Analytic Estimates of Class Numbers and Relative Class Numbers

Korneel Debaene

A DISSERTATION PRESENTED
TO
THE FACULTY OF SCIENCES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF SCIENCE: MATHEMATICS

PROMOTOR : PROF. DR. ANDREAS WEIERMANN
CO-PROMOTOR : PROF. DR. JAN-CHRISTOPH SCHLAGE-PUCHTA

GHENT UNIVERSITY
GHENT, BELGIUM
MAY 2015

Contents

Acknowledgments

I am profoundly grateful for the role that Jan-Christoph Schlage-Puchta and Andreas Weiermann have played as my promotors. Andreas, thank you for all your help in overcoming administrative hurdles — this dissertation would quite literally not have been possible without your support. Jan-Christoph, thank you for imparting on me your perspective on research, for sharing all your valuable ideas, and for your patient encouragement through the years.

Several people have been of indispensable help to finish this dissertation. The typographical, literary, and mathematical qualities of this dissertation have benefited enormously from the proofreading efforts, most notably by Bert Seghers and Greet Derudder, and also by Wouter Castryck, Karsten Naert, Andreas Debrouwere, Jasson Vindas, and Martine Vanacker. I am very much indebted to Marie Debaene for designing the magnificent cover.

To all those that have had a positive influence on my nascent mathematical life, I offer a sincere thanks. I will not attempt to make an exhaustive list, but in any case I cannot omit my formidable office mate Karsten Naert, with whom I have enjoyed countless conversations, as well as Andreas Debrouwere, Bert Seghers, Jeroen Van der Meeren, and Jan Vonk. I also acknowledge that this dissertation is not only the culmination of a mathematics education, but also reliant on a good upbringing, for which I thank my parents.

Lastly, Laure, where would I be if it wasn't for your overwhelmingly colourful, adventurous, and loving spirit, which has filled my last five years with such love. Thank you for rocking my world.

The Road goes ever on and on
Down from the door where it began.
Now far ahead the Road has gone,
And I must follow, if I can,
Pursuing it with eager feet,
Until it joins some larger way
Where many paths and errands meet.
And whither then? I cannot say.

J.R.R. Tolkien

0

Preface

The main theme of this dissertation lies within the field of analytic number theory. Broadly put, the goal is to investigate some arithmetic properties of algebraic number fields. More precisely, we focus our attention on the class number and the completely splitting primes. The methods lie predominantly in sieve theory and the theory of L-functions.

In this preface, we refrain from addressing at length the mathematical content of this dissertation, and will instead start each chapter with a comprehensive introduction. Nevertheless we trust that the theme which connects the different chapters will be apparent.

We wish to make a few comments on the style of this dissertation. Firstly, a dissertation should in our opinion not be written like a syllabus, it should not quite be written like a book, nor should it be written completely like a research article. We would hope it to be in small part a popularising piece, in part a review article, and for the biggest part a research article.

We will strive to be sufficiently narrative and descriptive in at least the introductions to each chapter to give the unacquainted reader a sense, a feeling, an intuition of what this research is about. Hence, it is not our intention to be self-contained, or even to define all relevant concepts. We are not misguided by the belief that the readers who do not already know the basic definitions would merit by the inclusion of them. Nor do we think it helpful to prove basic lemmata for those readers who would not be able to supply (or look up) a proof themselves.

While, necessarily, the complexity of the introductions will escalate quickly, we will try to give priority to the "why" rather than to the "what exactly". At the same time, this informal style of highlighting only some portions of the buildup can also be of value to the cognoscenti. We hope to impart on those knowledgeable readers our perspective, what we perceive as the key motivations and the basis fundaments.

All proofs included in the text are original proofs. It is conceivable that the essence of some lemmata might already be contained in the literature, but all theorems which we prove in this dissertation are new contributions to science. Section 2.2 forms the only exception to this rule, where we prove a reciprocity law whose precise statement is in principle new, but the proof is not; it is essentially a simplified version of the proof of Eisenstein's Reciprocity Law in [26].

1

Cyclotomic Fields

1.1 Introduction

How are the arithmetic laws governed once one transcends beyond the integers? This extremely basic question underlies much of the corpus of Algebraic Number Theory. It is a question that naturally comes up when one is interested in finding integer or rational solutions to diophantine equations.

If one ponders the possibility of integral solutions to

$$x^p + y^p = z^p,$$

one would like to somehow make use of the factorisation

$$x^p + y^p = \prod_{i=0}^{p} (x + \zeta_p^i y), \qquad \text{where } \zeta_p = e^{\frac{2\pi i}{p}}.$$

Indeed, one early motivation for starting the exploration of Ideal Theory by Kummer was the implications that knowledge on the arithmetic of $\mathbb{Z}[\zeta_p]$ would have to Fermat's Last Theorem via the above factorisation. Put more concretely, if all factors $x + \zeta_p^i y$ would for example be coprime, then one might hope that their product being equal to z^p, a p-th power, implies that all factors are already p-th powers. The story goes that in 1847, Lamé put this idea forward as a starting point of his attempted proof of Fermat's Last Theorem, implicitly assuming that the properties of $\mathbb{Z}$ carry over to the ring $\mathbb{Z}[\zeta_p]$. Lamé's idea was rebutted by Liouville, but his key idea was picked up by Kummer who devoted his attention to the arithmetical structure of $\mathbb{Z}[\zeta_p]$ in order to salvage a proof for Fermat's Last Theorem. He succeeded for a certain subset of the primes, which he christened as *regular primes*.

There are three basic features which distinguish rings of integers in number fields from the integers $\mathbb{Z}$ in $\mathbb{Q}$.

The first is one is the fact that while in the set of *ideals* the law of unique factorisation in prime factors holds, it is not so in general that all ideals are principal, which prevents one to carry this over to unique factorisation of integral elements in prime elements. The standard way that one can express the deviation of the ring of integers from a principal ideal domain is by means of the class group CL_K, the quotient of the group of non-zero fractional ideals by the principal ideals. We shall mainly consider the class number h_K, the order of the class group. Most notably, $h_K = 1$ is equivalent to disposing of unique factorisation in prime elements.

The second feature is the existence of many units, that is, integral elements whose multiplicative inverse is an integral element. This further impedes the possibility to pass from ideals to elements. Especially problematic is the highly non-trivial subject of their absolute value, when embedded in $\mathbb{C}$. One measure of the absolute value of the units is the so-called regulator Reg_K.

The third feature is harder to describe in simple terms, and is arguably of lesser importance. It is the discriminant Δ_K, which can be interpreted either as a measure of *volume* of the ring of integers, or as a measure of ramification.

A beautiful result connecting these three quantities to the Dedekind-zeta function of K is the Analytic Class Number Formula.

Theorem 1.1. *(Analytic Class Number Formula) Let K be a number field of degree n, with r_1 real embeddings and r_2 pairs of complex embeddings. Denote by Δ_K the discriminant of the field, Reg_K the regulator, h_K the class number,* *and ω the number of roots of unity inside K. Then, if $\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$ is the Dedekind-zeta function of K, we have that*

$$\mathrm{res}_{s=1}\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}\mathrm{Reg}_K h_K}{\omega\sqrt{\Delta_K}}$$

This formula opens the doors to wielding analytic arguments to extract arithmetic information. Generally speaking, the strategy in applying the formula can be summarised as follows. The goal is to obtain bounds on h_K, the discriminant Δ_K can more or less be computed exactly, but ones attempts are thwarted by the regulator Reg_K. Even for real quadratic fields, which possess but a one-dimensional unit group, the mysterious nature of the size of the generator of the unit group is the key obstacle to making use of the Analytic Class Number Formula as one can do for imaginary quadratic fields, which do not possess any unwanted units.

We consider the cyclotomic fields $K = \mathbb{Q}(\zeta_\ell)$, where ℓ is an odd prime, whose property of containing a totally real subfield $K^+ = \mathbb{Q}(\zeta_\ell + \zeta_\ell^{-1})$ of index 2 we will exploit. One can show that the class number h_ℓ^+ of K^+ divides the class number h_ℓ of K. The quotient is denoted h_ℓ^- and is called the first factor of the class number, or the relative class number. This brings to mind the fact that Kummer's *regular primes* are those primes for which ℓ does not divide h_ℓ. The reason we consider K^+ is that the units in K are generated by the units of K^+ together with the roots of unity, and one may deduce that

$\mathrm{Reg}_K = 2^{\frac{\ell-3}{2}}\mathrm{Reg}_K^+$, so that we have eliminated the difficulty in applying the Analytic Class Number Formula to estimate the class number. We note that the subfield K^+ corresponds to the group of even Dirichlet characters mod ℓ. Thus, upon dividing the respective Analytic Class Number Formulas for K and K^+, we obtain (see[46] for full details)

$$h_\ell^- = 2\ell \left(\frac{\ell}{4\pi^2}\right)^{\frac{\ell-1}{4}} \prod_{\chi \bmod \ell,\ \text{odd.}} L(1,\chi). \tag{1.1}$$

We define $G(\ell) = 2\ell\left(\frac{\ell}{4\pi^2}\right)^{\frac{\ell-1}{4}}$. The hypothesis that h_ℓ^- is asymptotically equivalent to $G(\ell)$ is known as Kummer's Conjecture, and is deemed unlikely to be true. Granville has shown it to be false if one assumes the thruth of the Elliot-Halberstam and Hardy-Littlewood conjectures[11].

We will for a moment digress from our main discourse to highlight the dichotomy between effective and ineffective results in number theory. Any asymptotic statement can be said to be either effective or ineffective. Ineffectivity occurs when a certain statement (e.g. the behaviour of a certain function) is attested to hold whenever some parameter is big enough — but one cannot determine what "big enough" is. The statement thus contains an existential quantifier which we cannot replace with a concrete value.

We give an example of a very important but ineffective theorem due to Siegel, which is the source of ineffectivity in many theorems throughout analytic number theory. A proof can be found in [19, p.123]

Theorem 1.2. *(Siegel) Let χ be a primitive real character of modulus q.*

1. *For any $\varepsilon > 0$, there is a $c_1(\varepsilon) > 0$ such that $L(1,\chi) > c_1(\varepsilon)q^{-\varepsilon}$.*

2. *For any $\varepsilon > 0$, there is a $c_2(\varepsilon) > 0$ such that any real zero β of $L(s,\chi)$ satisfies $\beta < 1 - c_2(\varepsilon)q^{-\varepsilon}$.*

An effective version of Siegel's theorem does exist if one restricts to $\varepsilon > \frac{1}{2}$, but for smaller ε the constants $c_1(\varepsilon)$ and $c_2(\varepsilon)$ remain ineffective. By contrast, effective results are free of undeterminable constants. While it is not required that all constants are explicit, it should be shown that in principle, all implied constants can be replaced by a concrete, computable value. When it comes to applying theorems, effectivity is often an invaluable property.

Let us return to our main narrative, the estimation of the class number of the ℓ-th cyclotomic field by analytic methods. One of the earliest results is the following. Ankeny and Chowla[1] proved the following estimate on h_ℓ^-, relying heavily on the Siegel-Walfisz theorem — a theorem which has the same issue of ineffectiveness as the above theorem by Siegel.

Theorem 1.3. *(Ankeny-Chowla, '49) We have that*

$$\log\left(\frac{h_\ell^-}{G(\ell)}\right) = o(\log \ell).$$

This theorem already shows that roughly, the size of h_ℓ^- corresponds to $G(\ell)$, up to multiplication by $\ell^{o(1)}$. Tatuzawa[45] improved upon this, actually proving an effective upper bound, but an ineffective lower bound by using Siegel's Theorem.

Theorem 1.4. *(Tatuzawa, '52) For any positive* ε*, there exists a constant* $c(\varepsilon)$ *and an absolute constant* c *such that*

$$\frac{c(\varepsilon)}{\ell^{\varepsilon}} < \frac{h_\ell^-}{G(\ell)} < (\log \ell)^c.$$

The lower bound is of roughly the same quality as Ankeny and Chowla's, but the upper bound already shows that h_ℓ^- is at most $G(\ell)$ times a constant power of $\log \ell$.

Given the numerical data for the (relative) class numbers in Table 1.1, there seemed to be overwhelming experimental and theoretical support for the fact that $h_\ell^- = 1$ only for the primes $\ell \leq 19$. However, due to the ineffective nature of the lower bounds, the possibility of some large ℓ having h_ℓ^- equal to one could not be excluded. For this the world had to wait until 1976 when Montgomery and Masley[29] proved the following.

Theorem 1.5. *(Masley-Montgomery, '76) Let* $\ell \geq 200$ *be an odd prime. Then*

$$|\log(\frac{h_\ell^-}{G(\ell)})| \leq 7 \log \ell,$$

and thus the prime cyclotomic field $\mathbb{Q}(\zeta_\ell)$ *has class number* 1 *if and only if* $\ell \leq 19$.

ℓ	h_ℓ		ℓ	h_ℓ	
3	1		42	211	= 211
5	1		47	695	$= 5 \cdot 139$
7	1		53	4889	= 4889
11	1		59	41241	$= 3 \cdot 59 \cdot 233$
13	1		61	76301	$= 41 \cdot 1861$
17	1		67	853513	$= 67 \cdot 12739$
19	1		71	3882809	$= 7^2 \cdot 79241$
23	3	= 3	73	11957417	$= 89 \cdot 134353$
29	8	$= 2^3$	79	100146415	$= 5 \cdot 53 \cdot 377911$
31	9	$= 3^2$	83	838216959	$= 3 \cdot 279405653$
37	37	= 37	89	13379363737	$= 113 \cdot 118401449$
41	121	$= 11^2$	97	411322824001	$= 577 \cdot 3457 \cdot 206209$

Table 1.1: Values for the Class number h_ℓ. For ℓ in this range, $h_\ell = h_\ell^-$. The first irregular primes are 37, 59, 67.

They also determined all composite moduli for which the cyclotomic field has unique factorisation.

Their method was not to use cancellation in $\sum_\chi \log(L(1,\chi))$ in the form of e.g. Siegel-Walfisz, since these results are ineffective, but instead to bound $\sum_\chi \log(L(s,\chi))$ absolutely by a function which diverges as $s \to 1$. Then, using a zero-free region of the L-functions, the Borel-Carathéodory lemma can be used to yield a constant upper bound to the derivative in a neighbourhood of $s = 1$.

Schlage-Puchta[38] has improved upon this by introducing two new ideas. The first is to iterate the method in a certain way using higher derivatives as well. The second is to use a bigger zero-free region in order to have a stronger bound on the derivative, at the cost of dealing with a possible Siegel zero. A Siegel zero is defined as a zero of a Dirichlet L-function of modulus ℓ, which is inside the open ball $B(1, \frac{1}{c\log \ell})$ for a certain constant c. If c is big enough, it is known that there can be at most one L-function of modulus ℓ with a Siegel zero, which is then necessarily real and simple, and the associated character is quadratic. It is worth mentioning that if $\ell = 1 \bmod 4$, the odd characters are not quadratic, hence have no Siegel zero. Furthermore, the number of moduli for which a Siegel zero can exist is limited, see [5] for a comprehensive treatment. We use the index notation to denote iterated logarithms, e.g. $\log_2(x) = \log\log(x)$.

Theorem 1.6. *(Schlage-Puchta, '00) We have that*

$$\log(h_\ell^-/G(\ell)) = \log(1-\beta) + O((\log_2 \ell)^2),$$

where β is a Siegel zero of an L-series mod ℓ, and this term does only occur if such a zero is present and $\ell \equiv 3 \bmod 4$.

Finally, our improvement in [6] consists of a more efficient implementation of the idea of iterating the method using higher derivatives, and yields the following.

Theorem 1.7. *If no Siegel zero is present among the odd Dirichlet L-functions of conductor ℓ, then the relative class number of $\mathbb{Q}(\zeta_\ell)$ satisfies*

$$|\log(h_\ell^-/G(\ell))| \leq 2\log_2 \ell + O(\log_3 \ell)$$

If there is a Siegel zero β present among the odd Dirichlet L-functions of conductor ℓ, then the relative class number of $\mathbb{Q}(\zeta_\ell)$ satisfies

$$|\log(h_\ell^-/G(\ell)) - \log(1-\beta)| \leq 4\log_2 \ell + O(\log_3 \ell)$$

Since $\log(1-\beta)$ is negative, an upper bound without this term may be deduced. Since $\beta > 1 - \frac{1}{c\log \ell}$, the term $-\log(1-\beta)$ is at least $\log_2 \ell$, thus the above result can be seen to be qualitatively optimal in the sense that the error term is of the size of a possible main term. We also mention that this result sharpens the best known estimate, by Lepistö [27]. Indeed, he proves an upper bound for $\log(h_\ell^-/G(\ell))$ with main term $5\log_2 \ell$.

Finally, we mention that one can do better if one is only concerned with a subset of the primes. Murty and Petridis succeed in proving that for almost all ℓ, h_ℓ^- equals $G(\ell)$ up to a constant factor.

Theorem 1.8. *(Murty-Petridis, '01) There exists a positive constant c such that for almost all odd primes ℓ*

$$c^{-1} \leq \frac{h_\ell^-}{G(\ell)} \leq c.$$

That is, the number of primes up to x satisfying the bounds is asymptotic to $x/\log x$ as $x \to \infty$.

Assuming the Elliot-Halberstam conjecture they can replace c by $1+\varepsilon$. We will now give a detailed account of the proof of our Theorem 1.7.

1.2 Arithmetic Input

It is opportune to study the logarithm of equation (1.1) because the orthogonality property of characters gives us

$$\begin{aligned}\sum_{\chi \bmod \ell,\, \mathbf{odd}} \log(L(s,\chi)) &= \sum_{p^m}\sum_{\chi} \frac{\chi(p^m)}{mp^{ms}} - \sum_{p^m}\sum_{\chi\, \mathbf{even}} \frac{\chi(p^m)}{mp^{ms}} \\ &= \frac{\ell-1}{2}\left(\sum_{p^m\equiv 1(\ell)} \frac{1}{mp^{ms}} - \sum_{p^m\equiv -1(\ell)} \frac{1}{mp^{ms}}\right). \qquad (1.2)\end{aligned}$$

In this section, we will use the equality (1.2) and a Brun-Titchmarsh inequality to bound the sums over prime powers $\pm 1 \bmod \ell$. We will not try to exploit the minus sign in (1.2). In order to cleanly handle the contribution of the prime powers, we define

$$\Pi(x,\ell,a) = \sum_{p^m \le x, p^m \equiv a(\ell)} \frac{1}{mp^m},$$

where p^m ranges over the prime powers. A Brun-Titschmarsh style bound is given by the following lemma.

Lemma 1.9. *Let ℓ be an odd prime. For $x > \ell$, and $\ell > 500$ we have that*

$$\Pi(x,\ell,\pm 1) \le \frac{2x}{(\ell-1)\log(x/\ell)}.$$

Proof. When $x \ge \ell^2$, we start from the following inequality (see [29], Lemma 1)

$$\Pi(x,\ell,\pm 1) \le \pi(x,\ell,\pm 1) + \frac{4\sqrt{x}}{\ell} + \log x.$$

In [33] the following strong version of the Brun-Titchmarsh inequality is proven

$$\pi(x,\ell,\pm 1) \le \frac{2x}{(\ell-1)(\log(x/\ell)+5/6)}.$$

Thus we only need to prove that

$$\frac{4\sqrt{x}}{\ell} + \log x < \frac{2x}{(\ell-1)}\left(\frac{1}{\log(x/\ell)} - \frac{1}{\log(x/\ell)+5/6}\right).$$

By setting $x = \ell X$, $X \geq \ell$, it suffices to prove that

$$g(X) := \frac{4}{\sqrt{\ell}} + \frac{\log(\ell X)}{\sqrt{X}} < h(X) := \frac{5\sqrt{X}}{3(\log X + 5/6)^2}.$$

Now, $g(X)$ decreases for $X \geq e^2$ and $h(X)$ increases for $X \geq e^{19/6}$, hence it suffices to check that

$$g(\ell) = \frac{4}{\sqrt{\ell}} + \frac{2\log(\ell)}{\sqrt{\ell}} < h(\ell) = \frac{5\sqrt{\ell}}{3(\log \ell + 5/6)^2}$$

for $\ell \geq 500$. Now, $g(\ell)$ decreases for $\ell \geq 2$ and $h(\ell)$ increases for $\ell \geq e^{19/6}$, hence it suffices to check that $g(500) < h(500)$, which is clear.

When $\ell < x < \ell^2$, any two prime powers in the sum $\Pi(x, \ell, \pm 1)$ are necessarily coprime. Indeed, their quotient would be $1 \bmod \ell$, so at least $\ell + 1$, implying that the smallest one should be less than $\frac{\ell^2}{\ell+1}$. The only option then is that $\ell - 1 = 2^m$ and $\ell^2 - 1 = 2^k$, but except for $\ell = 3$ this is impossible. Thus, $\Pi(x, \ell, \pm 1) \leq N(x, Q, \ell, \pm 1) + \pi(Q)$, where $N(x, Q, \ell, a)$ is the number of integers $n \equiv a \bmod \ell$, $n \leq x$ such that n is not divisible by any prime number less then Q. We may bound $\pi(Q)$ trivially by Q, so that the quantity to be bounded is $N(x, Q, \ell, \pm 1) + Q$.

In the proof of the Brun-Titchmarsh inequality

$$\pi(x, \ell, \pm 1) \leq \frac{2x}{(\ell - 1)\log(x/\ell)}$$

using the large sieve, as in [32, p.42-44], the first step is to bound $\pi(x, \ell, \pm 1)$ by exactly the quantity $N(x, Q, \ell, \pm 1) + Q$. This shows that in this range of x, the large sieve method for the Brun-Titchmarsh inequality can be applied with the same success for prime powers as for primes. $\square$

Let us define $f(s)$ by

$$f(s) = \Big(\sum_{\chi(-1)=-1} \log L(s, \chi) \Big) - \log(s - \beta),$$

in case that any of the L-functions with χ odd has a Siegel zero β in $]1 - \frac{1}{c \log \ell}, 1]$, where c is some big enough constant. Otherwise, we leave out the term with the Siegel zero. In any case f is holomorphic in $B(1, \frac{1}{c \log \ell})$.

Lemma 1.10. *For any c, $\ell \geq 500$, and $\sigma \in]1, 1 + \frac{1}{c \log \ell}]$, we have the following estimates.*

$$|f(\sigma)| \leq (1 + 1_\beta) \log \Big(\frac{1}{\sigma - 1} \Big) + \frac{3}{2} \tag{1.3}$$

$$|f^{(\nu)}(\sigma)| \leq \big(1 + 1_\beta + c_{\ell,\nu} \big) \frac{(\nu - 1)!}{(\sigma - 1)^\nu}, \tag{1.4}$$

where the notation 1_β stands for 1 if a Siegel zero is present and 0 otherwise, and we may choose the $c_{\ell,\nu}$ to be equal to $\frac{\log(2)}{2c^\nu (\nu-1)! \log \ell} + \frac{\log_2(\ell) + \log(c) - \log_2(2) + e^{-1}}{c^\nu (\nu-1)!} + \frac{1}{c \log \ell} + \frac{\sigma \lfloor \log \nu \rfloor}{\nu - \lfloor \log \nu \rfloor} + \frac{\sigma \nu}{c^{\lfloor \log \nu \rfloor} \lfloor \log \nu \rfloor !}$.

Proof. The case $\nu = 0$ can be proven as in [29]. The estimates for the derivatives are stated in [38], but the statement is slightly incorrect and the proof omitted, so we will prove them here in full. We bound the sums occurring in the ν-th derivative of (1.2) using Lemma 1.9 and partial summation.

$$
\begin{aligned}
\frac{\ell-1}{2}\sum_{p^m\equiv 1(\ell)}\frac{(m\log p)^\nu}{mp^{m\sigma}} &= \frac{\ell-1}{2}\int_{2\ell}^{\infty}\frac{(\log x)^\nu d(\Pi(x,\ell,1))}{x^\sigma}\\
&= \frac{\ell-1}{2}\int_{2\ell}^{\infty}\frac{\sigma x^{\sigma-1}(\log x)^\nu-\nu x^{\sigma-1}(\log x)^{\nu-1}}{x^{2\sigma}}\Pi(x,\ell,1)dx\\
&\leq \int_{2\ell}^{\infty}\frac{\sigma(\log x)^\nu}{x^\sigma\log(x/\ell)}dx\\
&= \frac{\ell\sigma}{\ell^\sigma}\int_{2}^{\infty}\frac{(\log x+\log\ell)^\nu}{x^\sigma\log x}dx =: I,
\end{aligned}
$$

where we possibly omitted the first term $\frac{(\ell-1)\log(\ell+1)^\nu}{2m(\ell+1)^\sigma}$ if $\ell+1$ is a prime power p^m. If this is the case, then $p=2$ and $m=\log(\ell+1)/\log(2)$. This term is smaller than $\varepsilon_1\frac{(\nu-1)!}{(\sigma-1)^\nu}$ for all σ in the desired range for $\varepsilon_1=\frac{\log(2)}{2c^\nu(\nu-1)!\log\ell}$. We expand the integrand with the binomial theorem, and get

$$
\begin{aligned}
I &= \frac{\ell\sigma}{\ell^\sigma}(\log\ell)^\nu\int_2^\infty\frac{1}{x^\sigma\log x}dx+\frac{\ell\sigma}{\ell^\sigma}\sum_{i=0}^{\nu-1}\frac{\nu!(\log\ell)^i}{(\nu-i)!i!}\int_2^\infty\frac{(\log x)^{\nu-i-1}}{x^\sigma}dx\\
&\leq \frac{\ell\sigma}{\ell^\sigma}(\log\ell)^\nu\int_2^\infty\frac{1}{x^\sigma\log x}dx+\frac{(\nu-1)!}{(\sigma-1)^\nu}\frac{\ell\sigma}{\ell^\sigma}\sum_{i=0}^{\nu-1}\frac{\nu}{\nu-i}\frac{((\sigma-1)\log\ell)^i}{i!},
\end{aligned}
$$

where we have used the identity

$$
\int_1^\infty\frac{(\log x)^a}{x^\sigma}dx=\int_0^\infty\frac{t^a}{e^{(\sigma-1)t}}dt=\frac{a!}{(\sigma-1)^{a+1}}.
$$

We consider first the term

$$\begin{aligned}
\frac{\ell\sigma}{\ell^\sigma}(\log \ell)^\nu \int_2^\infty \frac{1}{x^\sigma \log x} dx &= \frac{\ell\sigma}{\ell^\sigma}(\log \ell)^\nu \int_{\log 2}^\infty e^{-(\sigma-1)t}\frac{dt}{t} \\
&\leq \frac{\ell\sigma}{\ell^\sigma}(\log \ell)^\nu \left(\int_{(\sigma-1)\log 2}^1 \frac{1}{t}dt + \int_1^\infty e^{-t}dt\right) \\
&\leq (\log \ell)^\nu \left(\log(\frac{1}{\sigma-1}) - \log_2(2) + e^{-1}\right),
\end{aligned}$$

because $\ell\sigma \leq \ell^\sigma$. We now seek the ε_2 such that

$$(\log \ell)^\nu \left(\log(\frac{1}{\sigma-1}) - \log_2(2) + e^{-1}\right) \leq \varepsilon_2 \frac{(\nu-1)!}{(\sigma-1)^\nu}.$$

If we put $\varepsilon_2 = \frac{\log_2(\ell)+\log(c)-\log_2(2)+e^{-1}}{c^\nu(\nu-1)!}$, the inequality holds for $\sigma \to 1$ and for $\sigma = 1 + \frac{1}{c\log \ell}$. One may check that the derivative of the difference does not have a zero in the interval under consideration if $\ell > e^e$. Thus the difference is monotone, and the inequality holds throughout.

To deal with the rest of the terms efficiently, write $X = (\sigma-1)\log \ell \leq 1/c$. Then we have for any integer $B \geq 1$

$$\begin{aligned}
\frac{\ell\sigma}{\ell^\sigma}\sum_{i=0}^{\nu-1}\frac{\nu}{\nu-i}\frac{X^i}{i!} &\leq \frac{\ell\sigma}{\ell^\sigma}\sum_{i=0}^{B-1}\frac{\nu}{\nu-B}\frac{X^i}{i!} + \frac{\ell\sigma}{\ell^\sigma}X^B\sum_{i=B}^{\nu-1}\frac{\nu}{B!}\frac{X^{i-B}}{(i-B)!} \\
&\leq \frac{\ell\sigma}{\ell^\sigma}\frac{\nu}{\nu-B}e^X + \frac{\ell\sigma}{\ell^\sigma}\frac{\nu}{c^B B!}e^X = \frac{\nu\sigma}{\nu-B} + \frac{\nu\sigma}{c^B B!}
\end{aligned}$$

We now put $B = \lfloor \log \nu \rfloor$, and see that the sum is bounded by $(1+\varepsilon_3)\frac{(\nu-1)!}{(\sigma-1)^\nu}$, where $\varepsilon_3 = \frac{1}{c\log \ell} + \frac{\sigma\lfloor\log\nu\rfloor}{\nu-\lfloor\log\nu\rfloor} + \frac{\sigma\nu}{c^{\lfloor\log\nu\rfloor}\lfloor\log\nu\rfloor!}$

One may now bound $\varepsilon_1 + \varepsilon_2 + \varepsilon_3$ by the coefficient of $\frac{(\nu-1)!}{(\sigma-1)^\nu}$ except the 1_β in the statement of the lemma. We note that the sum over the prime powers congruent to $-1 \bmod \ell$ obeys the same bound, with the same proof as above. One of the sums is strictly positive and the other is strictly negative, thus we have proven that

$$|f^{(\nu)}(s) + (\log(\sigma-\beta))^{(\nu)}| \leq (1 + c_{p,\nu})\frac{(\nu-1)!}{(\sigma-1)^\nu},$$

or since $\frac{(\nu-1)!}{(\sigma-\beta)^\nu} \leq \frac{(\nu-1)!}{(\sigma-1)^\nu}$,

$$|f^{(\nu)}(s)| \leq (1 + 1_\beta + c_{p,\nu})\frac{(\nu-1)!}{(\sigma-1)^\nu}. \qquad \square$$

1.3 Analytic Input

On the other hand we can prove the following bound on the derivatives of f to the right of $s = 1$, using the holomorphic property of f on $B(1, \frac{1}{c\log\ell})$, when c is big enough. We note that due to Kadiri ([20], Theorem 12.1) the value $c = 6.4355$ is big enough.

Lemma 1.11. *For $c > 6.4355$, $\frac{\ell-1}{\log\ell} > c$, and $\sigma \in [1, 1 + \frac{2}{c\log\ell}]$, we have that*

$$|f^{(\nu)}(\sigma)| \leq 2c^\nu \nu!\, \ell \log^{\nu+1}\ell. \tag{1.5}$$

Proof. Recall the lemma of Borel-Caratheodory (see [7], p. 12) which states that if g is holomorphic, $\Re(g(s)) \leq M$ in $B(\sigma_0, R)$ and $g(\sigma_0) = 0$, then

$$|g^{(\nu)}(s)| \leq \frac{2M\nu!}{(R-r)^{\nu}}, \qquad s \in B(\sigma_0, r).$$

We wish to apply this to $f(s) - f(\sigma_0)$. This function vanishes at σ_0, and is holomorphic as long as $R \leq \sigma_0 - (1 - \frac{1}{c\log\ell})$. For the bound on the real part, consider

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = s\int_1^{\infty} \frac{\sum_{n\leq x}\chi(n)}{x^{s+1}}dx.$$

Since $|\sum_{n=1}^{x}\chi(n)| \leq \frac{\ell}{2}$, we have that $|L(s,\chi)| \leq |s|\int_1^{\infty}\frac{|\sum_{n\leq x}\chi(n)|}{x^{\sigma+1}}dx \leq \frac{|s|\ell}{2\sigma}$. This means that

$$\Re(f(s)) \leq \frac{\ell-1}{2}(\log\ell + \log(|s|/2\sigma)) - \log(|s-\beta|),$$

for s on the border of the domain determined by $3/4 < \Re(s) < 2$, $|\Im(s)| \leq \frac{1}{4}$, $|s|/2\sigma \leq \sqrt{10}/6$ and say $|s-\beta| > 1/8$, thus this bound is smaller than $\frac{\ell-1}{2}\log\ell$. Since $f(s)$ is harmonic with at most logarithmic singularities in which $\Re(f) \to -\infty$, the same bound also holds inside the domain. In the region $\sigma > 1$, consider the following estimation

$$|\Re(\log L(s,\chi))| = |\Re\Big(\sum_{p^m}\frac{\chi(p^m)}{mp^{ms}}\Big)| \leq \sum_{p^m}\frac{1}{mp^{ms}} = \log\zeta(\sigma) \leq \log(\frac{\sigma}{\sigma-1}),$$

consequently if $\sigma_0 > \ell/(\ell-1)$, then $|\Re(f(\sigma_0))| \leq \frac{\ell-1}{2}\log(\ell) + \log(\ell-1)$. In conclusion, as long as $\sigma_0 > \ell/(\ell-1)$,

$$\Re(f(\sigma) - f(\sigma_0)) \leq \ell \log \ell.$$

One retrieves the statement of the theorem by putting $\sigma_0 = 1 + \frac{1}{c\log\ell}$, $R = \frac{2}{c\log\ell}$, $r = \frac{1}{c\log\ell}$. □

1.4 Conclusion of the Method

Among all functions f that satisfy the bounds from the preceding sections, what is the largest value $f(1)$ can attain? We define σ_ν to be the point where the bound (1.4) and the absolute bound (1.5) coincide. We note that

$$\sigma_\nu - 1 = \frac{1}{c\log\ell}\sqrt[\nu]{\frac{1+1_\beta+c_{\ell,\nu}}{2\nu\ell\log\ell}} \geq \frac{1}{c\log\ell\sqrt[\nu]{2\nu\ell\log\ell}}. \tag{1.6}$$

Theorem 1.12. *For all $\ell > 500$, and $c > 6.4355$,*

$$|f(1)| \leq (1 + 1_\beta \cdot 2 + e^{1/c})\log_2(\ell) + O(1),$$

where the $O(1)$-term is bounded by $(3+e^{1/c})\log(c) + 0.791e^{1/c} + 10.720 + \frac{0.943}{c}$

Proof. We use the Taylor expansion of f with error term in integral form

$$\begin{aligned} f(1) = & f(\sigma_\nu) + (1-\sigma_\nu) f'(\sigma_\nu) + \frac{(1-\sigma_\nu)^2}{2} f^{(2)}(\sigma_\nu) + \dots \\ & + \int_{\sigma_\nu}^{1} \frac{f^{(\nu)}(x)}{(\nu-1)!} (1-x)^{\nu-1} dx. \end{aligned}$$

Now note that $|f^{(\nu)}(x)|$ is bounded above by the bound (1.5) for all x between 1 and σ_ν, which is equal to $|f^{(\nu)}(\sigma_\nu)|$. Using (1.3), (1.4) and (1.6), we get

$$\begin{aligned} |f(1)| &\leq |f(\sigma_\nu)| + \sum_{i=1}^{\nu} \frac{(\sigma_\nu - 1)^i}{i!} |f^{(i)}(\sigma_\nu)| \\ &\leq (1 + 1_\beta) \log(\frac{1}{\sigma_\nu - 1}) + \frac{3}{2} + \sum_{i=1}^{\nu} \frac{1 + 1_\beta + c_{\ell,i}}{i} \\ &\leq (1 + 1_\beta) \Big(\log_2(\ell) + \log(c) + \frac{\log(2\nu\ell \log \ell)}{\nu} \Big) + \frac{3}{2} + \sum_{i=1}^{\nu} \frac{1 + 1_\beta + c_{\ell,i}}{i}. \end{aligned}$$

Upon taking $\nu = \log \ell$, this first contribution is bounded by

$$(1 + 1_\beta) \Big(\log_2(\ell) + \log(c) + 1 + \frac{\log(2(\log \ell)^2)}{\log \ell} \Big) + 3/2.$$

In the rest of the terms, we find the first ν terms of some converging series;

$$\sum_{i=1}^{\nu} \frac{1}{c^i i!} \leq e^{1/c} - 1, \ \sum_{i=1}^{\nu} \frac{\lfloor \log \nu \rfloor}{\nu(\nu - \lfloor \log \nu \rfloor)} \leq 1.90, \ \sum_{i=1}^{\nu} \frac{1}{c^{\lfloor \log \nu \rfloor} \lfloor \log \nu \rfloor !} \leq 1.13.$$

Using this and the well-known estimate $\sum_{i=1}^{\nu}\frac{1}{i}\leq\log(\nu)+1$ we bound the last contribution as follows

$$\sum_{i=1}^{\nu}\frac{1+1_\beta+c_{\ell,i}}{i}\leq(1+1_\beta+\frac{1}{c\log\ell})(\log(\nu)+1)+(1+\frac{1}{c\log\ell})\cdot 3.03$$
$$+\Big(\frac{\log(2)}{2\log\ell}+\log_2(\ell)+\log(c)-\log_2(2)+e^{-1}\Big)(e^{1/c}-1).$$

Gathering everything and substituting $\ell=500$ for the terms converging to zero, we recover the statement of the theorem. $\square$

We now finish the proof of Theorem 1.7.

Proof. By the formula (1.1), we have that

$$\log(h_\ell^-/G(\ell))=\sum_{\chi\text{ even}}\log L(1,\chi)=f(1)+1_\beta\cdot\log(1-\beta).$$

We use Theorem 1.12 and we choose $c=\log_2(\ell)\frac{6.4355}{\log_2(500)}$. This proves the theorem for $\ell\geq 500$. For $\ell\leq 3000$, h_ℓ^- has been computed by Fung, Granville and Williams[10] from which it follows that in this range, $0.6046\leq h_\ell^-/G(\ell)\leq 1.4981$. $\square$

Remark 1.13. It is quite counterintuitive that a bigger value of c gives a better estimate in Theorem 1.12 while a smaller value of c means a bigger zero-free region, and consequently means a stronger input. In truth there is a tradeoff between having σ_ν *big* to control the main term coming from Lemma 1.10

and at the same time *not too big* to bound the term coming from ε_2 in the proof of Lemma 1.10. This ε_2 cannot be efficiently bounded by a lack of good bounds on the number of primes of the form $a\ell + 1$, where a is smaller than say $\log \ell$.

Remark 1.14. It is now clear that the general behaviour of h_ℓ^- is dominated by $G(\ell)$ and that the L-values can perturb this term only slightly. It is somewhat common (see e.g. [28]) to state upper bounds for h_ℓ^- in terms of $G(\ell)$, where $4\pi^2 = 39.4784$ is replaced by a smaller constant.

Corollary 1.15. *We have that* $h_\ell^- \leq 2\ell\left(\frac{\ell}{39}\right)^{\frac{\ell-1}{4}}$*, for all odd primes* $\ell > 9649$.

Proof. This follows from plugging in $c = \frac{6.4355 \log_2(\ell)}{\log_2(500)} = 3.523 \log_2(\ell)$ in Theorem 1.12 and checking that

$$|f(1)| \leq e^{\frac{\ell-1}{4}} \log(\frac{4\pi^2}{39}),$$

whenever $\ell > 9649$. □

As we will see in Chapter 3, the analytic input can be generalised to other situations. One key input whose generalisation is a very non-trivial problem is the Brun-Titchmarsh inequality. In the next chapter, we explore an approach to use sieve methods to count the number of completely splitting primes in a concrete family of fields.

2

Sieving for Completely Splitting Primes

2.1 Introduction

The distribution of primes with certain properties is a central topic in Analytic Number Theory. Historically, much emphasis has been laid on primes in arithmetic progressions. In hindsight, this is a natural generalisation; the subset of integers in a given arithmetic progression can in some sense be seen as analogous to the notion of a subspace. We denote by $\pi(x, a, q)$ the number of primes up to x congruent to $a \bmod q$.

Dirichlet proved that $\pi(x, a, q)/\pi(x)$ tends asymptotically to $\frac{1}{\phi(q)}$. A classical way to make this more precise is the theorem of Siegel-Walfisz.

Theorem 2.1. *(Siegel-Walfisz) Let $(a, q) = 1$. For any real number N there exists a constant C_N such that,*

$$\pi(x, a, q) = \frac{\mathrm{Li}(x)}{\phi(q)} + O(xe^{-C_N(\log x)^{1/2}}),$$

for any $q \leq (\log x)^N$.

The error term gives a saving of an arbitrary log-power, but unfortunately, the constant C_N is ineffective and the range for q is quite restricted. The ineffectivity originates in the use of Siegel's Theorem 1.2. When seeking to prove effective versions, it is exactly the possible presence of a Siegel-zero that gives rise to a potential second main term. Consider the following theorem[18].

Theorem 2.2. *Let $(a, q) = 1$. Let β be an exceptional zero for $L(s, \chi)$, where χ is a quadratic character to the modulus q. Then there exists a positive absolute and effective constant b such that*

$$\pi(x, a, q) = \frac{\mathrm{Li}(x)}{\phi(q)} + \frac{\chi(a)}{\phi(q)} \frac{\mathrm{Li}(x^\beta)}{\beta} + O(xe^{-b(\log x)^{1/2}}).$$

If there is no exceptional zero, we may leave out the term involving β.

Remember that $\beta \geq 1 - \frac{c}{\log q}$. Thus, depending on whether the value of $\chi(a)$ is ± 1, the number of primes is nearly twice as large as expected, or nearly negligible.

It is however the following result which is most important to our discussion. The famous Brun-Titchmarsh theorem succeeds in using sieve methods to give an upper bound for $\pi(x, a, q)$ of the following form.

Theorem 2.3. *(Brun-Titchmarsh) Let $(a, q) = 1$. Then, for all $x > q$,*

$$\pi(x, a, q) \leq \frac{2}{\phi(q)} \frac{x}{\log(x/q)}.$$

While originally proven with $2 + \varepsilon$ in place of 2, the above formulation was proven by Montgomery and Vaughan[33] in 1973. Further improvements concerning the factor $\frac{1}{\log(x/q)}$ have been made by e.g. Motohashi [34], see [30] for an overview of the state of the art. The constant 2 however seems out of reach of improvements; indeed, any improvement would imply that the Siegel-zero β cannot be present, and for this reason (along with the parity problem) the consensus is that one cannot expect sieve methods to improve on the factor 2. In conclusion, the price we have to pay for effectivity is the doubling of the expected term.

Another way to look at the primes with a given residue $\bmod q$, is to view them as the primes with a given Frobenius element in the Galois group of

$\mathbb{Q}(\zeta_q)$. This perspective offers possibilities for very broad generalisations : for any given finite Galois extension K of the rationals, we may separate the primes numbers (except for a finite set of ramified primes) into a number of classes depending on their splitting behaviour in the extension $K/\mathbb{Q}$. The question of determining the distribution of primes among those classes has been solved asymptotically, and the theorem is known as the Chebotaryov Density Theorem.

Theorem 2.4. *(Chebotaryov, '22) Let C be a conjugacy class in the Galois group G of a number field K. Let $\pi(x, C)$ denote the number of primes p up to x with Frobenius conjugacy class $\sigma_p = C$. Then*

$$\lim_{x\to\infty} \frac{\pi(x, C)}{\pi(x)} = \frac{|C|}{|G|}.$$

Though this is purely a limit result, there is also an effective version akin to the above Theorem 2.2 by Lagarias and Odlyzko[21].

We wish to establish a bound on the number of primes in Chebotaryov classes using Sieve methods. Specifically, we will investigate how one may apply the Selberg sieve to obtain an analogous statement to the Brun-Titchmarsh theorem, bounding the number of completely splitting primes of a certain family of fields $K = \mathbb{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \ldots, \sqrt[\ell]{q_n})$, where ℓ is an odd prime, and $q_i \neq \ell$ are primes. The arithmetic properties which distinguish these primes p from ordinary primes is that they are congruent to $1 \bmod \ell$, and all q_i are ℓ-th powers $\bmod p$, or more precisely, the polynomials $x^\ell - q_i$ have a solution in $\mathbb{F}_p$.

One key reason why sieve methods work for primes in arithmetic progressions is that one may start with confining those primes to the integers of this arithmetic progression - which already has about the right density in $\mathbb{Z}$ - and then sieve away all composite numbers. Our first mission is to describe these completely splitting primes as the primes within some set of integers, which already has about the right density. The main idea which is necessary for realising this is the use of a reciprocity law.

The main results of this chapter are the following. First and foremost we have the bound on the completely splitting primes, of which we give four different versions; Theorems 2.34, 2.38, 2.42, and 2.46. As a key lemma we prove an effective and explicit counting Lemma 2.26, which seems useful enough to be mentioned separately. It provides an estimate for the number of integral elements in a number field K, up to multiplication by units, in any subgroup of the additive group of ring of integers $\mathcal{O}_K$. In particular, it furnishes an estimate for the number of integral elements in ideals up to multiplication, which allows us to prove Theorem 2.27, an explicit version of Landau's proof of the analytic continuation of $\zeta_K(s)$ to $\mathrm{Re}(s) \geq 1 - \frac{1}{n}$.

2.2 A Reciprocity Law

An essential tool in our method is a reciprocity law, which presents an equivalence between the statement that *q is a ℓ-th power* $\bmod p$ and a statement of the form *some condition on p holds* $\bmod q$. Throughout the chapter, the symbols p and q are reserved for primes, and ℓ shall denote an odd prime.

The most famous reciprocity law is the law of quadratic reciprocity, which was discovered by Leonhard Euler and Adrien-Marie Legendre, and finally proven by Carl Friedrich Gauss in 1801.

Theorem 2.5. *(Quadratic Reciprocity) Let p and q be two odd primes. If at least one of p, q is congruent to* $1 \bmod 4$*, then*

$$p \text{ is a square} \bmod q \Leftrightarrow q \text{ is a square} \bmod p.$$

If both p and q are congruent to $3 \bmod 4$*, then*

$$p \text{ is a square} \bmod q \Leftrightarrow q \text{ is not a square} \bmod p.$$

Gauss provided six different proofs, and considered the theorem as his most beautiful result. Gauss' motivation to search for more proofs lies in his desire to generalise his result to higher powers. This quest has been taken on by the most illustrious of mathematicians in subsequent generations*, culminating in the general Eisenstein reciprocity law. In order to state this law, we introduce some definitions.

Definition 2.6. Let $\alpha \in \mathbb{Z}[\zeta_\ell]$, and let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}[\zeta_\ell]$. The ℓ-th power residue symbol $\left(\frac{\alpha}{\mathfrak{p}}\right)_\ell$ is defined as the unique root of unity such that

$$\alpha^{\frac{N(\mathfrak{p})-1}{\ell}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_\ell \bmod \mathfrak{p}.$$

For general ideals $\mathfrak{a}$, the ℓ-th power residue is defined multiplicatively: if $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$,

$$\left(\frac{\alpha}{\mathfrak{a}}\right)_\ell = \prod_i \left(\frac{\alpha}{\mathfrak{p}_i}\right)_\ell.$$

Thus, if $\mathfrak{p}$ is a prime ideal, $\left(\frac{\alpha}{\mathfrak{p}}\right)_\ell = 1$ implies that α is the ℓ-th power of some element of $\mathbb{Z}[\zeta_\ell]/\mathfrak{p}$.

Definition 2.7. An element $\alpha \in \mathbb{Z}[\zeta_\ell]$ coprime to ℓ is said to be semi-primary if there exists an integer a such that $\alpha \equiv a \bmod (1-\zeta_\ell)^2$.

This concept of semi-primary elements will be handy in handling the ambiguity of unit factors when passing from ideals to elements. We now state Eisenstein's reciprocity law.

*A total of 246 proofs of the quadratic reciprocity law have as of yet been published; one may consult an overview on Lemmermeyer's webpage[25]

Theorem 2.8. *(Eisenstein's Reciprocity Law, 1850) Let ℓ be an odd prime, and let a be an integer such that $(a, \ell) = 1$. Let $\alpha \in \mathbb{Z}[\zeta_\ell]$ be a semi-primary element such that $(a, \alpha) = 1$. Then*

$$\left(\frac{\alpha}{a}\right)_\ell = \left(\frac{a}{\alpha}\right)_\ell.$$

One may go further and view Artin's reciprocity law as a deep generalisation, but the statement is not reminiscent anymore of the earlier reciprocity laws. We will not state the theorem here since it uses the language of Class Field Theory and is not relevant for our further discussion. It is called a reciprocity law since one may derive concrete reciprocity laws from it, although this is certainly a non-trivial task, see for example [43, Theorem 2.3.5] for a proof of the cubic reciprocity law using Artin's reciprocity law.

We shall use a law of a slightly different flavour. Consider the field $K = \mathbb{Q}(\zeta_\ell)$, with ring of integers $\mathbb{Z}[\zeta_\ell]$. The Galois group is isomorphic to $\mathbb{Z}_\ell^* \cong C_{\ell-1}$, and we will write σ_i for the Galois elements corresponding to $i \in \mathbb{Z}_\ell^*$. Recall that the splitting behaviour of primes is determined by their order $\bmod \ell$. If p has order $e \bmod \ell$, then $p = \mathfrak{p}_1 \cdots \mathfrak{p}_f$, where $ef = \ell - 1$, and $N(\mathfrak{p}_i) = p^e$. We fix a set of integral ideals $B = \{\mathfrak{b}_c \in c \mid c \in CL_K\}$ containing one representative of each class of the class group. The ideal corresponding to the trivial class is $\mathbb{Z}[\zeta_\ell]$, the rest may be chosen arbitrarily, subject only to the condition that $(N(\mathfrak{b}), \ell) = 1$. We denote by θ the Stickelberger element times

ℓ, that is $\theta = \sum_{i=1}^{\ell-1} i\sigma_{i^{-1}}$, and recall that it annihilates the class group. The reciprocity statement most useful to our application reads as follows.

Theorem 2.9. *For each ideal* $\mathfrak{b}$ *in* B*, there exists an element* β *such that* $(\beta) = \mathfrak{b}^{\theta}$*,* $|\beta| \in \mathbb{Q}$ *and* β *is semi-primary. Let* p *be a prime congruent to* $1 \bmod \ell$*, such that* $(p) = \prod_{i=1}^{\ell-1} \mathfrak{p}^{\sigma_i}$*, and let* a *be the order of* $q \bmod \ell$*. Let* $\mathfrak{b} \in B$ *be an ideal in the inverse class of* $\mathfrak{p}$*, and choose* α *semi-primary such that* $\mathfrak{b}\mathfrak{p} = (\alpha)$*.*

Then q *is congruent to a* ℓ*-th power* $\bmod p$ *if and only if*

$$\left(\alpha^{\theta}\right)^{\frac{q^a-1}{\ell}} \equiv (\beta)^{\frac{q^a-1}{\ell}} \bmod q. \tag{2.1}$$

Remark 2.10. In the case that p splits into principal ideals (e.g. if $\ell \leq 19$), the condition simplifies to

$$\left(\alpha^{\theta}\right)^{\frac{q^{\ell-1}-1}{\ell}} \equiv 1 \bmod q,$$

where α is a semi-primary generator of $\mathfrak{p}$.

The novelty of this theorem is merely in its formulation. Indeed, our law is in fact contained in Eisenstein's reciprocity law, and we will indicate how it can be derived directly from it at the end of this section. However, we simply cannot withhold from the reader its beautiful proof using Gauss sums, which is based on the proof of Eisenstein's reciprocity law in [26].

Consider a character χ to the modulus p of order ℓ. Then the question of q being a ℓ-th power $\mathrm{mod} p$ is the question whether $\chi(q) = 1$.

Definition 2.11. The Gauss sum corresponding to the character χ to the modulus p is the expression

$$G(\chi) = \sum_{n=0}^{p-1} \chi(n)\zeta_p^n.$$

We recall some of the remarkable properties of Gauss sums.

Proposition 2.12. *Let χ be a character to the modulus p of order ℓ. Then*

1. $|G(\chi)| = \sqrt{p}$
2. $G(\chi)^\ell \in \mathbb{Z}[\zeta_\ell]$
3. $G(\chi)^\ell \equiv -1 \bmod \ell$
4. *(Stickelberger relation) There is an ideal factor $\mathfrak{p}$ of (p) such that the following factorisation in prime ideals holds:*

$$(G(\chi)^\ell) = \mathfrak{p}^\theta.$$

Proof. 1., 2. and 4. are contained in Theorem 1.1.4 and Theorem 11.2.8 in [2], and 3. follows from

$$G(\chi)^\ell \equiv \sum_{n=0}^{p-1} \chi^\ell(n)\zeta_p^{n\ell} \equiv \sum_{n=1}^{p-1} \zeta_p^{n\ell} \equiv -1 \mod \ell.$$

□

The following proposition shows how the Gauss sum indicates the value $\chi(q)$.

Proposition 2.13. *Let $p \equiv 1 \bmod \ell$, and let $q \neq \ell$ be a prime with order $a \bmod \ell$. Then*

$$G(\chi)^{q^a-1} \equiv \chi^{-a}(q) \bmod q$$

Proof. Consider the q^a-th power of the Gauss sum

$$\begin{aligned} G(\chi)^{q^a} &\equiv \sum_{n=0}^{p-1} \chi^{q^a}(n)\zeta_p^{q^a n} \bmod q \\ &\equiv \bar{\chi}(q^a) \sum_{n=0}^{p-1} \chi(q^a n)\zeta_p^{q^a n} \bmod q \\ &\equiv \chi^{-a}(q)G(\chi) \bmod q. \end{aligned}$$

□

We shall need the following properties of semi-primary elements.

Proposition 2.14. *Let ℓ be an odd prime. Then*

1. *Given an $\alpha \in \mathbb{Z}[\zeta_\ell]$ coprime to ℓ, exactly one element in the set $\{\zeta_\ell^i \alpha \mid i = 0, \ldots, \ell - 1\}$ is semi-primary.*

2. *The sum, product, and Galois conjugates of semi-primary elements are again semi-primary, provided, in the case of the sum, that the sum is coprime to ℓ.*

3. *An integral element* $\alpha = \sum_i a_i \zeta_\ell^i$ *is semi-primary if and only if* $(\alpha, \ell) = 1$ *and* $\sum_i i a_i \equiv 0 \mod \ell$.

Proof. The first and second statement are contained in [26, Lemma 11.6]. For the third statement, denote $\lambda = 1 - \zeta_\ell$. Then

$$\alpha = \sum_i a_i \zeta_\ell^i = \sum_i a_i (1+\lambda)^i \equiv \sum_i a_i + \lambda \sum_i i a_i \mod \lambda^2,$$

thus $\alpha \mod (1-\zeta_\ell)^2$ being an element of $\mathbb{Z}$ is equivalent to the sum $\sum_i i a_i$ being zero $\mod \lambda$, or, since it is rational, $\mod \ell$. $\square$

We are now ready to prove the reciprocity law, Theorem 2.9.

Proof. We claim that the element α as described in the statement of the theorem has the property that

$$\alpha^\theta = \beta G^\ell(\chi),$$

for some character χ of order ℓ, where β is as in the statement of the theorem, so that we may apply Proposition 2.13. We know by the factorisation of $G^\ell(\chi)$ in prime ideals that $(\alpha^\theta) = (\mathfrak{b}\mathfrak{p})^\theta = \mathfrak{b}^\theta(G(\chi)^\ell)$, and so that the above inequality must hold up to a unit u

$$\alpha^\theta = u \beta G^\ell(\chi).$$

We prove that the choice of $u\beta$ as a generator for the ideal $\mathfrak{b}$ is permitted, that is, that $|u\beta| \in \mathbb{Q}$ and that $u\beta$ is semi-primary.

First we note that

$$|\alpha^\theta| = \left(\alpha^{\sum i\sigma_{i-1}}\alpha^{\sum(\ell-i)\sigma_{i-1}}\right)^{\frac{1}{2}} = (\alpha^{\sum_i \sigma_i})^{\ell/2} = (N(\mathfrak{b})p)^{\ell/2} \in \mathbb{Z},$$

so that, writing $u\beta = \frac{\alpha^\theta}{G^\ell(\chi)}$ we have that $|u\beta| \in \mathbb{Q}$

Now note that $G^\ell(\chi)$ is semi-primary by virtue of Proposition 2.12, and since we have chosen α semi-primary, $u\beta$ is semi-primary as well by Proposition 2.14. It is worth noting that these two conditions determine $u\beta$ up to a sign. $\square$

We now indicate how the reciprocity law can also be proved by using Eisenstein's reciprocity law.

Proof. First of all we claim that q is an ℓ-th power in $\mathbb{Z}/p\mathbb{Z} \Leftrightarrow q$ is an ℓ-th power in $\mathbb{Z}[\zeta_\ell]/\mathfrak{p}$ for some prime $\mathfrak{p}|(p)$. As a proof one merely needs to consider the isomorphism $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}[\zeta_\ell]/\mathfrak{p}(\cong \mathbb{F}_p)$ which sends 1 to 1. Then the image of $q \bmod p$ is $q \bmod \mathfrak{p}$, and because the map is an isomorphism, they both are ℓ-th powers or both are not ℓ-th powers.

Thus, q is an ℓ-th power in $\mathbb{Z}/p\mathbb{Z}$ is and only if $\left(\frac{q}{\mathfrak{p}}\right)_\ell = 1$. For simplicity, we assume that $\mathfrak{p}$ is a principal ideal. The general case can be proven along the same lines. We choose a semi-primary α such that $\mathfrak{p} = (\alpha)$. Then, using

Eisenstein's reciprocity law,

$$\left(\frac{q}{(\alpha)}\right)_\ell = 1 \Leftrightarrow \left(\frac{\alpha}{q}\right)_\ell = 1$$

We choose a prime ideal $\mathfrak{q}_1 | q$, and we denote $\mathfrak{q}_i = \mathfrak{q}_1^{\sigma_i}$, so that $\{\mathfrak{q}_i | i \in \mathbb{Z}_\ell^*\}$ is an a-fold multiset over $\{\mathfrak{q} : \mathfrak{q} \mid q\}$. Since $(a, \ell) = 1$,

$$\left(\frac{\alpha}{q}\right)_\ell = 1 \Leftrightarrow \prod_{\mathfrak{q}|q} \left(\frac{\alpha}{\mathfrak{q}}\right)_\ell = 1 \Leftrightarrow \prod_i \left(\frac{\alpha}{\mathfrak{q}_i}\right)_\ell = 1.$$

Now if $\alpha^{\frac{N(\mathfrak{q}_i)-1}{\ell}} \equiv \zeta_\ell^j \bmod \mathfrak{q}_i$, then $(\alpha^{i\sigma_{i-1}})^{\frac{N(\mathfrak{q}_i)-1}{\ell}} \equiv \zeta_\ell^{ji\sigma_{i-1}} \equiv \zeta_\ell^j \bmod \mathfrak{q}_1$. In other words,

$$\left(\frac{\alpha}{\mathfrak{q}_i}\right)_\ell = \left(\frac{\alpha^{i\sigma_{i-1}}}{\mathfrak{q}_1}\right)_\ell.$$

Thus

$$\begin{aligned}\prod_i \left(\frac{\alpha}{\mathfrak{q}_i}\right)_\ell = 1 \Leftrightarrow \left(\frac{\alpha^\theta}{\mathfrak{q}_1}\right)_\ell = 1 &\Leftrightarrow (\alpha^\theta)^{\frac{q^a-1}{\ell}} = 1 \bmod \mathfrak{q}_1 \\ &\Leftrightarrow (\alpha^\theta)^{\frac{q^a-1}{\ell}} = 1 \bmod q.\end{aligned}$$

The last step is justified by noting that the choice of $\mathfrak{q}_1$ was arbitrary. $\square$

We conclude this section with an important observation regarding condition (2.1).

Proposition 2.15. *Fix β, and let V be the solution set of condition* (2.1)*, that is*

$$V = \{\alpha \in (\mathbb{Z}[\zeta_\ell]/q)^* \mid \left(\alpha^\theta\right)^{\frac{q^a-1}{\ell}} \equiv (\beta)^{\frac{q^a-1}{\ell}} \bmod q\}.$$

Then $|V| = \frac{\prod_{\mathfrak{q}|q}(N(\mathfrak{q})-1)}{\ell}$*. Furthermore, if $\alpha \in V$ then $t\alpha \in V$ for all $t \in \mathbb{Z}$.*

Proof. We first note that

$$\mathbb{Z}[\zeta_\ell]/q \cong \prod_{\mathfrak{q}|q} \mathbb{Z}[\zeta_\ell]/\mathfrak{q} \cong \mathbb{F}_{q^a}^{\frac{\ell-1}{a}}$$

, where a is the order of $q \bmod \ell$. From this isomorphism of rings we infer that $|(\mathbb{Z}[\zeta_\ell]/q)^*| = \prod_{\mathfrak{q}|q}(N(\mathfrak{q}) - 1)$. Let m be the largest natural number such that $q^a \equiv 1 \bmod \ell^m$ holds. Then, since $\mathbb{F}_{q^a}^*$ is a cyclic group of order $q^a - 1$, we find an element $a_\ell \in \mathbb{F}_{q^a}^*$ of order ℓ^m. Let b_ℓ be the element in $\mathbb{Z}[\zeta_\ell]/q$ which corresponds to a_k in each factor $\mathbb{F}_{q^a}$ in the above isomorphism. To prove the first part we show that $(b_\ell^\theta)^{\frac{N(\mathfrak{q})-1}{\ell}} \neq 1$, so that one out of every ℓ elements $x, b_k x, \ldots, b_k^{\ell-1}x$ of $(\mathbb{Z}[\zeta_\ell]/q)^*$ are in V.

Now, $b_\ell^{\frac{N(\mathfrak{q})-1}{\ell}}$ corresponds to an element of order ℓ in each factor $\mathbb{F}_{q^a}$, and by construction it corresponds to the same element in each factor, thus it equals ζ_ℓ^j in $\mathbb{Z}[\zeta_\ell]/q$ for a certain j. Then

$$(b_\ell^\theta)^{\frac{N(\mathfrak{q})-1}{\ell}} \equiv (b_\ell^{\frac{N(\mathfrak{q})-1}{\ell}})^\theta \equiv (\zeta_\ell^j)^\theta \equiv \prod_{i=1}^{\ell-1} \zeta_\ell^{ji\sigma_i{}^{-1}} \equiv \prod_{i=1}^{\ell-1} \zeta_\ell^j \equiv \zeta_\ell^{-j} \neq 1 \quad \bmod q.$$

To prove the second part, we show that $(t^\theta)^{\frac{N(\mathfrak{q})-1}{\ell}} \equiv 1 \bmod \mathfrak{q}$ for each $t \in \mathbb{Z}$ and each $\mathfrak{q}|q$. This follows from the fact that t^θ is an ℓ-th power;

$$t^\theta = \prod_{i=1}^{\ell-1} t^{i\sigma_{i-1}} = \prod_{i=1}^{\ell-1} t^i = t^{\frac{\ell(\ell-1)}{2}}. \qquad \square$$

2.3 Selberg's Sieve

Since the dawn of mathematical life, it has been observed that in order to count primes one should start by counting multiples. Eratosthenes (Cyrene c. 276 BC – Alexandria c. 195/194 BC) was the first to realise this idea as a workable algorithm, his famous Sieve of Eratosthenes. This is but one of his many scientific feats, among which we chiefly remember his ingenious method of accurately estimating the circumference of the earth — about 250.000 stadia.

By introducing the Möbius function, one can use the inclusion-exclusion principle to transform this *prime-detecting algorithm* into a *prime-counting algorithm*. Let $\mathcal{A}$ be any set of natural numbers of size at most N, and let $\mathcal{A}_d = \{n \in \mathcal{A} \mid d|n\}$ be the set of multiples of d in $\mathcal{A}$. A primitive sieving procedure can then be summarised by the equation

$$|\{p \in \mathcal{A} \mid p \geq z\}| \leq \sum_{\substack{d \text{ such that} \\ \forall p|d\,:\, p \leq z}} \mu(d)|\mathcal{A}_d|.$$

In fact, the right hand side counts all integers in $\mathcal{A}$ which are coprime to all primes less than z. This sifted set of numbers — those not divisible by any prime smaller than z in a given set of primes $\mathcal{P}$ — will be denoted $S(\mathcal{A}, \mathcal{P}, z)$. This set gives an upper bound for the number of primes in $\mathcal{A} \cap [z, N]$, and the overestimation approaches equality when z approaches $\sqrt{N}$. The main issue rendering the above sieving procedure mostly useless, is that due to the presence of the Möbius function, one is forced to keep z very small. This is because we cannot hope to have an exact quantity for $|\mathcal{A}_d|$, but rather we will see an error being introduced for each d appearing in the sieving procedure, and so it is imperative that the number of summands is restricted. Yet currently, summands appear for all squarefree d divisible only by primes smaller than z, with a factor of absolute value $|\mu(d)| = 1$.

Selberg was able to overcome this barrier by considering an approximation of the Möbius function. Concretely, pick arbitrary real numbers λ_d for each squarefree number d, with the constraint that $\lambda_1 = 1$. Then, writing $\Pi(z) = \prod_{p \leq z} p$,

$$S(\mathcal{A}, \mathcal{P}, z) = \sum_{d|\Pi(z)} \mu(d)|\mathcal{A}_d| = \sum_{n\in\mathcal{A}} \sum_{d|(n,\Pi(z))} \mu(d) \leq \sum_{n\in\mathcal{A}} \left(\sum_{d|(n,\Pi(z))} \lambda_d \right)^2 .$$

Do note the role of the inner sum

$$\sum_{d|(n,\Pi(z))} \mu(d) = \begin{cases} 1 & \text{if } (n, \Pi(z)) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

The inequality holds in this generality; for n coprime to $\Pi(z)$ the only term appearing in the right hand side is $\lambda_1 = 1$, so that the contribution for such n is the same as in the Möbius sum, while for any other n the contribution of the right hand side is at least non-negative. Selberg realised that a suitable choice for the λ_d, *the Selberg weights*, can be made which ensures that the inner Möbius sum is successfully approximated by $\left(\sum_{d|(n,\Pi(z))} \lambda_d\right)^2$, even when demanding that λ_d vanishes for $d > z$, thereby solving the problem of the accumulation of error terms due to the amount of d's present in the summation.

For a more concrete and comprehensive treatment, we refer to the book by Halberstam and Richert[13].

In our case, the reciprocity law enables us to describe the completely splitting primes in $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \ldots, \sqrt[\ell]{q_n})$ as a set susceptible for counting via a sieving procedure. Instead of counting the completely splitting primes in the integers, the proposition below allows us to count their representatives in $\mathbb{Z}[\zeta_\ell]$. In other words, we have found a natural *habitat* for the splitting primes, akin to the integers $a \bmod b$ being the natural habitat of the primes $a \bmod b$. Let

$\mathcal{F}$ be such that for each $\alpha \in \mathbb{Z}[\zeta_\ell]$ the intersection

$$\{u\alpha \mid u \text{ is a unit of infinite order}\} \cap \mathcal{F}$$

contains exactly one element. In the next section we will explicitly construct such an $\mathcal{F}$.

Proposition 2.16. *Let $\mathcal{S}^{\ell}_{q_1,\ldots,q_n}$ be the set of completely splitting primes in the field $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \ldots, \sqrt[\ell]{q_n})$, and let $\pi(x, \mathcal{S}^{\ell}_{q_1,\ldots,q_n})$ be the counting function. Then*

$$2(\ell-1)\pi(x, \mathcal{S}^{\ell}_{q_1,\ldots,q_n}) + \delta = \sum_{\mathfrak{b}\in B} \left| \left\{ \begin{array}{l} \alpha \in \mathfrak{b} \\ N(\alpha) \le xN(\mathfrak{b}) \\ \alpha \in \mathcal{F} \end{array} \middle| \begin{array}{l} \alpha \in \mathbb{Z} \bmod (1-\zeta_\ell)^2 \\ \alpha \text{ satisfies (2.1) for all } q_i \\ \frac{N(\alpha)}{N(\mathfrak{b})} \text{ is prime} \end{array} \right\} \right|,$$

where $0 \le \delta \le 2\ell$.

Proof. An element α of the set on the right hand side corresponds to an integral ideal $\mathfrak{p} = (\alpha)\mathfrak{b}^{-1}$ with prime norm $p \le x$. This implies that p either ramifies or splits completely and hence is equal to ℓ or congruent to $1 \bmod \ell$. If $p = 1 \bmod \ell$, since $(N(\mathfrak{b}), \ell) = 1$, $(\alpha, \ell) = 1$ so that α is semi-primary, and we may use the reciprocity Theorem 2.9 to conclude that each q_i is a ℓ-th power $\bmod p$. Thus p splits completely and is counted on the left hand side. If $p = \ell$ then $\mathfrak{p} = (1-\zeta_\ell)$ which is principal, so that $\mathfrak{b} = \mathbb{Z}[\zeta_\ell]$.

How many elements α corresponding to $p \equiv 1 \bmod \ell$ are counted on the right hand side? There are $\ell - 1$ different prime factors $\mathfrak{p}$ of p. Each of them determines an element α up to a unit. Let α_1 and α_2 be two such elements differing by a unit. Since they are both in $\mathcal{F}$, $\alpha_1 = \pm\zeta_\ell^i \alpha_2$ for some i, but since both of them are semi-primary, $i = 0$. Thus the element α corresponding to $\mathfrak{p}$ is determined up to sign, which shows that each prime in $\pi(x, \mathcal{S}^\ell_{q_1,\dots,q_n})$ is counted exactly $2(\ell - 1)$ times in the right hand side. The last thing to show is that at most 2ℓ elements α corresponding to $p = \ell$ can appear in the right hand side. Since $(\ell) = (1 - \zeta_\ell)^{\ell-1}$, α should be an element associate to $1 - \zeta_\ell$. Since we only count elements $\alpha \in \mathcal{F}$, the only possible candidates are the 2ℓ elements $\pm\zeta_\ell^i \alpha$ where $\alpha \in \mathcal{F}$ is associated to $1 - \zeta_\ell$. $\square$

For clarity of exposition, we shall henceforth work with only one root q. In section 2.6 we will show how the generalisation to n roots $q_1, \dots, q_n$ is achieved.

Our set $\mathcal{A}$ to be sifted will be a set of integral elements in the field K. It is then natural to use an adaptation to the Selberg Sieve to number fields, whose main merit is that the computations to come will be significantly smoother. This is not a novel idea, yet it is not often used. Adaptations of the Selberg Sieve to number fields for use in various concrete problems have been pursued in Schaal[42], Rieger[40], Sarges[41] and Hinz[16]. The main difference is that we will take for $\mathcal{P}$ not the usual set of rational primes, to sieve by all primes of size up to z, but instead

$$\mathcal{P} \subseteq \{\mathfrak{p} \text{ prime ideal in } \mathbb{Z}[\zeta_\ell]\},$$

where we shall sieve by all prime ideals $\mathfrak{p}$ of norm up to z. Analogously to the usual definitions one has a Möbius function μ, an Euler totient ϕ, and the function ν counting the number of prime factors, functions on the integral ideals of K. The Selberg sieve weights are now a collection of reals $\lambda_{\mathfrak{d}}$ where $\mathfrak{d}$ ranges over the squarefree integral ideals.

Provided one has the estimates

$$|\mathcal{A}_{\mathfrak{d}}| = \frac{\omega(\mathfrak{d})}{N(\mathfrak{d})} X + R_{\mathfrak{d}},$$

for each integral ideal $\mathfrak{d}$, where ω is multiplicative, the basic mechanisms of the Selberg Sieve carry over to this setting exactly as in [13, p.97–103]. For completeness, we give the definitions of the relevant quantities.

$$\begin{aligned}
\Pi(z) &= \prod_{N(\mathfrak{p})<z} \mathfrak{p} \\
g(\mathfrak{d}) &= \frac{\omega(\mathfrak{d})}{N(\mathfrak{d}) \prod_{\mathfrak{p}|\mathfrak{d}} (1 - \frac{\omega(\mathfrak{p})}{N(\mathfrak{p})})} \\
G_k(x) &= \sum_{\substack{N(\mathfrak{d})<x \\ (\mathfrak{d},k)=1}} \mu^2(\mathfrak{d}) g(\mathfrak{d}), \text{ and } G(x) = G_1(x) \\
\lambda_{\mathfrak{d}} &= \frac{\mu(\mathfrak{d})}{\prod_{\mathfrak{p}|\mathfrak{d}} (1 - \frac{\omega(\mathfrak{p})}{N(\mathfrak{p})})} \frac{G_{\mathfrak{d}}(z/N(\mathfrak{d}))}{G(z)} \\
W(x) &= \prod_{N(\mathfrak{p})<x} (1 - \frac{\omega(\mathfrak{p})}{N(\mathfrak{p})}).
\end{aligned}$$

In this way, the following general theorem holds, which is the adaptation of Theorem 3.2 in [13] to number fields.

Theorem 2.17. *Let K be any number field, let $\mathcal{A} \subseteq \mathcal{O}_K$, where $\mathcal{O}_K$ is the ring of integers of K, and let $\mathcal{P}$ be a collection of prime ideals. Assume that $0 \leq \frac{\omega(\mathfrak{p})}{N(\mathfrak{p})} \leq 1 - \frac{1}{A}$ for some suitable constant A. Then*

$$S(\mathcal{A}, \mathcal{P}, z) \leq \frac{X}{G(z)} + \Sigma_2,$$

where

$$\Sigma_2 \leq \sum_{\substack{N(\mathfrak{d})<z^2 \\ \mathfrak{d}|\Pi(z)}} 3^{\nu(\mathfrak{d})}|R_{\mathfrak{d}}|.$$

We conclude this section by stating our sieving setup. We define the set $\mathcal{A}(x)$ as the right hand side of Proposition 2.16 without the condition that $\frac{N(\alpha)}{N(\mathfrak{b})}$ is prime, and thus we wish to estimate the sets

$$\mathcal{A}_{\mathfrak{d}}(x) = \dot{\bigcup_{\mathfrak{b}\in B}} \left\{ \begin{array}{l|l} \alpha \in \mathfrak{b} & \alpha \in \mathbb{Z} \bmod (1-\zeta_k)^2 \\ N(\alpha) \leq xN(\mathfrak{b}) & \alpha \text{ satisfies (2.1) for } q \\ \alpha \in \mathcal{F} & \mathfrak{b}\mathfrak{d} \mid (\alpha) \end{array} \right\}, \tag{2.2}$$

where $\mathfrak{d}$ is a squarefree product of prime ideals in $\mathcal{P}$, and

$$\mathcal{P} = \{\mathfrak{p} \text{ prime ideals in } \mathbb{Z}[\zeta_\ell] \mid (\mathfrak{p}, q) = 1\}.$$

Using Proposition 2.16 we summarise the transformation of our counting problem into a sifting problem.

Corollary 2.18.

$$\pi(x, \mathcal{S}_q^\ell) \leq \frac{1}{2(\ell-1)} S(\mathcal{A}(x), \mathcal{P}, z).$$

2.4 Counting Integral Points in Bodies

We intend to estimate $\mathcal{A}_0$ by showing that it corresponds to a set of lattice points inside a certain region, which we then can approximate by the volume of this region. For our application, it is crucial to also obtain good, and completely explicit bounds on the error of the approximation.

We will first resolve the issue of the ambiguity of unit multiples of elements in $\mathcal{A}$. The unit group of the ring of integers $\mathcal{O}_K$ of a number field K is isomorphic to $T \times \mathbb{Z}^r$, where T is a finite group of roots of unity, and $r = r_1 + r_2 - 1$. The generators $\varepsilon_1, \ldots, \varepsilon_r$ of $\mathbb{Z}^r$ go by the name of fundamental units. As such, the fundamental units are not uniquely determined since we leave open the choice for a basis of $\mathbb{Z}^r$; we will later choose a basis which serves our needs best.

We will construct a fundamental domain under the action of the fundamental units, following the proof of the Analytic Class Number Formula, see e.g.[23]. Writing $\zeta_K(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$, where a_n is the number of ideals of norm n, one might already guess that the key step in the proof is to count all elements inside some ideal of bounded norm up to unit multiplication, for which one needs such a fundamental domain. Our situation similarly amounts to the counting of all elements inside some slightly more general set up to unit multiplication, but the challenge is to do so with explicit error terms.

Let K be a number field of degree n with r_1 real embeddings $\tau_i, i = 1, \ldots, r_1$ and r_2 pairs of complex embeddings $(\sigma_i, \bar{\sigma}_i), i = 1, \ldots, r_2$. We define the Minkowski embedding.

$$\begin{aligned} \phi : \mathcal{O}_K &\hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \\ \alpha &\longmapsto (\tau_1(\alpha), \ldots, \tau_{r_1}(\alpha), \sigma_1(\alpha), \ldots, \sigma_{r_2}(\alpha)) \end{aligned}$$

We shall frequently consider $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ as isomorphic to $\mathbb{R}^{r_1+2r_2}$ by taking real and complex parts in the r_2 complex dimensions. Note that the image in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ of any subring of $\mathcal{O}_K$ generated by $\{\alpha_i\}$ is a lattice, generated by $\{\phi(\alpha_i)\}$. It is in this space that we will construct a fundamental domain $\mathcal{F}$ under the action of the fundamental units. Consider the projection onto $\mathbb{R}_+^{r_1+r_2}$ given by taking absolute values, $(x_i)_{i=1}^{r_1+r_2} \mapsto (|x_i|^{e_i})_{i=1}^{r_1+r_2}$, where e_i is 1 or 2 for the real and complex embeddings respectively. Next, consider the isomorphism to $\mathbb{R}^{r_1+r_2}$ given by $(|x_i|^{e_1})_{i=1}^{r_1+r_2} \mapsto (e_i \log(|x_i|))_{i=1}^{r_1+r_2}$. Finally, we change coordinates to the coordinate system $(\xi, \xi_1, \ldots, \xi_{r_1+r_2-1})$ as follows

$$(e_i \log(|x_i|))_{i=1}^{r_1+r_2} = \frac{\log(\xi)}{n}\lambda + \sum_{j=1}^{r_1+r_2-1} \xi_j(\log(|\tau_1(\varepsilon_j)|), \ldots, 2\log(|\sigma_1(\varepsilon_j)|), \ldots), \tag{2.3}$$

where $\lambda = (1, \ldots, 1, 2, \ldots, 2)$.

Since all vectors corresponding to the units are orthogonal to $(1, \ldots, 1)$, it follows that $\xi = |N(x)|$. We omit the proof that the vectors corresponding to the units are linear independent, and limit ourselves to the claim that the Jacobian of the transformation from $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ to the real vector space spanned by $\xi, \xi_1, \ldots, \xi_{r_1+r_2-1}$, is equal to $2^{r_1}\pi^{r_2}\mathrm{Reg}_K$. Full details can be consulted in [23]. The upshot is that we may take as our fundamental domain $\mathcal{F} \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ all points $(x_i)_{i=1}^{r_1+r_2}$ such that after applying the transformation, $\xi_i \in [-\frac{1}{2}, \frac{1}{2})$.

Theorem 2.19. *The region $\mathcal{F}$ is a fundamental domain for the action of the non-torsion part of the unit group of $\mathcal{O}_K$. It is a cone, with* $\mathrm{Vol}(\mathcal{F}(t^n)) = t^n\mathrm{Vol}(\mathcal{F}(1))$*, where $\mathcal{F}(X) = \{x \in \mathcal{F} \mid |N(x)| \leq X\}$. Furthermore,*

$$\mathrm{Vol}(\mathcal{F}(1)) = 2^{r_1}\pi^{r_2}\mathrm{Reg}_K.$$

Proof. By (2.3), the map of multiplication with a unit $\varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}$, $a_i \in \mathbb{Z}$ corresponds to the map of addition by $(0, a_1, \ldots, a_r)$, $a_i \in \mathbb{Z}$ in the space spanned by $\xi, \xi_1, \ldots, \xi_{r_1+r_2-1}$. Hence $\mathcal{F}$ is a fundamental domain. By (2.3), the map of multiplication by an element $t \in \mathbb{Q}$ corresponds to multiplication of the norm ξ by a factor of t^n, and leaving all ξ_i fixed. Hence $\mathcal{F}$ is a cone. Given the value of the Jacobian, the volume of $\mathcal{F}(1)$ is given by

$$\int_0^1 \int_{-\frac{1}{2}}^{+\frac{1}{2}} \cdots \int_{-\frac{1}{2}}^{+\frac{1}{2}} 2^{r_1}\pi^{r_2}\mathrm{Reg}_K \, d\xi d\xi_1 \ldots d\xi_r = 2^{r_1}\pi^{r_2}\mathrm{Reg}_K \qquad \square$$

Before we set ourselves to explicitly estimating lattice points in $\mathcal{F}(X)$, we provide an image of the fundamental domain and the integral points in the case that $K = \mathbb{Q}(\zeta_5)$ where $n = 4 = 2r_2$. In this case, the monomorphism ϕ maps $\mathbb{Z}[\zeta_5]$ onto a lattice in $\mathbb{C}^2$, which unfortunately we cannot easily visualise. However, we can visualise the projection onto $\mathbb{R}^2$ by taking absolute values, or by taking logarithms of absolute values, or even plot the tuples (ξ, ξ_1). We mention that the fundamental unit $\varepsilon_1 = \zeta_5 + \zeta_5^{-1} = \frac{1+\sqrt{5}}{2}$.

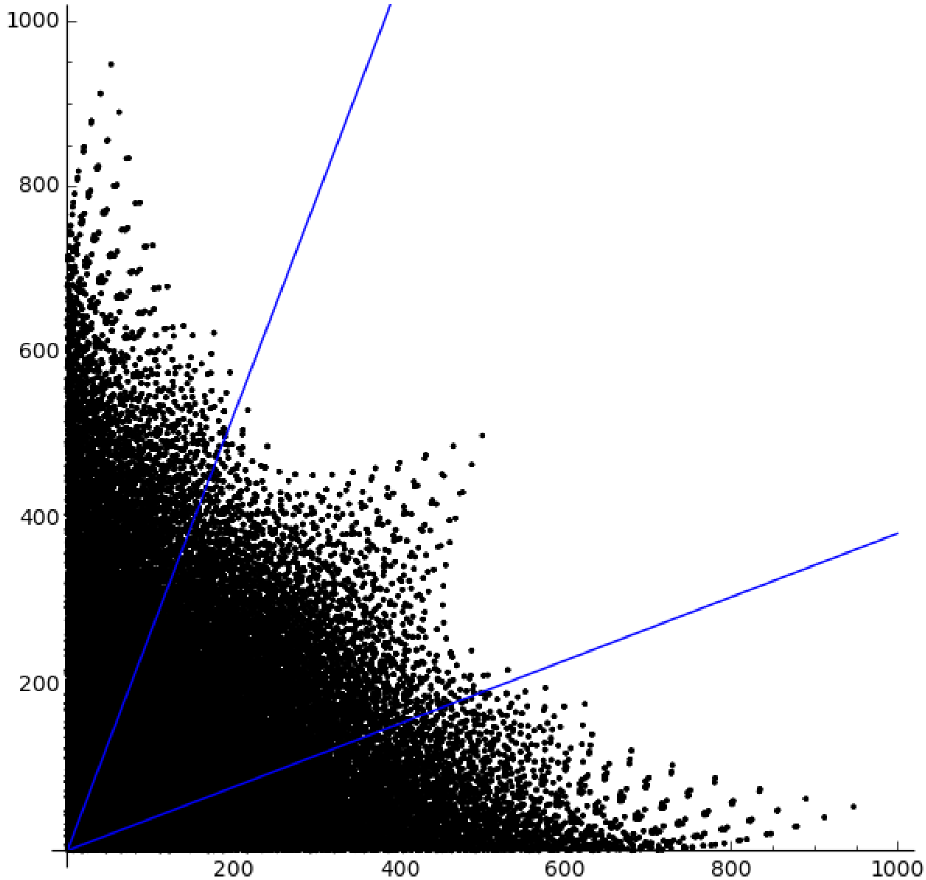

Figure 2.1: This is the projection of a cube in $\mathbb{Z}[\zeta_5]$ onto $\mathbb{R}^2$, by plotting for each element $\alpha = \sum_{i=1}^{4} a_i \zeta_5^i$ with $|a_i| \leq 10$ the tuple $(|\alpha|^2, |\alpha^\sigma|^2)$. The fundamental domain is the region between the two blue lines.

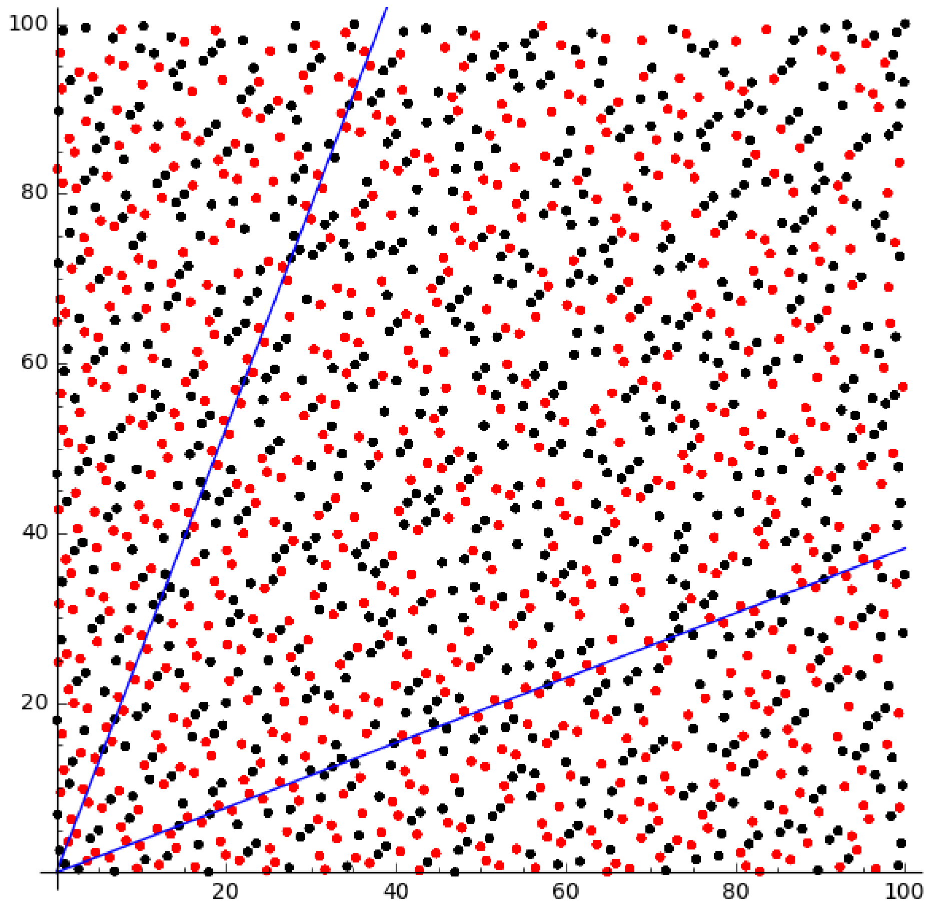

Figure 2.2: This is a zoomed-in version of Figure 2.1. Every $\alpha \in \mathbb{Z}[\zeta_5]$ with $\max(|\alpha|^2, |\alpha^\sigma|^2)| \leq 100$ is represented with a dot at coordinates $(|\alpha|^2, |\alpha^\sigma|^2)$. Red dots correspond to α's with prime norm. The fundamental domain is the region between the two blue lines.

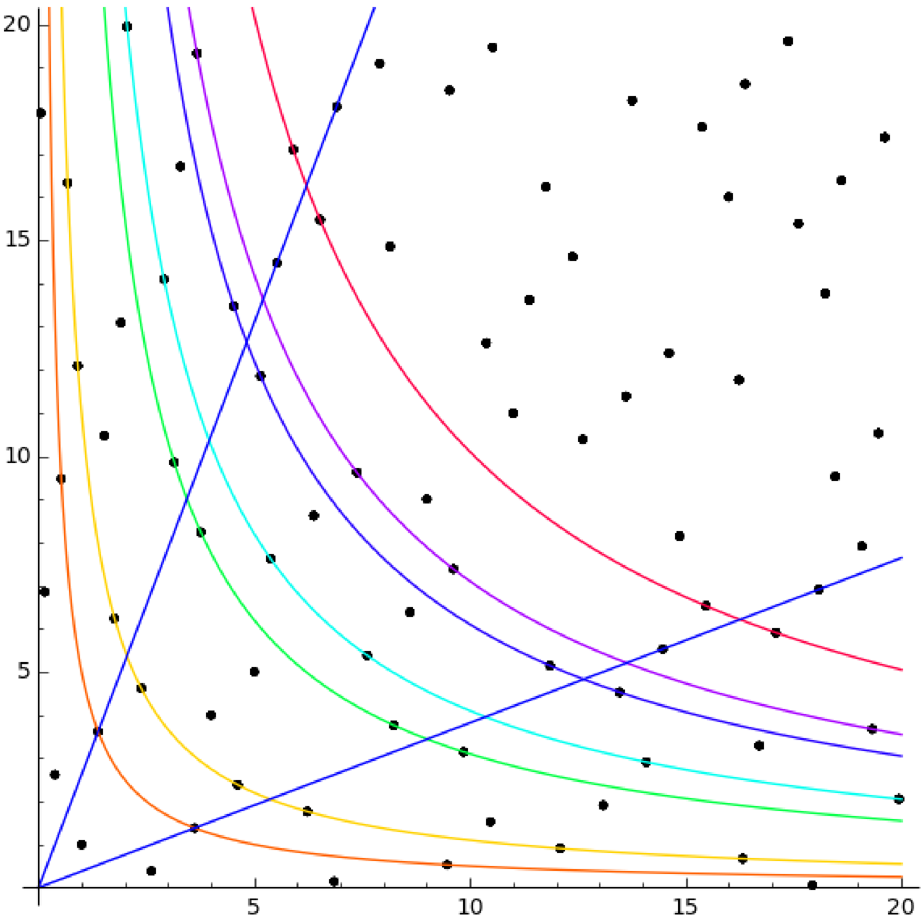

Figure 2.3: This is a further zoomed-in version of Figure 2.2. Every $\alpha \in \mathbb{Z}[\zeta_5]$ with $\max(|\alpha|^2, |\alpha^\sigma|^2)| \leq 20$ is represented with a dot at coordinates $(|\alpha|^2, |\alpha^\sigma|^2)$. Points on the same hyperbola have the same norm in absolute value. Pictured are the hyperbola of prime norm $5, 11, 31, 41, 61, 71, 101$. The fundamental domain is the region between the two blue lines.

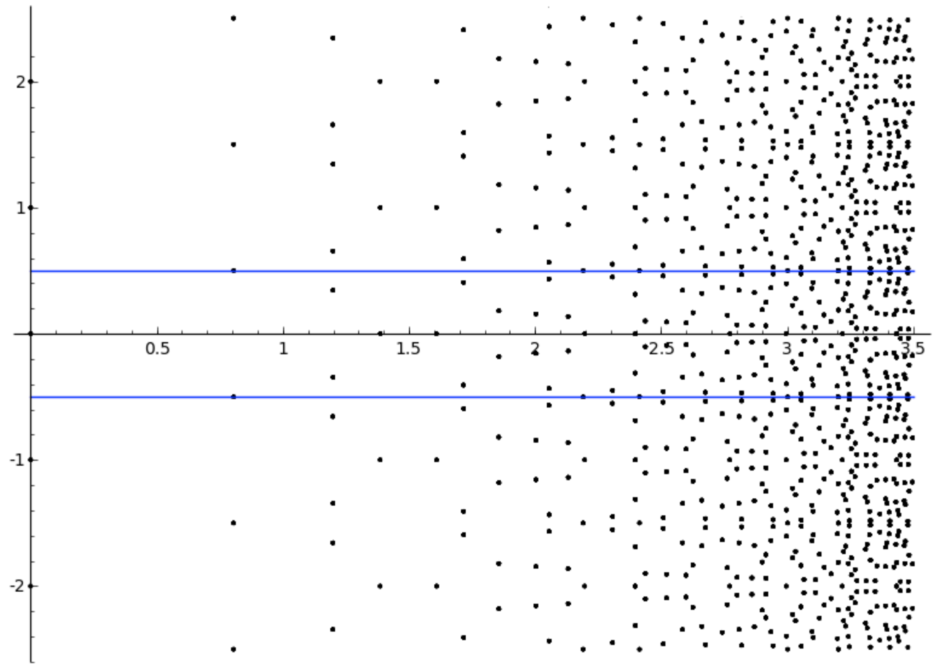

Figure 2.4: This is a plot of every $\alpha \in \mathbb{Z}[\zeta_5]$ with $N(\alpha) \leq e^7 \approx 1096$ and $|\xi_1| \leq \frac{5}{2}$ is represented with a dot at coordinates $(\frac{1}{2}\log(|N(\alpha)|), \xi_1)$. We recall that

$$\xi_1 = \frac{\log(|\alpha|/|\alpha^\sigma|)}{2\log(\frac{1+\sqrt{5}}{2})}.$$

The fundamental domain is the region between the two blue lines.

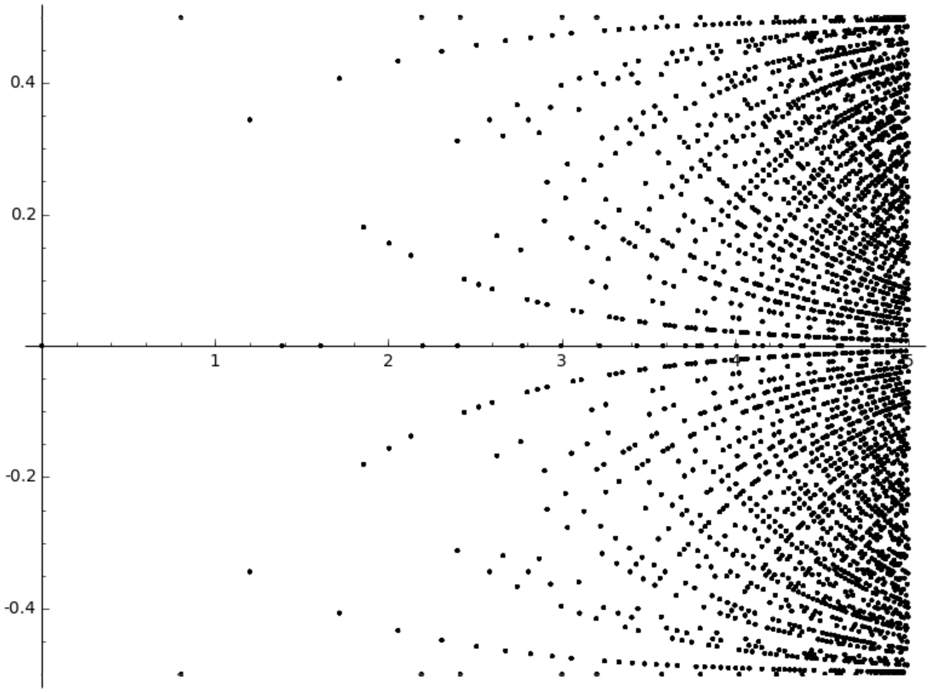

Figure 2.5: This is a zoomed-in version of Figure 2.4, showing only the fundamental domain. Every $\alpha \in \mathbb{Z}[\zeta_5]$ with $N(\alpha) \leq e^{10} \approx 22026$ and $|\xi_1| \leq \frac{1}{2}$ is represented with a dot at coordinates $\left(\frac{1}{2}\log(|N(\alpha)|), \xi_1\right)$. The reason why the points seem so clearly distributed along these curves has to do with the following two polynomials whose values for integer variables don't seem quite equidistributed:

$$x_1^2 + x_2^2 + x_3^2 + x_4^2, \qquad x_1x_2 + x_2x_3 + x_3x_4$$

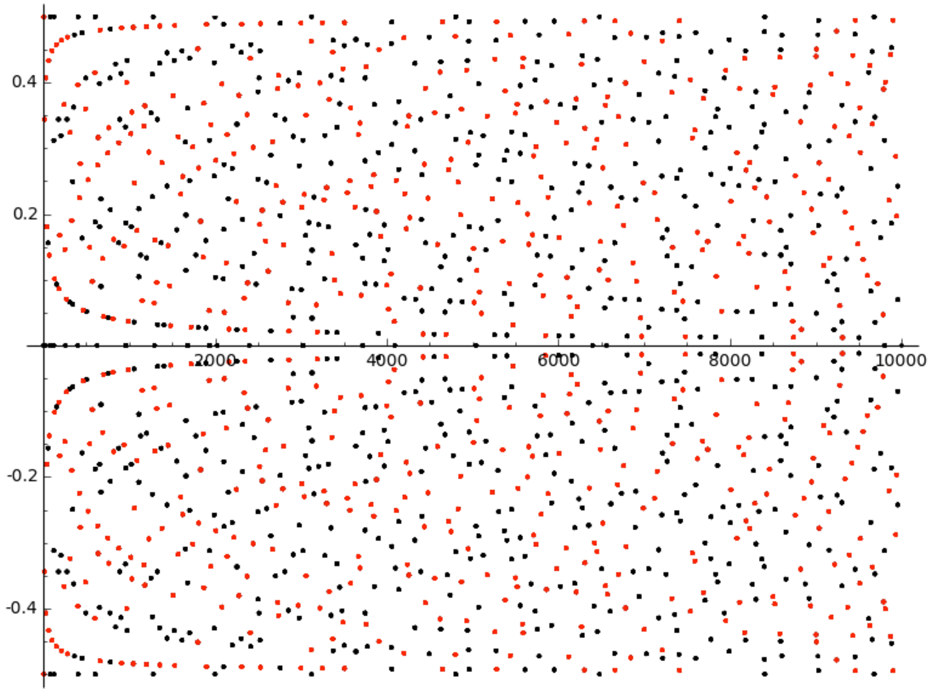

Figure 2.6: Finally, this is a picture of the fundamental domain in (ξ, ξ_1)-space. All α with $\xi = N(\alpha) \leq 10^6$ and $|\xi_1| \leq \frac{1}{2}$ are represented by a dot (ξ, ξ_1). Red dots correspond to elements α of prime norm.

A general credo in mathematics is that the number of points belonging to a lattice inside some smooth bounded region should be asymptotically proportional to the euclidean volume of this region, unless of course the region is actively preventing this from happening.

Consider for example the n-dimensional sphere $\mathrm{B}_n(0, t)$ and the standard lattice $\mathbb{Z}^n$. We write θ_n to be the least number such that for any $\theta > \theta_n$ we have

$$|\mathrm{B}_n(0, t) \cap \mathbb{Z}^n| = \mathrm{Vol}(\mathrm{B}_n(0, 1))t^n + O(t^\theta).$$

It is known that for dimensions 4 and up, $\theta_n = n - 2$, see e.g.[8]. In the two and three dimensional case the determination of θ_n is an open problem, but the conjectured values are equal to the proven lower bounds $\theta_2 \geq \frac{1}{2}, \theta_3 \geq 1$. In two dimensions this problem is known as Gauss' Circle Problem, and the best result is that of Huxley[17], who uses exponential sums to prove that $\theta_2 \leq 131/208$. In three dimensions Heath-Brown[15], see also [4], is able to prove $\theta_3 \leq 21/16$. We will be concerned with the high-dimensional case, be it with a more general region, namely $\mathcal{F}(t)$, and with lattices Γ more general than the standard lattice — but still quite special.

The notion of the boundary of the region being of Lipschitz-class is one criterion with which we can formulate the aforementioned credo into a theorem.

Definition 2.20. A subset $S \subset \mathbb{R}$ is of Lipschitz class $\mathcal{L}(n, M, L)$ if there are M maps $\phi_1, \ldots, \phi_M : [0, 1]^{n-1} \longrightarrow \mathbb{R}^n$ such that S is covered by the images of the maps ϕ_i, and the maps satisfy the Lipschitz condition

$$\|\phi_i(x) - \phi_i(y)\| \leq L\|x - y\| \text{ for } x, y \in [0,1]^{n-1}, i = 1, \ldots, M \tag{2.4}$$

We note that the Lipschitz constant of a blown-up region tR equals tL, where L is the Lipschitz constant of R. Thus the Lipschitz constant will take on the role of the scaling factor t.

Lemma 2.21. *Pick any $\delta > 0$, and let*

$$\mathcal{F}_\delta(t^n) = \{x \in \mathcal{F} \mid \delta t^n \leq |N(x)| \leq t^n\}.$$

The boundary $\partial\mathcal{F}_\delta(t^n)$ is of Lipschitz-class $\mathcal{L}(n, 2^{2r_1+r_2}, ct)$, where

$$c = \sqrt{n}\pi(r + \frac{1}{n\delta^{(n-1)/n}})m(\varepsilon)^{\frac{r}{2}} \log m(\varepsilon)$$

and $m(\varepsilon)$ is the maximal absolute value under any embedding of any fundamental unit or its inverse.

Proof. The construction of the fundamental domain $\mathcal{F}(1)$ comes with 2^{r_1} maps from $[0,1]^n$ to $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ whose image is exactly $\mathcal{F}(1)$ as follows. 1 dimension is for the norm, $r_1 + r_2 - 1$ dimensions restrict the multiplication by units, and r_2 dimensions are necessary to reconstruct a complex element from their absolute value. 2^{r_1} maps are needed to cover all choices of sign for the real dimensions. Concretely, let $(\eta_1, \ldots, \eta_{r_1})$ be a choice of r_1 signs.

$$
\begin{aligned}
(\xi, \xi_1, \ldots, \xi_r, a_1, \ldots, a_{r_2}) &\longmapsto (\rho_1, \ldots, \rho_{r_1+r_2}, a_1, \ldots, a_{r_2}) \\
&\longmapsto (\eta_1\rho_1, \ldots, \eta_{r_1}\rho_{r_1}, \sin(2\pi a_1)\rho_{r_1+1}, \cos(2\pi a_1)\rho_{r_1+1} \\
&\qquad \ldots, \sin(2\pi a_{r_2})\rho_r, \cos(2\pi a_{r_2})\rho_r)
\end{aligned}
$$

where $\xi = \prod_{i=1}^{r_1+r_2} \rho_i^{e_i}$, and

$$
\begin{cases}
\rho_1 &= \xi^{1/n} \prod_{j=1}^{r} |\varepsilon_j^{\tau_1}|^{\xi_j - 1/2} \\
\vdots & \\
\rho_{r_1} &= \xi^{1/n} \prod_{j=1}^{r} |\varepsilon_j^{\tau_{r_1}}|^{\xi_j - 1/2}
\end{cases}
\qquad
\begin{cases}
\rho_{r_1+1} &= \xi^{1/n} \prod_{j=1}^{r} |\varepsilon_j^{\sigma_1}|^{\xi_j - 1/2} \\
\vdots & \\
\rho_{r_1+r_2} &= \xi^{1/n} \prod_{j=1}^{r} |\varepsilon_j^{\sigma_{r_2}}|^{\xi_j - 1/2}
\end{cases}
$$

The boundary of $\mathcal{F}_\delta(1)$ is then covered by all 2^{r_1+r+1} maps where each map is given by a choice of signs $(\eta_1, \ldots, \eta_{r_1})$ and either fixing the value of ξ to be δ or 1, or fixing one of $\xi_1, \ldots \xi_r$ to be 1 or 0 in the above map. In order to bound the Lipschitz constant, we note in general that if $f(x_1, x_2, \ldots, x_n) = \prod_i g_i(x_i)$, where $|g_i(x_i) - g_i(x_i')| \leq L_i|x_i - x_i'|$ and $|g_i(x_i)| \leq M_i$, that

$$
|f(x_1, x_2, \ldots, x_n) - f(x_1', x_2', \ldots, x_n')| \leq \sum_i L_i \prod_{j \neq i} M_j \sqrt{\sum_i |x_i - x_i'|^2}. \quad (2.5)
$$

To this end we note that, for $(\xi, \xi_1, \ldots, \xi_r) \in [\delta, 1] \times [0,1]^r$,

$$\begin{cases} |\xi^{1/n}| \leq 1 \\ |\xi^{1/n} - \xi'^{1/n}| \leq \frac{1}{n\delta^{(n-1)/n}} |\xi - \xi'| \\ |a|^{\xi_i - 1/2} \leq \max(\sqrt{|a|}, \frac{1}{\sqrt{|a|}}) \\ ||a|^{\xi_i - 1/2} - |a|^{\xi'_i - 1/2}| \leq \log(|a|) \max(\sqrt{|a|}, \frac{1}{\sqrt{|a|}}) |\xi_i - \xi'_i| \end{cases} \tag{2.6}$$

Recall that

$$m(\varepsilon) = \max_{i,j} \{ |\varepsilon_j^{\tau_i}|, |\varepsilon_j^{\tau_i}|^{-1}, |\varepsilon_j^{\sigma_i}|, |\varepsilon_j^{\sigma_i}|^{-1} \},$$

so that we may combine (2.5) and (2.6) to bound, keeping ξ fixed,

$$|\rho_i(\xi, \xi_1, \ldots, \xi_r) - \rho_i(\xi, \xi'_1, \ldots, \xi'_r)| \leq r m(\varepsilon)^{\frac{r}{2}} \log m(\varepsilon) \sqrt{\sum_i |\xi_i - \xi'_i|^2},$$

and similarly for

$$|\rho_{r_1+i}(\xi, \xi_1, \ldots, \xi_r) \sin(2\pi a_i) - \rho_{r_1+i}(\xi, \xi'_1, \ldots, \xi'_r) \sin(2\pi a'_i)|,$$

so that for this map we may choose

$$L \leq \sqrt{n} \pi r \, m(\varepsilon)^{\frac{r}{2}} \log m(\varepsilon).$$

We now consider the maps where one of the ξ_i is fixed to be 0 or 1, and all others including ξ are allowed to vary. We may in the same way bound

$$|\rho_i(\xi, \xi_1, \dots, \xi_r) - \rho_i(\xi', \xi'_1, \dots, \xi'_r)| \\ \le (r - 1 + \frac{1}{n\delta^{(n-1)/n}}) m(\varepsilon)^{\frac{r}{2}} \log m(\varepsilon) \sqrt{\sum_i |\xi_i - \xi'_i|^2},$$

and similarly for

$$|\rho_{r_1+i}(\xi, \xi_1, \dots, \xi_r) \sin(2\pi a_i) - \rho_{r_1+i}(\xi', \xi'_1, \dots, \xi'_r) \sin(2\pi a'_i)|,$$

so that for these maps we may choose

$$L \le \sqrt{n}\pi(r - 1 + \frac{1}{n\delta^{(n-1)/n}})\, m(\varepsilon)^{\frac{r}{2}} \log m(\varepsilon),$$

so that finally the Lipschitz constant is bounded by

$$L \le \sqrt{n}\pi(r + \frac{1}{n\delta^{(n-1)/n}})\, m(\varepsilon)^{\frac{r}{2}} \log m(\varepsilon) \qquad \square$$

The fact that we cannot take $\delta = 0$ is not a major hurdle. It will be enough to take $\delta = \frac{1}{2}$, and use a dyadic composition. The appearance of $m(\varepsilon)$ in the Lipschitz-constant is more challenging to handle since the size of the units is notoriously unknown. Yet, we can exploit the freedom in choice of fundamental units. Choosing a suitable basis, we can prove the following.

Theorem 2.22. *Let $K = \mathbb{Q}(\zeta_\ell)$. There exists a choice of fundamental units ε_j such that*

$$m(\varepsilon) \leq \ell^{\frac{\ell-3}{4}}.$$

Proof. Consider the set of cyclotomic units $\left\{\frac{1-\zeta_\ell^i}{1-\zeta_\ell^j} \mid i,j = 1,\ldots,\ell-1\right\}$. It is known that they generate a finite-index subgroup of the full unit group[46] (in fact, the index is precisely h_p^+.) This implies that we can find r multiplicatively independent cyclotomic units. The ℓ_∞-norm of the image under the logarithmic Minkowski embedding of any cyclotomic unit is bounded as follows

$$\|\log\phi(\frac{1-\zeta_\ell^i}{1-\zeta_\ell^j})\|_\infty \leq |\log(\frac{2}{1-\zeta_\ell})| \leq \log\ell.$$

Now, since these r independent units do not necessarily constitute a basis, we use a lemma of Mahler-Weyl[3, Lemma 8, p.135], which yields that there exists a basis $\log\phi(\varepsilon_1),\ldots,\log\phi(\varepsilon_r)$ such that

$$\|\log\phi(\varepsilon_j)\|_\infty \leq \max(1,\frac{j}{2})\log\ell.$$

Thus for this choice of basis,

$$m(\varepsilon) \leq \max_j\|\log\phi(\varepsilon_j)\|_\infty \leq \frac{r}{2}\log\ell.$$ □

To ensure a good explicit error term with respect to the particular lattice Γ, we introduce two notions describing the key properties of the lattice. The first gives a measure of the minimal lengths of basis vectors, and the second a measure of the deviation from orthogonality of a basis.

Definition 2.23. We define the Successive Minima $\lambda_i(\Gamma), i = 1, \dots, n$ of a lattice Γ as

$$\lambda_i(\Gamma) = \inf\{\lambda \in \mathbb{R} \mid B(0, \lambda) \cap \Gamma \text{ contains } i \text{ linearly independent vectors}\}.$$

Definition 2.24. We define the Orthogonality Defect $\Omega(\Gamma)$ of a lattice Γ as

$$\Omega(\Gamma) = \inf_{(u_1,\dots,u_n)} \frac{|u_1| \cdots |u_n|}{\det \Gamma},$$

where the infimum runs over all bases $(u_1, \dots, u_n)$ of Γ.

In order to count lattice points, we will use the following theorem by Widmer [47, Theorem 5.4].

Theorem 2.25. *Let Γ be a lattice in $\mathbb{R}^n$ with successive minima $\lambda_1, \dots, \lambda_n$ and orthogonality defect Ω. Let S be a bounded set in $\mathbb{R}^n$ such that the boundary ∂S is of Lipschitz class $\mathcal{L}(n, M, L)$. Then S is measurable, and moreover,*

$$\left| |S \cap \Gamma| - \frac{\mathrm{Vol}(S)}{\det \Gamma} \right| \leq M 2^{n-1} (\sqrt{n}\Omega + 2)^n \max_{0 \leq i < n} \frac{L^i}{\lambda_1 \cdots \lambda_i},$$

or, since unconditionally we have $\Omega \leq \dfrac{n^{\frac{3}{2}n}}{(2\pi)^{\frac{n}{2}}}$,

$$\left| |S \cap \Gamma| - \frac{\mathrm{Vol}(S)}{\det \Gamma} \right| \leq M n^{3n^2/2} \max_{0 \leq i < n} \frac{L^i}{\lambda_1 \cdots \lambda_i},$$

For our uses, the virtue of this theorem is in its explicitness and, which is vital for our sieving process, in that it is optimal in terms of the successive minima λ_i. We now use this theorem to prove our key lemma in the estimation of $\mathcal{A}_{\mathfrak{d}}$. We state this key lemma in as general terms as possible, since it seems likely to be useful in other situations as well.

Lemma 2.26. *Let* $\mathfrak{a}$ *be an integral ideal of the ring of integers* $\mathcal{O}_K$ *of a number field* K *of degree* n*. Let* $\mathfrak{M} \subseteq \mathfrak{a}$ *be a subgroup of* $(\mathcal{O}_K, +)$*. Then*

$$\left| \left\{ \alpha \in \mathfrak{M} \;\middle|\; \phi(\alpha) \in \mathcal{F}(t^n) \right\} \right| = \frac{\omega \ \mathrm{res}_{s=1} \zeta_K(s)}{h_K [\mathcal{O}_K : \mathfrak{M}]} t^n + O\left(\max(1, \frac{t^{n-1}}{N(\mathfrak{a})^{\frac{n-1}{n}}}) \right),$$

where the constant in the O-term is bounded by $n^{4n^2} m(\varepsilon)^{\frac{nr}{2}}$*. Moreover, if* $K = \mathbb{Q}(\zeta_\ell)$*, the constant is bounded by* $\ell^{\frac{\ell^3}{2}}$*.*

Proof. To apply Theorem 2.25, we need to deal with points inside a region of Lipschitz class, which is why we decompose the set on the left hand side as

$$\sum_{k=0}^{\infty} \left| \left\{ \alpha \in \mathfrak{M} \;\middle|\; \phi(\alpha) \in \mathcal{F}_{\frac{1}{2}}(\tfrac{1}{2^k} t^n) \right\} \right|.$$

Since $\mathfrak{M}$ is an additive subgroup of $\mathcal{O}_K$, $\phi(\mathfrak{M})$ is a subgroup of the lattice $\phi(\mathcal{O}_K)$, and hence Theorem 2.25 applies. For the main term, we need the determinant of $\phi(\mathfrak{M})$. We note that since the index of $\phi(\mathfrak{M})$ in $\phi(\mathcal{O}_K)$ is equal to $[\mathcal{O}_K : \mathfrak{M}]$, it suffices to compute the determinant of $\mathcal{O}_K$. Now let α_i be a basis for the ring of integers, then we need to compute the determinant of the matrix with entries $(\alpha_i^{\tau_j})$ for $i = 1, \ldots, n$ and $j = 1, \ldots, r_1$, and alternately $(\mathrm{Re}(\alpha_i^{\sigma_j}))$ and $(\mathrm{Im}(\alpha_i^{\sigma_j}))$ for $i = 1, \ldots, n$ and $j = 1, \ldots, r_2$. The reader is advised to write along to see that this is a square matrix, and that we may replace the last $2r_2$ columns by alternately $(\alpha_i^{\sigma_j})$ and $(\alpha_i^{\bar{\sigma}_j})$ for $i = 1, \ldots, n$ and $j = 1, \ldots, r_2$, at the cost of introducing a factor 2 for each σ_j. This way we arrive at the square root of the usual definition of the discriminant of K, and have proven that

$$\det \phi(\mathcal{O}_K) = 2^{-r_2}\sqrt{\Delta_K}.$$

Finally, the main term equals

$$\sum_{k=0}^{\infty} \frac{\mathrm{Vol}(\mathcal{F}_{\frac{1}{2}}(\frac{1}{2^k}t^n))}{\det \phi(\mathfrak{M})} = \sum_{k=0}^{\infty} \frac{\mathrm{Vol}(\mathcal{F}_{\frac{1}{2}}(\frac{1}{2^k}))}{[\mathcal{O}_K : \mathfrak{M}]2^{-r_2}\sqrt{\Delta_K}} t^n = \frac{2^{r_1}(2\pi)^{r_2}\mathrm{Reg}_K}{[\mathcal{O}_K : \mathfrak{M}]\sqrt{\Delta_K}} t^n$$
$$= \frac{\omega \ \mathrm{res}_{s=1}\zeta_K(s)}{h_K[\mathcal{O}_K : \mathfrak{M}]} t^n.$$

For the error term, we give an upper bound to the successive minima by noting that each λ_i is the distance to the origin of a certain point x in the lattice.

As such, it is an element $\phi(\alpha)$ of $\phi(\mathfrak{a})$, and using the AM-GM inequality

$$|x|^2 = \sum_{i=1}^{r_1} |\alpha^{\tau_i}|^2 + 2\sum_{i=1}^{r_2} \frac{|\alpha^{\sigma_i}|^2}{2} \geq n \left(\frac{N(\alpha)^2}{2^{2r_2}}\right)^{1/n} \geq \frac{n}{4^{r_2/n}} \left(N(\mathfrak{a})\right)^{2/n},$$

thus $\lambda_i \geq \frac{\sqrt{n}}{2^{r_2/n}} \left(N(\mathfrak{a})\right)^{1/n} \geq \left(N(\mathfrak{a})\right)^{1/n}$. Thus, using Theorem 2.25, the error term is smaller than

$$\begin{aligned} \sum_{k=0}^{\infty} Mn^{3n^2/2} \max_{i \leq n-1} \frac{L^i}{\lambda_1 \cdots \lambda_i} \\ &\leq 2^{2r_1+r_2} n^{3n^2/2} \left(\pi n^{3/2} m(\varepsilon)^{\frac{r}{2}} \log m(\varepsilon)\right)^{n-1} \max_{i \leq n-1} \sum_{k=0}^{\infty} \frac{(t/2^{k/n})^i}{N(\mathfrak{a})^{i/n}} \\ &\leq n^{4n^2} m(\varepsilon)^{\frac{rn}{2}} \frac{t^{n-1}}{N(\mathfrak{a})^{\frac{n-1}{n}}}, \end{aligned}$$

where we have used the fact that $\sum_{k=0}^{\infty} \frac{1}{2^{k/n}} \leq n$. If $K = \mathbb{Q}(\zeta_\ell)$, we can use Theorem 2.22, which says that $m(\varepsilon) \leq \ell^{\frac{\ell-3}{2}}$ to dominate the constant by $\ell^{\frac{\ell^3}{2}}$. $\square$

We judge it prudent to remark that, in the case $\mathfrak{M} = \mathcal{O}_K$, such an explicit computation has been attempted in [35]. However, the argument is at best incomplete. (In their essential lemma 3.1 they do not take into account their "regulator condition" and hence only consider a small part of the boundary of $\mathcal{F}$. In lemma 3.2 the factor $\tilde{\beta}^n$ is dropped, whose presence would complicate the passage from the first to the second part of Theorem 5.)

We conclude with some critical remarks on the quality of the error term, and in particular we justify the use of Theorem 2.25.

1. With regards to the exponent of t, our lemma is less than optimal. In the case that $\mathfrak{M} = \mathfrak{a}$, Landau[22] was able to produce an error of $O(t^{n-\frac{2n}{n+1}})$, and he also proved that the error is at least $\Omega(t^{\frac{n}{2}-\frac{1}{2}})$. The upper bound has been improved slightly, using exponential sums, by Nowak[37], and Lao[24] has recently proven a more substantial improvement. He uses Heath-Browns subconvexity estimate[14] to obtain an error of $O(t^{n-\frac{3n}{n+6}})$. The lower bound has been improved by some logarithmic factors[12].

   A common feature of these results is that they do not treat the problem as a pure lattice counting problem. That is, the set of lattice points is interpreted as the partial sum of the coefficients of the Dedekind Zeta function, and one uses such analytic information as the functional equation for $\zeta_K(s)$. In this light a generalisation of the above results to general $\mathfrak{M}$ seems not very straightforward.

   However, at any rate a lowering of the exponent θ of t will naturally demand to likewise introduce the exponent θ in the successive minima λ, or thus in the power of $N(\mathfrak{b})$, which for our purposes, as we will see in Theorem 2.33, gives no improvement in the end.

2. It is best possible in terms of $N(\mathfrak{b})$. The saving of $N(\mathfrak{b})^{\frac{n-1}{n}}$ in the error term corresponds to being able to scale each direction with a factor $N(\mathfrak{b})^{\frac{1}{n}}$, which, since the determinant of the lattice is proportional to $N(\mathfrak{b})$, is optimal.

3. It is not very satisfactory in terms of the dimension n. However, given the presence of the maximal size of the absolute value of units, improvements in general seem very hard. We could mention that for those ℓ with $h_\ell^+ = 1$, we may take the cyclotomic units as fundamental units, and obtain roughly ℓ^{ℓ^2} instead of ℓ^{ℓ^3}. There is no reason to believe that the orthogonality defect of lattices coming from ideals would be significantly lower than the worst-case scenario. Indeed, lattices coming from ideals are rather special in the sense that their successive minima are very large, which is linked to a high orthogonality defect.

The key lemma enables us to make Landau's classical proof of the meromorphic continuation of $\zeta_K(s)$ to $\mathrm{Re}(s) > 1 - \frac{1}{n}$ effective. Recall that $\zeta_K(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$, where a_n is the number of ideals of norm n.

Theorem 2.27. *Let K be a number field of degree n, and let $\kappa = \mathrm{res}_{s=1}\zeta_K(s)$. Then, for all $x \geq 1$,*

$$\sum_{n\leq x} a_n = \kappa x + O(x^{1-\frac{1}{n}}),$$

where the constant in the O-term is bounded by $h_K n^{4n^2} m(\varepsilon)^{\frac{rn}{2}}$. Moreover, if $K = \mathbb{Q}(\zeta_\ell)$, the constant is bounded by ℓ^{ℓ^3}.

Proof. For each ideal class $\mathfrak{c}$ we pick an integral ideal $\mathfrak{b}$ in the inverse class $\mathfrak{b}$. We then have an isomorphism between the set of integral ideals in $\mathfrak{c}$ and the set of principal ideals in $\mathfrak{b}$

$$\mathfrak{a} \mapsto \mathfrak{a}\mathfrak{b} = (\alpha),$$

with inverse $(\alpha) \mapsto (\alpha)\mathfrak{b}^{-1}$, which is an integral ideal since $\mathfrak{b}|(\alpha)$. Thus we may count the ideals $\mathfrak{a}$ in the class $\mathfrak{c}$ of norm up to x by counting the principal ideals inside $\mathfrak{b}$ of norm up to $xN(\mathfrak{b})$. We do this by counting elements up to multiplication by units. If ω is the number of roots of unity in K, we may write the number of all ideals in $\mathfrak{c}$ of norm up to x as

$$\frac{1}{\omega}|\{\alpha \in \mathfrak{b} \mid \phi(\alpha) \in \mathcal{F}(xN(\mathfrak{b}))\}|.$$

Using the key lemma, we see that this equals

$$\frac{\mathrm{res}_{s=1}\zeta_K(s)}{h_K N(\mathfrak{b})} xN(\mathfrak{b}) + O\left(\frac{(N(\mathfrak{b})x)^{1-\frac{1}{n}}}{N(\mathfrak{b})^{\frac{n-1}{n}}}\right) = \frac{\mathrm{res}_{s=1}\zeta_K(s)}{h_K} x + O(x^{1-\frac{1}{n}}).$$

The statement of the theorem then follows by summation over all ideal classes. If $K = \mathbb{Q}(\zeta_\ell)$, we may finish the theorem with a crude estimate on the class number. A theorem by Minkowski states that every ideal class has as a representative a certain prime ideal of norm at most $\mathcal{M}(K) = \sqrt{|\Delta_K|}\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}$. Since there are at most n prime ideals of the same norm, the class number is bounded by n times the Minkowski bound. Using Stirling's approximation, we hence obtain for $K = \mathbb{Q}(\zeta_\ell)$,

$$h_K \leq (\ell-1)(\ell)^{\frac{\ell-2}{2}} \left(\frac{4}{\pi}\right)^{\frac{\ell-1}{2}} \frac{(\ell-1)^{3/2}}{e^{\ell-2}} \leq \ell^{\frac{\ell}{2}},$$

finishing the bound on the constant. $\square$

2.5 Conclusion of the Method

We now use our key lemma to bound the sets $\mathcal{A}_\mathfrak{d}$. We recall that

$$\mathcal{A}_\mathfrak{d}(t^{\ell-1}) = \dot{\bigcup_{\mathfrak{b}\in B}} \left\{ \begin{array}{l|l} \alpha \in \mathfrak{b} & \alpha \in \mathbb{Z} \bmod (1-\zeta_\ell)^2 \\ N(\alpha) \leq t^{\ell-1}N(\mathfrak{b}) & \alpha \text{ satisfies (2.1) for } q \\ \phi(\alpha) \in \mathcal{F} & \mathfrak{b}\mathfrak{d} \mid (\alpha) \end{array} \right\}, \tag{2.7}$$

Proposition 2.28. *Let $\mathfrak{d}$ be a squarefree integral ideal of $\mathbb{Z}(\zeta_\ell)$ with $(\mathfrak{d}, q) = 1$. We have for all $t \geq N(\mathfrak{d})^{\frac{1}{\ell-1}}$,*

$$|\mathcal{A}_\mathfrak{d}(t^{\ell-1})| = \frac{1}{N(\mathfrak{d})} \prod_{\mathfrak{q}|q} \left(1 - \frac{1}{N(\mathfrak{q})}\right) \frac{2\operatorname{res}_{s=1}\zeta_K(s)}{\ell} t^{\ell-1} + O\left(\frac{t^{\ell-2}}{N(\mathfrak{d})^{\frac{\ell-2}{\ell-1}}}\right),$$

where the constant in the O-term is bounded by $q^{\ell-2}\ell^{\ell^3}$.

Proof. The first step is to unravel the condition (2.1) as a number of additive conditions. By Proposition 2.15, there exist $\frac{\prod_{\mathfrak{q}|q}(N(\mathfrak{q})-1)}{\ell(q-1)}$ elements α_i such that the α that satisfy (2.1) are exactly the nonzero integer multiples of the α_i

modulo q. Consequently

$$|\mathcal{A}_{\mathfrak{d}}(t^{\ell-1})| = \sum_{\mathfrak{b}\in B}\sum_{\alpha_i}\left|\left\{\begin{array}{l|l} \alpha\in\mathfrak{b}\mathfrak{d} & \alpha\in\mathbb{Z} \bmod (1-\zeta_\ell)^2 \\ N(\alpha)\le t^{\ell-1}N(\mathfrak{b}) & \exists t\in\mathbb{Z} : \alpha\equiv t\alpha_i \bmod q \\ \phi(\alpha)\in\mathcal{F} & \end{array}\right\}\right|$$
$$-\frac{\prod_{\mathfrak{q}|q}(N(\mathfrak{q})-1)}{\ell(q-1)}\sum_{\mathfrak{b}\in B}\left|\left\{\begin{array}{l|l} \alpha\in q\mathfrak{b}\mathfrak{d} & \alpha\in\mathbb{Z} \bmod (1-\zeta_\ell)^2 \\ N(\alpha)\le t^{\ell-1}N(\mathfrak{b}) & \phi(\alpha)\in\mathcal{F} \end{array}\right\}\right|.$$

The points in the sets in the first summation are the points in an additive subgroup $\mathfrak{M}$ of $\mathbb{Z}[\zeta_\ell]$, containing $\mathfrak{b}\mathfrak{d}$, whose index can be seen to equal

$$[\mathbb{Z}[\zeta_\ell] : \mathfrak{M}] = [\mathbb{Z}[\zeta_\ell] : \mathfrak{b}\mathfrak{d}]\ell q^{\ell-2} = N(\mathfrak{b})N(\mathfrak{d})\ell q^{\ell-2}.$$

Indeed, the condition $\bmod(1-\zeta_\ell)^2$ describes a hyperplane $\bmod \ell$, that is, an index ℓ subspace of $\mathbb{Z}[\zeta_\ell]/\ell$. The condition $\bmod q$ evidently describes a line $\bmod q$, that is, an index $q^{\ell-2}$ subspace of $\mathbb{Z}[\zeta_\ell]/q$. In case that $1-\zeta_\ell \mid \mathfrak{d}$, the above index calculation still holds as the total condition $\bmod \ell$ now reduces to $(1-\zeta_\ell)^2 \mid \alpha$, describing a subspace of index $\ell^2 = \ell N(1-\zeta_\ell)$ in $\mathbb{Z}[\zeta_\ell]/\ell$.

Thus, using the key lemma,

$$\left|\left\{\begin{array}{l|l} \alpha \in \mathfrak{b}\mathfrak{d} & \alpha \in \mathbb{Z} \bmod (1-\zeta_\ell)^2 \\ N(\alpha) \leq t^{\ell-1}N(\mathfrak{b}) & \exists t \in \mathbb{Z} : \alpha \equiv t\alpha_i \bmod q \\ \phi(\alpha) \in \mathcal{F} & \end{array}\right\}\right|$$

$$= \frac{2\ell \operatorname{res}_{s=1}\zeta_K(s)}{h_\ell N(\mathfrak{b})N(\mathfrak{d})\ell q^{\ell-2}} N(\mathfrak{b})t^{\ell-1} + O\left(\frac{t^{\ell-2}N(\mathfrak{b})^{\frac{\ell-2}{\ell-1}}}{(N(\mathfrak{b})N(\mathfrak{d}))^{\frac{\ell-2}{\ell-1}}}\right)$$

$$= \frac{2 \operatorname{res}_{s=1}\zeta_K(s)}{h_\ell N(\mathfrak{d})q^{\ell-2}} t^{\ell-1} + O\left(\frac{t^{\ell-2}}{N(\mathfrak{d})^{\frac{\ell-2}{\ell-1}}}\right).$$

Likewise, the points in the sets in the second summation are the points in an additive subgroup $\mathfrak{M}$ of $\mathbb{Z}[\zeta_\ell]$ containing $q\mathfrak{b}\mathfrak{d}$, whose index is $[\mathbb{Z}[\zeta_\ell] : \mathfrak{M}] = N(q)N(\mathfrak{b})N(\mathfrak{d})\ell$. Bringing everything together,

$$\begin{aligned} |\mathcal{A}_\mathfrak{d}(t^{\ell-1})| &= h_\ell \frac{\prod_{\mathfrak{q}|q}(N(\mathfrak{q})-1)}{\ell(q-1)} \frac{2 \operatorname{res}_{s=1}\zeta_K(s)}{h_\ell N(\mathfrak{d})q^{\ell-2}} t^{\ell-1} + O\left(\frac{t^{\ell-2}}{N(\mathfrak{d})^{\frac{\ell-2}{\ell-1}}}\right) \\ &\quad - h_\ell \frac{\prod_{\mathfrak{q}|q}(N(\mathfrak{q})-1)}{\ell(q-1)} \frac{2 \operatorname{res}_{s=1}\zeta_K(s)}{h_\ell N(\mathfrak{d})N(q)} t^{\ell-1} + O\left(\frac{t^{\ell-2}}{q^{\ell-2}(N(\mathfrak{d}))^{\frac{\ell-2}{\ell-1}}}\right) \\ &= \prod_{\mathfrak{q}|q}\left(1-\frac{1}{N(\mathfrak{q})}\right) \frac{2 \operatorname{res}_{s=1}\zeta_K(s)}{\ell N(\mathfrak{d})} t^{\ell-1} + O\left(\frac{t^{\ell-2}}{N(\mathfrak{d})^{\frac{\ell-2}{\ell-1}}}\right). \end{aligned}$$

The constant in the O-term is bounded by the constant $\ell^{\frac{\ell^3}{2}}$ in the key Lemma 2.26 multiplied by $h_\ell \frac{\prod_{\mathfrak{q}|q}(N(\mathfrak{q})-1)}{\ell(q-1)}(1+\frac{1}{q^{\ell-2}}) \leq h_\ell q^{\ell-2}$. Using the Minkowski bound for the class number as in the end of Theorem 2.27, we obtain the stated upper bound for the constant. □

Thus, it turns out that in our case, ω is particularly simple. Recalling that

$$\mathcal{P} = \{\mathfrak{p} \text{ prime ideals in } \mathbb{Z}[\zeta_\ell] \mid (\mathfrak{p}, q) = 1\},$$

we have that

$$\omega(\mathfrak{p}) = \begin{cases} 1 & \text{if } \mathfrak{p} \in \mathcal{P} \\ 0 & \text{if } \mathfrak{p} \notin \mathcal{P}. \end{cases}$$

Set

$$X = \prod_{\mathfrak{q}|q} \left(1 - \frac{1}{N(\mathfrak{q})}\right) \frac{2 \operatorname{res}_{s=1}\zeta_K}{\ell} t^{\ell-1}.$$

Then we have shown, for each squarefree integral ideal $\mathfrak{d}$ coprime with q, that

$$\mathcal{A}_{\mathfrak{d}} = \frac{1}{N(\mathfrak{d})} X + R_{\mathfrak{d}}, \qquad \text{where } |R_{\mathfrak{d}}| \leq q^{\ell-2} \ell^{\ell^3} \max(1, \frac{t^{\ell-2}}{N(\mathfrak{d})^{\frac{\ell-2}{\ell-1}}}).$$

We now estimate two quantities which are relevant to our sieving situation. Recall that

$$\begin{aligned} G(z) &= \sum_{N(\mathfrak{d})<z} \mu^2(\mathfrak{d}) \frac{\omega(\mathfrak{d})}{N(\mathfrak{d}) \prod_{\mathfrak{p}|\mathfrak{d}}(1 - \frac{\omega(\mathfrak{p})}{N(\mathfrak{p})})} \\ &= \sum_{\substack{N(\mathfrak{d})<z \\ (\mathfrak{d},q)=1}} \frac{\mu^2(\mathfrak{d})}{\prod_{\mathfrak{p}|\mathfrak{d}}(N(\mathfrak{p}) - 1)} = \sum_{\substack{N(\mathfrak{d})<z \\ (\mathfrak{d},q)=1}} \frac{\mu^2(\mathfrak{d})}{\phi(\mathfrak{d})}. \end{aligned}$$

Lemma 2.29. *Let $K = \mathbb{Q}(\zeta_\ell)$. With $\mathcal{P}$ and $\omega(\mathfrak{p})$ as above, for all $z \geq 1$,*

$$G(z) \geq \prod_{\mathfrak{q}|q} \left(1 - \frac{1}{N(\mathfrak{q})}\right) \mathrm{res}_{s=1}\zeta_K(s) \left(\log(z) - \ell^{\ell^3}\right), \tag{2.8}$$

Proof. Note first that

$$\begin{aligned} G(z) \prod_{\substack{N(\mathfrak{q})<z \\ \mathfrak{q}|q}} \left(1 - \frac{1}{N(\mathfrak{q})}\right)^{-1} &= \sum_{\substack{(\mathfrak{d},q)=1 \\ N(\mathfrak{d})\leq z}} \frac{\mu^2(\mathfrak{d})}{\phi(\mathfrak{d})} \prod_{\substack{N(\mathfrak{q})<z \\ \mathfrak{q}|q}} \left(1 - \frac{1}{N(\mathfrak{q})}\right)^{-1} \\ &= \sum_{\substack{(\mathfrak{d},q)=1 \\ N(\mathfrak{d})\leq z}} \frac{\mu^2(\mathfrak{d})}{\phi(\mathfrak{d})} \prod_{\substack{N(\mathfrak{q})<z \\ \mathfrak{q}|q}} \left(1 + \frac{1}{N(\mathfrak{q})-1}\right) \\ &\geq \sum_{N(\mathfrak{d})\leq z} \frac{\mu^2(\mathfrak{d})}{\phi(\mathfrak{d})}. \end{aligned}$$

We may further reduce the sum

$$\sum_{N(\mathfrak{d})\leq z} \frac{\mu^2(\mathfrak{d})}{\phi(\mathfrak{d})} = \sum_{N(\mathfrak{d})\leq z} \frac{\mu^2(\mathfrak{d})}{N(\mathfrak{d})} \prod_{\mathfrak{p}|\mathfrak{d}} \left(1 - \frac{1}{N(\mathfrak{p})}\right)^{-1} \geq \sum_{N(\mathfrak{a})\leq z} \frac{1}{N(\mathfrak{a})}.$$

Put $\kappa = \mathrm{res}_{s=1}\zeta_K(s)$, and let a_n be the number of integral ideals of norm n. By partial summation,

$$\begin{aligned} \sum_{n\leq z} \frac{a_n}{n} &= \int_1^z \frac{\sum_{n\leq t} a_n}{t^2} dt + \frac{\sum_{n\leq z} a_n}{z} \\ &\geq \kappa \log(z) + O\left((\ell-1)(1 - \frac{1}{z^{\frac{1}{\ell-1}}})\right), \end{aligned}$$

where we have used Theorem 2.27 in the form

$$\sum_{n\leq z} a_n \geq \kappa z - h_\ell \ell^{\frac{\ell^3}{2}} z^{\frac{\ell-2}{\ell-1}},$$

thus the constant term is bounded by $\frac{1}{\kappa}(\ell-1)h_\ell \ell^{\frac{\ell^3}{2}}$. We use the analytic class number formula to substitute κ and bound the constant term by

$$\frac{\omega\sqrt{\Delta_K}}{\mathrm{Reg}_K (2\pi)^{\frac{\ell-1}{2}} h_\ell}(\ell-1)h_\ell \ell^{\frac{\ell^3}{2}} \leq \ell^{\ell^3}.$$

Indeed, Friedman [9] shows that all number fields have regulator at least 0.2052. Even more, $\frac{\mathrm{Reg}_K}{\omega}$ is at least 0.9058 — this bound is attained only by $\mathbb{Q}(\zeta_5)$. $\square$

Remark 2.30. The constant ℓ^{ℓ^3} appearing in the above lower bound for $G(z)$ is the main culprit for the large constant in our final Theorem 2.34. One might think that this is a side effect of our insistence to use Selberg's sieve in the ring $\mathbb{Z}[\zeta_\ell]$, but it is in fact the nature of the problem. If we reformulate our sieve problem over $\mathbb{Z}$, the multiplicative function ω will change values accordingly and give rise to the same $G(z)$.

Lemma 2.31. *Let $K = \mathbb{Q}(\zeta_\ell)$. Then, for all $z \geq 2\ell$,*

$$\prod_{N(\mathfrak{p})\leq z}\left(1+\frac{1}{N(\mathfrak{p})}\right) \leq 100\log^2(z/\ell). \tag{2.9}$$

Proof. We first estimate $\sum_{N(\mathfrak{p})\leq z} \frac{1}{N(\mathfrak{p})}$. Since the norm of the ideals lying above p equals p^m, where m is the order of $p \bmod \ell$, we have that

$$\sum_{N(\mathfrak{p})\leq z} \frac{1}{N(\mathfrak{p})} = \sum_{\substack{p^m\equiv 1(\ell)\\ p^m\leq z}} \frac{\ell-1}{m}\frac{1}{p^m},$$

and we may employ the Brun-Titchmarsh inequality, Theorem 2.3.

$$\begin{aligned}
(\ell-1)\sum_{\substack{p^m\equiv 1(\ell)\\ p^m\leq z}} \frac{1}{mp^m} &= (\ell-1)\int_{2\ell}^{z} \frac{d(\Pi(x,\ell,1))}{x} \\
&= (\ell-1)\int_{2\ell}^{z} \frac{\Pi(x,\ell,1)dx}{x^2} + (\ell-1)\frac{\Pi(z,\ell,1)}{z} \\
&\leq 2\int_{2\ell}^{z} \frac{dx}{x\log(x/\ell)} + \frac{2}{\log(z/\ell)} \\
&\leq 2\int_{2}^{z/\ell} \frac{dx}{x\log(x)} + \frac{2}{\log(2)} \\
&\leq 2\int_{\log(2)}^{\log(z/\ell)} \frac{dx}{x} + \frac{2}{\log(2)} \\
&= 2\log_2(z/\ell) - 2\log_2(2) + \frac{2}{\log(2)},
\end{aligned}$$

where we assumed that $k+1$ is not a prime power. If it is, it is a power of 2, and causes a contribution of $(\ell-1)\ell\log(2)\log(\ell)(\ell+1) \leq \log(2)/\log(3)$. Now, since

$$\log(2)/\log(3) - 2\log_2(2) + \frac{2}{\log(2)} \leq \log(100),$$

we may conclude that

$$\prod_{N(\mathfrak{p})\leq z}\left(1+\frac{1}{N(\mathfrak{p})}\right)\leq e^{\sum_{N(\mathfrak{p})\leq z}\frac{1}{N(\mathfrak{p})}}\leq 100\log^2(z/k). \qquad \square$$

Remark 2.32. In the usual setting of the Selberg Sieve, the above product for rational primes is bounded by a constant times $\log(z)$ by Mertens' Theorem. The exponent 2 is a consequence of our use of the Brun-Titchmarsh inequality. If one would be content to leave k fixed and z large, then one could replace the 2 by $1+\varepsilon$. However, this is of no consequence to our purposes.

Theorem 2.33. *With notation as above, for $z > \exp(\ell^{\ell^3})$ and $t^{\ell-1}\geq z^2$,*

$$S(\mathcal{A}(t^{\ell-1}),\mathcal{P},z)\leq \frac{2}{\ell}\frac{t^{\ell-1}}{\log(z)-\ell^{\ell^3}}+\Sigma_2,$$

where

$$|\Sigma_2|\leq q^{\ell-2}\ell^{\ell^3}t^{\ell-2}z^{2/(\ell-1)}10^6\log^6(z/\ell).$$

Proof. We apply Theorem 2.17, and retrieve the main term after plugging in the estimate for $G(z)$ (2.8) . To estimate Σ_2, we use the bound $|R_{\mathfrak{d}}|\leq q^{\ell-2}\ell^{\ell^3}\frac{t^{\ell-2}}{N(\mathfrak{d})^{\frac{\ell-2}{\ell-1}}}$ which holds since $t^{\ell-1}\geq z^2$, and all $\mathfrak{d}$ in the sum have $N(\mathfrak{d})\leq z^2$. So

$$
\begin{aligned}
\Sigma_2 &\le \sum_{\substack{N(\mathfrak{d})<z^2\\ \mathfrak{d}|\Pi(z)}} 3^{\nu(\mathfrak{d})}|R_{\mathfrak{d}}| \\
&\le q^{\ell-2}\ell^{\ell^3}t^{\ell-2}\sum_{\substack{N(\mathfrak{d})<z^2\\ \mathfrak{d}|\Pi(z)}} \frac{3^{\nu(\mathfrak{d})}}{N(\mathfrak{d})^{\frac{\ell-2}{\ell-1}}} \\
&\le q^{\ell-2}\ell^{\ell^3}t^{\ell-2}z^{2/(\ell-1)}\sum_{\substack{N(\mathfrak{d})<z^2\\ \mathfrak{d}|\Pi(z)}} \frac{3^{\nu(\mathfrak{d})}}{N(\mathfrak{d})}.
\end{aligned}
$$

Now,

$$
\sum_{\substack{N(\mathfrak{d})<z^2\\ \mathfrak{d}|\Pi(z)}} \frac{3^{\nu(\mathfrak{d})}}{N(\mathfrak{d})} \le \prod_{\substack{N(\mathfrak{p})<z\\ \mathfrak{p}\in\mathcal{P}}}\left(1+\frac{3}{N(\mathfrak{p})}\right) \le \prod_{\substack{N(\mathfrak{p})<z\\ \mathfrak{p}\in\mathcal{P}}}\left(1+\frac{1}{N(\mathfrak{p})}\right)^3
$$

and so, plugging in equation (2.9), it follows that

$$
|\Sigma_2| \le q^{\ell-2}\ell^{\ell^3}t^{\ell-2}z^{2/(\ell-1)}10^6\log^6(z/\ell). \qquad \square
$$

Theorem 2.34. *Let $\mathcal{S}_q$ be the set of completely splitting primes in $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{q})$. The following bound holds for all odd primes ℓ, for all primes $q \neq \ell$, and for all $x > q^{\frac{5(\ell-2)(\ell-1)}{4}}\ell^{\ell^{\ell^3}}$.*

$$
\pi(x,\mathcal{S}_q) \le \frac{3}{\ell(\ell-1)}\frac{x}{\log(x)-\log\left(q^{\frac{5(\ell-2)(\ell-1)}{4}}\ell^{\ell^{\ell^3}}\right)}.
$$

Proof. Using Corollary 2.18 and Theorem 2.33, we have that

$$\pi(t^{\ell-1}, \mathcal{S}_q) \leq \frac{1}{\ell(\ell-1)} \frac{t^{\ell-1}}{\log(z) - \ell^{\ell^3}} + q^{\ell-2} \ell^{\ell^3} t^{\ell-2} z^{2/(\ell-1)} 10^6 \log^6(z/\ell).$$

We put

$$z = \frac{t^{\frac{2(\ell-1)}{5}}}{q^{\frac{(\ell-2)(\ell-1)}{2}} \exp(\ell^{\ell^3})}.$$

The main term is then bounded by

$$\frac{5/2}{\ell(\ell-1)} \frac{t^{\ell-1}}{\log(t^{\ell-1}) - \log\left(q^{\frac{5(\ell-2)(\ell-1)}{4}} \ell^{\ell^{\ell^3}}\right)}.$$

The error term is then bounded by

$$\frac{1}{2\ell^2} t^{\ell-6/5} \log^6(t) \leq \frac{1}{2\ell^2} \frac{t^{\ell-1}}{\log t},$$

since $\log^7(t) \leq t^{1/5}$, which holds because $t = x^{1/(\ell-1)} \geq \ell^{\ell^{\ell^2}}$ and $\ell \geq 3$. Thus we retrieve the statement of the theorem. □

Remark 2.35. The main purpose of the theorem is to provide a generalised Brun-Titchmarsh bound when ℓ is fixed, but with all constants explicitly bounded. Thus one should interpret the factor $\ell^{\ell^{\ell^3}}$ as only a constant. One may infer at the same time that the approach of counting integers points in high-dimensional number fields is not likely to yield results useful to applications where one needs to be able to let ℓ tend to infinity. Of more importance is the exponent $\frac{5(\ell-2)(\ell-1)}{4}$ of q, which could be lowered to $(\ell-2)(\ell-1)$ — likewise, the constant factor 3 could be brought down to $2+\varepsilon$ — if one is willing to allow an error term to remain. We have instead opted to prove a clean statement, free of error terms.

2.6 Adding More Roots

We describe our final supplement to the Sieving method. The generalisation to multiple roots $q_1, \ldots, q_n$ is a fairly technical operation which does not require any special arguments but which was left out of the main argument for aesthetic motives. Recall that the q_i are primes, and we use the notation $Q = q_1 \cdots q_n$. We may use the same sieving strategy since we have proven Proposition 2.16 in the general case of n roots. The sets $\mathcal{A}_{\mathfrak{d}}(t^{\ell-1})$ are now defined as

$$\mathcal{A}_{\mathfrak{d}}(t^{\ell-1}) = \dot{\bigcup_{\mathfrak{b}\in B}} \left\{ \begin{array}{l|l} \alpha \in \mathfrak{b} & \alpha \in \mathbb{Z} \bmod (1-\zeta_\ell)^2 \\ N(\alpha) \leq t^{\ell-1} N(\mathfrak{b}) & \alpha \text{ satisfies (2.1) for } q_1, \ldots, q_n \\ \alpha \in \mathcal{F} & \frac{N(\alpha)}{N(\mathfrak{b})} \text{ is prime} \end{array} \right\}$$

Proposition 2.36. *Let $\mathfrak{d}$ be a squarefree integral ideal of $\mathbb{Z}(\zeta_\ell)$ with $(\mathfrak{d}, Q) = 1$. We have for all $t \geq N(\mathfrak{d})^{\frac{1}{\ell-1}}$,*

$$|\mathcal{A}_{\mathfrak{d}}(t^{\ell-1})| = \frac{1}{N(\mathfrak{d})} \prod_{\mathfrak{q}|Q} \left(1 - \frac{1}{N(\mathfrak{q})}\right) \frac{2\, \mathrm{res}_{s=1}\zeta_K(s)}{\ell^n} t^{\ell-1} + O\left(\frac{t^{\ell-2}}{N(\mathfrak{d})^{\frac{\ell-2}{\ell-1}}}\right),$$

where the constant in the O-term is bounded by $Q^{\ell-2}\ell^{\ell^3}\frac{2^n}{\ell^n}$

Proof. We again start with the unravelling of the conditions $\mathrm{mod} q_j$ into additive conditions using 2.15. Let α_i^j be such that the elements α satisfying condition (2.1) $\mathrm{mod} q_j$ are exactly the nonzero integer multiples of the $\alpha_i^j \bmod q_j$. Let V_j be the number of such α_i^j. We know that $V_j = \frac{\prod_{\mathfrak{q}|q_j}(N(\mathfrak{q})-1)}{\ell(q_j-1)}$. Using the inclusion-exclusion principle, we claim that

$$\left|\left\{\begin{array}{l|l} \alpha \in \mathfrak{b}\mathfrak{d} & \alpha \in \mathbb{Z} \bmod (1-\zeta_\ell)^2 \\ N(\alpha) \leq t^{\ell-1}N(\mathfrak{b}) & \alpha \text{ satisfies (2.1) } \bmod q_j, j = 1, \ldots, n \\ \phi(\alpha) \in \mathcal{F} & \end{array}\right\}\right| = \sum_{S \subseteq \{q_1, \ldots, q_n\}}$$

$$(-1)^{|S|}\prod_{q_j \in S} V_j \sum_{\alpha_i^j, q_j \notin S}\left|\left\{\begin{array}{l|l} \alpha \in \mathfrak{b}\mathfrak{d} & \alpha \in \mathbb{Z} \bmod (1-\zeta_\ell)^2 \\ N(\alpha) \leq t^{\ell-1}N(\mathfrak{b}) & \forall j \exists t_j \in \mathbb{Z} : \alpha \equiv t_j\alpha_i^j \bmod q_j \\ \phi(\alpha) \in \mathcal{F} & \alpha \equiv 0 \bmod q_j, \forall q_j \in S \end{array}\right\}\right|$$

Indeed, a point $(t_1\alpha_{i_1}^1, \ldots, t_n\alpha_{i_n}^n)$ is counted once on the left hand side, and once on the right hand side (in the summand corresponding to $S = \emptyset$). A point with zero entries in all coordinates corresponding to the set S is not counted on the left hand side, while on the right hand side it is counted

$$\sum_{S' \subseteq S}(-1)^{|S'|}\prod_{q_j \in S'} V_j \prod_{q_j \in S \setminus S'} V_j = \prod_{q_j \in S} V_j \sum_{S' \subseteq S}(-1)^{|S'|} = 0$$

times. Applying the key Lemma 2.26, and summing over $\mathfrak{b} \in B$, we get as a main term

$$h_\ell \sum_{S \subseteq \{q_1,\dots,q_n\}} (-1)^{|S|} \prod_{q_j \in S} V_j \prod_{q_j \notin S} V_j \frac{2\ell \operatorname{res}_{s=1}\zeta_K(s) t^{\ell-1} N(\mathfrak{b})}{h_\ell N(\mathfrak{b}) N(\mathfrak{d}) \ell \prod_{q_j \in S} q_j^{\ell-1} \prod_{q_j \notin S} q_j^{\ell-2}}$$
$$= \frac{\prod_{j=1}^n V_j}{\prod_{j=1}^n q_j^{\ell-1}} \prod_{j=1}^n (q_j - 1) \frac{2 \operatorname{res}_{s=1}\zeta_K(s)}{N(\mathfrak{d})} t^{\ell-1}$$
$$= \frac{1}{\ell^n} \prod_{\mathfrak{q}|Q} \left(1 - \frac{1}{N(\mathfrak{q})}\right) \frac{2 \operatorname{res}_{s=1}\zeta_K(s)}{N(\mathfrak{d})} t^{\ell-1}.$$

The error term is bounded by

$$h_\ell \sum_{S \subseteq \{q_1,\dots,q_n\}} \prod_{q_j \in S} V_j \prod_{q_j \notin S} V_j \max\big(1, \frac{t^{\ell-2}}{N(\mathfrak{d})^{\frac{\ell-2}{\ell-1}} \prod_{q_j \in S} q_j^{\ell-1}}\big)$$
$$\leq h_\ell \prod_{j=1}^n V_j \left(2^n + \prod_{j=1}^n \big(1 + \frac{1}{q_j^{\ell-1}}\big) \frac{t^{\ell-2}}{N(\mathfrak{d})^{\frac{\ell-2}{\ell-1}}} \right)$$
$$\leq h_\ell \frac{Q^{\ell-2}}{\ell^n} \left(2^n + 2 \frac{t^{\ell-2}}{N(\mathfrak{d})^{\frac{\ell-2}{\ell-1}}} \right)$$
$$\leq h_\ell Q^{\ell-2} \frac{2^n}{\ell^n} \frac{t^{\ell-2}}{N(\mathfrak{d})^{\frac{\ell-2}{\ell-1}}}$$

where we have used that $V_j \leq \frac{q_j^{\ell-2}}{\ell}$. The constants in ℓ may be bounded by ℓ^{ℓ^3} in the same way as in Theorem 2.28. □

Thus, the sieving setup is very similar. We define

$$\mathcal{P} = \{\mathfrak{p} \text{ prime ideals in } \mathbb{Z}[\zeta_\ell] \mid (\mathfrak{p}, Q) = 1\},$$

and again we have that

$$\omega(\mathfrak{p}) = \begin{cases} 1 & \text{if } \mathfrak{p} \in \mathcal{P} \\ 0 & \text{if } \mathfrak{p} \notin \mathcal{P}. \end{cases}$$

Set

$$X = \prod_{\mathfrak{q} \mid Q} \left(1 - \frac{1}{N(\mathfrak{q})}\right) \frac{2 \operatorname{res}_{s=1} \zeta_K}{\ell^n} t^{\ell-1},$$

then we have shown, for each squarefree integral ideal $\mathfrak{d}$ coprime with q, that

$$\mathcal{A}_{\mathfrak{d}} = \frac{1}{N(\mathfrak{d})} X + R_{\mathfrak{d}}, \quad \text{where } |R_{\mathfrak{d}}| \leq Q^{\ell-2} \ell^{\ell^3} \frac{2^n}{\ell^n} \max(1, \frac{t^{\ell-2}}{N(\mathfrak{d})^{\frac{\ell-2}{\ell-1}}}).$$

The following theorem analogous to Theorems 2.33 can be proven with literally the same proof, modified only by replacing q with Q.

Theorem 2.37. *With notation as above, for $z > \exp(\ell^{\ell^3})$ and $t^{\ell-1} \geq z^2$,*

$$S(\mathcal{A}(t^{\ell-1}), \mathcal{P}, z) \leq \frac{2}{\ell^n} \frac{t^{\ell-1}}{\log(z) - \ell^{\ell^3}} + \Sigma_2,$$

where

$$|\Sigma_2| \leq Q^{\ell-2} \frac{2^n}{\ell^n} \ell^{\ell^3} t^{\ell-2} z^{2/(\ell-1)} 10^6 \log^6(z/\ell).$$

In the final result, analogous to Theorem 2.34, one should be a little bit careful.

Theorem 2.38. *Let $Q = q_1, \ldots, q_n$. Let $\mathcal{S}_{q_1,\ldots,q_n}$ be the set of completely splitting primes in $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \ldots, \sqrt[\ell]{q_n})$. The following bound holds for all odd primes ℓ, for all primes $q_i \neq \ell$, and for all $x > Q^{\frac{5(\ell-2)(\ell-1)}{4}} \ell^{\ell^{\ell^3}} 2^{\frac{5(\ell-1)}{4}n}$.*

$$\pi(x, \mathcal{S}_{q_1,\ldots,q_n}) \leq \frac{3}{\ell^n(\ell-1)} \frac{x}{\log(x) - \log\left(Q^{\frac{5(\ell-2)(\ell-1)}{4}} \ell^{\ell^{\ell^3}} 2^{\frac{5(\ell-1)}{4}n}\right)}.$$

Proof. Using Corollary 2.18 and Theorem 2.37, we have that

$$\pi(t^{\ell-1}, \mathcal{S}_{q_1,\ldots,q_n}) \leq \frac{1}{\ell^n(\ell-1)} \frac{t^{\ell-1}}{\log(z) - \ell^{\ell^3}} + Q^{\ell-2} \frac{2^n}{\ell^n} \ell^{\ell^3} t^{\ell-2} z^{2/(\ell-1)} 10^6 \log^6(z/\ell).$$

We put

$$z = \frac{t^{\frac{2(\ell-1)}{5}}}{Q^{\frac{(\ell-2)(\ell-1)}{2}} \exp(\ell^{\ell^3}) 2^{f(\ell-1)2n}}.$$

The main term is then bounded by

$$\frac{5/2}{\ell(\ell-1)} \frac{t^{\ell-1}}{\log(t^{\ell-1}) - \log\left(Q^{\frac{5(\ell-2)(\ell-1)}{4}} \ell^{\ell^{\ell^3}} 2^{f5(\ell-1)4n}\right)}.$$

The error term is then bounded by

$$\frac{1}{2\ell^n} t^{\ell-6/5} \log^6(t) \leq \frac{1}{2\ell^n} \frac{t^{\ell-1}}{\log t},$$

since $\log^7(t) \leq t^{1/5}$, which holds because $t = x^{1/(\ell-1)} \geq \ell^{\ell^{\ell^2}}$ and $\ell \geq 3$. Thus we retrieve the statement of the theorem. $\square$

2.7 The cases $\ell = 3$ and $\ell = 5$

The general Theorem 2.38 is most useful if ℓ is treated as a fixed constant. If one has a small particular ℓ in mind and wishes an explicit Brun-Titchmarsh estimate for the number of completely splitting primes in $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \ldots, \sqrt[\ell]{q_n})$, then one may certainly improve the constant in ℓ by computing the fundamental units ε_i in order to bound the Lipschitz constant — and hence all subsequent constants — of the boundary of the fundamental domain $\mathcal{F}$.

For very small primes ℓ, a number of the technical hurdles which make the general case difficult, disappear. If $\ell \leq 19$, the class number h_ℓ is one, so there is no need for a summation over all ideal classes $\mathfrak{b} \in B$. With regards to the units; if the class number of the real subfield $h_\ell^+ = 1$, then the cyclotomic units generate the unit group. It is known by the recent work of Miller[31] that $h_\ell^+ = 1$ for $\ell \leq 151$. If one assumes the generalised Riemann hypothesis, then furthermore $h_\ell^+ = 1$ for $\ell \leq 241$, with the exceptions $h_{163}^+ = 4$, $h_{191}^+ = 11$, and $h_{229}^+ = 3$.

We will present the details for the examples $\ell = 3$ and $\ell = 5$. The case $\ell = 3$ is the most friendly since there are no units of infinite order and the class number is one. This means that in the Minkowski embedding (sending $\alpha \in \mathbb{Z}[\zeta_3]$ to $\alpha \in \mathbb{C}$), the fundamental domain $\mathcal{F}$ is the whole space $\mathbb{C}$.

The norm corresponds to the absolute value, and so the boundary $\partial\mathcal{F}(t^2)$ is the circle of radius t. It may be parametrised by arc length and as such it is of Lipschitz class $\mathcal{L}(2, 1, 2\pi t)$. We may improve the constant in our key Lemma 2.26 as follows.

Lemma 2.39. *Let* $\mathfrak{a}$ *be an integral ideal in* $\mathbb{Z}[\zeta_3]$. *Let* $\mathfrak{M} \subseteq \mathfrak{a}$ *be a subgroup of* $(\mathbb{Z}[\zeta_3], +)$. *Then*

$$\left|\left\{ \ \alpha \in \mathfrak{M} \ \middle| \ N(\alpha) \leq t^2 \ \right\}\right| = \frac{6 \operatorname{res}_{s=1}\zeta_K(s)}{[\mathbb{Z}[\zeta_3] : \mathfrak{M}]} t^2 + O\left(\max(1, \frac{t}{N(\mathfrak{a})^{\frac{1}{2}}}) \right), \tag{2.10}$$

where the constant in the O-term is bounded by 182.

Proof. According to Theorem 2.25, the error term in counting lattice points is bounded by

$$M 2^{n-1} (\sqrt{n}\Omega + 2)^n \max_{0 \leq i < n} \frac{L^i}{\lambda_1 \cdots \lambda_i}.$$

Using that $\Omega \leq \frac{n^{\frac{3}{2}n}}{(2\pi)^{\frac{n}{2}}} \leq \frac{4}{\pi}$, we see that the error is bounded by

$$2(\sqrt{2}\frac{4}{\pi} + 2)^2 \max(1, \frac{2\pi t}{N(\mathfrak{a})^{\frac{1}{2}}}) \leq 182 \max(1, \frac{t}{N(\mathfrak{a})^{\frac{1}{2}}}).$$

Since we don't have to do a dyadic decomposition, this bounds the error term.

$\square$

We now state the improved versions of Theorems 2.27, 2.29, and 2.36. In each case the constants arise after applying the improved key lemma a number of times.

Corollary 2.40. *For $K = \mathbb{Q}(\zeta_3)$, we have the following bounds. Let a_n be the number of integral ideals of norm n and let $\kappa = \mathrm{res}_{s=1}\zeta_K(s) = 0.6045$. For all $x \geq 1$,*

$$|\sum_{n \leq x} a_n - \kappa x| \leq 182 x^{\frac{1}{2}}.$$

For all $z \geq 1$,

$$G(z) \geq \prod_{\mathfrak{q}|Q} \big(1 - \frac{1}{N(\mathfrak{q})}\big)\kappa(\log(z) - 603).$$

Finally, for all $t \geq N(\mathfrak{d})^{\frac{1}{2}}$,

$$R_{\mathfrak{d}} \leq 182 Q \frac{2^n}{3^n} \frac{t}{N(\mathfrak{d})^{\frac{1}{2}}}.$$

Proof. The proof of the first statement uses the key lemma $h_\ell = 1$ times, thus has the same constant factor in the error. The proof of the second statement introduces an error $\frac{\ell-1}{\kappa} \leq \frac{603}{182}$ times the constant factor in the key lemma. The proof of the third statement has as a constant factor $Q^{\ell-3} h_\ell \frac{2^n}{\ell^n} = Q \frac{2^n}{3^n}$ times the constant factor in the key lemma. □

With these improved ingredients, the following theorem can be proven in literally the same way as Theorem 2.34.

Theorem 2.41. *With notation as above, for* $z > \exp(603)$ *and* $t^2 \geq z^2$,

$$S(\mathcal{A}(t^2), \mathcal{P}, z) \leq \frac{2}{3^n} \frac{t^2}{\log(z) - 603} + \Sigma_2,$$

where

$$|\Sigma_2| \leq Q \frac{2^n}{3^n} 182\, t z 10^6 \log^6(z),$$

We are now able to prove the main result.

Theorem 2.42. *Let* $Q = q_1, \ldots, q_n$. *Let* $\mathcal{S}_{q_1,\ldots,q_n}$ *be the set of completely splitting primes in* $\mathbb{Q}(\zeta_3, \sqrt[3]{q_1}, \ldots, \sqrt[3]{q_n})$. *The following bound holds for all primes* $q_j \neq 3$, *and for all* $x > (Q 2^n e^{603})^{2.23}$.

$$\pi(x, \mathcal{S}_{q_1,\ldots,q_n}) \leq \frac{2.29}{2 \cdot 3^n} \frac{x}{\log(x) - 2.23 \log\left(Q 2^n e^{603}\right)}.$$

Proof. Put $t = x^{1/2}$. Using Corollary 2.18 and Theorem 2.45, we have that

$$\pi(t^2, \mathcal{S}_{q_1,\ldots,q_n}) \leq \frac{1}{2 \cdot 3^n} \frac{t^2}{\log(z) - 603} + \frac{1}{4} Q \frac{2^n}{3^n} 182\, t z 10^6 \log^6(z)$$

We put

$$z = \frac{t^{1-\varepsilon}}{Q\, 2^n}.$$

The main term is then bounded by

$$\frac{1}{2\cdot 3^n}\frac{\frac{2}{1-\varepsilon}t^2}{\log(t^2)-\frac{2}{1-\varepsilon}\log\left(Q2^ne^{603}\right)}.$$

The error term is then bounded by

$$\frac{1}{3^n}\frac{182}{4}\cdot 10^6t^2\frac{\log^6(t)}{t^\varepsilon}.$$

We choose $\varepsilon=\frac{1}{10}$ and since $t\geq e^{603\cdot 1.115}$, we have that

$$\frac{t^\varepsilon}{\log^7(t)}\geq\frac{e^{67}}{(603\cdot 1.11)^7}\geq\frac{e^{67}}{e^{46}}.$$

Since $\frac{182}{4}\cdot 10^6\leq e^{18}$, is is now clear that the error term contributes at most one e^2-th of the main term, and the result follows since $\frac{2}{1-1/10}+\frac{1}{e^2}\leq 2.29$. $\square$

In the case $\ell = 5$, the non-torsion part of the unit group is generated by one element $\varepsilon = \frac{1+\sqrt{5}}{2}$. Hence, $m(\varepsilon) = |\frac{1+\sqrt{5}}{2}| = 1.6180$, and thus the boundary $\partial\mathcal{F}_{\frac{1}{2}}(t^4)$ is of Lipschitz class

$$\mathcal{L}(4,2^{2r_1+r_2},\sqrt{n}\pi(r+\frac{2^{n-1}n}{n})m(\varepsilon)^{\frac{r}{2}}\log(m(\varepsilon))t)\subseteq\mathcal{L}(4,4,5.47t)$$

.

Lemma 2.43. *Let* $\mathfrak{a}$ *be an integral ideal in* $\mathbb{Z}[\zeta_5]$. *Let* $\mathfrak{M} \subseteq \mathfrak{a}$ *be a subgroup of* $(\mathbb{Z}[\zeta_5], +)$. *Then*

$$\left|\left\{ \alpha \in \mathfrak{M} \;\middle|\; \phi(\alpha) \in \mathcal{F}(t^4) \right\}\right| = \frac{10 \operatorname{res}_{s=1}\zeta_K(s)}{[\mathbb{Z}[\zeta_5] : \mathfrak{M}]} t^4 + O\left(\max(1, \frac{t^3}{N(\mathfrak{a})^{\frac{3}{4}}}) \right), \tag{2.11}$$

where the constant in the O-term is bounded by e^{32}.

Proof. According to Theorem 2.25, the error term in counting lattice points is bounded by

$$M2^{n-1}(\sqrt{n}\Omega + 2)^n \max_{0 \leq i < n} \frac{L^i}{\lambda_1 \cdots \lambda_i}.$$

Using that $\Omega \leq \frac{n^{\frac{3}{2}n}}{(2\pi)^{\frac{n}{2}}} \leq (\frac{32}{\pi})^2$, we see that the error is bounded by

$$32(2(\frac{32}{\pi})^2 + 2)^4 (5.47)^3 \max(1, \frac{t^3}{N(\mathfrak{a})^{\frac{3}{4}}}) \leq e^{30} \max(1, \frac{t^3}{N(\mathfrak{a})^{\frac{3}{4}}}).$$

The error introduced by performing a dyadic decomposition is $\sum_{k=0}^{\infty} \frac{1}{\sqrt{2^k}} = 6.28$, so finally the constant is bounded above by e^{32}. □

Analogously to the case $\ell = 3$, we state the improved versions of Theorems 2.27, 2.29, and 2.36.

Corollary 2.44. *For* $K = \mathbb{Q}(\zeta_5)$, *we have the following bounds. Let* a_n *be the number of integral ideals of norm* n *and let* $\kappa = \operatorname{res}_{s=1}\zeta_K(s) = 0.3398$. *For all* $x \geq 1$,

$$|\sum_{n \leq x} a_n - \kappa x| \leq e^{32} x^{\frac{1}{2}}.$$

For all $z \geq 1$,

$$G(z) \geq \prod_{\mathfrak{q}|Q} \big(1 - \frac{1}{N(\mathfrak{q})}\big)\kappa(\log(z) - e^{35}).$$

Finally, for all $t \geq N(\mathfrak{d})^{\frac{1}{4}}$,

$$R_{\mathfrak{d}} \leq e^{32} Q^3 \frac{2^n}{5^n} \frac{t^3}{N(\mathfrak{d})^{\frac{3}{4}}}.$$

Proof. The proof of the first statement uses the key lemma $h_\ell = 1$ times, thus has the same constant factor in the error. The proof of the second statement introduces an error $\frac{\ell-1}{\kappa} \leq e^3$ times the constant factor in the key lemma. The proof of the third statement has as a constant factor $Q^{\ell-2} h_\ell \frac{2^n}{\ell^n} = Q^3 \frac{2^n}{5^n}$ times the constant factor in the key lemma. $\square$

With these improved ingredients, the following theorem can be proven in literally the same way as Theorem 2.34.

Theorem 2.45. *With notation as above, for $z > \exp(e^{35})$ and $t^4 \geq z^2$,*

$$S(\mathcal{A}(t^4), \mathcal{P}, z) \leq \frac{2}{5^n} \frac{t^4}{\log(z) - e^{35}} + \Sigma_2,$$

where

$$|\Sigma_2| \leq Q^3 \frac{2^n}{5^n} e^{35} t^3 z^{\frac{1}{2}} 10^6 \log^6(z).$$

We are now able to prove the main result.

Theorem 2.46. *Let $Q = q_1, \ldots, q_n$. Let $\mathcal{S}_{q_1,\ldots,q_n}$ be the set of completely splitting primes in $\mathbb{Q}(\zeta_5, \sqrt[5]{q_1}, \ldots, \sqrt[5]{q_n})$. Let $\gamma = 2 + \frac{1}{e^{19}}$. The following bound holds for all primes $q_j \neq 5$, and for all $x > \left(Q^6 2^{4n} e^{e^{35}}\right)^{\gamma}$.*

$$\pi(x, \mathcal{S}_{q_1,\ldots,q_n}) \leq \frac{\gamma}{4 \cdot 5^n} \frac{x}{\log(x) - \gamma \log\left(Q^6 2^{4n} e^{e^{35}}\right)}.$$

Proof. Put $t = x^{1/4}$. Using Corollary 2.18 and Theorem 2.45, we have that

$$\pi(t^4, \mathcal{S}_{q_1,\ldots,q_n}) \leq \frac{1}{4 \cdot 5^n} \frac{t^4}{\log(z) - e^{35}} + Q^3 \frac{2^n}{5^n} e^{32} t^3 z^{\frac{1}{2}} 10^6 \log^6(z).$$

We put

$$z = \frac{t^{2(1-\varepsilon)}}{Q^6 2^{4n}}.$$

The main term is then bounded by

$$\frac{1}{4 \cdot 5^n} \frac{\frac{2}{1-\varepsilon} t^4}{\log(t^4) - \frac{2}{1-\varepsilon} \log\left(Q^6 2^{4n} e^{e^{35}}\right)}.$$

The error term is then bounded by

$$\frac{1}{5^n} e^{32} 10^6 t^4 2^6 \frac{\log^6(t)}{t^{\varepsilon}}$$

We choose $\varepsilon = e^{-20}$ and since $t \geq e^{e^{36}/4}$, we have that

$$\frac{t^{\varepsilon}}{\log^7(t)} \geq \frac{e^{e^{15}/4}}{e^{7 \cdot 35}} \geq e^{2 \cdot 10^6}.$$

Since $e^{32}10^6 2^6 \leq e^{50}$, is is now clear that the error term contributes at most one e^{10^6}-th of the main term, and the result follows since $\frac{2}{1-e^{-20}} + \frac{1}{e^{10^6}} \leq 2 + \frac{1}{e^{19}}$. $\square$

2.8 Conclusion

We conclude the chapter by reviewing and commenting on the main points of the chapter.

We have formulated a reciprocity law, which is contained in Eisenstein's reciprocity law, giving a useful criterion of whether a prime splits completely in $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \ldots, \sqrt[\ell]{q_n})$, in terms of its — possibly ideal — factors in $\mathbb{Q}(\zeta_\ell)$.

We have used this criterion to be able to interpret the question of bounding the number of completely splitting primes in a sieve-theoretic way. We have striven to set the sieving process in its natural environment and with this intention we have sketched the extension of Selberg's sieve to $\mathbb{Z}[\zeta_\ell]$, sieving by its prime *ideals*.

We have introduced the needed machinery to count integral elements up to multiplication by units. This culminated in the proof of the general Lemma 2.26 which provides estimates for the number of elements — up to multiplication by units — in subgroups of the additive group of the ring of integers of a general number field K, which is fully explicit. As an application we gave an explicit version of Landau's proof for the analytic continuation of $\zeta_K(s)$ to $\mathrm{Re}(s) \geq 1 - \frac{1}{n}$. Equivalently, we have performed an effective count of the number of ideals of norm up to x. This was also of vital importance to make the sieving process explicit.

We have applied this key lemma to our sieving setup, which resulted in bounds for the completely splitting primes in $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \ldots, \sqrt[\ell]{q_n})$ which are fully explicit in all parameters $\ell, n, q_1, \ldots, q_n$. Our bounds can be said to be of Brun-Titchmarsh quality in that for any $\varepsilon > 0$, our method shows that the prime counting function is bounded by

$$\pi(x, \mathcal{S}_{q_1,\ldots,q_n}) \leq \frac{2+\varepsilon}{(\ell-1)\ell^n} \frac{x}{\log x} \qquad \text{for } x \gg_{\varepsilon,\ell,n,q_i} 1,$$

where the implied constants are effective.

We note that the family of fields is quite general. The degree tends to infinity as ℓ or n tends to infinity, and the discriminant tends to infinity as any parameter tends to infinity. It should be acknowledged that with respect to the parameter ℓ, the implied constants are of mindblowingly huge magnitude, and for any reasonable application it seems that ℓ would best be kept fixed and interpreted as a mere constant.

3

Kummer Fields

3.1 Introduction

To what extent do the methods used in the first chapter to bound the relative class number of $\mathbb{Q}(\zeta_p)$ carry over to more general situations? At the very heart of the argument, we have a method bounding a product of L-values at $s = 1$ when given the appropriate arithmetic and analytic input. Then, applying the analytical class number formula, we relate this to certain arithmetical invariants, such as the relative class number.

The accessibility of the relative class number is due to the well-understood relation between the unit group of $\mathbb{Q}(\zeta_\ell)$ and its quadratic subfield $\mathbb{Q}(\zeta_\ell + \zeta_\ell^{-1})$, which entails that we can relate the regulator of those two quantities. This is a common feature of CM-fields, that is, totally complex fields K which are a quadratic extension of a totally real field K^+, in which case the unit group of K^+ is a subgroup of finite index in the unit group of K.

If one is not in the CM-case, and one cannot eliminate the regulator, the method does not yield estimates of class numbers, but may still be used to bound the residue of the Dedekind zeta function at $s = 1$. These bounds can also be seen as an effective error term in the analytic density of the set of completely splitting primes. The analytic density measures subsets $\mathcal{S}$ of primes in the following way.

$$\delta(\mathcal{S}) = \lim_{s\to 1} \frac{\sum_{p\in\mathcal{S}} p^{-s}}{\sum_p p^{-s}} = \lim_{s\to 1} \frac{\sum_{p\in\mathcal{S}} p^{-s}}{\log\left(\frac{1}{s-1}\right)}.$$

Throughout this chapter, we will be concerned with the properties of the family of fields $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \ldots, \sqrt[\ell]{q_n})$, where ℓ is an odd prime, and all q_i are primes different from ℓ. In comparison with cyclotomic fields, two important features are absent. On the analytic side, the loss of the abelian property means that the relevant product of L-functions now contains Artin L-

functions as opposed to the much better understood Dirichlet L-functions. On the arithmetic side, more importantly, there is no estimate for the completely splitting primes which is of the quality of the classical Brun-Titchmarsh inequality, and we have to make do with our result from Chapter two.

We start by proving some preparatory observations on the specifics of the fields $K = \mathbb{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \dots, \sqrt[\ell]{q_n})$. We gather some useful facts concerning the Galois group $Gal(K)$, its representations and the splitting behaviour of primes in K in the following theorem.

Theorem 3.1. *Let $K = \mathbb{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \dots, \sqrt[\ell]{q_n})$. $Gal(K)$ is isomorphic to $\mathbb{F}_\ell^* \rtimes (\mathbb{F}_\ell^n, +)$. This group has exactly $\ell - 1$ different one-dimensional and exactly $\frac{\ell^n-1}{\ell-1}$ different $(\ell-1)$-dimensional irreducible representations. Let $p \neq q_i, \ell$ be a prime of order d in $(\mathbb{Z}/\ell\mathbb{Z})^*$. Then*

1. *If $d \neq 1$, (p) splits into $\ell^n \frac{(\ell-1)}{d}$ different prime ideals.*
2. *If $d = 1$ and $q_i \in \mathbb{F}_p^\ell$, for all q_i, then (p) splits completely.*
3. *If $d = 1$ and $q_i \notin \mathbb{F}_p^\ell$, for an q_i, then (p) splits into $\ell^{n-1}(\ell-1)$ different prime ideals.*

Proof. We first consider the case $n = 1$. A Galois element is determined by its action on ζ_ℓ and $\sqrt[\ell]{q}$. Denoting the element sending $\zeta_\ell \mapsto \zeta_\ell^x$ and $\sqrt[\ell]{q} \mapsto \zeta_\ell^y \sqrt[\ell]{q}$ by the matrix $\left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right)$, where $x \in \mathbb{F}_\ell^*$ and $y \in \mathbb{F}_\ell$, we have given an isomorphism from $Gal(K)$ to $AGL(1, \ell) \cong \mathbb{F}_\ell^* \rtimes (\mathbb{F}_\ell, +)$. This group has ℓ

different conjugacy classes: one for each value of x, except for $x = 1$, when we have the unit element and all other elementsin one class. Since, by considering the quotient map to $\mathbb{F}_\ell^*$, we have $\ell - 1$ linear irreducible representations, there can only be one more irreducible representation. Since $\ell(\ell-1)$ is the sum of the squares of the dimensions, this remaining irreducible representation has dimension $\ell - 1$.

For general n, we note that we may consider the Galois groups of normal subfields as quotients of $Gal(K)$. Considering the subfield $\mathbb{Q}(\zeta_\ell)$, we find $\ell - 1$ linear irreducible representations. Considering for each $(a_1 : a_2 : \cdots : a_n) \in \mathbb{P}_{n-1}(\ell)$, the subfield $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{\prod_i q_i^{a_i}})$, which is of type $n = 1$, we find one $(\ell-1)$-dimensional irreducible representation. Since

$$\ell - 1 + \frac{\ell^n - 1}{\ell - 1}(\ell - 1)^2 = (\ell - 1)\ell^n = |Gal(K)|,$$

we have given all irreducible representations.

To address the splitting behaviour, we again consider the Galois group. As in the the case $n = 1$, we describe a Galois element σ by the tuple $(x, y_1, \ldots, y_n)$, where $x \in \mathbb{F}_\ell^*$ and $y_i \in \mathbb{F}_\ell$, such that

$$\sigma : \begin{cases} \zeta_\ell \mapsto \zeta_\ell^x \\ \sqrt[\ell]{q_i} \mapsto \zeta_\ell^{y_i} \sqrt[\ell]{q_i}, \quad i = 1, \ldots, n. \end{cases}$$

Since the degree of the field is $\ell^n(\ell - 1)$, all possible tuples correspond to a Galois element. It is a straightforward calculation that multiplication of Galois elements corresponds to multiplication of the upper triangular matrices

$$\begin{pmatrix} x & & & \cdots & y_1 \\ & x & & \cdots & y_2 \\ & & \ddots & & \vdots \\ & & & x & y_n \\ & & & & 1 \end{pmatrix}.$$

We note that the k-th power of this matrix equals

$$\begin{pmatrix} x^k & & & \cdots & \frac{x^k-1}{x-1}y_1 \\ & x^k & & \cdots & \frac{x^k-1}{x-1}y_2 \\ & & \ddots & & \vdots \\ & & & x^k & \frac{x^k-1}{x-1}y_n \\ & & & & 1 \end{pmatrix}.$$

Now, recall that if σ_p is a Frobenius element for p, then p splits in $\frac{|Gal(K)|}{\mathrm{order}(\sigma_p)}$ factors. By the above calculation, the order of a matrix equals the order of x, unless when $x = 1$ and the matrix is not the unit matrix, in which case the order is ℓ. When we project Frobenius elements onto $\mathbb{F}_\ell^*$ by taking the coordinate x, this corresponds to taking the quotient to $Gal(\mathbb{Q}(\zeta_\ell))$, where the Frobenius element of a prime p equals $p \bmod \ell$. Thus, the Frobenius (in K) of p is a tuple with first coordinate $p \bmod \ell$, of which we have computed the order above. Thus, if $p \not\equiv 1 \bmod \ell$, then p splits in $\ell^n \frac{\ell-1}{d}$ factors. If $p \equiv 1 \bmod \ell$ but p does not split completely, then its Frobenius is a tuple $(x, y_1, \dots, y_n)$ with $x = 1$ and not all $y_i = 0$, and thus has order ℓ from which it follows that the number of factors is $\ell^{n-1}(\ell - 1)$. $\square$

We will need an upper bound for the discriminant of these fields. The difficulty in computing the exact value of the discriminant lies in the nontrivial question of determining the ring of integers. We prove the following bounds by explicitly constructing integral elements.

Theorem 3.2. *Let Δ_K be the discriminant of $K = \mathbb{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \dots, \sqrt[\ell]{q_n})$, where $\ell \neq q_i$, and set $Q = q_1 \cdots q_n$. Then*

$$\ell^{\ell^n(\ell-2)} Q^{\ell^{n-1}(\ell-1)^2} \mid \Delta_K \quad \text{and} \quad \Delta_K \mid \ell^{\ell^{n+1}} Q^{\ell^{n-1}(\ell-1)^2}$$

Proof. Recall the product formula for discriminants (see e.g. [36, p. 213]) in a tower of fields $K/L/\mathbb{Q}$

$$\Delta_K = \Delta_{L/\mathbb{Q}}^{[K:L]} N_{L/\mathbb{Q}}(\Delta_{K/L}).$$

We first take $L = \mathbb{Q}(\zeta_\ell)$. Since $\Delta_{L/\mathbb{Q}} = \ell^{\ell-2}$, we immediately find that $\ell^{\ell^n(\ell-2)}|\Delta_K$. In order to show that a certain power of q_i divides Δ_K we first take a closer look at the ring of integers of $L = \mathbb{Q}(\sqrt[\ell]{q_i})$.

Let v be the valuation corresponding to the element $\sqrt[\ell]{q_i}$. Let $\alpha \in \mathcal{O}_L$, so that

$$\alpha = a_0 + a_1\sqrt[\ell]{q_i} + \cdots + a_{\ell-1}\sqrt[\ell]{q_i}^{(\ell-1)},$$

with $a_j \in \mathbb{Q}$. Since $v(a_j) \equiv 0 \mod \ell$, the numbers $v(a_j\sqrt[\ell]{q_i}^j)$, for $a_j \neq 0$ are distinct $\mod \ell$. By standard facts on non-archimedean valuations, this implies that $v(\alpha) = \min_j(v(a_j\sqrt[\ell]{q_i}^j))$. Since $v(\alpha) \geq 0$, and $v(\sqrt[\ell]{q_i}^j) < \ell$, we must have $v(a_j) \geq 0$. Therefore q_i is not in the denominator of any a_i. Since $\mathrm{Tr}(\alpha) = \ell a_0 \in \mathbb{Z}$, we find that a_0 can only have ℓ in the denominator. Likewise, $\mathrm{Tr}(\sqrt[\ell]{q_i}^j\alpha) = \ell q_i a_{\ell-j} \in \mathbb{Z}$, and since q_i is not in the denominator, the a_i can only have ℓ in the denominator. In other words, $\mathcal{O}_L$ is contained in the submodule generated by the elements $\frac{\sqrt[\ell]{q_i}}{\ell}, \ldots, \frac{\sqrt[\ell]{q_i}^{(\ell-1)}}{\ell}$. This implies that Δ_L is divided by the square of the determinant of the matrix

$$\begin{pmatrix} 1/\ell & \sqrt[\ell]{q_i}/\ell & \sqrt[\ell]{q_i}^2/\ell & \cdots & \sqrt[\ell]{q_i}^{\ell-1}/\ell \\ 1/\ell & \zeta_\ell\sqrt[\ell]{q_i}/\ell & \zeta_\ell^2\sqrt[\ell]{q_i}^2/\ell & \cdots & \zeta_\ell^{\ell-1}\sqrt[\ell]{q_i}^{\ell-1}/\ell \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1/\ell & \zeta_\ell^{\ell-1}\sqrt[\ell]{q_i}/\ell & \zeta_\ell^{\ell-2}\sqrt[\ell]{q_i}^2/\ell & \cdots & \zeta_\ell\sqrt[\ell]{q_i}^{\ell-1}/\ell \end{pmatrix}.$$

Upon extracting $\sqrt[\ell]{q_i}^{\ell(\ell-1)/2}$, the determinant we have left is a Vandermonde determinant, with all differences $\zeta_\ell^j/\ell - \zeta_\ell^k/\ell$ only divisible by $1-\zeta_\ell$. Thus, $q_i^{\ell-1}$ divides Δ_L, and by the product formula, $q_i^{\ell^{n-1}(\ell-1)^2}|\Delta_K$.

We now turn our attention to upper bounds.

Denote $K_0 = \mathbb{Q}(\zeta_\ell)$ and $K_i = \mathbb{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \dots, \sqrt[\ell]{q_i})$, so that $K_n = K$. Using the product formula n times, we get

$$\begin{aligned}
\Delta_K &= \Delta_{K_0/\mathbb{Q}}^{\ell^n} N_{K_0/\mathbb{Q}}(\Delta_{K_n/K_0}) \\
&= \Delta_{K_0/\mathbb{Q}}^{\ell^n} N_{K_0/\mathbb{Q}}(\Delta_{K_1/K_0}^{\ell^{n-1}} N_{K_1/K_0}(\Delta_{K_n/K_1})) \\
&= \dots \\
&= \Delta_{K_0/\mathbb{Q}}^{\ell^n} N_{K_0/\mathbb{Q}}(\Delta_{K_1/K_0})^{\ell^{n-1}} N_{K_1/\mathbb{Q}}(\Delta_{K_2/K_1})^{\ell^{n-2}} \dots N_{K_{n-1}/\mathbb{Q}}(\Delta_{K_n/K_{n-1}}).
\end{aligned}$$

Recall the definition of the relative discriminant $\Delta_{K_i/K_{i-1}}$ as the ideal generated by all discriminants of all integral bases of K_i/K_{i-1}. Thus, replacing all $\Delta_{K_i/K_{i-1}}$ by the discriminant of a certain set of linear independent integral elements, we get that Δ_K divides the product on the right hand side. We will give two different bases.

Firstly, consider $(1, \sqrt[\ell]{q_i}, \sqrt[\ell]{q_i}^2, \ldots, \sqrt[\ell]{q_i}^{\ell-1})$ as a basis for K_i/K_{i-1}. Its discriminant equals the square of the determinant of the matrix

$$\begin{pmatrix} 1 & \sqrt[\ell]{q_i} & \sqrt[\ell]{q_i}^2 & \cdots & \sqrt[\ell]{q_i}^{\ell-1} \\ 1 & \zeta_\ell \sqrt[\ell]{q_i} & \zeta_\ell^2 \sqrt[\ell]{q_i}^2 & \cdots & \zeta_\ell^{\ell-1} \sqrt[\ell]{q_i}^{\ell-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_\ell^{\ell-1} \sqrt[\ell]{q_i} & \zeta_\ell^{\ell-2} \sqrt[\ell]{q_i}^2 & \cdots & \zeta_\ell \sqrt[\ell]{q_i}^{\ell-1} \end{pmatrix}.$$

Upon extracting $\sqrt[\ell]{q_i}^{\ell(\ell-1)/2}$, the determinant we have left is again a Vandermonde determinant, with all differences $\zeta_\ell^j - \zeta_\ell^k$ only divisible by $1-\zeta_\ell$. Thus, $N_{K_{i-1}/\mathbb{Q}}(\Delta_{K_i/K_{i-1}})^{\ell^{n-i}}$ divides some power of ℓ times $N_{K_{i-1}/\mathbb{Q}}(q_i^{\ell-1})^{\ell^{n-i}} = q_i^{(\ell-1)^2\ell^{n-1}}$. Consequently we have that Δ_K divides some power of ℓ times $Q^{(\ell-1)^2\ell^{n-1}}$.

The last step is to bound the power of ℓ. We will do this by considering another linear independent set of integral elements. First, let us consider for any $\tilde{q}$ with $(\tilde{q}, \ell) = 1$ the field $L = \mathbb{Q}(\zeta_\ell, \sqrt[\ell]{\tilde{q}})$. Assume that ℓ ramifies completely in this field extension, and let $(\ell) = (\lambda)^{(\ell-1)} = \mu^{\ell(\ell-1)}$, where $\lambda = 1-\zeta_\ell$, and μ is some integral ideal in L. Let m be the greatest integer such that ℓ^m divides $\tilde{q}^{(\ell-1)} - 1$. Then

$$\ell^m \mid \tilde{q}^{(\ell-1)} - 1 = \prod_{j=0}^{\ell-1} (\sqrt[\ell]{\tilde{q}}^{(\ell-1)} \zeta_\ell^j - 1).$$

Since all factors on the right are conjugates, and μ is fixed under all Galois conjugates, all factors on the right are divisible by the same power of μ. Hence, for all j,

$$\mu^{m(\ell-1)^2} \mid \frac{\tilde{q}^{(\ell-1)} - 1}{\sqrt[\ell]{\tilde{q}}^{(\ell-1)}\zeta_\ell^j - 1} = \sum_{k=0}^{\ell-1} \sqrt[\ell]{\tilde{q}}^{k(\ell-1)}\zeta_\ell^{jk}.$$

Since $\lambda^{(\ell-2)m} \mid \mu^{m(\ell-1)^2}$, the following are integral elements:

$$\alpha_j = \frac{1}{\lambda^{(\ell-2)m}} \sum_{k=0}^{\ell-1} \tilde{q}^{\ell-k-1}\zeta_\ell^{-jk}\sqrt[\ell]{\tilde{q}}^k. \tag{3.1}$$

We will use these elements as a basis for $L/\mathbb{Q}(\zeta_\ell)$ and compute the discriminant of this basis to bound the norm of the relative discriminant from L tot $\mathbb{Q}(\zeta_\ell)$. The linear independence of the α_j will follow form the non-singularity of a certain matrix. Consider

$$\begin{aligned} d(\alpha_1, \ldots, \alpha_\ell) &= \left(\frac{1}{\lambda^{(\ell-2)m}}\right)^{2\ell} d(\lambda^{(\ell-2)m}\alpha_1, \ldots, \lambda^{(\ell-2)m}\alpha_\ell) \\ &= \left(\frac{1}{\lambda^{(\ell-2)m}}\right)^{2\ell} [\mathfrak{a} : \mathfrak{a}']^2 d(1, \sqrt[\ell]{\tilde{q}}, \ldots, \sqrt[\ell]{\tilde{q}}^{\ell-1}) \end{aligned}$$

where $\mathfrak{a}$ is the submodule generated by $1, \sqrt[\ell]{\tilde{q}}, \ldots, \sqrt[\ell]{\tilde{q}}^{\ell-1}$ and $\mathfrak{a}'$ is the submodule generated by the $\lambda^{(\ell-2)m}\alpha_1, \ldots, \lambda^{(\ell-2)m}\alpha_\ell$. By the representation (3.1), we may compute this index as the determinant of the matrix of the base change

$$[\mathfrak{a} : \mathfrak{a}']^2 = \left| \begin{pmatrix} \tilde{q}^{\ell-1} & \tilde{q}^{\ell-2} & \tilde{q}^{\ell-3} & \cdots & 1 \\ \tilde{q}^{\ell-1} & \tilde{q}^{\ell-2}\zeta_\ell^{-1} & \tilde{q}^{\ell-3}\zeta_\ell^{-2} & \cdots & \zeta_\ell \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \tilde{q}^{\ell-1} & \tilde{q}^{\ell-2}\zeta_\ell^{-(\ell-1)} & \tilde{q}^{\ell-3}\zeta_\ell^{-(\ell-2)} & \cdots & \zeta_\ell^{-1} \end{pmatrix} \right|^2$$

$$= \tilde{q}^{\ell(\ell-1)} \left| \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta_\ell^{-1} & \zeta_\ell^{-2} & \cdots & \zeta_\ell \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_\ell^{-(\ell-1)} & \zeta_\ell^{-(\ell-2)} & \cdots & \zeta_\ell^{-1} \end{pmatrix} \right|^2 .$$

This determinant is a Vandermonde determinant, and since each difference $\zeta_\ell^i - \zeta_\ell^j$ has exactly one factor of λ, the total power of λ dividing this determinant squared is $\lambda^{2\binom{\ell}{2}} = \lambda^{\ell(\ell-1)}$. Since this matrix is non-singular, the α_j are linear independent. The determinant squared in the computation of $d(1, \sqrt[\ell]{\tilde{q}}, \ldots, \sqrt[\ell]{\tilde{q}}^{(\ell-1)})$, as we have seen in the first part of the proof, equals some power of $\tilde{q}$ times the same Vandermonde determinant, with ζ_ℓ in place of ζ_ℓ^{-1}. So likewise, the total power of λ dividing $d(1, \sqrt[\ell]{\tilde{q}}, \ldots, \sqrt[\ell]{\tilde{q}}^{(\ell-1)})$ is $\lambda^{\ell(\ell-1)}$. Thus the total power of λ dividing $d(\alpha_1, \ldots, \alpha_\ell)$ is, if $m = 1$, $\frac{\lambda^{2\ell(\ell-1)}}{\lambda^{2(\ell-2)\ell}} = \lambda^{2\ell}$. If $m \geq 2$, it is a negative power of λ, which is a contradiction and it follows that in this case λ does not ramify in L, or in other words, ℓ does not ramify completely in $L/\mathbb{Q}$. We finish the computation of Δ_L for

$L = \mathbb{Q}(\zeta_\ell, \sqrt[\ell]{\tilde{q}})$ in the case $m = 1$ by the formula

$$\Delta_L = \Delta_{\mathbb{Q}(\zeta_\ell)}^{\ell} N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(\Delta_{L/\mathbb{Q}(\zeta_\ell)}) \mid \ell^{\ell(\ell-2)} N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(d(\alpha_1, \dots, \alpha_\ell)),$$

which shows that the power of ℓ dividing Δ_L is at most ℓ^2.

We now finish the upper bound for Δ_K. Recall that $Gal(K/\mathbb{Q}(\zeta_\ell)) \cong \mathbb{F}_\ell^n$, and consider the inertia group $I \leqslant \mathbb{F}_\ell^n$ of the element $\lambda \in \mathbb{Q}(\zeta_\ell)$, and consider the orthogonal complement H in $\mathbb{F}_\ell^n$. Then λ ramifies completely up to the fixed field of H, but not further. Note that for all $(x_i) \in I$, $\prod_{i=1}^n \sqrt[\ell]{q_i}^{x_i}$ is fixed under H.

Now, choose a generator g for the multiplicative group $(\mathbb{Z}/\ell^2\mathbb{Z})^*$, and let a_i be the integers such that $q_i \equiv g^{a_i} \bmod \ell^2$. We define the hyperplane

$$V = \{(x_i) \in \mathbb{F}_\ell^n \mid \sum_i x_i a_i \equiv 0 \bmod \ell\}.$$

If $(x_i) \in V$, then, defining $\tilde{q} := \prod_i q_i^{x_i}$, we have that $\tilde{q}^{\ell-1} \equiv \prod_i g^{(\ell-1)a_i x_i} \equiv 1 \bmod \ell^2$, or in other words $m \geq 2$ so as we have seen before, λ does not ramify in the field $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{\tilde{q}})$. Hence, I intersects trivially with V, whence it follows that I is at most 1-dimensional. Thus, H is a maximal subspace (or the full space), and its fixed field is of the form $L = \mathbb{Q}(\zeta_\ell, \sqrt[\ell]{\tilde{q}})$ for a certain $\tilde{q}$ (or $\mathbb{Q}(\zeta_\ell)$). Using once more the formula

$$\Delta_K = \Delta_L^{[K:L]} N_{L/\mathbb{Q}}(\Delta_{K/L}),$$

where the second factor is coprime to ℓ, we see that the power of ℓ dividing Δ_K is bounded by ℓ^{n+1}. $\square$

3.2 Arithmetic input

Using our generalised Brun-Titchmarsh estimate for the number of completely splitting primes in K, Theorem 2.38, we may bound the Dedekind zeta function to the right of 1. Let us define

$$f(s) = \log(\zeta_K(s)(s-1)).$$

Using the Euler product representation, valid for $\mathrm{Re}(s) \geq 1$,

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1},$$

we infer that $f(s)$ can be written as a sum over prime powers. Let us write $\mathcal{S}^d$ for the set of primes which have order $d \bmod \ell$. We denote the set of completely splitting primes by $\mathcal{S}_Q$. Then we may write

$$f(s) = \log(s-1) + \Sigma_1 + \Sigma_2 + \Sigma_3 + \Sigma_4 + \Sigma_5,$$

where

$$\Sigma_1 = \ell^n(\ell-1)\sum_{p\in\mathcal{S}_Q}\sum_{m=1}^{\infty}\frac{1}{mp^{ms}} \qquad \Sigma_2 = \ell^{n-1}(\ell-1)\sum_{p\in\mathcal{S}^1\setminus\mathcal{S}_Q}\sum_{m=1}^{\infty}\frac{1}{mp^{\ell ms}}$$

$$\Sigma_3 = \sum_{\substack{d|\ell-1\\ d\neq 1}}\ell^n\frac{\ell-1}{d}\sum_{\substack{p\in\mathcal{S}^d\\ p\geq 2\ell}}\sum_{m=1}^{\infty}\frac{1}{mp^{dms}} \qquad \Sigma_4 = \sum_{\substack{d|\ell-1\\ d\neq 1}}\ell^n\frac{\ell-1}{d}\sum_{\substack{p\in\mathcal{S}^d\\ p\leq 2\ell}}\sum_{m=1}^{\infty}\frac{1}{mp^{dms}}$$

$$\Sigma_5 = \sum_{\mathfrak{p}|\ell Q}\sum_{m=1}^{\infty}\frac{1}{N(\mathfrak{p})^{ms}},$$

where we have used Theorem 3.1 for the splitting criteria in K.

Theorem 3.3. *For all $\sigma > 1$, we have*

$$|f(\sigma)| \ll \log\left(\frac{1}{\sigma-1}\right) + \ell^{n+3}\log\ell + \ell^n\log_2 Q,$$

where the implied constant is absolute and effective.

Proof. Let $T = Q^{\frac{5(\ell-2)(\ell-1)}{4}}\ell^{\ell^{\ell^3}}2^{5n/2}$. It is enough to prove that $|f(\sigma)| \ll \log(\frac{1}{\sigma-1}) + \ell^n\log_2 T$, since $2^n \leq Q$. We will show that Σ_1 constitutes the main term and all other sums are of inferior magnitude. We first bound an initial fragment of Σ_1, using the Brun-Titchmarsh inequality for $\pi(x,1,\ell)$. Note that $\ell+1$ cannot be prime.

$$
\begin{aligned}
\ell^n(\ell-1)\sum_{\substack{p\in\mathcal{S}_Q\\ p\leq 2T}}\sum_{m=1}^{\infty}\frac{1}{mp^{m\sigma}} &\leq \ell^n(\ell-1)\sum_{\substack{p\equiv 1 \bmod \ell\\ p\leq 2T}}\sum_{m=1}^{\infty}\frac{1}{mp^{m\sigma}}\\
&= \ell^n(\ell-1)\sum_{m\geq 1}\frac{1}{m}\int_{2\ell}^{2T}\frac{1}{x^{m\sigma}}d(\pi(x,1,\ell))\\
&= \ell^n(\ell-1)\sum_{m\geq 1}\frac{\pi(2T,1,\ell)}{m(2T)^{m\sigma}}+\sigma\int_{2\ell}^{2T}\frac{\pi(x,1,\ell)}{x^{m\sigma+1}}dx\\
&\leq 2\ell^n\sum_{m\geq 1}\frac{1}{mT^{m-1}}+2\ell^n\sum_{m\geq 1}\sigma\int_{2\ell}^{2T}\frac{1}{x^{m\sigma}\log(x/\ell)}dx
\end{aligned}
$$

The integral for $m=1$ gives

$$
\int_{2\ell}^{2T}\frac{1}{x^{\sigma}\log(x/\ell)}dx \leq \int_{2}^{2T/\ell}\frac{1}{x\log x}dx \leq \log_2(T/\ell)-\log_2(2).
$$

The integrals for $m\geq 2$ give

$$
\int_{2\ell}^{2T}\frac{1}{x^{m\sigma}\log(x/\ell)}dx \leq \frac{\ell}{\ell^{m\sigma}}\int_{2}^{\infty}\frac{1}{x^{m\sigma}\log x}dx \leq \frac{\ell}{\ell^{m\sigma}}\int_{2}^{\infty}\frac{1}{x^2}dx \leq \frac{\ell}{2\ell^{m\sigma}}.
$$

Hence, the total sum is bounded as follows

$$
\ell(\ell-1)\sum_{\substack{p\in\mathcal{S}_Q\\ p\leq 2T}}\sum_{m=1}^{\infty}\frac{1}{mp^{m\sigma}} \ll \ell^n\log_2 T+\ell^{n+1}\sum_{m\geq 2}\frac{1}{\ell^m} \ll \ell^n\log_2 T.
$$

The rest of Σ_1 can be handled using our generalised Brun-Titchmarsh inequality for $\pi(x, \mathcal{S}_Q)$, Theorem 2.38, where T has been chosen in such a way that the inequality is valid from $x \geq T$.

$$\begin{aligned}
\ell^n(\ell-1) \sum_{\substack{p \in \mathcal{S}_Q \\ p \geq 2T}} \sum_{m=1}^{\infty} \frac{1}{mp^{m\sigma}} &= \ell^n(\ell-1) \sum_{m \geq 1} \frac{1}{m} \int_{2T}^{\infty} \frac{1}{x^{m\sigma}} d(\pi(x, \mathcal{S}_Q)) \\
&\leq 3 \sum_{m \geq 1} \frac{m\sigma}{m} \int_{2T}^{\infty} \frac{dx}{x^{m\sigma} \log(x/T)} \\
&\leq 3 \sum_{m \geq 1} \frac{T\sigma}{T^{m\sigma}} \int_{2}^{\infty} \frac{dx}{x^{m\sigma} \log x}
\end{aligned}$$

Recall from Theorem 1.10 that

$$\int_2^{\infty} \frac{dx}{x^{\sigma} \log(x)} \leq \log \frac{1}{\sigma - 1} + e^{-1} - \log_2(2),$$

from which

$$\ell^n(\ell-1) \sum_{\substack{p \in \mathcal{S}_Q \\ p \geq 2T}} \sum_{m=1}^{\infty} \frac{1}{mp^{m\sigma}} \ll \log \frac{1}{\sigma-1} + \sum_{m \geq 2} \frac{1}{T^{m-1}} \ll \log \frac{1}{\sigma - 1} + \frac{1}{T}.$$

Thus the sum Σ_1 satisfies the stated bounds. The second sum Σ_2 can be handled in a similar way.

$$
\begin{aligned}
\Sigma_2 = \ell^{n-1}(\ell-1) \sum_{p \in \mathcal{S}^1 \setminus \mathcal{S}_Q} \sum_{m=1}^{\infty} \frac{1}{mp^{\ell m s}} &\leq \ell^{n-1}(\ell-1) \sum_{p \equiv 1 \bmod \ell} \sum_{m=1}^{\infty} \frac{1}{mp^{\ell m \sigma}} \\
&= \ell^{n-1}(\ell-1) \sum_{m \geq 1} \frac{1}{m} \int_{2\ell}^{\infty} \frac{1}{x^{\ell m \sigma}} d(\pi(x,1,\ell)) \\
&\leq 2\ell^{n-1} \sum_{m \geq 1} \frac{\ell m \sigma}{m} \int_{2\ell}^{\infty} \frac{dx}{x^{\ell m \sigma} \log(x/\ell)} \\
&\leq 2\ell^{n-1} \sum_{m \geq 1} \frac{\ell^2 \sigma}{\ell^{\ell m \sigma}} \int_{2}^{\infty} \frac{dx}{x^{\ell m \sigma} \log x} \\
&\leq \sum_{m \geq 1} \frac{\ell^{n+1} \sigma}{\ell^{\ell m \sigma}} \leq \frac{2\ell^{n+1}}{\ell^{\ell} - 1} \ll \ell^{n-1}
\end{aligned}
$$

Analogous still, we bound the sum Σ_3 as follows.

$$
\begin{aligned}
\sum_{\substack{d \mid \ell-1 \\ d \neq 1}} \ell^n \frac{\ell-1}{d} \sum_{\substack{p \in \mathcal{S}^{\ell \frac{\ell-1}{d}} \\ p \geq 2\ell}} \sum_{m=1}^{\infty} \frac{1}{mp^{dm\sigma}} &\leq \sum_{\substack{d \mid \ell-1 \\ d \neq 1}} \ell^n \frac{\ell-1}{d} \sum_{i=1}^{\phi(d)} \sum_{m=1}^{\infty} \frac{1}{m} \int_{2\ell}^{\infty} \frac{1}{x^{dm\sigma}} d(\pi(x, a_i, \ell)) \\
&\leq 2\ell^n \sum_{\substack{d \mid \ell-1 \\ d \neq 1}} \frac{\phi(d)}{d} \sum_{m=1}^{\infty} \frac{dm\sigma}{m} \int_{2\ell}^{\infty} \frac{dx}{x^{dm\sigma} \log(x/\ell)} \\
&\leq 2\ell^n \sum_{\substack{d \mid \ell-1 \\ d \neq 1}} \phi(d) \sum_{m=1}^{\infty} \frac{\ell \sigma}{\ell^{dm\sigma}} \int_{2}^{\infty} \frac{dx}{x^{dm\sigma} \log x} \\
&\ll \ell^{n+1} \sum_{\substack{d \mid \ell-1 \\ d \neq 1}} \phi(d) \sum_{m=1} \frac{1}{\ell^{dm}} \\
&\ll \ell^{n+1} \Big(\sum_{m \geq 1} \frac{1}{\ell^{2m}} + \ell \sum_{m \geq 1} \frac{1}{\ell^{3m}} \Big) \ll \ell^{n-1}
\end{aligned}
$$

The sum Σ_4 is not so straightforwardly bounded. While it depends only on ℓ, it constitutes a term whose magnitude we can show to be bounded only by a relatively small margin by $\ell^3 \log \ell$. We start with the most problematic primes, those below ℓ.

$$\sum_{\substack{d|\ell-1 \\ d\neq 1}} \ell^n \frac{\ell-1}{d} \sum_{\substack{p\in S^{\ell\frac{\ell-1}{d}} \\ p<\ell}} \sum_{m=1}^{\infty} \frac{1}{mp^{dm\sigma}} \leq \sum_{d|\ell-1} \frac{\ell^n(\ell-1)}{d} \sum_{\substack{p<\ell \\ p \text{ order } d}} \frac{2}{p^d}$$

Now note that magnitude of the $\phi(d)$ possible primes of order $d \bmod \ell$ are at least $\ell^{1/d}, (2\ell)^{1/d}, \ldots, (\phi(d)\ell)^{1/d}$, and so it follows that

$$\sum_{\substack{p<\ell \\ p \text{ order } d}} \frac{1}{p^d} \leq \frac{\log \phi(d)}{\ell}.$$

Consequently,

$$\begin{aligned}
\Sigma_4 \leq 2\ell^{n-1}(\ell-1) \sum_{d|\ell-1} \frac{\log(\phi(d))}{d} &\leq 2\ell^n \prod_{p^e|\ell-1} \left(1 + \frac{\log \phi(p)}{p} + \cdots + \frac{\log \phi(p^e)}{p^e}\right) \\
&\leq 2\ell^n) \prod_{p^e|\ell-1} \left(1 + \sum_{i=1}^{e} \frac{i\log(p)}{p^i}\right),
\end{aligned}$$

and since $\sum_i iX^i = X(\frac{1}{1-X})' = \frac{X}{(X-1)^2}$,

$$\sum_{i=1}^{e} \frac{i\log(p)}{p^i} \leq \frac{p\log p}{(p-1)^2} \leq \frac{\log p}{p} + 2\frac{\log p}{(p-1)^2}.$$

Thus,

$$\begin{aligned}\Sigma_4 &\leq 2\ell^n \prod_{p|\ell-1}\left(1+\frac{\log p}{p}+2\frac{\log p}{(p-1)^2}\right)\\ &\leq 2\ell^n \exp\left(\sum_{p|\ell-1}\frac{\log p}{p}+\sum_{p|\ell-1}2\frac{\log p}{(p-1)^2}\right).\end{aligned}$$

Since all summands are decreasing functions in p, it is clear that the sum is largest when $\ell-1$ is of the form $\prod_{p\leq y} p$, for some y. Since

$$\prod_{p\leq y} p = \exp\left(\sum_{p\leq y}\log p\right) \geq e^{y/2},$$

we have that $y \leq 2\log(\ell)$. Finally, using Mertens' theorem,

$$\begin{aligned}\Sigma_4 &\leq 2\ell^n \exp\left(\sum_{p\leq 2\log(\ell)}\frac{\log p}{p}+\sum_{p>1}2\frac{\log p}{(p-1)^2}\right)\\ &\leq 2\ell^n \exp\left(\log(2\log(\ell))+c\right) \ll \ell^n\log(\ell) \ll \ell^n \log_2 T.\end{aligned}$$

The primes in $[\ell, 2\ell]$ are not congruent to $1 \bmod \ell$, and hence

$$\begin{aligned}\sum_{\substack{d|\ell-1\\ d\neq 1}} \ell^n\frac{\ell-1}{d}\sum_{\substack{p\in\mathcal{S}^d\\ \ell<p<2\ell}}\sum_{m=1}^{\infty}\frac{1}{mp^{dm\sigma}} &\leq \sum_{d|\ell-1}\frac{\ell^n(\ell-1)}{d}\sum_{\substack{\ell<p<2\ell\\ p \text{ order } d}}\frac{2}{p^d}\\ &\leq \frac{\ell^{n+1}}{2}\frac{2}{(2\ell-1)^2}+\frac{\ell^{n+1}}{3}\ell\frac{2}{\ell^3} \ll \ell^{n-1}.\end{aligned}$$

Lastly, the sum Σ_5 over the ramified primes above ℓ and q is of insignificant magnitude. ℓ ramifies completely in $\mathbb{Q}(\zeta_\ell)$, and thus splits in at most ℓ^n primes in K, and since q_i ramifies completely in $\mathbb{Q}(\sqrt[\ell]{q_i})$, q splits in at most $\ell^{n-1}(\ell-1)$ primes in K. Thus the total contribution is bounded by

$$\begin{aligned}\Sigma_5 \leq \ell^n \log(1-\frac{1}{\ell}) + \ell^{n-1}(\ell-1)\sum_i \log(1-\frac{1}{q_i}) \ll \ell^{n-1} + \sum_i \frac{\ell^n}{q_i} \\ \ll \ell^n \sum_{p\leq Q} \frac{1}{p} \ll \ell^n \log_2 Q.\end{aligned}$$

Since we have shown that each Σ_i is smaller than the required bound, we have proven the statement. $\square$

Remark 3.4. The main difference with respect to the corresponding Theorem 1.10 is the appearance of tregardhe second main term $\ell \log_2 T$. It is a direct consequence of the fact that our sieving result Theorem 2.38 is valid only from $x \geq T$. With regard to the parameter Q, this second term is $O(\log_2 Q)$. With regard to the parameter ℓ, it is $O(\ell^{n+3}\log \ell)$, yet unlike in Theorem 1.10 where only prime powers congruent to 1 and $-1 \mod \ell$ are counted, here the small primes have to be reckoned with. As we have seen in the above proof, the primes below ℓ might contribute up to $\ell^n \log(\ell)$ if many small primes have low order $\mathrm{mod} \ell$. If ℓ is a Mersenne prime, for example, already the contribution is at least ℓ^n. In conclusion, the second main term is of very modest magnitude in Q, and of considerable magnitude in ℓ, yet if n is large, it is quite close to the magnitude of an unavoidable second main term.

3.3 Analytic input

In this section we will prove bounds on the derivatives of $f(s)$ complementary to the bound in Theorem 3.3, which in contrast do not diverge as s tends to 1. Allthough we will not use the full strength of the theorems in this section, we do strive to prove relatively optimal statements.

We note that since $\zeta_K(s)$ has an analytic continuation to the complex plane with only a simple pole at $s = 1$, the function $(s-1)\zeta_K(s)$ is entire. The fact that $\zeta_K(s)$ has no zeros in some region is then equivalent to $f(s)$ being holomorphic in this region.

We start by demarcating a zero-free region. In general, one expects to have a *near*-zero-free region of radius about $\frac{1}{\log(\Delta_K)}$ around $s = 1$, where one cannot exclude the possibility of the presence of a single real zero. Due to the special structure of the Galois group of $K = \mathbb{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \ldots, \sqrt[\ell]{q_n})$, we can prove a far stronger assertion.

Theorem 3.5. *Let $K = \mathbb{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \ldots, \sqrt[\ell]{q_n})$. $\zeta_K(s)$ has no zeros $\beta + i\gamma$ with*

$$\beta > 1 - \frac{1}{10\ell^2 \log Q} \qquad \text{and} \qquad |\gamma| < \frac{1}{10\ell^2 \log Q}.$$

Moreover, if $n = 1$, $\zeta_K(s)$ has no zeros $\beta + i\gamma$ with

$$\beta > 1 - \frac{1}{10\ell \log(\ell q)} \qquad \text{and} \qquad |\gamma| < \frac{1}{10\ell \log(\ell q)}.$$

Proof. For any character $\chi \bmod \ell$, $L(s,\chi)$ has no zeros in this region[19]. Consider the factorisation of the Dedekind zeta functions into Artin L-functions, where we use the description of the irreducible representations in Theorem 3.1.

$$\zeta_K(s) = \prod_{\chi} L(s,\chi)^{\dim(\chi)} = \zeta_{\mathbb{Q}(\zeta_\ell)}(s) \prod_{a \in PG(n-1,\ell)} L(s,\psi_a)^{\ell-1},$$

where ψ_a is the $(\ell-1)$-dimensional character belonging to the field $K_a = \mathbb{Q}(\zeta_\ell, \sqrt[\ell]{\prod_i q_n^{a_i}})$. Furthermore, we have that

$$\zeta_{K_a}(s) = \zeta_{\mathbb{Q}(\zeta_\ell)}(s) L(s,\psi_a)^{\ell-1}.$$

Since Artin-L-functions are meromorphic, it follows that any zero ρ of $\zeta_K(s)$ in this region is a zero with multiplicity at least $\ell - 1$ of a certain $\zeta_{K_a}(s)$.

The following inequality is a consequence of the Hadamard product formula and the functional equation, see e.g. [44]:

$$\sum_{\rho} \frac{1}{\sigma - \rho} \leq \frac{1}{\sigma - 1} + \frac{\log(\Delta_{K_a})}{2}, \tag{3.2}$$

where the sum runs over any subset of roots ρ of $\zeta_{K_a}(s)$ which is closed under complex conjugation. We choose $\sigma = 1 + \frac{\ell}{\log \Delta_{K_a}}$, and assume that β is a real zero with $\beta > 1 - \frac{\ell}{10 \log \Delta_{K_a}}$. Then

$$(\ell - 1)\frac{1}{\sigma - \beta} \geq (\ell - 1)\frac{\log \Delta_{K_a}}{\ell + \ell/10} \geq (\frac{1}{\ell} + \frac{1}{2}) \log \Delta_{K_a},$$

which gives a contradiction with (3.2). If $\rho = \beta + i\gamma$ is a complex zero with $\beta > 1 - \frac{\ell}{10 \log \Delta_{K_a}}$ and $|\gamma| < \frac{\ell}{10 \log \Delta_{K_a}}$, then

$$\begin{aligned}(\ell - 1)\frac{2(\sigma - \beta)}{(\sigma - \beta)^2 + \gamma^2} &\geq (\ell - 1)\frac{2(\sigma - 1)}{(\sigma - \beta)^2 + \gamma^2} \\ &\geq (\ell - 1)\frac{2\ell}{(11/10)^2\ell^2 + (1/10)^2\ell^2} \log \Delta_{K_a} \\ &\geq (\frac{1}{\ell} + \frac{1}{2}) \log \Delta_{K_a},\end{aligned}$$

hence we again arrive at a contradiction with (3.2). Now we note that if $n = 1$, there is only one a, and $K_a = K$, and thus $\frac{\ell}{10 \log \Delta_{K_a}} \geq \frac{1}{10\ell \log(\ell q)}$ by Theorem 3.1. If $n \neq 1$, the $(n = 1)$-version of Theorem 3.1 shows that $\Delta_{K_a} \leq (\ell \prod_i q_i^{a_i})^{\ell^2} \leq Q^{\ell^3}$ so that $\frac{\ell}{10 \log \Delta_{K_a}} \geq \frac{1}{10\ell^2 \log Q}$, which finishes the proof. $\square$

Remark 3.6. The Artin L-functions we encountered in the above proof are much less understood than their abelian analogues, the Dirichlet L-functions. Artin's Conjecture states that all Artin L-functions are holomorphic, but it has only been proven in some very special cases, e.g. for Artin L-functions corresponding to monomial characters. Using notation as in Theorem 3.2, the tower of Galois extensions $K_n/K_{n-1}/\ldots/K_1/K_0/\mathbb{Q}$ has cyclic Galois group in each step, which is to say that $G(K)$ is supersolvable. This implies that all irreducible characters are monomial, and hence we know that all factors $L(s, \psi_a)$ are holomorphic functions. However, we will not use this fact.

Our next ingredient concerns a bound for the real part of $f(s)$ in a neighbourhood of 1. Whereas in the first chapter this could be done directly by simply looking at the Dirichlet series of the relevant L-functions which converges even for s with real part smaller than 1, this simple approach is evidently no longer possible. One general strategy to bound L-functions inside the critical strip consists of estimating the L-function to the right of the critical strip, where the Dirichlet series converges, and using the functional equation to infer a bound on the L-function valid to the left of the critical strip. Finally a Phragmen-Lindelöf type theorem is applied to *interpolate* a bound which holds inside the critical strip. The result of this classical method is often called a convexity bound, and we will make use of the following which is due to Rademacher[39].

Theorem 3.7. *Let K be any number field of degree n. For $\eta \in (0, \frac{1}{2}]$, and $\sigma \in [-\eta, 1+\eta]$,*

$$|(s-1)\zeta_K(s)| \leq 3|s+1| \left(\Delta_K \left(\frac{|s+1|}{2\pi}\right)^n\right)^{1+\eta-\sigma} \zeta(1+\eta)^n. \tag{3.3}$$

Corollary 3.8. *Let* $K = \mathbb{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \ldots, \sqrt[\ell]{q_n})$. *For all* s *with bounded imaginary part and* $\sigma \in [1 - \frac{1}{\log(\ell Q)}, 1 + \frac{1}{\log(\ell Q)}]$, *we have*

$$\mathrm{Re}(\log f(s)) \ll \ell^{n+1} \log_2(\ell Q),$$

where the implied constant is absolute and effective.

Proof. Upon taking the logarithm of (3.3), we see that

$$\mathrm{Re}(\log f(s)) \ll (1 + \eta - \sigma)(\log \Delta_K + \ell^n(\ell - 1)) + \ell^n(\ell - 1) \log \zeta(1 + \eta).$$

We plug in the restriction $\sigma \in [1 - \eta, 1 + \eta]$ and use that $\zeta(1 + \eta) \ll \frac{1}{\eta}$ to obtain

$$\mathrm{Re}(\log f(s)) \ll \eta \ell^{n+1} \log(\ell Q) + \ell^{n+1} \log \frac{1}{\eta}.$$

The result follows upon choosing $\eta = \frac{1}{\log(\ell Q)}$. □

We now proceed to prove the necessary bounds on the derivatives on $f(s)$, similarly to the proof of Theorem 1.11, using the Borel-Carathéodory lemma.

Theorem 3.9. *For all* $\sigma \in [1 - \frac{1}{20\ell^2 \log Q}, 1 + \frac{1}{20\ell^2 \log Q}]$ *the bounds*

$$|f^{(\nu)}(\sigma)| \ll \nu! \left(20\ell^2 \log Q\right)^\nu \ell^{n+1} \log(\ell Q)$$

hold, where the implied constant is absolute and effective.

Proof. We start by giving a lower bound for the residue;

$$\mathrm{res}_{s=1}\zeta_K(s) = \frac{(2\pi)^{\frac{\ell^n(\ell-1)}{2}} h_K \mathrm{Reg}_K}{2\ell\sqrt{\Delta_K}} \geq 0.2\frac{(2\pi)^{\frac{\ell^n(\ell-1)}{2}}}{2\ell(\ell Q)^{\ell^{n+1}/2}} \geq \frac{1}{(\ell Q)^{\ell^{n+1}}},$$

since $h_K \geq 1$ and $\mathrm{Reg}_K \geq 0.2$ by [9]. This implies that

$$\mathrm{Re}(f(1)) \geq -\ell^{n+1}\log(\ell Q).$$

Using Corollary 3.8, it follows that

$$\mathrm{Re}(f(s) - f(1)) \ll \ell^{n+1}\log(\ell Q).$$

Since $f(s)$ is holomorphic in $B(1, \frac{1}{10\ell^2\log Q})$, we may apply the Borel-Carathéodory lemma with $R = \frac{1}{10\ell^2\log Q}$, and $r = \frac{1}{20\ell^2\log Q}$, and the result follows. □

3.4 Conclusion of the method

We can now prove the analogous theorem to Theorem 1.7.

Theorem 3.10. *Let $K = \mathbb{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \ldots, \sqrt[\ell]{q_n})$, for any odd prime ℓ and any primes $q_i \neq \ell$. We have*

$$|\log(\mathrm{res}_{s=1}\zeta_K(s))| \ll \ell^{n+3}\log\ell + \ell^n\log_2 Q.$$

Proof. We use the mean-value theorem and Theorem 3.3 to write

$$\begin{aligned} f(1) &= f(\sigma) + (\sigma - 1)f'(\sigma'), \\ &\ll \log \frac{1}{\sigma - 1} + \ell^{n+3} \log \ell + \ell^n \log_2 Q + (\sigma - 1)f'(\sigma') \end{aligned}$$

for a certain $\sigma' \in [1, \sigma]$. We choose $\sigma = 1 + \frac{1}{\ell^4 \log^2 Q}$ and use Theorem 3.9 to get

$$f(1) \ll \ell^{n+3} \log \ell + \ell^n \log_2 Q + \frac{1}{\ell^4 \log^2 Q}(20\ell^2 \log Q)\ell^{n+1} \log(\ell Q),$$

from which the result follows immediately. □

Remark 3.11. We remark that in contrast to Theorem 1.7, the first derivative suffices to reduce $|f(1)|$ to the term $\ell^{n+3} \log \ell + \ell^n \log_2 Q$, which will of course, no matter the number of derivatives used, remain there. Some remarks on the quality of this estimate are in order. With regard to Q it is of the same strength as Theorem 1.7 was with regard to ℓ. With regard to ℓ, the upper bound is pretty huge, but at least ℓ^n is unavoidable by the contribution of the small primes in Theorem 3.3.

We state the resulting bounds on $h_K \mathrm{Reg}_K$, which are likewise not very stringent in terms of ℓ, but quite so in terms of Q.

Corollary 3.12. *There exists an absolute constant c such that*

$$\frac{Q^{\frac{\ell^{n-1}(\ell-1)^2}{2}}}{\ell^{c\ell^{n+3}}(\log Q)^{c\ell^n}} \leq h_K \mathrm{Reg}_K \leq \ell^{c\ell^{n+3}} Q^{\frac{\ell^{n-1}(\ell-1)^2}{2}} (\log Q)^{c\ell^n}$$

Proof. Theorem 3.10 together with the Analytic Class Number Formula give us that for a certain absolute c,

$$\ell^{-c\ell^{n+3}}(\log Q)^{-c\ell^n} \leq \frac{(2\pi)^{\frac{\ell^n(\ell-1)}{2}} h_K \mathrm{Reg}_K}{2\ell\sqrt{\Delta_K}} \leq \ell^{c\ell^{n+3}}(\log Q)^{c\ell^n}.$$

We first use the upper bound for the discriminant from Theorem 3.2,

$$h_K \mathrm{Reg}_K \leq \frac{2\ell\ell^{\frac{\ell^{n+1}}{2}}\ell^{c\ell^{n+3}}}{(2\pi)^{\frac{\ell^n(\ell-1)}{2}}} Q^{\frac{\ell^{n-1}(\ell-1)^2}{2}} (\log Q)^{c\ell^n} \leq \ell^{c\ell^{n+3}} Q^{\frac{\ell^{n-1}(\ell-1)^2}{2}} (\log Q)^{c\ell^n}$$

where in the last inequality the value of c is different than before. Using the lower bound for the discriminant,

$$h_K \mathrm{Reg}_K \geq \frac{2\ell\ell^{\frac{\ell^{n+1}}{2}}}{\ell^{c\ell^{n+3}}(2\pi)^{\frac{\ell^n(\ell-1)}{2}}} \frac{Q^{\frac{\ell^{n-1}(\ell-1)^2}{2}}}{(\log Q)^{c\ell^n}} \geq \frac{Q^{\frac{\ell^{n-1}(\ell-1)^2}{2}}}{\ell^{c\ell^{n+3}}(\log Q)^{c\ell^n}},$$

where in the last inequality the value of c is different than before. □

Finally, we apply this to give the analytic density of the completely splitting primes with error term.

Corollary 3.13. *Let $\mathcal{S}_{q_1,\ldots,q_n}$ be the set of completely splitting primes in the field $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \ldots, \sqrt[\ell]{q_n})$. For $|s-1|$ small enough, we have that*

$$\left| \sum_{p \in \mathcal{S}_{q_1,\ldots,q_n}} p^{-s} - \frac{1}{\ell^n(\ell-1)} \log\left(\frac{1}{s-1}\right) \right| \ll \ell^2 \log \ell + \frac{\log_2 Q}{\ell}.$$

Proof. $\log\left(\zeta_K(s)(s-1)\right) = \log \zeta_K(s) - \log\left(\frac{1}{s-1}\right)$, and since in Theorem 3.3 all terms except $\sum_{p \in \mathcal{S}_{q_1,\ldots,q_n}} p^{-s}$ have been bounded by $\ell^{n+3} \log \ell + \ell^n \log_2 Q$, we have that

$$\begin{aligned} \left| \ell^n(\ell-1) \sum_{p \in \mathcal{S}_{q_1,\ldots,q_n}} p^{-s} - \log\left(\frac{1}{s-1}\right) \right| \ll & \ell^{n+3} \log \ell + \ell^n \log_2 Q \\ & + \log\left(\zeta_K(s)(s-1)\right). \end{aligned}$$

By Theorem 3.10, the right hand side is smaller than $\ell^{n+3} \log \ell + \ell^n \log_2 Q$ for $|s-1|$ small enough, whence the result follows. $\square$

A

Nederlandstalige samenvatting

Het hoofdthema van dit proefschrift situeert zich in de analytische getaltheorie. Meer specifiek kunnen we stellen dat L-functies en zeefmethoden centraal staan.

In hoofdstuk 1 beschouwen we het klassegetalprobleem voor cyclotome velden. De vraag welke klassegetallen gelijk zijn aan 1 werd in 1967 beantwoord door Masley en Montgomery [29], door het bewijzen van een effectieve afschatting op het asymptotisch gedrag van het klassegetal. Voorafgaande pogingen liepen steeds tegen de barrière van een mogelijk "exceptioneel" karakter aan en de innovatie van Montgomery en Masley bestond erin om een absolute maar divergente bovengrens te geven voor de L-functies, en door middel van een nulpuntenvrije regio, een absolute bovengrens op de afgeleiden van deze L-functies te geven. De combinatie van deze twee types bovengrenzen is de kern van de methoden, die werd verfijnd door Schlage-Puchta [38] en door de auteur [6], met als resultaat de volgende stelling.

Stelling A.1. *Zij ℓ een oneven priemgetal. Indien geen van de oneven Dirichlet L-functies met geleider ℓ een Siegel-nulpunt bezit, dan voldoet het relatieve klassegetal van $\mathbb{Q}(\zeta_\ell)$ aan*

$$|\log(h_\ell^-/G(\ell))| \leq 2\log_2 \ell + O(\log_3 \ell).$$

Indien er wel een van de oneven Dirichlet L-functies met geleider ℓ een Siegel-nulpunt β bezit, dan voldoet het relatieve klassegetal van $\mathbb{Q}(\zeta_\ell)$ aan

$$|\log(h_\ell^-/G(\ell)) - \log(1-\beta)| \leq 4\log_2 \ell + O(\log_3 \ell).$$

In hoofdstuk 2 ontwikkelen we een methode om een bovengrens te bewijzen op het aantal priemgetallen dat aan een zekere voorwaarde voldoet. We stellen onze aandacht op priemen die volledig splitsen in een zekere familie van velduitbreidingen $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \dots\sqrt[\ell]{q_n})$, en onderzoeken de mogelijkheid om door middel van zeeftheorie hier een bovengrens op te geven, analoog aan de klassieke Brun-Titchmarshongelijkheid voor $\mathbb{Q}(\zeta_\ell)$. De eerste stap betreft een wederkerigheidswet: een criterium opdat een priem volledig zou splitsen, in termen van deze priem modulo q_i. Op deze manier kunnen we het telprobleem formuleren als een zeefprobleem, waarbij we de zeef van Selberg formuleren in de ring van cyclotome gehelen. Op die manier wordt het probleem gereduceerd tot het begrenzen van resttermen, wat we volbrengen gebruik makend van volgend fundamenteel lemma voor het tellen van cyclotome gehelen op vermenigvuldiging met eenheden na.

Lemma A.2. *Zij $\mathfrak{a}$ een integraal ideaal in de ring van gehelen $\mathcal{O}_K$ van een getallenveld K van graad n. Zij $\mathfrak{M} \supseteq \mathfrak{a}$ een deelgroep van $(\mathcal{O}_K, +)$. Dan geldt*

$$\left|\left\{ \ \alpha \in \mathfrak{M} \ \middle| \ \phi(\alpha) \in \mathcal{F}(t^n) \ \right\}\right| = \frac{\omega \ \mathrm{res}_{s=1}\zeta_K(s)}{h_K[\mathcal{O}_K : \mathfrak{M}]} t^n + O\left(\max(1, \frac{t^{n-1}}{N(\mathfrak{a})^{\frac{n-1}{n}}})\right),$$

waar de constante in de O-term begrensd is door $n^{4n^2} m(\varepsilon)^{\frac{nr}{2}}$. Meer nog, als $K = \mathbb{Q}(\zeta_\ell)$, dan is de constante begrensd door $\ell^{\frac{\ell^3}{2}}$.

Met dit fundamenteel lemma kunnen we ook het klassieke bewijs van Landau over de analytische voortzetting van $\zeta_K(s)$ tot $\mathrm{Re}(s) \geq 1 - \frac{1}{n}$ expliciet maken. Het uiteindelijke resultaat van de zeefmethode is de volgende stelling.

Stelling A.3. *Zij $\mathcal{S}_{q_1,\ldots,q_n}$ de verzameling van volledig splitsende priemen in de getallenvelden $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \ldots, \sqrt[\ell]{q_n})$. Voor alle oneven priemen ℓ, voor alle* *priemen $q_j \neq \ell$, en voor alle $x > Q^{\frac{5(\ell-2)(\ell-1)}{4}} \ell^{\ell^{\ell^3}} 2^{\frac{5(\ell-1)}{4} n}$ geldt dat*

$$\pi(x, \mathcal{S}_Q) \leq \frac{3}{\ell^n(\ell-1)} \frac{x}{\log(x) - \log\left(Q^{\frac{5(\ell-2)(\ell-1)}{4}} \ell^{\ell^{\ell^3}} 2^{\frac{5(\ell-1)}{4} n}\right)}.$$

In hoofdstuk 3 tenslotte combineren we de fundamenten van de methode uit hoofdstuk 1 met de informatie op de volledig splitsende priemen in de velden $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \ldots, \sqrt[\ell]{q_n})$, om een bovengrens te geven op het residu van de Dedekind-zetafunctie van dit veld. Wat betreft de analytische kant van de methode werken we nu niet met Dirichlet-L-functies, maar met de algemenere Artin-L-functies, waarvan de theorie nog minder ontwikkeld is. Door de speciale structuur van de Galoisgroep van de velden slagen we erin om een omvangrijke nulpuntenvrije regio te vinden, en met behulp van een zogenaamde convexiteitsgrens bewijzen we de noodzakelijke analytische informatie. Het resultaat is minder scherp dan in hoofdstuk 1, vooral omdat onze ongelijkheid voor de volledig splitsende priemen pas geldt voor zeer grote x. Ook bezitten onze velden geen zogenaamde CM-structuur, waardoor we geen grens op het klassengetal bekomen, maar enkel een grens op het klassengetal maal de regulator.

Stelling A.4. *Zij ℓ een oneven priem, en zij $Q = q_1 \ldots q_n$ met $q_i \neq \ell$ priemen, en zij $K = \mathbb{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \ldots, \sqrt[\ell]{q_n})$. Dan geldt*

$$|\log(\mathrm{res}_{s=1}\zeta_K(s))| \ll \ell^{n+3} \log \ell + \ell^n \log_2 Q,$$

waar de impliciete constante absoluut en effectief is.

Bibliography

[1] N. C. Ankeny and S. Chowla. The class number of the cyclotomic field. *Proc. Nat. Acad. Sci. U. S. A.*, 35:529–532, 1949.

[2] B. C. Berndt, R. J. Evans, and K. S. Williams. *Gauss and Jacobi sums*. Canadian Mathematical Society Series of Monographs and Advanced Texts. John Wiley & Sons, Inc., New York, 1998. A Wiley-Interscience Publication.

[3] J. W. S. Cassels. *An introduction to the geometry of numbers*. Classics in Mathematics. Springer-Verlag, Berlin, 1997. Corrected reprint of the 1971 edition.

[4] F. Chamizo and H. Iwaniec. On the sphere problem. *Rev. Mat. Iberoamericana*, 11(2):417–429, 1995.

[5] H. Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2000. Revised and with a preface by Hugh L. Montgomery.

[6] K. Debaene. The first factor of the class number of the p-th cyclotomic field. *Arch. Math. (Basel)*, 102(3):237–244, 2014.

[7] T. Estermann. *Introduction to Modern Prime Number Theory*, volume 41 of *Cambridge Tracts in Mathematics and Mathematical Physics*. Cambridge University Press, 1961.

[8] F. Fricker. *Einführung in die Gitterpunktlehre*, volume 73 of *Lehrbücher und Monographien aus dem Gebiete der Exakten Wissenschaften (LMW). Mathematische Reihe [Textbooks and Monographs in the Exact Sciences. Mathematical Series]*. Birkhäuser Verlag, Basel-Boston, Mass., 1982.

[9] E. Friedman. Analytic formulas for the regulator of a number field. *Invent. Math.*, 98(3):599–622, 1989.

[10] G. Fung, A. Granville, and H. C. Williams. Computation of the first factor of the class number of cyclotomic fields. *J. Number Theory*, 42(3):297–312, 1992.

[11] A. Granville. On the size of the first factor of the class number of a cyclotomic field. *Invent. Math.*, 100(2):321–338, 1990.

[12] J. L. Hafner. The distribution and average order of the coefficients of Dedekind ζ functions. *J. Number Theory*, 17(2):183–190, 1983.

[13] H. Halberstam and H.-E. Richert. *Sieve methods*. Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1974. London Mathematical Society Monographs, No. 4.

[14] D. R. Heath-Brown. The growth rate of the Dedekind zeta-function on the critical line. *Acta Arith.*, 49(4):323–339, 1988.

[15] D. R. Heath-Brown. Lattice points in the sphere. In *Number theory in progress, Vol. 2 (Zakopane-Kościelisko, 1997)*, pages 883–892. de Gruyter, Berlin, 1999.

[16] J. G. Hinz. An application of algebraic sieve theory. *Arch. Math. (Basel)*, 80(6):586–599, 2003.

[17] M. N. Huxley. Exponential sums and lattice points. III. *Proc. London Math. Soc. (3)*, 87(3):591–609, 2003.

[18] H. Iwaniec. Prime numbers and *L*-functions. In *International Congress of Mathematicians. Vol. I*, pages 279–306. Eur. Math. Soc., Zürich, 2007.

[19] H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[20] H. Kadiri. *Régions explicites sans zéros pour les fonctions L de Dirichlet*. PhD thesis, Université de Lille I, 2002.

[21] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464. Academic Press, London, 1977.

[22] E. Landau. *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale*. Chelsea Publishing Company, New York, N. Y., 1949.

[23] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[24] H. Lao. On the distribution of integral ideals and Hecke Grössencharacters. *Chin. Ann. Math. Ser. B*, 31(3):385–392, 2010.

[25] F. Lemmermeyer. List of published proofs of the quadratic reciprocity law. `http://www.rzuser.uni-heidelberg.de/~hb3/rchrono.html`. Accessed: 2015-03-27.

[26] F. Lemmermeyer. *Reciprocity laws*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000. From Euler to Eisenstein.

[27] T. Lepistö. On the growth of the first factor of the class number of the prime cyclotomic field. *Ann. Acad. Sci. Fenn. Ser. A I*, (577):21, 1974.

[28] S. R. Louboutin. Mean values of L-functions and relative class numbers of cyclotomic fields. *Publ. Math. Debrecen*, 78(3-4):647–658, 2011.

[29] J. M. Masley and H. L. Montgomery. Cyclotomic fields with unique factorization. *J. Reine Angew. Math.*, 286/287:248–256, 1976.

[30] J. Maynard. On the Brun-Titchmarsh theorem. *Acta Arith.*, 157(3):249–296, 2013.

[31] J. C. Miller. Real cyclotomic fields of primes conductor and their class numbers. *Math. Comp.* Electronically Published on February 5, 2015, DOI: http://dx.doi.org/10.1090/S0025-5718-2015-02924-X.

[32] H. L. Montgomery. *Topics in multiplicative number theory*. Lecture Notes in Mathematics, Vol. 227. Springer-Verlag, Berlin-New York, 1971.

[33] H. L. Montgomery and R. C. Vaughan. The large sieve. *Mathematika*, 20:119–134, 1973.

[34] Y. Motohashi. On some improvements of the Brun-Titchmarsh theorem. *J. Math. Soc. Japan*, 26:306–323, 1974.

[35] M. R. Murty and J. Van Order. Counting integral ideals in a number field. *Expo. Math.*, 25(1):53–66, 2007.

[36] J. Neukirch. *Algebraic number theory*, volume 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.

[37] W. G. Nowak. On the distribution of integer ideals in algebraic number fields. *Math. Nachr.*, 161:59–74, 1993.

[38] J.-C. Puchta. On the class number of p-th cyclotomic field. *Arch. Math. (Basel)*, 74(4):266–268, 2000.

[39] H. Rademacher. On the Phragmén-Lindelöf theorem and some applications. *Math. Z*, 72:192–204, 1959/1960.

[40] G. J. Rieger. Verallgemeinerung der Siebmethode von A. Selberg auf Algebraische Zahlkörper. III. *J. Reine Angew. Math.*, 208:79–90, 1961.

[41] H. Sarges. Eine Anwendung des Selbergschen Siebes auf algebraische Zahlkörper. *Acta Arith.*, 28(4):433–455, 1975/76.

[42] W. Schaal. Obere und untere Abschätzungen in algebraischen Zahlkörpern mit Hilfe des linearen Selbergschen Siebes. *Acta Arith*, 13:267–313, 1967/1968.

[43] N. Snyder. *Artin L-functions : A Historical Approach*. PhD thesis, Harvard University, 2002.

[44] H. M. Stark. Some effective cases of the Brauer-Siegel theorem. *Invent. Math.*, 23:135–152, 1974.

[45] T. Tatuzawa. On the product of $L(1, \chi)$. *Nagoya Math. J.*, 5:105–111, 1953.

[46] L. C. Washington. *Introduction to Cyclotomic Fields*, volume 83 of *Graduate Texts in Mathematics*. Springer, 1982.

[47] M. Widmer. Counting primitive points of bounded height. *Trans. Amer. Math. Soc.*, 362(9):4793–4829, 2010.