ANNALES DE L'INSTITUT FOURIER

Kevin J. McGown & Amanda Tucker

Statistics of genus numbers of cubic fields

STATISTICS OF GENUS NUMBERS OF CUBIC FIELDS

by Kevin J. MCGOWN & Amanda TUCKER

––––––––

ABSTRACT. — We prove that approximately 96.23% of cubic fields, ordered by discriminant, have genus number one, and we compute the exact proportion of cubic fields with a given genus number. We also compute the average genus number. Finally, we show that a positive proportion of totally real cubic fields with genus number one fail to be norm-Euclidean.

RÉSUMÉ. — Nous prouvons qu'il y a approximativement 96.23% de corps de nombres cubiques, ordonnés par discriminant, dont le nombre de genres est un et nous calculons la proportion exacte des corps de nombres cubiques avec un nombre de genres donné. Nous calculons également le nombre de genres moyen. Finalement, nous montrons qu'il y a une proportion strictement positive de corps de nombres cubiques totalement réels avec un nombre de genres un qui ne sont pas euclidiens pour la norme.

1. Introduction

The genus theory of algebraic number fields can be traced back to Gauss's celebrated work on binary quadratic forms, and has its roots in earlier work of Euler, Lagrange, and others. It was Hasse who first defined the genus field of a quadratic extension when he reproved a classical theorem of Gauss using class field theory [22], and Leopoldt later defined the genus field of any absolutely abelian extension [27]. The definition of the genus field of a general number field, which we give forthwith, is due to Fröhlich [20].

The genus field of a number field K is defined to be the maximal extension K^* of K that is unramified at all finite primes and is a compositum of the form Kk^* where k^* is absolutely abelian. The genus number of K is defined as $g_K = [K^* : K]$. It follows right away that g_K divides h_K^+, the narrow class number of K. Since the class number h_K and the narrow class number

h_K^+ differ by a power of 2 and the genus number of a cubic field is a power of 3 (see Theorem 2.1), it follows that g_K divides h_K when K is cubic.

The class number is among the most important invariants associated to a number field, but it is very difficult to study. Conjecturally, its behavior at the "good" primes is governed by the (modified) heuristics of Cohen–Lenstra–Martinet (see [11, 12]). By contrast, the genus number (whose support is at "bad" primes) does not behave "randomly" and is therefore more amenable to study. It is very natural to ask about the density of genus number one fields among all number fields of a fixed degree and signature. In the present investigation, we will discuss the situation for cubic fields, as this is the simplest situation where this question has not been previously addressed.

Let K be a cubic field. If K is cyclic, then $g_K = 3^{e-1}$, where e is the number of odd prime factors of the discriminant Δ of K; it follows that 0% of cyclic cubic fields have genus number one, and that the average genus number in this setting is infinite. These same statistical questions become more subtle when one does not impose the restriction that K is Galois. In fact, since 0% of cubic fields are cyclic, the aforementioned facts have little bearing on the answers when one considers the collection of all cubic fields. In this paper, we show that roughly 96.23% of cubic fields have $g_K = 1$. In addition, we prove that the average genus number is roughly 1.0785.

Let $\mathcal{F}$ denote the collection of all cubic fields K with $g_K = 1$, and write $\mathcal{F}^+$, $\mathcal{F}^-$ to denote the subsets of $\mathcal{F}$ consisting of fields with positive and negative discriminants, respectively. Set $N^\pm(X) = \#\{K \in \mathcal{F}^\pm : |\Delta| \leqslant X\}$ and define constants $n^+ = 6$ and $n^- = 2$. (Note that we will always count cubic fields up to isomorphism, and isomorphic cubic fields have the same genus number.)

In Section 3, we prove our main result:

THEOREM 1.1.

$$N^\pm(X) = \frac{29}{54 n^\pm \zeta(2)} \prod_{p \equiv 2 \,(\mathrm{mod}\,3)} \left(1 + \frac{1}{p(p+1)}\right) X + O\left(X^{16/17+\varepsilon}\right).$$

COROLLARY 1.2. — *The proportion of cubic fields with genus number one (of positive or negative discriminant) equals*

$$\frac{29\,\zeta(3)}{27\,\zeta(2)} \prod_{p \equiv 2 \,(\mathrm{mod}\,3)} \left(1 + \frac{1}{p(p+1)}\right).$$

Consequently, roughly 96.23009% *of totally real cubic fields and* 96.23009% *of complex cubic fields have genus number one.*

In Section 4, we prove the following result regarding the average genus number of a cubic field:

THEOREM 1.3. — *The average genus number of a cubic field (in the positive or negative discriminant case) is given by*

$$
\lim_{X \to \infty} \frac{\sum_{0 < \pm \Delta \leqslant X} g_K}{\sum_{0 < \pm \Delta \leqslant X} 1}
$$
$$
= \frac{119\zeta(3)}{108\zeta(2)} \prod_{p \equiv 1 \,(\mathrm{mod}\, 3)} \left(1 + \frac{3}{p(p+1)}\right) \prod_{p \equiv 2 \,(\mathrm{mod}\, 3)} \left(1 + \frac{1}{p(p+1)}\right)
$$
$$
\approx 1.078541\,.
$$

The above sums are taken over all cubic fields K where the discriminant Δ falls in the specified range.

In Section 5, we give the exact proportion of cubic fields with a given genus number.

THEOREM 1.4. — *A positive proportion of cubic fields (of positive or negative discriminant) have $g_K = m$ iff m is a power of 3, and the exact proportion with $g_K = 3^k$ is given by*

$$
\frac{\zeta(3)}{\zeta(2)} \left[\frac{29}{27} \sum_{f \in T_k} \prod_{p \mid f} \frac{1}{p(p+1)} + \frac{1}{108} \sum_{f \in T_{k-1}} \prod_{p \mid f} \frac{1}{p(p+1)} \right],
$$

where T_k denotes the collection of squarefree integers coprime to 3 having exactly k prime factors p that satisfy $p \equiv 1 \pmod 3$.[1] *The approximate proportions are given in the following table:*

k	0	1	2	3
proportion	96.23%	3.72%	0.05%	*really small!*

Our initial interest in this question stemmed from the study of norm-Euclidean cubic fields. There are only finitely many norm-Euclidean cubic fields with negative discriminant, but it may very well be the case that there are infinitely many with positive discriminant (see [14, 23]). A norm-Euclidean field is necessarily class number one and, hence, genus number one; thus, if $g_K \neq 1$, we can trivially conclude that K is not norm-Euclidean. Consequently, it is of greater interest to study fields that fail to be norm-Euclidean for reasons other than genus theory. In Section 6, we prove the following result:

---

[1] If we adopt the convention that $T_{-1} = \emptyset$, then the formula holds for $k = 0$ as well.

THEOREM 1.5. — *A positive proportion of totally real cubic fields with genus number one fail to be norm-Euclidean.*

Our starting point is a theorem of Fröhlich which gives an explicit description of g_K when K is cubic. The main tool we employ is a powerful theorem, proved independently by Taniguchi–Thorne [33] and Bhargava–Shankar–Tsimerman [7], that allows one to compute the density of cubic discriminants satisfying specified local conditions with a very precise error term. This is a generalization of a classical theorem of Davenport–Heilbronn [15], who were the first to accomplish the counting of cubic fields.

In principle, our methods should work for degrees four and five as well, making use of the work of Bhargava [3, 4, 5, 6], Cohen–Diaz y Diaz–Olivier [10], Shankar–Tsimerman [32], and Ellenberg–Pierce–Wood [17]. This has been carried out for degree five [30]. The degree four case is work in progress. For any degree d, it is expected that the number of degree d number fields of discriminant up to X is asymptotic to a constant times X, but this is, as of yet, unproven. (The best known result for general d is due to Ellenberg–Venkatesh [18].) Consequently, we cannot hope to approach the "genus number one problem" when $d > 5$.

2. Preliminaries

Let K be a cubic field. Then the discriminant Δ takes one of the three forms df^2, $9df^2$, $81df^2$, where d is a fundamental discriminant and f is a squarefree positive integer coprime to 3. A prime $p \neq 3$ is totally ramified in K if and only if p divides f, and 3 is totally ramified in K if and only if Δ takes one of the forms $9df^2$, $81df^2$ [9]. The following theorem of Fröhlich gives an explicit expression for the genus number [20]; see also [24].

THEOREM 2.1 (Fröhlich). — *Let e denote the number of odd primes p such that p is totally ramified in K and $(d/p) = 1$, where (d/p) is the usual Legendre symbol. Then we have:*

$$g_K = \begin{cases} 3^{e-1} & \text{if } K \text{ is cyclic,} \\ 3^e & \text{if } K \text{ is not cyclic.} \end{cases}$$

Note that since the number of cyclic cubic fields with discriminant less than or equal to X is $O(X^{1/2})$, for our purposes we may neglect these fields [13, 21]. If K is cyclic and $g_K = 1$, then $\Delta = f^2$ where $f = 9$ or $f \equiv 1 \pmod 3$ is a prime; for each such f, there is exactly one such field. Therefore the number of cyclic cubic fields with genus number one is

$O(\pi(\sqrt{X}))$, which shows via the Prime Number Theorem that 0% of cyclic cubic fields have genus number one.

Our main tool is the following theorem, which is a strengthening of the classical Davenport–Heilbronn Theorem (see [7, 15, 33]). For what follows, set $m^+ = 1$ and $m^- = \sqrt{3}$.

THEOREM 2.2 (Taniguchi–Thorne, Bhargava–Shankar–Tsimerman). — *The number of cubic fields satisfying $0 < \pm\Delta \leqslant X$ equals*

$$\frac{1}{2n^{\pm}\zeta(3)}X + \frac{4m^{\pm}\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)}X^{5/6} + O(X^{7/9+\varepsilon}).$$

We note in passing that the secondary term was conjectured by Roberts [31] following computations carried out by Belabas [1], and that the existence of a power saving error term was first proved by Belabas–Bhargava–Pomerance in [2]; this whole story is summarized very nicely in [2].

In fact, both papers [7, 33] give a stronger version of Theorem 2.2 (which we will require) allowing one to specify local conditions. If local conditions are imposed at finitely many primes p, then the main term and the secondary term are multiplied by an additional factor for each p; moreover, in this case, the implicit constant in the O-term now depends upon the set of local conditions. For our application we need to specify infinitely many local conditions *and* we require an explicit dependence on these local conditions. In principle, either Theorem 7 of [7] or Theorem 1.3 of [33] will suffice, but the situation is such that neither accomplishes our aim "out-of-the-box" with no additional work. We have chosen to use Theorem 1.3 of [33] as our main work horse. At the appropriate juncture in our proofs, please see [33, §6] and [7, §4] for information regarding local density calculations.

Finally, we mention that there is a forthcoming paper [8] that improves the error term in Theorem 2.2 to $O(X^{2/3+\varepsilon})$. Substituting this result into our arguments would result in an improvement of our error terms.

3. Counting genus number one cubic fields

Recall that we write the discriminant of a cubic field K as $\Delta = df^2, 9df^2$, or $81df^2$ with f coprime to 3. Let $\mathcal{G}^{\pm}$ denote the collection of all cubic fields with $\text{sgn}(\Delta) = \pm 1$, and let $\mathcal{F}^{\pm} \subseteq \mathcal{G}^{\pm}$ denote the collection of all such cubic fields K with $g_K = 1$. Let $N^{\pm}(X) = \#\{K \in \mathcal{F}^{\pm} : |\Delta| \leqslant X\}$. Define

$$\mathcal{F}_1^{\pm} = \{K \in \mathcal{G}^{\pm} \mid p \equiv 2 \pmod 3 \text{ for all } p \text{ dividing } f\}$$
$$\mathcal{F}_2^{\pm} = \{K \in \mathcal{F}_1^{\pm} \mid 3 \text{ is totally ramified and } d \equiv 1 \pmod 3\}.$$

By Theorem 2.1, we have $\mathcal{F}^\pm = \mathcal{F}_1^\pm \backslash \mathcal{F}_2^\pm$, and therefore $N^\pm(X) = N_1^\pm(X) - N_2^\pm(X)$ where $N_i^\pm(X) = \#\{K \in \mathcal{F}_i^\pm : |\Delta| \leqslant X\}$. Indeed, when $p \neq 2, 3$ is totally ramified,

$$(d/p) = 1 \Longleftrightarrow p \equiv 1 \pmod{3}$$

(see [24, Example 6.10]), and, of course, $(d/3) = 1$ is equivalent to $d \equiv 1 \pmod 3$. In what follows, we will establish asymptotic formulas for $N_1^\pm(X)$, $N_2^\pm(X)$ individually and then obtain the desired result by subtraction.

For each square free f coprime to 3 we write $N^\pm(f; X)$ to denote the number of fields in $\mathcal{G}^\pm$ with $|\Delta| \leqslant X$ that are totally ramified at the primes dividing f and at no other primes, except possibly 3.

PROPOSITION 3.1.

$$N^\pm(f; X) = \frac{13}{24 n^\pm \zeta(2)} \prod_{p|f} \frac{1}{p(p+1)} X + O(f^{-1} X^{16/17+\varepsilon}).$$

Proof. — Write $M^\pm(f; X)$ to denote the number of cubic fields of positive (or negative) discriminant with $|\Delta| \leqslant X$ where all the primes dividing f are totally ramified (and no other restrictions). Observe that this constitutes only finitely many local conditions. Notice that, by the inclusion–exclusion principle,

$$N^\pm(f; X) = \sum_{(r,3f)=1} \mu(r) M^\pm(rf; X).$$

We will split this sum as $\sum_r = \sum_{r \leqslant Y} + \sum_{r > Y}$ where Y is some parameter to be specified. In all sums over r we will only consider values where $(r, 3f) = 1$. For $r \leqslant Y$, we will use Theorem 1.3 of [33] to obtain

$$M^\pm(f; X) = c_f^\pm X + d_f^\pm X^{5/6} + O(f^{16/9} X^{7/9+\epsilon}),$$

where the constant in the main term is

$$c_f^\pm = \frac{1}{2 n^\pm \zeta(3)} \prod_{p|f} \frac{1}{p^2 + p + 1},$$

and the constant in the secondary term is

$$d_f^\pm = \frac{4 m^\pm \zeta(1/3)}{5 \Gamma(2/3)^3 \zeta(5/3)} \prod_{p|f} \frac{p^{2/3} - 1}{(p^{5/3} - 1)(p - 1)} = O(f^{-2}).$$

On the other hand, when $r > Y$ we will use the estimate

$$M^\pm(f; X) = O(f^{-2+\varepsilon} X),$$

which follows immediately from Lemma 3.4 of [33], in light of the fact that $6^{\omega(f)} = O(f^\varepsilon)$. Consequently,

$$N^\pm(f;X) = \sum_{r \leqslant Y} \left(\mu(r)c_{rf}X + O((rf)^{-2}X^{5/6}) + O((rf)^{16/9}X^{7/9+\varepsilon}) \right)$$

$$+ \sum_{r > Y} O((rf)^{-2+\varepsilon}X)$$

$$= X \sum_{r \leqslant Y} \mu(r)c_{rf} + O(f^{-2}X^{5/6}) + O(Y^{25/9}f^{16/9}X^{7/9+\varepsilon})$$

$$+ O(Y^{-1+\varepsilon}f^{-2+\varepsilon}X).$$

We compute the constant in the main term:

$$\sum_{r \leqslant Y} \mu(r)c_{rf}$$

$$= \sum_r \mu(r)c_{rf} + O\left(\sum_{r > Y} c_{rf} \right)$$

$$= \frac{1}{2\zeta(3)n^\pm} \prod_{p|f} \frac{1}{p^2+p+1} \sum_{(r,3f)=1} \mu(r) \prod_{p|r} \frac{1}{p^2+p+1} + O\left(\sum_{r > Y} (rf)^{-2+\varepsilon} \right)$$

$$= \frac{1}{2\zeta(3)n^\pm} \prod_{p|f} \frac{1}{p^2+p+1} \prod_{p \nmid 3f} \left(1 - \frac{1}{p^2+p+1} \right) + O(Y^{-1+\varepsilon}f^{-2+\varepsilon})$$

$$= \frac{13}{24\zeta(3)n^\pm} \prod_{p|f} \frac{1}{p(p+1)} \prod_p \left(1 - \frac{1}{p^2+p+1} \right) + O(Y^{-1+\varepsilon}f^{-2+\varepsilon})$$

$$= \frac{13}{24\zeta(2)n^\pm} \prod_{p|f} \frac{1}{p(p+1)} + O(Y^{-1+\varepsilon}f^{-2+\varepsilon})$$

Setting $Y = f^{-1}X^{1/17}$ and putting this all together yields the result. $\qquad\square$

Let T denote the collection of all squarefree f with the property that $p \equiv 2 \pmod 3$ for all primes p dividing f. We have

$$N_1^\pm(X) = \sum_{f \in T} N^\pm(f;X)$$

$$= \sum_{\substack{f \in T \\ f \leqslant X^{1/2}}} \left(\frac{13}{24\zeta(2)n^\pm} \prod_{p|f} \frac{1}{p(p+1)} \cdot X + O(f^{-1}X^{16/17+\varepsilon}) \right)$$

$$= \frac{13}{24\zeta(2)n^{\pm}} \cdot X \sum_{f \in T} \prod_{p|f} \frac{1}{p(p+1)} + X \sum_{f > X^{1/2}} O(f^{-2})$$

$$+ \sum_{f \leqslant X^{1/2}} O(f^{-1}X^{16/17+\varepsilon})$$

(3.1) $$= \frac{13}{24\zeta(2)n^{\pm}} \prod_{p \in T} \left(1 + \frac{1}{p(p+1)}\right) \cdot X + O(X^{16/17+\varepsilon}).$$

This establishes the desired formula for $N_1^{\pm}(X)$. In order to deal with $N_2^{\pm}(X)$ we require a slight modification of the quantity $N(f; X)$. For each squarefree f coprime to 3 we write $N'(f; X)$ to denote the number of such fields that are totally ramified at 3 and the primes dividing f but no other primes *and* that also satisfy the extra condition $d \equiv 1 \pmod 3$. (For the remainder of this section we have dropped $\pm$ from most of the notation.)

PROPOSITION 3.2.
$$N'(f; X) = \frac{1}{216\zeta(2)n^{\pm}} \prod_{p|f} \frac{1}{p(p+1)} X + O(f^{-1}X^{16/17+\varepsilon}).$$

Proof. — As before, we can write

$$N'(f; X) = \sum_{(r,3f)=1} \mu(r)M'(rf; X)$$

and apply Theorem 1.3 of [33] to obtain

$$M'(f; X) = c'_f X + O(f^{-2}X^{5/6}) + O(f^{16/9}X^{7/9+\varepsilon}).$$

The calculation of c'_f is identical to that of c_f except for the local factor at the prime 3. We need to impose the additional conditions that 3 is totally ramified and $d \equiv 1 \pmod 3$. These conditions are definable in terms of congruence conditions on the coefficients of the corresponding cubic form; indeed, this is equivalent to saying $\Delta \equiv 3^4 \pmod{3^5}$.

At this juncture, computing the local densities on the "forms side" via the Delone–Fadeev correspondence is more convenient; please see [7, §4] for details regarding this type of local computation. Let S denote the collection of integral binary cubic forms having a triple root modulo 3, satisfying the maximality condition at 3, and satisfying our congruence condition on the discriminant. Let $\mu_3(S)$ denote the 3-adic density of the p-adic closure of S in $\mathbb{Z}_3^4$. (Here the additive measure μ_3 is normalized so that $\mu_3(\mathbb{Z}_3^4) = 1$.) In this notation, we have

$$c'_f = \mu_3(S)(1 - 3^{-2})^{-1}(1 - 3^{-3})^{-1}c_f.$$

All that remains is to compute $\mu_3(S)$. Since maximality is a condition modulo 3^2, we may do all our calculation modulo 3^2.

There are 8 forms over $\mathbb{Z}/3\mathbb{Z}$ with a triple root and $2/3$ of the lifts of these forms to $\mathbb{Z}/3^2\mathbb{Z}$ are maximal at 3. For each of these 432 forms, we compute the discriminant via the standard formula and then check whether the fundamental part of the discriminant satisfies $d \equiv 1 \pmod 3$. Precisely 48 of these fit the bill, in other words, $1/9$ of the forms under consideration. It follows that the 3-adic density is $\mu_3(S) = (8/3^4)(2/3)(1/9) = 16/2187$.

Observe that
$$\frac{16/2187}{(1-3^{-2})(1-3^{-3})} = 1/117,$$
which leads to
$$c'_f = \frac{1}{234\zeta(3)n^{\pm}} \prod_{p|f} \frac{1}{p^2+p+1}.$$
(The extra factor can also be computed as $(1/9)(3^2+3+1)^{-1} = 1/117$.) The rest of the proof proceeds exactly as in the proof of Proposition 3.1. $\square$

Applying the previous proposition and following the same procedure we used to obtain our formula for $N_1(X)$ yields
$$N_2(X) = X\frac{1}{216n^{\pm}\zeta(2)} \prod_{p\in T} \left(1 + \frac{1}{p(p+1)}\right) + O\left(X^{16/17+\varepsilon}\right).$$

Finally, subtracting, we have
$$N(X) = X\frac{29}{54n^{\pm}\zeta(2)} \prod_{p\equiv 2 \pmod 3} \left(1 + \frac{1}{p(p+1)}\right) + O\left(X^{16/17+\varepsilon}\right).$$

This proves Theorem 1.1, and Corollary 1.2 follows.

4. The average genus number

First, we verify that the cyclic fields do not contribute to the average. When K is cyclic, we have $\Delta \in \{f^2, (9f)^2\}$ and, by Theorem 2.1, $g_K = 3^{e-1}$; in this case, e is the number of (odd) primes that are (totally) ramified in K. Moreover, there are 2^{e-1} fields with each possible discriminant. Therefore, we have
$$\sum_{\substack{0<\pm\Delta\leqslant X \\ K\text{cyclic}}} g_K \ll \sum_{k=1}^{\infty} \pi_k(\sqrt{X})6^k,$$
where $\pi_k(y)$ denotes the number of positive integers $\leqslant y$ with exactly k prime factors. Notice that the sum on the righthand side above is finite since

$\pi_k(y) = 0$ for $k > c \log y / \log \log y$, where $c > 0$ is an absolute constant. The elementary estimate

$$\sum_{k=1}^{\varepsilon \log y} \pi_k(y) 6^k \ll y \sum_{k=1}^{\varepsilon \log y} 6^k \ll y^{1+\varepsilon}$$

leads to

$$\sum_{\substack{0 < \pm \Delta \leqslant X \\ K \text{ cyclic}}} g_K = O\left(X^{1/2+\varepsilon}\right).$$

The fact that the above expression is $o(X)$ tells us that cyclic fields do not contribute to the average genus number. Although we will not use it here, we mention in passing that estimates for $\pi_k(y)$ (see [25]) allow one to show that the sum of genus numbers above is $\gg X^{1/2}(\log X)^c$ with $c > 0$ and therefore the average genus number taken over cyclic cubic fields is infinite.

We now turn to the main part of the proof. Define $\psi(n)$ to be the number of primes p dividing n satisfying $p \equiv 1 \pmod 3$. As we are ignoring cyclic fields, everything that follows holds up to an error of $O(X^{1/2+\varepsilon})$. We have

$$\sum_{0 < \pm \Delta \leqslant X} g_K = \sum_{0 < \pm \Delta \leqslant X} 3^{\psi(f)} - {\sum_{0 < \pm \Delta \leqslant X}}' 3^{\psi(f)} + {\sum_{0 < \pm \Delta \leqslant X}}' 3^{\psi(f)+1}$$

$$= \sum_{0 < \pm \Delta \leqslant X} 3^{\psi(f)} + 2 {\sum_{0 < \pm \Delta \leqslant X}}' 3^{\psi(f)}$$

$$= {\sum_{(f,3)=1}}^{\flat} 3^{\psi(f)} N(f;X) + 2 {\sum_{(f,3)=1}}^{\flat} 3^{\psi(f)} N'(f;X),$$

where $\sum'$ denotes only summing over those fields where 3 is totally ramified with $d \equiv 1 \pmod 3$ and the $\sum^{\flat}$ denotes summing over squarefree f.

Applying Proposition 3.1 to compute the first sum above, we obtain:

$${\sum_{(f,3)=1}}^{\flat} 3^{\psi(f)} N(f;X)$$

$$= \frac{13}{24\zeta(2)n^{\pm}} X {\sum_{\substack{(f,3)=1 \\ f \leqslant X^{1/2}}}}^{\flat} 3^{\psi(f)} \prod_{p | f} \frac{1}{p(p+1)} + {\sum_{\substack{(f,3)=1 \\ f \leqslant X^{1/2}}}}^{\flat} 3^{\psi(f)} O(f^{-1} X^{16/17+\varepsilon}).$$

After performing manipulations similar to (3.1) this yields

$$\frac{13}{24n^{\pm}\zeta(2)} X \prod_{p \neq 3} \left(1 + \frac{3^{\psi(p)}}{p(p+1)}\right)$$

$$+ \sum_{f > X^{1/2}} 3^{\psi(f)} O(f^{-2} X) + \sum_{f \leqslant X^{1/2}} 3^{\psi(f)} O(f^{-1} X^{16/17+\varepsilon}).$$

The main term is

$$\frac{13}{24n^\pm\zeta(2)}X\prod_{p\equiv 1\,(\text{mod}\,3)}\left(1+\frac{3}{p(p+1)}\right)\prod_{p\equiv 2\,(\text{mod}\,3)}\left(1+\frac{1}{p(p+1)}\right).$$

Because $3^{\psi(f)}=O(f^\varepsilon)$, the error term is

$$\sum_{f>X^{1/2}}O(f^{-2+\varepsilon}X)+\sum_{f\leqslant X^{1/2}}O(f^{-1+\varepsilon}X^{16/17+\varepsilon})=O(X^{16/17+\varepsilon}).$$

In exactly the same manner, we apply Proposition 3.2 to compute the second term

$$\sum_{(f,3)=1}^{\flat}3^{\psi(f)}N'(f;X).$$

This simply results in multiplying the first outcome by a factor of $1/117$. Thus the whole sum is the first term multiplied by $1+2/117=119/117$. Hence, we obtain

$$\frac{119}{216n^\pm\zeta(2)}X\prod_{p\equiv 1\,(\text{mod}\,3)}\left(1+\frac{3}{p(p+1)}\right)\prod_{p\equiv 2\,(\text{mod}\,3)}\left(1+\frac{1}{p(p+1)}\right),$$

plus $O(X^{16/17+\varepsilon})$. Dividing the above by $1/(2n^\pm\zeta(3))$ yields the desired expression, thereby proving Theorem 1.3.

5. Counting cubic fields with given genus number

As before, $\mathcal{G}^\pm$ will denote the collection of all cubic fields with $\text{sgn}(\Delta)=\pm 1$. We now let $\mathcal{F}^\pm\subseteq\mathcal{G}^\pm$ denote the collection of all cubic fields K with $g_K=3^k$. As before, define $N^\pm(X)=\#\{K\in\mathcal{F}^\pm:|\Delta|\leqslant X\}$. Let T_k denote the collection of squarefree integers n coprime to 3 with $\psi(n)=k$ (i.e., having exactly k prime factors p satisfying $p\equiv 1\pmod 3$).

$\mathcal{F}_1^\pm=\{K\in\mathcal{G}^\pm\mid f\in T_k\}$

$\mathcal{F}_2^\pm=\{K\in\mathcal{G}^\pm\mid f\in T_k,\ 3\text{ is totally ramified, and }d\equiv 1\pmod 3\}$

$\mathcal{F}_3^\pm=\{K\in\mathcal{G}^\pm\mid f\in T_{k-1},\ 3\text{ is totally ramified, and }d\equiv 1\pmod 3\}.$

By Theorem 2.1, we have $\mathcal{F}^\pm=(\mathcal{F}_1^\pm\setminus\mathcal{F}_2^\pm)\cup\mathcal{F}_3^\pm$, and therefore $N^\pm(X)=N_1^\pm(X)-N_2^\pm(X)+N_3^\pm(X)$ where $N_i^\pm(X)=\#\{K\in\mathcal{F}_i^\pm:|\Delta|\leqslant X\}$. Now we can proceed exactly as in Section 3 to find

$$N_1^\pm(X)=\frac{13}{24\zeta(2)n^\pm}X\sum_{f\in T_k}\prod_{p\mid f}\frac{1}{p(p+1)}+O(X^{16/17+\varepsilon})$$

and we multiply by $1/117$ to obtain

$$N_2^{\pm}(X) = \frac{1}{216\zeta(2)n^{\pm}} X \sum_{f \in T_k} \prod_{p|f} \frac{1}{p(p+1)} + O(X^{16/17+\varepsilon}).$$

Similarly, we obtain

$$N_3^{\pm}(X) = \frac{1}{216\zeta(2)n^{\pm}} X \sum_{f \in T_{k-1}} \prod_{p|f} \frac{1}{p(p+1)} + O(X^{16/17+\varepsilon}),$$

and this makes the desired proportion equal to

$$\frac{\zeta(3)}{\zeta(2)} \left[\frac{29}{27} \sum_{f \in T_k} \prod_{p|f} \frac{1}{p(p+1)} + \frac{1}{108} \sum_{f \in T_{k-1}} \prod_{p|f} \frac{1}{p(p+1)} \right].$$

We include here a table of approximations to the first few percentages.

k	0	1	2	3
proportion	96.23%	3.72%	0.05%	really small!

This concludes the proof of Theorem 1.4.

We note that the formulas for $N_1^{\pm}$, $N_2^{\pm}$, $N_3^{\pm}$ just derived can essentially be used to establish Theorems 1.1, 1.3, and 1.4 but we have chosen to structure the paper in this manner for clarity of exposition.

6. Norm-Euclidean cubic fields

Davenport showed that there are only finitely many norm-Euclidean cubic fields with negative discriminant [14]. Heilbronn showed that there are only finitely many norm-Euclidean cyclic cubic fields with positive discriminant [23], and the first author completely determined these fields under the GRH [28, 29]. This leaves open the case of non-cyclic totally real cubic fields. In fact, Heilbronn says that he would "be surprised to learn that the analogue of [the finiteness theorem] is true in this case". Lemmermeyer carried out computations (up to discriminant $1.3 \cdot 10^4$) in this setting (see [26]) and observed that the percentage of norm-Euclidean fields was decreasing, and consequently he stated that "it is tempting to conjecture that the norm-Euclidean cubic fields have density 0."

This leads to the following problem: Give an upper bound on the proportion of totally real cubic fields that are norm-Euclidean. To our knowledge, no one has given a nontrivial upper bound in this setting, i.e., a bound less than 100%. The first thing one might try to do is to use genus theory; in light of Corollary 1.2, one knows that less than 96.24% of totally real cubic

fields are norm-Euclidean. The question then is whether one can improve on the upper bound coming from genus theory. Theorem 1.5 accomplishes this, albeit very modestly. In order to give our results in more detail, we must first state Heilbronn's criterion in our situation.

Let K be a totally real cubic field, and adopt the previous notation for Δ, d, f. Denote by F the product of all the totally ramified primes in K. Notice that $F = f$ or $F = 3f$ depending upon whether 3 is totally ramified. The following is the natural adaptation to our setting of a result of Heilbronn on cyclic cubic fields, which has its roots in a theorem of Erdös–Ko [19]; it is also a special case of a more general theorem due to Egami [16] who attributed it to Lenstra.

LEMMA 6.1 (Heilbronn's criterion). — *If we can write $F = a + b$ with $a, b \in \mathbb{Z}^+$ where a, b are not norms and a is a cubic residue modulo F, then K is not norm-Euclidean.*

One amusing observation is that if $p \not\equiv 1 \pmod 3$ then every number is a cubic residue modulo p, so Heilbronn's criterion is more easily verified in the genus number one setting (where all p dividing F have this property).

LEMMA 6.2. — *Suppose K has genus number one. If we can write $F = a+b$ with $a, b \in \mathbb{Z}^+$ where a, b are not norms, then K is not norm-Euclidean.*

Let $H(X)$ denote the number of genus number one cubic fields with $0 < \Delta \leqslant X$ to which Heilbronn's criterion applies, and let $H(F; X)$ denote the number of such fields with fixed F. We have

$$H(X) = \sum_{F \leqslant X^{1/2}} H(F; X)$$

PROPOSITION 6.3. — *We have*

$$H(F; X) = \frac{b_F}{12\zeta(2)} \prod_{p \mid F} \frac{1}{p(p+1)} X + O(e^F X^{16/17+\varepsilon})$$

for some explicitly computable $b_F \in \mathbb{Q} \cap [0, 1]$.

F	1	2	3	5	6	10	11	15	17	22
b_F	0	0	0	$\frac{1}{18}$	0	$\frac{7}{96}$	$\frac{55}{288}$	$\frac{1574}{15309}$	$\frac{231205}{653184}$	$\frac{1292771}{4354560}$
$\approx$	0	0	0	0.0556	0	0.0729	0.191	0.103	0.354	0.297

Using the previous proposition, we will prove the main result of this section which immediately implies Theorem 1.5.

THEOREM 6.4. — *We have $H(X) \sim BX$ with $5.7 \cdot 10^{-4} \leqslant B \leqslant 6.1 \cdot 10^{-4}$. Consequently, Heilbronn's criterion applies to strictly between $4/5$ of a percent and 1 percent of all totally real cubic fields with genus number one.*

Admittedly, the proportion in the previous theorem is rather small. The main interest here is to know that such a density exists and is positive. We obtain the rather weak corollary that less than 96% of totally real cubic fields are norm-Euclidean. However, this theorem does say something about the limitations of these methods; in particular, one cannot hope to beat 95% by using only genus theory and totally ramified primes (via Lemma 6.1) — one would need to inject some new ideas. In principle, one could use the ideas presented here to compute B more accurately, but we have not pursued this (because of the reasons just mentioned).

Remark 6.5. — Even though the total proportion given in Theorem 6.4 is rather small, if we only consider fields where F is large we can give much stronger results. For example, when $F = 167$, we compute $b_F \approx 0.9421$. In fact, the precise number is:

$$\frac{5707366742127207720711393876905481748779979640006818006913}{6058037125307413601957148346537399067112071383363249766400}$$

The upshot is the following: Suppose we know that 167 is the only totally ramified prime in K. Then K has less than a 5.8% chance of being norm-Euclidean.

Before launching into the proofs, we recast Heilbronn's criterion into a form that is more convenient for our purposes. We define the set

$$S = \{a \in \mathbb{Z} \mid 0 < a < F, \, a \notin N_{K/\mathbb{Q}}(\mathcal{O}_K)\},$$

and rewrite the condition in Heilbronn's criterion as

$$(\dagger) \qquad\qquad \exists \, a \in S \text{ such that } F - a \in S.$$

Recall that $n \neq 0$ is a norm if and only if $3 \mid v_p(n)$ for all inert $p \mid n$. In light of this, we immediately see that $(\dagger)$ holds iff there exists an $a \in (0, F)$ and a pair of inert primes $\{p, q\}$ such that $p \mid a$, $q \mid F - a$, and $3 \nmid v_p(a) v_q(F - a)$. If this condition is satisfied, we call the set of two primes $\{p, q\}$ a Heilbronn pair for F.

Example 6.6. — We find all the Heilbronn pairs for $F = 11$. By symmetry, there are 5 possible choices of $(a, F - a)$ we must consider. We can reject the values $(1, 10)$ and $(3, 8)$ because they contain cubes, which leaves three remaining choices for $(a, F - a)$. The choice $(2, 9)$ leads to the H-pair

$\{2,3\}$, the choice $(4,7)$ leads to the H-pair $\{2,7\}$, and the choice $(5,6)$ leads to the H-pairs $\{5,2\}$, $\{5,3\}$. In summary, the Heilbronn pairs for $F = 11$ are $\{2,3\}$, $\{2,5\}$, $\{2,7\}$, $\{3,5\}$. This means Heilbronn's criterion applies to a cubic field K with $F = 11$ if and only if the collection of primes that are inert in K contains at least one of these four H-pairs.

Let $\mathcal{I}$ be a subset of the primes p with $p < F$ and $(p, F) = 1$. We say that $\mathcal{I}$ is admissible if it contains both primes in a Heilbronn pair. Let $H(F, \mathcal{I}; X)$ denote the number of cubic fields with fixed F satisfying $0 < \Delta \leqslant X$ such that $\mathcal{I}$ is exactly the inert primes less than F. In light of discussion above, we have

$$(6.1) \qquad H(F; X) = \sum_{\mathcal{I} \text{ admissible}} H(F, \mathcal{I}; X).$$

PROPOSITION 6.7. — *Suppose 3 is not totally ramified in K. Then*

$$H(f, \mathcal{I}; X) = \frac{1}{12\zeta(2)} \prod_{p \mid f} \frac{1}{p(p+1)} \prod_{\substack{p < f \\ p \nmid f}} \frac{a_p}{1 + p^{-1}} X + O(e^f X^{16/17 + \varepsilon})$$

where

$$a_p = \begin{cases} 1/3 & p \in \mathcal{I}, \\ 2/3 + 1/p & p \notin \mathcal{I}. \end{cases}$$

Proof. — Note that our hypothesis gives $\Delta = df^2$. We follow the same procedure as Proposition 3.1. However, this time there are many more local conditions being imposed. We impose the conditions:

(1) p is totally ramified for all $p \mid f$;
(2) p is either inert (if in $\mathcal{I}$) or not inert but not totally ramified (not in $\mathcal{I}$) for all $p < f$ with $p \nmid f$;
(3) p is not totally ramified for all $p > f$ (via inclusion–exclusion).

The constant in the main term is thus:

$$\frac{1}{12\zeta(3)} \prod_{p \mid f} \frac{1/p^2}{1 + p^{-1} + p^{-2}} \prod_{\substack{p < f \\ p \nmid f}} \frac{a_p}{1 + p^{-1} + p^{-2}} \sum_{\substack{r > f \\ (r, \Pi_{p \leqslant f} p) = 1}} \mu(r) \prod_{p \mid r} \frac{1}{p^2 + p + 1}$$

$$= \frac{1}{12\zeta(3)} \prod_{p \mid f} \frac{1}{p^2 + p + 1} \prod_{\substack{p < f \\ p \nmid f}} \frac{a_p}{1 + p^{-1} + p^{-2}} \prod_{p > f} \left(1 - \frac{1}{p^2 + p + 1} \right)$$

$$= \frac{1}{12\zeta(2)} \prod_{p|f} \frac{1}{p^2+p+1} \prod_{\substack{p<f \\ p\nmid f}} \frac{a_p}{1+p^{-1}+p^{-2}} \prod_{p\leqslant f} \left(1 - \frac{1}{p^2+p+1}\right)^{-1}$$

$$= \frac{1}{12\zeta(2)} \prod_{p|f} \frac{1}{p(p+1)} \prod_{\substack{p<f \\ p\nmid f}} \frac{a_p}{1+p^{-1}} \,.$$

When the smoke clears, the error term is equal to

$$O(f^{-2}X^{5/6}) + O(Y^{25/9}f^{8/9}e^f X^{7/9+\varepsilon}) + O(Y^{-1+\varepsilon}f^{-2+\varepsilon}X)\,.$$

The middle O-term above comes from the estimate

$$\prod_{p|f} \left(p^2\right)^{8/9} \prod_{\substack{p<f \\ p\nmid f}} p^{8/9} = f^{8/9} \exp\left((8/9)\theta(f)\right) \leqslant f^{8/9}\exp(f)\,.$$

Setting $Y = X^{1/17}f^{-13/17}e^{-9f/34}$ yields the error term

$$O(f^{-21/17+\varepsilon}e^{9f/34}X^{16/17+\varepsilon})\,. \qquad \square$$

If 3 is totally ramified in K, then the previous proposition still holds, but with f replaced by $F = 3f$ and the constant in the main term multiplied by a factor of $8/9$.

Example 6.8. — We return to our example of $F = 11$. We saw that the four H-pairs in this situation are $\{2,3\}$, $\{2,5\}$, $\{2,7\}$, $\{3,5\}$. Consequently, there are 9 admissible sets $\mathcal{I}$; namely: $\{2,3\}$, $\{2,3,5\}$, $\{2,3,7\}$, $\{2,3,5,7\}$, $\{2,5\}$, $\{2,5,7\}$, $\{2,7\}$, $\{3,5\}$, $\{3,5,7\}$. Consider for the moment the choice $\mathcal{I} = \{2,3,5\}$. In this situation, the extra factor is

$$\frac{1/3}{1+2^{-1}} \cdot \frac{1/3}{1+3^{-1}} \cdot \frac{1/3}{1+5^{-1}} \cdot \frac{2/3+1/7}{1+7^{-1}} = \frac{85}{7776}$$

and hence Proposition 6.7 yields

$$H(F,\mathcal{I};X) \sim \frac{85}{7776} \cdot \frac{1}{12\zeta(2)} \prod_{p|f} \frac{1}{p(p+1)} X$$

For each admissible $\mathcal{I}$ we get an additional rational factor; summing over all admissible $\mathcal{I}$ yields:

$$H(F;X) \sim \frac{55}{288} \cdot \frac{1}{12\zeta(2)} \prod_{p|f} \frac{1}{p(p+1)} X$$

Proof of Proposition 6.3. — This follows immediately from Proposition 6.7 since the sum appearing in (6.1) is finite. The calculation of the b_F

is along the lines of the previous example; namely, when F is not divisible by 3,

$$b_F = \sum_{\mathcal{I} \text{ admissible}} \prod_{\substack{p < F \\ p \nmid F}} \frac{a_p}{1 + p^{-1}},$$

and b_F is equal to the same expression times $8/9$ when F is divisible by 3. $\square$

Proof of Theorem 6.4. — Using Proposition 6.3 for $F < Y$ we obtain:

$$H(X) = \sum_{F < Y} H(F; X) + \sum_{F > Y} O(F^{-2+\varepsilon} X)$$

$$= \frac{1}{12\zeta(2)} X \sum_F b_F \prod_{p | f} \frac{1}{p(p+1)}$$

$$+ \sum_{F < Y} O(e^F X^{16/17+\varepsilon}) + \sum_{F > Y} O(F^{-2+\varepsilon} X)$$

$$= \frac{1}{12\zeta(2)} X \sum_F b_F \prod_{p | f} \frac{1}{p(p+1)} + O(e^Y X^{16/17+\varepsilon}) + O(Y^{-1+\varepsilon} X)$$

Choosing Y to be a small power of $\log X$ proves the result with

$$B = \frac{1}{12\zeta(2)} \sum_F b_F \prod_{p | f} \frac{1}{p(p+1)}. \qquad \square$$

Acknowledgements

BIBLIOGRAPHY

[1] K. Belabas, "A fast algorithm to compute cubic fields", *Math. Comput.* **66** (1997), no. 219, p. 1213-1237.

[2] K. Belabas, M. Bhargava & C. Pomerance, "Error estimates for the Davenport-Heilbronn theorems", *Duke Math. J.* **153** (2010), no. 1, p. 173-210.

[3] M. Bhargava, "Higher composition laws. III. The parametrization of quartic rings", *Ann. Math.* **159** (2004), no. 3, p. 1329-1360.

[4] ———, "The density of discriminants of quartic rings and fields", *Ann. Math.* **162** (2005), no. 2, p. 1031-1063.

[5] ———, "Higher composition laws. IV. The parametrization of quintic rings", *Ann. Math.* **167** (2008), no. 1, p. 53-94.

[6] ———, "The density of discriminants of quintic rings and fields", *Ann. Math.* **172** (2010), no. 3, p. 1559-1591.

[7] M. BHARGAVA, A. SHANKAR & J. TSIMERMAN, "On the Davenport-Heilbronn theorems and second order terms", *Invent. Math.* **193** (2013), no. 2, p. 439-499.

[8] M. BHARGAVA, T. TANIGUCHI & F. THORNE, "Improved error estimates for the Davenport-Heilbronn theorems", https://arxiv.org/abs/2107.12819, 2021.

[9] H. COHEN, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer, 1993, xii+534 pages.

[10] H. COHEN, F. DIAZ Y DIAZ & M. OLIVIER, "Enumerating quartic dihedral extensions of ℚ", *Compos. Math.* **133** (2002), no. 1, p. 65-93.

[11] H. COHEN & H. W. LENSTRA, JR., "Heuristics on class groups of number fields", in *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, Lecture Notes in Mathematics, vol. 1068, Springer, 1984, p. 33-62.

[12] H. COHEN & J. MARTINET, "Class groups of number fields: numerical heuristics", *Math. Comput.* **48** (1987), no. 177, p. 123-137.

[13] H. COHN, "The density of abelian cubic fields", *Proc. Am. Math. Soc.* **5** (1954), p. 476-477.

[14] H. DAVENPORT, "Euclid's algorithm in cubic fields of negative discriminant", *Acta Math.* **84** (1950), p. 159-179.

[15] H. DAVENPORT & H. A. HEILBRONN, "On the density of discriminants of cubic fields. II", *Proc. R. Soc. Lond., Ser. A* **322** (1971), no. 1551, p. 405-420.

[16] S. EGAMI, "On finiteness of the numbers of Euclidean fields in some classes of number fields", *Tokyo J. Math.* **7** (1984), no. 1, p. 183-198.

[17] J. S. ELLENBERG, L. B. PIERCE & M. M. WOOD, "On ℓ-torsion in class groups of number fields", *Algebra Number Theory* **11** (2017), no. 8, p. 1739-1778.

[18] J. S. ELLENBERG & A. VENKATESH, "The number of extensions of a number field with fixed degree and bounded discriminant", *Ann. Math.* **163** (2006), no. 2, p. 723-741.

[19] P. ERDÖS & C. KO, "Note on the Euclidean Algorithm", *J. Lond. Math. Soc.* **S1-13** (1938), no. 1, p. 3.

[20] A. FRÖLICH, "The genus field and genus group in finite number fields. I, II", *Mathematika* **6** (1959), p. 40-46, 142-146.

[21] H. HASSE, "Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage", *Math. Z.* **31** (1930), no. 1, p. 565-582.

[22] ———, "Zur Geschlechtertheorie in quadratischen Zahlkörpern", *J. Math. Soc. Japan* **3** (1951), p. 45-51.

[23] H. A. HEILBRONN, "On Euclid's algorithm in cubic self-conjugate fields", *Proc. Camb. Philos. Soc.* **46** (1950), p. 377-382.

[24] M. ISHIDA, *The genus fields of algebraic number fields*, Lecture Notes in Mathematics, vol. 555, Springer, 1976, vi+116 pages.

[25] E. LANDAU, *Elementary number theory*, Chelsea Publishing, 1958, Translated by J. E. Goodman, 256 pages.

[26] F. LEMMERMEYER, "The Euclidean algorithm in algebraic number fields", *Expo. Math.* **13** (1995), no. 5, p. 385-416.

[27] H. W. LEOPOLDT, "Zur Geschlechtertheorie in abelschen Zahlkörpern", *Math. Nachr.* **9** (1953), p. 351-362.

[28] K. J. MCGOWN, "Norm-Euclidean cyclic fields of prime degree", *Int. J. Number Theory* **8** (2012), no. 1, p. 227-254.

[29] ———, "Norm-Euclidean Galois fields and the generalized Riemann hypothesis", *J. Théor. Nombres Bordeaux* **24** (2012), no. 2, p. 425-445.

[30] K. J. McGown, F. Thorne & A. Tucker, "Counting quintic fields with genus number one", https://arxiv.org/abs/2006.12991, 2020.

[31] D. P. Roberts, "Density of cubic field discriminants", *Math. Comput.* **70** (2001), no. 236, p. 1699-1705 (electronic).

[32] A. Shankar & J. Tsimerman, "Counting S_5-fields with a power saving error term", *Forum Math. Sigma* **2** (2014), article no. e13 (8 pages).

[33] T. Taniguchi & F. Thorne, "Secondary terms in counting functions for cubic fields", *Duke Math. J.* **162** (2013), no. 13, p. 2451-2508.

Kevin J. MCGOWN
California State University, Chico (USA)
kmcgown@csuchico.edu

Amanda TUCKER
University of Rochester (USA)
abeeson@ur.rochester.edu