2015

The Least Prime Number That Splits Completely In S3-Sextic Number Fields

Zhenchao Ge
University of Mississippi

THE LEAST PRIME NUMBER THAT SPLITS COMPLETELY IN S_3-SEXTIC NUMBER FIELDS

DISSERTATION

A Dissertation
presented in partial fulfillment of requirements
for the degree of Master of Science
in the Department of Mathematics
The University of Mississippi

by

ZHENCHAO GE

December 2015

ABSTRACT

In number theory, an integer n is quadratic residue modulo an odd prime p if n is congruent to a perfect square modulo p. Otherwise, n is is called a quadratic nonresidue. Bounding the least prime quadratic residue and the least quadratic nonresidue are two very classical problems in number theory. These classical problems can be generalized to any number field K by asking for bounds the least for prime that splits completely or does not split completely, respectively, in the ring of integers of K.

The goal of this thesis is to bound the least prime that splits completely in certain nonabelian Galois number fields in terms of the discriminant of the number field. The analogous problem for for abelian number fields was recently considered by Pollack, using an old method of Linnik and Vinogradov. Our approach is different and requires estimating a certain sum in two ways using both analytic and algebraic tools. There is a "trivial" bound in this problem, and in this thesis we prove the first known nontrivial estimates for certain families of nonabelian Galois number fields.

ACKNOWLEDGEMENTS

My first and deepest gratitude is to my supervisor Dr. Micah B. Milinovich for his guidance and motivation in the past two years. I have been very fortunate to be his student. His continuous support helped me overcome many difficulties throughout my study. I am also very grateful to him for patiently guiding me to correct grammar and notation in my writing. His patience and encouragement helped me become a qualified researcher and teacher.

My sincere thanks also goes to my thesis committee Dr. Erwin Miña-Diaz and Dr. Thái Hoàng Lé for their carefully reading and commenting on my thesis. I appreciate their suggestions and questions which open my minds and enrich my ideas. I also would like to thank Dr. Paul Pollack. This thesis would not have been possible without his inspiration.

I am also very grateful to Drs. Sandra Spiroff, Gerard Buskes and Qingying Bu for giving me a solid algebra and analysis background. I would like to thank Drs. Bing Wei, Iwo Labuda, Hailin Sang, Martial Longla, Laura Sheppardson, and Samuel Lisi for their assistance. I also appreciate Mr. Marlow Dorrough and Ms. Colleen Gilman who help me organize the thesis defense.

I wish to thank my academic sister Dr. Caroline Turnage-Butterbaugh for helping me in formatting thesis. Also, I share the credit of my work with all my supportive classmates. Particularly, I would like to thank Thomas Naugle and Sooyeon Lee for their constant encouragement. I appreciate my best friends Jiaqi and Hao for cheering me up whenever I have late-night work. Finally, I warmly and deeply appreciate my parents for their love.

TABLE OF CONTENTS

1 INTRODUCTION

Let p be an odd prime. An integer a is called a *quadratic residue* of p if a is congruent to a perfect square modulo p. Problems concerning quadratic residues are very classical. Clearly 1 is the smallest quadratic residue modulo p and it is not hard to see that products of quadratic residues modulo p are quadratic residues. Therefore it is natural to ask what is the least prime quadratic residue modulo p.

I. M. Vinogradov conjectured the least prime quadratic residue modulo p it is $O(p^{\varepsilon})$ for any $\varepsilon > 0$. Big-O notation is described in Section 1.2. Using the Pólya-Vinogradov inequality and Siegel's Theorem, it can be shown that the least prime quadratic residue modulo p is $O(p^{1/2+\varepsilon})$ for any $\varepsilon > 0$. We call this the "trivial bound" and we prove this bound in the next chapter.

In 1966, A. I. Vinogradov & Ju. V. Linnik [VL66] proved the non-trivial bound that the least prime quadratic residue modulo p is $O(p^{1/4+\varepsilon})$. Eleven years later, J. Pintz [Pin77] proved the same result by a more elementary method. Both proofs use Siegel's Theorem and Burgess bound for character sums in place of the Pólya-Vinogradov inequality.

In this thesis, we determine a bound for the least prime that splits completely in the ring of integers in certain nonabelian Galois number fields. The definitions of these concepts are given in Section 1.1. This generalizes the above problem because the least prime quadratic residue modulo p is also the smallest prime which splits completely in the ring of integers of a certain quadratic number field. We focus on nonabelian Galois number fields because P. Pollack [Pol14] recently generalized Vinogradov & Linnik's result and showed that the least prime that splits completely in abelian Galois extension number field K is $O(|D_K|^{1/4+\varepsilon})$,

where D_K is the discriminant of K. As in the work of Vinogradov and Linnik, Pollack's proof also relies on Siegel's Theorem and Burgess bound for character sums.

In the nonabelian case, there is a generalization of Siegel's Theorem due to Brauer. However, there is no analogue of Burgess bound. Instead, first we deduce the "trivial" bound from an Atkinson-type summation formula of Friedlander and Iwaniec [FI05]. In particular, we show that the least prime that splits completely in *any* Galois number field is $O_\varepsilon(|D_K|^{1/2+\varepsilon})$. We provide a proof of this estimate in section 2.2.

The main goal of this thesis is to prove an non-trivial estimate for a family of non-abelian Galois number fields. We use level-aspect subconvexity estimates of certain automorphic L-functions. In particular, we prove that in an S_3-sextic field K the least prime that splits completely is $O(|D_K|^{0.499})$. We deduce this from a more general theorem that applies to other families of number fields, as well.

Before stating and proving the main results of this thesis, we first introduce some notation.

1.1 Background in algebraic number theory

One of the historical motivations of analytic number theory is to study the distribution of the prime numbers in $\mathbb{N}$ (or $\mathbb{Z}$). For this purpose, Riemann introduced the function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

where the product runs over the primes p. This function of a complex variable s is now called the Riemann zeta-function. Initially the sum and product converge in the half-plane $\Re(s) > 1$, but $\zeta(s)$ can be analytically continued to $\mathbb{C} \setminus \{1\}$. For background and history of prime number theory, see Davenport's classic book [Dav00]. The goal of this thesis is to generalize the study of the prime numbers to the ring of integers in an algebraic number field

using a generalization of the Riemann zeta-function known as the Dedekind zeta-function. In order to describe our main results, we first introduce some definitions and notation (all of which is consistent with the book of Ireland and Rosen [IR90]).

An *algebraic number field* is a finite degree field extension of the field of rational numbers. An *algebraic integer* is a root of a monic polynomial with integer coefficients. As is well-known, the set of all algebraic integers in an algebraic number field forms a ring called the *ring of integers* of the number field. Throughout this thesis, we will let K denote an algebraic number field and we say K has *degree* m if the dimension $[K : \mathbb{Q}] = m$ as a $\mathbb{Q}$-vector space. We will let $\mathcal{O}_K$ denote the ring of algebraic integers in K. More precisely, because $\mathcal{O}_K$ is subring of this $\mathbb{Q}$-vector space K, $\mathcal{O}_K$ is a finitely-generated $\mathbb{Z}$-module. The rank of $\mathcal{O}_K$ is exactly the degree of K and hence we have a $\mathbb{Z}$-basis $b_1, \cdots, b_m$ of $\mathcal{O}_K$.

An *embedding* of a field K into $\mathbb{C}$ is a ring homomorphism $\sigma : K \to \mathbb{C}$. And it is known that for a number field K with degree m, there are m embeddings into $\mathbb{C}$. Say they are $\sigma_1, \cdots, \sigma_m$. (See [Mar77, Appendix 2]). The *discriminant* D_K of K over $\mathbb{Q}$ is defined to be

$$D_K := \left(\det \begin{pmatrix} \sigma_1(b_1) & \sigma_1(b_2) & \cdots & \sigma_1(b_m) \\ \sigma_2(b_1) & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \sigma_m(b_1) & \cdots & \cdots & \sigma_m(b_m) \end{pmatrix} \right)^2 .$$

The discriminant is an important invariant of a number field which gives number fields a natural ordering.

It is useful to think of K as a generalization of $\mathbb{Q}$ and $\mathcal{O}_K$ as a generalization of $\mathbb{Z}$. However, in algebraic number theory, instead of studying prime elements one typically studies prime ideals. The reason for this is that, in general, elements in $\mathcal{O}_K$ do not factor uniquely into prime elements however ideals in $\mathcal{O}_K$ do factor uniquely into prime ideals. This was famously proved by Dedekind in the larger context of what are now called Dedekind domains (see [FT93, Chapter 2]).

Indeed, if we pick a prime $p \in \mathbb{N}$ then $p\mathcal{O}_K$ is an ideal of $\mathcal{O}_K$. By unique factorization, there exist prime ideals $\mathfrak{p}_i \in \mathcal{O}_K$ such that

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_g^{e_g}, \tag{1.1}$$

where e_i is called the *ramification index* of the prime ideal $\mathfrak{p}_i$. We call $f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}]$ the *inertia degree* or *degree* of the prime ideal $\mathfrak{p}_i$. In this context, we say that $\mathfrak{p}_i$ lies over the p or that p lies under the prime ideal $\mathfrak{p}_i$. It is known that every prime ideal in $\mathcal{O}_K$ lies over a unique (rational) prime p, see [Mar77, Theorem 20].

The degrees of prime ideals and their ramification indices are connected to the degree of the number field through the following formula [IR90, Chapter 12]:

$$\sum_{i=1}^{g} e_i f_i = m = [K : \mathbb{Q}]. \tag{1.2}$$

When $K/\mathbb{Q}$ is a Galois extenstion, then all the ramification indices are equal, $e_1 = e_2 = \cdots = e_g = e$, say. It follows that the inertia degrees are also equal, $f_1 = \cdots = f_g = f$, say. Thus, in the Galois case, formula (1.1) simplifies to

$$p\mathcal{O}_K = \mathfrak{p}_1^{e}\mathfrak{p}_2^{e}\cdots\mathfrak{p}_g^{e} \tag{1.3}$$

and formula (1.2) simplifies to

$$g \cdot e \cdot f = m = [K : \mathbb{Q}]. \tag{1.4}$$

See [IR90, Chapter 12].

Prime ideals are divided into various splitting types. For simplicity, we restrict to the case where $K/\mathbb{Q}$ is a finite Galois extension and we will only discuss the splitting types that occur in this thesis. In general, when K is not Galois over $\mathbb{Q}$ and all splitting types are

allowed, the discussion becomes much more complicated. Let p be a prime in $\mathbb{N}$. The cases we encounter are the following.

1. If $e > 1$ in (1.3), then we say that p is *ramified* in $\mathcal{O}_K$.

2. If $e = 1$ and $f = 1$, then we say that p *splits completely* in $\mathcal{O}_K$. In other words,

$$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_m$$

   for distinct prime ideals $\mathfrak{p}_i \in \mathcal{O}_K$ where $m = [K : \mathbb{Q}]$. Note that $e = 1$ and $f = 1$ implies that $g = m$.

3. Other cases: $e = 1$ and $f \geq 2$.

1.2 Asymptotic notation

We say "$f(x)$ is *big-O of* $g(x)$" and write $f(x) = O(g(x))$ if there is a constant $C > 0$ such that $|f(x)| \leq Cg(x)$ for all x in the appropriate domain. (Usually we are interested in the case that x tends to infinity.) Here the constant C is called the *implicit constant* and the function f could be complex-valued, but g must be non-negative.

Sometimes instead of writing $f(x) = O(g(x))$ we use Vinogradov's notation $f(x) \ll g(x)$ which has the same meaning and is read "$f(x)$ is *less-than-less-than* $g(x)$". We write $f(x) = O_\alpha(g(x))$ or $f(x) \ll_\alpha g(x)$ if the implicit constant depends on parameter α.

We say "$f(x)$ is *greater-than-greater-than* $g(x)$" and write $f(x) \gg g(x)$ if there is a positive constant c such that $f(x) \geq cg(x)$ for all x in some domain. Similarly, if the implicit constant depends on parameter α we write $f(x) \gg_\alpha g(x)$.

1.3 A sample result

Our main result is to give an upper bound for the smallest prime $p \in \mathbb{N}$ which splits completely in $\mathcal{O}_K$ as the number field K varies in certain families. Our inequality will be

given in terms of $|D_K|$, the absolute value of the discriminant of the number field. In this section, we state a sample result for a special family of non-abelian Galois number fields.

Definition 1.1. *Let K be a number field. Then we define q_K to be the smallest (rational) prime which splits completely in $\mathcal{O}_K$.*

It is not difficult to establish the following inequality for q_K for any Galois number field K, in terms of the discriminant of K which we will refer to as the *trivial bound*.

Theorem 1.2 (Trivial Bound for q_K)**.** *If K is a Galois extension of $\mathbb{Q}$, then*

$$q_K \ll_\varepsilon \left|D_K\right|^{1/2+\varepsilon}$$

for any $\varepsilon > 0$. This implied constant depends on ε and the degree of $K/\mathbb{Q}$.

This bound seems to be well-known but only as a folklore theorem. Therefore, we give a proof of this trivial bound in Section 2.2. Very recently, P. Pollack [Pol14] extended results of Vinogradov & Linnik [VL66] and proved the following theorem which improves upon the trivial bound for abelian number fields.

Theorem 1.3. (P. Pollack) *Let K be an abelian Galois extension of $\mathbb{Q}$. Then*

$$q_K \ll_\varepsilon |D_K|^{1/4+\varepsilon},$$

for any $\varepsilon > 0$. The implied constant depends on ε and the degree of $K/\mathbb{Q}$.

As far as the author is aware, before the results of this thesis, there seems to be no known example of a family of nonabelian number fields K for which q_K is known to be smaller than the trivial bound. To explain why, we note that Pollack's theorem was proved using three ingredients: factorization of the Dedekind zeta-function of an abelian number field into Dirichlet L-functions, Siegel's theorem for exceptional zeros of Dirichlet L-functions, and Burgess bound for short character sums. For nonabelian number fields, the

Dedekind zeta-function does not factor into Dirichlet L-functions and so Burgess bound for character sums is not applicable. There is, however, an analogue of Siegel's Theorem called the Siegel-Brauer Theorem.

In this thesis, using different tools, we give the first examples of families of nonabelian Galois number fields K for which q_K is provably smaller than the trivial bound. One natural type of family of number fields to consider is the following family.

Definition 1.4. *We say a number field K is an S_3-sextic field if K is Galois over $\mathbb{Q}$ with Galois group* $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$.

Since S_3 is the "simplest" nonabelian group, we see that S_3-sextic fields are the "simplest" family of nonabelian Galois number fields. Therefore, they are the natural first example to consider beyond Pollack's result for abelian number fields.

A consequence of the main result of this thesis is the following theorem.

Theorem 1.5. *If K is an S_3-sextic number field, then $q_K = O\big(|D_K|^{0.499}\big)$ as $|D_K| \to \infty$.*

This is a robust family of number fields. Bhargava & Wood [BW08] show that the number of S_3-sextic fields K with discriminant $|D_K| < X$ has an asymptotic formula.

$$\#\big\{K \mid \mathrm{Gal}(K/\mathbb{Q}) \cong S_3,\ |D_K| < X\big\} \sim CX^{1/3}$$

as $X \to \infty$, where C is some absolute constant. The explicit value of this constant can be found in paper [BW08] and an asymptotic formula with a strong error term can be found in the work of Taniguchi & Thorne [TT14].

We actually prove a more general result than Theorem 1.5 by assuming a subconvexity result of a certain type for the Dedekind zeta-function of a Galois number field. We deduce Theorem 1.5 as a special case since such a subconvexity bound is known to hold for S_3-sextic number fields. This more general result is stated as Theorem 1.7 in Section 1.5, but we need to introduce more definitions and notation before we can state it.

1.4 Dedekind zeta-function

Let $K/\mathbb{Q}$ be a Galois extension with $m = [K : \mathbb{Q}]$, and let $\mathfrak{P}$ be an prime ideal in $\mathcal{O}_K$. Then the (absolute) norm of $\mathfrak{P}$ is defined to be

$$N(\mathfrak{P}) := p^f,$$

where p is the unique rational prime lying under $\mathfrak{P}$ and where f is the inertia degree. If an arbitrary ideal $\mathfrak{A} \in \mathcal{O}_K$ has a (unique) factorization into prime ideals given by

$$\mathfrak{A} = \mathfrak{P}_1^{a_1}\mathfrak{P}_2^{a_2}\cdots\mathfrak{P}_t^{a_t},$$

then the (absolute) norm of $\mathfrak{A}$ is given by

$$N(\mathfrak{A}) = \prod_{\mathfrak{P}_i|\mathfrak{A}} N(\mathfrak{P}_i)^{f_i a_i}.$$

This implies that the norm is completely multiplicative, namely $N(\mathfrak{AB}) = N(\mathfrak{A})N(\mathfrak{B})$ for any pair of ideals $\mathfrak{A}, \mathfrak{B} \in \mathcal{O}_K$. Our definition of norm is not standard but in the Galois case it is consistent with the standard definition, see [IR90, Chapter 14].

Now we are in position to define the Dedekind zeta-function of a number field K. Using the unique factorization of ideals in $\mathcal{O}_K$ into prime ideals and the multiplicativity of the norm, the Dedekind zeta-function is defined as

$$\zeta_K(s) := \sum_{\mathfrak{a}\subseteq\mathcal{O}_K} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1}. \tag{1.5}$$

Here the sum runs over the nonzero ideals $\mathfrak{a} \in \mathcal{O}_K$, the product runs over the nonzero prime ideals in $\mathcal{O}_K$, and $N(\mathfrak{a})$ is the norm of the ideal $\mathfrak{a}$. In order to discuss convergence, it is

useful to write $\zeta_K(s)$ as the ordinary Dirichlet series

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{r_K(n)}{n^s},$$

where $r_K(n)$ denotes the number of ideals in $\mathcal{O}_K$ of norm n. It is known that

$$0 \leq r_K(n) \leq d_m(n)$$

where $d_m(n)$, the mth iterated divisor function, is the number of ways to write a natural number n as a product of m positive divisors. Here, as above, $m = [K : \mathbb{Q}]$. Since

$$1 \leq d_m(n) \ll_{\varepsilon,m} n^{\varepsilon}$$

for any $\varepsilon > 0$, this implies that series defining $\zeta_K(s)$ converges absolutely in (and uniformly on compact subsets of) the half-plane $\Re(s) > 1$. Analogous to the case of the Riemann zeta-function, E. Hecke proved that $\zeta_K(s)$ can be analytically continued to all of $\mathbb{C}$ apart from a simple pole at $s = 1$ and that it has a functional equation.

Let

$$\gamma_K(s) = \pi^{-ms/2}\Gamma\left(\frac{s}{2}\right)^{r_1+r_2}\Gamma\left(\frac{s+1}{2}\right)^{r_2} \tag{1.6}$$

where r_1 is the number of real embeddings of K into $\mathbb{C}$ and r_2 is the number of pairs of complex embeddings so that $m = r_1 + 2r_2$. And define

$$\Lambda_K(s) := |D_K|^{s/2}\gamma_K(s)\zeta_K(s).$$

Then the functional equation for $\zeta_K(s)$ is

$$\Lambda_K(s) = \Lambda_K(1-s). \tag{1.7}$$

In asymmetric form (which is useful later in the thesis), the functional equation states that

$$\zeta_K(1-s) = \hat{\gamma}_K(s)\zeta_K(s), \tag{1.8}$$

where

$$\hat{\gamma}_K(s) = |D_K|^{s-1/2} \frac{\Gamma_{\mathbb{R}}(s)^{r_1}}{\Gamma_{\mathbb{R}}(1-s)^{r_1}} \frac{\Gamma_{\mathbb{C}}(s)^{r_2}}{\Gamma_{\mathbb{C}}(1-s)^{r_2}} \tag{1.9}$$

with

$$\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right) \quad \text{and} \quad \Gamma_{\mathbb{C}}(s) = 2^{1-s}\pi^{-s}\Gamma(s). \tag{1.10}$$

Legendre's duplication formula for the gamma function can be used to show that both versions of the functional equation are equivalent.

From the asymmetric form of the functional equation, we can see that $\zeta_K(s)$ has zeros on the real axis. Suppose that degree $m \geq 2$. Since r_1 and r_2 are non-negative integers, we have $m = r_1 + 2r_2 \geq 2$ which implies that at least one of r_1 or r_2 is ≥ 1. Note that $\Gamma_{\mathbb{R}}(s)^{r_1}$ has a pole of order r_1 at $s = 0$ and at every negative even integer, and that $\Gamma_{\mathbb{C}}(s)^{r_2}$ has a pole of order r_2 at every non-positive integer. By (1.8) and (1.9), since $\zeta_K(s)$ is analytic on $\mathbb{C} \setminus \{1\}$, we see that $\zeta_K(s)$ must have a zero of order at least $r_1 + r_2 - 1$ at $s = 0$, a zero of order at least r_2 at every odd negative integer, and a zero of order at least $r_1 + r_2$ at every negative even integer. These are called the *trivial zeros* of $\zeta_K(s)$.

1.5 A general result on the least prime that splits completely

We are now at the position to state a theorem that is more general than Theorem 1.5 which depends on the size of $\zeta_K(s)$ in terms of the discriminant of K. A standard argument using the functional equation for $\zeta_K(s)$ and the Phragmén–Lindelöf convexity principle implies that, for $\Re(s) = 1/2$,

$$\zeta_K(s) \ll_{m,\varepsilon} |s|^N |D_K|^{1/4+\varepsilon}, \tag{1.11}$$

for any $\varepsilon > 0$ where N is an absolute constant. This is called a "convexity" bound for $\zeta_K(s)$ and, when K is Galois over $\mathbb{Q}$, it can be used to prove the "trivial" bound for the least prime that splits completely. In order to improve upon the trivial bound, we need a stronger "subconvexity" estimate $\zeta_K(s)$. We state the same subconvexity hypothesis that appears in the recent work of Einsiedler, Lindenstrauss, Michel & Venkatesh [ELMV11, page 880].

Hypothesis 1.6. *Let K be a number field of fixed degree m. There exists $\theta, N > 0$ (depending at most on m) such that for $\Re(s) = 1/2$,*

$$\zeta_K(s) \ll_m |s|^N |D_K|^{1/4-\theta}. \tag{1.12}$$

This hypothesis is not known to hold for all number fields K, but is known in some cases. For example when K is an abelian extension of $\mathbb{Q}$, this subconvexity bound holds by the work of Burgess [Bur63]. Due to the work of Duke, Friedlander & Iwaniec [DFI02] in 2002, this bound is also known to be true in some non-abelian cases, for instance when K is a dihedral extension field of $\mathbb{Q}$. Later Blomer, Harcos & Michel [BHM07] improved the estimate in [DFI02], allowing one to take $\theta = 1/1889 - \varepsilon$ for any $\varepsilon > 0$ in dihedral extensions.

Assuming Hypothesis 1.6, we prove a general theorem for the least prime that splits completely in a Galois number field.

Theorem 1.7 (Main Theorem)**.** *Let $K/\mathbb{Q}$ be a Galois extension and suppose that Hypothesis 1.6 holds for some $\theta, N > 0$. Then*

$$q_K \ll |D_K|^{1/2-2\theta+\varepsilon}, \tag{1.13}$$

for any $\varepsilon > 0$. The implied constant depends on ε and degree $[K : \mathbb{Q}]$.

Using the estimate of Blomer, Harcos & Michel [BHM07], some results from representation theory, and the fact that dihedral Artin L-functions are known to be automorphic, we deduce following corollary.

Corollary 1.8. *Let $K/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) \cong D_n$ where D_n with $n \geq 3$ is the dihedral group of $2n$ elements. Then*

$$q_K \ll_\varepsilon |D_K|^{\frac{1}{2}-\frac{2}{1889}+\varepsilon} \ll |D_K|^{0.499} \tag{1.14}$$

for any $\varepsilon > 0$. The implied constant depends on ε and degree $[K : \mathbb{Q}]$. In particular, this result holds if K is an S_3-sextic extension of $\mathbb{Q}$.

We will give the proof of Theorem 1.7 and its corollary in Chapter 4.

1.6 Arithmetic functions

An *arithmetic function* is a complex-valued function with domain $\mathbb{N}$. And we say an arithmetic function $f(n)$ is *multiplicative* provided $f(mn) = f(m)f(n)$ for $(m, n) = 1$. This implies that

$$f(n) = f(p_1^{a_1})f(p_2^{a_2}) \cdots f(p_i^{a_i})$$

if $n = p_1^{a_1}p_2^{a_2} \cdots p_i^{a_i}$ is the factorization of n into distinct primes $p_1, p_2, \cdots, p_i$. Further, function $f(n)$ is called *completely multiplicative* if $f(p^a) = f(p)^a$ for all prime p and power a. For arithmetic functions, there is a special binary operation called *Dirichlet convolution*. We denote the Dirichlet convolution of $f(n)$ and $g(n)$ by $(f * g)(n)$ and define it to be

$$(f * g)(n) := \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

We now introduce some arithmetic functions that will appear in later chapters. We define the completely multiplicative function $\mathbf{1}(n) = 1$ for $n \in \mathbb{N}$. Notice that using this, the sum $\sum_{d|n} f(n)$ can be written as $(f * \mathbf{1})(n)$. If a natural number n has prime factorization $n = p_1^{a_1}p_2^{a_2} \cdots p_i^{a_i}$, we define *Liouville function* by

$$\lambda(n) := (-1)^{a_1+a_2+\cdots+a_i}.$$

Note that Liouville function is also completely multiplicative. If we define

$$\Omega(n) := a_1 + a_2 + \cdots + a_i$$

to be the total number of primes dividing n, then the Liouville function $\lambda(n) = (-1)^{\Omega(n)}$.

1.7 Prime quadratic residue and prime splits completely

In this section our goal is to establish the connection between of prime quadratic residue and the prime that splits completely in quadratic number field. Here, we only discuss odd prime residues, although this is also true for prime 2.

Assume that K is a quadratic number field with monic irreducible polynomial x^2+bx+c, where b, c are rational integers. It is well known that the discriminant of this polynomial is $\Delta = b^2 - 4c$, hence it is not hard to see $\Delta \equiv 0$ or $1(\text{mod}4)$. And if one of the following holds:

1. Δ is odd and squarefree;

2. Δ is even, $\Delta/4$ is squarefree, and $\Delta/4 \equiv 2$ or 3 $(\text{mod}4)$.

Then this Δ is also the discriminant of quadratic field $K = \mathbb{Q}(\sqrt{\Delta})$ as defined in Section 1.1. Note that when $|\Delta|$ is a prime p, then $\Delta = \pm p$ where $p \equiv \pm 1(\text{mod}4)$.

Proposition 1.9. *Let K be a quadratic number field with discriminant Δ. Then an odd prime p splits completely if and only if Δ is a square modulo p.*

Proof. In a quadratic number field, $p\mathcal{O}_K$ only has three types of prime factorization. And p is ramified if and only if $p|\Delta$, which is equivalent to $\left(\frac{\Delta}{p}\right) = 0$.

Let $\mathfrak{p}$ be a prime ideal lying above p. We pick an element x in $\mathfrak{p}$. This x must be of the form $x = (a + b\sqrt{\Delta})/2$, where $a, b \in \mathbb{Z}$. Moreover, norm $N(\mathfrak{p})|N(x) = (a^2 - b^2\Delta)/4$, we hence have $a^2 \equiv \Delta b^2 (\text{mod } p)$.

Next we are going to show ($\Rightarrow$). Suppose prime p splits completely, so $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$. Claim that there exists x_1 in $\mathfrak{p}_1$ such that $a^2 \equiv \Delta b^2 (\text{mod } p)$ and $b \not\equiv 0 (\text{mod } p)$. If for every x, $p|b$, then $p|a$ and hence $p|x$. This implies that both prime ideals $\mathfrak{p}_i \subseteq p\mathcal{O}_K$. However, we assumed p splits completely, then $\mathfrak{p}_1, \mathfrak{p}_2$ are distinct ideals. Thus, $\mathfrak{p}_1\mathfrak{p}_2 \subsetneq \mathfrak{p}_1 \subseteq p\mathcal{O}_K$, which is a contradiction. This proves our claim. Now there exists such an x_1 with $p \nmid b$, so there exists $b^{-1}b \equiv 1 (\text{mod } p)$. It follows that $a^2(b^{-1})^2 \equiv \Delta (\text{mod } p)$.

Next we show ($\Leftarrow$). Suppose $\Delta \equiv a^2 (\text{mod } p)$. Let $\mathfrak{I}_1$ denote the ideal generated by p and $a + \sqrt{\Delta}$ (i.e. $\mathfrak{I}_1 = (p, a + \sqrt{\Delta})$). And similarly let $\mathfrak{I}_2 = (p, a - \sqrt{\Delta})$. It is easy to check that $\mathfrak{I}_1\mathfrak{I}_2 \subseteq p\mathcal{O}_K$. We claim p splits completely. If not, then p is either ramified or inert. Here, we suppose $p \nmid a$, so $p \nmid \Delta$ and p is not ramified. If p is inert, then $\mathfrak{I}_1\mathfrak{I}_2 \subseteq p\mathcal{O}_K = \mathfrak{p}$, for some prime ideal $\mathfrak{p}$. More precisely, every element $(a + \sqrt{\Delta})(a - \sqrt{\Delta}) \in \mathfrak{p}$. Further, $\mathfrak{p}$ is prime ideal, so at least one of $a + \sqrt{\Delta}$ and $a - \sqrt{\Delta}$ is in $\mathfrak{p}$. Say $a + \sqrt{\Delta} \in \mathfrak{p} = p\mathcal{O}_K$. Hence we have $a + \sqrt{\Delta} = pk_1$ and $pk_1(a - \sqrt{\Delta}) = pk_2$, for some rational integers k_1, k_2. Consider the second equation, if both sides divided by p, we get $(a - \sqrt{\Delta})k_1 = k_2$ for some rational integers k_1, k_2, which is clearly impossible. Therefore, p has to split completely. □

Corollary 1.10. *An odd prime p is a quadratic residue modulo an odd prime q if and only if p is a prime that splits completely in $\mathbb{Q}(\sqrt{\pm q})$ where $q \equiv \pm 1 (\text{mod} 4)$.*

Proof. First we suppose $q \equiv 1 (\text{mod} 4)$. The discriminant of the quadratic number field is q so the field is $\mathbb{Q}(\sqrt{q})$. Pick an odd rational prime p. If p is quadratic residue modulo q, then $\left(\frac{p}{q}\right) = 1$. Further quadratic reciprocity states that if $q \equiv 1 (\text{mod} 4)$, then $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = 1$. It follows from Proposition 1.9 that p splits completely.

Conversely, if p splits completely in $\mathbb{Q}(\sqrt{q})$, by previous proposition, $\left(\frac{q}{p}\right) = 1$. Next using reciprocity law, we can show that p is a residue modulo q.

Next suppose $q \equiv -1 (\text{mod} 4)$. The discriminant of the number field has to be $-q$ so the number field is $\mathbb{Q}(\sqrt{-q})$. If odd p is prime quadratic residue modulo q, then by reciprocity law, $\left(\frac{-q}{p}\right) = \left(\frac{p}{q}\right) = 1$. Hence, p splits in $\mathbb{Q}(\sqrt{-q})$. Conversely, if p split in $\mathbb{Q}(\sqrt{-q})$, then by Proposition 1.9 and reciprocity law, p is prime residue modulo q. □

2 TWO TRIVIAL BOUNDS

As stated in the introduction, the trivial bound for the least prime quadratic residue $(\mathrm{mod}\ p)$ is $O_\varepsilon(p^{1/2+\varepsilon})$ for any $\varepsilon > 0$ and trivial bound for the least prime that splits completely in a Galois number field K is $O_\varepsilon(|D_K|^{1/2+\varepsilon})$. In this chapter our purpose is to prove these bounds.

2.1 Trivial bound for least prime quadratic residue

In this section we are going to prove the trivial bound for the least prime quadratic residue modulo p, which we have stated in section 1.3. Let us recall the theorem.

Theorem 2.1 (Trivial Bound)**.** *Let p be an odd prime and let q be the least prime quadratic residue modulo p. Then, for any $\varepsilon > 0$, we have*

$$q \ll_\varepsilon p^{1/2+\varepsilon} \tag{2.1}$$

where the implied constant is ineffective.

We deduce the above theorem from the following two well-known results in number theory, Siegel's Theorem and the Pólya-Vinogradov inequality.

Theorem 2.2 (Siegel's Theorem)**.** *Let χ be a quadratic character modulo p. Then, for any $\varepsilon > 0$, there exists a positive number C_ε such that*

$$L(1, \chi) > C_\varepsilon\, p^{-\varepsilon}. \tag{2.2}$$

The constant C_ε is ineffective in the sense that the proof provides no explicit lower bound.

Theorem 2.3 (Pólya-Vinogradov inequality)**.** *Let χ be a non-principal character modulo p. Then for any integers M and N with $N > 0$,*

$$\sum_{n=M+1}^{M+N} \chi(n) \ll \sqrt{p} \log p. \tag{2.3}$$

The proof and statement of these theorems can be found in Montgomery & Vaughan's book [MV11, Theorem 11.14 and Theorem 9.18]. We now prove Theorem 2.1.

Proof of Theorem 2.1. Let χ be the unique quadratic character modulo p (also known as the Legendre symbol). If q is the least prime quadratic residue modulo p, then q is the smallest prime for which $\chi(q) = 1$. Thus, every prime ℓ less than q satisfies $\chi(\ell) = -1$ unless $\ell = p$, in which case $\chi(\ell) = 0$.

We will prove the theorem by estimating the sum

$$\sum_{n<q} \big(\chi * \mathbf{1}\big)(n) \tag{2.4}$$

in two different ways. Here $*$ denotes Dirichlet convolution. On one hand we show that the sum in (2.4) is small using the fact that $\chi(\ell) = -1$ for essentially every prime $\ell < q$. On the other hand, we estimate the sum asymptotically using Siegel's Theorem and the Pólya-Vinogradov inequality. Equating the two estimates gives the claimed relationship between q and p.

First consider n with $1 \le n < q$. This n must be a product of primes that are less than q. Since every prime $\ell < q$ has $\chi(\ell) = -1$ unless $\chi(p) = 0$ if $p < q$. Moreover, since $\chi(n)$ is multiplicative, if $p \nmid n$ then $\chi(n) = (-1)^{\Omega(n)}$ where $\Omega(n)$ is the number of prime factors of n (counting multiplicity). Hence $\chi(n) = \lambda(n)$ if $p \nmid n$, where $\lambda(n)$ is the *Liouville function*

which was introduced in Section 1.6. The Liouville function has the following property:

$$(\lambda * \mathbf{1})(n) = \sum_{d|n} \lambda(d) = \begin{cases} 1, & \text{if } n \text{ is a perfect square,} \\ 0, & \text{otherwise.} \end{cases}$$

Thus, for $1 \leq n < q$, we have

$$(\chi * \mathbf{1})(n) = \begin{cases} 1, & \text{if } p \nmid n \text{ and } n \text{ is a perfect square,} \\ 0, & \text{otherwise.} \end{cases}$$

It follows that the sum 2.4 is basically counting how many perfect squares less than q but multiple of p. Hence

$$\sum_{n<q} (\chi * \mathbf{1})(n) \leq \sum_{n<q} (\lambda * \mathbf{1})(n) = \lfloor \sqrt{q} \rfloor. \tag{2.5}$$

Next applying the inclusion-exclusion principle (also known as Dirichlet's trick of summing under the hyperbola) with a parameter y where $1 \leq y < q$, we have

$$\sum_{n<q} \big(\chi * \mathbf{1}\big)(n) = \sum_{n \leq y} \sum_{m < \frac{q}{n}} \chi(m) + \sum_{m \leq \frac{q}{y}} \chi(m) \sum_{n < \frac{q}{m}} \mathbf{1} - \sum_{n \leq y} \mathbf{1} \sum_{m \leq \frac{q}{y}} \chi(m). \tag{2.6}$$

On the right-hand side of (2.6), there are three double sums. We shall estimate them one at a time. Using the Pólya-Vinogradov inequality (setting $M = 0$ and $N = q/n$), we have

$$\sum_{n \leq y} \sum_{m < \frac{q}{n}} \chi(m) \ll \sum_{n \leq y} \sqrt{p} \log p \leq y\sqrt{p} \log p \tag{2.7}$$

which gives an estimate for the first double sum on the right-hand side of (2.6).

To estimate the second double sum, again we need use Pólya-Vinogradov inequality and find that

$$\begin{aligned}\sum_{m\le \frac{q}{y}} \chi(m) \sum_{n<\frac{q}{m}} \mathbf{1} &= \sum_{m\le \frac{q}{y}} \chi(m) \left\lfloor \frac{q}{m} \right\rfloor = q \sum_{m\le \frac{q}{y}} \frac{\chi(m)}{m} + O\left(\sum_{m\le \frac{q}{y}} |\chi(m)| \right) \\ &= q \sum_{m=1}^{\infty} \frac{\chi(m)}{m} - \sum_{m>\frac{q}{y}} \frac{\chi(m)}{m} + O\left(q/y\right) \\ &= qL(1,\chi) - \sum_{m>\frac{q}{y}} \frac{\chi(m)}{m} + O\left(q/y\right)\end{aligned} \tag{2.8}$$

Here in order to estimate the sum $\sum_{m>\frac{q}{y}} \chi(m) m^{-1}$, we use integration by parts and see that

$$\begin{aligned}\sum_{m>\frac{q}{y}} \frac{\chi(m)}{m} &= \int_{\frac{q}{y}}^{\infty} m^{-1}\, d\left(\sum_{i=1}^{m} \chi(i) \right) = \frac{1}{m} \sum_{i=1}^{m} \chi(i) \Big|_{\frac{q}{y}}^{\infty} + \int_{\frac{q}{y}}^{\infty} \left(\sum_{i=1}^{m} \chi(i) \right) m^{-2}\, dm \\ &= O\left(\frac{y}{q} \sqrt{p} \log p \right) + O(1) = O\left(y\sqrt{p} \log p \right).\end{aligned} \tag{2.9}$$

Here, again, we use the Pólya-Vinogradov inequality. Then we plug (2.9) into (2.8) and deduce that

$$\sum_{m\le \frac{q}{y}} \chi(m) \sum_{n<\frac{q}{m}} \mathbf{1} = qL(1,\chi) + O(y\sqrt{p}\log p) + O\left(q/y\right). \tag{2.10}$$

The third double sum is easier to estimate. By Pólya-Vinogradov inequality, we have

$$\sum_{n\le y} \mathbf{1} \sum_{m\le \frac{q}{y}} \chi(m) \ll y\sqrt{p}\log p. \tag{2.11}$$

Now put the estimate for the three double sums back into (2.6), and we find that

$$\sum_{n<q} \left(\chi * \mathbf{1}\right)(n) = qL(1,\chi) + O\left(y\sqrt{p}\log p\right) + O\left(q/y\right).$$

In order to minimize the error, we let $y = q^{\frac{1}{2}} p^{-\frac{1}{4}} (\log p)^{-\frac{1}{2}}$. Then the second estimate of sum (2.4) is

$$\sum_{n<q} (\chi * \mathbf{1})(n) = qL(1,\chi) + O\left(q^{\frac{1}{2}} p^{\frac{1}{4}} (\log p)^{\frac{1}{2}}\right). \tag{2.12}$$

At this point, we have two estimates for the same sum (2.4). Both of them are true but the second one (2.12) is a conditional estimate (the main term may not dominate the error). We pick some small positive δ and apply Siegel's Theorem 2.2. There is an ineffective constant $C_1 > 0$ such that $L(1,\chi) > C_1 p^{-\delta}$. And by definition of big-O notation, there exists $C_2 > 0$ such that the absolute value of error term is $\leq C_2 q^{\frac{1}{2}} p^{\frac{1}{4}} (\log p)^{\frac{1}{2}}$. Suppose

$$q > \tfrac{1}{4} \left(\tfrac{C_2}{C_1}\right)^2 p^{1/2+2\delta} (\log p). \tag{2.13}$$

It is easy to check that this assumption is equivalent to

$$q\, L(1,\chi) > q\, C_1 p^{-\delta} > \tfrac{1}{2} C_2 q^{\frac{1}{2}} p^{\frac{1}{4}} (\log p)^{\frac{1}{2}}. \tag{2.14}$$

Then the term $qL(1,\chi)$ dominates the second estimate (2.12), by above inequality, hence this sum $\sum_{n<q}(\chi * \mathbf{1})(n)$ does not vanish with lower bound:

$$\left| \sum_{n<q} (\chi * \mathbf{1})(n) \right| > \tfrac{1}{2} C_1 q p^{-\delta}.$$

Moreover, the first estimate (2.5) shows that

$$\left| \sum_{n<q} (\chi * \mathbf{1})(n) \right| < \sqrt{q}.$$

Combine above two inequalities we have

$$\tfrac{1}{2} C_1 q p^{-\delta} < \sqrt{q} \quad \Leftrightarrow \quad q < \tfrac{4}{C_1^2} p^{2\delta}. \tag{2.15}$$

Compare right-hand side of (2.15) with the assumption (2.13). The constants C_1 and C_2 are fixed for a δ. However, for large p, we find that

$$\left(\frac{C_2}{C_1}\right)^2 p^{\frac{1}{2}+2\delta}(\log p) < q < \frac{4}{C_1^2}p^{2\delta} \quad \Leftrightarrow \quad p^{\frac{1}{2}}\log p < \frac{4}{C_2^2},$$

which is a contradiction. Therefore the assumption (2.13) doesn't hold. We reverse the inequality in (2.13) and deduce that

$$q \leq \frac{1}{4}\left(\frac{C_2}{C_1}\right)^2 p^{\frac{1}{2}+2\delta}(\log p) \quad \Rightarrow \quad q \ll_\delta p^{\frac{1}{2}+3\delta}.$$

Choosing ε to be 3δ, we can get the same exponent in Theorem 2.1. □

2.2 Trivial bound for least prime that splits completely

Let q_K denote the prime that splits completely in K. In this section we are going to prove the following bound of q_K in terms of the discriminant D_K in arbitrary Galois extension number fields, which will be called the *trivial bound* for q_K.

Theorem 1.2 (Trivial Bound for q_K)**.** *If K is a Galois extension of $\mathbb{Q}$, then*

$$q_K \ll_\varepsilon \left|D_K\right|^{1/2+\varepsilon}$$

for any $\varepsilon > 0$. This implied constant depends on ε and the degree of $K/\mathbb{Q}$.

Recall that when proving the trivial bound for least prime quadratic residue, we used Pólya-Vinogradov inequality and Siegel's Theorem. Here, we need introduce some analogous tools (Siegel-Brauer Theorem and two propositions).

Theorem 2.4 (Siegel-Brauer Theorem)**.** *Let K be a normal algebraic number field with discriminant D_K and let $\zeta_K(s)$ be the Dedekind zeta-function of K. We have relation*

$$\log\left(\operatorname*{Res}_{s=1}\zeta_K(s)\right) = o\left(\log|D_K|\right). \tag{2.16}$$

The proof of the above theorem can be found in [Bra47, Theorem 2, part (b)]. In this proof, we are going to use a variation of upon theorem. By definition of "little-oh" notation, we have

$$\lim_{|D_K|\to\infty} \frac{\log\left(\operatorname*{Res}_{s=1}\zeta_K(s)\right)}{\log|D_K|} = 0,$$

which implies that for any $\varepsilon > 0$, there exists some N_ε for which if $|D_K| > N_\varepsilon$ then

$$\log\left(\operatorname*{Res}_{s=1}\zeta_K(s)\right) > -\varepsilon \log|D_K|.$$

Putting a natural base on both sides, we get the following inequality.

Corollary 2.5. *Let K be a normal algebraic number field with discriminant D_K and let $\zeta_K(s)$ be the Dedekind zeta-function of K. We have*

$$\operatorname*{Res}_{s=1}\zeta_K(s) > |D_K|^{-\varepsilon}, \tag{2.17}$$

for $|D_K|$ bigger than some ineffective N_ε.

This Corollary 2.5 is an analogy of $L(1,\chi) \gg_\varepsilon p^{-\varepsilon}$ in previous section. Instead of Siegel's Theorem, in number fields, we use this inequality to establish the trivial bound theorem 1.2. Actually, later we will use this inequality again to get a better bound.

Next we introduce a proposition that we use in place of the Pólya-Vinogradov inequality. This proposition is *analytic* properties of the Dedekind zeta-function and follows from a theorem of Friedlander and Iwaniec [FI05] but some details in this paper are stated without proof. For this reason, we give a detailed proof of this proposition in Chapter 5.

Proposition 2.6. *Let K be an algebraic number field with discriminant D_K and degree $m \geq 2$. Let $\zeta_K(s) = \sum_{n=1}^{\infty} r_K(n)n^{-s}$ be the Dedekind zeta-function of K. If $x \geq |D_K|^{\frac{1}{2}+\varepsilon}$,*

for any $\varepsilon > 0$, we have

$$\sum_{n \le x} r_K(n) = x \operatorname*{Res}_{s=1} \zeta_K(s) + O_\varepsilon \left(|D_K|^{\frac{1}{m+1}} x^{\frac{m-1}{m+1}+\varepsilon} \right), \tag{2.18}$$

for any $\varepsilon > 0$, where the implicit constant depends only on ε and K.

Moreover, we need another proposition which is proved using *algebraic* properties of the Galois extension K over $\mathbb{Q}$.

Proposition 2.7. *Let K be a Galois extension over $\mathbb{Q}$ with discriminant D_K and let q_K be the least prime that splits completely in K. Then*

$$\sum_{n < q_K} r_K(n) \ll q_K^{1/2+\varepsilon} |D_K|^{\varepsilon}, \tag{2.19}$$

for any $\varepsilon > 0$. And implied constant depends on ε and K.

We prove this proposition in next section. Now we conclude this section with the proof of Theorem 1.2, the trivial bound for q_K.

Proof of Theorem 1.2. This proof is very similar to the proof of Theorem 2.1. We focus on the partial sum $\sum_{n<q_K} r_K(n)$ and estimate it in two different ways. We pick a small δ with $0 < \delta < 1/12$. Proposition 2.7 shows that there exists some positive C_1 such that

$$\left| \sum_{n < q_K} r_K(n) \right| < C_1 q_K^{1/2+\delta} |D_K|^{\delta}. \tag{2.20}$$

Inequality (2.20) is the first estimate of partial sum $\sum_{n<q_K} r_K(n)$.

Next we use Proposition 2.6. By the big-O term, there exists a constant $C_2 > 0$ such that the absolute value of the error term is $\le C_2 |D_K|^{\frac{1}{m+1}} q_K^{\frac{m-1}{m+1}+\delta}$. Now we suppose

$$q_K > \tfrac{1}{2} C_2 |D_K|^{1/2+\delta}.$$

By Corollary 2.5, for this δ there exists $N_\delta > 0$ such that if $|D_K| > N_\delta$,

$$q_K \operatorname*{Res}_{s=1} \zeta_K(s) > q_K |D_K|^{-\delta}.$$

And since $\delta < 12$, it is easy to see that the assumption $q_K > \frac{1}{2} C_2 |D_K|^{1/2+\delta}$ implies

$$q_K \operatorname*{Res}_{s=1} \zeta_K(s) > q_K |D_K|^{-\delta} > \tfrac{1}{2} C_2 |D_K|^{\frac{1}{m+1}} q_K^{\frac{m-1}{m+1}+\delta}.$$

It follows that the partial sum $\sum_{n<q_K} r_K(n)$ does not vanish for large $|D_K|$. More precisely, it is

$$\sum_{n<q_K} r_K(n) > \tfrac{1}{2} q_K |D_K|^{-\delta}. \tag{2.21}$$

Now combine inequalities (2.20) and (2.21), we can see that

$$\tfrac{1}{2} q_K |D_K|^{-\delta} < C_1 q_K^{1/2+\delta} |D_K|^{\delta} \quad \Rightarrow \quad q_K^{1/2-\delta} < 2C_1 |D_K|^{2\delta}.$$

However, we assumed $q_K > \frac{1}{2} C_2 |D_K|^{1/2+\delta}$. Put it into above inequality, we get that

$$\left(\tfrac{1}{2} C_2\right)^{1/2-\delta} |D_K|^{1/4-\delta^2} < 2C_1 |D_K|^{2\delta}.$$

Note that for small $0 < \delta < 1/12$ and large $|D_K|$, the above inequality does not hold. Therefore the assumption $q_K > \frac{1}{2} C_2 |D_K|^{1/2+\delta}$ is not right for large $|D_K|$. It follows that $q_K \leq \frac{1}{2} C_2 |D_K|^{1/2+\delta}$ for some C_2 as $|D_K|$ approaching infinity. Choose ε to be this δ, hence the proof is complete. □

2.3 Proof of Proposition 2.7

In this section we aim to give a proof of Proposition 2.7 which appeared in last section. Before proving it, we need introduce the powerful number and two other propositions.

Integer n is called a *squarefull number* if $p|n$ implies $p^2|n$. It is natural to ask how many squarefull numbers are there from 1 to x. The following proposition states that there are roughly $\sqrt{x}$ squarefull numbers if counting from 1 to x up to some constant.

Proposition 2.8. *Let n be squarefull number and $x > 1$. We have*

$$\sum_{n<x} 1 \ll x^{1/2}. \tag{2.22}$$

Proof. Since every squarefull number can be uniquely written as $n = a^2b^3$, where $a, b \geq 1$ and b is square free, we have that

$$\begin{aligned} \sum_{n<x} 1 = \sum_{a^2<x} \sum_{b^3<\left\lfloor \frac{x}{a^2} \right\rfloor} 1 = \sum_{a^2<x} \sum_{c<\sqrt[3]{\left\lfloor \frac{x}{a^2} \right\rfloor}} \mu(c)^2 \leq \sum_{a^2<x} \frac{x^{1/3}}{a^{2/3}} \\ = x^{1/3} \left(\sum_{a<\sqrt{x}} a^{-2/3} \right) = x^{1/3} \left(x^{1/6} + O(1) \right) \ll x^{1/2}. \end{aligned} \tag{2.23}$$

This proves the proposition. □

Next proposition is about counting ramified primes and their composition numbers.

Proposition 2.9. *Let D be a positive integer and $D^\infty = \{n \in \mathbb{N} : p|n \Rightarrow p|D\}$. For any $\varepsilon > 0$, we have*

$$\sum_{n \in D^\infty} \frac{1}{\sqrt{n}} \ll_\varepsilon D^\varepsilon, \quad \text{as } D \to \infty. \tag{2.24}$$

Proof. This is a variation of proof of Tenenbaum [Ten95, pp82 Theorem 2] . Since n is product of prime divisors of D we can bound the sum by the product:

$$\sum_{n \in D^\infty} \frac{1}{\sqrt{n}} \leq \prod_{p|D} \left(\sum_{j=0}^{\infty} \frac{1}{(\sqrt{p})^j} \right) = \prod_{p|D} \left(\frac{1}{1 - \frac{1}{\sqrt{p}}} \right). \tag{2.25}$$

For any $\varepsilon > 0$ there is a $N_\varepsilon > 0$ such that $\frac{1}{\sqrt{n}-1} < \varepsilon$ for all $n > N_\varepsilon$. We split the product on the right-hand-side of (2.25) as

$$\begin{aligned} &\prod_{\substack{p|D \\ p\le N_\varepsilon}} \left(1+\frac{1}{\sqrt{p}-1}\right) \prod_{\substack{p|D \\ p> N_\varepsilon}} \left(1+\frac{1}{\sqrt{p}-1}\right) \\ &\le \prod_{p\le N_\varepsilon} \left(1+\frac{1}{\sqrt{p}-1}\right) \prod_{\substack{p|D \\ p> N_\varepsilon}} \left(1+\frac{1}{\sqrt{N_\varepsilon+1}-1}\right). \end{aligned} \tag{2.26}$$

Note that the first product runs over all primes that are less than or equal to N_ε, so this is a bounded constant only depending ε. Let $\omega(n)$ denote the number of distinct prime divisors of D. It is known that

$$\omega(n) \ll \frac{\log D}{\log\log D}.$$

Therefore,

$$\begin{aligned} \sum_{n\in D^\infty} \frac{1}{\sqrt{n}} &\ll_\varepsilon \prod_{\substack{p|D \\ p> N_\varepsilon}} \left(1+\frac{1}{\sqrt{N_\varepsilon}-1}\right) \le \left(1+\frac{1}{\sqrt{N_\varepsilon+1}-1}\right)^{\omega(D)} \\ &\ll D^{\frac{1}{\sqrt{N_\varepsilon+1}-1}} < D^\varepsilon. \end{aligned} \tag{2.27}$$

□

Now let us begin the proof of Proposition 2.7.

Proof of Proposition 2.7. First of all, let's recall some algebraic properties. In a Galois extension K with degree $m \ge 2$, there is

$$p\mathcal{O}_K = (\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_g)^e$$

and (1.4) $g\cdot e\cdot f = m$. And a prime p splits completely if and only if $g = m$ with $e = f = 1$.

Consider a prime $p < q_K$. Since q_K is the least prime that splits completely in K, p does not split completely. Thus, it must be $g < m$. More specifically, p is in at least one the following two cases. Let d be a divisor of m.

(i) $d \geq 2$ and $g = \frac{m}{d}$, $e = 1$, $f = d$. In this case, p is unramified with $p\mathcal{O}_K = \prod_{i=1}^{m/d} \mathfrak{p}_i$ and norm $N(\mathfrak{p}_i) = p^d$. It has local factor $\prod_{\mathfrak{p}}(1 - p^{-ds})^{-m/d}$.

(ii) p is ramified, $e > 1$. p is prime divisor of D_K.

Since this is true for every $p < q_K$. Every $n < q_K$ can be written as $n = uv$ where u is a product of primes in case (i) and v is product of ramified primes. And this factorization $n = uv$ is unique with $(u, v) = 1$. Here, we claim each u is a powerful number. Equation (1.5) implies that $\zeta_K(s)$ equals

$$\prod_{\mathfrak{p}}(1 - N(\mathfrak{p})^{-s})^{-1} = \prod_{\mathfrak{p}} \left(1 + \frac{1}{N(\mathfrak{p})^s} + \frac{1}{N(\mathfrak{p})^{2s}} + \cdots\right) = \sum_{n=1}^{\infty} \frac{r_K(n)}{n^s}.$$

Because u is a product of primes of case (i) and these primes have local factor

$$\prod_{\mathfrak{p}}(1 - p^{-ds})^{-m/d}, \quad \text{with } d \geq 2,$$

in order to get the u-th term $\frac{r_K(u)}{u^s}$, we can expand the product

$$\prod_{d|m, d\geq 2} \left(\prod_{\mathfrak{p}}(1 - p^{-ds})^{-m/d}\right) = \prod \left(1 + \frac{1}{p^d} + \cdots\right)^{m/d}.$$

Since $d \geq 2$, this u satisfies $p|u \Rightarrow p^2|u$. Hence it is a *squarefull number*.

Since p is ramified if and only if $p|D_K$ and v is product of ramified primes, this implies that v satisfies $p|v \Rightarrow p|D_K$. Hence $v \in D^{\infty}$.

Now because $n = uv$ is unique and $r_K(n)$ is multiplicative, we have the identity

$$\sum_{n<q_K} r_K(n) = \sum_{v\in D^\infty} \sum_{\substack{u \text{ squarefull} \\ u<\frac{q_K}{v}}} r_K(uv) = \sum_{v\in D^\infty} r_K(v) \sum_{\substack{u \text{ squarefull} \\ u<\frac{q_K}{v}}} r_K(u). \tag{2.28}$$

The remaining work is to estimate the upon double sum. Since u is squarefull number and also $r_K(n) \ll n^\varepsilon$ for any $\varepsilon > 0$, applying Proposition 2.8 on the right-hand-side of (2.28) we can see that

$$\begin{aligned}
\sum_{v\in D^\infty} r_K(v) \sum_{\substack{u \text{ squarefull} \\ u<\frac{q_K}{v}}} r_K(u) &\ll \sum_{v\in D^\infty} r_K(v) \left(\frac{q_K}{v}\right)^\varepsilon \sum_{\substack{u \text{ squarefull} \\ u<\frac{q_K}{v}}} 1 \\
&\ll \sum_{v\in D^\infty} v^\varepsilon \left(\frac{q_K}{v}\right)^{1/2+\varepsilon} \\
&= q_K^{1/2+\varepsilon} \sum_{v\in D^\infty} v^{-1/2}.
\end{aligned} \tag{2.29}$$

Using Proposition 2.9 , we have

$$\sum_{n<q_K} r_K(n) \ll_\varepsilon q_K^{1/2+\varepsilon} |D_K|^\varepsilon.$$

Thus, the proof of Proposition 2.7 is complete. □

3 A SMOOTH SUMMATION FORMULA WITH THE SUBCONVEXITY BOUND

We call a sum is *"smooth"* if $\sum_{n=1}^{\infty} f(n)W(n)$, where $f(n)$ is arbitrary and $W(n)$ is smooth analytically. Often in number theory, we want to estimate sum like $\sum_{n\leq x} f(n)$. It is typically easier to estimate the "smooth" sum of the form $\sum_{n=1}^{\infty} f(n)W(n/x)$, where $W(n)$ is smooth analytically and essentially supported on $[0,1]$.

In this chapter, we consider the smooth sum $\sum_{n=1}^{\infty} r_K(n)e^{-n/x}$. Note that since e^{-x} is smooth and decays very rapidly for x exceeding 1. In our case, if $n > x^{1+\varepsilon}$ for any $\varepsilon > 0$, then the tail of the smooth sum is very small, that is, $O(x^{-\varepsilon})$. Allowing such an error, this smooth sum and sharp sum $\sum_{n<x^{1+\varepsilon}} r_K(n)$ are almost the same. There are two reasons of using the smooth sum. One is that Mellin's transform does not have error terms however, in this case, using Perron's formula has some unnecessary error terms. Another reason is that we need use subconvexity bound on half line and the gamma factor from Mellin's transform simplifies the bound.

Throughout we let $\int_{(c)}$ denote $\int_{c-i\infty}^{c+i\infty}$ for any $c \in \mathbb{R}$.

3.1 Summation formula of $\sum_{n=1}^{\infty} r_K(n)e^{-n/x}$

Theorem 3.1. *Let $\zeta_K(s)$ be the Dedekind zeta-function with degree $m = r_1 + 2r_2 \geq 2$. We have*

$$\sum_{n=1}^{\infty} r_K(n)e^{-\frac{n}{x}} = \zeta_K(0) + x\operatorname*{Res}_{s=1}\zeta_K(s) + 2^{r_1}\frac{(2\pi)^{r_2}x}{\sqrt{|D_K|}}\sum_{n=1}^{\infty} r_K(n)W\big(\frac{nx}{|D_K|}\big), \tag{3.1}$$

where

$$W(y) = \frac{1}{2\pi i}\int_{(\frac{3}{2})}\Big(\cos\frac{s\pi}{2}\Big)^{r_1}\frac{\Gamma(s)^{r_1+r_2}}{\Gamma(1-s)^{r_2-1}}((2\pi)^m y)^{-s}ds. \tag{3.2}$$

The term $\zeta_K(0) = 0$ *if* $r_1 + r_2 \geq 2$.

Proof of Theorem 3.1. Our strategy here is that first transfer the summation formula to be a contour integral. Instead of Perron's formula, because of the weight function $e^{-\frac{n}{x}}$, we can use inverse Mellin's transform to do it. Secondly, we do contour shift. Applying residue theorem, we get the main terms and a vertical contour integral in left half plane. Next we flip the integral back to right half plane. Last step is simplifying the result and getting the $W(y)$ function.

Let us begin with the inverse Mellin's transform of Γ function. For $x > 0$ and $c > 0$, we have

$$e^{-x} = \frac{1}{2\pi i} \int_{(c)} \Gamma(s) x^{-s} ds.$$

Let c be $3/2$ and substitute n/x for the original x. Note that it it still valid for $0 < (n/x) < \infty$. Thus, we can see that

$$e^{-n/x} = \frac{1}{2\pi i} \int_{(\frac{3}{2})} \Gamma(s) \frac{x^s}{n^s}\, ds.$$

Multiplying both sides by $r_K(n)$ and adding them for n from 1 to ∞, we can deduce that

$$\begin{aligned} \sum_{n=1}^{\infty} r_K(n) e^{-n/x} &= \sum_{n=1}^{\infty} r_K(n) \left(\frac{1}{2\pi i} \int_{(\frac{3}{2})} \Gamma(s) \frac{x^s}{n^s}\, ds \right) \\ &= \sum_{n=1}^{\infty} \frac{1}{2\pi i} \int_{(\frac{3}{2})} \Gamma(s) \frac{r_K(n)}{n^s} x^s\, ds \\ &= \frac{1}{2\pi i} \int_{(\frac{3}{2})} \Gamma(s) \sum_{n=1}^{\infty} \frac{r_K(n)}{n^s} x^s\, ds \\ &= \frac{1}{2\pi i} \int_{(\frac{3}{2})} \Gamma(s) \zeta_K(s) x^s\, ds. \end{aligned} \tag{3.3}$$

Since the series $\sum r_K(n) n^{-s}$ defined initially for $\Re(s) > 1$ and it is absolutely convergent for $\Re(s) = 3/2 > 1$, we can switch the $\int$ and $\sum$ in upon formula.

Next we use residue theorem and move the integration to the vertical line $\Re(s) = -1/2$. (I will explain this contour shift in Section 3.4.) This contour shift passes the simple pole of $\zeta_K(s)$ at $s = 1$ and the simple pole of $\Gamma(s)$ at $s = 0$. Note that $\zeta_K(s)$ is analytic at

$s = 0$. If $r_1 + r_2 \geq 2$, $\zeta_K(s)$ holds a trivial zero at $s = 0$, which may cancel the simple pole of $\Gamma(s)$. Thus, $\zeta_K(s)\Gamma(s)x^s$ has residues at $s = 0, 1$. We let

$$\begin{aligned} R_0(x) &= \operatorname*{Res}_{s=0} \zeta_K(s)\Gamma(s)x^s = \zeta_K(0), \\ R_1(x) &= \operatorname*{Res}_{s=1} \zeta_K(s)\Gamma(s)x^s = x\operatorname*{Res}_{s=1} \zeta_K(s). \end{aligned} \tag{3.4}$$

By functional equation (1.7), we flip the vertical contour back to the vertical line of $\Re(s) = 3/2$. Then we can see that

$$\begin{aligned} \sum_{n=1}^{\infty} r_K(n)e^{-n/x} &= R_0(x) + R_1(x) + \frac{1}{2\pi i}\int_{(-\frac{1}{2})} \Gamma(s)\zeta_K(s)x^s\, ds \\ &= R_0(x) + R_1(x) + \frac{1}{2\pi i}\int_{\frac{3}{2}+i\infty}^{\frac{3}{2}-i\infty} \zeta_K(1-s)\Gamma(1-s)x^{1-s}\, d(1-s) \\ &= R_0(x) + R_1(x) + \frac{1}{2\pi i}\int_{(\frac{3}{2})} \hat{\gamma}(s)\zeta_K(s)\Gamma(1-s)x^{1-s}\, ds. \end{aligned} \tag{3.5}$$

Next we shall simplify the right integral in above formula. Let $I(x)$ denote this integral. Since $\zeta_K(s) = \sum r_K(n)n^{-s}$ converges normally in $\Re(s) > 1$, again we can switch $\sum$ and $\int$. Thus, $I(x)$ simplifies to

$$\begin{aligned} I(x) &= \frac{1}{2\pi i}\int_{(\frac{3}{2})} \hat{\gamma}(s)\zeta_K(s)\Gamma(1-s)x^{1-s}\, ds \\ &= \frac{1}{2\pi i}\int_{(\frac{3}{2})} \hat{\gamma}(s)\sum_{n=1}^{\infty}\frac{r_K(n)}{n^s}\Gamma(1-s)x^{1-s}\, ds \\ &= x\sum_{n=1}^{\infty} r_K(n)\frac{1}{2\pi i}\int_{(\frac{3}{2})} \hat{\gamma}(s)\Gamma(1-s)(nx)^{-s}\, ds. \end{aligned} \tag{3.6}$$

Insert the gamma factors $\hat{\gamma}(s)$ (1.9) and (1.10) into above formula, hence we continue simplifying and obtain that

$$\begin{aligned}
I(x) &= x\sum_{n=1}^{\infty} r_K(n)\frac{1}{2\pi i}\int_{(\frac{3}{2})} \hat{\gamma}_K(s)\Gamma(1-s)(nx)^{-s}\,ds \\
&= x\sum_{n=1}^{\infty} r_K(n)\frac{1}{2\pi i}\int_{(\frac{3}{2})} |D_K|^{s-\frac{1}{2}}\frac{\Gamma_{\mathbb{R}}(s)^{r_1}}{\Gamma_{\mathbb{R}}(1-s)^{r_1}}\frac{\Gamma_{\mathbb{C}}(s)^{r_2}}{\Gamma_{\mathbb{C}}(1-s)^{r_2}}\Gamma(1-s)(nx)^{-s}\,ds \\
&= x\sum_{n=1}^{\infty} r_K(n)\frac{1}{2\pi i}\int_{(\frac{3}{2})} |D_K|^{s-\frac{1}{2}}\Big[\pi^{\frac{1}{2}-s}\frac{\Gamma(\frac{s}{2})}{\Gamma(\frac{1-s}{2})}\Big]^{r_1}\Big[(2\pi)^{1-2s}\frac{\Gamma(s)}{\Gamma(1-s)}\Big]^{r_2}\Gamma(1-s)(nx)^{-s}\,ds \\
&= \pi^{r_1/2}\frac{(2\pi)^{r_2}x}{\sqrt{|D_K|}}\sum_{n=1}^{\infty} r_K(n)\frac{1}{2\pi i}\int_{(\frac{3}{2})} \Big[\frac{\Gamma(\frac{s}{2})}{\Gamma(\frac{1-s}{2})}\Big]^{r_1}\Big[\frac{\Gamma(s)}{\Gamma(1-s)}\Big]^{r_2}\Gamma(1-s)\Big(\frac{(2\pi)^m nx}{2^{r_1}|D_K|}\Big)^{-s}\,ds.
\end{aligned} \tag{3.7}$$

To simplify the left gamma ratio in last equation of (3.7), we need the Legendre's duplication formula:

$$\frac{\Gamma(\frac{s}{2})}{\Gamma(\frac{1-s}{2})} = \pi^{-\frac{1}{2}}2^{1-s}\cos\Big(\frac{s\pi}{2}\Big)\Gamma(s).$$

Using the duplication formula, the integral $I(x)$ becomes

$$I(x) = 2^{r_1}\frac{(2\pi)^{r_2}x}{\sqrt{|D_K|}}\sum_{n=1}^{\infty} r_K(n)W\Big(\frac{nx}{|D_K|}\Big), \tag{3.8}$$

where

$$W(y) = \frac{1}{2\pi i}\int_{(\frac{3}{2})}\Big(\cos\frac{s\pi}{2}\Big)^{r_1}\frac{\Gamma(s)^{r_1+r_2}}{\Gamma(1-s)^{r_2-1}}((2\pi)^m y)^{-s}\,ds. \tag{3.9}$$

Now the proof is complete. □

3.2 Two special cases

In this section we give the smooth summation formula in two special cases in which the weight function $W(y)$ has a nice form.

Example 3.2. *For $m = 2$ and $r_1 = 0, r_2 = 1$, we have*

$$\sum_{n=1}^{\infty} r_K(n)e^{-n/x} = \zeta_K(0) + x\operatorname*{Res}_{s=1}\zeta_K(s) + \frac{2\pi x}{\sqrt{|D_K|}}\sum_{n=1}^{\infty} r_K(n)e^{-4\pi^2 nx/|D_K|}. \tag{3.10}$$

Because $m = 2$, $r_1 = 0$ and $r_2 = 1$, by Theorem 3.1, we have that

$$\sum_{n=1}^{\infty} r_K(n)e^{-n/x} = \zeta_K(0) + x\operatorname*{Res}_{s=1}\zeta_K(s) + \frac{2\pi x}{\sqrt{|D_K|}}\sum_{n=1}^{\infty} r_K(n)W\Big(\frac{nx}{|D_K|}\Big)$$

where

$$W\Big(\frac{nx}{|D_K|}\Big) = \frac{1}{2\pi i}\int_{(\frac{3}{2})} \Gamma(s)\Big(\frac{4\pi^2 nx}{|D_K|}\Big)^{-s} ds.$$

We notice that the weight function $W(nx/|D_K|)$ satisfies the Mellin's inverse transform. It follows that

$$W\Big(\frac{nx}{|D_K|}\Big) = \frac{1}{2\pi i}\int_{(\frac{3}{2})} \Gamma(s)\left(\frac{4\pi^2 nx}{|D_K|}\right)^{-s} ds = \exp\left\{-\frac{4\pi^2 nx}{|D_K|}\right\}. \tag{3.11}$$

Therefore, the summation formula becomes

$$\sum_{n=1}^{\infty} r_K(n)e^{-n/x} = \zeta_K(0) + x\operatorname*{Res}_{s=1}\zeta_K(s) + \frac{2\pi x}{\sqrt{|D_K|}}\sum_{n=1}^{\infty} r_K(n)e^{-4\pi^2 nx/|D_K|}.$$

Example 3.3. *Let $m = 3$, $r_1 = 1$, and $r_2 = 1$. We have*

$$\sum_{n=1}^{\infty} r_K(n)e^{-n/x} = x\operatorname*{Res}_{x=1}\zeta_K(s) + \Re\left\{\frac{8\pi x}{\sqrt{|D_K|}}\sum_{n=1}^{\infty} r_K(n)K_0\left(2\sqrt{\frac{8\pi^3 inx}{|D_K|}}\right)\right\} \tag{3.12}$$

where $K_0(z)$ is the modified Bessel K-function.

Since $m = 3$, $r_1 = 1$ and $r_2 = 1$, we plug them into Theorem 3.1 and get that

$$\sum_{n=1}^{\infty} r_K(n)e^{-n/x} = x\operatorname*{Res}_{s=1}\zeta_K(s) + \frac{4\pi x}{\sqrt{|D_K|}}\sum_{n=1}^{\infty} r_K(n)W\Big(\frac{nx}{|D_K|}\Big), \tag{3.13}$$

with weight function:

$$W\Big(\frac{nx}{|D_K|}\Big) = \frac{1}{2\pi i}\int_{(\frac{3}{2})} \Big(\cos\frac{s\pi}{2}\Big)\Gamma(s)^2\Big(\frac{8\pi^3 nx}{|D_K|}\Big)^{-s} ds.$$

In order to simplify the upon formula, we first want to simplify the cosine part. Recall the Euler's identity:

$$\cos\Big(\frac{s\pi}{2}\Big) = \frac{e^{s\pi i/2} + e^{-s\pi i/2}}{2} = \frac{i^s + (-i)^s}{2}.$$

Using it, we can split the cosine to be two terms. It follows that

$$\begin{aligned} W\Big(\frac{nx}{|D_K|}\Big) &= \frac{1}{2\pi i}\int_{(\frac{3}{2})} \frac{1}{2}\Big(i^s + (-i)^s\Big)\Gamma(s)^2\Big(\frac{8\pi^3 nx}{|D_K|}\Big)^{-s} ds \\ &= \frac{1}{4\pi i}\int_{(\frac{3}{2})} \Gamma(s)^2\Big(\frac{-i8\pi^3 nx}{|D_K|}\Big)^{-s} ds \\ &+ \frac{1}{4\pi i}\int_{(\frac{3}{2})} \Gamma(s)^2\Big(\frac{i8\pi^3 nx}{|D_K|}\Big)^{-s} ds. \end{aligned} \tag{3.14}$$

Moreover, we have the following integral transform formula from Paris and Kaminski [PK01, page 97, (3.3.35)]:

$$\frac{1}{2\pi i}\int_{\sigma-\infty i}^{\sigma+\infty i} \Gamma(s+a)^2 z^{-s}\, ds = 2z^a K_0(2z^{1/2}), \tag{3.15}$$

where $\sigma > \Re(a)$ and $K_0(s)$ is the modified Bessel K-function. Analytic continuation enables (3.15) to be extended to $|\arg z| < \pi$. In our case, we set $a = 0$, $\sigma = 3/2$, and we have

$$\left|\arg\left(\frac{\pm 8\pi^3 inx}{|D_K|}\right)\right| = \frac{\pi}{2} < \pi.$$

Thus, the two integrals in (3.14) can be combined as

$$\frac{1}{4\pi i}\int_{(\frac{3}{2})} \Gamma(s)^2\left(\pm\frac{8\pi^3 inx}{|D_K|}\right)^{-s} ds = K_0\left(2\sqrt{\frac{\pm 8\pi^3 inx}{|D_K|}}\right). \tag{3.16}$$

It is known that Bessel-Kfunctions also satisfy the reflection principle $\overline{K_0(\overline{z})} = K_0(z)$. Now we can combine it with (3.16) and (3.14). The weight function becomes

$$\begin{aligned} W\Big(\frac{nx}{|D_K|}\Big) &= K_0\left(2\sqrt{\frac{8\pi^3 inx}{|D_K|}}\right) + K_0\left(2\sqrt{\frac{-8\pi^3 inx}{|D_K|}}\right) \\ &= K_0\left(2\sqrt{\frac{8\pi^3 inx}{|D_K|}}\right) + \overline{K_0\left(2\sqrt{\frac{8\pi^3 inx}{|D_K|}}\right)} \\ &= 2\Re\left\{K_0\left(2\sqrt{\frac{8\pi^3 inx}{|D_K|}}\right)\right\}. \end{aligned} \tag{3.17}$$

Inserting (3.17) back into (3.13), we can get the form stated in Example 3.3.

3.3 Subconvexity and an estimate of $\sum_{n=1}^{\infty} r_K(n)e^{-n/x}$

In this section our purpose is to use the subconvexity bound to estimate the smooth sum $\sum r_K(n)e^{-n/x}$. First let us recall the subconvexity hypothesis we stated in chapter one. (This hypothesis can be found in Einsiedler, Lindenstrauss, Michel and Venkatesh [ELMV11, page 880].)

Hypothesis 1.6. *Let K be a number field of fixed degree m. There exists $\theta, N > 0$ (depending at most on m) such that for $\Re(s) = 1/2$,*

$$\zeta_K(s) \ll_m |s|^N |D_K|^{1/4-\theta}. \tag{1.12}$$

If we assume this subconvexity bound, we deduce a "better" estimate as below.

Theorem 3.4. *Let $K/\mathbb{Q}$ be a finite extension with degree m and suppose Hypothesis 1.6 holds for some $\theta, N > 0$. Then*

$$\sum_{n=1}^{\infty} r_K(n)e^{-n/x} = x\operatorname*{Res}_{s=1}\zeta_K(s) + O_m(\sqrt{x}|D_K|^{1/4-\theta}). \tag{3.18}$$

Note that if suppose $x = \sqrt{|D_K|}$, the total error of Theorem 3.4, if in terms of x, is $O(x^{1-2\theta})$. This is better than the result from convexity bound. Essentially we use this key to beat the trivial bound for q_K.

Proof of Theorem 3.4. This proof is analogous to the proof of Theorem 3.1. We first use the inverse Mellin's transform. Then shift contour to half line $\Re s = 1/2$ to filter out the main term. Next we move it to half line so that we can apply the subconvexity bound.

The first step is the same as that in Theorem 3.1, hence we recall the formula (3.3) which is

$$\sum_{n=1}^{\infty} r_K(n) e^{-n/x} = \frac{1}{2\pi i} \int_{(\frac{3}{2})} \Gamma(s)\zeta_K(s) x^s \, ds.$$

At this position, we move contour $\Re s = 3/2$ to $\Re s = 1/2$. Again, I will explain the contour shift in section 3.4. Because $\Gamma(s)$, x^s are analytic in half plane $\Re s > 0$ and $\zeta_K(s)$ holds a pole at $s = 1$, this contour shift only passes the pole $s = 1$ of $\Gamma(s)\zeta_K(s)x^s$. Thus, we deduce that

$$\begin{aligned} \sum_{n=1}^{\infty} r_K(n) e^{-n/x} &= \operatorname*{Res}_{s=1}\Big(\Gamma(s)\zeta_K(s)x^s\Big) + \frac{1}{2\pi i} \int_{(\frac{1}{2})} \Gamma(s)\zeta_K(s) x^s \, ds. \\ &= x \operatorname*{Res}_{s=1} \zeta_K(s) + \frac{1}{2\pi i} \int_{(\frac{1}{2})} \Gamma(s)\zeta_K(s) x^s \, ds. \end{aligned} \tag{3.19}$$

Further, in order to estimate the contour integral in upon formula, we need use Stirling's formula:

$$\Gamma(\sigma + it) = \sqrt{2\pi}(it)^{\sigma - 1/2} e^{-\pi t/2} \left(t/e\right)^{it} \left\{1 + O\left(1/t\right)\right\}, \quad t > 0.$$

Since $\Gamma(s)$ satisfies the reflection principle, we have a symmetric estimate of $\Gamma(s)$ for $1/2 - it$. Thus, for $t > 0$, the gamma function on half line can be estimated as

$$\begin{aligned} \Gamma(1/2 + it) &= \sqrt{2\pi} e^{-\pi t/2} \left(t/e\right)^{it} \left\{1 + O\left(1/t\right)\right\} \ll e^{-\pi t/2}, \\ \Gamma(1/2 - it) &= \sqrt{2\pi} e^{-\pi t/2} \left(t/e\right)^{-it} \left\{1 + O\left(1/t\right)\right\} \ll e^{-\pi t/2}. \end{aligned} \tag{3.20}$$

To be short, we combine two formulas in (3.20). For any real t, we have that

$$\Gamma(1/2+it) \ll e^{-\pi|t|/2}. \tag{3.21}$$

Moreover, since we suppose the subconvexity hypothesis holds, we have that

$$x^{1/2+it} \ll |x^{1/2}x^{it}| = \sqrt{x}, \tag{3.22}$$

and

$$\zeta_K(1/2+it) \ll_m |1/2+it|^N |D_K|^{1/4-\theta} \ll |t|^N |D_K|^{1/4-\theta}. \tag{3.23}$$

Now we put (3.21),(3.22) and (3.23) into (3.19) and deduce that

$$\begin{aligned}
\sum_{n=1}^{\infty} r_K(n)e^{-n/x} &= x\operatorname*{Res}_{s=1}\zeta_K(s) + \lim_{T\to\infty}\frac{1}{2\pi i}\int_{\frac{1}{2}-iT}^{\frac{1}{2}+iT}\Gamma(1/2+it)\zeta_K(1/2+it)x^{1/2+it}d(1/2+it),\\
&= x\operatorname*{Res}_{s=1}\zeta_K(s) + O\Big(\lim_{T\to\infty}\frac{1}{2\pi i}\int_{-T}^{T}\sqrt{x}e^{-\pi|t|/2}|t|^N|D_K|^{1/4-\theta}\,dt\Big)\\
&= x\operatorname*{Res}_{s=1}\zeta_K(s) + O\Big(\sqrt{x}|D_K|^{1/4-\theta}\cdot\lim_{T\to\infty}\int_{-T}^{T}e^{-\pi|t|/2}|t|^N\,dt\Big)\\
&= x\operatorname*{Res}_{s=1}\zeta_K(s) + O\Big(\sqrt{x}|D_K|^{1/4-\theta}\cdot 2\lim_{T\to\infty}\int_{0}^{T}e^{-\pi t/2}t^N\,dt\Big).
\end{aligned} \tag{3.24}$$

Here let us look at the integral $\int_0^\infty e^{-\pi t/2}t^N\,dt$. We claim it is bounded. Since, we know there exists some $0 < M < \infty$ (M depends on N) such that $t^{N+2} \le e^{\pi t/2}$ whenever $t > M$. Next we truncate the integral to be $\{\int_0^M + \int_M^\infty\}e^{-\pi t/2}t^N dt$ and estimate them separately. For the second piece, we have that

$$\Big|\int_M^\infty e^{-\pi t/2}t^N\,dt\Big| \le \int_M^\infty |e^{-\pi t/2}t^N|\,dt \le \int_M^\infty t^{-2}\,dt < \infty.$$

The first integral is bounded (depending on N) as

$$\Big|\int_0^M e^{-\pi t/2}t^N\,dt\Big| \le \int_0^M M^N dt = M^{N+1} < \infty.$$

This constant N only depends on m (the degree of the number field K), hence we conclude that

$$\lim_{T\to\infty}\int_0^T e^{-\pi t/2}t^N\,dt=\left\{\int_0^M+\int_M^\infty\right\}e^{-\pi t/2}t^N\,dt=O_m(1).$$

Therefore, formula (3.24) becomes

$$\sum_{n=1}^{\infty}r_K(n)e^{-n/x}=x\operatorname*{Res}_{s=1}\zeta_K(s)+O(\sqrt{x}|D_K|^{1/4-\theta}),$$

which completes the proof. □

3.4 About contour shift

In this section we give the proof of the two contour shifts used in previous section. Here our start point is formula (3.3). One is shifting the contour from $\Re(s)=\frac{3}{2}$ to $\Re(s)=-\frac{1}{2}$ and get (3.5). Another is we shifting the same contour to $\Re(s)=\frac{1}{2}$ and get (3.19). Now let us begin the first one.

Proof of First Contour Shift. Consider

$$\frac{1}{2\pi i}\int_{(\frac{3}{2})}\Gamma(s)\zeta_K(s)x^s\,ds=\lim_{T\to\infty}\int_{\frac{3}{2}-iT}^{\frac{3}{2}+iT}\Gamma(s)\zeta_K(s)x^s\,ds. \tag{3.25}$$

Our goal is to move it to vertical line $\Re(s)=-1/2$. By residue theorem,

$$\begin{aligned}\frac{1}{2\pi i}\left\{\int_{\frac{3}{2}-iT}^{\frac{3}{2}+iT}+\int_{\frac{3}{2}+iT}^{-\frac{1}{2}+iT}+\int_{-\frac{1}{2}+iT}^{-\frac{1}{2}-iT}+\int_{-\frac{1}{2}-iT}^{\frac{3}{2}-iT}\right\}\Big(\Gamma(s)\zeta_K(s)x^s\Big)\,ds&\\ =\operatorname*{Res}_{s=0}\Big(\Gamma(s)\zeta_K(s)x^s\Big)+\operatorname*{Res}_{s=1}\Big(\Gamma(s)\zeta_K(s)x^s\Big).&\end{aligned}$$

For convenience, we let $R_0(x), R_1(x)$ denote the two residues. Then we can rewrite it as

$$\begin{aligned}\frac{1}{2\pi i}\int_{\frac{3}{2}-iT}^{\frac{3}{2}+iT}\Gamma(s)\zeta_K(s)x^s\,ds = R_0(x)+R_1(x)+\frac{1}{2\pi i}\int_{-\frac{1}{2}-iT}^{-\frac{1}{2}+iT}\Gamma(s)\zeta_K(s)x^s\,ds \\ +\frac{1}{2\pi i}\left\{\int_{\frac{3}{2}-iT}^{-\frac{1}{2}-iT}+\int_{-\frac{1}{2}+iT}^{\frac{3}{2}+iT}\right\}\Big(\Gamma(s)\zeta_K(s)x^s\Big)\,ds.\end{aligned} \tag{3.26}$$

Next we want to estimate the two horizontal contour integrals. Since they are conjugate, without loss of generality, we only need estimate the upper horizontal integral. We obtain that

$$\begin{aligned}\left|\int_{-\frac{1}{2}+iT}^{\frac{3}{2}+iT}\Gamma(s)\zeta_K(s)x^s\,ds\right| &= \left|\int_{-1/2}^{3/2}\Gamma(\sigma+iT)\zeta_K(\sigma+iT)x^{\sigma+iT}d\sigma\right| \\ &\le \int_{-1/2}^{3/2}|\Gamma(\sigma+iT)\zeta_K(\sigma+iT)x^{\sigma}|d\sigma.\end{aligned} \tag{3.27}$$

In order to bound the right-hand-side of (3.27), we need bound the $|\Gamma(s)|$, $|\zeta_K(s)|$ and $|x^\sigma|$ on the horizontal line segment. First and easiest is to bound $|x^\sigma|$. (Here we can suppose $x>1$, because this x determines the length of the support of the smooth summation.) Since $-1/2\le\sigma\le 3/2$, we get that

$$x^\sigma \le x^{3/2}. \tag{3.28}$$

To bound the $\Gamma(s)$ factor, again we use Stirling's formula and see that

$$|\Gamma(\sigma+iT)| \ll T^{\sigma-1/2}e^{-\pi T/2}. \tag{3.29}$$

To estimate $|\zeta_K(s)|$ on this horizontal contour, we use Phragmén-Lindelöf convexity principle. In order to apply the convexity principle, we first need the bounds at left and right vertices. Since for $\sigma>1$, $t>0$, by functional equation (1.2) and formula (5.3) we have that

$$\begin{aligned}&\zeta_K(\sigma+it) = O(1)\\ &\zeta_K(1-\sigma+it) = \hat{\gamma}_K(\sigma-it)\,\zeta_K(1-\sigma+it) \ll |D_K|^{\sigma-1/2}\,(t/2\pi)^{m(\sigma-1/2)}\end{aligned}$$

In particular, there are

$$\zeta_K(-\tfrac{1}{2}+iT) \ll |D_K|T^m, \quad \text{and} \quad \zeta_K(0+iT) \ll |D_K|^{1/2}T^{m/2}.$$

Thereafter, by convexity principle, we can deduce the bound of $\zeta_K(s)$. In the upper critical strip $0 \le \sigma \le 1$, $t > 0$, the estimate is that

$$\zeta_K(\sigma+it) \ll (|D_K|T^m)^{(1-\sigma)/2}. \tag{3.30}$$

It is clear to see that when $\sigma = -1/2$ the above bound is bigger. Now we put bounds of $\Gamma(s)$, $\zeta_K(s)$ and x^σ into (3.27) and obtain that

$$\begin{aligned}\Big| \int_{-\frac{1}{2}+iT}^{\frac{3}{2}+iT} \Gamma(s)\zeta_K(s)x^s\,ds\Big| &\ll \int_{-1/2}^{3/2} T^{1/2}e^{-\pi T/2}|D_K|T^m x^{3/2}\,d\sigma \\ &= \frac{2|D_K|T^{m+1/2}x^{3/2}}{e^{\pi T/2}} \to 0, \quad \text{as } T\to\infty.\end{aligned}$$

Symmetrically, the lower horizontal integral is also bounded as

$$\Big| \int_{-\frac{1}{2}-iT}^{\frac{3}{2}-iT} \Gamma(s)\zeta_K(s)x^s\,ds\Big| \to 0, \quad \text{as } T\to\infty.$$

Therefore, letting T go to ∞, (3.26) becomes

$$\frac{1}{2\pi i}\int_{\frac{3}{2}-i\infty}^{\frac{3}{2}+i\infty} \Gamma(s)\zeta_K(s)x^s\,ds = R_0(x) + R_1(x) + \frac{1}{2\pi i}\int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty} \Gamma(s)\zeta_K(s)x^s\,ds. \tag{3.31}$$

This proves the first contour shift. □

Next we show the second contour shift. The idea is very similar.

Proof of Second Contour Shift. In this proof we shift the contour of (3.3) from $\Re(s) = 3/2$ to half line $\Re(s) = 1/2$. Again by residue theorem,

$$\frac{1}{2\pi i}\left\{\int_{\frac{3}{2}-iT}^{\frac{3}{2}+iT} + \int_{\frac{3}{2}+iT}^{\frac{1}{2}+iT} + \int_{\frac{1}{2}+iT}^{\frac{1}{2}-iT} + \int_{\frac{1}{2}-iT}^{\frac{3}{2}-iT}\right\}\Big(\Gamma(s)\zeta_K(s)x^s\Big)ds = R_1(x).$$

We rewrite it to be

$$\begin{aligned}\frac{1}{2\pi i}\int_{\frac{3}{2}-iT}^{\frac{3}{2}+iT}\Gamma(s)\zeta_K(s)x^s\,ds = R_1(x) + \frac{1}{2\pi i}\int_{\frac{1}{2}-iT}^{\frac{1}{2}+iT}\Gamma(s)\zeta_K(s)x^s ds \\ + \frac{1}{2\pi i}\left\{\int_{\frac{1}{2}+iT}^{\frac{3}{2}+iT} + \int_{\frac{3}{2}-iT}^{\frac{1}{2}-iT}\right\}\Big(\Gamma(s)\zeta_K(s)x^s\Big)ds.\end{aligned} \tag{3.32}$$

Then we estimate the two horizontal contour integrals. Symmetrically, we only consider the upper horizontal integral. By the bounds of $\Gamma(s)$, $\zeta_K(s)$ and x^σ on the horizontal line segment. (They are (3.29), (3.30) and (3.28)), the integral can be bound as

$$\begin{aligned}\Big|\int_{\frac{1}{2}+iT}^{\frac{3}{2}+iT}\Gamma(s)\zeta_K(s)x^s\,ds\Big| &\le \int_{1/2}^{3/2}|\Gamma(\sigma+iT)\zeta_K(\sigma+iT)x^\sigma|d\sigma \\ &\ll \int_{1/2}^{3/2} Te^{-\pi T/2}(|D_K|T^m)^{1/4}x^{3/2}d\sigma \\ &= \frac{|D_K|^{1/4}T^{1+m/4}x^{3/2}}{e^{\pi T/2}} \;\to\; 0, \quad \text{as } T\to\infty.\end{aligned}$$

By the same method, the lower horizontal integral is bounded and

$$\Big|\int_{\frac{1}{2}-iT}^{\frac{3}{2}-iT}\Gamma(s)\zeta_K(s)x^s ds\Big| \;\to\; 0, \quad \text{as } T\to\infty.$$

Finally, let T tend to infinity. Then (3.31) becomes

$$\frac{1}{2\pi i}\int_{\frac{3}{2}-i\infty}^{\frac{3}{2}+i\infty}\Gamma(s)\zeta_K(s)x^s ds = R_1(x) + \frac{1}{2\pi i}\int_{\frac{1}{2}-i\infty}^{\frac{1}{2}+i\infty}\Gamma(s)\zeta_K(s)x^s ds. \tag{3.33}$$

This completes the second contour shift. □

4 THE LEAST PRIME THAT SPLITS COMPLETELY IN DIHEDRAL GALOIS NUMBER FIELDS

4.1 Proof of main theorem

We are going to prove the main theorem in this section. First let us recall it.

Theorem 1.7 (Main Theorem)**.** *Let $K/\mathbb{Q}$ be a Galois extension and suppose that Hypothesis 1.6 holds for some $\theta, N > 0$. Then*

$$q_K \ll |D_K|^{1/2-2\theta+\varepsilon}, \tag{1.13}$$

for any $\varepsilon > 0$. The implied constant depends on ε and degree $[K : \mathbb{Q}]$.

Proof of Main Theorem 1.7. Throughout we suppose the Hypothesis 1.6 holds and $\sup\{q_K\}$ is unbounded as $|D_K| \to \infty$. The second assumption is natural because if q_K is bounded in terms of D_K, then this is the ideal case.

We first give the sketch of the proof. We estimate the smooth sum $\sum_{n=1}^{\infty} r_K(n)e^{-n/x}$ in two different ways. In an *analytic* way, using Theorem 3.4 and Siegel-Brauer Theorem and *assuming* $q_K > C|D_K|^{1/2-2\theta}$, we can get a lower bound of this smooth sum, which is $q_K|D_K|^{-\varepsilon}$. In an *algebraic* way, by Proposition 2.7, we can get an upper bound of this sum, and that is $q_K^{1/2+\varepsilon}|D_K|^{\varepsilon}$. Equating them, we find $q_K|D_K|^{-\varepsilon} \ll q_K^{1/2+\varepsilon}|D_K|^{\varepsilon}$, which is a contradiction. Hence the inequality $q_K > C|D_K|^{1/2-2\theta}$ doesn't hold. It follows that $q_K \ll |D_K|^{1/2-2\theta+\varepsilon}$.

Since we suppose the subconvexity Hypothesis 1.6 holds, by Theorem 3.4, we have

$$\sum_{n=1}^{\infty} r_K(n)e^{-n/x} = x\operatorname*{Res}_{s=1}\zeta_K(s) + O_m(\sqrt{x}|D_K|^{1/4-\theta}).$$

Recall the corollary of Siegel-Brauer Theorem (Corollary 2.5), which states that for $|D_K|$ bigger than some ineffective N_ε, we have

$$\operatorname*{Res}_{s=1}\zeta_K(s) > |D_K|^{-\varepsilon}. \tag{4.1}$$

Now we put this into the previous formula, and deduce that

$$\sum_{n=1}^{\infty} r_K(n)e^{-n/x} > x|D_K|^{-\varepsilon} + O(\sqrt{x}|D_K|^{1/4-\theta}). \tag{4.2}$$

Next we use an algebraic way to bound this smooth sum. We want to truncate this sum first. If $n \geq x\log x$, then the tail of the smooth sum is

$$\begin{aligned}
\sum_{n\geq x\log x}^{\infty} r_K(n)e^{-\frac{n}{x}} &= \int_{x\log x}^{\infty} r_K(n)e^{-\frac{n}{x}}d(\lfloor n\rfloor) = \int_{x\log x}^{\infty} r_K(n)e^{-\frac{n}{x}}dn + O\left(x^{\varepsilon-1}\right) \\
&\ll x^{1+\varepsilon}\int_{x\log x}^{\infty}\frac{n^\varepsilon}{x^\varepsilon}e^{-\frac{n}{x}}\frac{dn}{x} + O(x^{\varepsilon-1}) \\
&\overset{t=\frac{n}{x}}{=} x^{1+\varepsilon}\int_{\log x}^{\infty} t^\varepsilon e^{-t}\,dt + O(x^{\varepsilon-1}) \\
&\ll x^{1+\varepsilon}\frac{\log^\varepsilon x}{x} \ll x^\varepsilon.
\end{aligned}$$

Thus, the truncated smooth sum equals the whole sum up to the error $O(x^\varepsilon)$. Precisely, it is

$$\sum_{n=1}^{\infty} r_K(n)e^{-\frac{n}{x}} = \sum_{n<x\log x} r_K(n)e^{-\frac{n}{x}} + O(x^\varepsilon).$$

Let the least prime that splits completely $q_K = x \log x$ and it is easy to get inequality $x \geq q_K / \log q_K$. By Propostion 2.7 and $e^{-\frac{n}{x}} \leq 1$, the smooth sum can be bounded as

$$\sum_{n=1}^{\infty} r_K(n) e^{-n/x} = \sum_{n<x\log x} r_K(n) e^{-n/x} + O(x^{\varepsilon}) \ll \sum_{n<q_K} r_K(n) \ll q_K^{1/2+\varepsilon} |D_K|^{\varepsilon}. \tag{4.3}$$

Moreover, we know $x \geq \frac{q_K}{\log q_K} \gg q_K^{1-\varepsilon}$. Plug it into (4.2), we have

$$\sum_{n=1}^{\infty} r_K(n) e^{-n/x} \geq \sum_{n=1}^{\infty} r_K(n) e^{-\frac{n \log q_K}{q_K}} \gg q_K^{1-\varepsilon} |D_K|^{-\varepsilon} + O\left(\sqrt{q_K^{1-\varepsilon}} |D_K|^{1/4-\theta} \right). \tag{4.4}$$

By the definition of Big-O notation, there exists a positive constant C_1 such that the error term in above formula is bounded by $C_1 \sqrt{q_K^{1-\varepsilon}} |D_K|^{\frac{1}{4}-\theta}$. Suppose, for large $|D_K|$, there is

$$\tfrac{1}{2} q_K^{1-\varepsilon} |D_K|^{-\varepsilon} > C_1 \sqrt{q_K^{1-\varepsilon}} |D_K|^{\frac{1}{4}-\theta}. \tag{4.5}$$

Consequently, it implies

$$q_K^{\frac{1}{2}-\varepsilon} \gg |D_K|^{\frac{1}{4}-\theta+\varepsilon}. \tag{4.6}$$

Furthermore, by this assumption, the right-hand-side of (4.4) does not vanish and the main term dominates the error. Hence, if we put the lower and upper bound together, we can see that

$$q_K^{1-\varepsilon} |D_K|^{-\varepsilon} \ll \sum_{n=1}^{\infty} r_K(n) e^{-\frac{n}{x}} \ll q_K^{\frac{1}{2}+\varepsilon} |D_K|^{\varepsilon} \quad \Rightarrow \quad q_K^{\frac{1}{2}} \ll |D_K|^{3\varepsilon}. \tag{4.7}$$

However, combining (4.7) with (4.6), we deduce that

$$|D_K|^{\frac{1}{4}-\theta+\varepsilon} \ll q_K^{1/2} \ll |D_K|^{3\varepsilon},$$

which is impossible for large $|D_K|$. Thus, the inequality (4.5) is not correct for large $|D_K|$. It follows that, if we reverse the inequality (4.5), there is

$$q_K^{1-\varepsilon} |D_K|^{-\varepsilon} \ll q_K^{\frac{1-\varepsilon}{2}} |D_K|^{\frac{1}{4}-\theta}.$$

Thus, $q_K \ll |D_K|^{\frac{1}{2}-2\theta+\varepsilon}$. Our prove is complete. □

4.2 The bound of q_K in S_3-sextic number fields

The Hypothesis1.6 is known to be true, in some Galois extension number fields. In this section we give two example families of number fields in which the Hypothesis 1.6 is known.

Example 4.1. *Let K be a S_3-sextic number field. The least prime that splits completely is $q_K = O_\varepsilon(|D_K|^{0.499})$.*

In order to show the upon result, we need verify the existence of the subconvexity bound in S_3-sextic number fields. Suppose $K/\mathbb{Q}$ is Galois with Galois group S_3, $n \geq 3$. Here we need consider the factorization the Dedekind zeta-function $\zeta_K(s)$ as a product of Artin L-functions. Actually we have (see [CF10, page 227])

$$\zeta_K(s) = \zeta(s)L(s,\chi)L(s,\psi)^2,$$

where $L(s,\chi)$ is a Dirichlet L-function and $L(s,\psi)$ is a degree 2 Artin L-function. Here, the dihedral Artin L-functions $L(s,\psi)$ are known to be GL_2-automorphic L-functions by the classical work of Hecke. By the work of Duke, Friedlander and Iwaniec [DFI02], it is known that all GL_2-automorphic L-functions have subconvexity bound. And by work of Blomer, Harcos & Michel [BHM07] and Burgess [Bur63], the Dedekind zeta-function $\zeta_K(s)$ of S_3-sextic number field on half line $\Re s = 1/2$ has subconvexity bound:

$$\zeta_K(s) \ll_\varepsilon |s|^N |D_K|^{\frac{1}{4}-\frac{1}{1889}+\varepsilon}, \tag{4.8}$$

where N is an absolute constant and for any $\varepsilon > 0$. Therefore by our main theorem (Theorem 1.7), the least prime splits completely is $O_\varepsilon(|D_K|^{0.499})$.

Example 4.2. *Let $K/\mathbb{Q}$ be Galois extension with* $\mathrm{Gal}(K/\mathbb{Q}) \cong D_n$ *and* $n \geq 3$. *We have* $q_K = O_\varepsilon(|D_K|^{0.499})$.

Due to the classical work of Artin and Brauer, it is known to factor the Dedekind zeta-function of a dihedral Galois number field. Depending on the parity of n, we have

$$\zeta_K(s) = \begin{cases} \zeta(s)L(s,\chi_1)L(s,\chi_2)L(s,\chi_3) \cdot \prod_{\rho_i} L(s,\rho_i)^2, & \text{if } n \text{ is even,} \\ \zeta(s)L(s,\chi_1) \cdot \prod_{\rho_i} L(s,\rho_i)^2, & \text{if } n \text{ is odd.} \end{cases}$$

Here, these $L(s,\rho_i)$ are known to be automorphic L-functions by Hecke. Then by the same works of [DFI02], [BHM07] and [Bur63], The Dedekind zeta-function of a dihedral Galois number field has the same subconvexity bound (4.8). Therefore, this example follows.

5 A SHARP SUMMATION FORMULA

In this chapter we aim to deduce a special case of the sharp summation formula of Friedlander and Iwaniec [FI05]. This formula implies the Proposition 2.6 used in Chapter 2. The following theorem is the main result of this chapter.

5.1 Sharp summation formula and proof of Propostion 2.6

Theorem 5.1. *Let $\zeta_K(s)$ be the Dedekind zeta function with degree $m \geq 2$. Then for $x \geq |D_K|^{\frac{1}{2}}$ and any N with $1 \leq N \leq x$, we have*

$$\sum_{n \leq x} r_K(n) = R_1(x) + (\pi^2 m)^{-\frac{1}{2}} |D_K|^{\frac{1}{2m}} x^{\frac{m-1}{2m}} B(x, N) + O(|D_K|^{\frac{1}{m}} N^{-\frac{1}{m}} x^{1-\frac{1}{m}+2\varepsilon}), \tag{5.1}$$

where $R_1(x) = x \operatorname*{Res}_{s=1} \zeta_K(s)$, and

$$B(x, N) = \sum_{n \leq N} r_K(n) n^{-\frac{m+1}{2m}} \cos\left(2\pi m \left(\frac{nx}{|D_K|}\right)^{\frac{1}{m}} + \frac{\pi(r_1 - 3)}{4}\right). \tag{5.2}$$

The implied constant depends on ε.

The Proposition 2.6 immediately follows from the above theorem.

Proof of Proposition 2.6. We trivially bound the cosine by $O(1)$ and $r_K(n) \ll n^{\varepsilon}$. Hence $B(x, N)$ can be bounded as

$$B(x, N) \ll \sum_{n \leq N} n^{-\frac{m+1}{2m}+\varepsilon} \ll N^{\frac{m-1}{2m}+\varepsilon}.$$

Next we let $N = |D_K|^{\frac{1}{m+1}} x^{\frac{m-1}{m+1}}$. Then our proposition follows. $\square$

The remainder of this chapter is to prove Theorem 5.1. First of all let us recall the *Stirling's formula*:

$$\Gamma(\sigma + it) = \sqrt{2\pi}(it)^{\sigma-1/2} e^{-\pi/2t} (t/e)^{it} \{1 + O(1/t)\}, \qquad t > 0.$$

We shall put the Stirling's formula into the gamma factor (1.9) of the number field K and simplify it. Note that Stirling's formula is true for imaginary part $t > 0$, so for those $\Gamma(\sigma - t)$ we need use reflection principle $\Gamma(\overline{s}) = \overline{\Gamma(s)}$. After simplifying it, we obtain that

$$\hat{\gamma}_K(\sigma + it) = \exp\left\{-\frac{r_1\pi i}{4}\right\} \left(\frac{\sqrt[m]{|D_K|}t}{2\pi}\right)^{m\left(\sigma-\frac{1}{2}\right)} \left(\frac{\sqrt[m]{|D_K|}t}{2\pi e}\right)^{imt} \left\{1 + O\left(\frac{1}{t}\right)\right\}.$$

Symmetrically we can get a similar estimate for $\hat{\gamma}_K(\sigma - it)$. For convenience we let

$$\begin{aligned} \omega &= \exp\{-r_1\pi i/4\} \\ Q &= \sqrt[m]{|D_K|}/2\pi. \end{aligned} \tag{5.3}$$

Thus the gamma factors can be written as

$$\begin{aligned} \hat{\gamma}_K(\sigma + it) &= \omega(Qt)^{m(\sigma-1/2)} (Qt/e)^{imt} \{1 + O(1/t)\} \\ \hat{\gamma}_K(\sigma - it) &= \overline{\omega}(Qt)^{m(\sigma-1/2)} (e/Qt)^{imt} \{1 + O(1/t)\} \end{aligned} \tag{5.4}$$

where $\sigma \geq 1/2$ and $t \geq 1$. By the above two equations, we can bound $\hat{\gamma}_K$ as

$$\hat{\gamma}_K(s) \ll (Q|s|)^{m(\sigma-1/2)}, \qquad \text{for } \sigma \geq 1/2. \tag{5.5}$$

Here we need keep the (5.4) in mind, because we shall use it several times in later proof.

5.2 Proof of sharp summation formula

Now we are at the position to prove the formula of $\sum_{n\leq x} r_K(n)$.

Proof of Theorem 5.1. First we show the sketch of this proof. Overall, there are five stages. In order to calculate the sum $\sum_{n\leq x} r_K(n)$, we first use Perron's formula to transfer the sum to be a contour integral $\int_{c-iT}^{c+iT} \zeta_K(s)x^s s^{-1}ds$ plus some error terms. Next we shall apply residue theorem on the previous contour integral so that we can filter out the main term which is the residues. Besides that we get errors and another vertical contour integral denoted by $I(x)$. The third step is flipping this $I(x)$ contour back to half plane $\Re s > 1/2$ by functional equation. We will see that this $I(x)$ is determined by some weight function $W(y)$. The next stage is to estimate $W(y)$ in which we will use the stationary phase lemma. The last step is to optimize all errors.

Let x be half of odd integer. By Perron's formula from Titchmarsh [Tit07, page 60, Lemma 3.12], we have

$$\sum_{n\leq x} r_K(n) = \frac{1}{2\pi i}\int_{c-iT}^{c+iT} \zeta_K(s)\frac{x^s}{s}\,ds + O\Big\{\frac{x^c}{T(c-1)}\Big\} + O\Big\{\frac{(2x)^\varepsilon x\log x}{T}\Big\} + O\Big\{\frac{N^\varepsilon x}{T|x-N|}\Big\},$$

where $c = 1+\frac{1}{\log x}$ and N is the nearest integer $\leq x$, $|x-N| = 1/2$. Since for large x, $\frac{1}{\log x}$ and $\frac{\log\log x}{\log x}$ are $\ll \varepsilon$ for any $\varepsilon > 0$. For our convenience we just call $c = 1+\varepsilon$. Hence we have $\log x \ll x^\varepsilon$ and $x^{\frac{1}{\log x}} \ll x^\varepsilon$. Now the first error term is $\ll x^{1+2\varepsilon}/T$. Similarly, second term is $\ll x^{1+2\varepsilon}/T$. The third term is $\ll x^{1+\varepsilon}/T$. We combine them and obtain

$$\sum_{n\leq x} r_K(n) = \frac{1}{2\pi i}\int_{c-iT}^{c+iT} \zeta_K(s)\frac{x^s}{s}\,ds + O\Big(\frac{x^{1+2\varepsilon}}{T}\Big) \tag{5.6}$$

for any $1 \leq T \leq x$.

Next we are going to use residue theorem. Let us consider this contour integration

$$\frac{1}{2\pi i}\Big\{\int_{c-iT}^{c+iT}+\int_{c+iT}^{1-c+iT}+\int_{1-c+iT}^{1-c-iT}+\int_{1-c-iT}^{c-iT}\Big\}\zeta_K(s)\frac{x^s}{s}\,ds$$
$$=\operatorname*{Res}_{s=1}\left(\zeta_K(s)\frac{x^s}{s}\right)+\operatorname*{Res}_{s=0}\left(\zeta_K(s)\frac{x^s}{s}\right)$$

Since the only pole of $\zeta_K(s)$ is $s=1$, and it is a simple pole. Thus $\zeta_K(s)x^s/s$ holds a simple pole at $s=0$ and a simple pole at $s=1$. The residues are

$$\begin{aligned}\operatorname*{Res}_{s=0}\Big(\zeta_K(s)x^s/s\Big)&=\zeta_K(0)\\ \operatorname*{Res}_{s=1}\Big(\zeta_K(s)x^s/s\Big)&=x\operatorname*{Res}_{s=1}\Big(\zeta_K(s)\Big).\end{aligned}\tag{5.7}$$

Now we use functional equation (1.7) and (1.6) to estimate $\zeta_K(0)$. In formula (1.7), we set $s=1$ and isolate $\zeta_K(0)$ on left-hand-side, then the other side is $\left(\frac{|D_K|}{\pi^m}\right)^{1/2}$ times a ratio of Γ functions and a simple pole(by $\zeta_K(1)$). The ratio of Γ functions gives a zero of order $r_1+r_2\geq 1$ which cancels the pole. Thus we can see

$$\zeta_K(0)\ll|D_K|^{1/2}\asymp Q^{\frac{m}{2}}.\tag{5.8}$$

For convenience, let us denote the two residues by $R_0(x),R_1(x)$, so we have that

$$\begin{aligned}\sum_{n\leq x}r_K(n)&=R_0(x)+R_1(x)+O\left(\frac{x^{1+2\varepsilon}}{T}\right)\\ &\quad+\left\{\int_{1-c-iT}^{1-c+iT}+\int_{1-c+iT}^{c+iT}+\int_{c-iT}^{1-c-iT}\right\}\zeta_K(s)\frac{x^s}{s}ds.\end{aligned}\tag{5.9}$$

Next we are going to estimate two horizontal contour integrals. Again, we only consider $\int_{1-c-iT}^{c-iT}\zeta_K(s)x^ss^{-1}ds$. Our tool is convexity principle. When $\sigma=1+\varepsilon$, at the right vertex, $\zeta_K(s)$ is analytic so

$$\left|\zeta_K(s)\frac{x^s}{s}\right|\ll\frac{x^{1+\varepsilon}}{T}.$$

At the left vertex ($s = -\varepsilon - iT$), we use functional equation (1.9), (5.4) and get that

$$\Big|\zeta_K(s)\frac{x^s}{s}\Big| \ll \frac{(QT)^{m(\frac{1}{2}+\varepsilon)}}{T}x^{-\varepsilon}.$$

By convexity principle, the absolute value reaches maximum at one of the two vertices. So combining the above two bounds, this horizontal contour integral is bounded as

$$\int_{1-c-iT}^{c-iT}\zeta_K(s)\frac{x^s}{s}\,ds \ll \frac{x^{1+\varepsilon}}{T} + \frac{(QT)^{\frac{m}{2}}}{T}\Big(\frac{(QT)^m}{x}\Big)^{\varepsilon}.$$

Because the lower horizontal contour is conjugate, we can bound it in a similar way. If we put the estimate of the horizontal contour back into (5.9), then it becomes

$$\sum_{n\le x} r_K(n) = R_0(x) + R_1(x) + I(x) + O\Big\{\frac{x^{1+2\varepsilon}}{T} + \frac{(QT)^{\frac{m}{2}}}{T}\Big(\frac{(QT)^m}{x}\Big)^{\varepsilon}\Big\} \tag{5.10}$$

where $I(x)$ is the vertical contour integral

$$I(x) = \frac{1}{2\pi i}\int_{1-c-iT}^{1-c+iT}\zeta_K(s)\frac{x^s}{s}ds.$$

Next we want to simplify this $I(x)$ and estimate it. Since this contour is in left half plane, we need apply functional equation (1.9) to flip it back to right half plane $\Re s > 1/2$. After some variable change, we shift $I(x)$ back to the original place and get that

$$\begin{aligned} I(x) &= \frac{1}{2\pi i}\int_{1-c-iT}^{1-c+iT}\zeta_K(s)\frac{x^s}{s}\,ds \\ &= \frac{1}{2\pi i}\int_{c+iT}^{c-iT}\zeta_K(1-s)\frac{x^{1-s}}{1-s}\,d(1-s) \\ &= \frac{1}{2\pi i}\int_{c-iT}^{c+iT}\hat{\gamma}_K(s)\zeta_K(s)\frac{x^{1-s}}{1-s}\,ds. \end{aligned} \tag{5.11}$$

Since $\zeta_K(s) = \sum_{n=1}^{\infty} r_K(n) n^{-s}$ converges absolutely in half plane $\Re(s) > 1$, if we expand $\zeta_K(n)$ to be the infinite sum, then we can switch the $\int$ and $\sum$. Thus,

$$\begin{aligned} I(x) &= \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \hat{\gamma}_K(s) \left(\sum_{n=1}^{\infty} \frac{r_K(n)}{n^s} \right) \frac{x^{1-s}}{1-s} \, ds \\ &= x \sum_{n=1}^{\infty} r_K(n) \left(\frac{1}{2\pi i} \int_{c-iT}^{c+iT} \frac{\hat{\gamma}_K(s)}{(nx)^s (1-s)} \, ds \right) \\ &= x \sum_{n=1}^{\infty} r_K(n) W(nx) \end{aligned} \tag{5.12}$$

where, if we let $y = nx$,

$$W(y) = \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \frac{\hat{\gamma}_K(s)}{1-s} y^{-s} \, ds. \tag{5.13}$$

By looking at (5.12), we note that the size of the weight function $W(y)$ determines the size of $I(x)$. Thus, next we only focus on this $W(y)$ and we want to bound it effectively by stationary phase lemmas. Let us put the gamma factor formula (5.4) into (5.13). Here we consider the upper vertical line segment, since the lower part can be done by conjugation. Thus, the integration on the upper line segment in (5.13) can bounded as

$$\frac{1}{2\pi i} \int_{c}^{c+iT} \frac{\hat{\gamma}_K(s)}{1-s} y^{-s} \, ds \ll Q^{m(c-\frac{1}{2})} y^{-c} + y^{-c} \int_1^T \frac{(Qt)^{m(c-\frac{1}{2})}}{t} \Big(\frac{Qt}{e y^{\frac{1}{m}}} \Big)^{imt} \, dt. \tag{5.14}$$

The right integral in above formula is an *oscillatory integral* which is in form of $\int g(t) e^{ikf(t)} dt$. For this type of integral, it is natural to use stationary phase lemmas to estimate them. Here in order to do it efficiently, we need know if it has stationary point or not. To solve this problem, we split the ranges of y to be $y > 2(QT)^m$ and $y \leq 2(QT)^m$.

For $y > 2(QT)^m$, the above oscillatory integral has no stationary point in $[1, T]$. Thereafter we apply Titchmarsh [Tit07, page 71, Lemma 4.3] and get that

$$\left| \int_1^T \frac{(Qt)^{m(c-\frac{1}{2})}}{t} \left(\frac{Qt}{e y^{\frac{1}{m}}} \right)^{imt} \, dt \right| \ll \frac{(QT)^{m(c-\frac{1}{2})}}{T}.$$

Then we put above bound into (5.14). The integral on the lower line segment has the same bound. Thus for $y > 2(QT)^m$, the bound of $W(y)$ is obtained as

$$W(y) \ll y^{-c}T^{-1}(QT)^{m(c-\frac{1}{2})}.$$

It follows that the tail of $I(x)$ is

$$\begin{aligned} x \sum_{nx>2(QT)^m} r_K(n)W(nx) &\ll x \sum_{nx>2(QT)^m} n^{\varepsilon}(nx)^{-c}T^{-1}(QT)^{m(c-\frac{1}{2})} \\ &\ll \frac{x^{1-c}(QT)^{m(c-\frac{1}{2})}}{T}\left(\frac{2(QT)^m}{x}\right)^{1+\varepsilon-c} \\ &\ll x^{-\varepsilon}T^{-1}(QT)^{m(\frac{1}{2}+\varepsilon)} \end{aligned} \tag{5.15}$$

If compare this bound with the error terms of Perron's formula in (5.10), we find this tail of $I(x)$ can be absorbed by the errors.

Now it remains the case $y \le 2(QT)^m$ with the finite sum

$$I_0(x) = x \sum_{nx\le 2(QT)^m} r_K(n)W(nx). \tag{5.16}$$

In order to simplify the our rest of calculation, we move the integration in $W(y)$ from line $\Re(s) = c$ to $\Re(s) = \beta = \frac{1}{2} + \frac{1}{m}$. Here we have a powerful stationary lemma (Lemma 5.2). To make it into use, we move the contour to $\Re s = \frac{1}{2} + \frac{1}{m}$ so that it simplifies the test function $(QT)^{m(c-1/2)}t^{-1}$ to be 1 on the line $\Re s = \frac{1}{2} + \frac{1}{m}$. Further, we only move the line segments with $1 \le |t| \le T$ for avoiding the pole $s = 1$.

Now shift $\int_{c+i}^{c+iT}$ to $\int_{\beta+i}^{\beta+iT}$. We need estimate two horizontal segments. Since $s/(1-s)$ is analytic in the rectangle region with vertices $c+i, c+iT, \beta+iT, \beta+i$, it is bounded by

some constant. Then, by convexity principle , in the strip $\beta \le \sigma \le c$, we have

$$\begin{aligned}\frac{\hat{\gamma}_K(s)}{s}y^{-s} &\ll \frac{(Qt)^{m(c-\frac{1}{2})}}{t}y^{-c} + \frac{(Qt)^{m(\beta-\frac{1}{2})}}{t}y^{-\beta} \\ &\ll \frac{(Qt)^{m(c-\frac{1}{2})}}{t}y^{-c}\left(1+\left(\frac{y}{(QT)^m}\right)^{c-\beta}\right) \\ &\le \frac{(Qt)^{m(c-\frac{1}{2})}}{t}y^{-c}\left(1+2^{\frac{1}{2}+\varepsilon-\frac{1}{m}}\right) \\ &\ll \frac{(Qt)^{m(c-\frac{1}{2})}}{ty^c}.\end{aligned}$$

In the upper rectangle region, we can see

$$\frac{\hat{\gamma}_K(s)}{1-s}y^{-s} = \frac{\hat{\gamma}_K(s)}{s}y^{-s}\cdot\frac{s}{1-s} \ll \frac{(Qt)^{m(c-\frac{1}{2})}}{ty^c}.$$

The lower rectangle region is conjugate, hence

$$W(y) = \frac{1}{2\pi i}\fint_{\beta-iT}^{\beta+iT}\frac{\hat{\gamma}_K(s)}{1-s}y^{-s}\,ds + O\left\{\frac{(QT)^{m(c-\frac{1}{2})}}{Ty^c}\right\}, \tag{5.17}$$

where $\fint$ denote the truncated integration with $1 \le |t| \le T$. And this implies $(1-s)^{-1} = it^{-1} + O(t^{-2})$. Now we put the estimate and (5.4) into the integral of upper line segment of (5.17) and deduce that

$$\begin{aligned}\int_{\beta+i}^{\beta+iT}\frac{\hat{\gamma}_K(s)}{(1-s)}y^{-s}\,ds &= \int_1^T \omega Qt\left(\frac{Qt}{e}\right)^{imt}\left(1+O(\frac{1}{t})\right)\times\left(\frac{i}{t}+O(\frac{1}{t^2})\right)y^{-\beta-it}i\,dt \\ &= -\frac{Q\omega}{y^\beta}\int_1^T\left(\frac{Qt}{ey^{\frac{1}{m}}}\right)^{imt}dt + O\left(\frac{Q}{y^\beta}\log T\right).\end{aligned}$$

By reflection principle, we can check that the integral of the lower line segment has the conjugate result. Combine two line segments. Then for $y \le 2(QT)^m$, the weight function $W(y)$ is

$$W(y) = \frac{Q}{\pi y^\beta}\Re\left[i\omega\int_1^T\left(\frac{Qt}{ey^{\frac{1}{m}}}\right)^{imt}dt\right] + O\left(\frac{(QT)^{\frac{m}{2}}}{Ty}\left(\frac{(QT)^m}{x}\right)^{\varepsilon}\right). \tag{5.18}$$

Now we get another oscillatory integral in above formula. This time, the range of the integral contains the stationary point. We cannot use the old lemma. Here let us introduce our main stationary phase lemma.

Lemma 5.2 (Main Lemma)**.** *Let $m > 0$ and $T \geq 1$. For real z with $2 \leq z \leq 2T$,*

$$\int_1^T \left(\frac{t}{ez}\right)^{imt} dt = \sqrt{\frac{2\pi z}{m}} e^{-imz+\frac{\pi i}{4}} + O(1) + E(T,m,z), \tag{5.19}$$

where this $E(T,m,z)$ is

$$E(T,m,z) = O\left(\min\left\{\sqrt{\frac{T}{m}}, \log T \left|m \log \frac{z}{T}\right|^{-1}\right\}\right).$$

And the main term exists only if $z \leq T$.

Since the proof of this lemma is very technical, we put it Chapter 6. For using it clearly, we let $z = Q^{-1}y^{\frac{1}{m}}$. Because of $y \leq 2(QT)^m$, this z has an upper bounded: $z \leq 2T$. Suppose $2 \leq z \leq 2T$, now it satisfies Lemma 5.2.

Using this lemma we see that the integral in (5.18) can be estimated as

$$\begin{aligned} i\omega \int_1^T \left(\frac{tQ}{ey^{\frac{1}{m}}}\right)^{imt} dt &= \omega\sqrt{\frac{2\pi y^{\frac{1}{m}}}{Qm}} \cdot \exp\left\{\frac{3\pi i}{4} - im\frac{y^{\frac{1}{m}}}{Q}\right\} + O\left(\left(\frac{1}{\sqrt{T}} + \frac{|\log \frac{z}{T}|}{\log T}\right)^{-1}\right) \\ &= \omega\Big(\frac{2\pi}{Qm}\Big)^{\frac{1}{2}} y^{\frac{1}{2m}} \exp\Big\{i\Big(\frac{3\pi}{4} - \frac{my^{\frac{1}{m}}}{Q}\Big)\Big\} + O\left(\Big(\frac{1}{\sqrt{T}} + \frac{|\log \frac{z}{T}|}{\log T}\Big)^{-1}\right). \end{aligned}$$

Because $2 \leq z$ and $y \leq 2(QT)^m$, we have $(2Q)^m \leq y \leq 2(QT)^m$. We put the above result back in $W(y)$ by (5.18). In the range $(2Q)^m \leq y \leq 2(QT)^m$, the weight function is

$$\begin{aligned} W(y) = &\Big(\frac{2Q}{\pi m}\Big)^{\frac{1}{2}} y^{-\frac{m+1}{2m}} \Re(\omega e^{i(\frac{3\pi}{4} - \frac{m}{Q}y^{\frac{1}{m}})}) \\ &+ O\left(\frac{Q\log T}{y^\beta}\Big(\frac{1}{\sqrt{T}} + \Big|\log\frac{(QT)^m}{y}\Big|\Big)^{-1} + \frac{(QT)^{\frac{m}{2}}}{Ty}\Big(\frac{(QT)^m}{x}\Big)^{\varepsilon}\right). \end{aligned} \tag{5.20}$$

Furthermore, if $0 < z < 2$, the main term in (5.19) is bounded and the error term $\ll (\log T)^{-1}$. It follows that the integral (5.19) is bounded. Equivalently the integral in (5.18) is bounded if $0 < y < (2Q)^m$. Thus, in range $0 < y < (2Q)^m$, we obtain

$$W(y) \ll \frac{Q}{y^\beta} + \frac{(QT)^{\frac{m}{2}}}{Ty}\Big(\frac{(QT)^m}{x}\Big)^\varepsilon.$$

In this range $W(y)$ is dominated by $(yT)^{-1}(QT)^{\frac{m}{2}}$. Hence we can say (5.20) is true for all y with $0 < y \leq 2(QT)^m$. Now by (5.20), our finite sum (5.16) becomes

$$I_0(x) = \Big(\frac{2Q}{\pi m}\Big)^{\frac{1}{2}} x^{\frac{m-1}{2m}} B_0(x,T) + O\Big\{\mathcal{E}Qx^{1+\varepsilon} + T^{-1}(QT)^{\frac{m}{2}}\Big(\frac{(QT)^m}{x}\Big)^{2\varepsilon}\Big\} \tag{5.21}$$

where $\mathcal{E}$ is an error term

$$\mathcal{E} = \sum_{n\leq 2N} (nx)^{-\beta}\Big(\frac{1}{\sqrt{T}} + \Big|\log\frac{N}{n}\Big|\Big)^{-1},$$

and

$$B_0(x,T) = \sum_{nx\leq (QT)^m} r_K(n) n^{-\frac{m+1}{2m}} \Re\Big(\omega e^{\frac{3\pi i}{4} - \frac{im}{Q}(nx)^{\frac{1}{m}}}\Big).$$

Because (5.19) has stationary point if $z \leq T$, which guarantees the existence of main term. This inequality implies $nx \leq (QT)^m$. We also set $N = \frac{(QT)^m}{x}$. Here we assume $N \leq x$, which gives a good connection between x, T, Q. Now we can substitute N for $(QT)^m x^{-1}$ in above formulas. Last work is to estimate the error term $\mathcal{E}$. If we denote $\sqrt{T}$ by M, by

Euler-Maclaurin Summation, we deduce that

$$\begin{aligned}\mathcal{E} &= \int_1^{2N} (ux)^{-\beta}\Big(\frac{1}{M} + \Big|\log\frac{u}{N}\Big|\Big)^{-1} du \\ &\quad + O\Big\{(2Nx)^{-\beta}\Big(\frac{1}{M}+\log 2\Big)^{-1} - x^{-\beta}\Big(\frac{1}{M}+\log N\Big)^{-1}\Big\} \\ &\ll \int_1^{2N} (ux)^{-\beta}\Big(\frac{1}{M} + \Big|\log\frac{u}{N}\Big|\Big)^{-1} du + (Nx)^{-\beta}M \\ &= x^{-\beta}N^{1-\beta}\int_{\frac{1}{N}}^{2} u^{-\beta}\Big(\frac{1}{M}+|\log u|\Big)^{-1} du + (Nx)^{-\beta}M.\end{aligned}$$

To bound the last integral in above formula, we truncate it be integrals $\int_{\frac{1}{N}}^{1-\delta}$,$\int_{1+\delta}^{2}$ and $\int_{1-\delta}^{1+\delta}$, where δ is a positive small number. We bound them separately.

(i) Since $|\log u| \asymp \delta$ when $1-\delta \le u \le 1+\delta$, we have

$$\int_{1-\delta}^{1+\delta} u^{-\beta}\Big(\frac{1}{M}+|\log u|\Big)^{-1} du \ll \int_{1-\delta}^{1+\delta} (1+\delta)^{-\beta}\Big(\frac{1}{M}+\delta\Big)^{-1} du \ll 2\delta M.$$

If this $\delta \le 1/2M$, then the middle piece is $O(1)$.

(ii) When $1+\frac{1}{2M} \le u \le 2$, $\min\{M, (\log u)^{-1}\} = (\log u)^{-1}$. Hence,

$$\begin{aligned}\int_{1+\delta}^{2} u^{-\beta}\Big(\frac{1}{M}+|\log u|\Big)^{-1} du = \int_{1+\delta}^{2}\frac{u^{-\beta}}{\log u}du &= \int_{1+\delta}^{2} u^{1-\beta}\Big(\frac{du}{u\log u}\Big) \\ &\le 2\int_{1+\delta}^{2}\frac{du}{u\log u} \ll \log\log(1+\frac{1}{2M}) \\ &\ll \log(2M).\end{aligned}$$

(iii) Similarly, $\min\{M, (\log u)^{-1}\} = (\log u)^{-1}$, if $\frac{1}{N} \le u \le 1 - \frac{1}{2M}$. And we pick a constant $\frac{1}{N} < C < 1 - \delta$, and get

$$\begin{aligned}\int_{\frac{1}{N}}^{1-\delta} u^{-\beta}\Big(\frac{1}{M} + |\log u|\Big)^{-1} du &= \int_{\frac{1}{N}}^{C} \frac{u^{-\beta}}{\log u} du + \int_{C}^{1-\delta} \frac{u^{-\beta}}{\log u} du \\ &\ll \log(2M) + \int_{\frac{1}{N}}^{C} u^{-\beta} du \\ &\ll \log(2M) + N^{\beta-1} \\ &\ll \log(2M).\end{aligned}$$

Therefore we have

$$\mathcal{E} \ll (Nx)^{-\beta}(M + N\log(2M)). \tag{5.22}$$

It follows that the first error term in (5.21) can be bounded as

$$x^{1+\varepsilon} Q\mathcal{E} \ll x^{1+\varepsilon} Q\sqrt{T}(QT)^{-\beta m} + Q(QT)^{(1-\beta)m}\log x. \tag{5.23}$$

Finally, put it into the finite sum (5.21) and combine it with (5.10) and (5.15). The summation formula becomes

$$\sum_{n\le x} r_K(n) = R_0(x) + R_1(x) + \Big(\frac{2Q}{\pi m}\Big)^{\frac{1}{2}} x^{\frac{m-1}{2m}} B_0(x,T) + O\Big\{(x + (QT)^{\frac{m}{2}})\frac{x^{2\varepsilon}}{T}\Big\}.$$

Since we let $N = (QT)^m x^{-1}$. $T = (Nx)^{\frac{1}{m}} Q^{-1}$, $Q = |D_K|^{\frac{1}{m}}(2\pi)^{-1}$, and the residue $R_0(x)$ can be absorbed by the errors. We rewrite it as

$$\begin{aligned}\sum_{n\le x} r_K(n) &= R_1(x) + \left(\frac{2|D_K|^{\frac{1}{m}}}{2\pi^2 m}\right)^{\frac{1}{2}} x^{\frac{m-1}{2m}} B_0(x,T) + O\left\{(x + (Nx)^{\frac{1}{2}}\frac{x^{2\varepsilon}Q}{(Nx)^{\frac{1}{m}}}\right\} \\ &= R_1(x) + |D_K|^{\frac{1}{2m}}\pi^{-1} m^{-\frac{1}{2}} x^{\frac{m-1}{2m}} B_0(x,T) + O\left\{x^{1-\frac{1}{m}+2\varepsilon}|D_K|^{\frac{1}{m}} N^{-\frac{1}{m}}\right\}.\end{aligned}$$

And the $B_0(x,T)$ becomes

$$\begin{aligned} B_0(x,T) &= \sum_{n\leq N} r_K(n) n^{-\frac{m+1}{2m}} \Re\left(\exp\left\{-\frac{r_1\pi i}{4}+\frac{3\pi i}{4}-2\pi i m\left(\frac{nx}{|D_K|}\right)^{\frac{1}{m}}\right\}\right) \\ &= \sum_{n\leq N} r_K(n) n^{-\frac{m+1}{2m}} \cos\left(2\pi m\left(\frac{nx}{|D_K|}\right)^{\frac{1}{m}}+\frac{(r_1-3)\pi}{4}\right). \end{aligned}$$

This completes our proof. □

6 TECHNICAL LEMMAS

6.1 Main Lemma

In this chapter our main work is to prove the main lemma we used in Chapter 5.

Lemma 5.2 (Main Lemma)**.** *Let $m > 0$ and $T \geq 1$. For real z with $2 \leq z \leq 2T$,*

$$\int_1^T \left(\frac{t}{ez}\right)^{imt} dt = \sqrt{\frac{2\pi z}{m}} e^{-imz+\frac{\pi i}{4}} + O(1) + E(T, m, z), \tag{5.19}$$

where this $E(T, m, z)$ is

$$E(T, m, z) = O\left(\min\left\{\sqrt{\frac{T}{m}}, \log T \left|m \log \frac{z}{T}\right|^{-1}\right\}\right).$$

And the main term exists only if $z \leq T$.

Throughout this chapter, we also write

$$\left(\frac{t}{ez}\right)^{imt} = e^{iF(t)},$$

where

$$F(t) = mt(\log t - \log z - 1). \tag{6.1}$$

The derivatives $F'(t)$ and $F''(t)$ are

$$\begin{aligned} F'(t) &= m \log \frac{t}{z}, \\ F''(t) &= \frac{m}{t}. \end{aligned} \tag{6.2}$$

Note that $F'(t) = 0$ if and only if $t = z$, which basically gives the integral $\int e^{iF(t)}dt$ a main value. This z is called the *stationary point*.

Since the proof of Lemma 5.2 is technical, before we proving it, let us show the sketch. The proof of Lemma 5.2 has three parts. First we will introduce some basic tools. Then we will use them to get a stationary phase lemma in dyadic form. Last step is to generalize the dyadic form to the main lemma we want. Let us look at some basic lemmas.

6.2 Some Basic Lemmas

In this section, we introduce three lemmas that will be used in proving our main lemma. Two of them are from Titchmarsh [Tit07, Chapter 4]. They are used for estimating the integral without stationary point. Below are the two lemmas.

Lemma 6.1. *Let $F(x)$ be a real differentiable function such that $F'(x)$ is monotonic, and $F'(x) \geq M > 0$, or $F'(x) \leq -M < 0$, throughout the interval $[a, b]$. Then*

$$\Big| \int_a^b e^{iF(x)}dx \Big| \leq \frac{4}{M}. \tag{6.3}$$

Lemma 6.2. *Let $F(x)$ be a real function, twice differentiable, and let $F''(x) \geq r > 0$, or $F''(x) \leq -r < 0$, throughout the interval $[a, b]$. Then*

$$\Big| \int_a^b e^{iF(x)}dx \Big| \leq \frac{8}{\sqrt{r}}. \tag{6.4}$$

The proofs of these two lemmas are very short and they can be found in [Tit07].

In addition to the above lemmas, we need one essential lemma to estimate the integral that has a stationary point. The following lemma [Gon84, Lemma 1] is what we need.

Lemma 6.3. *Let $m > 0$, and real $z \geq 2$. There exist a small $\delta > 0$ such that*

$$I_0 = \int_{z(1-\delta)}^{z(1+\delta)} \Big(\frac{t}{ez}\Big)^{imt} dt = \sqrt{\frac{2\pi z}{m}} e^{-imz+\pi i/4} + O(1). \tag{6.5}$$

Remark: This small positive δ can not be arbitrarily small. Later in the proof we will show that naturally we choose δ to be $\sqrt{(\log z)/z} < 0.6$ for $z \geq 2$.

Proof. First make a variable change $t = z(1+x)$. Then the integral becomes

$$I_0 = ze^{-imz} \int_{-\delta}^{\delta} \exp\left\{imz\left[(x+1)\log(x+1) - x\right]\right\} dx. \tag{6.6}$$

Consider the complex function $(s+1)\log(s+1) - s$. At $s = 0$ it has power series expansion

$$(s+1)\log(s+1) - s = \frac{s^2}{2} - \frac{s^3}{6} + \frac{s^4}{12} \cdots,$$

which shows it is analytic at zero. If we set $u(s) = \sqrt{2((s+1)\log(s+1) - s)}$, then near $s = 0$, we have

$$\begin{aligned} u(s) &= s + O(s^2), \\ u'(s) &= 1 + O(s), \\ \frac{1}{u'(s)} &= 1 + O(s). \end{aligned} \tag{6.7}$$

Now, we plug them into (6.6) and let u denote $u(s)$. The original integral becomes

$$\begin{aligned} I_0 &= ze^{-imz} \int_{u(-\delta)}^{u(\delta)} e^{imz\cdot\frac{1}{2}u(s)^2} \frac{1}{u'(s)} d(u(s)) \\ &= ze^{-imz} \int_{u(-\delta)}^{u(\delta)} e^{imzu^2/2} du + O\left(z \int_{u(-\delta)}^{u(\delta)} \frac{1}{imz} e^{imzu^2/2}\, d(imzu^2/2)\right) \\ &= ze^{-imz} \int_{u(-\delta)}^{u(\delta)} e^{imzu^2/2} du + O(1). \end{aligned} \tag{6.8}$$

Moreover, let $u = e^{\frac{\pi i}{4}}\sqrt{\frac{2}{mz}}v$, and use the method of Fresnel integral. The integral in above formula can be convert to be a Gaussian integral:

$$\int_{u(-\delta)}^{u(\delta)} e^{imzu^2/2}\, du = \sqrt{\frac{2}{mz}} e^{\pi i/4} \int_{-\infty}^{\infty} e^{-v^2} dv + O\left(\int_{\sqrt{z}u(\delta)}^{\infty} e^{-v^2} dv\right). \tag{6.9}$$

To estimate the above error term, we use integration by parts. Recall $u(\delta) = O(\delta)$. Hence we have

$$\int_{\sqrt{z}u(\delta)}^{\infty} e^{-v^2} dv = \frac{e^{-zu^2(\delta)}}{2\sqrt{z}u(\delta)} - \frac{1}{2}\int_{\sqrt{z}u(\delta)}^{\infty} \frac{e^{-v^2}}{v^2} dv = O\left(\frac{e^{-z\delta^2}}{\sqrt{z}\delta}\right).$$

Finally combining (6.9) and (6.8), we get error $O(\sqrt{z}\delta^{-1}e^{-z\delta^2})$. While we optimizing it with $O(1)$, it shows that δ can not be arbitrarily small; precisely, $1 > \delta \gg \sqrt{(\log z)/z}$. Thus, we can choose $\delta = \sqrt{(\log z)/z} < 0.6$ for $z \geq 2$. This completes the proof. □

6.3 Main Lemma in Dyadic Form

Now we've got all basic lemmas we need. In this section, we are able to prove the following lemma which can be seen as a dyadic version of Lemma 5.2. And it is also a variation of Gonek's [Gon84, Lemma 2].

Lemma 6.4. *For $A > 8$, $k \in \mathbb{N}$ and $A < z \leq 2^k A(1 - \frac{1}{\sqrt{2^k A}})^{-1}$,*

$$\int_A^{2^k A} e^{iF(t)} dt = \sqrt{\frac{2\pi z}{m}} e^{-imz + \pi i/4} + O(1) + E(A, z, k, m), \tag{6.10}$$

where

$$E(A, z, k, m) = O\left(\min\left\{\sqrt{\frac{2^k A}{m}}, k\left|m \log \frac{z}{2^k A}\right|^{-1}\right\}\right) \tag{6.11}$$

Remark: This lemma is still true if $A < z < 2^k A$, however the error would be $\sqrt{\frac{2^k A}{m}}$, because the logarithm is bigger for z near $2^k A$.

Proof. First of all, we truncate the original integral to be

$$\int_A^{2^k A} e^{iF(t)} dt = \left\{\int_A^{z(1-\delta)} + \int_{z(1-\delta)}^{z(1+\delta)} + \int_{z(1+\delta)}^{2^k A}\right\} e^{iF(t)} dt \tag{6.12}$$

where this $\delta = \sqrt{(\log 8)/8} < 1$. Since $z \geq A > 8$, it is easy to check that this $\delta \geq \sqrt{(\log z)/z}$. Our strategy of this proof is basically estimating the above three integrals in (6.12). We notice

that the middle integral satisfies Lemma 6.3. Hence we have

$$\int_{z(1-\delta)}^{z(1+\delta)} e^{iF(t)}\,dt = \sqrt{\frac{2\pi z}{m}} e^{-imz+\pi i/4} + O(1).$$

Next because the rest two integrals have no stationary point, we are going to use Lemma 6.1 and Lemma 6.2 to estimate them. Since $t \le 2^k A$ and $|F''(t)| \ge \frac{m}{2^k A}$, by Lemma 6.2, we have

$$\int_{A}^{z(1-\delta)} e^{iF(t)}dt \ll \sqrt{\frac{2^k A}{m}} \quad , \qquad \int_{z(1+\delta)}^{2^k A} e^{iF(t)}dt \ll \sqrt{\frac{2^k A}{m}}. \tag{6.13}$$

Furthermore, since for $z \in (\frac{3}{2}A, \frac{2}{3}2^k A)$,

$$|F'(t)| = \left| m \log \frac{t}{z} \right| \ge m \left| \log \left(\frac{z(1-\delta)}{z} \right) \right| = m|\log(1-\delta)| > 0.$$

By Lemma 6.1, we obtain

$$\int_{A}^{z(1-\delta)} e^{iF(t)}dt \ll m^{-1}|\log(1-\delta)|^{-1}.$$

Now we claim, this $|m\log(1-\delta)|^{-1} \ll k|m\log\frac{z}{2^k A}|^{-1}$. Consider the ratio:

$$\frac{|m\log(1-\delta)|^{-1}}{k|m\log\frac{z}{2^k A}|^{-1}} = \frac{1}{k}\left|\frac{\log\frac{z}{2^k A}}{\log(1-\delta)}\right| \ll \frac{1}{k}\frac{k\log 2}{\delta} \ll 1.$$

Thus, we combine it with (6.13), and the $\int_A^{z(1-\delta)} e^{iF(t)}dt$ has two bounds. Specifically, it is

$$\int_{A}^{z(1-\delta)} e^{iF(t)}dt \ll \min\left\{ k\left|m\log\frac{z}{2^k A}\right|^{-1}, \sqrt{\frac{2^k A}{m}} \right\}.$$

Note that $z(1-\delta)$ may be less than A. In this case, we over estimate $\int_{z(1-\delta)}^{A} e^{iF(t)}dt$. However, this error can be absorbed because, by Lemma 6.1,

$$\int_{z(1-\delta)}^{A} e^{iF(t)}dt \ll \left|m\log\frac{z}{A}\right|^{-1} = \left|\frac{m\log\frac{z}{2^kA}}{km\log\frac{z}{A}}\right| \cdot k\left|m\log\frac{z}{2^kA}\right|^{-1} \ll k\left|m\log\frac{z}{2^kA}\right|^{-1}.$$

Symmetrically, we use the same way to estimate $\int_{z(1+\delta)}^{2^kA} e^{iF(t)}dt$. Assume $z(1+\delta) \leq 2^kA$. Then by Lemma 6.1, we have $\int_{z(1+\delta)}^{2^kA} e^{iF(t)}dt \ll |m\log(1+\delta)|^{-1}$. We claim it is $O(k|m\log\frac{z}{2^kA}|^{-1})$. Using a similar ratio we have

$$\frac{|m\log(1+\delta)|^{-1}}{k|m\log\frac{z}{2^kA}|^{-1}} = \frac{1}{k}\left|\frac{\log\frac{z}{2^kA}}{\log(1+\delta)}\right| \ll \frac{1}{k}\frac{k\log 2}{\delta} \ll 1.$$

It follows that

$$\int_{z(1+\delta)}^{2^kA} e^{iF(t)}dt \ll \min\left\{k\left|m\log\frac{z}{2^kA}\right|^{-1}, \sqrt{\frac{2^kA}{m}}\right\}.$$

Similarly, we may also have $z(1+\delta) > 2^kA$, then integral we over estimated is $\int_{2^kA}^{z(1+\delta)} e^{iF(t)}dt$. In this range $(2^kA, z(1+\delta))$, the lower bound of $|F'(t)|$ is $|m\log\frac{z}{2^kA}|$. By Lemma 6.1,

$$\int_{2^kA}^{z(1+\delta)} e^{iF(t)}dt \ll \left|m\log\frac{z}{2^kA}\right|^{-1} \leq k\left|m\log\frac{z}{2^kA}\right|^{-1}.$$

Thus, it can be absorbed by the error. This completes the proof.

□

6.4 Proof of Lemma 5.2

Now we prove Lemma 5.2.

Proof of Lemma 5.2. In this proof we need discuss the situation for z in various ranges. In total, there are four cases.

Case I: If we have $T(1-\frac{1}{\sqrt{mT}})^{-1} \leq z \leq 2T$. The stationary point is not in $[1,T]$ which implies that $\int_1^T e^{iF(t)}dt$ has no main term. Now our goal is to use Lemma 6.1 and

Lemma 6.2. For $1 \le t \le T$ we have

$$\begin{aligned} |F'(t)| &\ge m \log \frac{z}{T}, \\ |F''(t)| &\ge \frac{m}{T}. \end{aligned} \tag{6.14}$$

By Lemma 6.1 and Lemma 6.2 we have

$$\int_1^T e^{iF(t)}\, dt \le \min\left\{ \frac{4}{m|\log \frac{z}{T}|}, \frac{8\sqrt{T}}{\sqrt{m}} \right\} \ll \min\left\{ \frac{1}{m|\log \frac{z}{T}|}, \sqrt{\frac{T}{m}} \right\}.$$

Case II: If we have $T(1+\frac{1}{\sqrt{mT}})^{-1} < z \le T(1-\frac{1}{\sqrt{mT}})^{-1}$. We can check that in this range

$$\sqrt{\frac{T}{m}} \le \left| m \log \frac{T}{z} \right|^{-1},$$

which means the minimum of $\sqrt{T/m}$ and $|m \log \frac{T}{z}|^{-1}$ is $\sqrt{T/m}$. Thus, in this case we only need bound the integral in terms of $\sqrt{T/m}$. Here we have two sub-cases:

(i) If $z > T$, there is no main term. By $|F''(t)| \ge m/T$ and Lemma 6.2, we have

$$\int_1^T e^{iF(t)}\, dt \ll \sqrt{\frac{T}{m}}.$$

(ii) If $z \le T$, pick small $\delta = 1/2$. Here we assume $T > 16$ otherwise the whole integral is trivially bounded by 16. Then this $\delta > \sqrt{(\log z)/z}$, for $T(1+\frac{1}{\sqrt{mT}})^{-1} \le z$. Hence it satisfies condition of Lemma 6.3. It follows that

$$\int_{z(1-1/2)}^{z(1+1/2)} e^{iF(t)}\, dt = \sqrt{\frac{2\pi z}{m}} e^{imz - \pi i/4} + O(1).$$

And since $|F''(t)| \ge m/T$, by Lemma 6.2, we have

$$\int_1^{z(1-1/2)} e^{iF(t)}\, dt \ll \sqrt{\frac{T}{m}}.$$

Actually we over estimated the piece $\int_T^{z(1+1/2)} e^{iF(t)}dt$. Now we bound it. For t in range $(T, 3T/2)$, the second derivative $|F''(t)| > 2m/3T > 0$. Apply Lemma 6.2 we know the error is bounded as

$$\left| \int_T^{z(1+1/2)} e^{iF(t)}\, dt \right| \leq 8\sqrt{\frac{3T}{2m}} \ll \sqrt{\frac{T}{m}}.$$

This completes case II.

Next we split the original interval to be dyadic segments $[\frac{T}{2^j}, \frac{T}{2^{j-1}}]$. Then the original integral can written as

$$\int_1^T e^{iF(t)}\, dt = \Big\{ \int_1^{T/2^k} + \sum_{j=1}^{k} \int_{T/2^j}^{T/2^{j-1}} \Big\} e^{iF(t)}\, dt \tag{6.15}$$

where k is the smallest integer such that $T/2^k < 16$. So $T/2^k > 8$, otherwise k is not smallest. Here we can assume $T \geq 24$, because if $T < 24$ all the error term are $O(1)$. Hence, we have $T \geq 24$ and $1 \leq k = \lfloor \frac{\log T}{\log 2} \rfloor - 3$.

Case III: In this case z is in range $2 \leq z \leq (3/2)\frac{T}{2^k}$. Because initially we set $8 < T/2^k < 16$, then $(3/2)\frac{T}{2^k} < 24$. Let $\delta = \sqrt{(\log 2)/2}$. We truncate the original integral to be

$$\int_1^T e^{iF(t)}dt = \left\{ \int_1^{z(1-\delta)} + \int_{z(1-\delta)}^{z(1+\delta)} + \int_{z(1+\delta)}^{24} + \int_{24}^{T} \right\} e^{iF(t)}dt. \tag{6.16}$$

First and easiest integral we can estimate is $\int_{z(1-\delta)}^{z(1+\delta)} e^{iF(t)}dt$. By Lemma 6.3,

$$\int_{z(1-\delta)}^{z(1+\delta)} e^{iF(t)}\, dt = \sqrt{\frac{2\pi z}{m}} e^{-imz+\pi i/4} + O(1). \tag{6.17}$$

And next for the first and third integral in (6.16), we get inequality

$$\left| \left\{ \int_1^{z(1-\delta)} + \int_{z(1+\delta)}^{24} \right\} e^{iF(t)}dt \right| \leq \int_1^{24} 1\, dt \leq 24 = O(1). \tag{6.18}$$

Moreover, for $24 \le t \le T$, the first and second derivative of $F(t)$ have bound

$$|F'(t)| \ge |m \log \frac{24}{z}| > 0$$
$$|F''(t)| \ge m/T > 0.$$

Hence, by Lemma 6.1 and 6.2, the fourth integral in (6.16) can be estimated as

$$\int_{24}^{T} e^{iF(t)}\, dt \ll \min\left\{\sqrt{\frac{T}{m}}, |m \log z|^{-1}\right\}.$$

If we write $z = T^{\alpha}$, this exponent satisfies $\frac{\log 2}{\log T} \le \alpha < \frac{\log 24}{\log T} < 1$. It implies the below inequality

$$\begin{aligned}\left||m \log z|^{-1} - |m \log \frac{T}{z}|^{-1}\right| &= \left|\frac{|m \log \frac{T}{z}| - |m \log z|}{|m \log z| \cdot |m \log \frac{T}{z}|}\right| = \frac{|(1-\alpha) - \alpha|}{m\alpha(1-\alpha)\log T} \\ &\le \frac{|1-2\alpha|}{m \log 2(1-\alpha)} = O(1).\end{aligned}$$

Thus it follows that the fourth integral has bound

$$\int_{24}^{T} e^{iF(t)}\, dt = O\left(\min\left\{\sqrt{\frac{T}{m}}, \left|m \log \frac{z}{T}\right|^{-1}\right\}\right) + O(1) \tag{6.19}$$

Therefore case III follows from (6.17), (6.18) and (6.19).

Case IV: In this case, our stationary point z is in range $(3/2)T/2^k < z < T(1 - \frac{1}{\sqrt{mT}})$. Now we let $A = \frac{T}{2^k}$, which gives us $8 < A < z < 2^k A$. It is exactly what we stated in Lemma 6.4. Thus we apply Lemma 6.4 and obtain

$$\int_{\frac{T}{2^k}}^{T} e^{iF(t)}\, dt = \sqrt{\frac{2\pi z}{m}} e^{-imz + \pi/4} + O(1) + E(T, z, m, k), \tag{6.20}$$

where

$$E(T, z, m, k) = O\left(\min\left\{\sqrt{\frac{T}{m}}, k\left|m \log \frac{z}{T}\right|^{-1}\right\}\right). \tag{6.21}$$

Recall that initially we set k to be $k = \lfloor \frac{\log T}{\log 2} \rfloor - 3$. By this expression, we can see k increase as T tends to infinite and $k \ll \log T$. Plug it into above error term (6.21) and we have

$$E(T, m, z) = O\left(\min\left\{ \sqrt{\frac{T}{m}}, \log T \left| m \log \frac{z}{T} \right|^{-1} \right\} \right).$$

It completes the case IV. And therefore the main lemma (Lemma 5.2) follows. □

BIBLIOGRAPHY

[BHM07] Valentin Blomer, Gergely Harcos, and Philippe Michel. Bounds for modular L-functions in the level aspect. *Ann. Sci. École Norm. Sup. (4)*, 40(5):697–740, 2007.

[Bra47] Richard Brauer. On the zeta-functions of algebraic number fields. *Amer. J. Math.*, 69:243–250, 1947.

[Bur63] D. A. Burgess. On character sums and L-series. II. *Proc. London Math. Soc. (3)*, 13:524–536, 1963.

[BW08] Manjul Bhargava and Melanie Matchett Wood. The density of discriminants of S_3-sextic number fields. *Proc. Amer. Math. Soc.*, 136(5):1581–1587, 2008.

[CF10] John William Scott Cassels and Albrecht Fröhlich, editors. *Algebraic Number Thoery*. London Mathematical Society, 2,revised edition, 2010.

[Dav00] Harold Davenport. *Multiplicative Number Theory*. Springer-Verlag New York, Inc., third edition revised by h.l. montgomery edition, 2000.

[DFI02] W. Duke, J. B. Friedlander, and H. Iwaniec. The subconvexity problem for Artin L-functions. *Invent. Math.*, 149(3):489–577, 2002.

[ELMV11] Manfred Einsiedler, Elon Lindenstrauss, Philippe Michel, and Akshay Venkatesh. Distribution of periodic torus orbits and Duke's theorem for cubic fields. *Ann. of Math. (2)*, 173(2):815–885, 2011.

[FI05] John B. Friedlander and Henryk Iwaniec. Summation formulae for coefficients of L-functions. *Canad. J. Math.*, 57(3):494–505, 2005.

[FT93] Albrecht Fröhlich and Martin J. Taylor. *Algebraic Number Theory*. Cambridge University Press, 1993.

[Gon84] S. M. Gonek. Mean values of the Riemann zeta function and its derivatives. *Invent. Math.*, 75(1):123–141, 1984.

[IR90] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer-Verlag New York, Inc., 1990.

[Lan99] Serge Lang. *Complex Analysis*. Springer-Verlag New York, Inc., 1999.

[Mar77] Daniel A. Marcus. *Number Field*. Springer-Verlag New York, Inc., 1977.

[MV11] Hugh L. Montgomery and Robert C. Vaughan. *Multiplicative Number Theory I. Classical Theory*. Cambrider University Press, 2011.

[Pin77] J. Pintz. Elementary methods in the theory of L-functions. VI. On the least prime quadratic residue (mod ρ). *Acta Arith.*, 32(2):173–178, 1977.

[PK01] R.B. Paris and D. Kaminski. *Asymptotics and Mellin-Barnes Integrals*. Cambridge University Press, 2001.

[Pol14] Paul Pollack. The smallest prime that splits completely in an abelian number field. *Proc. Amer. Math. Soc.*, 142(6):1925–1934, 2014.

[Ten95] Gérald Tenenbaum. *Introduction to Analytic and Probabilistic Number Theory.* Cambridge University Press, 1995.

[Tit07] E.T. Titchmarsh. *The Theory of the Riemann Zeta-function.* Oxford University Press, 2007.

[TT14] Takashi Taniguchi and Frank Thorne. An error estimate for counting S_3-sextic number fields. *Int. J. Number Theory*, 10(4):935–948, 2014.

[VL66] A. I. Vinogradov and Ju. V. Linnik. Hypoelliptic curves and the least prime quadratic residue. *Dokl. Akad. Nauk SSSR*, 168:259–261, 1966.

VITA

The author was born on May 23, 1989 in Suzhou, Jiangsu, China. In 2008, He enrolled at Jilin Normal University in China for his undergraduate studies and he graduated with a B.S. in Mathematics in 2012. He began his graduate studies at University of Mississippi in 2013. Now he is studying in analytic number theory under the direction of Professor Micah B. Milinovich.