ERROR ESTIMATES FOR THE DAVENPORT–HEILBRONN THEOREMS

KARIM BELABAS, MANJUL BHARGAVA, AND CARL POMERANCE

ABSTRACT. We obtain the first known power-saving remainder terms for the theorems of Davenport and Heilbronn on the density of discriminants of cubic fields and the mean number of 3-torsion elements in the class groups of quadratic fields. In addition, we prove analogous error terms for the density of discriminants of quartic fields and the mean number of 2-torsion elements in the class groups of cubic fields. These results prove analytic continuation of the related Dirichlet series to the left of the line $\Re(s) = 1$.

1. INTRODUCTION

Our primary goal is to prove the following theorems.

Theorem 1.1. *For any $\varepsilon > 0$, the number of isomorphism classes of cubic fields whose discriminant D satisfies $0 < D < X$ is*

$$\frac{1}{12\zeta(3)}X + O\big(X^{7/8+\varepsilon}\big), \tag{1}$$

and the number of isomorphism classes of cubic fields whose discriminant D satisfies $0 < -D < X$ is

$$\frac{1}{4\zeta(3)}X + O\big(X^{7/8+\varepsilon}\big). \tag{2}$$

Theorem 1.2. *Let D denote the discriminant of a quadratic field and let $\mathrm{Cl}_3(D)$ denote the 3-torsion subgroup of the ideal class group $\mathrm{Cl}(D)$ of D. For any $\varepsilon > 0$,*

$$\sum_{0<D<X} \#\,\mathrm{Cl}_3(D) = \frac{4}{3}\sum_{0<D<X} 1 + O\big(X^{7/8+\varepsilon}\big) \tag{3}$$

and

$$\sum_{0<-D<X} \#\,\mathrm{Cl}_3(D) = 2\sum_{0<-D<X} 1 + O\big(X^{7/8+\varepsilon}\big). \tag{4}$$

The main terms in both of these theorems were obtained in the seminal work of Davenport and Heilbronn [16]. The first attempted computational verifications of the Davenport–Heilbronn theorems were carried out in 1988 by Llorente and Quer [26], who tabulated all real cubic fields up to discriminant 10^7. Even up to this large discriminant they found, somewhat surprisingly, that there are fewer than 86% as many fields as predicted by the Davenport–Heilbronn main term. This work was followed up in 1990 and 1994 by Fung and Williams [19], who tabulated complex cubic fields up to absolute discriminant 10^6; they again found fewer number fields than suggested by the main term, in fact less than 88% as many

1991 *Mathematics Subject Classification.* 11R11, 11R29, 11R45.

fields. These computations suggested that the convergence to the main term in the Davenport–Heilbronn theorem was perhaps rather slow, thus raising questions about the magnitude of the error term.[1]

In 1997, the first author [1] computed cubic fields to absolute discriminant 10^{11}. The computations were found to agree far better with the asymptotics of Davenport–Heilbronn, and were enough for the author to hypothesize an error term that is smaller than $O(X/(\log X)^a)$ for any fixed a. A remainder estimate somewhat better than $O(X\exp(-\sqrt{\log X}))$ later appeared in [2].

In 2001, it was conjectured by Roberts [31] that (1), (2) and possibly (3), (4) hold with an error term of $O(X^{5/6})$, indeed with an explicit second term in $X^{5/6}$. The computations of discriminants of cubic fields to $X = 10^{11}$ in [1] strikingly support this conjecture, while the computations, also to 10^{11}, of 3-ranks of class groups of imaginary quadratic fields in [25], [24] are also supportive.

Theorems 1.1 and 1.2 represent the first known theoretical results exhibiting "power-saving" error terms in the Davenport–Heilbronn theorems.

Our techniques also allow us to prove analogous power-saving error terms in the quartic case.

Theorem 1.3. *For any $\varepsilon > 0$ and for $i = 0, 1, 2$, the number of isomorphism classes of S_4-quartic fields having $4 - 2i$ real embeddings, $2i$ complex embeddings, and absolute discriminant less than X is*

$$\begin{aligned} &\frac{\beta}{48}\cdot X + O(X^{23/24+\varepsilon}) && \text{if } i = 0;\\ &\frac{\beta}{8}\cdot X + O(X^{23/24+\varepsilon}) && \text{if } i = 1;\\ &\frac{\beta}{16}\cdot X + O(X^{23/24+\varepsilon}) && \text{if } i = 2, \end{aligned}$$

where $\beta = \prod_p (1 + p^{-2} - p^{-3} - p^{-4})$.

Theorem 1.4. *Let K_3 denote a cubic field, and let $\mathrm{Cl}_2(K_3)$ denote the 2-torsion subgroup of the ideal class group $\mathrm{Cl}(K_3)$ of K_3. For any $\varepsilon > 0$,*

$$\sum_{0<\mathrm{Disc}(K_3)<X} \#\,\mathrm{Cl}_2(K_3) = \frac{5}{4}\sum_{0<\mathrm{Disc}(K_3)<X} 1 \;+\; O\big(X^{23/24+\varepsilon}\big) \tag{5}$$

and

$$\sum_{0<-\mathrm{Disc}(K_3)<X} \#\,\mathrm{Cl}_2(K_3) = \frac{3}{2}\sum_{0<-\mathrm{Disc}(K_3)<X} 1 \;+\; O\big(X^{23/24+\varepsilon}\big). \tag{6}$$

[1]Concerning the count of Fung and Williams, they wrote, rather poetically: "Davenport and Heilbronn have proved a theorem which says that this density should approach the asymptotic limit of $(4\zeta(3))^{-1} \approx .20798$. If however, the reader were to plot the [empirical] density, he would be somewhat astonished to see that this density is increasing so slowly that his first impression would be that it will not make it to the Davenport–Heilbronn limit. Thus it remains a challenging problem, assuming the Davenport–Heilbronn limit is not in error, to explain the origin of this slow convergence. ... [O]n the real side, ... the problem is further aggravated by even slower convergence. To date, and to our knowledge, no good quantitative explanation of this phenomenon has been given."

The main terms of both these theorems appeared in [6]. There are exact counts to $X = 10^7$ of S_4-quartic fields in [9] and to $X = 10^9$ of totally real S_4-quartic fields in [27] that show a fairly leisurely convergence to the asymptotic limits in Theorem 1.3. The magnitude of the gap from the main term appears to grow like a power of X, but in contrast to the cubic case there does not appear to be a strong signal in the data for a sharp secondary term. In fact, anything from a term of order $X^{5/6} \log X$ to $X^{7/8}$ seems possible. As suggested in [10], there may be several error terms, with the most dominant only marginally so at computed levels. Though our error exponent $23/24$ is only slightly less than 1, it comes in the face of some pessimism on this topic, as Cohen wrote in [8]: "Here it is hopeless to think that one may *prove* anything."

The story regarding the asymptotics of 2-torsion in the class groups of cubic fields is quite interesting. The values $5/4$ and $3/2$ occurring in Theorem 1.4 were first predicted by the Cohen–Martinet heuristics (the analogues of the Cohen–Lenstra heuristics for noncyclic, higher degree fields). However, after the computations of Ennola and Turunen [18] on the sizes of 2-torsion subgroups of class groups of totally real cubic fields of discriminant less than 10^5 were published, there was much skepticism surrounding these heuristics especially at the prime 2 for class groups of cubic fields (even by Cohen and Martinet themselves; see [11]). Thus it came as somewhat of a surprise that the asymptotic formulas originally predicted by Cohen–Martinet are in fact correct. Theorem 1.4 states that not only are the main terms of these asymptotic formulas correct, but they in fact come with a power-saving error term.

There is a recent further twist to the story. More extensive computations have led Malle [28] to propose revised heuristics for the distribution of 2-ranks of class groups of cubic fields. However, these new densities do in fact yield the same predictions for *average* 2-torsion as the original Cohen–Martinet heuristics. When comparing the actual numbers with those predicted by the main term in Theorem 1.4, the error appears to grow like a power of X, but as with the situation of quartic fields mentioned above, there is not a clear signal as to a sharp secondary term. It is possible that there is a term of shape $X^{5/6} \log X$ with a smaller, but not negligible, tertiary term or terms.

For $n > 1$, let $\xi_n(s) := \sum_K |\operatorname{Disc} K|^{-s}$ where K runs over the isomorphism classes of number fields of degree n. In [7], Cohen asked whether the Dirichlet series ξ_n can be analytically continued even to the line $\Re(s) = 1$. This was known only for $n = 2$ previously. Theorems 1.1 and 1.3 (together with the known results for smaller Galois groups; see, e.g., [10] for a survey) also prove analytic continuation of $\xi_3(s)$ and $\xi_4(s)$, to $\Re(s) > 7/8$ and $\Re(s) > 23/24$ respectively, with simple poles located at $s = 1$.

Acknowledgments: This work was initiated at the "Explicit Methods in Number Theory" conference in Oberwolfach's math institute (July 2003), organized by H. Cohen, H. W. Lenstra Jr., and D. Zagier. We would like to thank the institute for its hospitality. The second author was supported by a Long-Term Prize Fellowship from the Clay Mathematics Institute. The third author was supported in part by NSF grant DMS-0703850.

2. Cubic fields

Throughout this paper, p denotes a prime number, q a squarefree positive integer, $\omega(n)$ is the number of distinct prime divisors of n and μ is the Möbius function, so that $\mu(n) = (-1)^{\omega(n)}$ for a squarefree n and 0 otherwise.

2.1. **Sketch.** A *ring of rank* k is a commutative ring with unit that is free of rank k as a $\mathbb{Z}$-module. Rings of rank 2, 3, and 4 are called *quadratic*, *cubic*, and *quartic rings* respectively. The *discriminant* of a ring $\mathcal{O}$ of rank k is defined as usual as the determinant of its "trace form" $\langle x, y\rangle = \mathrm{Tr}(xy)$ (see, e.g., [5, §2] for further details).

An *order* is a ring $\mathcal{O}$ of some finite rank k which is also an integral domain. Its field of fractions $K = \mathrm{Frac}(\mathcal{O}) = \mathcal{O} \otimes \mathbb{Q}$ is thus a number field, whose maximal order is denoted $\mathcal{O}_K$. More generally, if $\mathcal{O}$ is any ring of finite rank having nonzero discriminant, then $K = \mathcal{O} \otimes \mathbb{Q}$ is an étale extension of $\mathbb{Q}$, i.e., a direct sum of number fields, and its maximal order is denoted $\mathcal{O}_K$. The *index* of such a ring $\mathcal{O}$ is $(\mathcal{O}_K : \mathcal{O})$, the cardinality of the finite abelian group $\mathcal{O}_K/\mathcal{O}$.

The *content* of a ring $\mathcal{O}$ of rank k is the largest integer c such that $\mathcal{O}/\mathbb{Z} \cong c \cdot (\mathcal{O}'/\mathbb{Z})$ for some ring $\mathcal{O}'$ of rank k; we say the content of $\mathcal{O}$ is ∞ if there is no such largest integer. If the content c of $\mathcal{O}$ is finite, then the "principal part" $\mathcal{O}'$ is unique. Furthermore, if $\mathcal{O}$ has finite content c and index q, then $\mathcal{O}'$ has content 1 and index q/c^2. The ring $\mathcal{O}$ is said to be *primitive* if its content is 1. By "nondegenerate", we mean "having nonzero discriminant".

The crux of our method is the following result, due to Delone–Faddeev [17], which was later refined to apply also to degenerate rings by Gan–Gross–Savin [20].

Theorem 2.1. *The isomorphism classes of cubic rings are in bijection with the classes of integral binary cubic forms modulo* $\mathrm{GL}(2,\mathbb{Z})$. *The bijection preserves discriminant and content. In particular, it associates nondegenerate rings to nondegenerate forms, and primitive rings to primitive forms. Furthermore, it associates orders to irreducible forms.*

We recall that $G = \mathrm{GL}(2,\mathbb{R})$ acts on the vector space V of binary forms over $\mathbb{R}$ via

$$(\gamma \cdot F)(x, y) = (\mathrm{Det}\,\gamma)^{-1} F\big((x, y) \cdot \gamma\big).$$

The action of G on V has two orbits of nonzero discriminant, namely, V^+, consisting of those elements having positive discriminant, and V^-, consisting of the elements having negative discriminant.

Instead of cubic fields, we count isomorphism classes of their maximal orders, which are associated to certain $\mathrm{GL}(2,\mathbb{Z})$-orbits on $V_\mathbb{Z}$, the lattice in V consisting of integral cubic forms. Davenport and Heilbronn [16] gave a local characterization of these "maximal" classes (see also [3, 4]). Via reduction theory for binary cubics using Siegel sets (see [4]), we are eventually reduced to counting integral points, satisfying suitable congruences, in certain semi-algebraic sets in V.

2.2. **Orders of large index.** Let $N^\pm(q, X)$ denote the number of isomorphism classes of cubic orders of index divisible by q, whose discriminant D satisfies $0 < \pm D < X$, respectively. We require an upper bound for $N^\pm(q, X)$.

Lemma 2.2. *Letting* $n_+ = 6$ *and* $n_- = 2$, *we have*

$$N^\pm(1, X) \;=\; \frac{\pi^2}{12 n_\pm} X + O(X^{5/6}).$$

In particular, $N^{\pm}(1, X) = O(X)$.

The main term in Lemma 2.2 was obtained in [15], while the error term appeared in [32] (see also [4]).

Lemma 2.3. *For a fixed order* $\mathcal{O}$ *and* $n \in \mathbb{Z}_{>0}$, *let* $\mathrm{Ord}(\mathcal{O}, n)$ *denote the set of suborders* $\mathcal{O}'$ *of* $\mathcal{O}$ *with* $(\mathcal{O} : \mathcal{O}') = n$, *and let* $\psi(\mathcal{O}, n) := \#\,\mathrm{Ord}(\mathcal{O}, n)$. *Then* $n \mapsto \psi(\mathcal{O}, n)$ *is a multiplicative function.*

Proof. If $(a, b) = 1$, the map

$$\mathrm{Ord}(\mathcal{O}, a) \times \mathrm{Ord}(\mathcal{O}, b) \to \mathrm{Ord}(\mathcal{O}, ab),$$

where $(A, B) \mapsto A \cap B$, is a bijection. □

Lemma 2.4. *Let* $\mathcal{O}$ *be a fixed cubic order and* q *a squarefree integer coprime to the content of* $\mathcal{O}$. *The number of suborders of* $\mathcal{O}$ *with index* q *is bounded by* $3^{\omega(q)}$.

Proof. Since $n \mapsto \psi(\mathcal{O}, n)$ is multiplicative, we can assume that $q = p$ is prime. Let F be a representative of the class of forms associated to $\mathcal{O}$. The suborders of prime index p of $\mathcal{O}$ are associated to the roots of F in $\mathbb{P}^1(\mathbb{F}_p)$. More precisely, if $\mathcal{O} = \langle 1, u, v\rangle_{\mathbb{Z}}$, a suborder $\mathcal{O}' = \langle 1, u', v'\rangle_{\mathbb{Z}}$ of index p in $\mathcal{O}$ is given by $(u', v') = (u, v)M$, where $M = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} p & b \\ 0 & 1 \end{smallmatrix}\right)$, for some $0 \le b < p$. This submodule is a subring if and only if $F \circ M \equiv 0 \pmod{p}$. This amounts to $(b : 1)$ or $(1 : 0)$ being a root of $F \pmod{p}$. There are at most $\deg(F) = 3$ such roots, since the content of F is coprime to p, so that $F \not\equiv 0 \pmod{p}$. □

The assumption on the content is necessary: if it is divisible by a prime p, then all $p + 1$ submodules of index p in $\mathcal{O}$ are subrings.

Remark 2.5. A formula of Datskovsky and Wright [12] asserts that the generating function for the orders of index n in a fixed maximal cubic order $\mathcal{O}_K$ is

$$\eta_K(s) := \sum_{n \ge 1} \psi(\mathcal{O}_K, n) n^{-s} = \frac{\zeta_K(s)}{\zeta_K(2s)} \zeta(3s - 1)\zeta(2s), \tag{7}$$

where ζ_K is the Dedekind zeta function of the cubic number field K. This result implies Lemma 2.4. Conversely, (7) can be proven using elementary arguments analogous to the above. If $\mathcal{O} = \mathcal{O}_K$, then the bound in Lemma 2.4 is sharp if and only if all prime divisors of q split completely in K. This is proven either from (7) or a direct argument as above, using the fact that the splitting of $F \pmod{p}$ mirrors the splitting of p in K.

Remark 2.6. Shintani [32, 33] proved that

$$\sum_{\mathcal{O}} |\mathrm{Disc}\, \mathcal{O}|^{-s} = \sum_{K} |\mathrm{Disc}\, K|^{-s}\, \eta_K(2s) \qquad (\Re(s) > 1)$$

has an analytic continuation to $\mathbb{C}$, with simple poles at $s = 1$ and $s = 5/6$, where $\mathcal{O}$ and K run through the isomorphism classes of cubic orders and fields respectively.

Lemma 2.7. *For* q *a squarefree integer, we have*

$$N^{\pm}(q, X) = O\left(X \cdot 3^{\omega(q)}/q^2\right).$$

Proof. Let $N(q,X) = N^+(q,X) + N^-(q,X)$, and among the classes of orders counted by $N(q,X)$, let $N_0(q,X)$ denote the number of *primitive* orders. Let $\mathcal{O}$ be such a primitive order. By Lemma 2.3 and [4, Lemma 9], there exists an overorder $\mathcal{O}'$ such that $(\mathcal{O}' : \mathcal{O}) = q$. It follows that $\operatorname{Disc}\mathcal{O}' = q^{-2}\operatorname{Disc}\mathcal{O}$. By Lemma 2.2 there are $O(X/q^2)$ such orders $\mathcal{O}'$; moreover, $O(X/(q^2c'^4))$ of these $\mathcal{O}'$ have content equal to c'. Now if $\mathcal{O}'$ has content c' then, by Lemma 2.4, the number of suborders $\mathcal{O}$ of index q in $\mathcal{O}'$ is at most

$$3^{\omega(q/(q,c'))} \prod_{p|(q,c')} (p+1).$$

Therefore, the number of possibilities for $\mathcal{O}$ is

$$N_0(q,X) = \sum_{c'\geq 1} 3^{\omega(q/(q,c'))} \prod_{p|(q,c')} (p+1) O(\frac{X}{q^2c'^4}) = O(X\cdot 3^{\omega(q)}/q^2).$$

In the general case, $\mathcal{O}$ has a content c and there is a unique primitive order $\mathcal{O}'$ such that $c(\mathcal{O}'/\mathbb{Z}) \cong (\mathcal{O}/\mathbb{Z})$, so that

$$N(q,X) = \sum_{c\geq 1} N_0\left(q/(c^2,q), X/c^4\right) = O\left(\frac{3^{\omega(q)}}{q^2} X \sum_{c\geq 1} \frac{(c^2,q)^2}{c^4}\right).$$

Since q is squarefree, $(c^2,q) = (c,q) \leq c$ and the last sum is $O(1)$. □

We note that Lemma 2.7 could also be deduced via an analysis of the size of the coefficients of the Dirichlet series in (7).

2.3. **Orders of small index.** Let q be a squarefree integer. Let $S(q)$ denote the set of integral binary cubic forms corresponding to cubic rings $\mathcal{O}$ having index divisible by q in some other cubic ring $\mathcal{O}'$. In particular, if the binary cubic form is nondegenerate, then it lies in $S(q)$ if and only if it corresponds to a nondegenerate cubic ring having index divisible by q.

The set $S(q)$ is defined by congruence conditions modulo q^2 (see [16]). It follows that $S(q)$ may be expressed as the union of some number k of translates $L_1, \ldots, L_k$ of the lattice $q^2 \cdot V_{\mathbb{Z}}$. The following result, which follows from [16, Lemma 5] or [4, Lemma 13], gives us the number k as a function of q.

Lemma 2.8. *Let $\nu(q)$ be the multiplicative function defined on squarefree numbers q, where for prime p,*

$$\nu(p) = 1 - (1-p^{-3})(1-p^{-2}) = p^{-2} + p^{-3} - p^{-5}.$$

Then the number k of translates of the lattice $q^2 \cdot V_{\mathbb{Z}}$ that comprise $S(q)$ is $\nu(q)q^8$.

In each of the k translates $L_1, \ldots, L_k$ of $q^2 \cdot V_{\mathbb{Z}}$ which comprise $S(q)$, let $a_1, \ldots, a_k$, respectively, denote the smallest positive first coordinate of any element. Thus, $a_1, \ldots, a_k$ are all integers in the interval $[1, q^2]$, and from Lemma 2.8, there are $\nu(q)q^8 > q^6$ of them. We now discuss their distribution.

Proposition 2.9. *Let q be squarefree and let a be an integer in $[1, q^2]$. The number of translates L_j of $q^2 \cdot V_{\mathbb{Z}}$ that comprise $S(q)$ and have smallest positive first coordinate equal to a is*

$$\prod_{\substack{p|q \\ p^2\nmid a}} p^4 \cdot \prod_{\substack{p|q \\ p^2|a}} (p^5 - p^4 + p^3).$$

Proof. By the Chinese remainder theorem, it suffices to treat the case $q = p$, a prime.

We consider first those forms having content coprime to p. If such a form $f \in V_{\mathbb{Z}}$, when viewed modulo p, has three distinct roots in $\mathbb{P}^1(\bar{\mathbb{F}}_p)$, then its discriminant $\mathrm{Disc}(f)$ will also evidently be coprime to p; hence f will correspond to a cubic order that is maximal at p. Therefore, if a form f with content coprime to p is in $S(p)$, then modulo p it must have a multiple root in $\mathbb{P}^1(\bar{\mathbb{F}}_p)$ and thus in $\mathbb{P}^1(\mathbb{F}_p)$.

The following lemma (cf. [4, §3]) describes those binary cubic forms in $S(p)$ having a multiple root at $(0,1) \in \mathbb{P}^1(\mathbb{F}_p)$.

Lemma 2.10. *Let $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ be a form having content coprime to p such that $f \pmod p$ has a multiple root at $(0,1) \in \mathbb{P}^1(\mathbb{F}_p)$. Then $f \in S(p)$ if and only if $c \equiv 0 \pmod p$ and $d \equiv 0 \pmod{p^2}$.*

Applying the transformation $x \mapsto x - ry$, $y \mapsto y$ (resp. $x \mapsto y$, $y \mapsto x$) to the binary cubic form occurring in Lemma 2.10, we then immediately obtain:

Lemma 2.11. *Let $f(x,y)$ be a form having content coprime to p such that $f \pmod p$ has a multiple root at the point $\alpha \in \mathbb{P}^1(\mathbb{F}_p)$. If $\alpha = (r,1)$, then $f \in S(p)$ if and only if f can be expressed in the form*

$$ax^3 + (-3ar + b)x^2y + (3ar^2 - 2br + c)xy^2 + (-ar^3 + br^2 - cr + d)y^3 \tag{8}$$

where $c \equiv 0 \pmod p$ and $d \equiv 0 \pmod{p^2}$. If $\alpha = (1,0)$, then $f \in S(p)$ if and only if f can be expressed in the form

$$ax^3 + bx^2y + cxy^2 + dy^3 \tag{9}$$

where $a \equiv 0 \pmod{p^2}$ and $b \equiv 0 \pmod p$.

Lemma 2.11 explicitly describes all forms in $S(p)$ that have content coprime to p and have a given multiple root $\alpha \in \mathbb{P}^1(\mathbb{F}_p)$. We may now use this description to count the total number of binary cubic forms in $S(p)$ modulo p^2 that have content prime to p and first coefficient equal to any given value $a \in \mathbb{Z}/p^2\mathbb{Z}$.

If $\alpha = (r,1)$ for some $r \in \{0, \dots, p-1\}$, then the total number of forms in $S(p)$ (modulo p^2) having content coprime to p, a multiple root at $\alpha \in \mathbb{P}^1(\mathbb{F}_p)$, and a given value of $a \not\equiv 0 \pmod p$ is $p^2 \cdot p \cdot 1 = p^3$ (i.e., the product of the number of possibilities modulo p^2 for b, c, and d respectively). However, if $a \equiv 0 \pmod p$, then b cannot be $0 \pmod p$, for otherwise the third and fourth coefficients of f would also vanish $(\mathrm{mod}\ p)$. Thus the total number of forms in $S(p)$ (modulo p^2) having content coprime to p, a multiple root at $\alpha = (r,1) \in \mathbb{P}^2(\mathbb{F}_p)$, and a given value $a \equiv 0 \pmod p$ is $(p^2 - p) \cdot p \cdot 1 = p^3 - p^2$.

On the other hand, if $\alpha = (1,0)$ then all forms in $S(p)$ with content coprime to p and a multiple root at α satisfy $a \equiv 0 \pmod{p^2}$. For such forms, both c and d cannot both vanish modulo p for then the whole form would vanish modulo p. Therefore, the total number of forms in $S(p)$ (modulo p^2) having content coprime to p and a multiple root at $\alpha = (1,0) \in \mathbb{P}^1(\mathbb{F}_p)$ is $(p^4 - p^2) \cdot p = p^5 - p^3$ (i.e., the product of the number of possibilities modulo p^2 for (c,d) and b respectively).

Finally, for any $a \equiv 0 \pmod p$, there are clearly p^3 forms $(\mathrm{mod}\ p^2)$ having content a multiple of p, and these all lie in $S(p)$.

We conclude that the total number of forms in $S(p) \pmod{p^2}$ having a given value of a is

$$\begin{aligned} p \cdot p^3 = p^4, &\qquad \text{if } a \not\equiv 0 \pmod{p};\\ p \cdot (p^3 - p^2) + p^3 = p^4, &\qquad \text{if } a \equiv 0 \pmod{p},\ a \not\equiv 0 \pmod{p^2};\\ p(p^3 - p^2) + (p^5 - p^3) + p^3 = p^5 + p^4 - p^3, &\qquad \text{if } a \equiv 0 \pmod{p^2}. \end{aligned}$$

This concludes the proof of Proposition 2.9. □

We now consider fundamental domains for the action of $\mathrm{GL}(2,\mathbb{Z})$ on V, as constructed in [4, §5.1]. Namely, let $\mathcal{F}$ be the usual fundamental domain in $\mathrm{GL}(2,\mathbb{R})$ for $\mathrm{GL}(2,\mathbb{Z})\backslash \mathrm{GL}(2,\mathbb{R})$, in the sense of Gauss. Then for any vector $v \in V^{\pm}$, it is clear that the multiset $\mathcal{F}v \subset V$ is the union of $n_{\pm}$ fundamental domains for the action of $\mathrm{GL}(2,\mathbb{Z})$ on $V^{\pm}$, where again $n_+ = |\operatorname{Stab}_{G_{\mathbb{R}}}(v)| = 6$ for $v \in V^+$ and $n_- = |\operatorname{Stab}_{G_{\mathbb{R}}}(v)| = 2$ for $v \in V^-$.

Let $B = \{w = (a,b,c,d) \in V : a^2 + b^2 + c^2 + d^2 \le 10,\ |\operatorname{Disc}(w)| \ge 1\}$. Given a subset S of $V_{\mathbb{Z}}$, by "the expected number of elements of S in a fundamental domain for $G_{\mathbb{Z}}\backslash V^{\pm}$", we mean the expected number of points of S lying in $\mathcal{F}v$ divided by $n_{\pm}$, as v ranges over $B \cap V^{\pm}$ with respect to the measure $|\operatorname{Disc}(v)|^{-1}dv$. (For more details on the reasons for this choice of set B and measure $|\operatorname{Disc}(v)|^{-1}dv$, see [4].)

If S is a $G_{\mathbb{Z}}$-invariant subset (e.g., the set of irreducible forms corresponding to cubic orders having a given index q, which will be our main interest), then the expected number of points in S in a fundamental domain for $G_{\mathbb{Z}}\backslash V^{\pm}$ will coincide with the exact number in any given single fundamental domain $\mathcal{F}v$, where v is any point in $V^{\pm}$. If S is not $G_{\mathbb{Z}}$-invariant, however, then this number of points in S can vary with the choice of fundamental domain $\mathcal{F}v$. To control error terms, we will have occasion to consider non-$G_{\mathbb{Z}}$-invariant subsets S as well; it turns out that, in our methods, such sets can be controlled much better by averaging over several fundamental domains rather than by examining a single fundamental domain. In particular, the minimal cardinality of such a set, over all fundamental domains, is bounded above by any upper bound for the expected cardinality over these fundamental domains. Thus, we will frequently consider the "expected number" of points in a fundamental domain, rather than the "exact number" in any particular fundamental domain.

Our choice of fundamental domains implies that "most" points $(a,b,c,d) \in \mathcal{F}v$ ($v \in B$) have "small" a, and indeed a is always at most $O(\operatorname{Disc}(a,b,c,d)^{1/4})$ in size (see [4, Proof of Lemma 15]). In particular, many points in the fundamental domain $\mathcal{F}v$ satisfy $a = 0$, and are thus reducible as binary cubic forms. The following lemma, which is Lemma 15 in [4], shows that reducible forms in $\mathcal{F}v$ ($v \in B$) occur very rarely when $a \neq 0$.

Lemma 2.12. *Let $v \in B$. Then the number of integral binary cubic forms $ax^3 + bx^2y + cxy^2 + dy^3 \in \mathcal{F}v$ with $a \neq 0$ that are reducible and have absolute discriminant less than X is $O(X^{3/4+\varepsilon})$.*

We now state the following consequence of Section 5.5 of [4] which, in conjunction with Lemma 2.12, shows that irreducible points in fundamental domains $\mathcal{F}v$ ($v \in B$) are well-distributed with respect to congruences.

Theorem 2.13. *For a positive integer m, let L be any translate $v + m \cdot V_{\mathbb{Z}}$ ($v \in V_{\mathbb{Z}}$) of the sublattice $m \cdot V_{\mathbb{Z}}$ of $V_{\mathbb{Z}}$, and let a denote the smallest positive first coordinate of*

any element in L. Let $N^{\pm}(L;X)$ denote the expected number of lattice points in L, with first coordinate nonzero and discriminant less than X, lying in a fundamental domain for $G_{\mathbb{Z}}\backslash V^{\pm}$. Then

$$N^{\pm}(L;X) = m^{-4}\,N^{\pm}(1,X) + O\left(m^{-3}a^{-1/3}X^{5/6} + m^{-2}a^{-2/3}X^{2/3} + \log X\right) \tag{10}$$

where the implied constant is independent of both m and L.

Remark 2.14. In light of Lemma 2.2, the main term in (10) is dominated by the error estimate when $m \geq (X/\log X)^{1/4}$. Nevertheless, (10) may be read as an O-estimate for $N^{\pm}(L,X)$ for larger values of m.

Let $R^{\pm}(q,X)$ denote the expected number of reducible forms, with first coordinate nonzero, absolute discriminant less than X, and that correspond to a ring having index a multiple of q, lying in a fundamental domain for $G_{\mathbb{Z}}\backslash V^{\pm}$. Recall that a nondegenerate form f corresponds to an order having index a multiple of q if and only if it lies in $S(q)$. Thus $N^{\pm}(q,X)+R^{\pm}(q,X)$ gives the expected number of nondegenerate points, in a fundamental domain for $G_{\mathbb{Z}}\backslash V^{\pm}$, having nonzero first coordinate and lying in $S(q)$. This observation allows us to prove:

Corollary 2.15. *Let q be a squarefree integer. Then we have*

$$N^{\pm}(q,X) = \nu(q)N^{\pm}(1,X) - R^{\pm}(q,X) + O\left(\frac{q}{\varphi(q)}\left(q^{-2/3}X^{5/6} + q^6\log X\right)\right),$$

where φ is Euler's function.

Proof. To obtain $N^{\pm}(q,X)+R^{\pm}(q,X)$, we sum the count in Theorem 2.13 (with $m=q^2$) over the $\nu(q)q^8$ translates of $q^2\cdot V_{\mathbb{Z}}$ which comprise $S(q)$. The main term $\nu(q)N^{\pm}(q,X)$ is thus clear. The second part of the O-estimate follows from the inequality $\nu(q)q^8 \leq q^7/\varphi(q)$ together with the third part of the O-estimate in (10). Let the sequence of values of a which appear as the least positive first coordinates for the translates of $q^2\cdot V_{\mathbb{Z}}$ comprising $S(q)$ be denoted $a_1,\ldots,a_k$, where $k=\nu(q)q^8$. We first show that for any value of y with $1\leq y\leq q^2$, we have

$$\sum_{\substack{1\leq i\leq k\\ a_i\leq y}} 1 \leq \frac{q}{\varphi(q)}q^4 y. \tag{11}$$

Towards this end, for a positive integer a, let $s(a)$ denote the largest divisor of a which is squarefull (for each prime $p \mid s(a)$, we have $p^2 \mid s(a)$). Then, by Proposition 2.9

$$\begin{aligned}
\sum_{\substack{1\leq i\leq k\\ a_i\leq y}} 1 &= \sum_{a\leq y}\prod_{\substack{p\mid q\\ p^2\nmid a}} p^4 \prod_{\substack{p\mid q\\ p^2\mid a}}(p^5-p^4+p^3)\\
&\leq q^4\sum_{a\leq y}\prod_{\substack{p\mid q\\ p^2\mid a}} p \;=\; q^4\sum_{a\leq y}(s(a),q)\\
&= q^4\sum_{d\mid q} d\sum_{\substack{a\leq y\\ (s(a),q)=d}} 1 \;\leq\; q^4\sum_{d\mid q} d\cdot\frac{y}{d^2}\\
&= q^4 y\prod_{p\mid q}\left(1+\frac{1}{p}\right) \;\leq\; \frac{q}{\varphi(q)}q^4 y.
\end{aligned}$$

Thus, we have (11). Now let $0 < c < 1$ be an arbitrary, fixed real number. It follows from (11) and partial summation that

$$\begin{aligned}\sum_{1\le i\le k} a_i^{-c} &= (q^2)^{-c}\sum_{1\le i\le k} 1 + \int_1^{q^2} cy^{-1-c} \sum_{\substack{1\le i\le k\\ a_i\le y}} 1\, dy \\ &\le \nu(q)q^{8-2c} + \frac{q}{\varphi(q)}q^4\int_1^{q^2} cy^{-c}\, dy \\ &< \nu(q)q^{8-2c} + \frac{q}{\varphi(q)}\frac{c}{1-c}q^{6-2c} = O\left(\frac{q}{\varphi(q)}q^{6-2c}\right).\end{aligned}$$

Applying this calculation for $c = 1/3$ gives the first part of our O-estimate. The middle term in the O-estimate in (10) corresponds to $c = 2/3$, and this contribution in the corollary is $O(\frac{q}{\varphi(q)}q^{2/3}X^{2/3})$. It is easy to see that this expression is dominated by the sum of the two error estimates already calculated, so we have the corollary. □

2.4. **Maximal orders.**

Theorem 2.16. *The number of isomorphism classes of cubic fields whose discriminant D satisfies $0 < \pm D < X$ is*

$$\frac{1}{2n_\pm\zeta(3)}X + O\left(X^{7/8}\log^{15/8} X\right), \tag{12}$$

where $n_+ = 6$ and $n_- = 2$.

Proof. By inclusion-exclusion, the number of classes of *maximal* cubic orders, whose discriminant D satisfies $0 < \pm D < X$ is given by

$$\sum_{q\ge 1}\mu(q)N^\pm(q, X). \tag{13}$$

As maximal cubic orders correspond exactly with cubic fields, (13) also represents the count in the theorem. We sum (13) for q up to a large number Q (to be chosen later to minimize error terms) using Corollary 2.15, and truncate the tail using Lemma 2.7. We thus obtain that the number of such classes of maximal orders is equal to

$$N^\pm(1, X)\sum_{q\le Q}\mu(q)\nu(q) + O(E_1) + O(E_2) + O(E_3), \tag{14}$$

where

$$\begin{aligned}E_1 &= \sum_{q\le Q}\frac{q}{\varphi(q)}\left(q^{-2/3}X^{5/6} + q^6\log X\right), \\ E_2 &= \sum_{q>Q} N^\pm(q, X), \\ E_3 &= \sum_{q\le Q} R^\pm(q, X).\end{aligned}$$

A simple argument gives that

$$\sum_{q\le y}\frac{q}{\varphi(q)} = O(y) \tag{15}$$

(in fact the sum is asymptotically κy with $\kappa = \zeta(2)\zeta(3)/\zeta(6)$). Since

$$\sum_{q\le Q} \frac{q}{\varphi(q)} q^c \;=\; Q^c \sum_{q\le Q} \frac{q}{\varphi(q)} - \int_1^Q cy^{c-1} \sum_{q\le y} \frac{q}{\varphi(q)}\, dy,$$

we thus have

$$\sum_{q\le Q} \frac{q}{\varphi(q)} q^c \;=\; O(Q^{1+c}) \;\text{ for }\; c > -1.$$

Hence,

$$E_1 \;=\; O\left(Q^{1/3}X^{5/6} + Q^7 \log X\right).$$

Further, by Lemma 2.7 we have

$$E_2 \;\le\; X \sum_{q>Q} \frac{3^{\omega(q)}}{q^2}.$$

Note that

$$\begin{aligned}\sum_{q\le y} 3^{\omega(q)} \;&\le\; \sum_{n\le y} \sum_{n=uvw} 1 \;=\; \sum_{uv\le y} \sum_{w\le y/uv} 1 \;\le\; \sum_{uv\le y} \frac{y}{uv} \;\le\; y\left(\sum_{u\le y} \frac{1}{u}\right)^2 \\ &=\; O(y\log^2 y).\end{aligned}$$

Thus,

$$\sum_{q>Q} \frac{3^{\omega(q)}}{q^2} \;=\; \int_Q^\infty \frac{2}{y^3} \sum_{Q<q\le y} 3^{\omega(q)}\, dy \;=\; O\left(\int_Q^\infty \frac{\log^2 y}{y^2}\, dy\right) \;=\; O\left(\frac{\log^2 Q}{Q}\right),$$

which stands as our estimate for E_2.

To estimate E_3, note that any reducible form f of absolute discriminant at most X corresponds to an order of some index j in some étale cubic algebra, where $j \le X^{1/2}$. Therefore, f occurs among the set of forms counted by $R^{\pm}(q, X)$ only if q divides j, and the number of such q is evidently $O(j^\varepsilon) = O(X^\varepsilon)$. By Lemma 2.12, we conclude that $E_3 = O(X^\varepsilon \cdot X^{3/4+\varepsilon}) = O(X^{3/4+\varepsilon})$.

For the main term in (14) we use

$$\begin{aligned}\sum_{q\le Q} \mu(q)\nu(q) \;&=\; \sum_{q} \mu(q)\nu(q) - \sum_{q>Q} \mu(q)\nu(q) \\ &=\; \prod_p (1-\nu(p)) + O\left(\sum_{q>Q} \frac{q}{\varphi(q)} \frac{1}{q^2}\right) \\ &=\; \frac{1}{\zeta(2)\zeta(3)} + O\left(\frac{1}{Q}\right),\end{aligned}$$

where the last estimate follows from (15). We finally obtain that (13) is

$$\frac{1}{\zeta(2)\zeta(3)} N^{\pm}(1, X) + O\left(Q^{1/3}X^{5/6} + Q^7 \log\, X + XQ^{-1}\log^2 Q\right).$$

By Lemma 2.2 and choosing $Q = (X \log\, X)^{1/8}$, we obtain the desired result. □

3. 3-torsion in the class groups of quadratic fields

We follow the same general strategy as above. Let p be an odd prime (resp. $p = 2$); an integer $D \equiv 0, 1 \pmod 4$ is *fundamental at* p if it satisfies $p^2 \nmid D$ (resp. $D \not\equiv 0, 4 \pmod{16}$). An integer $D \equiv 0, 1 \pmod 4$ is a *fundamental discriminant* if it is fundamental at all primes. In other words, it is either 1 or the discriminant of a quadratic field. This provides a link between cubic orders and 3-ranks of quadratic fields.

Lemma 3.1 (Hasse [21])**.** *The number of isomorphism classes of cubic orders whose discriminant D is fundamental is $(\#\operatorname{Cl}_3(D) - 1)/2$.*

Remark 3.2. More generally, let K a cubic field with discriminant d_K and $k := \mathbb{Q}(\sqrt{d_K})$. Then d_K is fundamental at p if and only if the places above p in k are unramified in the cyclic cubic extension Kk/k.

We say an order is fundamental at p if its discriminant is. Let $M^{\pm}(q, X)$ be the number of isomorphism classes of cubic orders $\mathcal{O}$ whose discriminant D satisfies $0 < \pm D < X$ and is *not* fundamental at any prime divisor of q.

Lemma 3.3. *Let q be a squarefree positive integer. The number of isomorphism classes of* maximal *cubic orders $\mathcal{O}_K$ whose discriminants satisfy $0 < \pm D < X$ and which are not fundamental at any prime divisor of q is $O(X \cdot 3^{\omega(q)}/q^2)$.*

Proof. This is due to

$$\sum_{0<\pm D<X} \#\operatorname{Cl}_3(D) \;=\; O(X),$$

which follows from Lemmas 2.2 and 3.1, and a classical inequality bounding the 3-rank of the ring class group modulo q of $\mathbb{Q}(\sqrt{D})$ by $\omega(q)+r_3(\sqrt{D})+O(1)$, already used by Davenport and Heilbronn [16]. See Datskovsky and Wright [13] for a (more general) proof yielding $4^{\omega(q)}$ instead of $3^{\omega(q)}$. □

We are now in the position to prove the following analogue of Lemma 2.7.

Lemma 3.4. *For q a squarefree integer, we have*

$$M^{\pm}(q, X) \;=\; O\left(X \cdot 6^{\omega(q)}/q^2\right). \tag{16}$$

Proof. Let $\mathcal{O}$ be an order contained in a maximal order $\mathcal{O}_K$. Then $\mathcal{O}$ fails to be fundamental at p if and only if $\operatorname{Disc}(\mathcal{O}_K)$ is not fundamental at p, or p divides the index $(\mathcal{O}_K : \mathcal{O})$.

Let a, b, c be three integers such that $abc = q$, hence pairwise coprime. We want to count the number of (isomorphism classes of) orders $\mathcal{O}$ such that

- $|\operatorname{Disc}(\mathcal{O})| < X$,
- c divides the content of $\mathcal{O}$,
- b divides the index of $\mathcal{O}$ in its maximal order $\mathcal{O}_K$,
- $\mathcal{O}_K$ is not fundamental at any prime divisor of a.

Let cd be the content of such an $\mathcal{O}$, $I = bc^2de$ its index, for some integers $d, e \geq 1$. (Note that b and $(cd)^2$ divide the index, but we may have $(b, d) > 1$; on the other hand, $(b, c) = 1$ and b is squarefree.) The maximal order $\mathcal{O}_K$ containing $\mathcal{O}$ has discriminant less than X/I^2 in absolute value, so there are

$$O\left(X \cdot 3^{\omega(a)}/(aI)^2\right)$$

possibilities for $\mathcal{O}_K$ by Lemma 3.3. Let $\Omega(I)$ denote the number of prime divisors of I, counted with multiplicity. Applying repeatedly Lemma 2.4, each of these (primitive) maximal orders contains at most $3^{\Omega(I)}$ *primitive* suborders of index I.

Summing over d and e, we obtain $O(X \cdot 3^{\Omega(abc^2)}/(abc^2)^2)$ orders, that is

$$O(X \cdot 3^{\omega(q)}/q^2 \cdot 3^{\omega(c)}/c^2).$$

There are $3^{\omega(q)}$ ways to write $q = abc$ since q is squarefree, which would yield $9^{\omega(q)}$ instead of $6^{\omega(q)}$ in (16). We instead estimate

$$\sum_{\substack{a,b,c\\ abc=q}} \frac{3^{\omega(c)}}{c^2} \;=\; \sum_{c|q} \frac{3^{\omega(c)}}{c^2} 2^{\omega(q/c)} \;=\; 2^{\omega(q)} \prod_{p|q} \left(1 + \frac{3/2}{p^2}\right) \;=\; O(2^{\omega(q)}).$$

□

Let $W(q) \subset V_{\mathbb{Z}}$ denote the set of all forms corresponding to cubic rings that, for each prime $p \mid q$, are either not maximal at p, or maximal at p but also totally ramified at p. Thus, for a prime $q = p$, $W(p) = S(p) \cup T(p)$ where $T(p)$ denotes the set of forms corresponding to cubic orders that are maximal but also totally ramified at p. Note that $T(p)$ contains only irreducible forms, so that $S(q)$ and $W(q)$ coincide on reducible forms for all q.

Like $S(p)$, the set $T(p)$ is defined by congruence conditions modulo p^2. Indeed, a form is in $T(p)$ if and only if it is maximal at p (which we have already seen is a condition modulo p^2) and it has a triple root modulo p (which is clearly a condition modulo p).

By the Chinese Remainder Theorem it follows that for all positive integers q, the set $W(q)$ may be expressed as the union of some number $\kappa \geq k$ of translates $L_1, \ldots, L_\kappa$ of the lattice $q^2 \cdot V_{\mathbb{Z}}$. The following result, which follows from [16, Lemma 4] or [4, Lemma 13], gives us the number κ as a function of q.

Lemma 3.5. *Let $\tau(q)$ be the multiplicative function defined on squarefree numbers q, where for prime p,*

$$\tau(p) = 1 - (1 - p^{-2})^2 = 2p^{-2} - p^{-4}.$$

Then the number κ of translates of the lattice $q^2 \cdot V_{\mathbb{Z}}$ that comprise $W(q)$ is $\tau(q)q^8$.

In each of the κ translates $L_1, \ldots, L_\kappa$ of $q^2 \cdot V_{\mathbb{Z}}$ which comprise $W(q)$, let $a_1, \ldots, a_\kappa$, respectively, denote the smallest positive first coordinate of any element. Thus, $a_1, \ldots, a_\kappa$ are all integers in the interval $[1, q^2]$, and from Lemma 3.5, there are $\tau(q)q^8 > 2q^6$ of them. We now discuss their distribution, which is the analogue of Proposition 2.9 for $W(q)$.

Proposition 3.6. *Let q be squarefree and let a be an integer in $[1, q^2]$. The number of translates L_j of $q^2 \cdot V_{\mathbb{Z}}$ that comprise $W(q)$ and have smallest positive first coordinate equal to a is*

$$\prod_{\substack{p|q\\ p^2 \nmid a}} (2p^4 - p^3) \cdot \prod_{\substack{p|q\\ p^2|a}} (p^5 - p^4 + p^3).$$

Proof. By the Chinese Remainder Theorem, we may again assume that $q = p$ is a prime. It suffices to analyze $T(p)$, since $S(p)$ has already been treated in Proposition 2.9. We begin with the following lemma, which follows easily from Lemma 2.10.

Lemma 3.7. *Let $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ be a form such that $f \pmod p$ has a triple root at $(0,1) \in \mathbb{P}^1(\mathbb{F}_p)$. Then $f \in T(p)$ if and only if $a \not\equiv 0 \pmod p$, $b, c, d \equiv 0 \pmod p$ and $d \not\equiv 0 \pmod{p^2}$.*

Applying the transformation $x \mapsto x - ry$, $y \mapsto y$ (resp. $x \mapsto y$, $y \mapsto x$) to the binary cubic form occurring in Lemma 3.7, we then immediately obtain:

Lemma 3.8. *Let $f(x,y)$ be a form such that $f \pmod p$ has a triple root at the point $\alpha \in \mathbb{P}^1(\mathbb{F}_p)$. If $\alpha = (r,1)$, then $f \in T(p)$ if and only if f can be expressed in the form*

$$ax^3 + (-3ar + b)x^2y + (3ar^2 - 2br + c)xy^2 + (-ar^3 + br^2 - cr + d)y^3 \tag{17}$$

where $a \not\equiv 0 \pmod p$, $b, c, d \equiv 0 \pmod p$ and $d \not\equiv 0 \pmod{p^2}$. If $\alpha = (1,0)$, then $f \in T(p)$ if and only if f can be expressed in the form

$$ax^3 + bx^2y + cxy^2 + dy^3 \tag{18}$$

where $a, b, c \equiv 0 \pmod p$, $a \not\equiv 0 \pmod{p^2}$, and $d \not\equiv 0 \pmod p$.

Lemma 3.8 explicitly describes all forms in $T(p)$ that have a given triple root $\alpha \in \mathbb{P}^1(\mathbb{F}_p)$. We may now use this description to count the total number of binary cubic forms in $T(p)$ modulo p^2 whose first coefficient is equal to any given value $a \in \mathbb{Z}/p^2\mathbb{Z}$.

If $\alpha = (r,1)$ for some $r \in \{0, \dots, p-1\}$, then the total number of forms in $T(p)$ (modulo p^2) having a triple root at $\alpha \in \mathbb{P}^1(\mathbb{F}_p)$ and a given value of $a \not\equiv 0 \pmod p$ is $p \cdot p \cdot (p-1) = p^3 - p^2$ (i.e., the product of the number of possibilities modulo p^2 for b, c, and d respectively). Of course, the value $a \equiv 0 \pmod p$ does not occur for forms in $T(p)$ having a triple root at $\alpha = (r,1) \in \mathbb{P}^1(\mathbb{F}_p)$.

On the other hand, if $\alpha = (1,0)$ then all forms in $T(p)$ having a triple root at α satisfy $a \equiv 0 \pmod p$, $a \not\equiv 0 \pmod{p^2}$. For any such value of a, the total number of forms in $T(p)$ (modulo p^2) having a triple root at $\alpha = (1,0) \in \mathbb{P}^1(\mathbb{F}_p)$ is $(p^2 - p) \cdot p \cdot p = p^4 - p^3$ (i.e., the product of the number of possibilities modulo p^2 for d, c, and b respectively).

We conclude that the total number of forms in $T(p) \pmod{p^2}$ having a given value of a is

$$\begin{aligned} p \cdot (p^3 - p^2) = p^4 - p^3, &\qquad \text{if } a \not\equiv 0 \pmod p; \\ p^4 - p^3, &\qquad \text{if } a \equiv 0 \pmod p,\ a \not\equiv 0 \pmod{p^2}; \\ 0, &\qquad \text{if } a \equiv 0 \pmod{p^2}. \end{aligned}$$

In conjunction with Proposition 2.9, this yields Proposition 3.6. □

Theorem 1.2 is now proven as in the previous section, starting from

$$\begin{aligned} \sum_{0<\pm D<X} 1 &= \frac{3}{\pi^2}X + O(X^{1/2}), \\ \sum_{0<\pm D<X} (\#\operatorname{Cl}_3(D) - 1)/2 &= \sum_{q \geq 1} \mu(q) M^{\pm}(q, X), \end{aligned}$$

and the analogue of Corollary 2.15 (which may now be proven using Proposition 3.6 in the identical manner):

Lemma 3.9. *For a squarefree integer q, we have*

$$M^{\pm}(q,X) = \tau(q)N^{\pm}(1,X) - R^{\pm}(q,X) + O\left(2^{\omega(q)}\frac{q}{\varphi(q)}\left(q^{-2/3}X^{5/6} + q^6\log X\right)\right),$$

where τ is as in Lemma 3.5.

4. Quartic fields

4.1. **Sketch.** We call again an order of $\mathbb{Z}$-rank 4 a *quartic order*: it is an order in a quartic number field. More specifically, we say an order is an *S_4-quartic order* if it is an order in an *S_4-quartic field*, i.e., a quartic number field whose Galois closure has automorphism group S_4.

In order to count S_4-quartic number fields, we use an analogue for quartic rings of Theorem 2.1. To state this result, let $V_{\mathbb{Z}}$ now denote the space of pairs (A,B) of integer-coefficient ternary quadratic forms. Then, excluding degenerate cases, any element of $V_{\mathbb{Z}}$ gives two conics in $\mathbb{P}^2(\bar{\mathbb{Q}})$ which intersect in four distinct points. We say that an element $(A,B) \in V_{\mathbb{Z}}$ is *irreducible* if the field of definition of one (equivalently, any) of these intersection points is a quartic field. We say that an element $(A,B) \in V_{\mathbb{Z}}$ is *totally irreducible* if the field of definition of one (equivalently, any) of these intersection points is an S_4-quartic field. We say that two elements of $V_{\mathbb{Z}}$ are in the same class if one can be transformed into the other via an element of $G(\mathbb{Z}) = \mathrm{GL}(2,\mathbb{Z}) \times \mathrm{SL}(3,\mathbb{Z})$. One finds that the action of $G(\mathbb{Z})$ on $V_{\mathbb{Z}}$ has a unique polynomial invariant, called the *discriminant*; it is defined by $\mathrm{Disc}(A,B) = \mathrm{Disc}(\mathrm{Det}(Ax - By))$.

Finally, given an element $(A,B) \in V_{\mathbb{Z}}$, let Λ denote the rank 2 lattice of integer-coefficient ternary quadratic forms spanned over $\mathbb{Z}$ by A and B, and let Λ_0 denote the maximal rank 2 lattice of integer-coefficient ternary quadratic forms containing Λ. We define the *content* of (A,B) as the index of Λ in Λ_0.

We then have the following theorem parametrizing quartic rings.

Theorem 4.1 ([5])**.** *There is a canonical map from the set of classes of pairs of integer-coefficient ternary quadratic forms (A,B) to the set of isomorphism classes of quartic rings. This map preserves content and discriminant. In particular, the map sends nondegenerate elements in $V_{\mathbb{Z}}$ to nondegenerate quartic rings, and elements of content* 1 *in $V_{\mathbb{Z}}$ to primitive quartic rings. Furthermore, the map sends irreducible elements in $V_{\mathbb{Z}}$ to quartic orders, and totally irreducible elements to S_4-quartic orders. Finally, the number of preimages under this map of a given (isomorphism class of the) quartic ring Q is given by $\sigma(n)$, where n denotes the content of Q and σ is the usual sum-of-divisors function.*

Note that primitive quartic orders therefore have a single preimage under the map of Theorem 4.1.

We recall that an element $(g_2,g_3) \in \mathrm{GL}(2,\mathbb{R}) \times \mathrm{GL}(3,\mathbb{R})$ acts on the vector space V of pairs of ternary quadratic forms over $\mathbb{R}$ via

$$(g_2,g_3)\cdot(A,B) = (g_3Ag_3^t, g_3Bg_3^t)\cdot g_2^t,$$

where we view $(A,B) \in V$ as a pair of symmetric 3×3 matrices. The action of $G = \mathrm{GL}(2,\mathbb{R}) \times \mathrm{GL}(3,\mathbb{R})$ on V has three orbits of nonzero discriminant, namely, $V^{(0)}$, $V^{(1)}$, and $V^{(2)}$, where $V^{(i)}$ consists of those elements of V that yield a pair of conics in $\mathbb{P}^2(\mathbb{C})$ intersecting in $4-2i$ real points and $2i$ complex points. If

$v \in V_{\mathbb{Z}}^{(i)} = V_{\mathbb{Z}} \cap V^{(i)}$, then the fraction field of the quartic order corresponding to v via Theorem 4.1 will then have $4-2i$ real embeddings and $2i$ complex embeddings.

Instead of S_4-quartic fields, we count isomorphism classes of their maximal orders, which are associated to certain $G(\mathbb{Z})$-orbits on $V_{\mathbb{Z}}$. A local characterization of these "maximal" classes was given in [5, §4.2]. Via reduction theory for V using Siegel sets as in [4] and [6], we are reduced (as in the cubic case) to counting integral points, satisfying suitable congruences, in certain semi-algebraic sets in V.

4.2. **Orders of large index.** Adopting notation similar to the cubic case, we let $N^{(i)}(q,X)$ denote the number of classes of pairs of ternary quadratic forms in $V_{\mathbb{Z}}$ corresponding to isomorphism classes of S_4-quartic orders of index divisible by q whose fraction field has $4-2i$ real embeddings and $2i$ complex embeddings. We require an upper bound for $N^{(i)}(q,X)$.

Lemma 4.2. [6, Prop. 17] *Letting $n_0 = 24$, $n_1 = 4$, and $n_2 = 8$, we have*

$$N^{(i)}(1,X) \;=\; \frac{\zeta(2)^2\zeta(3)}{2n_i} \cdot X + O\left(X^{23/24+\varepsilon}\right).$$

In particular, $N^{(i)}(1,X) = O(X)$.

In fact, if the methods of [4] are used in conjunction with those of [6], then the error term above immediately reduces to $O(X^{11/12})$ (see Corollary 4.12 below).

Lemma 4.3. *For q a squarefree integer, we have*

$$N^{(i)}(q,X) = O\left(X \cdot 6^{\omega(q)}/q^2\right).$$

Proof. This follows from Lemma 2.3 and the arguments in [6, §3.2]. (A key ingredient is Nakagawa's work [30], which proves a quartic analogue of Datskovsky and Wright's formula (7).) □

4.3. **Orders of small index.** Let q be a squarefree integer. Then the set $S(q)$ of all pairs of ternary quadratic forms in $V_{\mathbb{Z}}$ corresponding to quartic rings Q having index a multiple of q in some other quartic ring Q' is defined by congruence conditions modulo q^2 (see [5]). It follows as with the cubic case that $S(q)$ may be expressed as the union of some number k of translates $L_1, \ldots, L_k$ of the lattice $q^2 \cdot V_{\mathbb{Z}}$. The following result, which follows from [5, eq. (45)], gives us the number k as a function of q.

Lemma 4.4. *Let $\nu(q)$ be the multiplicative function defined on squarefree numbers q, where for prime p,*

$$\begin{aligned}\nu(p) &= 1-(1-p^{-2})^2(1-p^{-3})(1+p^{-2}-p^{-3}-p^{-4})\\ &= p^{-2}+2p^{-3}+2p^{-4}-3p^{-5}-4p^{-6}-p^{-7}+3p^{-8}+3p^{-9}-p^{-10}-p^{-11}.\end{aligned}$$

Then the number k of translates of the lattice $q^2 \cdot V_{\mathbb{Z}}$ that comprise $S(q)$ is $\nu(q)q^{24}$.

In the cubic case, we examined the distribution of the first coordinate of binary cubic forms in the corresponding sets $S(q)$. In the quartic case, to obtain the best possible error terms via our methods, we are led to examine the distribution of the first *four* coordinates. For a pair of ternary quadratic forms $(A,B) \in V$, where $A(x_1,x_2,x_3) = \sum_{i\le j} a_{ij}x_ix_j$ and $B(x_1,x_2,x_3) = \sum_{i\le j} b_{ij}x_ix_j$ we say that the *first four coordinates of* (A,B) are given by a_{11}, a_{12}, a_{13}, and a_{22}. In each translate L of $q^2 \cdot V_{\mathbb{Z}}$, we consider its *standard member* as the one with each entry in the interval

$[1, q^2]$. (Indeed, the space of pairs of ternary quadratic forms $V_{\mathbb{Z}}$ may be thought of as the lattice $\mathbb{Z}^{12}$, and so L, as a coset of $q^2 \cdot V_{\mathbb{Z}}$, has each of its twelve entries running independently over particular residue classes modulo q^2.) For each of the k translates $L_1, \dots, L_k$ of $q^2 \cdot V_{\mathbb{Z}}$ which comprise $S(q)$, let $(a_1, b_1, c_1, d_1), \dots, (a_k, b_k, c_k, d_k)$ denote the respective quadruples consisting of the first four coordinates in their standard member. Thus, $(a_1, b_1, c_1, d_1), \dots, (a_k, b_k, c_k, d_k)$ are all quadruples of integers in $[1, q^2]^4 = [1, q^2] \times [1, q^2] \times [1, q^2] \times [1, q^2]$, and from Lemma 4.4, there are $k = \nu(q) q^{24} > q^{22}$ of them. We now discuss the distribution of these k quadruples.

We begin with the following lemma.

Lemma 4.5. *Suppose A is a ternary quadratic form over $\mathbb{Z}$, and let p be any prime. Let $\mathrm{rk}(A)$ denote the rank of A over $\mathbb{Z}/p\mathbb{Z}$. Then the number of values $\pmod{p^2}$ for the quadratic form B, such that (A, B) corresponds to a quartic ring that is not maximal at p, is*

$$\begin{array}{rll} p^{10} & + O(p^9), & \text{if } \mathrm{rk}(A) = 3; \\ \leq 3p^{10} & + O(p^9), & \text{if } \mathrm{rk}(A) = 2; \\ 2p^{11} & + O(p^{10}), & \text{if } \mathrm{rk}(A) = 1; \\ p^{12}, & & \text{if } \mathrm{rk}(A) = 0. \end{array}$$

Proof. Suppose $\mathrm{rk}(A) = 3$. For (A, B) to be nonmaximal at p, A and B must have a multiple point of intersection in $\mathbb{P}^2(\mathbb{F}_p)$. The number of $B \pmod{p^2}$ with this property is $p^{11} + O(p^{10})$. Indeed, A has $p+1$ points in $\mathbb{P}^2(\mathbb{F}_p)$, and the number of B that have at least a double intersection with A at a given $\mathbb{F}_p$-rational point of A is $p^{10} + O(p^3)$ (as this amounts to two linear conditions on $B \bmod p$). Thus the total number of B having a multiple point of intersection at an $\mathbb{F}_p$-rational point of A is $p^{11} + O(p^{10})$. Moreover, it is easy to see that the number of B having more than one multiple point of intersection with A in $\mathbb{P}^2(\overline{\mathbb{F}}_p)$ is negligible in comparison, i.e., $O(p^{10})$. Finally, by [6, §4.2], a proportion of $1/p + O(1/p^2)$ of these $p^{11} + O(p^{10})$ values of B will yield a quartic ring that is nonmaximal at p, yielding a total of $p^{10} + O(p^9)$ possible B's in the case $\mathrm{rk}(A) = 3$.

If $\mathrm{rk}(A) = 2$, then in $\mathbb{P}^2(\overline{\mathbb{F}}_p)$, the degenerate conic A is the union of two distinct lines. By similar reasoning, the number of $B \pmod{p^2}$ having a multiple intersection point with A is at most $2p^{11} + p^{11} = 3p^{11}$, and again a proportion of $1/p + O(1/p^2)$ of these will be nonmaximal at p, yielding the claim in this case.

If $\mathrm{rk}(A) = 1$, then in $\mathbb{P}^2(\mathbb{F}_p)$, the (degenerate) conic A is a double line. Any B will have a multiple intersection with A, when viewed as conics in $\mathbb{P}^2(\mathbb{F}_p)$; generically, there will be two double points of intersection. For each of these two double points of intersection, one obtains a proportion of $1/p + O(1/p^2)$ of these values of B that are nonmaximal at p. Thus we obtain a total of $2p^{11} + O(p^{10})$ values of B for which (A, B) is not maximal at p.

Finally, if $\mathrm{rk}(A) = 0$, then B can be any ternary quadratic form. All p^{12} values of B will give an (A, B) that is not maximal at p. This completes the proof. □

We now prove the following two propositions which give information on the distribution of the quadruple $(a_{11}, a_{12}, a_{13}, a_{22}) = (a, b, c, d)$ in $S(p)$.

Proposition 4.6. *Fix $a, b, c, d \in \mathbb{Z}/p^2\mathbb{Z}$, and suppose that at least one element of the set $\{a, b, c\}$, and at least one of the set $\{a, b, d\}$, is nonzero modulo p. Then the number of $(A, B) \pmod{p^2}$, with these values of a, b, c, d, such that (A, B) is not maximal at p is $p^{14} + O(p^{13})$.*

Proof. If a, b, c, d satisfy the conditions of the proposition, then $\mathrm{Det}(A)$, as a (quadratic, linear, or constant) polynomial function of $u = a_{23}$ and $v = a_{33}$, does not identically vanish. Hence the number of possible values of u, $v \pmod{p^2}$ for which $\mathrm{Det}(A)$ is nonzero $\pmod{p}$ is $p^4 + O(p^3)$. By the lemma, the number of values of (A, B) with $\mathrm{rk}(A) = 3$, (A, B) nonmaximal at p, and the given values of a, b, c, d, is $(p^4 + O(p^3))(p^{10} + O(p^9)) = p^{14} + O(p^{13})$.

It remains to consider those choices of u, v for which A has vanishing determinant $\pmod{p}$. The number of such choices for u, v is $O(p^3)$. The rank of $A \pmod{p}$ will then be either 2 or 1 in such a case. In particular, the number of u, v modulo p^2 for which $\mathrm{rk}(A) = 2$ is $O(p^3)$. By Lemma 4.5, the number of values of $(A, B) \pmod{p^2}$ with $\mathrm{rk}(A) = 2$, (A, B) nonmaximal at p, and the given values of a, b, c, d, is at most $(O(p^3))(3p^{10} + O(p^9)) = O(p^{13})$.

Finally, we consider the case $\mathrm{rk}(A) = 1$. Note that $A \pmod{p}$ will be of rank 1 only if $b^2 - 4ad \equiv c^2 - 4av \equiv bc - 2au \equiv 0$. If a is nonzero $\pmod{p}$, then (assuming $p > 2$) v and u are determined $\pmod{p}$ by the given information, so there are exactly p^2 choices possible for the pair $(u, v) \pmod{p^2}$ for which the condition $\mathrm{rk}(A) = 1$ holds. If a is zero $\pmod{p}$, then for $\mathrm{rk}(A) = 1$ to hold, we also then need $b \equiv 0 \pmod{p}$ and $c \equiv 0 \pmod{p}$, a contradiction. Thus, regardless of the value of a, there are at most p^2 values of $u, v \pmod{p^2}$ yielding $\mathrm{rk}(A) = 1$. By the lemma, we conclude that the number of values of (A, B) with $\mathrm{rk}(A) = 1$, (A, B) nonmaximal at p, and our given values of a, b, c, d is at most $p^2(2p^{11} + O(p^{10})) = O(p^{13})$. The proposition follows. □

Proposition 4.7. *Suppose $a, b, c, d \in \mathbb{Z}/p^2\mathbb{Z}$ and either $a \equiv b \equiv c \equiv 0 \pmod{p}$ or $a \equiv b \equiv d \equiv 0 \pmod{p}$. Then the number of $(A, B) \pmod{p^2}$, with these values of a, b, c, d, such that (A, B) is not maximal at p is at most $6p^{14} + O(p^{13})$.*

Proof. The condition on a, b, c, d implies that $\mathrm{Det}(A)$ vanishes $\pmod{p}$. Thus the rank of A is at most 2, regardless of $u = a_{23}$ and $v = a_{33}$. The number of values of u and $v \pmod{p^2}$ with $\mathrm{rk}(A) = 2$ is thus less than p^4; by Lemma 4.5, the number of (A, B) not maximal at p, with $\mathrm{rk}(A) = 2$ and the given values of a, b, c, d, is at most $3p^{14} + O(p^{13})$.

For $A \pmod{p}$ to be rank 1 for some values of u and v, first assume that $a \equiv b \equiv c \equiv 0 \pmod{p}$. Then $\mathrm{rk}(A) = 1$ occurs when $u^2 \equiv 4dv \pmod{p}$, so if d is not zero $\pmod{p}$, then $v \pmod{p}$ is determined by u (assuming $p > 2$), while if $d \equiv 0 \pmod{p}$, then $u \equiv 0 \pmod{p}$ and v may be any nonzero residue $\pmod{p}$. Thus, regardless of the value of d, the number of values of u and $v \pmod{p^2}$ with $\mathrm{rk}(A) = 1$ in this case is at most p^3. Note the hypotheses $a \equiv b \equiv d \equiv 0 \pmod{p}$ and $\mathrm{rk}(A) = 1$ implies too that $c \equiv 0 \pmod{p}$, the case we have just considered. By Lemma 4.5, the number of (A, B) not maximal at p, with $\mathrm{rk}(A) = 1$ and the given values of a, b, c, d, is at most $2p^{14} + O(p^{13})$.

Finally, for $A \pmod{p}$ to be rank 0, we must have $u \equiv v \equiv 0 \pmod{p}$. The number of values of u and $v \pmod{p^2}$ is thus p^2. By Lemma 4.5, the number of (A, B) not maximal at p, with $\mathrm{rk}(A) = 0$ and the given values of a, b, c, d, is at most p^{14}. The proposition follows. □

Corollary 4.8. *Let q be squarefree and let (a, b, c, d) be a quadruple of integers in $[1, q^2]^4$. The number of translates L_j of $q^2 \cdot V_{\mathbb{Z}}$ that comprise $S(q)$ and have (a, b, c, d) as the first four coordinates of some member is*

$$6^f \left(q^{14} + O\left(q^{13}\right)\right),$$

where

$$0 \le f \le \sum_{p \mid \gcd(q,a,b,cd)} 1.$$

Proof. This follows from Propositions 4.6 and 4.7, together with the Chinese Remainder Theorem. □

We construct fundamental domains for the action of $G_{\mathbb{Z}}$ on the 12-dimensional real vector space V in a manner analogous to that used in the cubic case (see [6, §2.1]), and the phrase "expected number" is also then defined analogously. As in the cubic case, our choice of fundamental domains $\mathcal{F}v \subset V$ ensures that the first coordinate a_{11} is generally small in these domains, and often 0. Although the condition $a_{11} = 0$ this time does not imply that (A, B) is not totally irreducible, we still have ([6, Lemma 11]):

Lemma 4.9. *The expected number of $(A, B) \in \mathcal{F}v$ with $a_{11} = 0$ that are totally irreducible and have absolute discriminant less than X is $O(X^{11/12})$.*

Moreover, in analogy with Lemma 2.12, we also have:

Lemma 4.10. *The number of $(A, B) \in \mathcal{F}v$ with $a_{11} \neq 0$ that are not totally irreducible and have absolute discriminant less than X is $O(X^{11/12+\varepsilon})$.*

Proof. This follows from [6, Lemmas 12 and 13] and [34, 35]. □

We are now ready to prove the quartic analogue of Theorem 2.13.

Theorem 4.11. *For a positive integer m, let L be any translate $v + m \cdot V_{\mathbb{Z}}$ ($v \in V_{\mathbb{Z}}$) of the sublattice $m \cdot V_{\mathbb{Z}}$ of $V_{\mathbb{Z}}$, and let (a, b, c, d) denote the smallest positive first four coordinates of any element in L. For $i = 0, 1, 2$, let $N^{(i)}(L; X)$ denote the expected number of lattice points in L, with first coordinate nonzero and discriminant less than X, lying in a fundamental domain for $G_{\mathbb{Z}} \backslash V^{(i)}$. Then*

(19)
$$N^{(i)}(L; X) = m^{-12}\, N^{(i)}(1, X) + O\Big(\sum_{S \subset \{a_{ij}, b_{ij}\}} m^{-|S|} a^{-\alpha_S} b^{-\beta_S} c^{-\gamma_S} d^{-\delta_S} X^{(|S|+\alpha_S+\beta_S+\gamma_S+\delta_S)/12} + \log X \Big),$$

where S ranges over the nonempty proper subsets of the set of 12 coordinates $\{a_{ij}, b_{ij}\}$ on $V_{\mathbb{Z}}$, and $\alpha_S, \beta_S, \gamma_S, \delta_S \in [0, 1]$ are real constants that depend only on S and satisfy $|S| + \alpha_S + \beta_S + \gamma_S + \delta_S \le 11$. Moreover, it is possible to choose $\alpha_S, \beta_S, \gamma_S, \delta_S \in [0, 1)$ for all S except for the following three sets:

1. *$\{b_{11}, b_{12}, b_{13}, b_{22}, b_{23}, b_{33}\}$, for which α_S, β_S, γ_S, $\delta_S = 1$;*
2. *$\{a_{13}, a_{23}, a_{33}, b_{13}, b_{23}, b_{33}\}$, for which $\gamma_S = 0$ and α_S, β_S, $\delta_S = 1$;*
3. *$\{a_{22}, a_{23}, a_{33}, b_{22}, b_{23}, b_{33}\}$, for which $\delta_S = 0$ and α_S, β_S, $\gamma_S = 1$.*

Proof. We proceed exactly as in the proof of Theorem 2.13, combining the error estimate techniques of [4] and Section 2 with the work of [6]. In particular, for each nonempty proper subset S of the coordinates on V, we wish to compute the expected m-scaled volume of the projection of the region $\mathcal{R}_X$ onto the coordinate hyperplane spanned by the coordinates in S. This expected volume is again expressible as an

integral over the variables of the Siegel set (see [6, §2.1]) and can be bounded by an absolute constant times an integral of the form

$$m^{-|S|}\int_{\lambda=C}^{X^{1/12}}\int_{s_1,s_2,s_3=1/2}^{\infty}\lambda^{|S|}s_1^{e_1}s_2^{e_2}s_3^{e_3}\,\frac{d\lambda}{\lambda}\,\frac{ds_1}{s_1}\,\frac{ds_2}{s_2}\,\frac{ds_3}{s_3}, \tag{20}$$

where, in the integral, the values of λ, s_1, s_2, s_3 are restricted to the region where

$$as_1s_2^4s_3^2\le\lambda,\quad bs_1s_2s_3^2\le\lambda,\quad cs_1s_2\le\lambda s_3,\quad\text{and}\quad ds_1s_3^2\le\lambda s_2^2, \tag{21}$$

and C is an absolute positive constant.

For a given choice of $S\subset\{a_{ij},b_{ij}\}$, the values of e_1,e_2,e_3 are determined by

$$s_1^{e_1}s_2^{e_2}s_3^{e_3}=s_1^{-2}s_2^{-6}s_3^{-6}\prod_{t\in S}s_1^{w_1(t)}s_2^{w_2(t)}s_3^{w_3(t)}, \tag{22}$$

where the values of $(w_1(t),w_2(t),w_3(t))$ for $t\in S$ are given in the following table:

$$\begin{array}{lll} a_{11}:(-1,-4,-2) & a_{12}:(-1,-1,-2) & a_{13}:(-1,-1,1)\\ a_{22}:(-1,2,-2) & a_{23}:(-1,2,1) & a_{33}:(-1,2,4)\\ b_{11}:(1,-4,-2) & b_{12}:(1,-1,-2) & b_{13}:(1,-1,1)\\ b_{22}:(1,2,-2) & b_{23}:(1,2,1) & b_{33}:(1,2,4). \end{array} \tag{23}$$

Using this table, one can evaluate the integral (20) for each value of S, and the result follows.[2] We sketch the details for the three exceptional sets of size 6 that are given in the theorem. For the first set, using (22) and (23), we have $e_1=4, e_2=-6, e_3=-6$, so the integral in (20) is

$$m^{-6}\int_{\lambda=C}^{X^{1/12}}\int_{s_1,s_2,s_3=1/2}^{\infty}\lambda^5s_1^3s_2^{-7}s_3^{-7}\,d\lambda\,ds_1\,ds_2\,ds_3.$$

The variable s_1 has a positive exponent, so we use (21) to bound s_1:

$$s_1\le\frac{\lambda}{as_2^4s_3^2},\quad s_1\le\frac{\lambda}{bs_2s_3^2},\quad s_1\le\frac{\lambda s_3}{cs_1s_2},\quad s_1\le\frac{\lambda s_2^2}{ds_3^2}.$$

The geometric mean of these inequalities yields

$$s_1\le\frac{\lambda}{(abcd)^{1/4}s_2s_3^{5/4}},$$

so that integrating gives an upper bound of a constant times $m^{-6}X^{5/6}/(abcd)$, as claimed. The other two extreme choices for S are treated similarly, except that only 3 of the 4 inequalities in (21) are useful. For the second set S it is s_3 that is to be bounded, and (21) gives

$$s_3\le\frac{\lambda^{1/2}}{a^{1/2}s_1^{1/2}s_2^2},\quad s_3\le\frac{\lambda^{1/2}}{b^{1/2}s_1^{1/2}s_2^{1/2}},\quad s_3\le\frac{\lambda^{1/2}s_2}{d^{1/2}s_1^{1/2}}.$$

[2]One does not need to explicitly work out all $2^{12}-2=4094$ integrals; it can be shown that the integral corresponding to any of these 4094 possibilities for S can be trivially bounded above by at least one of the integrals corresponding to a certain set of 33 choices of S. Evaluating these 33 integrals yields the theorem.

Thus, $s_3 \le \lambda^{1/2}/(abds_1s_2)^{1/2}$. The relevant inequalities for estimating the third set S are

$$s_2 \le \frac{\lambda^{1/4}}{a^{1/4}s_1^{1/4}s_3^{1/2}}, \quad s_2 \le \frac{\lambda}{bs_1s_3^2}, \quad s_2 \le \frac{\lambda s_3}{cs_1},$$

and here we take a weighted geometric mean leading to $s_2 \le \lambda/((abc)^{1/6}s_1^{1/2}s_3^{1/2})$. This concludes the proof of the theorem. □

Let $R^{(i)}(q,X)$ denote the expected number of points (A,B) in a fundamental domain that have first coordinate nonzero, are not totally irreducible, have absolute discriminant less than X, and correspond to a quartic order having index divisible by q. (Thus, these are contained among the points considered in Lemma 4.10.) To obtain an estimate for $N^{(i)}(q,X) + R^{(i)}(q,X)$, up to an error of $O(X^{11/12})$ due to the points in Lemma 4.9, we sum the estimate of Theorem 4.11 with $m = q^2$ over the $\nu(q)q^{24}$ translates of the lattice $q^2 \cdot V_{\mathbb{Z}}$ that comprise $S(q)$. We use Proposition 4.8 to sum the expression in the variables a, b, c, d, just as we used Proposition 2.9 in the proof of Corollary 2.15.

Corollary 4.12. *There is a constant θ such that if q is a positive squarefree integer, then*

$$N^{(i)}(q,X) = \nu(q)N^{(i)}(1,X) - R^{(i)}(q,X) + O\left(\left(\frac{q}{\varphi(q)}\right)^{\theta}\left(X^{11/12} + q^2X^{5/6}\log^4 X + q^{22}\log X\right)\right).$$

The constant θ in this result depends on the the O-constant in Corollary 4.8, the function $f(a,b,c,d)$ there, and also on the fact that $\nu(q)q^2 = O\left((q/\varphi(q))^2\right)$. The exact determination of θ is unimportant to our results.

It is possible to slightly improve Corollary 4.12 by being a little more careful with the three extreme sets S in the proof of Theorem 4.11, obtaining $\log X$ in place of $\log^4 X$. This improvement is also unimportant to our results.

4.4. **Maximal orders.** We are now ready to prove Theorem 1.3, which we restate in slightly stronger form.

Theorem 4.13. *For $i = 0, 1, 2$, the number of isomorphism classes of S_4-quartic fields having $4 - 2i$ real embeddings and absolute discriminant less than X is*

$$\frac{\beta}{2n_i}X + O\left(X^{23/24}\log^{29/6} X\right), \tag{24}$$

where β is as defined in Theorem 1.3.

Proof. By inclusion-exclusion, the number of classes of maximal quartic orders having $4 - 2i$ real embeddings and absolute discriminant less than X is given by

$$\sum_{q \ge 1} \mu(q)N^{(i)}(q,X). \tag{25}$$

As maximal quartic orders correspond exactly with quartic fields, (25) also represents the count in the theorem. We sum (25) for q up to a large number Q (to be chosen later to minimize error terms) using Corollary 4.12, and truncate the

tail using Lemma 4.3. We thus obtain that the number of such classes of maximal orders is equal to

$$N^{(i)}(1,X)\sum_{q\le Q}\mu(q)\nu(q)+O(E_1)+O(E_2)+O(E_3), \tag{26}$$

where

$$E_1=\sum_{q\le Q}\left(\frac{q}{\varphi(q)}\right)^{\theta}(X^{11/12}+q^2X^{5/6}\log^4 X+q^{22}\log X),\quad E_2=\sum_{q>Q}N^{(i)}(q,X),$$

and $E_3=\sum_{q\le Q}R^{(i)}(q,X)$.

It follows from Lemmas 4.9, 4.10, and an argument analogous to the one in the cubic case, that $E_3=O(X^{11/12+\varepsilon})$. Note that generalizing (15) we have $\sum_{q\le y}(q/\varphi(q))^{\theta}=O(y)$ for any fixed θ. Using Lemma 4.3 and proceeding just as in the proof of Theorem 2.16 to estimate E_1 and E_2, we then obtain that (25) is

$$\frac{\beta}{\zeta(2)^2\zeta(3)}N^{(i)}(1,X)+O\left(QX^{11/12}+Q^3X^{5/6}\log^4 X+Q^{23}\log X+XQ^{-1}\log^5 Q\right).$$

By Lemma 4.2 and choosing $Q=X^{1/24}(\log X)^{1/6}$ we obtain the desired result. □

5. 2-torsion in the class groups of cubic fields

We follow an analogous strategy. Let $\mathcal{O}$ be an order in an S_4-quartic field, and let $p\in\mathbb{Z}$ be a prime such that $\mathcal{O}$ is maximal at p. We say p is *overramified* in $\mathcal{O}$ if (p) factors into primes in $\mathcal{O}$ as P^4, P^2, or $P_1^2P_2^2$. Similarly, the archimedean prime of $\mathbb{Z}$ (the "prime at infinity") is *overramified* in $\mathcal{O}$ if it factors into the product of two ramified places (i.e., $\mathcal{O}\otimes\mathbb{R}$ is totally complex). A quartic maximal order $\mathcal{O}$ (or the quartic field K_4 in which it lies) is *nowhere overramified* if no prime of $\mathbb{Z}$ (finite or infinite) is overramified in $\mathcal{O}$.

The significance of being "nowhere overramified" is as follows. Given an S_4-quartic field K_4, let K_{24} denote its Galois closure. Let K_3 denote a cubic field contained in K_{24} (the "cubic resolvent field"), and let K_6 be the unique quadratic extension of K_3 such that the Galois closure of K_6 over $\mathbb{Q}$ is precisely K_{24}. Then one checks that the quadratic extension K_6/K_3 is unramified precisely when the quartic field K_4 is nowhere overramified. Conversely, if K_3 is a noncyclic cubic field, and K_6 is an unramified quadratic extension of K_3, then the Galois closure of K_6 is an S_4-extension K_{24} which contains up to conjugacy a unique, nowhere overramified quartic extension K_4.

In particular, we have following lemma due to Heilbronn.

Lemma 5.1 (Heilbronn [22])**.** *Let K_3 be a noncyclic cubic field. The number of isomorphism classes of S_4-quartic fields K_4 whose cubic resolvent field is isomorphic to K_3 is $\#\operatorname{Cl}_2(K_3)-1$.*

Let $M^{(i)}(q,X)$ be the number of isomorphism classes of S_4-quartic orders $\mathcal{O}$ with $4-2i$ real embeddings and absolute discriminant less than X such that, at every prime p dividing q, $\mathcal{O}$ is either nonmaximal at p or is maximal but overramified at p. Then:

Lemma 5.2. *For q a squarefree integer, we have*

$$M^{(i)}(q,X)\ =\ O(X\cdot 6^{\omega(q)}/q^2). \tag{27}$$

This follows from Lemma 2.3 and [6, §3.2].

Let $W(q) \subset V_{\mathbb{Z}}$ denote the set of all elements corresponding to quartic rings that, for every prime p dividing q, are either nonmaximal at p or are maximal at p but are overramified at p. Thus, for a prime $q = p$, $W(p) = S(p) \cup T(p)$, where $T(p)$ denotes the set of elements in $V_{\mathbb{Z}}$ corresponding to quartic orders that are maximal at p and overramified at p.

Like $S(p)$, the set $T(p)$ is defined by congruence conditions modulo p^2. Indeed, an element $(A, B) \in V_{\mathbb{Z}}$ is in $T(p)$ if and only if (a) it corresponds to a quartic order maximal at p (which we have already seen is a condition modulo p^2) and (b) it has either a quadruple point of intersection or two double points of intersection in $\mathbb{P}^2(\bar{\mathbb{F}}_p)$ (which is clearly a condition modulo p).

By the Chinese Remainder Theorem it follows that for all positive squarefree integers q, $W(q)$ may be expressed as the union of some number $\kappa \geq k$ of translates $L_1, \ldots, L_\kappa$ of the lattice $q^2 \cdot V_{\mathbb{Z}}$. The following result, which follows from [6, eq. (37)], gives us the number κ as a function of q.

Lemma 5.3. *Let $\tau(q)$ be the multiplicative function defined on squarefree numbers q, where for prime p,*

$$\tau(p) = 1-(1-p^{-2})^2(1-p^{-3})^2 = 2p^{-2}+2p^{-3}-p^{-4}-4p^{-5}-p^{-6}+2p^{-7}+2p^{-8}-p^{-10}.$$

Then the number κ of translates of the lattice $q^2 \cdot V_{\mathbb{Z}}$ that comprise $W(q)$ is $\tau(q)q^{24}$.

For each of the κ translates $L_1, \ldots, L_\kappa$ of $q^2 \cdot V_{\mathbb{Z}}$ which comprise $W(q)$, let $(a_1, b_1, c_1, d_1), \ldots, (a_\kappa, b_\kappa, c_\kappa, d_\kappa)$ denote the respective quadruples consisting of the first four coordinates in their standard member. Note that each (a_i, b_i, c_i, d_i) is in $[1, q^2]^4$. From Lemma 5.3, we have $\kappa = \tau(q)q^{24} > 2q^{22}$, so on average, each integer quadruple in $[1, q^2]^4$ is hit $> 2q^{14}$ times. We now discuss the finer distribution of these κ quadruples.

We first prove the following lemma, which is the analogue of Lemma 4.5 for $T(p)$.

Lemma 5.4. *Suppose A is a ternary quadratic form over $\mathbb{Z}$, and let p be any prime. Let $\mathrm{rk}(A)$ denote the rank of A over $\mathbb{Z}/p\mathbb{Z}$. Then the number of values $\pmod{p^2}$ for the quadratic form B, such that $(A, B) \in T(p)$ is*

$$\begin{array}{ll} p^{10} + O(p^9), & \text{if } \mathrm{rk}(A) = 3; \\ p^{10} + O(p^9), & \text{if } \mathrm{rk}(A) = 2; \\ p^{12} + O(p^{11}), & \text{if } \mathrm{rk}(A) = 1; \\ 0, & \text{if } \mathrm{rk}(A) = 0. \end{array}$$

Proof. Suppose $\mathrm{rk}(A) = 3$. Then the number of $B \pmod{p^2}$ resulting in two double points of intersection in $\mathbb{P}^2(\bar{\mathbb{F}}_p)$ is $p^{10} + O(p^9)$, while the number resulting in a quadruple point of intersection is $O(p^9)$. The proportion of these that yield a quartic order not maximal at p is as before $O(1/p)$, by [6, §4.2]. Thus the total number of $B \pmod{p^2}$ such that $(A, B) \in T(p)$ is $p^{10} + O(p^9)$, as claimed.

If $\mathrm{rk}(A) = 2$, then in $\mathbb{P}^2(\bar{\mathbb{F}}_p)$, the degenerate conic A is the union of two distinct lines. The only values of B giving a quadruple point of intersection with A, as conics in $\mathbb{P}^2(\bar{\mathbb{F}}_p)$, are those that yield degenerate conics having the same double point in $\mathbb{P}^2(\bar{\mathbb{F}}_p)$ as A. It is easy to see using [6, §4.2] that such (A, B) cannot be maximal at p. Meanwhile, the number of $B \pmod{p^2}$ such that (A, B) yield two double points of intersection in $\mathbb{P}^2(\bar{\mathbb{F}}_p)$ is $p^{10} + O(p^9)$, and again a negligible proportion $O(1/p)$ of these give quartic rings not maximal at p. This proves the claim in this case.

If $\mathrm{rk}(A) = 1$, then in $\mathbb{P}^2(\mathbb{F}_p)$, the (degenerate) conic determined by A is a double line. As conics in $\mathbb{P}^2(\bar{\mathbb{F}}_p)$, any B that does not share a component with A will have either a quadruple point or two double points of intersection with A. A negligible number of these $B \pmod{p^2}$ will correspond to quartic rings nonmaximal at p. Thus we obtain a total of $p^{12} + O(p^{11})$ values of B in this case.

Finally, if $\mathrm{rk}(A) = 0$, then as already noted in the proof of Lemma 4.5, no B gives an (A, B) that is maximal at p. This completes the proof. □

Proposition 5.5. *Fix $a, b, c, d \in \mathbb{Z}/p^2\mathbb{Z}$. Then modulo p^2, the number of $(A, B) \in T(p)$ with given values of a, b, c, d is*

$$\begin{array}{rll} p^{14} + O(p^{13}), & \text{if } b^2 - 4ad \not\equiv 0 \pmod{p}; \\ \leq 2p^{14} + O(p^{13}), & \text{if } b^2 - 4ad \equiv 0 \pmod{p} \text{ but } \gcd(a, c) \not\equiv 0 \pmod{p}; \\ p^{15} + O(p^{14}), & \text{otherwise.} \end{array}$$

Proof. If $b^2 - 4ad \not\equiv 0 \pmod{p}$, then $\mathrm{Det}(A)$, as a polynomial function of $u = a_{23}$ and $v = a_{33}$, does not identically vanish. Hence the number of possible values of u, $v \pmod{p^2}$ for which $\mathrm{Det}(A)$ is nonzero $\pmod{p}$ is $p^4 + O(p^3)$. By the lemma, the number of values of $(A, B) \pmod{p^2}$ with $\mathrm{rk}(A) = 3$, $(A, B) \in T(p)$, and the given values of a, b, c, d, is $(p^4 + O(p^3))(p^{10} + O(p^9)) = p^{14} + O(p^{13})$. We now consider those $O(p^3)$ choices of $u, v \pmod{p^2}$ for which A has vanishing determinant $\pmod{p}$. The rank of $A \pmod{p}$ will be 2 in such a case. By Lemma 5.4, the number of values of $(A, B) \pmod{p^2}$ with $\mathrm{rk}(A) = 2$, $(A, B) \in T(p)$, and the given values of a, b, c, d, is then $(O(p^3))(p^{10} + O(p^9)) = O(p^{13})$. This takes care of the first case.

Suppose we are now in the second case, i.e., $b^2 - 4ad \equiv 0 \pmod{p}$ but at least one of $a, c \not\equiv 0 \pmod{p}$. In this case, by the same argument as in the first case, we have at most $p^{14} + O(p^{13})$ possible values for $(A, B) \pmod{p^2}$ with $\mathrm{rk}(A) \geq 2$, $(A, B) \in T(p)$, and the given values of a, b, c, d. However, in this second case, we also have the possibility $\mathrm{rk}(A) = 1$. Note that $A \pmod{p}$ will be of rank 1 only if $c^2 - 4av \equiv bc - 2au \equiv 0$. If a is nonzero $\pmod{p}$, then (assuming $p > 2$) v and u are determined $\pmod{p}$ by the given information, so there are exactly p^2 choices possible for the pair $(u, v) \pmod{p^2}$ for which the condition $\mathrm{rk}(A) = 1$ holds. If a is zero $\pmod{p}$, then for $\mathrm{rk}(A) = 1$ to hold, we also then need $c \equiv 0 \pmod{p}$, a contradiction. Thus, regardless of the value of a, there are at most p^2 values of $u, v \pmod{p^2}$ yielding $\mathrm{rk}(A) = 1$. By Lemma 5.4, we conclude that the number of values of (A, B) with $\mathrm{rk}(A) = 1$, $(A, B) \in T_p$, and our given values of a, b, c, d is at most $p^2(p^{12} + O(p^{11})) = p^{14}$, which takes care of this case.

Finally, we consider the last case where $b^2 - 4ad \equiv a \equiv c \equiv 0 \pmod{p}$, which also implies $b \equiv 0 \pmod{p}$. The condition on a, b, c, d implies that $\mathrm{Det}(A)$ vanishes $\pmod{p}$. Thus the rank of A is at most 2, regardless of u and v. The number of values of u and $v \pmod{p^2}$ with $\mathrm{rk}(A) = 2$ is thus less than p^4; by Lemma 5.4, the number of $(A, B) \in T_p$, with $\mathrm{rk}(A) = 2$ and the given values of a, b, c, d, is at most $p^{14} + O(p^{13})$.

Now for $A \pmod{p}$ to be rank 1 for some values of u and v, we must have $u^2 \equiv 4dv \pmod{p}$, so if d is not zero $\pmod{p}$, then $v \pmod{p}$ is determined by u (assuming $p > 2$), while if $d \equiv 0 \pmod{p}$, then $u \equiv 0 \pmod{p}$ and v may be any nonzero residue $\pmod{p}$. Thus, regardless of the value of d, the number of values of u and $v \pmod{p^2}$ with $\mathrm{rk}(A) = 1$ in this case is p^3. By Lemma 5.4, the number of (A, B) not maximal at p, with $\mathrm{rk}(A) = 1$ and the given values of a, b, c, d, is $p^3(p^{12} + O(p^{11})) = p^{15} + O(p^{14})$. This completes the proof of the proposition. □

Corollary 5.6. *Let q be squarefree and let (a,b,c,d) be a quadruple of integers in $[1,q^2]^4$. The number of translates L_j of $q^2 \cdot V_{\mathbb{Z}}$ that comprise $W(q)$ and have (a,b,c,d) as the first four coordinates of some member is*

$$\left(2^g \gcd(q,a,b,c) + 6^f\right)\left(q^{14} + O\left(q^{13}\right)\right),$$

where f is as in Corollary 4.8 *and*

$$0 \le g \le \sum_{\substack{p \mid \gcd(q,b^2-4ad) \\ p \nmid \gcd(a,c)}} 1.$$

Proof. This follows from Corollary 4.8 and Proposition 5.5, together with the Chinese Remainder Theorem. □

Let $S^{(i)}(q,X)$ denote the expected number of points (A,B) in a fundamental domain that have first coordinate nonzero, are not totally irreducible, have absolute discriminant less than X, and correspond to a quartic order that for each prime p dividing q has either index divisible by p or is maximal at p but is overramified at p. Combining Theorem 4.11 and Corollary 5.6, we have the following result that is completely analogous to Corollary 4.12.

Corollary 5.7. *Let q be a positive squarefree integer. There is some positive constant θ such that for $i = 0, 1, 2$,*

$$M^{(i)}(q,X) = \tau(q)M^{(i)}(1,X) - S^{(i)}(q,X) + O\left(2^{\omega(q)}\left(\frac{q}{\varphi(q)}\right)^{\theta}\left(X^{11/12} + q^2X^{5/6}\log^4 X + q^{22}\log X\right)\right).$$

We are now ready to prove Theorem 1.4. We do so as we did Theorem 1.3 in the previous section, but we also use Theorem 1.1 plus the identities

$$\begin{aligned}\sum_{0<\mathrm{Disc}(K_3)<X} (\#\,\mathrm{Cl}_2(K_3) - 1) &= \sum_{q\ge 1}\mu(q)M^{(0)}(q,X),\\ \sum_{0<-\mathrm{Disc}(K_3)<X} (\#\,\mathrm{Cl}_2(K_3) - 1) &= \sum_{q\ge 1}\mu(q)M^{(1)}(q,X),\end{aligned}$$

where K_3 runs over *noncyclic* cubic fields.

Finally, we note that Wong's estimate [34, 35]

$$\sum_{\substack{0<\mathrm{Disc}(K_3)<X \\ K_3 \text{ cyclic}}} (\#\,\mathrm{Cl}_2(K_3) - 1) = O(X^{5/6+\varepsilon})$$

shows that the contribution of cyclic fields to the sums in (5) and (6) is negligible; thus the asymptotics of these sums, and the stated error terms, do not change regardless of whether or not these sums include cyclic cubic fields.

References

[1] K. Belabas, *A fast algorithm to compute cubic fields*, Math. Comp. **66** (1997), 1213–1237.

[2] ———, *On the mean 3-rank of quadratic fields*, Compositio Mathematica **118** (1999), 1–9, corrigendum *ibid.* **140** (2004), p. 1221.

[3] ———, *On quadratic fields with large 3-rank*, Math. Comp. **73** (2004), no. 248, 2061–2074.

[4] M. Bhargava, *Simple proofs of the Davenport–Heilbronn theorems*, preprint.

[5] ———, *Higher composition laws III: The parametrization of quartic rings and fields*, Ann. of Math. (2) **160** (2004), 1329–1360.

[6] ———, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), 1031–1063.
[7] H. Cohen, *Constructing and counting number fields*, Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002), Higher Ed. Press, 2002, pp. 129–138.
[8] ——— *Counting A_4 and S_4 number fields with given resolvent cubic*, High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, 159–168, Fields Inst. Commun., 41, Amer. Math. Soc., Providence, RI, 2004.
[9] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Construction of tables of quartic fields, using Kummer theory*, ANTS IV, Leiden, 257–268, Lecture Notes in Comput. Sci. **1838**, Springer, Berlin, 2000.
[10] ——— *Counting discriminants of number fields*, J. Théorie Nombres Bordeaux **18** (2006), 573–593.
[11] H. Cohen and J. Martinet, *Heuristics on class groups: some good primes are not too good*, Math. Comp. **63** (1994), 329–334.
[12] B. Datskovsky and D. J. Wright, *The adelic zeta function associated to the space of binary cubic forms. II. Local theory*, J. Reine Angew. Math. **367** (1986), 27–75.
[13] ———, *Density of discriminants of cubic extensions*, J. Reine Angew. Math. **386** (1988), 116–138.
[14] H. Davenport, *On the class-number of binary cubic forms. I*, J. London Math. Soc. **26** (1951), 183–192, errata *ibid.* **27** (1951), p. 512.
[15] ———, *On the class-number of binary cubic forms. II*, J. London Math. Soc. **26** (1951), 192–198.
[16] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London A **322** (1971), 405–420.
[17] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, Translations of Mathematical Monographs, vol. 10, American Mathematical Society, 1964.
[18] V. Ennola and R. Turunen, *On totally real cubic fields*, Math. Comp. **44** (1985), 495–518.
[19] G. W. Fung and H. C. Williams, *On the computation of a table of complex cubic fields with discriminant $D > -10^6$*, Math. Comp. **55** (1990), 313–325. Table Errata 615, *ibid.* **63** (1994), 433.
[20] W. T. Gan, B. Gross, and G. Savin, *Fourier coefficients of modular forms on G_2*, Duke Math. J. **115** (2002), 105–169.
[21] H. Hasse, *Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage*, Math. Zeitschrift **31** (1930), 565–582.
[22] H. Heilbronn, *On the 2-classgroup of cubic fields*, Studies in Pure Math., 117–119, Academic Press, London, 1971.
[23] C. Hermite, *Sur la réduction des formes cubiques à deux indéterminées*, C. R. Acad. Sci. Paris **48** (1859), 351–357.
[24] M. J. Jacobson Jr., private communication.
[25] M. J. Jacobson Jr., S. Ramachandran, and H. C. Williams, *Numerical results on class groups of imaginary quadratic fields*, ANTS VII, Berlin, 87–101, Lecture Notes in Comput. Sci. **4076**, Springer, Berlin, 2006.
[26] P. Llorente and J. Quer, *On totally real cubic fields with discriminant $D < 10^7$*, Math. Comp. **50** (1988), 581–594.
[27] G. Malle, *The totally real primitive number fields of discriminant at most 10^9*, ANTS VII, Berlin, 114–123, Lecture Notes in Comput. Sci. **4076**, Springer, Berlin, 2006.
[28] ———, *Cohen–Lenstra heuristic and roots of unity*, J. Number Theory **128**, 2823–2835.
[29] G.-B. Mathews, *On the reduction and classification of binary cubics which have a negative discriminant*, Proc. London Math. Soc. **10** (1912), 128–138.
[30] J. Nakagawa, *Orders of a quartic field*, Mem. Amer. Math. Soc. **122** (1996), no. 583.
[31] D. P. Roberts, *Density of cubic field discriminants*, Math. Comp. **70** (2001), 1699–1705.
[32] T. Shintani, *On Dirichlet series whose coefficients are class numbers of integral binary cubic forms*, J. Math. Soc. Japan **24** (1972), 132–188.
[33] ———, *On zeta-functions associated with the vector space of quadratic forms*, J. Fac. Sci. Univ. Tokyo, Sec. Ia **22** (1975), 25–66.
[34] S. Wong, *Automorphic forms on* GL(2) *and the rank of class groups*, J. Reine Angew. Math. **515** (1999), 125–153.

[35] ———, *Densities of quartic fields with even Galois groups*, Proc. Amer. Math. Soc. **133** (2005), 2873–2881.

Département de Mathématiques, Université Bordeaux 1, F-33405 Talence, France
E-mail address: Karim.Belabas@math.u-bordeaux.fr

Department of Mathematics, Princeton University, Princeton, NJ 08544, USA
E-mail address: bhargava@math.princeton.edu

Department of Mathematics, Dartmouth College, Hanover, NH 03784, USA
E-mail address: carl.pomerance@dartmouth.edu