COUNTING PROBLEMS: CLASS GROUPS, PRIMES, AND NUMBER FIELDS

LILLIAN B. PIERCE

ABSTRACT

Each number field has an associated finite abelian group, the class group, that records certain properties of arithmetic within the ring of integers of the field. The class group is well studied, yet also still mysterious. A central conjecture of Brumer and Silverman states that for each prime ℓ, every number field has the property that its class group has very few elements of order ℓ, where "very few" is measured relative to the absolute discriminant of the field. This paper surveys recent progress toward this conjecture, and outlines its close connections to counting prime numbers, counting number fields of fixed discriminant, and counting number fields of bounded discriminant.

MATHEMATICS SUBJECT CLASSIFICATION 2020

Primary 11R29; Secondary 11R45, 11N05

KEYWORDS

Class groups, counting number fields, distribution of primes

ICM INTERNATIONAL CONGRESS OF MATHEMATICIANS 2022 JULY 6—14

Proc. Int. Cong. Math. 2022, Vol. 3, pp. 1940–1965
DOI 10.4171/ICM2022/104

1. HISTORICAL PRELUDE

In a 1640 letter to Mersenne, Fermat stated that an odd prime p satisfies $p = x^2 + y^2$ if and only if $p \equiv 1 \pmod 4$. Roughly 90 years later, Euler learned of Fermat's statement through correspondence with Goldbach, and by 1749, he worked out a proof. This fits into a bigger question, which Euler studied as well: for each $n \geq 1$, which primes can be written as $p = x^2 + ny^2$? Even more generally: which binary quadratic forms $ax^2 + bxy + cy^2$ represent a given integer m? This question also motivated work of Lagrange and Legendre, and then appeared in Gauss's celebrated 1801 work *Disquisitiones Arithmeticae*; see [26].

Gauss partitioned binary quadratic forms of discriminant $D = b^2 - 4ac$ into equivalence classes under $\mathrm{SL}_2(\mathbb{Z})$ changes of variable. (Here we will speak only of *fundamental* discriminants D; for notes on the original setting, see [84].) Gauss showed that for each D there are finitely many such classes (the cardinality is the *class number*, denoted $h(D)$), and verified that the classes obey a group law (composition). Based on extensive computation, Gauss noticed that as $D \to -\infty$, small class numbers stopped appearing, writing: "*Nullum dubium esse videtur, quin series adscriptae revera abruptae sint…Demonstrationes autem* rigorosae *harum observationum perdifficiles esse videntur.*" ("It seems beyond doubt that the sequences written down do indeed break off… However, *rigorous* proofs of these observations appear to be most difficult" [43, P. 13].) As $D \to +\infty$, a quite different behavior seemed to appear, leading to a conjecture that $h(D) = 1$ for infinitely many $D > 0$.

It is hard to exaggerate the interest these two conjectures have generated. In the 1830s, Dirichlet proved a class number formula, relating the class number $h(D)$ of a (fundamental) discriminant D to the value $L(1, \chi)$ of an L-function associated to a real primitive character χ modulo D. Consequently, throughout the 1900s, Gauss's questions were studied via the theory of the complex-variable functions $L(s, \chi)$. A remarkable series of works by Hecke, Deuring, Mordell, and Heilbronn confirmed that for $D < 0$ the class number $h(D)$ attains any value only finitely many times. How many times? Famously, the work of Heegner, Baker, and Stark proved that there are 9 (fundamental) discriminants $D < 0$ with class number 1. In full generality, Goldfeld showed an effective lower bound for $h(D)$ when $D < 0$ would follow from a specific case of the Birch–Swinnerton-Dyer conjecture, which was then verified by Gross and Zagier; see [42]. Now, for each $1 \leq N \leq 100$, one may find the number of discriminants $D < 0$ with $h(D) = N$ in [93]. As for the other conjecture, that infinitely many (fundamental) discriminants $D > 0$ have class number 1, this remains open, and very mysterious. These historical antecedents hint at the intertwined currents of "counting" and the analytic study of L-functions, which will also be present in the work we will survey.

We briefly mention another historical motivation for the study of class numbers, namely the failure of unique factorization. For example, in the ring $\mathbb{Z}[\sqrt{-5}]$, $21 = 3 \cdot 7$ but it also factors into irreducible, nonassociated factors as $(1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$. Here is a problem where the failure of unique factorization has an impact. Suppose one is searching for solutions $x, y, z \in \mathbb{N}$ to the equation $x^p + y^p = z^p$ for a prime $p \geq 3$. If a nontrivial

solution (x, y, z) exists, then for ζ_p a pth root of unity, we could write

$$y \cdot y \cdots y = (z - x)(z - \zeta_p x) \cdots (z - \zeta_p^{p-1} x).$$

If $\mathbb{Z}[\zeta_p]$ possesses unique factorization, two such factorizations cannot exist, so (x, y, z) cannot exist—verifying Fermat's Last Theorem for this exponent p. But to the disappointment of many, unique factorization fails in $\mathbb{Z}[\zeta_p]$ for infinitely many p. As Neukirch writes, "Realizing the failure of unique factorization in general has led to one of the grand events in the history of number theory, the discovery of ideal theory by Eduard Kummer" [69, CH. I §3].

1.1. The class group

Let $K/\mathbb{Q}$ be a number field of degree n, with associated ring of integers $\mathcal{O}_K$. Every proper integral ideal $\mathfrak{a} \subset \mathcal{O}_K$ factors into a product of prime ideals $\mathfrak{p}_1 \cdots \mathfrak{p}_k$ in a unique way (salvaging the notion of unique factorization). Moreover, the fractional ideals of K form an abelian group J_K, the free abelian group on the set of nonzero prime ideals of $\mathcal{O}_K$. In the case that every ideal in J_K belongs to the subgroup P_K of principal ideals, $\mathcal{O}_K$ is a principal ideal domain, and unique factorization holds in $\mathcal{O}_K$. But more typically, some "expansion" occurs when passing to ideals; the class group of K is defined to measure this.

The class group of K is the quotient group

$$\mathrm{Cl}_K = J_K / P_K.$$

The elements in Cl_K are ideal classes, and the cardinality $|\mathrm{Cl}_K|$ is the class number. The quotient J_K/P_K is trivial (so that every ideal is a principal ideal, and $|\mathrm{Cl}_K| = 1$) precisely when unique factorization holds in $\mathcal{O}_K$. (Thus the above strategy for Fermat's Last Theorem works for p if $|\mathrm{Cl}_{\mathbb{Q}(\zeta_p)}| = 1$. In fact, Kummer showed that as long as the class number of $\mathbb{Q}(\zeta_p)$ is indivisible by p, the argument can be salvaged; see [31]. Such a prime is called a regular prime. Here is an open question: are there infinitely many regular prime numbers?)

By a result of Minkowski in the geometry of numbers, every ideal class in Cl_K contains an integral ideal $\mathfrak{b}$ with norm $\mathfrak{N}(\mathfrak{b}) = (\mathcal{O}_K : \mathfrak{b})$ satisfying

$$\mathfrak{N}(\mathfrak{b}) \le (2/\pi)^s \sqrt{D_K}, \tag{1.1}$$

where $D_K = |\mathrm{Disc}(K/\mathbb{Q})|$ and s counts the pairs of complex embeddings of K. As there are finitely many integral ideals of any given norm, Landau deduced (see [68, THM. 4.4]):

$$|\mathrm{Cl}_K| \ll_n D_K^{1/2} \log^{n-1} D_K. \tag{1.2}$$

In particular, the class group of a number field K is always a finite abelian group. (Throughout, $A \ll_\kappa B$ indicates that there exists a constant C_κ such that $|A| \le C_\kappa B$.)

When $K = \mathbb{Q}(\sqrt{D})$ is a quadratic field, this relates in a precise way to Gauss's construction of the class number for binary quadratic forms of discriminant D (see [8]). In modern terms, Gauss asked whether for each $h \in \mathbb{N}$, there are finitely many imaginary quadratic fields K with $|\mathrm{Cl}_K| = h$? (Yes.) Are there infinitely many real quadratic fields K with $|\mathrm{Cl}_K| = 1$? (We do not know.) In fact, here is an open question: are there infinitely many number fields, of arbitrary degrees, with class number 1? Here is another open question: are

there infinitely many number fields, of arbitrary degrees, with bounded class number? These difficult questions must consider the regulator R_K of the field K, due to the (ineffective) inequalities by Siegel (for quadratic fields) and Brauer (in general) [68, CH. 8]:

$$D_K^{1/2-\varepsilon} \ll_{n,\varepsilon} |\mathrm{Cl}_K| R_K \ll_{n,\varepsilon} D_K^{1/2+\varepsilon}, \quad \text{for all } \varepsilon > 0.$$

2. THE ℓ-TORSION CONJECTURE

In addition to studying the size of the class group, it is also natural to study its structure. We will focus on the ℓ-torsion subgroup, defined for each integer $\ell \geq 2$ by

$$\mathrm{Cl}_K[\ell] = \{[\mathfrak{a}] \in \mathrm{Cl}_K : [\mathfrak{a}]^\ell = \mathrm{Id}\}.$$

For example, the class number is divisible by a prime ℓ precisely when $|\mathrm{Cl}_K[\ell]| > 1$. Related problems include studying the exponent of the class group, or counting how many number fields of a certain degree have class number divisible, or indivisible, by a given prime ℓ. Such problems are addressed for imaginary quadratic fields in [4, 44, 45, 82].

In this survey, we will focus on upper bounds for the ℓ-torsion subgroup. The Minkowski bound (1.2) provides an upper bound for any field of degree n, and all ℓ:

$$1 \leq \left|\mathrm{Cl}_K[\ell]\right| \leq |\mathrm{Cl}_K| \ll_{n,\varepsilon} D_K^{1/2+\varepsilon}, \quad \text{for all } \varepsilon > 0. \tag{2.1}$$

Our subject is a conjecture on the size of the ℓ-torsion subgroup, which suggests that (2.1) is far from the truth. We will focus primarily on cases when ℓ is prime, since $|\mathrm{Cl}_K[m]|$ is multiplicative as a function of m, and for a prime ℓ, $|\mathrm{Cl}_K[\ell^t]| \leq |\mathrm{Cl}_K[\ell]|^t$ (see [73]).

Conjecture 2.1 (ℓ-torsion conjecture). *Fix a degree $n \geq 2$ and a prime ℓ. Every number field $K/\mathbb{Q}$ of degree n satisfies $|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\varepsilon}$ for all $\varepsilon > 0$.*

This conjecture is due to Brumer and Silverman, in the more precise form: is it always true that $\log_\ell |\mathrm{Cl}_K[\ell]| \ll_{n,\ell} \log D_K / \log\log D_K$ [17, QUESTION Cl(ℓ, d)]? Brumer and Silverman were motivated by counting elliptic curves of fixed conductor. Subsequently, this conjecture has appeared in many further contexts, including bounding the ranks of elliptic curves [34, §1.2]; bounding Selmer groups and ranks of hyperelliptic curves [10]; counting number fields [29, P. 166]; studying equidistribution of CM points on Shimura varieties [98, CONJECTURE 3.5]; and counting nonuniform lattices in semisimple Lie groups [6, THM. 7.5].

Conjecture 2.1 is known to be true for the degree $n = 2$ and the prime $\ell = 2$, when it follows from the genus theory of Gauss (see [68, CH. 8.3]). This is the only case in which it is known. Nevertheless, starting in the early 2000s, significant progress has been made. The purpose of this survey is to give some insight into the wide variety of methods developed in recent work toward the conjecture. As an initial measure of progress, we define:

Property $\mathbf{C}_{n,\ell}(\Delta)$. *Fix a degree $n \geq 2$ and a prime ℓ. Property $\mathbf{C}_{n,\ell}(\Delta)$ holds if for all number fields $K/\mathbb{Q}$ of degree n, $|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\Delta,\varepsilon} D_K^{\Delta+\varepsilon}$ for all $\varepsilon > 0$.*

Gauss proved that $\mathbf{C}_{2,2}(0)$ holds. Until recently, no other case with $\Delta < 1/2$ was known.

The first progress was for imaginary quadratic fields. Suppose $K = \mathbb{Q}(\sqrt{-d})$ for a square-free integer $d > 1$, and suppose that $[\mathfrak{a}]$ is a nontrivial element in $\mathrm{Cl}_K[\ell]$ for a prime $\ell \geq 3$; thus $[\mathfrak{a}]^\ell$ is the principal ideal class. Then by the Minkowski bound (1.1), there exists an integral ideal $\mathfrak{b}$ in $[\mathfrak{a}]$ such that $\mathfrak{N}(\mathfrak{b}) \ll d^{1/2}$. Moreover, $\mathfrak{b}^\ell$ is principal, say, generated by $(y + z\sqrt{-d})/2$ for some integers y, z, and so $(\mathfrak{N}(\mathfrak{b}))^\ell = \mathfrak{N}(\mathfrak{b}^\ell) = (y^2 + dz^2)/4$. Consequently, $|\mathrm{Cl}_K[\ell]|$ can be dominated (up to a factor d^ε) by the number of integral solutions to

$$4x^\ell = y^2 + dz^2, \quad \text{with } x \ll d^{1/2},\ y \ll d^{\ell/4},\ z \ll d^{\ell/4-1/2}. \tag{2.2}$$

When $\ell = 3$, this can be interpreted in several ways: counting solutions to a congruence $y^2 = 4x^3 \pmod d$; counting perfect square values of the polynomial $f(x, z) = 4x^3 - dz^2$; or counting integral points on a family of Mordell elliptic curves $y^2 = 4x^3 - D$, with $D = dz^2$. Pierce used the first two perspectives, and Helfgott and Venkatesh used the third perspective, to prove for the first time that property $\mathbf{C}_{2,3}(\Delta)$ holds for some $\Delta < 1/2$ [48,70, 71]. (The Scholz reflection principle shows that $\log_3 |\mathrm{Cl}_{\mathbb{Q}(\sqrt{-d})}[3]|$ and $\log_3 |\mathrm{Cl}_{\mathbb{Q}(\sqrt{3d})}[3]|$ differ by at most 1, so results for 3-torsion apply comparably to both real and imaginary quadratic fields [76].) When $\ell \geq 5$, the region in which x, y, z lie in (2.2) becomes inconveniently large relative to the trivial bound (2.1). Here is an open question: for a prime $\ell \geq 5$, are there at most $\ll d^\Delta$ integral solutions to (2.2), for some $\Delta < 1/2$?

Recently, Bhargava, Taniguchi, Thorne, Tsimerman, and Zhao made a breakthrough on property $\mathbf{C}_{n,2}(\Delta)$ for all $n \geq 3$. Fix a prime ℓ and a number field K of degree n. Given any nontrivial ideal class $[\mathfrak{a}] \in \mathrm{Cl}_K[\ell]$, they show it contains an integral ideal $\mathfrak{b}$ with $\mathfrak{b}^\ell$ a principal ideal generated by an element β lying in a well-proportioned "box." By an ingenious geometry of numbers argument, they show the number of such generators β in the box is $\ll D_K^{\ell/2-1/2}$. If $\ell \geq 3$, this far exceeds the trivial bound (2.1), but if $\ell = 2$, it slightly improves it. The striking refinement comes by recalling that any β of interest must also have $|N_{K/\mathbb{Q}}(\beta)| = \mathfrak{N}(\mathfrak{b}^\ell) = (\mathfrak{N}(\mathfrak{b}))^\ell$ be a perfect ℓth power of an integer, say, y^ℓ. For $\ell = 2$, they apply a celebrated result of Bombieri and Pila to count integral solutions (x, y) to the degree n equation $N_{K/\mathbb{Q}}(\beta + x) = y^2$ [15]. This strategy proves that property $\mathbf{C}_{n,2}(1/2 - 1/2n)$ holds for all degrees $n \geq 3$. Further refinements for degrees 3, 4 show $\mathbf{C}_{3,2}(0.2785\ldots)$ and $\mathbf{C}_{4,2}(0.2785\ldots)$ hold; see [10].

Only two further nontrivial cases of property $\mathbf{C}_{n,\ell}(\Delta)$ are known, and for these we introduce the Ellenberg–Venkatesh criterion.

2.1. The Ellenberg–Venkatesh criterion

An important criterion for bounding ℓ-torsion in the class group of a number field K relies on counting small primes that are noninert in K. The germ of the idea, which has been credited independently to Soundararajan and Michel, goes as follows. Suppose, for example, that $K = \mathbb{Q}(\sqrt{-d})$ is an imaginary quadratic field with d square-free, and ℓ is an odd prime. Let H denote $\mathrm{Cl}_K[\ell]$. Then $|H| = |\mathrm{Cl}_K|/[\mathrm{Cl}_K : H]$, and to show that $|H|$ is small, it suffices to show that the index $[\mathrm{Cl}_K : H]$ is large. Now suppose that $p_1 \neq p_2$ are rational primes not dividing $2d$ that both split in K, say, $p_1 = \mathfrak{p}_1\mathfrak{p}_1^\sigma$ and $p_2 = \mathfrak{p}_2\mathfrak{p}_2^\sigma$,

where σ is the nontrivial automorphism of K. We claim that as long as p_1, p_2 are sufficiently small, $\mathfrak{p}_1$ and $\mathfrak{p}_2$ must represent different cosets of H. Indeed, supposing to the contrary that $\mathfrak{p}_1 H = \mathfrak{p}_2 H$, one deduces that $\mathfrak{p}_1 \mathfrak{p}_2^{\sigma} \in H$ so that $(\mathfrak{p}_1 \mathfrak{p}_2^{\sigma})^{\ell}$ is a principal ideal, say, generated by $(y + z\sqrt{-d})/2$, for some $y, z \in \mathbb{Z}$. Taking norms shows

$$4(p_1 p_2)^{\ell} = y^2 + dz^2. \tag{2.3}$$

If $p_1, p_2 < (1/4)d^{1/(2\ell)}$, this forces $z = 0$, which yields a contradiction, since $4(p_1 p_2)^{\ell}$ cannot be a perfect square. This proves the claim. In particular, if there are M such distinct primes $p_1, \dots, p_M < (1/4)d^{1/2\ell}$ with $p_j \nmid 2d$ and p_j split in K, then $|\mathrm{Cl}_K[\ell]| \le |\mathrm{Cl}_K| M^{-1}$.

Ellenberg and Venkatesh significantly generalized this strategy to prove an influential criterion, which we state in the case of extensions of $\mathbb{Q}$ [34]. (Throughout this survey, we will focus for simplicity on extensions of $\mathbb{Q}$, but many of the theorems and questions we mention have analogues in the literature over any fixed number field.)

Ellenberg–Venkatesh criterion. *Suppose $K/\mathbb{Q}$ is a number field of degree $n \ge 2$, fix an integer $\ell \ge 2$, and fix $\eta < \frac{1}{2\ell(n-1)}$. Suppose that there are M prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_M \subset \mathcal{O}_K$ such that each $\mathfrak{p}_j$ has norm $\mathfrak{N}(\mathfrak{p}_j) < D_K^{\eta}$, $\mathfrak{p}_j$ is unramified in K and $\mathfrak{p}_j$ is not an extension of a prime ideal from any proper subfield of K. Then*

$$\left|\mathrm{Cl}_K[\ell]\right| \ll_{n,\ell,\varepsilon} D_K^{\frac{1}{2}+\varepsilon} M^{-1}, \quad \text{for all } \varepsilon > 0. \tag{2.4}$$

(A prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ lying above a prime $p \in \mathbb{Q}$ is unramified in $K/\mathbb{Q}$ if $\mathfrak{p}^2 \nmid p\mathcal{O}_K$; a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ is an extension of a prime ideal in a proper subfield $K_0 \subset K$ if there exists a prime ideal $\mathfrak{p}_0 \subset \mathcal{O}_{K_0}$ such that $\mathfrak{p} = \mathfrak{p}_0 \mathcal{O}_K$.) For example, if $p < D_K^{\eta}$ is a rational prime that splits completely in K, so that $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ for distinct prime ideals $\mathfrak{p}_j$, then each $\mathfrak{p}_j$ satisfies the hypotheses of the criterion. In particular, if M rational (unramified) primes $p_1, \dots, p_M < D_K^{\eta}$ split completely in K, then (2.4) holds. Alternatively, it suffices to exhibit prime ideals $\mathfrak{p}_j \subset \mathcal{O}_K$ of degree 1, since such a prime ideal cannot be an extension of a prime ideal from a proper subfield.

Here is one of Ellenberg and Venkatesh's striking applications, which shows that $\mathbf{C}_{2,3}(1/3)$ holds—the current record for $n = 2$, $\ell = 3$. Fix a large square-free integer $d > 1$. Any prime $p \nmid 6d$ that is inert in $\mathbb{Q}(\sqrt{-3})$ must split either in $\mathbb{Q}(\sqrt{d})$ or in $\mathbb{Q}(\sqrt{-3d})$. Thus for any $\eta < 1/6$, at least one field $K \in \{\mathbb{Q}(\sqrt{d}), \mathbb{Q}(\sqrt{-3d})\}$ has a positive proportion of the primes $(1/2)d^{\eta} \le p \le d^{\eta}$ split in K. By the Ellenberg–Venkatesh criterion (2.4), this field K then has the property that $|\mathrm{Cl}_K[3]| \ll D_K^{1/3+\varepsilon}$ for all $\varepsilon > 0$. By the Scholz reflection principle, this bound also applies to the other field in the pair, and $\mathbf{C}_{2,3}(1/3)$ holds.

The Scholz reflection principle has also been generalized by Ellenberg and Venkatesh to bound ℓ-torsion (for odd primes ℓ) in class groups of even-degree extensions of certain number fields. In particular, by pairing their criterion with a reflection principle, they show that $\mathbf{C}_{3,3}(1/3)$ holds and $\mathbf{C}_{4,3}(\Delta)$ holds for some $\Delta < 1/2$ [34, COR. 3.7]. This concludes the list of degrees n and primes ℓ for which property $\mathbf{C}_{n,\ell}(\Delta)$ is known for some $\Delta < 1/2$.

Here are open problems: reduce the value $\Delta < 1/2$ for which $\mathbf{C}_{n,\ell}(\Delta)$ holds, when $n \ge 3$ and $\ell = 2$, or when $n = 2, 3$ or 4 and $\ell = 3$. For $n = 2, 3$ or 4 and a prime $\ell \ge 5$,

prove for the first time that $\mathbf{C}_{n,\ell}(\Delta)$ holds for some $\Delta < 1/2$. For $n \geq 5$ and a prime $\ell \geq 3$, prove for the first time that $\mathbf{C}_{n,\ell}(\Delta)$ holds for some $\Delta < 1/2$.

The Ellenberg–Venkatesh criterion underlies most of the significant recent progress on bounding ℓ-torsion in class groups. What is the best result it can imply? Assuming the Generalized Riemann Hypothesis, given any number field $K/\mathbb{Q}$ of degree n with D_K sufficiently large, a positive proportion of primes $p < D_K^{\eta}$ split completely in K, implying

$$\left|\mathrm{Cl}_K[\ell]\right| \ll_{n,\ell,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell(n-1)}+\varepsilon}, \quad \text{for all } \varepsilon > 0. \tag{2.5}$$

As this is a useful benchmark, we will call this the GRH-bound, and for convenience set $\Delta_{\mathrm{GRH}} = \frac{1}{2} - \frac{1}{2\ell(n-1)}$ once n, ℓ have been fixed. Thus if GRH is true, for each n, ℓ, property $\mathbf{C}_{n,\ell}(\Delta_{\mathrm{GRH}})$ holds. There has been intense interest in proving this without assuming GRH, and this will be our next topic.

3. FAMILIES OF FIELDS

So far we have considered, for each degree n, the "family" of number fields $K/\mathbb{Q}$ of degree n. Let us formalize this, letting $\mathscr{F}_n(X)$ be the set of all degree n extensions K of $\mathbb{Q}$, with $D_K = |\mathrm{Disc}(K/\mathbb{Q})| \leq X$; let $\mathscr{F}_n = \mathscr{F}_n(\infty)$. It is helpful at this point to consider more specific families of fields of a fixed degree. For example, we could define $\mathscr{F}_2^-(X)$ to be the set of imaginary quadratic fields K with $D_K \leq X$, and similarly $\mathscr{F}_2^+(X)$ for real quadratic fields. In general, given a transitive subgroup $G \subset S_n$, define the family

$$\mathscr{F}_n(G;X) = \left\{K/\mathbb{Q} : \deg K/\mathbb{Q} = n, \mathrm{Gal}(\tilde{K}/\mathbb{Q}) \simeq G, D_K \leq X\right\}, \tag{3.1}$$

where all K are in a fixed algebraic closure $\overline{\mathbb{Q}}$, $\tilde{K}$ is the Galois closure of $K/\mathbb{Q}$, the Galois group is considered as a permutation group on the n embeddings of K in $\overline{\mathbb{Q}}$, and the isomorphism with G is one of permutation groups. When $\mathscr{F}$ is such a family, we define:

Property $\mathbf{C}_{\mathscr{F},\ell}(\Delta)$ *holds if for all fields $K \in \mathscr{F}$, $|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\Delta,\varepsilon} D_K^{\Delta+\varepsilon}$ for all $\varepsilon > 0$.*

Since Property $\mathbf{C}_{\mathscr{F},\ell}(\Delta)$ remains out of reach for almost all families, we also consider:

Property $\mathbf{C}^*_{\mathscr{F},\ell}(\Delta)$ *holds if for almost all fields $K \in \mathscr{F}$, $|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\Delta,\varepsilon} D_K^{\Delta+\varepsilon}$ for all $\varepsilon > 0$.* We say that a result holds for "almost all" fields in a family $\mathscr{F}$ if the subset $E(X)$ of possible exceptions is density zero in $\mathscr{F}(X)$, in the sense that

$$\frac{|E(X)|}{|\mathscr{F}(X)|} \to 0 \quad \text{as } X \to \infty.$$

Here too, the first progress came for imaginary quadratic fields. Soundararajan observed that among imaginary quadratic fields with discriminant in a dyadic range $[-X, -2X]$, at most one can fail to satisfy $|\mathrm{Cl}_K[\ell]| \ll D_K^{1/2-1/2\ell+\varepsilon}$ [82]. This verified $\mathbf{C}^*_{\mathscr{F}_2^-,\ell}(\Delta_{\mathrm{GRH}})$ for all primes ℓ. For $\ell = 3$ and quadratic fields, Wong observed that $\mathbf{C}^*_{\mathscr{F}_2^{\pm},3}(1/4)$ holds [96]. For any odd prime ℓ, Heath-Brown and Pierce went below the GRH-bound, proving $\mathbf{C}^*_{\mathscr{F}_2^-,\ell}(1/2 - 3/(2\ell+2))$ [46]. They used the large sieve to show that aside from at most $O(X^{\varepsilon})$ exceptions, all discriminants $-d \in [-X, -2X]$ have $|\mathrm{Cl}_{\mathbb{Q}(\sqrt{-d})}[\ell]|$

controlled by counting the number of distinct primes p_1, p_2 of a certain size such that (2.3) has a nontrivial integral solution (y, z). Then they showed there can be few such solutions, while averaging nontrivially over d. These methods relied heavily on the explicit nature of methods for imaginary quadratic fields. Fields of higher degree need a different approach.

3.1. Dual problems: counting primes, counting fields

To apply the Ellenberg–Venkatesh criterion, we face a question such as: "Given a field, how many small primes split completely in it?" This question is very difficult in general (and is related to the Generalized Riemann Hypothesis). There is a dual question: "Given a prime, in how many fields does it split completely?" Ellenberg, Pierce, and Wood devised a method to apply the Ellenberg–Venkatesh criterion by tackling the dual question instead [33]. The idea goes like this: suppose that each prime splits completely in a positive proportion of fields in a family $\mathscr{F}$. Then the mean number of primes $p \le x$ that split completely in each field should be comparable to $\pi(x)$, and unless the primes conspire, almost all fields in $\mathscr{F}$ should have close to the mean number of primes split completely in them. To prove that the primes cannot conspire, Ellenberg, Pierce, and Wood developed a sieve method, modeled on the Chebyshev inequality from probability.

As input the sieve requires precise counts for the cardinality

$$N_{\mathscr{F}}(X; p) = \big|\{K \in \mathscr{F}(X) : p \text{ splits completely in } K\}\big|.$$

It also requires analogous counts $N_{\mathscr{F}}(X; p, q)$ for when two primes $p \neq q$ split completely in K. Suppose one can prove that for some $\sigma > 0$ and $\tau < 1$, for all distinct primes p, q,

$$N_{\mathscr{F}}(X; p, q) = \delta(pq)\big|\mathscr{F}(X)\big| + O\big((pq)^{\sigma}\big|\mathscr{F}(X)\big|^{\tau}\big), \tag{3.2}$$

for a multiplicative density function $\delta(pq)$ taking values in $(0, 1)$. Then Ellenberg, Pierce, and Wood prove that there exists $\Delta_0 > 0$ (depending on τ, σ) such that the mean number of primes $p \le X^{\Delta_0}$ that split completely in fields in $\mathscr{F}(X)$ is comparable to $\pi(X^{\Delta_0})$. Moreover, there can be at most $O(|\mathscr{F}(X)|^{1-\Delta_0})$ exceptional fields K in $\mathscr{F}(X)$ such that fewer than half the mean number of primes split completely in K. Consequently, for any family $\mathscr{F}$ for which the crucial count (3.2) can be proved, combining this sieve with the Ellenberg–Venkatesh criterion proves that $\mathbf{C}^*_{\mathscr{F},\ell}(\Delta)$ holds for every integer $\ell \ge 2$, where $\Delta = \max\{\frac{1}{2} - \Delta_0, \Delta_{\mathrm{GRH}}\}$.

For which families of fields can (3.2) be proved? Counting number fields is itself a difficult question. For each integer $D \ge 1$, there are a finite number of extensions $K/\mathbb{Q}$ of degree n and discriminant exactly D, by Hermite's finiteness theorem [78, §4.1]. Let $N_n(X)$ denote the number of degree n extensions $K/\mathbb{Q}$ with $D_K \le X$ (counted up to isomorphism). A folk conjecture, sometimes associated to Linnik, states that

$$N_n(X) \sim c_n X \quad \text{as } X \to \infty. \tag{3.3}$$

When $n = 2$, this is essentially equivalent to counting square-free integers (see [33, APPENDIX]). For degree $n = 3$, this is a deep result of Davenport and Heilbronn [28]. For degree $n = 4$, it is known by celebrated results of Cohen, Diaz y Diaz, and Olivier (counting quartic fields

K with $\mathrm{Gal}(\tilde{K}/\mathbb{Q}) \simeq D_4$), and Bhargava (counting non-D_4 quartic fields) [7,20]. For degree $n = 5$, it is known by landmark work of Bhargava [9].

The sieve method of Ellenberg, Pierce, and Wood requires an even more refined count (3.2), with prescribed local conditions and a power-saving error term with explicit dependence on p, q. Power saving error terms for $N_n(X)$ were found for $n = 3$ by Belabas, Bhargava, and Pomerance [5], Bhargava, Shankar, and Tsimerman [11], Taniguchi and Thorne [85]; for $n = 4$ (non-D_4) by Belabas, Bhargava, and Pomerance [5]; and for $n = 5$ by Shankar and Tsimerman [79]. These results can be refined to prove (3.2). Ellenberg, Pierce, and Wood used this strategy to prove that when $\mathscr{F}$ is the family of fields of degree $n = 2, 3, 4$ (non-D_4), or 5, $\mathbf{C}^*_{\mathscr{F},\ell}(\Delta_{\mathrm{GRH}})$ holds for all sufficiently large primes ℓ. (For the few remaining small ℓ, $\mathbf{C}^*_{\mathscr{F},\ell}(\Delta)$ holds with a slightly larger $\Delta < 1/2$.) Counting quartic D_4-fields with local conditions, ordered by discriminant, remains an interesting open problem.

The probabilistic method of Ellenberg–Pierce–Wood uses the property that the density function $\delta(pq)$ in (3.2) is multiplicative (i.e., local conditions at p and q are asymptotically independent). Frei and Widmer have adapted this approach to prove $\mathbf{C}^*_{\mathscr{F},\ell}(\Delta_{\mathrm{GRH}})$ for all sufficiently large ℓ, for $\mathscr{F}$ a family of totally ramified cyclic extensions of k [40]. (That is, $\mathscr{F}$ comprises cyclic extensions K/k of degree n in which every prime ideal of $\mathcal{O}_k$ not dividing n is either unramified or totally ramified in K). This family is chosen since the density function $\delta(pq)$ is multiplicative. It would be interesting to investigate whether a probabilistic method can rely less strictly upon multiplicativity of the density function.

There is a great obstacle to expanding the above approach to the family of all fields of degree n when $n \geq 6$. Then, even the asymptotic (3.3) is not known. For each $n \geq 6$,

$$N_n(X) \leq a_n X^{c_0 (\log n)^2} \tag{3.4}$$

is the best-known bound, with $c_0 = 1.564$, by Lemke Oliver and Thorne [61]; this improves on Couveignes [25], Ellenberg and Venkatesh [36], and Schmidt [75]. For lower bounds, in general the record is $N_n(X) \gg X^{1/2+1/n}$, for all $n \geq 7$ [12]. For any n divisible by $p = 2, 3$ or 5, Klüners (personal communication) has observed that $N_n(X) \gg X$, since there exists a field $F/\mathbb{Q}$ of degree n/p such that degree p S_p-extensions of F exhibit linear asymptotics.

Tackling the problem of counting primes with certain splitting conditions in a specific field via the dual problem of counting fields with certain local conditions at specific primes seems out of reach for higher degree fields. How about tackling the problem of counting primes directly?

4. COUNTING PRIMES WITH L-FUNCTIONS

The prime number theorem states that the number $\pi(x)$ of primes $p \leq x$ satisfies $\pi(x) \sim \mathrm{Li}(x)$ as $x \to \infty$. To count *small* primes, or primes in short intervals, requires understanding the error term, as well as the main term. For each $1/2 \leq \Delta < 1$, the statement

$$\pi(x) = \mathrm{Li}(x) + O(x^{\Delta+\varepsilon}) \quad \text{for all } \varepsilon > 0 \tag{4.1}$$

is essentially equivalent to the statement that the Riemann zeta function $\zeta(s)$ is zero-free for $\Re(s) > \Delta$ [27, CH. 18]. The Riemann Hypothesis conjectures this is true for $\Delta = 1/2$; it is

not known for any $\Delta < 1$. The best known Vinogradov–Korobov zero-free region is:

$$\sigma \geq 1 - \frac{C}{(\log t)^{2/3}(\log\log t)^{1/3}}, \quad t \geq 3, \tag{4.2}$$

with an absolute constant $C > 0$ computed by Ford [37].

To count primes with a specified splitting type in a Galois extension $L/\mathbb{Q}$ of degree $n_L \geq 2$, consider the counting function

$$\pi_{\mathscr{C}}(x, L/\mathbb{Q}) = \left| \left\{ p \leq x : p \text{ unramified in } L, \left[\frac{L/\mathbb{Q}}{p}\right] = \mathscr{C} \right\} \right|, \tag{4.3}$$

in which $[\frac{L/\mathbb{Q}}{p}]$ is the Artin symbol and $\mathscr{C}$ is any fixed conjugacy class in $G = \mathrm{Gal}(L/\mathbb{Q})$. For example, when $L = \mathbb{Q}(e^{2\pi i/q})$, this can be used to count primes in a fixed residue class modulo q. Or, for example, for any Galois extension $L/\mathbb{Q}$, when $\mathscr{C} = \{\mathrm{Id}\}$, this counts primes that split completely in L. By the celebrated Chebotarev density theorem [88],

$$\pi_{\mathscr{C}}(x, L/\mathbb{Q}) \sim \frac{|\mathscr{C}|}{|G|}\,\mathrm{Li}(x), \quad \text{as } x \to \infty. \tag{4.4}$$

But just as for $\pi(x)$, to count *small* primes accurately requires more quantitative information. A central goal is to prove an asymptotic for $\pi_{\mathscr{C}}(x, L/\mathbb{Q})$ that is valid for x very small relative to $D_L = |\mathrm{Disc} L/\mathbb{Q}|$, and with an effective error term. This requires exhibiting a zero-free region for the Dedekind zeta function $\zeta_L(s)$. This is more complicated than (4.2), due to the possibility of an exceptional Landau–Siegel zero: within the region

$$\sigma \geq 1 - (4\log D_L)^{-1}, \quad |t| \leq (4\log D_L)^{-1}, \tag{4.5}$$

$\zeta_L(\sigma + it)$ can contain at most one (real, simple) zero, denoted β_0 if it exists. (As observed by Heilbronn and generalized by Stark, if β_0 exists then it must "come from" a quadratic field, in the sense that L contains a quadratic subfield F with $\zeta_F(\beta_0) = 0$ [47, 83].)

Lagarias and Odlyzko used the zero-free region (4.5) to prove there exist absolute, computable constants C_1, C_2 such that for all $x \geq \exp(10 n_L (\log D_L)^2)$,

$$\left| \pi_{\mathscr{C}}(x, L/\mathbb{Q}) - \frac{|\mathscr{C}|}{|G|}\,\mathrm{Li}(x) \right| \leq \frac{|\mathscr{C}|}{|G|}\,\mathrm{Li}(x^{\beta_0}) + C_1 x \exp\bigl(-C_2 n_L^{-1/2} (\log x)^{1/2}\bigr), \tag{4.6}$$

in which the β_0 term is present only if β_0 exists (see [60], and Serre [77]). This was the first effective Chebotarev density theorem. It can be difficult to apply to questions of interest because of the mysterious β_0 term, and because x must be a large power of D_L (certainly at least $x \geq D_L^{10 n_L}$). In contrast, to apply the Ellenberg–Venkatesh criterion to a field K of degree n, we aim to exhibit primes $p < D_K^{\eta}$ that split completely in the Galois closure $\tilde{K}$ (and hence in K), with $\eta \approx 1/(2\ell(n-1)) \to 0$ as $n, \ell \to \infty$. (These primes are even smaller relative to $D_{\tilde{K}}$, since $D_K^{|G|/n} \ll_G D_{\tilde{K}} \ll_G D_K^{|G|/2}$, where $G = \mathrm{Gal}(\tilde{K}/\mathbb{Q})$ [72].)

If GRH holds for $\zeta_L(s)$, then $\zeta_L(s)$ is zero-free for $\Re(s) > 1/2$, and Lagarias and Odlyzko improve (4.6) in three ways: (i) it is valid for $x \geq 2$; (ii) the β_0 term is not present; (iii) the remaining error term is $O(x^{1/2}\log(D_L x^{n_L}))$. Properties (i) and (ii) show that for every $\eta > 0$, for every degree n extension $K/\mathbb{Q}$ with D_K sufficiently large, at least $\gg \pi(D_K^{\eta})$ primes $p \leq D_K^{\eta}$ split completely in the Galois closure $\tilde{K}$ (and hence in K). When input into

the Ellenberg–Venkatesh criterion, this is the source of the GRH-bound (2.5) for all integers $\ell \geq 2$.

Here is a central goal: improve the Chebotarev density theorem (4.6) without assuming GRH, so that (i′) for any $\eta > 0$ it is valid for x as small as $x \geq D_L^{\eta}$ (for all D_L sufficiently large) and (ii) the β_0 term is not present. (For many applications, the final error term in (4.6) suffices as is.) If this held for $L = \tilde{K}$ the Galois closure of a field K, the Ellenberg–Venkatesh criterion would imply the GRH-bound (2.5) for ℓ-torsion in Cl_K for all integers $\ell \geq 2$, without assuming GRH. Recently, Pierce, Turnage-Butterbaugh, and Wood showed that the key improvements (i′) and (ii) hold if for some $0 < \delta \leq 1/4$, $\zeta_L(s)/\zeta(s)$ is zero-free for $s = \sigma + it$ in the box

$$1 - \delta \leq \sigma \leq 1, \quad |t| \leq \log D_L^{2/\delta}. \tag{4.7}$$

Proving this for any particular L-function $\zeta_L(s)/\zeta(s)$ of interest is out of reach. Instead, it can be productive to study a family of L-functions. In particular, if $\mathscr{F} = \mathscr{F}_n(G; X)$ is a family of degree n fields with fixed Galois group of the Galois closure, property $\mathbf{C}^*_{\mathscr{F},\ell}(\Delta_{\mathrm{GRH}})$ will follow (for all integers $\ell \geq 2$) if it is true for *almost all* fields $K \in \mathscr{F}_n(G; X)$, that $\zeta_{\tilde{K}}(s)/\zeta(s)$ is zero-free in the box (4.7). This was the strategy Pierce, Turnage-Butterbaugh, and Wood developed in [72], which we will now briefly sketch.

4.1. Families of L-functions

There is a long history of estimating the density of zeroes within a certain region, for a family of L-functions. If we can show there are fewer possible zeroes in the region than there are L-functions in the family, then some of the L-functions must be zero-free in that region. We single out a result of Kowalski and Michel, who used the large sieve to prove a zero density result for families of cuspidal automorphic L-functions [56]. In particular, for suitable families, their result implies that almost all L-functions in the family must be zero-free in a box analogous to (4.7).

There are two fundamental barriers to applying this to our problem of interest: the representation underlying $\zeta_{\tilde{K}}(s)/\zeta(s)$ is not always cuspidal, and it is not always known to be automorphic. Suppose G has irreducible complex representations $\rho_0, \rho_1, \ldots, \rho_r$, with ρ_0 the trivial representation. Then for $K \in \mathscr{F}_n(G; X)$, $\zeta_{\tilde{K}}$ is a product of Artin L-functions,

$$\zeta_{\tilde{K}}(s)/\zeta(s) = \prod_{j=1}^{r} L(s, \rho_j, \tilde{K}/\mathbb{Q})^{\dim \rho_j}. \tag{4.8}$$

The Artin (holomorphy) conjecture posits that for each nontrivial irreducible representation ρ_j, $L(s, \rho_j, \tilde{K}/\mathbb{Q})$ is entire. The (strong) Artin conjecture posits that for each nontrivial irreducible representation ρ_j, there is an associated cuspidal automorphic representation $\pi_{\tilde{K},j}$ of $\mathrm{GL}(m_j)/\mathbb{Q}$, and $L(s, \pi_{\tilde{K},j}) = L(s, \rho_j, \tilde{K}/\mathbb{Q})$. This is known for certain types of representations of certain groups, but otherwise is a deep open problem (see recent work in [19]). For the moment, we will proceed by assuming the strong conjecture. Then the factorization (4.8) naturally slices the family $\zeta_{\tilde{K}}(s)/\zeta(s)$, as K varies over $\mathscr{F}_n(G; X)$, into r families $\mathscr{L}_1(X), \mathscr{L}_2(X), \ldots, \mathscr{L}_r(X)$, where each $\mathscr{L}_j(X)$ is the set of cuspidal automorphic representations $\pi_{\tilde{K},j}$ associated to the representation ρ_j. Kowalski and Michel's result applies

to each family $\mathscr{L}_j(X)$ individually. This proves that every representation $\pi \in \mathscr{L}_j(X)$ has associated L-function $L(s,\pi)$ being zero-free in the box (4.7)—except for a possible subset of "bad" representations π, of density zero in $\mathscr{L}_j(X)$, for which $L(s,\pi)$ could have a zero in the box. (Of course, no such zero exists if GRH is true, but we are not assuming GRH.)

Now a crucial difficulty arises: if there were a "bad" representation $\pi \in \mathscr{L}_j(X)$, in how many products (4.8) could it appear, as K varies over $\mathscr{F}_n(G;X)$? Each field K for which the "bad" factor $L(s,\pi)$ appears could have a zero of $\zeta_{\tilde{K}}(s)/\zeta(s)$ in (4.7). Thus the crucial question is: for a fixed nontrivial irreducible representation ρ of G, how many fields $K_1, K_2 \in \mathscr{F}_n(G;X)$ have $L(s,\rho,\tilde{K}_1/\mathbb{Q}) = L(s,\rho,\tilde{K}_2/\mathbb{Q})$? This can be stated a different way. Given a subgroup H of G, let $\tilde{K}^H$ denote the subfield of $\tilde{K}$ fixed by H. It turns out that the question can be transformed into: how many fields $K_1, K_2 \in \mathscr{F}_n(G;X)$ have $\tilde{K}_1^{\mathrm{Ker}(\rho)} = \tilde{K}_2^{\mathrm{Ker}(\rho)}$? Let us call this a collision. If a positive proportion of fields in $\mathscr{F}_n(G;X)$ can collide for ρ_j, then via the factorization (4.8), the possible existence of even one "bad" element in $\mathscr{L}_j(X)$ could allow a positive proportion of the functions $\zeta_{\tilde{K}}(s)/\zeta(s)$ to have a zero in (4.7). In particular, then this approach would fail to prove $\mathbf{C}^*_{\mathscr{F},\ell}(\Delta_{\mathrm{GRH}})$ for the family $\mathscr{F} = \mathscr{F}_n(G;X)$. To rule this out, we aim to show that for each nontrivial irreducible representation ρ_j of G, collisions are rare.

We define the "collision problem" for the family $\mathscr{F}_n(G;X)$: how big is

$$\max_{\rho} \max_{K_1 \in \mathscr{F}_n(G;X)} \left|\left\{K_2 \in \mathscr{F}_n(G;X) : \tilde{K_1}^{\mathrm{Ker}(\rho)} = \tilde{K_2}^{\mathrm{Ker}(\rho)}\right\}\right|? \tag{4.9}$$

Here the maximum is over the nontrivial irreducible representations ρ of G with $\mathrm{Ker}(\rho)$ a proper normal subgroup of G. Suppose for a particular family $\mathscr{F}_n(G;X)$, the collisions (4.9) number at most $\ll X^{\alpha}$. Then the strategy sketched here ultimately shows that aside from at most $\ll X^{\alpha+\varepsilon}$ exceptional fields (for any $\varepsilon > 0$), every field in $K \in \mathscr{F}_n(G;X)$ has the property that an improved Chebotarev density theorem with properties (i′) and (ii) holds for its Galois closure $\tilde{K}$. If we can prove simultaneously that $|\mathscr{F}_n(G;X)| \gg X^{\beta}$ for some $\beta > \alpha$, then the improved Chebotarev density theorem holds for almost all fields in the family. Consequently, we would obtain property $\mathbf{C}^*_{\mathscr{F},\ell}(\Delta_{\mathrm{GRH}})$, for all integers $\ell \geq 2$.

Thus the goal of bounding ℓ-torsion in class groups of fields in the family $\mathscr{F}_n(G;X)$ has been transformed into a question of counting how often certain fields share a subfield. For which families can the collision problem (4.9) be controlled? For some groups, the number of collisions can be $\gg |\mathscr{F}_n(G;X)|$ (for example, $G = \mathbb{Z}/4\mathbb{Z}$). On the other hand, if G is a simple group, or if all nontrivial irreducible representations of G are faithful, the number of collisions is $\ll 1$ (but a lower bound $|\mathscr{F}_n(G;X)| \gg X^{\beta}$ for some $\beta > 0$ may not be known, yet). In general, controlling the collision problem is difficult.

One idea is to restrict attention to an advantageously chosen subfamily of fields, call it $\mathscr{F}_n^*(G;X) \subset \mathscr{F}_n(G;X)$. To bound (4.9) within a subfamily it suffices to count

$$\max_{H} \max_{\substack{F \\ \deg(F/\mathbb{Q})=[G:H]}} \left|\left\{K \in \mathscr{F}_n^*(G;X) : \tilde{K}^H = F\right\}\right|. \tag{4.10}$$

Here H ranges over the proper normal subgroups of G that appear as the kernel of some nontrivial irreducible representation. For some groups G, if $\mathscr{F}_n^*(G;X)$ is defined appropriately, this can be further transformed into counting number fields with *fixed* discriminant.

Let us see how this goes in the example $G = S_n$ with $n = 3$ or $n \geq 5$, so that A_n is the only nontrivial proper normal subgroup (the kernel of the sign representation). Consider the subfamily $\mathscr{F}_n^*(S_n; X)$ of fields with square-free discriminant. (These are a positive proportion of all degree n S_n-fields for $n \leq 5$ and conjecturally so for $n \geq 6$.) Then for $H = A_n$ and F a fixed quadratic field, it can be shown that any field K counted in (4.10) must have the property that $D_K = D_F$ (up to some easily controlled behavior of wildly ramified primes). Under this very strong identity of discriminants, (4.10) is dominated by

$$\max_{D \geq 1} \left| \left\{ K \in \mathscr{F}_n^*(S_n; X) : D_K = D \right\} \right|. \tag{4.11}$$

This strategy transforms the collision problem into counting fields of *fixed* discriminant.

For certain other groups G, (4.10) can also be dominated by a quantity analogous to (4.11) if the subfamily $\mathscr{F}_n^*(G; X)$ is defined by specifying that each prime that is tamely ramified in K has its inertia group generated by an element in a carefully chosen conjugacy class $\mathscr{I}$ of G. For such a group G, the final step in this strategy for proving improved Chebotarev density theorems for almost all fields in the family $\mathscr{F}_n^*(G; X)$ is to bound (4.11). If $|\mathscr{F}_n^*(G; X)| \gg X^\beta$ is known, it suffices to prove (4.11) is $\ll X^\alpha$ for some $\alpha < \beta$. In general, counting number fields with fixed discriminant is very difficult—we will return to this problem later. But for some families $\mathscr{F}_n^*(G; X)$, (4.11) can be controlled sufficiently well, relative to a known lower bound for $|\mathscr{F}_n^*(G; X)|$.

This is the strategy developed by Pierce, Turnage-Butterbaugh, and Wood in [72]. The result is an improved Chebotarev density theorem, with properties (i′) and (ii), that holds unconditionally for almost all fields in the following families: (a) $\mathscr{F}_p(C_p; X)$ cyclic extensions of any prime degree; (b) $\mathscr{F}_n^*(C_n; X)$ totally ramified cyclic extensions of any degree $n \geq 2$; (c) $\mathscr{F}_p^*(D_p; X)$ prime degree dihedral extensions, $\mathscr{I}$ being the class of order 2 elements; (d) $\mathscr{F}_n^*(S_n; X)$ fields of square-free discriminant, $n = 3, 4$; and (e) $\mathscr{F}_4^*(A_4; X)$, $\mathscr{I}$ being either class of order 3 elements. Conditional on the strong Artin conjecture, they proved the improved Chebotarev density theorem also holds for almost all fields in the following families: (f) $\mathscr{F}_5^*(S_5; X)$ quintic fields of square-free discriminant; and (g) $\mathscr{F}_n(A_n; X)$, for all $n \geq 5$. (There are other families, such as $\mathscr{F}_n^*(S_n; X)$ for $n \geq 6$, to which the strategy applies, but the current upper bound known for (4.11) is larger than the known lower bound for $|\mathscr{F}_n^*(S_n; X)|$.) As a consequence, Pierce, Turnage-Butterbaugh, and Wood proved for each family (a)–(e) that $\mathbf{C}^*_{\mathscr{F},n}(\Delta_{\mathrm{GRH}})$ holds unconditionally for all integers $\ell \geq 2$, and it holds for each family (f)–(g) under the strong Artin conjecture. This was the first time such a result was proved for families of fields of arbitrarily large degree.

4.2. Further developments

Since the work outlined above, many interesting new developments have followed, relating to zero density results for families of L-functions, Chebotarev density theorems for families of fields, and ℓ-torsion in class groups of fields in specific families.

First, there has been renewed interest in zero density results for families of L-functions, concerning potential zeroes in regions close to the line $\Re(s) = 1$, and extending the perspective of Kowalski and Michel [56]; see, for example, [18, 49, 87].

Second, several new strategies have focused on the problem of proving effective Chebotarev density theorems for almost all fields in a family. The work in [72] raised several desiderata. Some groups G have the property that no ramification restriction exists that allows the "collision problem" in the form (4.10) to be transformed into a "discriminant multiplicity problem" in the form (4.11). For example, this occurs for any noncyclic abelian group, or D_4. These cases remain open; instead, An recently proved a Chebotarev density theorem for almost all fields in a family of quartic D_4-fields associated to a fixed biquadratic field [2]. Another significant desideratum was to remove the dependence on the strong Artin conjecture. Thorner and Zaman recently achieved this, by proving a zero density estimate directly for Dedekind zeta functions, without passing through the factorization (4.8) [86]. But that work is still explicitly conditional on the ability to control a collision problem similar to (4.9), for which the best known strategy is still the approach of [72].

Most recently, the collision problem has been bypassed for certain groups G by interesting new work of Lemke Oliver, Thorner, and Zaman [62]. Their key idea when studying fields in a family $\mathscr{F}_n(G;X)$ is to prove a zero-free region not for $\zeta_{\tilde{K}}/\zeta$ but for $\zeta_{\tilde{K}}/\zeta_{\tilde{K}^N}$ where N is a nontrivial normal subgroup of G. This allows them to replace a collision problem like (4.9) by an "intersection multiplicity problem," bounding

$$\max_{K_1\in\mathscr{F}_n(G;X)}\left|\left\{K_2\in\mathscr{F}_n(G;X):\tilde{K}_1\cap\tilde{K}_2\neq\tilde{K}_1^N\cap\tilde{K}_2^N\right\}\right|. \tag{4.12}$$

The number of exceptional fields, for which a desired Chebotarev-type theorem cannot be verified, is then dominated by (4.12) (up to X^ε). This is advantageous if G has a unique minimal nontrivial normal subgroup N, so that (4.12) is $\ll 1$. But as a trade-off, one no longer obtains an effective Chebotarev density theorem for each conjugacy class $\mathscr{C}$ in G.

Let $\pi_K(x)$ count prime ideals $\mathfrak{p}\subset\mathcal{O}_K$ with $\mathfrak{N}_{K/\mathbb{Q}}\mathfrak{p}\le x$. Let $\mathscr{F}$ represent either of the two following families: degree p fields $K/\mathbb{Q}$ for p prime, or degree n S_n-fields $K/\mathbb{Q}$, for any $n\ge 2$. Lemke Oliver, Thorner, and Zaman prove that except for at most $\ll X^\varepsilon$ exceptional fields, every $K\in\mathscr{F}(X)$ has $|\pi_K(x)-\pi(x)|\le C_1 x\exp(-C_2\sqrt{\log x})$ for every $x\ge(\log D_K)^{C_3(n,\varepsilon)}$. In either family $\mathscr{F}$, they obtain results on ℓ-torsion by applying the Ellenberg–Venkatesh criterion using prime ideals of degree 1. If $\pi_K^*(x)$ counts only prime ideals of degree 1, then $\pi_K^*(x)=\pi_K(x)+O_n(\sqrt{x})$, so the above result exhibits many small prime ideals of degree 1. Thus for either family, $\mathbf{C}^*_{\mathscr{F},n}(\Delta_{\mathrm{GRH}})$ holds unconditionally for all ℓ (and the exceptional set is very small). (They also exhibit infinitely many degree n S_n-fields K with Cl_K as large as possible, but $|\mathrm{Cl}_K[\ell]|$ bounded by (2.5) for all ℓ; and infinitely many totally real degree n S_n-fields K with Cl_K containing an element of exact order ℓ and $|\mathrm{Cl}_K[\ell]|$ bounded by (2.5).) What happens when G does not have a unique minimal nontrivial normal subgroup? Here is an open question: in general, when N is a nontrivial normal subgroup of G (not necessarily unique or minimal), what is the true order of growth of (4.12) as $X\to\infty$? Questions about this "intersection multiplicity" are gathered in [62].

Third, increased attention has turned to bounding ℓ-torsion in class groups for *all* fields in special families specified by the Galois group: that is, proving property $\mathbf{C}_{\mathscr{F},\ell}(\Delta)$ for some $\Delta<1/2$. First, Klüners and Wang have proved $\mathbf{C}_{\mathscr{F},p}(0)$ for the family $\mathscr{F}_{p^r}(G;X)$ for any p-group G; this generalizes the application of genus theory to prove $\mathbf{C}_{2,2}(0)$ [54].

Second, let $G = (\mathbb{Z}/p\mathbb{Z})^r$ be an elementary abelian group of rank $r \geq 2$, with p prime. Wang has shown that for every ℓ, within the family of Galois G-fields $K/\mathbb{Q}$, property $\mathbf{C}_{\mathscr{F},\ell}(1/2 - \delta(\ell, p))$ holds for some $\delta(\ell, p) > 0$ [91]. Since the savings $\delta(\ell, p)$ is independent of the rank, for r sufficiently large this is better than $\mathbf{C}_{\mathscr{F},\ell}(\Delta_{\mathrm{GRH}})$. The method of proof plays off the interaction of three facts arising from the precise structure of G: first, $|\mathrm{Cl}_K[\ell]|$ factors as a product of $|\mathrm{Cl}_F[\ell]|$ where F varies over the $\approx p^{r-1}$ many degree p subfields of K, so it suffices to bound one of these factors nontrivially. Second, any rational prime splits completely in $\approx p^{r-2}$ of these subfields, so at least one subfield has a positive proportion of primes splitting completely in it. Third, the sizes of the discriminants of the subfields can be played against each other, so that known prime-counting results (which may *a priori* seem to count primes that are "too large") suffice for the application of the Ellenberg–Venkatesh criterion. This is an interesting counterpoint to the methods described earlier. In another direction, Wang has developed the notion of a forcing extension; certain nilpotent groups can be built from elementary p-groups via forcing extensions. If G' is constructed from G by a forcing extension, then $\mathbf{C}_{\mathscr{F}',\ell}(\Delta')$ can be deduced from $\mathbf{C}_{\mathscr{F},\ell}(\Delta)$, for some $\Delta, \Delta' < 1/2$, where $\mathscr{F}$ is the family of G-extensions and $\mathscr{F}'$ is the family of G'-extensions [89].

All of the results mentioned in this section (except where genus theory suffices) directly apply or build on the Ellenberg–Venkatesh criterion. Can this criterion be strengthened? Ellenberg has suggested some possible improvements in [32]. In particular, let $\eta(K) := \inf\{H_K(\alpha) : K = \mathbb{Q}(\alpha)\}$ denote the minimum (relative) multiplicative Weil height of a generating element of K. Roughly speaking, Ellenberg notes the criterion (2.4) can actually allow prime ideals with norms as large as $\eta(K)^{1/\ell}$. The restriction to norms $< D_K^{\frac{1}{2\ell(n-1)}}$ in (2.4) was made since the lower bound $\eta(K) \geq D_K^{\frac{1}{2(n-1)}}$ holds for all fields [80]. Widmer, also with Frei, has shown that $\eta(K)$ can be enlarged for almost all fields in certain families, leading to improved upper bounds for ℓ-torsion in those fields [41, 95]. That is, they improve the very notion of the "GRH-bound" (2.5), and show that the parameter we have called Δ_{GRH} can actually be taken smaller for some fields. Their work raises interesting open questions: what upper and lower bounds hold for $\eta(K)$, for all (or almost all) fields in a family? Ruppert [74] has conjectured uniform upper bounds $\eta(K) \leq D_K^{1/2}$ (now proved for almost all fields in some families by [72]). If this is true, the Ellenberg–Venkatesh criterion would hit a barrier, for most fields, with a result like $|\mathrm{Cl}_K[\ell]| \ll D_K^{1/2-1/2\ell+\varepsilon}$ for any degree n, still far from the ℓ-torsion Conjecture. It would be very interesting to find a new, different criterion.

5. WHY DO WE EXPECT THE ℓ-TORSION CONJECTURE TO BE TRUE?

Recall that the ℓ-torsion Conjecture 2.1 is still known only in the case stemming from Gauss's work, namely for $n = 2$, $\ell = 2$. It is a good idea to affirm why we believe the ℓ-torsion Conjecture should be true. We will consider this from three perspectives.

5.1. From the perspective of the Cohen–Lenstra–Martinet heuristics

So far, when we have mentioned a result for almost all fields in a family, we have not focused on the size of a potential exceptional set, other than showing it is smaller than the size of the full family. But to understand the ℓ-torsion Conjecture, we must quantify a potential exceptional set, and show that for all sufficiently large discriminants, it is empty.

Let us abstract this, for a family $\mathscr{F}_0(X)$ of fields K with D_K in a dyadic range $(X/2, X]$, from which more general results can easily be deduced by summing over $\ll \log X$ dyadic ranges. Suppose $f : \mathscr{F}_0(X) \to \mathbb{N}$ is a function with $f(K) \le D_K^a$ for all K. Suppose that for some $\Delta < a$ we can improve this to $f(K) \le D_K^\Delta$ for all K outside of some exceptional set $E_0^\Delta(X) \subset \mathscr{F}_0(X)$. Then

$$\sum_{K\in\mathscr{F}_0(X)} f(K) = \sum_{K\in\mathscr{F}_0(X)\setminus E_0^\Delta(X)} f(K) + \sum_{K\in E_0^\Delta(X)} f(K) \le \big|\mathscr{F}_0(X)\big|X^\Delta + \big|E_0^\Delta(X)\big|X^a. \tag{5.1}$$

As long as $|E_0^\Delta(X)| \ll |\mathscr{F}_0(X)|X^{-(a-\Delta)}$, this shows that $f(K) \ll X^\Delta$ on average. On the other hand, suppose we know $\sum_{K\in\mathscr{F}_0(X)} f(K) \le X^b$. Then a potential set of exceptions $E_0^\Delta(X) = \{K \in \mathscr{F}_0(X) : f(K) > D_K^\Delta\}$ can be controlled by

$$X^\Delta\big|E_0^\Delta(X)\big| \ll \sum_{K\in E_0^\Delta(X)} f(K) \le \sum_{K\in\mathscr{F}_0(X)} f(K) \le X^b. \tag{5.2}$$

Thus $|E_0^\Delta(X)| \ll X^{b-\Delta}$, and exceptional fields are density zero in $\mathscr{F}_0(X)$, provided $X^{b-\Delta} = o(|\mathscr{F}_0(X)|)$. That is, a nontrivial upper bound on ℓ-torsion for "almost all" fields in a family $\mathscr{F}$ is essentially equivalent to the same upper bound "on average."

To verify the ℓ-torsion Conjecture, we wish to show a "pointwise" bound: for every $\varepsilon > 0$, there exists D_ε such that when $D_K \ge D_\varepsilon$, there are *no* exceptions to the bound $|\mathrm{Cl}_K[\ell]| \le D_K^\varepsilon$. The key is to consider not averages but arbitrarily high kth moments. In the general setting above, suppose that we know $\sum_{K\in\mathscr{F}_0(X)} f(K)^k \le X^b$, for a real number $k \ge 1$. Then for any fixed $\Delta > 0$, adapting the argument (5.2) shows that $|E_0^\Delta(X)| \ll X^{b-k\Delta}$. If the kth moment is uniformly bounded by X^b for a sequence of $k \to \infty$, then for each $\Delta > 0$, we can take k sufficiently large to conclude that the set of exceptions is empty.

This perspective has been applied by Pierce, Turnage-Butterbaugh, and Wood in [73] to prove that the ℓ-torsion Conjecture holds for *all* fields in a family $\mathscr{F}(X)$ if there is a real number $\alpha \ge 1$ such that for a sequence of arbitrarily large k,

$$\sum_{K\in\mathscr{F}(X)} \big|\mathrm{Cl}_K[\ell]\big|^k \ll_{n,\ell,k,\alpha} \big|\mathscr{F}(X)\big|^\alpha, \quad \text{for all } X \ge 1. \tag{5.3}$$

The Cohen–Lenstra–Martinet heuristics predict that (5.3) holds, in the form of an even stronger asymptotic with $\alpha = 1$, for all integers $k \ge 1$, for families of Galois G-extensions, at least for all primes $\ell \nmid |G|$. The appropriate moment formulation can be found in [21] for degree 2 fields and in [92] for higher degrees, building on [22]. This confirms that the ℓ-torsion Conjecture follows from another well-known set of conjectures.

The Cohen–Lenstra–Martinet heuristics are a subject of intense interest and much recent activity. Here are some spectacular successes most closely related to our topic. Dav-

enport and Heilbronn [28] have proved

$$\sum_{\substack{\deg(K)=2\\ 0<D_K\le X}} \left|\mathrm{Cl}_K[3]\right| \sim \left(\frac{2}{3\zeta(2)}+\frac{1}{\zeta(2)}\right)X; \tag{5.4}$$

second-order terms have been found in [5,11,85]. Bhargava [7] has proved

$$\sum_{\substack{\deg(K)=3\\ 0<D_K\le X}} \left|\mathrm{Cl}_K[2]\right| \sim \left(\frac{5}{48\zeta(3)}+\frac{3}{8\zeta(3)}\right)X, \tag{5.5}$$

in which each isomorphism class of fields is counted once. Very recently, [63] obtained analogues of (5.4) for averages over $\mathscr{F}_{2^m}(G;X)$ for any permutation group $G\subset S_{2^m}$ that is a transitive permutation 2-group containing a transposition. See also the work of Smith on the distribution of 2^k-class groups in imaginary quadratic fields [81]; Koymans and Pagano on ℓ^k-class groups of degree ℓ cyclic fields [59]; Klys on moments of p-torsion in cyclic degree p fields (conditional on GRH for $p\ge 5$) [55]; Milovic and Koymans on 16-rank in quadratic fields [57,58]; Bhargava and Varma [13,14] elaborating on (5.4) and (5.5).

The perspective of moments (5.3) provides a strong motivation to prove the kth moment bounds for ℓ-torsion. Fouvry and Klüners have proved an asymptotic for the kth moments related to 4-torsion when K is quadratic, for all integers $k\ge 1$ [38]. Heath-Brown and Pierce have proved nontrivial bounds for the kth moments of ℓ-torsion for imaginary quadratic fields, for all odd primes ℓ [46]. For example, they establish second moment bounds

$$\sum_{\substack{K=\mathbb{Q}(\sqrt{\pm D})\\ D\le X}} \left|\mathrm{Cl}_K[3]\right|^2 \ll X^{23/18}, \qquad \sum_{\substack{K=\mathbb{Q}(\sqrt{-D})\\ D\le X}} \left|\mathrm{Cl}_K[\ell]\right|^2 \ll X^{2-\frac{3}{\ell+1}}, \quad \ell\ge 5 \text{ prime}, \tag{5.6}$$

as well as results for the kth moments for all $k\ge 1$. In general, proving tighter control on the size of an exceptional family $E_0^{\Delta}(X)$ can be used to deduce a better moment bound for $|\mathrm{Cl}_K[\ell]|$, similar to (5.1). This has recently been exploited by Frei and Widmer, in combination with refinements of the Ellenberg–Venkatesh criterion, to improve moment bounds on ℓ-torsion for the families of fields studied in [72] (if ℓ is sufficiently large); see [41].

Let us mention a connection to elliptic curves; this was after all the setting in which Brumer and Silverman initially posed the ℓ-torsion Conjecture. Let $E(q)$ denote the number of isomorphism classes of elliptic curves over $\mathbb{Q}$ with conductor q. Brumer and Silverman have conjectured that $E(q)\ll_\varepsilon q^\varepsilon$ for every $q\ge 1$, $\varepsilon>0$ [17]. Conditionally, this follows from GRH combined with a weak form of the Birch–Swinnerton-Dyer conjecture. They also showed this follows from the 3-torsion Conjecture for quadratic fields, by proving

$$E(q)\ll_\varepsilon q^\varepsilon \max_{1\le D\le 1728q} \left|\mathrm{Cl}_{\mathbb{Q}(\sqrt{\pm D})}[3]\right|, \quad \text{for all } \varepsilon>0. \tag{5.7}$$

Duke and Kowalski have combined this with the celebrated asymptotic (5.4) to bound $\sum_{1\le q\le Q} E(q)\ll Q^{1+\varepsilon}$ for every $\varepsilon>0$ [30]. (See also [39] for ordering by discriminant.) Pierce, Turnage-Butterbaugh, and Wood have recently proved that for all $k\ge 1$, the kth moment of 3-torsion in quadratic fields dominates the γkth moment of $E(q)$, for a numerical constant $\gamma\approx 1.9745\ldots$ coming from [48], which sharpened the relation (5.7). Thus

new moment bounds for $E(q)$ can be obtained from (5.6), for example. Here is an open problem: prove that $\sum_{1\le q\le Q} E(q) = o(Q)$. This would show for the first time that integers that are the conductor of an elliptic curve have density zero in $\mathbb{Z}$. In fact, it is conjectured by Watkins that this average is asymptotic to $c\,Q^{5/6}$ for a certain constant c [94] (building on an analogous conjecture by Brumer–McGuinness for ordering by discriminant [16]).

To conclude, in this section we saw that the truth of the ℓ-torsion Conjecture is implied by the truth of the well-known Cohen–Lenstra–Martinet heuristics on the distribution of class groups.

5.2. From the perspective of counting number fields of fixed discriminant

Let $K/\mathbb{Q}$ be a degree n extension. The Hilbert class field H_K is the maximal abelian unramified extension of K, and Cl_K is isomorphic to $\mathrm{Gal}(H_K/K)$. A second way to motivate the ℓ-torsion Conjecture is to count intermediate fields between K and H_K.

Here is an argument recorded by Pierce, Turnage-Butterbaugh, and Wood in [73]. Fix a prime ℓ and write Cl_K additively, so that $\mathrm{Cl}_K[\ell] \simeq \mathrm{Cl}_K/\ell\,\mathrm{Cl}_K$. Now define the fixed field $L = H_K^{\ell\,\mathrm{Cl}_K}$ lying between K and H_K, so $\mathrm{Gal}(L/K) \simeq \mathrm{Cl}_K[\ell]$. Each surjection $\mathrm{Cl}_K[\ell] \to \mathbb{Z}/\ell\mathbb{Z}$ generates an intermediate field M, with $K \subset M \subset L$ and $\deg(M/\mathbb{Q}) = n\ell$. If $|\mathrm{Cl}_K[\ell]| = \ell^r$, say, this produces $\approx \ell^{r-1}$ such fields M. The crucial point is that since H_K is an unramified extension, all these fields satisfy a rigid discriminant identity $D_M = D_K^{\ell}$. Consequently, if we can count how many number fields of degree $n\ell$ can share the same *fixed* discriminant, then we can bound ℓ-torsion in Cl_K. (We have seen this problem before.) We formalize the problem of counting number fields of fixed discriminant as follows:

Property $\mathbf{D}_n(\Delta)$. *Fix a degree $n \ge 2$. Property $\mathbf{D}_n(\Delta)$ holds if for every $\varepsilon > 0$ and for every fixed integer $D > 1$, at most $\ll_{n,\varepsilon} D^{\Delta+\varepsilon}$ fields $K/\mathbb{Q}$ of degree n have $D_K = D$.*

The strategy sketched above ultimately proves that property $\mathbf{D}_{n\ell}(\Delta)$ implies $\mathbf{C}_{n,\ell}(\ell\Delta)$. This leads inevitably to the question: is property $\mathbf{D}_{n\ell}(0)$ true? Here is a conjecture:

Conjecture 5.1 (Discriminant multiplicity conjecture). *For each $n \ge 2$, for every $\varepsilon > 0$, and for every integer $D > 1$, at most $\ll_{n,\varepsilon} D^{\varepsilon}$ fields $K/\mathbb{Q}$ of degree n have $D_K = D$.*

This conjecture has been recorded by Duke [29]. It implies the ℓ-torsion Conjecture, a link noted in [29, 35] and quantified in [73]. Recall the conjecture (3.3) for counting all fields of degree n and discriminant $D_K \le X$. The Discriminant Multiplicity Conjecture for degree n would immediately imply $N_n(X) \ll X^{1+\varepsilon}$, which indicates its level of difficulty. Of course, in general, property $\mathbf{D}_n(\Delta)$ implies $N_n(X) \ll X^{1+\Delta+\varepsilon}$ for all $\varepsilon > 0$. (In terms of lower bounds, Ellenberg and Venkatesh have noted there can be $\gg D^{c/\log\log D}$ extensions $K/\mathbb{Q}$ with a fixed Galois group and fixed discriminant D [35].)

The Discriminant Multiplicity Conjecture posits that $\mathbf{D}_n(0)$ holds for each $n \ge 2$. This is true for $n = 2$, but it is not known for any other degree. For degrees $n = 3, 4, 5$, the best-known results currently are $\mathbf{D}_3(1/3)$ by [34]; $\mathbf{D}_4(1/2)$ as found in [52, 72, 73, 97]; $\mathbf{D}_5(199/200)$ as found in [33], building on [9, 79]. Currently for $n \ge 6$, the only result for

$\mathbf{D}_n(\Delta)$ is a trivial consequence of counting fields of bounded discriminant, as in (3.4), so in particular $\Delta = c_0(\log n)^2 > 1$ in those cases. It would be very interesting to improve the exponent known for $\mathbf{D}_n(\Delta)$, for any fixed degree $n \geq 3$.

As is the case for many of the problems surveyed in this paper, it can also be profitable to study the problem within a family $\mathscr{F}$ of degree n extensions:

Property $\mathbf{D}_{\mathscr{F},n}(\Delta)$. *Fix a degree $n \geq 2$. Property $\mathbf{D}_{\mathscr{F},n}(\Delta)$ holds if for every $\varepsilon > 0$ and for every fixed integer $D > 1$, at most $\ll_{n,\varepsilon} D^{\Delta+\varepsilon}$ fields $K/\mathbb{Q}$ in the family $\mathscr{F}$ have $D_K = D$.*

This is the type of property Pierce, Turnage-Butterbaugh, and Wood used to control the collision problem, in the form (4.11) [72]. Property $\mathbf{D}_{\mathscr{F},n}(0)$ has recently been proved by Klüners and Wang, for the family $\mathscr{F} = \mathscr{F}_n(G;X)$ of degree n G-extensions for any nilpotent group G. This was built from the truth of property $\mathbf{C}_{\mathscr{F},p}(0)$ for $\mathscr{F}$ being the family of Galois H-extensions for H a p-group, in [54]. There are many other cases where it is an interesting open problem to improve the known bound for Property $\mathbf{D}_{\mathscr{F},n}(\Delta)$.

To conclude, in this section we saw that the ℓ-torsion Conjecture follows from the Discriminant Multiplicity Conjecture. Now, recall that we saw in the context of bounding ℓ-torsion that uniform bounds for arbitrarily high moments can imply strong "pointwise" results for *every* field. Can the method of moments be used to approach the Discriminant Multiplicity Conjecture too? We turn to this idea next.

5.3. From the perspective of counting number fields of bounded discriminant

We come to a third motivation to believe the ℓ-torsion Conjecture. Recall the definition (3.1) of a family $\mathscr{F}_n(G;X)$ of degree n fields $K/\mathbb{Q}$ with $\mathrm{Gal}(\tilde{K}/\mathbb{Q})$ isomorphic (as a permutation group) to a nontrivial transitive subgroup $G \subseteq S_n$. Each element $g \in G$ has an index defined by $\mathrm{ind}(g) = n - o_g$, where o_g is the number of orbits of g when it acts on a set of n elements. Define $a(G)$ according to $a(G)^{-1} = \min\{\mathrm{ind}(g) : 1 \neq g \in G\}$; we see that $\frac{1}{n-1} \leq a(G) \leq 1$. Malle has made a well-known conjecture [65]:

Conjecture 5.2 (Malle). *For each $n \geq 2$, for each transitive subgroup $G \subseteq S_n$,*

$$\left|\mathscr{F}_n(G;X)\right| \ll_{G,\varepsilon} X^{a(G)+\varepsilon}, \quad \text{for all } \varepsilon > 0. \tag{5.8}$$

Also, $|\mathscr{F}_n(G;X)| \gg_G X^{a(G)}$.

The full statement of this conjecture is an open problem. Its difficulty is indicated by the fact that it implies a positive solution to the inverse Galois problem for number fields. (A refinement in [66] specified a power of $\log X$ in place of X^{ε}; counterexamples to this refinement have been found in [50], but the upper bound in (5.8) is expected to be true.)

Malle's Conjecture has been proved for abelian groups, with a strategy by Cohn [24], and asymptotic counts by Mäki [64], Wright [97]. For $n = 3, 4, 5$, it is known for S_n by the asymptotic (3.3), and for D_4 by Baily [3] (refined to an asymptotic in [20]). It is known for $C_2 \wr H$ under mild conditions on H (in particular, for at least one group of order n for every even n) by [53], and for $S_n \times A$ with A an abelian group by [67, 90]. For prime

degree p D_p-fields, upper and lower bounds are closely related to p-torsion in class groups of quadratic fields, and have been studied in [23, 41, 51].

For many groups, it is a difficult open problem to prove upper or lower bounds approaching Malle's prediction. In many results surveyed here, proving a lower bound for $|\mathscr{F}_n(G;X)|$ has been an important step, to verify a result applies to "almost all" fields in a family. For many groups G, it is not even known that $|\mathscr{F}_n(G;X)| \gg X^{\beta}$ for some $\beta > 0$ as $X \to \infty$. Here is a tool to prove such a result: suppose $f(X, T_1, \dots, T_s) \in \mathbb{Q}[X, T_1, \dots, X_s]$ is a regular polynomial of total degree d in the T_i and of degree m in X with transitive Galois group $G \subset S_n$ over $\mathbb{Q}(T_1, \dots, T_s)$. Then $|\mathscr{F}_n(G;X)| \gg_{f,\varepsilon} X^{\beta-\varepsilon}$ for every $\varepsilon > 0$, with $\beta = \frac{1-|G|^{-1}}{d(2m-2)}$; this is proved in [72]. For $G = A_n$, a polynomial f exhibited by Hilbert can be input to this criterion, implying that $|\mathscr{F}_n(A_n;X)| \gg X^{\beta_n+\varepsilon}$ for some $\beta_n > 0$, providing the first lower bound that grows like a power of X. Here is an open problem: for many groups G, no such polynomial f has yet been exhibited.

Now we focus on the conjectured upper bound (5.8) for counting fields with bounded discriminant. For any family $\mathscr{F} = \mathscr{F}_n(G;X)$ of fields, the strong "pointwise" property $\mathbf{D}_{\mathscr{F},n}(0)$ implies Malle's "average" upper bound (5.8) for the group G; see [54]. What is more surprising is that there is a converse to this. This relates to our question: can the method of moments be used to deduce the Discriminant Multiplicity Conjecture? Formally, it can. Given a family $\mathscr{F}$ of fields, for each integer $D \geq 1$ let $m(D)$ denote the number of fields $K \in \mathscr{F}$ with $D_K = D$. If arbitrarily high kth moment bounds are known for the function $m(D)$, the Discriminant Multiplicity Conjecture follows; see [73]. But the first moment of $m(D)$ is the subject of the Malle Conjecture (5.8), so the method of moments certainly seems a difficult avenue to pursue. Yet interestingly, Ellenberg and Venkatesh have shown that in this context the kth moments can be repackaged as *averages*.

Informally, the idea is to replace bounding the kth moment of the function $m(D)$ for G-Galois fields in a family $\mathscr{F}$ by counting fields in a family $\mathscr{F}^{(k)}$ of G^k-Galois fields. Ellenberg and Venkatesh order the fields in $\mathscr{F}^{(k)}$ not by discriminant D_K, but (roughly speaking) by the square-free kernel $D_K^{\#}$ of the discriminant. They generalize the Malle Conjecture to posit that in this ordering, $\ll X^{1+\varepsilon}$ fields in $\mathscr{F}^{(k)}$ have $D_K^{\#} \leq X$, *uniformly* for all integers $k \geq 1$. Assuming this conjecture, suppose there are $m(D)$ many G-Galois fields $K_1, \dots, K_{m(D)}$ with $D_{K_i} = D$. Taking composita of k of these generates at least $\gg_k m(D)^k$ many G^k-Galois fields in the family $\mathscr{F}^{(k)}$, with $D_K^{\#} \leq D$. If we suppose $m(D) \geq D^{\alpha}$ for some $\alpha > 0$ and a sequence of $D \to \infty$, under the generalized Malle Conjecture it must be that $\alpha k \leq 1$ for all $k \geq 1$. Hence α must be arbitrarily small, as desired.

In full generality, Ellenberg and Venkatesh propose a generalized Malle Conjecture in terms of an f-discriminant, for any rational class function f, and an appropriate generalization $a_G(f)$ of the exponent in (5.8). They verify that for a particular choice of f, this implies the Discriminant Multiplicity Conjecture. More recently, Klüners and Wang have shown directly that Malle's Conjecture (5.8) for all groups G implies the Discriminant Multiplicity Conjecture (also over any number field) [54].

Let us sum up: the upper bound (5.8) in Malle's Conjecture for all groups G implies the Discriminant Multiplicity Conjecture. The Discriminant Multiplicity Conjecture implies

the ℓ-torsion Conjecture. Also, the Discriminant Multiplicity Conjecture for $\mathcal{F}_n(G;X)$ (that is, property $\mathbf{D}_{\mathcal{F},n}(0)$) implies Malle's Conjecture for $\mathcal{F}_n(G;X)$. Moreover, there is one more converse: Alberts has shown that if the ℓ-torsion Conjecture is true for all solvable extensions and all primes ℓ (even just in an average sense), then Malle's upper bound (5.8) holds for all solvable groups [1]. Thus Malle's Conjecture, the Discriminant Multiplicity Conjecture, and the ℓ-torsion Conjecture are truly equivalent, when restricted to solvable groups. These relationships provide clear motivation for why so many methods described in this survey have involved counting number fields.

In conclusion, we have seen from three different perspectives that the ℓ-torsion Conjecture should be true. But as Gauss wrote, "*Demonstrationes autem* rigorosae *harum observationum perdifficiles esse videntur*."

FUNDING

This work was partially supported by NSF CAREER DMS-1652173.

REFERENCES

[1] B. Alberts, The weak form of Malle's conjecture and solvable groups. *Res. Number Theory* **6** (2020), no. 1, 23, Paper No. 10.

[2] C. An, ℓ-torsion in class groups of certain families of D_4-quartic fields. *J. Théor. Nombres Bordeaux* **32** (2020), no. 1, 1–23.

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

[4] O. Beckwith, Indivisibility of class numbers of imaginary quadratic fields. *Res. Math. Sci.* **4** (2017), 11, Paper No. 20.

[5] K. Belabas, M. Bhargava, and C. Pomerance, Error estimates for the Davenport–Heilbronn theorems. *Duke Math. J.* **153** (2010), no. 1, 173–210.

[6] M. Belolipetsky and A. Lubotzky, Counting non-uniform lattices. *Israel J. Math.* **232** (2019), no. 1, 201–229.

[7] M. Bhargava, The density of discriminants of quartic rings and fields. *Ann. of Math.* **162** (2005), no. 2, 1031–1063.

[8] M. Bhargava, Higher composition laws and applications. In *ICM Proceedings. Vol. II*, pp. 271–294, Eur. Math. Soc., Zürich, 2006.

[9] M. Bhargava, The density of discriminants of quintic rings and fields. *Ann. of Math.* **172** (2010), no. 3, 1559–1591.

[10] 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. *J. Amer. Math. Soc.* **33** (2020), no. 4, 1087–1099.

[11] M. Bhargava, A. Shankar, and J. Tsimerman, On the Davenport–Heilbronn theorems and second order terms. *Invent. Math.* **193** (2013), no. 2, 439–499.

[12] M. Bhargava, A. Shankar, and X. Wang, Squarefree values of polynomial discriminants. 2016, arXiv:1611.09806v2.

[13] M. Bhargava and I. Varma, On the mean number of 2-torsion elements in the class groups, narrow class groups, and ideal groups of cubic orders and fields. *Duke Math. J.* **164** (2015), 1911–1933.

[14] M. Bhargava and I. Varma, The mean number of 3-torsion elements in the class groups and ideal groups of quadratic orders. *Proc. Lond. Math. Soc.* **112** (2016), 235–266.

[15] E. Bombieri and J. Pila, The number of integral points on arcs and ovals. *Duke Math. J.* **59** (1989), no. 2, 337–357.

[16] A. Brumer and O. McGuinness, The behavior of the Mordell–Weil group of elliptic curves. *Bull. Amer. Math. Soc. (N.S.)* **23** (1990), no. 2, 375–382.

[17] A. Brumer and J. H. Silverman, The number of elliptic curves over $\mathbb{Q}$ with conductor N. *Manuscripta Math.* **91** (1996), no. 1, 95–102.

[18] F. Brumley, J. Thorner, and A. Zaman, Zeros of Rankin–Selberg L-functions at the edge of the critical strip. *J. Eur. Math. Soc. (JEMS)* (2021). DOI 10.4171/JEMS/1134.

[19] F. Calegari, The Artin conjecture for some S_5-extensions. *Math. Ann.* **356** (2013), no. 1, 191–207.

[20] H. Cohen, F. Diaz y Diaz, and M. Olivier, Enumerating quartic dihedral extensions of $\mathbb{Q}$. *Compos. Math.* **133** (2002), no. 1, 65–93.

[21] H. Cohen and H. W. Lenstra Jr., Heuristics on class groups of number fields. In *Number theory*, pp. 33–62, Lecture Notes in Math., Springer, Berlin, 1984.

[22] H. Cohen and J. Martinet, Étude heuristique des groupes de classes des corps de nombres. *J. Reine Angew. Math.* **404** (1990), 39–76.

[23] H. Cohen and F. Thorne, On D_ℓ-extensions of odd prime degree ℓ. *Proc. Lond. Math. Soc. (3)* **121** (2020), no. 5, 1171–1206.

[24] H. Cohn, The density of abelian cubic fields. *Proc. Amer. Math. Soc.* **5** (1954), 476–477.

[25] J.-M. Couveignes, Enumerating number fields. *Ann. of Math.* **192** (2020), no. 2, 487–497.

[26] D. A. Cox, *Primes of the form $x^2 + ny^2$. 2nd edn.* Pure Appl. Math., John Wiley & Sons, Inc., Hoboken, NJ, 2013.

[27] H. Davenport, *Multiplicative number theory. 3rd edn.* Grad. Texts in Math. 74, Springer, 2000.

[28] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields II. *Proc. R. Soc. Lond. A* **322** (1971), 405–420.

[29] W. Duke, Bounds for arithmetic multiplicities. In *Proceedings of the International Congress of Mathematicians, Doc. Math., Jahresber. Dtsch. Math.-Ver., Vol. II (Berlin, 1998)*, pp. 163–172, 1998.

[30] W. Duke and E. Kowalski, A problem of Linnik for elliptic curves and mean-value estimates for automorphic representations. *Invent. Math.* **139** (2000), 1–39.

[31] H. M. Edwards, *Fermat's last theorem*. Grad. Texts in Math. 50, Springer, New York, 1996.

[32] J. Ellenberg, Points of low height on $\mathbb{P}^1$ over number fields and bounds for torsion in class groups. In *Computational arithmetic geometry*, pp. 45–48, Contemp. Math. 463, AMS, Providence, 2008.

[33] J. Ellenberg, L. B. Pierce, and M. M. Wood, On ℓ-torsion in class groups of number fields. *Algebra Number Theory* **11** (2017), 1739–1778.

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

[35] J. Ellenberg and A. Venkatesh, Counting extensions of function fields with bounded discriminant and specified Galois group. In *Prog. Math*, pp. 151–168, 235, Birkhäuser Boston, Boston, MA, 2005.

[36] J. Ellenberg and A. Venkatesh, The number of extensions of a number field with fixed degree and bounded discriminant. *Ann. of Math.* **163** (2006), no. 2, 723–741.

[37] K. B. Ford, Vinogradov's integral and bounds for the Riemann zeta function. *Proc. Lond. Math. Soc. (3)* **85** (2002), no. 3, 565–633.

[38] É. Fouvry and J. Klüners, On the 4-rank of class groups of quadratic number fields. *Invent. Math.* **167** (2006), no. 3, 455–513.

[39] É. Fouvry, M. Nair, and G. Tenenbaum, L'ensemble exceptionnel dans la conjecture de Szpiro. *Bull. Soc. Math. France* **120** (1992), no. 4, 485–506.

[40] C. Frei and M. Widmer, Average bounds for the ℓ-torsion in class groups of cyclic extensions. *Res. Number Theory* **4** (2018), no. 3, 25, Paper No. 34.

[41] C. Frei and M. Widmer, Averages and higher moments for the ℓ-torsion in class groups. *Math. Ann.* **379** (2021), no. 3–4, 1205–1229.

[42] D. Goldfeld, Gauss's class number problem for imaginary quadratic fields. *Bull. Amer. Math. Soc. (N.S.)* **13** (1985), no. 1, 23–37.

[43] C. Goldstein, N. Schappacher, and J. Schwermer (eds.), The shaping of arithmetic after C. F. Gauss's "Disquisitiones arithmeticae", Springer, Berlin, 2007.

[44] D. R. Heath-Brown, Quadratic class numbers divisible by 3. *Funct. Approx. Comment. Math.* **37(part 1)** (2007), 203–211.

[45] D. R. Heath-Brown, Imaginary quadratic fields with class group exponent 5. *Forum Math.* **20** (2008), 275–283.

[46] D. R. Heath-Brown and L. B. Pierce, Averages and moments associated to class numbers of imaginary quadratic fields. *Compos. Math.* **153** (2017), 2287–2309.

[47] H. Heilbronn, On real simple zeros of Dedekind ζ-functions. In *Proceedings of the number theory conference*, pp. 108–110, Univ. Colorado, Boulder, 1972.

[48] H. A. Helfgott and A. Venkatesh, Integral points on elliptic curves and 3-torsion in class groups. *J. Amer. Math. Soc.* **19** (2006), no. 3, 527–550.

[49] P. Humphries and J. Thorner, Zeros of Rankin–Selberg L-functions in families. 2021, arXiv:2103.05634.

[50] J. Klüners, A counterexample to Malle's conjecture on the asymptotics of discriminants. *C. R. Math. Acad. Sci. Paris* **340** (2005), 411–414.

[51] J. Klüners, Asymptotics of number fields and the Cohen–Lenstra heuristics. *J. Théor. Nombres Bordeaux* **18** (2006), 607–615.

[52] J. Klüners, The number of S_4-fields with given discriminant. *Acta Arith.* **122** (2006), no. 2, 185–194.

[53] J. Klüners, The distribution of number fields with wreath products as Galois groups. *Int. J. Number Theory* **8** (2012), no. 3, 845–858.

[54] J. Klüners and J. Wang, ℓ-torsion bounds for the class group of number fields with an ℓ-group as galois group. 2020, arXiv:2003.12161.

[55] J. Klys, The distribution of p-torsion in degree p cyclic fields. *Algebra Number Theory* **14** (2020), no. 4, 815–854.

[56] E. Kowalski and P. Michel, Zeros of families of automorphic L-functions close to 1. *Pacific J. Math.* **207** (2002), no. 2, 411–431.

[57] P. Koymans and D. Milovic, On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-2p})$ for primes $p \equiv 1 \mod 4$. *Int. Math. Res. Not. IMRN* **23** (2019), 7406–7427.

[58] P. Koymans and D. Milovic, Joint distribution of spins. *Duke Math. J.* **170** (2021), no. 8, 1723–1755.

[59] P. Koymans and C. Pagano, On the distribution of $\mathrm{Cl}(K)[\ell^\infty]$ for degree ℓ cyclic fields. 2018, arXiv:1812.06884.

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

[61] R. Lemke Oliver and F. Thorne, Upper bounds on number fields of given degree and bounded discriminant. 2020, arXiv:2005.14110.

[62] R. Lemke Oliver, J. Thorner, and A. Zaman, An approximate form of Artin's holomorphy conjecture and non-vanishing of Artin L-functions. 2021, arXiv:2012.14422v3.

[63] R. Lemke Oliver, J. Wang, and M. M. Wood, The average size of 3-torsion in class groups of 2-extensions. 2021, arXiv:2110.07712v2.

[64] S. Mäki, On the density of abelian number fields. *Ann. Acad. Sci. Fenn. Ser. A I Math. Diss.* **54** (1985), 104.

[65] G. Malle, On the distribution of Galois groups. *J. Number Theory* **92** (2002), 315–219.

[66] G. Malle, On the distribution of Galois groups II. *Exp. Math.* **13** (2004), 129–135.

[67] R. Masri, F. Thorne, W.-L. Tsai, and J. Wang, Malle's Conjecture for $G \times A$, with $G = S_3, S_4, S_5$. 2020, arXiv:2004.04651.

[68] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers. 2nd edn*. Springer, Berlin, 1990.

[69] J. Neukirch, *Algebraic number theory*. Springer, 1999.

[70] L. B. Pierce, The 3-part of class numbers of quadratic fields. *J. Lond. Math. Soc.* **71** (2005), 579–598.

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

[72] L. B. Pierce, C. 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. *Invent. Math.* **219** (2020), 701–778.

[73] L. B. Pierce, C. Turnage-Butterbaugh, and M. M. Wood, On a conjecture for ℓ-torsion in class groups of number fields: from the perspective of moments. *Math. Res. Lett.* **28** (2021), 575–621.

[74] W. M. Ruppert, Small generators of number fields. *Manuscripta Math.* **96** (1998), no. 1, 17–22.

[75] W. M. Schmidt, Number fields of given degree and bounded discriminant. *Astérisque* **(228):4** (1995), 189–195.

[76] A. Scholz, Über die Beziehung der Klassenzahlen quadratischer Körper. *J. Reine Angew. Math.* **166** (1932), 201–203.

[77] J.-P. Serre, Quelques applications du théorème de densité de Chebotarev. *Publ. Math. Inst. Hautes Études Sci.* **54** (1982), 123–201.

[78] J.-P. Serre, *Lectures on the Mordell–Weil theorem. 3rd edn*. Friedr. Vieweg and Sohn, Braunschweig, 1997.

[79] A. Shankar and J. Tsimerman, Counting S_5-fields with a power saving error term. *Forum Math. Sigma* **2** (2014).

[80] J. H. Silverman, Lower bounds for height functions. *Duke Math. J.* **51** (1984), no. 2, 395–403.

[81] A. Smith, 2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture. 2017, arXiv:1702.02325v2.

[82] K. Soundararajan, Divisibility of class numbers of imaginary quadratic fields. *J. Lond. Math. Soc. (2)* **61** (2000), no. 3, 681–690.

[83] H. M. Stark, Some effective cases of the Brauer–Siegel theorem. *Invent. Math.* **23** (1974), 135–152.

[84] H. M. Stark, The Gauss class-number problems. In *Analytic number theory*, pp. 247–256, Clay Math. Proc. 7, Amer. Math. Soc., 2007.

[85] T. Taniguchi and F. Thorne, The secondary term in the counting function for cubic fields. *Duke Math. J.* **162** (2013), 2451–2508.

[86] J. Thorner and A. Zaman, A zero density estimate for Dedekind zeta functions. 2019, arXiv:1909.01338.

[87] J. Thorner and A. Zaman, An unconditional GL_n large sieve. *Adv. Math.* **378** (2021), 107529.

[88] N. Tschebotareff, Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. *Math. Ann.* **95** (1926), no. 1, 191–228.

[89] J. Wang, Pointwise bound for ℓ-torsion in class groups II: nilpotent extensions. 2020, arXiv:2006.10295.

[90] J. Wang, Malle's conjecture for $S_n \times A$ for $n = 3, 4, 5$. *Compos. Math.* **157** (2021), no. 1, 83–121.

[91] J. Wang, Pointwise bound for ℓ-torsion in class groups: elementary abelian extensions. *J. Reine Angew. Math.* **773** (2021), 129–151.

[92] W. Wang and M. M. Wood, Moments and interpretations of the Cohen–Lenstra–Martinet heuristics. *Comment. Math. Helv.* **96** (2021), no. 2, 339–387.

[93] M. Watkins, Class numbers of imaginary quadratic fields. *Math. Comp.* **73** (2004), no. 246, 907–938.

[94] M. Watkins, Some heuristics about elliptic curves. *Exp. Math.* **17** (2008), no. 1, 105–125.

[95] M. Widmer, Bounds for the ℓ-torsion in class groups. *Bull. Lond. Math. Soc.* **50** (2018), no. 1, 124–131.

[96] S. Wong, Exponents of class groups and elliptic curves, corrigendum. *J. Number Theory* **90** (2001), no. 2, 376–377.

[97] D. Wright, Distribution of discriminants of abelian extensions. *Proc. Lond. Math. Soc.* **58** (1989), 17–50.

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

LILLIAN B. PIERCE

Mathematics Department, Duke University, Durham, NC 27708, USA,
pierce@math.duke.edu