CLASS NUMBERS OF TOTALLY REAL NUMBER FIELDS

BY JOHN C. MILLER

A dissertation submitted to the

Graduate School—New Brunswick

Rutgers, The State University of New Jersey

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Graduate Program in Mathematics

Written under the direction of

Henryk Iwaniec

and approved by

____

____

____

____

New Brunswick, New Jersey

May, 2015

ABSTRACT OF THE DISSERTATION

Class numbers of totally real number fields

by John C. Miller

Dissertation Director: Henryk Iwaniec

The determination of the class number of totally real fields of large discriminant is known to be a difficult problem. The Minkowski bound is too large to be useful, and the root discriminant of the field can be too large to be treated by Odlyzko's discriminant bounds. This thesis describes a new approach. By finding nontrivial lower bounds for sums over prime ideals of the Hilbert class field, we establish upper bounds for class numbers of fields of larger discriminant. This analytic upper bound, together with algebraic arguments concerning the divisibility properties of class numbers, allows us to determine the class numbers of many number fields that have previously been untreatable by any known method.

For example, we consider the cyclotomic fields and their real subfields. Surprisingly, the class numbers of cyclotomic fields have only been determined for fields of small conductor, e.g. for prime conductors up to 67, due to the problem of finding the class number of its maximal real subfield, a problem first considered by Kummer. Our results have significantly improved the situation.

We also study the cyclotomic $\mathbb{Z}_p$-extensions of the rationals. Based on the heuristics of Cohen and Lenstra, and refined by new results on class numbers of particular fields, we provide evidence for the following conjecture first suggested by Coates: For *all* primes p, every number field in a cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ has class number 1.

Acknowledgements

I would like to thank my advisor, Henryk Iwaniec, for introducing me to Weber's class number problem and other class number problems of cyclotomic fields. Without his steadfast encouragement, it would not have been possible to complete this thesis. There are many people who generously gave me advice, assisted me with my research and who otherwise provided help to me in ways large and small. I would like to make special mention of John Coates, Matthew de Courcy-Ireland, Takashi Fukuda, Keiichi Komatsu, Alex Kontorovich, Stephen D. Miller, Carl Pomerance, Réne Schoof, Takashi Taniguchi, Jerrold Tunnell, John Voight and Lawrence Washington. Much of this thesis has been previously published in several journals [18–21], and I thank the anonymous referees for their careful reading and feedback.

Most of all, I would like to thank my wife Seiko. She has been thoughtful, loving and patient throughout these years. I owe her my deepest gratitude.

Table of Contents

Abstract ii

Acknowledgements iii

1. Introduction 1

2. Upper bounds for class numbers 3

2.1. Upper bounds for class numbers of fields of small root discriminant . . . 4

2.2. An identity for the class number of a totally real number field 6

2.3. Upper bounds for class numbers of fields of large discriminant 7

2.4. Comparison with the Minkowski bound 10

3. Class numbers of cyclotomic fields 16

3.1. Cyclotomic fields of prime conductor 17

3.1.1. Upper bounds for class numbers beyond Odlyzko's discriminant bounds 18

3.1.2. The class number of $\mathbb{Q}(\zeta_p)^+$ for primes $p = 71, 73, 79, 83$ 19

3.1.3. The class number of $\mathbb{Q}(\zeta_p)^+$, prime p, $89 \leq p \leq 131$ 20

3.1.4. The class number of $\mathbb{Q}(\zeta_p)^+$ for primes $p = 137, 139, 149, 151$ . . 21

3.1.5. The class number of $\mathbb{Q}(\zeta_p)^+$ for primes p, $167 \leq p \leq 193$ 23

3.1.6. The class number of $\mathbb{Q}(\zeta_p)^+$ for primes p, $197 \leq p \leq 241$ 24

3.1.7. The class number of $\mathbb{Q}(\zeta_{251})^+$ 29

3.1.8. The class number of $\mathbb{Q}(\zeta_{257})^+$ 32

3.1.9. The class number of $\mathbb{Q}(\zeta_{263})^+$ 37

3.2. Cyclotomic fields of composite conductor 41

3.2.1. Real cyclotomic fields 42

3.2.2. The class number of the cyclotomic field of conductor 256 43

3.2.3. The class number of the cyclotomic field of conductor 512 46

3.2.4. Divisibility properties of the class numbers of real cyclotomic fields 55

3.2.5. The class number of the real cyclotomic field of conductor 148 . 58

3.2.6. Upper bounds for class numbers of real cyclotomic fields of degree less than or equal to 58 60

3.2.7. Class numbers of real cyclotomic fields of degree up to 58 62

3.2.8. The class number of the real cyclotomic field of conductor 145 . 68

3.2.9. The class number of the real cyclotomic field of conductor 212 . 70

4. Class numbers of cyclotomic $\mathbb{Z}_p$-extensions 72

4.1. New results on certain $\mathbb{B}_{p,n}$ 76

4.2. Cohen-Lenstra heuristics for totally real cyclic number fields 79

4.3. Cohen-Lenstra heuristics for cyclotomic $\mathbb{Z}_p$-extensions 81

4.4. The $\mathbb{Z}_2$-extension 82

4.5. The $\mathbb{Z}_3$-extension 84

4.6. The $\mathbb{Z}_5$-extension 85

4.7. The $\mathbb{Z}_p$-extensions for $7 \leq p \leq 31$ 87

4.8. First layers of the $\mathbb{Z}_p$-extensions 91

4.9. Sums over Sophie Germain primes 92

4.10. Revisiting the first layers $\mathbb{B}_{p,1}$ 96

4.11. Higher layers of the $\mathbb{Z}_p$-extensions 98

4.12. Summary of results and remarks 99

5. Conclusion and directions for further work 101

References 103

Chapter 1

Introduction

> *Le problème de la répartition des nombres de classes et des groupes de classes d'idéaux de corps de nombres se pose depuis Gauss. Bien que l'on ait fait de remarquables découvertes dans ce domaine, on peut raisonnablement affirmer que l'on ne connait presque rien.*
>
> H. Cohen and J. Martinet

The rational integers have the property of unique factorization into primes, but this property can fail in general number rings. This failure is measured by the ideal class group and its cardinality, the class number. The class number is perhaps the most important invariant of a number field, yet much about class numbers remains mysterious. For example, one of the great open problems in number theory is to prove there are infinitely many number fields with class number 1, or even bounded class number.

Given a number field K of degree n and signature (r_1, r_2), the classical method to calculate its class number is to employ the Minkowski bound

$$M_K = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|d(K)|}$$

where $d(K)$ denotes the discriminant of the field. In particular, to prove K has class number 1, it suffices to show that, for every prime number $p \leq M_K$, that p factors into prime ideals of K which are all principal.

Unfortunately this method becomes impractical for number fields of large discriminant. To address fields of large discriminant, it is useful to employ techniques from analytic number theory to establish upper bounds for class numbers and thereby calculate the precise class number. Such methods, based on Odlyzko's discriminant lower bounds, were employed by Masley [17] and van der Linden [16] to calculate the class numbers of abelian number fields. However, those methods suffered from the drawback that they could only be employed for number fields of small root discriminant, limiting their applicability. A new approach to class number upper bounds that can be applied to number fields of larger root discriminant will be introduced in Chapter 2.

The class number upper bounds will be applied to the calculation of class numbers of cyclotomic fields in Chapter 3. In Chapter 4, we will discuss new results and conjectures regarding the class numbers of fields in cyclotomic $\mathbb{Z}_p$-extensions of the rationals.

Much of the thesis has already been published in a series of four papers [18–21], so I would like to make special mention of some results in this thesis that is not contained in those four papers. In Section 2.4, we compare results from our class number upper bound to the Minkowski bound. Also, in Subsections 3.1.7, 3.1.8 and 3.1.9 we prove (under GRH) that the real cyclotomic fields of conductors 251, 257 and 263 have class number 1.

Chapter 2

Upper bounds for class numbers

To this day, it is not even known if there are infinitely many number fields (degree arbitrary) with class-number one (or even just bounded).
H. M. Stark, *Clay Math Proceedings*, Vol. 7

Although the class number is a fundamental invariant of number fields, the problem of determining the class number is rather difficult for fields of large discriminant. Even cyclotomic fields of relatively small conductor have discriminants too large for their class numbers to be calculated.

The difficulty is that the Minkowski bound

$$M_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d(K)|}$$

is often far too large to be useful. For example, to prove that the real cyclotomic field of conductor 256 has class number 1 using the Minkowski bound, we would need to check that every prime number below the Minkowski bound factors into principal prime ideals, requiring us to check more than 10^{78} primes!

The approach of using Odlyzko's discriminant bounds can handle fields of larger discriminant than using the Minkowski bound, but this technique, as applied by Masley [17] and van der Linden [16], encountered a barrier: Odlyzko's discriminant lower bounds can only establish an upper bound for the class number of a number field of degree n if its *root discriminant*, the nth root of the discriminant, is sufficiently small.

This barrier will be overcome by establishing lower bounds for sums over the prime ideals of the Hilbert class field.

2.1 Upper bounds for class numbers of fields of small root discriminant

In this section we briefly review the theory of root discriminants and the application of Odlyzko's discriminant bounds to find upper bounds for class numbers of totally real fields. Further details can be found in [16], [17] and [23].

Definition 2.1.1. Let K denote a number field of degree n over $\mathbb{Q}$. Let $d(K)$ denote its discriminant. The *root discriminant* $\mathrm{rd}(K)$ of K is defined to be:

$$\mathrm{rd}(K) = |d(K)|^{1/n}.$$

Proposition 2.1.2. *Let L/K be an extension of number fields. Then*

$$\mathrm{rd}(K) \leq \mathrm{rd}(L),$$

with equality if and only if L/K is an unramified at all finite primes, i.e. no prime ideal of K ramifies in L.

Proof. The discriminants of K and L are related by the formula

$$|d(L)| = N(d(L/K))|d(K)|^{[L:K]}$$

where $d(L/K)$ denotes the relative discriminant ideal and N denotes the absolute norm of the ideal, from which the first statement follows. A prime of K ramifies in L if and only if the prime divides the relative discriminant $d(L/K)$. Thus, L/K is unramified if and only if $d(L/K)$ is the unit ideal, proving the second statement. □

Corollary 1. *Let K be a number field. Then the Hilbert class field of K has the same root discriminant as K.*

Odlyzko constructed a tables [24,25] of pairs (A, E) such that a totally real field K of degree n has a lower bound for its discriminant,

$$|d(K)| > A^n e^{-E}.$$

Table [24] is conditional on GRH, and table [25] is unconditional. If we apply Odlyzko's discriminant bounds to the Hilbert class field of K and use the above corollary, we get

$$\log \operatorname{rd}(K) > \log A - \frac{E}{hn}.$$

If $\operatorname{rd}(K) < A$, then we obtain an upper bound for the class number h,

$$h < \frac{E}{n(\log A - \log \operatorname{rd}(K))}. \tag{2.1.1}$$

Thus, we can establish a class number upper bound for fields of small root discriminant.

Example 2.1.3. The maximal real subfield $\mathbb{Q}(\zeta_{212})^+$ of the cyclotomic field of conductor 212 has root discriminant approximately 98.2080. This root discriminant is too large for the class number to be treated by Odlyzko's unconditional discriminant bounds [25], but if we assume the generalized Riemann hypothesis, then we can choose a pair $(A, E) = (119.296, 118.11)$ from Odlyzko's table [24] of GRH conditional discriminant bounds to get an class number upper bound

$$h_{212}^+ \leq 11$$

which is conditional on the generalized Riemann hypothesis.

However, this method, used by Masley and van der Linden, encounters an obstacle if the field has large discriminant. If the root discriminant is larger than the maximum A in Odlyzko's table, the above method can not establish a class number upper bound. The maximum A in Odlyzko's table is 60.704 (or 213.626 under the assumption of the generalized Riemann hypothesis).

2.2 An identity for the class number of a totally real number field

Let F be an Schwarz class function on $\mathbb{R}$ with $F(0) = 1$ and $F(-x) = F(x)$. Let Φ be defined by

$$\Phi(s) = \int_{-\infty}^{\infty} F(x) e^{(s-1/2)x}\, dx.$$

Let K be a number field of degree n with r_1 real embeddings. Poitou's version [27] of Weil's "explicit formula" for the Dedekind zeta function of K states that

$$\begin{aligned}\log d(K) = r_1 \frac{\pi}{2} + n(\gamma + \log 8\pi) - n \int_0^{\infty} \frac{1 - F(x)}{2 \sinh \frac{x}{2}}\, dx \\ - r_1 \int_0^{\infty} \frac{1 - F(x)}{2 \cosh \frac{x}{2}}\, dx - 4 \int_0^{\infty} F(x) \cosh \frac{x}{2}\, dx \\ + \sum_{\rho} \Phi(\rho) + 2 \sum_{\mathfrak{P}} \sum_{m=1}^{\infty} \frac{\log N\mathfrak{P}}{N\mathfrak{P}^{m/2}} F(m \log N\mathfrak{P})\end{aligned}$$

where γ is Euler's constant. The first sum is over the nontrivial zeros of the Dedekind zeta function of K, and the second sum is over the prime ideals of K.

Let K be a totally real field. We can apply the explicit formula to the Hilbert class field $H(K)$ of K. Let h denote the class number of K. Since

$$\log d(H(K)) = hn \log \mathrm{rd}(H(K)) = hn \log \mathrm{rd}(K),$$

we have

$$\begin{aligned}hn \log \mathrm{rd}(K) = hn \left(\frac{\pi}{2} + \gamma + \log 8\pi - \int_0^{\infty} \frac{1 - F(x)}{2} \left(\frac{1}{\sinh \frac{x}{2}} + \frac{1}{\cosh \frac{x}{2}} \right) dx \right) \\ - 4 \int_0^{\infty} F(x) \cosh \frac{x}{2}\, dx + \sum_{\rho} \Phi(\rho) \\ + 2 \sum_{\mathfrak{P}} \sum_{m=1}^{\infty} \frac{\log N\mathfrak{P}}{N\mathfrak{P}^{m/2}} F(m \log N\mathfrak{P})\end{aligned}$$

where the two sums are now over the nontrivial zeros of the Dedekind zeta function of $H(K)$ and the prime ideals of $H(K)$ respectively. We rearrange this to get the identity

$$h = \frac{4\mathcal{H}(F)/n}{C - \mathcal{G}(F) - \log \mathrm{rd}(K) + \frac{1}{hn} \sum_{\rho} \Phi(\rho) + \frac{2}{hn} \sum_{\mathfrak{P}} \sum_{m=1}^{\infty} \frac{\log N\mathfrak{P}}{N\mathfrak{P}^{m/2}} F(m \log N\mathfrak{P})} \tag{2.2.1}$$

where

$$C = \frac{\pi}{2} + \gamma + \log 8\pi,$$

$$\mathcal{G}(F) = \int_0^\infty \frac{1-F(x)}{2}\left(\frac{1}{\sinh\frac{x}{2}} + \frac{1}{\cosh\frac{x}{2}}\right)dx,$$

and

$$\mathcal{H}(F) = \int_0^\infty F(x)\cosh\frac{x}{2}\,dx.$$

Suppose we choose F so that F is nonnegative and so that $\Phi(\rho) \geq 0$ for all nontrivial zeros ρ. If it is true that

$$C - \mathcal{G}(F) - \log \operatorname{rd}(K) > 0$$

then we get the upper bound for the class number,

$$h \leq \frac{4\mathcal{H}(F)}{n}\frac{1}{C - \mathcal{G}(F) - \log \operatorname{rd}(K)}.$$

If we choose F appropriately, we can recover the class number upper bounds (2.1.1) obtained by Odlyzko's discriminant bounds.

2.3 Upper bounds for class numbers of fields of large discriminant

If a number field has root discriminant greater than $4\pi e^{\gamma+1} = 60.839...$ (or greater than $8\pi e^{\gamma+\pi/2} = 215.33...$ if GRH is assumed), then we will have

$$C - \mathcal{G}(F) - \log \operatorname{rd}(K) < 0,$$

so we can not establish a class number upper bound following the approach of the previous section.

However, *if we have further knowledge of the zeros or the prime ideals of the Hilbert class field*, then we may be able establish a nontrivial lower bound for the sums

$$\frac{1}{hn}\sum_{\rho}\Phi(\rho)$$

or

$$\frac{2}{hn}\sum_{\mathfrak{P}}\sum_{m=1}^{\infty}\frac{\log N\mathfrak{P}}{N\mathfrak{P}^{m/2}}F(m\log N\mathfrak{P})$$

that is sufficiently large as to ensure a positive lower bound for the denominator of (2.2.1). Thus we may obtain a class number upper bound for fields with discriminants too large to have been treated by earlier methods. Since it is difficult to make any explicit estimates of the low-lying zeros of the zeta function of the Hilbert class field, we must rely on the contribution of the prime ideals.

In his proof [16] that $\mathbb{Q}(\zeta_{128})^+$ has class number 1, van der Linden used the contribution from the ramified prime above 2 to establish a class number upper bound. Unfortunately, there is only one ramified prime and its contribution in not sufficient for conductors 256 or 512. Fortunately, we can use the many unramified primes.

Suppose a prime integer p totally splits in the field K into principal prime ideals. Since principal ideals totally split in the Hilbert class field, we have hn prime ideals in the Hilbert class field that lie over p, each with a norm of p. Thus for such p we get a contribution to the prime ideal term of the explicit formula

$$\frac{2}{hn}\sum_{\mathfrak{P}|p}\sum_{m=1}^{\infty}\frac{\log N\mathfrak{P}}{N\mathfrak{P}^{m/2}}F(m\log N\mathfrak{P}) = 2\sum_{m=1}^{\infty}\frac{\log p}{p^{m/2}}F(m\log p).$$

The assumption of the generalized Riemann hypothesis now takes on critical importance. Without assuming that the nontrivial zeros lie on the critical line, the function F would have to be chosen so that Φ is nonnegative on the entire critical strip. Thus F would have to be of the form

$$F(x) = \frac{f(x)}{\cosh\frac{x}{2}},$$

with f nonnegative and a nonnegative Fourier transform [23]. Such a condition would force F to decay so rapidly that many prime ideals may be needed contribute significantly to the explicit formula.

If, on the other hand, we assume truth of the generalized Riemann hypothesis, specifically that the nontrivial zeros of the zeta function of the Hilbert class field lie on the critical line $\frac{1}{2}+it$, then F would only required to be nonnegative with nonnegative Fourier transform. For example, F could be chosen to be the Gaussian function,

$$F(x) = e^{-(x/c)^2}$$

for some positive constant c. For large c, this decays less rapidly, allowing for a larger contribution from the prime ideals.

We summarize the above discussion with the following two theorems. If we do not assume the generalized Riemann hypothesis,

Theorem 2.3.1. *Let K be a totally real field of degree n, and let*

$$F(x) = \frac{e^{-(x/c)^2}}{\cosh \frac{x}{2}}$$

for some positive constant c. Suppose S is a subset of the prime integers which totally split into principal prime ideals of K. Let

$$B = \frac{\pi}{2} + \gamma + \log 8\pi - \log \mathrm{rd}(K) - \int_0^\infty \frac{1 - F(x)}{2} \left(\frac{1}{\sinh \frac{x}{2}} + \frac{1}{\cosh \frac{x}{2}} \right) dx$$
$$+ 2 \sum_{p \in S} \sum_{m=1}^{\infty} \frac{\log p}{p^{m/2}} F(m \log p).$$

If $B > 0$ then we have an upper bound for the class number h of K,

$$h < \frac{2c\sqrt{\pi}}{nB}.$$

On the other hand, if we do assume the truth of the generalized Riemann hypothesis, we have the following theorem.

Theorem 2.3.2. *Let K be a totally real field of degree n, and let*

$$F(x) = e^{-(x/c)^2}$$

for some positive constant c. Suppose S is a subset of the prime integers which totally split into principal prime ideals of K. Let

$$B = \frac{\pi}{2} + \gamma + \log 8\pi - \log \mathrm{rd}(K) - \int_0^\infty \frac{1 - F(x)}{2} \left(\frac{1}{\sinh \frac{x}{2}} + \frac{1}{\cosh \frac{x}{2}} \right) dx$$
$$+ 2 \sum_{p \in S} \sum_{m=1}^{\infty} \frac{\log p}{p^{m/2}} F(m \log p).$$

If $B > 0$ then we have, under the generalized Riemann hypothesis, an upper bound for the class number h of K,

$$h < \frac{2c\sqrt{\pi}e^{(c/4)^2}}{nB}.$$

Given an element x of a Galois number field K, we define its *norm* to be

$$N(x) = \left| \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(x) \right|.$$

Note that if x is in the ring of integers of K, and if its norm is a prime integer p which is unramified in K, then p totally splits into principal ideals, and we can take p to be in the set S above. Once we find sufficiently many such prime integers which totally split into principal ideals, we can establish an upper bound for the class number.

2.4 Comparison with the Minkowski bound

Suppose that K is a totally real number field of degree n that we conjecture has class number 1. In order to prove that K has class number 1, for how many totally split primes p must we show that each p totally splits into principal prime ideals? The Minkowski bound, which arises from geometry of numbers considerations, provides one answer: If every prime p less than

$$M_K = \frac{n!}{n^n}\sqrt{|d(K)|}$$

factors into principal prime ideals in K, then K has class number 1.

An alternative approach is to use the class number upper bounds developed in the previous section. Given our field K of conjectural class number 1, we may calculate X such that if all $p \leq X$ factor into principal prime ideals, then Theorem 2.3.1 proves that $h_K < 2$, i.e. $h_K = 1$. Table 2.1 compares the Minkowski bound to the bound X required to show $h_K < 2$ using Theorem 2.3.1. For conductors up to around 1000, our new method substantially improves upon the Minkowski bound. However, it seems to be asymptotically worse than the Minkowski bound, for very large conductors.

If we have additional algebraic information about the field K, we may be able to prove class number 1 with a weaker bound than $h_K < 2$. For example, Schoof [31] gives a table of real cyclotomic fields of prime conductor that have conjectural class number 1. To prove that these fields in fact *do* have class number 1, it suffices to prove

Table 2.1: Comparison of bounds for real cyclotomic fields of prime conductor

Conductor	**Minkowski bound**	$h_K < 2$	$h_K < 80000$
79	2.06×10^{20}	2.90×10^{8}	317
151	2.44×10^{49}	3.61×10^{30}	2.29×10^{9}
251	8.73×10^{95}	1.55×10^{69}	1.62×10^{21}
1009	2.21×10^{538}	1.40×10^{508}	5.99×10^{155}
10007	1.71×10^{7834}	1.78×10^{9059}	1.66×10^{2777}

that their class number is less than 80000. Therefore it is also instructive to compare the Minkowski bound to the bound required to show $h_K < 80000$; such a comparison is given in Table 2.1. In this case, the improvement versus the Minkowski bound is particularly striking, and appears to hold for even very large conductors. We now give a more precise asymptotic analysis.

First, we recall the following version of the prime number theorem for arithmetic progressions.

Theorem 2.4.1. *Under the assumption of the generalized Riemann hypothesis, for* $x > q$

$$\sum_{\substack{p \leq x \\ p \equiv a(q)}} \log p = \frac{x}{\phi(q)} + O\left(x^{1/2}(\log x)^2\right).$$

We derive the following useful corollary:

Corollary 2. *Under the assumption of the generalized Riemann hypothesis, for every* $\alpha > 2$*, there exists a constant* C_α *such that*

$$\sum_{\substack{p \leq x \\ p \equiv a(q)}} \frac{\log p}{p+1} - \frac{\log x}{\phi(q)} \geq -\frac{\alpha \log q + C_\alpha}{\phi(q)},$$

for every $x > 0$*,* $q > 1$ *and* $(a, q) = 1$*.*

Proof. Fix $\alpha > 2$. This inequality is true trivially if $x \leq q^\alpha$, for any $C_\alpha \geq 0$. If $x > q^\alpha$, we proceed by partial summation. Let

$$\vartheta(x, q, a) = \sum_{\substack{p \leq x \\ p \equiv a(q)}} \log p.$$

By the prime number theorem for arithmetic progressions (under GRH) there exists a constant C such that

$$\vartheta(x,q,a) \geq \frac{x}{\phi(q)} - C\left(x^{1/2}(\log x)^2\right)$$

uniformly for all $q > 1$, $x > q$ and $(a,q) = 1$. By partial summation,

$$\sum_{\substack{p\leq x\\ p\equiv a(q)}} \frac{\log p}{p+1} \geq \int_{q^\alpha}^{x} \frac{\vartheta(t,q,a)}{(t+1)^2}dt \geq \frac{1}{\phi(q)}\int_{q^\alpha}^{x} \frac{t}{(t+1)^2}dt - C\int_{q^\alpha}^{\infty}\frac{(\log t)^2}{t^{3/2}}dt$$

$$\geq \frac{\log(x+1)}{\phi(q)} - \frac{\log(q^\alpha+1)}{\phi(q)} - \frac{1}{\phi(q)(q^\alpha+1)} - 2C\frac{\log^2 q^\alpha + 4\log q^\alpha + 8}{q^{\alpha/2}}$$

$$\geq \frac{\log x}{\phi(q)} - \frac{\alpha\log q}{\phi(q)} - \frac{2}{\phi(q)(q^\alpha+1)} - \frac{2C}{\phi(q)}\frac{\alpha^2\log^2 q + 4\alpha\log q + 8}{q^{-1+\alpha/2}}$$

proving the result, since $-1+\alpha/2 > 0$. □

We use this corollary to prove the following proposition.

Proposition 2.4.2. *Under the assumption of the generalized Riemann hypothesis, for every $\alpha > 2$, there exists a constant C_α such that*

$$\sum_{\substack{p\leq x\\ p\equiv a(q)}} \frac{\log p}{p+1}\exp\left(-\left(\frac{\log p}{\beta\log x}\right)^2\right) \geq \frac{\log x}{\phi(q)}\int_0^1 e^{-(u/\beta)^2}du - \frac{\alpha\log q + C_\alpha}{\phi(q)},$$

for every $x > 0$, $q > 1$, $(a,q) = 1$ and $\beta > 0$.

Proof. Let

$$\Phi(x,q,a) = \sum_{\substack{p\leq x\\ p\equiv a(q)}} \frac{\log p}{p+1}.$$

By partial summation,

$$\sum_{\substack{p\leq x\\ p\equiv a(q)}} \frac{\log p}{p+1}\exp\left(-\left(\frac{\log p}{\beta\log x}\right)^2\right) = \Phi(x,q,a)e^{-1/\beta^2} - \int_1^x \Phi(t,q,a)d\exp\left(-\left(\frac{\log t}{\beta\log x}\right)^2\right)$$

$$\geq \Phi(x,q,a)e^{-1/\beta^2} - \int_1^x \frac{\log t}{\phi(q)}d\exp\left(-\left(\frac{\log t}{\beta\log x}\right)^2\right) + \int_1^x \frac{\alpha\log q + C_\alpha}{\phi(q)}d\exp\left(-\left(\frac{\log t}{\beta\log x}\right)^2\right)$$

$$\geq \frac{1}{\phi(q)} \int_1^x \exp\left(-\left(\frac{\log t}{\beta \log x}\right)^2\right) \frac{dt}{t} - \frac{\alpha \log q + C_\alpha}{\phi(q)}$$
$$= \frac{\log x}{\phi(q)} \int_0^1 e^{-(u/\beta)^2} du - \frac{\alpha \log q + C_\alpha}{\phi(q)}.$$

□

The following corollary follows immediately from the proposition.

Corollary 3. *Let K be a totally real abelian number field of degree n and conductor q. Let*

$$F(x,c) = \frac{e^{-(x/c)^2}}{\cosh \frac{x}{2}},$$

and let

$$P(X,c) = 2 \sum_{\substack{p \leq X \\ p \, \text{totally splits}}} \sum_{m=1}^{\infty} \frac{\log p}{p^{m/2}} F(m \log p, c).$$

Then, under the assumption of the generalized Riemann hypothesis, for every $\alpha > 2$, there exists a constant C_α such that

$$P(X, \beta \log X) \geq \frac{4}{n} \left(\log X \int_0^1 e^{-(u/\beta)^2} du - \alpha \log q - C_\alpha \right).$$

Now we define $B(X,c)$ to be

$$B(X,c) = \frac{\pi}{2} + \gamma + \log 8\pi - \log \mathrm{rd}(K) - \int_0^\infty \frac{1 - F(x,c)}{2} \left(\frac{1}{\sinh \frac{x}{2}} + \frac{1}{\cosh \frac{x}{2}} \right) dx + P(X,c).$$

To simplify calculations, we will assume that $c \geq 15$. This is generally true in practice and certainly true asymptotically. Then we have:

$$B(X,c) = A - \log \mathrm{rd}(K) + P(X,c),$$

where A must lie in the narrow range $4.0758 < A < 4.1083$.

Given a fixed $c > 15$, suppose that we want to find X such that, if we show every prime $p < X$ factors into principal ideals, then we will establish a fixed class number upper bound of h_0. In other words, given the relation

$$h_0 = \frac{2c\sqrt{\pi}}{nB(X,c)},$$

we want to solve for X in terms of h_0, c and the invariants of K. We rearrange to get

$$B(X,c) = A - \log \mathrm{rd}(K) + P(X,c) = \frac{2c\sqrt{\pi}}{nh_0}.$$

We further rearrange to get

$$P(X,c) - \frac{2c\sqrt{\pi}}{nh_0} = \log \mathrm{rd}(K) - A.$$

Setting $c = \beta \log X$ and using the above corollary, we get

$$\frac{4}{n}\left(\log X \int_0^1 e^{-(u/\beta)^2} du - \alpha \log q - C_\alpha\right) - \frac{2\beta \log X \sqrt{\pi}}{nh_0} \leq \log \mathrm{rd}(K) - A.$$

We rearrange this to get

$$\log X \left(\int_0^1 e^{-(u/\beta)^2} du - \frac{\beta\sqrt{\pi}}{2h_0}\right) \leq \frac{1}{4}\log|d(K)| - \frac{nA}{4} + \alpha \log q + C_\alpha.$$

Now we choose our free parameter β to minimize our bound for X. This gives us the following:

$$\log X \leq \frac{1}{4M}\log|d(K)| - \frac{nA}{4M} + \frac{\alpha \log q + C_\alpha}{M}$$

where

$$M = \sup_{\beta>0}\left(\int_0^1 e^{-(u/\beta)^2} du - \frac{\beta\sqrt{\pi}}{2h_0}\right).$$

One remarkable consequence of this estimate is that the parameter β only depends on the desired class number bound h_0, and does not depend on the number field at all!

Example 2.4.3. If we desire a class number upper bound of $h_K < 2$ (in order to prove class number 1 without further algebraic argument), then we find that

$$M = \sup_{\beta>0}\left(\int_0^1 e^{-(u/\beta)^2} du - \frac{\beta\sqrt{\pi}}{2\cdot 2}\right) \approx 0.3064.$$

Thus we get

$$\log X \leq \frac{1}{1.2256}\log|d(K)| - \frac{nA}{1.2256} + \frac{\alpha \log q + C_\alpha}{0.3064}$$

which we can now see is asymptotically worse than the Minkowski bound

$$\log M_K = \frac{1}{2}\log|d(K)| + \log(n!) - n\log n = \frac{1}{2}\log|d(K)| - n + O(\ln n)$$

as the discriminant gets large.

Example 2.4.4. Suppose we are considering the real cyclotomic fields of prime conductor that are conjecturally class number 1 according to Schoof's table [31]. Then we need only establish a class number upper bound of $h_K < 80000$ in order to show that K has class number 1. In this case,

$$M = \sup_{\beta > 0} \left(\int_0^1 e^{-(u/\beta)^2} du - \frac{\beta\sqrt{\pi}}{2 \cdot 2} \right) \approx 0.9993.$$

Thus we get

$$\log X \leq \frac{1}{3.9972} \log |d(K)| - \frac{nA}{3.9972} + \frac{\alpha \log q + C_\alpha}{0.9993}$$

which is asymptotically better than the Minkowski bound as the discriminant gets large.

Chapter 3

Class numbers of cyclotomic fields

> *Mais si λ est plus grand, le calcul effectif de ce second facteur est tres pénible, parc qu'il exige qu'on recherche d'abord un système d'unités fondamentales.*
>
> E. E. Kummer, *J. Math. Pures Appl.* **16** (1851)

Ever since mathematicians more than a century ago established connections between Fermat's Last Theorem and the unique factorization properties of cyclotomic integers, the class numbers of cyclotomic fields have been investigated intensively. Among the most mysterious aspects remains the "plus part" of the class number, i.e. the class number of the maximal real subfield.

Recall that the class number h_m of a cyclotomic field $\mathbb{Q}(\zeta_m)$ of conductor m can be decomposed into the "plus part" and the "minus part"

$$h_m = h_m^+ h_m^-.$$

The "plus part" (or "second factor") h_m^+ is defined to be the class number of its maximal real subfield $\mathbb{Q}(\zeta_m)^+$, where

$$\mathbb{Q}(\zeta_m)^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1}) = \mathbb{Q}(2\cos(2\pi/m)).$$

The "minus part" (or "first factor" or "relative class number") h_m^-, also known as the relative class number, is defined to be the ratio

$$h_m^- = \frac{h_m}{h_m^+}.$$

So far this is just a tautology, but what is not tautological is to observe that the minus part h_m^- can be calculated quite explicitly, using the class number formula. Applying the class number formula both to the full cyclotomic field $\mathbb{Q}(\zeta_m)$ and its real subfield

$\mathbb{Q}(\zeta_m)^+$ and then taking the quotient, but difficult to handle terms such as the regulator cancel out, and we are left with the formula,

$$h_m^- = Qm \prod_{\chi \,\mathrm{odd}} \left(-\frac{1}{2} B_{1,\chi} \right),$$

where the product runs over the odd Dirichlet characters χ of conductor m. Here the $B_{1,\chi}$ are the generalized Bernoulli numbers and $Q = 1$ if m is a prime power and $Q = 2$ otherwise. Although the minus part h_m^- grows exponentially with the conductor m, the minus part can be calculated explicitly. Washington [34] provides a table of minus parts for all m with $\phi(m) \leq 256$, where ϕ is the Euler totient function.

The plus part, on the other hand, remains quite mysterious. For fields of larger conductor, their Minkowski bounds are far too large to be useful, and their discriminants are too large for their class numbers to be treated by Odlyzko's discriminant bounds.

3.1 Cyclotomic fields of prime conductor

Surprisingly, for cyclotomic fields of prime conductor, the plus part of the class number has only been determined up to conductor 67, and no further cyclotomic fields of prime conductor have had their class numbers determined unconditionally since the results of Masley [17] more than three decades ago.

The results of this thesis have improved the situation. Using the class number upper bounds introduced in Chapter 2, we obtain the following result.

Theorem 3.1.1. *Let p be a prime integer, and let $\mathbb{Q}(\zeta_p)^+$ denote the maximal real subfield of the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$. Then the class number of $\mathbb{Q}(\zeta_p)^+$ is 1 for $p \leq 151$.*

Furthermore, under the assumption of the generalized Riemann hypothesis, the class *number* h_p^+ *of* $\mathbb{Q}(\zeta_p)^+$ *is*

$$h_p^+ = \begin{cases} 1 & \text{if } p \leq 263 \text{ and } p \neq 163, 191, 229 \text{ and } 257, \\ 4 & \text{if } p = 163, \\ 11 & \text{if } p = 191, \\ 3 & \text{if } p = 229 \text{ or } 257. \end{cases}$$

3.1.1 Upper bounds for class numbers beyond Odlyzko's discriminant bounds

As discussed in Chapter 2, once we find sufficiently many integral elements of prime norm, we can establish an upper bound for the class number. Once an upper bound is established, we may use various "push up" and "push down" lemmas to pin down the exact class number. However, for prime conductors our preference will be to appeal to the results of Schoof [31]. Real cyclotomic fields of prime power conductor have the special property that the index of the group of cyclotomic units $\mathcal{O}_{\text{cyc}}^\times$ within the full group of units $\mathcal{O}^\times$ is equal to the class number. This allowed Schoof to study the Galois action on the quotient group $\mathcal{O}^\times/\mathcal{O}_{\text{cyc}}^\times$, rather than class group itself, to extract information about the class number. In his "Main Table," for each prime conductor p less than $10,000$, he gives a number $\tilde{h}_p$ such that the class number h_p^+ either equals $\tilde{h}_p$, or $h_p^+ > 80000 \cdot \tilde{h}_p$. In particular, if our upper bound for h_p^+ is less than 80000, then we have $h_p^+ = \tilde{h}_p$.

We recall a few facts about real cyclotomic fields of prime conductor. Let p be a prime integer, and let $\mathbb{Q}(\zeta_p)^+$ denote the pth real cyclotomic field, i.e. the maximal real subfield of the cyclotomic field $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive pth root of unity. The degree n of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is $n = (p-1)/2$, and its discriminant is given by

$$d(\mathbb{Q}(\zeta_p)^+) = p^{\frac{1}{2}(p-3)}.$$

Thus, its root discriminant is

$$\text{rd}(\mathbb{Q}(\zeta_p)^+) = p^{\frac{p-3}{p-1}}.$$

The prime integers which totally split in this field are precisely those which are congruent to ±1 modulo p.

The ring of integers of $\mathbb{Q}(\zeta_p)^+$ is

$$\mathbb{Z}[\zeta_p + \zeta_p^{-1}] = \mathbb{Z}[2\cos(2\pi/p)].$$

Until otherwise noted, the integral basis that we will use is $\{b_0, b_1, \ldots, b_{n-1}\}$, with $b_0 = 1$ and $b_j = 2\cos(2\pi j/p)$ for $j = 1, \ldots, n-1$.

3.1.2 The class number of $\mathbb{Q}(\zeta_p)^+$ for primes $p = 71, 73, 79, 83$

For $p = 71$, the root discriminant is approximately 62.85, which too large for the Odlyzko bounds to be useful. Our goal is to find to sufficiently many algebraic integers x in $\mathbb{Q}(\zeta_{71})^+$ such that its norm $N(x)$ is a prime integer congruent to ±1 modulo p, and then apply Theorem 2.3.1.

Lemma 3.1.2. *In the real cyclotomic field $\mathbb{Q}(\zeta_{71})^+$, there exist algebraic integers of norms* 283*,* 569*,* 709*,* 853*,* 1277*,* 1279*,* 1847*,* 1987*,* 2129*, and* 2131*, i.e. the ten smallest prime integers that are congruent to* ±1 *modulo* 71*.*

Proof. Let $b_0 = 1$ and $b_j = 2\cos(2\pi j/71)$ for j from 1 to 34. Then $\{b_0, b_1, \ldots, b_{34}\}$ is an integral basis of $\mathbb{Q}(\zeta_{71} + \zeta_{71}^{-1})$. We search over "sparse vectors," where almost all the coefficients are zero, and the remaining coefficients are ±1. We find the following ten elements and their norms:

Element	Norm
$b_0 + b_1 - b_6$	283
$b_0 + b_1 + b_8$	569
$b_0 + b_1 + b_4 - b_{22}$	709
$b_0 + b_1 - b_5$	853
$b_0 + b_1 + b_3 + b_{12}$	1277
$b_0 + b_1 - b_8 - b_{13}$	1279
$b_0 + b_1 + b_2 - b_{28}$	1847
$b_0 + b_1 - b_{13}$	1987
$b_0 + b_1 - b_3 + b_{10}$	2129
$b_0 + b_1 - b_{27}$	2131

□

Proposition 3.1.3. *The class number of* $\mathbb{Q}(\zeta_{71})^+$ *is* 1.

Proof. Let F be the function

$$F(x) = \frac{e^{-(x/c)^2}}{\cosh\frac{x}{2}}$$

with $c = 15$. We have the following lower found for the contribution of prime ideals,

$$2\sum_{p\in S}\sum_{m=1}^{\infty}\frac{\log p}{p^{m/2}}F(m\log p) > 2\sum_{p\in S}\frac{\log p}{\sqrt{p}}F(\log p) > 0.2448.$$

The following integral can be calculated using numerical integration:

$$\int_0^{\infty}\frac{1-F(x)}{2}\left(\frac{1}{\sinh\frac{x}{2}}+\frac{1}{\cosh\frac{x}{2}}\right)dx < 1.2964.$$

We have

$$B = \frac{\pi}{2}+\gamma+\log 8\pi-\log \mathrm{rd}(K)-\int_0^{\infty}\frac{1-F(x)}{2}\left(\frac{1}{\sinh\frac{x}{2}}+\frac{1}{\cosh\frac{x}{2}}\right)dx$$
$$+2\sum_{p\in S}\sum_{m=1}^{\infty}\frac{\log p}{p^{m/2}}F(m\log p) > 0.1796.$$

By Theorem 2.3.1, the class number is less than 9. Applying Schoof's table [31], or using more elementary algebraic arguments, we find that the class number is 1. □

The proofs for conductors 73, 79 and 83 are entirely similar. It is straightforward to find algebraic integers with the 10 smallest prime norms congruent to ±1 modulo p. This is sufficient to get an upper bound less than 80000. Using Schoof's table, we find that each has class number 1.

3.1.3 The class number of $\mathbb{Q}(\zeta_p)^+$, prime p, $89 \le p \le 131$

We first consider the conductor 131. The root discriminant of $\mathbb{Q}(\zeta_{131})^+$ is approximately 121.53. Quite a few prime ideals will be required in order to have a sufficiently large contribution to establish an upper bound for the class number.

Proposition 3.1.4. *The class number of* $\mathbb{Q}(\zeta_{131})^+$ *is* 1.

Proof. Let n denote the degree of the field. We calculate the norm of every element of the form

$$x = b_0 + b_1 + a_1 b_{j_1} + a_2 b_{j_2} + a_3 b_{j_3} + a_4 b_{j_4} + a_5 b_{j_5} + a_6 b_{j_6},$$

where $1 < j_1 < j_2 < j_3 < j_4 < j_5 < j_6 < n$ and $a_j \in \{-1, 0, 1\}$ for $1 \leq j \leq 6$. By searching these sparse vectors x and calculating their norms, we find 12,087 prime integers that are less than 20,000,000 and congruent to ±1 modulo 131.

Let S be the set of those 12,087 primes, and let

$$F(x) = \frac{e^{-(x/c)^2}}{\cosh \frac{x}{2}}$$

with $c = 1000$. We have the following lower found for the contribution of prime ideals,

$$2 \sum_{p \in S} \sum_{m=1}^{\infty} \frac{\log p}{p^{m/2}} F(m \log p) > 2 \sum_{p \in S} \sum_{m=1}^{2} \frac{\log p}{p^{m/2}} F(m \log p) > 0.708.$$

By numerical integration, we have

$$\int_0^{\infty} \frac{1 - F(x)}{2} \left(\frac{1}{\sinh \frac{x}{2}} + \frac{1}{\cosh \frac{x}{2}} \right) dx < 1.264.$$

We have $B > 0.015$, so by applying Theorem 2.3.1 we find that the class number is less than 3636. We can now use Schoof's table to find that the class number is 1. □

The proof for prime conductors between 89 and 127 is entirely similar, and we find that all have class number 1.

3.1.4 The class number of $\mathbb{Q}(\zeta_p)^+$ for primes $p = 137, 139, 149, 151$

As the root discriminant of the fields increases, so does the required contribution from the prime ideals. To find sufficiently many split primes in fields of larger discriminant, it is often quicker to additionally search over sparse vectors using an alternative basis. A useful alternative to the basis $b_0, b_1, \ldots, b_{n-1}$ is

$$c_k = \sum_{j=0}^{k} b_j, \quad k = 0, 1, \ldots, n-1.$$

Proposition 3.1.5. *The class number of* $\mathbb{Q}(\zeta_{151})^+$ *is* 1.

Proof. Let n denote the degree of the field, and let $\mathcal{O}$ denote the ring of integers.

We first consider all $x \in \mathcal{O}$ of the forms

$$x = b_0 + b_1 + a_1 b_{j_1} + a_2 b_{j_2} + a_3 b_{j_3} + a_4 b_{j_4} + a_5 b_{j_5} + a_6 b_{j_6},$$

and

$$x = b_1 + a_1 b_{j_1} + a_2 b_{j_2} + a_3 b_{j_3} + a_4 b_{j_4} + a_5 b_{j_5} + a_6 b_{j_6},$$

where $1 < j_1 < j_2 < j_3 < j_4 < j_5 < j_6 < n$ and $a_j \in \{-1, 0, 1\}$ for $1 \leq j \leq 6$.

We also search over the alternative basis,

$$x = c_0 + a_1 c_{k_1} + a_2 c_{k_2} + a_3 c_{k_3} + a_4 c_{k_4} + c_5 b_{k_5} + c_6 b_{k_6},$$

where $1 \leq k_1 < k_2 < k_3 < k_4 < k_5 < k_6 < n$ and $a_k \in \{-1, 0, 1\}$ for $1 \leq k \leq 6$.

Let T denote the set of all such elements x.

The ideal (151) is totally ramified. Thus, if $x \in \mathcal{O}$ has norm $N(x)$ divisible by 151, we can divide x by any element of norm 151, say $2b_0 - b_1$, to get an algebraic integer $(2b_0 - b_1)^{-1}x$ with norm $N(x)/151$. Therefore consider the non-151 parts of all norms $N(x)$. Initially we search these sparse vectors to find norms which are less than 10^{15} and congruent to ±1 modulo 151. We define the set U to be

$$U = \{\text{non-151 part of } N(x) | x \in T, N(x) < 10^{15}\}.$$

Let S_1 be the set of primes

$$S_1 = \{m : m \in U, m \text{ prime}, m \equiv \pm 1 \pmod{151}\}.$$

Unfortunately, we find that primes of S_1 make an insufficient contribution. We could attempt to search over sparse vectors with more nonzero coefficients, but this is very time consuming. Instead we find elements of larger norm, and take quotients, as will be described below.

Let S_2 be the set of primes defined by

$$S_2 = \{p : pq \in U, p \text{ prime}, p \notin S_1, q \in S_1\},$$

noting that if $N(x) = pq$ and $N(y) = q$, for $x, y \in \mathcal{O}$, then $x/\sigma(y)$ is in $\mathcal{O}$ with norm p for some Galois automorphism σ. Now put $S = S_1 \cup S_2$ and $c = 115$. We have the following lower found for the contribution of prime ideals,

$$2\sum_{p\in S}\sum_{m=1}^{\infty}\frac{\log p}{p^{m/2}}F(m\log p) > 2\sum_{p\in S}\sum_{m=1}^{2}\frac{\log p}{p^{m/2}}F(m\log p) > 0.8745.$$

Applying Theorem 2.3.1, we have $B > 0.0316$, so the class number is less than 171. We can now use Schoof's table to find the class number is 1. □

The proofs for conductors 137, 139 and 149 are entirely similar. We determine that all have class number 1, and have proved the first statement of Theorem 3.1.1.

3.1.5 The class number of $\mathbb{Q}(\zeta_p)^+$ for primes p, $167 \leq p \leq 193$

For prime conductors greater than 151, we will assume the generalized Riemann hypothesis. Using Odlyzko's discriminant bounds, van der Linden proved (under GRH) that the class number of $\mathbb{Q}(\zeta_p)^+$ is 1 for $p < 163$ and is 4 for $p = 163$ [16].

Although the question of the class number of $\mathbb{Q}(\zeta_{167})^+$ has remained open, we can find its class number as a direct consequence of Schoof's results [31]. Indeed, the root discriminant of $\mathbb{Q}(\zeta_{167})^+$ is only 162.93..., so it is small enough for Odlyzko's discriminant bounds to establish an upper bound for the class number, without any recourse to knowledge of the prime ideals. Choosing the pair $(A, E) = (170.633, 4790.3)$

from Odlyzko's table "Table 3: GRH Bounds for Discriminants" [24], we get an upper bound for the class number h_{167}^{+},

$$h_{167}^{+} < \frac{E}{n\,(\log A - \log \mathrm{rd}(\mathbb{Q}(\zeta_{167})^{+}))} < 1208.$$

Since $h < 80000$, we can use Schoof's table to prove $h_{167}^{+} = 1$ for $\mathbb{Q}(\zeta_{167})^{+}$.

Entirely similarly, we can use the Odlyzko GRH bounds together with Schoof's table to determine the class numbers of prime conductor between 173 and 193, all of which are 1 except for $\mathbb{Q}(\zeta_{191})^{+}$ which has class number 11.

3.1.6 The class number of $\mathbb{Q}(\zeta_p)^+$ for primes p, $197 \leq p \leq 241$

The root discriminant of $\mathbb{Q}(\zeta_{197})^{+}$ is only 186.66..., so we can also apply Odlyzko's GRH bounds here to get an upper bound of $h < 152927$. Unfortunately, this bound is not less than 80000, so we are not yet able use Schoof's table. To get a better upper bound for h, we will study the prime ideals of the field and apply Theorem 2.3.2.

Proposition 3.1.6. *Under the generalized Riemann hypothesis, the class number of* $\mathbb{Q}(\zeta_{197})^{+}$ *is* 1.

Proof. Searching for an algebraic integer with small prime norm congruent to ±1 modulo 197, we find the element

$$b_0 + b_1 + b_2 - b_{10} + b_{33} - b_{70} - b_{83}$$

which has norm 1181.

Assuming the generalized Riemann hypothesis, we apply Theorem 2.3.2 using $S = \{1181\}$ and $c = 9.25$ to prove that the class number is less than 1027. Now we use Schoof's table to find that the class number is 1. □

Proposition 3.1.7. *Under the generalized Riemann hypothesis, the class number of* $\mathbb{Q}(\zeta_{199})^{+}$ *is* 1.

Proof. As in the proof of the previous proposition, we find two algebraic integers of small prime norm congruent to ±1 modulo 199:

$$N(b_0 + b_1 - b_{14} - b_{23} + b_{59} - b_{77}) = 29453,$$

and

$$N(b_0 + b_1 + b_6 - b_{35} + b_{54} - b_{56} - b_{96}) = 26267.$$

We apply Theorem 2.3.2 using $S = \{26267, 29453\}$ and $c = 11.5$ to show that the class number is less than 47719, and use Schoof's table to prove that the class number is 1. □

Proposition 3.1.8. *Under the generalized Riemann hypothesis, the class number of* $\mathbb{Q}(\zeta_{211})^+$ *is* 1.

Proof. We find an algebraic integer of small prime norm congruent to ±1 modulo 211:

$$N(b_0 + b_1 - b_8 - b_{60} + b_{64} + b_{67}) = 2111.$$

We apply Theorem 2.3.2 using $S = \{2111\}$ and $c = 10.75$ to get that the class number is less than 13476, and use Schoof's table to find the class number is 1. □

For fields of larger discriminant, it is more difficult to find split primes of small norm. Often the quickest approach is to additionally search over sparse vectors using a different basis, and then take quotients of appropriately chosen algebraic integers. We use the alternative basis

$$c_k = \sum_{j=0}^{k} b_j, \quad k = 0, 1, \ldots, n-1$$

given earlier. This approach is used in the proof of the following proposition.

Proposition 3.1.9. *Under the generalized Riemann hypothesis, the class number of* $\mathbb{Q}(\zeta_{223})^+$ *is* 1.

Proof. Searching over the alternative basis (c_k), we find the algebraic integer

$$\alpha = c_0 - c_6 - c_{26} - c_{77} + c_{99}$$

which has norm $6689 \cdot 42284369$. Searching over the usual basis (b_j), we find

$$\beta = b_1 + b_{11} + b_{30} + b_{95}$$

which has norm 42284369. For some Galois automorphism σ, the quotient $\gamma = \sigma(\alpha)\beta$ is an algebraic integer of norm 6689. We also can find the algebraic integer

$$\delta = c_0 + c_6 - c_{11} - c_{15} + c_{25}$$

which has norm $2677 \cdot 6689$. Taking quotients again using a (possibly different) Galois automorphism σ, we can find an algebraic integer $\sigma(\delta)/\gamma$ of norm 2677. Letting $S = \{2677, 6689\}$ and $c = 10.5$, we can apply Theorem 2.3.2 to find that the class number is less than 6762, and we use Schoof's table [31] to find the class number is 1. □

Proposition 3.1.10. *Under the generalized Riemann hypothesis, the class number of* $\mathbb{Q}(\zeta_{227})^+$ *is* 1.

Proof. Searching over sparse vectors, using our two bases (b_j) and (c_k), we find the following elements and their norms:

Element	Norm
$b_0 + b_1 - b_{21} + b_{75} - b_{96} - b_{112}$	4053311
$c_0 + c_4 + c_{35} - c_{56} + c_{83}$	$4053311 \cdot 7717$
$c_0 + c_{40} + c_{68} + c_{77} + c_{83}$	$7717 \cdot 20431$
$b_1 - b_{12} - b_{41} - b_{53}$	$20431 \cdot 1361$

By successively taking quotients by the appropriate Galois conjugates, we can find algebraic integers of norms 7717, 20431 and 1361.

Setting $S = \{1361, 7717, 20431\}$ and $c = 9.75$, we apply Theorem 2.3.2 to get a class number upper bound of 1431. Using Schoof's table, we find the class number is 1. □

Proposition 3.1.11. *Under the generalized Riemann hypothesis, the class number of* $\mathbb{Q}(\zeta_{229})^+$ *is* 3.

Proof. Searching over sparse vectors, using our two bases (b_j) and (c_k), we find the following elements and their norms:

Element	Norm
$c_0 - c_4 - c_{10} - c_{41} + c_{106} + c_{112}$	4887317
$b_1 - b_6 + b_{54} + b_{107}$	$4887317 \cdot 2699453$
$c_0 + c_{10} + c_{53} + c_{71} - c_{79} + c_{87}$	$2699453 \cdot 49463$
$c_0 - c_{13} + c_{14} - c_{63} - c_{77} + c_{79}$	$49463 \cdot 207017$
$b_0 + b_1 - b_2 - b_{16} - b_{72} + b_{88}$	$207017 \cdot 43051$
$c_0 - c_3 - c_{41} - c_{45} + c_{67}$	$43051 \cdot 6871$
$c_0 - c_4 - c_{41} + c_{53} + c_{96}$	$6871 \cdot 2749$

By successively taking quotients by the appropriate Galois conjugates, we can find algebraic integers of norms 6871 and 2749.

Setting $S = \{2749, 6871\}$ and $c = 11$, we apply Theorem 2.3.2 to show a class number upper bound of 12734. Using Schoof's table, we prove the class number is 3. □

Proposition 3.1.12. *Under the generalized Riemann hypothesis, the class number of* $\mathbb{Q}(\zeta_{233})^+$ *is* 1.

Proof. Searching over sparse vectors, using our two bases (b_j) and (c_k), we find the following elements and their norms:

Element	Norm
$b_0 + b_1 + b_{14} + b_{69}$	53591
$b_1 + b_6 - b_{21} + b_{77} - b_{114}$	$53591 \cdot 76423$
$b_0 + b_1 - b_8 - b_{40} + b_{47} - b_{86}$	$76423 \cdot 174749$
$b_0 + b_1 + b_{20} + b_{95}$	$174749 \cdot 467$

By successively taking quotients by the appropriate Galois conjugates, we can find algebraic integers of norm 467.

Setting $S = \{467\}$ and $c = 9.5$, we apply Theorem 2.3.2 to find a class number upper bound of 1450. Using Schoof's table, we prove the class number is 1. □

Proposition 3.1.13. *Under the generalized Riemann hypothesis, the class number of* $\mathbb{Q}(\zeta_{239})^+$ *is* 1.

Proof. Searching over sparse vectors, using our two bases (b_j) and (c_k), we find the following elements and their norms:

Element	Norm
$b_0 + b_1 - b_{10} - b_{18} - b_{106} - b_{107} + b_{116}$	4423479397
$b_1 - b_2 - b_{33} - b_{60} + b_{83} - b_{84}$	$4423479397 \cdot 2389$
$b_0 + b_1 + b_{22} - b_{46}$	$2389 \cdot 271981$
$c_0 - c_{11} + c_{21} - c_{93} + c_{104}$	$271981 \cdot 10993$

By successively taking quotients by the appropriate Galois conjugates, we can find algebraic integers of norms 2389, 271981 and 10993.

Setting $S = \{2389, 10993, 271981\}$ and $c = 11.5$, we apply Theorem 2.3.2 to establish a class number upper bound of 32486. Using Schoof's table, we find the class number is 1. □

Proposition 3.1.14. *Under the generalized Riemann hypothesis, the class number of* $\mathbb{Q}(\zeta_{241})^+$ *is* 1.

Proof. Searching over sparse vectors, using our two bases (b_j) and (c_k), we find the following elements and their norms:

Element	Non-241 part of norm
$b_0 + b_1 - b_{37} - b_{52} - b_{118}$	5926189
$c_0 + c_8 - c_{12} + c_{43} - c_{47} + c_{99}$	$5926189 \cdot 87487819$
$b_0 + b_1 + b_{10} + b_{11} + b_{49} + b_{56} - b_{117}$	$87487819 \cdot 47237$
$c_0 - c_6 - c_{63} - c_{67} + c_{68}$	$47237 \cdot 12049$
$b_1 - b_2 + b_3 - b_{17} - b_{44} + b_{61}$	$12049 \cdot 68927$
$c_0 - c_{15} + c_{46} - c_{65} + c_{66}$	$68927 \cdot 56393$
$c_0 + c_3 + c_{42} + c_{53} + c_{95} + c_{100}$	$56393 \cdot 5783$
$b_1 + b_2 + b_{61} + b_{76} - b_{104}$	$5783 \cdot 1447$

Note that although the norm of $b_1 - b_2 + b_3 - b_{17} - b_{44} + b_{61}$ is actually $12049 \cdot 68927 \cdot 241$, we can divide by any element of norm 241, such as $2b_0 - b_1$, to get an algebraic integer of norm $12049 \cdot 68927$.

By successively taking quotients by the appropriate Galois conjugates, we can find algebraic integers of norms 12049, 5783 and 1447.

Setting $S = \{1447, 5783, 12049\}$ and $c = 10$, we apply Theorem 2.3.2 to show a class number upper bound of 2153. Using Schoof's table [31], we prove the class number is 1. □

3.1.7 The class number of $\mathbb{Q}(\zeta_{251})^+$

Proposition 3.1.15. *Under the generalized Riemann hypothesis, the class number of* $\mathbb{Q}(\zeta_{251})^+$ *is* 1.

Proof. Unlike the previous cases, a brute force search for elements of small prime norm, or a chain of almost primes, does not seem to easily yield sufficiently many elements. We must apply a more subtle approach. Searching over sparse vectors, using our two bases (b_j) and (c_k), we find the following integral elements α, β, γ and their norms:

Element	Norm
$\alpha = b_1 - b_7 + b_{65} - b_{71} - b_{78} + b_{100}$	$251 \cdot 503 \cdot 242467$
$\beta = c_0 + c_3 - c_{13} - c_{25} - c_{61} + c_{81} + c_{84}$	$503 \cdot 23593$
$\gamma = b_1 - b_2 - b_9 - b_{49} + b_{66} - b_{69} + b_{77}$	$23593 \cdot 242467$

Since the prime over 251 is totally ramified, we can divide α by $2b_0 - b_1$, which has norm 251, to get an integral element

$$\delta = \frac{\alpha}{2b_0 - b_1}$$

with norm $503 \cdot 242467$.

Now we can twist β and δ by the Galois action until it is divisible by γ. In other words, for each σ_1, σ_2 in $\mathrm{Gal}(\mathbb{Q}(\zeta_{251})^+/\mathbb{Q})$, we check the quotient

$$\eta = \frac{\beta^{\sigma_1}\delta^{\sigma_2}}{\gamma}$$

until we find a pair σ_1, σ_2 that yields an element η in the ring of integers of $\mathbb{Q}(\zeta_{251})^+$, which will necessarily have norm 503^2. Therefore the principal ideal generated by η factors as

$$(\eta) = PP^\tau$$

for some prime ideal P of norm 503 and some τ in $\mathrm{Gal}(\mathbb{Q}(\zeta_{251})^+/\mathbb{Q})$. From here it is not difficult to argue abstractly that P must be a principal ideal. However, we prefer here to proceed explicitly to find an actual generator for P.

The idea is as follows. Suppose that τ generates the entire Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{251})^+/\mathbb{Q})$, which is cyclic of order 125. Since the ideal generated by 503 totally splits, it would factor as:

$$(503) = PP^\tau P^{\tau^2} \cdots P^{\tau^{124}}.$$

Therefore the element

$$\frac{503}{\eta^\tau \eta^{\tau^3} \eta^{\tau^5} \cdots \eta^{\tau^{123}}}$$

would be an integral element that generates the prime ideal P of norm 503. However, when we check the quotient

$$\frac{503}{\eta^\sigma \eta^{\sigma^3} \eta^{\sigma^5} \cdots \eta^{\sigma^{123}}}$$

for each σ that generates $\mathrm{Gal}(\mathbb{Q}(\zeta_{251})^+/\mathbb{Q})$, we never get an integral element. Thus we conclude that τ can not generate the entire Galois group.

Proceeding similarly, we now assume that τ generates the index 5 subgroup of the Galois group. We can easily search in the quintic subfield for an element of norm

503 and lift it to an element λ in $\mathbb{Q}(\zeta_{251})^+$ of norm 503^{25}. In fact, using the basis $b_0, b_1, \ldots, b_{124}$, the element λ is

$\lambda = [15, 0, 0, 4, 0, 0, 4, 2, 0, 4, 0, 4, 4, 4, 2, 4, 0, 2, 4, 2, 0, 2, 4, 2, 4, 0, 4, 2, 2, 2, 4, 4, 0, 4, 2, 2, 4, 4, 2, 2, 0, 2,$
$2, 4, 4, 4, 2, 0, 4, 4, 0, 0, 4, 2, 2, 4, 2, 2, 2, 4, 4, 2, 4, 0, 0, 4, 4, 2, 2, 0, 2, 4, 4, 2, 4, 4, 2, 2, 2, 4, 0, 2, 2, 2, 2, 2,$
$4, 2, 4, 2, 4, 0, 2, 4, 0, 2, 4, 2, 4, 2, 0, 4, 0, 4, 4, 2, 2, 4, 2, 4, 4, 2, 2, 0, 2, 2, 2, 2, 4, 4, 4, 4, 2, 0, 4].$

Now assuming that τ generates the index 5 subgroup of the Galois group, then the ideal generated by λ factors as

$$(\lambda) = PP^{\tau}P^{\tau^2} \cdots P^{\tau^{24}}$$

and the quotient

$$\frac{\lambda}{\eta^{\tau}\eta^{\tau^3}\eta^{\tau^5}\cdots\eta^{\tau^{23}}}$$

would be an integral element that generates the prime ideal P of norm 503. Indeed, we check the quotient

$$\theta = \frac{\lambda}{\eta^{\sigma}\eta^{\sigma^3}\eta^{\sigma^5}\cdots\eta^{\sigma^{23}}}$$

for every σ that generates the index 5 subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_{251})^+/\mathbb{Q})$, and we do find such a σ that produces a quotient θ which is integral. Explicitly, using the basis $b_0, b_1, \ldots, b_{124}$, we find θ to be

$\theta = [29525608, 43553782, 54974405, 56758423, 22817830, 3665682, 27831104, 19279490, 21218318, -2806749, -22243683,$
$20248512, 24979411, 22270503, 13310103, 13980496, 42339501, 58097905, 52307380, 23800535, 45747322, 56983451, 50586512,$
$43520016, -3222986, 14213830, 30756307, 18770862, 10733689, -15326037, 2901922, 20991200, 24999724, 7943313, 12753694,$
$44440883, 52132909, 63675840, 28580934, 21643473, 58900838, 51500518, 50509614, 21983827, 4744116, 23512990, 21685403,$
$4880618, -13493327, 5214120, 20538934, 30286173, 19085108, -7502983, 29547177, 52528414, 58132760, 56167623, 23524185,$
$44674300, 54805868, 42003040, 25057614, 11894497, 25575933, 27903173, 19072870, -19256464, -14489922, 20438942,$
$21708086, 36960123, 7038865, 9557849, 49923836, 49197318, 51528625, 35018615, 42970510, 55900254, 54300085, 27671065,$
$145857, 24507518, 25628130, 27145403, 4561988, -27496147, 10045624, 20712414, 26250716, 21404521, 9275422, 37163356,$
$54965798, 50501403, 30082338, 41988513, 56539005, 54200482, 47239715, -714414, 6502707, 33897859, 22338937, 19422824,$
$-13376824, -10601439, 17875588, 22462536, 17899396, 14250075, 38431915, 50357625, 56335074, 32582673, 17402561,$
$59986501, 58443554, 57097257, 28134026, -8283917, 19123511, 21699008, 14563903].$

Moreoever, it can be explicitly verified that this element θ has norm 503. Setting $S = \{503\}$ and $c = 10.5$, we apply Theorem 2.3.2 to show a class number upper bound of 6998. Using Schoof's table [31], this proves that the class number is 1.

□

3.1.8 The class number of $\mathbb{Q}(\zeta_{257})^+$

First, we introduce a useful lemma for cyclic number fields that have 2-power degree.

Lemma 3.1.16. *Let K be a cyclic number field of degree 2^k, and let p be a prime number that totally splits in K. Suppose there exist elements α and β in the ring of integers $\mathcal{O}_K$ such that*

$$|N_{K/\mathbb{Q}}(\alpha)| = |N_{K/\mathbb{Q}}(\beta)| = p^2$$

and such that β/α^σ is not a unit of $\mathcal{O}_K$, for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Suppose further that β lies in the index 2 subfield of K. Then for any prime ideal P of K lying above p, the ideal P^2 is principal.

Proof. Since β lies in the index 2 subfield, it generates a principal ideal

$$(\beta) = PP^\eta$$

where η the order 2 element of $\mathrm{Gal}(K/\mathbb{Q})$. For a suitably chosen $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, we have a principal fractional ideal

$$\left(\frac{\beta}{\alpha^\sigma}\right) = \frac{P}{P^\tau}$$

for some prime ideal P over p and some $\tau \in \mathrm{Gal}(K/\mathbb{Q})$. Since β/α^σ is not a unit, τ is not the identity automorphism.

Suppose τ has order m in the Galois group. Since τ is not the identity, m must be even, so

$$\frac{P}{P^\eta} = \frac{P}{P^{\tau^{m/2}}} = \frac{P}{P^\tau}\frac{P^\tau}{P^{\tau^2}}\cdots\frac{P^{\tau^{m/2-1}}}{P^{\tau^{m/2}}}$$

is a principal fractional ideal. We conclude that

$$P^2 = (\beta)\frac{P}{P^\eta}$$

is a principal ideal. □

Proposition 3.1.17. *Under the generalized Riemann hypothesis, the class number of* $\mathbb{Q}(\zeta_{257})^+$ *is* 3.

Proof. Searching over sparse vectors, using our two bases (b_j) and (c_k), we find the following integral elements of $\mathbb{Q}(\zeta_{257})^+$ and their norms:

Element	Norm
$\alpha_1 = c_0 + c_8 - c_{48} - c_{78} - c_{81} + c_{119}$	$130043 \cdot 231299$
$\alpha_2 = b_0 + b_1 - b_{114}$	$130043 \cdot 529933$
$\alpha_3 = b_1 + b_4 - b_{48} - b_{49}$	$257 \cdot 231299 \cdot 529933$

Since the prime over 257 is totally ramified, we can divide α_3 by $2b_0 - b_1$, which has norm 257, to get an integral element α_4 with norm $231299 \cdot 529933$. Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{257})^+$, which is cyclic of order 128. By choosing appropriate σ_1, σ_2 in G, we can construct an integral element

$$\beta_1 = \frac{\alpha_1^{\sigma_1}\alpha_2^{\sigma_2}}{\alpha_4}$$

of norm 130043^2.

Let K be the index 2 subfield of $\mathbb{Q}(\zeta_{257})^+$. Inspired by the result of Lemma 3.1.16, we search for an integral element of K that has norm (in K) 130043. It is useful to have an integral basis for K. Let g be the automorphism that sends ζ_{257} to ζ_{257}^3, so that g generates G. Let $d_0 = 1$ and let

$$d_j = (\zeta_{257} + \zeta_{257}^{-1})^{g^{j-1}} + (\zeta_{257} + \zeta_{257}^{-1})^{g^{64+j-1}}$$

for $1 \leq j \leq 63$. Then $d_0, d_1, \ldots, d_{63}$ is an integral basis for K. To find elements in the ring of integers $\mathcal{O}_K$, we both search over sparse vectors in K using the basis (d_i), as well as searching sparse vectors in $\mathbb{Q}(\zeta_{257})^+$ using bases (b_j) and (c_k), and then taking the relative norm $\alpha \mapsto \alpha\alpha^{g^{64}}$ to get an element of K. We find the following integral elements of K and $\mathbb{Q}(\zeta_{257})^+$ and their respective absolute norms:

Field	Element	Norm
$\mathbb{Q}(\zeta_{257})^+$	$b_1 + b_2 - b_{18}$	1100175367
K	$d_1 - d_2 - d_5 + d_{13} + d_{14} - d_{20} - d_{53} - d_{61}$	$1100175367 \cdot 485731$
$\mathbb{Q}(\zeta_{257})^+$	$c_0 - c_4 + c_7 + c_{54} + c_{60} + c_{83}$	$485731 \cdot 227189$
K	$d_1 + d_3 + d_9 - d_{13} + d_{27} + d_{33} + d_{44} - d_{55}$	$227189 \cdot 777167$
K	$d_1 + d_2 - d_7 - d_{11} - d_{12} + d_{17} - d_{24}$	$777167 \cdot 1461301$
$\mathbb{Q}(\zeta_{257})^+$	$c_0 + c_6 - c_{18} - c_{24} + c_{75}$	$1461301 \cdot 559015091$
$\mathbb{Q}(\zeta_{257})^+$	$b_1 + b_{28} - b_{68} - b_{69}$	$257 \cdot 559015091 \cdot 30841$
$\mathbb{Q}(\zeta_{257})^+$	$c_0 - c_{17} + c_{39} + c_{45} + c_{116}$	$30841 \cdot 446142233$
K	$d_0 + d_1 + d_4 - d_{18} + d_{46} + d_{52} - d_{58} + d_{60}$	$446142233 \cdot 140837$
$\mathbb{Q}(\zeta_{257})^+$	$b_1 + b_2 - b_{43}$	$140837 \cdot 130043$

As usual, we can divide by $2b_0 - b_1$, which has norm 257, to get an integral element with norm $559015091 \cdot 30841$. For elements in $\mathbb{Q}(\zeta_{257})^+$, we take relative norms to produce elements of the same absolute norm in K. Finally, by taking quotients by appropriate Galois conjugates, we can construct an integral element β_2 of K, which has norm 10043, and which has norm 10043^2 when considered as an element of $\mathbb{Q}(\zeta_{257})^+$.

We can explicitly calculate that β_2/β_1^σ is not a unit for all σ in G. Thus we can apply Lemma 3.1.16 to show that, for any prime P lying above 10043, the ideal P^2 is principal. We can use the Parity Check Theorem (see Subsection 3.2.7) to see that the class number of $\mathbb{Q}(\zeta_{257})^+$ is odd, therefore P itself must be principal. From here it is relatively straightforward to find integral elements α of the form

$$(\alpha) = PQ$$

where Q is a prime ideal of small prime norm, thereby establishing a class number upper bound. However, we prefer to proceed more explicitly, finding actual generators for the prime ideals of small prime norm.

First we find σ in G such that

$$\gamma = \frac{\beta_2}{\beta_1^\sigma}$$

generates a principal fractional ideal of the form

$$(\gamma) = \frac{P}{P^\tau}$$

where P is a prime ideal of norm 130043, and $\tau \in G$. By taking certain products of Galois conjugates of γ, we can determine that τ generates G. This element γ is useful in the following situation: Suppose there exist integral elements x and y with norms pqr and pq respectively, where $p = 130043$, and q and r are prime numbers that totally split in the field. Then x generates an ideal of the form

$$(x) = PQR$$

where P, Q and R are prime ideals of norms p, q and r respectively. Similarly, a Galois conjugate of y generates the ideal

$$(y^{\sigma_1}) = P^{\sigma_2}Q$$

for some $\sigma_1, \sigma_2 \in G$. Suppose $\sigma_2 = \tau^k$. Then $\gamma\gamma^\tau \cdots \gamma^{\tau^{k-1}} y^{\sigma_1}$ generates the ideal PQ. Therefore, we can construct an integral element

$$\frac{x}{\gamma\gamma^\tau \cdots \gamma^{\tau^{k-1}} y^{\sigma_1}}$$

of norm r. In other words, we have used the element γ to "twist" the prime ideal P by a Galois action, when P is a factor of a composite ideal.

To make use of this idea, we use the following elements of $\mathbb{Q}(\zeta_{257})^+$ and their norms:

Element	Norm
$\alpha_2 = b_0 + b_1 - b_{114}$	$130043 \cdot 529933$
$\alpha_5 = c_0 + c_{54} + c_{59} + c_{112}$	$529933 \cdot 16205393$
$\alpha_6 = c_0 - c_7 - c_{19} + c_{36} - c_{88} + c_{115} + c_{123}$	$16205393 \cdot 8737$
$\alpha_7 = c_0 - c_1 + c_{13} - c_{52} + c_{106} - c_{121} + c_{122}$	$1275749 \cdot 8737^2$

By choosing the appropriate σ_1 and σ_2 in G, we can construct an element

$$\beta_3 = \frac{\alpha_2^{\sigma_1}\alpha_6^{\sigma_2}}{\alpha_5}$$

that has norm $130043 \cdot 8737$. Next we choose σ_3 and σ_4 in G such that the element

$$\beta_4 = \frac{\alpha_7 \beta_1}{\beta_3^{\sigma_3} \beta_3^{\sigma_4}}$$

generates the ideal

$$(\beta_4) = \frac{P^{\sigma_5} P^{\sigma_6} Q}{P^{\sigma_7} P^{\sigma_8}}$$

where P and Q are prime ideals of norm 130043 and 1275749 respectively. Now by multiplying β_4 by the appropriate Galois conjugates of γ, we can construct an integral element β_5 of norm 1275749.

Next we use the following integral elements and their norms.

Element	Norm
$\alpha_8 = c_1 - c_{18} + c_{40} + c_{56} - c_{75} + c_{105}$	$1275749 \cdot 4111 \cdot 16447$
$\alpha_9 = b_0 + b_1 - b_9 - b_{30} + b_{58} - b_{75} + b_{84}$	$130043 \cdot 16447$
$\alpha_{10} = b_1 + b_3 + b_{39} + b_{56} - b_{120}$	$1615501 \cdot 4111^2$
$\alpha_{11} = c_0 + c_{57} - c_{84} - c_{95} + c_{115}$	$1615501 \cdot 4454086019$
$\alpha_{12} = b_1 + b_{12} + b_{20} + b_{27} - b_{88} + b_{106}$	$4454086019 \cdot 4111$

By dividing α_8 by the appropriate conjugate of β_5, we can construct an integral element β_6 of norm $4111 \cdot 16447$. We can choose $\sigma_1, \sigma_2, \sigma_3, \sigma_4 \in G$ such that

$$\beta_7 = \frac{\alpha_{10} \alpha_9^{\sigma_1} \alpha_9^{\sigma_2}}{\beta_6^{\sigma_3} \beta_6^{\sigma_4}}$$

is an integral element of norm $1615501 \cdot 130043^2$. Now we can use the idea discussed above to divide β_7 by β_1 (which has norm 130043^2) after "Galois twisting" β_1 via multiplying by the appropriate conjugates of γ. This constructs an integral element β_8 of norm 1615501. Now we can divide α_{11} by the appropriate conjugate of β_8 to produce an element β_9 of norm 4454086019, and finally we can divide α_{12} by the appropriate conjugate of β_9 to construct an integral element β_{10} of norm 4111. Moreover, the foregoing calculations, while rather elaborate, do construct β_{10} explicitly. Using our basis (b_j), the following integral element has norm 4111:

[10428599412, −14580350932, −3376865511, −3282951359, 16341675835, 1606498420, 8793062613, −10418031177, −6534149268,
3959823353, 2343001669, 10405410440, −159350108, 1294971873, 14581294173, −21855534611, −10953699563, 1523537643,
−1917408750, 5120471172, 3796206827, 9634551567, 13161733282, −2891642657, 16236634832, 5812863383, 2291902524,
−927271498, 12344458809, −5339104130, −10449175119, 15360571789, 6867130480, 5172508006, −7549973967, 211995255,
−3763953981,−11433299663, −13615962461, 5355009796, −11297606817, −2556433074, 6233677121, 3183108998, 9711268884,
1358917812, −13181014917, −460664187, −9867390849, −7057095944, −1231901880, 17841337326, 6865141087, 7050234913,
3378609799, 2597830021, −1832197251, 3819792880, −6992348742, −5130633052, 14306839471, 12887464234, −18866257486,
25559309930, 15012086950, 7342448392, −1447037609, 10925064191, −2871628392, 13674056414, −12763449177, 6465755479,
−8530847721, 357435101, −5870464205, −1053588258, −6264126033, 3519819872, −10418872203, 1209803322, 18036790420,
−16494298977, −895762797, 6908038386, −6385671655, 2210043491, 14099425376, −102885514, 6525479595, −4275376660,
20281603850, 21656361938, −41020296, 1764621668, −1128485911, 2185909622, −3173565968, −8361116079, −16226275883,
6027752153, −16755055836, 714323813, 6857278901, 10406224009, 30155528, 9622569750, −14207419941, 790856920,
−6259612995, −4506190723, −22604391522, 7208517345, 13498834899, 12234015974, 6816024743, −8841527344, −7546114709,
−5966609027, 9218589829, −52711198, −939675580, −3878241077, −10089568359, −3270719023, 3458120705, −11928861316,
5827650658, 8477718634].

We can examine the quadratic subfield $\mathbb{Q}(\sqrt{257})$ (which has class number 3) to confirm that 4111 must be the smallest prime which totally splits into principal ideals in $\mathbb{Q}(\zeta_{257})^+$. We can also use $\beta_{10}, \beta_6, \alpha_9$ and β_3 to produce integral elements of norms 8737, 16447 and 130043. Setting $S = \{4111, 8737, 16447, 1300433\}$ and $c = 12$, we apply Theorem 2.3.2 to show a class number upper bound of 58532. Using Schoof's table [31], this proves that the class number is 3. □

3.1.9 The class number of $\mathbb{Q}(\zeta_{263})^+$

Proposition 3.1.18. *Under the generalized Riemann hypothesis, the class number of* $\mathbb{Q}(\zeta_{263})^+$ *is* 1.

Proof. As the conductor of the real cyclotomic field gets larger, it becomes much more difficult to directly find integral elements of small prime norm. The smallest prime norm that we found directly is 19062767, which is too large to be useful, so more elaborate methods must be used. Using our alternative basis of cyclotomic units, we find the following element and its norm, which will prove critical to our calculations:

$$N(c_0 - c_1 + c_{30} + c_{50} + c_{57} + c_{125}) = 263 \cdot 90473^2.$$

The prime 263 is totally ramified, and the element $2b_0 - b_1$ has norm 263, so the quotient

$$\beta_1 = (c_0 - c_1 + c_{30} + c_{50} + c_{57} + c_{125})/(2b_0 - b_1)$$

is integral and has norm 90473^2. Finding an element of square of prime norm is quite useful. It generates a principal ideal of the form PP^σ, where P is an prime ideal of norm 90473 and σ is a Galois automorphism (possibly trivial). Suppose the σ is nontrivial. Since the field is cyclic and of odd degree, P would have to be principal. Indeed, if σ is nontrivial, we would have $P = (\beta_2)$, where

$$\beta_2 = \frac{90473}{\beta_1^{\sigma} \beta_1^{\sigma^3} \beta_1^{\sigma^5} \cdots \beta_1^{\sigma^{65}}}.$$

To find verify that σ really is nontrivial and to calculate β_2 explicitly, we can, by trial and error, calculate the above quotient for each $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{263})^+/\mathbb{Q})$ until we find an element that is integral. We successfully find an element β_2 with norm 90473:

$$\beta_2 = [91093658332149, 46685768271369, 68361335338819, 70449701906399, 31843826845597, 71908870045208, 27348493133994,
33754439477092, 44962750769433, -1508515343175, 38936510401862, 5192389684002, 3856782750979, 30811441093606,
-13800153606985, 29501013048266, 12698371445207, 5972682159799, 47522592180973, 6984009026336, 47796072467378,
45431238836744, 28923021502479, 76508506511574, 36427352941694, 65288348301432, 70729148827096, 39222853791302,
83890582919007, 42561006315902, 54359680367799, 65856630526478, 21771108627025, 62485586062044, 26270613224325,
25094463692233, 47568054578494, 125103582406, 40199642477044, 17255996070330, 8020908354451, 43727515821674,
-1224030726933, 36725858965513, 28721683898737, 11059835997195, 55772756914003, 13963391285317, 44428872659723,
48817768645436, 20806767869799, 68256402498630, 29533198999197, 47647209752074, 61820560465718, 23399606060785,
68941541644779, 35080264238375, 39477647868923, 62954375684249, 17926845492145, 60044369932817, 35355012024759,
27811028989986, 61007592764110, 14202408842359, 51237426002148, 38049808198331, 19048314247332, 59172601836849,
12845180380311, 41215485711317, 39372324585845, 9507804081257, 53457153938823, 11150392769067, 29804191547363,
40985902129113, 4145466953423, 51035020787945, 17645569166106, 27171632487894, 51999047781356, 11617148558946,
58380593320006, 35709375065281, 34271393487151, 69329058912370, 26009828407571, 66912441681898, 53689198914325,
38297029552571, 78021970342828, 31559126022913, 60846711527437, 55304155983289, 24952006088441, 65163951384176,
18339935726356, 34630357356142, 39133556811954, -982220989357, 41344881716202, 2613790588508, 10778478428163,
31190967040067, -9846880977122, 37002211890541, 13289474010174, 15539069958255, 51634030002302, 11894975122939,
57793409741762, 46922638944671, 37965909423900, 81212332710005, 38872529472440, 73929528055148, 70028966094730,
44443940224036, 86511154348392, 40219032166425, 58939087815398, 60743505389903, 20146235684074, 59689390807667,
15613793165531, 21298434543273, 34515562251936, -11239938639024, 30781542318124].$$

This element has prime norm that is relatively small, so we can take quotients with it to find several other useful elements. Searching over sparse vectors, we find the following elements and their norms:

Element	Norm
$\alpha_1 = b_1 - b_2 - b_6 + b_{39} - b_{45} - b_{130}$	$90473 \cdot 123083$
$\alpha_2 = c_0 + c_{11} - c_{59} - c_{62} + c_{67}$	$123083 \cdot 699581$
$\alpha_3 = b_0 + b_1 - b_3 + b_{30} + b_{72} - b_{113} + b_{117}$	$123083 \cdot 4900741$
$\alpha_4 = b_1 + b_5 + b_9 - b_{34} - b_{38} - b_{65}$	$263 \cdot 4900741 \cdot 64930493$
$\alpha_5 = b_0 + b_1 + b_8 + b_{10} - b_{33} - b_{35} - b_{37}$	$64930493 \cdot 12308399$
$\alpha_6 = b_0 + b_1 + b_{51} - b_{100}$	$12308399 \cdot 1713181$
$\alpha_7 = b_0 + b_1 + b_2 + b_{27} - b_{57} + b_{115} + b_{119}$	$1713181 \cdot 476213047$
$\alpha_8 = c_0 + c_1 - c_{11} - c_{68} - c_{73} + c_{75} + c_{91}$	$476213047 \cdot 5458303$

As usual, we can divide α_4 by $2b_0 - b_1$ to get an integral element of norm $4900741 \cdot 64930493$. Then we can take quotients by the appropriate Galois conjugates to construct integral elements of β_3, β_4 and β_5 of prime norms 123083, 699581 and 5458303 respectively.

We recall an idea introduced in Subsection 3.1.7. If we have 3 elements of "almost prime" norms p_1p_2, p_2p_3 and p_3p_1 (where p_1, p_2 and p_3 are distinct primes), then we can take products and quotients by the appropriate Galois conjugates to construct an element of p_1^2. This generalizes to a sequence of elements of norms $p_1p_2, p_2p_3, p_3p_4, \ldots p_{2k}p_{2k+1}, p_{2k+1}p_1$. We can think of this in terms of graph theory: Let every prime number correspond to a vertex, and draw edges between vertices p_i and p_j whenever we find an element of norm p_ip_j. Then our goal is to find a cycle in the graph of *odd* length. In such a case, we can construct elements of square of prime norm p_i^2 for each vertex p_i in the cycle. We can then exploit this square of prime norm as before. To carry out this idea, we search over the sparse vectors and find:

Element	Norm
$(b_1 + b_6 + b_{74} + b_{81} - b_{111})/\beta_2^{\sigma_1}$	$1051 \cdot 970469$
$b_0 + b_1 - b_3 + b_{50} - b_{78}$	$970469 \cdot 127817$
$(c_0 - c_2 - c_{12} - c_{15} + c_{32} + c_{126})/\beta_3^{\sigma_2}$	$127817 \cdot 53653$
$c_0 - c_{13} + c_{63} + c_{77} + c_{96} + c_{102} + c_{111}$	$53653 \cdot 13166917739$
$b_1 + b_8 - b_{35}$	$13166917739 \cdot 1458599$
$(b_0 + b_1 - b_{13} - b_{59} + b_{85} - b_{120})/\beta_4^{\sigma_3}$	$1458599 \cdot 87317$
$(b_1 + b_2 - b_8 + b_{61} - b_{100} - b_{101})/(2b_0 - b_1)$	$87317 \cdot 44711$
$(b_0 + b_1 + b_3 - b_{12} - b_{14} - b_{55} - b_{62})/\beta_5^{\sigma_4}$	$44711 \cdot 6311$
$(c_0 + c_4 + c_{10} - c_{19} + c_{38} - c_{64} + c_{118})/\beta_3^{\sigma_5}$	$6311 \cdot 23143$
$c_0 - c_5 - c_{37} + c_{63} - c_{93} + c_{114} + c_{123}$	$23143 \cdot 4733$
$(b_1 + b_7 + b_{13} + b_{27} - b_{34} + b_{104})/\beta_2^{\sigma_6}$	$4733 \cdot 61453$
$(b_1 - b_7 + b_{26} - b_{97} + b_{103} - b_{118})/(2b_0 - b_1)$	$61453 \cdot 29983$
$b_0 + b_1 - b_{32} - b_{34} - b_{51} - b_{80}$	$29983 \cdot 213557$
$(b_0 + b_1 - b_{11} + b_{23} - b_{94} - b_{111} - b_{116})/\beta_2^{\sigma_7}$	$213557 \cdot 58802591$
$(b_1 - b_3 - b_{29} + b_{30})/(2b_0 - b_1)$	$58802591 \cdot 1051$

Note that, where necessary, we divided by the appropriate Galois conjugates of $\beta_2, \beta_3, \beta_4$ and β_5, or by the generator $2b_0 - b_1$ of the totally ramified prime over 263, in order to obtain quotients with our desired norms. We now have a cycle of odd length:

$$1051 \to 970469 \to 127817 \to 53653 \to 13166917739 \to 1458599 \to 87317 \to 44711$$

$$\to 6311 \to 23143 \to 4733 \to 61453 \to 29983 \to 213557 \to 58802591 \to 1051$$

From this cycle of elements almost prime norms, we can construct an integral element β_6 of norm 1051^2. Then we can proceed as we did earlier, checking the quotient

$$\frac{1051}{\beta_6^{\sigma}\beta_6^{\sigma^3}\beta_6^{\sigma^5}\cdots\beta_6^{\sigma^{65}}}$$

for each $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{263})^+/\mathbb{Q})$ until (possibly) finding an integral element which has norm 1051. Indeed, we can explicitly find such an element of norm 1051:

[4937323371016121050282685, 7580985651254745650097999, −15454228060200010194585361, 11608250910891216977766181,
8296951211820526848129067, −9495171525321871549373872, 17645422254251463645324666, 5037486883361967412831486,
8226092826053271032519287, −152383476435158076536001, 7435157508565396487106611, −16189201598582115346730956,
−7375143169639161472468879, 18268044283729666528882811, 4815485446067692852689706, 19177165581900105859528702,
11698772752195721891068003, 1041424353963302055215132, −2382318783343172818953068, 17044292631647803318016129,
3627486085528583685696700, 5661403194326210808810951, −6859888720765748512851989, −8044209564042405580987222,
40372271074116315444238221, 13514515623562583503868333, 1721876421192351601694493, 1854130892721851476750639,
−106818807941735581739542, −22188285281212830341990246, 12107713304363838848319057, 27876388900050076046304382,

−25065428653532648377872053, −539149836758209163160874, −2328448882933695126666404, 19720451192722162362715614,
5183402481594776272073056, 3070079613236588473348308, 557404178221304169517505, −15671421346530645752036888,
24465543254965552742381172, −3239194050065843348774007, 27687729968673161874914941, −6956905450300249689125728,
−9310875728833380148688706, 28950046397208797979470158, 2628209303620153073223782, 28878888265926542545187937,
6014131530894172652176016, 8786324643481982873069450, −7659052601761765596529789, 8651864403211799316467909,
15763559308497163469212481, −15462747089211699209073811, 7298456478753066853398345, 8131880066615816065040497,
22143388439637833489860792, −8624993606325920654380161, 8616543704285506374576379, 6439735433195270919019289,
−27441354570116405815700467, 8083412651361837040479448, 7140146458949969097444796, 2831087411345242355314988,
−4742431533824637454335, 8940076003727227903448952, 2163127651757719782350518, 3502293973161221804209283,
−362096683439023622623737, −6227887929413307287253518, 2950426141122150913844458, −6099713142344536185512967,
−6783533897373198256636445, 7308811535345218572623567, 15868491355070957666070338, −18251971386967251083847596,
12149565106976202046775609, −130615237535109853187008, −23730259142802785060592922, 28005213262079261333449884,
19766027253080412358252320, −3481629093702592372579574, −17208270895693481446856205, 9135854177896155087808817,
−6869463668800132145443618, 13705613590230971718353462, 35965041621721574748713073, 1755805938936159921997772,
13082737564209133441010535, −18898296341135944662999456, 17298879232295934189879251, 20798019859809522571449313,
−8727613794813937153770520, −6391516993999047903694707, 1005358431074813357784871, 20356866090384805785582136,
−5966863028929595238680899, 25708459248106153757803372, 3352626089863497362135314, −17371358398865691283651655,
1067957234249668753244868, 6895739498621604552642609, 9465262644597347439142424, −10130558278699310495908296,
13320906648123109938353254, 7171813282236382071494350, 18577304521007886613864306, 21519658902353620030959575,
5067751152625569650679454, −7270926680139746243053038, −1407546160726375513909224, 27804845975661324384600067,
7289774367789067076488795, 9911758503655367402135287, 4806026277539367212716851, −41014010804350294929013,
14796696251090875725776, 24646934442260944568444407, 17004395363060668135123584, −3609362046631864841561597,
6937048879782102271568180, −19617204369642735068052376, 19898251979525630228175596, −5546277103866192374748246,
−14317858989119013215370653, 14025821872815339163286543, −1796871838428920985559021, 5162993697982116313208980,
7059704827495415958136366, 21123139975575369993266070, −26108407463418308251799058]

We can now conclude that all the primes in the cycle given above totally split into principal ideals. Setting $S = \{1051, 4733, 6311\}$ and $c = 10$, we apply Theorem 2.3.2 to show a class number upper bound of 2152. Using Schoof's table [31], this proves that the class number is 1. □

This completes the proof of Theorem 3.1.1.

3.2 Cyclotomic fields of composite conductor

Exploiting Odlyzko's discriminant lower bounds, Masley [17] and van der Linden [16] were able to unconditionally establish the class numbers of all real cyclotomic fields of composite conductor m, provided that $m \leq 200$, $\phi(m) \leq 72$ and $m \neq 148, 152$. However, for fields of larger degree or conductor, the root discriminant becomes too large for their methods to handle. Instead, we make use of Theorem 2.3.1 to establish an unconditional upper bound for the class number. We make further algebraic arguments concerning the divisibility of class numbers in order to prove the following result.

Theorem 3.2.1. *Let m be a composite integer, $m \not\equiv 2 \pmod{4}$, and let $\mathbb{Q}(\zeta_m)^+$ denote the maximal real subfield of the m-th cyclotomic field $\mathbb{Q}(\zeta_m)$. Then the class number h_m^+ of $\mathbb{Q}(\zeta_m)^+$ is*

$$h_m^+ = \begin{cases} 1 & \text{if } \phi(m) \leq 116 \text{ and } m \neq 136, 145, 212, \\ 2 & \text{if } m = 136, \\ 2 & \text{if } m = 145, \\ 1 & \text{if } m = 256, \end{cases}$$

where ϕ is the Euler phi function. Furthermore, under the generalized Riemann hypothesis, $h_{212}^+ = 5$ and $h_{512}^+ = 1$.

For example, the real cyclotomic field of conductor 420 has class number 1. This is the largest conductor for which the class number of a cyclotomic field has been calculated unconditionally.

3.2.1 Real cyclotomic fields

We briefly recall a few additional facts about real cyclotomic fields. The degree of maximal real subfield $\mathbb{Q}(\zeta_m)^+$ of $\mathbb{Q}(\zeta_m)$ is $\phi(m)/2$, where ϕ is the Euler phi function.

The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times$, and the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)^+/\mathbb{Q})$ of the real cyclotomic field is isomorphic to the quotient group $(\mathbb{Z}/m\mathbb{Z})^\times/\{\pm 1\}$. Galois theory determines the subfields of $\mathbb{Q}(\zeta_m)^+$.

The ring of integers of $\mathbb{Q}(\zeta_m)^+$ is simply $\mathbb{Z}[\zeta_m + \zeta_m^{-1}] = \mathbb{Z}[2\cos(2\pi/m)]$. The prime integers which totally split in this field are precisely those which are congruent to ±1 modulo m.

Let $n = \phi(m)/2$ and let $a_1, a_1, \ldots, a_n$ be those positive integers (in increasing order) that are less than $m/2$ and coprime to m. Until otherwise noted, the integral basis of $\mathbb{Q}(\zeta_m)^+$ that we will use is $\{b_0, b_1, \ldots, b_{n-1}\}$, with $b_0 = 1$ and $b_j = 2\cos(2\pi a_j/m)$ for $j = 1, \ldots, n-1$.

3.2.2 The class number of the cyclotomic field of conductor 256

Weber [36] studied the class numbers of the real cyclotomic fields $\mathbb{Q}(\zeta_{2^k})^+$, and proved that their class numbers are odd for all k. Fukuda and Komatsu [10] went much further and proved that no primes less than 10^9 can divide these class numbers, which suggests that the class numbers of these fields may in fact all be 1. This conjecture, known as *Weber's class number problem*, is also supported by Cohen-Lenstra heuristics [4].

Using Odlyzko's discriminant bounds, van der Linden [16] proved that the class number of $\mathbb{Q}(\zeta_{128})^+$ is 1, and, under the assumption of the generalized Riemann hypothesis (GRH), proved that $\mathbb{Q}(\zeta_{256})^+$ has class number 1. However, due to their rather large discriminants, his method could neither unconditionally prove that $\mathbb{Q}(\zeta_{256})^+$ has class number 1, nor could it be applied to $\mathbb{Q}(\zeta_{512})^+$, even under the assumption of the generalized Riemann hypothesis. However, by counting sufficiently many prime ideals of the Hilbert class field, we overcome the problem of the large discriminants, and prove the following.

Proposition 3.2.2. *The class number of the real cyclotomic field* $\mathbb{Q}(\zeta_{256})^+$ *is* 1*.*

This proposition, together with knowledge of the relative class number [34, pg. 412], allows us to determine the class number of the full cyclotomic field.

Corollary 4. *The class number of the cyclotomic field* $\mathbb{Q}(\zeta_{256})$ *is*

$$10{,}449{,}592{,}865{,}393{,}414{,}737.$$

Proof. If the conductor is a power of 2, then the discriminant of the real cyclotomic field is given by

$$d(\mathbb{Q}(\zeta_{2^k})^+) = 2^{(k-1)2^{k-2}-1}$$

and the root discriminant is

$$\mathrm{rd}(\mathbb{Q}(\zeta_{2^k})^+) = d(\mathbb{Q}(\zeta_{2^k})^+)^{2^{-(k-2)}} = 2^{k-1-2^{-k+2}}.$$

In particular, we have

$$\mathrm{rd}(\mathbb{Q}(\zeta_{256})^+) = 127.9891....$$

This root discriminant is too large to use Odlyzko's unconditional discriminant bound tables to establish an upper bound for the class number. Therefore, we must show a sufficiently large contribution by prime ideals of small norm to the explicit formula in order to get an upper bound for the class number. Although it is not difficult to find principal prime ideals of small norm in the $\mathbb{Q}(\zeta_{256})^+$, an unconditional proof that $\mathbb{Q}(\zeta_{256})^+$ has class number 1 will require that we exhibit principal prime ideals for a rather large number of primes.

A prime integer p totally splits in $\mathbb{Q}(\zeta_{256})^+$ if and only if p is congruent to ±1 modulo 256. Thus, if there exists an algebraic integer with norm p congruent to ±1 modulo 256, then p totally splits into principal prime ideals.

Let $\mathcal{O}$ denote the ring of integers of $\mathbb{Q}(\zeta_{256})^+$. Let $b_0 = 1$ and $b_j = 2\cos\frac{2\pi j}{256}$ for $j = 1, \ldots, 63$, and let

$$c_k = \sum_{j=0}^{k} b_j.$$

for $k = 0, \ldots, 63$. Then $c_0, \ldots, c_{63}$ is the basis for $\mathcal{O}$ that we will use. The c_k form a basis for the cyclotomic units, but this fact will not be used directly.

Our strategy will be to search over a large number of "sparse" vectors with respect to the basis $c_o, \ldots, c_{63}$. We make a list of those elements of $\mathcal{O}$ that have norms which are prime and are congruent to ±1 modulo 256. We will need tens of thousands of these primes to successfully establish an unconditional upper bound for the class number.

We consider all $x \in \mathcal{O}$ of the form

$$x = c_0 + a_1 c_{j_1} + a_2 c_{j_2} + a_3 c_{j_3} + a_4 c_{j_4} + a_5 c_{j_5} + a_6 c_{j_6},$$

with $1 \leq j_1 < j_2 < j_3 < j_4 < j_5 < j_6 \leq 63$ and $a_i \in \{-1, 0, 1\}$ for $i = 1, \ldots, 6$. Let T be the set of all such x .

The ideal $2\mathcal{O}$ is totally ramified. Thus, if $x \in \mathcal{O}$ has even norm $N(x)$, we can divide x by any element of norm 2, say b_1, to get an algebraic integer $b_1^{-1}x$ with norm $N(x)/2$. Therefore we consider the odd parts of all norms $N(x)$. We define the set U to be

$$U = \{\text{odd part of } N(x) \mid x \in T\}.$$

Let S_1 be the set of prime numbers

$$S_1 = \{m \text{ prime} \mid m \in U, m \equiv \pm 1 \pmod{256}, m < 10^9\}.$$

The set S_1 does not contain enough primes to establish a class number upper bound. To supplement these primes, we can factor composites in U using primes from S_1. Let S_2 be set of primes

$$S_2 = \{p \text{ prime} \mid pq \in U, p \notin S_1, q \in S_1\},$$

noting that if $N(x) = pq$ and $N(y) = q$, for $x, y \in \mathcal{O}$ for distinct primes p and q, then $x/\sigma(y)$ is in $\mathcal{O}$ with norm p for some Galois automorphism σ.

Let $S = S_1 \cup S_2$. We apply Theorem 2.3.1, choosing $c = 210$ and putting

$$F(x) = \frac{e^{-(x/c)^2}}{\cosh \frac{x}{2}}.$$

A lower bound for the contribution from split primes is

$$2 \sum_{p \in S} \sum_{m=1}^{\infty} \frac{\log p}{p^{m/2}} F(m \log p) > 2 \sum_{p \in S} \sum_{m=1}^{2} \frac{\log p}{p^{m/2}} F(m \log p) > 0.7023.$$

This still is not quite enough, so we supplement our prime ideal contribution by considering the totally ramified prime 2. This factors as $2\mathcal{O} = P^{64}$ where P is a principal prime ideal of norm 2, giving a contribution

$$\frac{2}{64}\sum_{m=1}^{\infty}\frac{\log p}{p^{m/2}}F(m\log p) > \frac{2}{64}\sum_{m=1}^{20}\frac{\log p}{p^{m/2}}F(m\log p) > 0.0331.$$

We have that $\log \mathrm{rd}(\mathbb{Q}(\zeta_{256})^{+} = 4.8412...$ and we use numerical integration to find that

$$\mathcal{G}(F) = \int_0^{\infty}\frac{1-F(x)}{2}\left(\frac{1}{\sinh\frac{x}{2}}+\frac{1}{\cosh\frac{x}{2}}\right)dx < 1.2642.$$

Then we have

$$B = \left(\frac{\pi}{2}+\gamma+\log 8\pi\right) - \log \mathrm{rd}(K) - \mathcal{G}(F) + 2\sum_{\mathfrak{P}}\sum_{m=1}^{\infty}\frac{\log N\mathfrak{P}}{N\mathfrak{P}^{m/2}}F(m\log N\mathfrak{P})$$

$$> 5.3721 - 4.8412 - 1.2642 + 0.7023 + 0.0331 = 0.0021.$$

Thus, we get a class number upper bound of

$$h < \frac{2c\sqrt{\pi}}{nB} < 5539.$$

Finally, we apply the results of Fukuda and Komatsu [10] to prove that $h = 1$, proving the proposition. □

3.2.3 The class number of the cyclotomic field of conductor 512

Assuming the generalized Riemann hypothesis, we will calculate the class number of the cyclotomic field of conductor 512 and its maximal real subfield. The full cyclotomic field has degree 256 and discriminant of approximately 3×10^{616}. The author is unaware of any other number field of such large degree or discriminant for which the class number has been calculated conditionally under the GRH.

Proposition 3.2.3. *Under the assumption of the generalized Riemann hypothesis, the class number of the real cyclotomic field* $\mathbb{Q}(\zeta_{512})^{+}$ *is* 1.

Since we know the relative class number [34, pg. 412], this proposition allows us to determine the class number of the full cyclotomic field. It is striking that the class number of the real subfield is so small compared to the class number of the full cyclotomic field.

Corollary 5. *Under the generalized Riemann hypothesis, the class number of the cyclotomic field* $\mathbb{Q}(\zeta_{512})$ *is*

$$6{,}262{,}503{,}984{,}490{,}932{,}358{,}745{,}721{,}482{,}528{,}922{,}841{,}978{,}219{,}389{,}975{,}605{,}329.$$

The real cyclotomic field of conductor 512 has a root discriminant

$$\mathrm{rd}(\mathbb{Q}(\zeta_{512})^+) = 254.6175....$$

which exceeds $8\pi e^{\gamma+\pi/2} = 215.33....$ Therefore, we must show a contribution to the explicit formula by prime ideals of small norm to get an upper bound for the class number (even under the assumption of GRH).

In contrast to the unconditional proof that $\mathbb{Q}(\zeta_{256})^+$ has class number 1, under GRH proving that $\mathbb{Q}(\zeta_{512})^+$ has class number 1 will take knowledge of just a few principal prime ideals of small norm. We will explicitly give generators of such principal primes ideals, and prove the following lemma, although the generators of those ideals were rather difficult to find.

Lemma 3.2.4. *In the real cyclotomic field* $\mathbb{Q}(\zeta_{512})^+$*, there exist algebraic integers of norms* 3583*,* 5119*,* 6143*,* 7681*,* 8191*,* 10753*,* 11777*,* 12289*,* 12799 *and* 13313*.*

The existence of these algebraic integers of small prime norm allows us to prove the main result.

Proof of Proposition 3.2.3. Let $K = \mathbb{Q}(\zeta_{512})^+$, which has degree 128 over $\mathbb{Q}$. Let h be its class number. Let F be the function

$$F(x) = e^{-(x/c)^2},$$

with $c = 8.7$.

The following integral can be calculated using numerical integration:

$$\int_0^\infty \frac{1 - F(x)}{2} \left(\frac{1}{\sinh \frac{x}{2}} + \frac{1}{\cosh \frac{x}{2}} \right) dx < 0.3358.$$

A prime integer p totally splits in K if and only if p is congruent to ±1 modulo 512. Let S denote the set of primes,

$$\{3583, 5119, 6143, 7681, 8191, 10753, 11777, 12289, 12799, 13313\},$$

which are the ten smallest prime integers which are congruent to ±1 modulo 512. Using Lemma 3.2.4, there is a lower bound for the contribution from the prime ideals,

$$2 \sum_{p \in S} \sum_{m=1}^{\infty} \frac{\log p}{p^{m/2}} F(m \log p) > 2 \sum_{p \in S} \frac{\log p}{\sqrt{p}} F(\log p) > 0.6898.$$

We apply Theorem 2.3.2 to get an upper bound for the class number,

$$h < 147.$$

Finally, we can apply the results of [10] (or the Rank Corollary given in the next subsection) to see that $h = 1$. □

Proof of Lemma 3.2.4. It suffices to explicitly provide the elements which have the desired norms. The real cyclotomic field $\mathbb{Q}(\zeta_{512})^+$ has an integral basis, $\{b_0, b_1, \ldots, b_{127}\}$ where $b_0 = 1$ and $b_j = 2\cos(2\pi j/512)$ for j from 1 to 127. Given an element (a_j) of the field in this basis, the norm of (a_j) is the absolute value of

$$\prod_{k=0}^{127} \left(a_0 + \sum_{j=1}^{127} a_j \cos \frac{2\pi j(2k+1)}{512} \right)$$

Using this basis, we list ten algebraic integers.

This element has norm 3583:

[549, 471, 40, 400, 546, 13, 144, −222, 769, 1114, 4, 109, 1498, −48, −272, 1393, 337, 295, −304, 262, 653, −5, 487, 991, 1080, 604, −176, 147, 517, 299, −136, 5, 331, 1051, 943, 158, 281, 9, −299, −337, 685, 105, 65, 981, 1039, −104, −316, 999, 519, 195, 361, 367, 1033, 556, 435, 533, 126, −393, 391, 1413, 100, 142, 373, 268, −875, −246, −117, −327, 1530, 695, −210, 1137, 844, −882, 101, 254, −347, 281, 441, 1727, 909, −729, −397, −117, 478, −947, 67, 1040, 445, 138, 154, 473, 412, 324, −164, 625, −50, 156, 141, −7, 376, −985, −434, 1002, 503, −343, −204, −200, −67, 170, −922, 554, 867, −172, 29, 387, 797, −470, 155, 42, −270, −14, 31, 246, 385, 162, −137, 197].

This element has norm 5119:

[147, −104494, −26676, 12081, 25706, −14209, 71256, 99827, 36209, −47677, 66855, 65451, 4681, −88975, −15784, 32245, 41017, 45678, −5821, 127438, 17275, 161270, 121388, 141018, 76565, 18507, −25523, 8820, 86486, −3883, −59945, −32692, 7427, 168170, 79532, 111518, −40813, −721, 100225, 38681, 35033, −59976, −26151, −150361, 17703, −10107, 7624, −39793, −74576, 12244, 49328, 108034, 79004, −83833, −31377, 723, 70856, −19714, 6073, 22609, 4054, 29678, 26444, 144109, −16167, 13697, 4492, 36832, 68459, 100913, 66179, 7047, −3034, 156125, 61044, 32403, −6778, 114846, −30960, 2675, 25809, −21964, 1166, −119242, 24160, 13870, 29732, 10150, 24991, 54782, 55211, 12440, −65770, −63049, −36834, −77524, 18444, −165290, 500, −59284, 36279, 53748, 34020, 9670, 13433, 81430, 31887, 115248, −13390, −87277, −73639, −784, 62328, −25731, −8249, 68768, 9913, 136174, 153369, 108430, −60208, 10978, −25491, 27206, 4128, −8680, −41807, −88057].

This element has norm 6143:

[687, 1109, −264, −409, 1118, 826, −717, 215, −14, 920, 22, −20, 1564, −1030, 424, 959, 90, −540, 374, 435, −334, 207, 140, 65, 841, −339, 124, 378, −376, 114, −760, 672, 232, −973, 341, −71, −284, 495, 329, −106, −246, 78, 301, −475, −756, 1359, −410, 441, 265, −392, 1402, −27, 320, 599, 1365, 258, −473, 416, 260, 1033, 197, 212, 1541, −1026, 688, 1377, −1154, 743, 406, 298, 127, −1017, 7, −8, 987, 440, −730, 199, 359, −1041, −664, 706, −612, −125, 1, 104, −702, −215, 335, 4, 725, −88, −497, −665, −557, 590, −346, 856, 338, −862, 1369, −709, 40, 303, 711, 783, −572, 282, 68, −528, 837, 882, 565, 165, −50, 41, −535, 299, −351, 1012, 15, −183, −18, −615, 758, −158, −234, 1738].

This element has norm 7681:

[12419, −72, 3815, 1193, −3972, −4639, −9741, −525, 20798, −2284, −3016, 2627, 13769, 7618, 9084, 5902, 7104, 2023, 7378, 576, 16966, 1470, −15719, 1047, 4681, 1683, 9320, −2609, 6279, 3161, 1227, 4325, 5423, −2032, 1901, 4788, 15042, −4879, 2991, 4479, 11213, 11266, 1431, −17, 16203, 4789, 7726, −3520, −5160, −2409, −8557, 5297, 9307, −4523, 3415, −4331, −221, 4670, −1272, −5870, 532, 637, 1065, −415, 14452, −7845, 3158, 12392, 3004, 5689, 5914, −4077, 18668, 9144, −4237, −8474, −7417, 1399, 1158, 4120, 2845, −6194, 3372, 5412, 5860, 5527, −3739, −389, 3600, 32, 5343, −4709, 8512, 2466, 902, 11131, 8876, 187, 11267, 104, 6654, 2458, −10487, −2800, −10, 1120, −5029, −5069, −5301, −5294, 7063, 5281, −10073, 7, −5930, 2933, 16618, −8242, −4914, −2260, −1814, 4186, 5099, 2296, 4516, −1349, 10952, 1756].

This element has norm 8191:

[12200476407, −292487755, 12237320977, −308254192, 12300523691, −486916755, 12065092025, −758732357, 12260434117, −988892432, 12200465663, −959314971, 12023444230, −807694380, 11534015416, −285959572, 11389976464, 263767191, 11494483606, 118977394, 11822670966, −186682783, 11780632874, −30299156, 11717352645, 106809269, 11245815188, 100697928, 11092639613, −233023507, 11092354501, −231762119, 10881098713, 220511907, 9986637594, 698898280, 9678586036, 759689527, 9976530302, 456120687, 10566559282, 80998844, 10565421255, 498544865, 10139442513, 1100466640, 9626488800, 1042764202, 9674228265, 454041510, 9544786324, 488174658, 9210076976, 864190149, 8328870937, 1188900157, 8005203607, 765010284, 8638409778, 166529311, 9326591748, 57194082, 8907343957, 660242446, 8270761641, 1177075128, 7941394142, 1196657469, 8196375507, 475786322, 8151556459, 387573310, 7624292526, 778800668, 6924858402, 828150905, 6972011653, 36936460, 7364152427, −523531189, 7603045547, −522042227, 6942706650, 218982829, 6125518634, 669337729, 6123178426, 569668420, 6591787183, 75768606, 6400974331, 36431967, 5893316966, 101388020, 5319695264, 102495640, 5231238345, −682275789, 5286021245, −1039275885, 5013380379, −634603921, 4303406163, 30415910, 3658451229, 147125795, 3460063055, 75926902, 3703180326, −323853178, 3653655136, −238392752, 3198652693, −165979401, 2750313619, −104932882, 2492617006, −365121077, 1964774200, −432485961, 1418575903, −346397268, 795227753, 69588008, 117183978, 17091166, −84709442, 30059544].

This element has norm 10753:

[2115315, 294536700, −1259710, 290751233, −658734, 286253190, 6202172, 290637083, 1020656, 290423296, −785288, 286809730, 431913, 290849807, −1972309, 289141750, 1493136, 277079280, 5027120, 281808363, 2632769, 282772045, 2606799, 275911224, −1617886, 279800829, −2830788, 277631577, 6603296, 268177615, 1887075, 267705912, 2525056, 263121511, 8861721, 262918374, −2519628, 265098198, −2478906, 254252249, 7330168, 255187684, 1527574, 249540354, 3108613, 238201953, 6373217, 243789683, −264411, 242990286, 2452961, 229857806, 49331, 232535039, 2084912, 223094230, 9146065, 215098451, 115902, 219852521, 387854, 211046359, 6617566, 208066712, −5512979, 203853094, 2938804, 191528668, 10507462, 191238633, −124009, 186251412, 976595, 177087267, 1202043, 182974650, −2866736, 170675998, 2795285, 158104278, 1621262, 160310188, 2372332, 148894811, 5059504, 143612130, −6568863, 146665733, −1471899, 134710036, 2866574, 126299884, −3787243, 120781480, 2780159, 111599813, 3927794, 110874132, −4748117, 102000659, −2104084, 96925239, −305319, 91713010, −760194, 77534598, 2343950, 71004081, −388880, 72762622, −429211, 60416092, −2906516, 53531722, −4333035, 49933247, 1898531, 37573906, 3511913, 27924006, −1569879, 24254418, 65830, 21400232, −1564070,12689918, −4103286, 4118337].

This element has norm 11777:

[1309, 111, 323, 687, 443, 1010, 109, 133, 384, 217, 263, 610, 12, 183, −2, 663, 446, 1483, 241, 407, −32, 848, −145, 455, −982, 157, −434, 1121, −320, 789, 671, −16, 194, 752, −233, 1191, −367, 1, 382, 287, 23, 794, 488, 78, 125, −416, −28, 519, 1231, −387, 817, 479, 1294, 736, 697, −789, 45, 220, 291, 126, 1277, −1062, 577, −67, 1028, 1270, 788, −567, 719, 46, 716, −105, 6, −16, 80, 75, −194, 72, 657, −319, −311, 110, 1058, 691, 173, 39, −329, 164, −388, 241, 524, −45, −381, −1016, −60, 845, 110, 109, 508, 30, 1454, −291, −76, 17, 41, −465, 242, −49, 854, −286, −57, −612, 1553, −54, 364, 11, 948, −428, 189, −416, 612, 319, 515, −854, 237, 204, −978, −27].

This element has norm 12289:

[617693837477, 2370075244431, −339648780201, 2238090913237, −498204865353, 2221056021584, −152042916658, 3110568633642, −31712501506, 1411860086389, 80359803004, 2546233401730, −182447396621, 2299547040386, −290214250390, 2590997629540, −326219315631, 2312166834647, 48131827765, 1783289384553, 378442675003, 2329438770514, −580294589938, 2218401635376, −717839827005, 3197597713419, 704535529089, 1130283380417, −184355619389, 2116839801895, −414187025834, 2857033836333, −217842459574, 1843457953282, 62852900411, 2356758151872, −228936921555, 1651643367144, −266752316105, 2381610344981, 466861508085, 1879106118549, −578325063236, 2244797414571, −402842736038, 2139817462475, 171310567795, 1362268990875, 224229141506, 2092865456148, −301525068860, 2081510046657, −398952907693, 2330201794229, −255178406315, 1066318926881, 493751897628, 1729740541006, −103759157461, 2173771486057, −620363038292, 1867081383268, −151277221788, 1353941271448, 179948629945, 1479240060095, 342020052730, 2184516411619, −717841372895, 650389362044, −44740662985, 2315655696498, −4478644809, 1378542962891, −77525487333, 893047645591, 179430931459, 1668844385937, −220938039747, 1238056324819, −388417780359, 1758644487369, 49162113897, 574831985668, 101296936710, 1580353533011, 106296616993, 578837428302, −424400197895, 1585976564060, −288654893227, 1661210261127, 439833142557, −247202126371, −189885602018, 1069320100511, 14965483619, 1372382819001, −350945437549, 1166656722085, −26875340031, −112046953946, 264482159358, 971939323123, 315443374, 737076751102, −242050923233, 625328766932, −163049388264, 651831316391, 103505212143, 150204548047, 48732385133, 676366606419, 22487056291, 50736674216, 12330433962, 876281794400, −244619123714, −23141241475, −425071710999, 173800142051, 871047731302, −22908844162, 21071113068, 33711180585, -856494602158, 969230569158].

This element has norm 12799:

[184037827075, 27497694581842, −19626196308, 27547128880119, 110431733149, 27555147977579, −43762006334, 27628048533330, 363210681747, 27670842645800, 33491843358, 27407323326486, 288418234223, 27749482284368, 315874648397, 27372865864009, 330043125975, 27299903871399, 340523125682, 27015368233356, 391243147017, 27071327899417, 288329303744, 26642786767103, 149912398940, 26500392938787, 109894359842, 26144374880238, 146407833367, 26161831207103, −57910866992, 25492292196379, −274642305172, 25540457641474, 142369219973, 25160228118999, −129682164625, 24702675340198, −69429495725, 24538098116712, 46349415635, 24444616969505, 156136351425, 23931205738586, −2961224626, 23705831310594, 256615446179, 23524258730874, 140896966972, 23256896414578, 205005339494, 22739364944777, −15843992634, 22345779576504, 357116818963, 22065388666012, 80818167553, 21316751144174, −43890778334, 20910703796699, 42084499799, 20484469377007, 77475653685, 19785027507686, −263756725875, 19271681904259, −103004425019, 19020439605835, −269420692984, 18334556916614, −208404770122, 17932081887237, −248797915350, 17310365165180, −126861808332, 17069655283837, −89882204515, 16366181711576, −70223384746, 15894548371886, 59088655957, 15314097572833, 224287929661, 14934547282661, 44599857235, 14137788660464, 57486988045, 13843047543817, 144867254487, 12982325354549, −13428448847, 12509458887132, 8304629546, 11689066750504, −249842160599, 11153328440462, −30856843432, 10351054047936, −226948948743, 9587784962712, −178179267698, 8855105075807, −263989946416, 8459099826011, −46611349150, 7581871533541, −417612144252, 6960647418598, 53356750842, 6559779943246, −164811255782, 5847169871093, −22801282585, 5276876192677, −133695961049, 4561501186914, 267900193832, 4087343983235, 106671432015, 3102753616610, 112993348875, 2619490858980, 125041798071, 1829389680073, 297752663615, 1181872802028, -53529707223, 69559134213].

This element has norm 13313:

[8916659723289, 47268532674, 8908556110733, 70481864656, 8937291165906, 67739426562, 8861569846044, −7725649614, 8829707041453, 47638278771, 8861390871712, 48133856326, 8764144540244, −48910258200, 8687350180924, 1357021369, 8733804704947, 29074824782, 8616774037745, −70624616649, 8540760686368, −24859730341, 8532405397014, −11889210622, 8459821763982, −28518190023, 8372357336801, −56800374255, 8301117283526, −11761801095, 8281446215115, 17501367664, 8184340584635, −33759340894, 8063590959098, −5354668175, 8064978655183, 85625679864, 7966412060993, −8044159715, 7800415831985, 33108335988, 7800989809347, 100637609567, 7667310373669, 32871123796, 7512849402161, 35302340094, 7428424479889, 77578363916, 7318557559367, 52248738806, 7146998380511, 14965239152, 7002340196323, 20703950879, 6889137463326, 58623632102, 6752305608406, −14386714403, 6508893132068, −45339801496, 6432979746206, 50051731390, 6282439291691, −47946996920, 6027018399904, −74116504992, 5922613371875, 7112222086, 5791260006111, −33927849059, 5550734846917, −74105570364, 5414865621403, −7413305441, 5276451123686, −5031097618, 5096944465149, −12408772293, 4898309553471, −26654004178, 4753486648791, 61879736346, 4623095676929, 27625581497, 4356719254730, −11365677549, 4213264031932, 85683966203, 4081483059666, 64666311773, 3800571512362, −11699782794, 3619743124051, 84748679823, 3489223839999, 61110804212, 3204599108570, 3360620284, 3005433193669, 28675626079, 2812542786776, 40010051208, 2606574214541, 6075789802, 2332601110596, −49927165145, 2123416470081, 2846966847, 1957178717014, −2476742731, 1677693344486, −96508928231, 1427324401528, −31753778165, 1316756845314, 5835444314, 1028165661555, −97373171807, 795695608823, −24168787111, 656098328404, 2267514151, 418089679287, −30049678195, 184507943986, −25303639014].

□

While it is a straightforward matter to verify that the above elements have the desired norms, actually finding these elements poses a challenge. Since we must search a lattice of 128 dimensions, a brute force approach of searching over a suitably sized "box" is impractical. For example, given an integral basis, if we were to search all elements with coefficients between -2 and 2, that would mean checking the norms of $5^{128} \approx 10^{89}$ elements, which is substantially larger than the number of particles in the universe!

The more practical approach is to search over "sparse" vectors. The hope would be that we could find the desired elements of small prime norm, or elements that factor over primes of small norm and produce relations in the class group.

First we'll describe this process for the smaller field, $\mathbb{Q}(\zeta_{256})^+$, and then contrast it with the situation presented by $\mathbb{Q}(\zeta_{512})^+$.

Example 3.2.5 (Finding elements of small prime norm in $\mathbb{Q}(\zeta_{256})^+$)**.** The goal is to find algebraic integers in $\mathbb{Q}(\zeta_{256})^+$ which have norms that are prime and congruent to ± 1 modulo 256, i.e. the primes which totally split. The ten smallest of these are 257, 769, 1279, 3329, 3583, 5119, 6143, 6911, 7681, and 7937.

The integral basis that we'll use is $\{b_0, b_1, \ldots, b_{63}\}$ where $b_0 = 1$ and $b_j = 2\cos(2\pi j/256)$ for j from 1 to 63. We will search over sparse vectors where at most six coefficients are nonzero, and the nonzero coefficients are either 1 or -1. When we search over these sparse vectors, we do indeed find the ten prime norms we were looking for. For example, the element $b_0 + b_1 + b_{14}$ has norm 257, and the element $b_0 - b_3 + b_4 - b_{22} - b_{34} - b_{53}$ has norm 6143.

What happens if we repeat this above process with similar sparse vectors for the larger field $\mathbb{Q}(\zeta_{512})^+$? Unfortunately, we do not find any elements of small prime norm. In fact, the two smallest prime norms found this way are rather large: 6147073 and

9627649. In this respect, the properties of the field $\mathbb{Q}(\zeta_{512})^+$ are markedly different than that of the smaller field $\mathbb{Q}(\zeta_{256})^+$, so another approach is required.

Perhaps the best way to illustrate the approach used is to explicitly write down the particular calculations. We start with the integral basis $\{b_0, b_1, \ldots, b_{127}\}$ where $b_0 = 1$ and $b_j = 2\cos(2\pi j/512)$ for j from 1 to 127. As mentioned above, searching over sparse vectors led to two elements of prime norm:

$$N(b_0 + b_1 - b_8 - b_9 + b_{48}) = 6147073$$

$$N(b_0 + b_1 + b_2 + b_9 + b_{10} - b_{48}) = 9627649$$

We may also consider algebraic integers with norms which are even, since we can always repeatedly divide by any element of norm 2, such as b_1, until we get an algebraic integer of odd norm. For example,

$$b_1^{-2}(b_1 + b_{10} + b_{26} + b_{35} + b_{43} + b_{50} + b_{52} + b_{95}),$$

is algebraic integer of norm 1142783.

Another useful element is

$$b_1^{-1}(b_1 + b_{18} - b_{39} + b_{108} + b_{127}),$$

which has norm $9627649 \cdot 2078207$. This produces a relationship in the class group between a prime of norm 9627649, which is known to be principal, and a prime of norm 2078207. Therefore all primes of norm 2078207 are principal, and there exists a unique Galois automorphism σ for which

$$\frac{b_1^{-1}(b_1 + b_{18} - b_{39} + b_{108} + b_{127})}{\sigma(b_0 + b_1 + b_2 + b_9 + b_{10} - b_{48})}$$

is an algebraic integer of norm 2078207.

However, further search by the author of sparse vectors using the basis $\{b_0, \ldots, b_{127}\}$ found neither elements of small prime norm nor elements which produce useful relations in the class group. To find more suitable elements, we choose a different basis over which to search sparse vectors. For k from 0 to 127, put

$$c_k = \sum_{j=0}^{k} b_j.$$

The c_k are the cyclotomic units, and $\{c_0, \ldots, c_{127}\}$ form an integral basis. Sparse vectors over this basis can produce some algebraic integers of relatively small norm or produce interesting class group relations. Two algebraic integers that prove to be of critical importance are

$$c_0 + c_6 + c_{15} + c_{39} - c_{104} + c_{111} + c_{120}$$

which has norm $2078207 \cdot 6215646209$, and

$$c_0 + c_3 + c_{19} + c_{64} - c_{71} + c_{103} + c_{119}$$

which has norm $6143^2 \cdot 6215646209$. By choosing the appropriate Galois conjugates and taking quotients, we can explicitly write down an algebraic integer of norm 6215646209 and then also an algebraic integer α of norm 6143^2.

In the subfield $\mathbb{Q}(\zeta_{256})^+$, it is easy to find an algebraic integer of norm 6143 and by including that element in the larger field, we produce an algebraic integer β of norm 6143^2. One example is

$$\beta = b_0 - b_6 + b_8 - b_{44} - b_{68} - b_{106}.$$

Now given α and β as above, which both have norm 6143^2, consider the quotients $\sigma(\alpha)/\beta$ for each Galois automorphism σ. A calculation shows that none of the quotients are algebraic integers. Thus, we have an inequality of principal ideals

$$(\sigma(\alpha)) \neq (\beta)$$

for every σ.

Let η denote a generator of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{512} + \zeta_{512}^{-1})/\mathbb{Q})$, which is cyclic of order 128. Then η^{64} fixes the subfield $\mathbb{Q}(\zeta_{256} + \zeta_{256}^{-1})$, and

$$(\beta) = P \cdot \eta^{64}(P)$$

where P is some prime ideal of norm 6143 (noting that, as a prime of $\mathbb{Q}(\zeta_{256} + \zeta_{256}^{-1})$, β lies over 6143 so it does indeed split in $\mathbb{Q}(\zeta_{512} + \zeta_{512}^{-1})$).

For suitably chosen automorphism σ, we have that

$$(\sigma(\alpha)) = \tau(P) \cdot \eta^{64}(P)$$

where τ is not the identity automorphism. Taking quotients shows

$$\frac{P}{\tau(P)}$$

is a principal fractional ideal. Suppose τ has order m in the Galois group. Since τ is not the identity automorphism, m must be even, so

$$\frac{P}{\eta^{64}(P)} = \frac{P}{\tau^{m/2}(P)} = \frac{P}{\tau(P)}\frac{\tau(P)}{\tau^{2}(P)} \cdots \frac{\tau^{m/2-1}P}{\tau^{m/2}(P)}$$

is a principal fractional ideal. Thus

$$P^2 = (\beta)\frac{P}{\eta^{64}(P)}$$

is a principal ideal. But Weber [36] showed that the class number is odd, so P itself must be a principal ideal of norm 6143. This approach can be further extended to calculate an actual generator of P.

Once we have shown that a prime of such small norm is principal, it is relatively easy to use sparse vectors to generate more class group relations to show that other prime ideals of small norm are principal and to find their generators.

3.2.4 Divisibility properties of the class numbers of real cyclotomic fields

In the previous sections concerning cyclotomic fields of prime conductor or power of 2 conductor, we were able to take advantage of the extensive work of Schoof [31] on the divisibility properties of class numbers h_p^+ for p prime, and of Fukuda and Komatsu [10] on the divisibility properties of class numbers $h_{2^k}^+$.

However, once we move away from prime power conductors, the size of the quotient group $\mathcal{O}^\times/\mathcal{O}_{\text{cyc}}^\times$ is no longer equal to the class number, and the method of Schoof can not be directly applied. To some extent, Agathocleous, in her thesis [1], was able to get around this problem, but with the limitation of considering only composite conductors that are products pq of two distinct odd primes. This is actually quite a severe limitation for us: only 9 of the 50 fields of composite conductor that we consider have odd composite conductors of the form pq.

Therefore, in the current subsection, we return to the classical approach of exploiting the Galois action on the class group itself, as implemented by Masley [17] and van der Linden [16]. This approach has its limitations, especially when considering the p-part of the class number where p divides the degree of the field. Nevertheless, by establishing quite good upper bounds on the class numbers, we are able to successfully use these methods.

In order to carry out our strategy, we use several theorems described by van der Linden [16], Masley [17] and Washington [34].

Parity Check Theorem ((Masley [17], Thm 2.21))**.** *If h_m^- is odd, then h_m^+ is odd.*

Reflection Theorem ((Masley [17], Thm 2.22))**.** *Let p be a prime integer, and let M be the least common multiple of p and the conductor m. If p does not divide h_M^-, then p does not divide h_m^+.*

We will use the tables in Washington [34, p. 412] to find the minus part h_m^- of the class number.

Pushing Up Theorem ((Washington [34], Prop 4.11))**.** *Let L/K be an extension of number fields. If no intermediate field $M \neq K$ of L/K is abelian over K and unramified (at all primes, including the Archimedean ones) over K, then h_K divides h_L.*

Corollary 6. *h_m^+ divides h_{km}^+ for any positive integer k.*

Corollary 7. *If K is a subfield of a real cyclotomic field of prime power conductor p^k, then h_K divides $h_{p^k}^+$.*

Pushing Down Theorem ((Washington [34], Thm 10.4))**.** *Let L/K be a Galois extension of number fields whose degree is a power of a prime p. Suppose that there is at most one prime (finite or infinite) of K that ramifies in L. If p does not divide h_K, then p does not divide h_L.*

Theorem 3.2.6 ((Masley [17], Thm 2.10))**.** *Let $m = 4p, pq$ or $2^a q$, with $a \geq 3$, p and q odd primes, and $q \equiv 3 \pmod 4$. Then the maximal real abelian 2-extension K of $\mathbb{Q}$ with conductor m has odd class number.*

Rank Theorem ((Masley [17], Cor 2.15))**.** *Let L/K be a cyclic extension of degree n. Let p be a prime that does not divide h_E for all intermediate fields E with $K \subseteq E \subsetneq L$. If p divides h_L, then p^f divides h_L, where f is the order of p modulo n.*

We also give the more precise version of the Rank Theorem described by van der Linden [16]. Given a cyclic extension of number fields L/K of degree n, and a prime p not dividing n, we define $\mathrm{Cl}_p^*(L/K)$ to be

$$\mathrm{Cl}_p^*(L/K) = \{\alpha \in \mathrm{Cl}_p(L) : \alpha^{\Phi_n(\sigma)} = 1\},$$

where $\mathrm{Cl}_p(L)$ is the Sylow p-subgroup of the class group of L, σ is the generator of $\mathrm{Gal}(L/K)$, and Φ_n is the nth cyclotomic polynomial. For example, given the trivial extension K/K, we have $\mathrm{Cl}_p^*(K/K) = \mathrm{Cl}_p(K)$.

Theorem 3.2.7 ((van der Linden [16], Thm 8))**.** *Let L/K be a cyclic extension of degree n. Let p be a prime that does not divide n. Then $|\mathrm{Cl}_p^*(L/K)|$ is a power of p^f, possibly 1, where f is the order of p modulo n.*

Theorem 3.2.8 ((van der Linden [16], Thm 6))**.** *Let E/K be an abelian extension of number fields of degree n, and let p be a prime integer not dividing n. Then*

$$\mathrm{Cl}_p(E) \cong \oplus \, \mathrm{Cl}_p^*(L/K),$$

where the direct sum is over all the intermediate fields L for which L/K is cyclic.

Corollary 8. *Suppose p, K and E are as in the theorem above. If p divides h_E, then there exists a cyclic extension L/K, with $K \subseteq L \subseteq E$ and p dividing h_L.*

3.2.5 The class number of the real cyclotomic field of conductor 148

We give a detailed example of applying our upper bound to find the class number of the real cyclotomic field of conductor 148.

Van der Linden [16] proved that the class number of $\mathbb{Q}(\zeta_{148})^+$ has class number 1, conditional upon the generalized Riemann hypothesis. The root discriminant of this field is approximately 66.94, which is greater than 60.704, so Odlyzko's discriminant bounds could not be used to establish an unconditional upper bound on the class number. However, using our class number upper bound, we can now unconditionally prove that the real cyclotomic field of conductor 148 has class number 1.

Proposition 3.2.9. *The class number of* $\mathbb{Q}(\zeta_{148})^+$ *is* 1.

Proof. First, using our integral basis $\{b_0, b_1, \ldots, b_{n-1}\}$, we search over "sparse vectors" and find two elements of the ring of integers that have norms of 149 and 443.

$$N(b_0 + b_1 + b_8) = 149$$

$$N(b_0 + b_1 + b_9) = 443$$

Since the prime integers 149 and 443 are congruent to ±1 modulo 148, they totally split in $\mathbb{Q}(\zeta_{148})^+$, and split into principal ideals generated by the above elements and their conjugates.

We define our set S to be

$$S = \{149, 443\}.$$

Let F be the function

$$F(x) = \frac{e^{-(x/c)^2}}{\cosh \frac{x}{2}}$$

with $c = 20$. The contribution from prime ideals of the Hilbert class field is bounded below by

$$2\sum_{p\in S}\sum_{m=1}^{\infty}\frac{\log p}{p^{m/2}}F(m\log p) > 2\sum_{p\in S}\frac{\log p}{\sqrt{p}}F(\log p) > 0.1753.$$

The below integral can be estimated using numerical integration.

$$\int_0^{\infty}\frac{1-F(x)}{2}\left(\frac{1}{\sinh\frac{x}{2}}+\frac{1}{\cosh\frac{x}{2}}\right)dx < 1.2825.$$

Thus we find a lower bound for B,

$$\begin{aligned}B = \frac{\pi}{2}+\gamma+\log 8\pi-\log\mathrm{rd}(\mathbb{Q}(\zeta_{148})^+)-\int_0^{\infty}\frac{1-F(x)}{2}\left(\frac{1}{\sinh\frac{x}{2}}+\frac{1}{\cosh\frac{x}{2}}\right)dx\\ +2\sum_{p\in S}\sum_{m=1}^{\infty}\frac{\log p}{p^{m/2}}F(m\log p) > 0.0611.\end{aligned}$$

Now we can apply Theorem 2.3.1 to show that the class number has an upper bound

$$h_{148}^+ \leq 32.$$

It remains to use divisibility arguments to show that the class number is 1. We consider the possible prime divisors of h_{148}^+.

2-part Since $h_{148}^- = 4827501$ is odd, the Parity Check Theorem shows that h_{148}^+ is odd.

3-part The degree of $\mathbb{Q}(\zeta_{148})^+$ is 36. Consider its quartic subfield K_4. The prime integer 37 is totally ramified in K_4 and factors as

$$(37) = P^4$$

for a prime ideal P. The prime P is the only prime that ramifies in the degree 9 extension $\mathbb{Q}(\zeta_{148})^+/K_4$. Since K_4 has class number 1 (which has small enough degree that it can be calculated unconditionally in a software package such as Sage [29]), we can use the Pushing Down Theorem to show that 3 does not divide h_{148}^+.

p-part, $5 \leq p \leq 31$ $\mathbb{Q}(\zeta_{148})^+/\mathbb{Q}$ is a cyclic extension. Every proper subfield of $\mathbb{Q}(\zeta_{148})^+$ is either a subfield of $\mathbb{Q}(\zeta_{37})^+$, or is the degree 12 subfield K_{12}, or is the quartic subfield K_4. Using Sage, we can calculate unconditionally the K_4 and K_{12} have class number 1. Also, the subfield $\mathbb{Q}(\zeta_{37})^+$ has class number 1. Since $\mathbb{Q}(\zeta_{37})^+/\mathbb{Q}$ is totally ramified at 37, by the Pushing Up Theorem every subfield of $\mathbb{Q}(\zeta_{37})^+$ has class number 1. Thus, using the extension $\mathbb{Q}(\zeta_{148})^+/\mathbb{Q}$ and the upper bound $h_{148}^+ \leq 32$, we can apply the Rank Theorem to show that p does not divide h_{148}^+ for all p between 5 and 31.

Using the upper bound $h_{148}^+ \leq 32$, we conclude unconditionally that $h_{148}^+ = 1$.

□

Note that the Minkowski bound of $\mathbb{Q}(\zeta_{148})^+$ is approximately 2.5×10^{18}. It is striking, using our new approach, we needed to only check if *two* primes, 149 and 443, factored into principal ideals, in stark contrast to using the Minkowski bound, which would have required checking roughly 6×10^{16} primes!

As an alternative proof, in the following section we will show below that an upper bound of h_{148}^+ is 1, thus showing that $h_{148}^+ = 1$, without need for any additional algebraic arguments.

3.2.6 Upper bounds for class numbers of real cyclotomic fields of degree less than or equal to 58

Consider the real cyclotomic field of conductor m with degree n. For real cyclotomic fields of relatively small degree, it is possible to use relatively few prime ideals to find a class number upper bound. However, for fields of larger degree, the number of primes required is much greater. Our strategy will be to search over sparse vectors using both the basis $b_0, b_1, \dots b_{n-1}$ described above, as well as using an alternative basis,

$$c_k = \sum_{j=0}^{k} b_j, \quad k = 0, 1, \dots, n-1.$$

The advantage of using the alternative basis is its tendency to find elements that are of different norm than those found using sparse vectors in the original basis.

We calculate the norm of every element of the ring of integers of the form

$$x = b_0 + b_1 + a_1 b_{j_1} + a_2 b_{j_2} + a_3 b_{j_3} + a_4 b_{j_4} + a_5 b_{j_5},$$

and

$$x = b_1 + a_1 b_{j_1} + a_2 b_{j_2} + a_3 b_{j_3} + a_4 b_{j_4} + a_5 b_{j_5},$$

where $1 < j_1 < j_2 < j_3 < j_4 < j_5 < n$ and $a_j \in \{-1, 0, 1\}$ for $1 \leq j \leq 5$. Similarly, using the alternative basis, we also calculate the norm of every element of the form

$$x = c_0 + a_1 c_{k_1} + a_2 c_{k_2} + a_3 c_{k_3} + a_4 c_{k_4} + c_5 b_{k_5},$$

where $1 \leq k_1 < k_2 < k_3 < k_4 < k_5 < n$ and $a_k \in \{-1, 0, 1\}$ for $1 \leq k \leq 5$.

Let T denote the set of all such elements x, and let S denote the set of norms that are prime, congruent to ± 1 modulo the conductor m, and less than 10^{10},

$$S = \{N(x) : x \in T, N(x) \text{ prime}, N(x) \equiv \pm 1 \pmod{m}, N(x) < 10^{10}\}.$$

We calculate the set S for every real cyclotomic field of composite conductor m of degree up to 58, i.e. with $\phi(m) \leq 116$, except for the fields that have already been treated unconditionally by Masley or van der Linden. We also exclude the conductor 212, for reasons to be discussed later. We then apply Theorem 2.3.1. The results are given in Table 4.3 of conductors m, parameter c, and upper bounds of class numbers h_m^+.

m	c	$h_m^+ \le$
115	18	1
119	20	2
121	26	4
123	19	2
125	22	2
129	19	2
133	25	3
141	20	2
145	50	36
147	18	1
148	17	1
152	17	1
153	21	2
159	25	3
164	20	2
165	15	1
171	26	4
172	20	2
176	20	2
177	29	5
184	22	3
188	23	3
189	24	3
195	21	1
196	20	2
200	18	1
204	15	1
208	25	3
216	18	1
220	18	1
224	22	2
228	15	1
232	30	8
236	48	29
240	15	1
252	15	1
260	21	2
264	18	1
276	20	2
280	20	2
288	24	3
300	18	1
312	20	2
324	28	5
336	21	2
348	26	4
360	21	2
420	18	1

We are free to choose the parameter c. Recall that our class number bound is $h < 2c\sqrt{\pi}/nB$. If c is chosen to be too small, then the lower bound for the denominator B would be nonpositive or very small. On the other hand, if c is too large, this leads directly to a large class number bound. Thus, there is an optimal c that provides the best possible bound. However, since the class number is an integer, the class number bound is usually not sensitive to the precise choice of c, so it is easy to just compute an optimal c by testing in a reasonable interval.

We should also remark that if we had calculated the table of class number upper bounds using summations over a larger number of principal prime ideals, then we could have improved upper bounds, obviating the need for some of the algebraic arguments in Subsection 3.2.7. There is a trade-off between the amount of computation and the amount of algebraic argumentation.

3.2.7 Class numbers of real cyclotomic fields of degree up to 58

The above upper bounds are sufficiently strong to immediately show that the real cyclotomic fields of conductors

$$115, 147, 148, 152, 165, 195, 200, 204, 216, 220, 228, 240, 252, 264, 300, 420$$

have class number 1.

In the following, all invocations of the Parity Check Theorem and the Reflection Theorem use minus parts of the class numbers obtained from the table in Washington

[34, p. 412]. In particular, an application of the Parity Check Theorem shows that the real cyclotomic fields of conductors

$$119, 129, 141, 125, 176, 196$$

also have class number 1.

For conductor 145, we will need a better upper bound, so the proof of that class number will be postponed until the next section. The remaining fields are treated below.

Proposition 3.2.10. *The class number of* $\mathbb{Q}(\zeta_{121})^+$ *is* 1.

Proof. We have the upper bound $h_{121}^+ \leq 4$. By the Parity Check Theorem, h_{121}^+ is odd. The least common multiple of 3 and 121 is 363. Since 3 does not divide h_{363}^-, the Reflection Theorem shows that 3 does not divide h_{121}^+. □

Proposition 3.2.11. *The class numbers of* $\mathbb{Q}(\zeta_{123})^+$, $\mathbb{Q}(\zeta_{153})^+$, $\mathbb{Q}(\zeta_{164})^+$ *and* $\mathbb{Q}(\zeta_{224})^+$ *are* 1.

Proof. Let L denote one of these fields, and let K denote the maximal 2-subextension of $L/\mathbb{Q}$. We have the upper bound for the class number $h(L) \leq 2$. By Theorem 3.2.6, the class number of K is odd. We apply the Rank Theorem to the extension L/K to show that $h(L)$ is odd. □

Proposition 3.2.12. *The class number of* $\mathbb{Q}(\zeta_{133})^+$ *is* 1.

Proof. We know $h_{133}^+ \leq 3$. We apply Theorem 3.2.8 to the degree 27 extension $\mathbb{Q}(\zeta_{133})^+/\mathbb{Q}(\sqrt{133})$. The cyclic subextensions are of degree 1, 3 or 9. Since the class number of $\mathbb{Q}(\sqrt{133})$ is 1, by Theorems 3.2.7 and 3.2.8, the 2-part of h_{133}^+ must be a power of 4. Since $h_{133}^+ \leq 3$, we have that h_{133}^+ is odd.

For the 3-part, consider the sectic subfield K of $\mathbb{Q}(\zeta_{133})^+$ that has discriminant $7^5 \cdot 19^3$. The class number of K is 1. The prime integer 19 factors as $(19) = P^2$ in K for a prime ideal P. The prime P is the only prime of K that ramifies in $\mathbb{Q}(\zeta_{133})^+$, so we can apply the Pushing Down Theorem to show that 3 does not divide h_{133}^+. □

Proposition 3.2.13. *The class number of* $\mathbb{Q}(\zeta_{159})^+$ *is* 1.

Proof. We know $h_{159}^+ \leq 3$. By the Parity Check Theorem, h_{159}^+ is odd. Every proper subfield of $\mathbb{Q}(\zeta_{159})^+$ is either the quartic subfield K_4, is is a subfield of $\mathbb{Q}(\zeta_{53})^+$. Using Sage [29] we can calculate unconditionally that the class number of K_4 is 1. Also, $\mathbb{Q}(\zeta_{53})^+$ has class number 1. Since $\mathbb{Q}(\zeta_{53})^+/\mathbb{Q}$ is totally ramified at 53, by the Pushing Up Theorem every subfield of $\mathbb{Q}(\zeta_{53})^+$ has class number 1. Therefore, we can apply the Rank Theorem to the extension $\mathbb{Q}(\zeta_{159})^+/\mathbb{Q}$ to show that 3 does not divide h_{159}^+. □

Proposition 3.2.14. *The class number of* $\mathbb{Q}(\zeta_{171})^+$ *is* 1.

Proof. We know $h_{171}^+ \leq 4$. We apply Theorem 3.2.8 to the degree 27 extension $\mathbb{Q}(\zeta_{171})^+/\mathbb{Q}(\sqrt{57})$. The cyclic subextensions are of degree 1, 3 or 9. The class number of $\mathbb{Q}(\sqrt{57})$ is 1, and the four cubic extensions of $\mathbb{Q}(\sqrt{57})$ contained in $\mathbb{Q}(\zeta_{171})^+$ all have odd class number (either 1 or 3). So we need only concern ourselves with the degree 9 cyclic subextensions of $\mathbb{Q}(\zeta_{171})^+/\mathbb{Q}(\sqrt{57})$. Therefore, by Theorems 3.2.7 and 3.2.8, the 2-part of h_{171}^+ must be a power of 64. Since $h_{171}^+ \leq 4$, we have that h_{171}^+ is odd.

The prime 3 factors as $(3) = P^2$ in $\mathbb{Q}(\zeta_{57})^+$ for a prime ideal P. The prime P is the only prime of $\mathbb{Q}(\zeta_{57})^+$ that ramifies in $\mathbb{Q}(\zeta_{171})^+$, so we can apply the Pushing Down Theorem to show that 3 does not divide h_{171}^+. □

Proposition 3.2.15. *The class number of* $\mathbb{Q}(\zeta_{172})^+$ *is* 1.

Proof. We know $h_{172}^{+} \leq 2$. $\mathbb{Q}(\zeta_{172})^{+}$ is of degree 42. Let K denote its sectic subfield. We can use Sage [29] to show unconditionally that the class number of K is 1. We apply the Rank Theorem to the extension $\mathbb{Q}(\zeta_{172})^{+}/K$ to show that h_{172}^{+} is odd. □

Proposition 3.2.16. *The class number of* $\mathbb{Q}(\zeta_{177})^{+}$ *is* 1.

Proof. We know $h_{177}^{+} \leq 5$. By the Parity Check Theorem, h_{177}^{+} is odd. Every proper subfield of $\mathbb{Q}(\zeta_{177})^{+}$ is either $\mathbb{Q}(\sqrt{177})$ or is a subfield of $\mathbb{Q}(\zeta_{59})^{+}$. The quadratic subfield $\mathbb{Q}(\sqrt{177})$ has class number 1. Also, $\mathbb{Q}(\zeta_{59})^{+}$ has class number 1, as do its subfields by the Pushing Down Theorem. Therefore we can apply the Rank Theorem to the degree 58 cyclic extension $\mathbb{Q}(\zeta_{177})^{+}/\mathbb{Q}$ to show that neither 3 nor 5 divide h_{177}^{+}. □

Proposition 3.2.17. *The class numbers of* $\mathbb{Q}(\zeta_{184})^{+}$ *and* $\mathbb{Q}(\zeta_{276})^{+}$ *are* 1.

Proof. These fields have degree 44. Let L denote either of these fields, and K denote the quartic subfield. We know $h(L) \leq 3$. We can use Sage [29] to show unconditionally that the class number of K is 1. We apply the Rank Theorem to the extension L/K to show that neither 2 nor 3 divide h_L. □

Proposition 3.2.18. *The class number of* $\mathbb{Q}(\zeta_{188})^{+}$ *is* 1.

Proof. We know $h_{188}^{+} \leq 3$. By the Parity Check Theorem, h_{188}^{+} is odd. The least common multiple of 3 and 188 is 576. Since 3 does not divide h_{576}^{-}, the Reflection Theorem shows that 3 does not divide h_{188}^{+}. □

Proposition 3.2.19. *The class number of* $\mathbb{Q}(\zeta_{189})^{+}$ *is* 1.

Proof. We know $h_{189}^{+} \leq 3$. By the Parity Check Theorem, h_{189}^{+} is odd. The least common multiple of 3 and 189 is 189. Since 3 does not divide h_{189}^{-}, the Reflection Theorem shows that 3 does not divide h_{189}^{+}. □

Proposition 3.2.20. *The class numbers of* $\mathbb{Q}(\zeta_{208})^+$ *and* $\mathbb{Q}(\zeta_{288})^+$ *are* 1.

Proof. Let $m = 208$ or 288. We know $h_m^+ \leq 3$. By the Parity Check Theorem, h_m^+ is odd. Consider the degree 4 cyclic extension $\mathbb{Q}(\zeta_m)^+/\mathbb{Q}(\zeta_{m/4})^+$. Since we already know that $h_{m/4}^+ = h_{m/2}^+ = 1$, we can apply the Rank Theorem to the extension $\mathbb{Q}(\zeta_m)^+/\mathbb{Q}(\zeta_{m/4})^+$ to show that 3 does not divide h_m^+. □

Proposition 3.2.21. *The class number of* $\mathbb{Q}(\zeta_{232})^+$ *is* 1.

Proof. We know $h_{232}^+ \leq 8$.

The prime integer 2 is inert in $\mathbb{Q}(\zeta_{29})^+$. The prime ideal (2) is the only prime that ramifies in the degree 4 extension $\mathbb{Q}(\zeta_{232})^+/\mathbb{Q}(\zeta_{29})^+$. Since $h_{29}^+ = 1$, the Pushing Down Theorem shows that h_{232}^+ is odd.

Now let K be the octic subfield of $\mathbb{Q}(\zeta_{232})^+$. Since the class number of K is 1, we can apply the Rank Theorem to the degree 7 extension $\mathbb{Q}(\zeta_{232})^+/K$ to find that h_{232}^+ is not divisible by 3 or 5.

The prime 29 factors as $(29) = P^2$ in K for a prime ideal P. P is the only prime of K that ramifies in $\mathbb{Q}(\zeta_{232})^+$, so we can apply the Pushing Down Theorem to show that 7 does not divide h_{232}^+. □

Proposition 3.2.22. *The class number of* $\mathbb{Q}(\zeta_{236})^+$ *is* 1.

Proof. We know $h_{236}^+ \leq 29$. Since the class number of $\mathbb{Q}(\sqrt{59})$ is 1, we can apply the Rank Theorem to the degree 29 cyclic extension $\mathbb{Q}(\zeta_{236})^+/\mathbb{Q}(\sqrt{59})$ to show that no prime less than 29 divides h_{236}^+.

It remains to show that 29 does not divide h_{236}^+. The only prime ideal of $\mathbb{Q}(\sqrt{59})$ that ramifies in $\mathbb{Q}(\zeta_{236})^+$ is $(\sqrt{59})$, so we can apply the Pushing Down Theorem to show that 29 does not divide h^+_{236}. □

Proposition 3.2.23. *The class number of* $\mathbb{Q}(\zeta_{260})^+$ *is* 1.

Proof. We know $h^+_{260} \leq 2$, and $\mathbb{Q}(\zeta_{260})^+$ is of degree 48. Let L denote its degree 16 subfield. L has three octic subfields. Let K denote the octic subfield with discriminant $2^8 \cdot 5^4 \cdot 13^6$. Sage [29] can show unconditionally that K has class number 1. The prime integer 5 factors as $(5) = P^2$ in K for a prime ideal P. The only prime ideal of K that ramifies in L is P, so by the Pushing Down Theorem, the class number of L is odd. Now we can apply the Rank Theorem to the extension $\mathbb{Q}(\zeta_{260})^+/L$ to show that h^+_{260} is odd. □

Proposition 3.2.24. *The class numbers of* $\mathbb{Q}(\zeta_{280})^+$, $\mathbb{Q}(\zeta_{312})^+$ *and* $\mathbb{Q}(\zeta_{360})^+$ *are* 1.

Proof. Let $m = 280$, 312 or 360. We know $h^+_m \leq 2$. The prime integer 2 is inert in $\mathbb{Q}(\zeta_{m/8})^+$. The prime ideal (2) is the only prime that ramifies in the degree 4 extension $\mathbb{Q}(\zeta_m)^+/\mathbb{Q}(\zeta_{m/8})^+$. Since $h^+_{m/8} = 1$, the Pushing Down Theorem shows that h^+_m is odd. □

Proposition 3.2.25. *The class number of* $\mathbb{Q}(\zeta_{324})^+$ *is* 1.

Proof. We know $h^+_{324} \leq 5$. By the Parity Check Theorem, h^+_{324} is odd. The least common multiple of 3 and 324 is 324. Since 3 does not divide h^-_{324}, the Reflection Theorem shows that 3 does not divide h^+_{324}.

Finally, since $\mathbb{Q}(\zeta_{324})^+$ is cyclic of degree 54, every proper subfield of $\mathbb{Q}(\zeta_{324})^+$ is a subfield of $\mathbb{Q}(\zeta_{81})^+$, which has class number 1. Since $\mathbb{Q}(\zeta_{81})^+/\mathbb{Q}$ is totally ramified at 3, by the Pushing Up Theorem every subfield of $\mathbb{Q}(\zeta_{81})^+$ has class number 1. Therefore, we can apply the Rank Theorem to the extension $\mathbb{Q}(\zeta_{324})^+/\mathbb{Q}$ to show that 5 does not divide h_{324}^+.

□

Proposition 3.2.26. *The class number of* $\mathbb{Q}(\zeta_{336})^+$ *is* 1.

Proof. We know $h_{336}^+ \leq 2$. The prime integer 2 is inert in $\mathbb{Q}(\zeta_{21})^+$. The prime ideal (2) is the only prime that ramifies in the degree 8 extension $\mathbb{Q}(\zeta_{336})^+/\mathbb{Q}(\zeta_{21})^+$. Since $h_{21}^+ = 1$, the Pushing Down Theorem shows that h_{336}^+ is odd. □

Proposition 3.2.27. *The class number of* $\mathbb{Q}(\zeta_{348})^+$ *is* 1.

Proof. We know $h_{348}^+ \leq 4$. The prime integer 2 is inert in $\mathbb{Q}(\zeta_{87})^+$. The prime ideal (2) is the only prime that ramifies in the quadratic extension $\mathbb{Q}(\zeta_{348})^+/\mathbb{Q}(\zeta_{87})^+$. Since $h_{87}^+ = 1$, the Pushing Down Theorem shows that h_{348}^+ is odd.

Now let K be the octic subfield of $\mathbb{Q}(\zeta_{348})^+$. Since the class number of K is 1, we can apply the Rank Theorem to the degree 7 extension $\mathbb{Q}(\zeta_{348})^+/K$ to find that h_{348}^+ is not divisible by 3. □

3.2.8 The class number of the real cyclotomic field of conductor 145

Under the assumption of the generalized Riemann hypothesis, van der Linden [16] proved that the class number of $\mathbb{Q}(\zeta_{145})^+$ is 2, and he proved unconditionally that 2 divides h_{145}^+. So far, we have obtained the unconditional upper bound $h_{145}^+ \leq 36$. However, it is difficult to pin down the exact class number; the 2-parts and 7-parts of the class number pose difficulties. We will endeavor to find an improved upper bound.

We consider the sparse vectors

$$x = b_0 + b_1 + a_1 b_{j_1} + a_2 b_{j_2} + a_3 b_{j_3} + a_4 b_{j_4} + a_5 b_{j_5} + a_6 b_{j_6},$$

and

$$x = b_1 + a_1 b_{j_1} + a_2 b_{j_2} + a_3 b_{j_3} + a_4 b_{j_4} + a_5 b_{j_5} + a_6 b_{j_6},$$

where $1 < j_1 < j_2 < j_3 < j_4 < j_5 < j_6 < n$ and $a_j \in \{-1, 0, 1\}$ for $1 \leq j \leq 6$, and

$$x = c_0 + a_1 c_{k_1} + a_2 c_{k_2} + a_3 c_{k_3} + a_4 c_{k_4} + c_5 b_{k_5} + c_6 b_{k_6},$$

where $1 \leq k_1 < k_2 < k_3 < k_4 < k_5 < k_6 < n$ and $a_k \in \{-1, 0, 1\}$ for $1 \leq k \leq 6$.

Let T denote the set of all such elements x, and let U be the set of their norms, up to 10^{19}, that are congruent to ± 1 modulo the conductor m.

$$U = \{N(x) | x \in T, N(x) < 10^{19}, N(x) \equiv \pm 1 \pmod{m}\}.$$

Let S_1 be the set of prime norms

$$S_1 = \{p : p \in T, p \text{ prime}, \ p \equiv \pm 1 \pmod{m}\}.$$

For a field of such large discriminant and nontrivial class group, it is more difficult to find sufficiently many totally split primes of prime norm. An effective approach is to search for sparse vectors that have large composite norms, and then take quotients of appropriately chosen algebraic integers.

Following the above strategy, we define S_2 to be the set of primes defined by

$$S_2 = \{p : pq \in U, p \text{ prime}, \ p \notin S_1, q \in S_1\},$$

noting that if $N(x) = pq$ and $N(y) = q$, for x, y in the ring of integers $\mathcal{O}$, then $\frac{x}{\sigma(y)} \in \mathcal{O}$ with norm p for some Galois automorphism σ, and p is congruent to ± 1 modulo m.

Now put $S = S_1 \cup S_2$ and $c = 42$. We have the following lower found for the contribution of prime ideals,

$$2 \sum_{p \in S} \sum_{m=1}^{\infty} \frac{\log p}{p^{m/2}} F(m \log p) > 2 \sum_{p \in S} \sum_{m=1}^{2} \frac{\log p}{p^{m/2}} F(m \log p) > 0.5410.$$

Applying Theorem 2.3.1, we have $B > 0.1906$, so the class number is bounded above by 13.95. Therefore,

$$h_{145}^{+} \leq 13.$$

Now we can prove the following unconditionally.

Proposition 3.2.28. *The class number of* $\mathbb{Q}(\zeta_{145})^+$ *is* 2*.*

Proof. Let K be the octic subfield of $\mathbb{Q}(\zeta_{145})^+$. Using Sage [29], we can show unconditionally that K has class number 2. We apply Theorems 3.2.7 and 3.2.8 to the degree 7 extension $\mathbb{Q}(\zeta_{145})^+/K$ to find that the 2-part of h^+_{145} is equal to

$$2 \cdot 8^t$$

for some nonnegative integer t. Since $h^+_{145} \leq 13$, we have shown that the 2-part of h^+_{145} is precisely equal to 2.

We can also apply the Rank Theorem to $\mathbb{Q}(\zeta_{145})^+/K$ to show that neither 3 nor 5 divide h^+_{145}. Finally, since h^+_{145} is even and less than or equal to 13, we know that primes greater than or equal to 7 do not divide the class number. □

3.2.9 The class number of the real cyclotomic field of conductor 212

As we will see, the class group of the real cyclotomic field of conductor 212 is nontrivial, so it is of course more difficult to find principal prime ideals of small norm. The missing contribution from these primes of small norm must be replaced by a quite large number of primes of greater norm. In fact, so many principal prime ideals are required that it is difficult to establish an unconditional upper bound on the class number. However, if we assume the generalized Riemann hypothesis, it is quite easy to find an upper bound, as we've already seen in Example 2.1.3.

Proposition 3.2.29. *Under the assumption of the generalized Riemann hypothesis, the class number of* $\mathbb{Q}(\zeta_{212})^+$ *is* 5*.*

Proof. Using Odlyzko's discriminant lower bounds, we've already shown in Example 2.1.3 that

$$h^+_{212} \leq 11$$

conditional upon GRH.

Let K be the quartic subfield of $\mathbb{Q}(\zeta_{212})^+$. Using Sage [29], we can calculate the class number of K is 5. By the Pushing Up Theorem, 5 divides h_{212}^+. By the Parity Check Theorem, h_{212}^+ is odd, so we can conclude (conditional on GRH) the $h_{212}^+ = 5$. $\square$

Chapter 4

Class numbers of cyclotomic $\mathbb{Z}_p$-extensions

> *The dominant theme of [Iwasawa's] work in number theory is his revolutionary idea that deep and previously inaccessible information about the arithmetic of a finite extension F of $\mathbb{Q}$ can be obtained by studying coarser questions about the arithmetic of certain infinite Galois towers of number fields lying above F.*
>
> John Coates, *Notices of the AMS* **46** (10)

Let $\mathbb{B}_{p,n}$ denote the nth layer of the cyclotomic $\mathbb{Z}_p$-extension over the rationals, i.e. the unique real subfield of the cyclotomic field $\mathbb{Q}(\zeta_{p^{n+1}})$ of degree p^n over $\mathbb{Q}$ for odd primes p, and $\mathbb{Q}(\zeta_{2^{n+2}})^+)$ for $p = 2$. The class numbers of these fields have been the objects of intense investigation by number theorists, starting perhaps with Weber, who studied the $\mathbb{Z}_2$-extension. A key step in his proof of the Kronecker-Weber theorem is the following theorem [36].

Theorem 4.0.30 (Weber)**.** *For all positive integers n, the class number of $\mathbb{B}_{2,n}$ is odd.*

Weber's result was later generalized by Iwasawa [14] to all cyclotomic $\mathbb{Z}_p$-extensions over $\mathbb{Q}$.

Theorem 4.0.31 (Iwasawa)**.** *For all positive integers n and primes p, the class number of $\mathbb{B}_{p,n}$ is not divisible by p, i.e. the p-part of the class group is trivial.*

However, the non-p-part of the class groups of the $\mathbb{Z}_p$-extensions remains deeply mysterious. The only general result we have is Washington's "local" boundedness result [35].

Theorem 4.0.32 (Washington)**.** *Let q be a prime not equal to p, and let q^{e_n} be the exact power of q dividing the class number of $\mathbb{B}_{p,n}$. Then e_n is constant for sufficiently large n.*

On the other hand, much recent progress has been made regarding the $\mathbb{Z}_2$- and $\mathbb{Z}_3$-extensions. By analyzing properties of the cyclotomic units, Fukuda and Komatsu [10] went much further than Weber and proved the following striking result.

Theorem 4.0.33 (Fukuda, Komatsu). *For all positive integers n, the class number of $\mathbb{B}_{2,n}$ is not divisible by any prime less than 10^9.*

This suggests the following conjecture, known as *Weber's class number problem.*

Conjecture 4.0.34 (Weber's class number problem). *For all positive integers n, the class number of $\mathbb{B}_{2,n}$ is 1.*

Fukuda, Komatsu and Morisawa proved a similar result for the $\mathbb{Z}_3$-extension [11], which suggests that all the $\mathbb{B}_{3,n}$ too may have trivial class group.

Theorem 4.0.35 (Fukuda, Komatsu, Morisawa). *For all positive integers n, the class number of $\mathbb{B}_{3,n}$ is not divisible by any prime less than 10^9.*

Extending Weber's theorem in a different direction, Ichimura and Nakajima [13] proved a result concerning the parity of class numbers.

Theorem 4.0.36 (Ichimura, Nakajima). *For all positive integers n and primes $p < 500$, the class number of $\mathbb{B}_{p,n}$ is odd.*

Also, in unpublished work by T. Fukuda and his collaborators, they have calculated that the prime $2p + 1$ does not divide the class number of $\mathbb{B}_{p,1}$ for Sophie Germain primes p less than 1000 (T. Fukuda, private communication, July 25, 2014).

Notwithstanding the considerable interest in $\mathbb{Z}_p$-extensions and their class numbers, the precise class number has been successfully determined for only a very few of the $\mathbb{B}_{p,n}$, due to the inherent difficulties of calculating the class group for number fields of large discriminant and degree. The previously known results are summarized in Table 4.1. All the known class numbers are 1.

Table 4.1: $\mathbb{B}_{p,n}$ with previously known class numbers

$\mathbb{B}_{p,n}$	**Class number**	
$\mathbb{B}_{2,3}$	1	Cohn (1960) [9]
$\mathbb{B}_{2,4}$	1	Bauer (1969) [2]
$\mathbb{B}_{2,5}$	1	van der Linden (1982) [16]
$\mathbb{B}_{2,6}$	1 (under GRH)	van der Linden
$\mathbb{B}_{3,2}$	1	Bauer
$\mathbb{B}_{3,3}$	1	Masley (1978) [17]
$\mathbb{B}_{3,4}$	1 (under GRH)	van der Linden
$\mathbb{B}_{5,1}, \mathbb{B}_{7,1}$	1	Bauer
$\mathbb{B}_{11,1}, \mathbb{B}_{13,1}$	1 (under GRH)	van der Linden
$\mathbb{B}_{17,1}, \mathbb{B}_{19,1}, \mathbb{B}_{23,1}$	1 (under GRH)	Coates, Liang, Mihăilescu (2012) [5]

Table 4.2: $\mathbb{B}_{p,n}$ with new class number results

$\mathbb{B}_{p,n}$	**Class number**	
$\mathbb{B}_{2,6}$	1	Proposition 3.2.2
$\mathbb{B}_{2,7}$	1 (under GRH)	Proposition 3.2.3
$\mathbb{B}_{5,2}$	1	Corollary of Theorem 3.2.1
$\mathbb{B}_{11,1}$	1	Corollary of Proposition 3.2.10
$\mathbb{B}_{13,1}, \mathbb{B}_{17,1}, \mathbb{B}_{19,1}$	1	Theorem 4.0.37
$\mathbb{B}_{29,1}, \mathbb{B}_{31,1}$	1 (under GRH)	Pari via SageMathCloud$^{\text{TM}}$

In the previous chapter, we proved that certain real cyclotomic fields of prime power conductor have class number 1. Therefore their subfields also have class number 1, by a corollary of the Pushing Up Theorem. Also, by using the analytic upper bound for the class number developed in Chapter 2, we will prove unconditionally that several more fields have class number 1:

Theorem 4.0.37. *The fields $\mathbb{B}_{13,1}$, $\mathbb{B}_{17,1}$ and $\mathbb{B}_{19,1}$ have class number* 1*.*

Furthermore, using SageMathCloud$^{\text{TM}}$ [30], which calls underlying routines in the Pari library [26], we calculated that the fields $\mathbb{B}_{29,1}$ and $\mathbb{B}_{31,1}$ each have class number 1, under the assumption of the generalized Riemann hypothesis. We summarize these results in Table 4.2.

Coates [5] posed the following natural question: Do all $\mathbb{B}_{p,n}$ have class number 1? Unfortunately, resolving such a question is far beyond our current capabilities. Indeed, even proving that there are infinitely many number fields with class number 1 is one of the great open problems of number theory. On the other hand, the class group heuristics developed by Cohen and Lenstra [7, 8] provide a means by which we can attempt to estimate the probability that one or more of the $\mathbb{B}_{p,n}$ have nontrivial class groups.

The first steps in this direction were carried out by Buhler, Pomerance and Robertson [4]. By proving a certain quadruple sum is finite, they were led to the following conjecture.

Conjecture 4.0.38 (Buhler, Pomerance, Robertson)**.** *For all but finitely many pairs (p, n), where p is a prime and n is a positive integer, the class number of the real cyclotomic field of conductor p^{n+1} is equal to the class number of the real cyclotomic field of conductor p^n, i.e.*

$$h\left(\mathbb{Q}(\zeta_{p^{n+1}})^+\right) = h\left(\mathbb{Q}(\zeta_{p^n})^+\right).$$

A consequence of this conjecture is that the class number of $\mathbb{B}_{p,n}$ is equal to the class number of $\mathbb{B}_{p,n-1}$ for all but finitely many pairs (p, n).

In this chapter, we will study a similar quadruple sum and find an *explicit* upper bound for the sum, which essentially estimates the expected number of exceptional pairs (p, n). This upper bound is then further refined by known results on class numbers of the $\mathbb{B}_{p,n}$, including the new results established in this thesis. In fact, this refined upper bound is approximately 0.30, which is sufficiently smaller than 1 to suggest the following conjecture.

Main Conjecture. *For any prime p and positive integer n, the class number of $\mathbb{B}_{p,n}$ is 1.*

In order to rigorously establish an upper bound for the quadruple sum, an explicit sieve theory result of Siebert [33] and an improvement of Riesel and Vaughan [28] will prove vital. Along the way, we will also prove an upper bound for the sum of the reciprocals of the Sophie Germain primes, which surprisingly does not yet exist in the literature.

The rest of the chapter is organized as follows: In Section 4.1 we will discuss upper bounds on class numbers and prove Theorem 4.0.37. The application of Cohen-Lenstra heuristics to real cyclic number fields will be discussed in detail in Section 4.2. In Section 4.3 we specialize the Cohen-Lenstra heuristics to $\mathbb{Z}_p$-extensions. Sections 4.4, 4.5 and 4.6 study the $\mathbb{Z}_2$-, $\mathbb{Z}_3$- and $\mathbb{Z}_5$-extensions respectively, and Section 4.7 concerns the $\mathbb{Z}_p$-extensions for $7 \leq p \leq 31$. Section 4.8 discusses the first layers of $\mathbb{Z}_p$-extensions. In Section 4.9, we introduce the explicit sieve results and apply them to bounds on sums over Sophie Germain and similar primes. Using those bounds, in Section 4.10 we return to the discussion of the first layers. We study the higher layers in Section 4.11. The results are summarized in Section 4.12.

4.1 New results on certain $\mathbb{B}_{p,n}$

In his 1982 paper [16], van der Linden employed Odlyzko's discriminant lower bounds [24] to prove, conditionally upon the generalized Riemann hypothesis (GRH), that the class number of $\mathbb{B}_{13,1}$ is 1. However, the root discriminant of $\mathbb{B}_{13,1}$ is too large for the class number to be calculated unconditionally using van der Linden's methods, and the field $\mathbb{B}_{17,1}$ has root discriminant too large to be treated by those methods, even under the assumption of GRH. Using the class number upper bound from Chapter 2, we will unconditionally prove that $\mathbb{B}_{13,1}$, $\mathbb{B}_{17,1}$ and $\mathbb{B}_{19,1}$ have class number 1.

To find a generator of a principal ideal, it is useful to have an integral basis. The field $\mathbb{B}_{p,1}$ is the degree p subfield of the cyclotomic field of conductor p^2, which is cyclic. If σ generates the Galois group of the cyclotomic field, then the Galois subgroup generated by σ^p fixes the subfield $\mathbb{B}_{p,1}$. Let $\zeta = \exp(2\pi i/p^2)$. Given the generator σ, we'll use $\{b_0, b_1, \ldots, b_{p-1}\}$ as our integral basis, where $b_0 = 1$, and

$$b_j = \sum_{k=0}^{p-2} \zeta^{\sigma^{kp+j-1}}$$

for $1 \leq j \leq p-1$.

After using Theorem 2.3.1 to establish an upper bound for the class number, we will use the Rank Theorem (see Subsection 3.2.4) to pin down the exact class number.

Now we will prove our results for $\mathbb{B}_{13,1}$, $\mathbb{B}_{17,1}$ and $\mathbb{B}_{19,1}$.

Proposition 4.1.1. *The class number of* $\mathbb{B}_{13,1}$ *is* 1.

Proof. The root discriminant of $\mathbb{B}_{13,1}$ is approximately 113.90, which is too large to use Odlyzko's unconditional discriminant bounds. Alternatively, using the Minkowski bound of 479,001,600 would require testing whether roughly 20 million prime ideals were principal. However, using our new method, it suffices for us to find generators for *only two* principal prime ideals in order to employ Theorem 2.3.1 and establish an unconditional class number upper bound.

The Galois group of the cyclotomic field of conductor 169 is generated by $\sigma = (\zeta \mapsto \zeta^2)$, where $\zeta = \exp(2\pi i/169)$. Using the integral basis $\{b_0, b_1, \dots, b_{12}\}$ given above, we search over sparse vectors and find that the element

$$b_0 - b_1 - b_2 - b_3 - b_6 - b_7 - b_8$$

has norm 19, where the *norm* is taken to be the absolute value of the product of the Galois conjugates of the element. Similarly, the element

$$b_0 - b_1 - b_2 - b_4 + b_{12}$$

has norm 23. Therefore, the primes 19 and 23 totally split into principal ideals.

Now by Theorem 2.3.1, using $S = \{19, 23\}$ and $c = 10$, we get an upper bound for the class number,

$$h \leq 7.$$

Finally, by the Rank Theorem, we conclude that the class number is 1. □

Proposition 4.1.2. *The class number of* $\mathbb{B}_{17,1}$ *is* 1.

Proof. The fields $\mathbb{B}_{p,1}$ have root discriminant $p^{2(1-1/p)}$, so already $\mathbb{B}_{17,1}$ will require finding many thousands of principal prime ideals, rather the just two as was the case for $\mathbb{B}_{13,1}$. To find these primes, we will search over a large number of vectors, using an integral basis as given above. In particular, we consider the vectors

$$x = a_1 b_{j_1} + a_2 b_{j_2} + \cdots + a_{12} b_{j_{12}},$$

where $0 \leq j_1 < j_2 < j_3 < \cdots < j_{12} < 17$ and $a_j \in \{-1, 0, 1\}$ for $1 \leq j \leq 12$.

Let T denote the set of all such elements x, and let U be the set of their norms, up to 10^{12}.

$$U = \{N(x) | x \in T, N(x) < 10^{12}\}.$$

Let S_1 be the set of prime norms

$$S_1 = \{p : p \in U, p \text{ prime}\}.$$

For a field of such large root discriminant, it is difficult to find sufficiently many elements of prime norm. An effective approach is to search for elements that have large composite norms, and then take quotients by appropriately chosen algebraic integers. Following this strategy, we define S_2 to be the set of primes defined by

$$S_2 = \{p : pq \in U, p \text{ prime}, \, p \notin S_1, q \in S_1\},$$

noting that if $N(x) = pq$ and $N(y) = q$, for x, y in the ring of integers $\mathcal{O}$, then $x/y^\sigma \in \mathcal{O}$ with norm p for some Galois automorphism σ.

Now put $S = S_1 \cup S_2 \setminus \{17\}$ and $c = 22$. The contribution of prime ideals has a lower bound

$$2 \sum_{p \in S} \sum_{m=1}^{\infty} \frac{\log p}{p^{m/2}} F(m \log p) > 2 \sum_{p \in S} \sum_{m=1}^{2} \frac{\log p}{p^{m/2}} F(m \log p) > 2.092893.$$

Applying Theorem 2.3.1, we find that the class number is bounded above by

$$h \leq 5.$$

Therefore, by the Rank Theorem, we see that the class number is 1. □

Proposition 4.1.3. *The class number of* $\mathbb{B}_{19,1}$ *is* 1.

Proof. We follow an entirely similar proof to that of $\mathbb{B}_{17,1}$ to generate our set S. Using $c = 40$, we calculate a lower bound for the contribution of prime ideals of 1.671648. We apply Theorem 2.3.1 and find that the class number is bounded above by

$$h \leq 38.$$

By Theorem 4.0.31, the class number is not divisible by 19. For the other primes $p \neq 19$, we can apply the Rank Theorem to conclude that the class number is 1. □

4.2 Cohen-Lenstra heuristics for totally real cyclic number fields

If a number field is a Galois extension of the rationals, then its Galois group G acts on its ideals, so its ideal class group is a $\mathbb{Z}[G]$-module. Moreover, if

$$N = \sum_{g \in G} g,$$

then N acts as the norm on ideals, sending every ideal to a principal ideal, so that the class group is in fact a $\mathbb{Z}[G]/\langle N \rangle$-module. Roughly speaking, Cohen and Lenstra [7, 8] predicted that the class group of a totally real Galois number field K of Galois group G should behave as a "random" finite $\mathbb{Z}[G]/\langle N \rangle$-module modulo a random cyclic submodule. One can then ask what is the expected probability that a simple factor M occurs in the Jordan-Hölder decomposition of this quotient. When G is abelian, Cohen and Lenstra calculated that a random $\mathbb{Z}[G]/\langle N \rangle$-module modulo a random cyclic submodule should have such a simple factor M with probability:

$$1 - \prod_{k \geq 2} (1 - |M|^{-k}).$$

Here we are taking some license with our notion of "probability." In Cohen and Lenstra's formulation of their heuristics, probability has a precise meaning in terms of the density of number fields of a given Galois group and signature, as the discriminant varies. Our notion of probability will be in the Bayesian sense of a subjective prior probability, as described by Buhler, Pomerance and Robertson [4, p. 3]:

> We would like to apply this to class groups $Cl^+(\ell^n)$, but this is hard to formalize in the usual frequentist language of probability since there is no underlying probability space. Indeed, the original Cohen-Lenstra heuristics apply to a large collection of fields of a given degree, and we are applying them to a large collection of fields whose degrees are unbounded. Instead we adopt a subjective Bayesian view, where probability arises from ignorance. Thus we use the Cohen-Lenstra heuristics as the basis of the assignment of subjective probabilities, on the grounds that they are a plausible first guess.

Schoof also used such a notion of probability to analyze his results on the class numbers of real cyclotomic fields of prime conductor [31, p. 19]. Going forward, when we speak of the "probability" of a number field (or family of number fields) having class number 1, we mean probability in this Bayesian sense.

With this stipulation on the meaning of "probability," given a prime q not dividing the degree of K, the Cohen-Lenstra heuristics predict the probability that q does not divide the class number $h(K)$ of K is

$$\text{Prob}(q\text{-part of } h(K) \text{ is } 1) = \prod_{\substack{M \text{ simple} \\ |M| \text{ power of } q}} \prod_{k \geq 2} (1 - |M|^{-k}),$$

where the outer product runs over all simple $\mathbb{Z}[G]/\langle N \rangle$-modules M of order a power of q.

Now suppose K is a totally real degree n cyclic extension of the rationals, and suppose q is a prime not dividing n. Then the simple $\mathbb{Z}[G]$-modules M of size power of q are given by quotients of $\mathbb{Z}[G] \cong \mathbb{Z}[X]/(X^n - 1)$ by the maximal ideals generated by q and $f(X)$, where $f(X)$ is an irreducible divisor of the cyclotomic polynomial $\Phi_d(X)$ modulo q, for some d dividing n. To get the maximal ideals of $\mathbb{Z}[G]/\langle N \rangle$, we further require that $d > 1$. In other words, the simple $\mathbb{Z}[G]/\langle N \rangle$-modules M of size power of q are given by

$$M \cong \mathbb{Z}[\zeta_d]/P$$

for some divisor d of n, with $d > 1$, and for some prime ideal P lying over q.

Remark 4.2.1. Although we have the isomorphism,

$$\mathbb{Z}[G]/\langle N\rangle \cong \frac{\mathbb{Z}[X]}{(1+X+\cdots+X^{n-1})} = \frac{\mathbb{Z}[X]}{\left(\prod_{d|n,\,d>1}\Phi_d(X)\right)},$$

the homomorphism

$$\frac{\mathbb{Z}[X]}{\left(\prod_{d|n,\,d>1}\Phi_d(X)\right)} \longrightarrow \bigoplus_{d|n,\,d>1}\frac{\mathbb{Z}[X]}{(\Phi_d(X))} \cong \bigoplus_{d|n,\,d>1}\mathbb{Z}[\zeta_d],$$

is injective, but is not in general surjective. Nevertheless, the maximal ideals relatively prime to n are in bijective norm-preserving correspondence.

Therefore, given a prime q not dividing the degree n, we have the heuristic probability

$$\text{Prob}(q\text{-part of } h(K) \text{ is } 1) = \prod_{d|n,\,d>1}\ \prod_{\substack{P\subset\mathbb{Z}[\zeta_d]\\ P|q}}\ \prod_{k\geq 2}(1-NP^{-k}),$$

where the P are prime ideals of $\mathbb{Z}[\zeta_d]$ that lie over q, and NP is the norm of P. If the primes P over q have degree f, or equivalently if the order of q modulo d is f, then there are $\phi(d)/f$ primes P lying over q, where ϕ is the Euler totient function. So we can write

$$\text{Prob}(q\text{-part of } h(K) \text{ is } 1) = \prod_{d|n,\,d>1}\ \prod_{k\geq 2}(1-q^{-fk})^{\phi(d)/f}.$$

In particular, for a totally real cyclic field K of prime power degree p^n, the Cohen-Lenstra heuristics predict that

$$\text{Prob}(\text{non-}p\text{-part of } h(K) \text{ is } 1) = \prod_{\substack{q \text{ prime}\\ q\neq p}}\ \prod_{j=1}^{n}\ \prod_{k\geq 2}(1-q^{-fk})^{\phi(p^j)/f},$$

where f is the order of q modulo p^j.

4.3 Cohen-Lenstra heuristics for cyclotomic $\mathbb{Z}_p$-extensions

Since $\mathbb{B}_{p,n}$, the nth layer of the cyclotomic $\mathbb{Z}_p$-extension, is cyclic with prime power degree p^n, the heuristics for the non-p-part of the class group are described by the previous section. Moreover, Iwasawa [14] proved Theorem 4.0.31, i.e. that p does not divide the class number of $\mathbb{B}_{p,n}$ for any prime p and any positive integer n. Therefore, we may predict that the probability that $\mathbb{B}_{p,n}$ has class number 1 is

$$\mathrm{Prob}(h(\mathbb{B}_{p,n}) = 1) = \prod_{\substack{q \text{ prime} \\ q \neq p}} \prod_{j=1}^{n} \prod_{k \geq 2} (1 - q^{-fk})^{\phi(p^j)/f}.$$

We may conclude that a naive estimate of the probability P_T of our Main Conjecture being true is

$$P_T = \prod_{p \text{ prime}} \prod_{\substack{q \text{ prime} \\ q \neq p}} \prod_{j=1}^{\infty} \prod_{k \geq 2} (1 - q^{-fk})^{\phi(p^j)/f}.$$

It is convenient to linearize this product by taking logarithms:

$$-\log P_T = -\sum_{p \text{ prime}} \sum_{\substack{q \text{ prime} \\ q \neq p}} \sum_{j=1}^{\infty} \sum_{k \geq 2} \frac{\phi(p^j)}{f} \log(1 - q^{-fk}).$$

Buhler, Pomerance and Robertson [4] proved that this quadruple sum is finite. Calculating an explicit upper bound for such a sum will require certain results from sieve theory, in particular theorems of Siebert [33] and Riesel and Vaughan [28]. We will further refine our estimates by incorporating existing knowledge of class numbers of fields in $\mathbb{Z}_p$-extensions, including the new results of Theorem 4.0.37; for this it is useful to know that for $m < n$ the conditional probability that $h(\mathbb{B}_{p,n}) = 1$, given that $h(\mathbb{B}_{p,m}) = 1$, is

$$\prod_{\substack{q \text{ prime} \\ q \neq p}} \prod_{j=m+1}^{n} \prod_{k \geq 2} (1 - q^{-fk})^{\phi(p^j)/f}.$$

As a warm-up, we first estimate some important special cases of our Main Conjecture.

4.4 The $\mathbb{Z}_2$-extension

The layers of the $\mathbb{Z}_2$-extensions are precisely the real cyclotomic fields with power of 2 conductor. We have the following special case of our Main Conjecture, known as *Weber's class number problem*:

Conjecture 4.4.1 (Weber's class number problem)**.** *For any positive integer n, the class number of $\mathbb{B}_{2,n} = \mathbb{Q}(\zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1})$ is 1.*

In Chapter 3, we unconditionally proved that the class number of $\mathbb{B}_{2,6}$ is 1 and also (under GRH) that the class number of $\mathbb{B}_{2,7}$ is 1. Furthermore, Fukuda and Komatsu [10] have proven, for all primes $q < 10^9$, that the q-part of the class number of $\mathbb{B}_{2,n}$ is trivial, for all n. Thus we may estimate the probability P_T that the Weber conjecture is true by:

$$P_T = \prod_{\substack{q \text{ prime} \\ q>10^9}} \prod_{j=8}^{\infty} \prod_{k\geq 2} (1-q^{-fk})^{\phi(2^j)/f}.$$

The probability P_F that the Weber conjecture is false is bounded above by

$$P_F < -\log(1-P_F) = -\log P_T = -\sum_{\substack{q \text{ prime} \\ q>10^9}} \sum_{j=8}^{\infty} \sum_{k\geq 2} \frac{\phi(2^j)}{f} \log(1-q^{-fk}).$$

To estimate these probabilities, we have the following proposition.

Proposition 4.4.2. *The following triple sum has an upper bound*

$$-\sum_{\substack{q \text{ prime} \\ q>10^9}} \sum_{j=8}^{\infty} \sum_{k\geq 2} \frac{\phi(2^j)}{f} \log(1-q^{-fk}) < 1.3 \times 10^{-8},$$

where ϕ is the Euler totient function, and f is the order of q modulo 2^j.

Proof. Let S denote the triple sum. Since $q^{-fk} < 10^{-18}$, we have

$$-\log(1-q^{-fk}) < (1+10^{-17})q^{-fk}.$$

Therefore, the triple sum S is bounded above by

$$S < (1+10^{-17}) \sum_{\substack{q \text{ prime} \\ q>10^9}} \sum_{j=8}^{\infty} \frac{2^{j-1}}{fq^f(q^f-1)} < (1+10^{-8}) \sum_{\substack{q \text{ prime} \\ q>10^9}} \sum_{j=8}^{\infty} \frac{2^{j-1}}{fq^{2f}}.$$

Recall that f is the order of q modulo 2^j. Following the argument in [4, p. 6], we observe that $q^f = 1 + 2^j t$ for some positive integer t, so we have the upper bound

$$S < (1+10^{-8}) \sum_{j=8}^{\infty} \sum_{\substack{t=1 \\ 1+2^j t>10^9}}^{\infty} \frac{2^{j-1}}{(1+2^j t)^2} < (1+10^{-8}) \sum_{j=8}^{\infty} \sum_{\substack{t=1 \\ 1+2^j t>10^9}}^{\infty} \frac{1}{2^{j+1}t^2}.$$

We can rearrange this to get

$$S < \frac{1+10^{-8}}{2^8} \cdot \frac{\pi^2}{6} - \sum_{j=8}^{\infty} \sum_{\substack{t=1 \\ 1+2^j t \leq 10^9}}^{\infty} \frac{1}{2^{j+1}t^2} < 1.3 \times 10^{-8}.$$

□

Thus, assuming the validity of the Cohen-Lenstra heuristics, the probability that the Weber conjecture is true is at least 99.999998% (versus > 99.3% estimated in [4]).

4.5 The $\mathbb{Z}_3$-extension

The layers of the $\mathbb{Z}_3$-extensions are precisely the real cyclotomic fields with power of 3 conductor. We have the following special case of our Main Conjecture.

Conjecture 4.5.1. *For any positive integer n, the class number of $\mathbb{B}_{3,n} = \mathbb{Q}(\zeta_{3^{n+1}} + \zeta_{3^{n+1}}^{-1})$ is 1.*

Van der Linden [16] proved that the class number of $\mathbb{B}_{3,3}$ is 1 and also (under GRH) that the class number of $\mathbb{B}_{3,4}$ is 1. This conjecture is further supported by the work of Morisawa, who proved in his thesis [22] that all primes p less than $400,000$ do not the class number of $\mathbb{B}_{3,n}$ for all n. Morisawa's result has recently been further improved by Fukuda, Komatsu and Morisawa [11], who proved that no prime less than 10^9 divides the class number of $\mathbb{B}_{3,n}$.

Thus we have we may estimate the probability P_T that this conjecture is true by:

$$P_T = \prod_{\substack{q \text{ prime} \\ q>10^9}} \prod_{j=5}^{\infty} \prod_{k\geq 2} (1 - q^{-fk})^{\phi(3^j)/f}.$$

To estimate this probability, we have the following proposition.

Proposition 4.5.2. *The following triple sum has an upper bound*

$$-\sum_{\substack{q \text{ prime} \\ q>10^9}} \sum_{j=5}^{\infty} \sum_{k\geq 2} \frac{\phi(3^j)}{f} \log(1 - q^{-fk}) < 1.1 \times 10^{-8},$$

where ϕ is the Euler totient function, and f is the order of q modulo 3^j.

Proof. Let S denote the triple sum. Then we have

$$S < (1+10^{-8}) \sum_{\substack{q \text{ prime} \\ q>10^9}} \sum_{j=5}^{\infty} \frac{\phi(3^j)}{fq^{2f}} < (1+10^{-8}) \sum_{j=5}^{\infty} \sum_{\substack{t=1 \\ 1+3^j t>10^9}}^{\infty} \frac{2}{3^{j+1}t^2}.$$

We rearrange this to get

$$S < \frac{1+10^{-8}}{3^5} \cdot \frac{\pi^2}{6} - \sum_{j=5}^{\infty} \sum_{\substack{t=1 \\ 1+3^j t\leq 10^9}}^{\infty} \frac{2}{3^{j+1}t^2} < 1.1 \times 10^{-8}.$$

□

Thus, assuming the validity of the Cohen-Lenstra heuristics, the probability that the conjecture for the $\mathbb{Z}_3$-extension is true is at least 99.999998%.

4.6 The $\mathbb{Z}_5$-extension

We now study the following special case of our Main Conjecture:

Conjecture 4.6.1. *For any positive integer n, the class number of $\mathbb{B}_{5,n}$ is 1.*

From the earlier results on class numbers of cyclotomic fields of composite conductor in Chapter 3, we can prove unconditionally that the class number of $\mathbb{B}_{5,2}$ is 1. Furthermore, Ichimura and Nakajima [13] proved the class numbers of $\mathbb{B}_{5,n}$ are odd for all n, and Iwasawa [14] proved that 5 does not divide the class number of $\mathbb{B}_{5,n}$ for all n.

To estimate the probability that all $\mathbb{B}_{5,n}$ have class number 1, we calculate the following upper bounds.

Proposition 4.6.2. *There is an upper bound for the double sum*

$$\sum_{\substack{q \text{ prime} \\ q\neq 2,5}} \sum_{j=3}^{\infty} \frac{\phi(5^j)}{fq^{2f}} < 0.001860$$

and an upper bound for the triple sum

$$-\sum_{\substack{q \text{ prime} \\ q\neq 2,5}} \sum_{j=3}^{\infty} \sum_{k\geq 2} \frac{\phi(5^j)}{f} \log(1-q^{-fk}) < 0.001868,$$

where ϕ is the Euler totient function, and f is the order of q modulo 5^j.

Using this result, and assuming the validity of the Cohen-Lenstra heuristics, the probability that the conjecture for the $\mathbb{Z}_5$-extension is true is at least

$$e^{-0.001868} > 99.8\%.$$

Proof. We break the double sum into two parts:

$$\sum_{\substack{q \text{ prime} \\ q \neq 2,5}} \sum_{j=3}^{\infty} \frac{\phi(5^j)}{fq^{2f}} = \sum_{\substack{q \text{ prime} \\ q \neq 2,5}} \sum_{\substack{j=3 \\ q^f \leq 10^6}}^{\infty} \frac{\phi(5^j)}{fq^{2f}} + \sum_{\substack{q \text{ prime} \\ q \neq 2,5}} \sum_{\substack{j=3 \\ q^f > 10^6}}^{\infty} \frac{\phi(5^j)}{fq^{2f}}.$$

The first term on the right-hand side is in fact a finite sum, which we calculate explicitly

$$\sum_{\substack{q \text{ prime} \\ q \neq 2,5}} \sum_{\substack{j=3 \\ q^f \leq 10^6}}^{\infty} \frac{\phi(5^j)}{fq^{2f}} < 0.001854.$$

Similarly to the argument used for the $\mathbb{Z}_2$- and $\mathbb{Z}_3$-extensions, we note that $q^f = 1 + 5^j t$ for some positive integer t, so the second term can be bounded by

$$\sum_{\substack{q \text{ prime} \\ q \neq 2,5}} \sum_{\substack{j=3 \\ q^f > 10^6}}^{\infty} \frac{\phi(5^j)}{fq^{2f}} < \sum_{j=3}^{\infty} \sum_{\substack{t=1 \\ 1+5^j t > 10^6}}^{\infty} \frac{4(5^{j-1})}{(1+5^j t)^2} < \sum_{j=3}^{\infty} \sum_{\substack{t=1 \\ 1+5^j t > 10^6}}^{\infty} \frac{4}{5^{j+1} t^2}.$$

We rearrange this to get

$$\sum_{\substack{q \text{ prime} \\ q \neq 2,5}} \sum_{\substack{j=3 \\ q^f > 10^6}}^{\infty} \frac{\phi(5^j)}{fq^{2f}} < \frac{1}{5^3} \cdot \frac{\pi^2}{6} - \sum_{j=3}^{\infty} \sum_{\substack{t=1 \\ 1+5^j t \leq 10^6}}^{\infty} \frac{4}{5^{j+1} t^2} < 0.000006.$$

Thus, we have the upper bound

$$\sum_{\substack{q \text{ prime} \\ q \neq 2,5}} \sum_{j=3}^{\infty} \frac{\phi(5^j)}{fq^{2f}} < 0.001854 + 0.000006 = 0.001860.$$

Using this upper bound for the double sum, we can find an upper bound for the triple sum. Since $q^f \geq 1 + 5^3 \cdot 2 = 251$ and $q^{fk} \geq 251^2 = 63001$, we have

$$-\log(1 - q^{-fk}) \leq \frac{-\log(1 - 1/63001)}{1/63001} q^{-fk} < 1.000008 q^{-fk}.$$

We also have that

$$\sum_{k=2}^{\infty} q^{-fk} = q^{-2f}(1 - q^{-f})^{-1} \leq q^{-2f}(1 - 1/251)^{-1} \leq 1.004 q^{-2f}.$$

Thus, we have an upper bound for the triple sum

$$-\sum_{\substack{q\,\text{prime}\\ q\neq 2,5}}\sum_{j=3}^{\infty}\sum_{k\geq 2}\frac{\phi(5^j)\log(1-q^{-fk})}{f} < 1.000008\times 1.004\times 0.001860 < 0.001868.$$

□

4.7 The $\mathbb{Z}_p$-extensions for $7 \leq p \leq 31$

We now study the following special case of our Main Conjecture:

Conjecture 4.7.1. *For any positive integer n and any prime p such that $7 \leq p \leq 31$, the class number of $\mathbb{B}_{p,n}$ is 1.*

As discussed earlier, we have proved that the class numbers of $\mathbb{B}_{p,1}$ are 1 for $p \leq 31$ (conditional on GRH in the cases of $p = 23$, 29 and 31). Moreover, Ichimura and Nakajima [13] have proven that the class numbers of $\mathbb{B}_{p,n}$ for $p \leq 500$ are odd, and we have Iwasawa's result [14] that p does not divide the class number of $\mathbb{B}_{p,n}$.

To estimate the probability that all $\mathbb{B}_{p,n}$, $7 \leq p \leq 31$, have class number 1, we calculate the following upper bounds.

Proposition 4.7.2. *For primes p such that $7 \leq p \leq 31$, there are upper bounds for the* *double sums*

$$\sum_{\substack{q\,\mathrm{prime}\\ q\neq 2,p}}\sum_{j=2}^{\infty}\frac{\phi(p^j)}{fq^{2f}} < \begin{cases} 0.001617 & \textit{if}\ p=7,\\ 0.000896 & \textit{if}\ p=11,\\ 0.000446 & \textit{if}\ p=13,\\ 0.000051 & \textit{if}\ p=17,\\ 0.000026 & \textit{if}\ p=19,\\ 0.000017 & \textit{if}\ p=23,\\ 0.000040 & \textit{if}\ p=29,\\ 0.000018 & \textit{if}\ p=31, \end{cases}$$

and upper bounds for the triple sums

$$-\sum_{\substack{q\,\mathrm{prime}\\ q\neq 2,p}}\sum_{j=2}^{\infty}\sum_{k\geq 2}\frac{\phi(p^j)\log(1-q^{-fk})}{f} < \begin{cases} 0.001626 & \textit{if}\ p=7,\\ 0.000901 & \textit{if}\ p=11,\\ 0.000449 & \textit{if}\ p=13,\\ 0.000052 & \textit{if}\ p=17,\\ 0.000027 & \textit{if}\ p=19,\\ 0.000018 & \textit{if}\ p=23,\\ 0.000041 & \textit{if}\ p=29,\\ 0.000019 & \textit{if}\ p=31, \end{cases}.$$

where ϕ is the Euler totient function, and f is the order of q modulo p^j.

Using this result and assuming the validity of the Cohen-Lenstra heuristics, the conjecture that all the fields in all the $\mathbb{Z}_p$-extensions, $7 \leq p \leq 31$, have class number 1 is true with probability at least

$$e^{-(0.001626+0.000901+0.000449+0.000052+0.000027+0.000018+0.000041+0.000019)} > 99.6\%.$$

Proof. We follow closely the proof used for the $\mathbb{Z}_5$-extension. First we break the double sum into two parts,

$$\sum_{\substack{q \text{ prime} \\ q \neq 2,p}} \sum_{j=2}^{\infty} \frac{\phi(p^j)}{fq^{2f}} = \sum_{\substack{q \text{ prime} \\ q \neq 2,p}} \sum_{\substack{j=2 \\ q^f \leq 10^6}}^{\infty} \frac{\phi(p^j)}{fq^{2f}} + \sum_{\substack{q \text{ prime} \\ q \neq 2,p}} \sum_{\substack{j=2 \\ q^f > 10^6}}^{\infty} \frac{\phi(p^j)}{fq^{2f}}.$$

The first term on the right-hand side is a finite sum, which we calculate explicitly.

$$\sum_{\substack{q \text{ prime} \\ q \neq 2,p}} \sum_{\substack{j=2 \\ q^f \leq 10^6}}^{\infty} \frac{\phi(p^j)}{fq^{2f}} < \begin{cases} 0.001611 & \text{if } p = 7, \\ 0.000890 & \text{if } p = 11, \\ 0.000440 & \text{if } p = 13, \\ 0.000045 & \text{if } p = 17, \\ 0.000020 & \text{if } p = 19, \\ 0.000011 & \text{if } p = 23, \\ 0.000034 & \text{if } p = 29, \\ 0.000012 & \text{if } p = 31. \end{cases}$$

Since $q^f = 1 + p^j t$ for some positive integer t, the second term can be bounded by

$$\sum_{\substack{q \text{ prime} \\ q \neq 2,p}} \sum_{\substack{j=2 \\ q^f > 10^6}}^{\infty} \frac{\phi(p^j)}{fq^{2f}} < \sum_{j=2}^{\infty} \sum_{\substack{t=1 \\ 1+p^j t > 10^6}}^{\infty} \frac{(p-1)(p^{j-1})}{(1+p^j t)^2} < \sum_{j=2}^{\infty} \sum_{\substack{t=1 \\ 1+p^j t > 10^6}}^{\infty} \frac{p-1}{p^{j+1} t^2}.$$

We rearrange this to get

$$\sum_{\substack{q \text{ prime} \\ q \neq 2,p}} \sum_{\substack{j=2 \\ q^f > 10^6}}^{\infty} \frac{\phi(p^j)}{fq^{2f}} < \frac{1}{p^2} \cdot \frac{\pi^2}{6} - \sum_{j=2}^{\infty} \sum_{\substack{t=1 \\ 1+p^j t \leq 10^6}}^{\infty} \frac{p-1}{p^{j+1} t^2} < 0.000006,$$

which is valid for any prime $7 \leq p \leq 31$. Thus, we have the upper bound

$$\sum_{\substack{q \text{ prime} \\ q \neq 2,p}} \sum_{j=2}^{\infty} \frac{\phi(p^j)}{fq^{2f}} < \begin{cases} 0.001617 & \text{if } p = 7, \\ 0.000896 & \text{if } p = 11, \\ 0.000446 & \text{if } p = 13, \\ 0.000051 & \text{if } p = 17, \\ 0.000026 & \text{if } p = 19, \\ 0.000017 & \text{if } p = 23, \\ 0.000040 & \text{if } p = 29, \\ 0.000018 & \text{if } p = 31. \end{cases}$$

Using these upper bounds for the double sums, we can find upper bounds for the triple sums. The smallest prime power q^f that is congruent to 1 modulo p^j for $7 \leq p \leq 31$ and $j \geq 2$ is $1 + 7^2 \cdot 4 = 197$. Since $q^{fk} \geq 197^2 = 38809$, we have

$$-\log(1 - q^{-fk}) \leq \frac{-\log(1 - 1/38809)}{1/38809} q^{-fk} < 1.000013q^{-fk}.$$

We also have that

$$\sum_{k=2}^{\infty} q^{-fk} = q^{-2f}(1 - q^{-f})^{-1} \leq q^{-2f}(1 - 1/197)^{-1} < 1.005103q^{-2f}.$$

Thus, we have upper bounds for the triple sums

$$-\sum_{\substack{q\,\text{prime}\\ q\neq 2,p}}\sum_{j=2}^{\infty}\sum_{k\geq 2}\frac{\phi(p^j)\log(1-q^{-fk})}{f} < 1.005117\sum_{\substack{q\,\text{prime}\\ q\neq 2,p}}\sum_{\substack{j=2\\ q^f\leq 10^6}}^{\infty}\frac{\phi(p^j)}{fq^{2f}} < \begin{cases} 0.001626 & \text{if } p=7,\\ 0.000901 & \text{if } p=11,\\ 0.000449 & \text{if } p=13,\\ 0.000052 & \text{if } p=17,\\ 0.000027 & \text{if } p=19,\\ 0.000018 & \text{if } p=23,\\ 0.000041 & \text{if } p=29,\\ 0.000019 & \text{if } p=31.\end{cases}.$$

□

4.8 First layers of the $\mathbb{Z}_p$-extensions

The first layers $\mathbb{B}_{p,1}$ of the cyclotomic $\mathbb{Z}_p$-extensions of the rationals are of prime degree p. We consider another special case of our Main Conjecture:

Conjecture 4.8.1. *For any prime p, the class number of $\mathbb{B}_{p,1}$ is 1.*

From our earlier calculations, we know that this is true for primes $p \leq 19$ and also for $p = 23$, 29 and 31 under the assumption of GRH. Assuming the Cohen-Lenstra heuristics, the probability P_T that all first layers have class number 1 can be estimated by

$$P_T = \prod_{\substack{p\ \text{prime}\\ p>31}}\prod_{\substack{q\ \text{prime}\\ q\neq p}}\prod_{k\geq 2}(1-q^{-fk})^{\phi(p)/f},$$

where f is the order of q modulo p. Taking logarithms, we get the triple sum

$$-\log P_T = -\sum_{p>31}\sum_{q\neq p}\sum_{k\geq 2}\frac{p-1}{f}\log(1-q^{-fk}).$$

Since $q^f \equiv 1(\operatorname{mod} p)$, we have $q^f \geq 83$ and $q^{-fk} \leq 1/83^2$. It follows that

$$-\log(1-q^{-fk}) \leq \frac{-\log(1-1/83^2)}{1/83^2} q^{-fk} < 1.0001 q^{-fk}.$$

This gives us an upper bound

$$E_1 < 1.0001 \sum_{p>31} \sum_{q \neq p} \sum_{k \geq 2} \frac{p-1}{f q^{fk}} = 1.0001 \sum_{p>31} \sum_{q \neq p} \frac{p-1}{f q^f (q^f - 1)} < 1.02 \sum_{p>31} \sum_{q \neq p} \frac{p-1}{f q^{2f}}.$$

In the above double sum, the largest contribution is given by terms with $f = 1$:

$$\sum_{p>31} \sum_{\substack{q \text{ prime} \\ q \equiv 1(\text{ mod } p)}} \frac{p-1}{q^2} = \sum_{a \geq 1} \sum_{\substack{p>31 \text{ prime} \\ ap+1 \text{ prime}}} \frac{p-1}{(ap+1)^2}.$$

The sum $\sum_{q \equiv 1(p)} (p-1)/q^2$ is $O(1/p)$, which is not good enough for convergence of the sum over p. However, if we average over the various moduli p, we can hope for a $(\log p)^2$ savings, enough to show convergence. To achieve such savings, we will apply an explicit sieve theory result to sums over primes of the form $ap+1$.

4.9 Sums over Sophie Germain primes

Motivated by the discussion in the previous section, we first consider sums over the *Sophie Germain primes*, i.e. primes p such that $2p+1$ is also prime, and more generally sums over primes p such that $ap+1$ is prime, with a a given fixed even integer. Let $\pi_{ap+1}(x)$ denote the density of such primes,

$$\pi_{ap+1}(x) = \#\{p < x : p, ap+1 \text{ both prime}\}.$$

The methods of Hardy and Littlewood give the explicit conjectural asymptotics

$$\pi_{ap+1}(x) \sim 2C_2 \frac{x}{\log^2 x} \prod_{p|a,\, p \neq 2} \frac{p-1}{p-2},$$

where C_2, the *twin prime constant*, is

$$C_2 = \prod_{p>2} \frac{p(p-2)}{(p-1)^2} \approx 0.6601618158.$$

However, to get explicit upper bounds for sums over such primes, we need explicit density estimates. Fortunately, Siebert has provided us this key result [33], which is greater than the conjectural asymptotic by a factor of 8. Furthermore, for values of x greater than 1.63×10^{10}, we can strengthen Siebert's bound by incorporating results of Riesel and Vaughan [28, proof of Lemma 5].

Theorem 4.9.1 (Siebert [33], Riesel and Vaughan [28])**.** *Let a be an even integer. Then there is the explicit density estimate*

$$\pi_{ap+1}(x) \le 16C_2 \min\left(\frac{x}{(\log x)^2}, \frac{x}{(\log x)^2 + F(x)} + 2\sqrt{x}\right) \prod_{p|a,\, p\neq 2} \frac{p-1}{p-2},$$

where

$$F(x) = 8.463433 \log x - 9.260623 - 9310.077 x^{-1/6} - 29.50889 x^{-1/2}.$$

To estimate upper bounds for sums over these "$ap+1$" primes, we can calculate a certain number of terms explicitly, and then use the density estimate to get an upper bound for the remaining terms in the "tail" of the sum.

We start with the example of an upper bound for the sum of reciprocals of the Sophie Germain primes, a result which seems to have not previously appeared in the literature.

Proposition 4.9.2. *The sum of the reciprocals of the Sophie Germain primes has an upper bound*

$$\sum_{\substack{p \text{ prime} \\ 2p+1 \text{ prime}}} \frac{1}{p} < 1.88584.$$

Proof. We can calculate initial terms

$$\sum_{\substack{p<10^{10} \text{ prime} \\ 2p+1 \text{ prime}}} \frac{1}{p} < 1.476947.$$

We use the density estimate to calculate the tail of the sum

$$\sum_{\substack{p>10^{10} \text{ prime} \\ 2p+1 \text{ prime}}} \frac{1}{p} = \int_{10^{10}}^{\infty} \frac{1}{x} d\pi_{2p+1}(x) < \int_{10^{10}}^{\infty} \frac{\pi_{2p+1}(x)}{x^2} dx$$

$$\le 16C_2 \int_{10^{10}}^{\infty} \min\left(\frac{1}{(\log x)^2}, \frac{1}{(\log x)^2 + F(x)} + 2x^{-1/2}\right) \frac{dx}{x},$$

where $F(x) = 8.463433 \log x - 9.260623 - 9310.077x^{-1/6} - 29.50889x^{-1/2}$. It is much easier to evaluate this integral numerically if we first make the change of variable $y = \log x$.

$$\sum_{\substack{p>10^{10} \text{ prime} \\ 2p+1 \text{ prime}}} \frac{1}{p} < 16C_2 \int_{\log 10^{10}}^{\infty} \min\left(\frac{1}{y^2}, \frac{1}{y^2 + F(e^y)} + 2e^{-y/2}\right) dy < 0.408894.$$

Thus, we have an upper bound

$$\sum_{\substack{p \text{ prime} \\ 2p+1 \text{ prime}}} \frac{1}{p} < 1.476947 + 0.408894 = 1.885841.$$

□

Next is a similar result which will be used in our application to the Cohen-Lenstra heuristics. It turns out that this sum will be the largest contributor to our estimate of the quadruple sum associated to our Main Conjecture.

Proposition 4.9.3. *The following sum over Sophie Germain primes has an upper bound*

$$\sum_{\substack{p>31 \text{ prime} \\ 2p+1 \text{ prime}}} \frac{p-1}{(2p+1)^2} < 0.170121.$$

Proof. We break the sum into two parts and evaluate the integral numerically to get

$$\sum_{\substack{31<p<10^{10} \\ 2p+1 \text{ prime}}} \frac{p-1}{(2p+1)^2} + \sum_{\substack{p>10^{10} \\ 2p+1 \text{ prime}}} \frac{p-1}{(2p+1)^2} < 0.067897 + \frac{1}{4} \sum_{\substack{p>10^{10} \text{ prime} \\ 2p+1 \text{ prime}}} \frac{1}{p} < 0.170121.$$

□

Now we calculate an upper bound for a double sum over primes $p > 31$ and primes q congruent to 1 modulo p.

Proposition 4.9.4. *The following double sum has an upper bound*

$$\sum_{\substack{p \text{ prime} \\ p>31}} \sum_{\substack{q \text{ prime} \\ q\equiv 1(\bmod p)}} \frac{p-1}{q^2} = \sum_{a\geq 2} \sum_{\substack{p>31 \text{ prime} \\ ap+1 \text{ prime}}} \frac{p-1}{(ap+1)^2} < 0.319878.$$

Proof. We break the sum into several parts. In the previous proposition, we calculated an estimate for the $a = 2$ terms. Next we calculate the finite sum

$$\sum_{a=4}^{100} \sum_{\substack{31<p<10^9 \\ ap+1 \text{ prime}}} \frac{p-1}{(ap+1)^2} < 0.047986.$$

Now let

$$G(y) = \min\left(\frac{1}{y^2}, \frac{1}{y^2 + F(e^y)} + 2e^{-y/2}\right).$$

Using the density bound for π_{ap+1}, we get an upper bound for the sum

$$\sum_{a=4}^{100} \sum_{\substack{p>10^9 \\ ap+1 \text{ prime}}} \frac{p-1}{(ap+1)^2} < \sum_{\substack{a=4 \\ a \text{ even}}}^{100} \left(\frac{16C_2}{a^2} \int_{\log 10^9}^{\infty} G(y)\, dy \prod_{p|a,\, p\neq 2} \frac{p-1}{p-2}\right) < 0.095835.$$

Finally, we again use the density bound to get an upper bound for the sum

$$\sum_{a>100} \sum_{\substack{p>31 \\ ap+1 \text{ prime}}} \frac{p-1}{(ap+1)^2} < \sum_{\substack{a>100 \\ a \text{ even}}} \left(\frac{16C_2}{a^2} \int_{\log 37}^{\infty} G(y)\, dy \prod_{p|a,\, p\neq 2} \frac{p-1}{p-2}\right).$$

To get an upper bound for the product $\prod(p-1)/(p-2)$, we observe that if an even integer a has N distinct odd prime factors, we have

$$\prod_{p|a,\, p\neq 2} \frac{p-1}{p-2} = \frac{p_1-1}{p_1-2} \cdot \frac{p_2-1}{p_2-2} \cdots \frac{p_N-1}{p_N-2} \leq \frac{2}{1} \cdot \frac{3}{2} \cdots \frac{N+1}{N} = N+1.$$

Since the number N of odd prime divisors of a is less than $\log a$, we have

$$\sum_{a>100} \sum_{\substack{p>31 \\ ap+1 \text{ prime}}} \frac{p-1}{(ap+1)^2} < 16C_2 \int_{\log 37}^{\infty} G(y)\, dy \sum_{\substack{a>100 \\ a \text{ even}}} \frac{1+\log a}{a^2} < 0.005936.$$

This gives us an explicit upper bound for the double sum

$$\sum_{a\geq 2} \sum_{\substack{p>31 \text{ prime} \\ ap+1 \text{ prime}}} \frac{p-1}{(ap+1)^2} < 0.170121 + 0.047986 + 0.095835 + 0.005936 = 0.319878.$$

□

4.10 Revisiting the first layers $\mathbb{B}_{p,1}$

We return to the conjecture that all first layers $\mathbb{B}_{p,1}$ have class number 1. To estimate the probability that this conjecture is true, we calculate the following upper bound.

Proposition 4.10.1. *There is an upper bound for the double sum*

$$\sum_{p>31} \sum_{\substack{q \text{ prime} \\ q \neq p}} \frac{p-1}{fq^{2f}} < 0.321365$$

and an upper bound for the triple sum,

$$-\sum_{p>31} \sum_{\substack{q \text{ prime} \\ q \neq p}} \sum_{k \geq 2} \frac{p-1}{f} \log(1-q^{-fk}) < 0.327793,$$

where f is the order of q modulo p.

Proof. We first break the double sum into two pieces:

$$\sum_{p>31} \sum_{\substack{q \text{ prime} \\ q \neq p}} \frac{p-1}{fq^{2f}} = \sum_{p>31} \sum_{\substack{q \text{ prime} \\ q \neq p, f=1}} \frac{p-1}{fq^{2f}} + \sum_{p>31} \sum_{\substack{q \text{ prime} \\ q \neq p, f>1}} \frac{p-1}{fq^{2f}}$$
$$\leq \sum_{\substack{p \text{ prime} \\ p>31}} \sum_{\substack{q \text{ prime} \\ q \equiv 1 (\bmod p)}} \frac{p-1}{q^2} + \sum_{f \geq 2} \sum_{q \text{ prime}} \frac{1}{fq^{2f}} \sum_{\substack{p>31 \text{ prime} \\ p | q^f-1}} (p-1).$$

In Proposition 4.9.4, we proved that the first term on the right has an upper bound

$$\sum_{\substack{p \text{ prime} \\ p>31}} \sum_{\substack{q \text{ prime} \\ q \equiv 1 (\bmod p)}} \frac{p-1}{q^2} < 0.319878.$$

To estimate the terms with $f \geq 2$, we observe that the number of prime divisors $p > 31$ of an integer m is less than $\log_{37} m < 0.28 \log m$. Thus we have

$$\sum_{\substack{p>31 \text{ prime} \\ p | q^f-1}} (p-1) < 0.28(q^f-1)\log(q^f-1) < 0.28 f q^f \log q.$$

Using this estimate to bound the terms with $q^f > 10^6$,

$$\sum_{f \geq 2} \sum_{q \text{ prime}} \frac{1}{fq^{2f}} \sum_{\substack{p>31 \text{ prime} \\ p | q^f-1}} (p-1) < \sum_{f \geq 2} \sum_{\substack{q \text{ prime} \\ q^f < 10^6}} \frac{1}{fq^{2f}} \sum_{\substack{p | q^f-1 \\ p>31}} (p-1) + \sum_{f \geq 2} \sum_{\substack{q \text{ prime} \\ q^f > 10^6}} \frac{0.28 \log q}{q^f},$$

we can rearrange to get

$$\sum_{f\geq 2}\sum_{q \text{ prime}} \frac{1}{fq^{2f}} \sum_{\substack{p>31 \text{ prime} \\ p|q^f-1}} (p-1) < \sum_{f\geq 2}\sum_{q \text{ prime}} \frac{0.28\log q}{q^f} - \sum_{\substack{f\geq 2 \\ q^f<10^6}} \frac{1}{fq^{2f}} \left(0.28fq^f\log q - \sum_{\substack{p|q^f-1 \\ p>31}}(p-1)\right).$$

We then explicitly calculate the terms with $q^f < 10^6$

$$\sum_{\substack{f\geq 2 \\ q^f<10^6}} \frac{1}{fq^{2f}} \left(0.28fq^f\log q - \sum_{\substack{p|q^f-1 \\ p>31}}(p-1)\right) > 0.210016.$$

Thus, we have

$$\sum_{f\geq 2}\sum_{q \text{ prime}} \frac{1}{fq^{2f}} \sum_{\substack{p>23 \text{ prime} \\ p|q^f-1}} (p-1) < -0.210016 + 0.28 \sum_{q \text{ prime}} \frac{\log q}{q(q-1)}.$$

Since $\sum_{q \text{ prime}}(\log q)/q^2 = 0.4930911093\ldots$ (see [6]), it is a straightforward calculation to show that

$$\sum_{q \text{ prime}} \frac{\log q}{q(q-1)} < \sum_{q<10^6} \frac{\log q}{q(q-1)} + \frac{10^6}{10^6-1} \sum_{q>10^6} \frac{\log q}{q^2} < 0.755367.$$

Therefore, as expected, we find that the contribution from the $f \geq 2$ terms is relatively small

$$\sum_{f\geq 2}\sum_{q \text{ prime}} \frac{1}{fq^{2f}} \sum_{\substack{p>31 \text{ prime} \\ p|q^f-1}} (p-1) < -0.210016 + 0.28 \times 0.755367 < 0.001487.$$

We conclude that our double sum has an upper bound

$$\sum_{p>31}\sum_{\substack{q \text{ prime} \\ q\neq p}} \frac{p-1}{fq^{2f}} < 0.319878 + 0.001487 = 0.321365,$$

and that our triple sum has an upper bound

$$-\sum_{p>31}\sum_{\substack{q \text{ prime} \\ q\neq p}}\sum_{k\geq 2} \frac{p-1}{f}\log(1-q^{-fk}) < 1.02 \sum_{p>31}\sum_{\substack{q \text{ prime} \\ q\neq p}} \frac{p-1}{fq^{2f}} < 0.327793.$$

□

Let P_T denote the probability (based on the Cohen-Lenstra heuristics) that all the first level fields $\mathbb{B}_{p,1}$ have class number 1. Then, by the above proposition, we estimate that $-\log P_T < 0.327793$. We can further refine our estimate by considering the results of Hakkarainen [12], who calculated certain divisors of the class number for abelian number fields of conductors less than 2000. Since the fields $\mathbb{B}_{p,1}$ have conductor p^2, we can apply Hakkarainen's results to the fields $\mathbb{B}_{37,1}$, $\mathbb{B}_{41,1}$ and $\mathbb{B}_{43,1}$. He showed that the class numbers of those fields do not have any odd prime divisors less than 10000. By excluding these terms from our sum, we can reduce our estimate for $-\log P_T$ by 0.010431. Furthermore, by Theorem 4.0.36, we know the parity of the class number of $\mathbb{B}_{p,1}$ is odd for $p < 500$, so we can further reduce our estimate for $-\log P_T$ by 0.001131. Finally, we can incorporate unpublished results by T. Fukuda that $2p + 1$ does not divide the class number of $\mathbb{B}_{p,1}$ for Sophie Germain primes less than 1000. Fukuda's results reduce our estimate for $-\log P_T$ by 0.030415. This give us an adjusted upper bound for $-\log P_T$ of

$$-\log P_T < 0.327793 - 0.010431 - 0.001131 - 0.030415 = 0.285816.$$

This gives a lower bound for P_T of

$$P_T = \exp(-0.285816) > 0.75.$$

Thus, assuming the validity of the Cohen-Lenstra heuristics, the probability that the conjecture that all the first layers $\mathbb{B}_{p,1}$ have class number 1 is at least 75%.

4.11 Higher layers of the $\mathbb{Z}_p$-extensions

The higher layers of the $\mathbb{Z}_p$-extensions have a relatively small contribution to our estimates, and an upper bound is much easier to establish. Let P_T be the conditional probability that all the $\mathbb{B}_{p,n}$, for primes $p > 31$ and layers $n \geq 2$, have class number 1, conditional upon all of the first layers $\mathbb{B}_{p,1}$ having class number 1. We estimate P_T by applying the Cohen-Lenstra heuristics

$$P_T = \prod_{\substack{p \text{ prime} \\ p>31}} \prod_{\substack{q \text{ prime} \\ q \neq p}} \prod_{j \geq 2} \prod_{k \geq 2} (1 - q^{-fk})^{\phi(p^j)/f}.$$

We use the following proposition to estimate $-\log P_T$.

Proposition 4.11.1. *The following quadruple sum has an upper bound*

$$-\sum_{\substack{p\,\text{prime}\\p>31}}\sum_{\substack{q\,\text{prime}\\q\neq p}}\sum_{j\geq 2}\sum_{k\geq 2}\frac{\phi(p^j)}{f}\log(1-q^{-fk})<0.010398,$$

where ϕ is the Euler totient function and f is the order of q modulo p^j.

Proof. Let S denote the quadruple sum. Similarly to our earlier arguments, the sum S has an upper bound

$$S<1.02\sum_{p>31}\sum_{q\neq p}\sum_{j\geq 2}\frac{\phi(p^j)}{fq^{2f}}.$$

Since $q^f=1+p^jt$ for some integer t, we have

$$S<1.02\sum_{p>31}\sum_{j\geq 2}\sum_{t\geq 1}\frac{(p-1)p^{j-1}}{(1+p^jt)^2}<1.02\sum_{p>31}\sum_{j\geq 2}\sum_{t\geq 1}\frac{p-1}{p^{j+1}t^2}=1.02\frac{\pi^2}{6}\sum_{p>31}\frac{1}{p^2}.$$

Since $\sum_p 1/p^2=0.452247420041\ldots$, it is straightforward to calculate that

$$S<1.02\frac{\pi^2}{6}\times\sum_{p>31}1/p^2<1.02\frac{\pi^2}{6}\times 0.006197<0.010398.$$

□

4.12 Summary of results and remarks

We summarize the preceding results in Table 4.3, which gives upper bounds for $-\log P_T$, where P_T is the expected probability that the associated conjecture is true, based on the Cohen-Lenstra heuristics. In particular, for our Main Conjecture, we have that

$$-\log P_T=-\sum_{\substack{p\,\text{prime}\\ \text{excluding terms where the}\\ q\text{-part of the class group}\\ \text{is known to be trivial}}}\sum_{q\,\text{prime}}\sum_{j=1}^{\infty}\sum_{k\geq 2}\frac{\phi(p^j)}{f}\log(1-q^{-fk})<0.301215.$$

Thus, assuming the validity of the Cohen-Lenstra heuristics, the probability that the Main Conjecture is true is at least 74%.

$$P_T>e^{-0.301215}\approx 74\%.$$

Table 4.3: Upper bounds for $-\log P_T$

Prime p	**1st level**	**Level** > 1	**Total**
2	0	1.3×10^{-8}	1.3×10^{-8}
3	0	1.1×10^{-8}	1.1×10^{-8}
5	0	0.001868	0.001868
7	0	0.001626	0.001626
11	0	0.000901	0.000901
13	0	0.000449	0.000449
17	0	0.000052	0.000052
19	0	0.000027	0.000027
23	0	0.000018	0.000018
29	0	0.000041	0.000041
31	0	0.000019	0.000019
$p > 31$	0.285816	0.010398	0.296214
Total	0.285816	0.015399	**0.301215**

This is perhaps unduly pessimistic. If we were to replace the rigorous density bounds of Siebert with the conjectural asymptotics of Hardy and Littlewood, then our estimate for $-\log P_T$ would be approximately 0.126, giving a probability estimate of 88%. This gives strong heuristic support for our conjecture that all fields in the cyclotomic $\mathbb{Z}_p$-extensions over $\mathbb{Q}$ have trivial class group.

For the more skeptically-minded, our analysis indicates the most likely places to look for possible counterexamples. The largest contributions to our estimates arise from the 1st level $\mathbb{B}_{p,1}$ of the $\mathbb{Z}_p$-extension at the smaller Sophie Germain primes p; we then consider the $(2p+1)$-part of their class number. The smallest such prime p for which we do not know the $(2p+1)$-part of the class number is $p = 1013$. Nevertheless, such primes between 1000 and 10,000 still only contribute about 0.01 to our sum, so we would expect to only have about a 1% chance of producing a counterexample among those primes. Similarly, for primes p such that $53 \leq p \leq 10000$ and $4p+1$ is prime, we expect to have only an approximately 1% chance of producing a counterexample.

Chapter 5

Conclusion and directions for further work

It is remarkable to observe the power of analytic objects – the L-functions and their explicit formulae – when brought to bear on the essentially algebraic problem of determining the class number of a number field. For example, to unconditionally prove that $\mathbb{Q}[\zeta_{83} + \zeta_{83}^{-1}]$ is a principal ideal domain using the explicit formula, we really only need to prove three prime ideals are principal, which stands in stark contrast to using the Minkowski bound, which require approximately 10^{20} primes to be checked.

The techniques used in this thesis may be used to calculate upper bounds of class numbers of other totally real number fields of moderately large discriminant, allowing us to tackle the class number problem for a large group of number fields which previously had not been treatable by any known methods.

It is possible use the methods in this paper to unconditionally calculate the class numbers of abelian fields of even larger conductors, but the amount of required calculation of principal prime ideals would grow roughly exponentially with the conductor. This problem can be alleviated by assuming the generalized Riemann hypothesis, requiring us to find far fewer principal prime ideals. However, even under GRH, the "principal ideal problem" for fields of very large degree or discriminant becomes quite challenging.

In a different direction, these techniques can be extended to nonabelian fields. Compared to abelian fields, the arithmetic of nonabelian fields is highly nontrivial; in particular we lack a nonabelian class field theory. So it is of theoretical interest to have a better understanding of the behavior of their class groups. Yet aside from fields of small degree, very little is known.

One area that has been explored are the ray class fields of an imaginary quadratic field K, where the base field K has class number 1. These fields are nonabelian, with dihedral Galois group. Kucuksakalli [15] has studied the class number divisibility properties of these fields. Class number upper bound could be used determine these fields' precise class number. For example, using Odzlyko's discriminant bounds, we can produce a degree 204 number field with class number 1, the largest degree number field so far proved to have class number 1. Elliptic units and the theory of complex multiplication could be used to explicitly write down an integral basis for these fields.

Letting K still denote an imaginary quadratic field with class number 1, we can construct the usual cyclotomic $\mathbb{Z}_p$-extensions of K, and we can also construct $\mathbb{Z}_p$-extensions out of towers of ray class fields of K. Over $\mathbb{Q}$, these two types of $\mathbb{Z}_p$-extensions coincide, but they are not the same over K. In fact, their class groups seem to exhibit markedly different properties. The class numbers of fields in the cyclotomic $\mathbb{Z}_p$-extension of K grow rapidly as the level increases. But for these "ray class" $\mathbb{Z}_p$-extensions of K, the situation is similar to $\mathbb{Q}$: as yet there are no known examples of nontrivial class groups. Why do the class number properties of these "ray class" $\mathbb{Z}_p$-extensions differ so markedly from the properties of cyclotomic $\mathbb{Z}_p$-extensions? And might the Main Conjecture in Chapter 4 be reasonably extended, with appropriate modifications, from $\mathbb{Q}$ to such K?

Another family of nonabelian number fields bears exploration. Let K_n be the number fields given by

$$K_n = \mathbb{Q}[X]/(X^n - X - 1).$$

This curious family of mixed signature fields has Galois group isomorphic to the symmetric group S_n, and was studied by Serre [32] for $n \leq 4$ and by Bryk [3] for $n = 5$. We have calculated the class group for these fields for all $n \leq 51$ using SageMathCloud$^{\text{TM}}$ [30]. Surprisingly, all have class number 1! We seek a convincing explanation for this phenomenon, and hope that the exploration of such families gives us clues as to the deeper structure that controls their class numbers.

References

[1] E. Agathocleous, 'Class Numbers of Real Cyclotomic Fields of Conductor *pq*', Thesis (Ph.D.), University of Maryland (College Park). `http://drum.lib.umd.edu/handle/1903/9832`

[2] H. Bauer, *Numerische Bestimmung von Klassenzahlen reeller zyklischer Zahlkörper*, J. of Number Theory 1 (1969), 161–162. `http://dx.doi.org/10.1016/0022-314X(69)90034-1`

[3] J. Bryk, *On the roots of polynomials modulo primes*, Ph.D. thesis, Rutgers University (2012). `http://www.math.rutgers.edu/~jbryk/jb90900p.pdf`

[4] J. Buhler, C. Pomerance, and L. Robertson, *Heuristics for class numbers of prime-power real cyclotomic fields*, High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams, Banff, AB, 2003, Fields Inst. Commun., vol. 41, Amer. Math. Soc., Providence, RI (2004), 149–157.

[5] J. Coates, *The enigmatic Tate-Shafarevich group*, Fifth International Congress of Chinese Mathematicians, Part 1, AMS/IP Stud. Adv. Math. 51, Amer. Math. Soc., Providence, RI (2012), 43–50.

[6] H. Cohen, *High precision computation of Hardy-Littlewood constants*, preprint. `http://www.math.u-bordeaux1.fr/~cohen/hardylw.dvi`

[7] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups*, Number Theory, Lecture Notes in Math. 1052, Springer, Berlin (1984), 26–36. `http://dx.doi.org/10.1007/BFb0071539`

[8] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, Number Theory, Noordwijkerhout 1983, Lecture Notes in Math. 1068, Springer, Berlin (1984), 33–62. `http://dx.doi.org/10.1007/BFb0099440`

[9] H. Cohn, *A numerical study of Weber's real class number calculation, I*, Numer. Math. 2 (1960), 347–362. `http://dx.doi.org/10.1007/BF01386236`

[10] T. Fukuda and K. Komatsu, *Weber's class number problem in the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, III*, Int. J. Number Theory 7, no. 06 (2011), 1627–1635. `http://dx.doi.org/10.1142/S1793042111004782`

[11] T. Fukuda, K. Komatsu, and T. Morisawa, *Weber's class number one problem*, to appear in Iwasawa Theory 2012, Contrib. Math. Comput. Sci. 7 (2014).

[12] T. Hakkarainen, *On the computation of class numbers of real abelian fields*, Math. Comp. 78, no. 265 (2009), 555–573. `http://dx.doi.org/10.1090/S0025-5718-08-02169-8`

[13] H. Ichimura and S. Nakajima, *On the 2-part of the ideal class group of the cyclotomic $\mathbb{Z}_p$-extension over the rationals*, Abh. Math. Sem. Univ. Hamburg 80, (2010), 175–182. http://dx.doi.org/10.1007/s12188-010-0036-x

[14] K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg 20, (1956), 257–258.

[15] O. Kucuksakalli, *Class numbers of ray class fields of imaginary quadratic fields*, Math. Comp. 80, no. 274 (2011): 1099–1122. http://dx.doi.org/10.1090/S0025-5718-2010-02413-5

[16] F. J. van der Linden, *Class number computations of real abelian number fields*, Math. Comp. 39, no. 160 (1982), 693–707. http://dx.doi.org/10.1090/S0025-5718-1982-0669662-5

[17] J. M. Masley, *Class numbers of real cyclic number fields with small conductor*, Compos. Math. 37, no. 3 (1978), 297–319. https://eudml.org/doc/89385

[18] J. C. Miller, *Class numbers of totally real fields and applications to the Weber class number problem*, Acta Arith. 164, no. 4 (2014), 381–397. http://dx.doi.org/10.4064/aa164-4-4

[19] J. C. Miller, *Real cyclotomic fields of prime conductor and their class numbers*, published electronically in Math. Comp (2015). http://dx.doi.org/10.1090/S0025-5718-2015-02924-X

[20] J. C. Miller, *Class numbers of real cyclotomic fields of composite conductor*, LMS J. Comput. Math. 17, Special Issue A (2014), 404–417. http://dx.doi.org/10.1112/S1461157014000382

[21] J. C. Miller, *Class numbers in cyclotomic $\mathbb{Z}_p$-extensions*, J. Number Theory 150 (2015), 47–53. http://dx.doi.org/10.1016/j.jnt.2014.11.008

[22] T. Morisawa, *On Weber's class number problem*, Thesis (Ph.D.), Waseda University, 2012. https://dspace.wul.waseda.ac.jp/dspace/bitstream/2065/37750/3/Honbun-5869.pdf

[23] A. M. Odlyzko, *Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results*, Sém. Théor. Nombres Bordeaux (2) 2 (1990), no. 1, 119–141.

[24] A. M. Odlyzko, *Table 3: GRH bounds for discriminants*, http://www.dtc.umn.edu/~odlyzko/unpublished/discr.bound.table3

[25] A. M. Odlyzko, *Table 4: Unconditional bounds for discriminants*, http://www.dtc.umn.edu/~odlyzko/unpublished/discr.bound.table4

[26] The PARI Group, PARI/GP version 2.7.0, Bordeaux, 2014, http://pari.math.u-bordeaux.fr/.

[27] G. Poitou, *Sur les petits discriminants*, Séminaire Delange-Pisot-Poitou, Théorie des nombres 18, no. 1 (1976), 1–17.

[28] H. Riesel and R. C. Vaughan, *On sums of primes*, Ark. Mat. 21, (1983), 46–74. http://dx.doi.org/10.1007/BF02384300

[29] W. Stein et al., Sage Mathematics Software (Version 5.11), The Sage Development Team, 2013, http://www.sagemath.org.

[30] W. Stein et al., Sage Mathematics Software (Version 6.2.rc2), The Sage Development Team, 2014, http://www.sagemath.org.

[31] R. Schoof, *Class numbers of real cyclotomic fields of prime conductor*, Math. Comp. 72, no. 242 (2003), 913–937. http://dx.doi.org/10.1090/S0025-5718-02-01432-1

[32] J.-P. Serre, *On a theorem of Jordan*, Bull. Amer. Math. Soc. 40 (2003), 429–440. http://dx.doi.org/10.1090/S0273-0979-03-00992-3

[33] H. Siebert, *Montgomery's weighted sieve for dimension two*, Monatsh. Math. 82 (1976), no. 4, 327–336. http://dx.doi.org/10.1007/BF01540603

[34] L. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics 83, Second edition, Springer-Verlag, New York, 1997.

[35] L. Washington, *The non-p-part of the class number in a cyclotomic* $\mathbb{Z}_p$*-extension*, Inv. Math. 49 (1978), 87–97. http://dx.doi.org/10.1007/BF01399512

[36] H. Weber, *Theorie der Abel'schen Zahlkörper*, Acta Mathematica 8, no. 1 (1886): 193–263. http://dx.doi.org/10.1007/BF02417089