The Euclidean algorithm in quintic and septic cyclic fields

Pierre Lezowski, Kevin J. Mcgown

THE EUCLIDEAN ALGORITHM IN QUINTIC AND SEPTIC CYCLIC FIELDS

PIERRE LEZOWSKI AND KEVIN J. MCGOWN

Abstract. Conditionally on the Generalized Riemann Hypothesis (GRH), we prove the following results: (1) a cyclic number field of degree 5 is norm-Euclidean if and only if $\Delta = 11^4, 31^4, 41^4$; (2) a cyclic number field of degree 7 is norm-Euclidean if and only if $\Delta = 29^6, 43^6$; (3) there are no norm-Euclidean cyclic number fields of degrees 19, 31, 37, 43, 47, 59, 67, 71, 73, 79, 97. Our proofs contain a large computational component, including the calculation of the Euclidean minimum in some cases; the correctness of these calculations does not depend upon the GRH. Finally, we improve on what is known unconditionally in the cubic case by showing that any norm-Euclidean cyclic cubic field must have conductor $f \leq 157$ except possibly when $f \in (2 \cdot 10^{14}, 10^{50})$.

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 $|N(\alpha - \gamma\beta)| < |N(\beta)|$. Or equivalently, we may ask that for every $\xi \in K$ there exists $\gamma \in \mathcal{O}_K$ such that $|N(\xi - \gamma)| < 1$. In the quadratic setting, it is known that there are only finitely many norm-Euclidean fields and they have been identified [4, 2]; namely, a number field of the form $K = \mathbb{Q}(\sqrt{d})$ with d squarefree is norm-Euclidean if and only if

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

This result was partially generalized by Heilbronn [8] as follows.

Theorem 1.1 (Heilbronn)**.** *Let ℓ be a prime. Then there are at most finitely many cyclic number fields with degree ℓ which are norm-Euclidean.*

However, Heilbronn provided no upper bound on the discriminant of such fields. Building on work of Heilbronn, Godwin, and Smith (see [9, 5, 15, 7]), the second author proved the following result.

Theorem 1.2 ([13, Theorem 1.1])**.** *Assuming the GRH, the norm-Euclidean cyclic cubic fields are exactly those with discriminant*

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

Many of the results in the aforementioned paper go through for any cyclic field of odd prime degree. The main goal of this paper is to establish the analogue of Theorem 1.2 for quintic and septic fields.

Theorem 1.3. *Assume the GRH. A cyclic field of degree 5 is norm-Euclidean if and only if $\Delta = 11^4, 31^4, 41^4$. A cyclic field of degree 7 is norm-Euclidean if and only if $\Delta = 29^6, 43^6$.*

ℓ	f
3	7, 9, 13, 19, 31, 37, 43, 61, 67, 103, 109, 127, 157
5	11, 31, 41
7	29, 43
11	23, 67, 331
13	53, 131
17	137
23	47, 139
29	59
41	83
53	107
61	367
83	167, 499
89	179

TABLE 1.1. Possible norm-Euclidean fields in $\mathcal{F}$

Although we cannot give a complete determination for degree 11, it appears that for some degrees there are no norm-Euclidean cyclic fields whatsoever. This was observed (but not proved) for degree 19 in [12]. We prove the following:

Theorem 1.4. *Assuming the GRH, there are no norm-Euclidean cyclic fields of degrees* 19, 31, 37, 43, 47, 59, 67, 71, 73, 79, 97.

This list of primes is in no way intended to be complete, and in fact, there may well be infinitely many primes ℓ for which there are no norm-Euclidean cyclic fields of degree ℓ.

In other small degrees where we cannot give a complete determination, even under the GRH, we come very close. Let $\mathcal{F}$ denote the collection of cyclic number fields of prime degree $3 \leq \ell \leq 100$ and conductor f. In this setting the conductor-discriminant formula tells us that discriminant equals $\Delta = f^{\ell-1}$.

Theorem 1.5. *Assuming the GRH, Table 1.1 contains all norm-Euclidean fields in $\mathcal{F}$. (However, the possibility remains that some of these fields may not be norm-Euclidean.) Moreover, even without the GRH, the table is complete for $f \leq 10^{13}$.*

We remark that the top portion of this table (when $3 \leq \ell \leq 30$) appeared in [12] although it was unknown at the time (even under the GRH) whether the table was complete. A large part of establishing Theorems 1.3, 1.4, and 1.5 was a computation that took 3.862 (one-core) years of CPU time on a 96-core computer cluster.[1]

Finally, we also give a slight improvement on what is known unconditionally in the cubic case. In [12], it was shown that the conductor of any norm-Euclidean cyclic cubic field not listed in Theorem 1.2 must lie in the interval $(10^{10}, 10^{70})$. We improve this slightly, thereby obtaining:

[1]The cluster consists of 8 compute nodes, each with twelve 2 GHz cores, and 64 GB memory per node.

ℓ	3	5	7	11	13	17	19
unconditional	10^{70}	10^{78}	10^{82}	10^{88}	10^{89}	10^{92}	10^{94}
with the GRH	10^{11}	10^{12}	10^{13}	10^{13}	10^{14}	10^{14}	10^{14}

TABLE 2.1. Conductor bounds for norm-Euclidean fields in $\mathcal{F}$ established in [12] and [13]

ℓ	3	5	7	11	13	17	19	23
$f <$	$4 \cdot 10^{10}$	$6 \cdot 10^{10}$	$4 \cdot 10^{10}$	$2 \cdot 10^{11}$	$3 \cdot 10^{11}$	$6 \cdot 10^{11}$	$8 \cdot 10^{11}$	$2 \cdot 10^{11}$
ℓ	29	31	37	41	43	47	53	59
$f <$	$3 \cdot 10^{12}$	$3 \cdot 10^{12}$	$5 \cdot 10^{12}$	$6 \cdot 10^{12}$	$7 \cdot 10^{12}$	$9 \cdot 10^{12}$	$2 \cdot 10^{13}$	$2 \cdot 10^{13}$
ℓ	61	67	71	73	79	83	89	97
$f <$	$2 \cdot 10^{13}$	$3 \cdot 10^{13}$	$3 \cdot 10^{13}$	$3 \cdot 10^{13}$	$4 \cdot 10^{13}$	$4 \cdot 10^{13}$	$5 \cdot 10^{13}$	$6 \cdot 10^{13}$

TABLE 2.2. Conductor bounds for norm-Euclidean fields in $\mathcal{F}$ assuming the GRH

Theorem 1.6. *Any norm-Euclidean cyclic cubic field not listed in Theorem 1.2 must have discriminant $\Delta = f^2$ with $f \equiv 1 \pmod 3$ where f is a prime in the interval $(2 \cdot 10^{14}, 10^{50})$.*

Computing up to the new lower bound of $2 \cdot 10^{14}$ required an additional 3.104 years of CPU time on the same cluster.

2. Summary

For norm-Euclidean fields in $\mathcal{F}$ one has an upper bound on the conductor, which is greatly improved with the use of the GRH; in [12] and [13] the conductor bounds of Table 2.1 were established.

In this paper, we establish the following improved bounds:

Proposition 2.1. *Assuming the GRH, Table 2.2 gives conductor bounds for norm-Euclidean fields in $\mathcal{F}$.*

In [12] computations were carried out that show the portion of Table 1.1 where $3 \leq \ell \leq 30$ is complete up to $f = 10^{10}$. We have extended these computations, thereby obtaining the following unconditional result:

Proposition 2.2. *Table 1.1 contains all possible norm-Euclidean fields in $\mathcal{F}$ with $f \leq 10^{13}$. Additionally, when $50 \leq \ell \leq 100$, the table is complete up to the bounds listed in Table 2.2. Finally, when $\ell = 3$, the table is complete up to $2 \cdot 10^{14}$.*

Note that Propositions 2.1 and 2.2 imply the truth of Theorems 1.4 and 1.5. In the case of $\ell = 3$, it is known that all 13 of the fields listed in Table 1.1 are norm-Euclidean (see [15]). In the case of $\ell = 5$, Godwin [6] proved that $f = 11$ is norm-Euclidean and Cerri [3] has verified this. Up until this point, it seems that nothing was known about the remaining fields in the table. We use the algorithm of Cerri from [3] (which has recently been extended by the first author in [11]) with

ℓ	5			7	
f	11	31	41	29	43
$M(K)$	1/11	25/31	27/41	17/29	37/43

TABLE 2.3. Euclidean minima

ℓ	3	5	7	11	13	17	19	23
$f <$	10^{50}	10^{55}	10^{59}	10^{64}	10^{66}	10^{68}	10^{69}	10^{71}
ℓ	29	31	37	41	43	47	53	59
$f <$	10^{73}	10^{74}	10^{75}	10^{76}	10^{77}	10^{77}	10^{78}	10^{79}
ℓ	61	67	71	73	79	83	89	97
$f <$	10^{80}	10^{80}	10^{81}	10^{81}	10^{82}	10^{82}	10^{83}	10^{84}

TABLE 2.4. Conductor bounds for NE fields in $\mathcal{F}$

some additional modifications to show that all five fields with $\ell = 5$, 7 in Table 1.1 are norm-Euclidean. In fact, we compute the Euclidean minimum

$$M(K) = \sup_{\xi \in K} m_K(\xi), \text{ where } m_K(\xi) = \inf_{\gamma \in \mathcal{O}_K} |N(\xi - \gamma)|,$$

for each of these fields. It is well-known (and readily observed) that $M(K) < 1$ implies that K is norm-Euclidean.

Proposition 2.3. *Table 2.3 gives the Euclidean minimum $M(K)$ of the cyclic field K having degree ℓ and conductor f.*

It appears that the fields of degree 11 are currently out of reach of the algorithm; problems arise both from the time of computation required and from issues related to precision. In light of the discussion above, observe that the truth of the previous three propositions immediately implies Theorems 1.3, 1.4, and 1.5. We detail the computations necessary to justify Propositions 2.2 and 2.3 in Sections 3 and 4 respectively.

In Section 5 we derive the conductor bounds given in Proposition 2.1. This involves a trick which allows us to weaken the condition for "non-norm-Euclideanity" from [12] provided $\ell > 3$. We are also able to accomplish this in the cubic case by a different argument that takes advantage of the fact that the character takes only three values. This is carried out in Section 6.

Finally, the remainder of the paper is devoted to supplying the necessary justification for the upper bound on the conductor given in Theorem 1.6. The proof involves applying some recent results of Treviño concerning non-residues (see [18, 19, 17]) together with ideas in [14, 12]. For completeness, we provide improved (unconditional) conductor bounds for degrees $\ell > 3$ as well. However, as is the case when $\ell = 3$, these bounds are currently beyond our computational limits.

Proposition 2.4. *Table 2.4 gives (unconditional) conductor bounds for norm-Euclidean fields in $\mathcal{F}$.*

3. Computation for Proposition 2.2

Let K denote the cyclic field of prime degree ℓ and conductor f. We suppose that K has class number one. Assume that $(f, \ell) = 1$ so that K is not the field with $f = \ell^2$. No field of this type having $f = \ell^2$ is norm-Euclidean anyhow except for $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$; this is [12, Thereom 4.1]. We may assume that f is a prime with $f \equiv 1 \pmod{\ell}$; see [12, Section 2.1]. Denote by $q_1 < q_2$ the two smallest rational primes that are inert in K. Let χ denote any fixed primitive Dirichlet character of modulus f and order ℓ so that a rational prime p splits in K if and only if $\chi(p) = 1$. The following theorem is proved in [12].

Proposition 3.1 ([12, Theorem 3.1])**.** *Suppose that there exists $r \in \mathbb{Z}^+$ satisfying the following conditions:*

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

Then K is not norm-Euclidean.

Let $\mathcal{N}$ denote the image of the norm map from $\mathcal{O}_K$ to $\mathbb{Z}$. The proof of the previous proposition relies on:

Lemma 3.2 (Heilbronn's Criterion)**.** *If one can write $f = a + b$, with $a, b > 0$, $\chi(a) = 1$, $a \notin \mathcal{N}$, $b \notin \mathcal{N}$, then K is not norm-Euclidean.*

The advantage of Proposition 3.1 is that it requires far fewer steps than applying Lemma 3.2 directly. As K has class number one, we have that 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 $\chi(p) \neq 0, 1$).

To prove Proposition 2.2 we find q_1, q_2, r as described above. To save time, we look only for prime values of r. See [12] for the details. By applying Proposition 3.1, we show there are no norm-Euclidean fields of the given form with $10^4 \leq f \leq F_\ell$ where $F_\ell = 10^{13}$ when $3 \leq \ell \leq 50$ and F_ℓ equals the value in Table 2.2 when $50 \leq \ell \leq 100$. For example, Table 3 shows the values for the last ten fields in our calculation when $\ell = 97$.

To better manage the computation, the values of f being considered (for a given ℓ) were broken into subintervals of length 10^9. As mentioned earlier, this computation took 3.862 years of CPU time on a 96-core computer cluster. Another computation of the same nature was performed to check that there are no norm-Euclidean fields when $\ell = 3$ with $10^{13} \leq f \leq 2 \cdot 10^{14}$, which took an additional 3.104 years of CPU time on the same cluster. Combining the computation just described with the results mentioned in Section 1 proves Proposition 2.2.

4. Computation for Proposition 2.3

Previously, Cerri computed that the Euclidean minimum of the cyclic quintic field with conductor $f = 11$ is equal to $1/11$ (see [3]). We compute the Euclidean minimum of the remaining four fields K with $\ell = 5, 7$ in Table 1.1, using the algorithm described in [11].

The algorithm is divided into two main parts:

f	q_1	q_2	r
59 999 999 974 303	2	3	431
59 999 999 975 273	2	3	1933
59 999 999 977 213	2	3	241
59 999 999 979 929	2	3	673
59 999 999 981 869	2	3	797
59 999 999 989 823	2	3	2719
59 999 999 990 599	2	3	199
59 999 999 995 643	2	3	383
59 999 999 999 717	2	3	3709
59 999 999 999 911	2	3	2663

TABLE 3.1. Example calculation

ℓ	f	$M(K)$	C	CPU time
5	31	25/31	10	13.2 min
5	41	27/41	10	67.0 min
7	29	17/29	14	95.6 min
7	43	37/43	14	475.8 min

TABLE 4.1. Computation of the Euclidean minima

- Using an embedding of K into $\mathbb{R}^\ell$, we try to find a finite list of points $\mathcal{L} \subseteq K$ and some real number k such that any point $x \in K \setminus \mathcal{L}$ we have $m_K(x) < k$. If $k < 1$ and $\mathcal{L} = \emptyset$, this proves that K is norm-Euclidean.
- Next, we compute the Euclidean minimum of the remaining points in $\mathcal{L}$. If $\max\{m_K(x) \mid x \in \mathcal{L}\} > k$, then
$$M(K) = \max\{m_K(x) \mid x \in \mathcal{L}\}.$$
If not, we start again with smaller k.

The algorithm also returns the finite set of *critical points*, that is to say the points $x \in K/\mathcal{O}_K$ satisfying $M(K) = m_K(x)$. The results obtained are given in Table 4.1, where C is the cardinality of the set of critical points.

In carrying out these computations, the second part of the algorithm takes far longer than the first. Nevertheless, we can improve the running time with the following observation: The points considered in our four cases are always of the form α/β where α, β are nonzero elements of $\mathcal{O}_K$ such that $N\beta$ is the conductor f. This provides some information on the Euclidean minimum of α/β.

Lemma 4.1. *Let $\mathcal{N}$ denote the image of the norm map N. Let α and β be nonzero elements of $\mathcal{O}_K$ such that $N\beta = f$. Then*
$$m_K\left(\frac{\alpha}{\beta}\right) \geq \frac{\min\{|t| : t \in \mathcal{N},\, t \equiv N\alpha \pmod f\}}{f}.$$

Proof. By definition of the Euclidean minimum,
$$m_K\left(\frac{\alpha}{\beta}\right) = \frac{\min\{|N(\alpha - \beta z)| : z \in \mathcal{O}_K\}}{N\beta} = \frac{\min\{|N(\alpha - \beta z)| : z \in \mathcal{O}_K\}}{f}.$$

f	$M(K)$	C	CPU time
103	93/103	6	12 minutes
109	76/109	6	1 day 20 hours
127	94/127	6	2 days 17 hours

TABLE 4.2. Euclidean minima in some cyclic cubic cases

But for any $z \in \mathcal{O}_K$, $N(\alpha - \beta z) \equiv N\alpha \pmod f$. As $N(\alpha - \beta z)$ is obviously an element of $\mathcal{N}$, the result follows. ∎

In particular, for a point α/β of this form, if we can find some $z \in \mathcal{O}_K$ such that

$$|N(\alpha - \beta z)| = \min\{|t| : t \in \mathcal{N},\, t \equiv N\alpha \pmod f\},$$

we will then have

$$m_K\left(\frac{\alpha}{\beta}\right) = \frac{|N(\alpha - \beta z)|}{f}.$$

To illustrate this idea, consider the field $K = \mathbb{Q}(x)$ where $x^5 - x^4 - 12x^3 + 21x^2 + x - 5 = 0$, of degree 5 and conductor 31. At the end of running the algorithm, we get a list $\mathcal{L}$ of ten points of the form α/β as above. One of the points found has $\alpha = -\frac{106}{5}x^4 - \frac{162}{5}x^3 + \frac{866}{5}x^2 - \frac{28}{5}x - 41$, and $\beta = -4x^4 - 6x^3 + 33x^2 - 2x - 9$. Then $N\alpha = -25$ (and $N\beta = 31$). As $6 \notin \mathcal{N}$, Lemma 4.1 implies that $m_K(\alpha/\beta) \geq 25/31$. Of course, we have an equality because $|N(\alpha/\beta)| = 25/31$. Besides, the ten points found are in the same orbit under the action of the units on $K/\mathcal{O}_K$. Thus their Euclidean minimum is equal to 25/31, which is the Euclidean minimum of K, and they are the set of critical points, which has cardinality 10.

Remark 4.2. Lemma 4.1 is a variation on Heilbronn's Criterion (Lemma 3.2). If

$$\min\{|t| : t \in \mathcal{N}, t \equiv N\alpha \pmod f\} > f,$$

then we can deduce from it an equality

$$f = a + b,$$

where a is the integer in $(0, f)$ such that $N\alpha \equiv a \pmod f$ and $b = f - a$.

Remark 4.3. The algorithm may also be applied to calculate the Euclidean minimum of cyclic cubic number fields. Table 4.2 presents the results obtained in some of the norm-Euclidean cases where the Euclidean minimum was previously unknown. For conductors $f < 103$, one can refer to [10]. As observed in [7], the field with conductor 157 seems harder to deal with; to date, no one has successfully computed the Euclidean minimum of this field.

5. Improved GRH conductor bounds when $\ell > 3$

We adopt the notation given in the first paragraph of Section 3. In addition, from now on and throughout the paper, $r \in \mathbb{Z}^+$ will denote the smallest positive integer such that $(r, q_1q_2) = 1$ and $\chi(r) = \chi(q_2)^{-1}$. However, we do not assume any congruence conditions on r. The following lemma is an improvement of statement (3) from Theorem 3.1 of [12]; it is essentially a direct application of the same theorem.

Lemma 5.1. *Let us assume $q_1 \neq 2, 3, 7$. If K is norm-Euclidean, then*

$$f < \max\left\{q_1,\ \frac{2.1}{\ell} f^{1/\ell} \log f\right\} q_2 r.$$

Proof. Let u be the integer such that $0 < u < q_1$ and $uq_2r \equiv f \pmod{q_1}$. We set $v = (f - uq_2r)/q_1$, so that $f = uq_2r + q_1v$. This equation can be used with Heilbronn's Criterion provided $v > 0$ and $q_1v \notin \mathcal{N}$. Clearly $v \neq 0$ lest we contradict the fact that f is prime. Therefore, as we are assuming K is norm-Euclidean, it must be the case that $v < 0$ or $q_1v \in \mathcal{N}$. However, $v < 0$ immediately implies that $f < q_1q_2r$, and there is nothing more to prove. Hence it suffices to assume $v > 0$. In this case we must have $q_1v \in \mathcal{N}$ which implies $q_1^{\ell-1}$ divides v. Now we see that $v > 0$ leads to $q_1^{\ell-1} \leq v < f/q_1$ and hence $q_1 < f^{1/\ell}$. As $q_1 \neq 2, 3, 7$, we know from [12, Theorem 3.1] that $f < 2.1q_1q_2r \log q_1$ and the result follows. ∎

Proposition 5.2. *Assume the GRH. If K is norm-Euclidean and $f > 10^9$, then*

$$f \leq \max\left\{(1.17\log(f) - 6.36)^2,\ \frac{2.1}{\ell} f^{1/\ell} \log(f)\right\} \cdot \left(2.5(\ell - 1)\log(f)^2\right)^2.$$

Proof. We use the bound on q_1 given in [1] and the bounds on q_2 and r given in [13, Theorems 3.1 and 3.2]. If $q_1 \neq 2, 3, 7$, Lemma 5.1 together with these bounds gives the result. This completes the proof in most cases, but it remains to check that we obtain better bounds in the other special cases.

If $q_1 = 7$, then $f < 21 \log 7 \cdot q_2r$ by [12, Theorem 3.1]. We easily see that $(1.17 \log f - 6.36)^2 > 21 \log 7$ for any $f > 60,000$. The result now follows from [13, Theorem 3.2]. If $q_1 = 2, 3$ and $q_2 > 5$, then we obtain $f < 5q_2r$ from [12, Theorem 3.1] and the result follows in the same manner.

Finally, it remains to treat the two special cases: $(q_1, q_2) = (2, 3), (3, 5)$. At this point, we assume $f \geq 10^9$. Proposition 5.1 of [12] tells us that f is bounded above by $72(\ell - 1)f^{1/2} \log(4f) + 35$ and $507(\ell - 1)f^{1/2} \log(9f) + 448$ in the first and second case respectively. In either case, the quantity in question is bounded above by $568(\ell - 1)f^{1/2} \log f$. Consequently, we have $f \leq (568(\ell - 1) \log f)^2$. Now, one easily checks that $(1.17 \log f - 6.36)^2(2.5)^2 \geq 1442$ and $568^2(\ell - 1)^2(\log f)^2 \leq 1442(\ell - 1)^2(\log f)^4$, which implies the desired result. ∎

Invoking the previous proposition immediately yields the GRH conductor bounds given in Table 2.2 when $\ell > 3$. The $\ell = 3$ entry of Table 2.2 will be obtained in Corollary 6.2. This completes the proof of Theorems 1.3, 1.4, and 1.5.

6. The cyclic cubic case revisited

Unfortunately, the trick employed in the previous section does not help us when $\ell = 3$. Nonetheless, in the cubic case, we are able to slightly weaken the conditions for "non-norm-Euclideanity" given in [12, Theorem 3.1]. Notice that the following result contains no congruence conditions and there is no extra $\log q_1$ factor. The proof again relies on Heilbronn's Criterion (Lemma 3.2), but we will take advantage of the fact that χ only takes three different values in this very special case.

Proposition 6.1. *Let K be a cyclic cubic number field. If $q_1 \neq 2$ and $f \geq q_1q_2 \max(3r, 10q_1)$, then K is not norm-Euclidean.*

Proof. It will be crucial that $\ell = 3$, which of course implies that χ only takes three values: 1, $\chi(q_2)$, and $\chi(r)$. In addition, we have $\chi(r) = \chi(q_2)^{-1} = \chi(q_2)^2$.

Let u be the integer such that $0 < u < q_1$ and $uq_2r \equiv f \pmod{q_1}$. We set $v = (f - uq_2r)/q_1$, so that

$$f = uq_2r + q_1v. \tag{6.1}$$

Observe that $f \geq q_1q_2r$ implies $v \geq 0$; moreover, we may assume $v \neq 0$ lest we contradict the fact that f is a prime. If q_1 does not divide v, then we may apply Heilbronn's Criterion with (6.1). Hence we may assume that q_1 divides v. We break the proof into a number of cases.

(1) Suppose u is odd. Then $u + q_1$ is even and $0 < (u + q_1)/2 < q_1$, so every prime divisor p of $(u + q_1)/2$ is such that $\chi(p) = 1$. Besides, $(q_1, q_2r) = 1$ and q_1 divides v, so q_1 does not divide $v - q_2r$. As $q_1 > 2$ and $\chi(2) = 1$, we may apply Heilbronn's Criterion with

$$f = (u + q_1)q_2r + q_1(v - q_2r), \tag{6.2}$$

provided $v \geqslant q_2r$.

(2) Suppose u is even. We distinguish cases according to the value of $u + q_1$.
   (a) If $u + q_1$ is composite, then any prime factor p of $u + q_1$ is such that $p < q_1$. Therefore, we may again apply Heilbronn's Criterion with (6.2), provided $v \geqslant q_2r$.
   (b) If $u + q_1$ is prime and $\chi(u + q_1) = 1$, then we proceed similarly.
   (c) Suppose $u + q_1$ is prime and $\chi(u + q_1) = \chi(r)$. Notice that $r \leq u + q_1$.
      (i) If $\frac{u}{2} + q_1$ is composite or a prime such $\chi(\frac{u}{2} + q_1) = 1$, then $(q_2, \frac{u}{2} + q_1) = 1$ and we may use Heilbronn's Criterion with

$$f = (u + 2q_1)q_2r + q_1(v - 2q_2r), \tag{6.3}$$

provided $v \geq 2q_2r$.

      (ii) If $\frac{u}{2} + q_1$ is prime and $\chi(\frac{u}{2} + q_1) = \chi(q_2)$, then we have $q_2 \leq \frac{u}{2} + q_1 < \frac{3}{2}q_1$ which also implies $0 \leq u + 2(q_1 - q_2) < q_1$. If $u \neq 2(q_2 - q_1)$, then q_1 does not divide $v + r(u + 2(q_1 - q_2))$ and therefore we can apply Heilbronn's Criterion with

$$f = (u + 2q_1)(q_2 - q_1)r + q_1(v + r(u + 2(q_1 - q_2))),$$

provided $v \geq 2q_2r$. Indeed, if $(u + 2q_1)(q_2 - q_1)r \in \mathcal{N}$, then the valuation of $(u + 2q_1)(q_2 - q_1)r$ at $\frac{u}{2} + q_1$ is at least $\ell = 3$, so $(\frac{u}{2} + q_1)^2$ divides $r \leq u + q_1$. Then $q_1^2 < (\frac{u}{2} + q_1)^2 \leq r < 2q_1$, which is impossible.

If $u = 2(q_2 - q_1)$, then 4 divides u and $q_1 < \frac{u}{4} + q_1 < q_2$. Therefore, $(q_2, (u+4q_1)r) = 1$ and $(u+4q_1)q_2r \notin \mathcal{N}$. So we may apply Heilbronn's Criterion with

$$f = (u + 4q_1)q_2r + q_1(v - 4q_2r),$$

provided $v \geq 4q_2r$. Notice in this case that $q_2 \leq \frac{3}{2}q_1$ and $r \leq u + q_1 = 2q_2 - q_1 \leq 2q_1$.

      (iii) If $\frac{u}{2} + q_1$ is prime and $\chi(\frac{u}{2} + q_1) = \chi(r)$, then $q_2 < r \leq \frac{u}{2} + q_1$. Therefore, $(q_2, u+2q_1) = 1$. Besides, $r-q_1 < q_1$, so $(q_2, r-q_1) = 1$. As a result, $(u + 2q_1)q_2(r - q_1) \notin \mathcal{N}$. If $r \neq \frac{u}{2} + q_1$, then q_1 does not divide $q_2(u + 2q_1 - 2r)$, so we can apply Heilbronn's

Criterion with

$$f = (r - q_1)q_2(u + 2q_1) + q_1(v + q_2(u + 2q_1 - 2r)),$$

assuming $v \geq 2q_2r$.

If $r = \frac{u}{2} + q_1$, then $u + q_1 - r = \frac{u}{2}$. As $u + q_1$ is prime and satisfies $\chi(u + q_1) = \chi(r)$, we have $(u + q_1, (r - q_1)q_2) = 1$ and $(r - q_1)q_2(u + q_1) \notin \mathcal{N}$. So we may use Heilbronn's Criterion with

$$f = (r - q_1)q_2(u + q_1) + q_1(v + q_2(u + q_1 - r)),$$

assuming $v \geq 0$.

(d) Suppose $u + q_1$ is prime and $\chi(u + q_1) = \chi(q_2)$.

(i) If $\frac{u}{2} + q_1$ is composite or a prime such that $\chi(\frac{u}{2} + q_1) = 1$, then we may use Heilbronn's Criterion with (6.3).

(ii) If $\frac{u}{2}+q_1$ is prime and $\chi(\frac{u}{2}+q_1) = \chi(q_2)$, then $q_2 \leq \frac{u}{2}+q_1 < u+q_1$, so $(q_1q_2, u + q_1) = 1$, and by definition of r, $r \leq (u + q_1)^2$.

If $r < (u+q_1)^2$, then $(u+q_1)(q_2-q_1)r \notin \mathcal{N}$. Indeed, $q_2 \leq \frac{u}{2}+q_1$, so $q_2 - q_1 < q_1$. Besides, $(u + q_1)^2$ cannot divide $r < (u + q_1)^2$. Consequently, we may apply Heilbronn's Criterion with

$$f = (u + q_1)(q_2 - q_1)r + q_1(v + r(u + q_1 - q_2)), \tag{6.4}$$

assuming $v \geq q_2r$. Indeed, $q_2 \leq u + q_1 < 2q_1$, so $0 \leq u + q_1 - q_2 < q_1$, and $u = q_2 - q_1$ is impossible, because it would imply $q_1 < \frac{u}{2} + q_1 < q_2$, which contradicts $\chi(\frac{u}{2} + q_1) \neq 1$.

If $r = (u + q_1)^2$, then $(\frac{u}{2} + q_1)^2 < r$; in this case, it follows from the definition of r that $(\frac{u}{2}+q_1, q_2) \neq 1$ and we obtain $\frac{u}{2}+q_1 = q_2$. We may now apply Heilbronn's Criterion with

$$f = 2uq_2^2(u + q_1) + q_1(v - uq_2(u + q_1)),$$

assuming $v \geq uq_2(u+q_1)$ (which holds if $v \geq q_2(u+q_1)^2 = q_2r$).

(iii) If $\frac{u}{2} + q_1$ is prime and $\chi(\frac{u}{2} + q_1) = \chi(r)$, then $q_2 < r \leq \frac{u}{2} + q_1$. Therefore, $(u + q_1, (q_2 - q_1)r) = 1$ and $(u + q_1)(q_2 - q_1)r \notin \mathcal{N}$. Besides, $0 < q_2 - q_1 < u + q_1 - q_2 < 2q_1 - q_2 < q_1$, and we may apply Heilbronn's Criterion with (6.4), assuming $v \geq 0$.

Now we summarize. In all cases but one, the assumption $v \geq 2q_2r$ is sufficient and hence it is enough to require that $f \geq 3q_1q_2r$. (Recall that $v = (f - uq_2r)/q_1$.) In the exceptional case, we have shown that $v \geq 4q_2r$ is sufficient; but in that situation we also know $r \leq 2q_1$ and therefore it is enough to require that $f \geq 10q_1^2q_2$. ∎

Corollary 6.2. *Assume the GRH. Let K be a cyclic cubic field. If K is norm-Euclidean, then $f < 4 \cdot 10^{10}$.*

Proof. We use Proposition 6.1 and the bounds on q_1, q_2 and r given in [1, 13]. ∎

Although the previous corollary is already known, we want to point out that Proposition 6.1 allows one to prove Theorem 1.2 using less computation than is employed in [13]. More importantly, Proposition 6.1 will serve as one of the main ingredients in lowering the unconditional conductor bound (in the cubic case).

7. Character non-residues

Let χ be a non-principal Dirichlet character modulo a prime p. Suppose that $q_1 < q_2$ are the two smallest prime non-residues of χ. This section is devoted to

improving the constants appearing in [14]. We begin by quoting a result proved by Treviño:

Proposition 7.1 ([19, Theorem 1.2])**.** *Suppose $p > 3$. Then $q_1 < 0.9\, p^{1/4} \log p$ unless χ is quadratic and $p \equiv 3 \pmod 4$, in which case $q_1 < 1.1\, p^{1/4} \log p$.*

The following proposition will lead to improved bounds on q_2 and the product $q_1 q_2$:

Proposition 7.2. *Suppose $p \geq 10^6$, and that u is a prime with $u \geq A \log p$ where $A = (2/5)e^{3/2} \approx 1.79$. Suppose $\chi(n) = 1$ for all $n \in [1, H]$ with $(n, u) = 1$. Then*

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

where $g(p)$ is an explicitly given function. Moreover, $g(p)$ is decreasing for $p \geq 10^6$ and $g(p) \to 2.71512...$.

Proof. Similar to the proof of [14, Theorem 3], we may reduce to the case where $H \leq (A \log p - 1)^{1/2} p^{1/2}$. We may assume $H \geq K p^{1/4} \log p$ where $K := 2.7151$, or else there is nothing to prove. We set $h = \lfloor A \log p \rfloor$, $r = \lceil B \log p \rceil$, with $A = (2/5)e^{3/2}$ and $B = 1/5$.

For $1/2 \leq y \leq 1$, we have $\exp(y/2B) \leq \exp(1/2B)y$, so in particular

$$p^{1/2r} = \exp\left(\frac{1}{2B}\frac{B\log(p)}{r}\right) \leq \exp\left(\frac{1}{2B}\right)\frac{B\log(p)}{r}.$$

But $B\exp(1/2B)\log(p) = eA/2 \cdot \log(p) \leq e(h+1)/2$, from which we deduce

$$\left(\frac{2r}{e(h+1)}\right)^r \leq p^{-1/2}. \tag{7.1}$$

One verifies that $Kp^{1/4} > 32A$ for $p \geq 10^6$ and hence $H > 32h$. We set $X := H/(2h)$ and observe that we have the a priori lower bound

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

and, in particular, $X > 16$ from the previous sentence. We will make use of the function $f(X, u)$ defined by

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

observe that

$$\hat{f}(p) := f\left(\frac{Kp^{1/4}}{2A},\, A\log p\right) \leq f(X,u)\,.$$

Combining [14, Proposition 1], [19, Theorem 1.1], and an explicit version of Stirling's Formula (see [16], for example), we obtain

$$\frac{6}{\pi^2}\left(1-u^{-1}\right)h(h-2)^{2r}\left(\frac{H}{2h}\right)^2 \hat{f}(p) \;\leq\; \sqrt{2}\left(\frac{2r}{e}\right)^r ph^r + (2r-1)p^{1/2}h^{2r}. \tag{7.2}$$

Using the convexity of the logarithm, we establish the following estimates:

$$\left(\frac{h}{h-2}\right)^r \leq F(p)\,, \quad \left(\frac{h+1}{h}\right)^r \leq G(p) \tag{7.3}$$

$$F(p) := \exp\left(\frac{2B\log p + 2}{A\log p - 3}\right), \quad G(p) := \exp\left(\frac{B\log p + 1}{A\log p - 1}\right)$$

p_0	10^6	10^8	10^{10}	10^{12}	10^{14}	10^{16}	10^{18}	10^{20}
C	6.9236	4.1883	3.5764	3.3290	3.2019	3.1246	3.0716	3.0320
p_0	10^{22}	10^{24}	10^{26}	10^{28}	10^{30}	10^{32}	10^{34}	10^{36}
C	3.0008	2.9754	2.9542	2.9363	2.9208	2.9074	2.8956	2.8852
p_0	10^{38}	10^{40}	10^{42}	10^{44}	10^{46}	10^{48}	10^{50}	10^{52}
C	2.8759	2.8676	2.8601	2.8533	2.8471	2.8415	2.8363	2.8315

TABLE 7.1. Values of C for various choices of p_0

Note that $F(p)$ and $G(p)$ are both decreasing functions of p. Rearranging (7.2) and applying (7.3), (7.1) gives:

$$\begin{aligned}
(7.4)\qquad & \frac{6}{\pi^2}\left(1-u^{-1}\right)H^2\hat{f}(p) \\
&\leq 4h(2r-1)\left(\frac{h}{h-2}\right)^{2r}p^{1/2}\left[1+\frac{\sqrt{2}}{2r-1}\left(\frac{2r}{eh}\right)^{r}p^{1/2}\right] \\
&\leq 4h(2r-1)F(p)^2p^{1/2}\left[1+\frac{\sqrt{2}G(p)}{2r-1}\left(\frac{2r}{e(h+1)}\right)^{r}p^{1/2}\right] \\
&\leq 4(A\log p)(2B\log p+1)F(p)^2p^{1/2}\left(1+\frac{\sqrt{2}G(p)}{2r-1}\right) \\
&\leq 8ABp^{1/2}(\log p)^2F(p)^2\left(1+\frac{1}{2B\log p}\right)\left(1+\frac{\sqrt{2}G(p)}{2B\log p-1}\right) \\
(7.5)\qquad &\leq 8AB\,p^{1/2}(\log p)^2F(p)^2\left(1+\frac{5}{2\log p}\right)\left(1+\frac{5\sqrt{2}G(p)}{2\log p-5}\right)
\end{aligned}$$

Now the result follows provided we define:

$$g(p) := 2\pi F(p)\sqrt{\frac{A\left(1+\frac{5}{2\log p}\right)\left(1+\frac{5\sqrt{2}G(p)}{2\log p-5}\right)}{15\hat{f}(p)\left(1-\frac{1}{A\log p}\right)}}\,. \qquad \blacksquare$$

Proposition 7.3. *Fix a real constant $p_0 \geq 10^6$. There exists an explicit constant C (see Table 7.1) such that if $p \geq p_0$ and u is a prime with $u \geq 1.8\log p$, then there exists $n \in \mathbb{Z}^+$ with $(n,u)=1$, $\chi(n)\neq 1$, and $n < C\,p^{1/4}\log p$.*

Proof. Let n_0 denote the smallest $n \in \mathbb{Z}^+$ such that $(n,u)=1$ and $\chi(n)\neq 1$. We apply Proposition 7.2 to find

$$n_0 - 1 \leq g(p_0)\,p^{1/4}\log p\,.$$

Computation of the table of constants is routine; for each value of p_0, we compute (being careful to round up) the quantity

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

Corollary 7.4. *If $p \geq 10^{13}$, then $q_2 < 2.8\,p^{1/4}(\log p)^2$.*

	q_1 arbitrary	$q_1 > 100$
k	$D_1(k)$	$D_2(k)$
2	36.9582	5.6360
3	25.3026	3.8981
4	21.3893	3.3703
5	19.4132	3.1104
6	18.2048	2.9523
7	17.3797	2.8439
8	16.7819	2.7650
9	16.3162	2.7030
10	15.9414	2.6525

TABLE 8.1. Values of $D(k)$ when $2 \leq k \leq 10$ and $f \geq 10^{20}$

Proof. If $q_1 > 1.8 \log p$, then we apply the previous proposition and we are done. Hence we may assume that $q_1 \leq 1.8 \log p$. If $q_2 = 3$, then we are clearly done, so we may also assume $q_2 \neq 3$. In this case, we combine [14, Lemma 7] and [18, Theorem 1][2] to conclude $q_2 \leq (1.55 p^{1/4} \log p)(1.8 \log p) + 1 < 2.8 p^{1/4} (\log p)^2$. ∎

Corollary 7.5. *Suppose $p \geq 10^{30}$ and that χ has odd order. Then*

$$q_1 q_2 < 2.64\, p^{1/2} (\log p)^2 .$$

Proof. If $q_1 < 1.8 \log p$, we use the previous corollary (and its proof) to obtain $q_2 < 3 p^{1/4} (\log p)^2$, and hence $q_1 q_2 < 5.4 p^{1/4} (\log p)^3 \leq 0.01 p^{1/2} (\log p)^2$. If $q_1 \geq 1.8 \log p$, then we apply Proposition 7.1 (using the fact that χ has odd order) and Proposition 7.2 to find $q_1 q_2 \leq (0.9 p^{1/4} \log p)(2.93 p^{1/4} \log p)$. The result follows. ∎

8. Improved unconditional conductor bounds

In this section we will prove Proposition 2.4. First, we observe that applying Treviño's version of the Burgess Inequality (see [17]) immediately[3] gives better constants $D(k)$ for [12, Proposition 5.7] for $2 \leq k \leq 10$.

To establish our result, we follow the proof of [12, Theorem 5.8]. Details that are identical or very similar will be omitted. We may assume throughout that $f \geq 10^{40}$. If $q_1 \leq 100$, the techniques in [12] already give the desired result and hence we may assume $q_1 > 100$. We treat the cases of $\ell = 3$ and $\ell > 3$ separately.

First, we treat the cubic case. In light of Proposition 6.1, it suffices to verify that $10 q_1^2 q_2 \leq f$ and $3 q_1 q_2 r \leq f$. The former condition easily holds, since applying Proposition 7.1 and Corollary 7.5 immediately gives $10 q_1^2 q_2 < 24 f^{3/4} (\log f)^3 < f$. We turn to the latter condition. Proposition 5.7 of [12] (with the improved constants) gives:

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

[2] In a private correspondence, the author of [18] has indicated that the result contained therein holds when $p > 10^{13}$; a correction to [18] is forthcoming.

[3] In the technical condition appearing in the proposition, one must replace $4f^{1/2}$ by $2f^{1/2}$; however, in our application, this condition will be automatically met so this has no real effect. Moreover, it is shown in [17] that the technical condition may be dropped completely provided $k \geq 3$.

Applying Corollary 7.5, this leads to:

$$\begin{aligned} 3q_1q_2r &\leq 3 \cdot 2.64 f^{1/2} (\log f)^2 \cdot (D_2(k)(\ell-1))^k f^{\frac{k+1}{4k}} (\log f)^{\frac{1}{2}} \\ &\leq 8\, D_2(k)^k (\ell-1)^k f^{\frac{3k+1}{4k}} (\log f)^{\frac{5}{2}}, \end{aligned}$$

Choosing $k = 4$ we see that the desired condition holds when $f \geq 10^{50}$.

Now we turn to the case when $\ell > 3$. In light of Lemma 5.1, it suffices to verify that

$$\max\left\{q_1\,, f^{1/5}\log f\right\}\, q_2 r \leq f$$

Using Corollaries 7.4, 7.5 we have $q_1q_2 \leq 2.7 f^{1/2}(\log f)^2$ as well as

$$(f^{1/5}\log f) q_2 \leq 3 f^{9/20} (\log f)^2 < 2.7 f^{1/2} (\log f)^2\,.$$

Consequently, applying Proposition 5.7 of [12] as before, we now have:

$$\max\left\{q_1\,, f^{1/5}\log f\right\}\, q_2 r \leq 2.7\, D_2(k)^k (\ell-1)^k f^{\frac{3k+1}{4k}} (\log f)^{\frac{5}{2}}. \tag{8.1}$$

For the primes $\ell = 5, 7$ we use $k = 4$ and for the remaining values of ℓ we use $k = 3$. We check that the expression on the righthand side of (8.1) is less than f provided f is greater than the value given in Table 2.4.

Acknowledgements

The authors would like to thank Thomas Carroll of Ursinus College for graciously allowing the use of his computer cluster for this project. The research of the first author was funded by a grant given by région Auvergne. The second author was partially supported by an internal research grant from California State University, Chico. Both authors would like to thank the anonymous referee, whose remarks helped to improve the final version of the paper.

References

[1] Bach, E. *Explicit bounds for primality testing and related problems.* Math. Comp. 55 (1990), no. 191, 355–380.

[2] Barnes, E. S.; Swinnerton-Dyer, H. P. F. *The inhomogeneous minima of binary quadratic forms. I.* Acta Math. 87, (1952), 259–323.

[3] Cerri, J.-P. *Euclidean minima of totally real number fields: algorithmic determination.* Math. Comp. 76 (2007), no. 259, 1547–1575.

[4] Chatland, H.; Davenport, H. *Euclid's algorithm in real quadratic fields.* Canadian J. Math. 2, (1950), 289–296.

[5] Godwin, H. J. *On Euclid's algorithm in some cubic fields with signature one.* Quart. J. Math. Oxford Ser. (2) 18 (1967), 333–338.

[6] Godwin, H. J. *On Euclid's algorithm in some quartic and quintic fields.* J. London Math. Soc. 40 (1965), 699–704.

[7] Godwin, H. J.; Smith, J. R. *On the Euclidean nature of four cyclic cubic fields.* Math. Comp. 60 (1993), no. 201, 421–423.

[8] Heilbronn, H. *On Euclid's algorithm in cyclic fields.* Canad. J. Math. 3 (1951), 257–268.

[9] Heilbronn, H. *On Euclid's algorithm in cubic self-conjugate fields.* Proc. Cambridge Philos. Soc. 46, (1950), 377–382.

[10] Lemmermeyer, F. *The Euclidean Algorithm in Algebraic Number Fields.* Expo. Math. 13, (1995, updated in 2014), 385–416.

[11] Lezowski, P. *Computation of the Euclidean minimum of algebraic number fields.* Math. Comp. 83 (2014), 1397–1426.

[12] McGown, K. J. *Norm-Euclidean cyclic fields of prime degree.* Int. J. Number Theory 8 (2012), no. 1, 227–254.

[13] McGown, K. J. *Norm-Euclidean Galois fields and the generalized Riemann hypothesis.* J. Théor. Nombres Bordeaux 24 (2012), no. 2, 425–445.
[14] McGown, K. J. *On the second smallest prime non-residue.* J. Number Theory 133 (2013), no. 4, 1289–1299.
[15] Smith, J. R. *On Euclid's algorithm in some cyclic cubic fields.* J. London Math. Soc. 44 (1969), 577–582.
[16] Spira, Robert. *Calculation of the gamma function by Stirling's formula.* Math. Comp. 25 (1971), 317–322.
[17] Treviño, E. *The Burgess inequality and the least k-th power non-residue.* Int. J. Number Theory 11, (2015), no. 5, 1–26.
[18] Treviño, E. *On the maximum number of consecutive integers on which a character is constant.* Mosc. J. Comb. Number Theory 2 (2012), no. 1, 56–72.
[19] Treviño, E. *The least k-th power non-residue.* J. Number Theory 149 (2015), 201–224.

Université Blaise Pascal, Laboratoire de mathématiques UMR 6620, Campus Universitaire des Cézeaux, BP 80026, 63171 Aubière Cédex, France
E-mail address: pierre.lezowski@math.univ-bpclermont.fr

California State University, Chico, Department of Mathematics and Statistics, 601 E. Main St., Chico, CA, 95929, USA
E-mail address: kmcgown@csuchico.edu