BOUNDS FOR THE ℓ-TORSION IN CLASS GROUPS

MARTIN WIDMER

ABSTRACT. We prove for each integer $\ell \geq 1$ an unconditional upper bound for the size of the ℓ-torsion subgroup $Cl_K[\ell]$ of the class group of K, which holds for all but a zero density set of number fields K of degree $d \in \{4, 5\}$ (with the additional restriction in the case $d = 4$ that the field be non-D_4). For sufficiently large ℓ this improves recent results of Ellenberg, Matchett Wood, and Pierce, and is also stronger than the best currently known pointwise bounds under GRH. Conditional on GRH and on a weak conjecture on the distribution of number fields our bounds also hold for arbitrary degrees d.

1. INTRODUCTION

In this article we prove for each integer $\ell \geq 1$ an unconditional upper bound for the size of the ℓ-torsion subgroup $Cl_K[\ell]$ of the class group of K, which holds for all but a zero density set of number fields K of degree $d \in \{4, 5\}$ (with the additional restriction in the case $d = 4$ that the field be non-D_4). For sufficiently large ℓ these results improve results of Ellenberg, Matchett Wood, and Pierce [12], and are also stronger than the best currently known pointwise bounds assuming GRH due to Ellenberg and Venkatesh [11]. Conditional on GRH and on a weak conjecture on the distribution of number fields our bounds also hold for arbitrary degrees d.

We always assume $X \geq 2$, and that ℓ is a positive integer. We shall use the $O(\cdot)$, $\ll$, and $\gg$ notation; throughout the implied constants will depend only on the indicated parameters. Denote the modulus of the discriminant of the number field K by D_K, and its degree $[K : \mathbb{Q}]$ by d.

Bounding $\#Cl_K[\ell]$ by the size of the full class group, and using a classical bound (see, e.g., [16, Thm 4.4]) yields the trivial bound[1]

$$\#Cl_K[\ell] \ll_{d,\varepsilon} D_K^{1/2+\varepsilon}. \tag{1.1}$$

While it is conjectured (see, e.g., [11, Conjecture 1.1], [9, Section 3] and [25]) that

$$\#Cl_K[\ell] \ll_{d,\ell,\varepsilon} D_K^{\varepsilon},$$

unconditional nontrivial bounds that hold for all number fields of degree d are known only for $\ell = 2$, and for $d \leq 4$ and $\ell = 3$. For $d = \ell = 2$ the conjecture follows from Gauss' genus theory, whereas for $(d, \ell) = (2, 3)$ the first nontrivial bounds were obtained by Pierce [17, 18], and Helfgott and Venkatesh [14]. Currently the best bound is

$$\#Cl_K[3] \ll_{\varepsilon} D_K^{1/3+\varepsilon}$$

due to Ellenberg and Venkatesh [11] which holds also for cubic fields. Moreover, they established a nontrivial bound for quartic fields (with, e.g., an exponent $83/168 + \varepsilon$

Date: October 9, 2017, and in revised form ....

1991 *Mathematics Subject Classification.* Primary 11R29, 11R65, 11R45; Secondary 11G50.

Key words and phrases. ℓ-torsion, class group, number fields, small height.

[1]As usual ε denotes an arbitrarily small positive number.

provided K is an S_4 or A_4-field). Another, very recent, breakthrough due to Bhargava, Shankar, Taniguchi, Thorne, Tsimerman, and Zhao [3] provides for arbitrary d the bound

$$\#Cl_K[2] \ll_{d,\varepsilon} D_K^{1/2-1/(2d)+\varepsilon},$$

and for $d \in \{3,4\}$ they can even take the exponent 0.2784.

Regarding general ℓ there are only conditional results, assuming GRH. The latter is used to guarantee the existence of many small splitting primes; the idea of using these to investigate torsion in class groups has been around for a while, see, e.g., [6, 22]. However, Ellenberg and Venkatesh [11] have greatly extended this strategy, and proved the first (although conditional on GRH) nontrivial general upper bound

$$\#Cl_K[\ell] \ll_{d,\ell,\varepsilon} D_K^{1/2-1/(2\ell(d-1))+\varepsilon}. \tag{1.2}$$

So much for pointwise bounds; regarding results on the average Davenport and Heilbronn [8] showed that

$$\sum_{\substack{[K:\mathbb{Q}]=2\\ D_K\le X}} \#Cl_K[3] \sim 5/(3\zeta(2))X,$$

and Bhargava [1] established the asymptotics for 2-torsion in cubic fields

$$\sum_{\substack{[K:\mathbb{Q}]=3\\ D_K\le X}} \#Cl_K[2] \sim 23/(16\zeta(3))X.$$

No other asymptotics are known but Heath-Brown and Pierce [13] proved that for primes $\ell \ge 5$

$$\sum_{\substack{[K:\mathbb{Q}]\le 2\\ D_K\le X}}{}' \#Cl_K[\ell] \ll_{\ell,\varepsilon} X^{3/2-3/(2\ell+2)+\varepsilon},$$

where the apostrophe indicates that the sum is restricted to imaginary quadratic fields. Recently Ellenberg, Matchett Wood, and Pierce [12, Corollary 1.1.1 and 1.1.2] established the first nontrivial unconditional average bounds for arbitrary ℓ.

Corollary 1.1 (Ellenberg, Matchett Wood, and Pierce)**.** *Suppose $d \in \{2,3,4,5\}$, $\ell(2) = \ell(3) = 1$, $\ell(4) = 8$, $\ell(5) = 25$, and $\varepsilon > 0$. As K ranges over degree d number fields with $D_K \le X$ (and non-D_4 in the case $d = 4$), we have*

$$\sum_K \#Cl_K[\ell] \ll_{\ell,\varepsilon} X^{3/2-1/(2\ell(d-1))+\varepsilon}$$

if $\ell \ge \ell(d)$, and we have

$$\sum_K \#Cl_K[\ell] \ll_{\ell,\varepsilon} X^{3/2-\delta_0(d)+\varepsilon}$$

if $\ell < \ell(d)$, where $\delta_0(4) = 1/48$ and $\delta_0(5) = 1/200$.

Corollary 1.1 is an immediate consequence of their main result [12, Theorem 1.1] (see Theorem 1.2 below) which is *unconditional*, and gives upper bounds of the same size as the conditional result (1.2) outside a family of density zero, provided $d \le 5$ and ℓ is sufficiently large. To state their result in a uniform way we additionally set $\delta_0(2) = \delta_0(3) = 1$.

Theorem 1.2 (Ellenberg, Matchett Wood, and Pierce)**.** *Suppose $d \in \{2,3,4,5\}$, and $\varepsilon > 0$. Then for all but $O_{\ell,\varepsilon}(X^{1-\min\{1/(2\ell(d-1)),\delta_0(d)\}+\varepsilon})$ degree d number fields K with $D_K \le X$ (and non$-D_4$ when $d = 4$) we have*

$$\#Cl_K[\ell] \ll_{\ell,\varepsilon} D_K^{1/2-\min\{1/(2\ell(d-1)),\delta_0(d)\}+\varepsilon}.$$

Very roughly speaking, Ellenberg, Matchett Wood, and Pierce's strategy is to show that "most fields" have sufficiently many small splitting primes, and then to apply the general strategy of Ellenberg and Venkatesh (see Proposition 2.1 in Section 2). We follow this approach but combine it with a new idea, showing that for "most" number fields the smallest height of a primitive element is significantly bigger than in the worst case scenario, at least[2] when $d \geq 4$. Therefore, our main result improves (see Corollary 1.4) the quartic and quintic case of Theorem 1.2 and consequently Corollary 1.1 (see Corollary 1.5).

Theorem 1.3. *Suppose $d \in \{4,5\}$, $0 < \gamma \leq 1/(d+1)$, and $\varepsilon > 0$. Then for all but $O_{\ell,\gamma,\varepsilon}(X^{1-\min\{\gamma/\ell,\delta_0(d)\}+\varepsilon} + X^{\gamma(d+1)})$ degree d number fields K with $D_K \leq X$ (and non$-D_4$ when $d = 4$) we have*

$$\#Cl_K[\ell] \ll_{\ell,\gamma,\varepsilon} D_K^{1/2-\min\{\gamma/\ell,\delta_0(d)\}+\varepsilon}.$$

We set $\ell_4 = 10$ and $\ell_5 = 34$. With $\gamma = \ell/(\ell(d+1)+1)$ if $\ell \geq \ell_d$ and $\gamma = (1-\delta_0(d))(d+1)$ otherwise we have $1 - \min\{\gamma/\ell, \delta_0(d)\} = \gamma(d+1)$, and hence Theorem 1.3 yields immediately the following corollary which improves the quartic and quintic case of the main result [12, Theorem 1.1] when $\ell > 7$ ($d = 4$) and $\ell > 24$ ($d = 5$) respectively.

Corollary 1.4. *Suppose $d \in \{4,5\}$, and $\varepsilon > 0$. If $\ell \geq \ell_d$ then for all but $O_{\ell,\varepsilon}(X^{1-1/(\ell(d+1)+1)+\varepsilon})$ degree d number fields K with $D_K \leq X$ (and non$-D_4$ when $d = 4$) we have*

$$\#Cl_K[\ell] \ll_{\ell,\varepsilon} D_K^{1/2-1/(\ell(d+1)+1)+\varepsilon}.$$

If $\ell < \ell_d$ then for all but $O_{\ell,\varepsilon}(X^{1-\delta_0(d)+\varepsilon})$ degree d number fields K with $D_K \leq X$ (and non$-D_4$ when $d = 4$) we have

$$\#Cl_K[\ell] \ll_{\ell,\varepsilon} D_K^{1/2-\delta_0(d)+\varepsilon}.$$

Corollary 1.4 and dyadic summation, using the trivial bound (1.1) for the exceptional fields, yields our next result which improves the quartic and quintic case of [12, Corollary 1.1.1].

Corollary 1.5. *Suppose $d \in \{4,5\}$, and $\varepsilon > 0$. As K ranges over degree d number fields with $D_K \leq X$ (and non-D_4 in the case $d = 4$), we have*

$$\sum_K \#Cl_K[\ell] \ll_{\ell,\varepsilon} X^{3/2-1/(\ell(d+1)+1)+\varepsilon}$$

if $\ell \geq \ell_d$, and we have

$$\sum_K \#Cl_K[\ell] \ll_{\ell,\varepsilon} X^{3/2-\delta_0(d)+\varepsilon}$$

if $\ell < \ell_d$.

Bhargava [1, 2] proved that the conjectured asymptotics $c_d X$ for the number of degree d fields K with $D_K \leq X$ holds true for $d \in \{4,5\}$, and in the case $d = 4$ also (with a different positive constant) when restricting to non-D_4 fields. Thus, applying Theorem 1.3 with $\gamma = 1/(d+1) - \varepsilon$ we get the following corollary.

Corollary 1.6. *Suppose $d \in \{4,5\}$, and $\varepsilon > 0$. If $\ell \geq \ell_d$ then for 100% of non-D_4 degree d fields (when enumerated by modulus of the discriminant) we have*

$$\#Cl_K[\ell] \ll_{\ell,\varepsilon} D_K^{1/2-1/(\ell(d+1))+\varepsilon}.$$

[2]Actually, we do not know whether for "most" cubic fields the smallest generator is significantly bigger than in the worst case scenario, but Ruppert [20, Proposition 2] has shown that this is definitely not the case for quadratic fields. Consequently, we only get an improvement if $d \geq 4$ although Theorem 1.3 and its proof remain valid for $d \in \{2,3\}$.

Moreover, if $1 \leq \ell < \ell_d$ *then for* 100% *of non-*D_4 *degree* d *fields we have*

$$\#Cl_K[\ell] \ll_\varepsilon D_K^{1/2-\delta_0(d)+\varepsilon}.$$

We now turn to more general but conditional results.

Theorem 1.7. *Suppose* $m \mid d$, F *is a number field of degree* m, *and* $\varepsilon > 0$. *Assume GRH, and additionally that there are* $\gg_{F,d} X$ *number fields* K *of degree* d *with* $D_K \leq X$, *and containing* F. *Then for* 100% *of degree* d *fields* K *containing* F *we have*

$$\#Cl_K[\ell] \ll_{d,\ell,\varepsilon} D_K^{1/2-m/(\ell(m+d))+\varepsilon}.$$

So here we get an exponent which depends only on d/m (the degree of K/F) but is independent of the degree of $K/\mathbb{Q}$. The proof of Theorem 1.7 actually provides a more precise quantitative result analogous to Theorem 1.3.

Datskovsky and Wright [7, Theorem 4.2 and Theorem 1.1] have shown that there are $\gg_{F,d} X$ number fields K of degree d with $D_K \leq X$, and containing F, provided $2 \leq d/m \leq 3$, and recent work of Bhargava, Shankar, and Wang [4, Theorem 1.1] implies that this holds even for $2 \leq d/m \leq 5$. Hence, we get the following corollary.

Corollary 1.8. *Suppose* $m \mid d$, $2 \leq d/m \leq 5$, F *is a number field of degree* m, *and* $\varepsilon > 0$. *Assume GRH. Then for* 100% *of degree* d *fields* K *containing* F *we have*

$$\#Cl_K[\ell] \ll_{d,\ell,\varepsilon} D_K^{1/2-m/(\ell(m+d))+\varepsilon}.$$

2. Ellenberg and Venkatesh's Key Lemma

Let

$$H_K(\alpha) = \prod_{v \in M_K} \max\{1, |\alpha|_v\}^{d_v}$$

be the relative multiplicative Weil height of $\alpha \in K$. Here M_K denotes the set of places of K, and for each place v we choose the unique representative $|\cdot|_v$ that either extends the usual Archimedean absolute value on $\mathbb{Q}$ or a usual p-adic absolute value on $\mathbb{Q}$, and $d_v = [K_v : \mathbb{Q}_v]$ denotes the local degree at v. Note that this is exactly the height in [11, (2.2)] for the principal divisor $(\alpha, (\alpha))$ associated to $\alpha \in K^\times$. We also use the following invariant

$$\eta(K) = \inf\{H_K(\alpha); K = \mathbb{Q}(\alpha)\},$$

introduced by Roy and Thunder [19], and also studied[3] in [23, 24]. First we use the fact that the proof of the key lemma [11, Lemma 2.3] of Ellenberg and Venkatesh proves actually the following stronger statement. Recall from [11] that a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is said to be an extension of a prime ideal from a subfield $K_0 \subsetneq K$ if there exists a prime ideal $\mathfrak{p}_0$ of $\mathcal{O}_{K_0}$ such that $\mathfrak{p} = \mathfrak{p}_0 \mathcal{O}_K$. If $\mathfrak{p}$ and $\mathfrak{p}_0$ are non-zero prime ideals in $\mathcal{O}_K$ and $\mathcal{O}_{K_0}$ respectively and $\mathfrak{p} \mid \mathfrak{p}_0 \mathcal{O}_K$ then we say $\mathfrak{p}$ is unramified in K/K_0 if $\mathfrak{p}^2 \nmid \mathfrak{p}_0 \mathcal{O}_K$.

Proposition 2.1 (Ellenberg and Venkatesh)**.** *Suppose* K *is a number field of degree* d, $\eta(K) > D_K^\gamma$, $\delta < \gamma/\ell$, *and* $\varepsilon > 0$. *Moreover, suppose* $\mathfrak{p}_1, \dots, \mathfrak{p}_M$ *are* M *prime ideals in* $\mathcal{O}_K$ *of norm* $N(\mathfrak{p}_i) \leq D_K^\delta$ *that are unramified in* $K/\mathbb{Q}$ *and are not extensions of prime ideals from any proper subfield of* K. *Then we have*

$$\#Cl_K[\ell] \ll_{d,\ell,\gamma,\varepsilon} D_K^{1/2+\varepsilon} M^{-1}.$$

Proof. Exactly as in [11, Lemma 2.3] with $K_0 = \mathbb{Q}$ except that we replace their Lemma 2.2 by the hypothesis $\eta(K) > D_K^\gamma$. □

[3] In the cited works the author used the absolute instead of the relative height, and denoted the invariant by $\delta(K)$.

Ellenberg [10, Proposition 1] pointed out that the proof of [11, Lemma 2.3] even provides the stronger conclusion $\#Cl_K[\ell] \ll_{d,\ell,\varepsilon} D_K^{1/2+\varepsilon} M_K$, where $M_K := \inf_T(T^{-1/\ell}(1 + N'_K(T)))$, and $N'_K(T)$ denotes the number of primitive elements in K of (relative) height at most T.

3. The main proposition

Let $d > 1$ be an integer. We set

$$S_{\mathbb{Q},d} = \{K \subset \overline{\mathbb{Q}}; [K : \mathbb{Q}] = d\} \tag{3.1}$$

for the collection of all number fields of degree d. For a subset $S \subset S_{\mathbb{Q},d}$ we set

$$\begin{aligned}\mathscr{B}_S(X; Y, M) &:= \{K \in S; D_K \le X, \text{ at most } M \text{ primes } p \le Y \text{ split completely in } K\},\\ P_S &:= \{\alpha \in \overline{\mathbb{Q}}; \mathbb{Q}(\alpha) \in S\},\\ N_H(P_S, X) &:= \#\{\alpha \in P_S; H_{\mathbb{Q}(\alpha)}(\alpha) \le X\}.\end{aligned}$$

We can now formulate our main proposition. The setup is streamlined for our application, and the role of $\tilde{\delta}_0$ will become clear in Section 4.

Proposition 3.1. *Suppose $S \subset S_{\mathbb{Q},d}$ and $\theta > 0$ are such that*

$$N_H(P_S, X) \ll_{S,\theta} X^\theta.$$

Let $\gamma > 0$, $\varepsilon > 0$, $\tilde{\delta}_0 > 0$, $\delta_0 := \min\{\gamma/\ell - 2\varepsilon, \tilde{\delta}_0\}$, and $E_{\delta_0,\varepsilon}(\cdot)$ be an increasing function such that

$$\mathscr{B}_S(X; X^{\delta_0}, X^{\delta_0-\varepsilon}) \le E_{\delta_0,\varepsilon}(X).$$

Then we have

$$\#Cl_K[\ell] \ll_{d,\ell,\gamma,\varepsilon} D_K^{1/2-\delta_0+2\varepsilon}$$

for all but $O_{S,\theta}((\log X)E_{\delta_0,\varepsilon}(X) + X^{\gamma\theta})$ fields K in S with $D_K \le X$.

Proof. We set $\kappa_i = \log_2 X - [\log_2 X] + i$, and for $1 \le i \le [\log_2 X]$

$$D_{\delta_0,\gamma}(i) = \{K \in S; 2^{\kappa_i - 1} < D_K \le 2^{\kappa_i}, \eta(K) > D_K^\gamma, K \notin \mathscr{B}_S(2^{\kappa_i}; 2^{\kappa_i\delta_0}, 2^{\kappa_i(\delta_0-\varepsilon)})\}.$$

By Hermite's Theorem the inequality (3.2) below trivially holds true for all $K \in S$ with $D_K \le 2^{\delta_0/\varepsilon}$; so let's assume $D_K > 2^{\delta_0/\varepsilon}$. Note that for $K \in D_{\delta_0,\gamma}(i)$ there exist $\ge D_K^{\delta_0-\varepsilon}$ primes $p \le (2D_K)^{\delta_0} < D_K^{\delta_0+\varepsilon}$ that split completely in K. Since $\delta_0 + \varepsilon < \gamma/\ell$ we can apply Proposition 2.1 with $\delta = \delta_0 + \varepsilon$ and $M = \lceil D_K^{\delta_0-\varepsilon} \rceil$. Hence, we have shown that

$$\#Cl_K[\ell] \ll_{d,\ell,\gamma,\varepsilon} D_K^{1/2-\delta_0+2\varepsilon} \tag{3.2}$$

for all $K \in \cup_i D_{\delta_0,\gamma}(i)$. Next, we note that

$$\begin{aligned}&\#\cup_i D_{\delta_0,\gamma}(i)\\ &\ge \#\{K \in S; D_K \le X\} - \sum_i \#\mathscr{B}_S(2^{\kappa_i}; 2^{\kappa_i\delta_0}, 2^{\kappa_i(\delta_0-\varepsilon)}) - \#\{K \in S; D_K \le X, \eta(K) \le D_K^\gamma\}.\end{aligned}$$

By hypothesis $\#\mathscr{B}_S(2^{\kappa_i}; 2^{\kappa_i\delta_0}, 2^{\kappa_i(\delta_0-\varepsilon)}) \le E_{\delta_0,\varepsilon}(2^{\kappa_i})$, and since $2^{\kappa_i} \le X$ we conclude

$$\sum_i \#\mathscr{B}_S(2^{\kappa_i}; 2^{\kappa_i\delta_0}, 2^{\kappa_i(\delta_0-\varepsilon)}) \le (\log_2 X)E_{\delta_0,\varepsilon}(X).$$

Finally, we observe that the image of the map $\alpha \to \mathbb{Q}(\alpha)$ with domain

$$\{\alpha \in P_S; H_{\mathbb{Q}(\alpha)}(\alpha) \le X^\gamma\}$$

covers the set

$$\{K \in S; D_K \le X, \eta(K) \le D_K^\gamma\},$$

and using the hypothesis we conclude that

$$\#\{K \in S; D_K \le X, \eta(K) \le D_K^{\gamma}\} \le N_H(P_S, X^{\gamma}) \ll_{S,\theta} X^{\gamma\theta}.$$

Hence, we have shown that for all but $O_{S,\theta}((\log X)E_{\delta_0,\varepsilon}(X) + X^{\gamma\theta})$ fields K in S with $D_K \le X$ we have $\#Cl_K[\ell] \ll_{d,\ell,\gamma,\varepsilon} D_K^{1/2-\delta_0+2\varepsilon}$. □

4. Proofs of the Theorems

4.1. **Upper bounds for $N_H(P_S, X)$.** Let F be a number field of degree $m \mid d$, and define

$$S_{F,d} := \{K \subseteq \overline{\mathbb{Q}}; [K:\mathbb{Q}] = d, F \subseteq K\}.$$

Applying Schmidt's [21, Theorem] with Schmidt's (K, k, d, n) replaced by our $(F, m, d/m, 1)$ shows that the number of $P = (1:\alpha) \in \mathbb{P}^1(\overline{\mathbb{Q}})$ with $[F(\alpha):F] = d/m$ and $H_F(P) \le X$ (for Schmidt's projective field height [21, (1.2)]) is $\ll_{m,d} X^{d/m+1}$. Since $H_F(P) = H_{F(\alpha)}(\alpha)$ we conclude that

$$\#\{\alpha \in \overline{\mathbb{Q}}; [F(\alpha):F] = d/m, H_{F(\alpha)}(\alpha) \le X\} \ll_{m,d} X^{d/m+1}.$$

Note that if $\alpha \in P_{S_{F,d}}$ then $[F(\alpha):F] = d/m$ and $\mathbb{Q}(\alpha) = F(\alpha)$ so that $H_{\mathbb{Q}(\alpha)}(\alpha) = H_{F(\alpha)}(\alpha)$. Therefore,

$$N_H(P_{S_{F,d}}, X) \ll_{m,d} X^{d/m+1}. \tag{4.1}$$

4.2. **Proof of Theorem 1.3.** Let $S^*_{\mathbb{Q},4}$, the set of all non-D_4 number fields of degree 4. We apply Proposition 3.1 with $S = S^*_{\mathbb{Q},4}$ if $d = 4$, and with $S = S_{\mathbb{Q},5}$ if $d = 5$. As explained in Section 4.1 we can take $\theta = d+1$. Let $\varepsilon > 0$, and set $\tilde{\delta}_0 := \delta_0(d)$ so that $\delta_0 = \min\{\gamma/\ell - 2\varepsilon, \delta_0(d)\}$. By [12, Proposition 6.1] and [12, Theorems 2.2 and Theorem 2.3] we have[4] (cf. [12, Proposition 7.1])

$$\#\mathscr{B}_S(X; X^{\delta_0}, \frac{c_0(d)}{2} X^{\delta_0}(\log X^{\delta_0})^{-1}) \ll_{\varepsilon} X^{1-\delta_0+\varepsilon},$$

provided X is sufficiently large in terms of δ_0. Hence,

$$\#\mathscr{B}_S(X; X^{\delta_0}, X^{\delta_0-\varepsilon}) \ll_{\ell,\gamma,\varepsilon} X^{1-\delta_0+\varepsilon}.$$

Thus we can take $E_{\delta_0,\varepsilon}(X) = C_{\ell,\gamma,\varepsilon} X^{1-\delta_0+\varepsilon}$ for a sufficiently large constant $C_{\ell,\gamma,\varepsilon}$. We conclude from Proposition 3.1 that for all but $O_{\ell,\gamma,\varepsilon}(X^{1-\delta_0+2\varepsilon} + X^{\gamma(d+1)})$ fields $K \in S$ with $D_K \le X$ we have $\#Cl_K[\ell] \ll_{\ell,\gamma,\varepsilon} D_K^{1/2-\delta_0+2\varepsilon}$. Since $\delta_0 \ge \min\{\gamma/\ell, \delta_0(d)\} - 2\varepsilon$ and $\varepsilon > 0$ was arbitrary the statement of Theorem 1.3 follows.

4.3. **Proof of Theorem 1.7.** We will apply Proposition 3.1 with $S = S_{F,d}$. From Section 4.1 we know that we can take $\theta = d/m + 1$. Let $0 < \varepsilon < m/(3\ell(d+m))$, choose $\tilde{\delta}_0 = 1$ and $\gamma = m/(d+m) - \ell\varepsilon$, so that $\delta_0 = \min\{\gamma/\ell - 2\varepsilon, \tilde{\delta}_0\} = m/(\ell(d+m)) - 3\varepsilon > 0$. Since we assume GRH we can apply Lagarias and Odlyzko's effective Chebotarev density Theorem [15] to the normal closure of $K \in S$ to deduce[5] that for every $K \in S$ the number of primes $p \le Y$ that split completely in K is $> Y^{1-\varepsilon'}$, provided $Y \ge (\log D_K)^2$ and $Y \ge Y_0(F, d, \varepsilon')$. Setting $Y = X^{\delta_0-\varepsilon}$ and $\varepsilon' = \varepsilon/\delta_0$ we conclude that for all X large enough the set $\mathscr{B}_S(X; Y, Y^{1-\varepsilon'})$ is empty, and hence we have for all $X \ge 2$

$$\#\mathscr{B}_S(X; X^{\delta_0}, X^{\delta_0-\varepsilon}) \ll_{F,d,\ell,\varepsilon} 1.$$

Now we can apply Proposition 3.1 to conclude that for all but $O_{F,d,\ell,\varepsilon}(X^{1-\ell\varepsilon(d+m)/m})$ fields K of degree d with $D_K \le X$ and containing F we have $\#Cl_K[\ell] \ll_{d,\ell,\varepsilon} D_K^{1/2-m/(\ell(d+m))+5\varepsilon}$.

[4] Here , as in [12, Proposition 7.1], $c_0(d)$ denotes a positive constant depending only on d.

[5] We use that the degree of the normal closure L of K is at most $d!$ and that $\log D_L \le 2(d!)^2 \log D_K$ since each prime that ramifies in L must ramify in K, and the order to which a rational prime divides D_L is bounded from above by $2[L:\mathbb{Q}]^2$ (cf. [5, Theorem B.2.12.]).

By hypothesis there are $\gg_{F,d} X$ number fields K of degree d with $D_K \leq X$, and containing F. Since $\varepsilon > 0$ was arbitrarily small the statement of Theorem 1.7 follows.

Acknowledgments

I would like to thank the referees for carefully reading the manuscript and for useful remarks.

References

1. M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. **162** (2005), 1031–1063.
2. ———, *The density of discriminants of quintic rings and fields*, Ann. of Math. **172** (2010), 1559–1591.
3. M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, and Y. Zhao, *Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves* , arXiv:1701.02458v1 (2017), 12 pp.
4. M. Bhargava, A. Shankar, and X. Wang, *Geometry-of-numbers methods over global fields I: Prehomogeneous vector spaces*, arXiv:1512.03035 (2016), 27 pp.
5. E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, 2006.
6. D. Boyd and H. Kisilevsky, *On the exponent of the ideal class groups of complex quadratic fields*, Proc. Amer. Math. Soc. **31** (1972), 433–436.
7. B. Datskovsky and D. J. Wright, *Density of discriminants of cubic field extensions*, J. reine angew. Math. **386** (1988), 116–138.
8. H. Davenport and H. Heilbronn, *On the density of discriminants of cubic field extensions. II*, Proc. London. Math. Soc. **322** (1971), 405–420.
9. W. Duke, *Bounds for arithmetic multiplicities*, Proceedings of the International Congress of Mathematicians. Berlin, 1998.
10. J. Ellenberg, *Points of low height on $\mathbb{P}^1$ over number fields and bounds for torsion in class groups*, Computational arithmetic geometry, Contemp. Math., Amer. Math. Soc. **463** (2008), 45–48.
11. J. Ellenberg and A. Venkatesh, *Reflection principles and bounds for class group torsion*, Int. Math. Res. Not. **no.1, Art. ID rnm002** (2007).
12. J. Ellenberg, M. Matchett Wood, and L. B. Pierce, *On ℓ-torsion in class groups of number fields*, arXiv:1606.06103v1 [math.NT] (2016), 25 pp.
13. D. R. Heath-Brown and L. B. Pierce, *Averages and moments associated to class numbers of imaginary quadratic fields*, arXiv:1409.3177v1 (2014), 25 pp.
14. H. A. Helfgott and A. Venkatesh, *Integral points on elliptic curves and 3-torsion in class groups*, J. Amer. Math. Soc. **19** (2006), 527–550.
15. J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem. Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), pp. 409-464*, Academic Press Inc., New York, 1977.
16. W. Narkiewicz, *Elementary and analytic theory of algebrac numbers*, Springer, 1990.
17. L. B. Pierce, *3-part of class numbers of quadratic fields*, J. London Math. Soc. **71** (2005), 579–598.
18. ———, *A bound for the 3-part of class numbers of quadratic fields by means of the square sieve*, Forum Math. **18** (2006), 677–698.
19. D. Roy and J. L. Thunder, *A note on Siegel's lemma over number fields*, Monatsh. Math. **120** (1995), 307–318.
20. W. Ruppert, *Small generators of number fields*, Manuscripta math. **96** (1998), 17–22.
21. W. M. Schmidt, *Northcott's Theorem on heights I. A general estimate*, Monatsh. Math. **115** (1993), 169–183.
22. K. Soundararajan, *Divisibility of class numbers of imaginary quadratic fields*, J. London Math. Soc. **61, no.3** (2000), 681–690.
23. J. D. Vaaler and M. Widmer, *A note on small generators of number fields*, Diophantine Methods, Lattices, and Arithmetic Theory of Quadratic Forms, Contemporary Mathematics, vol. 587, Amer. Math. Soc., Providence, RI, 2013.
24. ———, *Number fields without small generators*, Math. Proc. Cam. Philos. Soc. **159, no. 3** (2015), 379–385.
25. S.-W. Zhang, *Equidistribution of CM-points on quaternion Shimura varieties*, Int. Math. Res. Not. **59** (2005), 3657–3689.

Department of Mathematics, Royal Holloway, University of London, TW20 0EX Egham, UK

E-mail address: martin.widmer@rhul.ac.uk