A PERSPECTIVE ON COUNTING NUMBER FIELDS WITH VARYING INVARIANTS

A dissertation

submitted by

Matthew D. Friedrichsen

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

in

Mathematics

TUFTS UNIVERSITY

May 2022

Advisor: Professor Robert J. Lemke Oliver

Abstract

In arithmetic statistics, counting number fields is a particularly interesting topic with a long history. Most of the results in the field have focused on counting number fields by discriminant to work towards some long standing conjectures. More recently, there have been results counting by number fields by a different invariant, the conductor. One argument that has been put forth in favor of the conductor is that results obtained by this method might tend to be nicer in a probabilistic sense.

In this thesis, we will present work using both methods. We will present joint work that uses the discriminant to compare counts of D_4 and S_4 quartic number field extensions to show that there is an infinite family of number fields with more D_4 extensions than S_4 extensions. Using the conductor, we will show how some algebraic structure of D_4 can be utilized to realize a secondary term when counting D_4 number fields. We will also generalize this result and use it to count $D_4 \wr H$ extensions by conductor, where H is some transitive subgroup of S_n for some n. With this result, we show that counting number fields by conductor may not always give a "nice" result.

To my lovely wife and our two beautiful sons. The best family to count on.

Acknowledgements

There are many people I need to acknowledge and I fear that I may leave some out accidentally. Absolutely impossible to forget though is my family, and especially my wife, Megan. Five years ago she agreed to move to Boston while still finishing up her graduate degree and had not yet lined up a job. It took a crazy leap of faith to support her husband in going back to school after a six year hiatus. Without her and the two wonderful boys (Elliot and Levi) we had along the way, I would not have stayed sane during graduate school and especially the last two years.

Thank you to my parents, Gary and Susan, for all of your love an support over the years. And thank you for encouraging me to pursue this degree even after I thought it was "too late."

I need to also thank my advisor. His mentoring has been indispensable in my growth as a mathematician. More importantly, he also respects me as a person. I remember one meeting I had with him before he was officially my advisor where I mentioned I was potentially interested in either academic or industry jobs after graduation. He took this in stride and has fully supported any career decisions I've made. I only had to promise that I wouldn't work in finance, a promise that was very easy for me to keep.

Thank you to George McNinch for humoring the questions of a budding number theorist who probably should have known a bit more algebra at times.

Thank you to Anna Haensch for agreeing to be pulled back in to number theory for a little bit to be on my committee, introducing me to her coworkers when I was looking for an internship, and for demonstrating that you can leave the academic field you love and still know that you're doing the right thing.

Thank you to Frank Thorne for taking the time to read and give thoughtful comments on published and submitted works, and for agreeing to write recommendations for me as I was applying to various number theory adjacent programs.

To my advisee twin, Daniel, thank you for listening to my half baked ideas before

I was ready to present them and for reading random number theory papers with me and scheming up ways we might be able to write another paper together. I sincerely hope our first paper together won't be our last!

I must also give a special thank you to Kim Ruane. When I applied to grad school again after working for six years, I received many rejections and much dead air. I emailed Kim one morning to inquire about the status of my application at Tufts. She replied within the hour (perhaps even within the half hour) that my application had somehow gotten lost in the system but she reviewed it and sent it around to others in the department, that they thought I was a strong candidate and should come out for a visit. I am deeply grateful that she took the time (on a weekend no less!) to reply to a random email and give me a chance.

Thank you to Sarah Rich and Noah Barrientos. I really enjoyed getting to work with you both. I hope I was able to make at least a small dent in the amount of work it takes to keep things running smoothly.

Thank you to all of my fellow students for making this grad program what it is. Thank you particularly to my office mates. I'd like to think of our office as the most fun in the department, which, doubtless, had little to do with me. Rest in peace, BP 202. Also, thank you to Daniel's office mates who often had to tolerate my presence and sometimes got asked random math questions as a result.

I also would not be here without the professors who wrote letters for me on many occasions. They are Bruce Hanson, my undergraduate advisor, Jill Dietz, who encouraged me to apply to Tufts specifically, and Joshua Holden, my REU advisor who continued to work with me after undergrad. While I was wondering if I would ever be able to go to graduate school, they never gave up on me.

Contents

List of Tables

A Perspective on Counting Number Fields with Varying Invariants

Chapter 1

Introduction

In the field of number theory lies the alcove of arithmetic statistics. Inside that alcove, there is sizable corner dedicated to counting number fields. An outstanding question in this area is a folklore conjecture (usually attributed to Linnik) we state below.

Conjecture (possibly Linnik) *Let k be a number field, and let $N_{k,n}(X)$ denote the number of degree n extensions L/k with relative discriminant bounded by X. Then,*

$$N_{k,n}(X) \sim c_{k,n}X,$$

where $c_{k,n}$ is a constant that depends both on k and n.

Note that when $k = \mathbb{Q}$, we may drop the k in the subscript.

Starting with $k = \mathbb{Q}$, Davenport and Heilbronn [15] proved the conjecture for $n = 2$ and 3, a combination of Cohen, Diaz y Diaz, and Olivier [12] and Bhargava [2] proved $n = 4$, and Bhargava [3] proved the conjecture for $n = 5$. The case $n = 6$ is not yet solved.

The $n = 4$ case is of particular interest because it demonstrates the relationship between this problem and the Galois group of a specific extension L/k. If L/k is not Galois (as is often the case), we mean the Galois group of the normal closure of L/k regarded as a permutation group on the embeddings of L in $\bar{k}$ for some fixed $\bar{k}$. (You know, what everyone means when they say "Galois group.") For $n = 4$, Cohen, Diaz y Diaz, and Olivier proved the conjecture for D_4 extensions, and Bhargava proved it for S_4 extensions. Together, their work shows that about 83% of quartic number fields have Galois group S_4 and 17% have Galois group D_4. In fact $n = 4$ is the first example where where S_n extensions are not 100% of the degree n number fields! But for $n = 5$, S_n number fields once again make up 100% of degree n number fields.

If we instead look at the Galois group of a random degree n polynomial, Hilbert's Irreducibility Theorem implies that it will cut out an S_n extension 100% of the time. Given this, we might expect S_n extensions to dominate any other possible Galois groups of a degree n number field. In Chapter 2, we present published joint work with Daniel Keliher [18] that shows that when we consider all possible quadratic number fields k, then 100% of those number fields have more D_4 quartic extensions L/k than S_4 ones. More precisely, we show

Theorem (F—Keliher, 2021) *For $\epsilon > 0$ sufficiently small, asymptotically 100% of quadratic number fields F ordered by discriminant (denoted D_F) have*

$$\lim_{X \to \infty} \frac{N_{F,4}(X; D_4)}{N_{F,4}(X; S_4)} \gg_\epsilon (\log |D_F|)^{\log 2 - \epsilon},$$

where $N_{k,n}(X;G)$ represents the number of degree n extensions of k with Galois group G and relative discriminant bounded by X.

Besides the cases already discussed above there are many other interesting results towards proving Linnik's conjecture. One approach has been to tackle the problem head on. To date, the best known results are due to Bhargava, Shankar, and Wang [6] and Lemke Oliver and Thorne [27]. Both of these works establish upper bounds on $N_{k,n}(X)$ that are $\gg_n X$.

The second approach, as we've discussed a bit already, is to count degree n extensions of k with some Galois group G that is a transitive subgroup of S_n. Much of the work in this line has been to towards proving Malle's Conjecture [23]. Malle's conjecture is particularly interesting because it goes further than Linnik's conjecture and gives explicit asymptotics for every finite group G, given knowledge about the permutation representation of the group.

Conjecture (Malle) *Let $G \neq 1$ be a transitive subgroup of S_n and let k be a number field. Then, there exists a constant $c_{k,G} > 0$ such that*

$$N_{k,n}(X;G) \sim c_{k,G} X^{a(G)} (\log X)^{b(k,G)-1},$$

where $a(G)$ and $b(G)$ are explicity defined in terms of properties of k and G.

While there are known counterexamples to Malle's conjecture as it was originally stated, it is still thought to be generally true and there are many results in addition to what we've already cited in relation to Linnik's conjecture [8,15,21,32,36]. Out of these, we take some time to highlight work of Klüners as it provides some motivation for the work presented in Chapter 4. In [21], he generalized the results of Cohen, Diaz y Diaz, and Olivier in some respects and showed that for any number field k transitive subgroup H of S_n such that there are not too many F/k extensions with Galois group H, then 100% of quadratic extensions L/F have $C_2 \wr H$ as their Galois group over k and that there are cX of them when bounded by relative discriminant.

Up until this point I've given the impression that we are only interested in counting number fields by their discriminant. The discriminant is a natural choice of invariant to use for counting as it is defined the same for any number field regardless of its Galois group, but any invariant will do. In [35], Wood discusses using either the conductor of a number field or the product of all ramified primes as alternative invariants to the discriminant. While counting number fields by these different invariants does not directly address either conjecture, they are interesting questions in their own right.

The existence of other possible methods for counting number fields raises a question that is maybe more philosophical than mathematical, but is nonetheless important to consider. Is there one invariant that is "better" than any other for ordering number fields? Wood [34] asks if perhaps the conductor is the better choice by giving an argument based on probabilities. To evaluate this, we will need to define the conductor. We promise that this will happen soon (down below in Section 1.2 if you want to verify our truthfulness).

To illustrate Wood's argument, we will consider the example of counting quadratic extensions over $\mathbb{Q}$. In this case, the discriminant and conductor of any quadratic extension are identical, so we can ignore the distinction. Every quadratic extension of $\mathbb{Q}$ can be written as $\mathbb{Q}(\sqrt{d})$, for some squarefree integer d. Therefore, counting quadratic extensions of $\mathbb{Q}$ can be done by counting squarefree integers. This yields

$$N_2(X) \sim \frac{1}{\zeta(2)}X,$$

where $\zeta(s)$ is the Riemann zeta function.

Now, for any rational prime p and $L/\mathbb{Q}$ quadratic, p either splits, ramifies, or is inert in L. That is, the ideal generated by p in the ring of integers of L factors as $\mathfrak{p}_1\mathfrak{p}_2, \mathfrak{p}^2$, or (p), respectively. For this prime p, you could ask with what probability does p split in a random quadratic number field? To answer this you look at

$$\lim_{X\to\infty} \frac{N_2(X; p \text{ splits})}{N_2(X)}$$

and hope that the limit converges. It does, and the limit is $\frac{p}{2(p+1)}$. We will call this the probability that p splits and denote it as $\mathbb{P}(p \text{ splits})$.

You might next take a finite set of your favorite primes and ask what the probability is that each of the primes does something specific in a random quadratic extension. Perhaps you want 3 to split, 5 to be inert, and 7 to ramify. On top of that you hope that the probabilities of the conditions on the individual primes is independent, or

$$\mathbb{P}(3 \text{ splits}, 5 \text{ is inert}, 7 \text{ ramifies}) = \mathbb{P}(3 \text{ splits})\mathbb{P}(5 \text{ is inert})\mathbb{P}(7 \text{ ramifies}).$$

This also turns out to be true for any finite set S of primes and it is the heart of Wood's line of questioning. For any abelian group G, she showed that counting G-extensions by conductor will yield an Euler product, but counting by discriminant might not. For a non-abelian example, we can turn back to D_4. The result obtained in [12] counting D_4 fields by discriminant turns out not to have a representation as an Euler product as shown in [33]. However, counting D_4 quartic extensions by conductor does yield such a product. This product is now known thanks to the work of Altuğ, Shankar, Varma, and Wilson [1].

Theorem (Altuğ—Shankar—Varma—Wilson, 2021) *Let* $N_4^C(X; D_4)$ *represent* *the number of quartic D_4 number fields over $\mathbb{Q}$ with conductor bounded by X. Then,*

$$N_4^C(X; D_4) \sim \frac{3}{8} \prod_p \left(1 - \frac{1}{p^2} - \frac{2}{p^3} + \frac{2}{p^4}\right) X \log X.$$

We are agnostic as to whether a result with or without an Euler product or independent probabilities makes one counting method better or worse than another. However, this will not prevent us from engaging with the question. Wood has already eloquently stated the case for the conductor, so we will add a brief argument for the discriminant.

For any two distinct transitive subgroups G and G' of S_n, counting by discriminant allows us compare their counts directly as we do with D_4 and S_4. We could, of course, still compare counts of G and G' when using the conductor. However, the results might be misleading. In the case of counting D_4 and S_4 extensions by conductor, the former dominates the latter completely as there are $c_{D_4} X \log X$ many D_4 number fields and $c_{S_4} X$ many S_4 number fields with conductor bounded by X. This is largely an accident as the conductor of an S_4 number field is also its discriminant and the conductor of a D_4 field is smaller than its discriminant by enough to beef up the asymptotic.

Our hope is that the complete thesis will present two different perspectives on the question of counting methods. We start off with the discriminant and use it to compare the counts of D_4 and S_4 extensions in Chapter 2. We then pivot to the conductor for the rest of the thesis. In Chapter 3, we build on [1] and obtain a secondary term and power saving error term when counting D_4 number fields.

Theorem *Let $N_4^C(X; D_4)$ denote the number of quartic D_4 extensions, L, with conductor $C_L \leq X$. Then,*

$$\begin{aligned} N_4^C(X; D_4) =& \frac{3}{8} \cdot \prod_p \left(1 - \frac{1}{p^2} - \frac{2}{p^3} + \frac{2}{p^4}\right) \cdot X \log X \\ &+ \left(\frac{3}{8} \cdot \left(1 - \frac{7 \log 2}{20} - 2 \sum_p \frac{\log p}{p^2 + 2p + 2}\right) \cdot \prod_p \left(1 - \frac{1}{p^2} - \frac{2}{p^3} + \frac{2}{p^4}\right) + c\right) \cdot X \\ &+ O_\epsilon(X^{11/12+\epsilon}) \end{aligned}$$

where c is explicit, but we will leave its definition for Chapter 3.

Lastly, in Chapter 4, we will prove the general case of counting D_4 extensions by conductor over any number field k. For this, we do show that that counting D_4 quartic extensions by conductor yields a nice result in the probabilistic sense. We then use this result to count $D_4 \wr H$ extensions by conductor, where H is the Galois group of some extension F/k and L/F is a quartic D_4 extension. Though we do give some reason to speculate in the $D_4 \wr H$ case that counting extensions by conductor will not always have a product as our result, like Klüners', is given by a sum. But don't take my word for it; see below.

Theorem *Let k be a number field $N^C_{k,4n}(X; D_4 \wr H)$ denote the number of degree $4n$ extensions L/k with Galois group $D_4 \wr H$ and conductor $C_{L/k} \leq X$. Assume that $N_{k,n}(X; H)$ is non-zero and bounded by $O_{k,\epsilon}(X^{1+\epsilon})$. Then,*

$$N^C_{k,4n}(X; D_4 \wr H) \sim X \log X \sum_{\substack{[F:k]=n \\ \mathrm{Gal}(F/k)\cong H}} \frac{3^{r_1}\left(\operatorname*{Res}_{s=1} \zeta_F(s)\right)^2}{2^{2r_1+3r_2+1} D^2_{F/k}} \prod_{\mathfrak{p}\subset \mathcal{O}_F} \left(1 - \frac{1}{\mathrm{N}\mathfrak{p}^2} - \frac{2}{\mathrm{N}\mathfrak{p}^3} + \frac{2}{\mathrm{N}\mathfrak{p}^4}\right),$$

where r_1 and r_2 represent the number of real and complex embeddings of F, respectively.

Before we dive into any of this though, we will establish much of the common notation that will be used throughout this thesis and fulfill our promise about defining the "conductor" of a number field.

1.1 Notation

- k is a number field
- k_v is the localization of k at the place v
- L/k is a finite extension of fields (either global or local)
- $\mathcal{O}_k$ is the ring of integers of a field k (either global or local)

- $I(K)$ is the group of fractional ideals of k
- $\mathrm{Cl}(k)$ is the ideal class group of k
- $\mathrm{Cl}_{\mathfrak{m}}(k)$ is the ray class group of k with modulus $\mathfrak{m}$
- $\mathrm{Cl}(k)[n]$ is the subgroup of n-torsion elements of $\mathrm{Cl}(k)$
- $h_n(k)$ is the cardinality of the n-torsion subgroup of the class group. If the subscript is dropped, it is the class number.
- $\mathrm{N}_{L/k}\mathfrak{a}$ is the ideal norm map. Dropping the subscript indicates that $k = \mathbb{Q}$ and $\mathrm{N}\mathfrak{a} = |\mathcal{O}_L/\mathfrak{a}|$.
- $\mathrm{N}_{L/k}(\alpha)$ is the element norm map. Dropping the subscript indicates that $k = \mathbb{Q}$
- $\mathfrak{d}_{L/k}$ is the relative discriminant ideal of L/k
- $D_{L/k}$ is $\mathrm{N}\mathfrak{d}_{L/k}$
- D_L is the absolute discriminant of $L/\mathbb{Q}$
- $C_{L/k}$ is the conductor of L/k. C_L is equivalent to $C_{L/\mathbb{Q}}$

1.2 Defining the Conductor

Before we can count any number field extensions by something we're calling the "conductor", we first need to define it (and a few other things along the way).

Let L/k be an extension of number fields with Galois group G. A *representation* of a finite group G is a homomorphism $\rho : G \to \mathrm{GL}_n(\mathbb{C})$, and the *character* χ of ρ is $\mathrm{Tr}(\rho(g))$.

If we can associate a representation ρ of G (or possibly multiple representations) to the extension L/k, then the *conductor* of L/k is defined to be the Artin conductor of ρ (or the lcm of the Artin conductors).

To make any sense of this we will need to define the Artin conductor of ρ and then describe how one can associate an extension with representations. The definition of the Artin conductor is quite cumbersome and we won't really use it to calculate the conductor of the representation we're interested in, but it is worth writing down for completeness. For more information see [26, Section VII.11].

For a Galois extension M/k and a prime $\mathfrak{p} \subset \mathcal{O}_k$ with $\mathfrak{P} \mid \mathfrak{p}$ in $\mathcal{O}_M$, we define the i-th ramification groups at $\mathfrak{p}$ to be $G_i = \{\sigma \in G \mid v_{\mathfrak{P}}(\sigma x - x) \geq i+1\}$ where x is any element of $\mathcal{O}_{L_{\mathfrak{P}}}$ such that $\mathcal{O}_{L_{\mathfrak{P}}} = \mathcal{O}_{K_{\mathfrak{p}}}[x]$. Also, for any ramification group G_i, let $\chi(G_i) = \frac{1}{g_i} \sum_{\sigma \in G_i} \chi(\sigma)$, where $g_i = |G_i|$.

The *local Artin conductor* of ρ with character χ at $\mathfrak{p}$ is $\mathfrak{f}_{\mathfrak{p}}(\chi) = \mathfrak{p}^{f(\chi,\mathfrak{p})}$ with

$$f(\chi, \mathfrak{p}) = \sum_{i \geq 0} \frac{g_i}{g_0} (\chi(1) - \chi(G_i)).$$

Finally, the *Artin conductor* of ρ with character χ is

$$\mathfrak{f}(\chi) = \prod_{\mathfrak{p} \nmid \infty} \mathfrak{f}_{\mathfrak{p}}(\chi).$$

Next, to associate a representation with L/k we will start with the subgroup $H \leq G$ such that L is the fixed field of H. Let $\mathbb{1}_H$ be the character of the trivial representation of H. We will induce this character from H to G and denote this by $\mathbb{1}_H^G$ (when referring back to the corresponding fields, we might also write this as $\mathbb{1}_L^k$). We know that $\mathbb{1}_H^G$ decomposes into a linear combination of irreducible characters of G. If $\{\chi_1, \ldots, \chi_n\}$ is the set of irreducible characters in this linear combination, then we define the *conductor* of L/k to be

$$C_{L/k} = |\mathcal{O}_k / \mathrm{lcm}(\mathfrak{f}(\chi_1), \ldots, \mathfrak{f}(\chi_n))|.$$

If we were to look at the Artin conductor of $\mathbb{1}_H^G$ directly, we get $\mathfrak{f}(\mathbb{1}_H^G) = \mathfrak{d}_{L/k}$ by a corollary in [26]. If L/k is Galois, then $\mathbb{1}_H^G$ is the character of the regular representation for G and we get

$$\mathfrak{f}(\mathbb{1}_H^G) = \mathfrak{d}_{L/k} = \prod_{\chi} \mathfrak{f}(\chi)^{\chi(1)},$$

where the product ranges over all of the irreducible characters of G. This is known as the *Conductor-Discriminant Formula* and is often used to access the Artin conductor without calculating the local Artin conductors defined above.

We'll use a quartic D_4 extension L/k as an example for finding the conductor. L has a unique quadratic subextension K. With H_L and H_K representing the subgroups corresponding to L and K respectively,

$$\begin{aligned}\mathbb{1}_{H_L}^{D_4} &= (\mathbb{1}_{H_L}^{H_K})^{D_4}\\ &= (\mathbb{1}_{H_K} + \chi)^{D_4}\\ &= \mathbb{1}_{H_K}^{D_4} + \chi^{D_4},\end{aligned}$$

Above, χ is the character of the sign representation of H_K/H_L, which becomes the unique 2-dimensional representation of D_4 when it is induced from H_K to D_4. Given that $N\mathfrak{f}(\mathbb{1}_{H_K}^{D_4}) = D_{K/k}$ and $D_{L/k} = D_{K/k}^2 D_{L/K}$, then $N\mathfrak{f}(\chi^{D_4}) = D_{K/k}D_{L/k}$. Since $\mathfrak{f}(\mathbb{1}_{H_K}^{D_4}) \mid \mathfrak{f}(\chi^{D_4})$, then $D_{K/k}D_{L/k}$ is also the conductor of L/k. At this point we note that in [1], the authors define the conductor of a D_4 quartic extension of $\mathbb{Q}$ to be the Artin conductor of χ^{D_4} and don't also consider the conductor of $\mathbb{1}_{H_k}^{D_4}$. However, our definitions coincide after considering the lcm of these Artin conductors.

Now our earlier promise should be satisfied, and we can proceed to the main body of the thesis.

Chapter 2

Comparing D_4 and S_4 Extensions

As mentioned earlier, Hilbert's Irreducibility Theorem implies that the Galois group of the splitting field of a "random" degree n polynomial over $\mathbb{Q}$ will be S_n 100% of the time. We might guess that picking a random degree n extension of $\mathbb{Q}$ will exhibit the same behavior. However, for $n = 4$, we have the first case where this is not true. Work of Bhargava [2] and Cohen, Diaz y Diaz, and Olivier [12] shows that only about 83% of quartic extensions of $\mathbb{Q}$ have Galois group S_4, with the remaining 17% having Galois group D_4 and 0% having Galois groups C_4, V_4, or A_4. In our work, which is also published here [18], we investigate this disparity for quartic extensions of an arbitrary number field F. In particular, we ask what proportion of quartic extensions of F are S_4 and what proportion are D_4.

Our first result shows that, when F is quadratic, there are typically many more D_4 than S_4 extensions. To make this precise, let $N_{F,n}(X;G) = \#\{K/F : |D_{K/F}| < X, [K : F] = n, \mathrm{Gal}(\widetilde{K}/F) = G\}$.

Theorem 2.0.1 *For $\epsilon > 0$, asymptotically 100% of quadratic number fields F ordered by discriminant have*

$$\lim_{X\to\infty} \frac{N_{F,4}(X;D_4)}{N_{F,4}(X;S_4)} \gg (\log|D_F|)^{\log 2-\epsilon}.$$

In particular, we have:

Corollary 2.0.2 100% *of quadratic number fields F have arbitrarily many more D_4 quartic extensions than S_4 quartic extensions.*

In practice, one can find quadratic number fields with small discriminant where D_4 quartic extensions vastly outnumber S_4 quartic extensions. For example, more than 90% of quartic extensions of $\mathbb{Q}(\sqrt{-210})$ and more than 99% of quartic extensions of $\mathbb{Q}(\sqrt{-510510})$ are D_4 quartic extensions. We give a general lower bound on the ratio for quadratic number fields in Theorem 2.3.1.

For general number fields we prove the following conditional statement. Let Cl_F be the the ideal class group of a number field F and let $h_2(F)$ be the number of elements of Cl_F with order dividing 2. Then we have the following:

Theorem 2.0.3 *Assume GRH and let F be a degree d number field over $\mathbb{Q}$. Then,*

$$\lim_{X\to\infty} \frac{N_{F,4}(X;D_4)}{N_{F,4}(X;S_4)} \gg_d \frac{h_2(F)-1}{(\log\log|D_F|)^d}.$$

The assumption of GRH is used for a lower bound on the residue of Dedekind zeta functions. In the course of proving Theorem 2.0.1, we prove that a weaker, but still sufficient bound holds for a positive proportion of quadratic Dirichlet L-functions in a restricted family. In particular, we show:

Theorem 2.0.4 *For 100% of fundamental discriminants D and for $\epsilon, \delta > 0$, a proportion $1-\delta$ of quadratic characters $\chi \pmod{|D|}$ have*

$$L(1,\chi) \geq \exp\left(-c(\log\log|D|)^{1-\frac{\log 2}{2}+\epsilon}\right),$$

where c depends on δ.

Granville and Soundararajan in [19] study the distribution of $L(1,\eta_D)$, where η_D is the primitive real character with modulus $|D|$, as D ranges over fundamental discriminants with $|D| \leq x$. Since we need to restrict our attention to the typical behavior of $L(1,\chi)$ for the much smaller family of quadratic characters of a fixed modulus $|D|$, their results do not port over directly to this setting.

In the next section we will show how to use field counting results of Bhargava, Shankar and Wang and of Cohen, Diaz y Diaz and Olivier [7, 12] to prove Theorem 2.0.3. In the following section, we consider the family of quadratic Dirichlet L-functions and prove Theorem 2.0.4. In Section 4, we complete the proof of Theorem 2.0.1, and in Section 5, we provide some examples.

2.1 Field Counting and Proof Strategy

For an extension of number fields L/F, let (r_1, r_2) denote the signature of F, D_F the absolute discriminant of F, and $D_{L/F}$ the norm of the relative discriminant of L/F. Note that $D_L = D_{L/F} D_F^{[L:F]}$. As above, Cl_F denotes the ideal class group of F and $\mathrm{Cl}_F[2]$ the elements of Cl_F with order dividing 2.

Bhargava, Shankar, and Wang [7] give asymptotic formulas for $N_{F,n}(X; S_n)$ when $n = 2, 3, 4$ or 5. In the $n = 4$ case they prove:

Theorem 2.1.1 (Bhargava, Shankar, Wang) *If F is a number field with r_1 real embeddings and r_2 complex embeddings, then*

$$N_{F,4}(X; S_4) \sim X \frac{1}{2} \operatorname*{Res}_{s=1} \ \zeta_F(s) \left(\frac{10}{4!}\right)^{r_1} \left(\frac{1}{4!}\right)^{r_2} \prod_{\mathfrak{p}} \left(1 + \frac{1}{N\mathfrak{p}^2} - \frac{1}{N\mathfrak{p}^3} - \frac{1}{N\mathfrak{p}^4}\right), \qquad (2.1)$$

where the product runs over prime ideals of F.

It follows that $\lim_{X\to\infty} \frac{1}{X} N_{F,4}(X; S_4) \asymp \operatorname*{Res}_{s=1} \zeta_F(s)$. Thus, it is bounds on the residue of $\zeta_F(s)$ that we'll need to control this term. For D_4, we recall work of Cohen, Diaz y Diaz, and Olivier [12] that gives an asymptotic formula for $N_{F,4}(X; D_4)$.

Theorem 2.1.2 (Cohen, Diaz y Diaz, Olivier) *If F is a number field with r_2 complex embeddings, then*

$$N_{F,4}(X; D_4) \sim X \sum_{[L:F]=2} \frac{1}{2^{r_2+1} D_{L/F}^2 \zeta_L(2)} \operatorname*{Res}_{s=1} \ \zeta_L(s), \qquad (2.2)$$

where the sum runs over quadratic extensions of F.

From these we obtain upper bounds on $N_{F,4}(X; S_4)$ and lower bounds on $N_{F,4}(X; D_4)$ so as to bound their ratio from below.

Restricting the summation in (2.2) to be over only those quadratic extensions L of F that are unramified, i.e. L such that $D_{L/F} = 1$, yields,

$$\lim_{X\to\infty} \frac{N_{F,4}(X; D_4)}{X} \gg_d \sum_{\substack{[L:F]=2 \\ D_{L/F}=1}} \operatorname*{Res}_{s=1} \zeta_L(s). \qquad (2.3)$$

If K is a number field of degree d over $\mathbb{Q}$ of discriminant D_K, then under GRH we have (see e.g. [10]),

$$\frac{1}{\log\log|D_K|} \ll \operatorname*{Res}_{s=1} \zeta_K(s) \ll (\log\log|D_K|)^{d-1}. \qquad (2.4)$$

Applying this bound to (2.1) gives an asymptotic upper bound for $N_{F,4}(X;S_4)$ and likewise applying it to (2.3) gives a lower bound for $N_{F,4}(X;D_4)$. In particular, conditional on GRH,

$$\lim_{X\to\infty}\frac{N_{F,4}(X;S_4)}{X} \ll (\log\log|D_F|)^{d-1} \text{ and } \lim_{X\to\infty}\frac{N_{F,4}(X;D_4)}{X} \gg \sum_{\substack{[L:F]=2\\ D_{L/F}=1}} \frac{1}{\log\log|D_L|} \qquad (2.5)$$

For a number field F, it follows from class field theory that there are $h_2(F)-1$ quadratic extensions L/F such that $D_{L/F}=1$. Using this fact and the estimates (2.5) we bound the ratio $N_{F,4}(X;D_4)/N_{F,4}(X;S_4)$. We immediately obtain Theorem 2.0.3. Note that for number fields F with odd class number, the lower bound given by the theorem is 0. However, you could obtain a similar lower bound by instead summing over quadratic extensions L/F with $D_{L/F}$ up to some bound.

If we specialize Theorem 2.0.3 to quadratic number fields F and note that $h_2(F)=2^{\omega(D_F)-m}$, where $m=1$ or 2 and $\omega(n)$ is the number of distinct prime divisors of n, we obtain the following:

Corollary 2.1.3 *Assume GRH and let F be any quadratic number field. Then,*

$$\lim_{X\to\infty}\frac{N_{F,4}(X;D_4)}{N_{F,4}(X;S_4)} \gg \frac{2^{\omega(D_F)}}{(\log\log|D_F|)^2}.$$

Even when $h(F)$ is odd, the lower bound from the corollary still holds because the sum on the right hand side of (2.5) can be expanded to include extensions L/F that ramify only at primes dividing 2.

The rest of the chapter is essentially concerned with removing the GRH assumption from Corollary 2.1.3. To do this we will restrict our attention to the case where F is a quadratic number field, and prove bounds analogous to (2.4) unconditionally for a positive proportion of the necessary L-functions. Theorem 2.0.1 will follow from such bounds.

2.2 Typical behavior of $L(1, \chi)$

We begin with a lemma that isolates the L-functions of interest.

Lemma 2.2.1 *Let F be a quadratic number field and L/F be an unramified quadratic extension. Then there are nonprincipal quadratic Dirichlet characters χ_1 and χ_2 such that $\chi_1\chi_2 = \chi_F$ and for which*

$$\zeta_L(s) = \zeta(s)L(s, \chi_F)L(s, \chi_1)L(s, \chi_2),$$

where $\chi_F = \left(\frac{D_F}{\cdot}\right)$.

Proof: Let F be a quadratic number field. We know from [29] that every unramified quadratic extension L/F is Galois and has Galois group V_4. Looking at the irreducible characters of V_4 in the context of $L/F/\mathbb{Q}$, we see that one character must be χ_F and the other two non-trivial characters (χ_1 and χ_2, say) must have the desired property.□

When we put this in the context of the ratio $N_{F,4}(X; D_4)/N_{F,4}(X; S_4)$, we see that each such unramified quadratic extension L of F has $\operatorname{Res}_{s=1} \zeta_F(s)$ dividing $\operatorname{Res}_{s=1} \zeta_L(s)$, leaving behind

$$\frac{\operatorname{Res}_{s=1} \zeta_L(s)}{\operatorname{Res}_{s=1} \zeta_F(s)} = L(1, \chi_1)L(1, \chi_2). \tag{2.6}$$

Therefore, in order to remove the GRH assumption and prove Theorem 2.0.1, it suffices to prove Theorem 2.0.4.

Rather than bound $L(1, \chi)$ directly, we'll consider $\log L(1, \chi)$ instead. We will find its second moment and then use a discrete analogue of Chebyshev's inequality to obtain the desired result.

2.2.1 The Second Moment of $\log L(1,\chi)$

Recall from [14, Chapter 20] that at most one nonprincipal real character $\chi \pmod D$ exists such that $L(s,\chi)$ has a real zero β with $\beta > 1 - c/\log D$ for some absolute constant c. If such a character exists, we say it has an exceptional zero. We will use this in the following key lemma.

Lemma 2.2.2 *For a fixed modulus D, let χ_0 denote the principal character and define*
$V = \{\chi \pmod D \mid \chi \neq \chi_0, \chi^2 = \chi_0,\ \chi$ *does not have an exceptional zero*$\}$. *Then*

$$\frac{1}{\#V}\sum_{\chi\in V}(\log L(1,\chi))^2 = O\left((\log\log D)(\log\omega_Y(D) + \log\log Y) + \frac{(\log\log D)^2}{2^{\omega_Y(D)}}\right),$$

for any $Y < D$ and where $\omega_Y(D) = \#\{p \leq Y : p \mid D\}$.

To prove the lemma, we need the following result of Brun and Titchmarsh [24, Theorem 2].

Theorem 2.2.3 (Brun-Titchmarsh) *Let a and q be coprime integers, $\pi(z;q,a)$ be the number of primes less that z that are congruent to $a \pmod q$, and let $x \geq 0$ and $y > q$ be real numbers. Then*

$$\pi(x+y;q,a) - \pi(x;q,a) \leq \frac{2y}{\varphi(q)\log y/q}.$$

Proof (Lemma 2.2.2): Recall that for a character $\chi \pmod D$,

$$\log L(1,\chi) = \sum_p \frac{\chi(p)}{p} + \sum_p\sum_{k=2}^{\infty}\frac{\chi(p)^k}{kp^k}.$$

The double sum on the right is absolutely convergent and bounded above and below by absolute constants. So we need only focus on the left-hand sum. Because the left-hand sum is not absolutely convergent, we will split the sum at some threshold T into

$$\sum_{p<T}\frac{\chi(p)}{p} + \sum_{p\geq T}\frac{\chi(p)}{p}.$$

From [14, Chapter 20], if χ does not have an exceptional zero, a choice of $T = D^{\log D/(4c_1^2)}$ for some absolute constant c_1, yields

$$\sum_{p\geq T}\frac{\chi(p)}{p} = O\left(\frac{1}{\exp(c_2\sqrt{\log T})\log T}\right),$$

where c_2 is an absolute constant. This makes

$$\log L(1,\chi) = \sum_{p<T}\frac{\chi(p)}{p} + O(1). \tag{2.7}$$

If we assume the set of all Dirichlet characters modulo D does not contain an exceptional zero and we use (2.7), then

$$\begin{aligned}\frac{1}{\#V}\sum_{\chi\in V}(\log L(1,\chi))^2 &= \frac{1}{\#V}\sum_{\chi\in V}\left(\sum_{p}\frac{\chi(p)}{p} + \sum_{p}\sum_{k=2}^{\infty}\frac{\chi(p)^k}{kp^k}\right)^2\\ &= \frac{1}{\#V}\sum_{\chi\in V}\left(\sum_{p<T}\frac{\chi(p)}{p} + O(1)\right)^2\\ &= \frac{1}{\#V}\sum_{\chi\in V}\left(\sum_{p,q<T}\frac{\chi(pq)}{pq} + O(1)\sum_{p<T}\frac{\chi(p)}{p} + O(1)\right).\end{aligned}$$

The cross term we can bound trivially as $O(\log\log T)$, so the object of our focus will be the leading term as we sum over the characters in our family. For the leading term, we include the principal character in the outer sum, apply orthogonality and then subtract off the contribution from the principal character. After summing over χ, this yields a main term of

$$\sum_{p<T}\frac{1}{p}\sum_{\substack{q<T\\ pq\equiv\square\,(D)}}\frac{1}{q} - \frac{1}{\#V+1}\sum_{p,q<T}\frac{1}{pq}. \tag{2.8}$$

Given that $\#V + 1 = 2^{\omega(D)}$, the right-hand term of (2.8) is on the order of $(\log\log T)^2/2^{\omega(D)}$. Since our goal is to show the second moment is small, we need to calculate an upper bound for the left-hand term of (2.8). For the analysis, we will break up the left-hand sum of (2.8) according to an auxiliary parameter $E < D$,

$$\sum_{p<T} \frac{1}{p} \sum_{\substack{q<T \\ pq \equiv \square\,(D)}} \frac{1}{q} = \sum_{p<T} \frac{1}{p} \left(\sum_{\substack{q<2E \\ pq \equiv \square\,(D)}} \frac{1}{q} + \sum_{\substack{2E \le q < 2D \\ pq \equiv \square\,(D)}} \frac{1}{q} + \sum_{\substack{2D \le q < T \\ pq \equiv \square\,(D)}} \frac{1}{q} \right). \tag{2.9}$$

We will a make a convenient choice of E later. For now, we will establish an upper bound on the rightmost sum over primes $2D \le q < T$ in (2.9). Note that given a fixed prime p, there are exactly $\dfrac{\phi(D)}{2^{\omega(D)}}$ congruence classes $a \in (\mathbb{Z}/D\mathbb{Z})^\times$ such that pa is a square modulo D. Hence,

$$\sum_{\substack{2D \le q < T \\ pq \equiv \square(D)}} \frac{1}{q} = \sum_{\substack{a \in (\mathbb{Z}/D\mathbb{Z})^\times \\ pa \equiv \square(D)}} \sum_{\substack{2D \le q < T \\ q \equiv a(D)}} \frac{1}{q}. \tag{2.10}$$

Using partial summation, the inner sum of (2.10) is

$$\begin{aligned} \sum_{\substack{2D \le q < T \\ q \equiv a(D)}} \frac{1}{q} &= \int_{2D}^{T} \frac{1}{t}\, d(\pi(t;a,D)) \\ &= \frac{\pi(t;a,D)}{t}\Big|_{2D}^{T} + \int_{2D}^{T} \frac{\pi(t;a,D)}{t^2}\, dt. \end{aligned}$$

We apply Theorem 2.2.3 to bound from above $\pi(t;a,D)$ when $t > D$.

$$\begin{aligned} \frac{\pi(t;a,D)}{t}\Big|_{2D}^{T} + \int_{2D}^{T} \frac{\pi(t;a,D)}{t^2}\, dt &\le \frac{2}{\phi(D)} \left(\frac{1}{\log(T/D)} - \frac{2}{\log 2} \right) + \frac{2}{\phi(D)} \int_{2D}^{T} \frac{1}{t \log(t/D)}\, dt \\ &= \frac{2}{\phi(D)} \left(\log\log(T/D) - \log\log 2 + \frac{1}{\log(T/D)} - \frac{2}{\log 2} \right). \end{aligned}$$

Note that the bound we obtained above by using Theorem 2.2.3 doesn't depend on a, so we may use the same bound for every relevant congruence class. This means the double sum (2.10) can be bounded by

$$\sum_{\substack{a \in (\mathbb{Z}/D\mathbb{Z})^\times \\ pa \equiv \square(D)}} \sum_{\substack{2D \le q < T \\ q \equiv a(D)}} \frac{1}{q} \le \frac{1}{2^{\omega(D)-1}} \left(\log\log(T/D) - \log\log 2 + \frac{1}{\log(T/D)} - \frac{2}{\log 2} \right).$$

Overall, this term is of order $O\left(\dfrac{\log\log D}{2^{\omega(D)}} \right)$.

Because Theorem 2.2.3 does not apply when $t \le D$, we need to handle the range

$2E \le q < 2D$ differently. Note that if $E \mid D$, then

$$\sum_{\substack{R \le q < S \\ q \equiv a(D)}} \frac{1}{q} \le \sum_{\substack{R \le q < S \\ q \equiv a(E)}} \frac{1}{q},$$

for any choice of $1 \le R < S$.

We will take E to be a sufficiently small divisor of D. Take $Y \le D$, let $\omega_Y(D) = \#\{p \mid D : p \le Y\}$, and define

$$E = \prod_{\substack{p \le Y \\ p \mid D}} p.$$

We can now use Theorem 2.2.3 with E as the modulus to obtain

$$\sum_{\substack{2E \le q < 2D \\ pq \equiv \square\,(D)}} \frac{1}{q} \le \sum_{\substack{2E \le q < 2D \\ pq \equiv \square\,(E)}} \frac{1}{q} \le \frac{1}{2^{\omega_Y(D)-1}} \left(\log\log(2D/E) - \log\log 2 + \frac{2}{\log(2D/E)} - \frac{2}{\log 2} \right)$$

where $\omega_Y(D)$ is the number of distinct prime divisors of D that are less than or equal to Y. Overall this is of order $O\left(\frac{\log\log D}{2^{\omega_Y(D)}}\right)$.

Finally, for the range $q < 2E$, we will use the trivial bound on the sum of reciprocal primes,

$$\sum_{\substack{q < 2E \\ pq \equiv \square\,(D)}} \frac{1}{q} \le \sum_{q < 2E} \frac{1}{q} = \log\log 2E + O(1).$$

Given that E is the product of primes that are at most Y, then

$$\begin{aligned} \log\log 2E &\le \log\log(2Y^{\omega_Y(D)}) \\ &= \log(\log 2 + \omega_Y(D)\log Y) \\ &= O(\log \omega_Y(D) + \log\log Y). \end{aligned}$$

Now, because

$$\sum_{p < T} \frac{1}{p} = \log\log T + O(1) = O(\log\log D)$$

and $\frac{(\log\log D)^2}{2^{\omega_Y(D)}} \gg \frac{(\log\log D)^2}{2^{\omega(D)}}$, then our whole sum is

$$O\left((\log\log D)(\log\omega_Y(D) + \log\log Y) + \frac{(\log\log D)^2}{2^{\omega_Y(D)}}\right). \tag{2.11}$$

This completes the proof of the lemma if the family of characters does not contain an exceptional zero. If the complete family of characters modulo D does admit an exceptional zero, then we also need to subtract off the contribution from the exceptional character χ'. Then (2.8) becomes

$$\sum_{p<T}\frac{1}{p}\sum_{\substack{q<T\\ pq\equiv\square(D)}}\frac{1}{q} - \frac{1}{\#V+2}\sum_{p,q<T}\frac{1}{pq} - \frac{1}{\#V+2}\sum_{p,q<T}\frac{\chi'(pq)}{pq}.$$

The term coming from the exceptional character is $O\left(\frac{(\log\log D)^2}{2^{\omega(D)}}\right)$ and does not change the rest of the analysis. □

Now that we know the order of the second moment for the family of quadratic Dirichlet L-functions, we want to use this to give a workable lower bound on $L(1,\chi)$ for most quadratic χ in V. This result is the following corollary.

Corollary 2.2.4 *For a modulus D, any $Y \leq D$, and a choice of $k \geq 1$ a proportion at least $1 - 1/k^2$ of non-exceptional quadratic characters χ modulo D have*

$$L(1,\chi) \geq (\log D)^{-kc\sqrt{\frac{\log\omega_Y(D)+\log\log Y}{\log\log D}+\frac{1}{2^{\omega_Y(D)}}}},$$

where c is an absolute constant.

Proof: Let $k \geq 1$ and σ^2 be any value such that

$$\frac{1}{\#V}\sum_{\chi\in V}(\log L(1,\chi))^2 \leq \sigma^2.$$

We bound $\#\{\chi\in V : |\log L(1,\chi)| \geq k\sigma\}$.

$$\#\{\chi\in V : |\log L(1,\chi)| \geq k\sigma\} = \sum_{\substack{\chi\in V\\ |\log L(1,\chi)|\geq k\sigma}} 1 \leq \sum_{\chi\in V}\frac{(\log L(1,\chi))^2}{k^2\sigma^2} \leq \frac{\#V}{k^2}.$$

The result follows from this argument and Lemma 2.2.2. □

2.2.2 Typical Behavior of ω_Y

From (2.11), the order of the second moment depends on the size of $\omega_Y(D)$. We will apply Chebyshev's inequality to give workable bounds on $\omega_Y(D)$. Because we will make frequent use of Chebyshev's inequality, we state it here for convenience.

Theorem 2.2.5 (Chebyshev's Inequality) *Let V be a finite set with cardinality N and let $f: V \to \mathbb{C}$. If f has mean and variance respectively given by*

$$\mu = \frac{1}{N}\sum_{v\in V} f(v) \quad \textit{and} \quad \sigma^2 = \frac{1}{N}\sum_{v\in V}(f(v)-\mu)^2,$$

then, for any k,

$$\#\{v \in V \mid |f(v)-\mu| \geq k\sigma\} \leq \frac{N}{k^2}.$$

To use this, we will need to understand the mean and variance of $\omega_Y(D)$ for most D.

Let $N(X)$ be the number of fundamental discriminants (both positive and negative) less than X. It is known that $N(X) c_2 X$ where $c_2 = 1/\zeta 2$.

Lemma 2.2.6 (Mean of $\boldsymbol{\omega_Y(n)}$) *Let $Y \leq X^{1-\delta}$ for some $\delta > 0$. For fundamental discriminants D such that $|D| \leq X$,*

$$\frac{1}{N(X)}\sum_{|D|\leq X}^{\flat} \omega_Y(D) = \sum_{p\leq Y}\frac{1}{p+1} + O\left(\frac{Y^{1/2}}{X^{1/2-\epsilon}}\right).$$

Proof: We have

$$\begin{aligned}\frac{1}{N(X)}\sum_{D\leq X}^{\flat}\omega_Y(D) &= \frac{1}{N(X)}\sum_{|D|\leq X}^{\flat}\sum_{\substack{p|D\\ p\leq Y}} 1\\ &= \frac{1}{N(X)}\sum_{p\leq Y}\sum_{\substack{p|D\\ |D|\leq X}}^{\flat} 1\\ &= \frac{1}{c_2 X}\sum_{p\leq Y}\left(c_2\frac{X}{p+1} + O\left(X^{1/2+\epsilon}p^{-1/2}\right)\right)\end{aligned}$$

$$= \sum_{p\le Y}\left(\frac{1}{p+1} + O(X^{-1/2+\epsilon}p^{-1/2})\right)$$
$$= \sum_{p\le Y}\frac{1}{p+1} + O\left(\frac{Y^{1/2}}{X^{1/2-\epsilon}}\right),$$

where the third equality is an immediate consequence of Theorem 2.1 of [22] in the degree 2 case, for example. □

Lemma 2.2.7 (Variance of $\boldsymbol{\omega_Y(n)}$) *Let $Y \le X^{1/2-\delta}$ for some $\delta > 0$ and $\mu = \sum_{p\le Y}\frac{1}{p+1}$. Then*

$$\frac{1}{N(X)}\sum_{|D|<X}^{\flat}(\omega_Y(D)-\mu)^2 = \sum_{p\le Y}\frac{1}{p+1}\left(1-\frac{1}{p+1}\right) + O\left(\frac{Y}{X^{1/2-\epsilon}}\right).$$

Proof: To calculate the variance, we need to evaluate

$$\frac{1}{N(X)}\sum_{|D|<X}^{\flat}(\omega_Y(D)-\mu)^2. \tag{2.12}$$

Expanding and distributing the sum over admissible D, this quantity is equal to

$$\frac{1}{N(X)}\sum_{|D|<X}^{\flat}\left(\sum_{\substack{p<Y\\ p|D}}1\right)^2 - \frac{2\mu}{N(X)}\sum_{|D|<X}^{\flat}\omega_Y(D) + \mu^2. \tag{2.13}$$

We'll address the two sums in (2.13) individually. Note that sums are taken over primes and that the notation is consistent with that in [22]. The leftmost term of (2.13) give us that

$$\frac{1}{N(X)}\sum_{|D|<X}^{\flat}\left(\sum_{\substack{p<Y\\ p|D}}1\right)^2 = \frac{1}{N(X)}\sum_{|D|<X}^{\flat}\left(\sum_{\substack{p,q<Y\\ p,q|D}}1\right)$$
$$= \frac{1}{N(X)}\sum_{p,q<Y}\sum_{\substack{|D|<X\\ p,q|D}}^{\flat}1$$
$$= \frac{1}{N(X)}\sum_{p=q<Y}\sum_{\substack{|D|<X\\ p|D}}^{\flat}1 + \frac{1}{N(X)}\sum_{\substack{p,q<Y\\ p\ne q}}\sum_{\substack{|D|<X\\ p,q|D}}^{\flat}1$$

$$= \sum_{p \le Y} \frac{1}{p+1} + \sum_{\substack{p,q<Y \\ p \ne q}} \left(\frac{1}{(p+1)(q+1)} + O(X^{-1/2+\epsilon}(pq)^{-1/2}) \right)$$

$$= \sum_{p \le Y} \frac{1}{p+1} + \sum_{\substack{p,q<Y \\ p \ne q}} \frac{1}{(p+1)(q+1)} + O\left(\frac{Y}{X^{1/2-\epsilon}} \right). \tag{2.14}$$

Where the last line follows from Theorem 2.1 of [22]. Now we address the second term of (2.13). It gives us that

$$\frac{2\mu}{N(X)} \sum_{|D|<X}^{\flat} \omega_Y(D) = 2\left(\sum_{p \le Y} \frac{1}{p+1} \right) \left(\sum_{q \le Y} \left[\frac{1}{q+1} + O\left(X^{-1/2+\epsilon} q^{-1/2} \right) \right] \right)$$

$$= 2\left(\sum_{p,q \le Y} \frac{1}{(p+1)(q+1)} + O\left(\frac{Y^{1/2} \log\log Y}{X^{1/2-\epsilon}} \right) \right). \tag{2.15}$$

Substituting (2.14) and (2.15) into (2.13) and expanding μ^2, we find

$$\frac{1}{N(X)} \sum_{|D|<X}^{\flat} (\omega_Y(D) - \mu)^2 = \sum_{p \le Y} \frac{1}{p+1} - \sum_{p \le Y} \frac{1}{(p+1)^2} + O\left(\frac{Y}{X^{1/2-\epsilon}} \right). \qquad \square$$

Now that we have some basic statistical facts about $\omega_Y(D)$, we can use Chebyshev's inequality to give a bound for $\omega_Y(D)$ for most D. For our purposes, we will take $Y = \log X$, which will give us mean and variance $\log\log\log X + O(1)$.

Theorem 2.2.8 *Let* $Y = \log X$. *For all* $\epsilon > 0$, *all but* $O\left(\frac{X}{(\log\log\log X)^{1-\epsilon}} \right)$ *fundamental discriminants* D *with* $|D| < X$ *are such that* $\omega_Y(D) \ge \log\log\log X - O\left((\log\log\log X)^{1-\epsilon} \right)$.

Proof: Use Chebyshev's inequality with Lemmas 2.2.6 and 2.2.7 taking $k = (\log\log\log X)^{1/2-\epsilon}$.$\square$

Applying Theorem 2.2.8 to (2.11) gives us that for 100% of fundamental discriminants D, the second moment of the family of quadratic characters modulo $|D|$ is $O\left((\log\log|D|)^{2-\log 2+\epsilon} \right)$. Using this we can now prove Theorem 2.0.4.

Proof (Theorem 2.0.4): Let $\epsilon, \delta > 0$ and let D be a fundamental discriminant such that $|\omega_Y(D) - \log\log\log|D||$ is $O\left((\log\log\log|D|)^{1-\epsilon} \right)$. By Theorem 2.2.8, 100% of fundamental disciriminants have this property.

Lemma 2.2.2 above shows that the second moment of the quadratic characters modulo $|D|$ is at most $O\left((\log\log|D|)^{2-\log 2+\epsilon}\right)$, when we take $Y = \log D$. Choosing $k = \delta^{-1/2}$ in Corollary 2.2.4, the result follows. □

2.3 Proof of Main Theorem

We are now ready to address ourselves to the proof of Theorem 2.0.1. The main idea is to use Theorem 2.0.4 to control the residues of the residues of Dedekind ζ-functions appearing in the D_4 and S_4 estimates in (2.5).

Proof (Theorem 2.0.1.): Let $F = \mathbb{Q}(\sqrt{d})$, with d squarefree, be a quadratic number field. Let W be the set quadratic extensions L/F where $L = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ and $d_1 d_2 = d$. Note that these extensions are such that $\zeta_L(s)$ factors in such a way as to give us (2.6), and so

$$\lim_{X\to\infty} \frac{N_{F,4}(X, D_4)}{N_{F,4}(X, S_4)} \gg \sum_{\substack{L\in W \\ [L:F]=2}} \frac{\mathrm{Res}_{s=1}\zeta_L(s)}{\mathrm{Res}_{s=1}\zeta_F(s)}. \tag{2.16}$$

This will be our starting point. First we'll estimate the residue term by combining (2.6) with Theorem 2.0.4 to see that for 100% quadratic extensions F and sufficiently small ϵ and δ, and a constant c, a proportion $\frac{1-\delta}{2}$ of $L \in W$ satisfy,

$$\frac{\operatorname*{Res}_{s=1} \zeta_L(s)}{\operatorname*{Res}_{s=1} \zeta_F(s)} \gg_\delta \exp(-c(\log\log|D_F|)^{1-\frac{\log 2}{2}+\epsilon})(\log\log|D_F|)^{-2},$$

the $\log\log|D_F|$ appearing on the right above being a correction factor created when we pass from quadratic characters modulo $|D_F|$ to the L-functions of the the corresponding quadratic number fields.

For any F, $\#W = 2^{\omega(d)}$. From Section 2.3 of [25] and Theorem 2.2.8 we have that 100% of quadratic fields $F = \mathbb{Q}(\sqrt{d})$ are such that $\#W = 2^{\omega(d)} \gg (\log|D_F|)^{\log 2-\epsilon'}$ for any $\epsilon' > 0$.

So for 100% of quadratic fields F, we conclude that

$$\lim_{X\to\infty} \frac{N_{F,4}(X,D_4)}{N_{F,4}(X,S_4)} \gg_\delta (\log|D_F|)^{\log 2-\epsilon'} \exp(-(\log\log|D_F|)^{1-\frac{\log 2}{2}+\epsilon})(\log\log|D_F|)^{-2}. \tag{2.17}$$

The statement of Theorem 2.0.1 follows. □

It is worth remarking that we have invoked two *different* 100% results above. The first is that 100% of quadratic number fields are such the bounds on $\omega_Y(D_F)$ are met (in order to get the bound on residues). The other is that 100% of quadratic number fields are such that the right condition on $\omega(D_F)$ is met (in order to get a suitable bound on $2^{\omega(D_F)}$). In the worst case, the exceptional sets for each of these results are distinct, but their proportion still goes to zero as our bound X on admissible D_F grows.

Applying the same reasoning from the proof for Theorem 2.0.1, but without using Theorem 2.2.8, gives the following lower bound on the ratio for any quadratic number field F.

Theorem 2.3.1 *Let F be a quadratic number field and fix $Y \le |D_F|$, then there is some constant c such that*

$$\lim_{X\to\infty} \frac{N_{F,4}(X;D_4)}{N_{F,4}(X;S_4)} \gg \frac{h_2(F)}{(\log\log|D_F|)^2(\log|D_F|)^{c\sqrt{\frac{\log\omega_Y(D_F)+\log\log Y}{\log\log|D_F|}+\frac{1}{2^{\omega_Y(D_F)}}}}}.$$

For a choice of quadratic number field F, the above expression shows that if you can pick Y sufficiently small such that $\omega_Y(D_F)$ is sufficiently large, there will be a bias in favor of D_4 quartic extensions of F. Further, if $\omega_Y(D_F)$ is very large, one should expect that $h_2(F)$ is large as well. For example, if we have $\omega_Y(D_F)$ is of size $\frac{\log|D_F|}{\log\log|D_F|}$ then $h_2(F)$ is at least of size $|D_F|^{\log 2/\log\log|D_F|}$.

2.4 Examples

Now that we've shown that most quadratic number fields have more D_4 quartic extensions than S_4, a couple of natural problems to address are constructing an explicit family of quadratic number fields with arbitrarily more D_4 than S_4 extensions, and finding the first quadratic number field with more D_4 than S_4 extensions.

For the first question, consider the family of number fields obtained by taking $F = \mathbb{Q}(\sqrt{\pm d})$ where $d = \prod_{p \le y} p$, as we take $y \to \infty$. For this family,

$$\omega(D_F) = \frac{\log|D_F|}{\log\log|D_F|}(1 + O(1/\log\log|D_F|)),$$

which immediately gives that $h_2(F)$ is about $\exp\left(\frac{\log 2 \log|D_F|}{\log\log|D_F|}\right)$. Because $\omega(D_F)$ is larger than average in this case, we can show that fields in this family have arbitrarily more D_4 than S_4 extensions without appealing to Theorem 2.0.4. Instead we can use a lower bound on $L(1,\chi)$ given by Theorem 11.4 in [25] which is only conditional on χ not having an exceptional zero.

In fact, because the formulae from [7, 12] are explicit, we can effectively approximate the constants $\lim_{X\to\infty} \dfrac{N_{F,4}(X; D_4)}{X}$ and $\lim_{X\to\infty} \dfrac{N_{F,4}(X; S_4)}{X}$, using either Sage or Magma. In Table 2.1, we see that in our family of fields the percentage of D_4 extensions quickly exceeds the percentage of S_4 extensions.

Using the same code, we can also answer the question of which quadratic number field is the "first" one with more D_4 extensions than S_4 extensions. Again, we assume $F = \mathbb{Q}(\sqrt{\pm d})$, but now d runs over square-free numbers rather than only the product of all primes up to y as above. If we order by $|d|$, then we see that about 56% of quartic extensions of $\mathbb{Q}(\sqrt{-10})$ are D_4. See Table 2.2.

$\pm d$	S_4 **Constant**	D_4 **Constant**	D_4 **Percentage**
2	0.06125	0.00255	3.99445
-2	0.02868	0.00242	7.77024
6	0.09898	0.03626	26.81255
-6	0.03389	0.03049	47.35530
30	0.12119	0.20786	63.16992
-30	0.02911	0.11788	80.19609
210	0.11894	0.68112	85.13409
-210	0.02161	0.26399	92.43194
2310	0.13033	1.95228	93.74184
-2310	0.02662	0.75727	96.60405
30030	0.08761	3.14195	97.28722
-30030	0.02961	1.81818	98.39736
510510	0.11305	8.63748	98.70812
-510510	0.02499	3.27599	99.24306

Table 2.1: D_4 percentage for ascending product of primes

$\pm d$	S_4 **Constant**	D_4 **Constant**	D_4 **Percentage**
-1	0.01916	0.00080	4.00075
2	0.06125	0.00241	3.77973
-2	0.02868	0.00235	7.55794
3	0.07729	0.02138	21.66628
-3	0.01480	0.00015	1.01581
5	0.04181	0.00041	0.97732
-5	0.03783	0.02618	40.90038
6	0.09898	0.03602	26.68166
-6	0.03389	0.03025	47.16238
7	0.11253	0.03552	23.99301
-7	0.02954	0.00051	1.68833
10	0.12577	0.07665	37.86747
-10	0.02468	0.03141	55.99729

Table 2.2: D_4 percentage for ascending squarefree numbers

Chapter 3

Counting D_4 Extensions by Conductor

For a quartic field L whose normal closure $M/\mathbb{Q}$ has Galois group D_4, Altuğ, Shankar, Varma, and Wilson [1] define the *conductor* of L (which we denote as C_L) to be the Artin conductor of the irreducible 2-dimensional Galois representation

$$\rho_M : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$$

that factors through $\mathrm{Gal}(M/\mathbb{Q}) \cong D_4$.

Using additional algebraic structure coming from an outer automorphism of D_4, they proved that if $N_4^C(X; D_4)$ denotes the number of isomorphism classes of D_4 quartic fields with conductor bounded by X, then

$$N_4^C(X; D_4) = \frac{3}{8} \cdot \prod_p \left(1 - \frac{1}{p^2} - \frac{2}{p^3} + \frac{2}{p^4}\right) \cdot X \log X + O(X \log\log X).$$

In this chapter, which is also in preprint form [17], we build on their result using an analogue of the Dirichlet hyperbola method that relies on the same algebraic structure and yields a secondary term. When counting number fields by discriminant, there are only a few cases for non-abelian extensions where a secondary term is proved to exist. For S_3 cubic fields, both Bhargava, Shankar, and Tsimerman [5] and Taniguchi and Thorne [30] proved a conjecture about a secondary term in the asymptotic formula. Wang [31] proved a similar result for $S_3 \times A$ extensions where A is an odd abelian group with minimal prime divisor greater than 5. Our result is below.

Theorem 3.0.1 *Let $N_4^C(X; D_4)$ denote the number of isomorphism classes $[L : \mathbb{Q}]$ where L is a quartic D_4 extension with conductor $C_L \leq X$. Then,*

$$N_4^C(X; D_4) = \frac{3}{8} \cdot \prod_p \left(1 - \frac{1}{p^2} - \frac{2}{p^3} + \frac{2}{p^4}\right) \cdot X \log X$$

$$+\left(\frac{3}{8}\cdot\left(1-\frac{7\log 2}{20}-2\sum_p\frac{\log p}{p^2+2p+2}\right)\cdot\prod_p\left(1-\frac{1}{p^2}-\frac{2}{p^3}+\frac{2}{p^4}\right)+c\right)\cdot X$$
$$+O_\epsilon(X^{11/12+\epsilon})$$

where c is given by (3.5).

In addition to their main theorem, [1] also proved asymptotics for D_4 quartic fields with certain local specifications. They define $\Sigma = (\Sigma_v)_v$ to be a *collection of local specifications* if for each place v of $\mathbb{Q}$, Σ_v contains pairs (L_v, K_v) consisting of a degree 4 étale alebra L_v of $\mathbb{Q}_v$ and a quadratic subalgebra K_v. Like them, we will define the *conductor* to be

$$C(L_p, K_p) = \mathrm{Disc}(L_p)/\mathrm{Disc}(K_p).$$

We will call a collection Σ *acceptable* if for all but finitely many places v, the set Σ_v contains all pairs (L_v, K_v). $\mathcal{L}(\Sigma)$ will denote all D_4 quartic fields L such that $L\otimes\mathbb{Q}_v \in \Sigma_v$ for all v, and $N_4^C(X; D_4; \Sigma)$ the number of isomorphism classes in $\mathcal{L}(\Sigma)$ whose conductor is bounded by X. To simplify notation, we will let

$$\mu(\Sigma_\infty) = \sum_{(L_\infty,K_\infty)\in\Sigma_\infty}\frac{1}{|\mathrm{Aut}(L_\infty,K_\infty)|},\ \text{and}\ \mu(\Sigma_p) = \sum_{(L_p,K_p)\in\Sigma_p}\frac{1}{|\mathrm{Aut}(L_p,K_p)|C(L_p,K_p)},$$

where ∞ is the sole infinite place of $\mathbb{Q}$ and p is a prime, and $|\mathrm{Aut}(L_v, K_v)|$ is the number of automorphisms of L_v that send K_v to itself.

In [1], quartic D_4 fields L are defined to have *central inertia* at odd primes p under certain conditions. This happens locally when $C(L_p, K_p) = p^2$ but K_p is not ramified at p. We will use $\mu(\Sigma_{p^2})$ to denote a sum over pairs (L_p, K_p) having central inertia that is constructed similarly to the sum for $\mu(\Sigma_p)$. As one might imagine, the case for $p = 2$ is more complicated. We will investigate this later, but for the moment we will use $\mu(\Sigma_{2^2}), \mu(\Sigma_{2^4})$, and $\mu(\Sigma_{2^6})$ without explanation. With that, we have the following theorem.

Theorem 3.0.2 *If $\Sigma = (\Sigma_v)_v$ is an acceptable collection of local specifications and*

m is the product of the primes p for which Σ_p does not contain every pair (L_p, K_p). When $m \ll X^{1/4}$,

$$N_4^C(X; D_4; \Sigma) = \frac{1}{2} X \cdot \left(\log X + 1 - 2 \sum_{p \neq 2} \frac{\log p \cdot \mu(\Sigma_{p^2})}{\mu(\Sigma_p)} - 2 \log 2 \frac{\mu(\Sigma_{2^2}) + 2\mu(\Sigma_{2^4}) + 3\mu(\Sigma_{2^6})}{\mu(\Sigma_2)} \right) \cdot \mu(\Sigma_\infty) \cdot \prod_p \left(\left(1 - \frac{1}{p}\right)^2 \mu(\Sigma_p) \right) + X c_\Sigma + O_\epsilon(X^{11/12+\epsilon} m^{1/3+\epsilon}),$$

where c_Σ is a non-multiplicative constant given in (3.20).

In order to prove Theorem 3.0.2, we need to count quadratic extensions of some number field k with a set of local specifications for each place of k. For a number field k we define $\Sigma_k = (\Sigma_{k,v})_v$ to be a *collection of local specifications over* k if for each place v of k, $\Sigma_{k,v}$ contains quadratic étale alegbras K_v over k_v. Similar to before, we will call Σ_k *acceptable* if $\Sigma_{k,v}$ contains all quadratic étale algebras K_v except for at possibly finitely many places. Let $\mathcal{K}(\Sigma_k)$ denote all quadratic extensions K/k such that $K \otimes_k k_v \in \Sigma_{k,v}$ and $\Phi_{k,2}(\Sigma_k; C_2, s)$ denote the Dirichlet series

$$\Phi_{k,2}(\Sigma_k; C_2, s) = \sum_{K \in \mathcal{K}(\Sigma_k)} \frac{1}{D_{K/k}^s},$$

where $D_{K/k}$ is the norm of the relative discriminant ideal of K/k.

Later on in the chapter, we will write down a different formula for this Dirichlet series that will be derived similarly to the method of proving Theorem 1.1 from [12]. The formula will give rise to the theorem below. To make the statement less cumbersome, we categorize some possibilities for incomplete $\Sigma_{k,\mathfrak{p}}$ at odd primes $\mathfrak{p}$. We will call $\Sigma_{k,\mathfrak{p}}$ *comprehensively ramified* if it contains both étale algebras that are ramified and no unramified étale algebras. We will call $\Sigma_{k,\mathfrak{p}}$ *selectively ramified* if it contains one ramified étale algebra and no unramified étale algebras. Similarly, we will call $\Sigma_{k,\mathfrak{p}}$ *comprehensively unramified* if it contains both unramified étale algebras and *selectively unramified* if it contains only one of them.

Theorem 3.0.3 *Let k be a number field, Σ_k be an acceptable collection of local specifications for k. Let $\mathfrak{r}_1$ (resp. $\mathfrak{u}_1$) be the product of odd primes $\mathfrak{p}$ for which $\Sigma_{k,\mathfrak{p}}$ is* *comprehensively ramified (resp. comprehensively unramified), and let* $\mathfrak{r}_2$ *(resp.* $\mathfrak{u}_2$*) be the product of odd primes for which* $\Sigma_{k,\mathfrak{p}}$ *is selectively ramified (resp. selectively unramified). Then, if* $N_{k,2}(X;C_2;\Sigma_k)$ *denotes the number of quadratic extensions* K/k *such that* $K \in \mathcal{K}(\Sigma_k)$ *with the norm of the relative discriminant bounded by* X*,*

$$N_{k,2}(X;C_2;\Sigma_k) = X\frac{\operatorname{Res}_{s=1}\zeta_k(s)}{\zeta_k(2)}\prod_{\sigma_v|\infty}\left(\sum_{K_v\in\Sigma_{k,v}}\frac{1}{|\mathrm{Aut}(K_v/k_v)|}\right)\prod_{\mathfrak{p}}\left(\left(1+\frac{1}{\mathrm{N}\mathfrak{p}}\right)^{-1}\sum_{K_\mathfrak{p}\in\Sigma_{k,\mathfrak{p}}}\frac{1}{|\mathrm{Aut}(K_\mathfrak{p}/k_\mathfrak{p})|D_{K_\mathfrak{p}/k_\mathfrak{p}}}\right)$$
$$+\,O_{n,\epsilon}\left(\#\mathrm{Cl}_{\mathfrak{m}}(k)[2]\frac{X^{\frac{n+2}{n+4}+\epsilon}|D_k|^{\frac{1}{n+4}+\epsilon}\mathrm{N}\mathfrak{u}_1^{\epsilon}\mathrm{N}\mathfrak{u}_2^{\frac{1}{n+4}+\epsilon}}{\mathrm{N}\mathfrak{r}_1^{\frac{n+2}{n+4}-\epsilon}\mathrm{N}\mathfrak{r}_2^{\frac{n+1}{n+4}-\epsilon}}\right),$$

where $n = [k:\mathbb{Q}]$*,* $|\mathrm{Aut}(K_v/k_v)|$ *denotes the number of automorphisms of* K_v *which fix* k_v*, and* $\mathfrak{m} = \mathfrak{m}_\infty\mathfrak{r}_2\mathfrak{u}_2\prod_{\mathfrak{p}|2}\mathfrak{p}^{2e(\mathfrak{p}|2)}$ *with* $\mathfrak{m}_\infty$ *as the product of real infinite embeddings* σ_v *such that* $\Sigma_{k,v}$ *is not complete at* v *and* $e(\mathfrak{p}|p)$ *is the ramification index for* $\mathfrak{p}$ *over* p*.*

3.1 Setup

As stated earlier, we will use the Dirichlet hyperbola method to derive Theorem 3.0.1. Recall that for the number of divisors function $\tau(n) = \sum_{a|n} 1$, the hyperbola method gives us

$$\sum_{n\leq X}\tau(n) = \sum_{a\leq X^{1/2}}\sum_{b\leq X/a}1 + \sum_{b\leq X^{1/2}}\sum_{a\leq X/b}1 - \sum_{a\leq X^{1/2}}\sum_{b\leq X^{1/2}}1.$$

Though quartic D_4 fields are not as easy to count as the number of divisors of an integer, there are two pieces from [1] that will allow us to use a similar construction.

The first is Theorem 5.3, which counts the number of quartic D_4 fields L up to conductor X with the discriminant of its quadratic subfield K bounded above by X^β for $0 < \beta < 2/3$. We will use $\beta = 1/2$ as suggested by the example above. Because the conductor C_L of a quartic D_4 field $L/\mathbb{Q}$ is

$$C_L = |D_K|\cdot D_{L/K}$$

where K is the quadratic subfield of L, we can extend the metaphor from the example above to count these fields. In the first double sum, counting a up to $X^{1/2}$ will instead be counting quadratic fields $K/\mathbb{Q}$ with $|D_K| < X^{1/2}$ and counting b up to X/a will be counting quadratic extensions L/K with $D_{L/K} < X/|D_K|$.

However, it's not obvious how to replicate the second double sum from the example and first count b and then a. This is where we need the second piece from [1]. Let M denote the Galois closure of $L/\mathbb{Q}$. Then, the second observation is that there is an outer automorphism $\phi \in \mathrm{Aut}(\mathrm{Gal}(M/\mathbb{Q}))$ such that the fixed field of $\phi(\mathrm{Gal}(M/L))$ is not isomorphic to L but has the same conductor as L. They denote this field as $\phi(L)$. Moreover, their Proposition 2.6 implies that if $|D_K| > C_L^{1/2}$ then if $\phi(K)$ is the quadratic subfield of $\phi(L)$, $|D_{\phi(K)}| < C_L^{1/2}$. This means that our equivalent of counting $b \leq X^{1/2}$ will be again to count quadratic fields $K/\mathbb{Q}$ with discriminant bounded by $X^{1/2}$. However, because we are counting isomorphism classes of quartic D_4 fields, we will end up multiplying our result by $1/2$ to account for pairs of fields L/K and L'/K that are both quartic D_4 fields over $\mathbb{Q}$ and are non-isomorphic over K, but are isomorphic over $\mathbb{Q}$.

To complete the metaphor, we need an equivalent of the third double sum. In the original problem, this counts the pairs (a, b) which were counted by both the first and second double sums. However, Proposition 2.6 actually implies a little more. It shows that $D_{L/K} = |D_{\phi(K)}|d^2 2^n$ for some squarefree, odd integer d and some integer n. The number d is, in fact, the product of primes p at which L has central inertia. We will also show later on that n must be a non-negative even integer. For convenience, we will say $q = 2^i d$. Thus, in our problem, we have to be careful how we set up this count because the relationship $D_{L/K} = |D_{\phi(K)}|q^2$ complicates which pairs (K, L) get counted multiple times. We will accomplish this by fixing $q < X^{1/4}$ and considering the quartic fields $L/\mathbb{Q}$ such that $D_{L/K}/|D_{\phi(K)}|$ is exactly q^2 and then summing over all possible q. [1] refers to $D_{L/K}/|D_{\phi(K)}|$ as $J(L)$, which we will also use here. For a specific pair (K, L), this leads us to two possibilities. If $|D_K| < X^{1/2}/q^2$, then the pair will be double counted if $D_{L/K} < X^{1/2}q^2$. But if $X^{1/2}/q^2 \leq |D_K| < X^{1/2}$, then the pair is double counted if $D_{L/K} < X/|D_K|$.

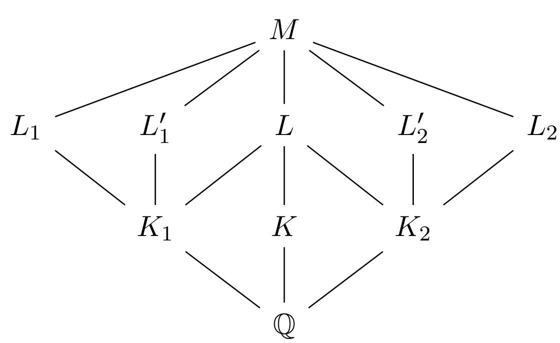
With this, we have finished our analogy to the original Dirichlet hyperbola method. So, the sum we want to analyze which counts quartic D_4 fields by conductor is

$$\sum_{\substack{[K:\mathbb{Q}]=2 \\ |D_K|<X^{1/2}}} \sum_{\substack{[L:K]=2 \\ D_{L/K}<X/|D_K|}} 1 - \frac{1}{2} \sum_{q<X^{1/4}} \left(\sum_{\substack{[K:\mathbb{Q}]=2 \\ |D_K|<X^{1/2}/q^2}} \sum_{\substack{[L:K]=2 \\ D_{L/K}<X^{1/2}q^2 \\ J(L)=q^2}} 1 + \sum_{\substack{[K:\mathbb{Q}]=2 \\ X^{1/2}/q^2 \le |D_K|<X^{1/2}}} \sum_{\substack{[L:K]=2 \\ D_{L/K}<X/|D_K| \\ J(L)=q^2}} 1 \right). \tag{3.1}$$

In Section 3, we will prove the relationship $J(L) = q^2$ more generally and discuss the possibilities for the valuation of q at 2. In Section 4, we will prove a theorem similar to Theorem 1.1 from [12] which will give us Theorem 3.0.3 for counting quadratic extensions K/k with local specifications. Finally, in Section 5, we will prove Theorems 3.0.1 and 3.0.2.

3.2 The Flipped Field

Going forward, for a quartic D_4 field $L/\mathbb{Q}$ with quadratic subfield K, we will call $\phi(K)$ the *flipped field*. If we let, L_1 be a D_4 field over $\mathbb{Q}$ and M be its normal closure, then in the subfield diagram below, K_2 is the flipped field with $\phi(L_1) = L_2$. L_1' and L_2' are the conjugate fields of L_1 and L_2, respectively.



The authors of [1] prove that the p-part of $J(L_1) = D_{L_1/K_1}/D_{K_2}$ (or $J_p(L_1)$) is either p^2 or 1 for odd primes p by examining the table of possible decomposition and inertia subgroups of D_4 for p and showing that $J_p(L_1) = p^2$ under a certain condition. We will prove this from a different perspective in the lemma below which will also allow us to show that $J_2(L_1)$ is a square.

Lemma 3.2.1 *Let k be a number field and L_1/k be a quartic D_4 extension of k. If K_1 is the quadratic subfield of L_1 and K_2 is the flipped field of L_1, then there exists an element $\alpha \in K_1$ such that $L_1 = K_1(\sqrt{\alpha})$ and $K_2 = k(\sqrt{\mathrm{N}_{K_1/k}(\alpha)})$.*

Proof: Because L_1/k is quartic with Galois closure D_4, we know that $L = k(\theta)$ for some θ with minimal polynomial $f(x) = x^4 + Ax^2 + B \in k[x]$ from Theorem 4.1 of [13]. Examining the proof of the theorem, we see that $K_1 = k(\theta^2)$ with $\theta^2 = (-A \pm \sqrt{A^2 - 4B})/2$ and $A^2 - 4B \neq \square \in k$. Without loss of generality, we can take $\alpha = (-A + \sqrt{A^2 - 4B})/2$ and $L = K(\sqrt{\alpha})$. We let $\bar{\beta} = (-A - \sqrt{A^2 - 4B})/2$. So, the complete set of roots for $f(x) = \{\pm\sqrt{\alpha}, \pm\sqrt{\bar{\beta}}\}$.

Now, from Theorem 1.2 and the proof of Theorem 3.14 in [13], we know that disc f is not a square in k and $K_2 = k(\sqrt{\mathrm{disc} f})$. But $\mathrm{disc} f = \prod_{i<j}(r_i - r_j)^2$ where r_i are the roots of $f(x)$. For convenience, lets say $r_1 = \sqrt{\alpha}$, $r_2 = -r_1$, $r_3 = \sqrt{\bar{\beta}}$, and $r_4 = -r_3$. Then, this product is

$$\begin{aligned}
\mathrm{disc} f &= 16 r_1^2 (r_1 - r_3)^4 (r_1 + r_3)^4 r_3^2 \\
&= 16 r_1^2 r_3^2 \left((r_1 - r_3)(r_1 + r_3)\right)^4 \\
&= 16 \cdot \mathrm{N}_{K_1/k}(\alpha) \cdot (r_1^2 - r_3^2)^4.
\end{aligned}$$

But $(r_1^2 - r_3^2)^4 = (A^2 - 4B)^2$, which is a square in k. Thus, $K_2 \cong k(\sqrt{\mathrm{N}_{K_1/k}(\alpha)})$. □

With this lemma, we can make the more general claim:

Lemma 3.2.2 *Let k be a number field and L_1/k be a quartic D_4 extension of k. If K_1 is the quadratic subfield of L_1 and K_2 is the flipped field of L_1, then $\mathrm{N}_{K_1/k}\mathfrak{d}_{L_1/K_1} = \mathfrak{d}_{K_2/k}\mathfrak{q}^2$ for some integral ideal $\mathfrak{q}$ of $\mathcal{O}_k$.*

Proof: To prove this statement, we will use the work of Cohen, Diaz y Diaz, and Olivier [12]. Their Proposition 3.4 states that if $L_1 = K_1(\sqrt{\alpha})$ as in Lemma 3.2.1, then $\mathfrak{d}_{L_1/K_1} = 4\mathfrak{a}/\mathfrak{c}^2$ where $\mathfrak{a}$ is the largest squarefree ideal dividing $\alpha\mathcal{O}_K$ and $\mathfrak{c}$ is the largest ideal dividing 2 such that $(\mathfrak{a}, \mathfrak{c}) = 1$ and $x^2 \equiv \alpha \pmod{^*\mathfrak{c}^2}$ has a solution. Here,

$x \equiv y \pmod{^*\mathfrak{a}}$ has the standard meaning from class field theory that $v_\mathfrak{p}(x-y) \geq v_\mathfrak{p}(\mathfrak{a})$ for every $\mathfrak{p}$ dividing $\mathfrak{a}$.

For any odd prime $\mathfrak{p}$ of $\mathcal{O}_k$, Proposition 3.4 and Lemma 3.2.1 together imply $v_\mathfrak{p}(\mathrm{N}_{K_1/k}\mathfrak{d}_{L_1/K_1}) \equiv v_\mathfrak{p}(\mathfrak{d}_{K_2/k}) \mod 2$ and $v_\mathfrak{p}(\mathrm{N}_{K_1/k}\mathfrak{d}_{L_1/K_1}) \geq v_\mathfrak{p}(\mathfrak{d}_{K_2/k})$. So, we need to consider the behavior at primes dividing 2.

As implied by the proof of Proposition 3.4 in [12], for any $\mathfrak{p} \mid 2, v_\mathfrak{p}(\mathfrak{d}_{K_2/k})$ is odd if any only if $\mathfrak{p}$ divides the squarefree part of $\mathrm{N}_{K_1/k}(\alpha)$. So, we have $v_\mathfrak{p}(\mathrm{N}_{K_1/k}\mathfrak{d}_{L_1/K_1}) \equiv v_\mathfrak{p}(\mathfrak{d}_{K_2/k}) \mod 2$. Moreover, if $v_\mathfrak{p}(\mathfrak{d}_{K_2/k})$ is odd, we also have $v_\mathfrak{p}(\mathrm{N}_{K_1/k}\mathfrak{d}_{L_1/K_1}) \geq v_\mathfrak{p}(\mathfrak{d}_{K_2/k})$ because $v_\mathfrak{p}(\mathrm{N}_{K_1/k}\mathfrak{d}_{L_1/K_1}) = 2e(\mathfrak{P}|\mathfrak{p})e(\mathfrak{p}|2) + 1$ for some prime $\mathfrak{P}$ lying over $\mathfrak{p}$ in $\mathcal{O}_{K_1}$ and $v_\mathfrak{p}(\mathfrak{d}_{K_2/k}) = 2e(\mathfrak{p}|2) + 1$.

Assume $v_\mathfrak{p}(\mathfrak{d}_{K_2/k})$ is even. By Proposition 3.4, we know that $v_\mathfrak{p}(\mathfrak{d}_{K_2/k}) = 2(e-m)$ where $e = e(\mathfrak{p} \mid 2)$ and $0 \leq m \leq e$ such that $\mathrm{N}_{K_1/k}(\alpha)$ is a square mod $\mathfrak{p}^{2m}$ but not mod $\mathfrak{p}^{2(m+1)}$ (except if $m = e$ in which case $\mathfrak{p}$ does not ramify in K_2). To show that $v_\mathfrak{p}(\mathrm{N}_{K_1/k}\mathfrak{d}_{L_1/K_1}) \geq v_\mathfrak{p}(\mathfrak{d}_{K_2/k})$, it will be enough to show that for any $\alpha \in K_1$ and $\mathcal{O}_k$-ideal $\mathfrak{c}$ if $\mathrm{N}_{K_1/k}(\alpha)$ is not a square mod $\mathfrak{c}$, then α is not a square mod $\mathfrak{c}\mathcal{O}_{K_1}$. We will do this by proving the contrapositive.

Assume $x^2 \equiv \alpha \pmod{^*\mathfrak{c}\mathcal{O}_{K_1}}$, so $\alpha = x^2 + c$ for some $c \in \mathfrak{c}\mathcal{O}_{K_1}$. Now, because K_1/k is quadratic, then $K_1 = k(\sqrt{\beta})$ for some $\beta \in k^\times \smallsetminus k^{\times 2}$ and $x = x_1 + x_2\sqrt{\beta}, c = c_1 + c_2\sqrt{\beta}$ for some $x_1, x_2, c_1, c_2 \in k$. Thus

$$\begin{aligned}
\mathrm{N}_{K_1/k}(\alpha) &= \mathrm{N}_{K_1/k}(x^2 + c) \\
&= (x_1^2 + x_2^2\beta + c_1)^2 - (2x_1x_2 + c_2)^2\beta \\
&= \mathrm{N}_{K_1/k}(x^2) + \mathrm{N}_{K_1/k}(c) + 2(x_1^2 + x_2^2\beta)c_1 - 4x_1x_2c_2\beta \\
&= \mathrm{N}_{K_1/k}(x^2) + \mathrm{N}_{K_1/k}(c) + \mathrm{Tr}_{K_1/k}(\bar{x}^2c) \\
&\equiv \mathrm{N}_{K_1/k}(x^2) \pmod{^*\mathfrak{c}}.
\end{aligned}$$

For the last two lines $\bar{x} = x_1 - x_2\sqrt{\beta}$ and we have $\mathrm{Tr}_{K_1/k}(\bar{x}^2c) \in \mathfrak{c}$ because $\bar{x}^2c \in \mathfrak{c}\mathcal{O}_{K_1}$ and K_1/k is Galois. □

Now, we can see that when $k = \mathbb{Q}$, the possible values for $J_2(L_1)$ are of the form

2^{2i} for $i = 0, 1, 2, 3$. But, we still don't have a way to count quartic D_4 fields where $J_2(L_1) = 2^{2i}$. For this we will need to think locally.

3.2.1 Local Fields and the Flipped Field

Let $L/\mathbb{Q}$ and $L'/\mathbb{Q}$ be non-isomorphic quartic D_4 fields such that L and L' have the same local conditions at 2. Ideally, we would have $J_2(L) = J_2(L')$, but since $J(L) = D_{L/K}/D_{\phi(K)}$, this would require that $\phi(K)$ and $\phi(K')$ have the same local conditions at 2. Fortunately, this is implied by the following lemma.

Lemma 3.2.3 *Let k be a number field, $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_k$, and L/k and L'/k be two non-isomorphic D_4 quartic extensions such that $L \otimes_k k_\mathfrak{p} \cong L' \otimes_k k_\mathfrak{p}$. Then, $\phi(K) \otimes_k k_\mathfrak{p} \cong \phi(K') \otimes_k k_\mathfrak{p}$.*

Before proving the lemma, let's consider a simpler case. If we have two quadratic extensions $K = k(\sqrt{\alpha})$ and $K' = k(\sqrt{\alpha'})$ and some prime ideal $\mathfrak{p}$ of $\mathcal{O}_k$, then $K \otimes_k k_\mathfrak{p} \cong K' \otimes_k k_\mathfrak{p}$ if and only if α and α' are in the same class of $k_\mathfrak{p}^\times / k_\mathfrak{p}^{\times 2}$. We will use this idea in the proof.

Proof: If K and K' are the quadratic subfields of L and L', respectively, then we know that

$$K \otimes_k k_\mathfrak{p} \cong K' \otimes_k k_\mathfrak{p} \cong \prod_{\substack{\mathfrak{P} \subset \mathcal{O}_K \\ \mathfrak{P} | \mathfrak{p}}} K_\mathfrak{P}.$$

Assume $L = K(\sqrt{\beta})$ and $L' = K'(\sqrt{\beta'})$ for some $\beta \in K$ and $\beta' \in K'$. Let $\Phi_K, \Phi_{K'}$ be the isomorphisms from $K \otimes_k k_\mathfrak{p}$ and $K' \otimes_k k_\mathfrak{p}$ to $\prod K_\mathfrak{P}$, and $\Phi_{K,\mathfrak{P}}, \Phi_{K',\mathfrak{P}}$ be the restriction maps to $K_\mathfrak{P}$. Then, because $L \otimes_k k_\mathfrak{p} \cong L' \otimes_k k_\mathfrak{p}$, we must have for each $\mathfrak{P}$ that $\Phi_{K,\mathfrak{P}}(\beta) = \Phi_{K',\mathfrak{P}}(\beta')a^2$ for some $a \in K_\mathfrak{P}$. So $\Phi_K(\beta) = \Phi_{K'}(\beta)'\bar{a}^2$ for some $\bar{a} \in \prod K_\mathfrak{P}$. Thus $N_{K \otimes_k k_\mathfrak{p}/k_\mathfrak{p}}(\beta) = N_{K' \otimes_k k_\mathfrak{p}/k_\mathfrak{p}}(\beta')b^2$ for some $b \in k_\mathfrak{p}$. □

With this lemma, we know that $J_2(L) = J_2(L')$ whenever L and L' share the same local conditions at 2 Thus, we can compute the weights

$$\mu(\Sigma_{2^{2i}}) = \sum_{\substack{(L_2, K_2) \\ J_2(L) = 2^{2i}}} \frac{1}{|\mathrm{Aut}(L_2, K_2)| C(L_2, K_2)}.$$

To get the correct values for each $\mu(\Sigma_{2^{2i}})$ later on we will use some tables computed using code found at https://github.com/friedrichsenm/d4_by_conductor. These tables are organized by the congruence conditions on D_K corresponding to different isomorphism classes for degree 2 étlae algebras over $\mathbb{Q}_2$. Though there are 8 different isomorphism classes to consider, we found that these can be reduced to 4 cases. Tables 3.3 and 3.4 are computed by adding together the results for all isomorphism classes of $K/\mathbb{Q}$ that reduce to the same congruence conditions on D_K.

Also, as $J_2(L)$ can be found by taking $v_2(D_{L/K}) - v_2(D_{\phi(K)})$, the entries of each table are organized by the different possibilities for $v_2(D_{L/K})$ and $v_2(D_{\phi(K)})$. So, each entry is the weight given by

$$\sum_{\substack{(L_2,K_2)\\ v_2(D_{L/K})=i \\ v_2(D_{\phi(K)})=j}}^{*} \frac{1}{|\mathrm{Aut}(L_2,K_2)|C(L_2,K_2)},$$

where the $\sum^*$ indicates that the sum is over a fixed congruence condition on D_K.

	$v_2(D_{\phi(K)})$ =0	2	3
$v_2(D_{L/K})$ =0	1/2	0	0
2	0	1/4	0
3	0	0	1/4
4	1/32	0	0
5	0	0	1/16
6	1/64	1/64	0

Table 3.1: Weights of $v_2(D_{L/K})$ vs $v_2(D_{\phi(K)})$ when $D_K \equiv 1 \bmod 8$

	$v_2(D_{\phi(K)})$ =0	2
$v_2(D_{L/K})$ =0	1/2	0
4	1/32	1/16
6	1/64	1/64

Table 3.2: Weights of $v_2(D_{L/K})$ vs $v_2(D_{\phi(K)})$ when $D_K \equiv 5 \bmod 8$

	$v_2(D_{\phi(K)})$ =0	3
$v_2(D_{L/K})$ =0	1/4	0
2	1/16	0
4	1/32	0
5	0	1/32

Table 3.3: Weights of $v_2(D_{L/K})$ vs $v_2(D_{\phi(K)})$ when $D_K \equiv 4 \bmod 8$

	$v_2(D_{\phi(K)})$ =0	2	3
$v_2(D_{L/K})$ =0	1/4	0	0
2	1/16	0	0
4	0	1/32	0
5	0	0	1/32

Table 3.4: Weights of $v_2(D_{L/K})$ vs $v_2(D_{\phi(K)})$ when $D_K \equiv 0 \bmod 8$

3.3 Counting Quadratic Fields with Local Conditions

As alluded to earlier on, we need to prove that the weights calculated using the mass formula match with weights when counting global fields L/K that match the local conditions. To do this we will prove a theorem in the vein of Theorem 1.1 from [12] that will allow us to single out specific local conditions at 2 we wish to include. Similar to [12], we let

$$\Phi_{k,2}(C_2,s) = \sum_{[K:k]=2} \frac{1}{D_{K/k}^s}.$$

Then, we have the following theorem.

Theorem 3.3.1 *Let k be a number field, $\mathfrak{n}$ be the maximal squarefree ideal divisor of 2 and $\mathfrak{m} = \prod_{\mathfrak{p}|2} \mathfrak{p}^{2e(\mathfrak{p}|2)+1}$. For each $\mathfrak{p} \mid 2$, select a uniformizer $\pi_{\mathfrak{p}} \in \mathcal{O}_k$ such that $\pi_{\mathfrak{p}} \equiv 1 \pmod{{}^*\mathfrak{q}}$ for every $\mathfrak{q} \mid 2$ where $\mathfrak{p} \neq \mathfrak{q}$. Then, the Dirichlet series $\Phi_{k,2}(C_2,s)$ is*

$$\Phi_{k,2}(C_2,s) = -1+\frac{1}{2^{g+i(k)}\zeta_k(2s)} \prod_{\mathfrak{p}|2} \left(1-\mathrm{N}\mathfrak{p}^{-2s}\right)^{-1} \sum_{\mathfrak{c}|\mathfrak{n}} \sum_{\bar{\beta}\in\mathcal{O}_{k,\mathfrak{m}}/\mathcal{O}_{k,\mathfrak{m}}^2} D_2(\pi_{\mathfrak{c}}\beta)^{-s} \sum_{\chi\in\mathrm{Cl}_{\mathfrak{m}}^2(\mathrm{k})} \chi(\pi_{\mathfrak{c}}^{-1}\beta^{-1}\mathfrak{c})L_k(s,\chi),$$

where g is the number of prime ideals in $\mathcal{O}_k$ dividing 2, $\mathcal{O}_{k,\mathfrak{m}} = (\mathcal{O}_k/\mathfrak{m})^\times$, $D_2(x) = \prod_{\mathfrak{p}|2} D_{k_\mathfrak{p}(\sqrt{x})/k_\mathfrak{p}}$, and $\pi_\mathfrak{c} = \prod_{\mathfrak{p}|\mathfrak{c}} \pi_\mathfrak{p}$, and β is a lift of $\bar{\beta}$ to $\mathcal{O}_{k,\mathfrak{m}}$.

In order to prove the theorem, we will use many of the same objects as in [12]. We will recall some of their definitions here:

- An element $u \in k^\times$ is a *virtual unit* if there exists an ideal $\mathfrak{q}$ such that $u\mathcal{O}_k = \mathfrak{q}^2$. It is clear that the set of virtual units $V(k)$ is a group.
- We will call the quotient group $S(k) = V(k)/k^{\times 2}$ the *Selmer group* of k.
- Let $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ be a modulus of k. The *ray Selmer group modulo* $\mathfrak{m}$ is the subgroup $S_\mathfrak{m}(k)$ of $S(k)$ of elements $\bar{u}$ such that for some lift u of $\bar{u}$ coprime to $\mathfrak{m}_0$ there exists a solution to $x^2 \equiv u \pmod{^*\mathfrak{m}_0}$ and for each real infinite prime $\sigma \mid \mathfrak{m}_\infty$ we have $\sigma(u) > 0$.

Note that this last definition is different from the one in [12] and we will want to reprove some results using this modified definiton. First, a modified version of Lemma 3.5 from [12]:

Lemma 3.3.2 *Let $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ be a modulus of k, and let $\mathfrak{a}$ be an integral ideal coprime to $\mathfrak{m}_0$ such that there exists an ideal $\mathfrak{q}$ also coprime to $\mathfrak{m}_0$ with $\mathfrak{a}\mathfrak{q}^2 = \alpha_0\mathcal{O}_k$. The following two conditions are equivalent.*

1. *There exists an element $\bar{u}$ of $S(k)$ such that, for any lift u of $\bar{u}$ coprime to $\mathfrak{m}_0$, the congruence $x^2 \equiv \alpha_0 u \pmod{^*\mathfrak{m}_0}$ has a solution and $\sigma(\alpha_0 u) > 0$ for every $\sigma \mid \mathfrak{m}_\infty$.*
2. *The class of $\mathfrak{a}$ is a square in the ray class group $\mathrm{Cl}_\mathfrak{m}(k)$.*

Proof: The proof will largely follow the proof of Lemma 3.5 in [12] with a few changes. Assume (1). Then $x^2 = \alpha_0 u\beta$ with $\beta \equiv 1 \pmod{^*\mathfrak{m}}$ and $\sigma(\beta) > 0$ for every $\sigma \mid \mathfrak{m}_\infty$. The rest of this direction of the proof is the same as in the cited proof.

Now, assume (2). The only part of this direction of the proof that is different is noting that $\sigma(\beta') > 0$ for every $\sigma \mid \mathfrak{m}_\infty$ and that because $\alpha_0 u = \beta'$, then $\sigma(\alpha_0 u) > 0$ for every $\sigma \mid \mathfrak{m}_\infty$. □

Next an equivalent of Lemma 3.7 from the same paper.

Lemma 3.3.3 *Let $\mathfrak{m}$ be a modulus as before and for notational simplicity, let $\mathcal{O}_{k,\mathfrak{m}} = (\mathcal{O}_k/\mathfrak{m}_0)^\times \times \{\pm 1\}^{|\mathfrak{m}_\infty|}$. Then, the following sequence is exact.*

$$1 \longrightarrow S_{\mathfrak{m}}(k) \longrightarrow S(k) \longrightarrow \mathcal{O}_{k,\mathfrak{m}}/\mathcal{O}_{k,\mathfrak{m}}^2 \longrightarrow \mathrm{Cl}_{\mathfrak{m}}(k)/\mathrm{Cl}_{\mathfrak{m}}(k)^2 \longrightarrow \mathrm{Cl}(k)/\mathrm{Cl}(k)^2 \longrightarrow 1.$$

Proof: The proof for this lemma is the same except to note that the element β used in the proof will also be positive for every $\sigma \mid \mathfrak{m}_\infty$. □

We will also be concerned with the cardinality of $S_{\mathfrak{m}}(k)$. But, there is not much for us to prove here. Like in [12],

$$|S_{\mathfrak{m}}(k)| = \frac{2^{r_u(k)+1+r_2(\mathrm{Cl}_{\mathfrak{m}}(k))}}{|\mathcal{O}_{k,\mathfrak{m}}/\mathcal{O}_{k,\mathfrak{m}}^2|},$$

where $r_u(k)$ is the rank of the unit group of k and $r_2(\mathrm{Cl}_{\mathfrak{m}}(k))$ is the 2-rank of the ray class group of k with modulus $\mathfrak{m}$.

Before proving Theorem 3.3.1, we will discuss the differences between our proof and the proof of Theorem 1.1 in [12]. Lemma 3.3 from [12] shows that quadratic extensions of any number field k are in bijection with pairs $(\mathfrak{a}, \bar{u})$ where $\mathfrak{a}$ is an integral, squarefree ideal with certain other conditions and $\bar{u}$ is a class in the $S(k)$. To construct $\Phi_{k,2}(C_2, s)$, they sum over integral, squarefree ideals $\mathfrak{a}$ with the appropriate conditions then sum over classes of $S(k)$ to pick up all pairs $(\mathfrak{a}, \bar{u})$. To handle ramification at 2, they look at all $\mathfrak{c} \mid 2$ and use the subgroup $S_{\mathfrak{c}^2}(k)$ to determine how many classes in $S(k)$ correspond to extensions with relative discriminant $\mathfrak{d}_{K,k} = 4\mathfrak{a}/\mathfrak{c}^2$.

In our proof we will construct the Dirichlet series by using the pairs $(\mathfrak{a}, \bar{u})$. However, because we are concerned with every class of $k_{\mathfrak{p}}^\times/k_{\mathfrak{p}}^{\times 2}$ for every $\mathfrak{p} \mid 2$, we will handle ramification differently. As such, we will use a different modulus $\mathfrak{m}$ to set up our subgroup $S_{\mathfrak{m}}(k)$. Because every element of $k_{\mathfrak{p}}$ can be written as $\pi^i u$ where π is the uniformizer, $i \in \mathbb{Z}$, and $u \in \mathcal{O}_{k_{\mathfrak{p}}}$, then we see that $k_{\mathfrak{p}}^\times/k_{\mathfrak{p}}^{\times 2} \cong \{\pm 1\} \times \mathcal{O}_{k_{\mathfrak{p}}}^\times/\mathcal{O}_{k_{\mathfrak{p}}}^{\times 2}$. Moreover, for any $\mathfrak{p} \mid 2$, $\mathcal{O}_{k_{\mathfrak{p}}}^\times/\mathcal{O}_{k_{\mathfrak{p}}}^{\times 2} \cong (\mathcal{O}_k/\mathfrak{p}^{2e(\mathfrak{p}|2)+1})^\times/(\mathcal{O}_k/\mathfrak{p}^{2e(\mathfrak{p}|2)+1})^{\times 2}$. Thus the modulus we want is $\mathfrak{m} = \prod_{\mathfrak{p}|2} \mathfrak{p}^{2e(\mathfrak{p}|2)+1}$ and the complete set of local conditions can be represented globally by $\{(\pi_{\mathfrak{c}}, \bar{\beta}) \mid \pi_{\mathfrak{c}} = \prod_{\mathfrak{p}|\mathfrak{c}} \pi_{\mathfrak{p}}, \bar{\beta} \in \mathcal{O}_{k,\mathfrak{m}}/\mathcal{O}_{k,\mathfrak{m}}^2\}$, where $\mathfrak{c}$ is an ideal dividing $\mathfrak{n}$ as in the statement of Theorem 3.3.1. With this in mind, we are ready to prove the theorem.

Proof (Theorem 3.3.1): Cohen, Diaz y Diaz, and Olivier start their proof of Theorem 1.1 with a sum over all squarefree $\mathfrak{a} \subset \mathcal{O}_k$ such that there exists $\mathfrak{q} \subset \mathcal{O}_k$ where $\mathfrak{a}\mathfrak{q}^2$ is principal. Because we will be manually handling cases where $\pi_{\mathfrak{c}} \neq 1$ we will instead start with a sum over $\mathfrak{c} \mid \mathfrak{n}$, where $\mathfrak{n} = \prod_{p|2} \mathfrak{p}$ and require that there exist a $\mathfrak{q} \subset \mathcal{O}_k$ such that $\mathfrak{c}\mathfrak{a}\mathfrak{q}^2$ is principal and $(\mathfrak{a}, 2) = 1$ So, we start with

$$\Phi_{k,2}(C_2, s) = -1 + \sum_{\mathfrak{c}|\mathfrak{n}} \sum_{\substack{\mathfrak{a}\ \square\text{-free} \\ \exists \mathfrak{q}, \mathfrak{c}\mathfrak{a}\mathfrak{q}^2 = \alpha_0 \mathcal{O}_k \\ (\mathfrak{a},2)=1}} \mathrm{N}\mathfrak{a}^{-s} S(\alpha_0, \mathfrak{a}, \mathfrak{c})$$

with

$$S(\alpha_0, \mathfrak{a}, \mathfrak{c}) = \sum_{\bar{u} \in S(k)} D_2(\alpha_0 u)^{-s}.$$

Since we want to count by the classes of $k_{\mathfrak{p}}^{\times}/k_{\mathfrak{p}}^{\times 2}$, we use the correspondence between $\alpha_0 u$ and $(\pi_{\mathfrak{c}}, \bar{\beta})$ and rewrite the above sum as

$$S(\alpha_0, \mathfrak{a}, \mathfrak{c}) = \sum_{\bar{\beta} \in \mathcal{O}_{k,\mathfrak{m}}/\mathcal{O}_{k,\mathfrak{m}}^2} D_2(\pi_{\mathfrak{c}}\beta)^{-s} f(\bar{\beta}, \mathfrak{a}, \mathfrak{c})$$

where β is some lift of $\bar{\beta}$ to $\mathcal{O}_{k,\mathfrak{m}}$ and

$$f(\bar{\beta}, \mathfrak{a}, \mathfrak{c}) = \sum_{\substack{\bar{u} \in S(k) \\ \overline{\pi_{\mathfrak{c}}^{-1}\alpha_0 u} = \bar{\beta}}} 1.$$

We use $\overline{\pi_{\mathfrak{c}}^{-1}\alpha_0 u} = \bar{\beta}$ to mean that the class of $\pi_{\mathfrak{c}}^{-1}\alpha_0 u$ in $\mathcal{O}_{k,\mathfrak{m}}/\mathcal{O}_{k,\mathfrak{m}}^2$ is $\bar{\beta}$. This is equivalent to there being a solution to $x^2 \equiv \pi_{\mathfrak{c}}^{-1}\beta^{-1}\alpha_0 u \pmod{^*\mathfrak{m}}$. With Lemma 3.3.2, this is the same as saying $\pi_{\mathfrak{c}}^{-1}\beta^{-1}\mathfrak{c}\mathfrak{a}$ is a square in $\mathrm{Cl}_{\mathfrak{m}}(k)$. Now, Lemma 3.10 from [12] says that $f(\bar{\beta}, \mathfrak{a}, \mathfrak{c}) = 0$ if $\pi_{\mathfrak{c}}^{-1}\beta^{-1}\mathfrak{c}\mathfrak{a}$ is not a square in $\mathrm{Cl}_{\mathfrak{m}}(k)$ and $|S_{\mathfrak{m}}(k)|$ if it is. Theorem 2.36 from [11] implies that $|\mathcal{O}_{k,\mathfrak{m}}/\mathcal{O}_{k,\mathfrak{m}}^2| = \prod_{\mathfrak{p}|2} 2 \cdot \mathrm{N}\mathfrak{p}^{2(e|\mathfrak{p})}$. Adding this in to the cardinality of $S_{\mathfrak{m}}(k)$, we get

$$|S_{\mathfrak{m}}(k)| = \frac{2^{r_u(k)+1+r_2(\mathrm{Cl}_{\mathfrak{m}}(k))}}{\prod_{\mathfrak{p}|2}(2\cdot \mathrm{N}\mathfrak{p}^{e(\mathfrak{p}|2)})} = \frac{2^{r_u(k)+1+r_2(\mathrm{Cl}_{\mathfrak{m}}(k))}}{2^{g+[k:\mathbb{Q}]}} = \frac{2^{r_2(\mathrm{Cl}_{\mathfrak{m}}(k))}}{2^{g+i(k)}}.$$

Like in [12] we will use orthogonality and sum over the quadratic characters of $\mathrm{Cl}_{\mathfrak{m}}(k)$ to pick out the ideals that are squares of classes. So we have

$$\begin{aligned}\Phi_{k,2}(C_2,s) &= -1 + \sum_{\mathfrak{c}|\mathfrak{n}} \sum_{\substack{\mathfrak{a}\ \square\text{-free} \\ \exists \mathfrak{q}, \mathfrak{c}\mathfrak{a}\mathfrak{q}^2=\alpha_0\mathcal{O}_k \\ (\mathfrak{a},2)=1}} \frac{S(\alpha_0,\mathfrak{a},\mathfrak{c})}{\mathrm{N}\mathfrak{a}^s} \\ &= -1 + \sum_{\mathfrak{c}|\mathfrak{n}} \sum_{\bar\beta\in\mathcal{O}_{k,\mathfrak{m}}/\mathcal{O}_{k,\mathfrak{m}}^2} \frac{|S_{\mathfrak{m}}(k)|}{D_2(\pi_{\mathfrak{c}}\bar\beta)^s} \frac{1}{2^{r_2(\mathrm{Cl}_{\mathfrak{m}}(k))}} \sum_{\chi} \sum_{\substack{\mathfrak{a}\ \square\text{-free} \\ (\mathfrak{a},2)=1}} \frac{\chi(\pi_{\mathfrak{c}}^{-1}\beta^{-1}\mathfrak{c}\mathfrak{a})}{\mathrm{N}\mathfrak{a}^s} \\ &= -1 + \frac{1}{2^{g+i(k)}} \sum_{\mathfrak{c}|\mathfrak{n}} \sum_{\bar\beta\in\mathcal{O}_{k,\mathfrak{m}}/\mathcal{O}_{k,\mathfrak{m}}^2} \frac{1}{D_2(\pi_{\mathfrak{c}}\bar\beta)^s} \sum_{\chi} \chi(\pi_{\mathfrak{c}}^{-1}\beta^{-1}\mathfrak{c}) \sum_{\substack{\mathfrak{a}\ \square\text{-free} \\ (\mathfrak{a},2)=1}} \frac{\chi(\mathfrak{a})}{\mathrm{N}\mathfrak{a}^s}.\end{aligned}$$

At this point, the next few steps are identical to the end of the proof for Theorem 1.1 in [12] with

$$\sum_{\substack{\mathfrak{a}\ \square\text{-free} \\ (\mathfrak{a},2)=1}} \frac{\chi(\mathfrak{a})}{\mathrm{N}\mathfrak{a}^s} = \frac{L_k(s,\chi)}{\zeta_k(2s)\prod_{\mathfrak{p}|2}(1-\mathrm{N}\mathfrak{p}^{-2s})},$$

thus proving the theorem. □

If we let $N_{k,C_2}(X)$ stand for the number of quadratic extensions K/k with $D_{K/k} \le X$, then one may use contour integration on our Dirichlet series from Theorem 3.3.1 to get the same result as their Corollary 1.2. To limit the count to only quadratic fields K/k with a specific local condition at 2, simply limit the sum to the set of $(\pi_{\mathfrak{c}}\bar\beta)$ in question. But, we can be more general than this and consider local specifications for other places of k.

Recalling our definition for an acceptable collection of local specifications Σ_k, let $S(\Sigma_k) = \{v \mid 2\} \cup \{v \text{ s.t. } \Sigma_{k,v} \text{ doesn't contain every degree 2 étale algebra of } k_v\}$. We assume that $\Sigma_{k,v}$ contains every degree 2 étale algebra when v is a complex infinite place as there is only one. This set contains all of the places with local information we need to write out $\Phi_{k,2}(\Sigma_k; C_2, s)$ with full detail. Each $K_v \in \Sigma_{k,v}$ corresponds to a class of $(\mathcal{O}_{k_v}/(\pi_v))/(\mathcal{O}_{k_v}/(\pi_v))^2$ for finite places and $\sigma_v(x) > 0$ or < 0 where $K_v = k_v(\sqrt{x})$ for the real infinite places. Using the weak approximation theorem, this extends to a set B containing elements of the form $(\pi, \bar{\beta})$ where π is a product (potentially empty) of uniformizers $\pi_v \in k_v$ for finite $v \in S(\Sigma_k)$ and $\bar{\beta} \in \mathcal{O}_{k,\mathfrak{m}}/\mathcal{O}_{k,\mathfrak{m}}^2$ for a modulus $\mathfrak{m}$ with $\mathfrak{m}_0 = \prod_{\mathfrak{p}|2} \mathfrak{p}^{2e+1} \prod_{\substack{v \text{ odd} \\ v \in S(\Sigma_k)}} \mathfrak{p}_v$ and $\mathfrak{m}_\infty = \prod_{\substack{v \text{ real} \\ v \in S(\Sigma_k)}} \sigma_v$. We require that each $\pi_\mathfrak{p}$ be $1 \pmod{^*q}$ for every other $\mathfrak{q} \mid \mathfrak{m}_0$ and $\sigma_v(\pi_\mathfrak{p}) > 0$ for every $\sigma_v \mid \mathfrak{m}_\infty$. We will write these elements as tuples $(\pi_\mathfrak{c}, \bar{\beta}) \in B$ where $\mathfrak{c}$ is some squarefree ideal divisor of $\mathfrak{m}_0$ and $\pi_\mathfrak{c}$ is defined as it was earlier.

Theorem 3.3.4 *Let k be a number field, Σ_k be an acceptable collection of local specifications for k, and B be the corresponding set of global conditions for $K \in \mathcal{K}(\Sigma_k)$. Let $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ be the corresponding modulus. Then,*

$$\Phi_{k,2}(\Sigma_k; C_2, s) = -\delta_{(1,\bar{1}) \in B} + \frac{1}{2^{|S(\Sigma_k)|+i(k)}\zeta_k(2s)} \prod_{\mathfrak{p}|\mathfrak{m}_0} \left(1 - \mathrm{N}\mathfrak{p}^{-2s}\right)^{-1} \cdot \sum_{(\pi_\mathfrak{c}, \bar{\beta}) \in B} D_{\mathfrak{m}_0}(\pi_\mathfrak{c}\beta)^{-s} \sum_\chi \chi(\pi_\mathfrak{c}^{-1}\beta^{-1}\mathfrak{c}) L_k(s, \chi),$$

where $D_{\mathfrak{m}_0}(x) = \prod_{\mathfrak{p}|\mathfrak{m}_0} D_{k_\mathfrak{p}(\sqrt{x})/k_\mathfrak{p}}$ and $\delta_{(1,\bar{1}) \in B}$ is 1 if $(1, \bar{1}) \in B$ and 0 otherwise.

Proof: The proof is almost identical to that of Theorem 3.3.1 save for few details. When choosing the lift β of $\bar{\beta}$, for each $\sigma_v \mid \mathfrak{m}_\infty$, we must require that $\sigma_v(\beta)$ be either greater than or less than 0 depending on if the corresponding $K_v \in \Sigma_{k,v}$ is $\mathbb{R}^2$ or $\mathbb{C}$, respectively. Also we now need to evaluate the cardinality of $\mathcal{O}_{k,\mathfrak{m}}/\mathcal{O}_{k,\mathfrak{m}}^2$ for a general modulus $\mathfrak{m}$. For this, we note that for any odd prime $\mathfrak{p}$, $\mathcal{O}_{k_\mathfrak{p}}^\times/\mathcal{O}_{k_\mathfrak{p}}^{\times 2} \cong (\mathcal{O}_k/\mathfrak{p})^\times/(\mathcal{O}_k/\mathfrak{p})^{\times 2}$ and $|(\mathcal{O}_k/\mathfrak{p})^\times/(\mathcal{O}_k/\mathfrak{p})^{\times 2}| = 2$. Also, for any real infinite place v, $|\mathcal{O}_{k_v}^\times/\mathcal{O}_{k_v}^{\times 2}| = 2$. □

We now have everything we need to prove Theorem 3.0.3.

Proof: To prove the theorem, we will apply Perron's formula on $\Phi_{k,2}(\Sigma_k; C_2, s)$ as given by Theorem 3.3.4 as this will give us $N_{k,2}(X; C_2; \Sigma_k)$. Let Σ_k be an acceptable collection of local specifications for k. We take the modulus $\mathfrak{m}$ to be defined as in the statement of Theorem 3.0.3.

We can exclude $\mathfrak{r}_1$ (resp. $\mathfrak{u}_1$) from the modulus $\mathfrak{m}$ and the set B because we don't need to pick a subset of the classes in $\mathcal{O}_{k,\mathfrak{r}_1}^\times \mathcal{O}_{k,\mathfrak{r}_1}^{\times 2}$ (resp. $\mathcal{O}_{k,\mathfrak{u}_1}^\times \mathcal{O}_{k,\mathfrak{u}_1}^{\times 2}$). To count these extensions we modify the sum over integral, squarefree ideals to be

$$\frac{1}{\mathrm{N}\mathfrak{r}_1^2} \sum_{\substack{\mathfrak{a}\ \square\text{-free} \\ (\mathfrak{a},\mathfrak{m}_0\mathfrak{r}_1)=1}} \frac{\chi(\mathfrak{a})}{\mathrm{N}\mathfrak{a}^2}.$$

This way, we are using a character χ from $\mathrm{Cl}_\mathfrak{m}(k)$ but we can modify the Euler products for $L_k(s,\chi)$ and $\zeta_k(2s)$ such that they exclude primes dividing r_1. A similar change to the sum can be made for the primes dividing $\mathfrak{u}_1$.

Now, note that all of the L-functions in the sum over quadratic characters of the ray class group are holomorphic on the entire complex plane with the exception of the trivial character, which has a pole at $s=1$. So, $\Phi_{k,2}(\Sigma_k; C_2, s)$ only has a pole at $s=1$ for $\mathrm{Re}(s) > 1/2$.

Using the standard convexity bounds on Hecke characters (e.g. [20, p. 142]), we get that

$$N_{k,2}(C_2,\Sigma_k,X) = \operatorname*{Res}_{s=1} \Phi_{k,2}(\Sigma_k;C_2,s)X + O_{n,\epsilon}\left(\#\mathrm{Cl}_\mathfrak{m}(k)[2] \frac{X^{\frac{n+2}{n+4}+\epsilon} |D_K|^{\frac{1}{n+4}+\epsilon} \mathrm{N}\mathfrak{u}_1^\epsilon \mathrm{N}\mathfrak{u}_2^{\frac{1}{n+4}+\epsilon}}{\mathfrak{r}_1^{\frac{n+2}{n+4}-\epsilon} \mathfrak{r}_1^{\frac{n+1}{n+4}-\epsilon}} \right).$$

Here, our modifications to the sum for $\mathfrak{r}_1$ and $\mathfrak{u}_1$ give a better error estimate because they are unaffected by the modulus of χ in the convexity bound.

Examining the residue of the Dirichlet function, we see that

$$\begin{aligned}
\operatorname*{Res}_{s=1} \Phi_{k,2}(\Sigma_k;C_2,s) &= \frac{\operatorname*{Res}_{s=1} L_k(s,\chi_0)}{2^{|S(\Sigma_k)|+i(k)}\zeta_k(2)} \prod_{\mathfrak{p}|\mathfrak{r}_1} (1+\mathrm{N}\mathfrak{p})^{-1} \prod_{\mathfrak{p}|\mathfrak{u}_1} \left(1+\frac{1}{\mathrm{N}\mathfrak{p}}\right)^{-1} \prod_{\mathfrak{p}|\mathfrak{m}_0} \left(1-\mathrm{N}\mathfrak{p}^{-2}\right)^{-1} \sum_{(\pi_\mathfrak{c},\bar{\beta})\in B} \frac{1}{D_{\mathfrak{m}_0}(\pi_\mathfrak{c}\beta)} \\
&= \frac{\operatorname*{Res}_{s=1} \zeta_k(s)}{2^{|S(\Sigma_k)|+i(k)}\zeta_k(2)} \prod_{\mathfrak{p}|\mathfrak{r}_1} (1+\mathrm{N}\mathfrak{p})^{-1} \prod_{\mathfrak{p}|\mathfrak{m}_0\mathfrak{u}_1} \left(1+\frac{1}{\mathrm{N}\mathfrak{p}}\right)^{-1} \sum_{(\pi_\mathfrak{c},\bar{\beta})\in B} \frac{1}{D_{\mathfrak{m}_0}(\pi_\mathfrak{c}\bar{\beta})} \\
&= \frac{\operatorname*{Res}_{s=1} \zeta_k(s)}{2^{|S(\Sigma_k)|+i(k)}\zeta_k(2)} \prod_{\sigma_v|\infty} \left(\sum_{K_v\in\Sigma_{k,v}} 1 \right) \prod_{\mathfrak{p}|\mathfrak{m}_0} \left(\left(1+\frac{1}{\mathrm{N}\mathfrak{p}}\right)^{-1} \sum_{K_\mathfrak{p}\in\Sigma_{k,\mathfrak{p}}} \frac{1}{D_{K_\mathfrak{p}/k_\mathfrak{p}}} \right)
\end{aligned}$$

$$= \frac{\operatorname{Res}_{s=1} \zeta_k(s)}{\zeta_k(2)} \prod_{\sigma_v|\infty} \left(\sum_{K_v \in \Sigma_{k,v}} \frac{1}{|\mathrm{Aut}(K_v/k_v)|} \right) \prod_{\mathfrak{p}} \left(\left(1 + \frac{1}{\mathrm{N}\mathfrak{p}}\right)^{-1} \sum_{K_\mathfrak{p} \in \Sigma_{k,\mathfrak{p}}} \frac{1}{|\mathrm{Aut}(K_\mathfrak{p}/k_\mathfrak{p})| D_{K_\mathfrak{p}/k_\mathfrak{p}}} \right).$$

We are able to extend the product to all finite primes by noting that

$$\left(1 + \frac{1}{\mathrm{N}\mathfrak{p}}\right)^{-1} \sum_{K_\mathfrak{p} \in \Sigma_{k,\mathfrak{p}}} \frac{1}{|\mathrm{Aut}(K_\mathfrak{p}/k_\mathfrak{p})| D_{K_\mathfrak{p}/k_\mathfrak{p}}} = 1$$

whenever $\Sigma_{k,\mathfrak{p}}$ contains every degree 2 étale algebra of $k_\mathfrak{p}$. □

We now have all the tools we need and can move on to the proof of the main theorem.

3.4 Proving Theorems 3.0.1 and 3.0.2

We will first prove the main theorem and then present an outline for proving Theorem 3.0.2, as it is very similar. We will prove Theorem 3.0.1 by considering the different pieces of (3.1) separately beginning with the double sum

$$\sum_{\substack{[K:\mathbb{Q}]=2 \\ |D_K|<X^{1/2}}} \sum_{\substack{[L:K]=2 \\ D_{L/K}<X/|D_K|}} 1.$$

We cannot simply use Theorem 5.3 from [1] as the error term is too large for our purposes. The key for us will be to prove our own version of Theorem 2 from [1].

Lemma 3.4.1 *For any $X \geq 1$,*

$$\sum_{\substack{[K:\mathbb{Q}]=2 \\ 0<D_K<X}} \frac{1}{|D_K|} \cdot \frac{L(1,K/\mathbb{Q})}{L(2,K/\mathbb{Q})} = (\log X + 1) \frac{\zeta(2)}{2} \prod_p \left(1 - \frac{1}{p^2} - \frac{2}{p^3} + \frac{2}{p^4}\right) + c^+ + O_\epsilon(X^{-5/18+\epsilon});$$

$$\sum_{\substack{[K:\mathbb{Q}]=2 \\ -X<D_K<0}} \frac{1}{|D_K|} \cdot \frac{L(1,K/\mathbb{Q})}{L(2,K/\mathbb{Q})} = (\log X + 1) \frac{\zeta(2)}{2} \prod_p \left(1 - \frac{1}{p^2} - \frac{2}{p^3} + \frac{2}{p^4}\right) + c^- + O_\epsilon(X^{-5/18+\epsilon}),$$

for some constants c^+ and c^-.

The proof of this lemma follows a similar outline to Theorem 2 of [1]. Where they approximate $L(1, K/\mathbb{Q})$ using a finite sum, we will use a smooth approximation instead.

Lemma 3.4.2 *Let $L(s, K/\mathbb{Q})$ be the Dirichlet L-function attached to the quadratic extension $K/\mathbb{Q}$. For any $N > 1$,*

$$L(1, K/\mathbb{Q}) = \sum_{n\geq 1} \frac{\chi_K(n)e^{-n/N}}{n} + O_\epsilon\left(\frac{D_K^{1/6+\epsilon}}{N^{1/2}}\right),$$

where χ_K is the Kronecker character for $K/\mathbb{Q}$.

Proof: Using an inverse Mellin transform similar to Perron's formula, we have that for any $c > 0$

$$\begin{aligned}\sum_{n\geq 1} \frac{\chi_K(n)e^{-n/N}}{n} &= \frac{1}{2\pi i}\int_{(c)} L(s+1, K/\mathbb{Q})N^s\Gamma(s)\, ds \\ &= L(1, K/\mathbb{Q}) + \frac{1}{2\pi i}\int_{(-1/2)} L(s+1, K/\mathbb{Q})N^s\Gamma(s)\, ds,\end{aligned}$$

where $\int_{(c)}$ indicates the contour integral from $c - i\infty$ to $c + i\infty$ and $\int_{(-1/2)}$ indicates a contour integral where part of the contour is pushed to $\Re(s) = -1/2$. The lemma follows from the subconvexity bound $L(1/2+it, K/\mathbb{Q}) \ll_\epsilon (D_K(1+t))^{1/6+\epsilon}$ of Petrow and Young [28]. □

Next, we look at sums over $\chi_K(n)$ as K varies and see that the largest contributions come from n being square.

Lemma 3.4.3 *For any integer $n \geq 1$ and number $X \geq 1$, if n is not a square,*

$$\sum_{\substack{[K:\mathbb{Q}]=2 \\ X<D_K<2X}} \chi_K(n) \ll X^{1/2}n^{1/4+\epsilon},$$

and

$$\sum_{\substack{[K:\mathbb{Q}]=2 \\ X<D_K<2X}} \chi_K(n) = \frac{X}{2\zeta(2)}\prod_{p|n}\frac{p}{p+1} + O(X^{1/2}n^\epsilon)$$

if n is a square.

Proof: When n is not a square, we rewrite $\chi_K(n)$ as $\left(\frac{D_K}{n}\right)$ use the inclusion-exclusion principle so we can sum over squarefree integers. Thus our sum is

$$\sum_{a<\sqrt{2X}} \mu(a) \sum_{\frac{X}{a^2}<d<\frac{2X}{a^2}} \left(\frac{a^2 d}{n}\right).$$

We now split the sum over a into two parts using an auxillarly parameter T. We will treat the first part with Polya-Vinogradov and the second with a trivial estimate.

$$\begin{aligned}\sum_{a<\sqrt{2X}} \mu(a) \sum_{\frac{X}{a^2}<d<\frac{2X}{a^2}} \left(\frac{a^2 d}{n}\right) &= \sum_{a<T} \mu(a) \sum_{\frac{X}{a^2}<d<\frac{2X}{a^2}} \left(\frac{a^2 d}{n}\right) + \sum_{T\le a<\sqrt{2X}} \mu(a) \sum_{\frac{X}{a^2}<d<\frac{2X}{a^2}} \left(\frac{a^2 d}{n}\right) \\ &= \sum_{a<T} O(n^{1/2+\epsilon}) + \sum_{T\le a<\sqrt{2X}} O(X/a^2) \\ &= O(Tn^{1/2+\epsilon} + X/T).\end{aligned}$$

Choosing $T = X^{1/2}/n^{1/4}$ yields the first part of the lemma.

When n is a square, the result follows from Theorem 3.0.3 but using results from counting squarefree integers to obtain the error term. See [25, Lemma 2.17] for a reference. □

We then combine these lemmas to analyze the sum of $\frac{L(1,K/\mathbb{Q})}{L(2,K/\mathbb{Q})}$ for D_K in the range X to $2X$.

Lemma 3.4.4 *For any $X \ge 1$,*

$$\sum_{\substack{[K:\mathbb{Q}]=2 \\ X<D_K<2X}} \frac{L(1,K/\mathbb{Q})}{L(2,K/\mathbb{Q})} = \frac{1}{2\zeta(2)} X \prod_p \left(1 + \frac{1}{(p+1)^2}\right) + O_\epsilon(X^{13/18+\epsilon}).$$

Proof: We start be rewriting $1/L(2,K/\mathbb{Q})$ as the Dirichlet series

$$\sum_{m\ge 1} \frac{\mu(m)\chi_K(m)}{m^2}$$

and combining this with Lemma 3.4.2. For $N > X^{1/3}$, we see that

$$\frac{L(1,K/\mathbb{Q})}{L(2,K/\mathbb{Q})} = \sum_{m\geq 1}\sum_{n\geq 1}\frac{\mu(m)\chi_K(mn)e^{-n/N}}{m^2 n} + O_\epsilon\left(\frac{D_K^{1/6+\epsilon}}{N^{1/2}}\right).$$

Therefore, summing D_K in the range X to $2X$ gives

$$\sum_{\substack{[K:\mathbb{Q}]=2\\ X<D_K<2X}}\frac{L(1,K/\mathbb{Q})}{L(2,K/\mathbb{Q})} = \sum_{m\geq 1}\sum_{n\geq 1}\frac{\mu(m)e^{-n/N}}{m^2 n}\sum_{\substack{[K:\mathbb{Q}]=2\\ X<D_K<2X}}\chi_K(mn) + O_\epsilon\left(\frac{X^{7/6+\epsilon}}{N^{1/2}}\right).$$

By Lemma 3.4.3, the inner sum is negligible unless mn is a square. Because m must also be squarefree, this can only happen when m is the squarefree part of n. If we let $\psi(n)$ be the multiplicative function such that $\psi(p^k) = p/(p+1)$, we can eliminate the sum over m because

$$\sum_{m\geq 1}\sum_{n\geq 1}\frac{\mu(m)e^{-n/N}}{m^2 n}\sum_{\substack{[K:\mathbb{Q}]=2\\ X<D_K<2X}}\chi_K(mn) = \frac{X}{2\zeta(2)}\sum_{n\geq 1}\frac{\mu(m)\psi(n)e^{-n/N}}{m^2 n} + O(X^{1/2+\epsilon}N^{1/4+\epsilon}).$$

We can simplify this even further.

$$\begin{aligned}\frac{X}{2\zeta(2)}\sum_{n\geq 1}\frac{\mu(m)\psi(n)e^{-n/N}}{m^2 n} + O(X^{1/2+\epsilon}N^{1/4+\epsilon}) &= \frac{X}{2\zeta(2)}\sum_{n\geq 1}\frac{\mu(m)\psi(n)}{m^2 n} + O(X/N + X^{1/2+\epsilon}N^{1/4+\epsilon})\\ &= \frac{X}{2\zeta(2)}\prod_p\left(1+\frac{1}{(p+1)^2}\right) + O(X/N + X^{1/2+\epsilon}N^{1/4+\epsilon}).\end{aligned}$$

Though the penultimate sum does not initially look like it should yield an Euler product of this form, analyzing it shows that there are geometric sub-series that, when combined, lead to the final product. Now, to optimize both error terms, we choose $N = X^{8/9}$. □

We can now prove Lemma 3.4.1 by using the above lemmas and partial summation.

Proof (Lemma 3.4.1): Let $S^+(X)$ denote $\sum_{\substack{[K:\mathbb{Q}]=2\\ 0<D_K<X}}\frac{L(1,K/\mathbb{Q})}{L(2,K/\mathbb{Q})}$. Then

$$\sum_{\substack{[K:\mathbb{Q}]=2\\ 0<D_K<X}}\frac{1}{|D_K|}\cdot\frac{L(1,K/\mathbb{Q})}{L(2,K/\mathbb{Q})} = \frac{S^+(t)}{t}\Big|_{1^-}^{X} + \int_{1^-}^{X}\frac{S^+(t)}{t^2}dt$$

$$= \frac{1}{2\zeta(2)} \prod_p \left(1 + \frac{1}{(p+1)^2}\right)(\log X + 1) + \int_{1^-}^{X} \frac{E^+(t)}{t^2} dt + O_\epsilon(X^{-5/18+\epsilon})$$
$$= \frac{1}{2\zeta(2)} \log(X) \prod_p \left(1 + \frac{1}{(p+1)^2}\right) + \int_{1^-}^{\infty} \frac{E^+(t)}{t^2} dt + O_\epsilon(X^{-5/18+\epsilon}).$$

Above, $E^+(X) = S^+(X) - \frac{1}{2\zeta(2)} X \prod_p \left(1 + \frac{1}{(p+1)^2}\right)$ with $\int_{1^-}^{X} \frac{E^+(t)}{t^2} dt = \int_{1^-}^{\infty} \frac{E^+(t)}{t^2} dt - \int_{X}^{\infty} \frac{E^+(t)}{t^2} dt$. This is justified because $E(X) = O(X^{13/18+\epsilon})$, so the integral $\int_{1^-}^{\infty} \frac{E^+(t)}{t^2} dt$ converges. With this, we define

$$c^+ = \int_{1^-}^{\infty} \frac{E^+(t)}{t^2} dt. \tag{3.2}$$

Defining $S^-(X)$ and $E^-(X)$ similarly, we also define

$$c^- = \int_{1^-}^{\infty} \frac{E^-(t)}{t^2} dt. \tag{3.3}$$

□

At this point, note that

$$\frac{1}{\zeta(2)} \prod_p \left(1 + \frac{1}{(p+1)^2}\right) = \zeta(2) \prod_p \left(1 - \frac{1}{p^2} - \frac{2}{p^3} + \frac{2}{p^4}\right).$$

We can now use Theorem 3.0.3 on the inner sum and Lemma 3.4.1 on the outer sum to get

$$\sum_{\substack{[K:\mathbb{Q}]=2 \\ |D_K|<X^{1/2}}} \sum_{\substack{[L:K]=2 \\ D_{L/K}<X/|D_K|}} 1 = X\left(\frac{1}{2}\log X + 1\right)\frac{3}{4}\prod_p \left(1 - \frac{1}{p^2} - \frac{2}{p^3} + \frac{2}{p^4}\right) + cX + O_\epsilon(X^{11/12+\epsilon}), \tag{3.4}$$

where

$$c = c^+ + \frac{1}{2}c^-. \tag{3.5}$$

3.4.1 The Second Sum

We will now turn our attention to the second sum from (3.1), namely

$$\sum_{q<X^{1/4}} \sum_{\substack{[K:\mathbb{Q}]=2 \\ |D_K|<X^{1/2}/q^2}} \sum_{\substack{[L:K]=2 \\ D_{L/K}<X^{1/2}q^2 \\ J(L)=q^2}} 1.$$

Now that we can count quadratic extensions L/K with $J_2(L) = 2^{2i}$ for some $i = 0, 1, 2,$ or 3, we will expand q to get $J(L) = 2^{2i}d^2$. So, our second sum is now

$$\sum_{\substack{q=2^i d<X^{1/4} \\ d \text{ odd, } \square\text{-free} \\ i\in\{0,1,2,3\}}} \sum_{\substack{[K:\mathbb{Q}]=2 \\ |D_K|<X^{1/2}/q^2}} \sum_{\substack{[L:K]=2 \\ D_{L/K}<X^{1/2}q^2 \\ J(L)=q^2}} 1. \tag{3.6}$$

For the odd part of $J(L)$, we will require that $(D_K, d) = 1$, and for $J_2(L)$, we will require that D_K fall into specific congruence classes mod 8 corresponding to Tables 3.1-3.4. To limits ourselves to extensions L/K such that the odd part of $J(L)$ is exactly d^2, we will use the inclusion/exclusion principle. Thus, the innermost sum of (3.6) becomes

$$\sum_{\substack{[L:K]=2 \\ D_{L/K}<X^{1/2}q^2 \\ J(L)=q^2}} 1 = \sum_{\substack{e<X^{1/4} \\ (e,|D_K|2d)=1}} \mu(e) \sum_{\substack{[L:K]=2 \\ D_{L/K}<X^{1/2}q^2 \\ d^2e^2|D_{L/K} \\ J_2(L)=2^{2i}}} 1. \tag{3.7}$$

Before we apply Theorem 3.0.3, we construct an acceptable collection of local conditions Σ for which Σ_2 only contains pairs (L_2, K_2) where $J_2(L) = 2^{2i}$ and Σ_p contains pairs (L_p, K_p) for all $p \mid de$ such that $J_p(L) = p^2$. Σ can be restricted to an acceptable collection Σ_K of local conditions for K. As we vary K later on in the argument, we will pick up every pair $(L_p, K_p) \in \Sigma_p$ for each $p \mid 2de$. Now, we apply the theorem on Σ_K and get

$$X^{1/2}\frac{q^2L(1,K/\mathbb{Q})}{2^{i(K)}\zeta(2)L(2,K/\mathbb{Q})}\prod_{\mathfrak{p}|2de}\left(\left(1+\frac{1}{\mathrm{N}\mathfrak{p}}\right)^{-1}\sum_{L_\mathfrak{p}\in\Sigma_{K,\mathfrak{p}}}\frac{1}{|\mathrm{Aut}(L_\mathfrak{p}/K_\mathfrak{p})|D_{L_\mathfrak{p}/K_\mathfrak{p}}}\right)+O_\epsilon\left(\frac{X^{1/3+\epsilon}q^\epsilon|D_K|^{1/6+\epsilon}}{e^{4/3+\epsilon}}\right).$$

We will pull everything but the product over primes dividing e in front of our sum over e. For those remaining primes, because $\Sigma_{K,\mathfrak{p}}$ contains only the $L_\mathfrak{p}$ that ramify we see that

$$\prod_{\mathfrak{p}|e}\left(1+\frac{1}{\mathrm{N}\mathfrak{p}}\right)^{-1}\sum_{L_\mathfrak{p}\in\Sigma_{K,\mathfrak{p}}}\frac{1}{|\mathrm{Aut}(L_\mathfrak{p}/K_\mathfrak{p})|D_{L_\mathfrak{p}/K_\mathfrak{p}}}=\prod_{p|e}\frac{1}{m(p)},\tag{3.8}$$

where $m(p)=1/(1+p)^2$ if p splits in K and $1/(1+p^2)$ if p is inert in K. So, the sum over e is

$$\sum_{\substack{e<X^{1/4}\\(e,|D_K|2d)=1}}\left(\mu(e)\prod_{p|e}\frac{1}{m(p)}+O_\epsilon\left(\frac{X^{1/3+\epsilon}q^\epsilon|D_K|^{1/6+\epsilon}}{e^{4/3+\epsilon}}\right)\right)=\prod_{p\nmid D_K2d}\left(1-\frac{1}{m(p)}\right)+O_\epsilon(X^{1/3+\epsilon}q^\epsilon|D_K|^{1/6+\epsilon}).$$

Before we turn to the sum over K, we will deal with some of the constants we have accrued. First, we let

$$\mu(\Sigma_{K,2^{2i}})=\prod_{\mathfrak{p}|2}\sum_{L_\mathfrak{p}\in\Sigma_{K,\mathfrak{p}}}\frac{1}{|\mathrm{Aut}(L_\mathfrak{p}/K_\mathfrak{p})|D_{L_\mathfrak{p}/K_\mathfrak{p}}}.$$

Additionaly, we see that if pull out $p=2$ from the Euler product for $\frac{L(1,K/\mathbb{Q})}{L(2,K/\mathbb{Q})}$ we get

$$\left(\frac{1-\chi_K(p)/p^2}{1-\chi_K(p)/p}\right)\prod_{\mathfrak{p}|2}\left(1+\frac{1}{\mathrm{N}\mathfrak{p}}\right)^{-1}=\left(1+\frac{1}{p}\right)^{-1}\tag{3.9}$$

regardless of if 2 splits, is inert, or ramifies in K.

Similarly, we also consider the factors of $\frac{L(1,K/\mathbb{Q})}{L(2,K/\mathbb{Q})}$ at odd primes p. For the primes dividing d, we can use (3.8) and get

$$\left(\frac{1}{m(p)}\right)\left(\frac{1-\chi_K(p)/p^2}{1-\chi_K(p)/p}\right)=\frac{1}{p(p+1)}.\tag{3.10}$$

For the remaining primes not dividing D_K,

$$\left(1 - \frac{1}{m(p)}\right)\left(\frac{1 - \chi_K(p)/p^2}{1 - \chi_K(p)/p}\right) = 1 + \frac{\chi_K(p)}{p+1}. \tag{3.11}$$

Applying all of this, the sum over K is

$$X^{1/2}\frac{2q^2}{3\zeta(2)}\prod_{p|d}\frac{1}{p(p+1)}\sum_{\substack{[K:\mathbb{Q}]=2\\ |D_K|<X^{1/2}/q^2\\ (D_K,d)=1\\ K_2\in\Sigma_{\mathbb{Q},2^{2i}}}}\frac{\mu(\Sigma_{K,2^{2i}})}{2^{i(K)}}\prod_{p\nmid 2d}\left(1+\frac{\chi_K(p)}{p+1}\right)+O_\epsilon\left(\frac{X^{11/12+\epsilon}}{q^{7/3-\epsilon}}\right), \tag{3.12}$$

where $\Sigma_{\mathbb{Q},2^{2i}}$ is an acceptable set of local conditions over $\mathbb{Q}$ that is complete at every odd prime and at $p = 2$ contains only quadratic extensions K that are quadratic subfields for quartic fields L with $J_2(L) = 2^{2i}$.

To analyze the sum, we first rewrite the Euler product as the sum

$$\sum_{\substack{[K:\mathbb{Q}]=2\\ |D_K|<X^{1/2}/q^2\\ (D_K,d)=1\\ K_2\in\Sigma_{\mathbb{Q},2^{2i}}}}\frac{\mu(\Sigma_{K,2^{2i}})}{2^{i(K)}}\sum_{\substack{n\geq 1\\ (n,2d)=1\\ n\ \square\text{-free}}}\frac{\chi_K(n)}{f(n)}, \tag{3.13}$$

where $f(n) = \prod_{p|n}(p+1)$. In a series of lemmas, we will consider how to estimate the inner sum of (3.13) and swap the order of summation to arrive at our conclusion. We again use the inverse Mellin transfrom from Lemma 3.4.2. To do this, we consider the following function.

$$F(s,\chi_K) = \sum_{\substack{n\geq 1\\ (n,d)=1}}\frac{\mu^2(n)\chi_K(n)\psi(n)}{n^s},$$

where $\psi(n) = \prod_{p|n}\frac{p}{p+1}$. Note that $F(1,\chi_K)$ is equivalent to the inner sum of (3.13).

Lemma 3.4.5 *Let $F(s,\chi_K)$ be the function given above. Then for any $N > 1$,*

$$F(1,\chi_K) = \sum_{\substack{n\geq 1\\ (n,d)=1\\ n\ \square\text{-free}}}\frac{\chi_K(n)e^{-n/N}}{f(n)} + O_\epsilon\left(\frac{|D_K|^{1/6+\epsilon}}{N^{1/2}}\right).$$

Proof: If we note that

$$F(s,\chi_K) = \prod_{p\nmid d}\left(1+\frac{\chi_K(p)}{p^{s-1}(p+1)}\right)$$
$$= L(s,\chi_K)\prod_{p\mid d}\left(1+\frac{\chi_K(p)}{p^s}\right)\prod_{p\nmid d}\left(1-\frac{\chi_K(p)}{p^s(p+1)}-\frac{1}{p^{2s-1}(p+1)}\right),$$

and the rightmost product is absolutely convergent for $\Re(s+1) > -1/2$, then the proof for this lemma is almost identical to Lemma 3.4.2. □

In addition to this, we also need two more lemmas also very similar to Lemmas 3.4.3 and 3.4.4. In the lemmas below, because $\mu(\Sigma_{K,2^{2i}})$ depends on the class that K_2 corresponds to in $\mathbb{Q}_2/\mathbb{Q}_2^{\times 2}$, we sum over K such that $D_K \equiv a \mod 8$ rather than $K_2 \in \Sigma_{\mathbb{Q},2^{2i}}$, where the value of a corresponds to the congruence conditions from Tables 3.1-3.4. Then, when we use the lemmas to analyze (3.13), we will combine the separate congruence conditions to get the sum over $K_2 \in \Sigma_{\mathbb{Q},2^{2i}}$.

Lemma 3.4.6 *For any squarefree integers $n, d \geq 1$ with $(n,d) = 1, X \geq 1$, and $a \in \{0,1,4,5\}$ we have*

$$\sum_{\substack{[K:\mathbb{Q}]=2\\ X<D_K<2X\\ (D_K,d)=1\\ D_K\equiv a \mod 8}} \chi_K(n) \ll_\epsilon X^{1/2+\epsilon}(nd)^{1/4+\epsilon}$$

if $n \neq 1$, and

$$\sum_{\substack{[K:\mathbb{Q}]=2\\ X<D_K<2X\\ (D_K,d)=1\\ D_K\equiv a \mod 8}} \chi_K(n) = X\frac{\mu(\Sigma_{\mathbb{Q},2^{2i},a})}{3\zeta(2)}\prod_{p\mid d}\frac{p}{p+1} + O_\epsilon(X^{1/2}d^\epsilon)$$

if $n = 1$, where

$$\mu(\Sigma_{\mathbb{Q},2^{2i},a}) = \sum_{\substack{K_2\in\Sigma_{\mathbb{Q},2^{2i}}\\ D_K\equiv a \mod 8}} \frac{1}{|\mathrm{Aut}(K_2/\mathbb{Q}_2)|D_{K_2/\mathbb{Q}_2}}.$$

Proof: The proof for this is nearly identical to Lemma 3.4.3 except that we consider

$\chi_K(n)$ as a character with conductor nd. □

Lastly, the clone of Lemma 3.4.4.

Lemma 3.4.7 *For any $X \geq 1$, we have*

$$\sum_{\substack{[K:\mathbb{Q}]=2 \\ X<D_K<2X \\ (D_K,d)=1 \\ D_K \equiv a \mod 8}} \sum_{\substack{n\geq 1 \\ (n,2d)=1 \\ n \ \square\text{-free}}} \frac{\chi_K(n)}{f(n)} = X\frac{\mu(\Sigma_{\mathbb{Q},2^{2i},a})}{3\zeta(2)} \prod_{p|d} \frac{p}{p+1} + O_\epsilon(X^{13/18+\epsilon} d^{1/4+\epsilon}).$$

Proof: The proof for this lemma is actually simpler than that of Lemma 3.4.4 because the sum over $\chi_K(n)$ only has a significant contribution when $n = 1$ as opposed to whenever n is a square. □

Turning our attention back to (3.13), we apply Lemma 3.4.7 by summing diadically to obtain

$$X^{1/2}\frac{\mu(\Sigma_{\mathbb{Q},2^{2i},a})}{2\zeta(2)q^2} \prod_{p|d} \frac{p}{p+1} + O_\epsilon\left(\frac{X^{13/36+\epsilon}}{q^{43/36-\epsilon}}\right).$$

Now we sum over a and expand the definitions for $\mu(\Sigma_{\mathbb{Q},2^{2i}}, a)$ and $\mu(\Sigma_{K,2^{2i}})$, which yields

$$\begin{aligned}\sum_{a\in\{0,1,4,5\}} \mu(\Sigma_{\mathbb{Q},2^{2i},a})\mu(\Sigma_{K,2^{2i}}) &= \left(\sum_{K_2\in\Sigma_{\mathbb{Q},2^{2i}}} \frac{1}{|\mathrm{Aut}(K_2/\mathbb{Q}_2)|D_{K_2/\mathbb{Q}_2}} \left(\prod_{\mathfrak{p}|2} \sum_{L_\mathfrak{p}\in\Sigma_{K,\mathfrak{p}}} \frac{1}{|\mathrm{Aut}(L_\mathfrak{p}/K_\mathfrak{p})|D_{L_\mathfrak{p}/K_\mathfrak{p}}}\right)\right) \\ &= \sum_{\substack{(L_2,K_2)\in\Sigma \\ J_2(L)=2^{2i}}} \frac{1}{|\mathrm{Aut}(L_2,K_2)|C(L_2,K_2)}. \qquad (3.14)\end{aligned}$$

We will denote this by as $\mu(\Sigma_{2^{2i}})$ Bringing this back into (3.12), we get

$$X\frac{\mu(\Sigma_{2^{2i}})}{3\zeta(2)^2} \prod_{p|d} \frac{1}{(p+1)^2} + O_\epsilon\left(\frac{X^{11/12+\epsilon}}{q^{7/3-\epsilon}}\right).$$

Summing over q, we get

$$X\frac{1}{3}\cdot\frac{9}{16}\left(\sum_{i=0}^{3}\mu(\Sigma_{2^{2i}})\right)\prod_{p\neq 2}\left(1-\frac{1}{p^2}-\frac{2}{p^3}+\frac{2}{p^4}\right) + O_\epsilon(X^{11/12+\epsilon}).$$

Lastly, we note the sum $\sum \mu(\Sigma_{2^{2i}})$ is simply

$$\sum_{(L_2,K_2)} \frac{1}{|\mathrm{Aut}(L_2,K_2)|C(L_2,K_2)}.$$

Moreover, Theorem 3 of [1] implies,

$$\left(1-\frac{1}{p}\right)^2 \sum_{(L_p,K_p)} \frac{1}{|\mathrm{Aut}(L_2,K_2)|C(L_2,K_2)} = \left(1-\frac{1}{p^2}-\frac{2}{p^3}+\frac{2}{p^4}\right).$$

Thus, our second sum comes to

$$X\frac{3}{4}\prod_p \left(1-\frac{1}{p^2}-\frac{2}{p^3}+\frac{2}{p^4}\right) + O_\epsilon(X^{11/12+\epsilon}). \tag{3.15}$$

3.4.2 The Third Sum

Our treatment of the third sum of (3.1) will look very similar to the second sum. We begin in the same way by summing over valid values for q and get

$$\sum_{\substack{q=2^i d<X^{1/4} \\ d \text{ odd, } \square\text{-free} \\ i\in\{0,1,2,3\}}} \sum_{\substack{[K:\mathbb{Q}]=2 \\ X^{1/2}/q^2\le|D_K|<X^{1/2}}} \sum_{\substack{[L:K]=2 \\ D_{L/K}<X/|D_K| \\ J(L)=q^2}} 1. \tag{3.16}$$

We treat the inner most sum identically by using the inclusion/exclusion principle to count only the quartic fields L with $J(L)=q^2$. We also use (3.9 – 3.11) with the end result

$$X\frac{2}{3\zeta(2)}\prod_{p|d}\frac{1}{p(p+1)} \sum_{\substack{[K:\mathbb{Q}]=2 \\ X^{1/2}/q^2\le|D_K|<X^{1/2} \\ (D_K,d)=1 \\ K_2\in\Sigma_{\mathbb{Q},2^{2i}}}} \frac{\mu(\Sigma_{K,2^{2i}})}{2^{i(K)}|D_K|} \sum_{\substack{n\ge1 \\ (n,2d)=1 \\ n\ \square\text{-free}}} \frac{\chi_K(n)}{f(n)} + O_\epsilon\left(\frac{X^{11/12+\epsilon}}{q^{4/3-\epsilon}}\right). \tag{3.17}$$

We will again sum over congruence conditions mod 8 as we did to analyze (3.13) and also use partial summation. We define

$$A(x) = \sum_{\substack{[K:\mathbb{Q}]=2 \\ 0<D_K<X \\ (D_K,d)=1 \\ D_K\equiv a \mod 8}} \sum_{\substack{n\geq 1 \\ (n,2d)=1 \\ n \ \square\text{-free}}} \frac{\chi_K(n)}{f(n)}.$$

Then, considering first the sum over real quadratic fields K

$$\sum_{\substack{[K:\mathbb{Q}]=2 \\ X^{1/2}/q^2\leq D_K<X^{1/2} \\ (D_K,d)=1 \\ D_K\equiv a \mod 8}} \frac{1}{D_K} \sum_{\substack{n=1 \\ (n,2d)=1 \\ n \ \square\text{-free}}}^{\infty} \frac{\chi_K(n)}{f(n)} = \frac{A(t)}{t}\Big|_{X^{1/2}/q^2}^{X^{1/2}} + \int_{X^{1/2}/q^2}^{X^{1/2}} \frac{A(t)}{t^2}dt$$
$$= \frac{\mu(\Sigma_{\mathbb{Q},2^{2i},a})\log(q^2)}{3\zeta(2)} \prod_{p|d} \frac{p}{p+1} + O_\epsilon\left(\frac{q^{29/36+\epsilon}}{X^{5/36-\epsilon}}\right).$$

As before, we extend the sum over the different congruence conditions and imaginary quadratic fields and bring this back into (3.17) to get

$$X\frac{1}{3\zeta(2)^2} \sum_{\substack{q=2^i d<X^{1/4} \\ d \text{ odd, } \square\text{-free} \\ i\in\{0,1,2,3\}}} \mu(\Sigma_{2^{2i}})\log(q^2)\prod_{p|d}\frac{1}{(p+1)^2} + O_\epsilon(X^{11/12+\epsilon}). \tag{3.18}$$

If we replace q with $2^i d$, we can split $\log(q^2)$ and consider the sum in two parts. First, we have

$$\sum_{\substack{q=2^i d<X^{1/4} \\ d \text{ odd, } \square\text{-free} \\ i\in\{0,1,2,3\}}} \mu(\Sigma_{2^{2i}})\log(d^2)\prod_{p|d}\frac{1}{(p+1)^2} = 5\sum_{d \text{ odd, } \square\text{-free}} \log d \prod_{p|d}\frac{1}{(p+1)^2} + O_\epsilon(X^{-1/4+\epsilon}).$$

We can rewrite this as a sum over odd primes p and get

$$5\sum_{d \text{ odd, } \square\text{-free}} \log d \prod_{p|d}\frac{1}{(p+1)^2} = 5\sum_{p\neq 2}\frac{\log p}{(p+1)^2}\prod_{r\neq p,2}\left(1+\frac{1}{(r+1)^2}\right)$$
$$= \frac{9}{4}\prod_{p}\left(1+\frac{1}{(p+1)^2}\right)\left(-\frac{\log 2}{5} + 2\sum_{p}\frac{\log p}{p^2+2p+2}\right).$$

The third sum is

$$2\log 2 \sum_{\substack{q=2^i d<X^{1/4}\\ d \text{ odd, } \square\text{-free}\\ i\in\{0,1,2,3\}}} i\cdot\mu(\Sigma_{2^{2i}})\prod_{p|d}\frac{1}{(p+1)^2} = \frac{9\log 2}{5}\prod_p\left(1+\frac{1}{(p+1)^2}\right)\left(\sum_{i=1}^{3} i\cdot\mu(\Sigma_{2^{2i}})\right)+O(X^{-1/4}).$$

Using Tables 3.1-3.4, we compute $\sum i\cdot\mu(\Sigma_{2^{2i}}) = 11/16$ and put everything back into (3.18).

$$X\frac{3}{4}\left(\frac{7\log 2}{20}+2\sum_p\frac{\log p}{p^2+2p+2}\right)\prod_p\left(1-\frac{1}{p^2}-\frac{2}{p^3}+\frac{2}{p^4}\right)+O_\epsilon(X^{11/12+\epsilon}). \tag{3.19}$$

The main theorem now follows from putting (3.4), (3.15), and (3.19) in the sum (3.1).

3.4.3 A Modified Argument for Theorem 3.0.2

To prove Theorem 3.0.2, one can follow the same outline as the main theorem by tackling each sum in (3.1) separately. Let $\Sigma = (\Sigma_v)_v$ be an acceptable collection of local specifications and let m be the product of primes p such that Σ_p doesn't contain every pair (L_p, K_p). If we again restrict Σ to Σ_K, then Theorem 3.0.3 gives

$$\sum_{\substack{[L:K]=2\\ L\in\mathcal{K}(\Sigma_K)\\ D_{L/K}\le X/|D_K|}} = X\frac{L(1,K/\mathbb{Q})}{|D_K|L(2,K/\mathbb{Q})}\cdot\mu(\Sigma_{K,\infty})\prod_{p|m}\left(\prod_{\mathfrak{p}|p}\frac{\mathrm{N}\mathfrak{p}}{1+\mathrm{N}\mathfrak{p}}\right)\cdot\mu(\Sigma_{K,p})+O_\epsilon(X^{2/3+\epsilon}|D_K|^{-1/2+\epsilon}m^{1/3+\epsilon}),$$

where

$$\mu(\Sigma_{K,\infty}) = \prod_{\sigma_v|\infty}\sum_{L_v\in\Sigma_{K,v}}\frac{1}{|\mathrm{Aut}(L_v/K_v)|},\ \text{ and } \mu(\Sigma_{K,p}) = \prod_{\mathfrak{p}|p}\sum_{L_\mathfrak{p}\in\Sigma_{K,\mathfrak{p}}}\frac{1}{|\mathrm{Aut}(L_\mathfrak{p}/K_\mathfrak{p})|D_{L_\mathfrak{p}/K_\mathfrak{p}}}.$$

The $m^{1/3+\epsilon}$ is a worst case estimate in which every prime p dividing m were either split or inert in K and $\mathfrak{p} \mid \mathfrak{u}_1$ for every $\mathfrak{p} \mid p$ in our application of Theorem 3.0.3.

At this point, we use (3.9) and note that we can pull these factors outside the sum over K as well as $\mu(\Sigma_{K,\infty})$ and $\mu(\Sigma_{K,p})$ and have

$$X\frac{\mu(\Sigma_{K,\infty})}{\zeta(2)}\prod_{p|m}\left(\left(1+\frac{1}{p}\right)^{-1}\mu(\Sigma_{K,p})\right)\sum_{\substack{[K:\mathbb{Q}]=2\\ K\in\mathcal{K}(\Sigma_{\mathbb{Q}})\\ |D_K|\leq X^{1/2}}}\frac{1}{|D_K|}\prod_{p\nmid m}\left(\frac{1-\chi_K(p)/p^2}{1-\chi_K(p)/p}\right)+O_\epsilon(X^{11/12+\epsilon}m^{1/3+\epsilon}).$$

To finish the first sum, only slight modifications to Lemmas 3.4.1 and 3.4.4 are needed. A modification worth mentioning is the one we need to define c_Σ in the theorem statement. In the modified Lemma 3.4.1 we would define

$$S_\Sigma^\pm(X)=\sum_{\substack{[K:\mathbb{Q}]=2\\ K\in\mathcal{K}(\Sigma_{\mathbb{Q}})\\ 0<\pm D_K<X}}\frac{1}{|D_K|}\cdot\frac{L(1,K/\mathbb{Q})}{L(2,K/\mathbb{Q})}.$$

Then,

$$E_\Sigma^\pm(X)=S_\Sigma^\pm(X)-\frac{1}{2}X\prod_p\left(\left(1-\frac{1}{p}\right)^2\sum_{(L_p,K_p)\in\Sigma_p}\frac{1}{|\mathrm{Aut}(L_p,K_p)|C(L_p,K_p)}\right).$$

With $c_\Sigma^\pm$ defined analogously to $c^\pm$, we have

$$c_\Sigma=c_\Sigma^++\frac{1}{2}c_\Sigma^-. \tag{3.20}$$

Apart from this, we should also note that given an acceptable collection of local specifications Σ that is not complete at some prime p, it is not clear that doubling the first sum yields that correct result as the second iteration of the sum is meant to count pairs (L,K) for which $D_{\phi(K)}<X^{1/2}$ and $(\phi(L),\phi(K))$ may not be in $\mathcal{L}(\Sigma)$. But, the discussion in section 9.2 of [1] shows that $\mu(\Sigma_p)=\mu(\phi(\Sigma_p))$ if we give $\phi(\Sigma_p)$ the meaning you might expect.

For the remaining two sums, the same sorts of modifications can be made without much change to the original arguments. Moreover, as each sum is only computed once, we don't need to worry about the equivalence of $\mu(\Sigma_p)$ and $\mu(\phi(\Sigma_p))$. However, we will note that the constant $\frac{7\log 2}{20}$ in the secondary term of Theorem 3.0.1 is

$$2\log 2\frac{2\mu(\Sigma_{2^4})+3\mu(\Sigma_{2^6})}{\mu(\Sigma_2)}$$

and, thus, agrees with Theorem 3.0.2 when Σ_2 contains all pairs (L_2, K_2).

Chapter 4

Counting General $D_4 \wr H$ Extensions by Conductor

In this final chapter, we establish a count of $D_4 \wr H$ $4n$-extensions of k, where k is a some number field and H is a transitive subgroup of S_n. In particular, we prove the following theorem.

Theorem 4.0.1 *Let k be a number field $N^C_{k,4n}(X; D_4 \wr H)$ denote the number of degree $4n$ extensions L/k with Galois group $D_4 \wr H$ and conductor $C_{L/k} \leq X$. Assume that $N_{k,n}(X; H)$ is non-zero and $O_{k,H,\epsilon}(X^{1+\epsilon})$. Then,*

$$N^C_{k,4n}(X; D_4 \wr H) \sim X \log X \sum_{\substack{[F:k]=n \\ \mathrm{Gal}(F/k)\cong H}} \frac{3^{r_1}\left(\operatorname*{Res}_{s=1} \zeta_F(s)\right)^2}{2^{2r_1+3r_2+1} D^2_{F/k}} \prod_{\mathfrak{p}\subset\mathcal{O}_F} \left(1 - \frac{1}{\mathrm{N}\mathfrak{p}^2} - \frac{2}{\mathrm{N}\mathfrak{p}^3} + \frac{2}{\mathrm{N}\mathfrak{p}^4}\right),$$

where r_1 and r_2 represent the number of real and complex embeddings of F, respectively.

A natural comparison to this work is that of Klüners [21], which counts $C_2 \wr H$ $2n$-extensions by discriminant. In this, he generalizes the work of Cohen, Diaz y Diaz, and Olivier [12] counting D_4 quartic extensions (as D_4 can be thought of as counting $C_2 \wr C_2$ extensions). He goes further and shows that for any tower of number fields $L/F/k$ with L/F quadratic and F/k a degree n H extension that the "expected" Galois group is $C_2 \wr H$ when ordered by discriminant. He does this by showing that $N_{k,2n}(X; C_2 \wr H) \sim c_{k,H} X$ and that any other possible Galois group G of the tower $L/F/k$ has $N_{k,2n}(X; G) = o(X)$. We will also show in proving Theorem 4.0.1, that $D_4 \wr H$ is the expected Galois group of a tower $L/K/F/k$ where both L/K and K/F are quadratic extensions.

En route to establishing Theorem 4.0.1, we will briefly discuss the wreath product and give an algebraic reason why it might be considered the expected Galois group of a tower of number fields. We will also use the definition of the conductor as laid out in Section 1.2 to find the conductor of a $D_4 \wr H$ extension L/k. In doing this, we will see how the conductor of D_4 quartic extensions show up and will need to prove the following theorem counting D_4 quartic extensions by conductor over general number fields.

Theorem 4.0.2 *Let $X > 1$ and $N^C_{k,4}(X; D_4)$ denote the number of D_4 quartic extensions L of k with $C_{L/k} < X$, we have*

$$\begin{aligned} N^C_{k,4}(X; D_4) = X \log X \cdot \frac{3^{r_1}\left(\operatorname{Res}_{s=1} \zeta_k(s)\right)^2}{2^{2r_1+3r_2+1}} \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathrm{N}\mathfrak{p}^2} - \frac{2}{\mathrm{N}\mathfrak{p}^3} + \frac{2}{\mathrm{N}\mathfrak{p}^4}\right) + Xc \\ + X\left(\frac{3^{r_1}\left(\operatorname{Res}_{s=1} \zeta_k(s)\right)^2}{2^{2r_1+3r_2+1}} \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathrm{N}\mathfrak{p}^2} - \frac{2}{\mathrm{N}\mathfrak{p}^3} + \frac{2}{\mathrm{N}\mathfrak{p}^4}\right)\right) \\ \cdot\left(1 - 2\sum_{\mathfrak{p}\nmid 2} \frac{\log \mathrm{N}\mathfrak{p}\,\mu(\Sigma_{\mathfrak{p}^2})}{\mu(\Sigma_{\mathfrak{p}})} - 2\sum_{\mathfrak{p}\mid 2} \frac{\log \mathrm{N}\mathfrak{p}}{\mu(\Sigma_{\mathfrak{p}})} \sum_{i=1}^{2e_{\mathfrak{p}}+1} i\mu(\Sigma_{\mathfrak{p}^{2i}})\right) \\ + O_{\epsilon,n}(h_2(k)^2 X^{\frac{4n+7}{4n+8}+\epsilon}|D_k|^{\frac{1}{n+2}+\epsilon} + h_2(k) X^{\frac{4n+21}{4n+24}+\epsilon}|D_k|^{\frac{3}{2n+12}+\epsilon}), \end{aligned}$$

with some constraints on the size of D_k with respect to X implied by the error term and c defined in (4.4).

Once all of the above is taken care of, we will be able to prove Theorem 4.0.1.

4.1 Wreath Products and Number Field Towers

In this brief section, we hope to argue why one might expect a wreath product as the Galois group of a tower of number fields from an algebraic standpoint as opposed to an analytical one. To answer this, we will discuss how the wreath product naturally shows up as the Galois group of an extension and then give some explanation for why it might be the "expected" one.

First, we define the wreath product. Let G and H be subgroups of S_n and S_m, respectively. The *wreath product* $G \wr H$ is the semidirect product $G^m \rtimes H \leq S_{nm}$

where H acts on the m copies of G as given by its representation as a subgroup of S_m. There are other equivalent ways of defining the wreath product. For a more detailed treatment see [9, Section 2.1].

If we have some number field k and a degree n extension L/k, we know that $\mathrm{Gal}(L/k)$ is a transitive subgroup of S_n. But, what if there is some intermediate field $L/F/k$ with $[F:k]=d$, $[L:F]=e$ and $n=de$? Then, $\mathrm{Gal}(L/k) \leq S_e \wr S_d$. In fact, if we know $\mathrm{Gal}(F/k)$ and $\mathrm{Gal}(L/F)$, we can be more specific and say that $\mathrm{Gal}(L/k) \leq \mathrm{Gal}(L/F) \wr \mathrm{Gal}(F/k)$ [16].

But why might we expect $\mathrm{Gal}(L/F) \wr \mathrm{Gal}(F/k)$ to be the Galois group of L/k as opposed to one of its subgroups? Of course, we can't be precise about this without proving a result like Klüners' (which we will do!). However, consider this heuristic argument. Assume that we have some fixed H extension F/k with some element α such that $F=k(\alpha)$. If we then take a random G extension L/F generated by some β (or $L=F(\beta)$), we would likely expect there to be little similarity between α and β other than that the minimal polynomial, of which β is a root, might have coefficients in terms of α. Extending this argument to the full Galois group $\mathrm{Gal}(L/k)$, we would expect an automorphism σ to permute the conjugates of F (i.e. $k(\sigma(\alpha))$ without affecting how the conjugates of L are permuted. Thus, without any constraints given by relationships between α and β, the Galois group should have maximal freedom to permute things, which gives the group $\mathrm{Gal}(L/F) \wr \mathrm{Gal}(F/k)$.

Now that we have laid some groundwork for why wreath products as Galois groups are natural objects of study, we move on to our specific case and define its conductor.

4.2 The Conductor of a $D_4 \wr H$ Extension

Let $L/F/k$ be a tower of number fields with L/F a quartic D_4 extension and F/k a degree n H extension. For the purpose of this section, we will assume that $\mathrm{Gal}(L/k) \cong D_4 \wr H$. To find the conductor $C_{L/k}$, we will step away from thinking of the Galois group as $D_4 \wr H$ for a second and instead think of it as $C_2 \wr (C_2 \wr H)$

for reasons that will become clear momentarily. Note that this is permissible since there is a quadratic extension K/F in between L and F and the wreath product is associative.

Like our treatment of the D_4 conductor in Section 1.2, we start with $\mathbb{1}_{H_L}$ and induce this to H_K. As before

$$\mathbb{1}_{H_L}^{H_K} = \mathbb{1}_{H_K} + \chi,$$

where χ is the sign representation of H_K/H_L. Like with D_4, we know that we know that the Artin conductor of $\mathbb{1}_{H_K}^{D_4 \wr H}$ is $\mathfrak{d}_{K/k}$, so the Artin conductor of $\chi^{D_4 \wr H}$ must be $\mathfrak{d}_{K/k}\mathfrak{d}_{L/K}$. If $\chi^{D_4 \wr H}$ is irreducible, then $C_{L/k}$ is $D_{K/k}D_{L/k}$ as it is when L/k is a quartic D_4 extension. Fortunately, the representations of wreath products are well studied and the following theorem from [9] will aid us in showing that $\chi^{D_4 \wr H}$ is indeed irreducible. In our attempt to reproduce the theorem below, we will elide some of the constructions for concision.

Theorem (2.5.1 of [9]) *Let G be a transitive subgroup of S_n for some finite n. Let $\theta \in C_2^n$ and χ_θ be the corresponding representation in $\widehat{C_2^n}$. For each θ, let G_θ represent the stabilizer of θ under the action of G and let $\widetilde{\chi}_\theta$ be the extension of χ_θ to $C_2 \wr G_\theta$. Now for a fixed θ, let η be an irreducible representation of G_θ and let $\overline{\eta}$ be the inflation of η to $C_2 \wr G_\theta$.*

If Θ is a system of representatives for the orbits of G on C_2^n, then every irreducible representation of $C_2 \wr G$ is of the form

$$(\widetilde{\chi}_\theta \otimes \overline{\eta})^{C_2 \wr G},$$

where $\theta \in \Theta$ and $\eta \in G_\theta$.

To see how this theorem helps us, we need to consider what H_L and H_K actually are as subgroups of $C_2 \wr (C_2 \wr H)$. We know that H_L is the stabilizer of some embedding of L in $\bar{k}$. Thus H_L is $C_2^{2n-1} \rtimes \mathrm{Stab}_H(1)$ and H_K (being the unique group of index 2 over H_L) is $C_2^{2n} \rtimes \mathrm{Stab}_H(1)$, or $C_2 \wr \mathrm{Stab}_H(1)$. The sign representation χ of H_K/H_L, which is defined by $\chi(g) = 1$ if $g \in H_L$ and -1 if $g \in H_K \smallsetminus H_L$, can be seen as an extension of an irreducible representation of C_2^n. Moreover, $\mathrm{Stab}_H(1)$ is precisely its stabilizer. Now, if we take $\overline{\eta}$ to be the lift of the trivial representation of $\mathrm{Stab}_H(1)$, we get that $\chi^{D_4 \wr H}$ is irreducible by the above theorem.

We've now shown that $C_{L/k} = D_{K/k} D_{L/K}$. But, given the presence of the intermediate field F between K and k, we get

$$C_{L/k} = D_{F/k}^2 D_{K/F} D_{L/K}. \tag{4.1}$$

This should also be recognizable as $D_{F/k}^2$ multiplied by the conductor of quartic D_4 extensions L/F. We will make use of this and end up counting $D_4 \wr H$ extensions L/k by counting D_4 extensions L/F on top of H extensions F/k. As such, we must begin a discussion of general D_4 extensions of a number fields before we can attempt our count of $D_4 \wr H$ extensions.

4.3 General D_4 Extensions

For this section, let k be a degree n number field and let L/k be a quartic D_4 extension.

Before we can begin counting D_4 quartic extensions of k by conductor, we need to address an important point about the counting method. The general method for counting D_4 extensions either by conductor or by discriminant is to count quadratic extensions of the base field k and then to count all quadratic extensions of each quadratic extension. The implied assumption here is that the overwhelming majority of fields counted this way will have Galois group D_4 as opposed to any other Galois group you could get by doing this (either C_4 or V_4). For counting by conductor, this was addressed explicitly by a lemma [1]. The original lemma was written in the context of counting D_4 extensions of $\mathbb{Q}$, but the proof is valid even in the more general setting, so we simply restate the lemma with minor changes to address the more general setting.

Lemma (4.4 of [1]) *Let $\beta > 1$ be fixed. The number of Galois quartic extensions L/k with $C_{L/k} < X$ and $D_{K/k} < X^{\beta}$, where K is a quadratic subfield of L is $O_{\epsilon}(D_k^{\epsilon} X^{(1+\beta)/2+\epsilon})$.*

We note that in [1], they define $C_{L/\mathbb{Q}}$ to be $D_K D_{L/K}$ for every quartic number field tower $L/K/\mathbb{Q}$ regardless of the Galois group of L.

With this technical point now accounted for, we now take another detour to discuss counting general D_4 extensions with respect to local conditions. Similar to Chapter 3, we will be able to prove a local version of Theorem 4.0.2. We use the same terminology and let Σ represent an acceptable collection of local conditions for pairs (L, K) over k and let Σ_K represent an acceptable collection of local conditions for quadratic extensions L/K.

Theorem 4.3.1 *Let $X > 1$ and Σ be an acceptable collection of local specifications. If m is the product of $\mathrm{N}\mathfrak{p}$ for primes $\mathfrak{p}$ of k such that $\Sigma_{\mathfrak{p}}$ does not contain every pair $(L_{\mathfrak{p}}, K_{\mathfrak{p}})$, then*

$$N_{k,4}^{C}(X; D_4; \Sigma) = \frac{1}{2} X \left(\log X + 1 - 2 \sum_{\mathfrak{p} \nmid 2} \frac{\log \mathrm{N}\mathfrak{p} \mu(\Sigma_{\mathfrak{p}^2})}{\mu(\Sigma_{\mathfrak{p}})} - 2 \sum_{\mathfrak{p} | 2} \frac{\log \mathrm{N}\mathfrak{p}}{\mu(\Sigma_{\mathfrak{p}})} \sum_{i=1}^{2e_{\mathfrak{p}}+1} i \mu(\Sigma_{\mathfrak{p}^{2i}}) \right) \cdot$$
$$\left(\operatorname*{Res}_{s=1} \zeta_k(s) \right)^2 \prod_{v | \infty} \mu(\Sigma_v) \cdot \prod_{\mathfrak{p}} \left(\left(1 - \frac{1}{\mathrm{N}\mathfrak{p}} \right)^2 \mu(\Sigma_{\mathfrak{p}}) \right) + c_{\Sigma} X$$
$$+ O_{e,n}(h_2(k)^2 X^{\frac{4n+7}{4n+8}+\epsilon} (m|D_k|)^{\frac{1}{n+2}+\epsilon} + h_2(k) X^{\frac{4n+21}{4n+24}+\epsilon} (m|D_k|)^{\frac{3}{2n+12}+\epsilon}),$$

where c_{Σ} is a non-multiplicative constant given in (4.12).

We note that the part of the error involving m is essentially a worst case estimate for when the error is as large as possible. This happens when the primes dividing m are selectively unramified (to use the terminology we established earlier). In the case where L and/or K are either selectively or comprehensively ramified at the primes dividing m, a better error can be obtained manually by following the proof of the theorem.

Without any more gilding the lily, we proceed with proving Theorem 4.0.2. We use the same approach as in Chapter 3 and use the hyperbola method to establish the count. To streamline the argument we handle the second and third sums together as much as possible. The argument will look very similar to the previous chapter, but we feel the argument bears repeating so that the reader can more easily verify the work (especially the error terms).

4.3.1 The First Sum

Recall from Chapter 3 that the first sum in question is simply a double count of quadratic K/k and quadratic L/K. In our context this will be

$$\sum_{\substack{[K:k]=2 \\ D_{K/k}<X^{1/2}}} \sum_{\substack{[L:K]=2 \\ D_{L/K}<X/D_{K/k}}} 1. \tag{4.2}$$

Using Theorem 3.0.3, the inner sum is

$$X\frac{\operatorname{Res}_{s=1} \zeta_k(s)}{\zeta_k(2)} \sum_{\substack{[K:k]=2 \\ D_{K/k}<X^{1/2}}} \frac{L(1,K/k)}{D_{K/k}2^{r_2(K)}L(2,K/k)} + O_{\epsilon,n}\left(h_2(k)^2 X^{\frac{4n+7}{4n+8}+\epsilon}|D_k|^{\frac{1}{n+2}+\epsilon}\right). \tag{4.3}$$

The dependence on the class group of k in the error above is due to the bound $h_2(K) \ll_\epsilon h_2(k)^2 D_K^\epsilon$. If we know k satisfies the ℓ-torsion conjecture for $\ell = 2$, then the dependence on $h_2(k)^2$ in the error term goes away.

Now, if the signature of k is (r_1, r_2), then the possibilities for $r_2(K)$ are $2r_2, \ldots, r_1 + 2r_2$. Therefore, we would like a way of handling the sum of

$$\sum_{\substack{[K:k]=2 \\ D_{K/k}<X \\ r_2(K)=2r_2+j}} \frac{L(1,K/k)}{L(2,K/k)},$$

where $0 \le j \le r_1$. To do this, we will use a series of lemmas similar to the previous chapter.

Lemma 4.3.2 *Let k be a number field and let K/k be a quadratic extension. For $T > 1$,*

$$L(1,K/k) = \sum_{\mathfrak{n}\subset\mathcal{O}_k} \frac{\chi_K(\mathfrak{n})e^{-\mathrm{N}\mathfrak{n}/T}}{\mathrm{N}\mathfrak{n}} + O_{\epsilon,n}\left(\frac{|D_k|^{1/4+\epsilon}D_{K/k}^{1/4+\epsilon}}{T^{1/2}}\right).$$

Proof: We follow the same approach as for Lemma 3.4.2. The only difference is that we use the standard convexity bound for Hecke characters as opposed to the best known subconvextiy bound for Dirichlet characters. □

Lemma 4.3.3 *Let k be a number field of degree n over $\mathbb{Q}$ with signature (r_1, r_2), $\mathfrak{n} \subset \mathcal{O}_k$, $0 \le j \le r_1$, and $X > 1$. If $\mathfrak{n}$ is not a square ideal, then*

$$\sum_{\substack{[K:k]=2 \\ D_{K/k}<X \\ r_2(K)=2r_2+j}} \chi_K(\mathfrak{n}) \ll_{\epsilon,n} h_2(k) X^{\frac{n+2}{n+4}+\epsilon} |D_k|^{\frac{1}{n+4}+\epsilon} \mathrm{N}\mathfrak{n}^{\frac{1}{n+4}+\epsilon}.$$

If $\mathfrak{n}$ is a square, then

$$\sum_{\substack{[K:k]=2 \\ D_{K/k}<X \\ r_2(K)=2r_2+j}} \chi_K(\mathfrak{n}) = X \frac{\binom{r_1}{j} \operatorname{Res}_{s=1} \zeta_k(s)}{2^{r_1+r_2}\zeta_k(2)} \prod_{\mathfrak{p}|\mathfrak{n}} \frac{\mathrm{N}\mathfrak{p}}{\mathrm{N}\mathfrak{p}+1} + O_{\epsilon,n}\left(h_2(k) X^{\frac{n+2}{n+4}+\epsilon} |D_k|^{\frac{1}{n+4}+\epsilon} \mathrm{N}\mathfrak{n}^{\epsilon}\right).$$

Proof: For both cases we will rely on Theorem 3.0.3. Recall that for a prime ideal $\mathfrak{p} \subset \mathcal{O}_k$, the character $\chi_K(\mathfrak{p})$ is 1 if $\mathfrak{p}$ splits in K, -1 if its is inert in K, or 0 if it is ramified in K. We can extend this multiplicatively to any integral ideal $\mathfrak{n} \subset \mathcal{O}_k$.

For the first case, we construct two sets of local conditions for every prime $\mathfrak{p} \mid \mathfrak{n}$. The first such that $\chi_K(n) = 1$ and the second such that it is -1. The main terms will cancel out leaving only the error term.

For the second case, we can simply count all extensions K/k where K is unramified at all the primes dividing $\mathfrak{n}$ since $\chi_K(\mathfrak{n})$ is always 1. The $\binom{r_1}{j}/2^{r_1+r_2}$ appears because for each real embedding of k, we must prescribe how it behaves in K and there are exactly $\binom{r_1}{j}$ ways for there to be exactly j real embeddings of k to ramify in K. □

Lemma 4.3.4 *For a number field k of degree n over $\mathbb{Q}$ with signature (r_1, r_2), let $0 \le j \le r_1$ and $X > 1$. Then*

$$\sum_{\substack{[K:k]=2 \\ D_{K/k}<X \\ r_2(K)=2r_2+j}} \frac{L(1,K/k)}{L(2,K/k)} = \frac{\binom{r_1}{j} \operatorname{Res}_{s=1} \zeta_k(s)}{2^{r_1+r_2}\zeta_k(2)} X \prod_{\mathfrak{p}} \left(1 + \frac{1}{(\mathrm{N}\mathfrak{p}+1)^2}\right) + O_{\epsilon,n}\left(h_2(k) X^{\frac{2n+9}{2n+12}+\epsilon} |D_k|^{\frac{3}{2n+12}+\epsilon}\right).$$

Proof: The proof for this lemma exactly follows that of Lemma 3.4.2 but now using Lemmas 4.3.2 and 4.3.3. □

Lemma 4.3.5 *For a number field k of degree n over $\mathbb{Q}$ with signature (r_1, r_2), let $0 \le j \le r_1$ and $X > 1$. Then*

$$\sum_{\substack{[K:k]=2\\ D_{K/k}<X}} \frac{1}{2^{r_2(K)} D_{K/k}} \cdot \frac{L(1,K/k)}{L(2,K/k)} = \operatorname*{Res}_{s=1} \zeta_k(s) \cdot \frac{3^{r_1}}{2^{2r_1+3r_2}} \cdot \zeta_k(2)(\log X + 1) \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathrm{N}\mathfrak{p}^2} - \frac{2}{\mathrm{N}\mathfrak{p}^3} + \frac{2}{\mathrm{N}\mathfrak{p}^4}\right)$$
$$+ c + O_{\epsilon,n}\left(h_2(k) X^{\frac{-3}{2n+12}+\epsilon} |D_k|^{\frac{3}{2n+12}+\epsilon}\right),$$

where c is given by (4.4).

Proof: We will prove the lemma by using partial summation on the results from Lemma 4.3.4 and summing over all possible j.

We define

$$S_j(X) = \sum_{\substack{[K:k]=2\\ D_{K/k}<X\\ r_2(K)=2r_2+j}} \frac{L(1,K/k)}{L(2,K/k)}.$$

Using partial summation as in the proof of Lemma 3.4.1, we get

$$\sum_{\substack{[K:k]=2\\ D_{K/k}<X\\ r_2(K)=2r_2+j}} \frac{1}{D_{K/k}} \cdot \frac{L(1,K/k)}{L(2,K/k)} = \frac{\binom{r_1}{j} \operatorname*{Res}_{s=1} \zeta_k(s)}{2^{r_1+r_2}\zeta_k(2)} \prod_{\mathfrak{p}} \left(1 + \frac{1}{(\mathrm{N}\mathfrak{p}+1)^2}\right)(\log X + 1)$$
$$+ \int_{1^-}^{\infty} \frac{E_j(t)}{t^2} dt + O_{\epsilon,n}(h_2(k) X^{\frac{-3}{2n+12}+\epsilon} |D_k|^{\frac{3}{2n+12}+\epsilon}),$$

where $E_j(X) = S_j(X) - \frac{\binom{r_1}{j} \operatorname*{Res}_{s=1} \zeta_k(s)}{2^{r_1+r_2}\zeta_k(2)} \prod_{\mathfrak{p}} \left(1 + \frac{1}{(\mathrm{N}\mathfrak{p}+1)^2}\right)$. Now we can define

$$c_j = \int_{1^-}^{\infty} \frac{E_j(t)}{t^2} dt.$$

When we sum over j and weight each result by $\frac{1}{2^{2r_2+j}}$, we obtain the lemma with c defined as

$$c = \sum_{j=0}^{r_1} \frac{1}{2^{2r_2+j}} c_j. \tag{4.4}$$

□

We now use Lemma 4.3.5 on (4.3) and find the first sum to be

$$X\left(\frac{1}{2}\log X + 1\right)\cdot\frac{3^{r_1}\left(\operatorname*{Res}_{s=1}\zeta_k(s)\right)^2}{2^{2r_1+3r_2}}\prod_{\mathfrak{p}}\left(1-\frac{1}{\mathrm{N}\mathfrak{p}^2}-\frac{2}{\mathrm{N}\mathfrak{p}^3}+\frac{2}{\mathrm{N}\mathfrak{p}^4}\right)$$
$$+ cX + O_{\epsilon,n}\left(h_2(k)^2X^{\frac{4n+7}{4n+8}+\epsilon}|D_k|^{\frac{1}{n+2}+\epsilon} + h_2(k)X^{\frac{4n+21}{4n+24}+\epsilon}|D_k|^{\frac{3}{2n+12}+\epsilon}\right). \quad (4.5)$$

4.3.2 The Second and Third Sums

Recall from Chapter 3 that for a quartic number field L, the value $J(L)$ was used to refer to the difference between the relative discriminant of L/K and the discriminant of the flipped field $\phi(K)$. In this case, $J(L) = q^2$ for some integer q. Before diving straight into the remaining sums, we need a brief discussion on what q is in the general number field case. If $L/K/k$ is a quartic D_4 extension and $\phi(K)$ is the flipped field, then $\mathrm{N}_{K/k}\mathfrak{d}_{L/K} = \mathfrak{d}_{\phi(K)/k}\mathfrak{q}^2$ for some integral ideal of $\mathcal{O}_k$ by Lemma 3.2.2. The odd part of $\mathfrak{q}$ will be squarefree, but the even part might not be.

If $\mathfrak{p} \subset \mathcal{O}_k$ divides 2 and $e_{\mathfrak{p}}$ is the ramification index of $\mathfrak{p}$ over 2, the maximal power of $\mathfrak{p}$ that could show up in an admissible $\mathfrak{q}$ is $\mathfrak{p}^{2e_{\mathfrak{p}}+1}$. This is implied by Proposition 3.4 of [12] and can be seen by considering the case where $\mathfrak{p}$ is inert in K and ramifies in L with the maximum possible power of $\mathfrak{p}$ dividing $\mathfrak{d}_{L/K}$.

With that in mind, the second and third sums are

$$\sum_{\mathfrak{q}<X^{1/4}}\ \sum_{\substack{[K:k]=2\\ D_{K/k}<X^{1/2}/\mathrm{N}\mathfrak{q}^2}}\ \sum_{\substack{[L:K]=2\\ D_{L/K}<X^{1/2}\mathrm{N}\mathfrak{q}^2\\ J(L)=\mathfrak{q}^2}} 1, \quad (4.6)$$

and

$$,\sum_{\mathfrak{q}<X^{1/2}}\ \sum_{\substack{[K:k]=2\\ X^{1/2}/\mathrm{N}\mathfrak{q}^2\le D_{K/k}<X^{1/2}}}\ \sum_{\substack{[L:K]=2\\ D_{L/K}<X/D_{K/k}\\ J(L)=\mathfrak{q}^2}} 1 \quad (4.7)$$

where the sums over $\mathfrak{q} < Y$ indicate a sum over admissible ideals $\mathfrak{q} \subset \mathcal{O}_k$ which have norm less than Y, and $J(L)$ denotes the ideal $\mathfrak{q}^2$ in the relationship $\mathrm{N}_{K/k}\mathfrak{d}_{L/K} = \mathfrak{d}_{\phi(K)/k}\mathfrak{q}^2$.

In both (4.6) and (4.7), the innermost sum will be treated exactly as in Chapter 3 by using inclusion/exclusion to get the count of L/K with $J(L) = \mathfrak{q}^2$. In our case, the innermost sum will become

$$\sum_{\substack{[L:K]=2 \\ D_{L/K}<Y \\ J(L)=\mathfrak{q}^2}} 1 = \sum_{\substack{\mathfrak{b}<Y^{1/2}/\mathrm{N}\mathfrak{q} \\ (\mathfrak{b},2\mathfrak{a}\mathfrak{d}_{K/k})}} \mu(\mathfrak{b}) \sum_{\substack{[L:K]=2 \\ D_{L/K}<Y \\ \mathfrak{a}^2\mathfrak{b}^2|\mathfrak{d}_{L/K} \\ J_2(L)=\mathfrak{c}^2}} 1,$$

where $\mathfrak{a}$ and $\mathfrak{c}$ are the odd and even parts of $\mathfrak{q}$, respectively, and $J_2(L)$ is the even part of $\mathfrak{q}^2$. Following the same analytical method, this is

$$Y\frac{\mu(\Sigma_{K,\mathfrak{c}^2})\operatorname{Res}_{s=1}\zeta_k(s)}{2^{r_2(K)}\zeta_k(2)}\prod_{\mathfrak{p}|2}\left(1+\frac{1}{\mathrm{N}\mathfrak{p}}\right)^{-1}\prod_{\mathfrak{p}|\mathfrak{a}}\left(\frac{1}{\mathrm{N}\mathfrak{p}(\mathrm{N}\mathfrak{p}+1)}\right)\prod_{\mathfrak{p}\nmid 2\mathfrak{a}}\left(1+\frac{\chi_K(\mathfrak{p})}{\mathrm{N}\mathfrak{p}+1}\right)$$
$$+ O_{\epsilon,n}\left(h_2(k)^2Y^{\frac{n+1}{n+2}+\epsilon}|D_k|^{\frac{1}{n+2}+\epsilon}D_{K/k}^{\frac{1}{2n+4}+\epsilon}\mathrm{N}\mathfrak{a}^{-\frac{2n+2}{n+2}+\epsilon}+Y^{1/2}\mathrm{N}\mathfrak{q}^{-1}|D_k|^{\epsilon}D_{K/k}^{\epsilon}\right), \quad (4.8)$$

where χ_K is the Hecke character defining K/k, $\Sigma_{K,\mathfrak{c}^2}$ is a set of local conditions at all primes dividing 2 in K such that for any L/K we have $J_2(L) = \mathfrak{c}^2$. Then

$$\mu(\Sigma_{K,\mathfrak{c}^2}) = \prod_{\substack{\mathfrak{P}|2 \\ \mathfrak{P}\subset\mathcal{O}_K}}\sum_{L_\mathfrak{P}\in\Sigma_{K,\mathfrak{P}}}\frac{1}{|\mathrm{Aut}(L_\mathfrak{P}/K_\mathfrak{P})|D_{L_\mathfrak{P}/K_\mathfrak{P}}}. \quad (4.9)$$

We note that all products over primes save for (4.9) are over primes in k as opposed to K.

We will now resolve the error term in (4.8) as it is cumbersome to keep around. If we analyze the error in the sum over K and then over $\mathfrak{q}$ for both cases ($Y = X^{1/2}\mathrm{N}\mathfrak{q}^2$ and $Y = X/D_{K/k}$), the error simplifies to $O_{\epsilon,n}\left(h_2(k)^2X^{\frac{4n+7}{4n+8}+\epsilon}|D_k|^{\frac{1}{n+2}+\epsilon}\right)$.

To continue on, we will rewrite the Euler product over primes not dividing $2\mathfrak{a}$ as the sum

$$\sum_{\substack{\mathfrak{n}\ \square\text{-free} \\ (\mathfrak{n},2\mathfrak{a})=1}}\frac{\chi_K(p)}{f(\mathfrak{n})},$$

where $f(\mathfrak{n})$ is the multiplicative function defined by $f(\mathfrak{p}) = (1+\mathrm{N}\mathfrak{p})$. To analyze this, we will need slight tweaks to Lemmas 4.3.2 – 4.3.4. We will skip the equivalents of

Lemmas 3.4.5 and 3.4.6 and reproduce the equivalent of Lemma 3.4.7 without proof as the techniques are exactly the same.

Lemma 4.3.6 *For any $X \geq 1$ and $0 \leq j \leq r_1$, we have*

$$\sum^*_{\substack{[K:k]=2 \\ D_{K/k}<X \\ (D_k,\mathfrak{a})=1 \\ r_2(K)=2r_2+j}} \sum_{\substack{\mathfrak{n}\ \square\text{-free} \\ (\mathfrak{n},2\mathfrak{a})=1}} \frac{\chi_K(\mathfrak{n})}{f(\mathfrak{n})} = X \frac{\binom{r_1}{j}\mu(\Sigma^*_{k,\mathfrak{c}^2})\operatorname{Res}_{s=1} \zeta_k(s)}{2^{r_1+r_2}\zeta_k(2)} \prod_{\mathfrak{p}|2\mathfrak{a}} \left(1+\frac{1}{\mathrm{N}\mathfrak{p}}\right)^{-1}$$
$$+ O_{\epsilon,n}\left(h_2(k) X^{\frac{2n+9}{2n+12}+\epsilon} |D_k|^{\frac{3}{2n+12}+\epsilon} \mathrm{N}\mathfrak{a}^{\frac{1}{n+4}+\epsilon}\right),$$

where $\sum^*$ indicates the sum over K fixes a particular equivalence class of $K_\mathfrak{p}$ for each $\mathfrak{p} \mid 2$ in k and $\Sigma^*_{k,\mathfrak{c}^2}$ is the restriction of the local conditions to this case.

For the second sum, we can simply use Lemma 4.3.6 to complete the sum over K as the sum over L didn't use $D_{K/k}$ in its bounds. When we sum over all possible j and restrictions of the local conditions at 2, this yields

$$X \frac{3^{r_1}\mu(\Sigma_{\mathfrak{c}^2})\left(\operatorname{Res}_{s=1} \zeta_k(s)\right)^2}{2^{2r_1+3r_2}\zeta_k(2)^2} \prod_{p|2}\left(1+\frac{1}{\mathrm{N}\mathfrak{p}}\right)^{-2} \prod_{\mathfrak{p}|\mathfrak{a}} \left(\frac{1}{(\mathrm{N}\mathfrak{p}+1)^2}\right)$$
$$+ O_{\epsilon,n}\left(h_2(k) X^{\frac{4n+21}{4n+24}+\epsilon} |D_k|^{\frac{3}{2n+12}+\epsilon} \mathrm{N}\mathfrak{a}^{-\frac{2n+9}{n+6}+\frac{1}{n+4}+\epsilon}\right).$$

We then get the final result for the second sum after summing over admissible $\mathfrak{q}$.

$$X \frac{3^{r_1}\left(\operatorname{Res}_{s=1} \zeta_k(s)\right)^2}{2^{2r_1+3r_2}} \prod_{\mathfrak{p}}\left(1-\frac{1}{\mathrm{N}\mathfrak{p}^2}-\frac{2}{\mathrm{N}\mathfrak{p}^3}+\frac{2}{\mathrm{N}\mathfrak{p}^4}\right)$$
$$+ O_{\epsilon,n}\left(h_2(k)^2 X^{\frac{4n+7}{4n+8}+\epsilon}|D_k|^{\frac{1}{n+2}+\epsilon} + h_2(k) X^{\frac{4n+21}{4n+24}+\epsilon}|D_k|^{\frac{3}{2n+12}+\epsilon}\right). \quad (4.10)$$

Now we turn our attention back to the third sum. For this, we will have to use partial summation with Lemma 4.3.6 in the same way that we proved Lemma 4.3.5. When we do this and also take into account all possible restrictions of local conditions and $0 \leq j \leq r_1$ in the sum over K, we get

$$X\frac{3^{r_1}\mu(\Sigma_{\mathfrak{c}^2})\left(\operatorname*{Res}_{s=1}\zeta_k(s)\right)^2}{2^{2r_1+3r_2}\zeta_k(2)^2}\cdot\log\mathrm{N}\mathfrak{q}^2\cdot\prod_{p|2}\left(1+\frac{1}{\mathrm{N}\mathfrak{p}}\right)^{-2}\prod_{\mathfrak{p}|\mathfrak{a}}\left(\frac{1}{(\mathrm{N}\mathfrak{p}+1)^2}\right)$$
$$+O_{\epsilon,n}\left(h_2(k)X^{\frac{4n+21}{4n+24}+\epsilon}|D_k|^{\frac{3}{2n+12}+\epsilon}\mathrm{N}\mathfrak{a}^{-\frac{2n+9}{n+6}+\epsilon}\right).$$

Because log is additive, we will analyze this in the context of the sum over admissible $\mathfrak{q}$ by writing $\mathfrak{q}$ in terms of its odd and even parts and handling them separately. Using the same methods as in Chapter 3, this gives us

$$X\frac{3^{r_1}\left(\operatorname*{Res}_{s=1}\zeta_k(s)\right)^2}{2^{2r_1+3r_2}}\cdot\prod_{\mathfrak{p}}\left(1-\frac{1}{\mathrm{N}\mathfrak{p}^2}-\frac{2}{\mathrm{N}2^3}+\frac{2}{\mathrm{N}\mathfrak{p}^4}\right)\cdot$$
$$\left(2\sum_{\mathfrak{p}\nmid 2}\frac{\log\mathrm{N}\mathfrak{p}\mu(\Sigma_{\mathfrak{p}^2})}{\mu(\Sigma_p)}+2\sum_{\mathfrak{p}|2}\frac{\log\mathrm{N}\mathfrak{p}}{\mu(\Sigma_{\mathfrak{p}})}\sum_{i=1}^{2e_{\mathfrak{p}}+1}i\mu(\Sigma_{\mathfrak{p}^{2i}})\right). \quad (4.11)$$

In the above equation $\mu(\Sigma_{\mathfrak{p}^j})$ is the weight from the set of local conditions on $L/K/k$ such that $J_{\mathfrak{p}}(L)=\mathfrak{p}^j$ and $\mu(\Sigma_{\mathfrak{p}})$ is the weight from the full set of local conditions at that prime.

Theorem 4.0.2 is now proved by combining (4.5), (4.10), and (4.11) with the correct weights.

4.3.3 A Note on the Local D_4 Theorem

Proving Theorem 4.3.1, which also takes into account local conditions, will look a lot like the general case without using any restrictive set of local conditions, so we will not repeat the proof. We will, however, remark on the masses coming from the infinite places of k and define c_Σ from the theorem statement.

Addressing first the infinite places, note that the constant $\frac{3^{r_1}}{2^{2r_1+3r_2}}$ from Theorem 4.0.2 is replaced by $\prod_{v|\infty}\mu(\Sigma_v)$ in Theorem 4.3.1. If the collection Σ is complete at v then $\mu(\Sigma_v)$ is 3/4 if v is real and 1/8 if v is imaginary. As with any place (finite or infinite) where Σ is incomplete $\mu(\Sigma_v)$ would need to be computed manually.

To wrap up c_Σ will be defined along the lines of the discussion in Section 3.4.3.

This will yield

$$c_\Sigma = \sum_{j=0}^{r_1} \frac{1}{2^{2r_2+j}} c_{j,\Sigma}. \tag{4.12}$$

4.4 $D_4 \wr H$ Extensions

We can now finally turn our attention to proving Theorem 4.0.1. In this section k is now a degree d number field, F is a degree n H extension of k, and L is a quartic D_4 extension of F. Given (4.1), the following sum to gives us the result

$$\sum_{\substack{[F:k]=n \\ \mathrm{Gal}(F/k)\cong H \\ D_{F/k}<X^{1/2}}} \sum_{\substack{[L:F]=4 \\ \mathrm{Gal}(L/F)\cong D_4 \\ C_{L/F}<X/D_{F/k}^2}} 1. \tag{4.13}$$

If we start on the obvious track of using Theorem 4.0.2 to analyze the innermost sum, we get the desired main term and use the class group results of [4] to get the error term $O_{\epsilon,dn}\left(X^{1-\frac{4}{dn(4dn+8)}+\epsilon}|D_k|^{n-1/d+\frac{n}{dn+2}+\epsilon} + X^{\frac{4n+21}{4n+24}+\epsilon}|D_k|^{\frac{n}{2}-\frac{1}{2d}+\frac{3n}{2dn+12}+\epsilon}\right)$ coming from the relationship $|D_F| = |D_k|^n D_{F/k}$. The terms relating to D_k in the error term look rather alarming, but k is fixed and as X tends towards infinity, the dependence on D_k will not matter significantly. Note that the assumption that $N_{k,n}(X;H)$ is $O_{k,H,\epsilon}(X^{1+\epsilon})$ is important here. Without it, we cannot guarantee that either the sum over F/k converges or that the error term above is accurate. If we know that the ℓ-torsion conjecture holds for $\ell = 2$ in our H extensions, then the bound on $N_{k,n}(X;H)$ can be relaxed quite a bit more.

We are not yet finished though. As before, we must also show that any number field tower $L/F/k$ counted this way with $G = \mathrm{Gal}(L/k) \ncong D_4 \wr H$ is $o(X \log X)$. To do this we will use a lemma from [21].

Lemma (5 of [21]) *Let $G \le S_n$ be a transitive group containing a transposition. Then:*

1. *All transpositions are conjugated in G.*

2. *$G = S_e \wr H$ for some $1 \neq e, emidn$ and $H \le S_{n/e}$ transitive.*

Klüners uses this lemma to show that any number field tower $L/F/k$ where L/F is quadratic has Galois group $C_2 \wr H$ whenever the Galois group can be shown to have a transposition and where $H = \mathrm{Gal}(F/k)$. We will use it in a similar way to show that the number field tower $L/F/k$ with L/F a quartic D_4 extension has Galois group $\mathrm{Gal}(L/k) = D_4 \wr H$ under the right set of conditions.

Lemma 4.4.1 *Let k be a number field with F/k a degree n extension with Galois group H and L/F a quartic D_4 extension. Let K denote the unique quadratic subfield of L. Assume there exists a rational prime p such that:*

1. *p splits completely in F into $\mathfrak{p}_1, \ldots, \mathfrak{p}_{dn}$*
2. *Exactly one $\mathfrak{p}_i$ in F is inert in K and the rest split completely*
3. *The $\mathfrak{p}_i$ that is inert in K is unramified in L*
4. *Of the remaining $\mathfrak{p}_j, j \neq i$ in F that split completey in K, exactly one of the conjugates in K ramifies in L and the rest are unramified*

Then Gal$(L/k) \cong D_4 \wr H$.

Proof: Assume the hypothesis of the lemma. Because both 1 and 2 are true, the Frobenius element corresponding to p in $\mathrm{Gal}(K/k)$ transposes a pair of embeddings of K because exactly one conjugate of p in K has inertial degree 2 and ramification index 1, while the rest have inertial degree and ramification index 1. Thus, Lemma 5 of [21] shows that $\mathrm{Gal}(K/k) \cong C_2 \wr H$.

Now, with 3 and 4 also being true, the inertia group for p is generated by an element that transposes a pair of embeddings of L because exactly one conjugate of p is ramified in L with ramification index 2 and the rest are unramified. We again use Lemma 5 of [21] and get that $\mathrm{Gal}(L/k) \cong C_2 \wr (C_2 \wr H)$. □

We should note that the conditions from Lemma 4.4.1 are not the only ones under which $\mathrm{Gal}(L/k)$ will be $D_4 \wr H$. Another set of local conditions that will produce the same result is if you have two primes p and q that split completely in F. For p, assume that one conjugate is inert in K, the rest split completely in K. The behavior of the conjugates of p in L can be unrestrained. For q, assume that it also splits completely in K and that exactly on K conjugate is inert in L but the rest split completely. A similar argument to the proof of the lemma also gives the desired Galois group.

It is also not necessary that p be a rational prime that splits completely in F. A prime $\mathfrak{p}$ of k that splits completely in F will also work. We didn't make this more general argument because we will need that $\mathrm{N}\mathfrak{p} = p$ for the proof of the larger theorem.

Proof (Theorem 4.0.1): Let k be a degree d number field and F be a degree n H extension of k. Let S be a finite set of rational primes that split completely in F. We know that we can find such a set by the Chebotarev Density Theorem.

We now need to find the count of D_4 quartic extensions of F that avoid conditions 2-4 in Lemma 4.4.1 at every prime in $p \in S$. This is most easily done by using Theorem 4.3.1 to find the weight of one prime meeting all the conditions of Lemma 4.4.1 and subtract this from the weight of all D_4 quartic extensions at p without any restrictions.

Using

$$\begin{aligned}\mu(\Sigma_{\mathfrak{p}}) &= \sum_{(L_{\mathfrak{p}},K_{\mathfrak{p}})\in\Sigma_{\mathfrak{p}}} \frac{1}{|\mathrm{Aut}(L_{\mathfrak{p}},K_{\mathfrak{p}})|C(L_{\mathfrak{p}},K_{\mathfrak{p}})} \\ &= \sum_{(-,K_{\mathfrak{p}})\in\Sigma_{\mathfrak{p}}} \frac{1}{|\mathrm{Aut}(K_{\mathfrak{p}}/F_{\mathfrak{p}})|D_{K_{\mathfrak{p}}/F_{\mathfrak{p}}}} \prod_{\mathfrak{P}|\mathfrak{p}} \sum_{(L_{\mathfrak{P}},K_{\mathfrak{p}})\in\Sigma_{\mathfrak{p}}} \frac{1}{|\mathrm{Aut}(L_{\mathfrak{P}}/K_{\mathfrak{p}})|D_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}},\end{aligned}$$

we get that the weight for a single prime p that meets all of the conditions of Lemma 4.4.1 is

$$\frac{2n(n-1)}{2^n}\frac{1}{p}. \tag{4.14}$$

We are initially ignoring the degree d of $k/\mathbb{Q}$ as each of the d conjugates of p in k has n conjugates in F and we can treat each of the d k-conjugates separately for our purposes as each one must avoid the conditions of Lemma 4.4.1 for the Galois group not to be $D_4 \wr H$. The $2n(n-1)$ in the denominator comes from the fact that exactly one of the n conjugates of p in F is inert in K, and then exactly one of the

$2(n-1)$ completely split conjugates of p in K ramifies in L.

When we take (4.14) in the context of our full set of primes S, we get that the contribution coming from these primes is

$$\prod_{p\in S}\left(\left(1-\frac{1}{p^2}-\frac{2}{p^3}+\frac{2}{p^4}\right)^n-\frac{2n(n-1)}{2^n}\frac{1}{p}\left(1-\frac{1}{p}\right)^{2n}\right)^d. \tag{4.15}$$

As horrendous as this product may be to look at, the presence of the $1/p$ coming from (4.14) is the key piece to focus on. Because there are infinitely many primes that split completely in F, we can push the primes in the set out towards infinity. As the set of all primes that split completely in F has positive density, this will make (4.15) tend to 0 as the size of S tends towards infinity. This shows that the set of towers $L/F/k$ in our count with Galois group $G \not\cong D_4 \wr H$ is $o(X \log X)$.

Before we wrap up the proof though, we need to comment on the effect of the set S on the error term in Theorem 4.3.1. In the worst case, the error has a positive power for each prime $p \in S$, which will blow up as we send S towards infinity. However, we can let X tend to infinity as we also increase the number of primes in S. As long as X is sufficiently large, the error will be manageable. □

Bibliography

[1] S. Ali Altuğ, Arul Shankar, Ila Varma, and Kevin H. Wilson, *The number of D_4-fields ordered by conductor*, J. Eur. Math. Soc. (JEMS), 23 (2021), pp. 2733–2785.

[2] Manjul Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2), 162 (2005), pp. 1031–1063.

[3] ——, *The density of discriminants of quintic rings and fields*, Ann. of Math. (2), 172 (2010), pp. 1559–1591.

[4] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, and Y. Zhao, *Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves*, J. Amer. Math. Soc., 33 (2020), pp. 1087–1099.

[5] Manjul Bhargava, Arul Shankar, and Jacob Tsimerman, *On the Davenport-Heilbronn theorems and second order terms*, Invent. Math., 193 (2013), pp. 439–499.

[6] Manjul Bhargava, Arul Shankar, and Xiaoheng Wang, *An improvement on schmidt's bound on the number of number fields of bounded discriminant and small degree*, 2022.

[7] Manjul Bhargava, Arul Shankar, and Wang Xiaoheng, *Geometry-of-numbers methods over global fields i: Prehomogeneous vector spaces*. https://arxiv.org/abs/1512.03035.

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

[9] Tullio Ceccherini-Silberstein, Fabio Scarabotti, and Filippo Tolli, *Representation theory and harmonic analysis of wreath products of finite groups*, vol. 410 of London Mathematical Society Lecture Note Series, Cambridge University Press, Cambridge, 2014.

[10] Peter J. Cho and Henry H. Kim, *Probabilistic properties of number fields*, J. Number Theory, 133 (2013), pp. 4175–4187.

[11] Pete Clark, *Algebraic number theory ii: Valuations, local fields and adeles*. http://alpha.math.uga.edu/~pete/8410FULL.pdf.

[12] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier, *Enumerating quartic dihedral extensions of* $\mathbb{Q}$, Compositio Math., 133 (2002), pp. 65–93.

[13] Keith Conrad, *Galois groups of cubics and quartics in all characteristics*. https://kconrad.math.uconn.edu/blurbs/galoistheory/cubicquarticallchar.pdf.

[14] Harold Davenport, *Multiplicative number theory*, vol. 74 of Graduate Texts in Mathematics, Springer-Verlag, New York, third ed., 2000. Revised and with a preface by Hugh L. Montgomery.

[15] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A, 322 (1971), pp. 405–420.

[16] Bart De Smit, *Galois groups and wreath products*. https://www.math.leidenuniv.nl/~desmit/notes/krans.pdf.

[17] Matthew Friedrichsen, *A secondary term for d_4 quartic fields ordered by conductor*, 2021.

[18] Matthew Friedrichsen and Daniel Keliher, *Comparing the density of D_4 and S_4 quartic extensions of number fields*, Proc. Amer. Math. Soc., 149 (2021), pp. 2357–2369.

[19] A. Granville and K. Soundararajan, *The distribution of values of $L(1, \chi_d)$*, Geom. Funct. Anal., 13 (2003), pp. 992–1028.

[20] Henryk Iwaniec and Emmanuel Kowalski, *Analytic number theory*, vol. 53 of American Mathematical Society Colloquium Publications, American Mathematical Society, Providence, RI, 2004.

[21] Jürgen Klüners, *The distribution of number fields with wreath products as Galois groups*, Int. J. Number Theory, 8 (2012), pp. 845–858.

[22] Robert J. Lemke Oliver and Frank Thorne, *The number of ramified primes in number fields of small degree*, Proc. Amer. Math. Soc., 145 (2017), pp. 3201–3210.

[23] Gunter Malle, *On the distribution of Galois groups. II*, Experiment. Math., 13 (2004), pp. 129–135.

[24] H. L. Montgomery and R. C. Vaughan, *The large sieve*, Mathematika, 20 (1973), pp. 119–134.

[25] Hugh L. Montgomery and Robert C. Vaughan, *Multiplicative number theory. I. Classical theory*, vol. 97 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 2007.

[26] Jürgen Neukirch, *Algebraic number theory*, vol. 322 of Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[27] Robert J. Lemke Oliver and Frank Thorne, *Upper bounds on number fields of given degree and bounded discriminant*, 2020.

[28] Ian Petrow and Matthew P. Young, *The Weyl bound for Dirichlet L-functions of cube-free conductor*, Ann. of Math. (2), 192 (2020), pp. 437–486.

[29] Blair K. Spearman and Kenneth S. Williams, *Unramified quadratic extensions of a quadratic field*, Rocky Mountain J. Math., 25 (1995), pp. 783–788.

[30] Takashi Taniguchi and Frank Thorne, *Secondary terms in counting functions for cubic fields*, Duke Math. J., 162 (2013), pp. 2451–2508.

[31] Jiuya Wang, *Secondary term of asymptotic distribution of $S_3 \times A$ extensions over $\mathbb{Q}$*. https://arxiv.org/abs/1710.10693v1.

[32] ——, *Malle's conjecture for $S_n \times A$ for $n = 3, 4, 5$*, Compos. Math., 157 (2021), pp. 83–121.

[33] Melanie Matchett Wood, *Mass formulas for local Galois representations to wreath products and cross products*, Algebra Number Theory, 2 (2008), pp. 391–405.

[34] ——, *On the probabilities of local behaviors in abelian field extensions*, Compos. Math., 146 (2010), pp. 102–128.

[35] ——, *Asymptotics for number fields and class groups*, in Directions in number theory, vol. 3 of Assoc. Women Math. Ser., Springer, [Cham], 2016, pp. 291–339.

[36] David J. Wright, *Distribution of discriminants of abelian extensions*, Proc. London Math. Soc. (3), 58 (1989), pp. 17–50.