NORM-EUCLIDEAN CYCLIC FIELDS OF PRIME DEGREE

KEVIN J. MCGOWN

ABSTRACT. Let K be a cyclic number field of prime degree ℓ. Heilbronn showed that for a given ℓ there are only finitely many such fields that are norm-Euclidean. In the case of $\ell = 2$ all such norm-Euclidean fields have been identified, but for $\ell \neq 2$, little else is known. We give the first upper bounds on the discriminants of such fields when $\ell > 2$. Our methods lead to a simple algorithm which allows one to generate a list of candidate norm-Euclidean fields up to a given discriminant, and we provide some computational results.

1. INTRODUCTION

Let K be a number field with ring of integers $\mathcal{O}_K$, and denote by $N = N_{K/\mathbb{Q}}$ the absolute norm map. For brevity, we will sometimes use the term field to mean a number field. 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 $|N(\alpha - \gamma\beta)| < |N(\beta)|$. In the quadratic setting, it is known that there are only finitely many norm-Euclidean fields and they have been identified; namely, a number field of the form $K = \mathbb{Q}(\sqrt{d})$ with d squarefree is norm-Euclidean if and only if

$$d = -1, -2, -3, -7, -11, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\,.$$

In his third and final paper on the Euclidean algorithm (see [13]), Heilbronn proves a finiteness result for various classes of cyclic fields. For us, the most important part of Heilbronn's result states:

Theorem 1.1 (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 [9, 21, 10]):

Theorem 1.2 (Godwin & Smith, 1993)**.** *The norm-Euclidean Galois cubic fields with discriminant $|\Delta| < 10^8$ are exactly those with*

$$\Delta = 7^2, 9^2, 13^2, 19^2, 31^2, 37^2, 43^2, 61^2, 67^2, 103^2, 109^2, 127^2, 157^2\,.$$

Lemmermeyer has further verified that this list constitutes all fields with $|\Delta| < 2.5 \cdot 10^{11}$ (see [15]). We prove the following result, which gives an upper bound on the discriminant for the fields considered in Theorem 1.1.

Theorem 1.3. *Let ℓ be an odd prime. There exists computable constant C_ℓ such that if K is a Galois number field of odd prime degree ℓ, conductor f, and discriminant Δ, which is norm-Euclidean, then $f < C_\ell$ and $0 < \Delta < C_\ell^{\ell-1}$.*

2010 *Mathematics Subject Classification.* 11A05, 11L40, 11R16, 11R32, 11R80, 11Y40.

Key words and phrases. norm-Euclidean, cyclic fields, cubic fields, character sums.

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}

Table 1.1. Values of C_ℓ for primes $\ell < 100$

Although the results of the previous theorem represent a significant step forward, the magnitude of the constants leaves something to be desired, especially if one is interested in determining all such fields, for any fixed ℓ. As is frequently the case in estimates of number theoretic quantities, under the Generalized Riemann Hypothesis (GRH) one should be able to obtain much sharper results. This is the subject of a forthcoming paper (see [17]).

In order to prove Theorem 1.3, we derive explicit inequalities which guarantee the failure of the norm-Euclidean property. Our inequalities (see Theorem 3.1) involve the existence of small integers satisfying certain splitting and congruence conditions. This also leads to an algorithm (see §6.2) for tabulating a list of candidate norm-Euclidean Galois fields (of prime degree ℓ) up to a given discriminant. We have implemented this algorithm in the programming language C, thereby obtaining the following result:

Theorem 1.4. *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 $f \leq 10^{10}$. (Of course, some of these fields may not be norm-Euclidean.)*

ℓ	$f \leq 10^{10}$
3	7, 9, 13, 19, 31, 37, 43, 61, 67, 73, 103, 109, 127, 157
5	11, 31, 41
7	29, 43
11	23, 67, 331
13	53, 131
17	137
19	
23	47, 139
29	59

Table 1.2. Candidate norm-Euclidean fields of small degree

Amusingly, there are no norm-Euclidean Galois fields of degree 19 with $f \leq 10^{10}$. Notice that when $\ell = 3$, we cover all possible $|\Delta| < 10^{20}$ (as $\Delta = f^2$ in this case) and that our results are consistent with Theorem 1.2. In the case of $\ell = 3$, we know that exactly 13 of the fields listed are norm-Euclidean, $f = 73$ being the only spurious value (see [21]). In the case of $\ell = 5$, Godwin (see [8]) proved that $f = 11$ is norm-Euclidean and Cerri (see [4]) has verified this. Nothing seems to be known about the remaining fields in the table. It would be interesting to study these fields on a case-by-case basis to decide which among them are norm-Euclidean.[1] No effort has been made in this direction by the author, but this may be the subject of a future investigation.

Combining Theorems 1.2, 1.3, and 1.4 leads to the following result which represents the current state of knowledge for norm-Euclidean Galois cubic fields:

Theorem 1.5. *The Galois cubic fields with*

$$\Delta = 7^2, 9^2, 13^2, 19^2, 31^2, 37^2, 43^2, 61^2, 67^2, 103^2, 109^2, 127^2, 157^2$$

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* $(10^{10},\, 10^{70})$.

Finally, we mention that under the GRH we can significantly improve on the above result (see [17]).

2. Preliminaries

2.1. **The setup.** Throughout this paper, K will denote a Galois number field of odd prime degree ℓ, conductor f, and discriminant Δ, which is necessarily cyclic. By the conductor–discriminant formula, we have $\Delta = f^{\ell-1}$.

Recall that via class field theory, there is a one-to-one correspondence between cyclic extensions $K/\mathbb{Q}$ of conductor f and degree ℓ and cyclic groups $\langle\chi\rangle$ of order ℓ generated by primitive Dirichlet characters χ of conductor f and order ℓ. The choice of χ amounts to the choice of a primitive ℓ-th root of unity among the $\phi(\ell)$ possibilities, and this correspondence is such that a rational prime p splits in K if and only if $\chi(p) = 1$. Unless otherwise specified, χ will always denote a (fixed) character associated to K.

In establishing our results, it will be no restriction to assume that K has class number one, and hence we will do so throughout. In this case, genus theory tells us that either f is a prime with $f \equiv 1 \pmod{\ell}$, or $f = \ell^2$.

2.2. **Heilbronn's criterion.** We set

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

$$\mathcal{P} := \{n \in \mathbb{Z} \mid \gcd(n, f) = 1\,,\ x^\ell \equiv n \pmod f \text{ is soluble}\}\,,$$

and

$$\mathcal{S} := \{n \in \mathcal{P} \mid 1 \le n < f\,,\ n \notin \mathcal{N}\}\,.$$

Since K has class number one, an integer $n \neq 0$ lies in $\mathcal{N}$ if and only if ℓ divides the p-adic valuation of n for all primes p which are inert in K (i.e., all primes p for which $\chi(p) \neq 0, 1$). It follows that

$$\mathcal{S} = \{n \in \{1, \ldots, f-1\} \mid n = bc,\ (b, c) = 1,\ \chi(b) \neq 1,\ \chi(bc) = 1\}\,.$$

Although not stated in this way, Heilbronn proves the following [13]:

[1] Of course, to begin with, one could determine which have class number one.

Lemma 2.1 (Heilbronn's Criterion)**.** *Suppose $(f,\ell)=1$. 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 [6], turns the problem into one of additive number theory. For the sake of completeness, we provide the argument.

Proof. 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 $(f,\ell)=1$, we know 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. Conditions for the Failure of the Norm-Euclidean Property

Throughout this section, we assume that $(f,\ell)=1$ so that K is not the field with $f=\ell^2$. Denote by $q_1<q_2$ the two smallest rational primes that are inert in K. Building on the work of Heilbronn, we prove the following theorem, which gives various conditions under which K fails be norm-Euclidean.

Theorem 3.1. *Suppose that there exists $r\in\mathbb{Z}^+$ with*

$$(r,q_1q_2)=1,\quad \chi(r)=\chi(q_2)^{-1},$$

such that any of the following conditions hold:

(1) $rq_2k\not\equiv f\pmod{q_1^2},\quad k=1,\dots,q_1-1,$
$(q_1-1)(q_2r-1)\le f$

(2) $q_1\neq 2,3,\quad 3q_1q_2r\log q_1<f$

(3) $q_1\neq 2,3,7,\quad 2.1\,q_1q_2r\log q_1<f$

(4) $q_1=2,\ q_2\neq 3,\quad 3q_2r<f$

(5) $q_1=3,\ q_2\neq 5,\quad 5q_2r<f$

Then K is not norm-Euclidean.

The first condition in the above theorem places no restrictions on q_1 or q_2 but requires congruence conditions which hold "most of the time", although they can be rather awkward to verify. The remaining conditions resulted from an effort to remove these congruences.

Lemma 3.2. *If there exists $s\in\mathcal{S}$ such that $(q_1,s)=1$ and $(q_1-1)(s-1)\le f$, 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. Choose $u\in\{0,\dots,q_1-1\}$ so that $us\equiv f\pmod{q_1}$ and set $v=(f-us)/q_1$. One checks that $v\ge-(q_1-1)/q_1>-1$ and hence $v\ge0$. 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. 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 2.1 implies that K is not norm-Euclidean. ∎

Proposition 3.3. *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 3.2 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. ∎

When $q_1 \neq 2, 3$, we can eliminate the congruence condition of Proposition 3.3, but for a small price.

Proposition 3.4. *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 3.2 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 2.1 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

$$(u + nq_1)s < p_0 q_1 s < Bq_1 s \log q_1 \leq f\,.$$

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 2.1 gives the result. ∎

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

Lemma 3.5. *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 [20] with a small amount of computation.[2] Using this fact together with the hypothesis that $u < q$, one sees that it suffices to show

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

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 3.6. *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 3.2 we may assume $f = s + 2v$ with $2 \mid v$. In this case, we write $f = 3s + 2(v - s)$. If it were the case that $2 \mid (v - s)$, then we would have $2 \mid s$, 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 3.7. *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 3.2 we may assume $f = us + 3v$ with $0 < u < 3$, $v > 0$, and $3 \mid v$. 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 Theorem 3.1. If condition (1) holds, we apply Proposition 3.3 with $s = q_2 r$. If either of conditions (2) or (3) hold, then we apply Proposition 3.4 with $s = q_2 r$ and invoke Lemma 3.5. If conditions (4) or (5) hold, we apply Propositions 3.6 or 3.7 respectively. ∎

4. The Wildly Ramified Case

In the previous section we assumed that $(f, \ell) = 1$, which was reasonable since we were only neglecting at most one norm-Euclidean field for each ℓ. In this section we show that we were only neglecting one field in total!

Theorem 4.1. *Let K be a Galois number field of odd prime degree $\ell > 3$ and conductor f. If K is norm-Euclidean, then f is a prime with $f \equiv 1 \pmod{\ell}$.*

Note that by Theorem 1.2 the Galois cubic field of conductor 9 is norm-Euclidean. Apparently, Davenport was the first to establish the norm-Euclidean nature of this field (see [5]). One amusing consequence of all this is the following: there is exactly one wildly ramified norm-Euclidean Galois field of odd prime degree! In order to prove Theorem 4.1 we first establish two lemmas.

Lemma 4.2 (Variant of Heilbronn's Criterion)**.** *Suppose $f = \ell^2$. If one can write $\ell = a + b$ with $a, b > 0$ and $a, b \notin \mathcal{N}$, then K is not norm-Euclidean.*

[2] In fact, one can demonstrate this using the elementary methods given in Ch. XXII of [12] together with an explicit version of Stirling's formula if one is willing to do a little more computation.

Proof. The proof is similar to that of Lemma 2.1. We factor $\ell = u\pi^\ell$ in K where π is a first degree prime and u is a unit. There exists $\alpha \in \mathcal{O}_K$ such that $a \equiv \alpha \pmod{\pi}$ with $|N(\alpha)| < |N(\pi)| = \ell$. Conjugation gives $a \equiv \alpha^\sigma \pmod{\pi}$ for all embeddings $\sigma : K \to \mathbb{C}$, and hence $a \equiv a^\ell \equiv N(\alpha) \pmod{\ell}$. Since $|N(\alpha)| < \ell$, we have either $N(\alpha) = a$ or $N(\alpha) = a - \ell = -b$. Thus a or $-b$ lies in $\mathcal{N}$, a contradiction. ∎

Lemma 4.3. *Suppose $k \in \mathbb{Z}$ with $k \geq 5$. If $n_1, \ldots, n_k \in \mathbb{Z}$ with $1 = n_1 < n_2 < \cdots < n_k \leq 2k$, then $\#\{n_i n_j \mid 1 \leq i, j \leq k\} \geq 2k + 1$.*

Proof. We prove the result by induction on k. One checks the base case of $k = 5$ by hand. For the inductive step, suppose we have $1 = n_1 < n_2 < \cdots < n_k \leq 2k$ as in the hypothesis, and that the result holds for any smaller value of k.

If $n_k \neq n_{k-1} + 1$, then we have $1 = n_1 < n_2 < \cdots < n_{k-1} \leq 2(k-1)$ and we invoke the inductive hypothesis to obtain $2k - 1$ products. Augmenting these products with $n_{k-1}n_k$ and $n_k n_k$ gives the desired $2k+1$ products, which completes the proof in this case.

If $n_k = n_{k-1} + 1$, then the following $3k - 3$ products are distinct:

$$\begin{gathered} n_1n_1,\ n_2n_1,\ \ldots,\ n_kn_1, \\ n_2n_{k-1},\ n_3n_{k-1},\ \ldots,\ n_{k-1}n_{k-1}, \\ n_2n_k,\ n_3n_k,\ \ldots,\ n_kn_k, \end{gathered}$$

Since $k \geq 4$, we know $3k - 3 \geq 2k + 1$ and thus the proof is complete. ∎

Proof of Theorem 4.1. Suppose $f = \ell^2$ and $\ell \neq 3$. We will ultimately invoke Lemma 4.2 to show that K is not norm-Euclidean. For small values of ℓ we apply the lemma directly; for $\ell = 5$ we use the decomposition $2 + 3 = 5$, and for $\ell = 7$ we use $2 + 5 = 7$. Hence we may assume $\ell \geq 11$.

Let χ denote a primitive Dirichlet character modulo ℓ^2 of order ℓ so that for primes $p \neq \ell$ we have that p splits in K iff $\chi(p) = 1$ iff $p \in \mathcal{N}$. Let T denote the set of positive integers less than ℓ^2 which are coprime to ℓ.

It suffices to show that $\ell = a + b$ with $a, b > 0$ and $a, b \notin \mathcal{N}$. Suppose we cannot accomplish this. Then for each $a = 1, \ldots, (\ell - 1)/2$, one of $\{a, \ell - a\}$ is a norm and hence there are at least $k := (\ell - 1)/2$ norms in $\{1, \ldots, \ell - 1\}$; say $n_1, \ldots, n_k \in \mathcal{N}$ where $n_1 = 1$. Now Lemma 4.3 implies that there are at least ℓ norms in T. In light of this, we have $\#\{n \in T \mid \chi(n) = 1\} \geq \ell$, which is a clear contradiction as the aforementioned set has $\varphi(\ell^2)/\ell = \ell - 1$ elements. ∎

5. Discriminant Bounds

In light of Theorem 4.1 we may assume that $f \equiv 1 \pmod{\ell}$, provided we stay away from the cubic field with $f = 9$. Indeed, the reader will see that for any proof in this section it will be no restriction to assume $f > 9$.

5.1. Some special cases.

The goal in §5.1 is to prove the following proposition which treats 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.

Proposition 5.1. *Denote by $q_1 < q_2$ the two smallest rational primes that are inert in K. Suppose either of the following conditions hold:*

(1) $q_1 = 2$, $q_2 = 3$,
$72(\ell-1)f^{1/2}\log 4f + 35 \le f$

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

Then K is not norm-Euclidean.

The above inequalities are completely explicit, and for fixed ℓ they hold beyond some easily computed value of f. The following corollary is an example of the type of discriminant bound we can obtain from Proposition 5.1.

Corollary 5.2. *Suppose K is a norm-Euclidean Galois cubic field of conductor f. If the primes 2 and 3 are inert in K, then $f < 10^7$.*

First we prove a lemma about Dirichlet characters.

Lemma 5.3. *Suppose χ is a Dirichlet character modulo m of order ℓ. 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 5.4. *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. Given that $m \ge 2\cdot 10^4$, the explicit version of the Pólya–Vinogradov inequality given in [1] implies that for for any $y > 0$, we have

$$\left|\sum_{n<y}\chi(n)\right| \le m^{1/2}\log m\,. \tag{5.1}$$

We write

$$\sum_{\substack{n<x\\(n,p)=1}}\chi(n) = \sum_{n<x}\chi(n) - \chi(p)\sum_{n<x/p}\chi(n)\,. \tag{5.2}$$

Applying the triangle inequality to (5.2) and invoking (5.1) twice gives the result. ∎

Lemma 5.5. *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*

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

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

Proof. Using the orthogonality relations for characters, we find

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

We now observe that

$$S(A) := \frac{1}{\phi(q)} \sum_{\substack{\psi \\ \text{mod } q}} \sum_{a\in A} \overline{\psi}(a) = 1 - S(\overline{A}) ,$$

where $\overline{A} := (\mathbb{Z}/q\mathbb{Z})^* \setminus A$. Therefore $|S(A)| \leq \#A \leq \phi(q)/2$ if $\#A \leq \phi(q)/2$ and $|S(A)| \leq 1 + |S(\overline{A})| \leq 1 + \phi(q) - \#A \leq \phi(q)/2$ if $\#A \geq \phi(q)/2 + 1$. The result follows. ∎

Proof of Proposition 5.1. 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 5.3 we have:

$$\#\{n < x \mid n \text{ has property } (\star)\} \ \leq \ (\ell - 1) \max_{k=1,\ldots,\ell-1} \left| \sideset{}{^\star}\sum_{n<x} \chi^k(n) \right| \tag{5.3}$$

First we estimate the quantity on the left-hand side of (5.3) 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 (5.3) from above. By Lemma 5.4 and Lemma 5.5, we have

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

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 to the first. 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

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

and

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

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. ∎

5.2. **Upper bounds on q_1, q_2, and r.** Here we give bounds on the quantities q_1, q_2, and r appearing in Theorem 3.1. First we quote the following result, which is proved elsewhere:

Theorem 5.6. *Let χ be a non-principal Dirichlet character modulo a prime $p \geq 10^{19}$ having odd order. Suppose that $q_1 < q_2$ are the two smallest prime non-residues of χ. Then we have:*

1. $q_1 < 3.9\, p^{1/4} \log p$
2. $q_2 < 53\, p^{1/4} (\log p)^2$
3. $q_1 q_2 < 24\, p^{1/2} (\log p)^2$

The bound on q_1 above is due to Norton (see [19]), and the bounds on q_2 and the product $q_1 q_2$ are due to the author (see [16]). In order to bound r, we will use the character sum estimate (see Theorem 7.1) given in §7; however, we remark that Theorem 5.6 gives a stronger bound for q_1 and q_2 than one would achieve via Theorem 7.1.

Now we state and prove a result which gives an upper bound on r. Having dealt with the two special cases in §5.1, we do not need to impose any additional congruence conditions on r. Larger values of q_1 lead to better constants, and so we provide two sets of constants.

Proposition 5.7. *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*

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

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

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

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 5.1. Values of $D(k)$ when $2 \leq k \leq 15$, with q_1 arbitrary

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

Table 5.2. Values of $D(k)$ when $2 \leq k \leq 15$, assuming $q_1 > 100$

Proof. Define the constant $C(k)$ as in Theorem 7.1, 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

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

We will show that Proposition 5.7 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 $(n, q_1 q_2) = 1$ and $\chi(n) = \zeta$. We observe that $x \leq 4 f^{\frac{1}{2} + \frac{1}{4k}}$ by hypothesis; in particular, we find $x < 4 f^{5/8} < f$.

Applying Lemma 5.3 we have:

$$\#\{n < x \mid (n, q_1 q_2) = 1\} \;\le\; (\ell - 1) \max_{k=1,\dots,\ell-1} \left| \sum_{\substack{n<x \\ (n,q_1q_2)=1}} \chi^k(n) \right| \tag{5.4}$$

We bound the left-hand side of (5.4) from below:

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

Now we wish to bound the character sum on right-hand side of (5.4) from above. We fix an arbitrary $k \in \{1, \dots, \ell - 1\}$, and for notational convenience, we will write ψ in place of χ^k. We have:

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

Now we apply the triangle inequality to the above and invoke Theorem 7.1 to bound each term. This gives

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

Combining everything, we have

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

which leads to

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

a contradiction.[3] ∎

5.3. **The general case.** Having paved the way, we are ready to prove the following result from which Theorem 1.3 follows immediately.

Theorem 5.8. *Fix an integer $2 \le k \le 8$ and define $E(k)$ as in Table 5.3. If*

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

then K is not norm-Euclidean.

k	$E(k)$
2	$3.4936 \cdot 10^3$
3	$5.5369 \cdot 10^3$
4	$1.2215 \cdot 10^4$
5	$2.8503 \cdot 10^4$
6	$6.7566 \cdot 10^4$
7	$1.6095 \cdot 10^5$
8	$3.8375 \cdot 10^5$

Table 5.3. Values of $E(k)$

[3] Computation of the table of constants is routine. For the first set of constants, we use $q_1 \ge 2$, $q_2 \ge 3$, and for the second set we use $q_1 \ge 101$, $q_2 \ge 103$.

Proof of Theorem 1.3. If $\ell = 3$, then set $k = 5$. If $3 < \ell < 61$, then set $k = 4$. Otherwise set $k = 3$. Apply Theorem 5.8.[4] ∎

We note in passing that we could derive a similar inequality to that given in Theorem 5.8 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 $k \leq 8$.

Proof of Theorem 5.8. 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 $f \geq 10^{40}$. We adopt the notation from the hypothesis of Theorem 3.1, and set $\zeta = \chi(q_2)^{-1}$.

For now we will assume $q_1 > 100$. 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

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

Using Theorem 5.6, we have $q_1 q_2 < 24\, f^{1/2} (\log f)^2$, and $q_1 < 3.9\, f^{1/4} \log f < f^{3/8}$, which implies $\log q_1 < (3/8) \log f$. Thus, we have

$$2.1\, q_1 q_2 \log q_1 < 18.9\, f^{1/2} (\log f)^3\,.$$

Using Proposition 5.7 we obtain an integer r with the desired properties such that

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

provided

$$(D_2(k)(\ell - 1))^k (\log f)^{\frac{1}{2}} \leq 4 f^{\frac{1}{4}}\,. \tag{5.5}$$

We define the constant

$$E(k) := 18.9\, D_2(k)^k\,.$$

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 (5.5), 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 $q_1 \leq 100$. Having dealt with two special cases in §5.1, the remaining cases fall under conditions (2) through (5) of Theorem 3.1. Namely, 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

$$932\, q_2 r < f\,, \tag{5.6}$$

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

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

[4] Since any choice of k will give a discriminant bound, we merely test numerically the values of $k \in [2, 8]$ to see which choice gives the least exponent in the bound. It appears that after a certain point, $k = 2$ will be the best choice.

We apply Lemma 7 and Theorem 4 of [16] to find that $q_1 \leq 100$ implies $q_2 < 711\, p^{1/4} \log p$. Using Proposition 5.7 we obtain an integer r with the desired properties such that

$$r \leq \left(D_1(k)\,(\ell-1)\right)^k \; f^{\frac{k+1}{4k}} (\log f)^{\frac{1}{2}}\,,$$

provided

$$(D_1(k)(\ell-1))^k\,(\log f)^{\frac{1}{2}} \leq 4 f^{\frac{1}{4}}\,. \tag{5.7}$$

We obtain

$$932\, q_2 r < E'(k)(\ell-1)^k f^{\frac{1}{2}+\frac{1}{4k}} (\log f)^{\frac{3}{2}}\,,$$

where

$$E'(k) = (932)(711) D_1(k)^k\,.$$

To complete the proof, it suffices to show

$$E'(k)(\ell-1)^k f^{\frac{1}{2}+\frac{1}{4k}} (\log f)^{\frac{3}{2}} \leq f\,, \tag{5.8}$$

as (5.8) implies both (5.6) and (5.7).

But one checks that (5.8) follows from our hypothesis provided

$$\frac{E'(k)}{E(k)} \leq f^{1/4} (\log f)^2\,. \tag{5.9}$$

Finally, using the fact that $f \geq 10^{40}$ implies $f^{1/4}(\log f)^2 \geq 10^{13}$, an easy numerical computation shows that (5.9) holds for $k = 2, \dots, 8$. ∎

6. An Algorithm and Some Computations

In this section we give the algorithm to which we alluded in §1. In §6.1 we give the main idea behind the algorithm, in §6.2 we give a full statement of the algorithm, and in §6.3 we give some results obtained from our computations which lead to the proof of Theorem 1.4.

6.1. **Idea behind the algorithm.** Let us first state our aims in designing such an 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 $K \in \mathcal{F}_\ell(A,B)$. By Theorem 4.1, we only need to consider fields where f is a prime with $f \equiv 1 \pmod{\ell}$, except for the single field where $\ell = 3$ and $f = 9$.

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.

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, then an upper bound on the average number of character evaluations to find q_1, q_2, r as just described is: $\ell(2 + 2/(\ell-1))$.

This gives a rough heuristic for how many character evaluations are necessary. For example, when $\ell = 3$, it should take almost 9 character evaluations on average to prove that any given cubic field is not norm-Euclidean.[5] However, it is important to keep in mind that on occasion it may take many more character evaluations than the average.

Finally, thanks to a comment from the referee, we note that we don't actually have to evaluate the characters! Indeed, $\chi(p) = 1$ if and only if $p^{(f-1)/\ell} \equiv 1 \pmod{f}$ and $\chi(r) = \chi(q_2)^{-1}$ if and only if $(rq_2)^{(f-1)/\ell} \equiv 1 \pmod{f}$. Thus these conditions can be checked very quickly using fast modular exponentiation.

6.2. **Statement of the algorithm.** In the statement of Algorithm 1 below, a lowercase or uppercase latin letter will denote an element of $\mathbb{Z}$, and an uppercase script letter will denote a list of elements in $\mathbb{Z}$.

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

```
Generate a list $\mathcal{P}$ of all primes $p \le \max\{1000, \sqrt{B}\}$ 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
  $e \leftarrow (f-1)/\ell$
  $q_1 \leftarrow 0$; $q_2 \leftarrow 0$; $r \leftarrow 0$
  for $p \in \mathcal{P}$ do
    if $p \ge f$ then
      break
    end if
    if ($p^e \not\equiv 1 \pmod{f}$) then
      if $q_1 = 0$ then
        $q_1 \leftarrow p$
      else if $q_2 = 0$ then
        $q_2 \leftarrow p$
        $\mathcal{A} \leftarrow \{fk^{-1} \mod q_1^2 \mid k = 1, \ldots, q_1 - 1\}$
      else if $(pq_2)^e \equiv 1 \pmod{f}$ AND $(pq_2) \mod q_1^2 \notin \mathcal{A}$ 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 $\ell = 3$ AND $9 \in [A, B]$ then
  print 9
end if
```

Verifying the correctness of Algorithm 1 is straightforward. For a given f, our algorithm either finds q_1, q_2, and r satisfying the appropriate conditions or it doesn't;

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

if it doesn't, then that value of f is outputted. However, we do give a number of comments regarding the algorithm which we deem to be 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 for that matter.
(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) Lines 26 and 27 account for the "exceptional field" (see Theorem 4.1).

6.3. **Results of the computations.** We have implemented the algorithm in C, using NTL with GMP for large integer arithmetic. Running our program on all $f \leq 10^{10}$ gives the results in Table 6.1 below. The computation took 16.9 hours of CPU time using a MacBook Pro with a 2.26 GHz Intel Core 2 Duo processor and 4 GB of RAM, running Mac OS 10.6.[6]

Using Heilbronn's criterion (i.e., Lemma 2.1) directly on the fields in Table 6.1, which takes less than a minute, allows us to pair it down a bit, thereby obtaining Theorem 1.4. (For example, when $\ell = 5$ the decomposition $431 = 145 + 286$ makes Lemma 2.1 applicable and allows us to eliminate this field.)

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

Table 6.1. Output of Algorithm 1

In the cubic case, we provide 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
```

[6] Running the algorithm on all $f \leq 10^4$, which produces the same table, takes about 1 second!

```
f=9999999943, q1=5, q2=7, r=19
f=9999999967, q1=5, q2=7, r=11
```

7. An Explicit Version of Burgess' Character Sum Estimate

In this section, we prove an explicit version of a character sum estimate of Burgess (see [3]), following a method due to Iwaniec (see [14] and [7]). Booker proves a similar result when χ is quadratic (see [2]). The reader who is willing to accept Theorem 7.1 may skip the rest of this section.

Theorem 7.1. *Suppose χ is a non-principal Dirichlet character modulo a prime $p \geq 2 \cdot 10^4$. 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 7.1. 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. However, it seems that to drop it, at least in the current proof, one may have to accept the slightly worse exponent of $1/r$ on the $\log p$ term.

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 7.2.

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

Definition 7.3.

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

We seek a bound of the form $S_\chi(H) < C\, E(H)$. (An explicit way of choosing C will appear in the statement of Theorem 7.9.) 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 7.4. 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 7.5. *Suppose* $|S_\chi(H_0)| \leq C\,E(H_0)$ *for all* $H_0 < H$. *Fix* $H_0 = AB < H$. *Then*

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

Proof. Applying a shift $n \mapsto n + h$ with $1 \leq h \leq H_0$ 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 $|\theta| \leq 1$, 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

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

and hence

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

The result follows. ∎

Lemma 7.6. *Suppose* $a_1 \neq a_2$ *are prime and* $b \in \mathbb{Z}$. *Then the number of integer solutions* $(x, y) \in \mathbb{Z}^2$ *to the equation* $a_1 x - a_2 y = b$ *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 $a_1 x - a_2 y = b$ 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 7.7. *Fix $A \in \mathbb{Z}$ with $1 < A < p$. If $2AH \leq p$, then*

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

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

$$a_1 n_2 \equiv a_2 n_1 \pmod{p}$$

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 treat 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 7.6 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

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

This gives the result. ∎

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

Lemma 7.8. *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 what is essentially the main result of this section, from which Theorem 7.1 follows.

Theorem 7.9. *Suppose χ is a non-principal Dirichlet character modulo an odd prime p. Fix a positive integer $r \geq 2$. Suppose $d > 4$, $C \geq 1$, $p_0 \geq 2$ are real constants satisfying*

$$C^r p_0^{\frac{1}{4}-\frac{1}{4r}} (\log p_0)^{\frac{1}{2}} \geq 4d(d+1)r \tag{7.1}$$

and

$$C \geq \frac{((d+1)(2r-1)(4r-1))^{\frac{1}{2r}}}{\left(1 - \frac{2}{d^{1-\frac{1}{r}}}\right)} . \tag{7.2}$$

If

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

then for $p \geq p_0$ we have

$$|S_\chi(H)| \leq C\, E(H) .$$

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 (7.1).

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

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

We also have

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

In particular, using (7.1), we see that $A > d > 4$.

Applying Lemma 7.5 and our inductive hypothesis, we have

$$\begin{aligned} |S_\chi(H)| &\leq \frac{1}{\pi(A)B} \sum_{x \in \mathbb{F}_p} \nu_A(x) \left| \sum_{1 \leq b \leq B} \chi(x+b) \right| + 2C\, E(H_0) \\ &\leq \frac{1}{\pi(A)B} \sum_{x \in \mathbb{F}_p} \nu_A(x) \left| \sum_{1 \leq b \leq B} \chi(x+b) \right| + \frac{2C}{d^{1-\frac{1}{r}}} E(H) . \qquad (7.3) \end{aligned}$$

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:

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

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 7.7 to show that

$$\sum_{x\in\mathbb{F}_p}\nu_A(x)^2\le 2\pi(A)H\,, \tag{7.4}$$

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 7.7 applicable. Lemma 7.8 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 [20], 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 (7.4) by invoking Lemma 7.7.

To bound the third sum, we apply Lemma 2.2 of [18]; this gives

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

Notice that $B+1>4rp^{\frac{1}{2r}}$, and, in particular, since $B\in\mathbb{Z}$ we have $B\ge 4r$. By a convexity argument one sees that $r\le B\log 2$ implies $(B+1)^r\le 2B^r$. (Indeed, this follows immediately using the inequality $r\log(1+1/B)\le r/B\le\log 2$.)

Using all this, 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

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

Using (3.5) of [20] 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

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

allows us to estimate

$$\frac{H}{\pi(A)}\ \le\ \frac{H(\log A+1)}{A}\ \le\ (d+1)B(\log A+1)\ \le\ 4r(d+1)\left(\frac{1}{2}-\frac{1}{4r}\right)p^{\frac{1}{2r}}\log p.$$

Therefore

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

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

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

Finally, using (7.3), this gives

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

Now we see that $|S_\chi(H)|\le C\,E(H)$, which would complete our induction, provided

$$((d+1)(2r-1)(4r-1))^{\frac{1}{2r}}+\frac{2C}{d^{1-\frac{1}{r}}}\le C. \tag{7.5}$$

Using the fact

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

and solving (7.5) for C allows us to see that (7.5) is equivalent to (7.2). ∎

Proof of Theorem 7.1. We apply Theorem 7.9 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 7.1 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.

Acknowledgments.

This paper is based upon a portion of the author's Ph.D. dissertation under the supervision of Harold Stark. The author would like to thank Professor Stark for his invaluable guidance and support at all stages of this work.

The author would also like to thank Tom Schmidt and the referee for their helpful comments which improved the quality of this manuscript.

References

1. G. Bachman and L. Rachakonda, *On a problem of Dobrowolski and Williams and the Pólya-Vinogradov inequality*, Ramanujan J. **5** (2001), no. 1, 65–71.
2. A. Booker, *Quadratic class numbers and character sums*, Math. Comp. **75** (2006), no. 255, 1481–1492.
3. D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. (3) **12** (1962), 179–192.
4. J.-P. Cerri, *Euclidean minima of totally real number fields: algorithmic determination*, Math. Comp. **76** (2007), no. 259, 1547–1575.
5. H. Davenport, *On the product of three non-homogeneous linear forms*, Proc. Cambridge Philos. Soc. **43** (1947), 137–152.
6. P. Erdös and C. Ko, *Note on the Euclidean algorithm*, J. London Math. Soc. **13** (1938), 3–8.
7. J. Friedlander, *Primes in arithmetic progressions and related topics*, Analytic number theory and Diophantine problems (Stillwater, OK, 1984), Progr. Math., vol. 70, Birkhäuser Boston, Boston, MA, 1987, pp. 125–134.
8. H. J. Godwin, *On Euclid's algorithm in some quartic and quintic fields*, J. London Math. Soc. **40** (1965), 699–704.
9. ———, *On the inhomogeneous minima of totally real cubic norm-forms*, J. London Math. Soc. **40** (1965), 623–627.
10. H. J. Godwin and J. R. Smith, *On the Euclidean nature of four cyclic cubic fields*, Math. Comp. **60** (1993), no. 201, 421–423.
11. E. Grosswald, *On Burgess' bound for primitive roots modulo primes and an application to $\Gamma(p)$*, Amer. J. Math. **103** (1981), no. 6, 1171–1183.
12. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, fifth ed., The Clarendon Press Oxford University Press, New York, 1979.
13. H. Heilbronn, *On Euclid's algorithm in cyclic fields*, Canadian J. Math. **3** (1951), 257–268.
14. H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004.
15. F. Lemmermeyer, *The Euclidean algorithm in algebraic number fields*, Exposition. Math. **13** (1995), no. 5, 385–416.
16. K. McGown, *On the second smallest prime non-residue*, (submitted).
17. ———, *Norm-Euclidean Galois fields and the Generalized Riemann Hypothesis*, J. Théor. Nombres Bordeaux (to appear).
18. ———, *On the constant in Burgess' bound for the number of consecutive residues or non-residues*, Funct. Approx. Comment. Math. (to appear).

19. 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.

20. J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.

21. J. R. Smith, *On Euclid's algorithm in some cyclic cubic fields*, J. London Math. Soc. **44** (1969), 577–582.

Department of Mathematics, University of California, San Diego, 9500 Gilman Drive, La Jolla, CA 92093

Current address: Department of Mathematics, Oregon State University, 368 Kidder Hall, Corvallis, OR 97331

E-mail address: mcgownk@math.oregonstate.edu