Title:
Norm-Euclidean Galois fields

Author:
McGown, Kevin Joseph

Acceptance Date:
01-01-2010

Series:
UC San Diego Electronic Theses and Dissertations

Degree:
Ph. D., UC San Diego

Permalink:
http://escholarship.org/uc/item/359664zv

Local Identifier:
b6851546

Abstract:
In this work, we study norm-Euclidean Galois number fields. In the quadratic setting, it is known that there are finitely many and they have been classified. In 1951, Heilbronn showed that for each odd prime l, there are finitely many norm-Euclidean Galois fields of degree l. Unfortunately, his proof does not provide an upper bound on the discriminant, even in the cubic case. We give, for the first time, an upper bound on the discriminant for this class of fields. Namely, for each odd prime l we give an upper bound on the discriminant of norm-Euclidean Galois fields of degree l. In Chapter 3, we derive various inequalities which guarantee the failure of the norm- Euclidean property. Our inequalities involve the existence of small integers satisfying certain splitting and congruence conditions; this reduces the problem to the study of character non-residues. This also leads to an algorithm for tabulating a list of candidate norm- Euclidean Galois fields (of prime degree l up to a given discriminant. We have implemented this algorithm and give some numerical results when l < 30. The cubic case is especially interesting as Godwin and Smith have classified all norm-Euclidean Galois cubic fields with [Delta] < 10□. Using an efficient implementation of our algorithm, we extend their classification to include all fields with [Delta] < 10²□. In Chapter 4, we turn to the study of character non-residues. In sect. 4.1, we give a new estimate of the second smallest prime non-residue, and in sect. 4.2, we derive an explicit version of a character sum estimate due to Burgess following a method of Iwaniec. In Chapter 5, we combine a result of Norton on the smallest non-residue with our results from Chapter 4 to obtain the aforementioned discriminant bounds. In Chapter 6, we give strengthened versions of all our results assuming the Generalized Riemann Hypothesis. Finally, in Chapter 7, we summarize what our results say in the cubic case and use a combination of theory and computation to give, assuming the GRH, a complete determination of all norm-Euclidean Galois cubic fields

UNIVERSITY OF CALIFORNIA, SAN DIEGO

Norm-Euclidean Galois Fields

A dissertation submitted in partial satisfaction of the
requirements for the degree
Doctor of Philosophy

in

Mathematics

by

Kevin Joseph McGown

Committee in charge:

Professor Harold Stark, Chair
Professor Wee Teck Gan
Professor Ronald Graham
Professor Russell Impagliazzo
Professor Cristian Popescu

2010

The dissertation of Kevin Joseph McGown is approved, and it is acceptable in quality and form for publication on microfilm and electronically:

_____

_____

_____

_____

_____
Chair

University of California, San Diego

2010

DEDICATION

To my wife

TABLE OF CONTENTS

LIST OF TABLES

ACKNOWLEDGEMENTS

I would like to thank Professor Harold Stark for his invaluable guidance throughout my dissertation research, and for our many interesting mathematical discussions over lunch. I would like to thank Professor Gan, Professor Popescu, and Professor Stark for sharing their unique perspectives on number theory inside and outside the classroom, and for their encouragement throughout my doctoral education. The Mathematics Department at the University of California, San Diego has been a truly wonderful place to study number theory.

I would like to thank my wife Derya for her unwavering support throughout my graduate career, and my parents Susan and Robert for supporting my interests from childhood to adulthood. Finally, I thank my cat Boncuk and my dog Kuma for being the perfect companions during solitary days of theorem proving.

VITA

2004	B. S. in Mathematics, magna cum laude, Oregon State University
2004	B. S. in Computer Science, magna cum laude, Oregon State University
2004–2005	Graduate Teaching Assistant, Oregon State University
2005	M. S. in Mathematics, Oregon State University
2005–2010	Graduate Teaching Assistant, University of California, San Diego
2007–2008	Adjunct Professor, San Diego Miramar College
2008	C. Phil. in Mathematics, University of California, San Diego
2009	Associate Instructor, University of California, San Diego
2010	Ph. D. in Mathematics, University of California, San Diego

ABSTRACT OF THE DISSERTATION

Norm-Euclidean Galois Fields

by

Kevin Joseph McGown
Doctor of Philosophy in Mathematics
University of California San Diego, 2010
Professor Harold Stark, Chair

In this work, we study norm-Euclidean Galois number fields. In the quadratic setting, it is known that there are finitely many and they have been classified. In 1951, Heilbronn showed that for each odd prime ℓ, there are finitely many norm-Euclidean Galois fields of degree ℓ. Unfortunately, his proof does not provide an upper bound on the discriminant, even in the cubic case. We give, for the first time, an upper bound on the discriminant for this class of fields. Namely, for each odd prime ℓ we give an upper bound on the discriminant of norm-Euclidean Galois fields of degree ℓ.

In Chapter 3, we derive various inequalities which guarantee the failure of the norm-Euclidean property. Our inequalities involve the existence of small integers satisfying certain splitting and congruence conditions; this reduces the problem to the study of character non-residues. This also leads to an algorithm for tabulating a list of candidate norm-Euclidean Galois fields (of prime degree ℓ) up to a given discriminant. We have implemented this algorithm and give some numerical results when $\ell < 30$. The cubic case is especially interesting as Godwin and Smith have classified all norm-Euclidean Galois cubic fields with $|\Delta| < 10^8$. Using an efficient implementation of our algorithm, we extend their classification to include all fields with $|\Delta| < 10^{20}$.

In Chapter 4, we turn to the study of character non-residues. In §4.1, we give a new estimate of the second smallest prime non-residue, and in §4.2, we derive

an explicit version of a character sum estimate due to Burgess following a method of Iwaniec. In Chapter 5, we combine a result of Norton on the smallest non-residue with our results from Chapter 4 to obtain the aforementioned discriminant bounds. In Chapter 6, we give strengthened versions of all our results assuming the Generalized Riemann Hypothesis.

Finally, in Chapter 7, we summarize what our results say in the cubic case and use a combination of theory and computation to give, assuming the GRH, a complete determination of all norm-Euclidean Galois cubic fields.

1 Introduction

1.1 First Notions

Around 300 B.C. Euclid discovered the algorithm now bearing his name which allows one to compute the greatest common divisor d of two integers $a, b \in \mathbb{Z}$, and moreover, to express d as a $\mathbb{Z}$-linear combination of a and b. From this it follows that if a prime p divides ab, then p divides a or p divides b. This leads immediately to the remarkable conclusion that every positive integer factors uniquely as the product of primes, known as the Fundamental Theorem of Arithmetic. Gauss follows exactly this argument in *Disquisitiones Arithmeticae*, where he gives what is possibly the first clear statement and proof of this theorem [20, 33]. Euclid's geometric language lacked the ability to state the theorem [23, 30], although one could argue that the theorem was known, in principle, since his time. It is the following crucial property of $\mathbb{Z}$ that guarantees the Euclidean algorithm will terminate after a finite number of steps: for every $a, b \in \mathbb{Z}$, $b \neq 0$ there exists $q, r \in \mathbb{Z}$ such that $a = qb + r$ with $|r| < |b|$. In the words of Hardy and Wright [23]: "Euclid knew very well that the theory of numbers turned upon his algorithm."

Now we widen our scope beyond the rational numbers. Let K be an algebraic number field with ring of integers $\mathcal{O}_K$, and denote by $N = N_{K/\mathbb{Q}}$ the absolute norm map. (We briefly recall that a number field K is a finite extension of $\mathbb{Q}$, or more concretely $K = \mathbb{Q}(\theta)$ for some algebraic $\theta \in \mathbb{C}$, and that $\mathcal{O}_K$ is the subring of K consisting of algebraic integers; the norm is defined as $N(\alpha) := \prod_\sigma \sigma(\alpha)$, where the product runs over all field embeddings $\sigma : K \to \mathbb{C}$.) We call a number field K norm-Euclidean if for every $\alpha, \beta \in \mathcal{O}_K$, $\beta \neq 0$, there exists $\gamma \in \mathcal{O}_K$ such that $|N(\alpha - \gamma\beta)| < |N(\beta)|$. Or equivalently, for every $\alpha \in K$ there exists $\gamma \in \mathcal{O}_K$ such

that $|N(\alpha-\gamma)|<1$. If we set $K=\mathbb{Q}$, this reduces to the aforementioned property of $\mathbb{Z}$.

Although the generalization of the Euclidean property to number fields just described is the natural and classical one, the reason for the prefix "norm" is that there is a more general notion of a Euclidean ring. If R is an integral domain, then we say that R is Euclidean if there exists a function $\partial : R \setminus \{0\} \to \mathbb{Z}^+$ such that for every $a, b \in R$, $b \neq 0$ there exists $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $\partial(r) < \partial(b)$. Using this definition, when we say K is norm-Euclidean, we really mean that the ring $\mathcal{O}_K$ is Euclidean with respect to the function $\partial(\alpha) = |N(\alpha)|$; this slight abuse of language should create no confusion.

Following the same proof as in the case of the rational integers, one finds that if K is Euclidean then $\mathcal{O}_K$ is a unique factorization domain, i.e., K has class number one. However, the converse does not hold in general; the number field $\mathbb{Q}(\sqrt{-19})$ furnishes an example of a class number one field that is not Euclidean with respect to any function [45]. Once number fields are introduced, it is natural to ask — which number fields are norm-Euclidean? This innocent question proves to be very difficult.

1.2 History

The simplest number fields, other than $\mathbb{Q}$, are the quadratic ones, where $K = \mathbb{Q}(\sqrt{d})$. We will assume d is squarefree, so that the discriminant of K satisfies either $\Delta = d$ or $\Delta = 4d$ depending upon the congruence class of d modulo 4. If K is imaginary quadratic ($d < 0$), then it is a homework exercise to show that there are finitely many K which are norm-Euclidean and that they occur exactly when

$$d = -1, -2, -3, -7, -11\,.$$

Of course these 5 fields necessarily have the unique factorization property (class number one). There are precisely 4 additional imaginary quadratic fields which have class number one, but are not norm-Euclidean: $d = -19, -43, -67, -163$. The fact that there are only 9 imaginary quadratic fields with class number one is a deep result, sometimes known as the Stark–Baker–Heegner Theorem, which we

won't discuss further here. We only mention this so as to contrast this case against the real quadratic case ($d > 0$), where it is conjectured there are infinitely many fields with class number one. Although the Cohen–Lenstra heuristics (see [12]) purport to give the exact proportion of real quadratic fields of prime discriminant with class number one ($\approx 75.446\%$), at present it seems hopeless even to prove that there are infinitely many. In spite of the apparent abundance of class number one fields, Heilbronn showed (see [24]):

Theorem 1.1 (Heilbronn, 1938)**.** *There are only finitely many real quadratic number fields which are norm-Euclidean.*

This result brings partially into light how much stronger the norm-Euclidean property is than the unique factorization property. Once one knows that there are finitely many number fields with a given property, of course the natural inclination is to classify them. Eventually, the following was shown:

Theorem 1.2 (1952)**.** *The norm-Euclidean real quadratic fields are exactly those with*

$$d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\,.$$

The classification above is usually attributed to Chatland and Davenport as they completed some of the final crucial steps (see [15, 10, 11]), but all told it took the work of over a dozen mathematicians, most of which took place in the two decades from 1930 – 1950. Additionally, there was a small mistake in the original classification regarding the mistaken identity of $\mathbb{Q}(\sqrt{97})$ which was corrected by Barnes and Swinnerton–Dyer in 1952 [4, 5]. We note in passing that the determination of norm-Euclidean real quadratic fields was completed just over a century after Wantzel first showed that $d = 2, 3, 5$ were norm-Euclidean [53].

Davenport was the first to prove a finiteness result for a class of fields outside of the quadratic setting (see [14]). His work on real quadratic fields generalized to show:

Theorem 1.3 (Davenport, 1950)**.** *There are only finitely many norm-Euclidean fields among all non-totally real cubic fields and totally complex quartic fields.*

In short, Davenport's techniques apply when the unit group has rank one. Inspired by Davenport's result, Heilbronn gives a generalization of his own work (see [25]) to show:

Theorem 1.4 (Heilbronn, 1950)**.** *There are only finitely many Galois cubic fields that are norm-Euclidean.*

This leaves open the case of totally real non-Galois cubic fields; although Heilbronn doesn't go so far as to conjecture that there are infinitely many norm-Euclidean fields of this type, he says that he would "be surprised to learn that the analogue of [the finiteness theorem] is true in this case." In his third and final paper on the Euclidean algorithm (see [26]), Heilbronn generalizes his finiteness result to various classes of cyclic fields. For us, the most important part of Heilbronn's result says:

Theorem 1.5 (Heilbronn, 1951)**.** *Given a prime ℓ, there are only finitely many norm-Euclidean Galois fields of degree ℓ.*

However, Heilbronn's result on cyclic fields does not give an upper bound on the discriminant, even in the cubic case. The case of Galois cubic fields is especially interesting, as we have the following (see [21, 48, 22]):

Theorem 1.6 (Godwin & Smith, 1993)**.** *The norm-Euclidean Galois cubic fields with discriminant $|\Delta| < 10^8$ are exactly those with*

$$\Delta = 7^2, 9^2, 13^2, 19^2, 61^2, 67^2, 103^2, 109^2, 127^2, 157^2 \,.$$

Lemmermeyer has further verified that this list constitutes all fields with $|\Delta| < 2.5 \cdot 10^{11}$ (see [33]).

1.3 Open Problems

Theorem 1.5 of Heilbronn leads to the following open problem:

Problem 1. *For each odd prime ℓ, give an upper bound on the discriminant of norm-Euclidean Galois fields of degree ℓ.*

If this problem can be solved, then in principle it should be possible to classify all such fields, for any fixed ℓ. This leads to:

Problem 2. *Fix an odd prime ℓ. Find an efficient way to generate a list containing all norm-Euclidean Galois fields of degree ℓ up to a given discriminant. The list should be of a reasonable length in the sense that it should be possible to treat the remaining fields on a case by case basis.*

Turning to the cubic case, we propose a special case of the previous problem:

Problem 3. *Give an efficient algorithm to extend Godwin and Smith's classification of Galois cubic fields to include all fields with $|\Delta| < 10^{20}$.*

If one could find an especially good upper bound for the discriminant in the cubic case, then one could hope to solve the following problem:

Problem 4. *Classify all norm-Euclidean Galois cubic fields.*

This final problem represents a very concrete, long-standing open problem in the study of algebraic number fields. It is quite likely that Godwin and Smith's list constitutes the complete classification, but no one seems to have raised this question or put forth a conjecture on the matter.

1.4 Main Results

Now we give a brief summary of the author's main results, omitting proofs and technical details. Most of the results stated in this section are special cases of more detailed results found throughout the dissertation. Let $K/\mathbb{Q}$ denote a Galois number field of odd prime degree ℓ and discriminant Δ, which is necessarily cyclic. If K is norm-Euclidean, then it has class number one and therefore the discriminant of K must satisfy $\Delta = f^{\ell-1}$ where f is a prime with $f \equiv 1 \pmod{\ell}$; this is true provided, for each ℓ, we ignore a single field of discriminant $\ell^{2(\ell-1)}$. Building on the work of Heilbronn, we obtain various conditions under which K fails to be norm-Euclidean. In particular, we show:

Theorem. *Let K be a Galois number number of odd prime degree ℓ and conductor f with $(f, \ell) = 1$, and let χ be a primitive Dirichlet character modulo f of order ℓ. Denote by $q_1 < q_2$ the smallest rational primes which are inert in K. If there exists $r \in \mathbb{Z}^+$ with*

$$(r, q_1 q_2) = 1\,, \quad \chi(r) = \chi(q_2)^{-1}\,,$$
$$(q_1 - 1)(q_2 r - 1) \leq f$$
$$r q_2 k \not\equiv f \pmod{q_1^2}\,, \quad k = 1, \ldots, q_1 - 1\,,$$

then K is not norm-Euclidean.

Although the congruence condition in the above result is awkward to deal with in theoretical considerations, it is relatively harmless in computation as it is satisfied more than half the time. Based on the above result, the author has devised a simple algorithm, which provides a solution to Problem 2. We have implemented the algorithm in the mathematics software SAGE, thereby obtaining:

Theorem. *The following list contains all possible norm-Euclidean Galois number fields of prime degree ℓ and conductor f with $3 \leq \ell \leq 30$ and $f \leq 10^4$. (Of course, some of these fields may not be norm-Euclidean.)*

Table 1.1: Candidate norm-Euclidean fields of small degree

ℓ	$f \leq 10^4$
3	7, 9, 13, 19, 31, 37, 43, 61, 67, 73, 103, 109, 127, 157, 277, 439, 643, 997, 1597
5	11, 25, 31, 41, 61, 71, 151, 311, 431
7	29, 43, 49, 127, 239, 673, 701, 911
11	23, 67, 89, 121, 331, 353, 419, 617
13	53, 79, 131, 157, 169, 313, 443, 521, 937
17	137, 289, 443, 1259, 2687
19	191, 229, 361, 1103
23	47, 139, 277, 461, 529, 599, 691, 967, 1013, 1289
29	59, 233, 523, 841, 929, 2843, 3191

For the cubic case, we have implemented an efficient version of the algorithm in C, which takes advantage of the cubic reciprocity law. After 91 hours of computation, we met the goal set forth in Problem 3, thereby obtaining:

Theorem. *The norm-Euclidean Galois cubic fields with discriminant* $|\Delta| < 10^{20}$ *are exactly those with*

$$\Delta = 7^2, 9^2, 13^2, 19^2, 61^2, 67^2, 103^2, 109^2, 127^2, 157^2 .$$

In order to obtain discriminant bounds, we first remove the extra congruence condition from the earlier result. However, in doing this, there is a small price to be paid.

Theorem. *Let* K *be a Galois number number of odd prime degree* ℓ *and conductor* f *with* $(f, \ell) = 1$*, and let* χ *be a primitive Dirichlet character modulo* f *of order* ℓ*. Denote by* $q_1 < q_2$ *the smallest rational primes which are inert in* K*. Moreover, suppose* $q_1 \neq 2, 3$*. If there exists* $r \in \mathbb{Z}^+$ *such that*

$$(r, q_1 q_2) = 1 , \quad \chi(r) = \chi(q_2)^{-1} ,$$

$$3 q_1 q_2 r \log q_1 \leq f ,$$

then K *is not norm-Euclidean.*

In truth there are several variations on the above result, but this will suffice for illustrative purposes. Ignoring the restriction $q_1 \neq 2, 3$, which we will ultimately overcome, the basic strategy for obtaining discriminant bounds is clear. One would like to give very good explicit upper bounds on q_1, q_2, and r, as this would immediately yield an explicit inequality which clearly holds beyond some easily computable value of f. Of course, this is easier said than done, but it nonetheless reduces the problem to the study of character non-residues.

Let χ be a non-principal Dirichlet character modulo p, and denote by $q_1 < q_2$ the two smallest primes such that $\chi(q_1), \chi(q_2) \neq 1$. Motivated by the the discussion in the previous paragraph, we seek explicit upper bounds on q_1 and q_2. Norton gives an excellent bound on q_1 using a modification of a method due to Burgess (see [40]); namely, he shows $q_1 \leq 4.7\, p^{1/4} \log p$. We give another modification of Burgess' method which provides a bound on q_2, as long as q_1 is not too small.

Theorem. *Let* χ *be a non-principal Dirichlet character modulo a prime* $p \geq 10^{10}$*. Suppose* $q_1 < q_2$ *are the two smallest primes such that* $\chi(q_1), \chi(q_2) \neq 1$*. If* $q_1 > e^2 \log p$*, then*

$$q_2 < 7\, p^{1/4} \log p .$$

From the above, we can obtain a very good bound on the product $q_1 q_2$, which is what is required in our application.

Corollary. *Let χ be a non-principal Dirichlet character modulo a prime $p \geq 10^{12}$ having odd order. Suppose $q_1 < q_2$ are the two smallest primes such that $\chi(q_1), \chi(q_2) \neq 1$. Then*

$$q_1 q_2 < 25\, p^{1/2} (\log p)^2 .$$

With the above result in hand, it only remains to give a bound on r. To achieve this, we first prove an explicit version of a character sum estimate due to Burgess following a method of Iwaniec. Both the character sum estimate and the explicit bound on r are fairly involved to state, so we omit their statements here. It suffices to say that after this is complete, we can prove the following:

Theorem. *Let K be a Galois number field of odd prime degree ℓ and conductor f. If*

$$9000\,(\ell - 1)^3 (\log f)^{7/2} \leq f^{1/6} ,$$

then K is not norm-Euclidean.

Actually we derive several inequalities of the above form which involve a positive integer parameter. Using the inequalities to which we have alluded, we finally obtain the following theorem which gives the much sought-after solution to Problem 1.

Theorem. *Let K be a Galois number field of odd prime degree ℓ, conductor f, and discriminant Δ. There exists a computable constant C_ℓ such that if K is norm-Euclidean, then $f < C_\ell$ and $0 < \Delta < C_\ell^{\ell-1}$.*

Table 1.2: Conductor bounds when $\ell < 100$

ℓ	C_ℓ	ℓ	C_ℓ	ℓ	C_ℓ
3	10^{70}	29	10^{98}	61	10^{106}
5	10^{78}	31	10^{99}	67	10^{107}
7	10^{82}	37	10^{101}	71	10^{107}
11	10^{88}	41	10^{102}	73	10^{108}
13	10^{89}	43	10^{102}	79	10^{108}
17	10^{92}	47	10^{103}	83	10^{109}
19	10^{94}	53	10^{104}	89	10^{109}
23	10^{96}	59	10^{105}	97	10^{110}

Although the results of the previous theorem represent a significant step forward, their magnitude leaves something to be desired, especially if one is interested in classifying such fields. As is frequently the case in analytic estimates of number theoretic quantities, under the Generalized Riemann Hypothesis (GRH) one should be able to obtain much sharper results. The GRH asserts that all the non-trivial zeros of all Dirichlet L-functions lie on the critical line; in a certain sense, this hypothesis encodes our intuition on the distribution of primes and character residues, although it is currently unproven in every single instance.

Under the GRH, Bach gives a very good explicit bound on q_1 (see [2]); he shows that if χ is a non-principal Dirichlet character modulo m, then $q_1 < 2(\log m)^2$. Using Bach's method, we prove the following result, which gives a bound on q_2 in the situation we are interested in.

Theorem. *Assume the GRH. Let χ be a non-principal Dirichlet character modulo $m \geq 10^9$ with $\chi(-1) = 1$. Denote by $q_1 < q_2$ the two smallest primes such that $\chi(q_1), \chi(q_2) \neq 1$. Then*

$$q_2 < 2.5(\log m)^2 .$$

Moreover, by taking character combinations of Bach's explicit formulas and estimating a sum over the zeros of the Dedekind zeta function of K we obtain the following:

Theorem. *Assume the GRH. Suppose that χ is a non-principal Dirichlet character modulo $f \geq 10^8$ of order ℓ, where ℓ and f are both odd primes. Denote by $q_1 < q_2$ the two smallest rational primes such that $\chi(q_1), \chi(q_2) \neq 1$. Fix any ℓ-th root of unity ζ. There exists $r \in \mathbb{Z}^+$ such that $(r, q_1 q_2) = 1$, $\chi(r) = \zeta$, and*

$$r < 2.5(\ell - 1)^2 (\log f)^2 .$$

The last three results allow us to give a GRH version of our earlier result:

Theorem. *Assume the GRH. Let K be a Galois number field of odd prime degree ℓ and conductor f. If*

$$38(\ell - 1)^2 (\log f)^6 \log\log f < f ,$$

then K is not norm-Euclidean.

In the proof of the above result, we actually obtain something slightly stronger, and using this, we obtain the following GRH discriminant bounds:

Theorem. *Assume the GRH. Let K be a Galois number field of odd prime degree ℓ, conductor f, and discriminant Δ. There exists a computable constant C_ℓ such that if K is norm-Euclidean, then $f < C_\ell$ and $0 < \Delta < C_\ell^{\ell-1}$.*

Table 1.3: Conductor bounds when $\ell < 100$, assuming the GRH

ℓ	C_ℓ
3	10^{11}
5	10^{12}
7	10^{13}
11	10^{13}
13	10^{14}
17	10^{14}
19	10^{14}
23	10^{14}

ℓ	C_ℓ
29	10^{15}
31	10^{15}
37	10^{15}
41	10^{15}
43	10^{15}
47	10^{15}
53	10^{15}
59	10^{15}

ℓ	C_ℓ
61	10^{15}
67	10^{15}
71	10^{16}
73	10^{16}
79	10^{16}
83	10^{16}
89	10^{16}
97	10^{16}

Using a combination of theory and computation along the lines discussed, we obtain the following two theorems which represent the "state of the art" for norm-Euclidean Galois cubic fields.

Theorem. *Assuming the GRH, the norm-Euclidean Galois cubic fields are exactly those with*

$$\Delta = 7^2, 9^2, 13^2, 19^2, 61^2, 67^2, 103^2, 109^2, 127^2, 157^2\,.$$

This gives a solution, albeit conditional, to Problem 4. In any case, we are now willing to conjecture that Godwin and Smith's list is complete! The following is the best we can prove unconditionally:

Theorem. *The fields listed in the previous theorem are norm-Euclidean, and any remaining norm-Euclidean Galois cubic field must have discriminant $\Delta = f^2$ with $f \equiv 1 \pmod 3$ where f is a prime in the interval $(10^{10}, 10^{70})$.*

2 Preliminaries

In this chapter we will recall some known definitions and theorems. This will serve as a rapid introduction for the non-expert and it will allow us to establish some notations that we will use throughout this dissertation. We do not aim for our treatment in this chapter to be exhaustive by any means.

For excellent accounts of the rudiments of algebraic and analytic number theory, we refer the reader to [35] and [16]. For any results that are not contained in these two texts, we will attempt to give additional references as the need arises. In §2.6 and §2.7 we provide proofs, as these results are a little harder to find in the literature.

2.1 Algebraic Number Fields

An element $\alpha \in \mathbb{C}$ is said to be an algebraic number if it is the root of a polynomial with coefficients in $\mathbb{Z}$, and we say that α is an algebraic integer if this polynomial can be chosen to be monic. The set of all algebraic numbers, denoted by $\overline{\mathbb{Q}}$, forms a field, and the set of all algebraic integers forms a subring of this field.

A number field K is a finite extension of $\mathbb{Q}$, or more concretely $K = \mathbb{Q}(\theta)$ for some algebraic $\theta \in \mathbb{C}$. The ring of integers of K, denoted $\mathcal{O}_K$, is the subring of K consisting of algebraic integers. One of the first things that one discovers is that unique factorization does not necessarily hold in $\mathcal{O}_K$. As an example, consider the factorizations $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$ in the ring of integers of $\mathbb{Q}(\sqrt{-5})$. The crucial property which fails is that if π is an irreducible element of $\mathcal{O}_K$, then one does not necessarily have the result that $\pi \mid \alpha\beta$ implies $\pi \mid \alpha$ or $\pi \mid \beta$.

Eisenstein put his finger on this property in an 1844 letter which translates as [52]: "If one had the theorem which states that the product of two complex numbers can be divisible by a prime number only when one of the factors is – which seems completely obvious – then one would have the whole theory at a single blow; but this theorem is totally false." Indeed, if one had this property, then it would follow immediately that $\mathcal{O}_K$ is a unique factorization domain by considering two factorizations of the same number and performing cancellations.

A number field of degree n has n field embeddings $\sigma : K \to \mathbb{C}$, and we write $n = r_1 + 2r_2$, where r_1 is the number of real embeddings and r_2 is the number of conjugate pairs of complex embeddings. The absolute norm $N = N_{K/\mathbb{Q}} : K \to \mathbb{Q}$ is defined as $N(\alpha) := \prod_\sigma \sigma(\alpha)$, where the product runs over all field embeddings $\sigma : K \to \mathbb{C}$; the norm is multiplicative and preserves integrality. We call a number field K norm-Euclidean if for every $\alpha, \beta \in \mathcal{O}_K$, $\beta \neq 0$, there exists $\gamma \in \mathcal{O}_K$ such that $|N(\alpha - \gamma\beta)| < |N(\beta)|$. As explained in §1.1 this is equivalent to saying that $\mathcal{O}_K$ is Euclidean with respect to the function $\partial(\alpha) = |N(\alpha)|$.

If $\mathcal{O}_K$ is Euclidean with respect to the function $\partial : \mathcal{O}_K \setminus \{0\} \to \mathbb{Z}^+$, then one can develop the Euclidean algorithm in $\mathcal{O}_K$ by repeated division exactly analogous to the case of the rational integers $\mathbb{Z}$, except that now the function ∂ measures the "size" of an integer. This allows one to show that given two integers $\alpha, \beta \in \mathcal{O}_K$, the greatest common divisor (α, β) exists and is expressible as an $\mathcal{O}_K$-linear combination of α and β. Now it is easy to demonstrate that the property referred to by Eisenstein holds in this case. Indeed, suppose an irreducible element $\pi \in \mathcal{O}_K$ satisfies $\pi \,|\, \alpha\beta$ but $\pi \nmid \alpha$; then as $(\pi, \alpha) = 1$ we have $S\pi + T\alpha = 1$ for some $S, T \in \mathcal{O}_K$ which implies $S\pi\beta + T\alpha\beta = \beta$ and it is plain that $\pi \,|\, \beta$. It follows that if $\mathcal{O}_K$ is Euclidean, then $\mathcal{O}_K$ is a unique factorization domain.

As we have seen, unique factorization does not hold in the general case. Fortunately, one can partially restore unique factorization by introducing ideals, which are the descendants of Kummer's "ideal numbers". The ideal class group Cl_K (which we won't define here) is a finite abelian group which measures the failure of the unique factorization property. The class number of K, denoted h_K, is defined to be the size of Cl_K. When $h_K = 1$, we say that K has class number

one; this condition is equivalent to $\mathcal{O}_K$ being a unique factorization domain (and also equivalent to $\mathcal{O}_K$ being a principal ideal domain). Using this terminology, we have seen that if K is norm-Euclidean, then K has class number one.

Finally, we remark that an important invariant associated to a number field K is its discriminant, which we will denote by Δ; in some sense $|\Delta|$ measures the "size" of the number field. The rational primes dividing the discriminant of K are precisely those that ramify. We will assume the reader is familiar with the splitting of primes in extensions and ramification. One important situation for us is when $K/\mathbb{Q}$ is a Galois extension of prime degree ℓ; if we let p denote a rational prime, then in this case there are only three possibilities: p splits completely, p is inert, or p is totally ramified.

2.2 Dirichlet Characters

Let $m \in \mathbb{Z}^+$. A Dirichlet character modulo m is a function $\chi : \mathbb{Z} \to \mathbb{C}$ satisfying three properties:

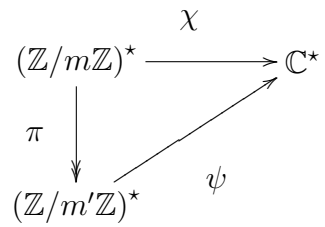
1. $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in \mathbb{Z}$
2. $\chi(n + km) = \chi(n)$ for all $k \in \mathbb{Z}$.
3. $\chi(n) = 0$ if and only if $(n, m) > 1$

There is an obvious correspondence between Dirichlet characters as defined above and homomorphisms of multiplicative groups $\chi : (\mathbb{Z}/m\mathbb{Z})^\star \to \mathbb{C}^\star$. The principal character modulo m is defined as:

$$\chi_0(n) = \begin{cases} 1 & \text{if } (n, m) = 1 \\ 0 & \text{if } (n, m) > 1 \end{cases}$$

The set of all Dirichlet characters modulo m forms a group under pointwise multiplication with the principal character serving as the identity element; this group is non-canonically isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\star$ and therefore has $\phi(m)$ elements. The order of a Dirichlet character is defined to be the smallest integer r such that $\chi^r = \chi_0$, or alternatively, the order of χ inside the character group. We say a

character ψ mod m' induces the character χ mod m if $m' \,|\, m$ and the following diagram commutes:



A character which is not induced by another character of smaller modulus is said to be primitive. The conductor of χ, denoted by $f = f_\chi$, is defined to be the modulus of the primitive character which induces χ.

We comment briefly on the connection between Dirichlet characters and power residues modulo primes. Fix an integer $k \geq 2$. We say that $n \in \mathbb{Z}$ is a k-th power residue modulo p if the equation $x^k \equiv n \pmod{p}$ is soluble in x. As the case of $n \equiv 0 \pmod{p}$ is trivial, we will assume $(n, p) = 1$. Suppose χ is any Dirichlet character modulo p of order $(k, p-1)$. One can easily show that $\chi(n) = 1$ if and only if n is a k-th power residue modulo p. Here we might as well assume $(k, p-1) > 1$, or else every integer is a k-th power residue modulo p and the only such χ is the principal character. If we denote by $C_p = (\mathbb{Z}/p\mathbb{Z})^\star$ the multiplicative group consisting of the integers modulo p and by C_p^k the subgroup of k-th powers modulo p, then the value of $\chi(n)$ determines to which coset of C_p/C_p^k the integer n belongs.

One of the most fundamental results in the analytic study of Dirichlet characters is the Pólya–Vinogradov inequality, which states that if χ is a non-principal Dirichlet character modulo m, then for any integers N, H,

$$\sum_{n=N+1}^{N+H} \chi(n) = O(m^{1/2} \log m)\,.$$

We will find useful the following explicit version (see [3]):

Theorem 2.1 (Bachman & Rachakonda, 2001)**.** *If χ is a non-principal Dirichlet character to the modulus m, then for any $N, H \in \mathbb{Z}$,*

$$\left| \sum_{n=N+1}^{N+H} \chi(n) \right| \leq \frac{1}{3 \log 3} \sqrt{m} \log m + 6.5 \sqrt{m}\,.$$

2.3 Residue Symbols in Number Fields

Let K be a number field and let μ_ℓ denote the ℓ-th roots of unity, where $\ell \in \mathbb{Z}^+$. If $\mu_\ell \subset K$, then for any prime $\mathfrak{p}$ of K with $(\mathfrak{p}, \ell) = 1$, we can define the ℓ-th power residue symbol $(\,\cdot\,/\mathfrak{p})_\ell$ as follows (see [34]): For $\alpha \in \mathcal{O}_K$ with $(\alpha, \mathfrak{p}) = 1$, let $(\alpha/\mathfrak{p})_\ell \in \mu_\ell$ be the unique root of unity satisfying

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

and for those $\alpha \in \mathcal{O}_K$ with $\mathfrak{p} \mid \alpha$ we set $(\alpha/\mathfrak{p})_\ell = 0$. Moreover, we define the symbol $(\alpha/\mathfrak{b})_\ell$ for any integral ideal $\mathfrak{b}$ of K with $(\mathfrak{b}, \ell) = 1$ by multiplying these symbols together; that is, we write $\mathfrak{b} = \mathfrak{p}_1^{a_1} \dots \mathfrak{p}_t^{a_t}$ and for any $\alpha \in \mathcal{O}_K$ we define

$$\left(\frac{\alpha}{\mathfrak{b}}\right)_\ell = \left(\frac{\alpha}{\mathfrak{p}_1}\right)_\ell^{a_1} \cdots \left(\frac{\alpha}{\mathfrak{p}_t}\right)_\ell^{a_t}.$$

This is an example of a more general character than those discussed up to this point; it is a character on the multiplicative group $(\mathcal{O}_K/\mathfrak{b})^\star$. However, we can obtain a Dirichlet character out of this symbol by setting $\chi(n) = (n/\mathfrak{b})_\ell$; indeed, this yields a Dirichlet character modulo $N(\mathfrak{b})$ with $\chi^\ell = \chi_0$. One important special case is when $K = \mathbb{Q}(\zeta_\ell)$, where ζ_ℓ denotes an ℓ-th root of unity. Henceforth, when we write the symbol $(\alpha/\mathfrak{b})_\ell$ we will implicitly mean that $\alpha \in \mathbb{Z}[\zeta_\ell]$ and $\mathfrak{b}$ is an integral ideal of $\mathbb{Q}(\zeta_\ell)$ with $(\mathfrak{b}, \ell) = 1$. If it happens that $\mathbb{Q}(\zeta_\ell)$ has class number one, then $\mathfrak{b} = (\beta)$ for some $\beta \in \mathbb{Z}[\zeta_\ell]$ with $(\beta, \ell) = 1$ and we may instead write $(\alpha/\beta)_\ell$. If $b \in \mathbb{Z}$ is odd and positive, then the symbol $(\,\cdot\,/b)_2$ is the usual Jacobi symbol.

2.4 Class Field Theory

We will review some well-known facts regarding class field theory over $\mathbb{Q}$ which will be useful in the sequel; one reference (among many possibilities) is [19]. The famous Kronecker–Weber Theorem states that every abelian extension $K/\mathbb{Q}$ is contained in a cyclotomic extension. In other words, if $\mathrm{Gal}(K/\mathbb{Q})$ is an abelian group, then $K \subseteq \mathbb{Q}(\zeta_m)$ for some $m \in \mathbb{Z}^+$. For any such m, it follows that

$\mathrm{Gal}(K/\mathbb{Q})$ is a quotient of $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\star$. The conductor of K is defined to be the smallest $f \in \mathbb{Z}^+$ such that $K \subseteq \mathbb{Q}(\zeta_f)$. The set of primes dividing the conductor is the same as the set of primes dividing the discriminant; i.e., $p \,|\, f$ if and only if $p \,|\, \Delta$.

Suppose $K/\mathbb{Q}$ is abelian and $K \subseteq \mathbb{Q}(\zeta_m)$. We associate a character group X_K to K in the following manner. Via Galois theory, we can identify K with a subgroup H of $(\mathbb{Z}/m\mathbb{Z})^\star$, and we define X_K to be the subgroup of Dirichlet characters modulo m that are trivial on H; that is,

$$X_K := \{\chi : (\mathbb{Z}/m\mathbb{Z})^\star \to \mathbb{C}^\star \mid \chi(n) = 1 \text{ for all } n \in H \}.$$

Different choices of m lead to isomorphic character groups X_K in a natural way. Moreover, one observes that $X_K \simeq \mathrm{Gal}(K/\mathbb{Q})$. The map $K \mapsto X_K$ gives a one-to-one correspondence between subfields of $\mathbb{Q}(\zeta_m)$ and subgroups of the character group of $(\mathbb{Z}/m\mathbb{Z})^\star$. Perhaps the most important property of this correspondence is that a rational prime p splits in K if and only if $\chi(p) = 1$ for all $\chi \in X_K$.

In the case of interest to us, $K/\mathbb{Q}$ will be a cyclic number field of degree ℓ. Suppose K has conductor f, and view X_K as a subgroup of the group of Dirichlet characters modulo f. In this case X_K is cyclic and any generator is a primitive character modulo f of order ℓ. Hence we have the following one-to-one correspondence:

$$\left\{ \begin{array}{c} \text{Cyclic extensions} \\ K/\mathbb{Q} \text{ of conductor } f \\ \text{and degree } \ell \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Primitive Dirichlet characters} \\ \chi : \mathbb{Z} \to \mathbb{C} \text{ of modulus } f \\ \text{and order } \ell \end{array} \right\} \Big/ \sim$$

The equivalence is given by the natural action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$; namely, $\chi \sim \psi$ if $\sigma \circ \chi = \psi$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. If we are considering fields of degree ℓ it suffices to only consider those $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$ as Dirichlet characters of order ℓ take values in $\mathbb{Q}(\zeta_\ell)$, and so this equivalence amounts to a choice of a primitive ℓ-th root of unity among the $\phi(\ell)$ possibilities. Moreover, this correspondence is such that a rational prime p splits in K if and only if $\chi(p) = 1$.

2.5 Zeta Functions and L-Functions

Using the notation of §2.1, let K denote a number field with discriminant Δ and write $[K : \mathbb{Q}] = r_1 + 2r_2$. The Dedekind zeta function of K is defined for $\Re(s) > 1$ as

$$\zeta_K(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s} ,$$

where it satisfies the so-called Euler product

$$\zeta_K(s) = \prod_{\mathfrak{P}} \left(1 - N\mathfrak{P}^{-s}\right)^{-1} .$$

The sum is taken over integral ideals and product is taken over prime ideals; the fact that the two are equal is the analytic expression of the fact that the ideals of K factor uniquely into prime ideals. For the special case of $K = \mathbb{Q}$, the above definition reduces to the familiar Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p} (1 - p^{-s})^{-1} .$$

The Dedekind zeta function has an analytic continuation to the entire complex plane except for a simple pole at $s = 1$, and satisfies a functional equation; if one defines

$$\xi_K(s) = \left(\frac{|\Delta|}{4^{r_2}\pi^{r_1+2r_2}}\right)^{s/2} \Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma\left(\frac{s+1}{2}\right)^{r_2} \zeta_K(s) ,$$

then the functional equation takes the form $\xi_K(s) = \xi_K(1 - s)$. Both the analytic continuation and functional equation for the Dedekind zeta function were first proved by Hecke. Two references for this and the rest of the results of this section are [39] and [38].

In light of its Euler product representation, $\zeta_K(s)$ has no zeros in the half-plane defined by $\Re(s) > 1$, and one also knows that there are no zeros on the line $\Re(s) = 1$. Using the functional equation, one sees that in the half-plane defined by $\Re(s) \leq 0$, zeros can only occur at rational integer values; these zeros are known as the trivial zeros, and may occur at the even locations, odd locations, or both, depending upon the values of r_1 and r_2. In any case, all non-trivial zeros must lie in the region $0 < \Re(s) < 1$, which is known as the critical strip. The

line $\Re(s) = 1/2$, which runs through this region and is the line of symmetry for the functional equation, is known as the critical line. The Generalized Riemann Hypothesis (GRH) for $\zeta_K(s)$ asserts that all the non-trivial zeros of $\zeta_K(s)$ lie on the critical line. In some sense, the GRH for $\zeta_K(s)$ encodes our intuition on how the primes of K should be distributed. In the case of $K = \mathbb{Q}$, where $\zeta_K(s) = \zeta(s)$, this is known as the Riemann Hypothesis (RH), which constitutes one of the greatest unsolved problems in mathematics.

Besides the Dedekind zeta function, the other analytic functions that will be of interest to us in this work are Dirichlet L-functions. (As our extensions will be abelian, we will not require more general L-functions.) Let χ denote a Dirichlet character modulo m. For $\Re(s) > 1$, the Dirichlet L-function attached to χ is given by

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

This function also has an analytic continuation to the complex plane, with one important difference — when χ is not the principal character, the function $L(s, \chi)$ is actually entire, but when χ is the principal character, $L(s, \chi)$ differs from $\zeta(s)$ only by the finite product $\prod_{p \mid m}(1 - p^{-s})$. If χ is primitive, then $L(s, \chi)$ satisfies a functional equation; we will not state the functional equation here, but we mention that it takes a slightly different form depending upon whether the character is even, meaning $\chi(-1) = 1$, or odd, meaning $\chi(-1) = -1$. The trivial zeros of $L(s, \chi)$ lie at either $s = 0, -2, -4, \ldots$, or $s = -1, -3, -5, \ldots$, depending on whether χ is even or odd. As before, the GRH for $L(s, \chi)$ asserts that all non-trivial zeros of $L(s, \chi)$ lie on the critical line.[1]

To conclude this section, we state some results regarding the factorization of the Dedekind zeta function. For the remainder of this section, assume $K/\mathbb{Q}$ is abelian. For a Dirichlet character χ, we will write χ' to denote the primitive character modulo f_χ that induces χ. This allows one to write down explicitly the factorization of the Dedekind zeta function of K in terms of Dirichlet L-functions

[1] Provided we restrict ourselves to abelian number fields, the definition of the GRH given in §1.4 implies the GRH for all the functions described in this section.

as

$$\zeta_K(s) = \prod_{\chi \in X_K} L(s, \chi')\,,$$

where X_K is the character group associated to K described in §2.4. A related result is the conductor–discriminant formula, which reads

$$\Delta = (-1)^u \prod_{\chi \in X_K} f_\chi\,,$$

where u is the number of odd characters in X_K.

Now we specialize further to the situation where K is Galois of odd prime degree ℓ. Such a field is necessarily cyclic and hence $X_K = \langle \chi \rangle$ for some primitive character modulo f of order ℓ, where f is the conductor of K; i.e. let χ denote one of the characters associated to K via the correspondence given in §2.4. Moreover, since X_K has prime order, we see that χ^k is primitive for $k = 1, \ldots, \ell - 1$; in particular, we have $f_{\chi^k} = f$ for $k = 1, \ldots, \ell - 1$. Hence in this case, we have

$$\zeta_K(s) = \zeta(s) \prod_{k=1}^{\ell-1} L(s, \chi^k)\,, \quad \Delta = f^{\ell-1}\,.$$

2.6 Number Fields with Class Number One

In trying to locate Euclidean fields we may restrict our attention to the case where K has class number one, so it is useful to see what extra conditions this places on our fields. The result contained in the next lemma is perhaps most elegantly demonstrated via genus theory (see [28]), and so we first recall some definitions. The genus field of an abelian number field K, denoted by K^{g}, is the largest absolutely abelian extension of K that is unramified at all finite primes, and the genus number of K is defined by $g_K := [K^{\mathrm{g}} : K]$. It is well known that g_K divides the narrow class number h_K^+. (Indeed, this follows immediately from class field theory by considering the narrow Hilbert class field of K.)

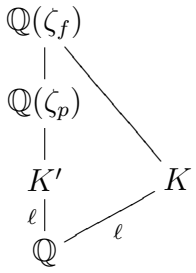
Lemma 2.2. *Suppose $K/\mathbb{Q}$ is cyclic with odd prime degree ℓ and discriminant Δ. If t distinct rational primes divide Δ, then ℓ^{t-1} divides h_K.*

Proof. By Theorem 5 of [28] we have $g_K = \ell^{t-1}$. We know g_K divides h_K^+; moreover, since ℓ is an odd prime and h_K^+ differs from h_K only by a power of 2, we conclude that g_K divides h_K as well. ∎

Lemma 2.3. *Suppose $K/\mathbb{Q}$ is cyclic with odd prime degree ℓ, conductor f, and discriminant Δ. Further, suppose that K has class number one. In this case, one has $\Delta = f^{\ell-1}$. Moreover:*

- *If $(f, \ell) = 1$, then f is a prime with $f \equiv 1 \pmod{\ell}$.*
- *If $(f, \ell) > 1$, then $f = \ell^2$.*

Proof. Since K has class number one, Lemma 2.2 allows us to conclude that $|\Delta|$ is a prime power. Also, note that K is totally real (as it is Galois of odd degree) and hence $\Delta > 0$. Since K is cyclic of prime degree, the conductor–discriminant formula allows us to conclude that $\Delta = f^{\ell-1}$. It remains to determine f. Since f is the conductor of K, we have the following inclusion of fields: $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_f)$. Since Δ is only divisible by one prime, f must also be divisible by a single prime; say, $f = p^k$ for some prime p and $k \in \mathbb{Z}^+$. Thus $[\mathbb{Q}(\zeta_f) : \mathbb{Q}] = \phi(f) = (p-1)p^{k-1}$. From the inclusion of fields, we see $[K : \mathbb{Q}]$ divides $[\mathbb{Q}(\zeta_f) : \mathbb{Q}]$; that is, ℓ divides $(p-1)p^{k-1}$. At this point, we break the proof into cases. First, suppose that $(f, \ell) = 1$, so that $\ell \neq p$. In this case, we must have ℓ divides $p - 1$; that is, $p \equiv 1 \pmod{\ell}$. This implies, via Galois theory, that there exists a cyclic field K' as depicted below:



As there cannot be two cyclic fields of degree ℓ contained in $\mathbb{Q}(\zeta_f)$, we must have that $K = K'$ and hence the conductor of K satisfies $f = p$. This proves the result in the case where $(f, \ell) = 1$.

Turning to the case of $(f, \ell) > 1$, we have $p = \ell$. We argue as before, but this time we have ℓ divides $(\ell - 1)\ell^{k-1}$; this implies $k \geq 2$. But we observe, as

before, that $\mathbb{Q}(\zeta_{\ell^2})$ already contains a cyclic field of order ℓ, and hence $f = \ell^2$, which completes the proof. ∎

2.7 Heilbronn's Criterion

In order to state Heilbronn's criterion, we distinguish two subsets of the rational integers: the norms,

$$\mathcal{N} := N_{K/\mathbb{Q}}(\mathcal{O}_K) = \{n \in \mathbb{Z} \mid N_{K/\mathbb{Q}}(\alpha) = n \text{ for some } \alpha \in \mathcal{O}_K\},$$

and the ℓ-th power residues modulo f,

$$\mathcal{P} := \{n \in \mathbb{Z} \mid x^\ell \equiv n \pmod{f} \text{ is soluble}\}.$$

Although not stated in this way, Heilbronn proves the following [26]:

Lemma 2.4 (Heilbronn's Criterion)**.** *Let K be a Galois number field of odd prime degree ℓ and conductor f, with $(f, \ell) = 1$. If one can write $f = a + b$ with $a, b > 0$, where $a, b \notin \mathcal{N}$ and $a \in \mathcal{P}$, then K is not norm-Euclidean.*

This simple yet ingenious observation, which has its roots in a paper of Erdös and Ko on quadratic fields [17], turns the problem into one of additive number theory. For the sake of completeness, we provide the argument.

Proof. Let K be as in the hypothesis, and moreover, assume that K is norm-Euclidean. Suppose $f = a + b$ with $a, b > 0$ where $a, b \notin \mathcal{N}$ and $a \in \mathcal{P}$. We seek a contradiction.

Since K is norm-Euclidean, it has class number one. It follows from Lemma 2.3 that f is a prime, and since K has prime degree we know that f is totally ramified in K. We factor $f = u\pi^\ell$ in K where π is a first degree prime and u is a unit. Fix an arbitrary $n \in \mathbb{Z}^+$. There exists $\alpha \in \mathcal{O}_K$ such that $n \equiv \alpha \pmod{\pi}$ with $|N(\alpha)| < |N(\pi)| = f$. Conjugation gives $n \equiv \alpha^\sigma \pmod{\pi}$ for all embeddings $\sigma : K \to \mathbb{C}$, and hence $n^\ell \equiv N(\alpha) \pmod{f}$. Now we choose n so that $a \equiv n^\ell \pmod{f}$ and we have $a \equiv N(\alpha) \pmod{f}$. Since $|N(\alpha)| < f$, we have either $N(\alpha) = a$ or $N(\alpha) = a - f = -b$. Thus a or $-b$ lies in $\mathcal{N}$, a contradiction! ∎

3 Norm-Euclidean Galois Fields

3.1 Conditions for the Failure of the Euclidean Property

The aim of this section is to prove the following theorem, which gives various conditions under which K fails be norm-Euclidean.

Theorem 3.1. *Let K be a Galois number field of odd prime degree ℓ and conductor f with $(f, \ell) = 1$, and let χ be a primitive Dirichlet character modulo f of order ℓ. Denote by $q_1 < q_2$ the two smallest rational primes that are inert in K. Suppose that there exists $r \in \mathbb{Z}^+$ with*

$$(r, q_1 q_2) = 1, \quad \chi(r) = \chi(q_2)^{-1},$$

such that any of the following conditions hold:

1. $rq_2k \not\equiv f \pmod{q_1^2}, \quad k = 1, \ldots, q_1 - 1,$
   $(q_1 - 1)(q_2 r - 1) \leq f$
2. $q_1 \neq 2, 3, \quad 3q_1 q_2 r \log q_1 < f$
3. $q_1 \neq 2, 3, 7, \quad 2.1\, q_1 q_2 r \log q_1 < f$
4. $q_1 = 2,\ q_2 \neq 3, \quad 3q_2 r < f$
5. $q_1 = 3,\ q_2 \neq 5, \quad 5q_2 r < f$

Then K is not norm-Euclidean.

Some remarks are in order. The first condition places no restrictions on q_1 or q_2 but requires congruence conditions which hold "most of the time", but they can be rather awkward to verify. The remaining conditions resulted from an effort to remove these congruences. As an example of condition 1, we give two special cases that will be employed later: If $q_1 = 2$, $q_2 = 3$, then condition 1 becomes $r \not\equiv 3f \pmod 4$, $3r - 1 \leq f$. If $q_1 = 3$, $q_2 = 5$, then condition 1 becomes $r \not\equiv f, 2f \pmod 9$, $10r - 2 \leq f$.

As in the statement of the above theorem, we will assume throughout this section that K is a Galois number field of odd prime degree ℓ and conductor f, with $(f, \ell) = 1$, and we will denote by $q_1 < q_2$ the two smallest rational primes that are inert in K. It suffices to assume that K has class number one (otherwise it is immediate that K is not norm-Euclidean), and we will do so. Now Lemma 2.3 tells us that the discriminant of K satisfies $\Delta = f^{\ell-1}$, where f is a prime satisfying $f \equiv 1 \pmod \ell$. In light of Lemma 2.4, the following subset of $\mathbb{Z}^+$ will play a crucial role:

Definition 3.2. *Let $\mathcal{S}$ denote the subset of positive integers less than f which consists of ℓ-th power residues that are not norms. In the notation of §2.7,*
$\mathcal{S} := \mathcal{P} \cap \mathcal{N}^C \cap (0, f)$.

The following simple lemma characterizes $\mathcal{S}$ in terms of χ, and it will be used without comment in the arguments that follow.

Lemma 3.3.

$$\mathcal{S} = \{n \in \mathbb{Z} \cap (0, f) \mid n = bc,\ (b, c) = 1,\ \chi(b), \chi(c) \neq 1,\ \chi(bc) = 1\}$$

Proof. Suppose $n \in \mathbb{Z}$ with $0 < n < f$. One knows that $n \in \mathcal{P}$ if and only if $\chi(n) = 1$, and that $n \notin \mathcal{N}$ if and only if one can write $n = bc$ with $(b, c) = 1$ and $\chi(b) \neq 1$. The result follows. ∎

Lemma 3.4. *If there exists $s \in \mathcal{S}$ such that $(q_1, s) = 1$ and $(q_1 - 1)(s - 1) \leq f$, then we can write $f = us + vq_1$ with $0 < u < q_1$ and $v > 0$. If $(q_1, v) = 1$ in this expression, then K is not norm-Euclidean.*

Proof. By a well-known theorem in elementary number theory, the facts $(q_1, s) = 1$ and $(q_1 - 1)(s - 1) \leq f$ imply that there exists $u, v \in \mathbb{Z}_{\geq 0}$ such that $f = us + vq_1$. However, since f is a prime not equal to q_1 and s is composite, we must have $u, v > 0$, lest we arrive at a contradiction. Without loss of generality, we can assume $u < q_1$. Indeed, we just subtract multiples of q_1 from u and add them to v as necessary, and the resulting u and v will remain positive for the same reason as before. Since $u < q_1$, we have $\chi(p) = 1$ for every prime p dividing u, and it follows that $us \in \mathcal{S}$. If it were the case that $(q_1, v) = 1$, then we would have $vq_1 \notin \mathcal{N}$ since $q_1 \notin \mathcal{N}$; in this case Lemma 2.4 implies that K is not norm-Euclidean. ∎

Proposition 3.5. *If there exists $s \in \mathcal{S}$ such that $(s, q_1) = 1$,*

$$sk \not\equiv f \pmod{q_1^2}, \quad k = 1, \ldots, q_1 - 1,$$

$$(q_1 - 1)(s - 1) \leq f,$$

then K is not norm-Euclidean.

Proof. By Lemma 3.4 we can write $f = us + vq_1$ with $0 < u < q_1$, $v > 0$ and we may assume $q_1 \mid v$. This implies $f \equiv us \pmod{q_1^2}$, a contradiction. ∎

For $q_1 \neq 2, 3$, we can eliminate the congruence condition of Proposition 3.5, but we must pay a small price.

Proposition 3.6. *Fix $q_1 \neq 2, 3$. Suppose there exists a constant $1 \leq B \leq 3$ such that for all $u \in (0, q_1)$ there exists a prime $p_0 < B \log q_1$ with $(p_0, u) = 1$. If there exists $s \in \mathcal{S}$ such that $(s, q_1) = 1$ and*

$$Bq_1 s \log q_1 \leq f,$$

then K is not norm-Euclidean.

Proof. By Lemma 3.4 we can write $f = us + vq_1$ with $0 < u < q_1$, $v > 0$ and we may assume $q_1 \mid v$. By our hypothesis, there exists a prime such that $(p_0, u) = 1$ and $p_0 < B \log q_1$ for some $B \in [1, 3]$. In particular, we have $p_0 < q_1$ since $3 \log q_1 < q_1$ for $q_1 \geq 5$. Let n denote the smallest positive solution to the congruence

$$u + nq_1 \equiv 0 \pmod{p_0},$$

so that $0 < n < p_0$. We claim that the expression

$$f = (u + nq_1)s + (v - ns)q_1 \tag{3.1}$$

is of the desired form (to which Lemma 2.4 applies). First we note that

$$u + nq_1 < q_1 + (p_0 - 1)q_1 = p_0 q_1 \, .$$

To see that both terms in (3.1) are positive we observe

$$(u + nq_1)s < p_0 q_1 s < B q_1 s \log q_1 \leq f \, .$$

Notice that every prime p dividing $u+nq_1$ is less than q_1, which says $(u+nq_1)s \in \mathcal{S}$, as before. If it were the case that $q_1 | v-ns$, then we would have $q_1 | s$, a contradiction; hence $(q_1, v - ns) = 1$. Now Lemma 2.4 gives the result. ∎

Motivated by the previous proposition, we introduce the following lemma which gives the existence of the constant B.

Lemma 3.7. *Suppose q is prime and $0 < u < q$. If $q \neq 2, 3$, then there exists a prime $p_0 < 3 \log q$ such that $(p_0, u) = 1$. If $q \neq 2, 3, 7$, then there exists a prime $p_0 < 2.1 \log q$ such that $(p_0, u) = 1$.*

Proof. To show there exists a prime $p_0 \leq x$ with $(p_0, u) = 1$ it suffices to show

$$\sum_{p \leq x} \log p > \log u \, ,$$

as this implies the desired result. For any $x \geq 5$ we have the inequality

$$\sum_{p \leq x} \log p > \frac{x}{2.1} \, , \tag{3.2}$$

which is easily deduced from Corollary 3.16 of [44] with a small amount of computation.[1] Using this fact together with the hypothesis that $u < q$, one sees that it suffices to show

$$\log q \leq \frac{x}{2.1} \, . \tag{3.3}$$

[1] In fact, one can demonstrate this inequality using the elementary methods given in [23] together with an explicit version of Stirling's formula if one is willing to do a little more computation.

This condition clearly holds when we set $x = 2.1 \log q$. When $q \geq 11$, we have $x \geq 2.1 \log 11 > 5$, and the proof is complete. The cases of $q = 5, 7$ are done by direct inspection. ∎

Proposition 3.8. *Suppose $q_1 = 2$, $q_2 \neq 3$. If there exists $s \in \mathcal{S}$ such that $(q_1, s) = 1$ and $3s < f$, then K is not norm-Euclidean.*

Proof. By Lemma 3.4 we may assume $f = s + 2v$ with $2 \,|\, v$. In this case, we write $f = 3s + 2(v - s)$. If it were the case that $2 \,|\, (v - s)$, then we would have $2 \,|\, s$, a contradiction. Also observe that $\chi(3) = 1$ and hence $3s \in \mathcal{S}$. Finally, notice that $3s < f$, which implies $v - s > 0$. ∎

Proposition 3.9. *Suppose $q_1 = 3$, $q_2 \neq 5$. If there exists $s \in \mathcal{S}$ such that $(q_1, s) = 1$ and $5s < f$, then K is not norm-Euclidean.*

Proof. By Lemma 3.4 we may assume $f = us + 3v$ with $0 < u < 3$, $v > 0$, and $3 \,|\, v$. We treat separately the cases of $u = 1$ and $u = 2$. If $u = 1$, we have $f = s + 3v$, which we rewrite as $f = 4s + 3(v - s)$. Proceeding as before we find this expression is of the desired form (since $\chi(2) = 1$), provided $4s \leq f$. If $u = 2$, we have $f = 2s + 3v$, which we rewrite as $f = 5s + 3(v - s)$, which is of the desired form (since $\chi(5) = 1$), provided $5s < f$. ∎

Now we are ready:

Proof of the theorem. If condition (1) holds, we apply Proposition 3.5 with $s = q_2 r$. If either of conditions (2) or (3) hold, then we apply Proposition 3.6 with $s = q_2 r$ and invoke Lemma 3.7. If conditions (4) or (5) hold, we apply propositions 3.8 or 3.9 respectively. ∎

3.2 An Algorithm and Some Computations

In this section we give an algorithm which provides a solution to Problem 2 of §1.3. In §3.2.1 we give the main idea behind the algorithm, in §3.2.2 we discuss character evaluations, and in §3.2.3 we give a full statement of the algorithm. Finally, in §3.2.4 we give some results obtained from our computations, including the solution to Problem 3.

3.2.1 Idea behind the algorithm

Let us first state our aims in designing such as algorithm. The input should be an odd prime ℓ and positive integers A, B. If we let $\mathcal{F}_\ell(A, B)$ denote the collection of all Galois number fields K of degree ℓ with conductor $f \in [A, B]$, then the output should be a list $\mathcal{L} \subset [A, B]$ which contains the conductors of all norm-Euclidean $K \in \mathcal{F}_\ell(A, B)$. We do not require our list to consist of only norm-Euclidean fields, but the list should be manageable in the sense that we could eventually hope to treat the remaining fields on a case by case basis. Our goal is to sift through a very large amount of fields as quickly as possible. We will use the first condition from Theorem 3.1 exclusively. For the reader's convenience, we give this part of the theorem again:

Theorem. *Let K be a Galois number field of odd prime degree ℓ and conductor f with $(f, \ell) = 1$, and let χ be a primitive Dirichlet character modulo f of order ℓ. Denote by $q_1 < q_2$ the two smallest rational primes with $\chi(q_1), \chi(q_2) \neq 1$. Suppose that there exists $r \in \mathbb{Z}^+$ with*

$$\begin{aligned} &(r, q_1 q_2) = 1, \quad \chi(r) = \chi(q_2)^{-1}, \\ &r q_2 k \not\equiv f \pmod{q_1^2}, \quad k = 1, \ldots, q_1 - 1\,, \\ &(q_1 - 1)(q_2 r - 1) \leq f\,. \end{aligned}$$

Then K is not norm-Euclidean.

Although this is the most awkward condition (among those given in Theorem 3.1) to apply in order to obtain theoretical bounds, it is useful in computation as the congruence condition is satisfied most of the time. Indeed, if we assume the congruence class of r inside $(\mathbb{Z}/q_1^2\mathbb{Z})^\star$ is chosen randomly, the chances the condition is satisfied are $(q_1 - 1)/q_1$. Therefore, when q_1 is large, it is very likely that any value we take for r will automatically satisfy our congruences; on the other hand, when q_1 is small, the congruences may fail on occasion, but in this case we have lots of room to look for r. In addition, the conditions above only require computation within $\mathbb{Z}$ and character evaluations, and hence one can avoid the additional considerations of precision that come along computing logarithms.

In searching for the integer r required to apply the above theorem, performing character evaluations is unavoidable. The basic idea is to arrange things so that character evaluations are almost the only computations needed, and that we carry out as few of them as possible. To this end, our algorithm will only perform character evaluations on primes. This has the advantage that we won't have to sieve out a list of integers coprime to $q_1 q_2$ for each f; instead, for each f we evaluate a fixed character χ against a precomputed list of primes.

Based on the above discussion, the basic strategy is as follows: compute $\chi(p)$ for primes $p < f$ until we find the smallest prime non-residues q_1, q_2 and a prime r with $\chi(r) = \chi(q_2)^{-1}$ satisfying our congruences. If we are able to do this before we run out of primes, then we simply check whether $(q_1 - 1)(q_2 r - 1) \leq f$. Assuming any of the ℓ-th roots of unity are equally likely to occur, and that our congruences are satisfied at least half the time[2], then an upper bound on the average number of character evaluations to find q_1, q_2, r as just described is:

$$\ell \left(2 + \frac{2}{\ell - 1} \right)$$

This gives a rough heuristic for how many character evaluations are necessary. For example, when $\ell = 3$, it should take roughly 9 character evaluations on average to prove that any given cubic field is not norm-Euclidean.[3] However, it is important to keep in mind that on occasion it may take many more character evaluations than the average. We could assume the GRH and attempt to perform a rigorous analysis of the mean and variance of this statistic, but feel that this would be too tangential to our current aims.

3.2.2 Character evaluations

Before stating the algorithm formally, we detour for a brief discussion as to how we will carry out our character evaluations, as this will be the most crucial portion of the computations. Fix $\chi = \chi_f$, a primitive Dirichlet character modulo f of order ℓ where f and ℓ are both odd primes and $f \equiv 1 \pmod{\ell}$.

[2]This assumption is reasonable as the chances should be $(q_1 - 1)/q_1$ if we assume the congruence class inside $(\mathbb{Z}/q_1^2\mathbb{Z})^\star$ is chosen randomly.

[3]A quick test using the range $100 \leq f \leq 300$ yields an average of ≈ 8.7.

If we are performing multiple evaluations of a single character, and the modulus f is small, then perhaps one of the best strategies is to first build a lookup table. Once this is completed, we can perform character evaluations in small constant time. One straightforward way to do this is to first find a primitive root for f. We won't go into algorithms for this here.

When f is too large, building a lookup table is not a good option as it becomes infeasible to store such a table in memory, and seems excessive given that it is very likely that we will only need to evaluate the character a small number of times.

We describe an alternative approach based on the following observation: If $\mathfrak{p}$ is a prime in $\mathbb{Q}(\zeta_\ell)$ with $\mathfrak{p} \mid f$, then $\chi(n) = (n/\mathfrak{p})_\ell$ is a Dirichlet character modulo f of order ℓ, where $(\,\cdot\,/\mathfrak{p})_\ell$ is the ℓ-th power residue symbol described in §2.3. In fact the $\ell - 1$ choices of $\mathfrak{p}$ lying over f account for $\ell - 1$ Dirichlet characters modulo f of order ℓ; hence we may assume

$$\chi_f(n) = \left(\frac{n}{\mathfrak{p}}\right)_\ell .$$

Moreover, if we assume $\ell \leq 19$, then $\mathbb{Q}(\zeta_\ell)$ has class number one (see [36]) and hence we may write

$$\chi_f(n) = \left(\frac{n}{\pi}\right)_\ell ,$$

for some prime $\pi \in \mathbb{Z}[\zeta_\ell]$ with $\pi \mid f$.[4] In this case, we can use Eisenstein's reciprocity law for power residues to compute the above symbol very rapidly, using computations in $\mathbb{Z}[\zeta_\ell]$, in a manner completely analogous to the usual method of computing Legendre symbols via the Jacobi symbol. In this work, we employ this procedure in the cubic setting only; see [13] for details on how the computation of the cubic residue symbol can be carried out, including the statement of the cubic reciprocity law.

[4]The prime π can be computed as $\gcd(\zeta_\ell - w, f)$, where w is a solution to $\Phi_\ell(x) \equiv 0 \pmod{f}$; here $\Phi_\ell(x) = x^{\ell-1} + \cdots + x + 1$ denotes the ℓ-th cyclotomic polynomial.

3.2.3 Statement of the algorithm

The input to our algorithm consists of positive integers A, B and an odd prime ℓ. The output is a list $\mathcal{L} \subset [A, B]$ containing the conductors of all $K \in \mathcal{F}_\ell(A, B)$. In the statement of Algorithm 1 below, a lowercase or uppercase latin letter will denote an element of $\mathbb{Z}$, an uppercase script letter will denote a list of elements in $\mathbb{Z}$, and ζ will denote an ℓ-th root of unity (which can be stored as an integer in the interval $[0, \ell)$). We will denote by χ_f a primitive Dirichlet character modulo f of order ℓ; it does not matter which one we take as long use just one character for each f.

As far as verifying the correctness of Algorithm 1, there is really nothing to prove. For a given f, our algorithm either finds q_1, q_2, and r satisfying the conditions in the theorem or it doesn't; if it doesn't, then that value of f is outputted. However, we do give a number of comments regarding the algorithm which we feel are relevant:

1. In line 1, the reason for the number 1000 is that if B is especially small, we don't want to run out of primes. Of course, the number 1000 is arbitrary – any relatively manageable number will do.

2. If we do run out of primes, the value of r will remain at zero when the loop over $\mathcal{P}$ finishes. This will cause the relevant value of f to be output, and so we need not worry about missing an f due to lack of primes or due to the non-existence of the value r.

3. In calculating the list $\mathcal{F}$ in line 2, one should sieve using the primes in $\mathcal{P}$ – this is why we stored primes up to $\sqrt{B}$.

4. Notice that the command "Initiate scheme to evaluate χ_f" on line 4 is only run once for each f. Whether we are building a lookup table or finding a prime π over f (see §3.2.2), this step is carried out just once and results in fast character evaluations during the inner loop over $\mathcal{P}$.

5. Although $\chi_f(p)$ appears on lines 10, 15, and 17, we of course only compute $\chi_f(p)$ once.

Algorithm 1 Output a list of all possible conductors $f \in [A, B]$

Generate a list $\mathcal{P}$ of all primes $p \leq \max\{1000, \sqrt{B}\}$ using the Sieve of Eratosthenes.
Generate a list $\mathcal{F}$ all primes $f \in [A, B]$ such that $f \equiv 1 \pmod{\ell}$.
for $f \in \mathcal{F}$ **do**
  Initiate scheme to evaluate χ_f (see §3.2.2).
  $q_1 \leftarrow 0$; $q_2 \leftarrow 0$; $r \leftarrow 0$
  for $p \in \mathcal{P}$ **do**
    if $p \geq f$ **then**
      break
    end if
    if $(\chi_f(p) \neq 1)$ **then**
      if $q_1 = 0$ **then**
        $q_1 \leftarrow p$
      else if $q_2 = 0$ **then**
        $q_2 \leftarrow p$
        $\zeta \leftarrow \chi_f(p)^{-1}$
        $\mathcal{A} \leftarrow \{fq_2^{-1}k^{-1} \mod q_1^2 \mid k = 1, \ldots, q_1 - 1\}$
      else if $\chi_f(p) = \zeta$ AND $p \bmod q_1^2 \notin \mathcal{A}$ **then**
        $r \leftarrow p$
        break
      end if
    end if
  end for
  if $r = 0$ OR $(q_1 - 1)(q_2 r - 1) > f$ **then**
    print f
  end if
end for
if $\ell^2 \in [A, B]$ **then**
  print ℓ^2
end if

6. The code on lines 15 and 16 to store values in ζ and $\mathcal{A}$ only gets executed at most once for each f.

7. The modular arithmetic that takes place on lines 16 and 17 is modulo q_1^2, and typically q_1 is very small.[5]

3.2.4 Results of the computations

We have implemented the algorithm in the mathematics software SAGE (http://www.sagemath.org), using a lookup table for character evaluations. The following result took only 18.3 minutes of CPU time to complete on a MacBook Pro with a 2.26 GHz Intel Core 2 Duo processor and 4 GB of RAM, running Mac OS 10.6.

Theorem 3.10. *The following table contains all possible norm-Euclidean Galois number fields of prime degree ℓ and conductor f with $3 \leq \ell \leq 30$ and $f \leq 10^4$. (Of course, some of these fields may not be norm-Euclidean.)*

Table 3.1: Candidate norm-Euclidean fields of small degree

ℓ	$f \leq 10^4$
3	7, 9, 13, 19, 31, 37, 43, 61, 67, 73, 103, 109, 127, 157, 277, 439, 643, 997, 1597
5	11, 25, 31, 41, 61, 71, 151, 311, 431
7	29, 43, 49, 127, 239, 673, 701, 911
11	23, 67, 89, 121, 331, 353, 419, 617
13	53, 79, 131, 157, 169, 313, 443, 521, 937
17	137, 289, 443, 1259, 2687
19	191, 229, 361, 1103
23	47, 139, 277, 461, 529, 599, 691, 967, 1013, 1289
29	59, 233, 523, 841, 929, 2843, 3191

Notice that for the case of $\ell = 3$ we cover all possible $\Delta \leq 10^8$ (as $\Delta = f^2$ in this case) and that our results are consistent with Godwin and Smith's (see Theorem 1.6). As these computations didn't take long to complete, there is the possibility of extending the above table in the near future without too much

[5]Using rough heuristics as in §3.2.2, we find that in the cubic case $q_1 \in \{2, 3, 5, 7\}$ roughly 98.8% of the time, and as ℓ gets larger, this probability increases substantially.

additional effort. It would also be interesting to study the fields in this table using other methods, possibly on a case-by-case basis if necessary, to decide which ones are actually norm-Euclidean.[6] In the case of $\ell = 3$, we know that exactly 10 of the fields listed are norm-Euclidean, but not too much seems to be known about the remaining fields in the table.

For the cubic case, we have implemented an efficient version of our algorithm in C, performing character evaluations using the equality $\chi_f(n) = (n/\pi)_3$, as described in §3.2.2. We use NTL with GMP for large integer arithmetic, and we use the algorithms given in [13] to compute the cubic residue symbol and the greatest common divisor in $\mathbb{Z}[\zeta_3]$. Running this code on all conductors $f \leq 10^{10}$ produced the same list of conductors as the $\ell = 3$ entry in the table of Theorem 3.10 above. This took 91.3 hours of CPU time on an iMac with a 3.06 GHz Intel Core 2 Duo processor and 4 GB of RAM, running Mac OS 10.6.

Combining this computation with Godwin and Smith's result, we obtain:

Theorem 3.11. *The norm-Euclidean Galois cubic fields with discriminant* $|\Delta| < 10^{20}$ *are exactly those with*

$$\Delta = 7^2, 9^2, 13^2, 19^2, 61^2, 67^2, 103^2, 109^2, 127^2, 157^2 .$$

Not only does Theorem 3.11 extend the computations given in Theorem 3.10, but it provides a consistency check for the implementation of our character evaluations in both cases as the two implementations are in two different languages using two completely different strategies for character evaluation. We give the values of q_1, q_2, r for the last 10 fields in our computation:

```
f=9999999673, q1=5, q2=7, r=17
f=9999999679, q1=2, q2=3, r=19
f=9999999703, q1=2, q2=3, r=11
f=9999999727, q1=7, q2=11, r=19
f=9999999769, q1=3, q2=5, r=37
f=9999999781, q1=2, q2=5, r=7
f=9999999787, q1=3, q2=5, r=29
f=9999999817, q1=2, q2=3, r=13
f=9999999943, q1=5, q2=7, r=19
f=9999999967, q1=5, q2=7, r=11
```

[6] Of course, to begin with, one could see which have class number one.

3.3 Discriminant Bounds in Some Special Cases

The goal of this section is to obtain explicit inequalities which will give us discriminant bounds in two very special cases. The purpose of this is two-fold: This will serve as an illustration of the type of inequalities we seek, and this will allow us to rid ourselves of these two cases which are particularly troublesome. Here is the result:

Theorem 3.12. *Let K be a Galois number field of odd prime degree ℓ and conductor f. Denote by $q_1 < q_2$ the two smallest rational primes that are inert in K. Suppose either of the following conditions hold:*

1. $q_1 = 2$, $q_2 = 3$,
   $72(\ell - 1)f^{1/2} \log 4f + 35 \leq f$
2. $q_1 = 3$, $q_2 = 5$,
   $507(\ell - 1)f^{1/2} \log 9f + 448 \leq f$

Then K is not norm-Euclidean.

Notice that the above inequalities are completely explicit, they involve only ℓ and f, and for fixed ℓ they clearly hold beyond some easily computed value of f. Ultimately, we will derive an analogous result which holds regardless of the values of q_1 and q_2 (see Theorem 5.1). The following corollary, whose proof is immediate, is an example of the type of discriminant bounds we can obtain from Theorem 3.12.

Corollary 3.13. *Suppose K is a norm-Euclidean Galois cubic field of conductor f and discriminant Δ. If the primes 2 and 3 are inert in K, then $f < 10^7$ and $0 < \Delta < 10^{14}$.*

First we prove a lemma about Dirichlet characters.

Lemma 3.14. *Suppose χ is a Dirichlet character of order ℓ to the modulus m. Fix an ℓ-th root of unity ζ. Let $(\star)$ be any property of integers. Suppose there are no integers $n \le x$ having property $(\star)$ such that $\chi(n) = \zeta$. Then*

$$\#\{n < x \mid n \text{ has property } (\star),\ (n,m) = 1\} \ = \ -\sum_{k=1}^{\ell-1} \zeta^{-k} \sum_{n \le x}^{\star} \chi^k(n)\,,$$

where $\sum^{\star}$ means that the sum is taken only over those positive integers having property $(\star)$.

Proof. Summing the identity

$$\sum_{k=1}^{\ell} \zeta^{-k} \chi^k(n) = \begin{cases} \ell & \chi(n) = \zeta \\ 0 & \text{otherwise} \end{cases}.$$

over all $n \le x$ satisfying $(\star)$ and isolating the trivial character from the resulting expression gives the desired conclusion. ∎

Lemma 3.15. *Let χ be a non-principal Dirichlet character modulo $m \ge 2 \cdot 10^4$, and let p be a prime. For $x > 0$, we have*

$$\left| \sum_{\substack{n<x \\ (n,p)=1}} \chi(n) \right| \le 2\sqrt{m} \log m\,.$$

Proof. When $m \ge 2 \cdot 10^4$, we have

$$\frac{1}{3 \log 3} + \frac{6.5}{\log m} < 1\,.$$

Thus by Theorem 2.1, for any $y > 0$ we have

$$\left| \sum_{n<y} \chi(n) \right| \le m^{1/2} \log m\,. \tag{3.4}$$

Notice that

$$\sum_{\substack{n<x \\ (n,p)=1}} \chi(n) = \sum_{n<x} \chi(n) - \chi(p) \sum_{n<x/p} \chi(n)\,. \tag{3.5}$$

Applying the triangle inequality to (3.5) and invoking (3.4) twice gives the result. ∎

Lemma 3.16. *Suppose χ is a Dirichlet character modulo m. Suppose $q \geq 3$ is a positive integer, and let A be a subset of $(\mathbb{Z}/q\mathbb{Z})^*$. Let $(\star)$ be any property of integers. We have*

$$\left| \sum_{a \in A} \sideset{}{^\star}\sum_{\substack{n \leq x \\ n \equiv a \ (q)}} \chi(n) \right| \leq \frac{\phi(q)}{2} \max_{\substack{\psi \\ mod\ q}} \left| \sideset{}{^\star}\sum_{n \leq x} (\psi\chi)(n) \right| ,$$

where $\sum^\star$ means that the sum is only taken over those positive integers n having property $(\star)$.

Proof. For notational convenience we denote $N := \#A$. We begin by summing the identity

$$\frac{1}{\phi(q)} \sum_{\substack{\psi \\ \text{mod } q}} \overline{\psi}(a)\psi(n)\chi(n) = \begin{cases} \chi(n) & n \equiv a \ (q) \\ 0 & \text{otherwise} \end{cases} ,$$

over all $n \leq x$ satisfying $(\star)$ and all $a \in A$, to obtain

$$\begin{aligned} \sum_{a \in A} \sideset{}{^\star}\sum_{\substack{n \leq x \\ n \equiv a \ (q)}} \chi(n) &= \sum_{a \in A} \sideset{}{^\star}\sum_{n \leq x} \frac{1}{\phi(q)} \sum_{\substack{\psi \\ \text{mod } q}} \overline{\psi}(a)\psi(n)\chi(n) \\ &= \frac{1}{\phi(q)} \sum_{\substack{\psi \\ \text{mod } q}} \left(\sum_{a \in A} \overline{\psi}(a) \right) \left(\sideset{}{^\star}\sum_{n \leq x} (\psi\chi)(n) \right) \end{aligned}$$

Observe that

$$\left| \sum_{a \in A} \overline{\psi}(a) \right| \leq N .$$

Therefore if $N \leq \phi(q)/2$, we are done. Hence we may assume that $\phi(q)/2 + 1 \leq N \leq \phi(q)$. In this case, we observe that when ψ is not the trivial character mod q we have

$$\sum_{a \in A} \overline{\psi}(a) = -\sum_{a \notin A} \overline{\psi}(a) ,$$

and the result follows upon observing that

$$\begin{aligned} \frac{1}{\phi(q)} \sum_{\substack{\psi \\ \text{mod } q}} \left| \sum_{a \in A} \overline{\psi}(a) \right| &\leq \frac{(\phi(q) - N)(\phi(q) - 1) + N}{\phi(q)} \\ &\leq \frac{\phi(q)}{2} . \ \blacksquare \end{aligned}$$

Proof of Theorem 3.12. We may assume $f > \ell^2 \geq 9$ as this is implied by either inequality appearing in our hypothesis. Now by Lemma 2.3, we may assume that f is a prime with $f \equiv 1 \pmod{\ell}$.

First suppose that $q_1 = 2$ and $q_2 = 3$. We will say that $n \in \mathbb{Z}^+$ has property $(\star)$ if $(6, n) = 1$ and $n \not\equiv 3f \pmod 4$. By condition 1 of Theorem 3.1, we must prove that there exists $r \in \mathbb{Z}^+$ satisfying condition $(\star)$ with $\chi(r) = \chi(3)^{-1} =: \zeta$ such that $3r - 1 \leq f$. By way of contradiction, suppose there are no positive integers $n < x$ satisfying condition $(\star)$ with $\chi(n) = \zeta$. We will choose x later, but for now, we assume $0 < x < f$. Applying Lemma 3.14 we have:

$$\#\{n < x \mid n \text{ has property } (\star)\} \;\leq\; (\ell - 1) \max_{k=1,\ldots,\ell-1} \left| \sideset{}{^\star}\sum_{n<x} \chi^k(n) \right| \tag{3.6}$$

First we estimate the quantity on the left-hand side of (3.6) from below. Observe that:

$$\begin{aligned} \#\{n < x \mid n \text{ has property } (\star)\} &= \#\{n < x \;\mid\; n \equiv 3f + 2,\, 3f + 10 \pmod{12}\} \\ &\geq \frac{x}{6} - 2 \end{aligned}$$

Now we estimate the sum on the right-hand side of (3.6) from above. By Lemma 3.15 and Lemma 3.16, we have

$$\begin{aligned} \left| \sideset{}{^\star}\sum_{n<x} \chi^k(n) \right| &\leq \max_{\psi \bmod 4} \left| \sum_{\substack{n<x \\ (3,n)=1}} (\psi\chi^k)(n) \right| \\ &\leq 2(4f)^{1/2} \log 4f \,. \end{aligned}$$

Putting everything together, we have

$$\frac{x}{6} - 2 < 4(\ell - 1) f^{1/2} \log 4f \,,$$

which implies

$$x < 24(\ell - 1) f^{1/2} \log 4f + 12 \,.$$

Hence there exists an $r \in \mathbb{Z}^+$ with $\chi(r) = \zeta$ and

$$r \leq 24(\ell - 1) f^{1/2} \log 4f + 12 \,,$$

lest we arrive at a contradiction. In light of this, to satisfy condition 1 of Theorem 3.1, which reads $3r - 1 \leq f$ in this case, it is enough to assume

$$3(24(\ell - 1)f^{1/2} \log 4f + 12) - 1 \leq f \,,$$

which is true by hypothesis.

Now we treat the second case of $q_1 = 3$ and $q_2 = 5$. We only sketch the proof as it is very similar. This time, we will say that $n \in \mathbb{Z}^+$ has property $(\star)$ if $(15, n) = 1$ and $n \not\equiv f, 2f \pmod 9$; we find that this holds exactly when n belongs to one of 16 particular residue classes modulo 45. By condition 1 of Theorem 3.1, we must prove that there exists $r \in \mathbb{Z}^+$ satisfying condition $(\star)$ with $\chi(r) = \chi(5)^{-1} =: \zeta$ such that $10r - 2 \leq f$. By way of contradiction, suppose there are no positive integers $n < x$ satisfying condition $(\star)$ with $\chi(n) = \zeta$. We find

$$\#\{n < x \mid n \text{ has property } (\star)\} \;\; > \;\; \frac{16\,x}{45} - 16$$

and

$$\begin{aligned} \left| \sideset{}{^\star}\sum_{n<x} \chi^k(n) \right| \;\; &\leq \;\; 3 \max_{\psi \bmod 9} \left| \sum_{\substack{n<x \\ (5,n)=1}} (\psi\chi^k)(n) \right| \\ &\leq \;\; 6(9f)^{1/2} \log 9f \,. \end{aligned}$$

Combining the above, using the same argument as before, we find

$$\frac{16}{45}\, x < 18(\ell - 1)f^{1/2} \log 9f + 16 \,.$$

Proceeding as before, we arrive at the desired result. ∎

4 The Distribution of Character Non-Residues

In this chapter we establish some results regarding character non-residues, which are motivated by wanting to use Theorem 3.1 to obtain discriminant bounds. In §4.1 we state a known upper bound on q_1 and prove a new result which gives an upper bound on q_2. In §4.2 we prove an explicit version of a character sum estimate due to Burgess, following a method of Iwaniec; this will assist us in obtaining an upper bound on the value of r in Theorem 3.1, which is carried out in Chapter 5.

4.1 The Two Smallest Non-Residues

Let χ be a non-principal Dirichlet character modulo p. We will denote by $q_1 < q_2$ the two smallest prime non-residues of χ; i.e., the smallest primes such that $\chi(q_1), \chi(q_2) \neq 1$. We will tacitly assume $p \geq 5$ so that q_1 and q_2 are less than p. The question of putting an upper bound on q_1 is a classical problem which goes all the way back to the study of the least quadratic non-residue. The literature on this problem is extensive and we will not review it here except to say that the work of Burgess (see [8] and [9]) significantly advanced existing knowledge on this matter. The best known explicit bound on q_1 was given by Norton (see [40]) by applying Burgess' method with some modifications.

Theorem 4.1 (Norton, 1971)**.** *Let χ be a non-principal Dirichlet character modulo a prime p. Suppose q_1 is the smallest prime such that $\chi(q_1) \neq 1$. Then*

$$q_1 < 4.7\, p^{\frac{1}{4}} \log p\,.$$

Norton also shows that the constant 4.7 in the above theorem can be improved to 3.9 when the order of χ and $(p-1)/2$ have a common factor. As the characters in our application have odd order, we will take advantage of this slight sharpening of the constant. Our goal is to use Burgess' method to give a bound on q_2, or more particularly for our application, a bound on the product $q_1 q_2$. We prove the following theorem, which can be viewed as a generalization of Theorem 4.1, but with a slightly weaker constant.

Theorem 4.2. *Fix a real constant $p_0 \geq 10^7$. There exists a constant C (depending only upon p_0) such that if χ is a Dirichlet character modulo $p \geq p_0$ and u is a prime with $u \geq e^2 \log p$, then there exists $n \in \mathbb{Z}^+$ with $(n,u) = 1$, $\chi(n) \neq 1$, and*

$$n < C\, p^{1/4} \log p\,.$$

Table 4.1: Values of C for various choices of p_0

p_0	C
10^7	11.0485
10^8	8.2777
10^9	7.2914
10^{10}	6.8125
10^{11}	6.5498
10^{12}	6.3965
10^{13}	6.3034

p_0	C
10^{14}	6.2452
10^{15}	6.2078
10^{16}	6.1829
10^{17}	6.1659
10^{18}	6.1537
10^{19}	6.1445
10^{20}	6.1374

Corollary 4.3. *Fix a real constant $p_0 \geq 10^7$. Let χ be a non-principal Dirichlet character modulo a prime $p \geq p_0$. Suppose $q_1 < q_2$ are the two smallest primes such that $\chi(q_1), \chi(q_2) \neq 1$. If $q_1 > e^2 \log p$, then*

$$q_2 < C\, p^{\frac{1}{4}} \log p\,.$$

The constant C is the same constant as in the statement of the previous theorem.

Corollary 4.4. *Fix a real constant $p_0 \geq 10^7$. Let χ be a non-principal Dirichlet character modulo a prime $p \geq p_0$ having odd order. Suppose $q_1 < q_2$ are the two smallest primes such that $\chi(q_1), \chi(q_2) \neq 1$. Then*

$$q_1 q_2 < C'\, p^{\frac{1}{2}} (\log p)^2\,.$$

Table 4.2: Values of C' for various choices of p_0

p_0	C'
10^7	43.0892
10^8	32.2831
10^9	28.4365
10^{10}	26.5688
10^{11}	25.5443
10^{12}	24.9464
10^{13}	24.5833

p_0	C'
10^{14}	24.3563
10^{15}	24.2105
10^{16}	24.1134
10^{17}	24.0471
10^{18}	23.9995
10^{19}	23.9636
10^{20}	23.9359

The main idea behind Burgess' method is to combine upper and lower bounds for the following sum:

Definition 4.5. *If $h, r \in \mathbb{Z}^+$ and χ is a Dirichlet character modulo p, then we define*

$$S(\chi, h, r) := \sum_{x=0}^{p-1} \left| \sum_{m=1}^{h} \chi(x+m) \right|^{2r} .$$

The following character sum estimate was first given by Weil, as a consequence of his deep work on the Riemann hypothesis for function fields (see [54]). It is also proved as Theorem 2C' in [47] using an elementary method due to Stepanov (see [51]), which was later extended by both Bombieri (see [6]) and Schmidt (see [46]).

Lemma 4.6. *Let χ be a non-principal Dirichlet character to the prime modulus p, having order n. Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with m distinct roots, which is not an n-th power in $\mathbb{F}_p[x]$, where $\mathbb{F}_p$ denotes the finite field with p elements. Then*

$$\left| \sum_{x \in \mathbb{F}_p} \chi(f(x)) \right| \leq (m-1)\, p^{1/2} .$$

The next lemma is a slight improvement over Lemma 2 in [8] which gives an upper bound on $S(\chi, h, r)$. The proof is not difficult if we grant ourselves Lemma 4.6.

Lemma 4.7. *Suppose χ is any non-principal Dirichlet character to the prime modulus p. If $r, h \in \mathbb{Z}^+$, then*

$$S(\chi, h, r) < \frac{1}{4}(4r)^r p h^r + (2r-1) p^{1/2} h^{2r} .$$

Proof. First we claim that we may assume, without loss of generality, that $r < h < p$. We commence by observing that $h = p$ implies $S(\chi, h, r) = 0$, in which case there is nothing to prove. We see that $h > p$ implies $S(\chi, h-p, r) = S(\chi, h, r)$, which allows us to inductively bring h into the range $0 < h < p$. Additionally, we notice that if $h \leq r$, then the theorem is trivial since in this case we would have $S(\chi, h, r) \leq h^{2r}p \leq (hr)^r p$. This establishes the claim.

Now, to begin the proof proper, we observe that

$$S(\chi, h, r) = \sum_{1 \leq m_1, \ldots, m_{2r} \leq h} \sum_{x=0}^{p-1} \chi(x+m_1) \ldots \chi(x+m_r)\overline{\chi}(x+m_{r+1}) \ldots \overline{\chi}(x+m_{2r}) \,.$$

Define

$$\mathcal{M} := \{\mathbf{m} = (m_1, \ldots, m_{2r}) \mid 1 \leq m_1, \ldots, m_{2r} \leq h\} \,.$$

We can rewrite the above as

$$S(\chi, h, r) = \sum_{\mathbf{m} \in \mathcal{M}} \sum_{x \in \mathbb{F}_p} \chi(f_{\mathbf{m}}(x)) \,,$$

where

$$f_{\mathbf{m}}(x) = (x+m_1) \ldots (x+m_r)(x+m_{r+1})^{n-1}(x+m_{2r})^{n-1} \,,$$

and n denotes the order of χ. If $f_{\mathbf{m}}(x)$ is not an n-th power mod p, then by Lemma 4.6 we have

$$\left| \sum_{x \in \mathbb{F}_p} \chi(f_{\mathbf{m}}(x)) \right| \leq (2r-1)\sqrt{p} \,.$$

Otherwise, we must settle for the trivial bound of p.

It remains to count the number of exceptions – that is, the number of $\mathbf{m} \in \mathcal{M}$ such that $f_{\mathbf{m}}(x)$ is an n-th power mod p. A little care is required here – as an example, if $r = n = 3$ and $p \geq 5$, then the vectors $\mathbf{m} = (1,2,3,1,2,3)$ and $\mathbf{m} = (1,1,1,2,2,2)$ are both exceptions, but the way in which they arise is slightly different; as r gets larger compared to n, the situation only gets worse. In light of this difficulty, we will actually count (as Burgess does in [9]) the number of $\mathbf{m} = (m_1, \ldots, m_{2r}) \in \mathcal{M}$ such that each m_j is repeated at least once. We let u denote the number of distinct m_j (so that $u \leq r < h$) and denote by $1 = j_1 < j_2 < \cdots < j_u \leq 2r$ the indices corresponding to the first occurrence of

each of the u values among the m_j. The number of ways to choose the j_k is bounded by $\binom{2r-1}{u-1}$, and there are at most h choices for each m_{j_k} while the remaining m_j are restricted to at most u values. In light of all this, we find that the number of exceptions is bounded above by

$$\sum_{u=1}^{r}\binom{2r-1}{u-1}h^u u^{2r-u} \;\leq\; (hr)^r\sum_{u=1}^{r}\binom{2r-1}{u-1}\left(\frac{u}{h}\right)^{r-u} \;\leq\; (hr)^r\sum_{u=1}^{r}\binom{2r-1}{u-1}.$$

Finally, to complete the proof, we observe

$$(hr)^r\sum_{u=1}^{r}\binom{2r-1}{u-1} \;=\; (hr)^r 2^{2r-2} \;=\; \frac{1}{4}(4rh)^r\,. \;\blacksquare$$

Having achieved an upper bound on the sum $S(\chi,h,r)$, the next aim is to give a lower bound on the same sum, under some extra conditions. The idea is to locate a large number of disjoint intervals on which χ is "almost" constant. For the remainder of this section p will denote a prime with $p\geq 5$, and h, H will denote positive integers. The following are the intervals that will be of interest to us:

Definition 4.8. *For integers with $0\leq t<q$, we define the intervals*

$$\mathcal{I}(q,t)=\left(\frac{pt}{q},\frac{H+pt}{q}\right]\,,\quad \mathcal{I}(q,t)^\star=\left(\frac{pt}{q},\frac{H+pt}{q}-h\right]\,,$$
$$\mathcal{J}(q,t)=\left[-\frac{H+pt}{q},-\frac{pt}{q}\right)\,,\quad \mathcal{J}(q,t)^\star=\left[-\frac{H+pt}{q},-\frac{pt}{q}-h\right)\,.$$

We note that the intervals $\mathcal{I}(q,t)^\star$, $\mathcal{J}(q,t)^\star$ might be empty. In fact, they are non-empty exactly when $h<H/q$, which will always be the case whenever we employ them.

Lemma 4.9. *Let $X>1$ be a real number and suppose $XH<p$. Then the intervals $\mathcal{I}(q,t)$ where $0\leq t<q\leq X$ with $(t,q)=1$ are disjoint, and similarly for $\mathcal{J}(q,t)$.*

Proof. If $\mathcal{I}(q_1,t_1)$ and $\mathcal{I}(q_2,t_2)$ intersect, then we have:

$$pt_1/q_1\leq (H+pt_2)/q_2$$
$$pt_2/q_2\leq (H+pt_1)/q_1$$

It follows that

$$|t_1q_2-t_2q_1|\leq\frac{XH}{p}<1\,;$$

whence $t_1q_2 = t_2q_1$ which implies $t_1 = t_2$, $q_1 = q_2$. (When $t_1 = t_2 = 0$, the condition $(q_1, t_1) = (q_2 = t_2) = 1$ forces $q_1 = q_2 = 1$, so the argument goes through in this case as well.) The proof for the intervals $\mathcal{J}(q,t)$ is the same. ∎

Lemma 4.10. *Let $h, u \in \mathbb{Z}^+$ with u prime and $h \leq u$. Suppose that χ is a Dirichlet character modulo p such that $\chi(n) = 1$ for all $n \in [1, H]$ with $(n, u) = 1$. If $z \in \mathcal{I}(q,t)^\star \cup \mathcal{J}(q,t)^\star$ and $(q, u) = 1$, then*

$$\left|\sum_{m=0}^{h-1} \chi(z+m)\right| \geq h - 2$$

Proof. We note that by hypothesis $\mathcal{I}(q,t)^\star \cup \mathcal{J}(q,t)^\star \neq \emptyset$ and hence $h < H/q$. First suppose $z \in \mathcal{I}(q,t)^\star$. We will show that the values $\chi(z+n)$ for $n = 0, \ldots, h-1$ are all equal except for possibly one value of n. This will immediately give the result upon application of the triangle inequality. For $n = 0, \ldots, h-1$, we have $z + n \in \mathcal{I}(q,t)$ and hence $q(z+n) - pt \in (0, H]$. Provided u does not divide $q(z+n) - pt$, we have

$$\chi(z+n) = \overline{\chi}(q)\chi(q(z+n)) = \overline{\chi}(q)\chi(q(z+n) - pt) = \overline{\chi}(q)\,.$$

But if u divides $q(z+n) - pt$ for two distinct values of n, say n_1 and n_2, we find that u divides $q(n_1 - n_2)$. Since $(u, q) = 1$, we conclude that u divides $n_1 - n_2$ and hence $|n_1 - n_2| \geq u$. This leads to $h \leq u \leq |n_1 - n_2| \leq h - 1$, a contradiction. The proof for $z \in \mathcal{J}(q,t)^\star$ is similar. ∎

Lemma 4.11. *Suppose that $X > 1$ is a real number and $u \in \mathbb{Z}^+$ is prime. Then*

$$\sum_{\substack{n \leq X \\ (n,u)=1}} n = \frac{(1 - u^{-1})}{2} X^2 + \theta_{X,u} X\,,$$

where the sum is taken over positive integers and $\theta_{X,u}$ denotes a real number, depending on X and u, that belongs to the interval $(-1, 1)$.

Proof. For any $Y > 0$ we have

$$\sum_{n \leq Y} n = \frac{\lfloor Y \rfloor (\lfloor Y \rfloor + 1)}{2}\,.$$

Upon an application of the obvious inequality $Y - 1 < \lfloor Y \rfloor \leq Y$, we obtain the identity

$$\sum_{n \leq Y} n = \frac{Y^2}{2} + \frac{Y}{2}\theta_Y \,,$$

where $\theta_Y \in (-1, 1]$. Now we write

$$\begin{aligned} \sum_{\substack{n \leq X \\ (n,u)=1}} n &= \sum_{n \leq X} n - u \sum_{n \leq X/u} n \\ &= \frac{X^2}{2}(1 - u^{-1}) + \frac{X}{2}(\theta_X - \theta_{X/u}) \,, \end{aligned}$$

and observe that

$$-2 < \theta_X - \theta_{X/u} < 2 \,.$$

The result follows. ∎

Lemma 4.12. *Suppose $X > 1$ and $u \in \mathbb{Z}^+$ is prime. Then*

$$\sum_{\substack{1 \leq q \leq X \\ (q,u)=1}} \phi(q) \;\geq\; \frac{3}{\pi^2}(1 - u^{-1})X^2 f(X, u) \,,$$

where

$$f(X, u) = 1 - \frac{\pi^2}{3}\left(\frac{1}{2X^2} + \frac{1}{2X} + \frac{1}{1 - u^{-1}} \cdot \frac{1 + \log X}{X}\right) .$$

Proof. First we observe:

$$\begin{aligned} \sum_{\substack{1 \leq q \leq X \\ (q,u)=1}} \phi(q) &= \sum_{\substack{1 \leq q \leq X \\ (q,u)=1}} \sum_{m | q} \frac{q}{m}\,\mu(m) \\ &= \sum_{\substack{1 \leq m \leq X \\ (m,u)=1}} \mu(m) \sum_{\substack{1 \leq r \leq X/m \\ (r,u)=1}} r \end{aligned}$$

Applying Lemma 4.11 to the above gives:

$$\sum_{\substack{1 \leq q \leq X \\ (q,u)=1}} \phi(q) \;=$$

$$\frac{X^2}{2}\left(1 - u^{-1}\right)\left(\sum_{\substack{1 \leq m \leq X \\ (m,u)=1}} \frac{\mu(m)}{m^2}\right) + \; X\left(\sum_{\substack{1 \leq m \leq X \\ (m,u)=1}} \frac{\mu(m)}{m}\,\theta_{X/m,u}\right)$$

Now we use the bounds:

$$\sum_{\substack{1\le m\le X\\(m,u)=1}} \frac{\mu(m)}{m^2} \ge \frac{6}{\pi^2} - \frac{1}{X^2} - \frac{1}{X}\,,$$

$$\left|\sum_{\substack{1\le m\le X\\(m,u)=1}} \frac{\mu(m)}{m}\,\theta_{X/m,u}\right| \le \sum_{1\le m\le X} \frac{1}{m} \le 1+\log X$$

The result now follows from an application of the triangle inequality and some rearrangement. ∎

Finally, we are ready to give the lower bound we have alluded to.

Proposition 4.13. *Let $h, r, u \in \mathbb{Z}^+$ with u prime and $h \le u$. Suppose that χ is a Dirichlet character modulo p such that $\chi(n) = 1$ for all $n \in [1, H]$ satisfying $(n, u) = 1$. Assume $2h < H \le (2hp)^{1/2}$ and set $X := H/(2h) > 1$. Then*

$$S(\chi, h, r) \ge \frac{6}{\pi^2}(1-u^{-1})h(h-2)^{2r}X^2 f(X,u)\,.$$

The function $f(X,u)$ is defined in Lemma 4.12.

Proof. We begin by noting that $H/q \ge H/X = 2h$. Using Lemma 4.9 and Lemma 4.10 we have:

$$\begin{aligned}
S(\chi,h,r) &= \sum_{x=0}^{p-1}\left|\sum_{m=0}^{h-1}\chi(x+m)\right|^{2r}\\
&\ge \sum_{\substack{0\le t<q\le X\\(q,u)=(q,t)=1}}\ \sum_{z\in\mathcal{I}^\star_{q,t}\cup\mathcal{J}^\star_{q,t}}\left|\sum_{m=0}^{h-1}\chi(z+m)\right|^{2r}\\
&\ge \sum_{\substack{0\le t<q\le X\\(q,tu)=1}} 2\left(\frac{H}{q}-h\right)(h-2)^{2r}\\
&\ge \sum_{\substack{0\le t<q\le X\\(q,tu)=1}} 2h(h-2)^{2r}\\
&= 2h(h-2)^{2r}\sum_{\substack{1\le q\le X\\(q,u)=1}}\phi(q)
\end{aligned}$$

Now the result follows from Lemma 4.12. ∎

Lemma 4.14. *Suppose $h, r \geq 1$. Then*

$$h \geq 6r+5 \implies \frac{1}{2h}\left(\frac{4r}{h-2}\right)^r \leq \frac{1}{h+1}\left(\frac{4r}{h+1}\right)^r$$

$$h \geq 16r+2 \implies \left(\frac{h}{h-2}\right)^r < \frac{7}{6}$$

$$h \geq 2r-1 \implies \frac{2r-1}{h} \leq \frac{2r}{h+1}$$

Proof. By the convexity of the logarithm, we have $\log t \geq (2\log 2)(t-1)$ for all $t \in [1/2, 1]$. Applying this, together with the hypothesis that $6(r+1) \leq h+1$, we get

$$\log\left(\frac{h-2}{h+1}\right) \geq -\frac{6\log 2}{h+1} \geq -\frac{\log 2}{r+1}\,.$$

This yields

$$\frac{1}{2} \leq \left(\frac{h-2}{h+1}\right)^{r+1},$$

and first implication follows. For the proof of the second implication, we observe (again by convexity) that $\log t \leq t-1$ for all t and hence

$$r\log\left(\frac{h}{h-2}\right) \leq \frac{2r}{h-2} \leq \frac{1}{8}\,;$$

this leads to

$$\left(\frac{h}{h-2}\right)^r \leq \exp\left(\frac{1}{8}\right) < \frac{7}{6}\,.$$

The third implication is trivial. ∎

The following is the main result of §4.1, from which Theorem 4.2 will follow:

Theorem 4.15. *Suppose that χ is a non-principal Dirichlet character modulo $p \geq 10^7$, and that u is a prime with $u \geq e^2 \log p$. Suppose $\chi(n) = 1$ for all $n \in [1, H]$ with $(n, u) = 1$. If*

$$H \leq (2e^2 \log p - 2)^{1/2} p^{1/2}\,,$$

then

$$H \leq K g(p)\, p^{1/4} \log p\,,$$

where

$$K = \frac{\pi e}{\sqrt{2}} \approx 6.0385$$

and

$$g(p) = \sqrt{\frac{\left(1+\frac{4}{3\log p}\right)}{\left(1-\frac{1}{e^2\log p}\right) f\left(\frac{Kp^{1/4}}{2e^2}, 89\right)}}\,.$$

The function $g(p)$ is positive and decreasing for $p \geq 10^7$, with $g(p) \to 1$ as $p \to \infty$. The function $f(X,u)$ is defined in Lemma 4.12.

Proof. First, we may assume $H \geq Kp^{1/4}\log p$, or else there is nothing to prove. We set $h = \lfloor A\log p \rfloor$, $r = \lfloor B\log p \rfloor$ with $A = e^2$, $B = 1/4$ and verify that r, h satisfy all three conditions in Lemma 4.14. The constants A and B were chosen to minimize the quantity AB subject to the constraint $A \geq 4B\exp(1/(2B))$. One verifies that $Kp^{1/4} > 28e^2$ for $p \geq 10^7$ and hence $H > 28h$. We set $X := H/(2h)$ and observe that we have the a priori lower bound

$$X = \frac{H}{2h} \geq \frac{Kp^{1/4}\log p}{2e^2\log p} = \frac{Kp^{1/4}}{2e^2}\,,$$

and, in particular, $X > 14$ from the previous sentence. Since $p \geq 10^5$ and $e^2\log(10^5) \approx 85.1$, we know $u \geq 89$ and hence $f(X,u) \geq f(X,89)$. For notational convenience, we will write $f(X) := f(X,89)$. Combining Lemma 4.7 and Proposition 4.13, we obtain

$$\frac{6}{\pi^2}\left(1-u^{-1}\right) h(h-2)^{2r}\left(\frac{H}{2h}\right)^2 f(X) \;\leq\; \frac{1}{4}(4r)^r p h^r + (2r-1)p^{1/2}h^{2r}\,.$$

Rearranging the above and applying Lemma 4.14 gives

$$\begin{aligned}
&\frac{6}{\pi^2}\left(1-u^{-1}\right) H^2 f(X) \\
&\quad\leq 4h^2p^{1/2}\left[\frac{1}{4h}\left(\frac{4r}{h-2}\right)^r\left(\frac{h}{h-2}\right)^r p^{1/2} + \frac{2r-1}{h}\left(\frac{h}{h-2}\right)^{2r}\right] \\
&\quad\leq 4h^2p^{1/2}\left[\frac{1}{h+1}\left(\frac{4r}{h+1}\right)^r p^{1/2} + \frac{3r}{h+1}\right]. \qquad (4.1)
\end{aligned}$$

Plugging in our choices of r, h and using the fact that

$$A \geq 4B\exp\left(\frac{1}{2B}\right) \implies \left(\frac{4B}{A}\right)^r \leq p^{-1/2}$$

we obtain

$$\begin{aligned}\frac{6}{\pi^2}\left(1-u^{-1}\right)H^2 f(X) &\leq 4A^2(\log p)^2 p^{1/2}\left[\frac{1}{A\log p}\left(\frac{4B}{A}\right)^r p^{1/2}+\frac{3B}{A}\right]\\ &\leq 4A^2 p^{1/2}(\log p)^2\left(\frac{1}{A\log p}+\frac{3B}{A}\right)\\ &= 12AB p^{1/2}(\log p)^2\left(1+\frac{1}{3B\log p}\right). \qquad (4.2)\end{aligned}$$

Plugging in our choices of A and B yields: [1]

$$\frac{6}{\pi^2}\left(1-u^{-1}\right)H^2 f(X) \leq 3e^2 p^{1/2}(\log p)^2\left(1+\frac{4}{3\log p}\right) \qquad (4.3)$$

As $f(X)$ is increasing and positive for $X \geq 14$, the result now follows upon solving (4.3) for H. ∎

Proof of Theorem 4.2. Suppose $p \geq 10^7$. Let n_0 denote the smallest $n \in \mathbb{Z}^+$ such that $(n,u)=1$ and $\chi(n) \neq 1$. Set $H := n_0 - 1$ so that $\chi(n) = 1$ for all $n \in [1,H]$ with $(n,u)=1$.

First we show that $H \leq (2e^2\log p - 2)^{1/2}p^{1/2}$. By way of contradiction, suppose $H > (2e^2\log p - 2)^{1/2}p^{1/2}$. In this case we set $H_0 = \lfloor (2e^2\log p - 2)^{1/2}p^{1/2}\rfloor$, and note that we still have $\chi(n)=1$ for all $n \in [1,H_0]$ with $(n,u)=1$ for this smaller value H_0. We invoke Theorem 4.15 to conclude that $H_0 < Kg(p)p^{1/4}\log p$ where $Kg(p) \leq Kg(10^7) < 12$. Using again the fact that $p \geq 10^7$, we have

$$H_0 < 12p^{1/4}\log p < (2e^2\log p - 2)^{1/2}p^{1/2} - 1 < H_0\,,$$

which is a contradiction. This proves that $H \leq (2e^2\log p - 2)^{1/2}p^{1/2}$.

Having shown that H satisfies the required condition, we apply Theorem 4.15 to find $H \leq Kg(p_0)\,p^{1/4}\log p$ when $p \geq p_0 \geq 10^7$. Therefore

$$n_0 \leq Kg(p_0)\,p^{1/4}\log p + 1\,,$$

for $p \geq p_0 \geq 10^7$. Computation of the table of constants is routine; for each value of p_0, we compute (being careful to round up) the quantity

$$Kg(p_0) + \frac{1}{p_0^{1/4}\log p_0}\,. \;\blacksquare$$

[1] At this point our choices of A and B are properly motivated – the condition $A \geq 4B\exp(1/(2B))$ was to ensure that the quantity in the square brackets of (4.1) remains bounded as $p \to \infty$, and we wanted to minimize AB so that the constant appearing in (4.2) was as small as possible.

Proof of Corollary 4.3. Apply Theorem 4.2 with $u = q_1$ and observe that the smallest $n \in \mathbb{Z}^+$ with $(n, q_1) = 1$ and $\chi(n) \neq 1$ is equal to q_2. ∎

In order to prove Corollary 4.4, we will use the following result which gives a weak bound on q_2, but requires no extra hypotheses on q_1.

Lemma 4.16. *Let χ be a non-principal Dirichlet character modulo m. Suppose $q_1 < q_2$ are the two smallest primes such that $\chi(q_1), \chi(q_2) \neq 1$. Then*

$$q_2 < \begin{cases} 3\, m^{1/2} \log m & \text{if } m \geq 10^7 \\ 2\, m^{1/2} \log m & \text{if } m \geq 10^{15} \end{cases} .$$

Proof. The proof is an application of Theorem 2.1. For $x > 1$, we have

$$\begin{aligned} \left| \sum_{\substack{n<x \\ (n,q_1)=1}} \chi(n) \right| &= \left| \sum_{n<x} \chi(n) - \chi(q_1) \sum_{n<x/q_1} \chi(n) \right| \\ &\leq \left| \sum_{n<x} \chi(n) \right| + \left| \sum_{n<x/q_1} \chi(n) \right| \\ &\leq 2 \left(\frac{1}{3 \log 3}\, m^{1/2} \log m + 6.5\, m^{1/2} \right) . \end{aligned}$$

If $\chi(n) = 1$ for all $n \leq x$ with $(n, q_1) = 1$, then

$$\left| \sum_{\substack{n<x \\ (n,q_1)=1}} \chi(n) \right| \geq (1 - q_1^{-1})x - 1 .$$

Thus for $1 < x < q_2$, we have

$$(1 - q_1^{-1})x - 1 \leq 2 \left(\frac{1}{3 \log 3}\, m^{1/2} \log m + 6.5\, m^{1/2} \right) .$$

Using the fact that $q_1 \geq 2$ and letting x approach q_2 from the left, we obtain:

$$q_2 \leq 4 \left(\frac{1}{3 \log 3}\, m^{1/2} \log m + 6.5\, m^{1/2} \right) + 2 .$$

The result follows. ∎

Proof of Corollary 4.4. If $q_1 < e^2 \log p$, we use Lemma 4.16 to obtain $q_2 < 3p^{1/2} \log p$ and hence $q_1 q_2 < 3e^2 p^{1/2} (\log p)^2$. If $q_1 \geq e^2 \log p$, then we apply Theorem 4.1 (using the fact that χ has odd order) and Corollary 4.3 to find $q_1 q_2 \leq C'\, p^{1/2} (\log p)^2$ with $C' = 3.9\, C$. As $C \geq 6$, we have $3e^2 < 3.9 \cdot 6 \leq 3.9\, C = C'$, which completes the proof. ∎

4.2 A Character Sum Estimate of Burgess

In this section, we prove an explicit version of a character sum estimate of Burgess (see [8]), following a method due to Iwaniec (see [29] and [18]). Booker proves a similar result when χ is quadratic (see [7]).

Theorem 4.17. *Suppose χ is a non-principal Dirichlet character to the prime modulus $p \geq 2 \cdot 10^4$. Let $N, H \in \mathbb{Z}$ with $H \geq 1$. Fix a positive integer $r \geq 2$. Then there exists a computable constant $C(r)$ such that whenever $H \leq 4p^{\frac{1}{2}+\frac{1}{4r}}$ we have*

$$\left| \sum_{n \in (N, N+H]} \chi(n) \right| < C(r)\, H^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{2r}} .$$

Table 4.3: Values for the constant $C(r)$ when $2 \leq r \leq 15$:

r	$C(r)$
2	10.0366
3	4.9539
4	3.6493
5	3.0356
6	2.6765
7	2.4400
8	2.2721

r	$C(r)$
9	2.1467
10	2.0492
11	1.9712
12	1.9073
13	1.8540
14	1.8088
15	1.7700

We note in passing that the assumption $H \leq 4p^{\frac{1}{2}+\frac{1}{4r}}$ is of a technical nature. It seems that to drop it, at least in the current proof, one may have to accept a slightly worse exponent on the $\log p$ term. In any case, this condition is essentially automatic for our application in Chapter 5.

Throughout this section, χ will denote a Dirichlet character modulo an odd prime p and N, H will be integers with $0 \leq N < p$ and $1 \leq H < p$. The latter assumption is justified as reducing N and H modulo p leaves the sum in the above theorem unchanged. The letter r will denote a positive integer parameter with $r \geq 2$. We begin with some definitions.

Definition 4.18.

$$S_\chi(H) := \sum_{n \in (N, N+H]} \chi(n) .$$

Definition 4.19.

$$E(H) := H^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{2r}}$$

We seek a bound of the form $S_\chi(H) < C(r)\, E(H)$. (An explicit choice of $C(r)$ is given in Theorem 4.25.) It is plain that $S_\chi(H)$ also depends upon N and that $E(H)$ also depends upon p and r, but we have chosen to avoid excess decoration of our notations.

Definition 4.20. *Fix $A \in \mathbb{Z}$ with $1 < A < p$. For $x \in \mathbb{F}_p$, we define $\nu_A(x)$ to be the number of ways we can write*

$$x \equiv \overline{a}n \pmod{p},$$

where $a \in [1, A]$ is a prime and $n \in (N, N + H]$ is an integer.

In the above definition and in the rest of this section $\overline{a}$ will denote a multiplicative inverse of a modulo p. We note that $\nu_A(x)$ also depends upon N, H, p. Before launching the main part of the proof, we will require a series of lemmas.

Lemma 4.21. *Suppose $|S_\chi(H_0)| \le C\, E(H_0)$ for all $H_0 < H$. Fix $H_0 = AB < H$. Then*

$$|S_\chi(H)| \le \frac{1}{\pi(A)B} \sum_{x \in \mathbb{F}_p} \nu_A(x) \left| \sum_{1 \le b \le B} \chi(x+b) \right| + 2C\, E(H_0).$$

Proof. Applying a shift $n \mapsto n + h$ with $1 \le h \le H_0$ gives

$$S_\chi(H) = \sum_{n \in (N, N+H]} \chi(n+h) + 2C\theta E(H_0).$$

(The letter θ will denote a complex number with $|\theta| \le 1$, possibly different each time it appears.) We set $h = ab$ in the above, and average over all primes $a \in [1, A]$ and all integers $b \in [1, B]$. This gives

$$S_\chi(H) = \frac{1}{\pi(A)B} \sum_{a,b}{}' \sum_{n \in (N, N+H]} \chi(n+ab) + 2C\theta E(H_0),$$

where $\sum'$ here indicates that we are summing over all primes $a \in [1, A]$ and all integers $b \in [1, B]$. Rearranging the sum in the above expression yields

$$\sum_{a,b}{}' \sum_{n \in (N, N+H]} \chi(n+ab) = \sum_{\substack{1 \le a \le A \\ a \text{ prime}}} \sum_{n \in (N, N+H]} \chi(a) \sum_{1 \le b \le B} \chi(\overline{a}n + b),$$

and hence

$$\left|\sideset{}{'}\sum_{a,b}\sum_{n\in(N,N+H]}\chi(n+ab)\right| \leq \sum_{x\in\mathbb{F}_p}\nu_A(x)\left|\sum_{1\leq b\leq B}\chi(x+b)\right|.$$

The result follows. ∎

Lemma 4.22. *Suppose $a_1 \neq a_2$ are prime and $b \in \mathbb{Z}$. Then the number of integral solutions $(x,y) \in \mathbb{Z}^2$ to the equation $a_1x - a_2y = b$ with $x, y \in (N, N+H]$ is at most*

$$\frac{H}{\max\{a_1,a_2\}} + 1\,.$$

Proof. Let Q denote the number of solutions to $a_1x - a_2y = b$ with $x, y \in (N, N+H]$. We will show $Q \leq H/a_2 + 1$. It will immediately follow from the same argument that $Q \leq H/a_1 + 1$ as well; indeed, just multiply both sides of the equation by -1 and interchange the roles of x and y. Suppose we have two solutions (x,y) and (x',y'). It follows that

$$a_1(x-x') = a_2(y-y')\,,$$

and since $a_1 \neq a_2$ are prime, we see that a_2 divides $x-x'$ which implies $|x-x'| \geq a_2$. The result follows. ∎

Lemma 4.23. *Fix $A \in \mathbb{Z}$ with $1 < A < p$. If $2AH \leq p$, then*

$$\sum_{x\in\mathbb{F}_p}\nu_A(x)^2 < \pi(A)H\left(1 + \frac{2}{\pi(A)}\sum_{\substack{a\leq A\\ a\ prime}}\frac{\pi(a)-1}{a} + \frac{2}{\pi(A)H}\sum_{\substack{a\leq A\\ a\ prime}}(\pi(a)-1)\right).$$

Proof. Define S to be the set of all quadruples (a_1,a_2,n_1,n_2) with

$$a_1n_2 \equiv a_2n_1 \pmod{p}$$

where $a_1, a_2 \in [1,A]$ are prime and $n_1, n_2 \in (N, N+H]$ are integers. We observe that $\#S = \sum_{x\in\mathbb{F}_p}\nu_A(x)^2$. Suppose $(a_1,a_2,n_1,n_2) \in S$ with $a_1 = a_2$. Then we have $n_1 \equiv n_2 \pmod{p}$ and hence $n_1 = n_2$ since $n_1, n_2 \in (N, N+H]$ and $H \leq p$. Thus there are exactly $\pi(A)H$ solutions of this form.

Now we deal with the remaining cases. Let $(a_1, a_2, n_1, n_2) \in S$ with $a_1 \neq a_2$. Then $a_1 n_2 - a_2 n_1 = kp$ for some k. Writing $n_1 = N + h_1$ and $n_2 = N + h_2$ with $0 < h_1, h_2 \leq H$, we have

$$\begin{aligned} k &= \frac{a_1(N+h_2) - a_2(N+h_1)}{p} \\ &= \frac{a_1 - a_2}{p} N + \frac{a_1 h_2 - a_2 h_1}{p} \\ &= \frac{a_1 - a_2}{p}\left(N + \frac{H}{2}\right) + \frac{a_1(h_2 - H/2) - a_2(h_1 - H/2)}{p}, \end{aligned}$$

which gives

$$\left| k - \left(\frac{a_1 - a_2}{p}\right)\left(N + \frac{H}{2}\right)\right| < \frac{(a_1 + a_2)H}{2p} \leq \frac{AH}{p} \leq \frac{1}{2}.$$

This implies that a_1 and a_2 determine k. Now Lemma 4.22 tells us that there are at most

$$\frac{H}{\max\{a_1, a_2\}} + 1$$

choices of (n_1, n_2) for each fixed (a_1, a_2). Thus the number of elements in S with $a_1 \neq a_2$ is bounded above by

$$2 \sum_{\substack{a_2 \leq A \\ a_2 \text{ prime}}} \sum_{\substack{a_1 < a_2 \\ a_1 \text{ prime}}} \left(\frac{H}{a_2} + 1\right) \;<\; 2H \sum_{\substack{a \leq A \\ a \text{ prime}}} \frac{\pi(a) - 1}{a} + 2 \sum_{\substack{a \leq A \\ a \text{ prime}}} (\pi(a) - 1).$$

This gives the result. ∎

The next estimate is very weak, but has the advantage that it holds for all X.

Lemma 4.24. *For $X \in \mathbb{Z}^+$ we have*

$$\frac{1}{\pi(X)} \sum_{\substack{a \leq X \\ a \text{ prime}}} \frac{\pi(a) - 1}{a} < \frac{1}{3}.$$

Proof. The result holds for $X \leq 100$ by direct computation. Using the Sieve of Eratosthenes, one easily shows that

$$\frac{\pi(n) - 1}{n} \leq \frac{1}{3}.$$

for all $n \geq 100$. The result follows. ∎

Now we are ready to state and prove the main result of §4.2, from which Theorem 4.17 will follow.

Theorem 4.25. *Suppose χ is a non-principal Dirichlet character to the prime modulus p. Fix a positive integer $r \geq 2$. Suppose $d > 4$, $C \geq 1$, $p_0 \geq 2$ are real constants satisfying*

$$C^r p_0^{\frac{1}{4}-\frac{1}{4r}} (\log p_0)^{\frac{1}{2}} \geq 4d(d+1)r \tag{4.4}$$

and

$$C \geq \frac{((d+1)(2r-1)(4r-1))^{\frac{1}{2r}}}{\left(1-\frac{2}{d^{1-\frac{1}{r}}}\right)}\,. \tag{4.5}$$

If

$$H \leq \sqrt{rd}\, p^{\frac{1}{2}+\frac{1}{4r}}\,,$$

then for $p \geq p_0$ we have

$$|S_\chi(H)| \leq C H^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{2r}}\,.$$

Proof. We may assume

$$H \geq C^r p^{\frac{1}{4}+\frac{1}{4r}} (\log p)^{\frac{1}{2}}\,,$$

or else the result follows from the trivial bound $|S_\chi(H)| \leq H$. We will prove the result by induction on H. We assume that $|S_\chi(H_0)| \leq CE(H_0)$ for all $H_0 < H$. We choose an integer H_0 with

$$\frac{H}{d+1} < H_0 \leq \frac{H}{d}\,,$$

for which we can write $H_0 = AB$ with $A, B \in \mathbb{Z}^+$, where

$$B = \lfloor 4rp^{\frac{1}{2r}} \rfloor\,.$$

Accomplishing this is possible provided

$$H \geq 4d(d+1)rp^{\frac{1}{2r}}\,;$$

given our a priori lower bound on H, this condition follows from (4.4).

Before proceeding further, we give upper and lower bounds on A. Observe that

$$A \le \frac{H}{dB} \le \frac{\sqrt{rd}\, p^{\frac{1}{2}+\frac{1}{4r}}}{3drp^{\frac{1}{2r}}} = \frac{1}{3\sqrt{rd}} p^{\frac{1}{2}-\frac{1}{4r}} .$$

We also have

$$A > \frac{H}{(d+1)B} \ge \frac{C^r p^{\frac{1}{4}+\frac{1}{4r}} (\log p)^{\frac{1}{2}}}{(d+1)4rp^{\frac{1}{2r}}} = \frac{C^r p^{\frac{1}{4}-\frac{1}{4r}} (\log p)^{\frac{1}{2}}}{4(d+1)r} .$$

In particular, using (4.4), we see that $A > d > 4$.

Applying Lemma 4.21 and our inductive hypothesis, we have

$$\begin{aligned} |S_\chi(H)| &\le \frac{1}{\pi(A)B} \sum_{x\in\mathbb{F}_p} \nu_A(x) \left| \sum_{1\le b\le B} \chi(x+b) \right| + 2C\, E(H_0) \\ &\le \frac{1}{\pi(A)B} \sum_{x\in\mathbb{F}_p} \nu_A(x) \left| \sum_{1\le b\le B} \chi(x+b) \right| + \frac{2C}{d^{1-\frac{1}{r}}} E(H) . \end{aligned} \tag{4.6}$$

In order to bound the sum above, we apply Hölder's inequality to the functions $\nu_A(x)^{1-\frac{1}{r}}$, $\nu_A(x)^{\frac{1}{r}}$, and $\left|\sum_{1\le b\le B} \chi(x+b)\right|$ using the Hölder exponents $(1-1/r)^{-1}$, $2r$, and $2r$ respectively; this yields:

$$\begin{aligned} &\sum_{x\in\mathbb{F}_p} \nu_A(x) \left| \sum_{1\le b\le B} \chi(x+b) \right| \\ &\qquad \le \left(\sum_{x\in\mathbb{F}_p} \nu_A(x) \right)^{1-\frac{1}{r}} \left(\sum_{x\in\mathbb{F}_p} \nu_A(x)^2 \right)^{\frac{1}{2r}} \left(\sum_{x\in\mathbb{F}_p} \left| \sum_{1\le b\le B} \chi(x+b) \right|^{2r} \right)^{\frac{1}{2r}} \end{aligned}$$

We bound each of the three sums above in turn. Clearly, one has

$$\sum_{x\in\mathbb{F}_p} \nu_A(x) = \pi(A)H .$$

We will shortly apply Lemma 4.23 to show that

$$\sum_{x\in\mathbb{F}_p} \nu_A(x)^2 \le 2\pi(A)H , \tag{4.7}$$

but first we need to make a few estimates which involve the relevant quantities.

Our upper bound on A allows us to verify that $2AH < p$, which makes Lemma 4.23 applicable. Lemma 4.24 gives

$$\frac{2}{\pi(A)} \sum_{\substack{a\le A \\ a \text{ prime}}} \frac{\pi(a)-1}{a} < \frac{2}{3} .$$

Using (3.6) of [44], we have $\pi(A) \le 1.26A/\log A$ for $A > 1$ and therefore

$$\frac{\pi(A)}{H} \le \frac{1.26A}{H\log A} \le \frac{1.26}{dB\log A} \le \frac{1.26}{d(4r-1)\log A} \le \frac{1.26}{4(4\cdot 2-1)\log 4} < 0.1\,.$$

Now we see that

$$\frac{2}{\pi(A)H}\sum_{\substack{a\le A\\ a \text{ prime}}}(\pi(a)-1) \le \frac{2\pi(A)}{H} < 0.2\,.$$

Putting all this together, we have successfully verified (4.7) by invoking Lemma 4.23.

To bound the third sum, we apply Lemma 4.7; this gives

$$\sum_{x\in\mathbb{F}_p}\left|\sum_{1\le b\le B}\chi(x+b)\right|^{2r} \le B^{2r}p^{1/2}\left[\frac{1}{4}\left(\frac{4r}{B}\right)^r p^{1/2} + (2r-1)\right]\,.$$

Using the convexity of the logarithm and the fact that $B \ge 2r-1$ (in a manner similar to Lemma 4.14), together with the fact that $B+1 > 4rp^{\frac{1}{2r}}$, we have

$$\frac{1}{2}\left(\frac{4r}{B}\right)^r \le \left(\frac{4r}{B+1}\right)^r \le \frac{1}{p^{1/2}}\,,$$

and hence

$$\sum_{x\in\mathbb{F}_p}\left|\sum_{1\le b\le B}\chi(x+b)\right|^{2r} \le B^{2r}p^{1/2}\left(2r-\frac{1}{2}\right)\,.$$

All together, this gives

$$\sum_{x\in\mathbb{F}_p}\nu_A(x)\left|\sum_{1\le b\le B}\chi(x+b)\right| \le D_1\,\pi(A)^{1-\frac{1}{2r}}H^{1-\frac{1}{2r}}Bp^{\frac{1}{4r}}$$

with

$$D_1 = 2^{\frac{1}{2r}}\left(2r-\frac{1}{2}\right)^{\frac{1}{2r}} = (4r-1)^{\frac{1}{2r}}\,.$$

Therefore

$$\frac{1}{\pi(A)B}\sum_{x\in\mathbb{F}_p}\nu_A(x)\left|\sum_{1\le b\le B}\chi(x+b)\right| \;\le\; D_1\,H^{1-\frac{1}{r}}p^{\frac{1}{4r}}\left(\frac{H}{\pi(A)}\right)^{\frac{1}{2r}}\,.$$

Using (3.5) of [44] and some simple computation, provided $A \ge 3$ and $A \in \mathbb{Z}$, we have $\pi(A) \ge A/(1+\log A)$; using this, together with the bound

$$\begin{aligned}\log A &\le \left(\frac{1}{2}-\frac{1}{4r}\right)\log p - \log(3\sqrt{rd})\\ &< \left(\frac{1}{2}-\frac{1}{4r}\right)\log p - 1\,,\end{aligned}$$

allows us to estimate

$$\begin{aligned}\frac{H}{\pi(A)} &\leq \frac{H(\log A+1)}{A}\\ &\leq (d+1)B(\log A+1)\\ &\leq 4r(d+1)\left(\frac{1}{2}-\frac{1}{4r}\right)p^{\frac{1}{2r}}\log p\,.\end{aligned}$$

Therefore

$$\left(\frac{H}{\pi(A)}\right)^{\frac{1}{2r}} \leq D_2\, p^{\frac{1}{4r^2}}(\log p)^{\frac{1}{2r}}$$

with

$$D_2 = \left[4r(d+1)\left(\frac{1}{2}-\frac{1}{4r}\right)\right]^{\frac{1}{2r}} = ((d+1)(2r-1))^{\frac{1}{2r}}\,,$$

which leads to

$$\frac{1}{\pi(A)B}\sum_{x\in\mathbb{F}_p}\nu_A(x)\left|\sum_{1\leq b\leq B}\chi(x+b)\right| \;\leq\; D_1D_2\,H^{1-\frac{1}{r}}p^{\frac{r+1}{4r^2}}(\log p)^{\frac{1}{2r}} = D_1D_2E(H)\,.$$

Finally, using (4.6), this gives

$$|S_\chi(H)| \leq \left[((d+1)(2r-1)(4r-1))^{\frac{1}{2r}} + \frac{2C}{d^{1-\frac{1}{r}}}\right]E(H)\,.$$

Now we see that $|S_\chi(H)| \leq C\,E(H)$ provided

$$((d+1)(2r-1)(4r-1))^{\frac{1}{2r}} + \frac{2C}{d^{1-\frac{1}{r}}} \leq C\,. \tag{4.8}$$

Using the fact

$$d>4 \quad\Longrightarrow\quad 1-\frac{2}{d^{1-\frac{1}{r}}}>0\,,$$

and solving (4.8) for C allows us to see that (4.8) is equivalent to (4.5). ∎

Proof of Theorem 4.17. We apply Theorem 4.25 with $d=11$, $p_0=2\cdot 10^4$ and perform the necessary numerical computations, being careful to round up in our computations of values for $C(r)$. ∎

The choices of p_0 and d in the proof of Theorem 4.17 were designed to easily derive a widely applicable version of the character sum estimate with decent constants for all r. This will suit our purposes here. However, if one wanted to achieve a slightly better constant for a specific application, one would proceed as follows: for any given r and p_0, choose (or numerically estimate) the parameter d so as to minimize C.

5 Discriminant Bounds

Having laid the groundwork in chapters 3 and 4, in the present chapter we derive the sought-after discriminant bounds. The following result gives the inequalities to which we have alluded.

Theorem 5.1. *Let K be a Galois number field of odd prime degree ℓ and conductor f. Fix an integer $2 \leq k \leq 6$. There exists a computable constant $E(k)$ such*

$$E(k)(\ell - 1)^k (\log f)^{\frac{7}{2}} \leq f^{\frac{1}{4} - \frac{1}{4k}}$$

implies that K is not norm-Euclidean.

Table 5.1: Values of $E(k)$

k	$E(k)$
2	$5.2497 \cdot 10^3$
3	$8.3199 \cdot 10^3$
4	$1.8354 \cdot 10^4$
5	$4.2830 \cdot 10^4$
6	$1.0153 \cdot 10^5$

We note in passing that we could derive a similar inequality to that given in Theorem 5.1 for all $k \geq 2$, but as these results will not improve our ultimate discriminant bounds, we have opted to use the simplifying assumption of $k \leq 6$. Once Theorem 5.1 is established, the following discriminant bounds will easily follow.

Theorem 5.2. *Let K be a Galois number field of odd prime degree ℓ, conductor f, and discriminant Δ. There exists a computable constant C_ℓ such that if K is norm-Euclidean, then $f < C_\ell$ and $0 < \Delta < C_\ell^{\ell-1}$.*

Table 5.2: Conductor bounds when $\ell < 100$

ℓ	C_ℓ
3	10^{70}
5	10^{78}
7	10^{82}
11	10^{88}
13	10^{89}
17	10^{92}
19	10^{94}
23	10^{96}

ℓ	C_ℓ
29	10^{98}
31	10^{99}
37	10^{101}
41	10^{102}
43	10^{102}
47	10^{103}
53	10^{104}
59	10^{105}

ℓ	C_ℓ
61	10^{106}
67	10^{107}
71	10^{107}
73	10^{108}
79	10^{108}
83	10^{109}
89	10^{109}
97	10^{110}

First, we prove upper bounds on the quantities q_2 and r appearing in Theorem 3.1 using the character sum estimate from §4.2. The bound on q_2 that follows is weaker than the one derived in §4.1, but, like Lemma 4.16, it requires no additional hypothesis on q_1. In this chapter we will make use of both estimates.

Proposition 5.3. *Let χ be a non-principal Dirichlet character modulo $p \geq 10^{16}$. Denote by $q_1 < q_2$ the two smallest primes such that $\chi(q_1), \chi(q_2) \neq 1$. Then*

$$q_2 < 5000\, p^{1/3} (\log p)^{1/2}\,.$$

Proof. Suppose $p \geq 10^{16}$. Define

$$x := 5000\, p^{\frac{1}{3}} (\log p)^{\frac{1}{2}}\,,$$

and observe that $x < 4\, p^{\frac{7}{12}} < p$. If $q_2 < x$, then there is nothing to prove and hence we may assume $q_2 \geq x$. Therefore $\chi(n) = 1$ for all integers $n < x$ with $(n, q_1) = 1$.

We give upper and lower bounds on the sum

$$\sum_{\substack{n<x \\ (n,q_1)=1}} \chi(n)\,,$$

and proceed similar to the proof of Lemma 4.16, except that we use the character sum estimate given in Theorem 4.17 instead of the one given in Theorem 2.1. We obtain

$$(1 - q_1^{-1})x - 1 < 5 \left(1 + q_1^{-2/3}\right) x^{2/3} p^{1/9} (\log p)^{1/6}\,,$$

which leads to

$$x < 16.4\, x^{2/3} p^{1/9} (\log p)^{1/6}\,,$$

and hence

$$x < 4500\, p^{1/3} (\log p)^{1/2}\,,$$

a contradiction. ∎

The following gives an upper bound on the quantity r appearing in Theorem 3.1. Larger values of q_1 lead to better constants, and so we provide two sets of constants.

Theorem 5.4. *Let χ be a non-principal Dirichlet character modulo f of order $\ell > 2$, where f is a prime with $f \geq 2 \cdot 10^4$. Let $q_1 < q_2$ be primes. Fix an ℓ-th root of unity ζ, and $k \in \mathbb{Z}$ with $k \geq 2$. There exists a computable positive constant $D(k)$ such that whenever f is large enough so that*

$$\left(D(k)(\ell-1)\right)^k (\log f)^{\frac{1}{2}} \leq 4 f^{\frac{1}{4}}\,,$$

there exists $r \in \mathbb{Z}^+$ such that $(r, q_1 q_2) = 1$, $\chi(r) = \zeta$, and

$$r \leq \left(D(k)\,(\ell-1)\right)^k\; f^{\frac{k+1}{4k}} (\log f)^{\frac{1}{2}}\,.$$

Table 5.3: Values of $D(k)$ when $2 \leq k \leq 15$, with q_1 arbitrary

k	$D_1(k)$	k	$D_1(k)$
2	89.1550	9	20.0133
3	43.1104	10	19.2768
4	31.9985	11	18.6920
5	26.9751	12	18.2160
6	24.1129	13	17.8211
7	22.2635	14	17.4877
8	20.9692	15	17.2028

Table 5.4: Values of $D(k)$ when $2 \leq k \leq 15$, assuming $q_1 > 100$

k	$D_2(k)$	k	$D_2(k)$
2	13.5958	9	3.3154
3	6.6415	10	3.2075
4	5.0420	11	3.1215
5	4.3220	12	3.0513
6	3.9103	13	2.9929
7	3.6430	14	2.9434
8	3.4550	15	2.9011

Proof. Define the constant $C(k)$ as in Theorem 4.17, and two more quantities which depend on q_1, q_2, k:

$$K_1 := \left(1 + q_1^{1/k-1}\right)\left(1 + q_2^{1/k-1}\right), \quad K_2 := \left(1 - q_1^{-1}\right)\left(1 - q_2^{-1}\right)$$

Fix a constant $D(k)$ such that

$$D(k) \geq \frac{K_1\,(1 + C(k)^{-1})}{K_2}\,C(k)\,.$$

We will show that the theorem holds for this choice of $D(k)$. Set

$$x := (D(k)(\ell - 1))^k\, f^{\frac{k+1}{4k}} (\log f)^{\frac{1}{2}}\,,$$

and suppose there are no positive integers $n < x$ with $(n, q_1q_2) = 1$ and $\chi(n) = \zeta$. We observe that $x \leq 4f^{\frac{1}{2}+\frac{1}{4k}}$ by hypothesis; in particular, we find $x < 4f^{5/8} < f$.

Applying Lemma 3.14 we have:

$$\#\{n < x \mid (n, q_1q_2) = 1\} \;\leq\; (\ell - 1) \max_{k=1,\ldots,\ell-1} \left| \sum_{\substack{n<x \\ (n,q_1q_2)=1}} \chi^k(n) \right| \tag{5.1}$$

We bound the left-hand side of (5.1) from below:

$$\#\{n < x \mid (n, q_1q_2) = 1\} > (1 - q_1^{-1})(1 - q_2^{-1})x - 2$$

Now we wish to bound the character sum on right-hand side of (5.1) from above. We fix an arbitrary $k \in \{1, \ldots, \ell - 1\}$, and for notational convenience, we will write χ in place of χ^k. We have:

$$\sum_{\substack{n<x \\ (n,q_1q_2)=1}} \chi(n) = \sum_{n<x} \chi(n) - \chi(q_1) \sum_{n<x/q_1} \chi(n) - \chi(q_2) \sum_{n<x/q_2} \chi(n) + \chi(q_1q_2) \sum_{n<x/q_1q_2} \chi(n)$$

Now we apply the triangle inequality to the above and invoke Theorem 4.17 to bound each term. This gives

$$\left| \sum_{\substack{n<x \\ (n,q_1q_2)=1}} \chi^k(n) \right| \leq C(k) \left(1 + q_1^{1/k-1}\right)\left(1 + q_2^{1/k-1}\right) x^{1-1/k} f^{\frac{k+1}{4k^2}} (\log f)^{\frac{1}{2k}}\,.$$

Combining everything, we have

$$\begin{aligned} K_2\, x &< (\ell-1)K_1\, C(k)x^{1-\frac{1}{k}} f^{\frac{k+1}{4k^2}} (\log f)^{\frac{1}{2k}} + 2 \\ &\leq (\ell-1)K_1 \left(1 + C(k)^{-1}\right) C(k)x^{1-\frac{1}{k}} f^{\frac{k+1}{4k^2}} (\log f)^{\frac{1}{2k}}\,, \end{aligned}$$

which leads to

$$x < \left(D(k)(\ell-1)\right)^k f^{\frac{k+1}{4k}} (\log f)^{\frac{1}{2}}\,,$$

a contradiction. ∎

Before proving Theorem 5.1 in full, we establish a similar result which holds when q_1 is small.

Theorem 5.5. *Let K be a Galois number field of odd prime degree ℓ and conductor f. Fix an integer $2 \leq k \leq 8$. Let q_1 denote the smallest rational prime that is inert in K, and suppose $q_1 < 100$. There exists a computable constant $E'(k)$ such*

$$E'(k)(\ell-1)^k \log f \leq f^{\frac{5}{12}-\frac{1}{4k}}$$

implies that K is not norm-Euclidean.

Table 5.5: Values of $E'(k)$

k	$E'(k)$
2	$3.7041 \cdot 10^{10}$
3	$3.7337 \cdot 10^{11}$
4	$4.8855 \cdot 10^{12}$
5	$6.6559 \cdot 10^{13}$
6	$9.1598 \cdot 10^{14}$
7	$1.2634 \cdot 10^{16}$
8	$1.7420 \cdot 10^{17}$

Proof. Our choice of $E'(k)$ will be such that $E'(k) \geq 10^3$. Using this, together with $\ell \geq 3$, $k \geq 2$, our hypothesis leads to the inequality $4 \cdot 10^3 \log f \leq f^{5/12}$ which implies $f \geq 10^{10}$. It equally clear from our hypothesis that $f > \ell^2$. Using Lemma 2.3, we may assume f is a prime with $f \equiv 1 \pmod{\ell}$.

We adopt the notation from the hypothesis of Theorem 3.1. Set $\zeta = \chi(q_2)^{-1}$. Using Theorem 3.1, we must show there exists $r \in \mathbb{Z}^+$ such that $(r, q_1 q_2) = 1$, $\chi(r) = \zeta$, which also satisfies an additional inequality. We will prove the bound

$$932\, q_2 r < f\,, \tag{5.2}$$

which will establish the result in all cases; in particular, we observe that

$$(2.1)(97)(\log 97) < 932\,.$$

Using Proposition 5.3 and Theorem 5.4 we obtain

$$932\, q_2 r < E'(k)(\ell-1)^k f^{\frac{7}{12}+\frac{1}{4k}} \log f\,,$$

where

$$E'(k) = (932)(5000) D_1(k)^k\,.$$

Thus our hypothesis implies (5.2). ∎

Proof of Theorem 5.1. Our ultimate choice of $E(k)$ will be such that $E(k) \geq 10^3$. Using this, together with $k \geq 2$, $\ell \geq 3$, our hypothesis leads to the inequality $4 \cdot 10^3 (\log f)^{\frac{7}{2}} \leq f^{\frac{1}{4}}$ which easily implies $f \geq 10^{40}$. One also checks that $f > \ell^2$, from the hypothesis. Using Lemma 2.3, we may assume f is a prime with $f \equiv 1 \pmod{\ell}$.

We adopt the notation from the hypothesis of Theorem 3.1. Set $\zeta = \chi(q_2)^{-1}$. For now we will assume $q_1 > 100$. (We deal with the case where q_1 is small later in the proof.) Using Theorem 3.1, we must show there exists $r \in \mathbb{Z}^+$ such that $(r, q_1 q_2) = 1$, $\chi(r) = \zeta$, which also satisfies the inequality

$$2.1\, q_1 q_2 r \log q_1 \leq f\,.$$

In estimating $\log q_1$, we can't really hope to do better than a multiple of $\log f$, so we needn't work too hard; using Lemma 4.16, we find

$$q_1 < q_2 < 2\, f^{1/2} \log f < f^{9/16}$$

which implies

$$\log q_1 < \frac{9}{16} \log f\,.$$

Corollary 4.4 gives

$$q_1 q_2 < 24\, f^{1/2} (\log f)^2\,,$$

Thus, we have

$$2.1\, q_1 q_2 \log q_1 < 28.4\, f^{1/2} (\log f)^3\,.$$

Using Theorem 5.4 we obtain an integer r with the desired properties such that

$$r \leq (D_2(k)\,(\ell-1))^k\ f^{\frac{k+1}{4k}} (\log f)^{\frac{1}{2}}\,,$$

provided

$$(D_2(k)(\ell-1))^k\,(\log f)^{\frac{1}{2}} \leq 4 f^{\frac{1}{4}}\,. \tag{5.3}$$

We define the constant

$$E(k) := 28.4\, D_2(k)^k\,.$$

Combining everything, and using the hypothesis, we have the bound

$$2.1\, q_1 q_2 r \log q_1 < E(k)(\ell-1)^k (\log f)^{\frac{7}{2}} f^{\frac{3k+1}{4k}} \leq f\,.$$

It remains to verify (5.3), but having defined $E(k)$, we easily verify that this condition is automatic from our hypothesis as one has:

$$\begin{aligned}(D_2(k)(\ell-1))^k\,(\log f)^{\frac{1}{2}} &\leq E(k)(\ell-1)^k(\log f)^{\frac{1}{2}}\\ &\leq \frac{f^{\frac{1}{4}-\frac{1}{4k}}}{(\log f)^3}\\ &< f^{\frac{1}{4}}\end{aligned}$$

This completes the proof in the case that $q_1 > 100$.

Now we consider what happens when $q_1 \leq 100$. Provided $k \leq 6$, one shows that the condition in our hypothesis implies the condition in Theorem 5.5 (using the fact that $f \geq 10^{40}$). ∎

Proof of Theorem 5.2. If $\ell = 3$, then set $k = 5$, and otherwise set $k = 4$. Apply Theorem 5.1.[1] ∎

[1]Since any choice of k will give a discriminant bound, we merely test numerically the values of $k \in [2, 6]$ to see which choice gives the least exponent in the bound. At around roughly $\ell \approx 130$, the choice of $k = 3$ starts giving a better bound than $k = 4$, and given the trend, it appears that after a certain point, $k = 2$ will be the best choice.

6 Consequences of the Generalized Riemann Hypothesis

In §6.1 we give some results for character non-residues, assuming the GRH. In §6.2 we use these results to obtain sharper versions of theorems 5.1 and 5.2, assuming the GRH.

6.1 GRH Bounds for Non-Residues

In [2], Bach proves an explicit version of a theorem due to Ankeny (see [1]) regarding the least element outside of a given non-trivial subgroup of $(\mathbb{Z}/m\mathbb{Z})^\star$. The main idea behind Bach's proof appears in [37], but to obtain explicit results there are many details to work out; Bach uses a slightly different kernel and introduces a parameter in order to achieve good numerical results. Using the tables in [2], we obtain the following special case which will be useful to us in the present context.

Theorem 6.1 (Bach, 1990)**.** *Assume the GRH. Let χ be a non-principal Dirichlet character modulo $m \geq 10^8$, and denote by q_1 the smallest prime such that $\chi(q_1) \neq 1$. Then*

$$q_1 < (1.17 \log m - 6.36)^2 < 1.37(\log m)^2 .$$

We will follow Bach's approach to give a bound on q_2 and r. In §6.1.1 we give some explicit formulas relating sums over prime powers to sums over zeros of L-functions, and in §6.1.2 we give some GRH estimates for the sums over zeros.

Then in §6.1.3 and §6.1.4 we give GRH upper bounds on q_2 and r, respectively. Although the results we derive in this chapter undoubtably hold in more generality, we will not hesitate to specialize to our situation if it affords us certain technical conveniences.

6.1.1 An explicit formula

Lemma 6.2. *Let χ be a Dirichlet character modulo m. (Here we allow the possibility that χ is the principal character or even that $m = 1$.) For $x > 1$ and $a \in (0,1)$, we have*

$$-\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \frac{x^s}{(s+a)^2}\frac{L'(s,\chi)}{L(s,\chi)}\,ds = \sum_{n<x}\chi(n)\Lambda(n)(n/x)^a\log(x/n)\,.$$

Proof. This is Lemma 4.2 of [2]. We provide only a brief sketch here. We plug the Dirichlet series

$$\frac{L'(s,\chi)}{L(s,\chi)} = -\sum_{n=1}^{\infty}\chi(n)\Lambda(n)n^{-s}$$

into the right-hand side above and interchange the order of summation and integration. Next, we use the fact that for $y > 0$ one has

$$\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\frac{y^s}{(s+a)^2}\,ds = \begin{cases} y^{-a}\log y & \text{if } y > 1 \\ 0 & \text{otherwise} \end{cases},$$

and the result follows. ∎

Lemma 6.3. *Let χ be a non-principal primitive Dirichlet character modulo m with $\chi(-1) = 1$. For $x > 1$ and $a \in (0,1)$ we have*

$$\begin{aligned}\sum_{n<x}\chi(n)\Lambda(n)(n/x)^a\log(x/n) \;=\; & -\sum_{\rho \text{ of } L_\chi}\frac{x^\rho}{(\rho+a)^2} - \sum_{n=1}^{\infty}\frac{x^{-2n}}{(a-2n)^2} - \frac{1}{a^2} \\ & -\frac{\log x}{x^a}\left(\frac{L_\chi'}{L_\chi}\right)(-a) - \frac{1}{x^a}\left(\frac{L_\chi'}{L_\chi}\right)'(-a)\end{aligned}$$

Proof. Formally, this follows immediately by evaluating the integral in Lemma 6.2 by residues. For more details, see Lemma 4.4 of [2]. ∎

Lemma 6.4. *For $x > 1$ and $a \in (0,1)$ we have*

$$\begin{aligned}\sum_{n<x} \Lambda(n)(n/x)^a \log(x/n) &= \frac{x}{(a+1)^2} - \sum_{\rho \text{ of } \zeta} \frac{x^\rho}{(\rho+a)^2} - \sum_{n=1}^{\infty} \frac{x^{-2n}}{(a-2n)^2} \\ &\quad - \frac{\log x}{x^a}\left(\frac{\zeta'}{\zeta}\right)(-a) - \frac{1}{x^a}\left(\frac{\zeta'}{\zeta}\right)'(-a)\end{aligned}$$

Proof. This is similar to the previous result. ∎

For our bounds on q_2 and r, we will need to exclude certain primes from consideration; this will require the following estimate:

Lemma 6.5. *Let $u \in \mathbb{Z}^+$.*

$$\sum_{\substack{n<x \\ (n,u)>1}} \Lambda(n)(n/x)^a \log(x/n) \leq \omega(u)(\log x)^2\,,$$

where $\omega(u)$ denotes the number of distinct prime factors of u.

Proof. If $u = 1$, the result is trivial. Suppose $u = p_1^{a_1} \dots p_t^{a_t}$. Then

$$\begin{aligned}\sum_{\substack{n<x \\ (n,u)>1}} \Lambda(n) &= \sum_{k=1}^{t} \sum_{a=1}^{\lfloor \log_{p_k} x \rfloor} \log p_k \\ &\leq \sum_{k=1}^{t} \log x \\ &= t \log x\,.\end{aligned}$$

The result easily follows. ∎

6.1.2 Sums over zeros

In order to prove our results, we will need to bound the sums over zeros appearing in lemmas 6.3 and 6.4. Eventually we will take character combinations of the formulas appearing in these lemmas as well, and so it will be useful to bound the corresponding sum over all the zeros of the Dedekind zeta function of a number field K.

Let K be a number field of discriminant Δ with r_1 real embeddings and $2r_2$ complex embeddings. We define

$$\psi_K(s) := \frac{r_1 + r_2}{2}\,\psi\left(\frac{s}{2}\right) + \frac{r_2}{2}\,\psi\left(\frac{s+1}{2}\right) - \frac{1}{2}\,[K:\mathbb{Q}]\log\pi\,, \quad \psi(s) := \frac{\Gamma'(s)}{\Gamma(s)}\,,$$

where $\Gamma(s)$ is the usual gamma function. In particular,

$$\psi_{\mathbb{Q}}(s) = \frac{1}{2}\left(\psi\left(\frac{s}{2}\right) - \log\pi\right).$$

In order to expedite the proofs of this section, we quote some formulae, all of which can be derived from (5.9) of [31]. For all $s \in \mathbb{C}$, we have:

$$\frac{\zeta_K'(s)}{\zeta_K(s)} = B_K + \sum_{\rho \text{ of } \zeta_K}\left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) - \frac{1}{2}\log|\Delta| - \frac{1}{s} - \frac{1}{s-1} - \psi_K(s) \quad (6.1)$$

$$\frac{\zeta'(s)}{\zeta(s)} = B + \sum_{\rho \text{ of } \zeta}\left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) - \frac{1}{s} - \frac{1}{s-1} - \psi_{\mathbb{Q}}(s) \quad (6.2)$$

If χ is a non-principal primitive Dirichlet character modulo f, with $\chi(-1) = 1$, then for all $s \in \mathbb{C}$ we have:

$$\frac{L_\chi'(s)}{L_\chi(s)} = B_\chi + \sum_{\rho \text{ of } L_\chi}\left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) - \frac{1}{2}\log f - \psi_{\mathbb{Q}}(s) \quad (6.3)$$

Each sum above is over the non-trivial zeros ρ of the corresponding functions, and is absolutely and uniformly convergent on compact subsets of $\mathbb{C}$. Henceforth we adopt the notation that ρ will always denote a non-trivial zero with $0 < \Re(\rho) < 1$. Each equation involves a constant B which can be difficult to estimate. Fortunately, in all three cases this constant can be eliminated from the equation as follows. Provided the sum is taken in symmetric order[1] , one has

$$B + \sum_{\rho \text{ of } \zeta}\frac{1}{\rho} = 0\,, \quad (6.4)$$

and similarly for B_K and B_χ. See [16] for a simple argument which gives this result for the constant B. The corresponding result for B_K follows by a similar argument and was first exploited by Stark to give lower bounds for discriminants

[1]Taking the sum in symmetric order means: $\sum_{\rho} = \lim_{T\to\infty} \sum_{\substack{\rho=\sigma+it \\ |t|<T}}$

(see [49, 50]). The analogous result for B_χ is not obvious; in fact, it wasn't known until the introduction of the Weil formulas (see [55, 56]). Plugging $s = 1$ into (6.3) and comparing against (2.3.1) of [27] gives a proof of this result. See [42, 43, 41] for results regarding the use of explicit formulae to obtain discriminant bounds.

We begin with a lemma which goes back to Landau (see [32]).

Lemma 6.6. *Let χ be a primitive Dirichlet character modulo f with $\chi(-1) = 1$. Then for $\sigma \in \mathbb{R}$, we have*

$$\sum_{\rho \text{ of } L_\chi} \left(\frac{1}{\sigma - \rho} + \frac{1}{\sigma - \overline{\rho}} \right) = \log f + 2\Re \frac{L'(\sigma, \chi)}{L(\sigma, \chi)} + 2\psi_{\mathbb{Q}}(\sigma)\,.$$

Proof. We substitute $s = \sigma$ into (6.3) and add the result to it's conjugate. The result now follows upon invoking the fact that

$$\Re \left(B_\chi + \sum_{\rho \text{ of } L_\chi} \frac{1}{\rho} \right) = 0\,. \ \blacksquare$$

Lemma 6.7. *Suppose χ is a non-principal primitive Dirichlet character modulo f with $\chi(-1) = 1$. Assume the RH and the GRH for $L(s, \chi)$. For $a \in (0, 1)$ we have*

$$\sum_{\rho \text{ of } \zeta, L_\chi} \frac{1}{|\rho + a|^2} \leq \frac{1}{2a+1} \left(\log f + 2 \left(\frac{1}{a+1} + \frac{1}{a} \right) + 4\psi_{\mathbb{Q}}(a+1) \right)\,.$$

Proof. We consider the following two formulae:

$$\begin{aligned} \sum_{\rho \text{ of } \zeta} \left(\frac{1}{\sigma - \rho} + \frac{1}{\sigma - \overline{\rho}} \right) &= 2\frac{\zeta'(\sigma)}{\zeta(\sigma)} + 2\left(\frac{1}{\sigma} + \frac{1}{\sigma - 1} \right) + 2\psi_{\mathbb{Q}}(\sigma) \\ \sum_{\rho \text{ of } L_\chi} \left(\frac{1}{\sigma - \rho} + \frac{1}{\sigma - \overline{\rho}} \right) &= \log f + 2\Re \frac{L'(\sigma, \chi)}{L(\sigma, \chi)} + 2\psi_{\mathbb{Q}}(\sigma) \end{aligned}$$

The second formula above is Lemma 6.6 and the first can be proved in exactly the same manner. Setting $\sigma = a + 1$ and supposing that $\Re(\rho) = 1/2$, we find:

$$\frac{1}{|\rho + a|^2} = \frac{1}{2a+1} \left(\frac{1}{\sigma - \rho} + \frac{1}{\sigma - \overline{\rho}} \right) \tag{6.5}$$

To complete the proof, we combine everything above and note that

$$\frac{\zeta'(\sigma)}{\zeta(\sigma)} + \Re \frac{L'(\sigma, \chi)}{L(\sigma, \chi)} < 0\,,$$

by considering the Dirichlet series for $(\zeta'/\zeta + L'_\chi/L_\chi)(s)$. $\blacksquare$

We give a special case of the previous lemma:

Lemma 6.8. *Suppose χ is a non-principal primitive Dirichlet character modulo f with $\chi(-1) = 1$. Assume the RH and the GRH for $L(s, \chi)$. We have*

$$\sum_{\rho \ of \ \zeta, L_\chi} \frac{1}{\left|\rho + \frac{1}{2}\right|^2} \leq \frac{1}{2} \log f + 0.437 \, .$$

Proof. Use the fact

$$\psi_{\mathbb{Q}}(3/2) \approx -1.1153 \tag{6.6}$$

and apply the previous lemma with $a = 1/2$. ∎

Having completed the desired estimates over the zeros of $\zeta(s)$ and $L(s, \chi)$, we turn turn to $\zeta_K(s)$.

Lemma 6.9. *Let K be a number field with discriminant Δ. Then we have*

$$\sum_{\rho \ of \ \zeta_K} \frac{1}{\sigma - \rho} + \frac{1}{\sigma - \overline{\rho}} = \log |\Delta| + 2 \left(\frac{1}{\sigma} + \frac{1}{\sigma - 1} \right) + 2\psi_K(\sigma) + 2 \frac{\zeta_K'(\sigma)}{\zeta_K(\sigma)} \, .$$

Proof. This is exactly analogous to Lemma 6.6. ∎

Lemma 6.10. *Let K be a number field with discriminant Δ. Suppose the GRH holds for $\zeta_K(s)$. For $a \in (0, 1)$ we have*

$$\sum_{\rho \ of \ \zeta_K} \frac{1}{|\rho + a|^2} \ < \ \frac{1}{2a+1} \left[\log |\Delta| + 2 \left(\frac{1}{a+1} + \frac{1}{a} \right) + 2\psi_K(a+1) \right] \, .$$

Proof. Let $\sigma = a + 1$. Applying Lemma 6.6 and using (6.5) gives

$$\sum_{\rho \text{ of } \zeta_K} \frac{1}{|\rho + a|^2} = \frac{1}{2a+1} \left[\log |\Delta| + 2 \left(\frac{1}{a+1} + \frac{1}{a} \right) + 2\psi_K(a+1) + 2 \frac{\zeta_K'(a+1)}{\zeta_K(a+1)} \right] \, .$$

The result follows upon observing that $\zeta_K'(\sigma)/\zeta_K(\sigma) < 0$ as in Lemma 6.7. ∎

We give a special case of the previous lemma:

Lemma 6.11. *Let K be a totally real number field with discriminant Δ. Suppose the GRH holds for $\zeta_K(s)$. We have*

$$\sum_{\rho \ of \ \zeta_K} \frac{1}{\left|\rho + \frac{1}{2}\right|^2} < \frac{1}{2} \left(\log |\Delta| + \frac{16}{3} + 2 \, \psi_{\mathbb{Q}}(3/2) \, [K : \mathbb{Q}] \right) \, .$$

Proof. Since $r_1 = [K : \mathbb{Q}]$, $r_2 = 0$, we have

$$\psi_K(s) = [K : \mathbb{Q}]\psi_{\mathbb{Q}}(s)$$

The result now follows from the previous lemma upon setting $a = 1/2$. ∎

Now we specialize even further to our situation:

Lemma 6.12. *Let K be a totally real number field of degree ℓ and discriminant $\Delta = f^{\ell-1}$. Suppose the GRH holds for $\zeta_K(s)$. We have*

$$\sum_{\rho \text{ of } \zeta_K} \frac{1}{\left|\rho + \frac{1}{2}\right|^2} < \frac{1}{2}\left[(\ell - 1)\log f - 2.23\,\ell + 5.34\right] .$$

Proof. We apply the previous lemma, using the approximation given in (6.6). ∎

6.1.3 An upper estimate on q_2

Theorem 6.13. *Let χ be a non-principal Dirichlet character modulo $m \geq 10^9$ with $\chi(-1) = 1$. Assume the RH and the GRH for $L(s, \chi)$. Denote by $q_1 < q_2$ the two smallest primes such that $\chi(q_1), \chi(q_2) \neq 1$. Then*

$$q_2 < 2.5(\log m)^2 .$$

We establish a series of results, building up to the proof of the above theorem.

Lemma 6.14. *Let χ be a non-principal Dirichlet character modulo m with $\chi(-1) = 1$. For $a \in (0, 1)$ and $x > 0$ we have*

$$\begin{aligned}\frac{x}{(a+1)^2} + \frac{1}{a^2} \;=\; & \sum_{\rho \text{ of } \zeta} \frac{x^\rho}{(\rho + a)^2} - \sum_{\rho \text{ of } L_\chi} \frac{x^\rho}{(\rho + a)^2} \\ & + \sum_{\substack{n < x \\ \chi(n) \neq 1}} (1 - \chi(n))\Lambda(n)(n/x)^a \log(x/n) \\ & + \frac{\log x}{x^a}\left[\left(\frac{\zeta'}{\zeta}\right)(-a) - \left(\frac{L'_\chi}{L_\chi}\right)(-a)\right] \\ & + \frac{1}{x^a}\left[\left(\frac{\zeta'}{\zeta}\right)'(-a) - \left(\frac{L'_\chi}{L_\chi}\right)'(-a)\right]\end{aligned}$$

Proof. Subtract Lemma 6.3 from Lemma 6.4. ∎

Lemma 6.15. *Let χ be a non-principal primitive Dirichlet character modulo f with $\chi(-1) = 1$. For $a \in (0,1)$ we have*

$$\left|\left(\frac{\zeta'}{\zeta}\right)(-a) - \left(\frac{L'_\chi}{L_\chi}\right)(-a)\right| \leq (a+2) \sum_{\rho \text{ of } \zeta, L_\chi} \frac{1}{|(\rho+a)(2-\rho)|} + 2\left|\frac{\zeta'(2)}{\zeta(2)}\right| + \frac{1}{a} + \frac{1}{a+1} + \frac{3}{2}.$$

Proof. We begin with the formulas which hold for all $s \in \mathbb{C}$ provided the sums are taken in symmetric order:

$$\left(\frac{\zeta'}{\zeta}\right)(s) = \sum_{\rho \text{ of } \zeta} \frac{1}{s-\rho} - \frac{1}{s} - \frac{1}{s-1} - \psi_{\mathbb{Q}}(s) \tag{6.7}$$

$$\left(\frac{L'_\chi}{L_\chi}\right)(s) = \sum_{\rho \text{ of } L_\chi} \frac{1}{s-\rho} - \frac{1}{2}\log f - \psi_{\mathbb{Q}}(s) \tag{6.8}$$

Formulas (6.7) and (6.8) are obtained from (6.2) and (6.3) respectively by applying the facts $\sum_{\rho \text{ of } \zeta} \rho^{-1} + B = 0$ and $\sum_{\rho \text{ of } L_\chi} \rho^{-1} + B_\chi = 0$. Plugging $s = 2$ into (6.7) and subtracting it from itself, and similarly for (6.8), yields:

$$\left(\frac{\zeta'}{\zeta}\right)(s) = \left(\frac{\zeta'}{\zeta}\right)(2) + \sum_\rho \left(\frac{1}{s-\rho} - \frac{1}{2-\rho}\right) + \frac{3}{2} - \frac{1}{s} - \frac{1}{s-1} + \psi_{\mathbb{Q}}(2) - \psi_{\mathbb{Q}}(s)$$

$$\left(\frac{L'_\chi}{L_\chi}\right)(s) = \left(\frac{L'_\chi}{L_\chi}\right)(2) + \sum_\rho \left(\frac{1}{s-\rho} - \frac{1}{2-\rho}\right) + \psi_{\mathbb{Q}}(2) - \psi_{\mathbb{Q}}(s)$$

Using the above, together with the fact

$$\frac{1}{-a-\rho} - \frac{1}{2-\rho} = -\frac{a+2}{(\rho+a)(2-\rho)},$$

we can write

$$\left(\frac{\zeta'}{\zeta}\right)(-a) - \left(\frac{L'_\chi}{L_\chi}\right)(-a) = (a+2)\left(\sum_{\rho \text{ of } L_\chi} \frac{1}{(\rho+a)(2-\rho)} - \sum_{\rho \text{ of } \zeta} \frac{1}{(\rho+a)(2-\rho)}\right) + \left(\frac{\zeta'}{\zeta}\right)(2) - \left(\frac{L'_\chi}{L_\chi}\right)(2) + \frac{3}{2} + \frac{1}{a} + \frac{1}{a+1}.$$

The result follows upon taking absolute values and using the fact that

$$\left|\left(\frac{L_\chi'}{L_\chi}\right)(2)\right| \le \left|\left(\frac{\zeta'}{\zeta}\right)(2)\right| . \ \blacksquare$$

Lemma 6.16. *Suppose $a \in (0,1)$ and $\Re(\rho) = 1/2$. Then*

$$\frac{1}{|(\rho+a)(2-\rho)|} \le \frac{1}{|\rho+a|^2} .$$

Proof. Use $|2-\rho| \ge |\rho+a|$. $\blacksquare$

Lemma 6.17. *Let χ be a non-principal primitive Dirichlet character modulo f with $\chi(-1) = 1$. For $a \in (0,1)$ we have*

$$\left|\left(\frac{\zeta'}{\zeta}\right)'(-a) - \left(\frac{L_\chi'}{L_\chi}\right)'(-a)\right| < \sum_\rho \frac{1}{|\rho+a|^2} + \frac{1}{a^2} + \frac{1}{(a+1)^2} ,$$

where the sum is taken over all zeros ρ of $\zeta(s)$ and $L(s,\chi)$.

Proof. We start by differentiating (6.7) and (6.8); this gives

$$\left(\frac{\zeta'}{\zeta}\right)'(s) = -\sum_\rho \frac{1}{(s-\rho)^2} + \frac{1}{s^2} + \frac{1}{(s-1)^2} - \psi_{\mathbb{Q}}'(s) \tag{6.9}$$

$$\left(\frac{L_\chi'}{L_\chi}\right)'(s) = -\sum_\rho \frac{1}{(s-\rho)^2} - \psi_{\mathbb{Q}}'(s) , \tag{6.10}$$

which allows us to write

$$\left(\frac{\zeta'}{\zeta}\right)'(-a) - \left(\frac{L_\chi'}{L_\chi}\right)'(-a) = \sum_{\rho \text{ of } L_\chi} \frac{1}{(\rho+a)^2} - \sum_{\rho \text{ of } \zeta} \frac{1}{(\rho+a)^2} + \frac{1}{a^2} + \frac{1}{(a+1)^2} .$$

The result follows. $\blacksquare$

Proposition 6.18. *Let χ be a non-principal primitive Dirichlet character modulo f with $\chi(-1) = 1$. Assume the RH and the GRH for $L(s,\chi)$. We define*

$$\sum_\rho := \sum_{\rho \ of \ \zeta, L_\chi} \frac{1}{\left|\rho + \frac{1}{2}\right|^2} .$$

For $x > 0$ we have

$$\begin{aligned} \frac{x}{9/4} + 4 \le \sqrt{x}\sum_\rho + 2 \sum_{\substack{n<x \\ \chi(n)\neq 1}} \Lambda(n)(n/x)^{1/2}\log(x/n) \\ + \frac{\log x}{\sqrt{x}}\left(\frac{5}{2}\sum_\rho + 2\left|\frac{\zeta'(2)}{\zeta(2)}\right| + \frac{25}{6}\right) + \frac{1}{\sqrt{x}}\left(\sum_\rho + \frac{40}{9}\right) \end{aligned}$$

Proof. Set $a = 1/2$. Combine lemmas 6.14, 6.15, 6.16, and 6.17. ∎

Proof of Theorem 6.13. The result for a general character follows from the corresponding result for primitive characters and hence we may assume χ is a primitive character modulo f.

Define $x := 2.5(\log f)^2$. Since $f \geq 10^9$, we have $x > 1073$. By way of contradiction, suppose that $\chi(n) = 1$ for all $n < x$ with $(n, q_1) = 1$. Under this assumption, we apply Lemma 6.5 with $u = q_1$ gives

$$\sum_{\substack{n<x \\ \chi(n)\neq 1}} \Lambda(n)(n/x)^{1/2}\log(x/n) \leq (\log x)^2\,.$$

Combining the above with Proposition 6.18 and dividing by $\sqrt{x}$ yields

$$\frac{\sqrt{x}}{9/4} + \frac{4}{\sqrt{x}} \leq \sum_{\rho} + \frac{2(\log x)^2}{\sqrt{x}} + \frac{\log x}{x}\left[\frac{5}{2}\sum_{\rho} + 2\left|\frac{\zeta'(2)}{\zeta(2)}\right| + \frac{25}{6}\right] + \frac{1}{x}\left[\sum_{\rho} + \frac{40}{9}\right].$$

By Lemma 6.8, we have

$$\sum_{\rho} \leq \frac{1}{2}\log f + 0.437\,,$$

and in particular,

$$\frac{1}{\sqrt{x}}\sum_{\rho} \leq \frac{1}{3}\,.$$

We see

$$\begin{aligned}\frac{\log x}{x}\left[\frac{25}{6}\right] + \frac{1}{x}\left[\sum_{\rho} + \frac{40}{9}\right] &\leq \frac{1}{\sqrt{x}}\left(\frac{\log x}{\sqrt{x}}\cdot\frac{25}{6} + \frac{1}{3} + \frac{1}{\sqrt{x}}\frac{40}{9}\right) \\ &< \frac{4}{\sqrt{x}}\,,\end{aligned}$$

and therefore

$$\frac{\sqrt{x}}{9/4} \leq \sum_{\rho} + \frac{2(\log x)^2}{\sqrt{x}} + \frac{\log x}{x}\left[\frac{5}{2}\sum_{\rho} + 2\left|\frac{\zeta'(2)}{\zeta(2)}\right|\right].$$

We have

$$\frac{1}{\sqrt{x}}\left[\frac{5}{2}\sum_{\rho} + 2\left|\frac{\zeta'(2)}{\zeta(2)}\right|\right] < 0.869$$

and

$$\frac{\log x}{\sqrt{x}} \leq 0.214$$

which leads to

$$\frac{\sqrt{x}}{9/4} \leq \frac{1}{2}\log f + 0.437 + \frac{2(\log x)^2}{\sqrt{x}} + 0.186\,.$$

Now we observe

$$\frac{2(\log x)^2}{\sqrt{x}} \;\leq\; 2.98\,.$$

All together, we have

$$\frac{\sqrt{x}}{9/4} \;\leq\; \frac{1}{2}\log f + 3.61$$

This leads to:

$$\begin{aligned}\sqrt{x} &\leq \frac{9}{8}(\log f) + 8.13\\ &\leq 1.52\,\log f\end{aligned}$$

Squaring both sides yields

$$x \leq 2.32\,(\log f)^2\,,$$

a contradiction. ∎

6.1.4 An upper estimate on r

Theorem 6.19. *Let K be a Galois number field of degree ℓ and conductor $f \geq 10^8$, where ℓ and f are both odd primes and $f \equiv 1 \pmod{\ell}$. Assume the GRH for $\zeta_K(s)$. Denote by $q_1 < q_2$ the two smallest rational primes that are inert in K. Let χ be a primitive Dirichlet character modulo f of order ℓ. Fix any ℓ-th root of unity ω. There exists $r \in \mathbb{Z}^+$ such that $(r, q_1q_2) = 1$, $\chi(r) = \omega$, and*

$$r < 2.5(\ell - 1)^2(\log f)^2\,.$$

Lemma 6.20. *Let χ be a non-principal Dirichlet character modulo a prime p of order ℓ with $\chi(-1) = 1$. Fix any ℓ-th root of unity ω. For $a \in (0,1)$ and $x \in (1,p)$*

we have

$$\begin{aligned}\frac{x}{(a+1)^2}+\frac{1}{a^2} &= \sum_{k=1}^{\ell}\omega^{-k}\sum_{\rho\ of\ L_{\chi^k}}\frac{x^\rho}{(\rho+a)^2}\\ &\quad+\ell\sum_{\substack{n<x\\ \chi(n)=\omega}}\Lambda(n)(n/x)^a\log(x/n)\\ &\quad+\frac{\log x}{x^a}\left[\left(\frac{\zeta'}{\zeta}\right)(-a)+\sum_{k=1}^{\ell-1}\omega^{-k}\left(\frac{L'_{\chi^k}}{L_{\chi^k}}\right)(-a)\right]\\ &\quad+\frac{1}{x^a}\left[\left(\frac{\zeta'}{\zeta}\right)'(-a)+\sum_{k=1}^{\ell-1}\omega^{-k}\left(\frac{L'_{\chi^k}}{L_{\chi^k}}\right)'(-a)\right].\end{aligned}$$

Proof. First we note that χ^k for $k=1,\dots,\ell-1$ are all non-principal primitive characters as χ is a character modulo a prime p of order ℓ; moreover, $\chi^\ell(n)=1$ for all $n<x$ as $x<p$. Multiplying the identity

$$\sum_{k=1}^{\ell}\omega^{-k}\chi^k(n)=\begin{cases}\ell & \chi(n)=\omega\\ 0 & \text{otherwise}\end{cases}$$

by

$$g(x,n):=\Lambda(n)(n/x)^a\log(x/n)$$

and summing over all $n<x$ yields

$$\sum_{n<x}g(x,n)\sum_{k=1}^{\ell}\omega^{-k}\chi^k(n)=\ell\sum_{\substack{n<x\\ \chi(n)=\omega}}g(x,n).$$

Interchanging the order of summation gives

$$\sum_{k=1}^{\ell}\omega^{-k}\sum_{n<x}g(x,n)\chi^k(n)=\ell\sum_{\substack{n<x\\ \chi(n)=\omega}}g(x,n).$$

Now we apply Lemma 6.3 and Lemma 6.4 and use the facts:

$$\sum_{k=1}^{\ell}\omega^{-k}=0,\quad \sum_{k=1}^{\ell-1}\omega^{-k}=-1.$$

The result follows. ∎

Lemma 6.21. *Let χ be a non-principal Dirichlet character modulo a prime p of order ℓ with $\chi(-1) = 1$. Fix any ℓ-th root of unity ω. For $a \in (0,1)$ we have*

$$\left| \left(\frac{\zeta'}{\zeta}\right)(-a) + \sum_{k=1}^{\ell-1} \omega^{-k} \left(\frac{L'_{\chi^k}}{L_{\chi^k}}\right)(-a) \right| \leq (a+2) \sum_{\rho} \frac{1}{|(\rho+a)(2-\rho)|} + \ell \left| \frac{\zeta'(2)}{\zeta(2)} \right| + \frac{1}{a} + \frac{1}{a+1} + \frac{3}{2},$$

where the sum is taken over all non-trivial zeros ρ of $L(s, \chi^k)$ for $k = 1, \ldots, \ell$.

Proof. Using the formulas given in the proof of Lemma 6.15 allows us to write:

$$\begin{aligned} &\left(\frac{\zeta'}{\zeta}\right)(-a) + \sum_{k=1}^{\ell-1} \omega^{-k} \left(\frac{L'_{\chi^k}}{L_{\chi^k}}\right)(-a) \\ &= (a+2) \sum_{k=1}^{\ell} \omega^{-k} \sum_{\rho \text{ of } L_{\chi^k}} \frac{1}{(\rho+a)(2-\rho)} \\ &\quad + \left(\frac{\zeta'}{\zeta}\right)(2) + \sum_{k=1}^{\ell-1} \left(\frac{L'_{\chi^k}}{L_{\chi^k}}\right)(2) + \frac{3}{2} + \frac{1}{a} + \frac{1}{a+1} \end{aligned}$$

The result follows in a similar manner as Lemma 6.15. ∎

Lemma 6.22. *Let χ be a non-principal Dirichlet character modulo a prime p of order ℓ with $\chi(-1) = 1$. Fix any ℓ-th root of unity ω. For $a \in (0,1)$ we have*

$$\left| \left(\frac{\zeta'}{\zeta}\right)'(-a) + \sum_{k=1}^{\ell-1} \omega^{-k} \left(\frac{L'_{\chi^k}}{L_{\chi^k}}\right)'(-a) \right| \leq \sum_{\rho} \frac{1}{|\rho+a|^2} + \frac{1}{a^2} + \frac{1}{(a+1)^2},$$

where the sum is taken over all non-trivial zeros ρ of $L(s, \chi^k)$ for $k = 1, \ldots, \ell$.

Proof. Using (6.9) and (6.10) allows us to write

$$\begin{aligned} &\left(\frac{\zeta'}{\zeta}\right)'(-a) + \sum_{k=1}^{\ell-1} \omega^{-k} \left(\frac{L'_{\chi^k}}{L_{\chi^k}}\right)'(-a) \\ &= \frac{1}{a^2} + \frac{1}{(a+1)^2} - \sum_{k=1}^{\ell} \omega^{-k} \sum_{\rho \text{ of } L_{\chi^k}} \frac{1}{(\rho+a)^2}. \end{aligned}$$

∎

Proposition 6.23. *Let χ be a non-principal Dirichlet character modulo a prime p of order ℓ with $\chi(-1)=1$. Fix any ℓ-th root of unity ω. Denote by K the unique degree ℓ subfield of $\mathbb{Q}(\zeta_p)$. Suppose that the GRH holds for $\zeta_K(s)$. We define*

$$\sum_{\rho} := \sum_{\rho} \frac{1}{\left|\rho+\frac{1}{2}\right|^2},$$

where the sum is taken over all non-trivial zeros of $\zeta_K(s)$. For $x \in (1,p)$ we have

$$\begin{aligned}\frac{x}{9/4}+4 \;\leq\; \sqrt{x}\sum_{\rho} + \ell \sum_{\substack{n<x\\ \chi(n)=\omega}} \Lambda(n)(n/x)^{1/2}\log(x/n) \\ + \frac{\log x}{\sqrt{x}}\left(\frac{5}{2}\sum_{\rho}+\ell\left|\frac{\zeta'(2)}{\zeta(2)}\right|+\frac{25}{6}\right)+\frac{1}{\sqrt{x}}\left(\sum_{\rho}+\frac{40}{9}\right).\end{aligned}$$

Proof. The field K was defined so that

$$\zeta_K(s) = \zeta(s)\prod_{k=1}^{\ell-1} L(s,\chi^k).$$

Thus $\sum_\rho$ can also be thought of as the sum over the non-trivial zeros of $L(s,\chi^k)$ for $k=1,\dots,\ell$ (counting multiplicities). Now set $a=1/2$ and combine lemmas 6.20, 6.21, 6.16, 6.22. ∎

Proof of Theorem 6.19. Define $x := 2.5(\ell-1)^2(\log f)^2$. Since $f \geq 10^8$ and $\ell \geq 3$, we have $x > 3393$. By way of contradiction, suppose that $\chi(n) \neq \omega$ for all $n<x$ with $(n, q_1q_2)=1$. Under this assumption, we apply Lemma 6.5 with $u=q_1q_2$ gives

$$\sum_{\substack{n<x\\ \chi(n)=\omega}} \Lambda(n)(n/x)^{1/2}\log(x/n) \leq 2(\log x)^2.$$

Combining the above with Proposition 6.23 and dividing by $\sqrt{x}$ yields:

$$\frac{\sqrt{x}}{9/4}+\frac{4}{\sqrt{x}} \leq \sum_{\rho}+\frac{2\ell(\log x)^2}{\sqrt{x}}+\frac{\log x}{x}\left[\frac{5}{2}\sum_{\rho}+\ell\left|\frac{\zeta'(2)}{\zeta(2)}\right|+\frac{25}{6}\right]+\frac{1}{x}\left[\sum_{\rho}+\frac{40}{9}\right]$$

By Lemma 6.12, we have

$$\sum_{\rho} \leq \frac{1}{2}\left[(\ell-1)\log f - 2.23\,\ell + 5.34\right],$$

and in particular,

$$\frac{1}{\sqrt{x}} \sum_{\rho} \leq \frac{1}{2\sqrt{2.5}} .$$

We see

$$\begin{aligned} \frac{\log x}{x} \left[\frac{25}{6}\right] + \frac{1}{x} \left[\sum_{\rho} + \frac{40}{9}\right] &\leq \frac{1}{\sqrt{x}} \left(\frac{\log x}{\sqrt{x}} \cdot \frac{25}{6} + \frac{1}{2\sqrt{2.5}} + \frac{1}{\sqrt{x}} \frac{40}{9} \right) \\ &< \frac{4}{\sqrt{x}} , \end{aligned}$$

and therefore

$$\frac{\sqrt{x}}{9/4} \leq \sum_{\rho} + \frac{2\ell (\log x)^2}{\sqrt{x}} + \frac{\log x}{x} \left[\frac{5}{2} \sum_{\rho} + \ell \left| \frac{\zeta'(2)}{\zeta(2)} \right| \right] .$$

We have

$$\frac{1}{\sqrt{x}} \left[\frac{5}{2} \sum_{\rho} + \ell \left| \frac{\zeta'(2)}{\zeta(2)} \right| \right] < 0.82$$

and

$$\frac{\log x}{\sqrt{x}} \leq 0.14 ,$$

which leads to

$$\frac{\sqrt{x}}{9/4} \leq \frac{1}{2} \left[(\ell - 1) \log f - 2.23\, \ell + 5.34 \right] + \frac{2\ell (\log x)^2}{\sqrt{x}} + 0.12 .$$

Now we observe

$$\frac{2\ell (\log x)^2}{\sqrt{x}} \leq 2.27 \ell .$$

All together, we have

$$\begin{aligned} \frac{\sqrt{x}}{9/4} &\leq \frac{1}{2} \left[(\ell - 1) \log f - 2.23\, \ell + 5.34 \right] + 2.27\ell + 0.12 \\ &\leq \frac{1}{2} (\ell - 1)(\log f) + 1.16\ell + 2.79 \end{aligned}$$

This leads to:

$$\begin{aligned} \sqrt{x} &\leq \frac{9}{8} (\ell - 1)(\log f) + 2.61\ell + 6.28 \\ &\leq 1.51 (\ell - 1) \log f \end{aligned}$$

Squaring both sides yields

$$x \leq 2.3 (\ell - 1)^2 (\log f)^2 ,$$

a contradiction. ∎

6.2 GRH Bounds for Norm-Euclidean Fields

In this section we derive GRH versions of theorems 5.1 and 5.2. First we deal separately with the situation where q_1 is small.

Theorem 6.24. *Let K be a Galois number field of odd prime degree ℓ and conductor f. Assume the GRH for $\zeta_K(s)$. Let q_1 denote the smallest rational prime which is inert in K. Suppose $q_1 < 100$. If*

$$5825(\ell-1)^2(\log f)^4 < f\,,$$

then K is not norm-Euclidean.

Proof. Set $A = 5825$. One checks that our hypothesis implies $f \geq 10^9$ and $f > \ell^2$. By Lemma 2.3 we know that f is a prime with $f \equiv 1 \pmod{\ell}$. We adopt the notation from the statement of Theorem 3.1. Since $q_1 < 100$, we have $q_1 \leq 97$, and by theorems 6.13 and 6.19, we have

$$\begin{aligned} q_2 &< 2.5(\log f)^2\,, && (6.11)\\ r &< 2.5(\ell-1)^2(\log f)^2\,; && (6.12) \end{aligned}$$

hence we have

$$\begin{aligned} 2.1\, q_1 q_2 r \log q_1 &< (2.1)(97)(2.5)(\log f)^2(2.5)(\ell-1)^2(\log f)^2(\log 97)\\ &< A(\ell-1)^2(\log f)^4\,. \end{aligned}$$

If $q_1 \neq 2, 3, 7$, then it follows from Theorem 3.1 that the condition given in our hypothesis is sufficient. If $q_1 = 7$, then we observe that

$$\begin{aligned} 3\, q_1 q_2 r \log q_1 &< (3)(7)(2.5)(\log f)^2(2.5)(\ell-1)^2(\log f)^2(\log 7)\\ &< A(\ell-1)^2(\log f)^4\,. \end{aligned}$$

Now we deal with the special case where $q_1 = 2$, $q_2 = 3$. Our hypothesis gives

$$(\ell-1) < \frac{1}{\sqrt{A}}\,\frac{f^{1/2}}{(\log f)^2}\,.$$

In order to use Theorem 3.12, we estimate

$$\begin{aligned} 72(\ell-1)f^{1/2}\log 4f + 35 &< \frac{72}{\sqrt{A}}\frac{\log 4f}{(\log f)^2}\, f + 35 \\ &< 0.1f + 35 \\ &< f\,; \end{aligned}$$

thus the theorem applies. When $q_1 = 3$, $q_2 = 5$, we use a similar estimate to conclude that

$$507(\ell-1)f^{1/2}\log 9f + 448 < .4f + 448 < f\,,$$

and hence Theorem 3.12 applies again.

The remaining cases fall under conditions 4 and 5 of Theorem 3.1. We will prove the bound

$$5\,q_2 r < f\,,$$

which will deal with all remaining cases. From the estimates (6.11) and (6.12) we have

$$\begin{aligned} 5\,q_2 r &< 32(\ell-1)^2(\log f)^4 \\ &< A(\ell-1)^2(\log f)^4 \\ &< f\,. \end{aligned}$$

This completes the proof. ∎

Corollary 6.25. *Let K be a cubic Galois number field with conductor $f \geq 6\cdot 10^9$. Assume the GRH for $\zeta_K(s)$. Let q_1 denote the smallest rational prime which is inert in K. If $q_1 < 100$, then K is not norm-Euclidean.*

Theorem 6.26. *Let K be a Galois number field of odd prime degree ℓ and conductor f. Assume the GRH for $\zeta_K(s)$. If*

$$38(\ell-1)^2(\log f)^6 \log\log f < f\,,$$

then K is not norm-Euclidean.

Proof. As $\ell \geq 3$, the hypothesis implies $f \geq 10^{10}$. We will apply Theorem 3.1 as in the proof of Theorem 6.24. Applying theorems 6.1, 6.13, and 6.19, we have:

$$\begin{aligned} q_1 &\leq (1.17 \log f - 6.3)^2 \\ q_2 &\leq 2.5(\log f)^2 \qquad (6.13) \\ r &\leq 2.5(\ell - 1)^2 (\log f)^2 \qquad (6.14) \end{aligned}$$

For the moment, we assume $q_1 \neq 2, 3, 7$. Combining everything, this gives

$$2.1\, q_1 q_2 r \log q_1 < 26.25(\ell - 1)^2 (1.17 \log f - 6.3)^2 \log(1.17 \log f - 6.3)(\log f)^4 .$$

Hence a sufficient condition is:

$$26.25(\ell - 1)^2 (1.17 \log f - 6.3)^2 \log(1.17 \log f - 6.3)(\log f)^4 \leq f \qquad (6.15)$$

The condition given in our hypothesis implies the above condition. To deal with the remaining cases, we note that (6.15) implies the condition given in the statement of Theorem 6.24; hence (6.15) is sufficient in all cases. ∎

Theorem 6.27. *Let K be a Galois number field of odd prime degree ℓ, conductor f, and discriminant Δ. Assume the GRH for $\zeta_K(s)$. There exists a computable constant C_ℓ such that if K is norm-Euclidean, then $f < C_\ell$ and $0 < \Delta < C_\ell^{\ell-1}$.*

Table 6.1: Conductor bounds when $\ell < 100$, assuming the GRH

ℓ	C_ℓ
3	10^{11}
5	10^{12}
7	10^{13}
11	10^{13}
13	10^{14}
17	10^{14}
19	10^{14}
23	10^{14}

ℓ	C_ℓ
29	10^{15}
31	10^{15}
37	10^{15}
41	10^{15}
43	10^{15}
47	10^{15}
53	10^{15}
59	10^{15}

ℓ	C_ℓ
61	10^{15}
67	10^{15}
71	10^{16}
73	10^{16}
79	10^{16}
83	10^{16}
89	10^{16}
97	10^{16}

Proof. This is a direct consequence of Theorem 6.26 after some simple computations. For $\ell \neq 3$, we apply the condition given in the statement of theorem to obtain the bounds given in the table. For $\ell = 3$, we apply the slightly more complicated condition (6.15) to find that $f < 7 \cdot 10^{10}$. ∎

7 Galois Cubic Fields

The main result of this chapter is the following:

Theorem 7.1. *Assuming the GRH, the norm-Euclidean Galois cubic fields are exactly those with*

$$\Delta = 7^2, 9^2, 13^2, 19^2, 61^2, 67^2, 103^2, 109^2, 127^2, 157^2 .$$

Without the GRH, there may be further norm-Euclidean fields, but we can bound their discriminants.

Theorem 7.2. *The fields listed in Theorem 7.1 are norm-Euclidean, and any remaining norm-Euclidean Galois cubic field must have discriminant* $\Delta = f^2$ *with* $f \equiv 1 \pmod 3$ *where* f *is a prime in the interval* $(10^{10}, 10^{70})$.

Theorem 7.2 follows upon combining Combining Theorem 3.11, Lemma 2.3, and Theorem 5.2. We use the remainder of this chapter to establish Theorem 7.1. Let K be a norm-Euclidean Galois cubic field with conductor f and discriminant Δ which is not any of the ten fields listed in the statement of Theorem 7.1. In light of Theorem 3.11, we may assume $f \geq 10^{10}$. Moreover, Lemma 2.3 allows us to conclude that $\Delta = f^2$ and that f is a prime with $f \equiv 1 \pmod 3$. By the proof of Theorem 6.27 we know $f < 7 \cdot 10^{10}$.

It remains to deal with the cases where $f \in (10^{10}, 7 \cdot 10^{10})$. Let χ be a primitive cubic character modulo f, and let q_1 denote the smallest prime such that $\chi(q_1) \neq 1$. By Corollary 6.25, to show that K is not norm-Euclidean, assuming $f \in (10^{10}, 7 \cdot 10^{10})$, it suffices to show $q_1 < 100$. Using the method of character evaluation described in §3.2.2, we obtain the following lemma which completes the proof of Theorem 7.1.

Lemma 7.3. *Suppose f is a prime with $f \equiv 1 \pmod 3$. Let χ be a cubic character modulo f, and denote by q_1 the smallest prime with $\chi(q_1) \neq 1$. If $f \leq 7 \cdot 10^{10}$, then $q_1 \leq 61$.*

The computation given in the above Lemma was carried out on an iMac with a 3.06 GHz Intel Core 2 Duo processor and 4 GB of RAM, running Mac OS 10.6. It took 8.4 days of CPU time to complete.

As an additional curiosity we have kept a list of record values of q_1. That is, each time we encounter a value of q_1 which is strictly greater than all previous values, we have outputted the values of f and q_1. Here are the results:

```
Record: f=7, q1=2
Record: f=31, q1=3
Record: f=307, q1=5
Record: f=643, q1=7
Record: f=5113, q1=11
Record: f=21787, q1=13
Record: f=39199, q1=17
Record: f=360007, q1=23
Record: f=4775569, q1=29
Record: f=10318249, q1=37
Record: f=65139031, q1=41
Record: f=387453811, q1=43
Record: f=913900417, q1=47
Record: f=2278522747, q1=53
Record: f=2741702809, q1=59
Record: f=25147657981, q1=61
```

Bibliography

[1] N. C. Ankeny. The least quadratic non residue. *Ann. of Math. (2)*, 55:65–72, 1952.

[2] Eric Bach. Explicit bounds for primality testing and related problems. *Math. Comp.*, 55(191):355–380, 1990.

[3] Gennady Bachman and Leelanand Rachakonda. On a problem of Dobrowolski and Williams and the Pólya-Vinogradov inequality. *Ramanujan J.*, 5(1):65–71, 2001.

[4] E. S. Barnes and H. P. F. Swinnerton-Dyer. The inhomogeneous minima of binary quadratic forms. I. *Acta Math.*, 87:259–323, 1952.

[5] E. S. Barnes and H. P. F. Swinnerton-Dyer. The inhomogeneous minima of binary quadratic forms. II. *Acta Math.*, 88:279–316, 1952.

[6] Enrico Bombieri. Counting points on curves over finite fields (d'après S. A. Stepanov). In *Séminaire Bourbaki, 25ème année (1972/1973), Exp. No. 430*, pages 234–241. Lecture Notes in Math., Vol. 383. Springer, Berlin, 1974.

[7] Andrew R. Booker. Quadratic class numbers and character sums. *Math. Comp.*, 75(255):1481–1492 (electronic), 2006.

[8] D. A. Burgess. On character sums and primitive roots. *Proc. London Math. Soc. (3)*, 12:179–192, 1962.

[9] D. A. Burgess. A note on the distribution of residues and non-residues. *J. London Math. Soc.*, 38:253–256, 1963.

[10] H. Chatland. On the Euclidean algorithm in quadratic number fields. *Bull. Amer. Math. Soc.*, 55:948–953, 1949.

[11] H. Chatland and H. Davenport. Euclid's algorithm in real quadratic fields. *Canadian J. Math.*, 2:289–296, 1950.

[12] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups. In *Number theory (New York, 1982)*, volume 1052 of *Lecture Notes in Math.*, pages 26–36. Springer, Berlin, 1984.

[13] Ivan Bjerre Damgård and Gudmund Skovbjerg Frandsen. Efficient algorithms for the gcd and cubic residuosity in the ring of Eisenstein integers. *J. Symbolic Comput.*, 39(6):643–652, 2005.

[14] H. Davenport. Euclid's algorithm in cubic fields of negative discriminant. *Acta Math.*, 84:159–179, 1950.

[15] H. Davenport. Indefinite binary quadratic forms, and Euclid's algorithm in real quadratic fields. *Proc. London Math. Soc. (2)*, 53:65–82, 1951.

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

[17] P. Erdös and C. Ko. Note on the Euclidean algorithm. *J. London Math. Soc.*, 13:3–8, 1938.

[18] John Friedlander. Primes in arithmetic progressions and related topics. In *Analytic number theory and Diophantine problems (Stillwater, OK, 1984)*, volume 70 of *Progr. Math.*, pages 125–134. Birkhäuser Boston, Boston, MA, 1987.

[19] Dennis Garbanati. Class field theory summarized. *Rocky Mountain J. Math.*, 11(2):195–225, 1981.

[20] C. F. Gauss. *Disquisitiones Arithmeticae*. 1801.

[21] H. J. Godwin. On the inhomogeneous minima of totally real cubic norm-forms. *J. London Math. Soc.*, 40:623–627, 1965.

[22] H. J. Godwin and J. R. Smith. On the Euclidean nature of four cyclic cubic fields. *Math. Comp.*, 60(201):421–423, 1993.

[23] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. The Clarendon Press Oxford University Press, New York, fifth edition, 1979.

[24] H. Heilbronn. On Euclid's algorithm in real quadratic fields. *Proc. Cambridge Philos. Soc.*, 34:521–526, 1938.

[25] H. Heilbronn. On Euclid's algorithm in cubic self-conjugate fields. *Proc. Cambridge Philos. Soc.*, 46:377–382, 1950.

[26] H. Heilbronn. On Euclid's algorithm in cyclic fields. *Canadian J. Math.*, 3:257–268, 1951.

[27] Yasutaka Ihara, V. Kumar Murty, and Mahoro Shimura. On the logarithmic derivatives of Dirichlet L-functions at $s = 1$. *Acta Arith.*, 137(3):253–276, 2009.

[28] Makoto Ishida. *The genus fields of algebraic number fields*. Lecture Notes in Mathematics, Vol. 555. Springer-Verlag, Berlin, 1976.

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

[30] W. Knorr. Problems in the interpretation of Greek number theory: Euclid and the "fundamental theorem of arithmetic". *Studies in Hist. and Philos. Sci.*, 7(4):353–368, 1976.

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

[32] Edmund Landau. Zur Theorie der Heckeschen Zetafunktionen, welche komplexen Charakteren entsprechen. *Math. Z.*, 4(1-2):152–162, 1919.

[33] Franz Lemmermeyer. The Euclidean algorithm in algebraic number fields. *Exposition. Math.*, 13(5):385–416, 1995.

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

[35] Daniel A. Marcus. *Number fields*. Springer-Verlag, New York, 1977. Universitext.

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

[37] Hugh L. Montgomery. *Topics in multiplicative number theory*. Lecture Notes in Mathematics, Vol. 227. Springer-Verlag, Berlin, 1971.

[38] Władysław Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer-Verlag, Berlin, second edition, 1990.

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

[40] Karl K. Norton. *Numbers with small prime factors, and the least kth power non-residue*. Memoirs of the American Mathematical Society, No. 106. American Mathematical Society, Providence, R.I., 1971.

[41] 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(1):119–141, 1990.

[42] Georges Poitou. Minorations de discriminants (d'après A. M. Odlyzko). In *Séminaire Bourbaki, Vol. 1975/76 28ème année, Exp. No. 479*, pages 136–153. Lecture Notes in Math., Vol. 567. Springer, Berlin, 1977.

[43] Georges Poitou. Sur les petits discriminants. In *Séminaire Delange-Pisot-Poitou, 18e année: (1976/77), Théorie des nombres, Fasc. 1 (French)*, pages Exp. No. 6, 18. Secrétariat Math., Paris, 1977.

[44] J. Barkley Rosser and Lowell Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6:64–94, 1962.

[45] Pierre Samuel. About Euclidean rings. *J. Algebra*, 19:282–301, 1971.

[46] Wolfgang M. Schmidt. Zur Methode von Stepanov. *Acta Arith.*, 24:347–367. (errata insert), 1973. Collection of articles dedicated to Carl Ludwig Siegel on the occasion of his seventy-fifth birthday, IV.

[47] Wolfgang M. Schmidt. *Equations over finite fields. An elementary approach*. Lecture Notes in Mathematics, Vol. 536. Springer-Verlag, Berlin, 1976.

[48] J. R. Smith. On Euclid's algorithm in some cyclic cubic fields. *J. London Math. Soc.*, 44:577–582, 1969.

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

[50] H. M. Stark. The analytic theory of algebraic numbers. *Bull. Amer. Math. Soc.*, 81(6):961–972, 1975.

[51] S. A. Stepanov. Elementary method in the theory of congruences for a prime modulus. *Acta Arith.*, 17:231–247, 1970.

[52] Ian Stewart and David Tall. *Algebraic number theory and Fermat's last theorem*. A K Peters Ltd., Natick, MA, third edition, 2002.

[53] P. L. Wantzel. Extraits des proces-verbaux des seances. *Soc. Philomatique de Paris*, pages 19–22, 1848.

[54] André Weil. On some exponential sums. *Proc. Nat. Acad. Sci. U. S. A.*, 34:204–207, 1948.

[55] André Weil. Sur les "formules explicites" de la théorie des nombres premiers. *Comm. Sém. Math. Univ. Lund [Medd. Lunds Univ. Mat. Sem.]*, 1952(Tome Supplementaire):252–265, 1952.

[56] André Weil. Sur les formules explicites de la théorie des nombres. *Izv. Akad. Nauk SSSR Ser. Mat.*, 36:3–18, 1972.