ON ℓ-TORSION IN CLASS GROUPS OF NUMBER FIELDS

JORDAN ELLENBERG, LILLIAN. B. PIERCE, AND MELANIE MATCHETT WOOD

Abstract. For each integer $\ell \geq 1$, we prove an unconditional upper bound on the size of the ℓ-torsion subgroup of the class group, which holds for all but a zero-density set of field extensions of $\mathbb{Q}$ of degree d, for any fixed $d \in \{2,3,4,5\}$ (with the additional restriction in the case $d = 4$ that the field be non-D_4). For sufficiently large ℓ (specified explicitly), these results are as strong as a previously known bound that is conditional on GRH. As part of our argument, we develop a probabilistic "Chebyshev sieve," and give uniform, power-saving error terms for the asymptotics of quartic (non-D_4) and quintic fields with chosen splitting types at a finite set of primes.

1. Introduction

The distribution of class groups is a great mystery. The Cohen-Lenstra heuristics [CL84] (for quadratic fields) and the Cohen-Lenstra-Martinet heuristics [CM90] (for more general number fields) make predictions for the distribution of class groups, including for the average size of the ℓ-torsion subgroups for certain "good" primes ℓ. However, the questions of proving anything towards these predictions are almost entirely open, and mostly apparently inaccessible.

The main goal of the present work is to prove, for each integer $\ell \geq 1$, an unconditional upper bound for the size of the ℓ-torsion subgroup of the class group, which holds for all but a zero-density set of field extensions of $\mathbb{Q}$ of degree d, for any fixed $d \in \{2,3,4,5\}$ (with the additional restriction in the case $d = 4$ that the field be non-D_4). Alternatively, these results may be viewed as the first unconditional upper bounds for the average size of ℓ-torsion in class groups as the field varies over extensions of $\mathbb{Q}$ of fixed degree $d \in \{2,3,4,5\}$ (and non-D_4 in the case $d = 4$).

Let K be a degree d field extension of $\mathbb{Q}$ with absolute discriminant $D_K = |\operatorname{disc} K/\mathbb{Q}|$. We will denote the class group by Cl_K and the ℓ-torsion subgroup by $\mathrm{Cl}_K[\ell]$. We note the trivial pointwise upper bound (see for example [Nar80, Thm 4.4])

$$|\mathrm{Cl}_K[\ell]| \leq |\mathrm{Cl}_K| \ll_{d,\varepsilon} D_K^{1/2+\varepsilon}, \tag{1.1}$$

for every $\varepsilon > 0$. (Throughout, $\varepsilon > 0$ is allowed to be arbitrarily small (possibly taking a different value in different occurrences), and $A \ll B$ indicates that $|A| \leq cB$ for an implied constant c, which we allow in any instance to depend on ℓ, d, ε.)

It is conjectured that

$$|\mathrm{Cl}_K[\ell]| \ll D_K^{\varepsilon} \tag{1.2}$$

for every $\varepsilon > 0$, but improving on the trivial bound (1.1) has proved difficult. (Impetus for this conjecture may be found in Duke [Duk98], Zhang [Zha05, page 10], and Brumer and Silverman [BS96, "Question CL(ℓ, d)"].) For K quadratic, Gauss's genus theory [Gau01] implies (1.2) in the case $\ell = 2$. Recently, [BST$^+$17] obtained nontrivial upper bounds for 2-torsion in fields of degree d for all $d \geq 3$, proving $|\mathrm{Cl}_K[2]| \ll D_K^{0.2784\ldots+\varepsilon}$ for $d = 3, 4$ and $|\mathrm{Cl}_K[2]| \ll D_K^{1/2-1/2d+\varepsilon}$ for $d \geq 5$. For $\ell = 3$, after initial incremental improvement in [HV06], [Pie05], [Pie06] over the trivial bound (1.1) for quadratic fields, Ellenberg and Venkatesh proved [EV07, Prop. 3.4, Cor. 3.7] that

$$|\mathrm{Cl}_K[3]| \ll D_K^{1/3+\varepsilon} \tag{1.3}$$

2010 *Mathematics Subject Classification.* 11R29, 11N36 11R45 .

Key words and phrases. number fields, class groups, ℓ-torsion, Cohen-Lenstra heuristics, sieves.

holds for both quadratic and cubic fields, and moreover there is a positive constant $\delta > 0$ such that

$$|\mathrm{Cl}_K[3]| \ll D_K^{1/2-\delta+\varepsilon} \tag{1.4}$$

holds for quartic fields. (In particular, one may take $\delta = 1/168$ in (1.4) for quartic fields with Galois closure having Galois group A_4 or S_4.) At this time, these are the best bounds in the literature that are unconditional and hold for all such fields.

In the realm of average results, there is little known, with the exceptions being spectacular successes. For 3-torsion in quadratic fields, Davenport and Heilbronn [DH71] proved

$$\sum_{\substack{\deg(K)=2\\ 0<D_K\le X}} |\mathrm{Cl}_K[3]| \sim \left(\frac{2}{3\zeta(2)} + \frac{1}{\zeta(2)}\right) X, \tag{1.5}$$

in which the first contribution is from fields with $\operatorname{disc} K/\mathbb{Q} > 0$ and the second is from fields with $\operatorname{disc} K/\mathbb{Q} < 0$; this has recently been improved to reflect second order terms by [BST13], [TT13] and [Hou]. For 2-torsion in cubic fields, Bhargava [Bha05] proved the asymptotic

$$\sum_{\substack{\deg(K)=3\\ 0<D_K\le X}} |\mathrm{Cl}_K[2]| \sim \left(\frac{5}{48\zeta(3)} + \frac{3}{8\zeta(3)}\right) X, \tag{1.6}$$

in which each isomorphism class of fields is counted once, and the first contribution is from fields with $\operatorname{disc} K/\mathbb{Q} > 0$ and the second is from fields with $\operatorname{disc} K/\mathbb{Q} < 0$. For 4-torsion in quadratic fields, Fouvry and Klüners [FK06] have determined the asymptotics, for each non-negative integer k,

$$\sum_{\substack{\deg(K)=2\\ 0<D_K\le X}} |\mathrm{Cl}_K^2[2]|^k \sim (c_k + p^{-k}(c_{k+1} - c_k))X, \tag{1.7}$$

where c_k is the number of vector subspaces of $\mathbb{F}_2^k$. See also the recent work of Klys [Kly16] giving analogous results on 3-torsion in cyclic cubic fields, and the recent work of Milovic on 16-rank in quadratic fields, e.g. [Mil15].

Turning to conditional results, Klys's results [Kly16] extend to p-torsion in cyclic degree p fields under GRH and Smith [Smi16] has results on 8-torsion averages in quadratic fields under GRH as well. In the case of quadratic fields, Wong [Won99b] proved that, conditional on the Birch–Swinnerton-Dyer conjecture and the Riemann Hypothesis, $|\mathrm{Cl}_K[3]| \ll D_K^{1/4+\varepsilon}$. Before the proof of (1.3), Soundararajan noted (as communicated in [HV06]) that one could prove $|\mathrm{Cl}_K[3]| \ll D_K^{1/3+\varepsilon}$ for K quadratic if one assumed the truth of the Riemann Hypothesis for only the L-function $L(s,\chi)$ of the quadratic character χ associated to the quadratic field K. The key idea of the latter bound was the use of many small primes that split in K; the role of the Riemann Hypothesis was to guarantee the existence of sufficiently many such primes. This approach has been generalized by Ellenberg and Venkatesh [EV07] to number fields of any degree; we recall the key result in the special case of field extensions of $\mathbb{Q}$:

Theorem A (Lemma 2.3 of [EV07])**.** *Let K be a field extension of $\mathbb{Q}$ of degree d, and let ℓ be a positive integer. Let $\delta < \frac{1}{2\ell(d-1)}$. Suppose that $\{\mathfrak{p}_1, \dots, \mathfrak{p}_M\}$ are M prime ideals in $\mathcal{O}_K$ with $\mathrm{Norm}(\mathfrak{p}_j) \le D_K^{\delta}$ that are unramified in $K/\mathbb{Q}$ and are not extensions of ideals from any proper subfield $K_0 \subsetneq K$. Then*

$$|\mathrm{Cl}_K[\ell]| \ll_{d,\ell,\varepsilon} D_K^{1/2+\varepsilon} M^{-1}. \tag{1.8}$$

(Here we recall the convention in [EV07] that an ideal $\mathfrak{p}$ in $\mathcal{O}_K$ is said to be an extension of a prime ideal from a subfield $K_0 \subsetneq K$ if there is a prime ideal $\mathfrak{p}_0$ in $\mathcal{O}_{K_0}$ such that $\mathfrak{p} = \mathfrak{p}_0\mathcal{O}_K$.)

Upon assuming GRH, an application of the effective Chebotarev theorem of Lagarias and Odlyzko [LO75] guarantees, for any fixed $\eta > 0$, the existence of $\gg D_K^{\eta-\varepsilon}$ rational primes of size $\le D_K^{\eta}$ that split completely in K. Upon choosing $\eta = \frac{1}{2\ell(d-1)} - \varepsilon_0$ for arbitrarily small $\varepsilon_0 > 0$, one obtains the following bound, currently the state of the art for conditional pointwise upper bounds for $|\mathrm{Cl}_K[\ell]|$:

Theorem B (Prop. 3.1 of [EV07])**.** *Let K be a field extension of $\mathbb{Q}$ of degree d and ℓ a positive integer. Assuming GRH,*

$$|\mathrm{Cl}_K[\ell]| \ll_{d,\ell,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell(d-1)}+\varepsilon}, \tag{1.9}$$

for any $\varepsilon > 0$.

One may attempt to remove the conditionality by proving results that hold on average, or for all but a small exceptional family. In this vein, in the case of imaginary quadratic fields, Soundararajan [Sou00] noted that for all but at most one imaginary quadratic field K with $D_K \in [X, 2X]$, one has the bound $|\mathrm{Cl}_K[\ell]| \ll X^{1/2-1/2\ell+\varepsilon}$, for any prime ℓ. Also in the imaginary quadratic case, a recent result of Heath-Brown and Pierce [HBP17] provides an upper bound for averages (and in addition higher moments) of $|\mathrm{Cl}_K[\ell]|$, for example proving for any prime $\ell \geq 5$ that

$$\sideset{}{'}\sum_{\substack{\deg(K)=2\\ 0<D_K\leq X}} |\mathrm{Cl}_K[\ell]| \ll X^{\frac{3}{2}-\frac{3}{2\ell+2}+\varepsilon}, \tag{1.10}$$

with the sum restricted to imaginary quadratic fields.

In this paper, we prove *unconditional* results for $|\mathrm{Cl}_K[\ell]|$ that are as strong as (1.9) for all sufficiently large positive integers ℓ, and hold for all but a zero-density family of quadratic, cubic, non-D_4-quartic, or quintic field extensions of $\mathbb{Q}$.

For this we work with families of fields. Let $N_d(X)$ denote the number of degree d extensions of $\mathbb{Q}$ with $0 < D_K \leq X$, in which each isomorphism class is counted once; it is conjectured that for an appropriate constant c_d,

$$N_d(X) \sim c_d X. \tag{1.11}$$

Importantly for our work, this is known to be true for $d = 2$ (classical), $d = 3$ by Davenport and Heilbronn [DH71], $d = 4$ by Cohen, Diaz y Diaz, and Olivier [CDyDO02] and Bhargava [Bha05], and $d = 5$ by Bhargava [Bha10]. Throughout our work, in the case of $d = 4$, we restrict our attention to non-D_4-quartic fields (that is, quartic extensions whose Galois closure does not have Galois group D_4); see Remark 4.1. Thus we let $\tilde{N}_4(X)$ denote the further restricted count of non-D_4-quartic extensions of $\mathbb{Q}$; then (1.11) is also known to hold for $\tilde{N}_4(X)$, with a different constant [Bha05].

As a consequence of the field counts (1.11) combined with the trivial bound (1.1), a trivial average bound for $|\mathrm{Cl}_K[\ell]|$ is

$$\sum_{\substack{\deg(K)=d\\ 0<D_K\leq X}} |\mathrm{Cl}_K[\ell]| \ll_{d,\varepsilon} X^{3/2+\varepsilon}. \tag{1.12}$$

Our approach to improve upon (1.12) is to show that "most" degree d fields K contain sufficiently many small primes that split completely in K for Theorem A to give a good upper bound for $|\mathrm{Cl}_K[\ell]|$. Roughly speaking, we will show that there is some small $\delta_0 > 0$ such that for all but at most $O(X^{1-\delta_0})$ of the degree d fields K with $0 < D_K \leq X$, at least a fixed positive proportion of the primes $p \leq X^{\delta_0}$ split completely in K. (Under GRH, the small set of exceptional fields is in fact empty.)

Our main results are as follows:

Theorem 1.1. *Let $d \in \{2, 3, 4, 5\}$ and let ℓ be any positive integer with $\ell \geq \ell(d)$ where*

$$\ell(2) = \ell(3) = 1, \qquad \ell(4) = 8, \qquad \ell(5) = 25.$$

Then for all but $O_{d,\ell,\varepsilon}(X^{1-\frac{1}{2\ell(d-1)}+\varepsilon})$ degree d fields $K/\mathbb{Q}$ with $D_K \leq X$ (and non-D_4 in the case $d = 4$),

$$|\mathrm{Cl}_K[\ell]| \ll_{d,\ell,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell(d-1)}+\varepsilon},$$

for all $\varepsilon > 0$. For $d = 4, 5$, in the remaining cases of positive integers $\ell < \ell(d)$, for all but $O_{d,\varepsilon}(X^{1-\delta_0(d)+\varepsilon})$ degree d fields $K/\mathbb{Q}$ with $0 < D_K \leq X$ (and non-D_4 in the case $d = 4$),

$$|\mathrm{Cl}_K[\ell]| \ll_{d,\ell,\varepsilon} D_K^{\frac{1}{2}-\delta_0(d)+\varepsilon},$$

for all $\varepsilon > 0$, where we may take

$$\delta_0(d) = \begin{cases} 1/48 & \text{if } d = 4 \\ 1/200 & \text{if } d = 5. \end{cases}$$

Remark 1.1. Theorem 2.1 states a version of this result in terms of bounding the number of exceptional fields that fail to have many small split primes. One notes from Theorem 2.1 that for sufficiently large ℓ, the limiting reagent is not the availability of small completely split primes, but the constraint $\delta < (2\ell(d-1))^{-1}$ in Theorem A.

As immediate corollaries, we note:

Corollary 1.1.1. *Let $d \in \{2,3,4,5\}$. As K ranges over degree d extensions of $\mathbb{Q}$ with discriminant $0 < D_K \leq X$ (and non-D_4 in the case $d = 4$),*

$$\sum_{\substack{\deg(K)=d \\ 0<D_K\leq X}} |\mathrm{Cl}_K[\ell]| \ll_{d,\varepsilon} X^{\frac{3}{2}-\frac{1}{2\ell(d-1)}+\varepsilon},$$

for all integers $\ell \geq \ell(d)$, where $\ell(2) = \ell(3) = 1$, $\ell(4) = 8$, $\ell(5) = 25$.

Corollary 1.1.2. *For positive integers $\ell \leq 7$, averaging over non-D_4-quartic fields,*

$$\sum_{\substack{\deg(K)=4 \\ 0<D_K\leq X}}{}' |\mathrm{Cl}_K[\ell]| \ll_{d,\varepsilon} X^{\frac{3}{2}-\frac{1}{48}+\varepsilon}.$$

For positive integers $\ell \leq 24$, averaging over quintic fields,

$$\sum_{\substack{\deg(K)=5 \\ 0<D_K\leq X}} |\mathrm{Cl}_K[\ell]| \ll_{d,\varepsilon} X^{\frac{3}{2}-\frac{1}{200}+\varepsilon}.$$

Our strategy is as follows. Recall that $N_d(X)$ denotes the number of degree d fields K over $\mathbb{Q}$, up to isomorphism, with $0 < D_K \leq X$, and let $N_d(X;p)$ denote the number of degree d fields K over $\mathbb{Q}$, up to isomorphism, with $0 < D_K \leq X$, such that the rational prime p splits completely in K. (For $d = 4$ we define $\tilde{N}_4(X;p)$ analogously, restricting to non-D_4-quartic fields.) Suppose we know that for each fixed prime p, $N_d(X;p)$ is a positive proportion of $N_d(X)$, so p splits completely in a positive proportion of the fields. Then one would expect the fields in which the primes split completely to distribute somewhat evenly, so that "most fields" have the property that "near the average number" of primes split completely in them; that is, one would expect that the primes do not conspire to cause many fields to fail the criterion of Theorem A. We will make this argument precise by developing a flexible "Chebyshev sieve" (Lemma 3.1, related to Chebyshev's inequality); the crucial input to the sieve will be asymptotics for $N_d(X;p)$ with power-saving error and explicitly given dependence on p (Lemma 2.2, Theorem C, Theorems 2.3 and 2.4).

Counting quadratic fields may be accomplished by a simple classical argument (given in an appendix, Section 8). Power-saving error terms for $N_d(X)$ were first found in the cases $d = 3, 4$ by Belabas, Bhargava, and Pomerance [BBP10], and first found in the case $d = 5$ by Shankar and Tsimerman [ST14]. In the case $d = 3$, Bhargava, Shankar, and Tsimerman [BST13] and Taniguchi and Thorne [TT13] have also proved a second main term and improved the power-saving error term. For the refined estimates that we require on $N_d(X;p)$, we quote the necessary asymptotics for $d = 3$ from [TT13], while for $d = 4, 5$ we prove the necessary estimates using the methods and results from [BBP10] and [ST14]. In fact, in Sections 4 and 5, we give the field counting asymptotics for fields with any chosen splitting types at a finite set of primes with the expectation that they could be useful in other applications; see Theorems 4.1 and 5.1. Our counting theorems improve upon analogous results that appear in four recent papers, three [Yan09, CK15, SST15b] in the area of finding symmetry groups of families of L-functions (see [SST15a] for a general overview of the area) and one [OT14] studying the distribution of ramified primes in small-degree number fields. See Sections 4 and 5 for detailed comparisons to these previous works.

2. Anatomy of the proof

2.1. **Reduction to counting bad fields.** We now outline the strategy in more detail; for the sake of motivation, we focus temporarily on proving upper bounds on average. Let us fix d and define for any degree d field K over $\mathbb{Q}$ and any real parameter $Y \geq 1$,

$$N(K;Y) = \#\{\text{rational primes } p \leq Y \text{ that split completely in } K\}.$$

(Implicitly, in the case $d = 4$ we further restrict to non-D_4-quartic fields.) Let us fix a positive integer ℓ and a parameter $\delta_1 < \frac{1}{2\ell(d-1)}$, to be chosen precisely later. Then by Theorem A, for any $X \geq 1$,

$$\begin{aligned}\sum_{X<D_K\leq 2X} |\mathrm{Cl}_K[\ell]| &\ll \sum_{X<D_K\leq 2X} D_K^{1/2+\varepsilon} N(K; D_K^{\delta_1})^{-1} \\ &\ll X^{1/2+\varepsilon} \sum_{X<D_K\leq 2X} N(K; X^{\delta_1})^{-1}.\end{aligned}$$

Now given real parameters $X \geq 1$ and $1 \leq M \leq Y$, we define $\mathscr{B}_d^0(X; Y, M)$ to be the set

$$\mathscr{B}_d^0(X; Y, M) = \{K/\mathbb{Q},\ \deg(K) = d,\ X < D_K \leq 2X :\ \text{at most } M \text{ primes } p \leq Y \text{ split completely in } K\},$$

(with the usual further restriction in the case $d = 4$).

We denote by $\pi(Y)$ the number of rational primes $p \leq Y$, and let us regard $1 \leq M \leq \pi(X^{\delta_1})$ as fixed for the moment, to be specified later. Then we may make the decomposition

$$\sum_{X<D_K\leq 2X} |\mathrm{Cl}_K[\ell]| \ll X^{1/2+\varepsilon} \left(\sum_{\substack{X<D_K\leq 2X \\ K\notin \mathscr{B}_d^0(X;X^{\delta_1},M)}} N(K; X^{\delta_1})^{-1} + \sum_{K\in \mathscr{B}_d^0(X;X^{\delta_1},M)} N(K; X^{\delta_1})^{-1} \right).$$

Since $N(K; X^{\delta_1}) \geq M$ if $K \notin \mathscr{B}_d^0(X; X^{\delta_1}, M)$, we have

$$\sum_{X<D_K\leq 2X} |\mathrm{Cl}_K[\ell]| \ll X^{1/2+\varepsilon} \left(\sum_{\substack{X<D_K\leq 2X \\ K\notin \mathscr{B}_d^0(X;X^{\delta_1},M)}} M^{-1} + \sum_{K\in \mathscr{B}_d^0(X;X^{\delta_1},M)} 1 \right),$$

and we may conclude that

$$\sum_{X<D_K\leq 2X} |\mathrm{Cl}_K[\ell]| \ll X^{3/2+\varepsilon} M^{-1} + \#\mathscr{B}_d^0(X; X^{\delta_1}, M) X^{1/2+\varepsilon}. \tag{2.1}$$

Then upon defining (with the usual further restriction in the case $d = 4$) the set

$$\mathscr{B}_d(X; Y, M) = \{K/\mathbb{Q},\ \deg(K) = d,\ 0 < D_K \leq X :\ \text{at most } M \text{ primes } p \leq Y \text{ split completely in } K\}, \tag{2.2}$$

we may trivially replace the expression $\#\mathscr{B}_d^0(X; X^{\delta_1}, M)$ in (2.1) by $\#\mathscr{B}_d(2X; X^{\delta_1}, M)$ and only increase the right-hand side.

We now suppose that we can bound from above the cardinality of the "bad set" $\mathscr{B}_d(2X; X^{\delta_1}, M)$ for appropriate δ_1 and M. Note that one expects via the Chebotarev density theorem that a positive proportion of the primes up to X^{δ_1} split completely in K, so that a reasonable choice for M will be proportional to $\pi(X^{\delta_1})$. Precisely, we suppose that there is a small fixed $\delta_2 > 0$ such that for every $X \geq 1$ and an appropriate choice of M with $X^{\delta_1}/\log X \ll M \ll X^{\delta_1}/\log X$ we have

$$\#\mathscr{B}_d(2X; X^{\delta_1}, M) \ll X^{1-\delta_2+\varepsilon}, \tag{2.3}$$

for all $\varepsilon > 0$. Then upon summing over $O(\log X)$ ranges and applying (2.1) and (2.3) within each range, we see that for any $X \geq 1$,

$$\begin{aligned}\sum_{0<D_K\leq X} |\mathrm{Cl}_K[\ell]| &\leq \sum_{0\leq j\leq \lceil \log_2 X\rceil} \sum_{2^{j-1}<D_K\leq 2^j} |\mathrm{Cl}_K[\ell]| \\ &\ll \sum_{0\leq j\leq \lceil \log_2 X\rceil} \left\{ (2^{j-1})^{3/2+\varepsilon} (2^{(j-1)\delta_1})^{-1} \log 2^j + \#\mathscr{B}_d(2^j; 2^{(j-1)\delta_1}, M)(2^{j-1})^{1/2+\varepsilon} \right\} \\ &\ll \log X \sum_{0\leq j\leq \lceil \log_2 X\rceil} \left\{ (2^j)^{3/2-\delta_1+\varepsilon} + (2^j)^{3/2-\delta_2+2\varepsilon} \right\} \ll X^{3/2-\delta+3\varepsilon}, \qquad (2.4)\end{aligned}$$

where $\delta = \min\{\delta_1, \delta_2\}$ and $\varepsilon > 0$ is arbitrarily small. Thus we see that an upper bound of the form (2.3) is the key to obtaining an average result in the shape of Corollaries 1.1.1 and 1.1.2; this upper bound plays a similarly crucial role in obtaining the results of Theorem 1.1, as we show in Section 7.

Ultimately, we will prove the following version of (2.3), which controls the number of possible bad fields:

Theorem 2.1. *Let $\mathscr{B}_d(X;Y,M)$ be defined as in (2.2). Set*

$$\delta_0(d) = \begin{cases} 1/6 & \text{if } d=2 \\ 2/25 & \text{if } d=3 \\ 1/48 & \text{if } d=4 \\ 1/200 & \text{if } d=5. \end{cases} \tag{2.5}$$

For each $d=2,3,4,5$, there is a constant $0<c_0(d)<1$ such that for every $0<\delta\le\delta_0(d)$ and every $X\ge 1$,

$$\#\mathscr{B}_d(X;(X/2)^\delta, \frac{1}{2}c_0(d)\frac{(X/2)^\delta}{\log(X/2)^\delta}) \ll X^{1-\delta+\varepsilon}$$

for every $\varepsilon>0$.

Remark 2.1. The methods of this paper also prove an analogous theorem if the condition "split completely" in the definition (2.2) is replaced by another fixed splitting type.

2.2. **Counting bad fields via a sieve and counts for fields with local conditions.** We prove Theorem 2.1 via a sieve we develop for this purpose; to describe the strategy, we first recall the simplest classical setting of a sieve. Let $\mathscr{A}$ be a finite set of elements of cardinality N, and let $\mathscr{P}$ denote the set of all rational primes. We assume a certain property of interest has been specified so that each element $a\in\mathscr{A}$ either satisfies it or not, with respect to p, for each $p\in\mathscr{P}$. For each prime $p\in\mathscr{P}$ we let $\mathscr{A}_p$ denote the finite subset of $\mathscr{A}$ that satisfies the fixed property with respect to the prime p. Moreover we assume we know that for each p there exists a real number $0\le\delta_p<1$ and a real number R_p with $|R_p|\le N$ such that

$$\#\mathscr{A}_p = \delta_p N + R_p. \tag{2.6}$$

In simplest terms, a classical aim of a sieve is to provide an upper bound for the number of elements in the set $\mathscr{A}$ such that the designated property fails for all primes $p\le z$, for some fixed threshold z. Thus one could use a sieve to provide an upper bound for

$$\#(\mathscr{A}\setminus\bigcup_{p\le z}\mathscr{A}_p).$$

For example, to sieve for prime numbers, the set $\mathscr{A}$ is a finite set of integers, and the property is that $p|a$. Slightly more generally, one could apply a classical sieve such as the Turán sieve to count

$$\#(\mathscr{A}\setminus\bigcup_{p\in P_0}\mathscr{A}_p) \tag{2.7}$$

for an arbitrary fixed finite set of primes P_0.

In our application, the set $\mathscr{A}$ is the set of fields $K/\mathbb{Q}$ of degree d with $D_K\in(0,X]$ and the property is that p splits completely in K, so that $\mathscr{A}_p$ is the subset of fields in which the prime p splits completely. In this setting, assuming we possess an appropriate understanding of $\#\mathscr{A}_p$ as in (2.6), then (2.7) would allow us to count those degree d fields K with $D_K\in(0,X]$ in which a *fixed* set of primes fail to split completely. But in order to bound the bad set $\mathscr{B}_d(X;X^{\delta_1},M)$ we require more flexibility: a field belongs to this set if all the primes in a sufficiently large set fail to split completely in K, but the relevant large set of primes might be different for two different bad fields K. Thus we develop in Section 3 a flexible new sieve that allows us to count elements $a\in\mathscr{A}$ that fail to lie in $\mathscr{A}_p$ for many p, without specifying which p fail for any given a.

The key input to any sieve is an understanding of $\mathscr{A}_p$ that provides the expression (2.6). In our case, this requires an understanding of $N_d(X)$, $N_d(X;p)$, and $N_d(X;pq)$ for two distinct primes p,q; here $N_d(X;pq)$ counts the number of degree d fields $K/\mathbb{Q}$ in which both p and q split completely. In the case of quartic fields, we let $\tilde{N}_4(X)$, $\tilde{N}_4(X;p)$ and $\tilde{N}_4(X;pq)$ denote the analogous quantities, restricted to non-D_4-quartic fields $K/\mathbb{Q}$.

We now summarize the key results we will require for the sieve. For quadratic fields, we record:

Lemma 2.2. *There exists a constant $c_2 > 0$, such that for $e = e_1$ or $e = e_1e_2$ for distinct primes e_1, e_2,*

$$N_2(X) = c_2X + O(X^{1/2}) \tag{2.8}$$

$$N_2(X;e) = \delta_e c_2 X + O(eX^{1/2}) \tag{2.9}$$

where δ_e is a multiplicative function defined for any prime e by

$$\delta_e = \frac{1}{2}\frac{1}{(1+e^{-1})}. \tag{2.10}$$

For completeness, we record a simple proof of this classical result in an appendix (Section 8); the error terms given here can be improved (see for example the survey [Pap05]) but will suffice for our application.

In contrast, the results for cubic, quartic, and quintic fields are deep. For cubic fields, we cite work of Taniguchi and Thorne [TT13]:

Theorem C (Theorems 1.1, 1.3 [TT13])**.** *There exist constants $c_3 > 0$, $c_3' < 0$ such that for $e = e_1$ or $e = e_1e_2$ for distinct primes e_1, e_2,*

$$N_3(X) = c_3X + c_3'X^{5/6} + O(X^{7/9+\varepsilon}) \tag{2.11}$$

$$N_3(X;e) = \delta_e c_3 X + \delta_e' c_3' X^{5/6} + O(e^{8/9}X^{7/9+\varepsilon}) \tag{2.12}$$

where δ_e and δ_e' are multiplicative functions defined for any prime e by

$$\delta_e = \frac{1}{6}\frac{1}{(1+e^{-1}+e^{-2})}, \qquad \delta_e' = \frac{1}{6} + O(e^{-1/3}). \tag{2.13}$$

For quartic fields, we have:

Theorem 2.3. *There exists a constant $c_4 > 0$ such that for $e = e_1$ or $e = e_1e_2$ for distinct primes e_1, e_2,*

$$\tilde{N}_4(X) = c_4X + O(X^{23/24+\varepsilon}) \tag{2.14}$$

$$\tilde{N}_4(X;e) = \delta_e c_4 X + O(e^{1/2+\varepsilon}X^{23/24+\varepsilon}) \tag{2.15}$$

where δ_e is a multiplicative function defined for any prime e by

$$\delta_e = \frac{1}{24}\frac{1}{(1+e^{-1}+2e^{-2}+e^{-3})}. \tag{2.16}$$

We note (2.14) is due to [BBP10, Theorem 1.3]; we deduce (2.15) in Section 4, using the methods of Belabas, Bhargava, and Pomerance [BBP10], which build on the work of Bhargava [Bha05] that obtained the original count of S_4-quartic fields with an $o(X)$ error term. See Theorem 4.1 for our most general result of this type, of which Theorem 2.3 is a special case.

For quintic fields, we have:

Theorem 2.4. *There exists a constant $c_5 > 0$ such that for $e = e_1$ or $e = e_1e_2$ for distinct primes e_1, e_2,*

$$N_5(X) = c_5X + O(X^{199/200+\varepsilon}) \tag{2.17}$$

$$N_5(X;e) = \delta_e c_5 X + O(e^{1/2+\varepsilon}X^{79/80+\varepsilon} + X^{199/200+\varepsilon}) \tag{2.18}$$

where δ_e is a multiplicative function defined for any prime e by

$$\delta_e = \frac{1}{120}\frac{1}{(1+e^{-1}+2e^{-2}+2e^{-3}+e^{-4})}. \tag{2.19}$$

We note (2.17) is due to [ST14]; we deduce (2.18) in Section 5, using the methods of Shankar and Tsimerman [ST14], which build on the work of Bhargava [Bha10] that obtained the original count of S_5-quintic fields with an $o(X)$ error term. (We also fill in a missing step from [ST14].) See Theorem 5.1 for our most general result, of which Theorem 2.4 is a special case.

We remark that the techniques for counting number fields that produced these results for $N_d(X;e)$ continue to be refined, and we may expect that the error terms will continue to be reduced. Thus in our subsequent computations involving $N_d(X;e)$ we have worked more generally with error terms of the form $O(e^\sigma X^\tau)$, so that it will be immediately clear how improvements in counting fields will lead to refinements of our results. (In particular, improved error terms for *smoothed* versions of the counting functions $N_d(X;e)$ would suffice for our application.) We note that the mechanism we employ will apply equally well to higher degree

extensions of $\mathbb{Q}$ (or extensions of a fixed number field, using the more general form of Theorem A available in [EV07, Lemma 2.3]) if suitable results for $N_d(X)$ and $N_d(X;e)$ (or their analogues for extensions of a fixed number field) become available. In addition, one might consider other families of fields for which precise asymptotics are known, such as abelian fields over $\mathbb{Q}$ with a fixed Galois group, ordered either by discriminant [Wri89, FLN15] or by conductor [Woo10]. It would be an interesting question to see whether the existing methods can be refined to produce an appropriate power-saving error term with sufficiently explicit dependence on a finite number of local conditions.

3. The Chebyshev sieve

We now develop in a fully general setting a new sieve that allows us to give an upper bound for the number of elements a belonging to a set $\mathscr{A}$ that satisfy a desired property with respect to p for "few" p (without specifying for which p it is satisfied). We will see that the principal idea is probabilistic, relating to Chebyshev's inequality, thus we dub it the Chebyshev sieve.

As before, let $\mathscr{A}$ be a finite set of cardinality N, let $\mathscr{P}$ denote the set of all rational primes, and let $\mathscr{A}_p$ denote the finite subset of $\mathscr{A}$ that satisfies the fixed property with respect to the prime p. For a fixed real parameter $z \geq 1$, we let

$$P(z) = \prod_{\substack{p \in \mathscr{P} \\ p \leq z}} p$$

and we define for each $a \in \mathscr{A}$ the quantity

$$N(a) = \#\{p | P(z) : a \in \mathscr{A}_p\}.$$

Next, we set

$$M(z) = \frac{1}{N} \sum_{a \in \mathscr{A}} N(a) = \frac{1}{N} \sum_{p | P(z)} \#\mathscr{A}_p \tag{3.1}$$

to be the mean number of sets $\mathscr{A}_p$ (with $p \leq z$) to which a typical element $a \in \mathscr{A}$ belongs. (In non-vacuous cases, $M(z)$ is nonzero.) We would expect that a typical element $a \in \mathscr{A}$ has $N(a)$ being about size $M(z)$, and we want to bound from above the number of $a \in \mathscr{A}$ which have $N(a)$ being unusually small, that is, less than a fixed small proportion of $M(z)$.

Given $1 \leq M \leq z$, we define $\mathscr{E}(\mathscr{A}; z, M)$ to be the set of elements $a \in \mathscr{A}$ such that at most M primes $p | P(z)$ have $a \in \mathscr{A}_p$. (Or in other words, $\mathscr{E}(\mathscr{A}; z, M)$ is the set of elements $a \in \mathscr{A}$ such that $N(a) \leq M$.) Then we set

$$E(\mathscr{A}; z, M) = \#\mathscr{E}(\mathscr{A}; z, M).$$

Our sieve lemma will provide us with an upper bound for $E(\mathscr{A}; z, \frac{1}{2}M(z))$; that is, the number of elements in $\mathscr{A}$ that lie in $\mathscr{A}_p$ for fewer than half the mean number of p.

For the purposes of the lemma, we introduce the following notation. Given distinct primes p, q we let $\mathscr{A}_{pq} = \mathscr{A}_p \cap \mathscr{A}_q$, and let $R_{p,q}$ denote the quantity such that

$$\#\mathscr{A}_{pq} = \delta_p \delta_q N + R_{p,q}.$$

(For notational convenience, we will interpret $R_{p,p}$ as R_p.) Finally, we set

$$U(z) = \sum_{p | P(z)} \delta_p.$$

We now state the key sieve lemma.

Lemma 3.1 (Chebyshev Sieve)**.** *With the setting described above,*

$$E(\mathscr{A}; z, \frac{1}{2}M(z)) \leq \frac{4N}{M(z)^2} \left(U(z) + \frac{1}{N} \sum_{p,q | P(z)} |R_{p,q}| + \frac{2U(z)}{N} \sum_{p | P(z)} |R_p| + \left(\frac{1}{N} \sum_{p | P(z)} |R_p| \right)^2 \right).$$

3.1. **Proof of the sieve lemma.** We note that the sieve inequality we prove is related to the classical Turán sieve (see for example Theorem 4.1.1 of [CM06]), and can be seen as an application of Chebyshev's inequality

$$\mathbb{P}(|X-\mu| \geq \alpha) \leq \sigma^2/\alpha^2,$$

for X a random variable with mean μ and variance σ^2, applied to the random variable $N(a)$ when a is drawn uniformly from $\mathscr{A}$.

We prove the lemma directly. We begin by noting that

$$\frac{1}{N}E(\mathscr{A};z,\frac{1}{2}M(z))(\frac{1}{2}M(z))^2 \leq \frac{1}{N}\sum_{a\in\mathscr{E}(\mathscr{A};z,\frac{1}{2}M(z))}(N(a)-M(z))^2 \leq \frac{1}{N}\sum_{a\in\mathscr{A}}(N(a)-M(z))^2.$$

It then suffices to prove the variance term on the right-hand side satisfies

$$\frac{1}{N}\sum_{a\in\mathscr{A}}(N(a)-M(z))^2 \leq U(z)+\frac{1}{N}\sum_{p,q|P(z)}|R_{p,q}|+2U(z)\left(\frac{1}{N}\sum_{p|P(z)}|R_p|\right)+\left(\frac{1}{N}\sum_{p|P(z)}|R_p|\right)^2. \tag{3.2}$$

We first note from (3.1) that the mean satisfies

$$M(z)=\frac{1}{N}\sum_{p|P(z)}\#\mathscr{A}_p=\frac{1}{N}\sum_{p|P(z)}(\delta_p N+R_p)=U(z)+\frac{1}{N}\sum_{p|P(z)}R_p. \tag{3.3}$$

We now consider the left-hand side of (3.2), which we trivially expand as

$$\frac{1}{N}\sum_{a\in\mathscr{A}}N(a)^2-\frac{2}{N}\sum_{a\in\mathscr{A}}N(a)M(z)+M(z)^2=\frac{1}{N}\sum_{a\in\mathscr{A}}N(a)^2-M(z)^2. \tag{3.4}$$

The first term on the right-hand side of (3.4) is equal to

$$\begin{aligned}\frac{1}{N}\sum_{p,q|P(z)}\#(\mathscr{A}_p\cap\mathscr{A}_q) &= \frac{1}{N}\left(\sum_{p|P(z)}\delta_p N+\sum_{\substack{p,q|P(z)\\p\neq q}}\delta_p\delta_q N+\sum_{p,q|P(z)}R_{p,q}\right)\\ &= \sum_{p|P(z)}\delta_p+\left(\sum_{p|P(z)}\delta_p\right)^2-\sum_{p|P(z)}\delta_p^2+\frac{1}{N}\sum_{p,q|P(z)}R_{p,q}\\ &= \sum_{p|P(z)}\delta_p(1-\delta_p)+U(z)^2+\frac{1}{N}\sum_{p,q|P(z)}R_{p,q}.\end{aligned}$$

On the other hand, we may expand $M(z)^2$ via (3.3) and see that after cancellation of the $U(z)^2$ factor, the right-hand side of (3.4) is equal to

$$\sum_{p|P(z)}\delta_p(1-\delta_p)+\frac{1}{N}\sum_{p,q|P(z)}R_{p,q}-2U(z)\left(\frac{1}{N}\sum_{p|P(z)}R_p\right)-\left(\frac{1}{N}\sum_{p|P(z)}R_p\right)^2.$$

As R_p may be either positive or negative, we take absolute values; then using the fact that $\delta_p \leq 1$ we see the resulting inequality simplifies to (3.2), thus proving the lemma.

4. Asymptotic count of non-D_4-quartic fields

In this section we will prove the following, of which Theorem 2.3 is a special case.

Theorem 4.1. *Let P be a finite set of primes. For each prime $p \in P$ we choose a splitting type at p and assign a corresponding density as follows:*

$$\delta_p := \frac{1}{24}(1 + p^{-1} + 2p^{-2} + p^{-3})^{-1} \qquad \text{for } p = \wp_1\wp_2\wp_3\wp_4$$

$$\delta_p := \frac{1}{4}(1 + p^{-1} + 2p^{-2} + p^{-3})^{-1} \qquad \text{for } p = \wp_1\wp_2\wp_3$$

$$\delta_p := \frac{1}{3}(1 + p^{-1} + 2p^{-2} + p^{-3})^{-1} \qquad \text{for } p = \wp_1\wp_2 \text{ with } \wp_2 \text{ inertia degree 3}$$

$$\delta_p := \frac{1}{8}(1 + p^{-1} + 2p^{-2} + p^{-3})^{-1} \qquad \text{for } p = \wp_1\wp_2 \text{ with } \wp_i \text{ inertia degree 2}$$

$$\delta_p := \frac{1}{4}(1 + p^{-1} + 2p^{-2} + p^{-3})^{-1} \qquad \text{for } p = \wp_1$$

$$\delta_p := \frac{p^{-1} + 2p^{-2} + p^{-3}}{(1 + p^{-1} + 2p^{-2} + p^{-3})} \qquad \text{for } p \text{ ramified.}$$

Let $\delta_P := \prod_{p\in P} \delta_p$ and let $e = \prod_{p\in P} p$. Let $\tilde{N}_4(X; P)$ be the number of non-D_4 quartic fields with absolute discriminant at most X such that for each $p \in P$, the prime p splits in the quartic field in the splitting type chosen for p above. There exists a constant $c_4 > 0$ such that

$$\tilde{N}_4(X; P) \quad = \quad \delta_P c_4 X + O(e^{1/2+\varepsilon} X^{23/24+\varepsilon}), \tag{4.1}$$

where the implied constant in the O term is absolute (does not depend on P). Moreover, we may choose more than one splitting type at each prime and let δ_p be the sum of the corresponding densities and the result still holds.

Bhargava [Bha05] first determined the asymptotic count of non-D_4-quartic fields, and Belabas, Bhargava, and Pomerance [BBP10] gave a power-saving asymptotic for this count. We will follow the method of [BBP10], additionally requiring our chosen splitting types. While the main term for such a restricted count appears in [Bha05, Theorem 3] (at least for one prime, and the same argument would work for more primes), we require a power-saving error term *with explicit dependence* on the primes. In fact, such results have appeared at least four times recently, but we will improve upon the exponents in all of these results and remove various hypotheses that don't hold in the situation in which we need to apply the bound. Yang [Yan09, Proposition 3.1.7] proved such a power-saving error of the form $\tilde{N}_4(X; P) = \delta_P c_4 X + O(e^2 X^{143/144+\varepsilon})$. ([Yan09, Proposition 3.1.7] only states this for one local condition, but [CK15, Section 7] remarked it can be extended to finitely many local conditions.) Lemke Oliver and Thorne [OT14, Theorem 2.1] proved a power-saving error (in which we may only specify that p is ramified) of $\tilde{N}_4(X; P) = \delta_P c_4 X + O(e^{9/10} X^{239/240+\varepsilon})$. Shankar, Södergren, and Templier [SST15b] proved $\tilde{N}_4(X; P) = \delta_P c_4 X + O(e^{12} X^{23/24+\varepsilon})$ when P contains a single prime.

The exposition of the method in [Bha05] and [BBP10] is quite clear, so we will focus here on the particular aspects of the computation we need. Instead of directly counting quartic fields, the method, equivalently, counts maximal quartic orders. The parametrization of quartic rings with their cubic resolvents due to Bhargava [Bha04] (see also [BBP10, Theorem 4.1]) gives an injection from the set of isomorphism classes of maximal quartic orders to the set of $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ classes of pairs of ternary quadratic forms with integral coefficients. Pairs of integral ternary quadratic forms comprise a 12 dimensional lattice $V_\mathbb{Z} = \mathbb{Z}^{12}$. Counting $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ classes of lattice points in $\mathbb{Z}^{12}$ is the same as counting lattice points in a fundamental domain for $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ on $\mathbb{R}^{12}$. In this paper, we need to count only these lattice points in particular translates of sublattices of $\mathbb{Z}^{12}$. We collect some basic facts about the lattice translates corresponding to our desired fields, apply the geometry of numbers result from [BBP10] to count the necessary lattice points, and then work to minimize the resulting error terms.

As in [Bha05, Section 2.2] and [BBP10, Section 4] we use a certain random fundamental domain for the action of $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ on $\mathbb{R}^{12}$. For a positive integer m, let L be a translate $v + mV_\mathbb{Z}$ ($v \in V_\mathbb{Z}$) of the sublattice $mV_\mathbb{Z}$ of $V_\mathbb{Z}$. Let $N'(L; X)$ denote the expected number of lattice points in L, with first coordinate non-zero and discriminant less than X, in a random fundamental domain. (This notion of expected value for a random fundamental domain is defined as in [Bha05, Equation (5)], with S the set of points of L with first coordinate non-zero, but *without* the "abs. irr." condition that appears in [Bha05, Equation (5)]. See

also [BBP10, p. 198].) Let $N_{S_4}(q;X)$ be the number of classes in $V_{\mathbb{Z}}$ corresponding to isomorphism classes of S_4-quartic orders and whose index in their maximal order is divisible by q and whose discriminant is less than X. We have the following result that estimates these counts.

Theorem D (Theorem 4.11 of [BBP10]). *Let L be a translate $v + mV_{\mathbb{Z}}$ ($v \in V_{\mathbb{Z}}$). Let (a,b,c,d) denote the smallest positive first four coordinates of any element of L. Then*

$$N'(L,X) = \frac{N_{S_4}(1;X)}{m^{12}} + O(\sum_S \frac{X^{(|S|+\alpha_S+\beta_S+\gamma_S+\delta_S)/12}}{m^{|S|}a^{\alpha_S}b^{\beta_S}c^{\gamma_S}d^{\delta_S}} + \log X)$$

where S ranges over the non-empty proper subsets of the set of 12 coordinates 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 $|S| + \alpha_S + \beta_S + \gamma_S + \delta_S \leq 11$.

Let q be square-free and $(q,e) = 1$. First, we will assume that we have chosen unramified splitting types at each prime in P. Now, we will start by counting the expected number $N'(q,e;X)$ of lattice points in a random fundamental domain that satisfy the following conditions: (1) their first coordinate is non-zero, (2) their discriminant is less than X, (3) their corresponding quartic ring is not maximal at each prime dividing q and is maximal and of chosen splitting type at primes in P. We do this by summing Theorem D over the collection T of translates of $eq^2V_{\mathbb{Z}}$ that give quartic rings that are not maximal at each prime dividing q, and are maximal and with chosen local splitting at each $p \in P$. (See [Bha04, Section 4] for a description of which pairs of ternary quadratic forms correspond to quartic rings that are maximal or split in a certain way at a prime.)

Given $(a,b,c,d) \in [1,eq^2]^4$, we need to bound the number of translates in T that have (a,b,c,d) as the smallest positive first four coordinates of any element. By [BBP10, Corollary 4.8], there are $O(6^{\omega(q)}q^{14})$ translates of $q^2V_{\mathbb{Z}}$ that are congruent to (a,b,c,d) modulo q^2 and whose lattice points correspond to quartic rings that are not maximal at each prime dividing q. Since $V_{\mathbb{Z}}$ is 12 dimensional, there are e^8 translates of $eV_{\mathbb{Z}}$ congruent to (a,b,c,d) modulo e. Thus by the Chinese Remainder Theorem, there are $O(6^{\omega(q)}q^{14}e^8)$ translates in T that have (a,b,c,d) as the smallest positive first four coordinates of any element.

For q square-free, we define $\nu(q)$ to be the multiplicative function defined for a prime p by

$$\nu(p) := p^{-2} + 2p^{-3} + 2p^{-4} - 3p^{-5} - 4p^{-6} - p^{-7} + 3p^{-8} + 3p^{-9} - p^{-10} - p^{-11}.$$

This is the density of lattice points that correspond to quartic rings non-maximal at p [BBP10, Lemma 4.4]. Then $\#T = \nu(q)q^{24}e^{12}\Gamma_P$, where

$$\Gamma_P := \prod_{p \in P} \delta_p(1 - \nu(p)),$$

and $0 \leq \delta_p \leq 1$ is the density of lattice points corresponding to quartic rings that are split as we chose at p as a subset of those corresponding to quartic rings that are maximal at p [Bha04, Lemma 23].

If $q^2 > X$, then all the classes counted by $N'(q,e;X)$ have discriminant 0, and by [BBP10, Lemma 4.10], in this case there are $O(X^{11/12+\varepsilon})$ such classes.

So now we consider the case when $q^2 \leq X$, in which case by Theorem D,

$$\begin{aligned} &N'(q,e;X) \\ &\quad = \nu(q)\Gamma_P N_{S_4}(1;X) + O\left(\sum_{(a,b,c,d)\in[1,eq^2]^4} 6^{\omega(q)}q^{14}e^8\left(\sum_S \frac{X^{(|S|+\alpha_S+\beta_S+\gamma_S+\delta_S)/12}}{(eq^2)^{|S|}a^{\alpha_S}b^{\beta_S}c^{\gamma_S}d^{\delta_S}} + \log X\right)\right). \end{aligned}$$

We have

$$\begin{aligned}
&\sum_{(a,b,c,d)\in[1,eq^2]^4} 6^{\omega(q)}q^{14}e^8\left(\sum_S \frac{X^{(|S|+\alpha_S+\beta_S+\gamma_S+\delta_S)/12}}{(eq^2)^{|S|}a^{\alpha_S}b^{\beta_S}c^{\gamma_S}d^{\delta_S}} + \log X\right)\\
&= 6^{\omega(q)}q^{14}e^8\left(e^4q^8\log X + \sum_S \frac{X^{(|S|+\alpha_S+\beta_S+\gamma_S+\delta_S)/12}}{(eq^2)^{|S|}} \sum_{(a,b,c,d)\in[1,eq^2]^4} \frac{1}{a^{\alpha_S}b^{\beta_S}c^{\gamma_S}d^{\delta_S}}\right)\\
&\le 6^{\omega(q)}q^{14}e^8\left(e^4q^8\log X + \sum_S \frac{X^{(|S|+\alpha_S+\beta_S+\gamma_S+\delta_S)/12}}{(eq^2)^{|S|}} \left((eq^2)^{4-\alpha_S-\beta_S-\gamma_S-\delta_S}\log^4(eq^2)\right)\right)\\
&= 6^{\omega(q)}q^{22}e^{12}\left(\log X + \sum_S (X^{1/12}e^{-1}q^{-2})^{(|S|+\alpha_S+\beta_S+\gamma_S+\delta_S)}\log^4(eq^2)\right).
\end{aligned}$$

Since $0 \le |S| + \alpha_S + \beta_S + \gamma_S + \delta_S \le 11$, and recalling that $q^2 \le X$, the above is

$$\begin{aligned}
&= O\left(6^{\omega(q)}q^{22}e^{12}\left((X^{1/12}e^{-1}q^{-2})^{11}\log^4(eq^2) + \log^4(eq^2) + \log X\right)\right)\\
&= O\left(e^{1+\varepsilon}X^{11/12+\varepsilon} + q^{22}e^{12+\varepsilon}X^{\varepsilon}\right).
\end{aligned}$$

Let $N_{S_4}(q,e;X)$ be the number of classes in $V_{\mathbb{Z}}$, or equivalently lattice points in a fundamental domain, corresponding to isomorphism classes of S_4-quartic orders, whose index in their maximal order is divisible by q and whose discriminant is less than X, and that are maximal and of chosen splitting type at $p \in P$. Now, by inclusion-exclusion, as in the proof of [BBP10, Theorem 4.13], we have that the number of isomorphism classes of maximal S_4-quartic orders splitting as chosen for $p \in P$ and having (absolute) discriminant less than X is given by

$$\sum_{q\ge1}{}' \mu(q)N_{S_4}(q,e;X)$$

where the sum is restricted to square-free q that are relatively prime to e.

Now we compare $N_{S_4}(q,e;X)$ and $N'(q,e;X)$. Note that the difference is that $N'(q,e;X)$ excludes those lattice points with first coordinate 0, and $N_{S_4}(q,e;X)$ excludes those lattice points that do not correspond to orders in S_4-quartic fields. So by [BBP10, Lemmas 4.9 and 4.10], we have

$$|N_{S_4}(q,e;X) - N'(q,e;X)| = O(X^{11/12+\varepsilon}).$$

Thus by our previous computation for $N'(q,e;X)$,

$$N_{S_4}(q,e;X) = \nu(q)\Gamma_P N_{S_4}(1;X) + O\left(e^{1+\varepsilon}X^{11/12+\varepsilon} + q^{22}e^{12+\varepsilon}X^{\varepsilon}\right). \tag{4.2}$$

So for a fixed Q (to be chosen in terms of X, e later), we sum over square-free q with $(q,e)=1$ as in (4.2), obtaining

$$\begin{aligned}
\sum_{q\ge1}{}' \mu(q)N_{S_4}(q,e;X) &= \sum_{1\le q\le Q}{}' \mu(q)N_{S_4}(q,e;X) + \sum_{q>Q}{}' \mu(q)N_{S_4}(q,e;X)\\
&= \sum_{1\le q\le Q}{}' \mu(q)\nu(q)\Gamma_P N_{S_4}(1;X) + O(E_1) + O(E_2)\\
&= \sum_{q\ge1}{}' \mu(q)\nu(q)\Gamma_P N_{S_4}(1;X) + O(E_1) + O(E_2) + O(E_3)\\
&= \prod_p(1-\nu(p)) \prod_{p\in P}\delta_p N_{S_4}(1;X) + O(E_1) + O(E_2) + O(E_3)
\end{aligned}$$

where

$$E_1 = \sum_{1\le q\le Q}{}' \left(e^{1+\varepsilon}X^{11/12+\varepsilon} + q^{22}e^{12+\varepsilon}X^{\varepsilon}\right)$$
$$E_2 = \sum_{q>Q}{}' \mu(q)N_{S_4}(q,e;X)$$
$$E_3 = \sum_{q>Q}{}' \nu(q)\Gamma_P N_{S_4}(1;X).$$

(Note that we handle the terms slightly differently than in [BBP10], so that E_3 above does not correspond to their E_3 term.)

We have $E_1 = O(e^{1+\varepsilon}QX^{11/12+\varepsilon} + Q^{23}e^{12+\varepsilon}X^{\varepsilon})$. By [BBP10, Lemma 4.3], we have $N_{S_4}(q,e;X) = O(Xq^{-2+\varepsilon})$, and so $E_2 = O(XQ^{-1+\varepsilon})$. We have $E_3 = O(Q^{-1+\varepsilon}X)$, since by [BBP10, Lemma 4.2], we have $N_{S_4}(1;X) = O(X)$, and by definition $\nu(q) = O(q^{-2+\varepsilon})$.

If $e \le X^{1/12}$, then we take $Q = X^{1/24}e^{-1/2}$, and we have

$$\sum_{q\ge 1}{}' \mu(q)N_{S_4}(q,e;X) = \prod_p(1-\nu(p)) \prod_{p\in P}\delta_p N_{S_4}(1;X) + O(e^{1/2+\varepsilon}X^{23/24+\varepsilon}).$$

By [BBP10, Lemma 4.2], we have that

$$\prod_p(1-\nu(p))N_{S_4}(1;X) = c_4X + O(X^{23/24+\varepsilon}),$$

for some positive constant c_4. Thus we conclude that the number of isomorphism classes of maximal S_4-quartic orders with our chosen splitting types at $p \in P$ and having (absolute) discriminant less than X is

$$\delta_P c_4 X + O(e^{1/2+\varepsilon}X^{23/24+\varepsilon}).$$

If $e > X^{1/12}$, then the number of isomorphism classes of maximal S_4-quartic orders with chosen splitting types for $p \in P$ and having (absolute) discriminant less than X is $O(X)$ by [BBP10, Lemma 4.2], which we may then also write as

$$\delta_P c_4 X + O(e^{1/2+\varepsilon}X^{23/24+\varepsilon}).$$

There are at most $O(X^{7/8+\varepsilon})$ quartic extensions with $D_K < X$ with Galois closure having Galois group C_4, K_4 or A_4 (Baily [Bai80], and Wong [Won99a]). So we can conclude Theorem 4.1 holds for unramified splitting types. This argument shows we can also choose more than one splitting type at each p, and sum the corresponding densities.

Now, given P and choices for local splitting types some of which may be ramified, let P_1 be the subset of P for which we choose only unramified splitting types. We can find $\tilde{N}_4(X;P_1)$ using the result already proven. For any subset $P_2 \subset P \setminus P_1$, write $\tilde{N}_4(X;P_1 \cup \bar{P_2})$ for the number of non-D_4 quartic fields with absolute discriminant at most X such that for each $p \in P_1$ the prime p splits in one of our chosen spitting type, and for each $p \in P_2$ the prime p *does not* split in one of our chosen splitting types. We can also apply the result already proven to find $\tilde{N}_4(X;P_1 \cup \bar{P_2})$. Then using inclusion exclusion, we have

$$\begin{aligned}\tilde{N}_4(X;P) &= \sum_{P_2\subset P\setminus P_1}(-1)^{|P_2|}\tilde{N}_4(X;P_1\cup\bar{P_2}) \\ &= \delta_P c_4 X + \sum_{P_2\subset P\setminus P_1}(-1)^{|P_2|}O(e^{1/2+\varepsilon}X^{23/24+\varepsilon}).\end{aligned}$$

Since each set P_2 corresponds to a distinct divisor of e there are $O(e^{\varepsilon})$ terms in the sum and Theorem 4.1 follows.

Remark 4.1. On the other hand, the number of D_4-quartic fields with $D_K < X$ is $\sim cX$ with $c \approx 0.052326...$, as initially indicated (as an order of magnitude) by Baily [Bai80] and refined with an explicit constant by Cohen, Diaz y Diaz and Olivier [CDyDO02]. It is an interesting open problem to count D_4 fields with local conditions such as certain primes being split completely, and for now we exclude them from our consideration.

5. Asymptotic count of quintic fields

In this section we will prove the following, of which Theorem 2.4 is a special case.

Theorem 5.1. *Let P be a finite set of primes. For each prime $p \in P$ we choose a splitting type at p and assign a corresponding density as follows:*

$$\begin{aligned}
\delta_p &:= \frac{1}{120}(1+p^{-1}+2p^{-2}+2p^{-3}+p^{-4})^{-1} && \text{for } p = \wp_1\wp_2\wp_3\wp_4\wp_5\\
\delta_p &:= \frac{1}{12}(1+p^{-1}+2p^{-2}+2p^{-3}+p^{-4})^{-1} && \text{for } p = \wp_1\wp_2\wp_3\wp_4\\
\delta_p &:= \frac{1}{8}(1+p^{-1}+2p^{-2}+2p^{-3}+p^{-4})^{-1} && \text{for } p = \wp_1\wp_2\wp_3 \text{ with } \wp_2, \wp_3 \text{ inertia degree 2}\\
\delta_p &:= \frac{1}{6}(1+p^{-1}+2p^{-2}+2p^{-3}+p^{-4})^{-1} && \text{for } p = \wp_1\wp_2\wp_3 \text{ with } \wp_3 \text{ inertia degree 3}\\
\delta_p &:= \frac{1}{6}(1+p^{-1}+2p^{-2}+2p^{-3}+p^{-4})^{-1} && \text{for } p = \wp_1\wp_2 \text{ with } \wp_2 \text{ inertia degree 3}\\
\delta_p &:= \frac{1}{4}(1+p^{-1}+2p^{-2}+2p^{-3}+p^{-4})^{-1} && \text{for } p = \wp_1\wp_2 \text{ with } \wp_2 \text{ inertia degree 4}\\
\delta_p &:= \frac{1}{5}(1+p^{-1}+2p^{-2}+2p^{-3}+p^{-4})^{-1} && \text{for } p = \wp_1\\
\delta_p &:= \frac{p^{-1}+2p^{-2}+2p^{-3}+p^{-4}}{(1+p^{-1}+2p^{-2}+2p^{-3}+p^{-4})} && \text{for } p \text{ ramified.}
\end{aligned}$$

Let $\delta_P := \prod_{p\in P}\delta_p$ and let $e = \prod_{p\in P} p$. Let $N_5(X;P)$ be the number of quintic fields with absolute discriminant at most X such that for each $p \in P$, the prime p splits in the quartic field in the splitting type chosen for p above. There exists a constant $c_5 > 0$ such that

$$N_5(X;P) \quad = \quad \delta_P c_5 X + O(e^{1/2+\varepsilon}X^{79/80+\varepsilon} + X^{199/200+\varepsilon}), \tag{5.1}$$

where the implied constant in the O term is absolute (does not depend on P). Moreover, we may choose more than one splitting type at each prime and let δ_p be the sum of the corresponding densities and the result still holds.

Bhargava [Bha10] gave the first asymptotic count of quintic number fields, and Shankar and Tsimerman [ST14], building on Bhargava's work, gave the first power-saving error term. Both proofs fundamentally rely on Bhargava's [Bha08] parametrization of quintic rings. We will follow the outline of the argument of [ST14], additionally requiring our chosen splitting conditions. While the main term for such a restricted count appears in [Bha10, Theorem 3] (at least for one prime, and the same argument would work for more primes), we require a power-saving error term *with explicit dependence* on the primes. While such bounds have appeared in at least three recent papers, we will improve on the exponents in all of them, as well as remove hypotheses that do not hold in our cases of interest. Lemke Oliver and Thorne [OT14, Theorem 2.1] have shown, assuming that we choose ramification at each prime $p \in P$, that $N_5(X;P) = \delta_P c_5 X + O(eX^{199/200+\varepsilon})$. Cho and Kim [CK15, Section 6] have recently proven a bound of the sort we desire; it seems they show $N_5(X;P) = \delta_P c_5 X + O(e^{2-\varepsilon}X^{399/400+\varepsilon})$. Also, Shankar, Södergren, and Templier [SST15b] stated the bound $N_5(X;P) = \delta_P c_5 X + O(e^{40}X^{79/80+\varepsilon} + X^{199/200+\varepsilon})$ when P contains a single prime.

Instead of directly counting quintic fields, the method, equivalently, counts maximal quintic orders. Analogously to the quartic case, we use a parametrization of quintic rings with their sextic resolvents due to Bhargava [Bha08]. Let $V_{\mathbb{Z}} = \mathbb{Z}^{40}$ denote the space of quadruples of 5×5 skew-symmetric matrices with integer coefficients. Then quintic rings with their sextic resolvents are parametrized by $\mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$ orbits on $V_{\mathbb{Z}}$ [Bha08, Theorem 1]. These orbits correspond to lattice points in a fundamental domain for $\mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$ on $\mathbb{R}^{40}$. As in [Bha10, Section 2.2] and [ST14, Section 2.2], we take a certain random fundamental domain for the action of $\mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$ on $\mathbb{R}^{40}$. For a subset $S \subset V_{\mathbb{Z}}$, let $N_{\mathrm{dom}}(S;X)$ denote the expected number of elements of S with absolute discriminant less than X and whose associated quintic ring is an integral domain (i.e. is an order in a quintic field), in a random fundamental domain (as in [ST14, Equation (1)], summed over the implicit i there). Let $N^*(S;X)$ denote the expected number of elements of

S with absolute discriminant less than X, in a random fundamental domain (as in the equation after (1) in [ST14], summed over the implicit i there).

We first consider the case in which only unramified splitting types are chosen. Let a_{12} denote the $(1,2)$ coordinate of the first matrix in a quadruple of 5×5 skew-symmetric matrices. For a square-free integer q relatively prime to e, let $W_{q,e} \subset V_{\mathbb{Z}}$ denote the set of elements corresponding to quintic rings that are not maximal at each prime dividing q and are maximal and of chosen splitting type at primes dividing e. Recall from [Bha08, Section 12] that $W_{q,e}$ is defined by congruence conditions modulo q^2e (for maximality, an argument analogous to that in [Bha04, Lemma 22] is necessary). Let $U_e \subset V_{\mathbb{Z}}$ denote the set of elements corresponding to quintic rings that are maximal at all primes and of chosen splitting type at the primes dividing e. Then counting $N_{\mathrm{dom}}(U_e; X)$ will provide us with precisely the count $N_5(X; e)$ we require. We will count lattice points in U_e by using inclusion-exclusion to reduce to counting lattice points in the $W_{q,e}$.

By [Bha10, Equation (27)] (see also [ST14, Equation (4)]), if L is a translate of the lattice $mV_{\mathbb{Z}}$ and $m = O(X^{1/40})$, then

$$N^*(L \cap \{a_{12} \neq 0\}; X) = c_0 m^{-40} X + O(m^{-39} X^{39/40}), \tag{5.2}$$

for some positive absolute constant c_0.

Bhargava gives the density of lattice points corresponding to rings maximal at a given prime [Bha08, Equation (48)] and the density of lattice points corresponding to rings maximal and of each splitting type [Bha08, Lemma 20]. Using these two computed densities, we conclude that of the $(q^2e)^{40}$ quadruples of 5×5 skew-symmetric matrices mod q^2e, we have that $W_{q,e}$ corresponds to $\nu(q) q^{80} \delta_P e^{40} \prod_{p \in P} (1 - \nu(p))$ of them, where

$$\nu(p) = 1 - \frac{(p-1)^8 p^{12} (p+1)^4 (p^2+1)^2 (p^2+p+1)^2 (p^4+p^3+p^2+p+1)(p^4+p^3+2p^2+2p+1)}{p^{40}},$$

and we extend this to a multiplicative function $\nu(q)$ for square-free q. (Here, $\nu(p)$ is the density of lattice points correspond to rings that are *non-maximal* at p from [Bha08, Equation (48)].) Note that $\nu(p) = p^{-2} + O(p^{-3})$ and thus $\nu(q) = O(q^{-2+\varepsilon})$.

We have that $\delta_P \leq 1$ and $1 - \nu(p) \leq 1$. So, when $q^2 e = O(X^{1/40})$, by summing Equation (5.2) over all the translates of $q^2 e V_{\mathbb{Z}}$ that comprise $W_{q,e}$, we find that

$$\begin{aligned} &N^*(W_{q,e} \cap \{a_{12} \neq 0\}; X) \\ &= \nu(q) q^{80} \delta_P e^{40} \prod_{p \in P} (1 - \nu(P)) c_0 q^{-80} e^{-40} X + O(\nu(q) q^{80} \delta_P e^{40} \prod_{p \in P} (1 - \nu(p)) q^{-78} e^{-39} X^{39/40}) \\ &= \nu(q) \delta_P \prod_{p \in P} (1 - \nu(p)) c_0 X + O(\nu(q) q^2 \delta_P e \prod_{p \in P} (1 - \nu(p)) X^{39/40}) \\ &= \nu(q) \delta_P \prod_{p \in P} (1 - \nu(p)) c_0 X + O(q^{\varepsilon} e X^{39/40}), \end{aligned} \tag{5.3}$$

where in the last identity we have used the fact that $\nu(q) = O(q^{-2+\varepsilon})$.

We then, by inclusion-exclusion as in [ST14, Section 4], have for an appropriate Q (to be chosen later in terms of X),

$$\begin{aligned}
N_{\mathrm{dom}}(U_e \cap \{a_{12} \neq 0\}; X) &= \sum_{q\geq 1}{}' \mu(q) N_{\mathrm{dom}}(W_{q,e} \cap \{a_{12} \neq 0\}; X) \\
&= \sum_{1\leq q\leq Q}{}' \mu(q) N_{\mathrm{dom}}(W_{q,e} \cap \{a_{12} \neq 0\}; X) \\
&\quad + \sum_{q>Q}{}' \mu(q) N_{\mathrm{dom}}(W_{q,e} \cap \{a_{12} \neq 0\}; X) \\
&= \sum_{1\leq q\leq Q}{}' \mu(q) N^*(W_{q,e} \cap \{a_{12} \neq 0\}; X) \\
&\quad + \sum_{1\leq q\leq Q}{}' \mu(q) \left(N_{\mathrm{dom}}(W_{q,e} \cap \{a_{12} \neq 0\}; X) - N^*(W_{q,e} \cap \{a_{12} \neq 0\}; X)\right) \\
&\quad + \sum_{q>Q}{}' \mu(q) N_{\mathrm{dom}}(W_{q,e} \cap \{a_{12} \neq 0\}; X),
\end{aligned}$$

where the sums are over square-free q relatively prime to e.

By [ST14, Lemma 3], we have $N_{\mathrm{dom}}(W_{q,e}; X) = O(q^{-2+\varepsilon}X)$ and we use this for the sum for $q > Q$. We will use Equation (5.3) for the first $1 \leq q \leq Q$ sum. For the second $1 \leq q \leq Q$ sum, note that each lattice point corresponding to a non-domain of discriminant D is counted with coefficient $-\sum_{1\leq q\leq Q, q|D} \mu(q)$, which is $O(D^{\varepsilon}) = O(X^{\varepsilon})$, and by [ST14, Equation (8)] there are at most $O(X^{199/200+\varepsilon})$ lattice points corresponding to non-domains. (This step, or something similar, should be added to the proof in [ST14].)

As a result, as long as $Q = O(X^{1/80}e^{-1/2})$,

$$N_{\mathrm{dom}}(U_e \cap \{a_{12} \neq 0\}; X) = \sum_{q\geq 1}{}' \mu(q)\nu(q)\delta_P \prod_{p\in P}(1-\nu(p))c_0 X + O(E_1) + O(E_2) + O(E_3),$$

where

$$\begin{aligned}
E_1 &= \sum_{1\leq q\leq Q} O(q^{\varepsilon} e X^{39/40}) \\
E_2 &= O(X^{199/200+\varepsilon}) \\
E_3 &= \sum_{q>Q} q^{-2+\varepsilon} X \\
E_4 &= \sum_{q>Q} \mu(q)\nu(q)\delta_P \prod_{p\in P}(1-\nu(p))c_0 X.
\end{aligned}$$

These terms trivially admit the estimates

$$\begin{aligned}
E_1 &= O(Q^{1+\varepsilon} e X^{39/40}) \\
E_2 &= O(X^{199/200+\varepsilon}) \\
E_3 &= O(Q^{-1+\varepsilon} X) \\
E_4 &= O(Q^{-1+\varepsilon} X),
\end{aligned}$$

where in the last estimate we have used the fact that $\nu(q) = O(q^{-2+\varepsilon})$.

We take $Q = X^{1/80}e^{-1/2}$, and have

$$\begin{aligned}
N_{\mathrm{dom}}(U_e \cap \{a_{12} \neq 0\}; X) &= \sum_{q\geq 1}{}' \mu(q)\nu(q)\delta_P \prod_{p\in P}(1-\nu(p))c_0 X + O(e^{1/2}X^{79/80+\varepsilon} + X^{199/200+\varepsilon}) \\
&= \prod_{p}(1-\nu(p))\delta_P c_0 X + O(e^{1/2}X^{79/80+\varepsilon} + X^{199/200+\varepsilon}).
\end{aligned}$$

From [Bha10, Lemma 11], we have that $N_{\mathrm{dom}}(\{a_{12}=0\};X)=O(X^{39/40})$, and so

$$N_{\mathrm{dom}}(U_e\cap\{a_{12}=0\};X)=O(X^{39/40}).$$

It follows that

$$N_5(X;P)=N_{\mathrm{dom}}(U_e;X)=\prod_p(1-\nu(p))\delta_P c_0X+O(e^{1/2}X^{79/80+\varepsilon}+X^{199/200+\varepsilon})$$

We thus conclude Theorem 5.1 holds with, $c_5=\prod_p(1-\nu(p))c_0$ when we only choose unramified splitting types. As at the end of Theorem 4.1, we can apply the result we have just proven and inclusion-exclusion to prove Theorem 5.1 in general.

6. Application of the sieve

6.1. **Summary of the asymptotic inputs to the sieve.** We now turn to the application of the sieve lemma to degree d field extensions of $\mathbb{Q}$. Note that when applying the sieve, it is crucial to have error terms with explicit dependence on local conditions (such as we have derived in Theorems 2.3 and 2.4): without such an explicit dependence, we would not have quantitative control of the right-hand side of the key sieve inequality in Lemma 3.1, since we would not have an explicit bound for R_p in terms of p.

Let $\mathscr{A}$ and $\mathscr{A}_p$ (for each rational prime p) be the sets so that $\#\mathscr{A}=N_d(X)$ and $\#\mathscr{A}_p=N_d(X;p)$ (or $\tilde{N}_4(X)$, $\tilde{N}_4(X;p)$ in the case of $d=4$). With these definitions, the quantity $E(\mathscr{A};z,\frac{1}{2}M(z))$ treated in the sieve (Lemma 3.1), which we will now denote by $E_d(\mathscr{A};z,\frac{1}{2}M(z))$, is the number of degree d extensions K of $\mathbb{Q}$ with $0<D_K\le X$ (up to isomorphism, and non-D_4 when $d=4$) such that there are at most $\frac{1}{2}M(z)$ primes $p\le z$ that split completely in K.

We recall the collection $\mathscr{B}_d(X;Y,M)$ of bad fields, as defined in (2.2). We will think of $Y=z=(X/2)^{\delta_0}$ for $\delta_0>0$ to be chosen precisely later, and define $M(z)$ as in (3.1). In particular, the set of bad fields satisfies

$$\#\mathscr{B}_d(X;(X/2)^{\delta_0},\frac{1}{2}M((X/2)^{\delta_0}))=E_d(\mathscr{A};(X/2)^{\delta_0},\frac{1}{2}M((X/2)^{\delta_0})).$$

We will need to apply the sieve separately to fields of each degree, since in several cases the count for $N_d(X;p)$ takes a somewhat different form, but in an effort to unify the presentation, we re-state the asymptotics we will assume in more general form. We write the results of Lemma 2.2, Theorem C, Theorems 2.3 and 2.4 as follows.

Quadratic fields: for δ_e as in (2.10), there is some $\sigma_2>0$ and $0<\tau_2\le 1/2$ such that

$$\begin{aligned}N_2(X)&=c_2X+O(X^{\tau_2+\varepsilon})\\ N_2(X;e)&=\delta_e c_2X+O(e^{\sigma_2}X^{\tau_2+\varepsilon}).\end{aligned}$$

Cubic fields: for δ_e,δ_e' as in (2.13), there is some $\sigma_3>0$ and $0<\tau_3<5/6$ such that

$$\begin{aligned}N_3(X)&=c_3X+c_3'X^{5/6}+O(X^{\tau_3+\varepsilon})\\ N_3(X;e)&=\delta_e c_3X+\delta_e'c_3'X^{5/6}+O(e^{\sigma_3}X^{\tau_3+\varepsilon}).\end{aligned}$$

Non-D_4-quartic fields: for δ_e as in (2.16), there is some $\sigma_4>0$ and $0<\tau_4<1$ such that

$$\begin{aligned}\tilde{N}_4(X)&=c_4X+O(X^{\tau_4+\varepsilon})\\ \tilde{N}_4(X;e)&=\delta_e c_4X+O(e^{\sigma_4}X^{\tau_4+\varepsilon}).\end{aligned}$$

Quintic fields: for δ_e as in (2.19), there is some $\sigma_5>0$ and $0<\tau_5<1$ as well as some $0<\gamma<1$ such that

$$\begin{aligned}N_5(X)&=c_5X+O(X^{\gamma+\varepsilon})\\ N_5(X;e)&=\delta_e c_5X+O(e^{\sigma_5}X^{\tau_5})+O(X^{\gamma+\varepsilon}).\end{aligned}$$

The main result of the sieve in this context is the following:

Proposition 6.1. *With the notation as above, we have*

$$E_d(\mathscr{A};(X/2)^{\delta_0},\frac{1}{2}M((X/2)^{\delta_0}))\ll X^{1-\delta_0+\varepsilon},$$

for any δ_0 such that

$$\delta_0 \le \begin{cases} \frac{1-\tau_d}{1+2\sigma_d} & \text{if } d = 2, 4 \\ \min\{\frac{1-\tau_d}{1+2\sigma_d}, 1/4\} & \text{if } d = 3, \\ \min\{\frac{1-\tau_d}{1+2\sigma_d}, 1-\gamma\} & \text{if } d = 5. \end{cases} \tag{6.1}$$

Moreover, for any such δ_0 there exist positive real constants $c_0(d) < c_1(d) < 1$ and $X_d = X_d(\delta_0) \ge 1$ such that for all $X \ge X_d$,

$$c_0(d)\frac{(X/2)^{\delta_0}}{\log(X/2)^{\delta_0}} \le M((X/2)^{\delta_0}) \le c_1(d)\frac{(X/2)^{\delta_0}}{\log(X/2)^{\delta_0}}. \tag{6.2}$$

The requirement that $X \ge X_d$ simply is a quantification of the requirement that X be sufficiently large, and will be incorporated later simply by enlarging certain implicit constants.

Proposition 6.1 immediately provides the upper bound we require for the bad set $\mathscr{B}_d(X; Y, M)$ defined in (2.2), with an appropriate choice of the parameters Y, M. As there are $\pi(Y) = Y(\log Y)^{-1} + O(Y(\log Y)^{-2})$ primes $p \le Y$, we could of course only expect at most $Y(\log Y)^{-1}$ primes $p \le Y$ to split completely in any given field. Proposition 6.1 shows that, up to a constant factor, this is a reasonable expectation, in that the mean $M((X/2)^{\delta_0})$ is approximately $\mu\pi((X/2)^{\delta_0})$, for some $\mu \in [c_0(d), c_1(d)]$; moreover Proposition 6.1 provides an upper bound for the number of fields with $D_K \le X$ in which at most $\frac{1}{2}M((X/2)^{\delta_0})$ primes $p \le (X/2)^{\delta_0}$ split completely.

We will prove Proposition 6.1 case by case.

6.2. **Sieve for quadratic fields.** For notational convenience, in this section we write σ, τ for σ_2, τ_2. We compute that for any prime p,

$$R_p = \#\mathscr{A}_p - \delta_p \#\mathscr{A} = N_2(X; p) - \delta_p N_2(X) = O(p^\sigma X^{\tau+\varepsilon}).$$

Similarly, for distinct primes p, q

$$R_{pq} = \#\mathscr{A}_{pq} - \delta_p\delta_q \#\mathscr{A} = N_2(X; pq) - \delta_p\delta_q N_2(X) = O(p^\sigma q^\sigma X^{\tau+\varepsilon}).$$

Thus since $\#\mathscr{A} \gg X$,

$$\frac{1}{\#\mathscr{A}} \sum_{p|P(z)} |R_p| \ll z^{1+\sigma} X^{\tau-1+\varepsilon}, \qquad \frac{1}{\#\mathscr{A}} \sum_{p,q|P(z)} |R_{pq}| \ll z^{2+2\sigma} X^{\tau-1+\varepsilon}.$$

We compute

$$U(z) = \sum_{p|P(z)} \delta_p = \frac{1}{2} \sum_{p|P(z)} \frac{1}{1+p^{-1}},$$

from which we deduce that

$$\frac{1}{3} z(\log z)^{-1} + O(z(\log z)^{-2}) \le U(z) \le \frac{1}{2} z(\log z)^{-1} + O(z(\log z)^{-2}). \tag{6.3}$$

Indeed, letting $\varepsilon_p = (1+p^{-1})^{-1}$, the upper bound follows directly from the prime number theorem and the fact that $0 < \varepsilon_p < 1$, while the lower bound only requires noticing

$$U(z) \ge \frac{1}{2} \sum_{p|P(z)} \varepsilon_2 = \frac{1}{3} \sum_{p|P(z)} 1 = \frac{1}{3} z(\log z)^{-1} + O(z(\log z)^{-2}).$$

We may compute the mean as in (3.3):

$$M(z) = U(z) + \frac{1}{\#\mathscr{A}} \sum_{p|P(z)} R_p = U(z) + O(z^{1+\sigma} X^{\tau-1+\varepsilon}).$$

Recalling (6.3) and that $z = (X/2)^{\delta_0}$ for a parameter δ_0 to be chosen later, we see the last error term will be $< \frac{1}{2}U(z)$ for sufficiently large X as long as

$$\delta_0 < \frac{1-\tau}{\sigma}. \tag{6.4}$$

Assuming this, for sufficiently large X we have

$$c_0 z(\log z)^{-1} \le \frac{1}{2}U(z) \le M(z) \le \frac{3}{2}U(z) \le c_1 z(\log z)^{-1}$$

for absolute constants $0 < c_0 < c_1 \le 1$. We apply Lemma 3.1 to see that

$$\begin{aligned} E_2(\mathscr{A}; z, \frac{1}{2}M(z)) &\ll \frac{X^{1+\varepsilon}}{z^2}\left(z + z^{2+2\sigma}X^{\tau-1} + z(z^{1+\sigma}X^{\tau-1}) + (z^{1+\sigma}X^{\tau-1})^2\right) \\ &\ll X^{\varepsilon}(Xz^{-1} + z^{2\sigma}X^{\tau}), \end{aligned}$$

still assuming (6.4). Balancing the terms in the last expression above would set

$$\delta_0 = (1-\tau)/(1+2\sigma), \tag{6.5}$$

which certainly satisfies (6.4); as a consequence, for any $\delta_0 \le (1-\tau)/(1+2\sigma)$, we obtain

$$E_2(\mathscr{A}; (X/2)^{\delta_0}, \frac{1}{2}M((X/2)^{\delta_0})) \ll X^{1-\delta_0+\varepsilon},$$

which proves Proposition 6.1 in the case of quadratic fields.

6.3. **Sieve for cubic fields.** For notational convenience, in this section we write σ, τ for σ_3, τ_3. We compute that

$$R_p = \#\mathscr{A}_p - \delta_p \#\mathscr{A} = c_3'(\delta_p' - \delta_p)X^{5/6} + O(p^{\sigma}X^{\tau+\varepsilon}) = O(p^{-1/3}X^{5/6} + p^{\sigma}X^{\tau+\varepsilon}).$$

For distinct primes p, q,

$$R_{pq} = c_3'(\delta_p'\delta_q' - \delta_p\delta_q)X^{5/6} + O(p^{\sigma}q^{\sigma}X^{\tau+\varepsilon}) = O(p^{-1/3}X^{5/6} + q^{-1/3}X^{5/6} + p^{\sigma}q^{\sigma}X^{\tau+\varepsilon}).$$

Since $\#\mathscr{A} \gg X$, we may compute that

$$\begin{aligned} \frac{1}{\#\mathscr{A}}\sum_{p|P(z)}|R_p| &\ll z^{2/3}X^{-1/6} + z^{1+\sigma}X^{\tau-1+\varepsilon}, \\ \frac{1}{\#\mathscr{A}}\sum_{p,q|P(z)}|R_{p,q}| &\ll z^{5/3}X^{-1/6} + z^{2+2\sigma}X^{\tau-1+\varepsilon}. \end{aligned}$$

Next, we note that

$$U(z) = \sum_{p|P(z)}\delta_p = \frac{1}{6}\sum_{p|P(z)}\frac{1}{1+p^{-1}+p^{-2}} = \frac{1}{6}\sum_{p|P(z)}e_p,$$

say. From this we can deduce (as in the case of quadratic fields) that

$$\frac{2}{21}z(\log z)^{-1} + O(z(\log z)^{-2}) \le U(z) \le \frac{1}{6}z(\log z)^{-1} + O(z(\log z)^{-2}). \tag{6.6}$$

Finally, we compute the mean

$$M(z) = U(z) + \frac{1}{\#\mathscr{A}}\sum_{p|P(z)}R_p = U(z) + O(z^{2/3}X^{-1/6} + z^{1+\sigma}X^{\tau-1+\varepsilon}).$$

Recalling (6.6) and that $z = (X/2)^{\delta_0}$ for a parameter δ_0 to be chosen later, we see the last error term will be $< \frac{1}{2}U(z)$ for sufficiently large X as long as the analogue of (6.4) holds, in which case

$$c_0 z(\log z)^{-1} \le \frac{1}{2}U(z) \le M(z) \le \frac{3}{2}U(z) \le c_1 z(\log z)^{-1}.$$

for absolute constants $0 < c_0 < c_1 \le 1$.

We now apply Lemma 3.1, which shows that

$$\begin{aligned} E_3(\mathscr{A}; z, \frac{1}{2}M(z)) \ll \frac{X^{1+\varepsilon}}{z^2}\Big(z + \{z^{5/3}X^{-1/6} + z^{2+2\sigma}X^{\tau-1}\} \\ + z\{z^{2/3}X^{-1/6} + z^{1+\sigma}X^{\tau-1}\} + \{z^{2/3}X^{-1/6} + z^{1+\sigma}X^{\tau-1}\}^2\Big). \end{aligned}$$

As long as $\delta_0 \le 1/4$, we have $z^{5/3}X^{-1/6} \ll z$; after further simplification and still assuming the analogue of (6.4), we see that

$$E_3(\mathscr{A}; z, \frac{1}{2}M(z)) \ll X^{\varepsilon}(Xz^{-1} + z^{2\sigma}X^{\tau}).$$

This is optimized by choosing δ_0 as in (6.5) as before, which satisfies (6.4). In particular, for any $\delta_0 \le \min\{1/4, (1-\tau)/(1+2\sigma)\}$, we obtain

$$E_3(\mathscr{A}; (X/2)^{\delta_0}, \frac{1}{2}M((X/2)^{\delta_0})) \ll X^{1-\delta_0+\varepsilon},$$

which proves Proposition 6.1 in the case of cubic fields.

6.4. **Sieve for non-D_4-quartic fields.** The case of non-D_4-quartic fields is very similar to that for real quadratic fields, thus we only mention the highlights, with σ, τ denoting σ_4, τ_4. We have

$$\begin{aligned} R_p &= \#\mathscr{A}_p - \delta_p \#\mathscr{A} = O(p^{\sigma}X^{\tau+\varepsilon}), \\ R_{pq} &= \#\mathscr{A}_{pq} - \delta_p\delta_q\#\mathscr{A} = O(p^{\sigma}q^{\sigma}X^{\tau+\varepsilon}), \\ U(z) &= \sum_{p|P(z)} \delta_p = \frac{1}{24}\sum_{p|P(z)} \frac{1}{1+p^{-1}+2p^{-2}+p^{-3}}. \end{aligned}$$

We deduce that

$$\frac{1}{3\cdot 17} z(\log z)^{-1} + O(z(\log z)^{-2}) \le U(z) \le \frac{1}{24} z(\log z)^{-1} + O(z(\log z)^{-2}). \tag{6.7}$$

Next we compute the mean

$$M(z) = U(z) + \frac{1}{\#\mathscr{A}} \sum_{p|P(z)} R_p = U(z) + O(z^{1+\sigma}X^{\tau-1+\varepsilon}).$$

Recalling (6.7) and that $z = (X/2)^{\delta_0}$, we see that as long as the analogous condition to (6.4) holds and X is sufficiently large,

$$c_0 z(\log z)^{-1} \le \frac{1}{2}U(z) \le M(z) \le \frac{3}{2}U(z) \le c_1 z(\log z)^{-1}$$

for absolute constants $0 < c_0 < c_1 \le 1$.

We apply Lemma 3.1 to see that under the assumption (6.4)

$$E_4(\mathscr{A}; z, \frac{1}{2}M(z)) \ll \frac{X^{1+\varepsilon}}{z^2}\left(z + z^{2+2\sigma}X^{\tau-1} + z(z^{1+\sigma}X^{\tau-1}) + (z^{1+\sigma}X^{\tau-1})^2\right) \ll X^{\varepsilon}(Xz^{-1} + z^{2\sigma}X^{\tau}),$$

so that

$$E_4(\mathscr{A}; (X/2)^{\delta_0}, \frac{1}{2}M((X/2)^{\delta_0})) \ll X^{1-\delta_0+\varepsilon}$$

for any $\delta_0 \le (1-\tau)/(1+2\sigma)$.

6.5. **Sieve for quintic fields.** Finally, we apply the sieve to quintic fields, denoting σ_5, τ_5 by σ, τ. We compute that for any $p = O(X^{\rho})$,

$$R_p = \#\mathscr{A}_p - \delta_p\#\mathscr{A} = O(X^{\varepsilon}(p^{\sigma}X^{\tau} + X^{\gamma})).$$

For distinct primes p, q,

$$R_{pq} = \#\mathscr{A}_{pq} - \delta_p\delta_q\#\mathscr{A} = O(X^{\varepsilon}(p^{\sigma}q^{\sigma}X^{\tau} + X^{\gamma})).$$

We compute

$$U(z) = \sum_{p|P(z)} \delta_p = \frac{1}{120}\sum_{p|P(z)} \frac{1}{1+p^{-1}+2p^{-2}+2p^{-3}+p^{-4}},$$

from which we deduce that

$$\frac{2}{15\cdot 37} z(\log z)^{-1} + O(z(\log z)^{-2}) \le U(z) \le \frac{1}{120} z(\log z)^{-1} + O(z(\log z)^{-2}).$$

The mean may be expressed as

$$M(z) = U(z) + \frac{1}{\#\mathscr{A}} \sum_{p|P(z)} R_p = U(z) + O(X^{\varepsilon}(z^{1+\sigma}X^{\tau-1} + zX^{\gamma-1+\varepsilon})).$$

The last term will be $< \frac{1}{2}U(z)$ for sufficiently large X as long as $\gamma < 1$ and the analogous condition to (6.4) holds. Assuming this, we have

$$c_0 z(\log z)^{-1} \le \frac{1}{2}U(z) \le M(z) \le \frac{3}{2}U(z) \le c_1 z(\log z)^{-1}$$

for absolute constants $0 < c_0 < c_1 \le 1$.

We apply Lemma 3.1 to see that under the assumptions $\tau, \gamma < 1$ and (6.4),

$$E_5(\mathscr{A}; z, \frac{1}{2}M(z)) \ll \frac{X^{1+\varepsilon}}{z^2}\left(z + z^2X^{-1}(z^{2\sigma}X^{\tau} + X^{\gamma}) + zX^{-1}(z^{\sigma}X^{\tau} + X^{\gamma}) + z^2X^{-2}(z^{\sigma}X^{\tau} + X^{\gamma})^2\right).$$

After simplification, this shows

$$E_5(\mathscr{A}; z, \frac{1}{2}M(z)) \ll \frac{X^{1+\varepsilon}}{z^2}(z + z^2X^{\gamma-1} + z^{2+2\sigma}X^{\tau-1}) \ll X^{\varepsilon}(Xz^{-1} + X^{\gamma} + z^{2\sigma}X^{\tau}).$$

Assuming $z = (X/2)^{\delta_0}$, we may conclude that for any $\delta_0 \le \min\{(1-\tau)/(1+2\sigma), 1-\gamma\}$, we have

$$E_5(\mathscr{A}; (X/2)^{\delta_0}, \frac{1}{2}M((X/2)^{\delta_0})) \ll X^{1-\delta_0+\varepsilon}.$$

This completes the proof of Proposition 6.1.

7. Proof of the main theorem and corollaries

7.1. **Proof of Theorem 2.1.** We now derive Theorem 2.1 from Proposition 6.1. By definition, if $M_1 \le M_2$ then $\mathscr{B}_d(X; Y, M_1) \subseteq \mathscr{B}_d(X; Y, M_2)$. If X is sufficiently large so that (6.2) holds, say $X \ge X_d(\delta)$, we may apply (6.2) to write

$$\#\mathscr{B}_d(X; (X/2)^{\delta}, \frac{1}{2}c_0(d)\frac{(X/2)^{\delta}}{\log(X/2)^{\delta}}) \le \#\mathscr{B}_d(X; (X/2)^{\delta}, \frac{1}{2}M((X/2)^{\delta})) = E_d(\mathscr{A}; (X/2)^{\delta}, \frac{1}{2}M((X/2)^{\delta})).$$

We then apply Proposition 6.1 and deduce that for $X \ge X_d(\delta)$,

$$\#\mathscr{B}_d(X; (X/2)^{\delta}, \frac{1}{2}c_0(d)\frac{(X/2)^{\delta}}{\log(X/2)^{\delta}}) \ll X^{1-\delta+\varepsilon}$$

for every $\varepsilon > 0$, and for δ constrained by (6.1). When we make the constraints in (6.1) precise by applying the results of Lemma 2.2, Theorem C, Theorems 2.3 and 2.4, we obtain the parameters defined in (2.5). For any δ satisfying (2.5), we may remove the explicit assumption that $X \ge X_d(\delta)$ by including an appropriate implicit constant, so that

$$\#\mathscr{B}_d(X; (X/2)^{\delta}, \frac{1}{2}c_0(d)\frac{(X/2)^{\delta}}{\log(X/2)^{\delta}}) \ll_{d,\delta,\varepsilon} X^{1-\delta+\varepsilon} \tag{7.1}$$

for every $X \ge 1$ and every $\varepsilon > 0$.

7.2. **Proof of Theorem 1.1.** To derive Theorem 1.1 from Theorem 2.1, we proceed via a standard dyadic argument, which we now make precise. Let $\varepsilon > 0$ be fixed and for this ε, let the implied constant in Theorem A be denoted by $C_0 = C_0(d, \varepsilon)$, so that (1.8) becomes

$$|\mathrm{Cl}_K[\ell]| \le C_0 D_K^{1/2+\varepsilon} M^{-1}. \tag{7.2}$$

Fix any $\delta < \frac{1}{2\ell(d-1)}$. Then if K is a degree d extension of $\mathbb{Q}$ with $D_K \in (X, 2X]$ that is not in the bad set $\mathscr{B}_d^0(X; X^{\delta}, \frac{1}{2}c_0(d)X^{\delta}/\log X^{\delta})$, we see from (7.2) that

$$\begin{aligned} |\mathrm{Cl}_K[\ell]| &\le C_0(\frac{1}{2}c_0(d))^{-1} D_K^{1/2+\varepsilon} X^{-\delta}\log(X^{\delta}) \\ &\le C_0' D_K^{1/2-\delta+\varepsilon}\log(D_K^{\delta}), \end{aligned}$$

where it suffices to take $C_0' = C_0 2^{1+\delta}(\frac{1}{2}c_0(d))^{-1}$. Now we assume that X is sufficiently large, say $X \ge C(d, \ell, \varepsilon)$, so that for all $\delta < \frac{1}{2\ell(d-1)}$, and for all $D_K \in (X, 2X]$, we have $\log(D_K^{\delta}) \le D_K^{\varepsilon}$. Under this assumption we have

$$|\mathrm{Cl}_K[\ell]| \le C_0' D_K^{1/2-\delta+2\varepsilon} \tag{7.3}$$

for all these fields not in $\mathscr{B}_d^0(X; X^\delta, \frac{1}{2}c_0(d)X^\delta/\log X^\delta)$.

Let $F_{d,\ell}^0(X;\delta,\varepsilon)$ denote the collection of fields $K/\mathbb{Q}$ of degree d with $X < D_K \le 2X$ that fail the bound (7.3); we may conclude that for any $\delta < \frac{1}{2\ell(d-1)}$ and for all $X \ge C(d,\ell,\varepsilon)$,

$$F_{d,\ell}^0(X;\delta,\varepsilon) \subseteq \mathscr{B}_d^0(X, X^\delta, \frac{1}{2}c_0(d)X^\delta/\log X^\delta). \tag{7.4}$$

Now let $F_{d,\ell}(X;\delta,\varepsilon)$ denote the collection of fields $K/\mathbb{Q}$ of degree d with $0 < D_K \le X$ that fail the bound (7.3); then

$$F_{d,\ell}(X;\delta,\varepsilon) \subseteq \bigcup_{0\le j\le \lceil \log_2 X\rceil} F_d^0(2^j;\delta,\varepsilon).$$

Set j_0 to be the smallest j such that $2^{j_0} \ge C(d,\ell,\varepsilon)$. Then for $j \le j_0$, we apply the trivial bound, $\#F_{d,\ell}^0(2^j,\delta,\varepsilon) \ll 2^j$. (This bound is only "trivial" in the sense that we know by (1.11) how to count fields of degree d with $0 < D_K \le X$, for $d \le 5$.) For $j > j_0$ we apply (7.4) to write

$$\bigcup_{j_0<j\le\lceil\log_2 X\rceil} F_{d,\ell}^0(2^j;\delta,\varepsilon) \subseteq \bigcup_{j_0<j\le\lceil\log_2 X\rceil} \mathscr{B}_d^0(2^j, 2^{j\delta}, \frac{1}{2}c_0(d)2^{j\delta}/\log 2^{j\delta}).$$

Trivially enlarging each of the last sets to the non-dyadic version $\mathscr{B}_d(2^{j+1}, 2^{j\delta}, \frac{1}{2}c_0(d)2^{j\delta}/\log 2^{j\delta})$ and applying the result of Theorem 2.1 to each such set, we obtain

$$\#F_{d,\ell}(X;\delta,\varepsilon) \ll C(d,\ell,\varepsilon) + \sum_{j_0<j\le\lceil\log_2 X\rceil} 2^{j(1-\delta+\varepsilon')} \ll_{c,d,\ell,\varepsilon,\varepsilon'} X^{1-\delta+\varepsilon'}. \tag{7.5}$$

which now holds (with a sufficiently large implicit constant) for all $X \ge 1$, for all $\varepsilon' > 0$ arbitrarily small, and for all $\delta < \min\{\frac{1}{2\ell(d-1)}, \delta_0(d)\}$ where $\delta_0(d)$ is defined as in (2.5) in Theorem 2.1. For sufficiently large ℓ, the first constraint on δ is a stronger constraint than the second.

To be precise, we now break down into cases depending on d. For $d = 2$, Theorem 1.1 is implied in the case $\ell = 2$ by Gauss genus theory, and in the case $\ell = 3$ by the known asymptotic (1.5). For integers $\ell \ge 4$, Theorem 1.1 follows from (7.5), since $1/2\ell = \min\{1/6, \frac{1}{2\ell}\}$ for $\ell \ge 4$. (Of course, for primes $\ell \ge 5$ and imaginary quadratic fields, Theorem 1.1 is implied by the stronger result (1.10), or indeed by an earlier result of Soundararajan [Sou00] that at most one imaginary quadratic field K with $D_K \in [X, 2X]$ can have $|\mathrm{Cl}_K[\ell]| \gg D_K^{1/2-1/2\ell+\varepsilon}$; see also Corollary 2.2 of [HBP17].) For $d = 3$, Theorem 1.1 is implied for $\ell = 2$ by the known asymptotic (1.6), and for $\ell = 3$ by the stronger known result (1.3). The cases $\ell \ge 4$ are implied by (7.5), since $1/4\ell = \min\{2/25, \frac{1}{4\ell}\}$ for $\ell \ge 4$. For $d = 4$, Theorem 1.1 follows from (7.5) since $1/6\ell = \min\{\frac{1}{48}, \frac{1}{6\ell}\}$ for $\ell \ge 8$; the remaining cases of $\ell \le 7$ follow from the choice $\delta_0 = 1/48$. Finally, for $d = 5$, Theorem 1.1 similarly follows from (7.5) since $1/8\ell = \min\{\frac{1}{200}, \frac{1}{8\ell}\}$ for $\ell \ge 25$; the remaining cases of $\ell \le 24$ follow from the choice $\delta_0 = 1/200$.

Corollaries 1.1.1 and 1.1.2 now follow from Theorem 1.1, or can be derived directly from Theorem 2.1, as already demonstrated in Section 2.1.

8. Appendix: counting quadratic fields

In this appendix we prove the following result, from which Lemma 2.2 may be deduced immediately.

Proposition 8.1. *Let P be a finite set of primes. For each prime $p \in P$ we choose a splitting type at p and assign a corresponding density as follows:*

$$\delta_p := \frac{1}{2}(1+p^{-1})^{-1} \qquad \text{for } p = \mathfrak{p}_1\mathfrak{p}_2$$
$$\delta_p := \frac{1}{2}(1+p^{-1})^{-1} \qquad \text{for } p = \mathfrak{p}_1$$
$$\delta_p := (p+1)^{-1} \qquad \text{for } p \text{ ramified.}$$

Let $e = \prod_{p\in P} p$ and $\delta_e = \prod_{p\in P}\delta_p$. Let $N_2^{\pm}(X;P)$ denote the number of real (respectively imaginary) quadratic extensions of $\mathbb{Q}$ with fundamental discriminant $|D_K| \le X$ such that for each $p \in P$, the prime p

splits in the quadratic field with splitting type chosen for p above. Then

$$N_2^{\pm}(X;P) = \delta_e \left(\frac{1}{3}+\frac{1}{6}\right)\frac{1}{\zeta(2)}X + O(e\sqrt{X}). \tag{8.1}$$

We remark that in (8.1), the first term is contributed by fundamental discriminants $\equiv 1 \pmod 4$ and the second by fundamental discriminants $\equiv 0 \pmod 4$. We prove the proposition explicitly for $N_2^+(X;P)$, and omit the analogous argument for $N_2^-(X;P)$. Upon combining the counts for real and imaginary fields, this implies Lemma 2.2 as a special case.

The proof is a simple elaboration on the classical method for counting square-free integers $\leq X$. Recall that, for a fundamental discriminant D, a prime p is ramified in $\mathbb{Q}(\sqrt{D})$ precisely when $p|D$; otherwise a prime $p \nmid D$ splits in $\mathbb{Q}(\sqrt{D})$ if the Kronecker symbol $\left(\frac{D}{p}\right)$ evaluates as $+1$, and is non-split if $\left(\frac{D}{p}\right) = -1$ (see e.g. [Hua82, Theorem 10.3, Chapter 16]). Thus for each unramified $p \in P$ we assign $\varepsilon_p \in \{-1,+1\}$ according to the specified splitting type of p. Let P_0 be the set of ramified primes in P and set $P' = P \setminus P_0$; define $e_0 = \prod_{p\in P_0} p$ and $e' = \prod_{p\in P'} p$. Then we may write

$$N_2^+(X;P) = \#\{\text{fundamental discriminants } 1 \leq n \leq X : e_0|n,\ \left(\frac{n}{p}\right) = \varepsilon_p, \forall p \in P'\}.$$

We will find a count for this by sieving for fundamental discriminants (that is, elements that are free of odd squares) in the following two sets:

$$\mathcal{A}^{(1)} = \{1 \leq n \leq X : n \equiv 1 \pmod 4, e_0|n, \left(\frac{n}{p}\right) = \varepsilon_p, \forall p \in P'\}$$

$$\mathcal{A}^{(0)} = \{1 \leq n \leq X : n \equiv 8, 12 \pmod{16}, e_0|n, \left(\frac{n}{p}\right) = \varepsilon_p, \forall p \in P'\}.$$

More generally, fix a power g and define for any $b \pmod{2^g}$ the set

$$\mathcal{A} = \{1 \leq n \leq X : n \equiv b \pmod{2^g}, e_0|n, \left(\frac{n}{p}\right) = \varepsilon_p, \forall p \in P'\}.$$

For each odd prime q let $\mathcal{A}_q = \{n \in \mathcal{A} : q^2|n\}$. Note that certainly $\mathcal{A}_q$ is empty as soon as $q > \sqrt{X}$; we let M be the index of the greatest prime $q_M \leq \sqrt{X}$. We will denote by $\overline{\mathcal{A}}_q$ the complement $\mathcal{A} \setminus \mathcal{A}_q$. We will deduce Proposition 8.1 from the following lemma:

Lemma 8.2. *Let $\mathcal{A}$ be as above, with $P = P_0 \cup P'$ a set of odd primes. Then*

$$\bigcap_{q \text{ odd}} \overline{\mathcal{A}}_q = \frac{X}{3\cdot 2^{g-2}\zeta(2)} \prod_{p\in P'} \delta_p \prod_{p\in P_0} \delta_p + O(e\sqrt{X}),$$

with δ_p as defined in Proposition 8.1.

If the set P specified in Proposition 8.1 is a set of odd primes, then the proposition follows immediately from this lemma, by applying it to $\mathcal{A}^{(1)}$ with $g = 2$, $b = 1$ and then partitioning $\mathcal{A}^{(0)}$ into two disjoint sets with $g = 4$ and $b = 8$ or 12, respectively, and applying the lemma to each.

If 2 belongs to the set P specified in Proposition 8.1, then we consider separately the case when 2 is specified to be ramified or unramified. If $2 \in P_0$ then $\mathcal{A}^{(1)}$ is empty. We already have $2|n$ for every $n \in \mathcal{A}^{(0)}$, so we set $P_{00} = P_0 \setminus \{2\}$ and apply Lemma 8.2 to $\mathcal{A}^{(0)}$ with $P = P_{00} \cup P'$ (as before, separating $\mathcal{A}^{(0)}$ into two disjoint sets and applying the lemma to each). We obtain

$$\bigcap_{q \text{ odd}} \overline{\mathcal{A}}_q = 2\cdot\frac{X}{3\cdot 4\zeta(2)} \prod_{p\in P'} \delta_p \prod_{p\in P_{00}} \delta_p + O(e\sqrt{X}) = \delta_2 \cdot \frac{X}{2\zeta(2)} \prod_{p\in P'} \delta_p \prod_{p\in P_{00}} \delta_p + O(e\sqrt{X}),$$

with $\delta_2 = 1/3$, as claimed.

If $2 \in P'$ then $\mathcal{A}^{(0)}$ is empty. We recall that for $p = 2$ and $n \equiv 1 \pmod 4$, the Kronecker symbol $\left(\frac{n}{2}\right) = +1$ if $n \equiv 1 \pmod 8$ and -1 if $n \equiv 5 \pmod 8$. Thus if $2 \in P'$, we set $P'' = P' \setminus \{2\}$ and $\mathcal{A}^{(1)}$ becomes

$$\mathcal{A}^{(1)} = \{1 \leq n \leq X : n \equiv b \pmod 8, e_0|n, \left(\frac{n}{p}\right) = \varepsilon_p, \forall p \in P''\},$$

with $b = 1$ if the original specification was $\varepsilon_2 = +1$ and $b = 5$ if $\varepsilon_2 = -1$. Applying Lemma 8.2, we see that

$$\bigcap_{q \text{ odd}} \overline{\mathcal{A}}_q = \frac{X}{3 \cdot 2\zeta(2)} \prod_{p \in P''} \delta_p \prod_{p \in P_0} \delta_p + O(e\sqrt{X}) = \delta_2 \cdot \frac{X}{2\zeta(2)} \prod_{p \in P''} \delta_p \prod_{p \in P_0} \delta_p + O(e\sqrt{X}),$$

with $\delta_2 = 1/3$, again as claimed. This proves Proposition 8.1.

We now prove Lemma 8.2. By the inclusion-exclusion principle,

$$\bigcap_{q \text{ odd}} \overline{\mathcal{A}}_q = \sum_{m=0}^{M} (-1)^m \sum_{q_1 < \cdots < q_m} |\mathcal{A}_{q_1} \cap \cdots \cap \mathcal{A}_{q_m}|, \tag{8.2}$$

in which for the $m = 0$ term we sum the full set $|\mathcal{A}|$. A priori, any fixed term in (8.2) can be written as

$$|\mathcal{A}_{q_1} \cap \cdots \cap \mathcal{A}_{q_m}| = \#\{n \le X : q_1^2 \cdots q_m^2 | n, n \equiv b \pmod{2^g}, e_0 | n, \left(\frac{n}{p}\right) = \varepsilon_p, \forall p \in P'\}.$$

Denote the set on the right-hand side by S, and let $Q := \{q_1, \dots, q_m\}$. We first observe that if any $p \in P'$ belongs to Q then the set S must be empty. Thus we may reduce to considering the case in which P' and Q are disjoint, in which case we will prove that

$$\#S = \frac{1}{2^g} \frac{X}{q_1^2 \cdots q_m^2} \frac{\gcd(q_1 \cdots q_m, e_0)}{e_0} \prod_{p \in P'} \frac{1}{2} \left(\frac{p-1}{p}\right) + O(e'). \tag{8.3}$$

First note that if a prime p in P_0 belongs to Q as well, then the condition $q_1^2 \cdots q_m^2 | n$ already specifies that p is ramified. Thus upon defining $e_{00} = \prod_{p \in P_0 \setminus Q} p$, we may deduce that

$$S = \{k \le X(q_1^2 \cdots q_m^2 e_{00})^{-1} : k \equiv b(q_1^2 \cdots q_m^2 e_{00})^{-1} \pmod{2^g}, \left(\frac{k}{p}\right) = \varepsilon'_p, \forall p \in P'\}, \tag{8.4}$$

where for each $p \in P'$ we have defined $\varepsilon'_p = \varepsilon_p \left(\frac{e_{00}}{p}\right)$.

We note that for any integer $K \ge 1$ and any residue class b modulo 2^g, the quantity

$$\#\{k \le K : k \equiv b \pmod{2^g}, \left(\frac{k}{p}\right) = \varepsilon'_p, \forall p \in P'\}$$

may be expressed as

$$\begin{aligned}
&\sum_{\substack{a \pmod{e'} \\ (a,e')=1}} \left(\prod_{p \in P'} \frac{1}{2} \left(1 + \varepsilon'_p \left(\frac{a}{p}\right)\right) \right) \sum_{\substack{k \le K \\ k \equiv a \pmod{e'} \\ k \equiv b \pmod{2^g}}} 1 \\
&= \frac{1}{2^{|P'|}} \sum_{\substack{a \pmod{e'} \\ (a,e')=1}} \prod_{p \in P'} \left(1 + \varepsilon'_p \left(\frac{a}{p}\right)\right) \left(\frac{K}{2^g e'} + O(1)\right) \\
&= \left(\prod_{p \in P'} \frac{p-1}{p} \right) \frac{K}{2^{g+|P'|}} + 0 + O(e');
\end{aligned}$$

all the intermediate terms vanish by orthogonality of characters. Applying this to S in (8.4), we obtain

$$\#S = \frac{X}{q_1^2 \cdots q_m^2 e_{00}} \frac{1}{2^{g+|P'|}} \prod_{p \in P'} \left(\frac{p-1}{p}\right) + O(e'),$$

proving (8.3).

Applying (8.3) to the inclusion-exclusion in (8.2) shows that

$$\bigcap_{q \text{ odd}} \overline{\mathcal{A}}_q = \sum_{\substack{d \le \sqrt{X} \\ (d, 2e')=1}} \mu(d) \left(\frac{X}{2^g d^2} \frac{\gcd(d, e_0)}{e_0} \prod_{p \in P'} \frac{1}{2} \left(\frac{p-1}{p}\right) + O(e') \right).$$

The error term contributes $O(e\sqrt{X})$, while the main term contributes

$$X\frac{1}{2^g}\left(\prod_{p\in P'}\frac{1}{2}\left(\frac{p-1}{p}\right)\right)\sum_{\substack{d=1\\(d,2e')=1}}^{\infty}\frac{\mu(d)}{d^2}\frac{\gcd(d,e_0)}{e_0}+O(X\sum_{d>\sqrt{X}}\frac{1}{d^2}).$$

Here the error term is $O(\sqrt{X})$, with an implied constant which may be taken to be independent of P.

We now simplify the main term. We note that since P consists of odd primes and $(e_0,e')=1$, upon setting $d=\delta f$ with $\delta=\gcd(d,e_0)$, we have

$$\begin{aligned}\sum_{\substack{d=1\\(d,2e')=1}}^{\infty}\frac{\mu(d)}{d^2}\frac{\gcd(d,e_0)}{e_0} &= \sum_{\delta|e_0}\sum_{\substack{f=1\\(\delta f,2e')=(f,e_0)=1}}^{\infty}\frac{\mu(\delta f)}{\delta^2 f^2}\frac{\delta}{e_0}\\ &= \frac{1}{e_0}\left(\sum_{\delta|e_0}\frac{\mu(\delta)}{\delta}\right)\left(\sum_{\substack{f=1\\(f,2e'e_0)=1}}^{\infty}\frac{\mu(f)}{f^2}\right).\end{aligned}$$

The sum over $\delta|e_0$ is a multiplicative function with respect to e_0. For p prime we have

$$\sum_{\delta|p}\frac{\mu(\delta)}{\delta}=1-\frac{1}{p}$$

and thus for e_0 square-free we may compute by multiplicativity that

$$\frac{1}{e_0}\sum_{\delta|e_0}\frac{\mu(\delta)}{\delta}=\prod_{p\in P_0}\frac{p-1}{p^2}.$$

We next recall that for any $\Re(s)>1$ and any distinct primes $q_1,\dots,q_r$,

$$\left(\prod_{i=1}^{r}(1-\frac{1}{q_i^s})\zeta(s)\right)^{-1}=\prod_{p\notin\{q_1,\dots,q_r\}}\left(1-\frac{1}{p^s}\right)=\sum_{\substack{d=1\\(d,\prod q_i)=1}}^{\infty}\frac{\mu(d)}{d^s}.$$

Thus

$$\sum_{\substack{f=1\\(f,2e'e_0)=1}}^{\infty}\frac{\mu(f)}{f^2}=(1-\frac{1}{2^2})^{-1}\prod_{p\in P}(1-\frac{1}{p^2})^{-1}\frac{1}{\zeta(2)}.$$

Assembling this all together, we see that

$$\bigcap_{q\text{ odd}}\overline{\mathcal{A}}_q=\frac{X}{2^g}(1-\frac{1}{2^2})^{-1}\frac{1}{\zeta(2)}\prod_{p\in P'}\left(\frac{p-1}{2p}\frac{1}{1-\frac{1}{p^2}}\right)\prod_{p\in P_0}\left(\frac{p-1}{p^2}\frac{1}{1-\frac{1}{p^2}}\right)+O(e\sqrt{X}).$$

This reduces to

$$\bigcap_{q\text{ odd}}\overline{\mathcal{A}}_q=\frac{X}{3\cdot 2^{g-2}\zeta(2)}\prod_{p\in P'}\frac{1}{2}\frac{1}{(1+p^{-1})}\prod_{p\in P_0}\frac{1}{1+p}+O(e\sqrt{X}),$$

proving Lemma 8.2, with δ_p as in Proposition 8.1.

Acknowledgements

The authors thank Paul Pollack, Arul Shankar, Frank Thorne, and Jacob Tsimerman for very helpful conversations and the referee for helpful comments on exposition. We thank Frank Thorne in particular for a suggestion that helped improved the exponent in Theorem 5.1. Ellenberg is partially supported by National Science Foundation Grant DMS-1402620 and a Guggenheim Fellowship. Pierce has been partially supported by National Science Foundation Grant DMS-1402121 and CAREER grant DMS-1652173. Wood is partially supported by an American Institute of Mathematics Five-Year Fellowship, a Packard Fellowship for Science and Engineering, a Sloan Research Fellowship, and National Science Foundation Grant DMS-1301690.

References

[Bai80] A. M. Baily. On the density of discriminants of quartic fields. *J. Reine Angew. Math.*, 315:190–210, 1980.

[BBP10] K. Belabas, M. Bhargava, and C. Pomerance. Error estimates for the Davenport-Heilbronn theorems. *Duke Mathematical Journal*, 153(1):173–210, May 2010.

[Bha04] M. Bhargava. Higher composition laws III: The parametrization of quartic rings. *Annals of Mathematics*, 159(3):1329–1360, May 2004.

[Bha05] M. Bhargava. The density of discriminants of quartic rings and fields. *Annals of Mathematics*, 162(2):1031–1063, September 2005.

[Bha08] M. Bhargava. Higher composition laws IV: The parametrization of quintic rings. *Annals of Mathematics*, 167(1):53–94, January 2008.

[Bha10] M. Bhargava. The density of discriminants of quintic rings and fields. *Annals of Mathematics*, 172(3):1559–1591, October 2010.

[BS96] A. Brumer and J. H. Silverman. The number of elliptic curves over $\mathbf{Q}$ with conductor N. *Manuscripta Math.*, 91(1):95–102, 1996.

[BST13] M. Bhargava, A. Shankar, and J. Tsimerman. On the Davenport–Heilbronn theorems and second order terms. *Inventiones mathematicae*, 193(2):439–499, August 2013.

[BST+17] Manjul Bhargava, Arul Shankar, Takashi Taniguchi, Frank Thorne, Jacob Tsimerman, and Yongqiang Zhao. Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves. *arXiv:1701.02458*, 2017.

[CDyDO02] H. Cohen, F. Diaz y Diaz, and M. Olivier. Enumerating quartic dihedral extensions of $\mathbb{Q}$. *Compositio Math.*, 133(1):65–93, 2002.

[CK15] P. J. Cho and H. H. Kim. Central limit theorem for Artin L-functions. *(preprint)*, arXiv:1506.07416v1, 2015.

[CL84] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[CM90] H. Cohen and J. Martinet. Étude heuristique des groupes de classes des corps de nombres. *Journal für die Reine und Angewandte Mathematik*, 404:39–76, 1990.

[CM06] A. C. Cojocaru and M. R. Murty. *An Introduction to Sieve Methods and their Applications*. London Mathematical Society, Student Texts 66, 2006.

[DH71] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields II. *Proc. Roy. Soc. Lond. A.*, 322:405–420, 1971.

[Duk98] W. Duke. Bounds for arithmetic multiplicities. In *Proceedings of the International Congress of Mathematicians, Vol. II (Berlin, 1998)*, number Extra Vol. II, pages 163–172, 1998.

[EV07] J. S. Ellenberg and A. Venkatesh. Reflection principles and bounds for class group torsion. *Int. Math. Res. Not. IMRN*, (1):Art. ID rnm002, 18, 2007.

[FK06] Étienne Fouvry and Jürgen Klüners. On the 4-rank of class groups of quadratic number fields. *Inventiones mathematicae*, 167(3):455–513, November 2006.

[FLN15] C. Frei, D. Loughran, and R. Newton. The Hasse norm principle for abelian extensions. *arXiv:1508.02518*, 2015.

[Gau01] C. F. Gauss. *Disquisitiones Arithmeticae*. trans. Arthur A. Clarke, Yale University Press, 1965, 1801.

[HBP17] D.R. Heath-Brown and L. B. Pierce. Averages and moments associated to class numbers of imaginary quadratic fields. *Compositio Math. (to appear)*, 2017.

[Hou] R. Hough. Average equidistribution of Heegner points associated to the 3-part of the class group of imaginary quadratic fields. *arXiv:1005.1458v2*.

[Hua82] L.-K. Hua. *Introduction to Number Theory*. Springer–Verlag, Berlin–New York, 1982.

[HV06] H. A. Helfgott and A. Venkatesh. Integral points on elliptic curves and 3-torsion in class groups. *J. Amer. Math. Soc.*, 19(3):527–550, 2006.

[Kly16] Jack Klys. The Distribution of p-Torsion in Degree p Cyclic Fields. *arXiv:1610.00226 [math]*, October 2016.

[LO75] J. Lagarias and A. Odlyzko. *Effective versions of the Chebotarev density theorem*, pages 409–464. Proc. Sympos., Univ. Durham, Durham, 1975.

[Mil15] Djordjo Milovic. On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-8p})$ for $p \equiv -1 \pmod 4$. *arXiv:1511.07127*, 2015.

[Nar80] W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers*. Springer-Verlag, Berlin, 1980.

[OT14] R. Lemke Oliver and F. Thorne. The number of ramified primes in number fields of small degree. *arXiv:1408.1018v2*, 2014.

[Pap05] F. Pappalardi. A survey on k-freeness. In *Number Theory*, volume 1 of *Ramanujan Math. Soc. Lect. Notes Ser.*, pages 71–88. Ramanujan Math. Soc., 2005.

[Pie05] L. B. Pierce. The 3-part of class numbers of quadratic fields. *J. London Math. Soc.*, 71:579–598, 2005.

[Pie06] L. B. Pierce. A bound for the 3-part of class numbers of quadratic fields by means of the square sieve. *Forum Math.*, 18:677–698, 2006.

[Smi16] Alexander Smith. Governing fields and statistics for 4-Selmer groups and 8-class groups. *arXiv:1607.07860 [math]*, July 2016.

[Sou00] K. Soundararajan. Divisibility of class numbers of imaginary quadratic fields. *J. London Math. Soc. (2)*, 61(3):681–690, 2000.

[SST15a] Peter Sarnak, Sug-Woo Shin, and Nicolas Templier. Families of L-functions and their symmetry. *arXiv:1401.5507v2*, 2015.

[SST15b] Arul Shankar, Anders Södergren, and Nicolas Templier. Low-lying zeros of certain families of Artin L-functions. *arXiv:1507.07031v1*, 2015.

[ST14] A. Shankar and J. Tsimerman. Counting S_5-fields with a power saving error term. *Forum of Mathematics, Sigma*, 2, 2014.

[TT13] T. Taniguchi and F. Thorne. The secondary term in the counting function for cubic fields. *Duke Mathematical Journal*, 162:2451–2508, 2013.

[Won99a] S. Wong. Automorphic forms on GL(2) and the rank of class groups. *J. Reine Angew. Math.*, 515:125–153, 1999.

[Won99b] S. Wong. On the rank of ideal class groups. *Proc. Fourth Canad. Number Theory Conf.*, pages 377–383, 1999.

[Woo10] Melanie Matchett Wood. On the probabilities of local behaviors in abelian field extensions. *Compos. Math.*, 146(1):102–128, 2010.

[Wri89] David J. Wright. Distribution of discriminants of abelian extensions. *Proc. London Math. Soc. (3)*, 58(1):17–50, 1989.

[Yan09] A. Yang. *Distribution problems associated to zeta functions and invariant theory*. ProQuest LLC, Ann Arbor, MI, 2009. Thesis (Ph.D.)–Princeton University.

[Zha05] S.-W. Zhang. Equidistribution of CM-points on quaternion Shimura varieties. *Int. Math. Res. Not.*, (59):3657–3689, 2005.

Department of Mathematics, 480 Lincoln Dr., Madison, WI 53706 USA
E-mail address: ellenber@math.wisc.edu

Department of Mathematics, Duke University, 120 Science Drive, Durham NC 27708
E-mail address: pierce@math.duke.edu

Department of Mathematics, 480 Lincoln Dr., Madison, WI 53706 USA, and American Institute of Mathematics, 600 East Brokaw Road, San Jose, CA 95112 USA
E-mail address: mmwood@math.wisc.edu