AVERAGE BOUNDS FOR THE ℓ-TORSION IN CLASS GROUPS OF CYCLIC EXTENSIONS

CHRISTOPHER FREI AND MARTIN WIDMER

Dedicated to Professor Robert F. Tichy on the occasion of his 60th birthday.

ABSTRACT. For all positive integers ℓ, we prove non-trivial bounds for the ℓ-torsion in the class group of K, which hold for almost all number fields K in certain families of cyclic extensions of arbitrarily large degree. In particular, such bounds hold for almost all cyclic degree-p-extensions of F, where F is an arbitrary number field and p is any prime for which F and the p-th cyclotomic field are linearly disjoint. Along the way, we prove precise asymptotic counting results for the fields of bounded discriminant in our families with prescribed splitting behavior at finitely many primes.

Contents

1. INTRODUCTION

Let F be a number field with ring of integers $\mathscr{O}_F$ and algebraic closure $\overline{F}$. Let $n > 1$ be an integer such that F and $\mathbb{Q}(\mu_n(\overline{F}))$ are linearly disjoint over $\mathbb{Q}$, where $\mu_n(\overline{F})$ is the group of n-th roots of unity in $\overline{F}$. In this paper, we consider the family $\mathscr{T}_{F,n}$ of Galois extensions $K \subseteq \overline{F}$ of F with cyclic Galois group of order n that satisfy the following condition:

> every prime ideal of $\mathscr{O}_F$ not dividing n is either unramified or totally ramified in K.

This condition is vacuous if n is prime, so in this case $\mathscr{T}_{F,n}$ is the family of all cyclic degree-n-extensions of F. We prove for each integer $\ell \geq 1$ an unconditional non-trivial 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 fields $K \in \mathscr{T}_{F,n}$. The case $n = 2$ over the ground field $F = \mathbb{Q}$ has been proven recently by Ellenberg, Pierce, and Wood [6].

1.1. **Background.** We always assume $X \geq 2$, and that ℓ is a positive integer. We shall use the $O(\cdot)$, $\ll$, and $\gg$ notation; unless explicitly stated otherwise, 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 [12, Thm 4.4] yields the trivial bound[1]

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

valid for all number fields K and positive integers ℓ. A widely open conjecture (see, e.g., [7, Conjecture 1.1], [5, Section 3] and [28]) states that

$$(1.2) \qquad\qquad \#Cl_K[\ell] \ll_{d,\ell,\varepsilon} D_K^{\varepsilon}.$$

For $d = \ell = 2$ the conjecture follows from Gauss' genus theory but unconditional non-trivial 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 $(d, \ell) = (2, 3)$ the first non-trivial bounds were obtained by Pierce [13, 14], and Helfgott and Venkatesh [10]. Currently the record is Ellenberg and Venkatesh's [7] bound

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

which holds also for cubic fields. They also established a non-trivial bound for quartic fields (with, e.g., an exponent $83/168+\varepsilon$ provided K is an S_4 or A_4-field). More recently Bhargava, Shankar, Taniguchi, Thorne, Tsimerman, and Zhao [1] showed 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 (consequently giving the new world record upper bound for the number of A_4-extensions of bounded discriminant). Their method is entirely different and based on geometry of numbers, but unfortunately seems not to extend to any $\ell > 2$. The most general non-trivial bound is due to Ellenberg and Venkatesh [7, Proposition 3.1] and states

$$(1.3) \qquad\qquad \#Cl_K[\ell] \ll_{d,\ell,\varepsilon} D_K^{1/2-1/(2\ell(d-1))+\varepsilon}.$$

This bound holds for all number fields K and all ℓ but unfortunately is conditional on GRH. More generally, if F is an arbitrary number field and K/F is an extension of degree n then, assuming GRH, [7, Lemma 2.3] provides the upper bound $\#Cl_K[\ell] \ll_{F,n,\ell,\varepsilon} D_K^{1/2-1/(2\ell(n-1))+\varepsilon}$; in the sequel we shall refer to this as the "GRH-bound".

It is worthwhile mentioning that the Cohen-Lenstra heuristics (and their generalisations to arbitrary number fields by Cohen and Martinet [4]) predict the bound (1.2) but only for almost all fields K of degree d and certain "good" primes ℓ. In this direction Ellenberg, Pierce and Wood [6] have shown that the above GRH-bound (1.3) holds unconditionally for almost all fields K of degree d, at least for small degrees d and sufficiently large ℓ.

Theorem 1.1 (Ellenberg, Pierce, Wood). *Suppose $d \in \{2, 3, 4, 5\}$, $\nu_0(2) = \nu_0(3) = 1$, $\nu_0(4) = 1/48$, $\nu_0(5) = 1/200$, and $\varepsilon > 0$. Then for all but*

$$O_{\ell,\varepsilon}(X^{1-\min\{1/(2\ell(d-1)),\nu_0(d)\}+\varepsilon})$$

degree d number fields K with $D_K \leq X$ (and non-D_4 when $d = 4$) we have

$$(1.4) \qquad\qquad \#Cl_K[\ell] \ll_{\ell,\varepsilon} D_K^{1/2-\min\{1/(2\ell(d-1)),\nu_0(d)\}+\varepsilon}.$$

---

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

Note that the number of fields K of degree $d \leq 5$ (and non-D_4 when $d = 4$) with $D_K \leq X$ grows linearly in X, so that 100% of these fields satisfy the bound (1.4) when enumerated by modulus of the discriminant. The cases $d = 4, 5$ were recently improved by the second author [25].

1.2. **Results.** Theorem 1.1 relies on uniform, power-saving error terms for the asymptotics of degree d-fields with chosen splitting types at a finite set of primes; the results in [6] are formulated in such a way that whenever such asymptotics are available then the GRH-bound (1.3) will hold for almost all K and all ℓ sufficiently large. As already mentioned in [6, last paragraph of Section 2.], this extends straightforwardly to allow arbitrary ground fields F. Our first result combines this extension with an idea from [25] to make further progress by showing that one can even go beyond the GRH-bound, at least for $n > 3$. Here we content ourselves with a simple consequence of Theorem 6.4.

Let $\mathscr{F}$ be a family of degree n extensions $K \subseteq \overline{F}$ of F, let $\mathscr{E}$ be a finite set of prime ideals $\mathfrak{p}$ in $\mathcal{O}_F$, and set

$$N_{\mathscr{F}}(X) := \#\{K \in \mathscr{F}; D_K \leq X\}.$$

Let $\mathfrak{e} = \mathfrak{p}$ or $\mathfrak{e} = \mathfrak{p}\mathfrak{q}$ for distinct prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ of $\mathcal{O}_F$ with $\mathfrak{p}, \mathfrak{q} \notin \mathscr{E}$, and let $N_{\mathscr{F}}(\mathfrak{e}; X)$ be the number of fields K counted in $N_{\mathscr{F}}(X)$ in which the prime ideals dividing $\mathfrak{e}$ split completely. Suppose that $c_{\mathscr{F}} > 0$, $0 \leq \tau < 1$, and $\sigma \geq 0$, and that we have

$$(1.5) \qquad\qquad N_{\mathscr{F}}(X) = c_{\mathscr{F}} X + O_{\mathscr{F}, \varepsilon}\left(X^{\tau + \varepsilon}\right),$$

$$(1.6) \qquad\qquad N_{\mathscr{F}}(\mathfrak{e}; X) = \delta_{\mathfrak{e}} c_{\mathscr{F}} X + O_{\mathscr{F}, \varepsilon}\left((\mathfrak{N}(\mathfrak{e}))^{\sigma} X^{\tau + \varepsilon}\right),$$

where $\delta_{\mathfrak{e}}$ is a multiplicative function with $1 \ll_{\mathscr{F}} \delta_{\mathfrak{p}} \leq 1$ if $\mathfrak{p} \notin \mathscr{E}$.

Theorem 1.2. *Suppose F is a number field, and $\mathscr{F}$ is a family of degree n extensions $K \subseteq \overline{F}$ of F. Let $\varepsilon > 0$, and suppose (1.5) and (1.6) do hold for the family $\mathscr{F}$ and some finite set $\mathscr{E}$ of primes in $\mathcal{O}_F$. Then we have for all sufficiently large ℓ*

$$(1.7) \qquad\qquad \#Cl_K[\ell] \ll_{\mathscr{F}, \ell, \varepsilon} D_K^{1/2 - \frac{1}{\ell(n+1)} + \varepsilon}$$

for 100% of $K \in \mathscr{F}$ (when enumerated by modulus of the discriminant).

The hypotheses of Theorem 1.2 are believed to hold, for example, for the family of degree-n-extensions of F whose normal closure has Galois group S_n. However, at present times this is known only for a few cases, for instance when $n \leq 5$ and $F = \mathbb{Q}$ (see [6]).

Our first main result generalises the case $d = 2$ of Theorem 1.1 in two different directions[2]. Write $m = [F : \mathbb{Q}]$, and recall that $\mathscr{T}_{F,n}$ is a certain family of cyclic degree-n-extensions of F. We define

$$(1.8) \qquad\qquad \tilde{\delta} = \tilde{\delta}(m, n) := \begin{cases} \frac{1}{8\phi(n)(n-1)} & \text{if } m = 1 \\ \frac{1}{2(m+1)\phi(n)(n-1)} & \text{if } m \geq 2, \end{cases}$$

where $\phi(\cdot)$ denotes Euler's totient function.

Theorem 1.3. *Suppose F and $\mathbb{Q}(\mu_n(\overline{F}))$ are linearly disjoint over $\mathbb{Q}$, and $\varepsilon > 0$. Then for all but $O_{F,n,\varepsilon}(X^{\frac{1}{n-1} - \min\{\frac{1}{2\ell(n-1)}, \tilde{\delta}\} + \varepsilon})$ fields K in $\mathscr{T}_{F,n}$ with $D_K \leq X$ we have*

$$(1.9) \qquad\qquad \#Cl_K[\ell] \ll_{F,n,\ell,\varepsilon} D_K^{\frac{1}{2} - \min\{\frac{1}{2\ell(n-1)}, \tilde{\delta}\} + \varepsilon}.$$

---

[2]The cases $\ell \leq 3$ are actually not covered but these cases are superseded by the aforementioned stronger pointwise bounds. And in fact our stronger Theorem 6.2 fully covers the case $d = 2$ of Theorem 1.1 too.

Since the number of $K \in \mathscr{T}_{F,n}$ with $D_K \leq X$ grows with the order $X^{1/(n-1)}$ (cf. Theorem 1.5 below), we conclude that when enumerated by D_K then 100% of the fields $K \in \mathscr{T}_{F,n}$ satisfy the bound (1.9). Theorem 1.3 offers several ways of obtaining families of number fields of arbitrarily large degree, for which non-trivial bounds for $\# \mathrm{Cl}_K[\ell]$ are known for every given ℓ, for almost all members of the family.

For which ℓ does the bound on the right-hand side of (1.9) become the GRH-bound? For $m \geq 2$, we get the GRH-bound if and only if $\ell \geq m + 1$. Theorem 1.3 will follow from Theorem 6.2, which holds for slightly more general families of number fields and provides a slightly larger value for $\tilde{\delta}$.

Partial summation, using the trivial bound (1.1) for the exceptional fields, immediately gives the following average bound.

Corollary 1.4. *Suppose F and $\mathbb{Q}(\mu_n(\overline{F}))$ are linearly disjoint over $\mathbb{Q}$, and $\varepsilon > 0$. Then we have*

$$\sum_{\substack{K \in \mathscr{T}_{F,n} \\ D_K \leq X}} \# Cl_K[\ell] \ll_{F,n,\ell,\varepsilon} X^{\frac{1}{2} + \frac{1}{n-1} - \min\{\frac{1}{2\ell(n-1)}, \tilde{\delta}\} + \varepsilon}.$$

A result quite similar to Theorem 1.3 is obtained independently by Pierce, Turnage-Butterbaugh and Wood as part of a very recent preprint [15]. The main differences seem to be that they obtain much better bounds on the size of the exceptional set, but their results are restricted to the base field $F = \mathbb{Q}$, and it seems unclear to which extent their arguments extend to other number fields. Their proofs are based on an effective version of the Chebotarev density theorem for certain families of number fields, for which they also include several further applications. For example, they also obtain conditional results for S_n-extensions of degree n and squarefree discriminant. It would be interesting to see whether the ideas from our Section 6.2 could be used beneficially in their proofs to beat the GRH-bound.

Our second main result and crucial new input to establish Theorem 1.3 is a counting result for the number of fields in the family $\mathscr{T}_{F,n}$ of bounded discriminant satisfying prescribed local conditions, with a fairly explicit error term.

We write $\Delta(K/F)$ for the relative discriminant ideal of the extension K/F and $\mathfrak{N}\Delta(K/F)$ for its absolute norm. In our notation, we will not distinguish between prime ideals of the ring of integers $\mathscr{O}_F$ and the corresponding non-archimedean places of F. For $l \geq 0$ and a set $\mathfrak{P} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_l\}$ of pairwise distinct non-archimedean places of F not dividing n, we study the counting function

$$N_{\mathscr{T}_{F,n}}(\mathfrak{P}; X) := \# \{K \in \mathscr{T}_{F,n}; \ \mathfrak{p}_1, \ldots, \mathfrak{p}_l \text{ split completely in } K, \ \mathfrak{N}\Delta(K/F) \leq X\}.$$

Theorem 1.5. *Suppose F and $\mathbb{Q}(\mu_n(\overline{F}))$ are linearly disjoint over $\mathbb{Q}$, and $\varepsilon > 0$. Then*

$$N_{\mathscr{T}_{F,n}}(\mathfrak{P}; X) = \delta_{\mathfrak{p}_1 \cdots \mathfrak{p}_l} c_{F,n} X^{1/(n-1)} + O_{F,n,l,\varepsilon}\left(\mathfrak{N}(\mathfrak{p}_1 \cdots \mathfrak{p}_l)^{1/(2m)+\varepsilon} X^{(1-\beta)/(n-1)}\right),$$

as $X \to \infty$, where

$$\beta := \begin{cases} 1/(4\phi(n)) & \text{if } m = 1, \\ 1/(2m\phi(n)) & \text{if } m \geq 2. \end{cases}$$

The constant $c_{F,n}$ is positive and can be computed explicitly. The constant $\delta_{\mathfrak{d}}$ is multiplicative[3] in $\mathfrak{d}$ and satisfies

$$(1.10) \qquad \delta_{\mathfrak{p}} := \begin{cases} 1/n & \text{if } \mathfrak{N}(\mathfrak{p}) \not\equiv 1 \bmod n \\ 1/(n(1 + \phi(n)\mathfrak{N}(\mathfrak{p})^{-1})) & \text{if } \mathfrak{N}(\mathfrak{p}) \equiv 1 \bmod n. \end{cases}$$

---

[3]Of course, for $l = 0$ we set $\mathfrak{p}_1 \cdots \mathfrak{p}_l := \mathscr{O}_F$ and $\delta_{\mathscr{O}_F} := 1$.

If n is prime, a weaker version of Theorem 1.5, with an error term of the shape $O_{F,n,\mathfrak{P}}(X^{1/(n-1)-\gamma})$, for some $\gamma > 0$, follows from [8, Theorem 1.7]. It is crucial for our work here to know the dependence of the error term on $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$ explicitly, as well as the value of γ. The multiplicativity of the constant $\delta_{\mathfrak{d}}$ can be interpreted as asymptotic independence of the local conditions imposed at $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$. This is required for our application in Theorem 1.3 and constitutes the main reason for restricting our attention to the family $\mathscr{T}_{F,n}$. The family of all cyclic degree-n-extensions would not show this independence behavior with respect to local conditions when counted by discriminant, unless n is prime.

Comparing our Theorem 1.5 with [8, Theorem 1.7], we observe that $\mathscr{T}_{F,n}$ has density zero in the family of all cyclic degree-n-extensions of F, unless n is prime. Not many other precise counting results for interesting zero-density families of number field extensions with fixed Galois group are available in the literature. A zero-density family of biquadratic fields was recently considered in [16].

The hypothesis that F be linearly disjoint from $\mathbb{Q}(\mu_n(\overline{F}))$ is necessary for the result to hold. If it is not satisfied, the asymptotic formula for $N_{\mathscr{T}_{F,n}}(\mathfrak{P}; X)$ will involve logarithms and secondary main terms. For prime n, this can be observed from [8, Theorem 1.7].

1.3. **Discriminant zeta function.** We prove Theorem 1.5 by studying the corresponding zeta function, using the approach of [26, 8]. For locally compact abelian groups A and B, we denote by $\mathrm{Hom}(A, B)$ the group of *continuous* homomorphisms from A to B, equipped with the compact-open topology. Let $G = \mu_n$ be the group of n-th roots of unity in $\mathbb{C}$. We let $G\text{-ext}(F) \subseteq \mathrm{Hom}(\mathrm{Gal}(\overline{F}/F), G)$ be the set of continuous *surjective* homomorphisms $\mathrm{Gal}(\overline{F}/F) \to G$. A homomorphism $\varphi \in G\text{-ext}(F)$ corresponds uniquely to a pair $(K_\varphi/F, \psi)$, where K_φ/F is a Galois extension and ψ is an isomorphism $\mathrm{Gal}(K_\varphi/F) \to G$. Indeed, we take K_φ to be the fixed field of $\ker \varphi$ and ψ the homomorphism induced by φ on the quotient $\mathrm{Gal}(K_\varphi/F)$. Clearly, each K_φ is induced by $\#\mathrm{Aut}(G) = \phi(n)$ different $\varphi \in G\text{-ext}(F)$. We write $\Delta(\varphi) := \Delta(K_\varphi/F)$.

For each place v, we fix an algebraic closure $\overline{F}_v \supseteq \overline{F}$. Then each homomorphism $\varphi \in \mathrm{Hom}(\mathrm{Gal}(\overline{F}/F), G)$ defines local homomorphisms $\varphi_v \in \mathrm{Hom}(\mathrm{Gal}(\overline{F}_v/F_v), G)$. Let $e(\varphi_v)$ denote the ramification index of the corresponding local extension K_{φ_v}/F_v. For non-archimedean v, we denote the cardinality of its residue field by q_v.

Theorem 1.5 will follow immediately from Theorem 1.6 below, which provides better error terms and handles slightly more general families of fields, for which we also allow local restrictions at places dividing $n\infty$.

For $v \mid n\infty$, let $\Lambda_v \subseteq \mathrm{Hom}(\mathrm{Gal}(\overline{F}_v/F_v), G)$ be any subset containing the trivial homomorphism 1. With $\Lambda := (\Lambda_v)_{v \mid n\infty}$, we consider the family

$$\mathscr{T}_{F,n}(\Lambda) := \{\varphi \in G\text{-ext}(F); \ K_\varphi \in \mathscr{T}_{F,n} \text{ and } \varphi_v \in \Lambda_v \text{ for all } v \mid n\infty\}$$

and the counting functions

$$N_{\mathscr{T}_{F,n}}(\Lambda, \mathfrak{P}; X) := \#\{\varphi \in \mathscr{T}_{F,n}(\Lambda); \ \mathfrak{p}_1, \ldots, \mathfrak{p}_l \text{ split completely in } K_\varphi, \ \mathfrak{N}\Delta(\varphi) \leq X\}.$$

Theorem 1.6. *Suppose F and $\mathbb{Q}(\mu_n(\overline{F}))$ are linearly disjoint over $\mathbb{Q}$, and $\varepsilon > 0$. With Λ as above, we have*

$$N_{\mathscr{T}_{F,n}}(\Lambda, \mathfrak{P}; X) = \delta_{\mathfrak{p}_1 \cdots \mathfrak{p}_l} c_{F,n,\Lambda} X^{1/(n-1)} + O_{F,n,l,\varepsilon}\left(\mathfrak{N}(\mathfrak{p}_1 \cdots \mathfrak{p}_l)^{a+\varepsilon} X^{(1-b)/(n-1)+\varepsilon}\right),$$

as $X \to \infty$, where

$$a := \begin{cases} 3/16 & \text{if } n = 2 \text{ and } m = 1, \\ 103/512 & \text{if } n = 2 \text{ and } m = 2, \\ 1/(2m) & \text{if } n \geq 3 \text{ or } m \geq 3, \end{cases}$$

and

$$b := \begin{cases} 13/32 & \text{if } n = 2 \text{ and } m = 1, \\ 153/512 & \text{if } n = 2 \text{ and } m = 2, \\ \min\{1/4, 64/(103\phi(n)m)\} & \text{if } n \geq 3 \text{ or } m \geq 3. \end{cases}$$

The constant $c_{F,n,\Lambda}$ is positive and can be computed explicitly. The constant $\delta_{\mathfrak{d}}$ is multiplicative in $\mathfrak{d}$ and satisfies (1.10).

With the choice $\Lambda_v := \text{Hom}(\text{Gal}(\overline{F}_v/F_v), G)$ for all $v \mid n\infty$, we get $N_{\mathcal{T}_{F,n}}(\Lambda, \mathfrak{P}; X) = \phi(n)N_{\mathcal{T}_{F,n}}(\mathfrak{P}; X)$. Thus, with the observation that

(1.11) $a \leq 1/(2m)$ and $b > \begin{cases} 1/(4\phi(n)) & \text{if } m = 1, \\ 1/(2m\phi(n)) & \text{if } m \geq 2, \end{cases}$

one sees immediately that Theorem 1.6 implies Theorem 1.5. But our more general setup allows us to count other interesting families as well, for example the family of all cyclic extensions of degree n of F, in which every tamely ramified prime ideal is totally ramified, or the family in which every ramified prime ideal is totally ramified.

For the proof of Theorem 1.6, we define a function $f(\mathfrak{P}; \varphi) := \prod_v f_v(\mathfrak{P}; \varphi_v)$ on $\text{Hom}(\text{Gal}(\overline{F}/F), G)$ locally by

$$f_v(\mathfrak{P}; \varphi_v) := \begin{cases} 1 & \text{if } v \mid n\infty \text{ and } \varphi_v \in \Lambda_v, \\ 1 & \text{if } v \in \mathfrak{P} \text{ and } \varphi_v = 1, \\ 1 & \text{if } v \notin \mathfrak{P}, \ v \nmid n\infty, \text{ and } e(\varphi_v) \in \{1, n\}, \\ 0 & \text{otherwise.} \end{cases}$$

With this definition, $f(\mathfrak{P}; \varphi) = 1$ if and only if $\varphi \in \mathcal{T}_{F,n}(\Lambda)$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$ split completely in K_φ/F. Thus, writing $\Delta(\varphi) := \Delta(K_\varphi/F)$, the Dirichlet series corresponding to $N_{\mathcal{T}_{F,n}}(\Lambda, \mathfrak{P}; X)$ is

$$D(\Lambda, \mathfrak{P}; s) := \sum_{\varphi \in G\text{-ext}(F)} \frac{f(\mathfrak{P}; \varphi)}{\mathfrak{N}(\Delta(\varphi))^s}.$$

Proposition 1.7. *The Dirichlet series $D(\Lambda, \mathfrak{P}; s)$ converges absolutely in the half-plane $(n-1)\Re(s) > 1$. It has a meromorphic continuation to the half-plane $(n-1)\Re(s) > 1/2$. The only pole in this half-plane is a simple pole at $s = 1/(n-1)$. The residue has the form $\delta_{\mathfrak{p}_1 \cdots \mathfrak{p}_l} c_{F,n,\Lambda}(n-1)^{-1}$, as in Theorem 1.6. Let*

$$\alpha := \begin{cases} 3/8 & \text{if } F = \mathbb{Q} \text{ and } n = 2 \\ 103/256 & \text{otherwise.} \end{cases}$$

Then, for any $\eta \in (0, 1)$ and $\varepsilon > 0$, we have the estimate

(1.12) $\dfrac{\left|s - \frac{1}{n-1}\right|}{|s|} D(\Lambda, \mathfrak{P}; s) \ll_{F,n,l,\eta,\varepsilon} (\mathfrak{N}(\mathfrak{p}_1 \cdots \mathfrak{p}_l)(1 + |\Im s|)^m)^{\phi(n)\alpha(1+\eta-(n-1)\Re s)+\varepsilon}$

in the vertical strip $1/2 + \varepsilon \leq (n-1)\Re(s) < 1 + \eta$.

We will first prove Proposition 1.7 with help of the techniques from [8] and then deduce Theorem 1.5 from it via Perron's formula and tauberian arguments.

2. PROOF OF PROPOSITION 1.7: ANALYSIS OF THE DISCRIMINANT ZETA FUNCTION

The aim of this section is to prove Proposition 1.7. In §2.2, we apply class field theory, Möbius inversion and a version of the Poisson summation formula to express $D(\Lambda, \mathfrak{P}; s)$ as a sum of Euler products. The arguments are very similar to [8], so we will be concise. In §2.3, we analyse these Euler products and show that they behave like certain Artin L-functions. This will yield a meromorphic continuation of $D(\Lambda, \mathfrak{P}; s)$. In §2.4, we deduce

(1.12) from subconvex bounds of our Artin L-functions, and in §2.5, we determine the residue of $D(\Lambda, \mathfrak{P}; s)$ at $s = 1/(n-1)$.

2.1. Preliminaries.

Lemma 2.1. *Let F be a number field, $n > 1$ an integer and S a finite set of places of F containing all places dividing $n\infty$. Then the number of cyclic extensions K/F with $[K : F] = n$ that are unramified at all places not in S is $\ll_{F,n} n^{[F(\mu_n(\overline{F})):F]\cdot \#S}$.*

Proof. Consider first the case where $\mu_n(\overline{F}) \subseteq F$. We may assume, without loss of generality, that S contains enough places to ensure that the ring of S-integers $\mathcal{O}_S$ of F is a principal ideal domain.

By Kummer theory, cyclic extensions K/F of degree n are of the form $K = F(\sqrt[n]{a})$, with $a \in F^\times/F^{\times n}$. For finite places $\mathfrak{p} \notin S$, the extension $F(\sqrt[n]{a})/F$ is unramified if and only if n divides the exponential $\mathfrak{p}$-adic valuation $\mathrm{ord}_{\mathfrak{p}}(a)$. Consider the exact sequence

$$(2.1) \qquad 1 \to \mathcal{O}_S^\times \to F^\times \to \prod_{\mathfrak{p} \notin S} \mathbb{Z} \to 1,$$

where the third map is given by the exponential valuations at $\mathfrak{p} \notin S$. Taking the tensor product with $\mathbb{Z}/n\mathbb{Z}$, we get

$$\mathcal{O}_S^\times/\mathcal{O}_S^{\times n} \to F^\times/F^{\times n} \to \prod_{\mathfrak{p} \notin S} \mathbb{Z}/n\mathbb{Z} \to 1,$$

so the number of possible values of $a \in F^\times/F^{\times n}$ is bounded by

$$\#\mathcal{O}_S^\times/\mathcal{O}_S^{\times n} \ll_{F,n} n^{\#S}.$$

Now we consider the general case. For every K as in the lemma, we get a cyclic extension $K(\mu_n(\overline{F}))/F(\mu_n(\overline{F}))$ of degree at most n, which is unramified at all places not lying above places in S. By what we proved above, the number of such extensions of $F(\mu_n(\overline{F}))$ is $\ll_{F,n} n^{[F(\mu_n(\overline{F})):F]\cdot \#S}$. The lemma follows, since each cyclic extension field of $F(\mu_n(\overline{F}))$ of degree bounded by n has $\ll_{F,n} 1$ subfields. $\qquad \square$

2.2. **Set-up and Poisson summation.** We follow the strategy of [8, §4] with our $f(\cdot) = f(\mathfrak{P}; \cdot)$, additionally keeping track of the dependence on $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$. During this proof, all implicit constants in O- and $\ll$-notation may always depend on F, n, l, but not on $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$. Since there are only finitely many possibilities for Λ, once n and F are fixed, the implicit constants are also independent of Λ.

Since $f(\mathfrak{P}; \varphi) \leq 1$ for all $\varphi \in G\text{-ext}(F)$, it is clear from Wright's result [26] that $D(\Lambda, \mathfrak{P}; s)$ converges absolutely whenever $\Re s$ is large enough.

Let $\mathbf{A}^\times$ be the idele group of F. Since $G = \mu_n$ is abelian, global class field theory allows us to identify the groups $\mathrm{Hom}(\mathrm{Gal}(\overline{F}/F), G)$ and $\mathrm{Hom}(\mathbf{A}^\times/F^\times, G)$, and we interpret f as a function on the latter group. Via the natural embedding $F_v^\times \subseteq \mathbf{A}^\times$, each $\varphi \in \mathrm{Hom}(\mathbf{A}^\times/F^\times, G)$ induces local homomorphisms $\varphi_v \in \mathrm{Hom}(F_v^\times, G)$ corresponding via local class field theory to elements of $\mathrm{Hom}(\mathrm{Gal}(\overline{F}_v/F_v), G)$. Thus, we may describe the local factors of f by

$$f_v(\mathfrak{P}; \varphi_v) = \begin{cases} 1 & \text{if } v \mid n\infty \text{ and } \varphi_v \in \Lambda_v, \\ 1 & \text{if } v \in \mathfrak{P} \text{ and } \varphi_v = 1, \\ 1 & \text{if } v \notin \mathfrak{P}, \ v \nmid n\infty, \text{ and } [\mathcal{O}_v^\times : \mathcal{O}_v^\times \cap \ker(\varphi_v)] \in \{1, n\}, \\ 0 & \text{otherwise.} \end{cases}$$

The following derivations are a direct application of [8, §2] to the present situation. By the conductor-discriminant formula and Möbius inversion to remove the surjectivity

condition, we get (cf. [8, Lemma 2.2])

$$(2.2) \qquad D(\Lambda, \mathfrak{P}; s) = \sum_{d|n} \mu(n/d) F_d(\mathfrak{P}; sn/d),$$

where

$$F_d(\mathfrak{P}; s) := \sum_{\varphi \in \operatorname{Hom}(\mathbf{A}^\times/F^\times, \ \mu_d)} \frac{f(\varphi)}{\Phi_d(\varphi)^s},$$

with

$$(2.3) \qquad \Phi_d(\varphi) := \prod_{a \bmod d} \Phi(\varphi^a),$$

and $\Phi(\psi)$ the reciprocal of the idelic norm of the conductor of the character ψ.

If d is a proper divisor of n and $\varphi \in \operatorname{Hom}(\mathbf{A}^\times/F^\times, \ \mu_d)$, then $f(\varphi) = 0$ unless the corresponding extension K_φ is unramified at all places v not dividing $n\infty$. By Lemma 2.1, this occurs for at most $\ll 1$ extensions. Thus, $F_d(\mathfrak{P}; s)$ is a finite sum and entire. Moreover,

$$(2.4) \qquad F_d(\mathfrak{P}; s) \ll 1 \quad \text{for} \quad \Re s \geq 0, \quad \text{if } d \neq n.$$

Thus, the analytic behavior of $D(\Lambda, \mathfrak{P}; s)$ is determined by $F_n(\mathfrak{P}; s)$. We let $S := S' \cup \mathfrak{P}$, where S' is the set of places of F dividing $n\infty$.

By [8, Proposition 3.8], a version of the Poisson summation formula adapted to the present situation, the series $F_n(\mathfrak{P}; s)$ has the form

$$(2.5) \qquad F_n(\mathfrak{P}; s) = \frac{1}{\#\mathscr{O}_F^\times/\mathscr{O}_F^{\times n}} \sum_{x \in F^\times/F^{\times n}} \widehat{f}(x; s) \quad \text{for } \Re s \gg 1,$$

where $\widehat{f}(x; s)$ is a Fourier transform defined in [8, §3.3]. Denote by x_v the image of $x \in F^\times/F^{\times n}$ under the natural map to $F_v^\times/F_v^{\times n}$. Using the observation that $f_v(\mathfrak{P}; \cdot)$ is invariant under $\operatorname{Hom}(F_v^\times/\mathscr{O}_v^\times, \mu_n)$ for all $v \notin S$ and [8, Lemma 3.6], we see that the sum in (2.5) extends in fact only over the finite group

$$\mathscr{U}_S(n) := \{x \in F^\times/F^{\times n} \ : \ x_v \in \mathscr{O}_v^\times/\mathscr{O}_v^{\times n} \text{ for all } v \notin S\}.$$

The Fourier transform $\widehat{f}(x; s)$ is an Euler product $\widehat{f}(x; s) = \prod_v \widehat{f}_v(x_v; s)$, whose local factors at $v \nmid n\infty$ we now describe explicitly. As in [8, §3.3], we define for $\chi_v \in \operatorname{Hom}(\mathscr{O}_v^\times, \mu_n)$ and $x_v \in F_v^\times/F_v^{\times n}$ the average

$$\tau_{f_v}(\chi_v, x_v) := \frac{1}{n} \sum_{\psi_v \in \operatorname{Hom}(F_v^\times/\mathscr{O}_v^\times, \ \mu_n)} f_v(\mathfrak{P}; \chi_v \psi_v) \psi_v(x_v).$$

Here we identified $\operatorname{Hom}(F_v^\times, \mu_n) = \operatorname{Hom}(\mathscr{O}_v^\times, \mu_n) \oplus \operatorname{Hom}(F_v^\times/\mathscr{O}_v^\times, \mu_n)$ by the choice of a uniformiser. By [8, Lemma 3.3], we get the formula

$$(2.6) \qquad \widehat{f}_v(x_v; s) = \sum_{m|(n, q_v-1)} \left(\sum_{\substack{\chi_v \in \operatorname{Hom}(\mathscr{O}_v^\times, \ \mu_n) \\ \ker(\chi_v) = \mathscr{O}_v^{\times m}}} \tau_{f_v}(\chi_v, x_v) \chi_v(x_v) \right) q_v^{-n(1-1/m)s},$$

where we wrote $(n, q_v - 1)$ for the greatest common divisor. For $v \in \mathfrak{P}$, we clearly have

$$\tau_f(\chi_v, x_v) = \begin{cases} \frac{1}{n} & \text{if } \chi_v = 1, \\ 0 & \text{otherwise,} \end{cases}$$

and thus

$$(2.7) \qquad \widehat{f}_v(x_v; s) = \frac{1}{n} \quad \text{for} \quad v \in \mathfrak{P}.$$

At the remaining places not dividing $n\infty$, we find the following situation.

Lemma 2.2. *Let $v \notin \mathfrak{P}$, $v \nmid n$ be a non-archimedean place of F and $x_v \in \mathscr{O}_v^{\times}/\mathscr{O}_v^{\times n}$. Let $d_v(x_v)$ be the largest divisor d of n, for which $x_v \in \mathscr{O}_v^{\times d}/\mathscr{O}_v^{\times n}$. Then*

$$\widehat{f}_v(x_v; s) = \begin{cases} 1 & \text{if } q_v \not\equiv 1 \bmod n, \\ 1 + \left(\sum_{d \mid d_v(x_v)} \mu(n/d) d \right) q_v^{-(n-1)s} & \text{if } q_v \equiv 1 \bmod n. \end{cases}$$

Proof. The $\mathrm{Hom}(k_v^{\times}/\mathscr{O}_v^{\times}, \mu_n)$-invariance of $f_v(\mathfrak{P}, \cdot)$ implies that $\tau_f(\chi_v, x_v) = f_v(\mathfrak{P}; \chi_v)$. Recall the definition of $f_v(\mathfrak{P}, \cdot)$ and the fact that $[\mathscr{O}_v^{\times} : \mathscr{O}_v^{\times m}] = [F(v)^{\times} : F(v)^{\times m}] = m$ whenever $m \mid q_v - 1$, where $F(v)$ is the residue field. Thus, we get from (2.6) the identities

$$\widehat{f}_v(x_v; s) = 1 \quad \text{if} \quad n \nmid q_v - 1$$

and

$$\widehat{f}_v(x_v; s) = 1 + \left(\sum_{\substack{\chi_v \in \mathrm{Hom}(\mathscr{O}_v^{\times}, \ \mu_n) \\ \ker \chi_v = \mathscr{O}_v^{\times n}}} \chi_v(x_v) \right) q_v^{-n(1-1/n)s} \quad \text{if} \quad n \mid q_v - 1.$$

To see that the sum inside the parentheses has the desired shape, use inclusion-exclusion and the fact that, for $d \mid n$,

$$\sum_{\chi_v \in \mathrm{Hom}(\mathscr{O}_v^{\times}/\mathscr{O}_v^{\times d}, \ \mu_n)} \chi_v(x_v) = \begin{cases} \# \mathrm{Hom}(\mathscr{O}_v^{\times}/\mathscr{O}_v^{\times d}, \mu_n) = d & \text{if } x_v \in \mathscr{O}_v^{\times d}/\mathscr{O}_v^{\times n}, \\ 0 & \text{otherwise.} \end{cases}$$

$\square$

The lemma shows in particular that the Euler product defining $\widehat{f}(x; s)$ converges absolutely and defines a holomorphic function in the half-plane $(n-1)\Re(s) > 1$. The same holds thus for the Dirichlet series $F_n(\mathfrak{P}; s)$ and $D(\Lambda, \mathfrak{P}; s)$, since they have non-negative coefficients.

2.3. **Analysis of the local factors.** We will now compare the local factors $\widehat{f}_v(x_v; s)$ to the local factors of certain Artin L-functions. Let $F_0 := F(\mu_n(\overline{F}))$. Our hypotheses on F imply that $[F_0 : F] = \phi(n)$. For $x \in \mathscr{U}_S(n)$, we choose a representative $a \in F^{\times}$ of x and an n-th root $\alpha \in \overline{F}$ of a. We consider the field

$$F_x := F_0(\alpha) = F(\mu_n(\overline{F}), \alpha),$$

which is clearly independent of the choice of a and α. Since $\mu_n(\overline{F}) \subseteq F_0$, we see that F_x/F_0 is cyclic of degree dividing n.

Let $v \notin S$ with $q_v \equiv 1 \bmod n$, so F_v has primitive n-th roots of unity and v splits completely in F_0. Let w a place of F_0 above v, then w is unramified in F_x, and we denote its Frobenius automorphism by $\sigma_w \in \mathrm{Gal}(F_x/F_0)$.

Let $n_v(x) := n/d_v(x_v)$, then $n_v(x)$ is the smallest positive integer with the property that $\alpha^{n_v(x)} \in F_v = F_{0,w}$, so $F_{0,w}(\alpha)/F_{0,w}$ is cyclic of degree $n_v(x)$. In particular, the order of $\sigma_w \in \mathrm{Gal}(F_x/F_0)$ is $n_v(x)$.

Lemma 2.3. *Let $v \notin S$ with $q_v \equiv 1 \bmod n$. Let $\sigma \in \mathrm{Gal}(F_x/F_0)$ be of order $n_v(x)$. Then there are exactly $\phi(n)/\phi(n_v(x))$ places $w \mid v$ of F_0 with $\sigma_w = \sigma$.*

Proof. Write $G := \mathrm{Gal}(F_x/F)$ and $A := \mathrm{Gal}(F_x/F_0)$. Let $n' := [F_x : F_0]$. Then $A \cong \mathbb{Z}/n'\mathbb{Z}$ is a normal subgroup of G, so G acts on A by conjugation. Fix a primitive n-th root of unity $\zeta \in F_0$, then any $\sigma \in \mathrm{Gal}(F_x/F)$ is determined by $\sigma(\zeta)$ and $\sigma(\alpha)$. Let $\sigma \in \mathrm{Gal}(F_x/F_0)$, then $\sigma(\alpha) = \zeta^{an/n'}\alpha$, for $a \in \mathbb{Z}/n'\mathbb{Z}$. For any $b \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, there are n' automorphisms $\tau \in G$ with $\tau(\zeta) = \zeta^b$. For any such τ, we get $\tau\sigma\tau^{-1}(\alpha) = \zeta^{ban/n'}\alpha$, so $\tau\sigma\tau^{-1} = \sigma^b$. Thus, the orbit of σ under conjugation by G is the set of all $\sigma' \in A$ with order $|\sigma'| = |\sigma|$, and the stabilizer has order $n'\phi(n)/\phi(|\sigma|)$.

The group G also acts transitively on the prime ideals of F_0 above v via $w \mapsto \tau(w)$, and for the corresponding Frobenius elements we have $\tau\sigma_w\tau^{-1} = \sigma_{\tau(w)}$. Since v splits completely, the stabilizer of any w is A of order n'. This shows that every $\sigma \in A$ of order $n_w(x)$ is the Frobenius element $\sigma = \tau\sigma_w\tau^{-1} = \sigma_{\tau(w)}$ for precisely $\phi(n)/\phi(n_v(x))$ different places $\tau(w)$ above v. $\qquad\square$

Since $\mathrm{Gal}(F_x/F_0)$ is cyclic, the same holds for its character group. For any character of full order, we have the following identity.

Lemma 2.4. Let $v \notin S$ with $q_v \equiv 1 \bmod n$. Let $\chi \in \mathrm{Hom}(\mathrm{Gal}(F_x/F_0), \mathbb{C}^\times)$ be a character of order $|\chi| = [F_x : F_0]$. Then

$$(2.8) \qquad \sum_{w|v} \chi(\sigma_w) = \sum_{d|d_v(x_v)} \mu(n/d)d.$$

The sum on the left-hand side runs over all places w of F_0 above v.

Proof. Write $n' = [F_x : F_0]$ and $n_v = n_v(x)$, so that $\mathrm{Gal}(F_x/F_0) \cong \mathbb{Z}/n'\mathbb{Z}$. Using Lemma 2.3, inclusion-exclusion and character orthogonality, we obtain

$$\sum_{w|v} \chi(\sigma_w) = \frac{\phi(n)}{\phi(n_v)} \sum_{\substack{a \in \mathbb{Z}/n'\mathbb{Z} \\ |a| = n_v}} \chi(a) = \frac{\phi(n)}{\phi(n_v)} \sum_{d|n_v} \mu(n_v/d) \sum_{\substack{a \in \mathbb{Z}/n'\mathbb{Z} \\ |a| | d}} \chi(a) = \frac{\phi(n)}{\phi(n_v)} \mu(n_v).$$

To show that the last expression equals the right-hand side of (2.8), we recall that $n_v = n/d_v(x_v)$. If $v_p(n) > v_p(d_v(x_v)) + 1$ for some prime p, then both expressions are zero.

Thus, let us assume that $v_p(n) \in \{v_p(d_v(x)), v_p(d_v(x)) + 1\}$ for all primes p. We group together all prime factors p of n, for which $v_p(n) = v_p(d_v(x))$ by writing $n = mD$, $d_v(x) = fD$, with $(m, D) = (f, D) = 1$ and $v_p(m) = v_p(f) + 1$ for all primes p. The right-hand side in (2.8) is then equal to

$$\phi(D) \sum_{d|f} \mu(m/d)d = \phi(D)\mu(m/f)f = \phi(D)f\mu(n_v) = \frac{\phi(n)}{\phi(n_v)}\mu(n_v).$$

The last equality holds, since $\phi(n) = \phi(D)\phi(m) = \phi(D)\phi(m/f)f$. $\qquad\square$

For any character χ of $\mathrm{Gal}(F_x/F_0)$, we consider the Artin L-function

$$L(F_x/F_0, \chi, s) = \prod_w \frac{1}{1 - \chi(\sigma_w)q_w^{-s}},$$

the product running over all places w of F_0 that are unramified in F_x. For a place $v \notin S$ of F, the local factor of $L(F_x/F_0, \chi, s)$ at v is

$$L_v(F_x/F_0, \chi, s) = \prod_{w|v} \frac{1}{1 - \chi(\sigma_w)q_w^{-s}}.$$

Lemma 2.5. Let χ be a character of $\mathrm{Gal}(F_x/F_0)$ of order $[F_x : F_0]$ and $v \notin S$. Then

$$\widehat{f_v}(x_v; s) = L_v(F_x/F_0, \chi, (n-1)s) + O(q_v^{-2(n-1)s}) \quad \text{for} \quad (n-1)\Re(s) > 1/2.$$

Proof. For $\Re(s) > 1/2$, we have

$$L_v(F_x/F_0, \chi, s) = 1 + \sum_{w|v} \chi(\sigma_w)q_w^{-s} + O(q_v^{-2s}).$$

If $q_v \not\equiv 1 \bmod n$, then v does not split completely in F_0, so $q_w \geq q_v^2$ for all $w \mid v$ and $L_v(F_x/F_0, \chi, s) = 1 + O(q_v^{-2s})$. If $q_v \equiv 1 \bmod n$, then $q_w = q_v$ and, by (2.8),

$$L_v(F_x/F_0, \chi, s) = 1 + \left(\sum_{d|d_v(x_v)} \mu(n/d)d \right) q_v^{-s} + O(q_v^{-2s}).$$

Compare these expressions to Lemma 2.2. □

Lemma 2.6. *Let χ be a character of $\mathrm{Gal}(F_x/F_0)$ of order $[F_x : F_0]$ and $\varepsilon > 0$. There is a holomorphic function $g(x;s)$ on $(n-1)\Re(s) > 1/2$, satisfying $g(x;s) \ll_\varepsilon 1$ on $(n-1)\Re(s) \geq 1/2 + \varepsilon$, such that*

$$\widehat{f}(x;s) = g(x;s)L(F_x/F_0, \chi, (n-1)s) \quad on \quad (n-1)\Re(s) > 1.$$

Proof. Let $(n-1)\Re(s) > 1$. Lemma 2.5 implies that

$$\prod_{v \notin S} \widehat{f}_v(x_v; s) = h(x;s)L(F_x/F_0, \chi, (n-1)s),$$

with a holomorphic function $h(x;s)$ on $(n-1)\Re(s) > 1/2$ satisfying $1 \ll_\varepsilon h(x;s) \ll_\varepsilon 1$ on $(n-1)\Re(s) \geq 1/2 + \varepsilon$. Muptiply $h(x;s)$ by the $|S| \ll 1$ local factors $\widehat{f}_v(x_v; s)$ at $v \in S$ to get $g(x;s)$. The upper bound for $g(x;s)$ remains intact, since $\widehat{f}_v(x_v; s) \ll 1$ for $\Re(s) \geq 0$ and all $v \in S$. □

From Lemma 2.6, we obtain a meromorphic continuation of $\widehat{f}(x;s)$, and thus also of $F_n(\mathfrak{P}; s)$ and $D(\Lambda, \mathfrak{P}; s)$, to $(n-1)\Re s > 1/2$. Since $\mathrm{Gal}(F_x/F_0)$ is abelian, the Artin L-function $L(F_x/F_0, \chi, s)$ is a Hecke L-function and as such entire whenever χ is non-trivial. Thus, the only possible pole of $D(\Lambda, \mathfrak{P}; s)$ in $(n-1)\Re s > 1/2$ is a simple pole at $s = 1/(n-1)$, coming from $\widehat{f}(x;s)$ for $x \in \mathscr{U}_S(n)$ with $F_x = F_0$, in which case $L(F_x/F_0, \chi, s)$ is the Dedekind zeta function $\zeta_{F_0}(s)$ of F_0.

2.4. **Estimates in vertical strips.**

Let us prove next the estimate (1.12) for $D(\Lambda, \mathfrak{P}; s)$ in the vertical strip. We use the best available subconvexity bounds in conjunction with the Phragmen-Lindelöf principle to estimate $L(F_x/F_0, \chi, s)$. As F_x/F_0 is abelian, this coincides with the Hecke L-function $L(\psi, s)$ of some Dirichlet character of F_0 whose conductor $\mathfrak{f}_\psi$ divides the conductor of F_x/F_0. Since only places w of F_0 above places $v \in S$ can ramify in F_x, and since places above $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$ are at worst tamely ramified, we get $\mathfrak{N}(\mathfrak{f}_\psi) \ll \mathfrak{N}(\mathfrak{p}_1 \cdots \mathfrak{p}_l)^{\phi(n)}$.

First assume that $[F_x : F_0] > 1$. Then χ is non-trivial, so ψ is a non-principal Dirichlet character. For $t \in \mathbb{R}$, we consider the twist $\psi_t := \psi |\cdot|^{it}$, where $|\cdot|$ is the norm character on the idele class group of F_0. Then ψ_t is a Hecke character of the same conductor $\mathfrak{f}_\psi$ and analytic conductor $C(\psi_t) \leq \mathfrak{N}(\mathfrak{f}_\psi)(2 + |t|)^{m\phi(n)}$.

From [27, Theorem 1.1], applied to ψ_t, we get

$$(2.9) \qquad L(1/2 + it; \psi) \ll_\varepsilon \left(\mathfrak{N}(\mathfrak{f}_\psi)(1 + |t|)^{m\phi(n)} \right)^{\alpha/2+\varepsilon},$$

where

$$\alpha = \frac{1}{2} - \frac{1 - 2\theta}{8},$$

with θ any exponent towards the Ramanujan-Petersson conjecture. By [2], one may take $\theta = 7/64$. If $F = \mathbb{Q}$ and $n = 2$, then $L(s; \psi)$ is a Dirichlet L-function and we get from [9] the bound (2.9) with $\alpha = 3/8$.

For any $\gamma \in (0, 1)$, the previous bounds in conjunction with the Phragmen-Lindelöf principle yield

$$L(F_x/F_0, \chi, s) = L(s; \psi) \ll_{\eta, \varepsilon} \left(\mathfrak{N}(\mathfrak{f}_\psi)(1 + |\Im(s)|)^{m\phi(n)} \right)^{\alpha(1+\eta-\Re(s))+\varepsilon}$$

in the strip $1/2 \leq \Re(s) \leq 1 + \eta$. By a similar argument, we find in case $F_x = F_0$ that

$$\frac{|s-1|}{|s|} L(F_x/F_0, \chi, s) = \frac{|s-1|}{|s|} \zeta_{F_0}(s) \ll_{\eta, \varepsilon} (1 + |\Im(s)|)^{m\phi(n)\alpha(1+\eta-\Re(s))+\varepsilon}.$$

Together with Lemma 2.6 and the fact that $\#\mathscr{O}_S^\times/\mathscr{O}_S^{\times n} \ll 1$, these observations are enough to prove the estimate (1.12).

2.5. **Residues.** It remains to show that the $D(\Lambda, \mathfrak{P}; s)$ does indeed have a pole at $s = 1/(n-1)$ and to compute the residue. We have already seen that only the summands $\widehat{f}(x; s)$ with $F_x = F_0$ contribute to the residue. Recall that $S = S' \cup \mathfrak{P}$, with S' the set of places of F dividing $n\infty$.

Lemma 2.7. *Let $x \in \mathscr{U}_S(n)$ with $F_x = F_0$. Then $x \in \mathscr{U}_{S'}(n)$.*

Proof. Let $a \in F^\times$ be any representative of x. Since $F_x = F_0$, there is $\alpha \in F_0$ with $\alpha^n = a$. Let $v \notin S'$ be any place of F. To prove the lemma, we must show that the v-adic valuation $\mathrm{ord}_v(a)$ is in $n\mathbb{Z}$. Since F_0/F is unramified outside S', we see that $F_v(\alpha)/F_v$ is unramified as well. Thus, with w the extension of v to $F_v(\alpha)$,

$$\mathrm{ord}_v(a) = \mathrm{ord}_w(a) = n \cdot \mathrm{ord}_w(\alpha) \in n\mathbb{Z}.$$

$\square$

Moreover, if $F_x = F_0$, almost all the local factors $\widehat{f}_v(x_v; s)$ are independent of x.

Lemma 2.8. *Let $x \in \mathscr{U}_{S'}(n)$ with $F_x = F_0$ and $v \notin S'$. Then*

$$\widehat{f}_v(x_v; s) = \begin{cases} \frac{1}{n} & \text{if } v \in \mathfrak{P}, \\ 1 & \text{if } v \notin \mathfrak{P} \text{ and } q_v \not\equiv 1 \bmod n, \\ 1 + \phi(n)q_v^{-(n-1)s} & \text{if } v \notin \mathfrak{P} \text{ and } q_v \equiv 1 \bmod n. \end{cases}$$

Proof. For $v \in \mathfrak{P}$, this is (2.7). For $v \notin \mathfrak{P}$ with $q_v \not\equiv 1 \bmod n$, it is Lemma 2.2. In the remaining case, it also follows from Lemma 2.2, since then $F_x = F_0$ implies that $d_v(x_v) = n$. Indeed, let $a \in F^\times$ be a representative of x and $\alpha \in F_0$ with $\alpha^n = a$. Since $q_v \equiv 1 \bmod n$, we get $F_{0,w} = F_v$ for any place w of F_0 above v, so $\alpha \in F_{0,w} = F_v$, and thus $a \in F_v^{\times n}$. $\square$

With $\alpha := n - 1$ and $\zeta_{F_0, v}(s)$ defined as the product of all local factors of $\zeta_{F_0}(s)$ at places above v, the residue of $D(\Lambda, \mathfrak{P}; s)$ at $1/(n-1)$ has the form $c(\Lambda, \mathfrak{P}) \mathrm{Res}_{s=1/\alpha} \zeta_{F_0}(\alpha s)$, where $c(\Lambda, \mathfrak{P}) := \lim_{s \to 1/\alpha} \zeta_{F_0}(\alpha s)^{-1} D(\Lambda, \mathfrak{P}; s)$. Using Lemma 2.7 and Lemma 2.8, we compute $c(\Lambda, \mathfrak{P})$ as

$$c(\Lambda, \mathfrak{P}) = \lim_{s \to 1/\alpha} \zeta_{F_0}(\alpha s)^{-1} F_n(\mathfrak{P}; s) = \frac{1}{|\mathscr{O}_F^\times / \mathscr{O}_F^{\times n}|} \sum_{x \in \mathscr{U}_S(n)} \lim_{s \to 1/\alpha} \zeta_{F_0}(\alpha s)^{-1} \widehat{f}(x; s)$$

$$= \frac{1}{|\mathscr{O}_F^\times / \mathscr{O}_F^{\times n}|} \sum_{\substack{x \in \mathscr{U}_{S'}(n) \\ F_x = F_0}} \prod_v \frac{\widehat{f}_v(x_v; 1/\alpha)}{\zeta_{F_0, v}(1)}$$

$$= \prod_{v \in \mathfrak{P}} \frac{1}{n \zeta_{F_0, v}(1)} \prod_{\substack{v \notin \mathfrak{P} \\ v \nmid n\infty \\ q_v \not\equiv 1 \bmod n}} \frac{1}{\zeta_{F_0, v}(1)} \prod_{\substack{v \notin \mathfrak{P} \\ v \nmid n\infty \\ q_v \equiv 1 \bmod n}} \frac{1 + \varphi(n)q_v^{-1}}{\zeta_{F_0, v}(1)}$$

$$\cdot \frac{1}{|\mathscr{O}_F^\times / \mathscr{O}_F^{\times n}|} \sum_{\substack{x \in \mathscr{U}_{S'}(n) \\ F_x = F_0}} \prod_{v | n\infty} \frac{\widehat{f}_v(x_v, 1/\alpha)}{\zeta_{F_0, v}(1)}$$

$$= \delta_{\mathfrak{p}_1} \cdots \delta_{\mathfrak{p}_l} \cdot c(\Lambda, \emptyset),$$

with $\delta_{\mathfrak{p}}$ as in (1.10). Thus, we identify the residue as

$$\delta_{\mathfrak{p}_1} \cdots \delta_{\mathfrak{p}_l} \frac{c_{F, n, \Lambda}}{n - 1},$$

with $c_{F, n, \Lambda} := (n - 1)c(\Lambda, \emptyset) \cdot \mathrm{Res}_{s=1/\alpha} \zeta_{F_0}(\alpha s)$.

To finish the proof of Proposition 1.7, we must show that $c(\Lambda, \emptyset) > 0$, so $D(\Lambda, \mathfrak{P}; s)$ does indeed have a pole at $s = 1/(n-1)$. We accomplish this first in the case $\Lambda = \Lambda_0 :=$

$(\{1\})_{v|n\infty}$, where all places $v \mid n\infty$ are required to split completely in K_φ/K. In this case, one sees immediately from the definition of the local fourier transform in [8, §3.3] that

$$\widehat{f}_v(x_v; s) = \begin{cases} 1 & \text{if } v \mid \infty \\ 1/n & \text{if } v \mid n. \end{cases}$$

Since moreover $x = 1 \in \mathscr{U}_{S'}(n)$ satisfies $F_x = F_0$, we conclude that

$$\sum_{\substack{x \in \mathscr{U}_{S'}(n) \\ F_x = F_0}} \prod_{v|n\infty} \frac{\widehat{f}_v(x_v, 1/\alpha)}{\zeta_{F_0,v}(1)} > 0,$$

which is enough to show that $c(\Lambda_0, \emptyset) > 0$. For general Λ, we have $D(\Lambda, \mathfrak{P}; s) \geq D(\Lambda_0, \mathfrak{P}; s)$ for all $s > 1/(n-1)$, and thus $D(\Lambda, \mathfrak{P}; s)$ must also have a pole at $s = 1/(n-1)$.

3. Proof of Theorem 1.6: Contour integration

In this section, we deduce Theorem 1.6 from Proposition 1.7.

3.1. **Preliminaries and set-up.** We need the following lemma to estimate the coefficients of a Dirichlet series. Still, all implied constants may always depend on F, n, l.

Lemma 3.1. *For $m \in \mathbb{N}$, let*

$$b_m := \{K/F \text{ cyclic}; \; [K:F] = n \;\; \text{and} \;\; \mathfrak{N}(\Delta(K/F)) = m\}.$$

Then $b_m \ll_\varepsilon m^\varepsilon$ holds for all $\varepsilon > 0$.

Proof. Let S be the set of all places of F dividing $mn\infty$. Every extension K/F with $\mathfrak{N}(\Delta(K/F)) = m$ is unramified outside S. From Lemma 2.1, we deduce the bound $b_m \ll n^{\phi(n)|S|} \ll_\varepsilon m^\varepsilon$. $\qquad\qquad\square$

Write $a_m := \#\{\varphi \in G\text{-ext}(F); \; \mathfrak{N}(\Delta(\varphi)) = m, \; f(\mathfrak{P}; \varphi) = 1\}$. Then

$$N_{\mathscr{T}_{F,n}}(\Lambda, \mathfrak{P}; X) = \sum_{m \leq X} a_m \quad \text{and} \quad D(\Lambda, \mathfrak{P}; s) = \sum_{m \in \mathbb{N}} \frac{a_m}{m^s}.$$

3.2. **The case** $n = 2$. Let us first consider the case $n = 2$. Choose $\eta \in (0, 1/2)$, $\sigma_0 \in (1, 1+\eta)$ and $T \in [1, X]$. By a truncated version of Perron's formula ([11, Corollary 5.3]), we see that

$$(3.1) \quad N_{\mathscr{T}_{F,n}}(\Lambda, \mathfrak{P}; X) - \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} D(\Lambda, \mathfrak{P}; s) \frac{X^s}{s} \mathrm{d}s$$

$$\ll \sum_{X/2 \leq m \leq 2X} a_m \min\left\{1, \frac{X}{T|X-m|}\right\} + \frac{4^{\sigma_0} + X^{\sigma_0}}{T} \sum_{m \in \mathbb{N}} \frac{a_m}{m^{\sigma_0}}.$$

Using Lemma 3.1 to estimate $a_m \ll_\varepsilon m^\varepsilon$ and replacing the minimum by its second term unless $|X - m| < 1$, the first error term is

$$(3.2) \qquad\qquad \ll_\varepsilon X^\varepsilon \left(1 + \frac{X}{T}(\log X)\right) \ll_\varepsilon \frac{X^{1+2\varepsilon}}{T}.$$

For $\varepsilon \in (0, \sigma_0 - 1)$, we see that the second error term is

$$(3.3) \qquad\qquad\qquad \ll_{\varepsilon, \sigma_0} \frac{X^{\sigma_0}}{T}.$$

Recall the analytic facts about $D(\Lambda, \mathfrak{P}; s)$ from Proposition 1.7. Shifting the line of integration to $\Re s = \sigma_1 := 1 - \lambda$, for some $\lambda \in (0, 1/2 - \eta]$, we see that the integral in (3.1) equals

$$(3.4)\quad 2\pi i \operatorname{Res}_{s=1}\left(D(\Lambda, \mathfrak{P}; s)\frac{X^s}{s}\right) + \left(-\int_{\sigma_1 - iT}^{\sigma_0 - iT} + \int_{\sigma_1 - iT}^{\sigma_1 + iT} + \int_{\sigma_1 + iT}^{\sigma_0 + iT}\right) D(\Lambda, \mathfrak{P}; s)\frac{X^s}{s}\mathrm{d}s.$$

Here,

$$\operatorname{Res}_{s=1}\left(D(\Lambda, \mathfrak{P}; s)\frac{X^s}{s}\right) = X \operatorname{Res}_{s=1}(D(\Lambda, \mathfrak{P}; s)) = \delta_{\mathfrak{p}_1 \cdots \mathfrak{p}_l} c_{F,n} X$$

is the main term in our asymptotic expansion of $N_{\mathscr{T}_{F,n}}(\mathfrak{P}; X)$. Let us estimate the integrals in (3.4) from above. Using the estimate (1.12), we see that

$$D(\Lambda, \mathfrak{P}; s) \ll_{\eta, \varepsilon} (\mathfrak{N}(\mathfrak{p}_1 \cdots \mathfrak{p}_l) T^m)^{\alpha(\eta + \lambda) + \varepsilon} \quad \text{for} \quad s \in (\sigma_1 \pm iT, \sigma_0 \pm iT),$$

and thus

$$(3.5)\quad \int_{\sigma_1 \pm iT}^{\sigma_0 \pm iT} D(\Lambda, \mathfrak{P}; s)\frac{X^s}{s}\mathrm{d}s \ll_{\eta, \varepsilon, \sigma_0, \lambda} \mathfrak{N}(\mathfrak{p}_1 \cdots \mathfrak{p}_l)^{\alpha(\eta + \lambda) + \varepsilon} T^{m\alpha(\eta + \lambda) + \varepsilon - 1} X^{\sigma_0}.$$

Moreover,

$$\int_{\sigma_1 - iT}^{\sigma_1 + iT} D(\Lambda, \mathfrak{P}; s)\frac{X^s}{s}\mathrm{d}s \ll_{\eta, \varepsilon, \lambda} X^{1 - \lambda}\mathfrak{N}(\mathfrak{p}_1 \cdots \mathfrak{p}_l)^{\alpha(\eta + \lambda) + \varepsilon}\left(1 + \int_{t=1}^{T} t^{m\alpha(\eta + \lambda) + \varepsilon - 1}\mathrm{d}t\right)$$

$$(3.6)\qquad\qquad\qquad \ll_{\eta, \lambda, \varepsilon} X^{1 - \lambda}\mathfrak{N}(\mathfrak{p}_1 \cdots \mathfrak{p}_l)^{\alpha(\eta + \lambda) + \varepsilon} T^{m\alpha(\eta + \lambda) + \varepsilon}.$$

To optimise our error terms in case $m \geq 3$, we choose ε small, $\eta = 4\varepsilon$, $\sigma_0 = 1 + 2\varepsilon$, $\lambda = 1/(2m\alpha)$ and $T = X^\lambda$. Then the sum of the error terms (3.2)–(3.6) is

$$\ll_\varepsilon \mathfrak{N}(\mathfrak{p}_1 \cdots \mathfrak{p}_l)^{1/(2m) + 3\varepsilon} X^{1 - 64/(103m) + 5\varepsilon}.$$

If $m \in \{1, 2\}$, we choose $\eta = 4\varepsilon$, $\sigma_0 = 1 + 2\varepsilon$, $\lambda = 1/2 - 5\varepsilon$, $T = X^{1/2}$. This allows us to bound the sum of (3.2)–(3.6) by

$$\ll_\varepsilon \mathfrak{N}(\mathfrak{p}_1 \cdots \mathfrak{p}_l)^{3/16 + \varepsilon} X^{1 - 13/32 + 6\varepsilon}$$

in case $m = 1$ and, if $m = 2$, by

$$\ll_\varepsilon \mathfrak{N}(\mathfrak{p}_1 \cdots \mathfrak{p}_l)^{103/512 + \varepsilon} X^{1 - 153/512 + 6\varepsilon}.$$

This concludes the proof of Theorem 1.6 when $n = 2$.

3.3. **The case** $n \geq 3$. In case $n \geq 3$, a direct application of the truncated Perron formula would not yield satisfactory bounds. Thus, as in standard proofs of tauberian theorems (see, e.g., [3, Appendice A]), we consider first the weighted counting function

$$\tilde{N}_{\mathscr{T}_{F,n}}(\Lambda, \mathfrak{P}; X) := \sum_{m \leq X} a_m \log(X/m).$$

Moreover, we observe that

$$2b = \min\{1/2, 1/(2\phi(n)m\alpha)\},$$

with $\alpha = 103/256$ as in Propositon 1.7. In the following derivations, ε denotes a small positive constant. Its precise value may change between its occurrences. From (1.12) with $\eta = \varepsilon$, we conclude that

$$(3.7)\qquad \frac{|s - 1/(n-1)|}{|s|} D(\Lambda, \mathfrak{P}; s) \ll_\varepsilon \mathfrak{N}(\mathfrak{p}_1 \cdots \mathfrak{p}_l)^{1/(2m) + \varepsilon}(1 + |\Im s|)^{1/2 + \varepsilon}$$

for $(n-1)\Re s \geq 1 - 2b + \varepsilon$.

Lemma 3.2. *We have the asymptotic formula*

$$\tilde{N}_{\mathscr{T}_{F,n}}(\Lambda, \mathfrak{P}; X) = (n-1)\delta_{\mathfrak{p}_1 \cdots \mathfrak{p}_l} c_{F,n} X^{1/(n-1)} + O_\varepsilon(\mathfrak{N}(\mathfrak{p}_1 \cdots \mathfrak{p}_l)^{1/(2m) + \varepsilon} X^{(1 - 2b)/(n-1) + \varepsilon}).$$

Proof. Let $\sigma_0 = 1/(n-1) + \varepsilon$. The integral representation

$$\tilde{N}_{\mathscr{T}_{F,n}}(\mathfrak{P}; X) = \frac{1}{2\pi i} \int_{\sigma_0 - i\infty}^{\sigma_0 + i\infty} D(\Lambda, \mathfrak{P}; s) \frac{X^s}{s^2} \mathrm{d}s$$

converges absolutely due to (3.7). Moving the line of integration to

$$\Re s = \sigma_1 := \frac{1 - 2b + \varepsilon}{n - 1},$$

we pick up the pole at $s = 1/(n-1)$ with residue

$$\mathrm{Res}_{s = \frac{1}{n-1}} \left(D(\Lambda, \mathfrak{P}; s) \frac{X^s}{s^2} \right) = (n-1)\delta_{\mathfrak{p}_1 \cdots \mathfrak{p}_l} c_{F,n} X^{1/(n-1)}.$$

Thus, $\tilde{N}_{\mathscr{T}_{F,n}}(\mathfrak{P}; X) - (n-1)\delta_{\mathfrak{p}_1 \cdots \mathfrak{p}_l} c_{F,n} X^{1/(n-1)}$ equals

$$\frac{1}{2\pi i} \lim_{T \to \infty} \left(-\int_{\sigma_1 - iT}^{\sigma_0 - iT} + \int_{\sigma_1 - iT}^{\sigma_1 + iT} + \int_{\sigma_1 + iT}^{\sigma_0 + iT} \right) D(\Lambda, \mathfrak{P}; s) \frac{X^s}{s^2} \mathrm{d}s.$$

The two horizontal integrals tend to 0 for $T \to \infty$, due to (3.7). The vertical integral becomes

$$\int_{\sigma_1 - i\infty}^{\sigma_1 + i\infty} D(\Lambda, \mathfrak{P}; s) \frac{X^s}{s^2} \mathrm{d}s \ll_\varepsilon X^{\sigma_1} \mathfrak{N}(\mathfrak{p}_1 \cdots \mathfrak{p}_l)^{1/(2m)+\varepsilon} \left(1 + \int_{t=1}^{\infty} t^{-3/2+\varepsilon} \mathrm{d}t \right),$$

which is covered by the Lemma's error term. $\qquad\qquad\qquad\qquad\qquad\square$

We now deduce an asymptotic formula for $N(X) := N_{\mathscr{T}_{F,n}}(\Lambda, \mathfrak{P}; X)$ from the formula for $\tilde{N}(X) := \tilde{N}_{\mathscr{T}_{F,n}}(\Lambda, \mathfrak{P}; X)$. Clearly, for $0 < u < 1$, we have

$$\frac{\tilde{N}(X(1-u)) - \tilde{N}(X)}{\log(1-u)} \le N(X) \le \frac{\tilde{N}(X(1+u)) - \tilde{N}(X)}{\log(1+u)}.$$

Moreover, for $u \in (-1, 1) \smallsetminus \{0\}$, it follows from Lemma 3.2 and the elementary inequality

$$|u| \le 2|\log(1+u)| \quad \text{for} \quad |u| < 1,$$

that

$$\frac{\tilde{N}(X(1+u)) - \tilde{N}(X)}{\log(1+u)} = (n-1)\delta_{\mathfrak{p}_1 \cdots \mathfrak{p}_l} c_{F,n} X^{1/(n-1)} \frac{(1+u)^{1/(n-1)} - 1}{\log(1+u)}$$
$$+ O_\varepsilon(\mathfrak{N}(\mathfrak{p}_1 \cdots \mathfrak{p}_l)^{1/(2m)+\varepsilon} X^{(1-2b)/(n-1)+\varepsilon} |u|^{-1}).$$

With the further elementary estimate

$$\frac{(1+u)^{1/(n-1)} - 1}{\log(1+u)} = \frac{1}{n-1} + O_\varepsilon(u), \quad \text{for} \quad u \in [-1+\varepsilon, 1] \smallsetminus \{0\},$$

and using (1.10), Theorem 1.5 follows immediately from the choice $u := \pm X^{-b/(n-1)}$.

4. HEIGHTS AND SMALL SPLITTING PRIMES

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 $d_v = [L_v : \mathbb{Q}_v]$ denotes the local degree at v. Note that this is exactly the height in [7,

(2.2)] for the principal divisor $(\alpha, (\alpha))$ associated to $\alpha \in K^\times$. For an extension of number fields K/F we also use the following invariant

$$\eta(K/F) = \inf\{H_K(\alpha); K = F(\alpha)\},$$

introduced in [17, 23], and also studied[4] in [21, 22]. First we recall the key lemma [7, Lemma 2.3] of Ellenberg and Venkatesh; in fact we state a slightly more precise version. Recall from [7] that a prime ideal $\mathfrak{B}$ of $\mathscr{O}_K$ is said to be an extension of a prime ideal from a subfield $K_0 \subsetneq K$ if there exists a prime ideal $\mathfrak{p}$ of $\mathscr{O}_{K_0}$ such that $\mathfrak{B} = \mathfrak{p}\mathscr{O}_K$. If $\mathfrak{B}$ and $\mathfrak{p}$ are non-zero prime ideals in $\mathscr{O}_K$ and $\mathscr{O}_F$ respectively and $\mathfrak{B} \mid \mathfrak{p}\mathscr{O}_K$ then we say $\mathfrak{B}$ is unramified in K/F if $\mathfrak{B}^2 \nmid \mathfrak{p}\mathscr{O}_K$.

Proposition 4.1 (Ellenberg and Venkatesh)**.** *Suppose $F \subseteq K$ are number fields, $[K : \mathbb{Q}] = d$, $\eta(K/F) > \mathfrak{N}(\Delta(K/F))^\gamma$, $\delta < \gamma/\ell$, and $\varepsilon > 0$. Moreover, suppose $\mathfrak{B}_1, \ldots, \mathfrak{B}_M$ are unramified prime ideals in K/F of norm $\mathfrak{N}(\mathfrak{B}_i) \leq \mathfrak{N}(\Delta(K/F))^\delta$ and are not extensions of prime ideals from any proper subfield of K containing F. Then we have*

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

Proof. Exactly as in [7, Lemma 2.3] except that we replace their Lemma 2.2 by the hypothesis $\eta(K/F) > \mathfrak{N}(\Delta(K/F))^\gamma$. $\qquad\square$

Recall that F is a number field of degree m with algebraic closure $\overline{F}$, and let $n \geq 2$ be an integer. We set

$$(4.1) \qquad\qquad \mathscr{F}_{F,n} := \{K \subseteq \overline{F}; F \subseteq K \text{ and } [K : F] = n\}$$

for the collection of all field extensions of F of degree n. For a subset $\mathscr{F} \subseteq \mathscr{F}_{F,n}$ we set

$$\mathscr{B}_{\mathscr{F}}(X; Y, M) := \left\{K \in \mathscr{F};\ D_K \leq X,\ \begin{array}{l}\text{at most } M \text{ prime ideals } \mathfrak{p} \text{ in } \mathscr{O}_F \text{ with}\\ \mathfrak{N}(\mathfrak{p}) \leq Y \text{ split completely in } K\end{array}\right\}.$$

The following proposition is a slight adaption of [25, Proposition 3.1]. The set up is chosen such that it applies in the most forward manner; in particular, that is the reason why we introduce the quantity $\tilde{\delta}_0$.

Proposition 4.2. *Suppose $\mathscr{F} \subseteq \mathscr{F}_{F,n}$, and suppose $\gamma > 0$ and $\theta \geq 0$ are such that*

$$\#\{K \in \mathscr{F}; D_K \leq X, \eta(K/F) \leq D_K^\gamma\} \ll_{\mathscr{F},\gamma,\theta} X^\theta.$$

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

$$\#\mathscr{B}_{\mathscr{F}}(X; X^{\delta_0}, X^{\delta_0-\varepsilon}) \leq E_{\delta_0,\varepsilon}(X).$$

Then we have

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

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

Proof. The proof is essentially identical to the one of [25, Proposition 3.1]; in short, use Proposition 4.1 and dyadic splitting. $\qquad\square$

---

[4]In the cited works the authors used the absolute instead of the relative height, and denoted the invariant by $\delta(K/k)$ and $\delta(K)$ respectively.

5. Ellenberg, Pierce and Wood's Chebyshev sieve

In this section we describe the Chebysev sieve recently introduced by Ellenberg, Pierce and Wood. This is one of the key ideas in their work [6] and allows them to show that almost all number fields of degree d have sufficiently many small splitting primes, at least if $d \leq 5$ (and excluding D_4-fields if $d = 4$). Our sieve setting is slightly more general than the original one in [6], but no new arguments are needed.

Let $P(z) := \prod_{\mathfrak{N}(\mathfrak{p}) \leq z} \mathfrak{p}$ be the product of all (non-zero) prime ideals in $\mathscr{O}_F$ of norm below z, and let $\mathscr{A}$ be a finite set of cardinality N. To each prime $\mathfrak{p}$ we associate a property $(\mathfrak{p})$ that an element of $\mathscr{A}$ might have or not have. We put

$$\mathscr{A}_\mathfrak{p} := \{a \in \mathscr{A}; a \text{ has property } (\mathfrak{p})\},$$

and for distinct primes $\mathfrak{p}, \mathfrak{q}$ we set $\mathscr{A}_{\mathfrak{p}\mathfrak{q}} := \mathscr{A}_\mathfrak{p} \cap \mathscr{A}_\mathfrak{q}$. Let $0 \leq \delta_\mathfrak{p} < 1$ and $R_\mathfrak{p}$ and $R_{\mathfrak{p},\mathfrak{q}}$ such that

$$\#\mathscr{A}_\mathfrak{p} = \delta_\mathfrak{p} N + R_\mathfrak{p},$$
$$\#\mathscr{A}_{\mathfrak{p}\mathfrak{q}} = \delta_\mathfrak{p} \delta_\mathfrak{q} N + R_{\mathfrak{p},\mathfrak{q}}.$$

Furthermore, we introduce

$$N(a) := \#\{\mathfrak{p}|P(z); a \in \mathscr{A}_\mathfrak{p}\}$$

and its mean

(5.1) $$M(z) := \frac{1}{N} \sum_{a \in \mathscr{A}} N(a) = \frac{1}{N} \sum_{\mathfrak{p}|P(z)} \#\mathscr{A}_\mathfrak{p}.$$

The quantity we want to bound from above is the number of $a \in \mathscr{A}$ for which $N(a)$ is significantly below the mean $M(z)$. For $M > 0$ let us introduce

$$E(\mathscr{A}; z, M) := \#\{a \in \mathscr{A}; N(a) \leq M\}.$$

In this setting their statement [6, Proposition 3.1] reads as follows.

Lemma 5.1 (Ellenberg, Pierce, Wood). *Suppose $M(z) > 0$. Then we have*

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

where $U(z) = \sum_{\mathfrak{p}|P(z)} \delta_\mathfrak{p}$.

Proof. The proof is exactly the same as in [6]. $\square$

5.1. Application of the Chebyshev sieve.

Let $\mathscr{F} \subseteq \mathscr{F}_{F,n}$, let $\mathscr{E}$ be a finite set of prime ideals $\mathfrak{p}$ in $\mathscr{O}_F$, and set

$$\mathscr{A} := \{K \in \mathscr{F}; D_K \leq X\}.$$

For (non-zero) prime ideals $\mathfrak{p}$ in $\mathscr{O}_F$ outside of $\mathscr{E}$ we let the property $(\mathfrak{p})$ be "$\mathfrak{p}$ splits completely", so that $\mathscr{A}_\mathfrak{p}$ is the set of fields K in $\mathscr{A}$ in which $\mathfrak{p}$ splits completely, and we set $\mathscr{A}_\mathfrak{p} = \emptyset$ if $\mathfrak{p} \in \mathscr{E}$. Let $\mathfrak{e} = \mathfrak{p}$ or $\mathfrak{e} = \mathfrak{p}\mathfrak{q}$ for distinct prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ in $\mathscr{O}_F$. Put $N_\mathscr{F}(X) := \#\mathscr{A}$, $N_\mathscr{F}(\mathfrak{e}; X) := \#\mathscr{A}_\mathfrak{p}$ if $\mathfrak{e} = \mathfrak{p}$ and $N_\mathscr{F}(\mathfrak{e}; X) := \#(\mathscr{A}_\mathfrak{p} \cap \mathscr{A}_\mathfrak{q})$ if $\mathfrak{e} = \mathfrak{p}\mathfrak{q}$. Suppose that $c_\mathscr{F} > 0$, $0 \leq \tau < \rho \leq 1$, and $\sigma \geq 0$, and that we have

(5.2) $$N_\mathscr{F}(X) = c_\mathscr{F} X^\rho + O_{\mathscr{F},\varepsilon}\left(X^{\tau+\varepsilon}\right),$$

(5.3) $$N_\mathscr{F}(\mathfrak{e}; X) = \delta_\mathfrak{e} c_\mathscr{F} X^\rho + O_{\mathscr{F},\varepsilon}\left((\mathfrak{N}(\mathfrak{e}))^\sigma X^{\tau+\varepsilon}\right),$$

where $\delta_\mathfrak{e}$ is a multiplicative function with $1 \ll_\mathscr{F} \delta_\mathfrak{p} \leq 1$ if $\mathfrak{p} \notin \mathscr{E}$ and $\delta_\mathfrak{p} = 0$ if $\mathfrak{p} \in \mathscr{E}$.

Note that with $N := N_\mathscr{F}(X)$ we have

$$N_\mathscr{F}(\mathfrak{e}; X) = \delta_\mathfrak{e} N + O_{\mathscr{F},\varepsilon}\left((\mathfrak{N}(\mathfrak{e}))^\sigma X^{\tau+\varepsilon}\right),$$

and hence,

$$|R_{\mathfrak{p}}| = O_{\mathscr{F},\varepsilon}\left((\mathfrak{N}(\mathfrak{p}))^{\sigma} X^{\tau+\varepsilon}\right),$$
$$|R_{\mathfrak{p},\mathfrak{q}}| = O_{\mathscr{F},\varepsilon}\left((\mathfrak{N}(\mathfrak{p}\mathfrak{q}))^{\sigma} X^{\tau+\varepsilon}\right).$$

Lemma 5.2. *Suppose that $\varepsilon > 0$ and*

$$\delta_0 \leq \frac{\rho - \tau}{1 + 2\sigma}.$$

Then we have

$$\frac{X^{\delta_0}}{\log X} \ll_{\mathscr{F},\delta_0,\mathscr{E}} M(X^{\delta_0}) \ll_{\mathscr{F},\delta_0,\mathscr{E}} \frac{X^{\delta_0}}{\log X},$$

and

$$E(\mathscr{A}; X^{\delta_0}, \frac{1}{2}M(X^{\delta_0})) \ll_{\mathscr{F},\delta_0,\mathscr{E},\varepsilon} X^{\rho-\delta_0+\varepsilon},$$

provided X is large enough in terms of $\mathscr{F}, \delta_0, \mathscr{E}$, and ε.

Proof. We follow the proof of [6, Proposition 6.1] with the obvious modifications. In this proof the implicit constants in the Vinogradov-symbols and in the $O(\cdot)$-notation depend only on $\mathscr{F}, \delta_0, \mathscr{E}$, and ε. First we note that

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

Now

$$U(z) = \sum_{\mathfrak{p}|P(z)} \delta_{\mathfrak{p}} = \sum_{\substack{\mathfrak{p}|P(z) \\ \mathfrak{p}\notin\mathscr{E}}} \delta_{\mathfrak{p}},$$

and using Landau's prime ideal theorem we find that for $z \gg 1$ we have

$$c_0 z(\log z)^{-1} \leq U(z) \leq 2z(\log z)^{-1},$$

for a constant $c_0 > 0$ depending on $\mathscr{F}$ and $\mathscr{E}$. Now we use (5.1) to compute the mean

$$M(z) = U(z) + \frac{1}{\#\mathscr{A}} \sum_{\mathfrak{p}|P(z)} |R_{\mathfrak{p}}| = U(z) + O_{\mathscr{F},\varepsilon}(z^{1+\sigma} X^{\tau-\rho+\varepsilon}).$$

From now on we assume that $z = X^{\delta_0}$. Noting that $\delta_0 \leq \frac{\rho-\tau}{1+2\sigma} < \frac{\rho-\tau}{\sigma}$ we conclude that for sufficiently large X the last error term is bounded by $U(z)/2$, and hence for $X \gg 1$ we get

$$c_1 X^{\delta_0}(\log X)^{-1} \leq \frac{1}{2}U(X^{\delta_0}) \leq M(X^{\delta_0}) \leq \frac{3}{2}U(X^{\delta_0}) \leq c_2 X^{\delta_0}(\log X)^{-1}$$

for constants $0 < c_1 < c_2 \leq 1$ depending only on $\mathscr{F}, \delta_0$ and $\mathscr{E}$. Applying Lemma 5.1 and simplifying terms yields

$$E(\mathscr{A}; X^{\delta_0}, \frac{1}{2}M(X^{\delta_0})) \ll X^{\varepsilon}(X^{\rho-\delta_0} + X^{2\sigma\delta_0+\tau}) \leq 2X^{\rho-\delta_0+\varepsilon}.$$

$\square$

We conclude from Lemma 5.2 that for $X \gg_{\mathscr{F},\delta_0,\mathscr{E},\varepsilon} 1$ we have $E(\mathscr{A}; X^{\delta_0}, X^{\delta_0-\varepsilon}) \leq E(\mathscr{A}; X^{\delta_0}, \frac{1}{2}M(X^{\delta_0}))$, and thus

(5.4) $$E(\mathscr{A}; X^{\delta_0}, X^{\delta_0-\varepsilon}) \ll_{\mathscr{F},\delta_0,\mathscr{E},\varepsilon} X^{\rho-\delta_0+\varepsilon}.$$

6. Proofs of Theorems 1.2 and 1.3

In this section we fix $\mathscr{F} \subseteq \mathscr{F}_{F,n}$ and $\mathscr{E}$, and we suppose that we are in exactly the same setting as in §5.1. In particular, we have (5.2) and (5.3), with a multiplicative function $\delta_{\mathfrak{e}}$ that satisfies $1 \ll_{\mathscr{F}} \delta_{\mathfrak{p}} \leq 1$ if $\mathfrak{p} \notin \mathscr{E}$ and $\delta_{\mathfrak{p}} = 0$ if $\mathfrak{p} \in \mathscr{E}$. Furthermore, we set

$$(6.1) \qquad \tilde{\delta}_0 := \frac{\rho - \tau}{1 + 2\sigma}.$$

Proposition 6.1. *Let $\varepsilon > 0$. Then we have*

$$(6.2) \qquad \#Cl_K[\ell] \ll_{\mathscr{F},\ell,\varepsilon} D_K^{1/2 - \min\{\frac{1}{2\ell(n-1)}, \tilde{\delta}_0\} + \varepsilon}$$

for all but $O_{\mathscr{F},\tilde{\delta}_0,\mathscr{E},\varepsilon}(X^{\rho - \min\{\frac{1}{2\ell(n-1)}, \tilde{\delta}_0\} + \varepsilon})$ fields K in $\mathscr{F}$ with $D_K \leq X$.

Proof. We have $\#\mathscr{B}_{\mathscr{F}}(X; Y, M) \leq E(\mathscr{A}; Y, M)$, so that (5.4) provides the required bound for $\#\mathscr{B}_{\mathscr{F}}(X; X^{\delta_0}, X^{\delta_0 - \varepsilon})$. Furthermore, from [7, Lemma 2.2] (see also [20] for an older and more general result) we have $\eta(K/F) \gg_{F,n} D_K^{1/(2(n-1))}$. Hence we can apply Proposition 4.2 with $\gamma = 1/(2(n-1)) + \varepsilon$, $\theta = 0$, and $\tilde{\delta}_0$ as defined in (6.1). This completes the proof of Proposition 6.1. $\qquad\square$

6.1. **Proof of Theorem 1.3.** Now we restrict ourselves to those families for which Theorem 1.6 provides the required asymptotic formulas (5.2) and (5.3). For every place $v \mid n\infty$ of F, let M_v be a set of Galois-extensions $K \subseteq \overline{F}_v$ of F_v with cyclic Galois group of order dividing n, and assume that $F_v \in M_v$. For $K \in \mathscr{F}_{F,n}$, we write $K_v \in M_v$ if the completion K_w at any place w of K above v is F_v-isomorphic to a field in M_v. Writing $M = (M_v)_{v \mid n\infty}$, we consider the family

$$\mathscr{F}_{F,n}(M) := \{K \in \mathscr{F}_{F,n};\ K_v \in M_v \text{ for all } v \mid n\infty\}.$$

We define

$$\tilde{\delta}' = \tilde{\delta}'(m,n) := \frac{b}{(n-1)(1+2a)},$$

where $a = a(m,n)$ and $b = b(m,n)$ are defined in Theorem 1.6. Using the bounds (1.11), one sees easily that $\tilde{\delta}' \geq \tilde{\delta}$, where $\tilde{\delta}$ is defined in (1.8). Hence, the following theorem is a more precise and slightly more general version of Theorem 1.3.

Theorem 6.2. *Suppose F and $\mathbb{Q}(\mu_n(\overline{F}))$ are linearly disjoint over $\mathbb{Q}$, and $\varepsilon > 0$. Then for all but $O_{F,n,\varepsilon}(X^{\frac{1}{n-1} - \min\{\frac{1}{2\ell(n-1)}, \tilde{\delta}'\} + \varepsilon})$ fields K in $\mathscr{F}_{F,n}(M)$ with $D_K \leq X$, we have*

$$\#Cl_K[\ell] \ll_{F,n,\ell,\varepsilon} D_K^{\frac{1}{2} - \min\{\frac{1}{2\ell(n-1)}, \tilde{\delta}'\} + \varepsilon}.$$

Proof. Take $\mathscr{F} := \mathscr{F}_{F,n}(M)$ and $\mathscr{E}$ to be the set of those prime ideals in $\mathscr{O}_F$ that divide the ideal $n\mathscr{O}_F$. Then by Theorem 1.6 we have (5.2) and (5.3) with $\rho = 1/(n-1)$, $\sigma = a + \varepsilon'$ and $\tau = (1-b)/(n-1)$, and $\delta_{\mathfrak{e}}$ is a multiplicative function with $\delta_{\mathfrak{p}}$ as defined in (1.10) if $\mathfrak{p} \notin \mathscr{E}$ and $\delta_{\mathfrak{p}} = 0$ otherwise. Applying Proposition 6.1 with

$$\tilde{\delta}_0 = \frac{\rho - \tau}{1 + 2\sigma} = \frac{b}{(n-1)(1+2a+2\varepsilon')}$$

and using that $\varepsilon' > 0$ can be chosen arbitrarily small proves the theorem. $\qquad\square$

6.2. **Proof of Theorem 1.2: improving the GRH-bound.** Here we lay out a general strategy to improve upon the GRH-bound building on an idea from [25]. We still fix $\mathscr{F} \subseteq \mathscr{F}_{F,n}$ and $\mathscr{E}$, and we continue to assume that we have (5.2) and (5.3). The idea is to show that for "most" extensions K/F the lower bound for the crucial quantity $\eta(K/F)$ is significantly bigger than Silverman's bound $D_K^{1/(2(n-1))}$, and then to capitalise on this via Proposition 4.2.

We introduce the set of elements in $\overline{F}$ that generate a field in $\mathscr{F}$

$$P_{\mathscr{F}} := \{\alpha \in \overline{F}; F(\alpha) \in \mathscr{F}\},$$

and its counting function

$$N_H(P_{\mathscr{F}}, X) := \#\{\alpha \in P_{\mathscr{F}}; H_{F(\alpha)}(\alpha) \leq X\}.$$

If we have a good upper bound on this counting function then we can improve the exponent in (6.2).

Proposition 6.3. *Suppose λ is a real number such that*

$$N_H(P_{\mathscr{F}}, X) \ll_{\mathscr{F},\lambda} X^{\lambda},$$

and suppose $\gamma \geq 0$, and $\varepsilon > 0$. Then we have

$$\#Cl_K[\ell] \ll_{\mathscr{F},\ell,\gamma,\varepsilon} D_K^{1/2-\min\{\frac{\gamma}{\ell},\tilde{\delta}_0\}+\varepsilon}$$

for all but $O_{\mathscr{F},\tilde{\delta}_0,\gamma,\lambda,\mathscr{E},\varepsilon}(X^{\rho-\min\{\frac{\gamma}{\ell},\tilde{\delta}_0\}+\varepsilon} + X^{\lambda\gamma})$ fields K in $\mathscr{F}$ with $D_K \leq X$.

Proof. Observe that the image of the map $\alpha \to F(\alpha)$ with domain

$$\{\alpha \in P_{\mathscr{F}}; H_{F(\alpha)}(\alpha) \leq X^{\gamma}\}$$

covers the set

$$\{K \in \mathscr{F}; D_K \leq X, \eta(K/F) \leq D_K^{\gamma}\}.$$

Using the hypothesis we conclude that

$$(6.3) \qquad \#\{K \in \mathscr{F}; D_K \leq X, \eta(K/F) \leq D_K^{\gamma}\} \leq N_H(P_{\mathscr{F}}, X^{\gamma}) \ll_{\mathscr{F},\lambda} X^{\lambda\gamma}.$$

As in the proof of Proposition 6.1 we apply Proposition 4.2 with $\tilde{\delta}_0$ as defined in (6.1), but this time with $\theta = \lambda\gamma$. This completes the proof of Proposition 6.3. $\square$

Let us now consider the special case $\mathscr{F} = \mathscr{F}_{F,n}$. Note that for $F = \mathbb{Q}$ the cardinality of the set of algebraic numbers of degree n over F with height at most X is bounded from above by n times the number of (irreducible) degree n polynomials in $\mathbb{Z}[x]$ of Mahler measure at most X. The Mahler measure in turn is bounded from below by 2^{-n} times the maximum norm of the coefficient vector. This shows that for $F = \mathbb{Q}$

$$N_H(P_{\mathscr{F}}, X) \ll_n X^{n+1}.$$

For arbitrary ground fields F a similar argument applies (see [19, Theorem]) and provides

$$(6.4) \qquad\qquad N_H(P_{\mathscr{F}}, X) \ll_{n,m} X^{n+1}.$$

Of course, this bound also holds for any $\mathscr{F} \subseteq \mathscr{F}_{F,n}$. Applying Proposition 6.3 with this bound proves the following theorem.

Theorem 6.4. *Suppose F is a number field and $\mathscr{F} \subseteq \mathscr{F}_{F,n}$ such that (1.5) and (1.6) do hold. Let $\varepsilon > 0$ and $0 \leq \gamma < 1/(n+1)$. Then for all but*

$$O_{\mathscr{F},\tilde{\delta}_0,\gamma,\mathscr{E},\varepsilon}(X^{1-\min\{\frac{\gamma}{\ell},\tilde{\delta}_0\}+\varepsilon} + X^{\gamma(n+1)})$$

fields K in $\mathscr{F}$ with $D_K \leq X$, we have

$$\#Cl_K[\ell] \ll_{\mathscr{F},\ell,\gamma,\varepsilon} D_K^{\frac{1}{2}-\min\{\frac{\gamma}{\ell},\tilde{\delta}_0\}+\varepsilon}.$$

Assuming the hypotheses of Theorem 6.4 and taking γ close enough to $1/(n+1)$ shows that for $\ell > 1/(\tilde{\delta}_0(n+1))$, the bound (1.7) holds true for 100% of $K \in \mathscr{F}$, counted by discriminant, thus proving Theorem 1.2.

To get an improvement in Theorem 1.3 we would need that with $\mathscr{F} = \mathscr{T}_{F,n}$

$$(6.5) \qquad\qquad N_H(P_{\mathscr{F}}, X) \ll_{\mathscr{F}} X^{\lambda}$$

for some $\lambda < 2$. However, by Schanuel's Theorem [18] even the contribution from a single field $K \in \mathscr{F}$ is already $\gg_K X^2$, so that (6.5) with $\lambda < 2$ cannot be true.

6.3. **Further remarks.**

Finally, for $e \mid n$ let $\mathscr{F}_{F,n}(e) \subseteq \mathscr{F}_{F,n}$ be the subfamily of fields K that contain a field $F \subseteq L \subseteq K$ of degree $[L : F] = e$. For $\mathscr{F} = \mathscr{F}_{\mathbb{Q},n}(e)$ it follows immediately from [24, Theorem 1.1] that

$$(6.6) \qquad N_H(P_{\mathscr{F}}, X) \ll_{e,n} X^{e+n/e}.$$

Applying Proposition 6.3 with $\mathscr{F} = \mathscr{F}_{\mathbb{Q},n}(e)$, and using the above bound (6.6) proves that if (1.5) and (1.6) do hold for $\mathscr{F} = \mathscr{F}_{\mathbb{Q},n}(e)$, then we have

$$\#Cl_K[\ell] \ll_{e,n,\ell,\varepsilon} D_K^{\frac{1}{2}-\min\{\frac{1}{\ell(e+n/e)},\bar{\delta}_0\}+\varepsilon}$$

for 100% of all fields K in $\mathscr{F}_{\mathbb{Q},n}(e)$. Particularly interesting is the case $n = e^2$. In this case we would get for all sufficiently large ℓ and 100% of the fields $K \in \mathscr{F}_{F,n}(\sqrt{n})$ an improvement over the trivial exponent by $1/(2\ell\sqrt{n})$ whereas in all other known cases of families the improvement decays like $O(1/n)$ as n gets large.

Unfortunately, the required multiplicativity of $\delta_{\mathfrak{e}}$ may not hold for the family $\mathscr{F}_{\mathbb{Q},n}(e)$, no matter how we choose $\mathscr{E}$. However, note that if $\mathscr{F}$ is a subfamily of $\mathscr{F}_{\mathbb{Q},n}(e)$ with linear growth rate, and we can guarantee the existence of sufficiently many small splitting primes for 100% of all $K \in \mathscr{F}$ then Proposition 4.1 combined with (6.3) and (6.6) provide an improvement to the GRH-bound for 100% of all $K \in \mathscr{F}$. For example, if we assume GRH then we have an improvement over the trivial exponent by $1/(\ell(e + n/e))$ instead of just $1/(2\ell(n-1))$.

References

1. 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* , preprint, arXiv:1701.02458v1, 2017.
2. V. Blomer and F. Brumley, *On the Ramanujan conjecture over number fields*, Ann. of Math. (2) **174** (2011), no. 1, 581–605. MR 2811610
3. A. Chambert-Loir and Yu. Tschinkel, *Fonctions zêta des hauteurs des espaces fibrés*, Rational points on algebraic varieties, Progr. Math., vol. 199, Birkhäuser, Basel, 2001, pp. 71–115. MR 1875171 (2003a:11079)
4. H. Cohen and J. Martinet, *Étude heuristique des groupes de classes des corps de nombres*, Journal für die Reine und Angewandte Mathematik **404** (1990), 39–76.
5. W. Duke, *Bounds for arithmetic multiplicities*, Proceedings of the International Congress of Mathematicians. Berlin, 1998.
6. J. Ellenberg, L. B. Pierce, and M. M. Wood, *On ℓ-torsion in class groups of number fields*, Algebra Number Theory (to appear, 2017), 25 pp.
7. J. Ellenberg and A. Venkatesh, *Reflection principles and bounds for class group torsion*, Int. Math. Res. Not. **no.1, Art. ID rnm002** (2007).
8. C. Frei, D. Loughran, and R. Newton, *The Hasse norm principle for abelian extensions*, Amer. J. Math. (to appear, 2017).
9. D. R. Heath-Brown, *Hybrid bounds for Dirichlet L-functions. II*, Quart. J. Math. Oxford Ser. (2) **31** (1980), no. 122, 157–167. MR 576334
10. 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.
11. H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007. MR 2378655
12. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Springer-Verlag, Berlin, 1980.
13. L. B. Pierce, *3-part of class numbers of quadratic fields*, J. London Math. Soc. **71** (2005), 579–598.
14. ———, *A bound for the 3-part of class numbers of quadratic fields by means of the square sieve*, Forum Math. **18** (2006), 677–698.
15. L. B. Pierce, C. L. Turnage-Butterbaugh, and M. M. Wood, *An effective Chebotarev density theorem for families of number fields, with an application to ℓ-torsion in class groups*, preprint, arXiv:1709.09637v1, 2017.

16. N. Rome, *The Hasse Norm Principle For Biquadratic Extensions*, preprint, arXiv:1707.00412v1, 2017.

17. D. Roy and J. L. Thunder, *A note on Siegel's lemma over number fields*, Monatsh. Math. **120** (1995), 307–318.

18. S. H. Schanuel, *Heights in number fields*, Bull. Soc. Math. France **107** (1979), 433–449.

19. W. M. Schmidt, *Northcott's Theorem on heights I. A general estimate*, Monatsh. Math. **115** (1993), 169–183.

20. J. Silverman, *Lower bounds for height functions*, Duke Math. J. **51** (1984), 395–403.

21. 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.

22. _____, *Number fields without small generators*, Math. Proc. Cam. Philos. Soc. **159, no. 3** (2015), 379–385.

23. M. Widmer, *Counting primitive points of bounded height*, Trans. Amer. Math. Soc. **362** (2010), 4793–4829.

24. _____, *On number fields with nontrivial subfields*, Int. J. Number Theory **7** (2011), 695–720.

25. _____, *Bounds for the ℓ-torsion in class groups*, submitted (2017), 8 pp.

26. D. J. Wright, *Distribution of discriminants of abelian extensions*, Proc. London Math. Soc. (3) **58** (1989), no. 1, 17–50. MR 969545 (90b:11115)

27. H. Wu, *Burgess-like subconvexity for GL_1*, preprint, arXiv:1604.08551v3, 2016.

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

School of Mathematics, University of Manchester, Oxford Road, Manchester M13 9PL, UK

   E-mail address: `christopher.frei@manchester.ac.uk`

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

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