Euler product (3.1) determines E up to isogeny over K for the following reasons. We denote by $T_l(E)$ the l-adic Tate module which is defined to be

$$T_l(E) := \varprojlim_n E[l^n],$$

with respect to the maps

$$E[l^{n+1}] \xrightarrow{\times l} E[l^n], \quad P \mapsto lP.$$

We denote by $V_l(E)$ the rational Tate module, which is defined by

$$V_l(E) := T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l = T_l(E)[\tfrac{1}{l}].$$

Then $T_l(E)$ is a free $\mathbb{Z}_l$-module and $V_l(E) \cong \mathbb{Q}_l^2$ as a $\mathbb{Q}_l$-vector space. The absolute Galois group $G_K = \mathrm{Gal}(K^s/K)$ acts on $V_l(E)$, and this action induces the l-adic representation:

$$\rho_{E,l} : G_K \to \mathrm{Aut}(V_l(E)) \cong \mathrm{GL}_2(\mathbb{Q}_l).$$

Theorem 3.1.2 (Faltings, 1988)**.** Let K be a number field and let $G_K = \mathrm{Gal}(K^s/K)$. If A and B are two abelian varieties over K, then the natural

map
$$\mathrm{Hom}_K(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to \mathrm{Hom}_{G_K}(T_l(A), T_l(B))$$
is an isomorphism

In short, Faltings's isogeny theorem reduces a geometric problem to a problem in terms of Galois representations. We list some consequences of the theorem.

Proposition 3.1.3. Let E_1 and E_2 be elliptic curves over a number field K. Then the following are equivalent:

(1) E_1 and E_2 are isogenous over K,

(2) For all prime l not dividing $v \in S$, $V_l(E_1) \cong V_l(E_2)$ as G_K-modules,

(3) For some prime l not dividing $v \in S$, $V_l(E_1) \cong V_l(E_2)$ as G_K-modules,

(4) $L_v(E_1, s) = L_v(E_2, s)$ for all places $v \notin S$ of K,

(5) $L_v(E_1, s) = L_v(E_2, s)$ for almost all places $v \notin S$ of K.

For the L-function to have a meromorphic continuation to the whole of $\mathbb{C}$ and satisfy a functional equation, we must add some factors to the incomplete L-function, corresponding to the infinite places and the finite places of bad reduction. For finite $v \in S$, we define the local L-factor

$$L_v(E/K, s) = \begin{cases} 1 & \text{if } E \text{ has additive reduction at } v; \\ (1 - q_v^{-s})^{-1} & \text{if } E \text{ has split multiplicative reduction at } v; \\ (1 + q_v^{-s})^{-1} & \text{if } E \text{ has non-split multiplicative reduction at } v. \end{cases}$$

We can define the Hasse-Weil L-function as follows.

Definition 3.1.4. The Hasse-Weil L-function of E/K is

$$L(E/K, s) = L_S(E/K, s) \prod_{\substack{v \in S, \\ v \nmid \infty}} L_v(E/k, s) = \prod_{v \nmid \infty} L_v(E/k, s).$$

Adding factors at the infinite places, the completed Hasse-Weil L-function is

$$\Lambda(E/K, s) = \left((2\pi)^{-s}\Gamma(s)\right)^{[K:\mathbb{Q}]} L(E/K, s).$$

The following two quantities measure bad reduction.

Definition 3.1.5. The minimal discriminant of an elliptic curve E over a number field K is the integral ideal of K defined by

$$\mathcal{D}_{E/K} = \prod_{v \nmid \infty} \mathfrak{p}_v^{v(\triangle_v)}$$

where $\triangle_v$ is the discriminant of a minimal equation for E/K_v and $\mathfrak{p}_v$ is the prime ideal associated to the finite place v.

Definition 3.1.6. The conductor of E is the integral ideal given by

$$N_{E/K} = \prod_{v \nmid \infty} \mathfrak{p}_v^{f_v},$$

where

$$f_v = \begin{cases} 0 & \text{if } E \text{ has good reduction at } v; \\ 1 & \text{if } E \text{ has multiplicative reduction at } v; \\ 2 + \delta_v & \text{if } E \text{ has additive reduction at } v, \end{cases}$$

where δ_v is a non-negative integer depending on the action of wild inertia at v on $T_l(E)$. It is zero whenever the characteristic of v is not equal to 2 or 3.

Remark 3.1.7. In fact, the conductor of E is the Artin conductor of the Tate module of E. It is related to $\mathcal{D}_{E/K}$ by Ogg's formula

$$f_v = \mathrm{ord}_v(\mathcal{D}_{E/K}) + 1 - m_v,$$

where m_v is the number of irreducible components of the Néron model of E at v. (cf. [Sil94, Chapter 4, Section 11])

Conjecture 3.1.8. Let K be a number field, and E/k an elliptic curve. Then the complex analytic function $\Lambda(E/K, s)$ on the right half plane $\mathrm{Re}(s) > 3/2$ admits an analytic continuation to the entire complex plane and satisfies the functional equation

$$\Lambda(E/K, s) = \pm A^{1-s}\Lambda(E/K, 2-s)$$

where A is the product of the absolute norm of conductor $N_{E/K}$ with the square of the discriminant of K.

Wiles and Taylor [TW95, Wil95] proved this conjecture in the case when $K = \mathbb{Q}$ and the conductor $N_{E/K}$ is square-free. In [BCDT01], their methods were extended to cover all elliptic curves over. Some other cases when K is a totally real number field are known.

3.2 The conjecture of Birch and Swinnerton-Dyer

Conjecture 3.2.1 (Birch and Swinnerton-Dyer)**.** Let E/K be an elliptic curve over a number field, and assume that $L(E/K, s)$ has a meromorphic continuation to a neighborhood of the point $s = 1$.

(1) BSD rank conjecture: If n is the algebraic rank of $E(K)$, then

$$\mathrm{ord}_{s=1} L(E/K, s) = n.$$

(2) Strong BSD conjectrue: Let $c(E/K)$ be the leading term in the Taylor expansion at $s = 1$, that is,

$$L(E/K, s) \sim c(E/K) \cdot (s-1)^n \quad \text{as} \quad s \to 1.$$

Then

$$c(E/K) = P(E/K) \cdot R(E/K) \cdot \#Ш(K, E),$$

where

(a) the period of E/K, $P(E/K)$ is defined by

$$P(E/K) = \prod_{v \nmid \infty} \left(L_v(E/K, 1) \cdot \int_{E(K_v)} |\omega_v| \right) \cdot \prod_{v \mid \infty} \int_{E(K_v)} |\omega_v|,$$

with a non-zero invariant differential ω on E/K,

(b) the regulator of E/K, $R(E/K)$ is defined by

$$R(E/K) = \det(\langle P_i, P_j \rangle)/I^2,$$

with the Néron-Tate height $\langle\, , \rangle : E(K) \times E(K) \to \mathbb{R}$, a basis of free part of the Hasse-Weil group $\{P_i\}_{i=1}^n$, and $I = [E(K) : \langle P_1, \cdots, P_n \rangle]$,

(c) the Tate-Shafarevich group, $Ш(K, E)$ is defined by

$$Ш(K, E) = \ker \left(H^1(K, E) \to \prod_v H^1(K_v, E) \right)$$

(for detail, see [Gro11]).

3.3 An elliptic curve with complex multiplication

3.3.1 The Grössencharakter

Let $\mathfrak{m}$ be an integral ideal of the number field K, and let $J^{\mathfrak{m}}$ be the group of all non-zero fractional ideals of K which are relatively prime to $\mathfrak{m}$. Searching for the most comprehensive class of characters $\chi : J^{\mathfrak{m}} \to S^1$ for which the corresponding L-series could have a functional equation, Hecke was led to the notion of a Grössencharakter mod $\mathfrak{m}$.

We introduce the sets

$$K^{(\mathfrak{m})} = \{a \in K^{\times} \mid (a, \mathfrak{m}) = 1\},$$

$$K^{\mathfrak{m}} = \{a \in K^{\times} \mid a \equiv 1 \pmod{\mathfrak{m}}\},$$

$$\mathcal{O}^{(\mathfrak{m})} = \{a \in \mathcal{O}^{\times} \mid (a, \mathfrak{m}) = 1\},$$

and

$$\mathcal{O}^{\mathfrak{m}} = \{a \in \mathcal{O}^{\times} \mid a \equiv 1 \pmod{\mathfrak{m}}\}.$$

We denote by $\mathbf{R}$ the Minkowski space, which is

$$\mathbb{R} \otimes_{\mathbb{Q}} K \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

in the usual way (cf. [Neu99, Chapter 1, Section 5]).

Definition 3.3.1. A Grössencharakter mod $\mathfrak{m}$ is a character $\chi : J^{\mathfrak{m}} \to S^1$ which there exists a pair of characters (i.e., a continuous homomorphism)

$$\chi_f : (\mathcal{O}/\mathfrak{m})^{\times} \to S^1, \quad \chi_{\infty} : \mathbf{R}^{\times} \to S^1$$

such that

$$\chi(\langle a \rangle) = \chi_f(a)\chi_{\infty}(a)$$

for any $a \in \mathcal{O}^{(\mathfrak{m})}$.

Remark 3.3.2. The following can be deduced easily:

(1) A finite component $\chi_f : (\mathcal{O}/\mathfrak{m})^{\times} \to S^1$ is a character of a finite abelian group and so $\chi_f(a) = 1$ when $a \in \mathcal{O}^{\mathfrak{m}}$.

(2) An infinite component $\chi_{\infty} : \mathcal{O}^{\times} \to S^1$ that deals with contributions from the units $\mathcal{O}^{\times}$, under the map j from $K^{\times}$ to the multiplicative Minkowski space $\mathbf{R}^{\times}$.

(3) For $a \in \mathcal{O}^\times$, $\chi_f(a)\chi_\infty(a) = \chi(\langle a \rangle) = 1$.

(4) $\mathcal{O}^\mathfrak{m} \subset \mathcal{O}^\times$ and for $a \in \mathcal{O}^\mathfrak{m}$, $\chi_\infty(a) = \chi_f(a)\chi_\infty(a) = \chi(\langle a \rangle) = 1$. Hence $\chi_\infty : \mathbf{R}^\times/\mathcal{O}^\mathfrak{m} \to S^1$.

(5) For $a \in K^\mathfrak{m}$ (i.e., $a = b/c$ with $b, c \in \mathcal{O}^{(\mathfrak{m})}$, $b \equiv c \bmod \mathfrak{m}$), $\chi_\infty(a) = \chi(\langle a \rangle)$ and $K^\mathfrak{m}$ is dense in $\mathbf{R}^\times$. Hence χ_∞ is determined uniquely by χ (and so is χ_f).

The infinite components can be given explicitly as follows. The multiplicative Minkowski space is written by

$$\mathbf{R}^\times \cong (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2},$$

via the map $x = (x_\tau)_\tau \mapsto ((x_\rho), (x_\sigma)_\sigma)$. The characters of

$$(\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} \cong (\{\pm 1\} \times \mathbb{R}_{>0})^{r_1} \times (S^1 \times \mathbb{R}_{>0})^{r_2}$$

have the form

$$(x_1, \cdots, x_{r_1+r_2}) \mapsto \prod_{j=1}^{r_1+r_2} \left(\frac{x_j}{|x_j|} \right)^{p_j} |x_j|^{iq_j},$$

where

$$p_j \in \begin{cases} \{0, 1\}, & \text{when } j = 1, \cdots, r_1, \\ \mathbb{Z}, & \text{when } j = r_1 + 1, \cdots, r_1 + r_2, \end{cases}$$

and $q_j \in \mathbb{R}$ for each $j = 1, \cdots, r_1 + r_2$. Hence every χ_∞ is in the form

$$x = (x_\tau)_\tau \mapsto N\left(\left(\frac{x}{|x|} \right)^p |x|^{iq} \right),$$

where $p \in \prod_\tau \mathbb{Z}$ and $q \in \prod_\tau \mathbb{R}$ such that:

(1) $p_\rho = 0, 1$ for all ρ, and $p_\sigma p_{\overline{\sigma}} = 0$ for all σ, and

(2) $q_\sigma q_{\overline{\sigma}} = 0$ for all σ.

Such an element is called admissible. Then we say that χ is of type (p, q), and we call $p - iq$ the exponent of the Grössencharakter χ.

3.3.2 The Hecke L-function

We may assume that χ is a primitive Grössencharakter mod $\mathfrak{m}$, i.e., that the corresponding finite component χ_f of $(\mathcal{O}/\mathfrak{m})^*$ is primitive. The L-series of an arbitrary character differs from the L-series of the corresponding primitive character only by finitely many Euler factors. So analytic continuation and functional equation of one follow from those of the other.

The L-function of the $G(\mathbb{C}|\mathbb{R})$-set $X = \mathrm{Hom}(K, \mathbb{C})$ is defined by

$$L_X(s\mathbf{1}) = L_{\mathbb{R}}(s)^{r_1} L_{\mathbb{C}}(s)^{r_2},$$

with $\mathbf{1} = (1, \cdots, 1)$ where the number of 1 is $n = \#X$, i.e., the degree of $K/\mathbb{Q}$, and

$$\begin{aligned} L_{\mathbb{R}}(s) &= \pi^{-s/2}\Gamma(s/2) = L_Y(s) \quad \text{if } Y = \{\rho\}, \\ L_{\mathbb{C}}(s) &= 2(2\pi)^{-s}\Gamma(s) = L_Y(s) \quad \text{if } Y = \{\sigma, \overline{\sigma}\}. \end{aligned}$$

Recall that an infinite comoponent χ_∞ of $\mathbf{R}^*$ is given as

$$\chi_\infty(x) = N\left(x^p|x|^{-p+iq}\right),$$

for an admissible (p, q) with $p \in \prod_\tau \mathbb{Z}$ and $q \in \prod_\tau \mathbb{R}$. Let

$$L_\infty(\chi, s) = L_X(s\mathbf{1} + p - iq).$$

Let $\Lambda(\chi, s)$ be the completed Hecke L-series which is defined to be

$$\Lambda(s, \chi) = (|d_K|N(\mathfrak{m}))^{s/2} L_\infty(s, \chi)L(s, \chi).$$

Theorem 3.3.3. Let χ be a primitive Grössencharakter mod $\mathfrak{m}$ of a number field K. Then the function

$$\Lambda(s,\chi) = (|d_K| N(\mathfrak{m}))^{s/2} L_\infty(s,\chi) L(s,\chi), \quad \mathrm{Re}(s) > 1,$$

has a meromorphic continuation to the complex plane $\mathbb{C}$ and satisfies the functional equation

$$\Lambda(s,\chi) = W(\chi)\Lambda(1-s,\bar{\chi}),$$

where $|W(\chi)| = 1$. It is holomorphic on all of $\mathbb{C}$, if $\mathfrak{m} \neq 1$ or $p \neq 0$.

3.3.3 Deuring's theorem

Theorem 3.3.4 (Deuring)**.** Let E/F be an elliptic curve with complex multiplication by the ring of integers $\mathcal{O}_K$ of imaginary quadratic field K.

(1) Assume that K is contained in F. Then

$$\widetilde{L}(E/F,s) = L(s,\psi_F)L(s,\overline{\psi_F})$$

for some primitive Grössencharakter ψ_F of F,

(2) Assume that K is not contained in F, and let $F' = FK$. Then

$$\widetilde{L}(E/F,s) = L(s,\psi_{F'})$$

for some primitive Grössencharakter $\psi_{F'}$ of F',

where $\widetilde{L}(E/F,s)$ is the normalized Hasse-Weil L-function such that the critical line is $s = 1/2$.

In the case of an elliptic curve $E/\mathbb{Q}$ with complex multiplication by the ring of integers $\mathcal{O}_K$ of imaginary quadratic field K,

$$L(E/\mathbb{Q},s) = L(s,\psi) \tag{3.2}$$

for a primitive Grössencharakter (quasi-character) ψ mod $\mathfrak{f}$ of some normalized ψ_K.

For $X = \mathrm{Hom}(K, \mathbb{C})$, $r_1 = 0$ and $r_2 = 1$. If $\psi : J^{\mathfrak{f}} \to S^1$ is a Grössencharakter then for $a \in K^{\mathfrak{f}}$,

$$\psi_K(\langle a \rangle) = \psi_{K,f}(a)\psi_{K,\infty}(a) = \psi_{K,\infty}\big((a_\sigma)_\sigma\big)$$

and

$$\psi_{K,\infty}\big((a_\sigma)_\sigma\big) = N\left(\left(\frac{a_\sigma}{|a_\sigma|}\right)^p |a_\sigma|^{iq}\right) = a^p|a|^{iq-p},$$

for some $p = p_\sigma \in \mathbb{Z}$ and $q = q_\sigma \in \mathbb{R}$. Since the left-hand side in (3.2) has the Dirichlet series with rational coefficients, $q = 0$. In this case, there is a functional equation given by

$$\Lambda(s, \chi) = W(\chi)\Lambda(1 + p - s, \overline{\chi}),$$

which implies that the integer p must be equal to one and

$$\psi(\langle a \rangle) = a \quad \text{for } a \in K^{\mathfrak{f}}.$$

In short, the Grössencharakter attached to an elliptic curve over $\mathbb{Q}$ with CM must be of type $(1, 0)$.

3.3.4 Theory of complex multiplication

Let K be an imaginary quadratic field, let $\mathrm{Cl}(K)$ be the class group of K, and let h_K be the class number of K. We will see that if E is an elliptic curve with CM by $\mathcal{O}_K$, then $j(E)$ generates the Hilbert class field of K. Let

$$\mathcal{E}_{\mathbb{C}}(K) = \{\mathbb{C}\text{-isomorphism classes of elliptic curves over } \mathbb{C} \text{ with CM by } \mathcal{O}_K\}.$$

There is a well-defined map

$$\begin{aligned} \mathrm{Cl}(\mathsf{K}) &\to \mathcal{E}_{\mathbb{C}}(\mathsf{K}) \\ [\mathfrak{a}] &\mapsto \mathbb{C}/\mathfrak{a}. \end{aligned}$$

Let

$\mathcal{E}_{\bar{\mathbb{Q}}}(\mathsf{K}) = \{\bar{\mathbb{Q}}$-isomorphism classes of elliptic curves over $\mathbb{C}$ with CM by $\mathcal{O}_{\mathsf{K}}\}$.

Then there is a natural map $\mathcal{E}_{\bar{\mathbb{Q}}}(\mathsf{K}) \to \mathcal{E}_{\mathbb{C}}(\mathsf{K})$.

Lemma 3.3.5. The above two maps are bijective.

Now we simply write $\mathcal{E}(\mathsf{K})$ and we define an action of $\mathrm{Cl}(\mathsf{K})$ on $\mathcal{E}(\mathsf{K})$. Let $[\mathfrak{a}] \in \mathrm{Cl}(\mathsf{K})$ and let $\mathbb{C}/\mathfrak{b} \in \mathcal{E}(\mathsf{K})$ for a fractional ideal $\mathfrak{b}$ of K. Set

$$[\mathfrak{a}] \cdot \mathbb{C}/\mathfrak{b} = \mathbb{C}/(\mathfrak{a}^{-1}\mathfrak{b}).$$

By the above lemma, this action is transitive.

For each $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathsf{K})$ there is a unique ideal class $[\mathfrak{a}] \in \mathrm{Cl}(\mathsf{K})$ such that $\mathsf{E}^{\sigma} \cong [\mathfrak{a}] \cdot \mathsf{E}$. This defines a map

$$\mathsf{S} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathsf{K}) \to \mathrm{Cl}(\mathsf{K}).$$

Theorem 3.3.6. Let E be an elliptic curve with CM by $\mathcal{O}_{\mathsf{K}}$. Suppose that $\mathsf{E} = \mathsf{E}_1, \mathsf{E}_2, \cdots \mathsf{E}_{h_{\mathsf{K}}}$ is a complete set of representatives of $\mathcal{E}(\mathsf{K})$. Then

(1) $\mathsf{H} = \mathsf{K}(\mathsf{j}(\mathsf{E}))$ is the Hilbert class field of K,

(2) $[\mathbb{Q}(\mathsf{j}(\mathsf{E})) : \mathbb{Q}] = [\mathsf{K}(\mathsf{j}(\mathsf{E})) : \mathsf{K}] = h_{\mathsf{K}}$,

(3) $\mathsf{j}(\mathsf{E}_1), \cdots, \mathsf{j}(\mathsf{E}_{h_{\mathsf{K}}})$ is a complete set of conjugates for $\mathsf{j}(\mathsf{E})$.

(4) (Reciprocity Law) Let $j(\mathfrak{c}) := j(\mathbb{C}/\mathfrak{c})$ for a fractional ideal $\mathfrak{c}$ of K. If $\mathfrak{a}$ and $\mathfrak{b}$ are fractional ideals of K then

$$j(\mathfrak{b})^{(\mathfrak{a},H/K)} = j(\mathfrak{a}^{-1}\mathfrak{b})$$

(for detail, see [Gha03]).

Remark 3.3.7. More generally if E is an elliptic curve with End(E) an arbitrary order of K then it turns out that $j(E)$ generates a (not necessarily unramified) abelian extension of K.

3.4 The symmetric square L-function attached to an elliptic curve

3.4.1 The primitive symmetric square L-function

Let E be an elliptic curve over $\mathbb{Q}$ with conductor N and let $\tilde{L}(E/\mathbb{Q}, s)$ be the normalized Hasse-Weil L-function such that its critical line is $s = 1/2$. We write the Euler product of $\tilde{L}(E/\mathbb{Q}, s) = L(E/\mathbb{Q}, s + 1/2)$ as follows:

$$\begin{aligned}
\tilde{L}(E/\mathbb{Q}, s) &= \sum_{n=1}^{\infty} \frac{a_n(E)}{n^s} \\
&= \prod_p (1 - a_p(E)p^{-s} + 1_N(p)p^{-2s})^{-1} \\
&= \prod_p (1 - \alpha_p p^{-s})^{-1}(1 - \beta_p p^{-s})^{-1},
\end{aligned}$$

where

$$\begin{cases}
\text{for } \ p \nmid N, & \alpha_p + \beta_p = a_p(E), \ \ |\alpha_p| = |\beta_p| = 1, \ \ \alpha_p = \bar{\beta}_p, \\
\text{for } \ p \parallel N, & \alpha_p = \pm\frac{1}{\sqrt{p}}, \ \ \beta_p = 0, \\
\text{for } \ p^2 \mid N, & \alpha_p = \beta_p = 0.
\end{cases}$$

We denote by $L(\mathrm{Sym}_i^2 E, s)$ an imprimitive (normalized) symmetric square L-function associated to $E/\mathbb{Q}$, which is defined as follows.

Definition 3.4.1.

$$\begin{aligned} L(\mathrm{Sym}_i^2 E, s) &= \prod_p (1-\alpha_p^2 p^{-s})^{-1}(1-\alpha_p\beta_p p^{-s})^{-1}(1-\beta_p^2 p^{-s})^{-1} \\ &= \tilde{L}(E, \tfrac{s}{2})\tilde{L}(E\otimes\lambda, \tfrac{s}{2})\zeta_N(s). \end{aligned}$$

By [CS87], there exists the symmetric square conductor $B \in \mathbb{Z}$, the primitive (normalized) symmetric square L-function $L(\mathrm{Sym}_p^2 E, s)$ and the Euler product $U(E, s)$ such that

$$\begin{aligned} \Lambda(\mathrm{Sym}^2 E, s) &:= \left(\frac{B}{\pi^{3/2}}\right)^s \Gamma\left(\frac{s+1}{2}\right)^2 \Gamma\left(\frac{s+2}{2}\right) L(\mathrm{Sym}_p^2 E, s) \\ &:= \left(\frac{B}{\pi^{3/2}}\right)^s \Gamma\left(\frac{s+1}{2}\right)^2 \Gamma\left(\frac{s+2}{2}\right) L(\mathrm{Sym}_i^2 E, s)\cdot U(E, s) \end{aligned}$$

satisfies the functional equation

$$\Lambda(\mathrm{Sym}^2 E, s) = \Lambda(\mathrm{Sym}^2 E, 1-s), \tag{3.3}$$

and the Euler product $U(E, s) = \prod_{p|N} U_p(E, s)$.

Also, $U_p(E, s)$ is given as follows. Let $F = E_D$ be a global minimal twist of E and we write invariants with subscripts according to E or F. We have $L(\mathrm{Sym}_p^2 E, s) = L(\mathrm{Sym}_p^2 F, s)$, $B_E = B_F = B$. Let

$$\begin{aligned} S_1 &= S_1(E, F, D) &= \{p : p \mid D,\ p \nmid N_F\}, \\ S_2 &= S_1(E, F, D) &= \{p : p \mid D,\ p \| N_F\}. \end{aligned}$$

Note that for any odd prime p, if $p \in S_1$ or $p \in S_2$, $\mathrm{ord}_p(N_E) = 2$ and if

$p^2 \mid N_F$, $\mathrm{ord}_p(N_E) = \mathrm{ord}_p(N_F)$. Also we can write

$$\begin{aligned} N_E &= MD_1^2D_2^2 2^{\lambda_E}, \\ N_F &= MD_2 2^{\lambda_F}, \end{aligned}$$

where M is odd, D_1 is the product of the odd primes in S_1, D_2 is the product of the odd primes in S_2, and 2-adic valuations $\lambda_E \geq \lambda_F$. From the definition of imprimitive symmetric square L-functions,

$$\begin{aligned} L(\mathrm{Sym}_i^2 E, s) = L(\mathrm{Sym}_i^2 F, s) &\times \prod_{p \in S_1} (1 - \alpha_p^2(F)p^{-s})(1 - p^{-s})(1 - \beta_p^2(F)p^{-s}) \\ &\times \prod_{p \in S_2} (1 - p^{-s-1}). \end{aligned} \tag{3.4}$$

Let $B_E = B_F = \prod_p p^{\delta_p}$. Then for a global minimal twist elliptic curve F, we have

$$\begin{cases} \text{for } p \nmid N_F, & \delta_p = 0,\ U_p(F, s) = 1, \\ \text{for } p \parallel N_F, & \delta_p = 1,\ U_p(F, s) = 1, \\ \text{for } p^2 \mid N_F, & \delta_p \geq 1, \text{ there are three possibilities for} \\ & U_p(F, s) : 1,\ (1 \pm p^{-s})^{-1} \end{cases} \tag{3.5}$$

(cf. [CS87], [Del03] and [Wak02]).

3.4.2 Watkins' theorem

In [Wak], Watkins showed the following theorem.

Theorem 3.4.2. [Wak, Lemma 3.4] Let E be an elliptic curve with $B \geq 12$. Then $L(\mathrm{Sym}_p^2 E, 1) \geq \frac{0.033}{2 \log B}$.

We give a sketch of proof as follows. Watkins made the argument of [GHL94] explicit, in the case of an elliptic curve which is not $GL(1)$-lift, and then he derived an explicit zero-free region for $L(\mathrm{Sym}_p^2 E, s)$.

For an elliptic curve with CM, Watkins acquired an explicit zero-free region for the corresponding Hecke L-function.

To turn that into a lower bound for $L(\mathrm{Sym}_p^2 E, 1)$, Watkins used

$$F(s) = \zeta(s) L(\mathrm{Sym}_p^2 E, s) = \sum_n a_n n^{-s},$$

which is the Dirichlet series with nonnegative coefficients. He calculated the following integral moving the contour to $s = 1/2 - b$:

$$\int_{(2)} \Gamma(s) X^s F(s+b) \frac{ds}{2\pi i} = \sum_n \frac{a_n}{n^b e^{n/X}}, \geq e^{-1/X},$$

where $b = 1 - \frac{1}{25 \log(B)}$. The above zero-free region implies that $F(s)$ has no Siegel zero in $[b, 1)$, and so the residue value is

$$L(\mathrm{Sym}_p^2 E, 1) X^{1-b} \Gamma(1-b) + F(b),$$

with $F(b) < 0$. By the residue theorem, he derived the result.

Part II

Goldfeld's method

Chapter 4

Explicit Goldfeld's Theorem

4.1 Main results

Goldfeld obtained an effective lower bound for $L(1, \chi_d)$ as follows.

Theorem 4.1.1. [Gol76, Theorem 1] Let E be an elliptic curve over $\mathbb{Q}$ with conductor N. If E has complex multiplication and the L-function associated to E has a zero of order g at $s = 1$, then for any χ_d with $(d, N) = 1$ and $|d| > \exp\exp(c_1 N g^3)$, we have

$$L(1, \chi_d) > \frac{c_2}{g^{4g} N^{13}} \frac{(\log|d|)^{g-\mu-1} \exp(-21\sqrt{g \log\log|d|})}{\sqrt{|d|}},$$

where $\mu = 1$ or 2 is suitably chosen so that $\chi_d(-N) = (-1)^{g-\mu}$, and the constants c_1, $c_2 > 0$ can be effectively computed and are independent of g, N and d.

In fact, Goldfeld proved Theorem 4.1.1 under assumption that the associated base change Hasse-Weil L-function $L_{E/\mathbb{Q}(\sqrt{d})}(s)$ has a zero of order $\geq g$. Thus the proof of Theorem 4.1.1 in [Gol76] also implies the following theorem with effective constants.

Theorem 4.1.2. [BK18, Theorem 1.3] Let E be an elliptic curve over $\mathbb{Q}$ with conductor N and $g \geq 4$ be a positive integer. If E has complex multiplication and the associated base change Hasse-Weil L-function $L_{E/\mathbb{Q}(\sqrt{d})}(s)$ has a zero of order $\geq g$ at $s = 1$, then for any such d with $(d, N) = 1$ and $|d| > \exp\exp(400Ng^3)$, we have

$$L(1, \chi_d) > \frac{10^{180}}{g^{4g}N^5} \frac{(\log d)^{g-3}\exp(-21\sqrt{g \log\log d})}{\sqrt{d}}.$$

Remark 4.1.3. Let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication by an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-k})$. In the proof of Theorem 4.1.2, we use the fact that $-k$ is one of $-3, -4, -7, -8, -11, -19, -43, -67, -163$ (cf. statement (2) in theorem 3.3.6 or [Sil09, Example 11.3.1]), so $k \leq 163$, instead of the fact $k \leq N$ (because $k \mid N$), which is used in the proof of [Gol76, Theorem 1]. That is why there is a difference for exponents of N between Theorem 4.1.1 and Theorem 4.1.2.

We will improve theorem 4.1.2 to the following theorem in section 5.2.

Theorem 4.1.4. [BK19, Theorem 1.3] Let $d > 0$ be a fundamental discriminant of a real quadratic field $\mathbb{Q}(\sqrt{d})$. Let E be an elliptic curve over $\mathbb{Q}$ with conductor N of which the symmetric square conductor B is greater than 11, and let $g \geq 4$ be a positive integer. If the associated base change Hasse-Weil L-function $L(E/\mathbb{Q}(\sqrt{d}), s)$ has a zero of order $\geq g$ at $s = 1$, then for any such d with $(d, N) = 1$ and $d > \exp\exp(330Ng^3)$, we have

$$L(1, \chi_d) > \frac{6 \times 10^{184}}{g^{4g}N} \frac{(\log d)^{g-3}\exp(-21\sqrt{g \log\log d})}{\sqrt{d}}.$$

Remark 4.1.5. The previous version of Theorem 4.1.4, which is [BK19, Theorem 1.3], failed to consider the cases of non global minimal twist. Also, the proof in [BK19] works under the additional assumption that E is a global minimal twist of itself.

4.2 Proofs of main results

Let E be an elliptic curve over $\mathbb{Q}$ and assume the same conditions as in Theorem 4.1.2 or 4.1.4. As [Gol76], let

$$\varphi(s) = L_E(s+\tfrac{1}{2})L_E(s+\tfrac{1}{2},\chi_d) = \sum_{n=1}^{\infty} a_n n^{-s}$$

and

$$\varphi_1(2s) = L_E(s+\tfrac{1}{2})L_E(s+\tfrac{1}{2},\lambda), \tag{4.1}$$

where $\lambda(n) = \prod_{p^r \| n}(-1)^r$. We note that $\varphi(s) = L_{E/\mathbb{Q}(\sqrt{d})}(s+\frac{1}{2})$ and $\varphi(s)$ has a zero of order $\geq g$ at $s = \frac{1}{2}$. Let

$$G(s) = \frac{\varphi(s)}{\varphi_1(2s)} = \sum_{n=1}^{\infty} g_n n^{-s} \text{ and } G(s,x) = \sum_{n<x} g_n n^{-s}. \tag{4.2}$$

For $A = \frac{dN}{4\pi^2}$ and $U = (\log d)^{8g}$, let

$$H = \left(\tfrac{d}{ds}\right)^{g-\mu}\left[A^s\Gamma^2(s+\tfrac{1}{2})G(s,U)\varphi_1(2s)\right]_{s=\frac{1}{2}}.$$

In [Gol76], Goldfeld proved that for $d > \exp\exp(cNg^3)$ and c sufficiently large, either $L(1,\chi_d) > (\log d)^{g-\mu-1}\frac{1}{\sqrt{d}}$ or else

$$|H| \gg gN^{-12+\frac{1}{2}}(\log d)^{g-\mu-1}\prod_{\substack{\chi_d(p)\neq -1 \\ p<U}}(1+p^{-\frac{1}{2}})^{-4} \text{ [Gol76, p.662]}, \tag{4.3}$$

and that for $d > \exp(500g^3)$, either $L(1,\chi_d) > (\log d)^{g-\mu-1}\frac{1}{\sqrt{d}}$ or else

$$|H| \ll g^{4g}NL(1,\chi_d)A(\log\log A)^{g-\mu+6} \text{ [Gol76, (52)]}. \tag{4.4}$$

We see that both $L(1,\chi_d) > (\log d)^{g-\mu-1}\frac{1}{\sqrt{d}}$ and (4.3), (4.4) imply Theorem 4.1.1. To prove Theorem 4.1.2, we need the following propositions corresponding to (4.3) and (4.4), respectively.

Proposition 4.2.1. Assume the same conditions as in Theorem 4.1.2. Then for any such $d \geq \exp\exp(400Ng^3)$, either $L(1,\chi_d) > (\log d)^{g-\mu-1}\frac{1}{\sqrt{d}}$ or else

$$|H| \geq 1.8 \times 10^{-5} \cdot gN^{-4}\sqrt{d}(\log d)^{g-\mu-1} \prod_{\substack{\chi_d(p)\neq -1 \\ p<U}} \left(\frac{1-p^{-\frac{1}{2}}}{1+p^{-\frac{1}{2}}}\right)^2.$$

Proposition 4.2.2. Assume the same conditions as in Theorem 4.1.2. Then for any such $d \geq \exp\exp(400Ng^3)$, either $L(1,\chi_d) > (\log d)^{g-\mu-1}\frac{1}{\sqrt{d}}$ or else

$$|H| \leq 2 \times 10^9 \cdot (\tfrac{80}{e})^g g^{2g+4.5} L(1,\chi_d)A(\log\log A)^{g-\mu+6}.$$

We will prove Proposition 4.2.1 in Section 4.3 and Proposition 4.2.2 in Section 4.4. If we assume Proposition 4.2.1 and 4.2.2, then we can prove Theorem 4.1.2 as follows.

Proof of Theorem 4.1.2. Let $\mathcal{P}$ be the set of primes $p < (\log d)^{8g}$ for which $\chi_d(p) \neq -1$. We may assume

$$L(1,\chi_d) \leq (\log d)^{g-\mu-1}\frac{1}{\sqrt{d}} \ \ (\ d \geq \exp\exp(400Ng^3)).$$

From the inequality $2^{|\mathcal{P}|} \leq \frac{1}{4\log 2}(\log d)^{g-\mu-1}$ in the proof of [Gol76, Lemma 9], we see that $|\mathcal{P}| < \frac{1}{\log 2}g(\log\log d)$. So we have

$$\begin{aligned} & \log\prod_{p\in\mathcal{P}}\left(\frac{1+p^{-\frac{1}{2}}}{1-p^{-\frac{1}{2}}}\right)^2 = \sum_{p\in\mathcal{P}} 2\log\left(\frac{1+p^{-\frac{1}{2}}}{1-p^{-\frac{1}{2}}}\right) \\ \leq & \sum_{p\in\mathcal{P}} 2\left(\frac{1+p^{-\frac{1}{2}}}{1-p^{-\frac{1}{2}}} - 1\right) = \sum_{p\in\mathcal{P}} \frac{4}{\sqrt{p}-1} \\ \leq & \int_2^{|\mathcal{P}|} \frac{4}{\sqrt{x}-1}dx = \left[8x^{\frac{1}{2}} + 8\log(x^{\frac{1}{2}} - 1)\right]_2^{|\mathcal{P}|} \end{aligned}$$

$$
\begin{aligned}
&\leq 16|\mathcal{P}|^{\frac{1}{2}} \\
&\leq 20g^{\frac{1}{2}}(\log\log d)^{\frac{1}{2}}.
\end{aligned}
$$

From Proposition 4.2.1 and Proposition 4.2.2, we have for $d \geq \exp\exp(400Ng^3)$,

$$
\begin{aligned}
& 2\times 10^9 \cdot (\tfrac{80}{e})^g g^{2g+4.5} L(1,\chi_d) A (\log\log A)^{g-\mu+6} \\
\geq\ & 1.8\times 10^{-5}\cdot gN^{-4}\sqrt{d}(\log d)^{g-\mu-1}\exp\big(-20g^{\frac{1}{2}}(\log\log d)^{\frac{1}{2}}\big).
\end{aligned}
$$

Let $f(N,g,d) = \exp\big(g^{\frac{1}{2}}(\log\log d)^{\frac{1}{2}}\big)\cdot(\frac{80}{e})^{-g}g^{2g-4.5}(\log\log\frac{dN}{4\pi^2})^{-g-5}$. We claim that if $N > 10$, $g \geq 3$ and $d \geq \exp\exp(400Ng^3)$, then

$$
f(N,g,d) \geq \exp(450).
$$

Since $\log\log\frac{dN}{4\pi^2} \leq \log\log d^e = \log\log d + 1$, we have

$$
\begin{aligned}
& \log f(N,g,d) \\
\geq\ & \big(g^{\frac{1}{2}}(\log\log d)^{\frac{1}{2}}\big) - g\log\tfrac{80}{e} + (2g-4.5)\log g - (g+5)\log(\log\log d + 1),
\end{aligned}
$$

which is an increasing function for d because its partial derivative with respect to d is

$$
\begin{aligned}
& \frac{\sqrt{g}}{2\sqrt{\log\log d}(\log d)d} - \frac{g+5}{(\log\log d+1)(\log d)d} \\
>\ & \frac{\sqrt{g(\log\log d)} - 2(g+5)}{2(\log\log d)(\log d)d} \\
>\ & 0.
\end{aligned}
$$

So we have

$$
\begin{aligned}
& \log f(N,g,d) \\
\geq\ & (400N)^{\frac{1}{2}}g^2 - g\log\tfrac{80}{e} + (2g-4.5)\log g - (g+5)\log(400Ng^3+1),
\end{aligned}
$$

which is an increasing function for g because its partial derivative with respect to g is

$$\begin{aligned} & 2(400N)^{\frac{1}{2}}g - \log\left(\tfrac{80}{e}\right) + 2\log g + \frac{2g-4.5}{g} \\ & -\log\left(400Ng^3+1\right) - \frac{3\cdot 400Ng^2(g+5)}{400Ng^3+1} \\ > \ & 2(400N)^{\frac{1}{2}}g - \log\left(\tfrac{80}{e}\right) - \tfrac{4.5}{g} - 3\log g - \log\left(400N+1\right) - \tfrac{3(g+5)}{g} \\ > \ & 0. \end{aligned}$$

So we have

$$\begin{aligned} & \log f(N,g,d) \\ \geq \ & (400N)^{\frac{1}{2}}\cdot 3^2 - 3\log\tfrac{80}{e} + 1.5\log 3 - 8\log\left(400\cdot 3^3N+1\right), \end{aligned}$$

which is an increasing function for N because its derivative with respect to N is

$$\frac{\sqrt{400}\cdot 3^2}{2\sqrt{N}} - \frac{8\cdot 400\cdot 3^3}{400\cdot 3^3N+1} > \frac{\sqrt{400}\cdot 3^2}{2\sqrt{N}} - \frac{8}{N} > 0.$$

So we have

$$\begin{aligned} & \log f(N,g,d) \\ \geq \ & \sqrt{4000}\cdot 3^2 - 3\log\tfrac{80}{e} + 1.5\log 3 - 8\log\left(4000\cdot 3^3+1\right) \\ > \ & 450 \end{aligned}$$

and the claim is proved. Thus we have

$$\exp\left(g^{\frac{1}{2}}(\log\log d)^{\frac{1}{2}}\right) > \exp(450)\cdot\left(\tfrac{80}{e}\right)^g g^{-2g+4.5}\left(\log\log\tfrac{dN}{4\pi^2}\right)^{g+5}.$$

Recall $A = \frac{dN}{4\pi^2}$. Then we have for $d \geq \exp\exp\left(400Ng^3\right)$,

$$
\begin{aligned}
L(1,\chi_d) &> \frac{1.8\times 10^{-5}\cdot gN^{-4}}{2\times 10^{9}\cdot(\frac{80}{e})^{g}g^{2g+4.5}}\cdot\frac{\sqrt{d}(\log d)^{g-\mu-1}\exp\big(-20g^{\frac12}(\log\log d)^{\frac12}\big)}{A(\log\log A)^{g-\mu+6}}\\
&> \frac{1.8\times 10^{-5}\cdot 4\pi^2\cdot gN^{-5}}{2\times 10^{9}\cdot(\frac{80}{e})^{g}g^{2g+4.5}}\cdot\frac{(\log d)^{g-\mu-1}\exp\big(-20g^{\frac12}(\log\log d)^{\frac12}\big)}{\sqrt{d}(\log\log\frac{dN}{4\pi^2})^{g-\mu+6}}\\
&> \frac{1.8\times 10^{-5}\cdot 4\pi^2\cdot \exp(450)}{2\times 10^{9}\cdot g^{4g}N^{5}}\cdot\frac{(\log d)^{g-3}\exp\big(-21g^{\frac12}(\log\log d)^{\frac12}\big)}{\sqrt{d}}\\
&> \frac{10^{180}}{g^{4g}N^{5}}\cdot\frac{(\log d)^{g-3}\exp\big(-21g^{\frac12}(\log\log d)^{\frac12}\big)}{\sqrt{d}}. \qquad \square
\end{aligned}
$$

4.3 A proof of Proposition 4.2.1

In this section, we will prove Proposition 4.2.1 Let $\kappa = g - \mu$. From [Gol76, (53)], we define H_1 and H_2 by

$$
\begin{aligned}
H &= H_1 + H_2\\
&= 2\kappa\sqrt{A}(\log A)^{\kappa-1}G(\tfrac12,U)\varphi_1'(1)\\
&\quad+\sqrt{A}\sum_{r=2}^{\kappa}\binom{\kappa}{r}(\log A)^{\kappa-r}\left(\tfrac{d}{ds}\right)^{r}\left[\Gamma^2(s+\tfrac12)G(s,U)\varphi_1(2s)\right]_{s=\frac12}.
\end{aligned}
$$

Since $|H| \geq |H_1| - |H_2|$, to get an explicit lower bound for $|H|$, we need an explicit upper bound for $|H_2|$ and an explicit lower bound for $|H_1|$.

Upper Bound for $|H_2|$. Using Leibniz' rule and Cauchy's Theorem (for detail, see [Gol76, p. 657 and p. 658]) we have

$$\begin{aligned}
|H_2| &= \Bigg|\sqrt{A}\sum_{r=2}^{\kappa}\binom{\kappa}{r}(\log A)^{\kappa-r} \\
&\quad \cdot\Big(\sum_{h=0}^{r-1}\binom{r}{h}\left(\tfrac{d}{ds}\right)^{r-h}\left[\Gamma^2(s+\tfrac{1}{2})\varphi_1(2s)\right]_{s=\frac{1}{2}}\cdot\left(\tfrac{d}{ds}\right)^{h}\left[G(s,U)\right]_{s=\frac{1}{2}}\Big)\Bigg| \\
&\le \sqrt{A}\sum_{r=2}^{\kappa}\binom{\kappa}{r}(\log A)^{\kappa-r} \\
&\quad \cdot\Big(\sum_{h=0}^{r-1}\binom{r}{h}2^{3(r-h)}(r-h)!\max_{s\in\mathbf{C_2}}|\Gamma^2(s+\tfrac{1}{2})\varphi_1(2s)|\cdot 2^{2h}h!\max_{s\in\mathbf{C_1}}|G(s,U)|\Big) \\
&\le \sqrt{A}\sum_{r=2}^{\kappa}8^r r! r\binom{\kappa}{r}(\log A)^{\kappa-r}\max_{s\in\mathbf{C_2}}|\Gamma^2(s+\tfrac{1}{2})|\max_{s\in\mathbf{C_2}}|\varphi_1(2s)|\max_{s\in\mathbf{C_1}}|G(s,U)|,
\end{aligned} \tag{4.5}$$

where $\mathbf{C_1}$ is the circle of radius $\frac{1}{4}$ centered at $s=\frac{1}{2}$ and $\mathbf{C_2}$ is the circle of radius $\frac{1}{8}$ centered at $s=\frac{1}{2}$.

By [Gol76, (46)], we have for $s=\sigma+it\in\mathbf{C_2}$,

$$\begin{aligned}
\max_{s\in\mathbf{C_2}}|\Gamma^2(s+\tfrac{1}{2})| &\le \max_{s\in\mathbf{C_2}}\left\{\sqrt{2\pi}\exp\left(\tfrac{1}{12(\sigma+\frac{1}{2})}\right)|s+\tfrac{1}{2}|^{\sigma}\exp\left(-\sigma-\tfrac{1}{2}\right)\right\}^2 \\
&\le \left(\sqrt{2\pi}(\tfrac{9}{8})^{\frac{5}{8}}\exp\left(\tfrac{1}{12}\cdot\tfrac{8}{7}-\tfrac{7}{8}\right)\right)^2 \\
&\le 1.6.
\end{aligned} \tag{4.6}$$

We need the following lemma, which is an explicit version of [Gol76, (49)]. Also, the following lemma will be reproved without the assumption of complex multiplication, as Lemma 5.2.5 in section 5.2.

Lemma 4.3.1. For $s=\sigma+it\in\mathbb{C}$,

$$|\varphi_1(s)|\le\begin{cases} 3\times 10^{12}\cdot N^3t^6 & \text{if } 1-\frac{1}{100800\log|t|}\le\sigma\le\frac{3}{2}, \quad |t|\ge 2+\frac{1}{840}, \\ 10^5\cdot N^3\frac{1}{|s-1|} & \text{if } \frac{3}{4}\le\sigma\le\frac{3}{2}, \quad |t|\le 2+\frac{1}{840}. \end{cases}$$

Proof. Let ψ be the primitive Grössencharakter of $K = \mathbb{Q}(\sqrt{-k})$ with conductor $\mathfrak{f}$ such that $L_E(s) = L_K(s,\psi)$ (cf. (3.2) or [Gol76, Theorem 2]). By [Gol76, Lemma 2], we have

$$\varphi_1(s) = L_K(s+1,\psi^2)\frac{L(s,\chi_k)}{\zeta(s)}\prod_{p|k}(1-p^{-s})^{-1}, \tag{4.7}$$

where χ_k is a real primitive Dirichlet character (mod k).

From [Gol76, p. 654], we have for $0 \le \sigma \le \frac{3}{2}$,

$$\left|L_K(s+1,\psi^2)\right| \le \tfrac{10N^3}{4\pi^2}|s+3|^2. \tag{4.8}$$

By [Jam03, Theorem 5.3.13], we have if $|t| \ge 2 + \frac{1}{840}$ and $\sigma \ge 1 - \frac{1}{840\cdot 6(\log|t|+11)}$, then

$$|\zeta(s)^{-1}| \le 56\cdot 840^2(\log|t|+11)^3.$$

By [Jam03, Proposition 3.1.16], we have for $\sigma > -1$,

$$\zeta(s) = \tfrac{1}{s-1} + \tfrac{1}{2} + r_1^*(s),$$

where $|r_1^*(s)| \le |\frac{s(s+1)}{8(\sigma+1)}|$. So we have if $|t| \le 2 + \frac{1}{840}$ and $\frac{3}{4} \le \sigma \le \frac{3}{2}$, then

$$\begin{aligned} |\zeta(s)| &\ge |\tfrac{s+1}{2(s-1)}| - |r_1^*(s)| \\ &\ge \frac{|s+1|}{8|s-1|(\sigma+1)}(4(\sigma+1) - |s||s-1|) \\ &\ge 1/13. \end{aligned}$$

Thus we have the following explicit version of a statement in [Gol76, p. 653].

$$|\zeta(s)^{-1}| \le \begin{cases} 56\cdot 840^2\cdot 6^3|t|^3 & \text{if } \sigma \ge 1 - \frac{1}{840\cdot 6\cdot 20\log|t|}, \quad |t| \ge 2 + \frac{1}{840}, \\ 13 & \text{if } \frac{3}{4} \le \sigma \le \frac{3}{2}, \quad |t| \le 2 + \frac{1}{840}. \end{cases} \tag{4.9}$$

We note that

$$L(s,\chi_k) = \sum_{n=1}^{\infty} \frac{\chi_k(n)}{n^s} = \frac{1}{k^s} \sum_{l=1}^{k-1} \chi_k(l)\zeta(s, \tfrac{l}{k}),$$

where $\zeta(s,a)$ is the Hurwitz zeta function and $0 < a \leq 1$. By [Apo76, Theorem 12.21], we have for any integer $M \geq 0$ and $\sigma > 0$,

$$\zeta(s,a) = \sum_{n=0}^{M} \frac{1}{(n+a)^s} + \frac{(M+a)^{1-s}}{s-1} - s\int_M^{\infty} \frac{x-[x]}{(x+a)^{s+1}} dx.$$

So we have, for $\sigma \geq \frac{1}{2}$,

$$|\zeta(s,a) - a^{-s}| \leq \sum_{n=1}^{M} \frac{1}{\sqrt{n}} + \frac{(M+1)^{1-\sigma}}{\sqrt{(\sigma-1)^2+t^2}} + \frac{\sqrt{\sigma^2+t^2}}{\sigma M^{\sigma}}. \tag{4.10}$$

By applying (4.10) with $M = \lfloor t \rfloor$ to the region; $\frac{1}{2} \leq \sigma \leq 2$ and $t \geq 2 + \frac{1}{840}$, we have

$$\begin{aligned} |\zeta(s,a) - a^{-s}| &\leq 1 + \int_1^{\lfloor t \rfloor} \frac{1}{\sqrt{x}} dx + \frac{\sqrt{t+1}}{t} + \frac{\sqrt{1+4t^2}}{\sqrt{t-1}} \\ &\leq 5\sqrt{t}, \end{aligned}$$

which gives

$$\begin{aligned} |L(s,\chi_k)| &\leq k^{-\sigma} \sum_{l=1}^{k-1} \left(\left(\tfrac{l}{k}\right)^{-\sigma} + 5\sqrt{t} \right) \\ &\leq \left(\sum_{l=1}^{k-1} l^{-\frac{1}{2}}\right) + \frac{5(k-1)}{\sqrt{k}}\sqrt{t} \\ &< 7\sqrt{kt}. \end{aligned}$$

By applying (4.10) with $M = 1$ to the region; $\frac{1}{2} \leq \sigma \leq 2$ and $0 \leq t \leq 2 + \frac{1}{840}$, we have

$$|\zeta(s,a) - a^{-s}| \leq 1 + \tfrac{\sqrt{2}}{|s-1|} + \sqrt{1+4t^2} < \tfrac{16}{|s-1|},$$

which gives

$$\begin{aligned} |L(s,\chi_k)| &\leq k^{-\sigma} \sum_{l=1}^{k-1} \left(\left(\tfrac{l}{k}\right)^{-\sigma} + \tfrac{16}{|s-1|} \right) \\ &\leq \left(\sum_{l=1}^{k-1} l^{-\frac{1}{2}} \right) + \tfrac{16(k-1)}{\sqrt{k}} \tfrac{1}{|s-1|} \\ &< \tfrac{22\sqrt{k}}{|s-1|}. \end{aligned}$$

We note that $L(\bar{s},\chi_k) = \overline{L(s,\chi_k)}$. Then we have the following explicit version of a statement in [Gol76, p. 653].

$$|L(s,\chi_k)| \leq \begin{cases} 7\sqrt{k|t|} & \text{if } \frac{1}{2} \leq \sigma \leq 2, \quad |t| \geq 2 + \frac{1}{840}, \\ 22\sqrt{k}|s-1|^{-1} & \text{if } \frac{1}{2} \leq \sigma \leq 2, \quad |t| \leq 2 + \frac{1}{840}. \end{cases} \tag{4.11}$$

Since $\sigma \geq \frac{1}{2}$ and $\{p : p|k\}$ is a set containing only one prime from Remark 4.1.3, we have $|\prod_{p|k}(1-p^{-s})^{-1}| \leq |(1-2^{-s})^{-1}| \leq \frac{\sqrt{2}}{\sqrt{2}-1}$. Thus Lemma 4.3.1 follows from (4.7), (4.8), (4.9), (4.11) and Remark 4.1.3. □

From Lemma 4.3.1, we have

$$\begin{aligned} \max_{s\in \mathbf{C_2}} |\varphi_1(2s)| &\leq \max_{s\in \mathbf{C_2}} \left(10^5 \tfrac{N^3}{|2s-1|}\right) \\ &\leq 4 \cdot 10^5 N^3. \end{aligned} \tag{4.12}$$

Moreover,

$$\max_{s\in \mathbf{C_1}} |G(s,U)| < \prod_{\substack{\chi_d(p)\neq -1 \\ p<U}} (1-p^{-\frac{1}{4}})^{-4} \ \text{(cf. [Gol76, p. 657])}. \tag{4.13}$$

Thus from (4.5), (4.6), (4.12) and (4.13) we have

$$|H_2| \leq 4 \cdot 10^8 N^3 g^2 \sqrt{A} (\log A)^{\kappa-2} \prod_{\substack{\chi_d(p) \neq -1 \\ p<U}} (1 - p^{-\frac{1}{4}})^{-4}. \tag{4.14}$$

Lower Bound for $|H_1|$. We need the following lemma, which is an explicit version of [Gol76, (55)]. (We use $\prod \left(\frac{1-p^{-\frac{1}{2}}}{1+p^{-\frac{1}{2}}} \right)^2$ in Lemma 4.3.2 instead of $\prod (1 + p^{-\frac{1}{2}})^{-4}$ in [Gol76, (55)].)

Lemma 4.3.2. If $d > \exp(500g^3)$, then either $L(1, \chi_d) > (\log d)^{\kappa-1} \frac{1}{\sqrt{d}}$ or else we have

$$|G(\tfrac{1}{2}, U)| \geq \prod_{\substack{\chi_d(p) \neq -1 \\ p<U}} \left(\frac{1-p^{-\frac{1}{2}}}{1+p^{-\frac{1}{2}}} \right)^2 - (\log d)^{-2g}.$$

Proof. We denote by $P(s, U)$ the partial Euler product of $G(s)$ for primes $p \leq U$ and write

$$G(s, U) = P(s, U) - R(s, U).$$

From [Gol76, Lemma 1], we see that

$$|P(\tfrac{1}{2}, U)| \geq \prod_{\substack{\chi_d(p) \neq -1 \\ p<U}} \left(\frac{1-p^{-\frac{1}{2}}}{1+p^{-\frac{1}{2}}} \right)^2.$$

So we only need to show that

$$|R(\tfrac{1}{2}, U)| \leq (\log d)^{-2g}.$$

If

$$\mathcal{N}_U = \{n \text{ such that } p|n \;\Rightarrow\; p < U\}$$

then

$$R(s,U)=\sum_{n>U,\ n\in\mathcal{N}_U} g_n n^{-s}.$$

We write

$$|R(\tfrac{1}{2},U)|\leq \sum_{U<n\leq\frac{1}{4}\sqrt{d}}|g_n|n^{-\frac{1}{2}}+\sum_{\frac{1}{4}\sqrt{d}<n,\ n\in\mathcal{N}_U}|g_n|n^{-\frac{1}{2}} \ =R_1+R_2.$$

We may assume

$$L(1,\chi_d)\leq(\log d)^{\kappa-1}\tfrac{1}{\sqrt{d}}\ \ (d>\exp(500g^3)).$$

Let $\frac{\zeta(s)L(s,\chi_d)}{\zeta(2s)}=\sum_{n=1}^{\infty}\frac{\nu_n}{n^s}$. Then by [Gol76, Lemma 1 and Lemma 4], we have

$$\begin{aligned}
R_1 &\leq U^{-\frac{1}{2}}(\sum_{n\leq\frac{1}{4}\sqrt{d}}\nu_n)^2\\
&\leq U^{-\frac{1}{2}}(\tfrac{1}{4\log 2})^2(\log d)^{2(\kappa-1)}\\
&= (\tfrac{1}{4\log 2})^2(\log d)^{-2(g+\mu+1)}.
\end{aligned}$$

Now we estimate R_2. Let

$$P_1(s,U)=\prod_{\substack{\chi_d(p)\neq-1\\ p<U}}(1-p^{-s})^{-4}.$$

Since $|\mathcal{P}|<\frac{1}{\log 2}g(\log\log d)$ (cf. Proof of Theorem 4.1.2), we have

$$\log P_1(\tfrac{1}{6},U)=\log\prod_{p\in\mathcal{P}}\left(\frac{1}{1-p^{-\frac{1}{6}}}\right)^4$$

$$\leq\ \sum_{p\in\mathcal{P}}\frac{4}{\sqrt[6]{p}-1}$$

$$\begin{aligned}
&\le \int_2^{|\mathcal{P}|} \tfrac{4}{\sqrt[6]{x}-1}\,dx \\
&= \left[\tfrac{24}{5}x^{\frac{5}{6}} + 6x^{\frac{2}{3}} + 8x^{\frac{1}{2}} + 12x^{\frac{1}{3}} + 24x^{\frac{1}{6}} + 24\log\left(x^{\frac{1}{6}}-1\right)\right]_2^{|\mathcal{P}|} \\
&\le 58|\mathcal{P}|^{\frac{5}{6}} \\
&\le 80(g\log\log d)^{\frac{5}{6}}.
\end{aligned}$$

So we have

$$\begin{aligned}
R_2 &\le \lim_{N\to\infty}\int_{2-i\infty}^{2+i\infty} P_1(\tfrac{1}{2}+z,U)\tfrac{N^z-(\sqrt{d}/4)^z}{z(z+1)}\,dz \\
&= \lim_{N\to\infty}\int_{-\frac{1}{3}-i\infty}^{-\frac{1}{3}+i\infty} P_1(\tfrac{1}{2}+z,U)\tfrac{N^z-(\sqrt{d}/4)^z}{z(z+1)}\,dz \\
&\le \lim_{N\to\infty}\int_{-\infty}^{\infty} P_1(\tfrac{1}{6},U)\tfrac{N^{-\frac{1}{3}}+(\sqrt{d}/4)^{-\frac{1}{3}}}{\left|(-\frac{1}{3}+it)(\frac{2}{3}+it)\right|}\,dt \\
&\le P_1(\tfrac{1}{6},U)(\tfrac{\sqrt{d}}{4})^{-\frac{1}{3}}\int_{-\infty}^{\infty}\tfrac{1}{2/9+t^2}\,dt \\
&\le 3\sqrt[6]{2}\pi\exp\left(80(g\log\log d)^{\frac{5}{6}}\right)\cdot\tfrac{1}{\sqrt[6]{d}}.
\end{aligned}$$

Thus we have for $d \ge \exp(500g^3)$,

$$\begin{aligned}
\left|R(\tfrac{1}{2},U)\right| &\le (\tfrac{1}{4\log 2})^2(\log d)^{-2(g+\mu+1)} + 3\sqrt[6]{2}\pi\cdot\exp\left(80(g\log\log d)^{\frac{5}{6}}\right)\cdot\tfrac{1}{\sqrt[6]{d}} \\
&\le (\log d)^{-2g}. \qquad \square
\end{aligned}$$

To get an explicit lower bound for $|H_1|$, we need the following lemma, which is an explicit version of [Gol76, Lemma 12]. (We note that the inequality in [Gol76, Lemma 12] is in the wrong direction.)

Lemma 4.3.3.

$$\varphi_1'(1) = \frac{d}{ds}\Big|_{s=1}\Big(L_E(\tfrac{s}{2}+\tfrac{1}{2})L_E(\tfrac{s}{2}+\tfrac{1}{2},\lambda)\Big)$$

$$\geq \quad 0.98(kN^2)^{-2}.$$

We will prove Lemma 4.3.3 in section 5.1 and reprove it as Lemma 5.2.8 without the assumption of CM in section 5.2. If we assume Lemma 4.3.3, then by Lemma 4.3.2 we have for $d > \exp(500g^3)$, either

$$L(1,\chi_d) > (\log d)^{\kappa-1}\tfrac{1}{\sqrt{d}}$$

or else

$$|H_1| \geq 2\kappa\tfrac{0.98}{k^2N^4}\cdot\sqrt{A}(\log A)^{\kappa-1}\left(\prod_{\substack{\chi_d(p)\neq -1\\ p<U}}\left(\frac{1-p^{-\frac{1}{2}}}{1+p^{-\frac{1}{2}}}\right)^2-(\log d)^{-2g}\right). \tag{4.15}$$

Now we can prove Proposition 4.2.1.

Proof of Proposition 4.2.1. We may assume

$$L(1,\chi_d) \leq (\log d)^{\kappa-1}\tfrac{1}{\sqrt{d}} \ \ (d > \exp(500g^3)).$$

From (4.14) and (4.15), we have

$$\begin{aligned}
|H| &\geq |H_1|-|H_2| \\
&\geq \left[2\kappa\tfrac{0.98}{k^2N^4}\cdot\sqrt{A}(\log A)^{\kappa-1}\prod_{\substack{\chi_d(p)\neq -1\\ p<U}}\left(\tfrac{1-p^{-\frac{1}{2}}}{1+p^{-\frac{1}{2}}}\right)^2\right] \\
&\quad -\Bigg[2\kappa\tfrac{0.98}{k^2N^4}\cdot\sqrt{A}(\log A)^{\kappa-1}(\log d)^{-2g} \\
&\qquad +4\cdot 10^8N^3g^2\sqrt{A}(\log A)^{\kappa-2}\prod_{\substack{\chi_d(p)\neq -1\\ p<U}}(1-p^{-\frac{1}{4}})^{-4}\Bigg] \\
&= \tilde{H}_1-\tilde{H}_2.
\end{aligned}$$

If $\frac{1}{2}\tilde{H}_1 \geq \tilde{H}_2$, then we have

$$\begin{aligned}
|H| &\geq \frac{\tilde{H}_1}{2} \\
&\geq \kappa\frac{0.98}{k^2N^4} \cdot \sqrt{A}(\log A)^{\kappa-1} \prod_{\substack{\chi(p)\neq -1 \\ p<U}} \left(\frac{1-p^{-\frac{1}{2}}}{1+p^{-\frac{1}{2}}}\right)^2 \\
&\geq \frac{0.98}{2\cdot 163^2} \cdot gN^{-4}\sqrt{A}(\log A)^{\kappa-1} \prod_{\substack{\chi(p)\neq -1 \\ p<U}} \left(\frac{1-p^{-\frac{1}{2}}}{1+p^{-\frac{1}{2}}}\right)^2 \quad \text{(cf. Remark 4.1.3)}
\end{aligned}$$

as desired.

We see that

$$\begin{aligned}
\frac{\tilde{H}_2}{\tilde{H}_1} &= \frac{4\cdot 10^8 N^3 g^2\sqrt{A}(\log A)^{\kappa-2}\prod_{\substack{\chi_d(p)\neq -1 \\ p<U}}(1-p^{-\frac{1}{4}})^{-4}}{2\kappa\frac{0.98}{k^2N^4}\cdot\sqrt{A}(\log A)^{\kappa-1}\prod_{\substack{\chi_d(p)\neq -1 \\ p<U}}\left(\frac{1-p^{-\frac{1}{2}}}{1+p^{-\frac{1}{2}}}\right)^2} \\
&\quad + \frac{(\log d)^{-2g}}{\prod_{\substack{\chi_d(p)\neq -1 \\ p<U}}\left(\frac{1-p^{-\frac{1}{2}}}{1+p^{-\frac{1}{2}}}\right)^2} \\
&\leq \frac{4\cdot 10^8}{2\cdot 0.98(g-2)} \cdot 163^2\cdot N^7 g^2(\log d)^{-1} \prod_{\substack{\chi_d(p)\neq -1 \\ p<U}} \left(\frac{1+p^{-\frac{1}{2}}}{1-p^{-\frac{1}{2}}}\right)^2 \cdot \left(\frac{1}{1-p^{-\frac{1}{4}}}\right)^4 \\
&\quad + (\log d)^{-2g} \prod_{\substack{\chi_d(p)\neq -1 \\ p<U}} \left(\frac{1+p^{-\frac{1}{2}}}{1-p^{-\frac{1}{2}}}\right)^2 \\
&\leq 2\cdot\left(\frac{4\cdot 10^8}{2\cdot 0.98(g-2)} \cdot 163^2\cdot N^7 g^2(\log d)^{-1} \prod_{\substack{\chi_d(p)\neq -1 \\ p<U}} \left(\frac{1+p^{-\frac{1}{2}}}{1-p^{-\frac{1}{2}}}\right)^2 \cdot \left(\frac{1}{1-p^{-\frac{1}{4}}}\right)^4\right).
\end{aligned}$$

Let $\mathcal{P}$ be the set of primes $p < (\log d)^{8g}$ for which $\chi_d(p) \neq -1$. Since

$|\mathcal{P}| < \frac{g}{\log 2}(\log\log d)$, we have

$$\begin{aligned}
&\log \prod_{p\in\mathcal{P}} \left(\tfrac{1+p^{-\frac{1}{2}}}{1-p^{-\frac{1}{2}}}\right)^2 \cdot \left(\tfrac{1}{1-p^{-\frac{1}{4}}}\right)^4 \\
\leq\ & \sum_{p\in\mathcal{P}} \left(\tfrac{4}{\sqrt{p}-1} + \tfrac{4}{\sqrt[4]{p}-1}\right) \\
\leq\ & \int_2^{|\mathcal{P}|} \tfrac{4}{\sqrt{x}-1} + \tfrac{4}{\sqrt[4]{x}-1}\,dx \\
=\ & \left[\tfrac{16}{3}x^{\frac{3}{4}} + 16x^{\frac{1}{2}} + 16x^{\frac{1}{4}} + 8\log(x^{\frac{1}{2}}-1) + 16\log(x^{\frac{1}{4}}-1)\right]_2^{|\mathcal{P}|} \\
\leq\ & 6|\mathcal{P}|^{\frac{3}{4}} \\
\leq\ & 6\left(\tfrac{g}{\log 2}\log\log d\right)^{\frac{3}{4}}. \qquad (4.16)
\end{aligned}$$

Thus the sufficient condition of $\frac{1}{2}\tilde{H}_1 \geq \tilde{H}_2$ is that

$$\log\log d - 6\left(\tfrac{g}{\log 2}\log\log d\right)^{\frac{3}{4}} \geq \log\left(4\cdot\tfrac{4\cdot 10^8}{2\cdot 0.98}\cdot 163^2\cdot N^7\tfrac{g^2}{g-2}\right). \qquad (4.17)$$

We write $d \geq \exp\exp(c_1Ng^3)$ and assume $g \geq 3$. If c_1 is sufficiently large, the left hand in (4.17) is greater than

$$c_1Ng^3 - 6\left(\tfrac{1}{\log 2}c_1Ng^4\right)^{\frac{3}{4}} = g^3\left(c_1N - \tfrac{6}{(\log 2)^{3/4}}c_1^{3/4}N^{3/4}\right),$$

and the right hand in (4.17) is less than

$$31 + 7\log N + \log\tfrac{g^2}{g-2}.$$

Since $g \geq 3$ and $N > 10$, a sufficient condition of $\frac{1}{2}\tilde{H}_1 \geq \tilde{H}_2$ is that $c_1 \geq 389.7$. For convenience, if we choose $c_1 = 400$, then Proposition 4.2.1 follows. $\square$

4.4 A proof of Proposition 4.2.2

In this section, we will prove Proposition 4.2.2. From [Gol76, (24), (26) and (51)] and the assumption that $\varphi(s) = L_E(s + \frac{1}{2})L_E(s + \frac{1}{2}, \lambda)$ has a zero of order $\geq g$ at $s = \frac{1}{2}$, we can write

$$0 = (\tfrac{d}{ds})^{\kappa}\Big[A^s\Gamma^2(s + \tfrac{1}{2})\varphi(s)\Big]_{s=\frac{1}{2}} = T_1 + T_2, \tag{4.18}$$

where

$$T_1 = \delta\sum_{r=0}^{\kappa}\Big(\sum_{n\leq A_1} a_n\sqrt{A/n}(\log A/n)^{\kappa-r}I_r(n/A)\Big),$$

$$T_2 = \delta\sum_{r=0}^{\kappa}\Big(\sum_{n>A_1} a_n\sqrt{A/n}(\log A/n)^{\kappa-r}I_r(n/A)\Big),$$

$$\delta = 1 + (-1)^{\kappa}\chi_d(-N),$$

$$A_1 = A((8 + 2\kappa)\log A)^2,$$

and

$$I_r(M) = \int_{u_1=0}^{\infty}\int_{u_2=M/u_1}^{\infty} \exp(-(u_1 + u_2))(\log u_1u_2)^r du_1du_2 \ (M \geq 0).$$

By [Gol76, Lemma 10], we have

$$|T_2| \leq 1.$$

Thus by (4.18) and [Gol76, (27), (30), (31) and (39)], we have

$$\begin{aligned} & |2H| \\ = \ & |2H - T_1 - T_2| \\ \leq \ & |2H - T(G(s, U))| + |T(g(s))| + |S_1| + |S_2| + 1, \end{aligned} \tag{4.19}$$

where

$$T(F(s)) = (\tfrac{d}{ds})^{\kappa}\Big[\tfrac{\delta}{2\pi i}\int_{2-i\infty}^{2+i\infty} A^{s+z}\Gamma^2(s+z+\tfrac{1}{2})F(s+z)\varphi_1(2s+2z)\tfrac{dz}{z}\Big]_{s=\frac{1}{2}},$$

$$g(s) = G(s, A_0) - G(s, U),$$

$$A_0 = A(\log A)^{-20g},$$

$$S_1 = 2\sum_{r=0}^{\kappa}\binom{\kappa}{r}(\sum_{A_0\le n\le J} b_n\sqrt{A/n}(\log A/n)^{\kappa-r}I_r(n/A)),$$

$$S_2 = 2\sum_{r=0}^{\kappa}\binom{\kappa}{r}(\sum_{J\le n\le A_1} b_n\sqrt{A/n}(\log A/n)^{\kappa-r}I_r(n/A)),$$

$$J = A((\kappa+6)\log\log A)^2,$$

and

$$\sum_{n=1}^{\infty} b_n n^{-s} = G(s, A_1)\varphi_1(2s) - G(s, A_0)\varphi_1(2s).$$

So, to obtain an explicit upper bound for $|H|$, we need explicit upper bounds for $|S_1|$, $|S_2|$, $|T(g(s))|$ and $|2H - T(G(s, U))|$.

Upper Bound for $|S_1|$. From [Gol76, p. 649], we have

$$|S_1| \le 4^{\kappa+1}\kappa!(\log \tfrac{A}{A_0})^{\kappa}\sqrt{A}\sum_{A_0\le n\le J}\tfrac{|b_n|}{\sqrt{n}}. \tag{4.20}$$

We may assume

$$L(1, \chi_d) \le (\log d)^{\kappa-1}\tfrac{1}{\sqrt{d}} \quad (d > \exp\exp(400Ng^3)).$$

Then we can choose

$$y \;=\; L(1, \chi_d)^2 J$$

$$
\begin{aligned}
&\leq (\log A)^{2\kappa-2}\tfrac{J}{d} \\
&\leq A_0.
\end{aligned}
$$

Recall $\frac{\zeta(s)L(s,\chi_d)}{\zeta(2s)} = \sum_{n=1}^{\infty} \frac{\nu_n}{n^s}$. By [Gol76, (36)], we have

$$
\begin{aligned}
\sum_{A_0 \leq n \leq J} \frac{|b_n|}{\sqrt{n}} &\leq \sum_{k^2 \leq \frac{J}{A_0}} \frac{d(k)}{k} \sum_{A_0 \leq m \leq \frac{J}{k^2}} \frac{1}{\sqrt{m}} \sum_{f|m} \nu_f \nu_{m/f} \\
&\leq \Big(\sum_{k \leq \sqrt{\frac{J}{A_0}}} \frac{d(k)}{k} \Big) \Big(\sum_{y \leq m \leq J} \frac{1}{\sqrt{m}} \sum_{f|m} \nu_f \nu_{m/f} \Big),
\end{aligned} \tag{4.21}
$$

where $d(k) = \sum_{f|k} 1$.

Lemma 4.4.1. (cf. [Apo76, Problem 3, p. 70]) For $x \geq 3$,

$$
\sum_{n \leq x} \frac{d(n)}{n} \leq \tfrac{1}{2}\log^2 x + 2C \log x + 10
$$

where $C(< 0.6)$ is the Euler constant.

Proof. By Euler's summation formula,

$$
\begin{aligned}
\sum_{n \leq x} \frac{1}{n} &= \int_1^x \frac{dt}{t} - \int_1^x \frac{t-[t]}{t^2} dt + 1 - \frac{x-[x]}{x} \\
&= \log x + \Big(1 - \int_1^\infty \frac{t-[t]}{t^2} dt\Big) + \Big(\int_x^\infty \frac{t-[t]}{t^2} dt - \frac{x-[x]}{x}\Big) \\
&\leq \log x + C + \frac{1}{x}
\end{aligned}
$$

and

$$
\begin{aligned}
\sum_{n \leq x} \frac{\log n}{n} &= \int_1^x \frac{\log t}{t} dt + \int_1^x (t-[t]) \frac{1-\log t}{t^2} dt - (x-[x]) \frac{\log x}{x} \\
&= \frac{1}{2}\log^2 x + A(x).
\end{aligned}
$$

We note that

$$\begin{aligned}
|A(x)| &\leq \int_1^x \frac{\log t + 1}{t^2} dt + (x - [x]) \frac{\log x}{x} \\
&\leq \left[- \frac{\log t + 2}{t} \right]_1^x + (x - [x]) \frac{\log x}{x} \\
&\leq 2.
\end{aligned}$$

Thus

$$\begin{aligned}
\sum_{n \leq x} \frac{d(n)}{n} &= \sum_{d \leq x} \frac{1}{d} \sum_{q \leq \frac{x}{d}} \frac{1}{q} \leq \sum_{d \leq x} \frac{1}{d} \Big(\log \frac{x}{d} + C + \frac{d}{x} \Big) \\
&\leq \sum_{d \leq x} \Big(\frac{\log x + C}{d} - \frac{\log d}{d} + \frac{1}{x} \Big) \\
&\leq (\log x + C) \sum_{d \leq x} \frac{1}{d} - \sum_{d \leq x} \frac{\log d}{d} + 1 \\
&\leq (\log x + C) \Big(\log x + C + \frac{1}{x} \Big) - \Big(\frac{1}{2} \log^2 x + A(x) \Big) + 1 \\
&\leq \frac{1}{2} \log^2 x + 2C \log x + C^2 + 2 - A(x) + 1 \\
&\leq \frac{1}{2} \log^2 x + 2C \log x + 10. \qquad \square
\end{aligned}$$

Using (4.21), Lemma 4.4.1 and [Gol76, Lemma 7], we have

$$\begin{aligned}
&\sum_{A_0 \leq n \leq J} \tfrac{|b_n|}{\sqrt{n}} \\
\leq\ & \Big(\tfrac{1}{2} (\log \sqrt{\tfrac{J}{A_0}})^2 + 2C \log \sqrt{\tfrac{J}{A_0}} + 10 \Big) \\
& \times 1500 \Big(L(1, \chi)^2 J y^{-\frac{1}{2}} + L(1, \chi_d) J^{\frac{1}{2}} \Big) (\log y)^3 \\
\leq\ & (\log \tfrac{J}{A_0})^2 \big(2 \cdot 1500 L(1, \chi_d) J^{\frac{1}{2}} \big) (\log y)^3
\end{aligned}$$

$$
\begin{aligned}
&\le \big(20g\log\log A + 2\log\log\log A + 2\log(\kappa+6)\big)^2 \\
&\quad \times(3000L(1,\chi_d)\sqrt{A}(\kappa+6)\log\log A) \\
&\quad \times\big((2\kappa-2)\log\log A + 2\log\log\log A + \log\tfrac{N}{4\pi^2} + 2\log(\kappa+6)\big)^3 \\
&\le (3\cdot 20g\log\log A)^2 \\
&\quad \times(3000L(1,\chi_d)\sqrt{A}(\kappa+6)\log\log A) \\
&\quad \times(4\cdot(2\kappa-2)\log\log A)^3. \qquad (4.22)
\end{aligned}
$$

Using $\kappa \le g-1$, (4.20), (4.22) and the fact $n! \le e\sqrt{n}(\frac{n}{e})^n$, we have for $d \ge \exp\exp(400Ng^3)$,

$$
\begin{aligned}
|S_1| &\le 4^{\kappa+1}\kappa!(20g\log\log A)^\kappa\sqrt{A}\sum_{A_0\le n\le J}\tfrac{|b_n|}{\sqrt{n}} \\
&\le 3^2\cdot 4^3\cdot 3000(20g)^{\kappa+2}4^{\kappa+1}\kappa!(\kappa+6)(2\kappa-2)^3L(1,\chi_d)A(\log\log A)^{\kappa+6} \\
&\le 3^2\cdot 4^3\cdot 3000\cdot(20\cdot g\cdot(20g)^g)\cdot 4^g\cdot(g-1)!\cdot(2^3g^4)L(1,\chi_d)A(\log\log A)^{\kappa+6} \\
&\le 2^3\cdot 3^2\cdot 4^3\cdot 20\cdot 3000\cdot(20g)^g\cdot 4^g\cdot g!\cdot g^4L(1,\chi_d)A(\log\log A)^{\kappa+6} \\
&\le 2^3\cdot 3^2\cdot 4^3\cdot 20\cdot 3000\cdot e\cdot(\tfrac{80}{e})^g\cdot g^{2g+4.5}L(1,\chi_d)A(\log\log A)^{\kappa+6} \\
&= S_1^*. \qquad (4.23)
\end{aligned}
$$

Upper Bound for $|S_2|$. From [Gol76, (32)], we have

$$
|S_2| \le 4^{\kappa+1}(\kappa+1)!(\log\tfrac{A_1}{A})^\kappa\exp\big(-(\kappa+6)\log\log A\big)\sqrt{A}\sum_{J\le n\le A_1}\tfrac{|b_n|}{\sqrt{n}}. \qquad (4.24)
$$

(We note that the term $\sqrt{A}$ is missed in [Gol76, (32)].)

We may assume

$$
L(1,\chi_d) \le (\log d)^{\kappa-1}\tfrac{1}{\sqrt{d}} \quad (d > \exp\exp(400Ng^3)).
$$

Then we can choose

$$\begin{aligned} y &= L(1,\chi_d)^2 A_1 \\ &\le (\log A)^{2\kappa-2}\frac{A_1}{d} \\ &\le A_0. \end{aligned}$$

From [Gol76, (33)], we have

$$\begin{aligned} \sum_{J\le n\le A_1}\frac{|b_n|}{\sqrt{n}} &\le \sum_{k^2\le\frac{A_1}{A_0}}\frac{d(k)}{k}\sum_{A_0\le m\le\frac{A_1}{k^2}}\frac{1}{\sqrt{m}}\sum_{f|m}\nu_f\nu_{m/f} \\ &\le \Big(\sum_{k\le\sqrt{\frac{A_1}{A_0}}}\frac{d(k)}{k}\Big)\Big(\sum_{y\le m\le A_1}\frac{1}{\sqrt{m}}\sum_{f|m}\nu_f\nu_{m/f}\Big). \end{aligned} \tag{4.25}$$

(We note that we use $\frac{A_1}{A_0}$ instead of $\frac{A_1}{J}$ in [Gol76, (33)].)

Using (4.25), Lemma 4.4.1 and [Gol76, Lemma 7], we have

$$\begin{aligned} &\sum_{J\le n\le A_1}\frac{|b_n|}{\sqrt{n}} \\ \le\ & \Big(\frac{1}{2}(\log\sqrt{\frac{A_1}{A_0}})^2 + 2C\log\sqrt{\frac{A_1}{A_0}} + 10\Big) \\ & \times 1500\Big(L(1,\chi_d)^2 A_1 y^{-\frac{1}{2}} + L(1,\chi_d)A_1^{\frac{1}{2}}\Big)(\log y)^3 \\ \le\ & (\log\frac{A_1}{A_0})^2\big(2\cdot 1500 L(1,\chi_d)A_1^{\frac{1}{2}}\big)(\log y)^3 \\ \le\ & \big((20g+2)\log\log A + \log(2\kappa+8)\big)^2 \\ & \times\big(3000L(1,\chi_d)\sqrt{A}(2\kappa+8)\log A\big) \\ & \times\big(2\kappa\log\log A + \log\frac{N}{4\pi^2} + 2\log(2\kappa+8)\big)^3 \\ \le\ & \big(2\cdot(20g+2)\log\log A\big)^2 \\ & \times\big(3000L(1,\chi_d)\sqrt{A}(2\kappa+8)\log A\big) \\ & \times\big(3\cdot 2\kappa\log\log A\big)^3. \end{aligned} \tag{4.26}$$

Using $g-2 \le \kappa \le g-1$, (4.24), (4.26) and the fact $n! \le e\sqrt{n}(\frac{n}{e})^n$, we have for $d \ge \exp\exp(400Ng^3)$,

$$\begin{aligned}
|S_2| &\le 4^{\kappa+1}(\kappa+1)!\big(2\log\log A + 2\log(2\kappa+8)\big)^{\kappa}(\log A)^{-(\kappa+6)}\sqrt{A} \\
&\quad \times \sum_{J\le n\le A_1} \tfrac{|b_n|}{\sqrt{n}} \\
&\le 4^{\kappa+1}(\kappa+1)!\big(2\cdot 2\log\log A\big)^{\kappa}(\log A)^{-(\kappa+6)}\sqrt{A}\sum_{J\le n\le A_1}\tfrac{|b_n|}{\sqrt{n}} \\
&\le 2^2\cdot 3^3\cdot 3000\cdot 4\cdot 16^{\kappa}(\kappa+1)!(20g+2)^2(2\kappa+8)(2\kappa)^3 \\
&\quad \times L(1,\chi_d)A(\log A)^{-(\kappa+6)}(\log\log A)^{\kappa+5} \\
&\le 3^3\cdot 3000\cdot 16^{g}\cdot g!\cdot(20^2\cdot 2^7 g^6)\cdot(\log A)^{-(g+4)} \\
&\quad \times L(1,\chi_d)A(\log\log A)^{\kappa+5} \\
&\le 2^7\cdot 3^3\cdot 20^2\cdot 3000\cdot e\cdot(\tfrac{16}{e})^{g}\cdot g^{g+6.5}\cdot(400Ng^3)^{-(g+4)} \\
&\quad \times L(1,\chi_d)A(\log\log A)^{\kappa+5} \\
&< S_1^*.
\end{aligned} \tag{4.27}$$

Upper Bound for $|\mathbf{T}(g(s))|$. From [Gol76, p. 651], we have

$$|\mathbf{T}(g(s))| \le \kappa!\epsilon^{-\kappa}\cdot\max_{s\in\mathbf{C}}\left|\frac{1}{2\pi i}\int_{2\epsilon-i\infty}^{2\epsilon+i\infty} A^{s+z}\Gamma^2(s+z+\tfrac{1}{2})g(s+z)\varphi_1(2s+2z)\frac{dz}{z}\right|, \tag{4.28}$$

where $\mathbf{C}$ is the circle of radius $\epsilon = (\log d)^{-1}$ centered at $s = \frac{1}{2}$.

By the same argument in the proof of [Gol76, Lemma 7], we have for $x < d$ and $10^{10} < y < \min(\frac{1}{4}\sqrt{d}, x/10)$,

$$\sum_{y\le n\le x} n^{-\frac{1}{2}}\sum_{m|n}\nu_m\nu_{n/m} \le 1500(L(1,\chi_d)^2 d y^{-\frac{1}{2}} + L(1,\chi_d)x^{\frac{2}{5}}d^{\frac{1}{10}})(\log y)^3$$

instead of for $x < d$ and $10 < y < \min(\frac{1}{4}\sqrt{d}, x/10)$,

$$\sum_{y\le n\le x} n^{-\frac{1}{2}} \sum_{m|n} \nu_m \nu_{n/m} \ll (L(1,\chi_d)^2 d y^{-\frac{1}{2}} + L(1,\chi_d) x^{\frac{2}{5}} d^{\frac{1}{10}})(\log y)^3$$

in [Gol76, Lemma 8].

We may assume

$$L(1,\chi_d) \le (\log d)^{\kappa-1} \tfrac{1}{\sqrt{d}} \quad (d > \exp\exp(400Ng^3)).$$

Then by [Gol76, (40)], we have

$$\begin{aligned}
\max_{\substack{s\in\mathbf{T},\\ \mathrm{Re}(z)=2\epsilon}} |g(s+z)| &\le \sum_{U\le n\le A_0} n^{-\frac{1}{2}} \sum_{f|n} \nu_f \nu_{n/f} \\
&\le 1500\big(L(1,\chi_d)^2 dU^{-\frac{1}{2}} + L(1,\chi_d) A_0^{\frac{2}{5}} d^{\frac{1}{10}}\big)(\log U)^3 \\
&\le 1500 L(1,\chi_d)\sqrt{A} \\
&\quad \times\Big((\log d)^{\kappa-1} \tfrac{2\pi}{\sqrt{NU}} + (\log A)^{-8g}\big(\tfrac{4\pi^2}{N}\big)^{\frac{1}{10}}\Big)(\log U)^3. \quad (4.29)
\end{aligned}$$

(We use $dU^{-\frac{1}{2}}$ instead of $A_0 u^{-\frac{1}{2}}$ in [Gol76, (40)], so that it is a direct consequence of [Gol76, Lemma 8].)

By [Gol76, (41)], we have

$$\max_{\substack{s\in\mathbf{C},\\ \mathrm{Re}(z)=2\epsilon}} |\varphi_1(2s+2z)| \le \zeta^2(1-2\epsilon+4\epsilon) < \tfrac{1}{2}\epsilon^{-2}. \quad (4.30)$$

To estimate integral of Gamma function, using [Gol04, (4.6)],

$$\begin{aligned}
&\max_{s\in\mathbf{C}} \left| \tfrac{1}{2\pi i} \int_{2\epsilon-i\infty}^{2\epsilon+i\infty} A^{s+z}\Gamma^2(s+z+\tfrac{1}{2}) \tfrac{dz}{z} \right| \\
\le\ & A^{\frac{1}{2}+3\epsilon} \max_{s\in\mathbf{C}} \left| \int_0^\infty \int_0^\infty \Big(\tfrac{1}{2\pi i} \int_{2\epsilon-i\infty}^{2\epsilon+i\infty} (u_1u_2)^z \tfrac{dz}{z} \Big) e^{-u_1-u_2} (u_1u_2)^{s+\frac{1}{2}} \tfrac{du_1 du_2}{u_1u_2} \right|
\end{aligned}$$

$$
\begin{aligned}
&\le \; A^{\frac{1}{2}+3\epsilon}\int\int_{u_1u_2>1} e^{-u_1-u_2}(u_1u_2)^{1+\epsilon}\tfrac{du_1du_2}{u_1u_2}\\
&< \; A^{\frac{1}{2}+3\epsilon}.
\end{aligned}
\tag{4.31}
$$

Since $A \le d^2$, we have $A^{3\epsilon} \le d^{6\log_d e} \le e^6$. Thus by (4.28), (4.29), (4.30) and (4.31), we have for $d \ge \exp\exp(400Ng^3)$,

$$
\begin{aligned}
|\mathbf{T}(g(s))| \;&\le\; \kappa!\epsilon^{-\kappa}\cdot \max_{\substack{s\in\mathbf{C},\\ Re(z)=2\epsilon}} |g(s+z)\varphi_1(2s+2z)|\\
&\quad\times \max_{s\in\mathbf{C}}\left|\tfrac{1}{2\pi i}\int_{2\epsilon-i\infty}^{2\epsilon+i\infty} A^{s+z}\Gamma^2(s+z+\tfrac{1}{2})\tfrac{dz}{z}\right|\\
&\le\; \tfrac{1}{2}\cdot 1500\kappa!\epsilon^{-\kappa-2}\cdot L(1,\chi_d)A^{1+3\epsilon}\\
&\quad\times\Big((\log d)^{\kappa-1}\tfrac{2\pi}{\sqrt{NU}} + (\log A)^{-8g}\big(\tfrac{4\pi^2}{N}\big)^{\frac{1}{10}}\Big)(\log U)^3\\
&\le\; \tfrac{1}{2}\cdot 1500\cdot e^6\cdot\kappa!\cdot L(1,\chi_d)A\cdot(\log d)^{\kappa+2}\\
&\quad\times\Big((\log d)^{\kappa-1-4g}\tfrac{2\pi}{\sqrt{N}} + (\log A)^{-8g}\big(\tfrac{4\pi^2}{N}\big)^{\frac{1}{10}}\Big)(8g\log\log d)^3\\
&\le\; \tfrac{1}{2}\cdot 8^3\cdot 1500\cdot e^6\cdot g!\cdot g^3\cdot L(1,\chi_d)A\cdot(\log d)^{g+1}\\
&\quad\times\Big(2\cdot(\log d)^{-3g-2}\tfrac{2\pi}{\sqrt{N}}\Big)\cdot(\log\log d)^3\\
&\le\; 8^3\cdot 1500\cdot\tfrac{2\pi}{\sqrt{N}}\cdot e^{7-g}\cdot g^{g+3.5}\cdot(400Ng^3)^{-2g-1}\\
&\quad\times L(1,\chi_d)A(\log\log A)^3\\
&<\; S_1^*.
\end{aligned}
\tag{4.32}
$$

Upper Bound for $|2H-\mathbf{T}\big(G(s,U)\big)|$. We note that κ is determined so that $\delta = 1+(-1)^\kappa\chi_d(-N) = 2$. Then from [Gol76, (45)], we have

$$
\mathbf{T}(G(s,U)) = 2\cdot\tfrac{\kappa!}{2\pi i}\left[\int_{\mathbf{C}}(s-\tfrac{1}{2})^{-\kappa-1}\sum_{r=1}^{5} I_r(s)ds\right] \;+\; 2H, \tag{4.33}
$$

where $\mathbf{C}$ is the circle of radius $\frac{1}{2}\epsilon$ centered at $s = \frac{1}{2}$ and

$$I_1 = \int_{\frac{1}{8}+iM}^{\frac{1}{8}+i\infty}, \ I_2 = \int_{\frac{1}{8}-i\infty}^{\frac{1}{8}-iM}, \ I_3 = \int_{-\epsilon+iM}^{\frac{1}{8}+iM}, \ I_4 = \int_{\frac{1}{8}-iM}^{-\epsilon-iM}, \ I_5 = \int_{-\epsilon-iM}^{-\epsilon+iM}$$

of which the integrands are $\frac{1}{2\pi i}A^{s+z}\Gamma^2(s+z+\frac{1}{2})G(s+z,U)\varphi_1(2s+2z)\frac{dz}{z}$ and M is a large number to be determined later.

By [Gol76, (46)], for $\sigma > 0$,

$$|\Gamma(s)| \leq \sqrt{2\pi}\exp\left(\tfrac{1}{12\sigma}\right)|s|^{\sigma-\frac{1}{2}} \begin{cases} \exp(-\sigma) & \text{if } |\frac{\sigma}{t}| \geq \frac{\pi}{2} \\ \exp(-\frac{\pi}{2}|t|) & \text{if } |\frac{\sigma}{t}| \leq \frac{\pi}{2}. \end{cases} \tag{4.34}$$

From [Gol76, (47)], we have for $\mathrm{Re}(s+z) \geq 0$,

$$|G(s+z,U)| \leq (\log d)^{32g}. \tag{4.35}$$

To estimate $|\varphi_1(2s+2z)|$, we will use Lemma 4.3.1. Put $M = \log A$ and $\epsilon = (4\cdot 10^5 \log\log A)^{-1}$. Then we have

$$1 - \frac{1}{100800\log|\mathrm{Im}(2s+2z)|} \leq \mathrm{Re}(2s+2z) \quad \text{for} \quad z \in I_j \ (j = 1,2,3,4,5).$$

To estimate I_1, I_2, I_3 and I_4, we will use the fact that for $y > 1000$,

$$3\cdot(2y)^2\cdot(3y)^6\cdot y^{-1}\cdot e^{-3y} \leq 10^{-830}\cdot e^{-y}. \tag{4.36}$$

Firstly, we consider the integral I_1. For $z = \frac{1}{8} + iy, \quad M \leq y < \infty$, we write

$$\sigma = \mathrm{Re}(s+z+\tfrac{1}{2}) = \tfrac{9}{8} + \mathrm{Re}(\tfrac{\epsilon}{2}e^{i\theta}), \quad t = \mathrm{Im}(s+z+\tfrac{1}{2}) = y + \mathrm{Im}(\tfrac{\epsilon}{2}e^{i\theta}).$$

By applying (4.34), (4.35), (4.36) and Lemma 4.3.1 to the integral I_1, we have

$$\begin{aligned}
\max_{s\in\mathbf{C}}|I_1| &\leq \max_{\substack{s\in\mathbf{T},\\ \mathrm{Re}(z)=\frac{1}{8}}} |A^{s+z}G(s+z,U)| \\
&\quad \cdot \max_{s\in\mathbf{C}} \left| \int_{\frac{1}{8}+iM}^{\frac{1}{8}+i\infty} \frac{1}{2\pi i}\Gamma^2(s+z+\tfrac{1}{2})\varphi_1(2s+2z)\frac{dz}{z} \right| \\
&\leq 3\times 10^{12}\cdot N^3(\log d)^{32g}A^{\frac{5}{8}+\frac{\epsilon}{2}} \\
&\quad \cdot \max_{s\in\mathbf{C}} \int_{\frac{1}{8}+iM}^{\frac{1}{8}+i\infty} \exp\left(\tfrac{1}{6\sigma}\right)|s+z+\tfrac{1}{2}|^{2\sigma-1}\exp\left(-\pi t\right)(2t)^6|\tfrac{dz}{z}| \\
&\leq 3\times 10^{12}\cdot N^3(\log d)^{32g}A^{\frac{5}{8}+\frac{\epsilon}{2}} \\
&\quad \cdot \int_M^\infty 3(2y)^2\exp\left(-3y\right)(3y)^6 y^{-1}dy \\
&\leq 10^{-800}\cdot N^3(\log d)^{32g}A^{\frac{5}{8}+\frac{\epsilon}{2}}\int_M^\infty e^{-y}dy \\
&\leq 10^{-800}\cdot N^3(\log d)^{32g}A^{\frac{5}{8}+\frac{\epsilon}{2}}e^{-M}. \qquad (4.37)
\end{aligned}$$

Similarly

$$\max_{s\in\mathbf{C}}|I_2| \leq 10^{-800}\cdot N^3(\log d)^{32g}A^{\frac{5}{8}+\frac{\epsilon}{2}}e^{-M}. \qquad (4.38)$$

Secondly, we consider the integral I_3. For $z = x+iM, \quad -\epsilon \leq x < \frac{1}{8}$, we write

$$\sigma = \mathrm{Re}(s+z+\tfrac{1}{2}) = x+1+\mathrm{Re}(\tfrac{\epsilon}{2}e^{i\theta}), \quad t = \mathrm{Im}(s+z+\tfrac{1}{2}) = M+\mathrm{Im}(\tfrac{\epsilon}{2}e^{i\theta}).$$

By applying (4.34), (4.35), (4.36) and Lemma 4.3.1 to the integral I_3, we have

$$\max_{s\in\mathbf{C}}|I_3| \leq \max_{\substack{s\in\mathbf{C},\\ -\epsilon\leq \mathrm{Re}(z)\leq\frac{1}{8}}} |A^{s+z}G(s+z,U)|$$

$$
\begin{aligned}
& \cdot \max_{s\in\mathbf{C}} \left| \int_{-\epsilon+iM}^{\frac{1}{8}+iM} \tfrac{1}{2\pi i}\Gamma^2(s+z+\tfrac{1}{2})\varphi_1(2s+2z)\tfrac{dz}{z} \right| \\
\leq\ & 3\times 10^{12}\cdot N^3(\log d)^{32g}A^{\frac{5}{8}+\frac{\epsilon}{2}} \\
& \cdot \max_{s\in\mathbf{C}} \int_{-\epsilon+iM}^{\frac{1}{8}+iM} \exp\left(\tfrac{1}{6\sigma}\right)|s+z+\tfrac{1}{2}|^{2\sigma-1}\exp\left(-\pi t\right)(2t)^6|\tfrac{dz}{z}| \\
\leq\ & 3\times 10^{12}\cdot N^3(\log d)^{32g}A^{\frac{5}{8}+\frac{\epsilon}{2}} \\
& \cdot \int_{-\epsilon}^{\frac{1}{8}} 3(2M)^2\exp\left(-3M\right)(3M)^6M^{-1}dx \\
\leq\ & 10^{-800}\cdot N^3(\log d)^{32g}A^{\frac{5}{8}+\frac{\epsilon}{2}}e^{-M}. \qquad (4.39)
\end{aligned}
$$

Similarly

$$
\max_{s\in\mathbf{C}}|I_4| \leq 10^{-800}\cdot N^3(\log d)^{32g}A^{\frac{5}{8}+\frac{\epsilon}{2}}e^{-M}. \qquad (4.40)
$$

Finally, we will estimate the integral I_5. For $z=-\epsilon+iy,\quad -M\leq y\leq M$, we write

$$
\sigma = \mathrm{Re}(s+z+\tfrac{1}{2}) = 1-\epsilon+\mathrm{Re}(\tfrac{\epsilon}{2}e^{i\theta}), \quad t=\mathrm{Im}(s+z+\tfrac{1}{2}) = y+\mathrm{Im}(\tfrac{\epsilon}{2}e^{i\theta}).
$$

By applying (4.35) to the integral I_5, we have

$$
\begin{aligned}
\max_{s\in\mathbf{C}}|I_5| \leq\ & \max_{\substack{s\in\mathbf{C},\\ \mathrm{Re}(z)=-\epsilon}} |A^{s+z}G(s+z,U)| \\
& \cdot \max_{s\in\mathbf{C}} \left| \int_{-\epsilon-iM}^{-\epsilon+iM} \tfrac{1}{2\pi i}\Gamma^2(s+z+\tfrac{1}{2})\varphi_1(2s+2z)\tfrac{dz}{z} \right| \\
\leq\ & (\log d)^{32g}A^{\frac{1}{2}(1-\epsilon)} \\
& \cdot \max_{s\in\mathbf{C}} \int_{-\epsilon-iM}^{-\epsilon+iM} \tfrac{1}{2\pi}|\Gamma^2(s+z+\tfrac{1}{2})|\cdot|\varphi_1(2s+2z)|\cdot|\tfrac{dz}{z}|. \qquad (4.41)
\end{aligned}
$$

To apply (4.34) and Lemma 4.3.1 to the integral I_5, we consider the following four integrals. Let y_1, y_2 and y_3 as follows:

$$
\begin{aligned}
& \max_{s\in\mathbf{C}} \int_0^M \tfrac{1}{2\pi}|\Gamma^2(s+z+\tfrac{1}{2})|\cdot|\varphi_1(2s+2z)|\cdot\tfrac{dy}{\sqrt{\epsilon^2+y^2}} \\
\leq\ & \max_{s\in\mathbf{C}} \Big(\int_0^{\frac{1}{2\pi}(4-(6+\pi)\epsilon)} * + \int_{\frac{1}{2\pi}(4-(6+\pi)\epsilon)}^{\frac{1}{2\pi}(4+(\pi-2)\epsilon)} * + \int_{\frac{1}{2\pi}(4+(\pi-2)\epsilon)}^{2+\frac{1}{900}} * + \int_{2+\frac{1}{900}}^{M} * \Big) \\
=\ & \max_{s\in\mathbf{C}} \int_0^{y_1} * + \max_{s\in\mathbf{C}} \Big(\int_{y_1}^{y_2} * + \int_{y_2}^{y_3} * \Big) + \max_{s\in\mathbf{C}} \int_{y_3}^{M} *, \qquad (4.42)
\end{aligned}
$$

where $* = \frac{1}{2\pi}|\Gamma^2(s+z+\frac{1}{2})|\cdot|\varphi_1(2s+2z)|\cdot\frac{dy}{\sqrt{\epsilon^2+y^2}}$.

We note that for $0 \leq y \leq y_1$,

$$
\frac{\sigma}{t} \geq \frac{1-\frac{3\epsilon}{2}}{y_1+\frac{\epsilon}{2}} = \frac{\pi}{2}.
$$

Thus, by applying (4.34) and Lemma 4.3.1 to the first interval, we have

$$
\begin{aligned}
\max_{s\in\mathbf{C}} \int_0^{y_1} * \ \leq\ & 10^5\cdot N^3 \max_{s\in\mathbf{C}} \int_0^{y_1} \exp\left(\tfrac{1}{6\sigma}\right)|s+z+\tfrac{1}{2}|^{2\sigma-1}\exp(-2\sigma) \\
& \times \tfrac{1}{|2s+2z-1|}\tfrac{dy}{\sqrt{\epsilon^2+y^2}} \\
\leq\ & 10^5\cdot N^3 \int_0^{\frac{2}{\pi}} (y+1)\cdot\epsilon^{-2}dy \\
<\ & 10^5\cdot N^3\epsilon^{-2}. \qquad (4.43)
\end{aligned}
$$

We need the following observation to apply (4.34) to the second and third intervals. For $y_1 \leq y \leq y_2$, we have

$$
\begin{aligned}
& \max\Big\{\exp(-\sigma), \exp(-\tfrac{\pi}{2}|t|)\Big\} \\
\leq\ & \max\Big\{\exp\big(-(1-\tfrac{3\epsilon}{2})\big), \exp\big(-\tfrac{\pi}{2}(y_1-\tfrac{\epsilon}{2})\big)\Big\} \\
=\ & \exp(-1+\tfrac{3+\pi}{2}\epsilon).
\end{aligned}
$$

For $y_2 \le y \le y_3$, we have

$$\frac{\sigma}{t} \le \frac{1-\frac{\epsilon}{2}}{y_2-\frac{\epsilon}{2}} = \frac{\pi}{2}$$

and

$$\begin{aligned} & \exp\left(-\tfrac{\pi}{2}|t|\right) \\ \le\ & \exp\left(-\tfrac{\pi}{2}(y_2-\tfrac{\epsilon}{2})\right) \\ <\ & \exp\left(-1+\tfrac{3+\pi}{2}\epsilon\right). \end{aligned}$$

Thus, by applying (4.34) and Lemma 3.1 to the second and third interval, we have

$$\begin{aligned} \max_{s\in\mathbf{C}} \int_{y_1}^{y_3} * \ &\le\ 10^5 \cdot N^3 \max_{s\in\mathbf{C}} \int_{y_1}^{y_3} \exp\left(\tfrac{1}{6\sigma}\right)|s+z+\tfrac{1}{2}|^{2\sigma-1} \\ &\quad \times \exp\big(-2+(3+\pi)\epsilon\big)\tfrac{1}{|2s+2z-1|}\tfrac{dy}{\sqrt{\epsilon^2+y^2}} \\ &\le\ 10^5 \cdot N^3 \int_{\frac{1}{\pi}}^{y_3} (y+1)\cdot\pi\cdot\pi dy \\ &<\ 5\times 10^6 \cdot N^3. \end{aligned} \tag{4.44}$$

To estimate the fourth integral, we will use the fact that for $y \ge y_3$,

$$(y+1)\cdot(3y)^6\cdot y^{-1}\cdot e^{-3y} \le 2000\cdot e^{-y}.$$

Thus, by applying (4.34) and Lemma 4.4.1 to the fourth interval, we have

$$\begin{aligned} \max_{s\in\mathbf{C}} \int_{y_3}^{M} * \ &\le\ 3\cdot 10^{12}\cdot N^3 \\ &\quad \times \max_{s\in\mathbf{C}} \int_{y_3}^{M} \exp\left(\tfrac{1}{6\sigma}\right)|s+z+\tfrac{1}{2}|^{2\sigma-1}\exp(-\pi t)(2t)^6\tfrac{dy}{y} \end{aligned}$$

$$\begin{aligned}
&\leq 3\cdot 10^{12}\cdot N^3\int_{y_3}^{M}(y+1)\exp(-3y)(3y)^6y^{-1}dy\\
&\leq 3\cdot 10^{12}\cdot N^3\int_{y_3}^{M}2000e^{-y}dy\\
&< 9\times 10^{14}\cdot N^3. \qquad (4.45)
\end{aligned}$$

From (4.41), (4.42), (4.43), (4.44) and (4.45), we have

$$\begin{aligned}
|I_5| &\leq 2\cdot\Big(N^3(\log d)^{32g}A^{\frac{1}{2}(1-\epsilon)}\big(10^5\cdot\epsilon^{-2}+5\times 10^6+9\times 10^{14}\big)\Big)\\
&< N^3(\log d)^{32g}A^{\frac{1}{2}(1-\epsilon)}\cdot 2\cdot\big(10^5\cdot\epsilon^{-2}+10^{15}\big). \qquad (4.46)
\end{aligned}$$

Finally, by (4.33), (4.37), (4.38), (4.39), (4.40) and (4.46), we have

$$\begin{aligned}
&|2H-\mathbf{T}(G(s,U))|\\
=\ &\left|2\cdot\frac{\kappa!}{2\pi i}\int_{\mathbf{C}}(s-\tfrac{1}{2})^{-\kappa-1}\sum_{r=1}^{5}I_r(s)ds\right|\\
\leq\ &2^{\kappa+1}\kappa!\epsilon^{-\kappa}\sum_{r=1}^{5}\max_{s\in\mathbf{C}}|I_r(s)|\\
<\ &2^{\kappa+1}\kappa!\epsilon^{-\kappa}N^3(\log d)^{32g}\sqrt{A}\\
&\cdot\big(4\times 10^{-800}\cdot A^{\frac{1}{8}+\frac{\epsilon}{2}}e^{-M}+2\times 10^5\cdot A^{-\frac{\epsilon}{2}}\epsilon^{-2}+2\times 10^{15}\cdot A^{-\frac{\epsilon}{2}}\big)\\
<\ &2^{\kappa+1}\kappa!\epsilon^{-\kappa}N^3(\log d)^{32g}\sqrt{A}\cdot 3\cdot\big(2\times 10^5\cdot A^{-\frac{\epsilon}{2}}\epsilon^{-2}\big). \qquad (4.47)
\end{aligned}$$

For $d\geq\exp\exp(400Ng^3)$, we see that

$$2^{\kappa+1}\kappa!\epsilon^{-\kappa}N^3(\log d)^{32g}\cdot 3\cdot\big(2\times 10^5\cdot A^{-\frac{\epsilon}{2}}\epsilon^{-2}\big)<1,$$

so by (4.47), we have

$$|2H-\mathbf{T}(G(s,U))|<\sqrt{A}<S_1^*, \qquad (4.48)$$

as desired (cf. [Gol76, p. 656]).

Now we can prove Proposition 4.2.2

Proof of Proposition 4.2.2. We may assume

$$L(1,\chi_d) \leq (\log d)^{\kappa-1}\frac{1}{\sqrt{d}} \quad (d > \exp\exp(400Ng^3)).$$

From (4.19), (4.23), (4.27), (4.32) and (4.48), we have for $d \geq \exp\exp(400Ng^3)$,

$$\begin{aligned} & |2H| \\ \leq\ & |2H - \mathbf{T}(G(s,U))| + |T(g(s))| + |S_1| + |S_2| + 1 \\ \leq\ & 5S_1^* \\ <\ & 4\times 10^9 \cdot (\tfrac{80}{e})^g g^{2g+4.5} L(1,\chi) A (\log\log A)^{\kappa+6} \end{aligned}$$

and Proposition 4.2.2 immediately follows. $\square$

Chapter 5

Two proofs of Lemma 4.3.3 and applications

In this chapter, we prove Lemma 4.3.3 via two methods in section 5.1 and section 5.2, respectively. Also, section 5.2 contains a proof of Theorem 4.1.4. In section 5.3, we apply Theorem 4.1.2 to a certain family of real quadratic fields of narrow Richaud-Degert type.

5.1 Elliptic curves with complex multiplication

Recall that ψ is the primitive Grössencharakter of $K = \mathbb{Q}(\sqrt{-k})$ such that

$$L_E(s) = L_K(s, \psi).$$

From (4.7), we have

$$\begin{aligned} |\varphi_1'(1)| &= |L_K(2, \psi^2) L(1, \chi_k) \prod_{p|k} (1 - p^{-1})^{-1}| \\ &\geq |L_K(2, \psi^2) L(1, \chi_k)|. \end{aligned} \tag{5.1}$$

Proof of Lemma 4.3.3. Let ψ' be a primitive Grössencharakter with conductor $\mathfrak{f}'$ of $K = \mathbb{Q}(\sqrt{-k})$ which induces ψ^2. Then $\psi'(\langle\alpha\rangle) = \alpha^2$ for $\alpha \in K^{\mathfrak{f}'}$, i.e., of type $(2, 0)$. Since $L_E(s) = L_K(s, \psi)$, $L_K(s, \psi')$ is entire and has real coefficients.

We define (cf. [Gol76, p. 661])

$$F(s) = \zeta(s)L(s, \chi_k)L_K(s+1, \psi') = \sum_{n=1}^{\infty} c_n n^{-s},$$

where

$$c_1 = 1, \ \ c_n \geq 0 \ \text{(for } n > 1).$$

Since the Dirichlet series expansion of $F(s)$ is majorized by that of $\zeta(s)^4$, we have

$$c_n \leq \sum_{lm=n} d(l)d(m) \leq \sum_{lm=n} 4\sqrt{n} \leq 8n \quad \text{(for } n \geq 1) \tag{5.2}$$

where $d(k) = \sum_{f|k} 1 \leq 2\sqrt{k}$.

For fixed $x > 0$, we see that

$$\begin{aligned}
& \tfrac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \Gamma(s+1)F(s)x^s ds \\
= \ & \tfrac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\int_0^{\infty} e^{-u}u^s(\sum_{n=1}^{\infty} \tfrac{c_n}{n^s})x^s du ds \\
= \ & \tfrac{1}{2\pi i}\sum_{n=1}^{\infty} c_n \int_0^{\infty}\int_{2-i\infty}^{2+i\infty} (\tfrac{ux}{n})^s ds \cdot e^{-u} du \\
= \ & \sum_{n=1}^{\infty} \tfrac{c_n}{e^{n/x}} \\
\geq \ & e^{-1/x},
\end{aligned}$$

so we have

$$\begin{aligned} e^{-1/x} &\leq \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\Gamma(s+1)F(s)x^s ds \\ &= \Gamma(2)L(1,\chi_k)L_K(2,\psi')x + \frac{1}{2\pi i}\int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty}\Gamma(s+1)F(s)x^s ds. \qquad (5.3)\end{aligned}$$

The last integral in (5.3) can be estimated by using the following functional equations:

$$\zeta(s) = \pi^{s-\frac{1}{2}}\frac{\Gamma(\frac{1}{2}-\frac{s}{2})}{\Gamma(\frac{s}{2})}\zeta(1-s);$$
$$L(s,\chi_k) = (\tfrac{k}{\pi})^{\frac{1}{2}-s}\frac{\Gamma(1-\frac{s}{2})}{\Gamma(\frac{1}{2}+\frac{s}{2})}L(1-s,\chi_k);$$
$$L_K(s+1,\psi') = w(\tfrac{\sqrt{kN(f')}}{2\pi})^{1-2s}\frac{\Gamma(2-s)}{\Gamma(s+1)}L_K(2-s,\psi')$$

for some $w \in \mathbb{C},\ |w| = 1$.

Let $y = \frac{16\pi^4 x}{k^2 N(f')}$. Then by the duplication formula of Gamma function,

$$\begin{aligned} &\frac{1}{2\pi i}\int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty}\Gamma(s+1)F(s)x^s ds \\ &= w\frac{k\sqrt{N(f')}}{4\pi^2}\frac{1}{2\pi i}\int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty}\frac{\Gamma(1-s)}{\Gamma(s)}\Gamma(2-s)F(1-s)y^s ds. \qquad (5.4)\end{aligned}$$

Using (5.2) and the following properties of Bessel function $J_0(2\sqrt{t}) = \sum_{n=0}^{\infty}(-1)^n\frac{t^n}{(n!)^2}$;

$$0 \leq J_0(2\sqrt{t}) \leq \exp(-t) \quad \text{for} \quad t \geq 0,$$
$$\int_0^{\infty} J_0(2\sqrt{t})t^{-s}dt = \frac{\Gamma(1-s)}{\Gamma(s)},$$

we have

$$\frac{1}{2\pi i}\int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty}\frac{\Gamma(1-s)}{\Gamma(s)}\Gamma(2-s)F(1-s)y^s ds$$

$$
\begin{aligned}
&= \frac{1}{2\pi i}\int_{\frac{3}{2}-i\infty}^{\frac{3}{2}+i\infty}\frac{\Gamma(s)}{\Gamma(1-s)}\Gamma(s+1)F(s)y^{1-s}ds \\
&= \frac{1}{2\pi i}\sum_{n=1}^{\infty}\int_{\frac{3}{2}-i\infty}^{\frac{3}{2}+i\infty}\int_0^{\infty}\int_0^{\infty} J_0(2\sqrt{t})t^{s-1}\cdot u^s e^{-u}\cdot\frac{c_n}{n^s}\cdot y^{1-s}du\ dt\ ds \\
&= \sum_{n=1}^{\infty} c_n\int_0^{\infty}\int_0^{\infty}\frac{1}{2\pi i}\int_{\frac{3}{2}-i\infty}^{\frac{3}{2}+i\infty}(\frac{ut}{ny})^s ds\cdot J_0(2\sqrt{t})e^{-u}t^{-1}y\ du\ dt \\
&= \sum_{n=1}^{\infty} c_n\int\int_{ut=ny} J_0(2\sqrt{t})e^{-u}t^{-1}y\ du\ dt \\
&\leq \sum_{n=1}^{\infty}\frac{c_n}{n}\int\int_{ut=ny}\exp(-t)\exp(-u)\frac{ny}{t}\ du\ dt \\
&\leq 8\sum_{n=1}^{\infty}\int_0^{\infty}\exp(-t-\tfrac{ny}{t})\tfrac{ny}{t}dt. \qquad (5.5)
\end{aligned}
$$

Dividing integration with respect to t into two intervals $(0,\sqrt{ny})$ and $(\sqrt{ny},\infty)$, we have

$$
\begin{aligned}
& 8\sum_{n=1}^{\infty}\int_0^{\infty}\exp(-t-\tfrac{ny}{t})\tfrac{ny}{t}dt \\
&= 8\sum_{n=1}^{\infty}\Big(\int_0^{\sqrt{ny}}\exp(-t-\tfrac{ny}{t})\tfrac{ny}{t}dt+\int_{\sqrt{ny}}^{\infty}\exp(-t-\tfrac{ny}{t})\tfrac{ny}{t}dt\Big) \\
&\leq 8\sum_{n=1}^{\infty}\Big(\int_0^{\sqrt{ny}}\exp(-\tfrac{ny}{t})\tfrac{ny}{t}dt+\int_{\sqrt{ny}}^{\infty}\exp(-t)\tfrac{ny}{t}dt\Big) \\
&= 16\sum_{n=1}^{\infty}\int_{\sqrt{ny}}^{\infty}\exp(-t)\tfrac{ny}{t}dt \\
&\leq 16\sum_{n=1}^{\infty}\int_{\sqrt{ny}}^{\infty}\sqrt{ny}\exp(-t)dt \\
&= 16\sum_{n=1}^{\infty}\sqrt{ny}\exp(-\sqrt{ny}). \qquad (5.6)
\end{aligned}
$$

Now let $x = k^4N(\mathfrak{f}')^2$ so that $y = \frac{16\pi^4 x}{k^2N(\mathfrak{f}')} = 16\pi^4k^2N(\mathfrak{f}')$. Then by (5.4), (5.5) and

(5.6), we have

$$\begin{aligned}
&\left|\frac{1}{2\pi i}\int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty}\Gamma(s+1)F(s)x^s\,ds\right| \\
\leq\ & \frac{k\sqrt{N(\mathfrak{f}')}}{4\pi^2}\cdot 16\sum_{n=1}^{\infty}\sqrt{ny}\exp\left(-\sqrt{ny}\right) \\
\leq\ & \frac{k\sqrt{N(\mathfrak{f}')}}{4\pi^2}\cdot 16\cdot 5!\sum_{n=1}^{\infty}\frac{\sqrt{ny}}{(\sqrt{ny})^5} \\
\leq\ & \frac{k\sqrt{N(\mathfrak{f}')}}{4\pi^2}\cdot\frac{1}{(4\pi^2 k\sqrt{N(\mathfrak{f}')}\,)^4}\cdot 16\cdot 5!\sum_{n=1}^{\infty}\frac{1}{n^2} \\
<\ & (4\pi^2)^{-5}\cdot 16\cdot 5!\cdot\frac{\pi^2}{6} \\
<\ & 4\cdot 10^{-5}.
\end{aligned} \tag{5.7}$$

Since $x = k^4N(\mathfrak{f}')^2 \geq 3^4$, (5.3) and (5.7) give

$$|L_K(2,\psi')L(1,\chi_k)| \geq \frac{e^{-1/x}-4\cdot 10^{-5}}{x} \geq \frac{e^{-1/81}-4\cdot 10^{-5}}{k^4N(\mathfrak{f}')^2} \geq \frac{0.98}{k^4N(\mathfrak{f}')^2}.$$

From [Gol76, (4) and Theorem 2], we have

$$kN(\mathfrak{f}') \leq kN(\mathfrak{f}) = N$$

and by [Gol76, (59)], we have

$$|L_K(2,\psi^2)L(1,\chi_k)| \geq N^{-2}|L_K(2,\psi')L(1,\chi_k)| \geq \frac{0.98}{k^2N^4}. \qquad \square$$

5.2 Elliptic curves of symmetric square conductor greater than 11

5.2.1 A proof of Theorem 4.1.4

In [Gol76], Goldfeld remarked that Theorem 4.1.1 also holds for elliptic curves E without complex multiplication provided that $L_E(s)$ comes from a cusp form of $\Gamma_0(N)$, which is now true for every elliptic curves E over $\mathbb{Q}$ with conductor N according to the modularity theorem (cf. [Wil95], [TW95] and [BCDT01]). But he did not give the proof. In this section, we show that Theorem 4.1.1 works for elliptic curves without complex multiplication too and show that Theorem 4.1.4.

Remark 5.2.1. Let E be an elliptic curve with complex multiplication by an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-k})$. In the proof of Theorem 4.1.1, Goldfeld use the fact that $k \leq N$ as well as Deuring's theorem. In the proof of Theorem 4.1.2, we use the fact that $k \leq 163$ as well as Deuring's theorem. In the proof of Theorem 4.1.4, we use theory of the motivic (primitive) symmetric square L-function instead of Deuring's theorem. That is why there is a difference for exponents of N among Theorem 4.1.1, Theorem 4.1.2 and Theorem 4.1.4.

The following two propositions lead to Theorem 4.1.4 by the same proof as in the section 4.2.

Proposition 5.2.2. Assume the same conditions as in Theorem 4.1.4. Then for any such $d \geq \exp\exp(330Ng^3)$, either $L(1,\chi_d) > (\log d)^{g-\mu-1}\frac{1}{\sqrt{d}}$ or else

$$|H| \geq 1.2 \times 10^{-3} \cdot g\sqrt{N}(\log N)^{-1}\sqrt{d}(\log d)^{g-\mu-1} \prod_{\substack{\chi_d(p)\neq -1 \\ p<U}} \left(\frac{1-p^{-\frac{1}{2}}}{1+p^{-\frac{1}{2}}}\right)^2.$$

Proposition 5.2.3. Assume the same conditions as in Theorem 4.1.4. Then for any such $d \geq \exp\exp(330Ng^3)$, either $L(1, \chi_d) > (\log d)^{g-\mu-1}\frac{1}{\sqrt{d}}$ or else

$$|H| \leq 2 \times 10^9 \cdot (\tfrac{80}{e})^g g^{2g+4.5} L(1, \chi_d) A (\log\log A)^{g-\mu+6}.$$

Remark 5.2.4. Proposition 5.2.3 has the same result as in Proposition 4.2.2 except that we do not assume CM.

5.2.2 A proof of Proposition 5.2.2

Upper Bound for $|H_2|$. Following the notation in section 3.4.1, we write

$$L_E(s + \tfrac{1}{2}) = \tilde{L}(E, s) = \prod_p (1 - \alpha_p p^{-s})^{-1}(1 - \beta_p p^{-s})^{-1}. \tag{5.8}$$

Let F be a global minimal twist of E. From Definition 3.4.1 and (4.1), we have

$$\begin{aligned}
\varphi_1(s) &= \frac{L(\mathrm{Sym}_i^2 E, s)}{\zeta_{N_E}(s)} \\
&= \frac{L(\mathrm{Sym}_i^2 F, s)}{\zeta(s)} \times \prod_{p|N_E} (1 - p^{-s})^{-1} \\
&\quad \times \prod_{p \in S_1} \left\{ (1 - \alpha_p^2(F) p^{-s})(1 - p^{-s})(1 - \beta_p^2(F) p^{-s}) \right\} \times \prod_{p \in S_2} (1 - p^{-s-1}) \\
&= \frac{L(\mathrm{Sym}_p^2 F, s)}{\zeta(s)} \times \prod_{p|N_E} (1 - p^{-s})^{-1} \times \prod_{p^2|N_F} U_p(F, s)^{-1} \\
&\quad \times \prod_{p \in S_1} \left\{ (1 - \alpha_p^2(F) p^{-s})(1 - p^{-s})(1 - \beta_p^2(F) p^{-s}) \right\} \times \prod_{p \in S_2} (1 - p^{-s-1}).
\end{aligned} \tag{5.9}$$

The following lemma is a strong version of Lemma 4.3.1.

Lemma 5.2.5. For $s = \sigma + it \in \mathbb{C}$,

$$|\varphi_1(s)| \le \begin{cases} 2 \times 10^{10} \cdot NB^2 t^6 & \text{if } 1 - \frac{1}{100800 \log |t|} \le \sigma \le \frac{3}{2}, \quad |t| \ge 2 + \frac{1}{840}, \\ 2.5 \cdot NB^2 |s+2|^3 & \text{if } \frac{3}{4} \le \sigma \le \frac{3}{2}, \quad\quad\quad\quad\quad\quad |t| \le 2 + \frac{1}{840}, \end{cases}$$

where B is the symmetric conductor of E.

Proof. By the Euler product of $L(\mathrm{Sym}_p^2 F, s)$, we have

$$\left| L(\mathrm{Sym}_p^2 E, \tfrac{3}{2} - it) \right| \le \zeta(\tfrac{3}{2})^3 < 18.$$

From (3.3) we have

$$\begin{aligned} \left| L(\mathrm{Sym}_p^2 F, -\tfrac{1}{2} + it) \right| &= \frac{B^2}{\pi^3} \left| \frac{\Gamma(\frac{5}{4} - i\frac{t}{2})}{\Gamma(\frac{1}{4} + i\frac{t}{2})} \right|^2 \left| \frac{\Gamma(\frac{7}{4} - i\frac{t}{2})}{\Gamma(\frac{3}{4} + i\frac{t}{2})} \right| \\ &\quad \cdot \left| L(\mathrm{Sym}_p^2 F, \tfrac{3}{2} - it) \right| \\ &< 18 \frac{B^2}{\pi^3} \left| \frac{1}{4} + i\frac{t}{2} \right|^2 \left| \frac{3}{4} + i\frac{t}{2} \right| \\ &< 18 \frac{B^2}{8\pi^3} \left| \frac{3}{2} + it \right|^3 . \end{aligned}$$

Hence, the function

$$f(s) = L(\mathrm{Sym}_p^2 F, s)(s+2)^{-3}$$

is bounded by

$$C = 18 \frac{B^2}{8\pi^3}$$

on the lines $\sigma = -\frac{1}{2}$ and $\sigma = \frac{3}{2}$. By Lindelöf theorem (cf. [HR15, p. 15]), this implies that

$$\left| L(\mathrm{Sym}_p^2 F, s) \right| \le 18 \frac{B^2}{8\pi^3} |s+2|^3 \quad (-\tfrac{1}{2} \le \sigma \le \tfrac{3}{2}). \tag{5.10}$$

By (3.5), we have for $\sigma \geq 3/4$

$$\begin{aligned}
&\left|\prod_{p|N_E}(1-p^{-s})^{-1}\right| \times \left|\prod_{p^2|N_F} U_p(F,s)^{-1}\right| \\
&\times \left|\prod_{p\in S_1}\left\{(1-\alpha_p^2(F)p^{-s})(1-p^{-s})(1-\beta_p^2(F)p^{-s})\right\}\right| \times \left|\prod_{p\in S_2}(1-p^{-s-1})\right| \\
\leq\ & \prod_{p|N_E}\frac{1}{1-|p^{-s}|}\prod_{p^2|N_E}(1+|p^{-s}|)^3 \\
\leq\ & \prod_{p\|N_E}\frac{1}{1-|p^{-s}|}\prod_{p^2|N_E}(1+|p^{-s}|)^2\frac{1+|p^{-s}|}{1-|p^{-s}|} \\
\leq\ & \prod_{p\|N_E}\frac{p^{3/4}}{p^{3/4}-1}\prod_{p^2|N_E}\left(\frac{p^{3/4}+1}{p^{3/4}}\right)^2\frac{p^{3/4}+1}{p^{3/4}-1}.
\end{aligned}$$

Since

$$\begin{array}{llll}
\frac{2^{3/4}}{2^{3/4}-1} < 1.3\cdot 2 & \text{and} & \frac{p^{3/4}}{p^{3/4}-1} < p & \text{for} \quad p \geq 3, \\
\left(\frac{2^{3/4}+1}{2^{3/4}}\right)^2 < 1.3\cdot 2 & \text{and} & \left(\frac{p^{3/4}+1}{p^{3/4}}\right)^2 < p & \text{for} \quad p \geq 3, \\
\frac{2^{3/4}+1}{2^{3/4}-1} < 2\cdot 2 & \text{and} & \frac{p^{3/4}+1}{p^{3/4}-1} < p & \text{for} \quad p \geq 3,
\end{array}$$

from (5.9) we have for $\sigma \geq 3/4$

$$|\varphi_1(s)| \leq 2.6\cdot N_E \cdot \left|\frac{L(\mathrm{Sym}_p^2 F, s)}{\zeta(s)}\right|. \tag{5.11}$$

Thus Lemma 5.2.5 follows from Lemma (4.9), (5.9), (5.10) and (5.11). $\square$

Remark 5.2.6. In [Gol76, (49)] and Lemma 4.3.1, Deuring's Theorem and functional equation for the Hecke L-function are used to give upper bound for $\varphi_1(s)$ in the case of elliptic curves with complex multiplication. To remove complex multiplication condition, we use functional equation for the primitive symmetric square L-function. We also note that $B \leq N$ (because $B \mid N$) and so Lemma 5.2.5 implies Lemma 4.3.1.

From Lemma 5.2.5, we have

$$\begin{aligned}\max_{s\in\mathbf{C_2}}|\varphi_1(2s)| &\leq \max_{s\in\mathbf{C_2}}(2.5\cdot N^3|2s+2|^3)\\ &\leq 90N^3. \end{aligned}\tag{5.12}$$

Thus from (4.5), (4.6), (4.13) and (5.12) we have

$$|H_2| \leq 6\cdot 10^4 N^3 g^2\sqrt{A}(\log A)^{\kappa-2}\prod_{\substack{\chi_d(p)\neq -1\\ p<U}}(1-p^{-\frac{1}{4}})^{-4}.\tag{5.13}$$

Lower Bound for $|H_1|$. We use Watkins' result:

Lemma 5.2.7. [Wak, Lemma 3.4] Let E be an elliptic curve over $\mathbb{Q}$ of which the symmetric square conductor satisfies $B > 11$. Then

$$L(\mathrm{Sym}_p^2 E, 1) \geq \frac{0.033}{2\log B}.$$

Lemma 5.2.7 implies the following lemma, which is a generalization of Lemma 4.3.3.

Lemma 5.2.8. Let E be an elliptic curve over $\mathbb{Q}$ of which the symmetric square conductor is greater than 11. Then

$$\varphi_1'(1) = \left(\frac{d}{ds}\Big|_{s=1}\frac{L(\mathrm{Sym}_i^2 E)}{\zeta_{N_E}(s)}\right) \geq \frac{0.033}{2\log N}.$$

Proof. From (3.5) and (5.9) we have

$$\begin{aligned}\varphi_1'(1) \;=\; & L(\mathrm{Sym}_p^2 F, 1)\times\prod_{p|N_E}(1-p^{-1})^{-1}\times\prod_{p^2|N_F}U_p(F,1)^{-1}\\ &\times\prod_{p\in S_1}\left\{(1-\alpha_p^2(F)p^{-1})(1-p^{-1})(1-\beta_p^2(F)p^{-1})\right\}\times\prod_{p\in S_2}(1-p^{-2})\end{aligned}$$

$$\begin{aligned}
&\geq L(\mathrm{Sym}_p^2 F, 1) \times \prod_{p \mid N_E} (1-p^{-1})^{-1} \times \prod_{p^2 \mid N_F} (1-p^{-1}) \\
&\quad \times \prod_{p \in S_1} \left\{(1+p^{-2})(1-p^{-1})\right\} \times \prod_{p \in S_2} \left\{(1+p^{-1})(1-p^{-1})\right\} \\
&\geq L(\mathrm{Sym}_p^2 F, 1) \times \prod_{p \mid N_E} (1-p^{-1})^{-1} \times \prod_{p^2 \mid N_E} (1-p^{-1}) \\
&= L(\mathrm{Sym}_p^2 F, 1) \times \prod_{p \| N_E} (1-p^{-1})^{-1} \\
&\geq L(\mathrm{Sym}_p^2 F, 1) \\
&\geq \frac{0.033}{2 \log B}. \qquad \square
\end{aligned}$$

By Lemma 4.3.2 and Lemma 5.2.8, we have *for* $d > \exp(500g^3)$, *either* $L(1, \chi_d) > (\log d)^{\kappa-1} \frac{1}{\sqrt{d}}$ *or else*

$$|H_1| \geq 2\kappa \frac{0.033}{2 \log N} \cdot \sqrt{A} (\log A)^{\kappa-1} \left(\prod_{\substack{\chi_d(p) \neq -1 \\ p < U}} \left(\frac{1-p^{-\frac{1}{2}}}{1+p^{-\frac{1}{2}}} \right)^2 - (\log d)^{-2g} \right). \quad (5.14)$$

Now we can prove Proposition 5.2.2.

Proof of Proposition 5.2.2. We may assume

$$L(1, \chi_d) \leq (\log d)^{\kappa-1} \tfrac{1}{\sqrt{d}} \ \ (d > \exp(500g^3)).$$

From (5.13) and (5.14), we have

$$\begin{aligned}
|H| &\geq |H_1| - |H_2| \\
&\geq \left[2\kappa \tfrac{0.033}{2 \log N} \cdot \sqrt{A} (\log A)^{\kappa-1} \prod_{\substack{\chi_d(p) \neq -1 \\ p < U}} \left(\tfrac{1-p^{-\frac{1}{2}}}{1+p^{-\frac{1}{2}}} \right)^2 \right]
\end{aligned}$$

$$
\begin{aligned}
& -\Big[2\kappa\tfrac{0.033}{2\log N}\cdot\sqrt{A}(\log A)^{\kappa-1}(\log d)^{-2g} \\
& \qquad +6\cdot 10^4 N^3 g^2\sqrt{A}(\log A)^{\kappa-2}\prod_{\substack{\chi_d(p)\neq -1\\ p<U}}(1-p^{-\frac{1}{4}})^{-4}\Big] \\
= \;& \tilde{H}_1-\tilde{H}_2.
\end{aligned}
$$

If $\frac{1}{2}\tilde{H}_1\geq\tilde{H}_2$, then we have

$$
\begin{aligned}
|H| &\geq \frac{\tilde{H}_1}{2} \\
&\geq \kappa\frac{0.033}{2\log N}\cdot\sqrt{A}(\log A)^{\kappa-1}\prod_{\substack{\chi(p)\neq -1\\ p<U}}\left(\frac{1-p^{-\frac{1}{2}}}{1+p^{-\frac{1}{2}}}\right)^2 \\
&\geq \frac{0.033}{4}\cdot g(\log N)^{-1}\sqrt{A}(\log A)^{\kappa-1}\prod_{\substack{\chi(p)\neq -1\\ p<U}}\left(\frac{1-p^{-\frac{1}{2}}}{1+p^{-\frac{1}{2}}}\right)^2 \\
&\geq 1.2\times 10^{-3}\cdot g\sqrt{N}(\log N)^{-1}\sqrt{d}(\log d)^{\kappa-1}\prod_{\substack{\chi(p)\neq -1\\ p<U}}\left(\frac{1-p^{-\frac{1}{2}}}{1+p^{-\frac{1}{2}}}\right)^2
\end{aligned}
$$

as desired.

We see that

$$
\begin{aligned}
\frac{\tilde{H}_2}{\tilde{H}_1} &= \frac{6\cdot 10^4 N^3 g^2\sqrt{A}(\log A)^{\kappa-2}\prod_{\substack{\chi_d(p)\neq -1\\ p<U}}(1-p^{-\frac{1}{4}})^{-4}}{2\kappa\frac{0.033}{2\log N}\cdot\sqrt{A}(\log A)^{\kappa-1}\prod_{\substack{\chi_d(p)\neq -1\\ p<U}}\big(\frac{1-p^{-\frac{1}{2}}}{1+p^{-\frac{1}{2}}}\big)^2} \\
&\quad +\frac{(\log d)^{-2g}}{\prod_{\substack{\chi_d(p)\neq -1\\ p<U}}\big(\frac{1-p^{-\frac{1}{2}}}{1+p^{-\frac{1}{2}}}\big)^2} \\
&\leq \frac{6\cdot 10^4}{0.033(g-2)}\cdot N^3(\log N)g^2(\log d)^{-1}\prod_{\substack{\chi_d(p)\neq -1\\ p<U}}\left(\frac{1+p^{-\frac{1}{2}}}{1-p^{-\frac{1}{2}}}\right)^2\cdot\left(\frac{1}{1-p^{-\frac{1}{4}}}\right)^4
\end{aligned}
$$

$$
\begin{aligned}
&+(\log d)^{-2g} \prod_{\substack{\chi_d(p)\neq -1 \\ p<U}} \left(\tfrac{1+p^{-\frac{1}{2}}}{1-p^{-\frac{1}{2}}}\right)^2 \\
\leq\ & 2\cdot\Big(\frac{6\cdot 10^7}{33(g-2)}\cdot N^3(\log N)g^2(\log d)^{-1} \prod_{\substack{\chi_d(p)\neq -1 \\ p<U}} \left(\tfrac{1+p^{-\frac{1}{2}}}{1-p^{-\frac{1}{2}}}\right)^2 \cdot \left(\tfrac{1}{1-p^{-\frac{1}{4}}}\right)^4\Big).
\end{aligned}
$$

By (4.16), the sufficient condition of $\frac{1}{2}\tilde{H}_1 \geq \tilde{H}_2$ is that

$$
\log\log d - 6\left(\tfrac{g}{\log 2}\log\log d\right)^{\frac{3}{4}} \geq \log\left(4\cdot\frac{6\cdot 10^7}{33}N^3(\log N)\tfrac{g^2}{g-2}\right). \tag{5.15}
$$

We write $d \geq \exp\exp(c_1 N g^3)$ and assume $g \geq 3$. If c_1 is sufficiently large, the left hand in (5.15) is greater than

$$
c_1 N g^3 - 6\left(\tfrac{1}{\log 2}c_1 N g^4\right)^{\frac{3}{4}} = g^3\left(c_1 N - \tfrac{6}{(\log 2)^{3/4}}c_1^{3/4}N^{3/4}\right),
$$

and the right hand in (5.15) is less than

$$
16 + 3\log N + \log\log N + \log\tfrac{g^2}{g-2}.
$$

Since $g \geq 3$ and $N \geq 12$ (because $B \geq 12$), a sufficient condition of $\frac{1}{2}\tilde{H}_1 \geq \tilde{H}_2$ is that $c_1 \geq 324.7$. For convenience, if we choose $c_1 = 330$, then Proposition 5.2.2 follows. □

5.2.3 A proof of Proposition 5.2.3

Proof of Proposition 5.2.3. We may assume

$$
L(1,\chi_d) \leq (\log d)^{\kappa-1}\tfrac{1}{\sqrt{d}} \quad (d > \exp\exp(330 N g^3) \text{ and } N \geq 12).
$$

By section 4.4, we have for $d > \exp\exp(330Ng^3)$,

$$\begin{cases} |S_1| \leq S_1^*, \\ |S_2| \leq S_1^*, \\ |T(g(s))| \leq S_1^*. \end{cases} \tag{5.16}$$

Since Lemma 5.2.5 implies Lemma 4.3.1 (cf. Remark 5.2.6), we have for $d > \exp\exp(330Ng^3)$,

$$|2H - T(G(s,U))| \leq S_1^*. \tag{5.17}$$

By (4.19), (5.16) and (5.17) we have

$$\begin{aligned} & |2H| \\ \leq \;& 5S_1^* \\ < \;& 4 \times 10^9 \cdot (\tfrac{80}{e})^g g^{2g+4.5} L(1,\chi) A (\log\log A)^{\kappa+6} \end{aligned}$$

and Proposition 5.2.3 immediately follows. □

5.3 Applications

Finally, as an application, we give the following explicit lower bound for class numbers of certain real quadratic fields of narrow R-D type.

Theorem 5.3.1. Let m be an integer and $d_m = 4199^2(2m)^4 - 1$ be a square-free integer. Then for any $d_m \geq \exp\exp(3 \times 10^{13})$, we have

$$h(d_m) > 9 \times 10^{121} \cdot (\log d_m)^{1-10^{-10}}.$$

Proof. Let $E : y^2 = x^3 - 4199^2 x$ be an elliptic curve over $\mathbb{Q}$ of conductor $N = 32 \cdot 4199^2$. It is known that E has complex multiplication by $\mathbb{Q}(\sqrt{-1})$ and analytic rank $g_1 \geq 3$ (cf. [Elk94]).

Let $d_m = 4199^2(2m)^4 - 1$ be a square-free integer and $E_{d_m} : y^2 = x^3 - 4199^2(d_m)^2 x$ be the quadratic twist of E. Then E_{d_m} has a rational point $(4199^2(2m)^2 d_m, 4199^2(2m) d_m^2)$ of infinite order (cf. [Kob84, Proposition 17 in p. 44]). By [CW77, Theorem 1], E_{d_m} has analytic rank $g_{d_m} \geq 1$. We note that $4199 d_m \equiv 1 \pmod 8$, so E_{d_m} has the root number 1 (cf. [Kob84, Theorem in p. 84]) and has even analytic rank. Thus E_{d_m} has analytic rank $g_{d_m} \geq 2$ and $L_{E/\mathbb{Q}(\sqrt{d_m})}$ has a zero of order $g_1 + g_{d_m} \geq g = 5$ at $s = 1$.

For the real quadratic field $\mathbb{Q}(\sqrt{d_m})$, the fundamental unit $\epsilon_{d_m} = \sqrt{d_m + 1} + \sqrt{d_m} < d_m$. Since $(d_m, N) = 1$, by Theorem 4.1.2, for any

$$d_m > \exp\exp(400 \cdot 32 \cdot 4199^2 \cdot 5^3),$$

we have

$$h(d_m) \;>\; \frac{10^{180}}{2 \cdot 5^{20} \cdot (32 \cdot 4199^2)^5} (\log d_m) \exp(-21\sqrt{5 \log\log d_m}).$$

We note that if $d_m > \exp\exp(400 \cdot 32 \cdot 4199^2 \cdot 5^3)$, then for $\epsilon > 10^{-10}$,

$$\exp(21\sqrt{5 \log\log d_m})) < (\log d_m)^{\epsilon}.$$

Thus we have for any $d_m \geq \exp\exp(3 \times 10^{13})$,

$$h(d_m) > 9 \times 10^{121} \cdot (\log d_m)^{1-10^{-10}}. \quad \square$$

Remark 5.3.2. The above elliptic curve has the symmetric square conductor $B = 8$. Also, Elkies [Elk94] lists the 75 (4199 is the smallest integer.) values of $n < 2 \cdot 10^5$ with $n \equiv 7 \pmod 8$ for which the elliptic curve $E_n : y^2 = x^3 - n^2 x$ has analytic rank at least 3. We can apply the proof of Theorem 5.3.1 to such n.

Chapter 6

Further progress and research questions

As an application, Theorem 5.3.1 is not useful because it works for $d_m \geq \exp\exp(3 \times 10^{13})$, and the value is too large to classify real quadratic fields of R-D type with class number. The condition

$$d \geq \exp\exp(c_1 N g^3)$$

in Theorem 4.1.1 is mainly determined by the inequality (4.17). For the left-hand side in (4.17) to be positive, one asks for d to be greater than '$\exp\exp(3800)$' (because $6^4/\log^3 2 > 3800$) regardless of any invariants of an elliptic curve.

Recently, we have modified Oesterlé's method to apply real quadratic fields and it finally works. This method asks for d to be greater than '1'. Indeed, it makes a difference to use the partial Euler product of

$$\frac{L(E \otimes \chi_d, s)}{L(E \otimes \lambda, s)}$$

in Oesterlé's method, instead of the partial Dirichlet's series of that in Goldfeld's (cf. (4.2) in Section 4.2). In this case, the inequality is of slightly different form as follows:

$$\begin{cases} h(d)R(d) & \geq c_E(\log d)^{g-3}\theta(d) \quad \text{for any } d > 1, \\ h(d) & \geq c_2(\log d)^{g-4}\theta(d) \quad \text{for R-D type,} \end{cases}$$

where $\theta(d) = \prod_{p \in P(d)} \left(1 - \frac{\lfloor 2\sqrt{p} \rfloor}{p+1}\right)$ and $P(d)$ is the set of prime divisors of d except maximal one. We proved that c_E is given by

$$c_E = \frac{1}{2^{g+1}} \frac{L(\mathrm{Sym}_i^2 E, 1)}{\sqrt{N_E}} \cdot \prod_{i=1}^{g-3} \frac{(q_i - 1)(\sqrt{q_i} - 1)^2}{(q_i + 1)(\sqrt{q_i} + 1)^2},$$

where q_i is the i^{th} smallest splitting prime in the extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$.

We also used computer program to approximate c_2 via Lavrick's numerical method for the completed primitive symmetric square L-function attached to the same elliptic curve in Theorem 5.3.1 (cf. [Coh00, Appendix A], [Del03], [Dok04]). Hence we obtained that for any square-free integer

$$d_m = 4199^2(2m)^4 - 1,$$

we have

$$h(d_m) \geq 7.2 \times 10^{-10} \cdot (\log d_m)\theta(d_m)$$

(cf. [BK]).

The constant $c_2 = 7.2 \times 10^{-10}$, however, is too small to apply the inequality $h \leq 3$. For example, Watkins [Wak04] used $|d| \leq \exp(2.7 \times 10^8)$, which came from Oesterlé's theorem, to solve class number problem up to 100 for imaginary quadratic fields. Watkins mentioned that the computation took about seven months based on his intensive computer program.

Because c_E is mainly determined by $\frac{1}{\sqrt{N_E}}$, the following question is essential. How can we find an elliptic curve over $\mathbb{Q}$ with small conductor such that there exists a family of its twisted elliptic curves of high analytic rank?

Also, we note that using the following elliptic curve

$$y^2 + y = x^3 - 79x + 342, \quad N = 19047851$$

of algebraic rank 5, one can try to solve the class number problem for real quadratic fields of R-D type under the BSD rank conjecture.

Bibliography

[Apo76] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, New York, 1976.

[Bak69] A. Baker, *Linear forms in logarithms of algebraic numbers*, Mathematika, **13** (1969), 283-294.

[Bak71] A. Baker, *Imaginary quadratic fields with class number two*, Ann. of Math. (2) **94** (1971), 139-152.

[BCDT01] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic cuves over* $\mathbb{Q}$ *: wild* 3*-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843-939.

[BK18] D. Byeon and J. Kim, *An explicit lower bound for special values of Dirichlet* L*-functions*, J. Number Theory **189** (2018), 272-303.

[BK19] D. Byeon and J. Kim, *An explicit lower bound for special values of Dirichlet* L*-functions II*, J. Number Theory **205** (2019), 194-209.

[BK] D. Byeon and J. Kim, *Class numbers of real quadratic fields*, in preparation.

[BKL07] D. Byeon, M. Kim and J. Lee, *Mollin's conjecture*, Acta Arith. **126** (2007), 99-114.

[Cho48] S. Chowla, *Improvement of a theorem of Linnik and Walfisz*, Proceedings of the London Mathematical Society **50** (1948), 423-429.

[CS87] J. Coates and C. Schmidt, *Iwasawa Theory for the symmetric square of an elliptic curve*, J. Reine Angew. Math (1987), 104-156.

[CW77] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), 223-251.

[Coh00] H. Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics **193**, Springer-Verlag, New York, 2000.

[Deg58] G. Degert, *Über die Bestimmung der Grundeinheit gewisser reell-quadratischer Zhalkörper*, Abh. Math. Sem. Univ. Hamburg **22** (1958), 92-97.

[Del03] C. Delaunay, *Computing modular degrees using L-functions*, J. de Théorie Nombres de Bordeaux **15** (2003), 673-682.

[Deu33] M. Deuring, *Imaginär-quadratische Zahlkörper mit der Klassenzahl* (1), Math. Z. **37** (1933), 405-415.

[Dir] L. Dirichlet, *Recherches sur diverse applications de l'analyse infinitésimale à la théorie des nombres*, I, J. Reine Angew. Math. **19** (1839), 324-369; II, **21** (1840), 1-12.

[Dok04] T. Dokchitser, *Computing special values of motivic L-functions*, Exp. Math. **13** (2004), 137-149.

[Elk94] N. D. Elkies, *Heegner point computations*, Algorithmic number theory (Ithaca, New York, 1994), Lecture Notes in Compu. Sci. **877**, Springer-Verlag, Berlin, 1994, pp. 122-133.

[Gau] C. F. Gauss, *Disquisitiones Arithmeticae*, Göttengen (1801); English translation by A. Clarke, revised by W. Waterhouse, 1986 Springer-Verlag reprint of the Yale University Press, New Haven 1966 edition.

[Gha03] E. Ghate, *Complex multiplication*, in: A. K. Bhandari, D. S. Nagaraj, B. Ramakrishnan, T. N. Venkataramana (Eds.), Elliptic Curves, Modular Forms and Cryptography, Hindustan Book Agency, Gurgaon, 2003.

[Gol74] D. Goldfeld, *A simple proof of Siegel's theorem*, Proc. Nat. Acad. Sci. U.S.A. **71** (1974), 1055.

[Gol76] D. Goldfeld, *The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer*, Ann. Sc. Norm. Super. Pisa (4) **3** (1976), 623-663.

[Gol04] D. Goldfeld, *The Gauss class number problem for imaginary quadratic fields*, in: H. Darmon, S. Zhang (Eds.), Heegner Points and Rankin L-Series, Cambridge University Press, 2004.

[GHL94] D. Goldfeld, J. Hoffstein and D. Lieman, appendix to [HL94].

[Gro11] B. Gross, *Lectures on the Conjecture of Birch and Swinnerton-Dyer*, in: C. Popescu, K. Rubin, A. Silverberg (Eds.), Arithmetic of L-functions, IAS/Park City Math. Ser. **18**, Amer. Math. Soc., Providence, RI, 2011.

[GZ83] B. Gross and D. Zagier, *Points de Heegner et dérivées de fonctions L*, C. R. Acad. Sci. ParisSér. I Math. **297** (1983), 85-87.

[HK89] F. Halter-Koch, *Reell-quadratischer Zahlkörper mit größer Grundeinheit*, Abh. Math. Sem. Univ. Hamburg **59** (1989), 171-181.

[HR15] G. H. Hardy and M. Riesz, *The General Theory of Dirichlet's Series*, Cambridge University Press, 1915.

[HB83] D. R. Heath-Brown, *Prime twins and Siegel zeros*, Proc. London Math. Soc. (3) **47** (1983), 193-224.

[Hee52] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. **56** (1952), 227-253.

[Hei34] H. Heilbronn, *On the class number in imaginary quadratic fields*, Quart. J. Math. Oxford Ser. 2 **5** (1934), 150-160.

[Hof80] J. Hoffstein, *On the Siegel-Tatuzawa theorem*, Acta Arith. **38** (1980), 167-174.

[HL94] J. Hoffstein and P. Lockhart, *Coefficients of Mass forms and the Siegel zero*, Ann. of Math. (2) **140**, (1994), 161-181.

[JLW95] M. J. Jacobson, Jr., R. F. Lukes, and H. C. Williams, *An investigation of bounds for the regulator of quadratic fields*, Experiment. Math **4** (1995), 211-225.

[Jam03] G. J. O. Jameson, *The Prime Number Theorem*, Cambridge University Press, 2003.

[Kob84] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Graduate Texts in Mathematics **97**, Springer-Verlag, New York, 1984.

[Lan18] E. Landau, *Über die Klassenzahl imaginär-quadratischer Zahlkörper*, Göttinger Nachrichten (1918), 285-295.

[Lan35] E. Landau, Bemerkungen zum Heilbronnschen Satz, Acta Arith. **1** (1935), 1-18.

[Lit28] J. E. Littlewood, *On the class-number of the corpus* $\mathsf{P}(\sqrt{-\mathsf{k}})$, Proc. London Math. Soc. (2) **27** (1928), 358-372.

[Mol96] R. A. Mollin, *Quadratics*, CRC Press, Boca Raton, New York, London, Tokyo, 1996.

[Mor34] L. J. Mordell, *On the Riemann hypothesis and imaginary quadratic fields with a given class number*, J. London Math. Soc. **9** (1934), 289-298.

[Neu99] J. Neukirch, *Algebraic number theory*, translated from the 1992 German original by N. Schappacher, Grundlehren der Mathematischen Wissenschaften **322**, Springer-Verlag, Berlin,1999.

[Oes85] J. Oesterlé, *Nombres de classes des corps quadratiques imaginaires*, Astérique **121-122**, 309-323 (1985), 309-323.

[Oes88] J. Oesterlé, *Le problème de Gauss sur le nombre de classes*, Enseign. Math. **34** (1988), 43-67.

[Ove14] M. Overholt, *A course in analytic number theory*, Graduate Studies in Mathematics **160**, American Mathematical Society, Providence, RI, 2014.

[SZ02] P. Sarnak and A. Zaharescu, *Some remarks on Landau-Siegel zeroes*, Duke Math. J., **111** (2002), 495-507.

[Sil94] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer-Verlag, New York, 1994.

[Sil09] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 2009.

[Sta67] H. M. Stark, *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J. (1967), 1-27.

[Sta69] H. M. Stark, *On the "gap" in a theorem of Heegner*, J. Number Theory **1** (1969), 16-27.

[Sta71] H. M. Stark, *A transcendence theorem for class number problems*, Ann. of Math. (2) **94** (1971), 153-173

[Sie35] C. L. Siegel, *Über die Classenzahl quadratischer Zahlkörper*, Acta Arith. **1** (1935), 83-86.

[Tat51] T. TATUZAWA, On a theorem of Siegel, Jap. J. Math. **21** (1951), 163–178.

[TW95] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. *(2)* **141** (1995), 553-572.

[Wak02] M. Watkins, *Computing the modular degree of an elliptic curve*, Experiment. Math. **11** (2002), 487-502.

[Wak04] M. Watkins, *Class numbers of imaginary quadratic fields*, Math. Comp. **73** (2004), 907-938.

[Wak] M. Watkins, *Explicit lower bounds on the modular degree of an elliptic curve*, Preprint, 2004 https://arxiv.org/abs/math/0408126.

[Wil95] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. of Math. *(2)* **141** (1995), 443-551.

국문초록

가우스 류수 문제란 주어진 류수 값을 갖는 이차수체를 완전히 찾는 것이다. 지겔 정리에 의해, 주어진 류수에 대한 복소 이차수체와 리쇼-데제르 유형의 실 이차수체는 유한 개만 존재한다. 하지만 지겔 정리는 계산 불가능한 형태이므로 가우스 류수 문제를 풀 수 없다.

골드펠드는 타원곡선 이론을 이용하여, 복소 이차수체와 리쇼-데제르 유형의 실 이차수체에 대한 류수 문제를 풀 수 있는, 계산 가능한 방법을 고안하였다. 복소 이차수체 경우에는 외스테르레가 증명을 단순화하고 정확한 결과 값을 계산해서, 류수가 3인 복소 이차수체 류수 문제를 해결하였다.

저자는 골드펠드 방법에 나오는 상수 값을 정확히 계산하고, 이를 리쇼-데제르 유형의 실 이차수체에 대한 류수 문제에 적용한다.

주요어휘: 류수, 이차수체, 타원곡선.
학번: 2014-21201