Residual indices of fixed multiplicative subgroups over number fields: power savings and moment obstructions

Santiago Pineda Montoya

Departamento de Matemáticas, Facultad de Ciencias
Universidad Nacional de Colombia, Medellín 050034, Colombia

sapinedamo@unal.edu.co ORCID 0000-0001-5736-6634

hexagon:2611.01069v1

Abstract

The residual index of a multiplicative group at a good prime ideal is the index of its reduction in the multiplicative residue group. For a fixed finitely generated group of rank r over a number field, we prove a power-saving estimate for the full index distribution up to norm X, with errors weighted by t^σ, where t is the index. The estimate is uniform in a Frobenius restriction in a fixed finite Galois extension and allows torsion. Under the generalized Riemann hypothesis it holds for $r \geq 2$ and $0 \leq \sigma < (r-1)/(r+2)$. More generally, it follows from a common bound below $r/(r+1)$ for the real parts of the nontrivial zeta zeros of the relevant division-field composita. Model moments are finite unconditionally for positive orders below r, and empirical moments converge in the proved weight range.

We also give unconditional counterexamples to Ambrose's number-field generalization of Wagstaff's moment heuristic for fixed groups, using the unrestricted count over all residue degrees. For rational generators of rank $r > 1$ in a nontrivial finite Galois extension of $\mathbb{Q}$, the contribution of each occurring residue degree $f > 1$ contradicts the proposed scales at moment orders $1 < s < 1 + f(r-1)$. Higher-degree ideals have relative density zero, but their normalized first-moment tails carry a positive contribution, which diverges in rank one. Two rank-three groups over $\mathbb{Q}(i)$, including a group of norm one that generates the field, have second-moment sums at least of order $X^{3/2}/\log X$. For $\langle 2, 3, 5\rangle$, the lower-bound coefficient is $655\zeta(3)/(14\pi^4)$, where ζ is the Riemann zeta function.

1 Introduction

Artin's primitive root problem, formulated in his correspondence with Hasse [1, §17.2], asks how often a fixed rational number generates the full multiplicative group modulo a prime. For $a \in \mathbb{Q}^\times$ and a prime p dividing neither its numerator nor its denominator, let $\mathrm{ord}_p(a)$ denote its multiplicative order modulo p. The residual index of $\langle a\rangle$ at p is

$$I_p^{\mathbb{Q}}(a) := \frac{p-1}{\mathrm{ord}_p(a)}.$$

Artin's problem concerns the primes for which $I_p^{\mathbb{Q}}(a) = 1$.

Even if the density of primes with $I_p^{\mathbb{Q}}(a) = t$ exists for every fixed integer $t \geq 1$, a positive moment also depends on the weight carried by large indices. This distinction occurs for fixed groups over $\mathbb{Q}(i)$. In the examples below, the prime ideals of residue degree two have relative density zero, yet they contribute a positive amount to the normalized first moment above every fixed index cutoff.

We prove a conditional power-saving theorem for weighted residual-index distributions of fixed finitely generated multiplicative subgroups over number fields. Section 4 establishes unconditional higher-degree moment bounds, classwise refinements and explicit Gaussian coefficients. Section 5 deduces the admissible ranks and weights and separates the method's ceiling from the arithmetic obstruction at weight one.

1.1 The fixed-group moment problem

Let K be a number field with ring of integers $\mathcal{O}_K$, and fix a finitely generated multiplicative subgroup $\Gamma \leq K^\times$. Its torsion subgroup is denoted by Γ_{tor}, and its free rank $r \geq 1$ is given by $\Gamma/\Gamma_{\mathrm{tor}} \simeq \mathbb{Z}^r$. Choose a generating tuple of length m_Γ, so that $\Gamma = \langle \gamma_1, \dots, \gamma_{m_\Gamma} \rangle$.

For a nonzero prime ideal $\mathfrak{p}$ above a rational prime p, let $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ be its residue field and $q_\mathfrak{p} = |k_\mathfrak{p}|$ its absolute norm. Its absolute residue degree is $\deg(\mathfrak{p}) = [k_\mathfrak{p} : \mathbb{F}_p]$, where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Thus $q_\mathfrak{p} = p^{\deg(\mathfrak{p})}$. We call $\mathfrak{p}$ a higher-degree prime if $\deg(\mathfrak{p}) > 1$.

For $a \in K^\times$, write $v_\mathfrak{p}(a)$ for the normalized additive valuation, the exponent of $\mathfrak{p}$ in the principal fractional ideal $a\mathcal{O}_K$. The finite set of primes of bad reduction for Γ is

$$S_\Gamma = \bigcup_{j=1}^{m_\Gamma} \{\mathfrak{p} : v_\mathfrak{p}(\gamma_j) \neq 0\}.$$

A prime $\mathfrak{p}$ is good if $\mathfrak{p} \notin S_\Gamma$, or equivalently if the whole group Γ lies in the unit group of the local ring $\mathcal{O}_{K,\mathfrak{p}}$, the localization of $\mathcal{O}_K$ at $\mathfrak{p}$. At such a prime the reduction map $\mathrm{red}_\mathfrak{p} : \mathcal{O}_{K,\mathfrak{p}}^\times \to k_\mathfrak{p}^\times$ sends a/b to $\bar{a}\,\bar{b}^{-1}$ for $a, b \in \mathcal{O}_K \setminus \mathfrak{p}$, where the bars denote residue classes modulo $\mathfrak{p}$ [2, Chs. 3–4]. The reduced subgroup is

$$\Gamma_\mathfrak{p} = \mathrm{red}_\mathfrak{p}(\Gamma) = \langle\, \mathrm{red}_\mathfrak{p}(\gamma_j) : 1 \leq j \leq m_\Gamma \rangle \;\leq\; k_\mathfrak{p}^\times.$$

Its residual index is

$$I_\mathfrak{p} = [k_\mathfrak{p}^\times : \Gamma_\mathfrak{p}] = \frac{q_\mathfrak{p} - 1}{|\Gamma_\mathfrak{p}|}. \tag{1}$$

For $\Gamma \leq \mathbb{Q}^\times$ and a good rational prime p, denote reduction modulo p by red_p and write $I_p^{\mathbb{Q}} = [\mathbb{F}_p^\times : \mathrm{red}_p(\Gamma)]$. For $\Gamma = \langle a \rangle$ this recovers $I_p^{\mathbb{Q}}(a)$.

For a real norm bound $X \geq 2$, let $\pi_K(X)$ count all nonzero prime ideals of K with $q_\mathfrak{p} \leq X$, including every residue degree, and write $\pi(X) = \pi_{\mathbb{Q}}(X)$. For $\pi_K(X) > 0$ and an integer $t \geq 1$, define

$$P_X(t) = \frac{\#\{\mathfrak{p} \notin S_\Gamma : q_\mathfrak{p} \leq X,\ I_\mathfrak{p} = t\}}{\pi_K(X)}.$$

This is the proportion of all prime ideals up to norm X that are good and have residual index t. These frequencies are the masses of the empirical measure P_X.

For real $s > 0$, put

$$S_s(X) = \sum_{\substack{\mathfrak{p} \notin S_\Gamma \\ q_\mathfrak{p} \leq X}} I_\mathfrak{p}^s, \qquad \frac{S_s(X)}{\pi_K(X)} = \sum_{t \geq 1} t^s P_X(t).$$

The normalized sum $S_s(X)/\pi_K(X)$ is the s-th moment of P_X. To recover its limit from the fixed-index frequencies, split at a fixed cutoff $T \geq 1$ on the index,

$$\frac{S_s(X)}{\pi_K(X)} = \sum_{t \leq T} t^s P_X(t) + \sum_{t > T} t^s P_X(t).$$

Suppose that $P_X(t)$ converges for every fixed t and that the limiting frequencies have finite s-th moment. For each fixed T, the first sum then converges term by term. Convergence of the full normalized moment to the moment of the limiting frequencies is equivalent to the tail condition

$$\lim_{T\to\infty} \limsup_{X\to\infty} \sum_{t>T} t^s P_X(t) = 0.$$

We ask for which exponents the tail condition holds and how fast the moment converges. Theorem 1.1 gives a rate for the weighted index distribution under a common bound on zeta zeros, and Corollary 1.2 deduces a range of convergent moments. Theorem 1.3 treats the obstruction at weight one unconditionally.

1.2 The distribution theorem

We may restrict the primes by their splitting behavior in a fixed finite Galois extension F/K with group $G_F = \mathrm{Gal}(F/K)$. Let $\mathfrak{d}_{F/K}$ be the relative discriminant ideal. A prime ideal $\mathfrak{p}$ is *admissible* if it is good for Γ and unramified in F/K, equivalently if it lies outside $S_{\mathrm{exc}} = S_\Gamma \cup \{\mathfrak{p} : \mathfrak{p} \mid \mathfrak{d}_{F/K}\}$. Choose a prime ideal $\mathfrak{P}$ of the ring of integers $\mathcal{O}_F$ above an admissible $\mathfrak{p}$, so $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. The stabilizer of $\mathfrak{P}$ in G_F is its decomposition group. The arithmetic Frobenius at $\mathfrak{P}$ is the unique element of this group inducing $x \mapsto x^{q_\mathfrak{p}}$ on $k_\mathfrak{P} = \mathcal{O}_F/\mathfrak{P}$. Its order is $[k_\mathfrak{P} : k_\mathfrak{p}]$, and its conjugacy class $\mathrm{Frob}_{\mathfrak{p},F/K}$ is independent of $\mathfrak{P}$ [2, Ch. 8, pp. 139–143]. The identity class selects the primes that split completely. For $F/K = \mathbb{Q}(i)/\mathbb{Q}$, the identity and complex conjugation select $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$, respectively.

Let C be a union of conjugacy classes in G_F, the *Frobenius filter*. Let $\mathcal{P}_C(X)$ be the admissible primes with $q_\mathfrak{p} \le X$ and $\mathrm{Frob}_{\mathfrak{p},F/K} \subseteq C$. For $\pi_K(X) > 0$, the filtered empirical measure $P_{X,C}$ has mass at an integer $t \ge 1$ equal to the proportion of all prime ideals counted by $\pi_K(X)$ that belong to $\mathcal{P}_C(X)$ and have residual index t. The corresponding frequencies and unnormalized moment sums are

$$P_{X,C}(t) = \frac{\#\{\mathfrak{p} \in \mathcal{P}_C(X) : I_\mathfrak{p} = t\}}{\pi_K(X)}, \qquad S_{s,C}(X) = \sum_{\mathfrak{p}\in\mathcal{P}_C(X)} I_\mathfrak{p}^s.$$

With this normalization, Chebotarev's theorem gives $\sum_{t\ge1} P_{X,C}(t) = |\mathcal{P}_C(X)|/\pi_K(X) \to |C|/|G_F|$ [2, Theorem 8.31]. Taking $F = K$ and $C = \{1\}$ recovers $P_X(t)$ and $S_s(X)$. The moment decomposition and tail criterion of Section 1.1 apply to $P_{X,C}$ and $S_{s,C}$ under the same hypotheses.

Write $\mathrm{Li}(X) = \int_2^X dt/\log t$. Motivated by Wagstaff's work on Fermat pseudoprimes [3], Ambrose proposed a heuristic for these moments [4, §4.2, p. 27, (4.2)]. In our notation, its literal prime-ideal formulation predicts, for a fixed group and nonempty C, positive constants $\mathcal{A}_j$ depending on the fixed data and on s, with

$$S_{s,C}(X) \sim \begin{cases} \mathcal{A}_1 \,\mathrm{Li}(X), & 0 < s < r, \\ \mathcal{A}_2 X, & s = r, \\ \mathcal{A}_3 \,\mathrm{Li}(X^{s-r+1}), & s > r. \end{cases} \tag{2}$$

Ambrose's results on averages over generating tuples establish asymptotic formulae and growth bounds [4, Theorems 6.1–6.2]. For the fixed groups considered here, we establish the first line of (2) in a conditional range of small positive exponents, with a power-saving error and an explicit leading constant. We also exhibit two fixed groups for which that line fails at a larger exponent.

To construct the model for exact indices, first fix an integer $n \ge 1$ and count the primes at which $n \mid I_\mathfrak{p}$. In a fixed algebraic closure of K, let μ_n denote the group of n-th roots of unity and $\Gamma^{1/n}$ the set of n-th roots of elements of Γ. The division field $K_n = K(\mu_n, \Gamma^{1/n})$ and its

compositum $E_n = FK_n$ are finite Galois over K [5, Chs. 3 and 5]. At an admissible prime $\mathfrak{p}$ of residue characteristic coprime to n, the condition $n \mid I_{\mathfrak{p}}$ is equivalent to complete splitting in K_n/K (Section 2.1). Chebotarev therefore gives the density $b_C(n)$ of admissible primes satisfying the filter and $n \mid I_{\mathfrak{p}}$ at this fixed level. Write $k_n = [K_n : K]$ and $H_n = \mathrm{Gal}(E_n/K_n)$. Let B_n be the set of automorphisms of E_n that fix K_n and whose restriction to F belongs to C. With μ denoting the Möbius function [6, Ch. 2], put

$$B_n = \{h \in H_n : h|_F \in C\}, \qquad b_C(n) = \frac{|B_n|}{[E_n : K]}, \qquad D_C(t) = \sum_{v \geq 1} \mu(v) b_C(tv). \tag{3}$$

The last sum applies Möbius inversion to pass from divisibility by n to the model mass at the exact index t. The notation B_n suppresses the fixed filter. Section 2.1 proves absolute convergence and shows that D_C is a nonnegative measure on $\mathbb{N}$ of mass $|C|/|G_F|$. For such a measure ν we write $\nu(t) = \nu(\{t\})$.

For a number field L, write ζ_L for its Dedekind zeta function and $\zeta = \zeta_{\mathbb{Q}}$. For $1/2 \leq \theta < 1$, let $\mathcal{Z}(\theta)$ mean that every nontrivial zero z of every ζ_{E_n} satisfies $\Re z \leq \theta$. Here nontrivial means $0 < \Re z < 1$ [7, Ch. VI, §1 and Ch. VIII, §10]. For the completed function see [8, §5, (5.5)–(5.8)]. The generalized Riemann hypothesis (GRH) for this family places all these zeros on $\Re z = 1/2$ and gives $\mathcal{Z}(1/2)$.

In the following estimate σ is the exponent of the weight t^σ. The proof uses X^u as a cutoff on divisibility levels. The exponent δ_* measures the unweighted power saving, up to the arbitrarily small loss ε, and σ_* is the upper endpoint of the range of weights.

Theorem 1.1 (Weighted distribution)**.** *Suppose $\mathcal{Z}(\theta)$ holds with $1/2 \leq \theta < r/(r+1)$. Define*

$$u = \frac{r + 1 - r\theta}{2r + 1}, \qquad \delta_* = \frac{r - (r+1)\theta}{2r + 1}, \qquad \sigma_* = \frac{\delta_*}{u}. \tag{4}$$

For $0 \leq \sigma < \sigma_*$ and $\varepsilon > 0$, uniformly over the unions C in G_F,

$$\sum_{t \geq 1} t^\sigma |P_{X,C}(t) - D_C(t)| \ll_{K,F,\Gamma,\theta,\sigma,\varepsilon} X^{-\delta_* + u\sigma + \varepsilon} \qquad (X \to \infty). \tag{5}$$

Theorem 1.1 provides the control of large indices required in Section 1.1. For $0 < s < \sigma_*$, its estimate, together with the finiteness of the model moment in Corollary 1.2, implies the tail condition for $P_{X,C}$. Section 5.1 gives the exact least admissible rank for a prescribed zero bound and weight.

The weighted total variation norm in (5) is the full sum of absolute discrepancies. It equals the supremum of $\left|\sum_t w(t)(P_{X,C}(t) - D_C(t))\right|$ over $|w(t)| \leq t^\sigma$, even if w depends on X. At $\sigma = 0$ this bounds the discrepancy on every set of indices. The hypotheses force $r \geq 2$ and $\delta_* > 0$, so the estimate saves a power of X whenever $\sigma < \sigma_*$. Taking $w(t) = t^s$ gives the moment estimate below. By the prime ideal theorem, $\pi_K(X) \sim \mathrm{Li}(X)$.

Corollary 1.2 (Positive moments of a fixed group)**.** *For $s > 0$ let J_s be the generalized Jordan totient*

$$J_s(n) = n^s \prod_{\ell \mid n} (1 - \ell^{-s}),$$

where ℓ runs over the distinct prime divisors of n and the empty product equals one. For $0 < s < r$ the series $M_{s,C} = \sum_{n \geq 1} J_s(n) b_C(n)$ converges, and unconditionally

$$M_{s,C} = \sum_{t \geq 1} t^s D_C(t), \qquad M_{s,C} \geq |C|/|G_F|. \tag{6}$$

Under the hypotheses of Theorem 1.1, for $0 < s < \sigma_*$ one has uniformly in C

$$S_{s,C}(X) = M_{s,C}\,\mathrm{Li}(X) + O_{K,F,\Gamma,\theta,s,\varepsilon}(X^{1 - \delta_* + us + \varepsilon}) \qquad (\varepsilon > 0). \tag{7}$$

Under GRH this includes every $0 < s < (r-1)/(r+2)$.

Corollary 1.2 answers the moment question in Section 1.1. Under the hypotheses of Theorem 1.1, the normalized moments $S_{s,C}(X)/\pi_K(X)$ converge to the explicit constant $M_{s,C}$ for $0 < s < \sigma_*$, with the power-saving rate furnished by (5). Unconditionally, the model moments are finite for $0 < s < r$. For nonempty C, the first line of (2) holds in the range of empirical convergence with $\mathcal{A}_1 = M_{s,C}$.

The generalized Jordan totient enters through the divisor identity $\sum_{d|n} J_s(d) = n^s$, proved for real $s > 0$ in (44).

The examples below concern larger positive moments of fixed groups whose reductions satisfy the same algebraic constraint at every prime of a given splitting type.

1.3 Why higher-degree primes affect the mean

Consider $\Gamma = \langle 2, 3, 5\rangle$ in $K = \mathbb{Q}(i)$. A good prime $p \equiv 3 \pmod 4$ is inert, so $(p) = p\mathbb{Z}[i]$ is a single prime ideal of norm p^2. The three rational generators still reduce into $\mathbb{F}_p^\times$, while the ambient group now has order $p^2 - 1$. Consequently

$$I_{(p)} = \frac{p^2 - 1}{p - 1} I_p^{\mathbb{Q}} = (p + 1)I_p^{\mathbb{Q}} \geq p + 1.$$

Up to norm X, the inert ideals come from rational primes $p \leq \sqrt{X}$, so they have relative density zero. In the interval $\sqrt{X}/2 < p \leq \sqrt{X}$, however, there are $\asymp \sqrt{X}/\log X$ inert primes by the prime number theorem for arithmetic progressions. Each has index at least $\sqrt{X}/2$. Their contribution to the first-moment sum is therefore $\gg X/\log X$. Since $\pi_K(X) \sim X/\log X$, this gives a positive lower bound for their normalized contribution. For every fixed T all these indices exceed T once X is sufficiently large (see (46)).

More generally, let $K/\mathbb{Q}$ be finite Galois with group G of order d, and suppose that Γ has rational generators. For a good unramified rational prime p with Frobenius class U, let f_U be the common order of the elements of U. Then $\deg(\mathfrak{p}) = f_U$ for every $\mathfrak{p} \mid p$. Since $\Gamma_{\mathfrak{p}} \subseteq \mathbb{F}_p^\times$, its index is $I_{\mathfrak{p}} = ((p^{f_U} - 1)/(p - 1))I_p^{\mathbb{Q}}$. To retain the rational factor, let $b_U^{\mathbb{Q}}(n)$ be the density among all rational primes of those with Frobenius class U and $n \mid I_p^{\mathbb{Q}}$, as in (3) with base $\mathbb{Q}$ and auxiliary extension K. With φ denoting Euler's totient, sum over the nonidentity conjugacy classes to define

$$c_K^\sharp(\Gamma) = \sum_{U \neq \{1\}} \frac{d}{f_U} \sum_{n \geq 1} \varphi(n) b_U^{\mathbb{Q}}(n), \qquad c_K = \sum_{U \neq \{1\}} \frac{|U|}{f_U}.$$

The series defining $c_K^\sharp(\Gamma)$ may take the value $+\infty$. Since $b_U^{\mathbb{Q}}(1) = |U|/d$, the $n = 1$ terms contribute exactly c_K.

Theorem 1.3 (Residue-degree obstruction)**.** *Let $K/\mathbb{Q}$ be a nontrivial finite Galois extension with group G, and let Γ be a fixed finitely generated multiplicative subgroup of $\mathbb{Q}^\times$ of positive rank, viewed inside $K^\times$. Write* ord(g) *for the order of an element g of G. Use the unrestricted count $F = K$, $C = \{1\}$. In this setting we omit the filter subscript from $P_{X,C}, D_C, S_{s,C}, M_{s,C}$ and b_C. For each order $f > 1$ of an element of G, and each fixed $s > 0$,*

$$S_s(X) \gg_{K,\Gamma,s,f} \frac{X^{a_f(s)}}{\log X}, \qquad a_f(s) = \frac{1 + (f - 1)s}{f}. \tag{8}$$

For every fixed $T \geq 1$, the contribution of ideals of absolute degree greater than one to the normalized first-moment tail $\sum_{t>T} tP_X(t)$ has lower limit at least $c_K^\sharp(\Gamma) > c_K$ as $X \to \infty$. This constant is finite for $r > 1$ and infinite for $r = 1$. For a nonnegative measure ν on $\mathbb{N}$ of finite first moment $\sum_{t\geq 1} t\nu(t) < \infty$ and a weight exponent $\sigma \geq 0$, put $V_\sigma(X, \nu) = \sum_{t\geq 1} t^\sigma |P_X(t) - \nu(t)|$, allowing the value $+\infty$. Then

$$\liminf_{X\to\infty} V_1(X, \nu) \geq c_K^\sharp(\Gamma), \qquad \lim_{X\to\infty} V_\sigma(X, \nu) = +\infty \quad (\sigma > 1). \tag{9}$$

When $r > 1$, the model first moment is finite. Separating the degree-one contribution gives the additional unconditional lower bound $\liminf_{X\to\infty} S_1(X)/\pi_K(X) \geq \sum_t tD(t) + c_K^\sharp(\Gamma)$ in the setting of Theorem 1.3, as proved in (52).

For $\Gamma = \langle 2, 3, 5\rangle$ in $\mathbb{Q}(i)$, $r = 3$, $c_K = 1/2$ and $a_2(2) = 3/2$. Section 4 also treats a rank-three group whose elements generate $\mathbb{Q}(i)$ as a field and have norm one, meaning that $\gamma\bar{\gamma} = 1$, where the bar denotes complex conjugation. At an inert prime their reductions lie in the subgroup of order $p + 1$ in $\mathbb{F}_{p^2}^\times$, so their index is a multiple of $p - 1$. For both groups the second moment satisfies

$$\liminf_{X\to\infty} \frac{(\log X)S_2(X)}{X^{3/2}} \geq \frac{329}{648}.$$

For the rational group Corollary 4.4 raises the coefficient to $655\zeta(3)/(14\pi^4)$. At $s = 2 < r$, the scale $X^{3/2}/\log X$ already exceeds the predicted $\mathrm{Li}(X)$ when all prime ideals are included in the count. At weight one the inert ideals contribute a lower limit of at least $(5887/12000)\zeta(3)$ to every fixed normalized first-moment tail for the rational group, and at least $251/432$ for the norm-one group (Sections 4.3 and 4.4). Theorem 4.3 gives the classwise lower coefficients for all positive moment orders. For the norm-one group, Proposition 4.5 also gives a lower limit for the full normalized mean of at least $\frac{3}{2}\sum_{t\geq 1} tD(t)$.

1.4 Antecedents and the proof

Primitive roots and prescribed indices. For the rational primitive-root problem, an admissible integer base is an integer other than -1 or a perfect square. For each such base, Hooley proved the primitive-root density assuming GRH for the relevant splitting fields [9]. Cooke and Weinberger treated the number-field problem [10, Theorem 1.1]. Lenstra works over global fields. His formulation includes a finitely generated subgroup and a Frobenius restriction [11, Theorem (3.1)]. Wagstaff related prescribed indices to pseudoprimes and considered their mean [3]. Murata obtained conditional asymptotics for a prescribed index [12]. Moree surveys these developments [13]. For rational groups of higher rank, Pappalardi studied how large the reduction is at almost all primes and the conditional density for index one [14, 15]. Cangelmi and Pappalardi calculated higher-rank constants, improved the GRH error term and gave an unconditional upper estimate [16, Theorems 1–2 and p. 123, (14)]. Sieve methods were used by Gupta and Murty [17] and Heath-Brown [18] to obtain lower bounds. For instance, at least one of $2, 3, 5$ is a primitive root at infinitely many rational primes. Pappalardi and Susa obtained prescribed-index densities in rank at least two [19, Theorem 1]. Abdullah, Mustafa and Pappalardi studied the algebraic constants for groups containing negative rationals [20, Theorem 1]. Nontrivial intersections between fields obtained by adjoining roots of the generators account for correction factors in these constants, as in the treatments by Moree and Stevenhagen and by Akbary and Fakhari [21, 22].

Weighted indices over the rationals. The rational fixed-index problem already has the strict threshold $\theta < r/(r + 1)$. Felix gives a prescribed-index theorem for groups generated by independent integers and a power saving for the mean of $\log I_p^{\mathbb{Q}}$ under a common half-plane [23, Theorems 3.1.3 and 3.1.5]. Pappalardi and Susa explicitly record the common-half-plane extension of their fixed-index asymptotic [19, p. 322]. Pappalardi had formulated the more general weighted-index problem [24, p. 377]. Bach, Lukes, Shallit and Williams studied the logarithmic weight for base two [25]. Fomenko, Felix and Murty, and Felix in higher rank developed the logarithmic mean-value theory [26–28]. For one rational base, Moree studied the order and index in congruence classes [29–31], and Felix studied density constants for arbitrary sets of indices [32].

Index distributions over number fields. For a number field, Ziegler treated a single algebraic number [33], and Sgobba studied conditions on the orders and indices of several separate generators under GRH [34, Theorems 1 and 3]. Järviniemi and Perucca and, subsequently, Järviniemi, Perucca and Sgobba studied the map sending a prime to the tuple of residual indices of several subgroups and the densities of the primes giving prescribed tuples [35, 36]. For a single generator with positive primitive-root density, Perucca and Shparlinski bound the ratio of this density to its Artin constant. If j is the largest integer for which the generator has a j-th root in K, the constant is the product over primes ℓ of $1-1/(\ell-1)$ for $\ell \mid j$ and $1-1/(\ell(\ell-1))$ for $\ell \nmid j$ [37, §1]. Perucca gives a closed formula over a general number field, and Chan obtains sharp bounds for quadratic fields [38, 39]. For a single torsion-free group, the theorem of Moree, Perucca and Sgobba [40, Theorem 1 and Lemma 5] has the same coefficients $D_C(t)$. Under GRH their error for an arbitrary set $S \subseteq \mathbb{N}$ in the unnormalized count is $O_{K,F,\Gamma}(X/(\log X)^{2-1/(r+1)})$. The implied constant is independent of S and C. Write $P_{X,C}(S) = \sum_{t\in S} P_{X,C}(t)$ and $D_C(S) = \sum_{t\in S} D_C(t)$. The prime ideal theorem in their (2) gives $\pi_K(X) = X/\log X + O_K(X/\log^2 X)$. Dividing the count by $\pi_K(X)$ gives

$$P_{X,C}(S) - D_C(S) = \left(\frac{X}{\pi_K(X)\log X} - 1\right) D_C(S) + O_{K,F,\Gamma}\big((\log X)^{-r/(r+1)}\big).$$

The first term is $O_K(1/\log X)$ since $0 \le D_C(S) \le 1$. To pass to the full sum of absolute errors, put $a_t = P_{X,C}(t) - D_C(t)$ and take $S_+ = \{t : a_t > 0\}$ and $S_- = \{t : a_t < 0\}$. Then

$$\sum_t |a_t| = \big(P_{X,C}(S_+) - D_C(S_+)\big) + \big(D_C(S_-) - P_{X,C}(S_-)\big).$$

The same bound applies to each term, even though these sets depend on X, and an empty set contributes zero. This yields the unweighted total variation bound $O((\log X)^{-r/(r+1)})$.

Estimate over a number field under GRH	Rank	Normalized discrepancy
Moree–Perucca–Sgobba, Thm. 1	$r \ge 1$	Unweighted, $O((\log X)^{-r/(r+1)})$ for torsion-free groups.
Theorem 1.1	$r \ge 2$	Weighted by t^σ, with a power saving for $0 \le \sigma < (r-1)/(r+2)$, also with torsion.

Both bounds are uniform over the Frobenius filter in a fixed extension. At rank one the balance in our proof gives zero saving even at zero weight.

Weighted sums and averages over generators. For a function $\Phi : \mathbb{N} \to \mathbb{C}$, its Möbius transform is the Dirichlet convolution $\Delta_\Phi(n) = \sum_{d\mid n} \mu(d)\Phi(n/d)$. Write $\tau_k(n)$ for the number of ordered k-tuples of positive integers with product n, put $\tau = \tau_2$ [6, Ch. 2]. For a fixed rational integer base, the GRH theorem of Felix and Murty [27, Theorem 1.7] assumes $|\Delta_\Phi(n)| \ll \tau_k(n)^R (\log n)^\alpha$ for fixed positive integers k, R and $0 \le \alpha < 1$, for $n \ge 2$. In Sgobba's unconditional theorem for a group over a number field [41, (3), Theorem 8 and (8)], a sufficient condition is $\sum_{n>z} |\Delta_\Phi(n)|/\varphi(n) \ll z^{-\eta}$ for some $0 < \eta \le 2$. For $\Phi = \mathbf{1}_{\{1\}}$, $\Delta_\Phi = \mu$ and the latter series diverges on primes. For $\Phi(t) = t^s$, $s > 0$, one has $\Delta_\Phi(p) = p^s - 1$. The first criterion would require $p^s - 1 \ll (\log p)^\alpha$, and the prime subseries $\sum_p (p^s-1)/(p-1)$ in the second diverges.

Goldfeld and Stephens obtained early average results for primitive roots [42, 43]. In Ambrose's theorem on prime ideals the generators vary over tuples in each residue field [44]. Akbary and Felix average functions of the index over bases and primes [45, Theorem 1.4]. Menici and Pehlivan average prescribed-index counts over rational groups [46, Theorem 1]. Kurlberg and Pomerance treat the mean order of one rational base, and Pehlivan studies powers of the order for a higher-rank group [47, 48]. A power of the order is $(q_\mathfrak{p} - 1)^s I_\mathfrak{p}^{-s}$. Pehlivan also bounds the number of rational primes with $I_p^{\mathbb{Q}} \ge L$ by $O_\Gamma(\pi(X)L^{-r})$, for $1 \le L \le \log X$ under GRH [48, Theorem 9 of the preprint version].

Splitting type and effective estimates. At inert primes of real quadratic fields, Ishikawa and Kitaoka and Chen, Kitaoka and Yu studied the image of the unit group [49, 50]. A fundamental unit generates the units of a real quadratic field modulo $\{1, -1\}$ [2, Ch. 5]. If this unit has norm one and p is inert, its residual index at the prime ideal above p is divisible by $p-1$ [50, p. 167]. Roskam, Cohen and Kimmel studied multiplicative orders at rational primes of specified splitting type [51–53]. Section 4 uses restrictions of this kind to count the contribution of higher-degree prime ideals to positive moments.

The Kummer degree estimate used in Section 2.1 is due to Perucca and Sgobba [54, Theorem 1.1]. An effective Chebotarev estimate bounds the error in counting primes by Frobenius class. Lagarias and Odlyzko reduce the count to cyclic subgroups and express a weighted prime-power sum in terms of zeros of L-functions [8]. For the cyclotomic–Kummer fields, Sgobba gives the required discriminant bound and an effective estimate for a single divisibility level under GRH [55, Proposition 9 and Lemma 24, (34) in arXiv v2]. The small-reduction estimate follows the arguments of Matthews, Gupta and Murty, and Narkiewicz [17, 56, 57]. See also Graves for multiplicative monoids of algebraic integers (sets containing one and closed under multiplication) [58, Theorem 5 of the preprint version] and Cohen for algebraic numbers [52, Lemma 1.7 of the preprint version].

Proof strategy. The proof of Theorem 1.1 in Section 3 cuts off the whole divisibility level $n = tv$ in (3) and sums absolute errors with weight t^σ. This gives three contributions. Below the cutoff, Lemma 2.1 gives a Chebotarev estimate uniform in n. Above it, grouping the omitted divisors by prime lets Lemma 2.2 bound their combined empirical contribution through the full residual index. The degree bound (14) controls the remaining tail of the algebraic coefficients. Balancing the first two errors selects the cutoff X^u, at which the third error is strictly smaller. Dividing by $\pi_K(X)$ gives Theorem 1.1. The Jordan divisor identity then identifies the model moment, and the weighted estimate gives Corollary 1.2. Section 2 establishes the three inputs.

In the rational prescribed-index proof of Pappalardi and Susa [19, §5, p. 326], cutting off prime divisors at y leaves $2^{\pi(y)}$ divisors of their product. At index one the model-tail majorant has size $\mathrm{Li}(X)y^{-r}$. For this majorant to yield a relative saving X^{-c} with $c > 0$, one needs $y \gg X^{c/r}$. Then $\log(2^{\pi(y)}) = \pi(y)\log 2 \gg y/\log y$, so summing a separate error bound of size $X^{\theta+\varepsilon}$ for every such divisor exceeds the target error.

Moree, Perucca and Sgobba [40, Lemma 5] use terms of sizes $X/(y^r \log X)$ and $Xy/\log^2 X$. Equating them gives $y^{r+1} = \log X$. At $y = (\log X)^{1/(r+1)}$, each term has size $X/(\log X)^{1+r/(r+1)}$. Dividing by $X/\log X$ gives the logarithmic saving in the table.

Felix [23, §2.4 and pp. 53–54] groups divisor contributions at primes with large index and uses a cutoff by divisor size in rational-base problems. One balance in his logarithmic-moment argument equates $\theta + u$ and $(1-u)(r+1)/r$. In Section 3 this balance gives a power saving for the sum of all absolute discrepancies weighted by a positive power of the index, for a fixed group over K and uniformly in the filter.

Section 4 proves the higher-degree bounds and their classwise and norm-one refinements, evaluates the two Gaussian examples, and extends the subfield growth mechanism beyond Galois extensions. Section 5 gives the rank criteria, their conditional illustrations, and the endpoint and rank-one limitations. Section 6 summarizes the results, their relation to earlier work, and the remaining questions.

Notation used across sections.

$I_{\mathfrak{p}},\ \mathcal{I}_{\mathfrak{P}}$	Residual index at a good prime and inertia subgroup for a chosen prime above $\mathfrak{P}$, respectively.
$K_n,\ E_n,\ F \cap K_n$	Division field, compositum FK_n, and intersection of the two defining fields.
$\mathfrak{d}_{L/K_n},\ d_L$	For an extension L/K_n, its relative discriminant ideal and the absolute value of the discriminant of $L/\mathbb{Q}$.
$\mu_n,\ \mu(n)$	Group of n-th roots of unity and value of the arithmetic Möbius function.
$A_n(X),\ \pi_U(Y)$	Counts of filtered prime ideals of norm at most X with $n \mid I_{\mathfrak{p}}$, and of good unramified rational primes up to Y in class U.

2 Divisibility, field degrees, and small reduction groups

We first prove the splitting criterion and the convergence, nonnegativity and total mass of D_C. We then establish the uniform divisibility count of Lemma 2.1 under $\mathcal{Z}(\theta)$ and the unconditional bound of Lemma 2.2 for large residual indices.

2.1 Splitting conditions and the algebraic measure

For a fixed filter C and $n \geq 1$, let

$$A_n(X) = \#\{\mathfrak{p} \in \mathcal{P}_C(X) : n \mid I_{\mathfrak{p}}\}.$$

As in B_n, the dependence of $A_n(X)$ on C is implicit. We first identify the limit of $A_n(X)/\pi_K(X)$ at each fixed n by expressing the divisibility condition as complete splitting. The degree estimates then give absolute convergence of the Möbius series defining D_C. A finite sieve establishes its nonnegativity, and Möbius inversion recovers its divisibility densities and total mass. These steps construct the algebraic model without a zero hypothesis.

Division fields and restriction of automorphisms. For each fixed generator γ_j of Γ, choose β_j in the fixed algebraic closure with $\beta_j^n = \gamma_j$. If $\gamma = \prod_j \gamma_j^{e_j}$, with $e_j \in \mathbb{Z}$, then every n-th root of γ has the form $\xi \prod_j \beta_j^{e_j}$, $\xi \in \mu_n$. Thus $K_n = K(\mu_n, \beta_1, \ldots, \beta_{m_\Gamma})$ is the common splitting field of $Z^n - 1$ and $Z^n - \gamma_j$ for $1 \leq j \leq m_\Gamma$. These polynomials are separable in characteristic zero, so K_n/K is finite Galois. Hence E_n/K is finite Galois as well.

Put $G_n = \mathrm{Gal}(K_n/K)$. Since F and K_n are Galois over K, so is their intersection $F \cap K_n$. Restriction gives

$$\mathrm{Gal}(E_n/K) \ \simeq\ \{(a, b) \in G_F \times G_n : a|_{F\cap K_n} = b|_{F\cap K_n}\}. \tag{10}$$

Indeed, F and K_n generate E_n, so the map is injective, and both restrictions agree on their intersection. The image of H_n in G_F has fixed field $F \cap E_n^{H_n} = F \cap K_n$. The correspondence between subgroups and fixed fields [5, Ch. 3] identifies this image with $\mathrm{Gal}(F/(F \cap K_n))$. Given a compatible pair (a, b), the extension theorem for field embeddings extends b from K_n to a K-embedding of E_n into the algebraic closure. Normality of E_n/K makes this embedding an automorphism $\widetilde{b}$ of E_n [5, Ch. 2]. Then $a(\widetilde{b}|_F)^{-1}$ fixes $F \cap K_n$. Choose $h \in H_n$ with this restriction to F. The element $h\widetilde{b}$ induces the prescribed pair, proving (10).

Taking $b = 1$ in (10) shows that restriction to F gives an isomorphism $H_n \to \mathrm{Gal}(F/(F\cap K_n))$. Since E_n/K_n is Galois, taking orders and applying the tower formula gives

$$[E_n : K_n] = |H_n| = [F : F \cap K_n], \qquad [E_n : K] = [E_n : K_n][K_n : K].$$

The same restriction maps B_n bijectively onto the set $C \cap \mathrm{Gal}(F/(F \cap K_n))$, hence

$$|B_n| = |C \cap \mathrm{Gal}(F/(F \cap K_n))|.$$

Substituting these identities and $k_n = [K_n : K]$ into $b_C(n) = |B_n|/[E_n : K]$ from (3) gives

$$H_n \simeq \mathrm{Gal}(F/(F \cap K_n)), \qquad [E_n : K] = k_n[F : F \cap K_n],$$
$$b_C(n) = \frac{|C \cap \mathrm{Gal}(F/(F \cap K_n))|}{k_n[F : F \cap K_n]}. \tag{11}$$

Here $\mathrm{Gal}(F/(F \cap K_n))$ is viewed as a subgroup of G_F. For $h \in B_n$ and $\eta \in \mathrm{Gal}(E_n/K)$, the restriction of $\eta h \eta^{-1}$ to K_n is trivial. Its restriction to F is conjugate in G_F to $h|_F$, hence lies in C. This proves conjugacy invariance in the full group, as required for the density calculation.

The splitting criterion. Let $\mathfrak{p}$ be a good prime over p and put $q = q_\mathfrak{p} = p^{\deg(\mathfrak{p})}$. If $p \mid n$, then $p \nmid q - 1$, so $n \nmid I_\mathfrak{p}$ by (1). For $p \nmid n$, cyclicity of $k_\mathfrak{p}^\times$ [5, proof of Prop. 4.19] gives

$$n \mid I_\mathfrak{p} \quad \Longleftrightarrow \quad n \mid q - 1 \ \text{ and } \ \mathrm{red}_\mathfrak{p}(\gamma_j) \in (k_\mathfrak{p}^\times)^n \quad (1 \le j \le m_\Gamma).$$

These conditions say precisely that $Z^n - 1$ and all $Z^n - \mathrm{red}_\mathfrak{p}(\gamma_j)$ split over $k_\mathfrak{p}$. Since $p \nmid n$ and the generators are units at $\mathfrak{p}$, all these reductions are separable. At a prime of K_n above $\mathfrak{p}$, distinct roots of each polynomial have distinct residues. Inertia fixes those residues and therefore each root, so K_n/K is unramified there. Frobenius fixes a root exactly when its residue lies in $k_\mathfrak{p}$. As the roots generate K_n, this proves

$$n \mid I_\mathfrak{p} \quad \Longleftrightarrow \quad \mathfrak{p} \text{ splits completely in } K_n/K \qquad (\mathfrak{p} \text{ admissible}, \ p \nmid n). \tag{12}$$

An admissible $\mathfrak{p}$ with $p \nmid n$ is also unramified in E_n/K. Its inertia fixes both F and K_n, hence their compositum. Its Frobenius restricts to the Frobenius on each of these two fields by the common q-power action. Therefore such a prime satisfies the splitting condition and the filter precisely when its Frobenius class in E_n/K is contained in B_n. For fixed n, the bad primes, the primes ramified in F/K, and those over rational prime divisors of n form a finite set. Apply the fixed-field Chebotarev density theorem [8, §1, (1.1)] to each conjugacy class in B_n, and to K/K for the denominator. It gives

$$\lim_{X \to \infty} \frac{A_n(X)}{\pi_K(X)} = b_C(n), \qquad 0 \le b_C(n) \le \frac{|H_n|}{[E_n : K]} = \frac{1}{k_n}. \tag{13}$$

These assertions include $B_n = \varnothing$. The use of Chebotarev here is at a fixed level.

Degree and absolute convergence. By the structure theorem for finitely generated abelian groups, fix, independently of n, r lifts $g_1, \dots, g_r \in \Gamma$ of a basis of the free abelian group $\Gamma/\Gamma_{\mathrm{tor}}$. They generate a torsion-free group Γ_0 of rank r, and $\Gamma = \Gamma_{\mathrm{tor}} \times \Gamma_0$.

To bound $[K_n : K]$, we use the Kummer degree theorem of Perucca and Sgobba [54, Theorem 1.1]. Their theorem states that for any number field P and any finitely generated torsion-free subgroup $\Lambda \subset P^\times$ of rank $a > 0$, there is an integer $c(P, \Lambda) \ge 1$ such that for every $n \ge 1$

$$\frac{n^a}{[P(\mu_n, \Lambda^{1/n}) : P(\mu_n)]} \quad \text{is an integer dividing } c(P, \Lambda).$$

Applying this with $(P, \Lambda) = (K, \Gamma_0)$ and using $\Gamma_0 \subset \Gamma$ gives

$$[K_n : K(\mu_n)] \ge [K(\mu_n, \Gamma_0^{1/n}) : K(\mu_n)] \ge \frac{n^r}{c(K, \Gamma_0)}.$$

This also holds when n and $|\Gamma_{\mathrm{tor}}|$ have a common factor. Moreover,

$$[K(\mu_n) : K] = [\mathbb{Q}(\mu_n) : K \cap \mathbb{Q}(\mu_n)] = \frac{\varphi(n)}{[K \cap \mathbb{Q}(\mu_n) : \mathbb{Q}]} \ge \frac{\varphi(n)}{[K : \mathbb{Q}]}.$$

By the tower formula, $k_n = [K_n : K(\mu_n)][K(\mu_n) : K]$. Combining the two degree bounds above with (13) therefore gives, with $c_1 = [K : \mathbb{Q}]c(K, \Gamma_0)$,

$$k_n \geq \frac{\varphi(n)n^r}{c_1}, \qquad 0 \leq b_C(n) \leq \frac{c_1}{\varphi(n)n^r}. \tag{14}$$

This fixed choice of Γ_0 makes this constant independent of n, F, C.

The standard divisor estimate and Euler's product formula [6, Theorems 13.12 and 2.4] give, for every $\lambda > 0$,

$$\tau(n) \ll_\lambda n^\lambda, \qquad \frac{n}{\varphi(n)} = \prod_{\ell \mid n}(1 - \ell^{-1})^{-1} \leq \tau(n). \tag{15}$$

Fix $0 \leq s < r$ and choose $0 < 2\lambda < r - s$. All terms in the following regrouping are nonnegative. For $n = tv$ the sum contains at most $\tau(n)$ terms, each with $t^s|\mu(v)| \leq n^s$. Using (14) and then (15) gives

$$\begin{aligned}\sum_{t,v\geq 1} t^s|\mu(v)|b_C(tv) &= \sum_{n\geq 1} b_C(n) \sum_{t\mid n} t^s|\mu(n/t)| \\ &\leq c_1 \sum_{n\geq 1} n^{-1-r+s}\tau(n)\frac{n}{\varphi(n)} \ll_{K,\Gamma,\lambda} \sum_{n\geq 1} n^{-1-r+s+2\lambda} < \infty. \end{aligned} \tag{16}$$

The last series converges because $r - s - 2\lambda > 0$. Thus, for each t, the series defining $D_C(t)$ in (3) converges absolutely. The triangle inequality then gives

$$\sum_{t\geq 1} t^s|D_C(t)| \leq \sum_{t,v\geq 1} t^s|\mu(v)|b_C(tv) < \infty.$$

This absolute convergence also justifies the subsequent rearrangements.

Nonnegativity and total mass. For $t \geq 1$ and $z \geq 2$, put

$$Q_z = \prod_{\substack{\ell \leq z \\ \ell \text{ prime}}} \ell.$$

For a condition A, write $\mathbf{1}_A = 1$ if A holds and $\mathbf{1}_A = 0$ otherwise. For every positive integer I,

$$\mathbf{1}_{t\mid I} \prod_{\ell \mid Q_z} (1 - \mathbf{1}_{t\ell\mid I}) = \sum_{v\mid Q_z} \mu(v)\mathbf{1}_{tv\mid I}. \tag{17}$$

If $t \nmid I$, both sides vanish. For $I = tm$, both sides equal $\mathbf{1}_{\gcd(m,Q_z)=1}$ by finite inclusion–exclusion.

Sum (17) over $\mathfrak{p} \in \mathcal{P}_C(X)$ with $I = I_\mathfrak{p}$, and divide by $\pi_K(X)$. Taking $X \to \infty$ for fixed z, t gives the finite sum $\sum_{v\mid Q_z} \mu(v)b_C(tv)$ by (13). It is nonnegative since the left-hand side counts a set. A squarefree v omitted from this sum has a prime divisor greater than z, hence $v > z$. Nonsquarefree v have $\mu(v) = 0$. Therefore

$$\left| D_C(t) - \sum_{v\mid Q_z} \mu(v)b_C(tv) \right| \leq \sum_{v>z} |\mu(v)|b_C(tv) \longrightarrow 0 \qquad (z \to \infty)$$

by (16). Thus $D_C(t)$ is a limit of nonnegative numbers. This argument takes $X \to \infty$ at a fixed sieve cutoff before passing to the limit in the algebraic series.

The measure recovers each divisibility density. Fix $n \geq 1$. The subseries of (16) with $s = 0$ and $n \mid t$ justifies the rearrangement

$$\sum_{j\geq 1} D_C(nj) = \sum_{j,v\geq 1} \mu(v)b_C(njv) = \sum_{m\geq 1} b_C(nm) \sum_{v\mid m} \mu(v) = b_C(n).$$

In particular, taking $n = 1$ gives

$$\sum_{t\geq 1} D_C(t) = \sum_{n\geq 1} b_C(n) \sum_{v|n} \mu(v) = b_C(1) = \frac{|C|}{|G_F|}. \tag{18}$$

The last equality uses $K_1 = K,\ E_1 = F,\ H_1 = G_F,\ B_1 = C$. The total mass lies in $[0, 1]$ and is one when $C = G_F$.

The degree estimate (14) will also control the weighted tail of the model coefficients beyond a growing cutoff in Section 3, giving (39). The density arguments above use Chebotarev only at fixed levels. For a quantitative comparison with the empirical measures, the next lemma supplies an error estimate uniform over the levels that grow with X.

2.2 A uniform estimate at a single level

The fixed-level density in (13) must now be made quantitative for levels that grow with X. We need one bound for $A_n(X) - b_C(n)\pi_K(X)$, uniform both in the level and in the Frobenius filter. Under GRH, Sgobba's cyclotomic–Kummer count has an error $O_{F,\Gamma_0}(\sqrt{X}\log(m_{\mathrm{cyc}}X))$ at cyclotomic level m_{cyc} for a fixed torsion-free group Γ_0 and a Frobenius filter [55, Lemma 24, (34) in arXiv v2], using Serre's effective Chebotarev theorem [59, §2.4, Theorem 4, formula (14R) and Remark 1]. Cojocaru gives a related estimate under a zero bound for a Galois extension of $\mathbb{Q}$ [60, Lemma 3(2)].

Here we need the common zero bound $\mathcal{Z}(\theta)$ over a general base field, including groups with torsion. To preserve uniformity as the fields vary with n, the proof retains their degrees and discriminants in the explicit formula until the count is descended to K. This yields the single error constant for $1 \leq n \leq X$ used below.

Lemma 2.1 (Divisibility counts)**.** *Assume $\mathcal{Z}(\theta)$, where $1/2 \leq \theta < 1$. For every $\lambda > 0$, uniformly in $1 \leq n \leq X$ and in C,*

$$A_n(X) = b_C(n)\pi_K(X) + O_{K,F,\Gamma,\theta,\lambda}(X^{\theta+\lambda}). \tag{19}$$

The same estimate holds with $\mathrm{Li}(X)$ *in place of* $\pi_K(X)$.

Proof. Fix n for the moment. Put $L = E_n$, $H = H_n = \mathrm{Gal}(L/K_n)$ and $h = |H|$. For any number field M, write $n_M = [M : \mathbb{Q}]$ and let d_M be the absolute value of its discriminant over $\mathbb{Q}$. The root discriminant of M is d_M^{1/n_M}. We first bound $\log d_L/n_L$, since this controls the dependence on the varying fields in the error after descent to K. An element of H fixing F fixes both fields generating $L = FK_n$. Restriction is therefore injective on H, and

$$h \leq [F : K], \qquad n_{K_n} = k_n[K : \mathbb{Q}], \qquad n_L = hk_n[K : \mathbb{Q}]. \tag{20}$$

The set B_n is a union of at most h conjugacy classes of H.

Let $w = |\Gamma_{\mathrm{tor}}|$. Since $\Gamma_{\mathrm{tor}} = \mu_w$, its n-th roots form μ_{wn}. Thus $L = F(\mu_{wn}, \Gamma_0^{1/n})$, also when $(w, n) > 1$. To bound $\log d_L/n_L$, we use Sgobba's discriminant estimate [55, Proposition 9]. Let P be any number field, let $\Lambda \subset P^\times$ be fixed, finitely generated and torsion-free of rank $a > 0$, and let $m, n \geq 1$ with $n \mid m$. Write $W = P(\mu_m, \Lambda^{1/n})$ and let s_Λ be the product of the rational primes below the prime ideals of P at which some element of Λ is not a local unit, with empty product one. The estimate is

$$\frac{\log d_W}{[W : \mathbb{Q}]} \leq \log(\varphi(m)mn^a) + \log(s_\Lambda d_P).$$

Take $P = F, \Lambda = \Gamma_0, m = wn$, so $W = L$. Writing $S_0 = s_\Lambda$ for this choice gives

$$\begin{aligned}\frac{\log d_L}{n_L} &\le \log\left(\varphi(wn)wn\, n^r\right) + \log(S_0 d_F)\\ &\le (r+2)\log n + 2\log w + \log(S_0 d_F),\\ \frac{\log d_L + n_L}{k_n} &= h[K:\mathbb{Q}]\left(1 + \frac{\log d_L}{n_L}\right) \ll_{K,F,\Gamma} \log(2n). \end{aligned} \tag{21}$$

The last estimate includes $n = 1$ and $d_L = 1$.

We next use the explicit formula to estimate sums over powers of prime ideals of K_n selected by a Frobenius class. For a nonzero integral ideal $\mathfrak{a}$ in any number field M, write $\mathrm{N}\mathfrak{a} = |\mathcal{O}_M/\mathfrak{a}|$ for its absolute norm. In particular $\mathrm{N}\mathfrak{p} = q_\mathfrak{p}$ for primes of K. For a conjugacy class U of H, choose $g \in U$ and put $a = |U|/h$. We write $\mathbf{1}_U(x) = \mathbf{1}_{x\in U}$ for its indicator function. Let $H_g = \langle g\rangle$, $h_g = |H_g|$, and let $P_g = L^{H_g}$ be the fixed field of H_g. For $y \ge 2$, write $\psi_U(y)$ for the sum of $\log \mathrm{N}\mathfrak{P}$ over $\mathfrak{P}^j$ with $(\mathrm{N}\mathfrak{P})^j \le y$, where $\mathfrak{P}$ is a prime of K_n unramified in L, $j \ge 1$, and the j-th power of any representative of its Frobenius class belongs to U. For $\chi \in \widehat{H}_g = \mathrm{Hom}(H_g, \mathbb{C}^\times)$, use the primitive Hecke L-function $L(z,\chi)$ over P_g attached by abelian reciprocity, with finite conductor ideal $\mathfrak{f}_\chi$ and arithmetic Frobenius convention [7, Ch. V, §3 and Ch. VIII, §10, pp. 261–263]. Let $\rho_\chi = \beta_\chi + i\gamma_\chi$ run over its zeros in the open critical strip, with multiplicity. For $v \in H_g$, orthogonality of the characters of the cyclic group H_g gives

$$\sum_\chi \overline{\chi(g)}\chi(v) = \sum_\chi \chi(g^{-1}v) = h_g \mathbf{1}_{\{g\}}(v).$$

Let $Z_H(g) = \{b \in H : bg = gb\}$ be the centralizer of g, and write $\mathrm{Ind}_{H_g}^H$ for induction of class functions from H_g to H. Inducing $h_g\mathbf{1}_{\{g\}}$ gives, at $x \in H$,

$$\mathrm{Ind}_{H_g}^H(h_g\mathbf{1}_{\{g\}})(x) = \frac{1}{h_g}\sum_{b\in H} h_g \mathbf{1}_{\{g\}}(b^{-1}xb) = |Z_H(g)|\mathbf{1}_U(x).$$

Indeed, the solutions of $b^{-1}xb = g$ form the coset $b_0 Z_H(g)$ if $x \in U$, for any one solution b_0, and the solution set is empty otherwise. Orbit–stabilizer gives $a = |U|/h = 1/|Z_H(g)|$. Combining the preceding two identities yields the class function used in the prime-power sum,

$$\mathbf{1}_U = a \sum_{\chi\in\widehat{H}_g} \overline{\chi(g)}\,\mathrm{Ind}_{H_g}^H \chi.$$

For a finite-dimensional complex representation ϱ of H on V, the Artin L-function has Euler factors $\det(1 - q^{-z}\varrho(\phi) \mid V^{\mathcal{I}})^{-1}$. Here q is the norm of a prime of K_n, $\mathcal{I}$ is its inertia group in L/K_n for a chosen prime above it, ϕ lifts its arithmetic Frobenius, and $V^{\mathcal{I}}$ is the subspace fixed by $\mathcal{I}$. The induction identity for Artin L-functions identifies the function over K_n of $\mathrm{Ind}_{H_g}^H \chi$ with the one over P_g of χ. Thus the displayed linear combination applies to their logarithmic derivatives. The trivial character alone supplies the pole at one and has coefficient a, giving the term ay in the explicit formula [8, Lemma 4.1, (4.1)–(4.2) and Theorem 7.1].

This reduction lets us apply the explicit formula of Lagarias and Odlyzko [8, Theorem 7.1, (7.4)–(7.5)], with their base field, extension field and cyclic fixed field equal to K_n, L, P_g, respectively. For real $y, T \ge 2$, define the zero sum and remainder bound by

$$S_U(y,T) = a\sum_\chi \overline{\chi(g)}\left(\sum_{|\gamma_\chi|<T}\frac{y^{\rho_\chi}}{\rho_\chi} - \sum_{|\rho_\chi|<1/2}\frac{1}{\rho_\chi}\right), \tag{22}$$

$$\begin{aligned}R_U(y,T) = a\left[\left(1 + \frac{y\log y}{T}\right)\log d_L + n_L\log y + \frac{n_L y\log y\log T}{T}\right]\\ + (\log d_L)\log y + \frac{n_{K_n} y(\log y)^2}{T}.\end{aligned} \tag{23}$$

Then $|\psi_U(y) - ay + S_U(y,T)| \ll R_U(y,T)$ with an absolute constant, including when T is an ordinate of a zero. The intermediate term $n_{K_n} \log y$ in their (3.18) is covered even for $L = \mathbb{Q}$, since $an_L = |U| n_{K_n} \geq n_{K_n}$.

We check the contribution from ramified primes to (23) to keep its dependence on n explicit. For a prime $\mathfrak{P}$ of K_n, choose a prime of L above it, let $\mathcal{I}_{\mathfrak{P}}$ be its inertia group in L/K_n, the subgroup acting trivially on the residue field. Let $\phi_{\mathfrak{P}}$ be a lift of the residue-field Frobenius to its decomposition group. At a ramified prime the power map specifies an element of the quotient by inertia. Hence the coset $\phi_{\mathfrak{P}}^j \mathcal{I}_{\mathfrak{P}}$ is independent of the chosen lift for every $j \geq 1$. The coefficient of $\log \mathrm{N}\mathfrak{P}$ at $\mathfrak{P}^j$ in the logarithmic-derivative sum for the class U is

$$c_U(\mathfrak{P}, j) = \frac{1}{|\mathcal{I}_{\mathfrak{P}}|} \sum_{\eta \in \mathcal{I}_{\mathfrak{P}}} \mathbf{1}_U(\phi_{\mathfrak{P}}^j \eta), \qquad 0 \leq c_U(\mathfrak{P}, j) \leq 1.$$

For an eigenvalue ξ of $\varrho(\phi_{\mathfrak{P}})$ on the inertia invariants, the negative logarithmic derivative of $(1 - \xi q^{-z})^{-1}$ is $(\log q) \sum_{k \geq 1} \xi^k q^{-kz}$ for $\Re z > 1$, with $q = \mathrm{N}\mathfrak{P}$. Summing over the eigenvalues with multiplicity replaces ξ^k by the trace of the k-th power on the invariants. The average $|\mathcal{I}_{\mathfrak{P}}|^{-1} \sum_{\eta \in \mathcal{I}_{\mathfrak{P}}} \varrho(\eta)$ projects onto the subspace fixed by every element of inertia. Multiplying by $\varrho(\phi_{\mathfrak{P}}^j)$ and taking the trace gives the displayed average for the character of ϱ. The characters of irreducible representations (those with no proper nonzero invariant subspace) form a basis of the class functions on H. Expanding $\mathbf{1}_U$ in this basis gives the formula for c_U. At an unramified prime it reduces to $\mathbf{1}_U(\phi_{\mathfrak{P}}^j)$.

Write $\mathfrak{d}_{L/K_n}$ for the relative discriminant ideal, using the same convention for the other extensions below. The absolute change on deleting the ramified prime powers to obtain $\psi_U(y)$ is at most

$$\begin{aligned} \sum_{\mathfrak{P} \mid \mathfrak{d}_{L/K_n}} \log \mathrm{N}\mathfrak{P} \left\lfloor \frac{\log y}{\log \mathrm{N}\mathfrak{P}} \right\rfloor &\leq \#\{\mathfrak{P} : \mathfrak{P} \mid \mathfrak{d}_{L/K_n}\} \log y \\ &\leq \frac{\log \mathrm{N}\mathfrak{d}_{L/K_n}}{\log 2} \log y \leq \frac{\log d_L}{\log 2} \log y. \end{aligned}$$

The last line uses $\mathrm{N}\mathfrak{P} \geq 2$ and $d_L = d_{K_n}^{[L:K_n]} \mathrm{N}\mathfrak{d}_{L/K_n}$. This accounts for the $(\log d_L) \log y$ term already included outside a in (23), with a constant independent of n and U [8, (3.6), (3.18)].

To use $\mathcal{Z}(\theta)$ in (22), we relate the Hecke zeros to the zeros of ζ_L. This requires the primitive Euler factors, including those at ramified primes. For a prime $\mathfrak{q}$ of P_g, write $q_{\mathfrak{q}} = \mathrm{N}\mathfrak{q}$. In the abelian extension L/P_g let $\mathcal{I}_{\mathfrak{q}}$ be the inertia group at a prime of L above it, $e = |\mathcal{I}_{\mathfrak{q}}|$, and let ϕ lift its arithmetic Frobenius. The relative residue degree f at $\mathfrak{q}$ is the order of $\phi \mathcal{I}_{\mathfrak{q}}$ in $H_g/\mathcal{I}_{\mathfrak{q}}$. On the one-dimensional space of χ, the inertia invariants have dimension one when $\chi|_{\mathcal{I}_{\mathfrak{q}}} = 1$ and zero otherwise. Thus its primitive local factor is

$$L_{\mathfrak{q}}(z, \chi) = \begin{cases} (1 - \chi(\phi) q_{\mathfrak{q}}^{-z})^{-1}, & \chi|_{\mathcal{I}_{\mathfrak{q}}} = 1, \\ 1, & \chi|_{\mathcal{I}_{\mathfrak{q}}} \neq 1. \end{cases}$$

The characters trivial on $\mathcal{I}_{\mathfrak{q}}$ are those of the cyclic group $H_g/\mathcal{I}_{\mathfrak{q}}$ of order h_g/e. A character sending a generator of this quotient to a primitive (h_g/e)-th root sends $\phi \mathcal{I}_{\mathfrak{q}}$, which has order f, to a primitive f-th root. Its successive powers give all characters, so evaluation takes each f-th root of unity exactly $(h_g/e)/f$ times. Using $\prod_{\xi^f = 1} (1 - \xi u) = 1 - u^f$, one obtains

$$\prod_{\chi} L_{\mathfrak{q}}(z, \chi) = \prod_{\xi^f = 1} (1 - \xi q_{\mathfrak{q}}^{-z})^{-h_g/(ef)} = (1 - q_{\mathfrak{q}}^{-fz})^{-h_g/(ef)}.$$

This is the factor of ζ_L from the $h_g/(ef)$ primes over $\mathfrak{q}$, each of norm $q_{\mathfrak{q}}^f$. Omitting a finite set of Euler factors from a primitive $L(z, \chi)$ would multiply it by the corresponding factors $1 - \chi(\phi) q_{\mathfrak{q}}^{-z}$

wherever $\chi|_{\mathcal{I}_\mathfrak{q}} = 1$. These are nonzero for $\Re z > 0$. With the primitive factors used here the exact identity is $\zeta_L(z) = \prod_\chi L(z,\chi)$, first for $\Re z > 1$ and then by meromorphic continuation [8, (8.1)]. Let χ_{triv} denote the trivial character. Its factor $L(z,\chi_{\mathrm{triv}}) = \zeta_{P_g}(z)$ has a simple pole at $z = 1$. All factors are holomorphic in the open critical strip. Thus the multiset of the ρ_χ is the multiset of nontrivial zeros of ζ_L. The functional equation of ζ_L sends each such zero ρ_χ to $1 - \overline{\rho_\chi}$. Applying the hypothesis on $L = E_n$ to these two zeros gives $\beta_\chi \le \theta$ and $1 - \beta_\chi \le \theta$. Consequently

$$1 - \theta \le \beta_\chi \le \theta, \qquad |y^{\rho_\chi}| \le y^\theta, \qquad |\rho_\chi| \ge 1 - \theta.$$

To bound the number of zeros, put $A(\chi) = d_{P_g} \mathrm{N}\mathfrak{f}_\chi$. Lagarias and Odlyzko [8, Lemma 5.4, (5.12)] give, for every real v, with an absolute implied constant,

$$\#\{\rho_\chi : |\gamma_\chi - v| \le 1\} \ll \log A(\chi) + n_{P_g} \log(|v| + 2).$$

For the abelian extension L/P_g, the conductor–discriminant formula gives $\mathfrak{d}_{L/P_g} = \prod_\chi \mathfrak{f}_\chi$ [7, Ch. V, Theorem 3.27, p. 165]. There are $h_g = [L : P_g]$ characters. By the discriminant formula in the tower $L/P_g/\mathbb{Q}$,

$$\prod_\chi A(\chi) = d_{P_g}^{h_g} \mathrm{N}\Big(\prod_\chi \mathfrak{f}_\chi\Big) = d_L, \qquad \sum_\chi n_{P_g} = h_g n_{P_g} = n_L.$$

Thus the sum of the terms $\log A(\chi)$ contributes just $\log d_L$ in each band [8, proof of Theorem 7.1]. Summing the preceding bound at $v = 0$ gives $O(\log d_L + n_L)$ zeros with $|\gamma_\chi| < 1$. For $j \ge 1$, using the centers $v = \pm(j + 1/2)$ gives $O(\log d_L + n_L \log(j+3))$ zeros in $j \le |\gamma_\chi| < j + 1$. In the latter band $|\rho_\chi| \ge j$. Consequently,

$$\begin{aligned}\sum_\chi \sum_{|\gamma_\chi| < T} \frac{y^{\beta_\chi}}{|\rho_\chi|} &\ll y^\theta \left(\frac{\log d_L + n_L}{1 - \theta} + \sum_{1 \le j \le T} \frac{\log d_L + n_L \log(j+3)}{j} \right) \\ &\ll_\theta y^\theta \big(\log d_L + n_L \log(3T) \big) \log(3T). \end{aligned} \tag{24}$$

Indeed,

$$\sum_{1 \le j \le T} \frac{\log d_L + n_L \log(j+3)}{j} \le (\log d_L + n_L \log(T+3))(1 + \log T).$$

For the second sum in (22), $|\rho_\chi| < 1/2$ implies $|\gamma_\chi| < 1$, and $|\rho_\chi| \ge 1 - \theta$. Hence

$$\sum_\chi \sum_{|\rho_\chi| < 1/2} \frac{1}{|\rho_\chi|} \le \frac{1}{1-\theta} \sum_\chi \#\{\rho_\chi : |\gamma_\chi| < 1\} \ll \frac{\log d_L + n_L}{1 - \theta}.$$

This includes real zeros. In particular the bound on the Dedekind zeta function of L controls all the Hecke factors used in this proof.

Now set $T = y$. The terms in (23) are bounded by

$$a\big((1+\log y)\log d_L + n_L \log y + n_L (\log y)^2\big) + (\log d_L)\log y + n_{K_n} (\log y)^2 \ll (\log d_L + n_L)\log^2(3y).$$

Since $a \le 1$, $|\chi(g)| = 1$ and $n_{K_n} \le n_L$, this estimate and (24) give

$$\psi_U(y) = ay + O_\theta\Big(y^\theta (\log d_L + n_L) \log^2(3y) \Big) \qquad (y \ge 2). \tag{25}$$

We now remove the higher prime powers from ψ_U, sum over the classes in B_n, and apply partial summation to obtain a prime count. If $j \ge 2$ and $(\mathrm{N}\mathfrak{P})^j \le y$, the rational prime below $\mathfrak{P}$ is at most $\sqrt{y}$. There are at most $n_{K_n}\sqrt{y}$ such prime ideals. The powers of each contribute at most $(\log y / \log \mathrm{N}\mathfrak{P}) \log \mathrm{N}\mathfrak{P} = \log y$. Their total $O(n_{K_n}\sqrt{y}\log y)$ is covered by the error in (25)

since $\theta \geq 1/2$. Let $\vartheta_{B_n}(y)$ denote the log-norm sum over the primes of K_n of norm at most y unramified in L with Frobenius in B_n, and $\Pi_{B_n}(y)$ their count. For the disjoint classes $U \subseteq B_n$, the main coefficients sum to $\sum_{U \subseteq B_n} |U|/h = |B_n|/h$. There are at most $h \leq [F : K]$ such error terms. Hence

$$\vartheta_{B_n}(y) = \frac{|B_n|}{h} y + O_{F,K,\theta}\Big(y^{\theta}(\log d_L + n_L)\log^2(3y)\Big).$$

Partial summation with weight $1/\log y$, including primes of norm two, gives [6, Theorem 4.2]

$$\begin{aligned}\Pi_{B_n}(X) &= \frac{\vartheta_{B_n}(X)}{\log X} + \int_2^X \frac{\vartheta_{B_n}(y)}{y \log^2 y}\, dy \\ &= \frac{|B_n|}{h}\operatorname{Li}(X) + O_{F,K,\theta}\Big(X^{\theta}(\log d_L + n_L)\log^2(3X)\Big). \end{aligned} \tag{26}$$

For the main term, $X/\log X + \int_2^X dy/\log^2 y = \operatorname{Li}(X) + 2/\log 2$. Since $|B_n|/h \leq 1$, the endpoint constant contributes at most $2/\log 2$, absorbed in the displayed error. For the integrated error use $\log(3y)/\log y \ll 1$ for $y \geq 2$ and $\int_2^X y^{\theta-1} dy \leq X^{\theta}/\theta$. In this integration the field is fixed at the chosen level n, including when $y < n$.

It remains to descend the prime count from K_n to K. Each contributing prime of K will be counted k_n times, so the error in (26) is divided by k_n. Write $\omega(n)$ for the number of distinct prime divisors of n. Discard primes of K_n above the exceptional set S_{exc} or above rational primes dividing n. These deletions cost at most $k_n(|S_{\mathrm{exc}}| + [K : \mathbb{Q}]\omega(n))$. The inequality $2^{\omega(n)} \leq n$ also holds at $n = 1$. Outside these exclusions, both K_n/K and F/K are unramified by the splitting argument in Section 2.1, so their compositum is unramified as well. For a prime $\mathfrak{P}$ of K_n over $\mathfrak{p}$, the relative residue degree is $f(\mathfrak{P}/\mathfrak{p}) = [\mathcal{O}_{K_n}/\mathfrak{P} : k_{\mathfrak{p}}]$, so $\mathrm{N}\mathfrak{P} = (\mathrm{N}\mathfrak{p})^{f(\mathfrak{P}/\mathfrak{p})}$. If this degree is at least two, then $\mathrm{N}\mathfrak{P} \geq (\mathrm{N}\mathfrak{p})^2$. The number of all such $\mathfrak{P}$ with norm at most X is consequently bounded by $k_n \pi_K(\sqrt{X}) \leq k_n [K : \mathbb{Q}]\sqrt{X}$ since at most $[K : \mathbb{Q}]$ primes of K lie above each rational prime.

For the remaining primes, relative degree one above $\mathfrak{p}$ is equivalent to complete splitting in the Galois extension K_n/K. There are then exactly k_n primes $\mathfrak{P}$ above $\mathfrak{p}$, all with $\mathrm{N}\mathfrak{P} = \mathrm{N}\mathfrak{p}$. Frobenius at each $\mathfrak{P}$ restricts on F to a representative of the Frobenius class at $\mathfrak{p}$ because the two residue norms coincide. Thus either all k_n pass the filter or none do. The criterion (12) identifies the contributing $\mathfrak{p}$ with those defining $A_n(X)$. If the residue characteristic divides n, then $n \nmid I_{\mathfrak{p}}$ since $I_{\mathfrak{p}} \mid \mathrm{N}\mathfrak{p} - 1$. The relative-degree restriction used in this descent leaves every allowed absolute residue degree of $\mathfrak{p}$ in the count. The three possible exclusions therefore give

$$0 \leq \Pi_{B_n}(X) - k_n A_n(X) \leq k_n\big(|S_{\mathrm{exc}}| + [K : \mathbb{Q}]\omega(n) + \pi_K(\sqrt{X})\big).$$

In particular $0 \leq \Pi_{B_n}(X)/k_n - A_n(X) \leq |S_{\mathrm{exc}}| + [K : \mathbb{Q}]\omega(n) + \pi_K(\sqrt{X})$. The main term from (26) becomes $(|B_n|/h)\operatorname{Li}(X)/k_n = b_C(n)\operatorname{Li}(X)$, since $hk_n = [E_n : K]$. The error from the explicit formula is divided by the same k_n, giving

$$\begin{aligned}|A_n(X) - b_C(n)\operatorname{Li}(X)| \ll_{K,F,\theta} X^{\theta}\log^2(3X)\frac{\log d_L + n_L}{k_n} \\ + |S_{\mathrm{exc}}| + [K : \mathbb{Q}]\omega(n) + \pi_K(\sqrt{X}).\end{aligned}$$

Using (21), $\omega(n) \leq \log n/\log 2$ and $\pi_K(\sqrt{X}) \leq [K : \mathbb{Q}]\sqrt{X}$ yields

$$A_n(X) = b_C(n)\operatorname{Li}(X) + O_{K,F,\Gamma,\theta}\Big(X^{\theta}\log(2n)\log^2(3X)\Big). \tag{27}$$

For $n = 1$ and $C = G_F$ the coefficient is one and $A_1(X)$ differs from $\pi_K(X)$ by at most $|S_{\mathrm{exc}}|$. Hence $\pi_K(X) - \operatorname{Li}(X) \ll_{K,F,\Gamma,\theta} X^{\theta}\log^2(3X)$. Since $0 \leq b_C(n) \leq 1$, (27) also holds with $\pi_K(X)$ as the main-term normalization. Finally, for $1 \leq n \leq X$, $\log(2n)\log^2(3X) \leq \log^3(3X) \ll_{\lambda} X^{\lambda}$.

The following bounds use the same constants for every filter C, including the empty one. In the first two rows the degree and discriminant of the varying field are shown explicitly.

Error in	Explicit scale	Constant depends on
$\psi_U(y)$, (25)	$y^\theta(\log d_L + n_L)\log^2(3y)$	θ
$\Pi_{B_n}(X)$, (26)	$X^\theta(\log d_L + n_L)\log^2(3X)$	$\theta, [F:K]$
$A_n(X)$, (27)	$X^\theta \log(2n)\log^2(3X)$	K, F, Γ, θ

Only the absorption of the logarithms in (19) requires $n \le X$ and introduces dependence on λ. □

Uniformity in the level is what permits the cutoff in Möbius inversion to grow with X. For a cutoff $1 \le Y \le X$, the errors in Lemma 2.1 at levels $n = tv \le Y$ share one constant, so Section 3 can sum them with the divisor weights to obtain (35). This accumulated error increases with Y; its balance with the omitted empirical contribution selects the cutoff in Theorem 1.1. Uniformity in C survives this summation. At $n = 1$, with the full filter, the same lemma also controls $\pi_K(X) - \mathrm{Li}(X)$, which is needed to express the moment asymptotic with $\mathrm{Li}(X)$ in Corollary 1.2.

2.3 Primes with small reduction groups

Lemma 2.1 controls the divisibility levels retained in Möbius inversion. To estimate the empirical contribution from omitted levels, we group all omitted divisors of $I_\mathfrak{p}$ at each prime. Each contributing prime has a large full residual index. For primes of norm at most X, the identity $I_\mathfrak{p} = (\mathrm{N}\mathfrak{p} - 1)/|\Gamma_\mathfrak{p}|$ reduces their count to a bound for small reduction groups. Cohen's estimate does this unconditionally for multiplicatively independent algebraic numbers over a number field [61, Lemma 5.7]. Its preprint formulation [52, Lemma 1.7] uses $|\Gamma_\mathfrak{p}| < y$; taking $y = T + 1 \le 2T$ for $T \ge 1$ gives the weak threshold used below. We include the proof to keep the constant explicit and to check that the count includes prime ideals of every residue degree.

Lemma 2.2 (Small reduction groups)**.** *Let $\Gamma \subset K^\times$ be a finitely generated subgroup of rank $r \ge 1$, and put $\kappa_r = 1 + 1/r$. For real $T \ge 1$, the number of good prime ideals $\mathfrak{p}$ with $|\Gamma_\mathfrak{p}| \le T$ is $O_{K,\Gamma}(T^{\kappa_r})$. Consequently, for $1 \le T_0 \le X$,*

$$\#\{\mathfrak{p} \text{ good} : \mathrm{N}\mathfrak{p} \le X,\ I_\mathfrak{p} > T_0\} \ll_{K,\Gamma} (X/T_0)^{\kappa_r}. \tag{28}$$

Proof. Choose multiplicatively independent elements $g_1, \dots, g_r$ of Γ, for instance the basis of Γ_0 fixed in Section 2.1, and fix expressions $g_j = a_j/b_j$ with nonzero $a_j, b_j \in \mathcal{O}_K$. Let S_{frac} be the finite set of prime ideals dividing the principal ideal $(\prod_{j=1}^r a_j b_j)\mathcal{O}_K$. A prime in S_{frac} can be good if the valuations in a numerator and denominator cancel. The good primes in this set contribute at most $|S_{\mathrm{frac}}|$. We work with the chosen fractions outside S_{frac}.

Fix a good prime $\mathfrak{p} \notin S_{\mathrm{frac}}$ for which $|\Gamma_\mathfrak{p}| \le T$. Put $B = \lceil T^{1/r} \rceil$, so $1 \le B \le T^{1/r} + 1 \le 2T^{1/r}$. To each $e \in \{0, \dots, B\}^r$ assign the residue of $\prod_j g_j^{e_j}$ in $\Gamma_\mathfrak{p}$. The domain has $(B+1)^r > T$ elements and the image at most T. Two distinct vectors therefore have the same image. Their difference is a nonzero $v \in \mathbb{Z}^r$ with $\|v\|_\infty = \max_j |v_j| \le B$, and $\prod_j g_j^{v_j} \equiv 1 \bmod \mathfrak{p}$.

For each $v = (v_1, \dots, v_r) \in \mathbb{Z}^r$, write $v_j^+ = \max(v_j, 0)$ and $v_j^- = \max(-v_j, 0)$. Set

$$U_v = \prod_{j=1}^r a_j^{v_j^+} b_j^{v_j^-}, \qquad W_v = \prod_{j=1}^r b_j^{v_j^+} a_j^{v_j^-}, \qquad h_v = U_v - W_v \in \mathcal{O}_K. \tag{29}$$

Then $U_v/W_v = \prod_j g_j^{v_j}$, so multiplicative independence gives $h_v \ne 0$ for every $v \ne 0$. For the vector produced above, W_v is a unit at $\mathfrak{p} \notin S_{\mathrm{frac}}$, and the congruence implies $h_v \in \mathfrak{p}$. The argument also applies in the presence of torsion, since the products lie in the independent subgroup and its image has at most $|\Gamma_\mathfrak{p}|$ elements.

To bound the norms of these nonzero algebraic integers, put $d = [K : \mathbb{Q}]$ and let $N_{K/\mathbb{Q}}$ denote the field norm on elements. Fix $H_\infty \geq 2$ at least as large as $|\iota(a_j)|$ and $|\iota(b_j)|$ for all j and embeddings $\iota : K \hookrightarrow \mathbb{C}$, independently of T. For $0 < \|v\|_\infty \leq B$, each monomial in (29) has total exponent $\sum_j (v_j^+ + v_j^-) = \sum_j |v_j|$. For every such embedding,

$$\begin{aligned} |\iota(h_v)| \leq |\iota(U_v)| + |\iota(W_v)| \leq 2H_\infty^{\sum_j |v_j|} \leq 2H_\infty^{rB}, \\ \log|N_{K/\mathbb{Q}}(h_v)| = \sum_{\iota : K \hookrightarrow \mathbb{C}} \log|\iota(h_v)| \leq d(\log 2 + rB \log H_\infty). \end{aligned} \tag{30}$$

Here $|N_{K/\mathbb{Q}}(h_v)| = \mathrm{N}(h_v \mathcal{O}_K)$ [2, Ch. 2 and Props. 4.1–4.2].

For $\mathcal{V}_B = \{v \in \mathbb{Z}^r : 0 < \|v\|_\infty \leq B\}$, we have

$$|\mathcal{V}_B| = (2B+1)^r - 1 \leq 3^r B^r.$$

Every counted $\mathfrak{p} \notin S_{\mathrm{frac}}$ divides at least one principal ideal (h_v) with $v \in \mathcal{V}_B$. All these ideals are nonzero. Counting each prime once, ideal factorization and multiplicativity of the norm therefore give, by (30) and $B \geq 1$,

$$\begin{aligned} \sum_{\substack{\mathfrak{p} \notin S_{\mathrm{frac}} \text{ good} \\ |\Gamma_\mathfrak{p}| \leq T}} \log \mathrm{N}\mathfrak{p} \leq \log \mathrm{N}\left(\prod_{v \in \mathcal{V}_B} (h_v) \right) = \sum_{v \in \mathcal{V}_B} \log|N_{K/\mathbb{Q}}(h_v)| \\ \leq 3^r d(\log 2 + r \log H_\infty)\, B^{r+1}. \end{aligned} \tag{31}$$

Dividing by $\log 2$, adding $|S_{\mathrm{frac}}|$, and substituting $B \leq 2T^{1/r}$ shows that a permissible coefficient of $T^{1+1/r}$ is

$$|S_{\mathrm{frac}}| + \frac{2^{r+1} 3^r d\,(\log 2 + r \log H_\infty)}{\log 2}.$$

It depends only on K, Γ and the choices fixed once for them. In particular (31) counts distinct prime ideals separately, also when several lie over the same rational prime or a residue degree exceeds one.

Finally $\mathrm{N}\mathfrak{p} \leq X$ and $I_\mathfrak{p} > T_0$ give

$$|\Gamma_\mathfrak{p}| = \frac{\mathrm{N}\mathfrak{p} - 1}{I_\mathfrak{p}} < \frac{X}{T_0}.$$

Since $T = X/T_0 \geq 1$, the first part bounds the number of all such primes by $O_{K,\Gamma}((X/T_0)^{1+1/r})$, which proves (28). □

For a divisibility cutoff $1 \leq Y \leq X$, applying (28) to dyadic ranges of the full index gives (38): up to an arbitrarily small power loss, the weighted remainder is bounded by $X^{\kappa_r} Y^{\sigma - \kappa_r}$. Since $\sigma < \kappa_r$, this decreases as Y grows and can be balanced against the increasing small-level error. This explains the role of κ_r in the rate and weight range of Theorem 1.1. The estimate counts all good prime ideals unconditionally, so imposing a Frobenius filter preserves its constant.

3 Proof of the distribution and moment estimates

We prove Theorem 1.1 by combining Lemmas 2.1–2.2 with the degree bound for the algebraic coefficients. Balancing the three errors in truncated Möbius inversion determines the cutoff and the power saving. We then deduce Corollary 1.2 and give an example over $\mathbb{Q}$.

3.1 Möbius inversion and the three errors

We truncate Möbius inversion [6, Ch. 2] at the full level $n = tv$, then sum over the exact indices t. The cutoff is chosen before normalization by $\pi_K(X)$.

Proof of Theorem 1.1. Fix X with $\pi_K(X) > 0$. If I, t are positive integers, then

$$\mathbf{1}_{\{I=t\}} = \sum_{tv|I} \mu(v), \qquad \pi_K(X) P_{X,C}(t) = \sum_{v\geq 1} \mu(v) A_{tv}(X). \tag{32}$$

The second identity sums the first over $\mathcal{P}_C(X)$, and its sum is finite since $tv \mid I_{\mathfrak{p}}$ implies $tv \leq I_{\mathfrak{p}} < X$.

The hypotheses imply $r \geq 2$ and $0 \leq \sigma < \sigma_* < 1 < \kappa_r$, hence $\sigma < r$. Thus (16) applies with weight t^σ. Define the nonnegative coefficient

$$w_\sigma(n) = \sum_{t|n} t^\sigma |\mu(n/t)| = n^\sigma \prod_{\ell|n} (1 + \ell^{-\sigma}) \leq n^\sigma \tau(n). \tag{33}$$

The product follows on writing $v = n/t$ and summing $|\mu(v)| v^{-\sigma}$ over $v \mid n$.

For a real cutoff $1 \leq Y \leq X$ and each fixed $t \geq 1$, split $\pi_K(X)(P_{X,C}(t) - D_C(t))$ at $tv = Y$ as

$$\sum_{tv\leq Y} \mu(v)\{A_{tv}(X) - \pi_K(X) b_C(tv)\} + \sum_{tv>Y} \mu(v) A_{tv}(X) - \pi_K(X) \sum_{tv>Y} \mu(v) b_C(tv).$$

Take absolute values, multiply by t^σ, and sum over t. Regrouping the nonnegative terms by $n = tv$ gives the inner sum $w_\sigma(n)$ over $t \mid n$, hence

$$\begin{aligned} \pi_K(X) \sum_{t\geq 1} t^\sigma |P_{X,C}(t) - D_C(t)| \leq \underbrace{\sum_{n\leq Y} w_\sigma(n) |A_n(X) - \pi_K(X) b_C(n)|}_{\mathcal{E}_1} + \underbrace{\sum_{n>Y} w_\sigma(n) A_n(X)}_{\mathcal{E}_2} \\ \underbrace{{} + \pi_K(X) \sum_{n>Y} w_\sigma(n) b_C(n)}_{\mathcal{E}_3}. \end{aligned} \tag{34}$$

For $\mathcal{E}_1$, fix $\lambda > 0$ and C_λ such that $\tau(n) \leq C_\lambda n^\lambda$, as in (15). Lemma 2.1 applies uniformly for $n \leq Y \leq X$, so (33) gives

$$\mathcal{E}_1 \ll_{K,F,\Gamma,\theta,\lambda} X^{\theta+\lambda} \sum_{n\leq Y} n^{\sigma+\lambda} \leq X^{\theta+\lambda} Y^{1+\sigma+\lambda} \leq X^{\theta+2\lambda} Y^{1+\sigma}. \tag{35}$$

To estimate $\mathcal{E}_2$, we group all omitted divisors by the prime at which they occur. Insert $A_n(X) = \sum_{\mathfrak{p}\in\mathcal{P}_C(X)} \mathbf{1}_{n|I_{\mathfrak{p}}}$. The sums are finite because $I_{\mathfrak{p}} < X$. Interchanging them gives

$$\mathcal{E}_2 = \sum_{\mathfrak{p}\in\mathcal{P}_C(X)} \sum_{\substack{n|I_{\mathfrak{p}} \\ n>Y}} w_\sigma(n). \tag{36}$$

For a fixed prime write $I = I_{\mathfrak{p}}$. For $I \leq Y$ the inner sum is empty. For $I > Y$, use the multiplicative inequality $\sum_{n|I} \tau(n) \leq \tau(I)^2$. Since $n^\sigma \leq I^\sigma$ for $n \mid I$ and $I < X$, we obtain

$$\sum_{\substack{n|I \\ n>Y}} w_\sigma(n) \leq I^\sigma \sum_{n|I} \tau(n) \leq I^\sigma \tau(I)^2 \leq C_\lambda^2 X^{2\lambda} I^\sigma. \tag{37}$$

Partition the primes with $I_{\mathfrak{p}} > Y$ into dyadic bands $Y_j < I_{\mathfrak{p}} \le 2Y_j$, where $Y_j = 2^j Y$, $j \ge 0$. A nonempty band has $Y_j < X$, and Lemma 2.2 bounds its size by $c_{K,\Gamma}(X/Y_j)^{\kappa_r}$, with $c_{K,\Gamma}$ depending only on K, Γ. Since $I_{\mathfrak{p}}^{\sigma} \le (2Y_j)^{\sigma}$ in that band, including all good primes gives

$$\begin{aligned}\mathcal{E}_2 &\le C_\lambda^2 X^{2\lambda} \sum_{\substack{\mathfrak{p} \text{ good, } \mathrm{N}\mathfrak{p} \le X \\ I_{\mathfrak{p}} > Y}} I_{\mathfrak{p}}^{\sigma} \\ &\le c_{K,\Gamma} C_\lambda^2 2^{\sigma} X^{\kappa_r + 2\lambda} Y^{\sigma - \kappa_r} \sum_{j \ge 0} 2^{j(\sigma - \kappa_r)} = \frac{c_{K,\Gamma} C_\lambda^2 2^{\sigma}}{1 - 2^{\sigma - \kappa_r}} X^{\kappa_r + 2\lambda} Y^{\sigma - \kappa_r}. \end{aligned} \tag{38}$$

Here $2^{\sigma - \kappa_r} < 1$. Taking bands of the full index bounds the combined contribution of every omitted divisor of each prime, whatever the absolute residue degree of the prime.

For $\mathcal{E}_3$, we sum the bound on the algebraic coefficients beyond the cutoff. Equation (14) gives $b_C(n) \le c_1/(\varphi(n) n^r)$. By Section 2.1, $n/\varphi(n) \le \tau(n)$. Applying these inequalities and (33) gives

$$w_\sigma(n) b_C(n) \le c_1 n^{-1-r+\sigma} \tau(n)^2 \le c_1 C_\lambda^2 n^{-1-r+\sigma+2\lambda}.$$

Take $2\lambda < r - \sigma$. Summing this majorant over $n > Y$ gives $O_{K,\Gamma,\sigma,\lambda}(Y^{\sigma - r + 2\lambda})$. Using $\pi_K(X) \le [K : \mathbb{Q}]X$ and $Y^{2\lambda} \le X^{2\lambda}$, we obtain

$$\mathcal{E}_3 \ll_{K,\Gamma,\sigma,\lambda} X Y^{\sigma - r + 2\lambda} \le X^{1 + 2\lambda} Y^{\sigma - r}. \tag{39}$$

We now choose the cutoff by balancing the three errors. Given $\eta > 0$, take $\lambda = \min\{\eta/4, (r - \sigma)/4\}$. Then $2\lambda \le \eta$ and $2\lambda < r - \sigma$. Inserting (35), (38) and (39) into (34) gives

$$\pi_K(X) \sum_{t \ge 1} t^{\sigma} |P_{X,C}(t) - D_C(t)| \ll_{K,F,\Gamma,\theta,\sigma,\eta} X^{\eta} \big(X^{\theta} Y^{1+\sigma} + X^{\kappa_r} Y^{\sigma - \kappa_r} + X Y^{\sigma - r} \big). \tag{40}$$

At $Y = X^u$, the three exponents inside the parentheses are respectively

$$e_1 = \theta + u + u\sigma, \qquad e_2 = \kappa_r(1 - u) + u\sigma, \qquad e_3 = 1 - ru + u\sigma. \tag{41}$$

The first increases with u and the second decreases since $\sigma < \kappa_r$. Equating them cancels the common $u\sigma$ and gives

$$\theta + u = \kappa_r(1 - u), \qquad (1 + \kappa_r)u = \kappa_r - \theta, \qquad u = \frac{\kappa_r - \theta}{1 + \kappa_r} = \frac{r + 1 - r\theta}{2r + 1}.$$

This choice lies in $(0, 1)$ since $0 \le \theta < 1 < \kappa_r$. Direct substitution yields

$$1 - \theta - u = \frac{(2r + 1)(1 - \theta) - (r + 1 - r\theta)}{2r + 1} = \frac{r - (r + 1)\theta}{2r + 1} = \delta_*.$$

Consequently $e_1 = e_2 = 1 - \delta_* + u\sigma$. To compare e_3, write $1 - \delta_* = \kappa_r(1 - u)$, so that $\delta_* = \kappa_r u - 1/r$. Thus

$$e_1 - e_3 = ru - \delta_* = (r - \kappa_r)u + 1/r > 0, \tag{42}$$

since $r - \kappa_r = r - 1 - 1/r \ge 1/2$ for $r \ge 2$. Thus e_3 is strictly smaller at the crossing. The monotonicity of e_1, e_2 then shows that this crossing minimizes the maximum of all three exponents. The right side of (40) is therefore $O_{K,F,\Gamma,\theta,\sigma,\eta}(X^{1 - \delta_* + u\sigma + \eta})$.

Since $\theta < 1$, (27) at $n = 1$ with the full filter gives $\pi_K(X) \sim \mathrm{Li}(X) \sim X/\log X$. Divide the preceding bound by $\pi_K(X)$ and take $\eta = \varepsilon/2$. The remaining factor $\log X \ll_\varepsilon X^{\varepsilon/2}$ proves (5), uniformly in C. Taking $\varepsilon = (\delta_* - u\sigma)/2 > 0$, for example, gives the saving

$$c = \frac{\delta_* - u\sigma}{2} = \frac{r - (r + 1)\theta - (r + 1 - r\theta)\sigma}{2(2r + 1)}. \qquad \square$$

For the test-function interpretation, put $a_t = P_{X,C}(t) - D_C(t)$. The finite empirical support and (16) ensure that $\sum_t t^\sigma |a_t| < \infty$. For test functions $\Phi : \mathbb{N} \to \mathbb{C}$, the triangle inequality gives the upper bound in

$$\sup_{\Phi:\,|\Phi(t)|\le t^\sigma\ \forall t} \left| \sum_{t\ge 1} \Phi(t) a_t \right| = \sum_{t\ge 1} t^\sigma |a_t|. \tag{43}$$

Since a_t is real, $\Phi(t) = t^\sigma \operatorname{sgn}(a_t)$ attains the supremum even among complex-valued functions. It may depend on X, C. Thus $\sigma = 0$ controls the discrepancy on every set $S_X \subseteq \mathbb{N}$, uniformly over such choices. For $0 < s < \sigma_*$, the choice $\sigma = s$, $\Phi(t) = t^s$ gives the moment discrepancy used below.

3.2 The moment constant and an example

We first identify the model moment $M_{s,C}$ for $0 < s < r$ and bound it uniformly in C, without a zero hypothesis. We then prove the empirical estimate of Corollary 1.2 for $0 < s < \sigma_*$ using Theorem 1.1. A group of rank two over $\mathbb{Q}$ illustrates the constant and the error under GRH.

Proof of Corollary 1.2. For $s > 0$, expanding the Euler factors and writing $k = d/e$ in the divisor sum gives

$$\begin{aligned} J_s(n) &= n^s \prod_{\ell \mid n} (1 - \ell^{-s}) = \sum_{e \mid n} \mu(e)(n/e)^s, \\ \sum_{d \mid n} J_s(d) &= \sum_{d \mid n} \sum_{e \mid d} \mu(e)(d/e)^s = \sum_{k \mid n} k^s \sum_{e \mid n/k} \mu(e) = n^s. \end{aligned} \tag{44}$$

For $0 < s < r$, (16) justifies regrouping the signed double sum over (t, v). Grouping by $n = tv$ and applying (44) gives

$$\begin{aligned} \sum_{t\ge 1} t^s D_C(t) &= \sum_{t,v\ge 1} t^s \mu(v) b_C(tv) = \sum_{n\ge 1} b_C(n) \sum_{t \mid n} t^s \mu(n/t) \\ &= \sum_{n\ge 1} b_C(n) J_s(n) = M_{s,C}. \end{aligned}$$

Using $J_s(1) = 1$, $0 < J_s(n) \le n^s$ and $0 \le b_C(n) \le 1/k_n$, we obtain

$$\frac{|C|}{|G_F|} = b_C(1) \le M_{s,C} \le \sum_{n\ge 1} \frac{n^s}{k_n} < \infty. \tag{45}$$

Indeed, choose $0 < \lambda < r - s$. Equations (14) and (15) give

$$\frac{n^s}{k_n} \ll_{K,\Gamma} \frac{n^s}{\varphi(n) n^r} = n^{s-r-1} \frac{n}{\varphi(n)} \ll_{K,\Gamma,\lambda} n^{-1-(r-s-\lambda)}.$$

This majorant is summable and independent of C. In particular $M_{s,C} > 0$ for nonempty C, while the empty filter gives $M_{s,C} = S_{s,C}(X) = 0$.

Now assume the hypotheses of Theorem 1.1 and take $0 < s < \sigma_*$. By definition $\sum_t t^s P_{X,C}(t) = S_{s,C}(X)/\pi_K(X)$. Apply (43) with $\Phi(t) = t^s$ and $\sigma = s$. After multiplication by $\pi_K(X) \ll_K X$, Theorem 1.1 gives

$$S_{s,C}(X) = M_{s,C} \pi_K(X) + O_{K,F,\Gamma,\theta,s,\varepsilon}(X^{1-\delta_*+us+\varepsilon}).$$

Lemma 2.1, at level one with the full filter, gives $\pi_K(X) = \operatorname{Li}(X) + O_{K,F,\Gamma,\theta,\varepsilon}(X^{\theta+\varepsilon})$. The upper bound in (45) makes the error from replacing $M_{s,C}\pi_K(X)$ by $M_{s,C} \operatorname{Li}(X)$ uniform in C. Since $1 - \delta_* + us = \theta + u(1 + s) > \theta$, this error is absorbed in (7).

For nonempty C, the lower bound $M_{s,C} \geq 1/|G_F|$ and $\mathrm{Li}(X) \asymp X/\log X$ give the relative error $O_{K,F,\Gamma,\theta,s,\varepsilon}(X^{-\delta_*+us+\varepsilon}\log X)$. Choosing $0 < \varepsilon < \delta_* - us$, possible precisely for $s < \sigma_*$, proves the relative asymptotic.

Under GRH, substituting $\theta = 1/2$ gives $u = (r+2)/(2(2r+1))$, $\delta_* = (r-1)/(2(2r+1))$, and hence $\sigma_* = (r-1)/(r+2)$. □

Take $K = F = \mathbb{Q}$, $C = \{1\}$, and $\Gamma = \langle 2, 3\rangle$. The valuations at 2 and 3 give rank two and independent square classes, so $K_2 = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ has degree four. Since $F = K$, all the level coefficients are $b_C(n) = 1/k_n$, in particular $b_C(2) = 1/4$. The $n = 1, 2$ terms give

$$M_{s,C} \geq 1 + \frac{2^s - 1}{4} > 1 \qquad (0 < s < 2).$$

The field degree and this lower bound are unconditional. Under GRH for the division fields, $u = 2/5$, $\delta_* = 1/10$, and the empirical moment estimate holds for $0 < s < 1/4$. At $s = 1/8$, the power saving is $1/20$, up to the arbitrarily small loss, and (7) reads

$$S_{1/8,C}(X) = M_{1/8,C}\,\mathrm{Li}(X) + O_\varepsilon(X^{19/20+\varepsilon}).$$

4 The contribution of higher-degree prime ideals

We prove the bounds for higher-degree primes in Theorem 1.3, study the two Gaussian examples, and refine their moment coefficients after separating the degree-one contribution to the first moment.

The comparison in this section uses the ordinary Chebotarev density theorem [8, §1, (1.1)] for the single extension $K/\mathbb{Q}$. The same theorem for the trivial extension K/K gives $\pi_K(X) \sim \mathrm{Li}(X) \sim X/\log X$. Both inputs are unconditional.

Proof of the growth bound and the elementary tail bound in Theorem 1.3. Put $d = [K : \mathbb{Q}] = |G|$. For a rational prime p unramified in K, Frob_p denotes its arithmetic Frobenius conjugacy class in G. Fix a conjugacy class U whose elements have order $f > 1$, and put $\alpha_U = |U|/d$. Let $\pi_U(Y)$ count the rational primes $p \leq Y$ with $\mathrm{Frob}_p = U$, omitting ramified primes and the rational primes below a prime ideal of bad reduction for Γ. By Chebotarev, $\pi_U(Y) \sim \alpha_U Y/\log Y$, whence

$$\pi_U(Y) - \pi_U(Y/2) = (\alpha_U/2 + o(1))\frac{Y}{\log Y} \qquad (Y \to \infty). \tag{46}$$

Each such p has d/f primes $\mathfrak{p}$ above it, all of norm p^f. Since the generators are rational, $\Gamma_\mathfrak{p} \subseteq \mathbb{F}_p^\times$. Hence

$$I_\mathfrak{p} = \frac{p^f - 1}{p - 1} I_p^{\mathbb{Q}} \;\geq\; \frac{p^f - 1}{p - 1} = 1 + p + \cdots + p^{f-1} \;\geq\; p^{f-1}. \tag{47}$$

Take $Y = X^{1/f}$. When $Y/2 < p \leq Y$ all the ideals just counted have norm at most X. For $s > 0$, (46) gives

$$\begin{aligned} S_s(X) &\geq \frac{d}{f}(\pi_U(Y) - \pi_U(Y/2))(Y/2)^{(f-1)s} \\ &\gg_{K,\Gamma,s,f} \frac{Y^{\,1+(f-1)s}}{\log Y} = f\,\frac{X^{(1+(f-1)s)/f}}{\log X}. \end{aligned}$$

This proves (8) for each of the finitely many possible orders $f > 1$.

To obtain the coefficient at $s = 1$, write $\sum_{p\le Y}^{U}$ for the sum over the primes counted by π_U. Partial summation, with $\pi_U(2^-) = 0$, gives

$$\sum_{p\le Y}^{U} p^{f-1} = Y^{f-1}\pi_U(Y) - (f-1)\int_2^Y t^{f-2}\pi_U(t)\,dt.$$

Using $\pi_U(t) \sim \alpha_U t/\log t$ and $\int_2^Y t^{f-1}\,dt/\log t \sim Y^f/(f\log Y)$ (see the proof of Lemma 4.2 with $\beta = f-1$), we obtain

$$\sum_{p\le Y}^{U} p^{f-1} = \left(\alpha_U - \frac{(f-1)\alpha_U}{f} + o(1)\right)\frac{Y^f}{\log Y} \;\sim\; \frac{\alpha_U Y^f}{f\log Y}. \tag{48}$$

For fixed $T \ge 1$, omitting $p^{f-1} \le T$ costs $O_{T,f}(1)$. Each remaining p gives d/f ideals with $I_{\mathfrak{p}} > T$. Let $\mathcal{H}_U(X)$ consist of all prime ideals above the primes counted by $\pi_U(X^{1/f})$. Combining (47) and (48) with $f\log(X^{1/f}) = \log X$ and $\pi_K(X) \sim X/\log X$ gives

$$\liminf_{X\to\infty} \frac{1}{\pi_K(X)} \sum_{\substack{\mathfrak{p}\in\mathcal{H}_U(X)\\ I_{\mathfrak{p}}>T}} I_{\mathfrak{p}} \ge \lim_{X\to\infty} \frac{d}{f}\,\frac{\alpha_U X}{f\log(X^{1/f})\,\pi_K(X)} = \frac{d\alpha_U}{f} = \frac{|U|}{f}. \tag{49}$$

Different classes give disjoint sets of ideals. There are finitely many classes, so the lower limit of their sum is at least the sum of the lower limits. With g_U any representative of U, we obtain, for every fixed T,

$$\liminf_{X\to\infty} \sum_{t>T} tP_X(t) \;\ge\; \sum_{U\neq\{1\}} \frac{|U|}{\operatorname{ord}(g_U)} = \sum_{\substack{g\in G\\ g\neq 1}} \frac{1}{\operatorname{ord}(g)} = c_K. \tag{50}$$

Every term used for this lower bound comes from an ideal of absolute degree greater than one.

Let ν be a nonnegative measure with $\sum_t t\nu(t) < \infty$. Fix $\sigma \ge 1$. Since $t^{\sigma-1} \ge T^{\sigma-1}$ for $t > T$,

$$\begin{aligned} V_\sigma(X,\nu) &\ge T^{\sigma-1}\sum_{t>T} t|P_X(t) - \nu(t)| \\ &\ge T^{\sigma-1}\left(\sum_{t>T} tP_X(t) - \sum_{t>T} t\nu(t)\right). \end{aligned}$$

At fixed T, (50) now implies

$$\liminf_{X\to\infty} V_\sigma(X,\nu) \ge T^{\sigma-1}\left(c_K - \sum_{t>T} t\nu(t)\right).$$

The parenthesis tends to $c_K > 0$ as $T \to \infty$. At $\sigma = 1$ this gives the lower bound c_K. For $\sigma > 1$ the right-hand side tends to $+\infty$, proving the divergence in (9). □

The ideals used in this proof have relative density zero among all prime ideals, yet their indices grow fast enough to prevent the first-moment tails from vanishing. Thus a contribution invisible to fixed-index frequencies can persist in the mean. The coefficient c_K uses only $I_p^{\mathbb{Q}} \ge 1$ in (47) and depends solely on the splitting types in $K/\mathbb{Q}$. Retaining $I_p^{\mathbb{Q}}$ and applying Chebotarev at each fixed divisibility level gives $c_K^\sharp(\Gamma)$ in Theorem 4.3. That argument also proves the strict improvement and the dependence on the rank, completing Theorem 1.3.

4.1 Two groups over the Gaussian field

The two examples impose different constraints on the reduced subgroup. For rational generators it lies in the prime field. For the second group it lies in the kernel of the residue-field norm, even though the generators generate K as a field. Thus the latter obstruction also occurs for a group that is not contained in a proper subfield.

In $K = \mathbb{Q}(i)$, each $p \equiv 3 \pmod 4$ yields one inert ideal $(p) = p\mathbb{Z}[i]$ of norm p^2, with Frobenius equal to complex conjugation. The number of these ideals up to norm X is asymptotic to $\sqrt{X}/(2\log\sqrt{X}) = o(\pi_K(X))$.

Rational generators. For $\Gamma = \langle 2, 3, 5\rangle$, the valuations at $2, 3, 5$ give rank three, and the bad ideals are precisely those above these primes. An inert prime $p \equiv 3 \pmod 4$ is good here except for $p = 3$. Since $\Gamma_{(p)} \subseteq \mathbb{F}_p^\times$, its index in $\mathbb{F}_{p^2}^\times$ is $I_{(p)} = (p+1)I_p^{\mathbb{Q}}$. By (8) with $f = 2$,

$$\frac{S_s(X)}{\pi_K(X)} \gg_s X^{(s-1)/2}. \tag{51}$$

Thus every normalized moment with $s > 1$ tends to infinity. In particular $S_2(X) \gg X^{3/2}/\log X$, whereas (2) would give a constant times $\mathrm{Li}(X)$ since $2 < 3$. At $s = 1$ the nonidentity element has order two, yielding $c_K = 1/2$ in (50).

A field-generating group of norm one. We use three elements of norm one whose group generates K over $\mathbb{Q}$. Set

$$\varpi_1 = 2 + i, \qquad \varpi_2 = 3 + 2i, \qquad \varpi_3 = 4 + i, \qquad g_j = \frac{\varpi_j}{\overline{\varpi_j}}, \qquad \Gamma = \langle g_1, g_2, g_3\rangle.$$

Write $q_j = \varpi_j\overline{\varpi_j}$, so $(q_1, q_2, q_3) = (5, 13, 17)$. The three distinct rational primes q_j split in $\mathbb{Z}[i]$, giving six distinct prime ideals with factorizations

$$(q_j) = (\varpi_j)(\bar\varpi_j), \qquad (g_j) = (\varpi_j)(\bar\varpi_j)^{-1}.$$

It follows that $v_{(\varpi_k)}(g_j) = \delta_{kj}$ and $v_{(\bar\varpi_k)}(g_j) = -\delta_{kj}$, so the g_j are multiplicatively independent. The equalities $g_1 = (2+i)^2/5 = (3+4i)/5$ and $i = (5g_1 - 3)/4$ prove $\mathbb{Q}(g_1) = K$.

All inert $p \equiv 3 \pmod 4$ are good for this group because its bad prime ideals lie over $5, 13, 17$. At such a prime, conjugation induces $z \mapsto z^p$ on $\mathbb{F}_{p^2}$, so the reductions lie in the kernel of the norm $z \mapsto z^{p+1}$, of order $p+1$ [5, Ch. 4 and Exercise A-24]. Hence $\#\Gamma_{(p)} \mid p+1$ and $p-1 \mid I_{(p)}$. The same local divisibility for norm-one units in real quadratic fields appears in [49] and in [50, p. 167].

Using $p - 1 \geq p/2$ in the dyadic-block argument gives (51) for this group as well. For the first moment, take U to be the class of complex conjugation. Then $\alpha_U = 1/2$, and (48) gives

$$\sum_{p\leq Y}^{U}(p-1) = \sum_{p\leq Y}^{U} p - \pi_U(Y) \sim \frac{Y^2}{4\log Y}, \qquad \pi_U(Y) = O(Y/\log Y).$$

Removing $p \leq T + 1$ costs $O_T(1)$ and ensures $I_{(p)} > T$. At $Y = \sqrt{X}$, one has $Y^2/(4\log Y) = X/(2\log X)$. Division by $\pi_K(X) \sim X/\log X$ gives the coefficient $1/2$ for this lower bound on every fixed first-moment tail. The final inequality in the proof of Theorem 1.3 therefore applies also to this group. It gives a lower bound $1/2$ at weight one and divergence of the discrepancy for every $\sigma > 1$. The stronger bound $M_1/2 \geq 251/432$ will be proved for these generators in Proposition 4.5, Section 4.4, by retaining the index inside the norm kernel.

An elementary lower bound for both second moments. For either group let $\pi_{\mathrm{in}}(Y)$ count its good inert rational primes up to Y. Then $\pi_{\mathrm{in}}(Y) \sim Y/(2\log Y)$, and each such p gives one ideal of norm p^2 with $I_{(p)} \geq p-1$. Sums marked in below run over these primes. Partial summation gives

$$\begin{aligned}\sum_{p\leq Y}^{\mathrm{in}} p^2 &= Y^2\pi_{\mathrm{in}}(Y) - 2\int_2^Y t\pi_{\mathrm{in}}(t)\,dt \\ &= \left(\frac{1}{2} - \frac{1}{3} + o(1)\right)\frac{Y^3}{\log Y}.\end{aligned}$$

Moreover,

$$0 \leq \sum_{p\leq Y}^{\mathrm{in}} (p^2 - (p-1)^2) \leq 2Y\pi_{\mathrm{in}}(Y) = O(Y^2/\log Y).$$

With $Y = \sqrt{X}$, one has $Y^3/\log Y = 2X^{3/2}/\log X$. Hence

$$S_2(X) \geq \sum_{p\leq\sqrt{X}}^{\mathrm{in}} (p-1)^2 = \left(\frac{1}{3} + o(1)\right)\frac{X^{3/2}}{\log X}.$$

Thus $1/3$ is a lower bound for the normalized lower limit of the full second moment. The refinements are proved in Corollary 4.4 and Proposition 4.5 below. Retaining three divisibility levels will give $329/648$ for both groups, and summing all levels will give the stronger coefficient for the rational group.

4.2 The first-moment coefficient and comparison with Ambrose

We first obtain an unconditional lower bound for the degree-one part of the mean from the fixed-level divisibility densities. We then combine it with the higher-degree contribution and compare the resulting growth with Ambrose's proposed scales. For the degree-one estimate, take any number field K, any fixed group $\Gamma \subset K^\times$ of rank $r > 1$, and the unrestricted filter. By Corollary 1.2 with $s = 1$, the model coefficient is

$$M_1 = \sum_{n\geq 1} \varphi(n)b(n) = \sum_{t\geq 1} tD(t).$$

We apply the positive divisor truncation used over the rational primes by Felix [23, §7.4, pp. 120–121] to the prime ideals of absolute degree one. Write $S_s^{(1)}(X)$ for the part of $S_s(X)$ over these ideals. For $B \geq 1$, each admissible prime satisfies $I_{\mathfrak{p}} = \sum_{n\mid I_{\mathfrak{p}}} \varphi(n) \geq \sum_{n\leq B,\, n\mid I_{\mathfrak{p}}} \varphi(n)$. Let $A_n^{(1)}(X)$ count the primes in $A_n(X)$ of absolute degree one. A prime ideal of higher degree and norm at most X lies over a rational prime at most $\sqrt{X}$. Since $d = [K:\mathbb{Q}]$, at most d prime ideals lie above each rational prime. Hence $0 \leq A_n(X) - A_n^{(1)}(X) \leq d\sqrt{X}$. For each *fixed* n, ordinary Chebotarev applied to K_n/K and the splitting criterion (12) give $A_n(X)/\pi_K(X) \to b(n)$. Removing higher degrees changes this ratio by at most $d\sqrt{X}/\pi_K(X) = O_K(\log X/\sqrt{X})$, which tends to zero. Interchanging the finite sums over $n \leq B$ and degree-one ideals now gives

$$\liminf_{X\to\infty} \frac{S_1^{(1)}(X)}{\pi_K(X)} \;\geq\; \lim_{X\to\infty} \sum_{n\leq B} \varphi(n)\frac{A_n^{(1)}(X)}{\pi_K(X)} = \sum_{n\leq B} \varphi(n)b(n).$$

The left side is independent of B. Positivity and convergence of the model series therefore give

$$\liminf_{X\to\infty} \frac{S_1^{(1)}(X)}{\pi_K(X)} \geq M_1.$$

The argument takes limits only at fixed divisibility levels. Pointwise convergence $P_X(t) \to D(t)$ for every t would be an additional hypothesis; already $t = 1$ is an Artin-type primitive-generation question.

Now impose the hypotheses of Theorem 1.3, including rational generators. The sum $S_1(X)$ contains the degree-one contribution and the disjoint higher-degree tail above any fixed cutoff. The strengthened tail bound will be proved in Theorem 4.3, Section 4.3, using only fixed-level Chebotarev counts. Combining that bound with the estimate just proved gives

$$\liminf_{X\to\infty} \frac{S_1(X)}{\pi_K(X)} \;\geq\; M_1 + c_K^{\sharp}(\Gamma) \qquad (r > 1). \tag{52}$$

For the Gaussian norm-one group, the separate splitting criterion proved in Proposition 4.5, Section 4.4, will instead give $3M_1/2$.

Ambrose defines $P_C(L/K)$ as "the set of all prime ideals $\mathfrak{p}$ of K, unramified in L, which satisfy" $\left[\frac{L|K}{\mathfrak{p}}\right] \subset C$, his notation for the Frobenius condition [4, pp. xvii–xviii]. His bounded set is $P_C(x, L/K) = \{\mathfrak{p} \in P_C(L/K) : \mathrm{N}\mathfrak{p} \leq x\}$. With good reduction imposed, his sum of $\mathrm{ind}_\Gamma(\mathfrak{p})^\kappa$ in (4.2) is exactly $S_{s,C}(X)$ on putting $L = F$, $x = X$, $\kappa = s$, and his rank $\gamma = r$. Thus his formula (4.2) gives the prediction stated in (2). The reference to imaginary quadratic fields qualifies his example of the full unit group. The two fixed Gaussian groups meet his stated hypotheses [4, §4.2, pp. 26–27, (4.2) and n. 10]. The examples show why a degree-one heuristic requires a separate higher-degree contribution when applied to the literal sum. Section 4.3 gives the exact decomposition and the classwise bounds. To compare powers for $r > 1$ and a fixed occurring degree $f > 1$, put $b_f = 1 + f(r-1)$ and use

$$a_f(s) - 1 = \frac{(f-1)(s-1)}{f}, \qquad a_f(s) - (s - r + 1) = \frac{1 + f(r-1) - s}{f}. \tag{53}$$

For fixed $b > 0$, $\mathrm{Li}(X^b) \sim X^b/(b \log X)$. Dividing the guaranteed scale in (8) by the corresponding scale in (2) gives

$$\frac{X^{a_f(s)}/\log X}{\mathrm{Li}(X)} \sim X^{(f-1)(s-1)/f} \qquad (0 < s < r),$$
$$\frac{X^{a_f(s)}/\log X}{\mathrm{Li}(X^{s-r+1})} \sim (s - r + 1) X^{(b_f - s)/f} \qquad (s > r).$$

At $s = r$ the denominator is X, so the ratio is $X^{(f-1)(r-1)/f}/\log X \to \infty$. Since $b_f - r = (f-1)(r-1) > 0$, the second ratio diverges for $r < s < b_f$, tends to a positive constant for $s = b_f$, and tends to zero for $s > b_f$. These are comparisons of scales. Table 1 records their implications for the proposed asymptotics.

If G contains elements of different orders > 1, taking the largest order gives the widest interval of contradictions. At rank one, $b_f = 1$, the heuristic predicts X at $s = 1$, and Theorem 4.3 gives $S_1(X)/(X/\log X) \to \infty$. This still permits growth of order X. For $s > 1$ the predicted exponent is s, which exceeds $a_f(s)$ by $(s-1)/f$. Thus this comparison supplies no growth contradiction at rank one. In both Gaussian rank-three examples $f = 2$, and the growth contradiction occurs precisely on $1 < s < 5$ by this argument. Ambrose's theorems on averages over generators [4, Theorems 6.1–6.2] and his residue-tuple averages [44] concern a different quantifier. Our lower bounds concern each of two fixed groups. The ideals used for the growth contradiction all have degree greater than one, so a count restricted to absolute degree one omits them.

Table 1: Ambrose's scales and the lower bounds for the unrestricted count in Theorem 1.3 with $r > 1$. The indicated residue degree $f > 1$ determines the threshold $b_f = 1 + f(r-1)$.

Weight	Predicted scale	Consequence of the bounds
$0 < s < 1$	$\mathrm{Li}(X)$	The lower bound has $a_f(s) < 1$. Corollary 1.2 proves the predicted asymptotic in its stated conditional range.
$s = 1$	$\mathrm{Li}(X)$	If $S_1(X) \sim \mathcal{A}_1 \mathrm{Li}(X)$, then $\mathcal{A}_1 \geq M_1 + c_K^\sharp(\Gamma)$ by (52).
$1 < s < r$	$\mathrm{Li}(X)$	Contradicted by $a_f(s) > 1$.
$s = r$	X	Contradicted since $a_f(r) > 1$.
$r < s < b_f$	$\mathrm{Li}(X^{s-r+1})$	Contradicted since $a_f(s) > s - r + 1$.
$s = b_f$	$\mathrm{Li}(X^{s-r+1})$	Identical powers and logarithmic factors. This family gives a lower bound of the predicted order.
$s > b_f$	$\mathrm{Li}(X^{s-r+1})$	The guaranteed lower bound has smaller order and leaves this case undecided.

4.3 Rational generators and the higher-degree coefficient

Let $K/\mathbb{Q}$ be finite Galois of degree $d > 1$ and let $\Gamma \subset \mathbb{Q}^\times$ be fixed of positive rank r. For a good rational prime p unramified in K, let U be its Frobenius class and $f = f_U$ the order of an element of U. The d/f prime ideals above p have the same index. Reduction of rational elements factors through $\mathbb{F}_p^\times$, so the exact local identity is

$$I_{\mathfrak{p}} = (1 + p + \cdots + p^{f-1}) I_p^{\mathbb{Q}} \qquad (\mathfrak{p} \mid p).$$

Keep $S_s^{(1)}(X)$ for the degree-one sum from Section 4.2. For each nonidentity conjugacy class U, let $S_{s,U}^{\mathrm{high}}(X)$ be the sum of $I_{\mathfrak{p}}^s$ over ideals above the good unramified rational primes in U with $p \leq X^{1/f_U}$; each such p contributes d/f_U ideals. Writing $\sum^U$ for these rational primes, one has

$$S_s(X) = S_s^{(1)}(X) + \sum_{U \neq \{1\}} S_{s,U}^{\mathrm{high}}(X) + O_{K,\Gamma,s}(1),$$

$$S_{s,U}^{\mathrm{high}}(X) = \frac{d}{f_U} \sum_{p \leq X^{1/f_U}}^{U} (1 + p + \cdots + p^{f_U - 1})^s (I_p^{\mathbb{Q}})^s.$$

The bounded remainder accounts for ramified rational primes with a higher-degree ideal. This separates the two sources of growth without prescribing an asymptotic for either.

To bound the rational-prime sum in this decomposition, we need the density of each joint Frobenius and divisibility condition and its version with the polynomial weight $p^{(f_U-1)s}$. Lemma 4.1 supplies the density, and Lemma 4.2 converts it into a weighted prime sum. Theorem 4.3 then combines these inputs with positive Jordan divisor truncation to retain the factor $(I_p^{\mathbb{Q}})^s$. Both inputs are unconditional: Chebotarev is applied at a fixed divisibility level before the divisor cutoff is allowed to grow.

Lemma 4.1 (Fixed joint density)**.** *Let U be a conjugacy class in* $\mathrm{Gal}(K/\mathbb{Q})$*, let $n \geq 1$, and put $Q_n = \mathbb{Q}(\mu_n, \Gamma^{1/n})$, so that $K_n = KQ_n$ for the rational group considered here. The density among rational primes of the joint conditions* $\mathrm{Frob}_p = U$ *and* $n \mid I_p^{\mathbb{Q}}$ *is*

$$b_U^{\mathbb{Q}}(n) = \frac{|U \cap \mathrm{Gal}(K/(K \cap Q_n))|}{[Q_n : \mathbb{Q}]\,[K : K \cap Q_n]}.$$

Proof. Outside the finite set of bad primes, primes dividing n, and primes ramified in K, equation (12) identifies the divisibility condition with complete splitting in Q_n. In the compositum KQ_n, Frobenius must fix Q_n and restrict on K to an element of U. Such a pair of restrictions

is compatible exactly when the element of U fixes $K \cap Q_n$, and (10) gives one automorphism for each compatible pair. The denominator in Chebotarev is $[KQ_n : \mathbb{Q}] = [Q_n : \mathbb{Q}][K : K \cap Q_n]$ by (11). This gives the density among all rational primes. At $n = 1$ it is $b_U^{\mathbb{Q}}(1) = |U|/d =: \alpha_U$. Dividing $b_U^{\mathbb{Q}}(n)$ by α_U gives the density conditional on the class U. □

Lemma 4.2 (Weighted prime sums)**.** *If nonnegative weights w_p on the rational primes satisfy $\sum_{p \le y} w_p = (b + o(1))y/\log y$ with $b \ge 0$, then for each fixed $\beta \ge 0$*

$$\sum_{p \le y} p^\beta w_p = \left(\frac{b}{1+\beta} + o(1)\right) \frac{y^{1+\beta}}{\log y}.$$

Proof. The case $\beta = 0$ is the hypothesis. For $\beta > 0$, put $W(t) = \sum_{p \le t} w_p$. Partial summation gives

$$\sum_{p \le y} p^\beta w_p = y^\beta W(y) - \beta \int_2^y t^{\beta-1} W(t)\, dt.$$

Differentiating $y^{1+\beta}/((1+\beta)\log y)$ shows that it is asymptotic to $\int_2^y t^\beta/\log t\, dt$. For any $\varepsilon > 0$, the difference $W(t) - bt/\log t$ is at most $\varepsilon t/\log t$ in absolute value above a fixed threshold. Its integral against $t^{\beta-1}$ below that threshold is bounded, and the part above it is at most $\varepsilon \int_2^y t^\beta/\log t\, dt$ in absolute value. Letting $\varepsilon \downarrow 0$, the coefficients of $y^{1+\beta}/\log y$ in the two main terms are b and $-\beta b/(1+\beta)$. Their sum is $b/(1+\beta)$, also when $b = 0$. □

Theorem 4.3 (Classwise lower bounds)**.** *For every $U \ne \{1\}$, $f = f_U$, $s > 0$, and fixed index cutoff $T \ge 1$, let $S_{s,U}^{\mathrm{high}}(X;T)$ be the part of $S_{s,U}^{\mathrm{high}}(X)$ with $I_\mathfrak{p} > T$. Then*

$$\liminf_{X\to\infty} \frac{\log X}{X^{a_f(s)}} S_{s,U}^{\mathrm{high}}(X;T) \;\ge\; \frac{d}{1+(f-1)s} \sum_{n\ge 1} J_s(n) b_U^{\mathbb{Q}}(n).$$

At $s = 1$ the sum over the nonidentity classes gives $c_K^\sharp(\Gamma)$ as a lower bound for the normalized higher-degree tail. In terms of the class-conditioned model moment $m_U = \alpha_U^{-1} \sum_{n\ge1} \varphi(n) b_U^{\mathbb{Q}}(n)$, this coefficient is $\sum_{U \ne \{1\}} |U| m_U / f_U$.

Proof. Fix an integer $n_{\max} \ge 1$ and the cutoff T. By (44) and positivity,

$$(I_p^{\mathbb{Q}})^s \ge \sum_{\substack{n \mid I_p^{\mathbb{Q}} \\ n \le n_{\max}}} J_s(n).$$

For $p > T^{1/(f-1)}$ all d/f ideals have $I_\mathfrak{p} > T$. With $Y = X^{1/f}$ and $\beta = (f-1)s$, retain p^β from the geometric factor. At each fixed n, Lemma 4.1 counts the joint condition, and Lemma 4.2, applied to its indicator, gives

$$\sum_{\substack{p \le Y \\ n \mid I_p^{\mathbb{Q}}}}^{U} p^\beta = \left(\frac{b_U^{\mathbb{Q}}(n)}{1+\beta} + o(1)\right) \frac{Y^{1+\beta}}{\log Y}.$$

Insert the truncated divisor sum into $S_{s,U}^{\mathrm{high}}(X;T)$. Both sums are finite, so the resulting lower bound is

$$\frac{d}{f} \sum_{n \le n_{\max}} J_s(n) \sum_{\substack{T^{1/(f-1)} < p \le Y \\ n \mid I_p^{\mathbb{Q}}}}^{U} p^\beta.$$

Omitting the primes below the threshold changes each inner sum by $O_{T,f,s}(1)$. Since $Y^{1+\beta} = X^{a_f(s)}$ and $\log X = f \log Y$, normalization multiplies $Y^{1+\beta}/\log Y$ by f. At fixed $n_{\max}$ the

classwise lower limit is therefore at least $\frac{d}{1+\beta}\sum_{n\le n_{\max}} J_s(n)b_U^{\mathbb{Q}}(n)$. This holds for every cutoff. Taking the supremum of these nonnegative partial sums proves the assertion, including a divergent series. The fixed-level limit precedes this supremum, so each error term may depend on its level.

For $s=1$, $a_f(1)=1$, $J_1=\varphi$, and $\pi_K(X)\sim X/\log X$. The prefactor for class U becomes d/f_U. The classes are disjoint and finite in number, so the lower limit of the total is at least the sum of the classwise lower bounds. Since $\alpha_U=|U|/d$, their sum is

$$\sum_{U\neq\{1\}}\frac{d}{f_U}\sum_{n\ge1}\varphi(n)b_U^{\mathbb{Q}}(n)=\sum_{U\neq\{1\}}\frac{d}{f_U}\alpha_U m_U=\sum_{U\neq\{1\}}\frac{|U|}{f_U}m_U=c_K^{\sharp}(\Gamma).$$

When $r>1$, Corollary 1.2 over $\mathbb{Q}$ identifies $\alpha_U m_U$ with the finite first moment of the filtered model. To obtain strict improvement and analyze rank one, let $N_0=2d\,d_K$, where d_K is the absolute discriminant. For $(n,N_0)=1$, put $\Omega_n=\mathbb{Q}(\mu_n)$. Any rational prime ramifying in $K\cap\Omega_n$ would ramify in both overfields and so divide both d_K and n. The intersection therefore has absolute discriminant one. Minkowski's discriminant bound gives $K\cap\Omega_n=\mathbb{Q}$ [2, Ch. 4], whence $[K\Omega_n:\Omega_n]=d$. Since n is odd, the n-th roots of each rational torsion element ±1 lie in Ω_n. For a basis $g_1,\dots,g_r$ of the free part Γ_0, this gives $Q_n=\Omega_n(g_1^{1/n},\dots,g_r^{1/n})$. An automorphism fixing Ω_n is determined by the multipliers on these r roots. They give an injective homomorphism into μ_n^r, since the automorphisms fix μ_n. Thus $[Q_n:\Omega_n]\mid n^r$.

The degrees d and $[Q_n:\Omega_n]$ are coprime. The degree of their compositum over Ω_n is a multiple of each by the tower formula and at most their product. It equals their product, so $[KQ_n:Q_n]=d$. As $K/\mathbb{Q}$ is Galois, this last degree is $[K:K\cap Q_n]$, giving $K\cap Q_n=\mathbb{Q}$. Lemma 4.1 now yields $b_U^{\mathbb{Q}}(n)=\alpha_U/[Q_n:\mathbb{Q}]$. The tower bound $[Q_n:\mathbb{Q}]\le\varphi(n)n^r$ and positivity give

$$c_K^{\sharp}(\Gamma)\ge\sum_{U\neq\{1\}}\frac{d}{f_U}\sum_{(n,N_0)=1}\varphi(n)\frac{\alpha_U}{\varphi(n)n^r}=c_K\sum_{(n,N_0)=1}\frac{1}{n^r}.$$

The terms $n=1$ and $n=1+N_0$ already give a sum greater than one. At $r=1$, summing over $n=1+kN_0$ gives at least $N_0^{-1}\sum_{k\ge0}(k+1)^{-1}$, since $1+kN_0\le N_0(k+1)$. For every nonidentity U the same divergent series has positive prefactor $d\alpha_U/f_U$, so each such class has divergent first-moment tail. Subtracting $\sum_{t>T}t\nu(t)$ and letting $T\to\infty$ as in the proof of (50) gives the strengthened V_1 bound in (9). This completes the coefficient and rank assertions of Theorem 1.3. □

What would give a classwise asymptotic. Fix a nonidentity conjugacy class U, put $f=f_U$, and let $s>0$. If $\sum_{p\le y}^{U}(I_p^{\mathbb{Q}})^s=(\mathcal{L}_{s,U}+o(1))y/\log y$ with $0<\mathcal{L}_{s,U}<\infty$, Lemma 4.2 and $(1+p+\cdots+p^{f-1})^s/p^{(f-1)s}\to1$ give $S_{s,U}^{\mathrm{high}}(X)\sim d\mathcal{L}_{s,U}X^{a_f(s)}/((1+(f-1)s)\log X)$. Indeed, the ratio of the two weights is $(1+p^{-1}+\cdots+p^{-(f-1)})^s$, which lies between 1 and $1+\varepsilon$ for all sufficiently large p. The finitely many remaining terms are bounded, while the weighted sum grows because $\mathcal{L}_{s,U}>0$. Corollary 1.2, applied with base $\mathbb{Q}$, auxiliary field K, and filter U, supplies the hypothesis in its conditional range, with $\mathcal{L}_{s,U}=\sum_n J_s(n)b_U^{\mathbb{Q}}(n)$. Its composita are exactly KQ_n. Dividing the classwise asymptotic by $\pi_K(X)\sim X/\log X$ leaves a power $X^{a_f(s)-1}=X^{-(1-s)(f-1)/f}$, which tends to zero for $s<1$. Outside the conditional range the fixed-level argument alone gives a lower bound. An additive expansion with a specified error for the total also requires control of the degree-one sum to the stated precision.

Corollary 4.4 (Gaussian rational generators)**.** *In $K=\mathbb{Q}(i)$, for every rational group of rank $r>1$,*

$$c_K^{\sharp}(\Gamma)\ge\tfrac{1}{2}(1-2^{-r})\zeta(r).$$

For $\Gamma = \langle 2, 3, 5\rangle$ one has exactly

$$c_K^\sharp(\Gamma) = \frac{5887}{12000}\zeta(3) = 0.589709082408\ldots.$$

Let U be the class of complex conjugation in $K/\mathbb{Q}$. For this group the inert second moment satisfies

$$\liminf_{X\to\infty} \frac{\log X}{X^{3/2}} S_{2,U}^{\mathrm{high}}(X) \;\geq\; \frac{2}{3}\sum_{n\geq 1} J_2(n) b_U^{\mathbb{Q}}(n) = \frac{655\,\zeta(3)}{14\pi^4} = 0.577349508443\ldots.$$

The same lower bound holds for the full second moment $S_2(X)$ with this normalization.

Proof. Here $d = 2$, $d_K = 4$ and U is the single nonidentity class with $f = 2$. The first bound follows from $N_0 = 16$ and $c_K = 1/2$ in the preceding coprimality estimate.

For the specific group put $Q_n = \mathbb{Q}(\mu_n, 2^{1/n}, 3^{1/n}, 5^{1/n})$ with positive real roots. The two cyclotomic bases are $\Omega_n = \mathbb{Q}(\mu_n)$ and $\Omega_n(i)$. At a good unramified prime splitting in Q_n, Frobenius restricts to the identity or conjugation on $K = \mathbb{Q}(i)$. In the first case it fixes both fields and hence their compositum, while the second case gives inertness in K. Subtracting the density of primes splitting completely in KQ_n from the corresponding density in Q_n therefore gives

$$b_U^{\mathbb{Q}}(n) = \frac{1}{[Q_n : \mathbb{Q}]} - \frac{1}{[KQ_n : \mathbb{Q}]}.$$

If $4 \mid n$, then $i \in Q_n$ and the difference is zero. For $4 \nmid n$, the two cyclotomic bases have degrees $\varphi(n)$ and $\varphi(\mathrm{lcm}(n, 4)) = 2\varphi(n)$, respectively.

For either base $\Omega \in \{\Omega_n, \Omega_n(i)\}$, Kummer theory [5, v5.10, Theorem 5.30, pp. 75–76] gives the degree $[\Omega Q_n : \Omega]$ as the size of the image of

$$(\mathbb{Z}/n\mathbb{Z})^3 \longrightarrow \Omega^\times/(\Omega^\times)^n, \qquad (e_2, e_3, e_5) \longmapsto [2^{e_2}3^{e_3}5^{e_5}].$$

Writing $\ker_\Omega$ for its kernel gives $[\Omega Q_n : \Omega] = n^3/|\ker_\Omega|$. For a kernel vector take $0 \leq e_j < n$ and write $a = 2^{e_2}3^{e_3}5^{e_5}$. One n-th root of a lies in Ω, and the others differ by elements of $\mu_n \subset \Omega$. Thus the positive real root $b = a^{1/n}$ belongs to Ω. As $\Omega/\mathbb{Q}$ is abelian, all its subgroups are normal and the subfield $\mathbb{Q}(b) \subset \mathbb{R}$ is Galois over $\mathbb{Q}$. Every conjugate of b is consequently a real root of $Z^n - a$. For odd n the unique real root is b. It follows that $b \in \mathbb{Q}$ and $n \mid e_j$ by the valuation at each $j = 2, 3, 5$, so all three e_j vanish.

For $n = 2m$ with m odd, every conjugate is b or $-b$, so $b^2 \in \mathbb{Q}$. As $a = (b^2)^m$, each e_j is either 0 or m. Write t for the product of those j with $e_j = m$. Then $a = t^m$ and $b = \sqrt{t}$. Conversely, each such squarefree product with $\sqrt{t} \in \Omega$ gives a kernel vector, including $t = 1$ for the zero vector.

For $t = 2, 3, 5, 6, 10, 15, 30$ the quadratic discriminants are respectively $8, 12, 5, 24, 40, 60, 120$, using t for $t \equiv 1 \bmod 4$ and $4t$ otherwise. The nontrivial primitive Dirichlet character of a quadratic field has conductor equal to the absolute value of its discriminant by the conductor–discriminant formula. The character–subfield correspondence places the field in $\mathbb{Q}(\mu_h)$ exactly when that primitive character induces a character modulo h, equivalently when its conductor divides h [62, Ch. 3, Theorem 3.11, p. 27]. For $n = 2m$ with m odd, none of the four discriminants divisible by 8 divides $4m$. Over $\Omega_n = \mathbb{Q}(\mu_m)$, the possible products are 1 and also 5 if $5 \mid m$. Over $\Omega_n(i) = \mathbb{Q}(\mu_{4m})$, each of these products can also be multiplied by 3 if $3 \mid m$. Thus the two kernel sizes are $2^{\mathbf{1}_{5\mid m}}$ and $2^{\mathbf{1}_{5\mid m}+\mathbf{1}_{3\mid m}}$, respectively.

Substituting the degrees into the density difference gives, for $4 \nmid n$,

$$\varphi(n) b_U^{\mathbb{Q}}(n) = \frac{|\ker_{\Omega_n}| - \frac{1}{2}|\ker_{\Omega_n(i)}|}{n^3}.$$

For odd n both kernels have size one. For $n = 2m$ with m odd, the numerator vanishes when $3 \mid m$. Otherwise it is $(1 + \mathbf{1}_{5|m})/2$, and $n^3 = 8m^3$. This gives

$$\varphi(n) b_U^{\mathbb{Q}}(n) = \begin{cases} (2n^3)^{-1}, & n \text{ odd}, \\ (1 + \mathbf{1}_{5|m})/(16m^3), & n = 2m,\ (m, 6) = 1, \\ 0, & 4 \mid n \text{ or } 6 \mid n. \end{cases}$$

At $n = 2, 3$ the kernels for Ω_n are trivial, so $[Q_2 : \mathbb{Q}] = \varphi(2)2^3 = 8$ and $[Q_3 : \mathbb{Q}] = \varphi(3)3^3 = 54$. The joint densities $b_U^{\mathbb{Q}}(n)$ for $n = 1, 2, 3$ are $1/2, 1/16, 1/108$, respectively. Their first-moment weights $\varphi(n)$ are $1, 1, 2$, giving $1/2 + 1/16 + 2/108 = 251/432$.

For the full first moment there is just one nonidentity class, with $d/f = 1$. Thus $c_K^\sharp(\Gamma) = \sum_{n \geq 1} \varphi(n) b_U^{\mathbb{Q}}(n)$. Separating the odd levels from $n = 2m$ in the case formula gives

$$c_K^\sharp(\Gamma) = \frac{1}{2} \sum_{n \text{ odd}} \frac{1}{n^3} + \frac{1}{16} \left(\sum_{(m,6)=1} \frac{1}{m^3} + \sum_{\substack{(m,6)=1 \\ 5|m}} \frac{1}{m^3} \right).$$

All three sums converge absolutely by comparison with $\zeta(3) = \sum_{n \geq 1} n^{-3}$. The sum over odd n equals $(1 - 2^{-3})\zeta(3)$ after subtracting the even terms. Inclusion–exclusion for multiples of 2 and 3 gives

$$\sum_{(m,6)=1} \frac{1}{m^3} = (1 - 2^{-3} - 3^{-3} + 6^{-3})\zeta(3) = (1 - 2^{-3})(1 - 3^{-3})\zeta(3).$$

The last sum counts the extra copy of every term with $5 \mid m$. Writing $m = 5k$ preserves coprimality with 6, so

$$\sum_{\substack{(m,6)=1 \\ 5|m}} \frac{1}{m^3} = 5^{-3} \sum_{(k,6)=1} \frac{1}{k^3}.$$

The two even-level sums therefore carry the factor $1 + 5^{-3}$. Combining them with the odd levels gives

$$\begin{aligned} c_K^\sharp(\Gamma) &= \left[\frac{1 - 2^{-3}}{2} + \frac{(1 - 2^{-3})(1 - 3^{-3})(1 + 5^{-3})}{16} \right] \zeta(3) \\ &= \left(\frac{7}{16} + \frac{637}{12000} \right) \zeta(3) = \frac{5887}{12000} \zeta(3). \end{aligned}$$

For the second moment, Theorem 4.3 gives the prefactor $d/(1 + (f - 1)s) = 2/3$. The respective weights at $n = 1, 2, 3$ are $J_2(1) = 1$, $J_2(2) = 2^2 - 1 = 3$ and $J_2(3) = 3^2 - 1 = 8$. Thus these three levels give $\frac{2}{3}(1/2 + 3/16 + 8/108) = 329/648$. To sum all levels, put

$$\psi_{\mathrm{D}}(n) = n \prod_{\ell | n} (1 + \ell^{-1}), \qquad Z_\psi = \sum_{n \geq 1} \frac{\psi_{\mathrm{D}}(n)}{n^3},$$

where ψ_{D} is the Dedekind psi function and the product is over primes. Dividing the prime products for $J_2(n)$ and $\varphi(n)$ gives $J_2(n)/\varphi(n) = n \prod_{\ell | n} \frac{1 - \ell^{-2}}{1 - \ell^{-1}} = \psi_{\mathrm{D}}(n)$. For odd m, the new factor at 2 gives $\psi_{\mathrm{D}}(2m) = 2(1 + 1/2)\psi_{\mathrm{D}}(m) = 3\psi_{\mathrm{D}}(m)$. The case formula for $\varphi(n) b_U^{\mathbb{Q}}(n)$ therefore yields

$$\sum_{n \geq 1} J_2(n) b_U^{\mathbb{Q}}(n) = \frac{1}{2} \sum_{n \text{ odd}} \frac{\psi_{\mathrm{D}}(n)}{n^3} + \frac{3}{16} \sum_{(m,6)=1} (1 + \mathbf{1}_{5|m}) \frac{\psi_{\mathrm{D}}(m)}{m^3}.$$

The Euler factor of Z_ψ at ℓ is

$$Z_{\psi,\ell} = 1 + (1+\ell^{-1})\sum_{k\geq 1}\ell^{-2k} = \frac{1+\ell^{-3}}{1-\ell^{-2}}.$$

Since $Z_{\psi,\ell}-1 = O(\ell^{-2})$, the product converges absolutely. Substituting $1+\ell^{-3} = (1-\ell^{-6})/(1-\ell^{-3})$ gives $Z_\psi = \zeta(2)\zeta(3)/\zeta(6)$. The factors at $2,3,5$ are respectively $3/2, 7/6, 21/20$. Restricting to $(m,6)=1$ removes the Euler factors at 2 and 3. Among these terms, those divisible by 5 are obtained by subtracting the sum with the factor at 5 removed as well. Hence

$$\sum_{\substack{(m,6)=1\\ 5\mid m}}\frac{\psi_{\mathrm{D}}(m)}{m^3} = \frac{Z_\psi}{Z_{\psi,2}Z_{\psi,3}} - \frac{Z_\psi}{Z_{\psi,2}Z_{\psi,3}Z_{\psi,5}} = \frac{Z_\psi}{Z_{\psi,2}Z_{\psi,3}}\left(1-Z_{\psi,5}^{-1}\right).$$

The indicator adds this amount to the unrestricted sum over $(m,6)=1$, giving the multiplier $2-Z_{\psi,5}^{-1} = 22/21$. The odd levels contribute $Z_\psi/(2Z_{\psi,2})$. Combining both parts yields

$$\begin{aligned}\frac{2}{3}\sum_{n\geq 1}J_2(n)b_U^{\mathbb{Q}}(n) &= \frac{2}{3}Z_\psi\left(\frac{1}{2Z_{\psi,2}} + \frac{3(2-Z_{\psi,5}^{-1})}{16Z_{\psi,2}Z_{\psi,3}}\right)\\ &= \frac{2}{3}Z_\psi\left(\frac{1}{3}+\frac{11}{98}\right) = \frac{131}{441}\frac{\zeta(2)\zeta(3)}{\zeta(6)}.\end{aligned}$$

Here the even coefficient is $(3/16)(22/21)/((3/2)(7/6)) = 11/98$. Finally, $\zeta(2) = \pi^2/6$ and $\zeta(6) = \pi^6/945$ give $\zeta(2)/\zeta(6) = 945/(6\pi^4)$, and $(131/441)(945/6) = 655/14$. Both exact coefficients evaluate the series in a lower bound. Equality with an empirical limiting moment would also require an upper bound for the contribution of large rational indices. □

For a finite comparison, at a good inert prime p the cyclic subgroup of $\mathbb{F}_p^\times$ generated by $2,3,5$ has order $\mathrm{lcm}(\mathrm{ord}_p(2),\mathrm{ord}_p(3),\mathrm{ord}_p(5))$, where $\mathrm{ord}_p(a)$ is the multiplicative order modulo p. Dividing $p-1$ by this least common multiple gives $I_p^{\mathbb{Q}}$. At $X = 10^{14}$, the 332397 good inert primes are exactly the $p \leq 10^7$ with $p \equiv 3 \bmod 4$ and $p \neq 3$. On this set the finite sums are

$$\sum_p I_p^{\mathbb{Q}} = 391823, \qquad \sum_p (p+1)I_p^{\mathbb{Q}} = 1\,888\,920\,079\,192.$$

Dividing the first by 332397 gives the unweighted mean $1.17878019\ldots$. The second is the inert contribution to $S_1(X)$ by the local index identity. Dividing it by $\mathrm{Li}(10^{14})$ gives 0.58937729 to eight decimal places.

4.4 A splitting criterion for the Gaussian norm-one group

We now prove the refined bounds announced for the field-generating norm-one group in Section 4.1. Its generators are not rational, so the joint-density formula of Lemma 4.1 does not apply to this group. Proposition 4.5 will supply a new Frobenius criterion for the index inside the norm kernel. Lemma 4.2 then converts its density into the required moment bounds. Let $K = \mathbb{Q}(i) \subset \mathbb{C}$, and let $\Gamma \subset K^\times$ be a fixed finitely generated group of rank $r > 1$ with $\gamma\bar{\gamma} = 1$ for every $\gamma \in \Gamma$. The division fields K_n and the unrestricted model moment M_1 now refer to this group over K. At a good inert prime p, write

$$T_p = \{x \in \mathbb{F}_{p^2}^\times : x^{p+1} = 1\}, \quad j_p = [T_p : \Gamma_{(p)}], \qquad I_{(p)} = (p-1)j_p.$$

The group T_p is the kernel of the finite-field norm to $\mathbb{F}_p^\times$, cyclic of order $p+1$. For $n \geq 1$, write $T_p^n = \{x^n : x \in T_p\}$ for its subgroup of n-th powers. Complex conjugation in $\mathbb{C}$ is denoted by c. The next result identifies divisibility of j_p with a Frobenius condition in $K_n/\mathbb{Q}$, allowing the positive divisor truncation to retain this additional local index.

Proposition 4.5 (Norm-one coefficient)**.** *Fix $n \geq 1$. The extension $K_n/\mathbb{Q}$ is Galois, and complex conjugation c is central in its Galois group. For every good inert rational prime $p \nmid n$ unramified in K_n,*

$$n \mid j_p \quad \Longleftrightarrow \quad \mathrm{Frob}_{p,K_n/\mathbb{Q}} = \{c\}.$$

The density among all rational primes of good inert primes with $n \mid j_p$ is $1/[K_n : \mathbb{Q}]$. Consequently for every fixed $T \geq 1$ the contribution of the inert ideals with $I_{(p)} > T$ to $S_1(X)/\pi_K(X)$ has lower limit at least

$$\sum_{n \geq 1} \frac{\varphi(n)}{[K_n : \mathbb{Q}]} = \frac{M_1}{2}.$$

The lower limit of the full mean is at least $3M_1/2$. With V_1 as defined in Theorem 1.3, $\liminf_{X\to\infty} V_1(X,\nu) \geq M_1/2$ for every nonnegative measure ν of finite first moment. For the three Gaussian generators in Section 4.1, $M_1/2 \geq 251/432$, and the second-moment lower bound is $\liminf_{X\to\infty}(\log X)S_2(X)/X^{3/2} \geq 329/648$.

Proof. If $\beta^n = \gamma \in \Gamma$, then $|\beta|^n = |\gamma| = 1$. A $\mathbb{Q}$-embedding of K_n restricts to the identity or conjugation on K, so it sends β to some $\xi\beta$ or $\xi\beta^{-1}$, with $\xi \in \mu_n$. These elements all belong to K_n, as do the conjugates of i and of μ_n. Thus the finite separable extension $K_n/\mathbb{Q}$ is normal. For $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q})$ the same description gives $|\sigma(\beta)| = 1$, whence

$$c\sigma(\beta) = \overline{\sigma(\beta)} = \sigma(\beta)^{-1} = \sigma(\beta^{-1}) = \sigma c(\beta).$$

The same identity holds on roots of unity, and the two restrictions commute on K, whose Galois group has order two. They therefore commute on the field generated by these elements. This proves that $\{c\}$ is a conjugacy class.

Omit the finitely many primes of bad reduction, primes ramified in $K_n/\mathbb{Q}$, and primes dividing n. At an inert prime choose an upper prime of K_n, and write ϕ for its arithmetic Frobenius over p. If u_p generates the cyclic group T_p of order $p+1$, then $\Gamma_{(p)} = \langle u_p^{j_p} \rangle$ and $j_p \mid p+1$. When $n \mid p+1$, the containment in $T_p^n = \langle u_p^n \rangle$ is equivalent to $j_p \equiv nk \bmod (p+1)$ for some integer k, or equivalently to $n \mid j_p$. Hence

$$n \mid j_p \quad \Longleftrightarrow \quad n \mid p+1 \text{ and } \Gamma_{(p)} \subset T_p^n.$$

Suppose $n \mid j_p$. As $n \mid p+1$, all n distinct n-th roots of unity lie in T_p after reduction. Each reduced generator has one n-th root in T_p by the power condition, and all its other roots differ by these roots of unity. Thus the residue x of each generator root satisfies $x^p = x^{-1}$. Inertness gives $\phi(\gamma) = \bar{\gamma} = \gamma^{-1}$, so $\phi(\beta)$ and β^{-1} are roots of the same polynomial $Z^n - \gamma^{-1}$ and have the same residue. Its reduction is separable because $p \nmid n$ and γ is a unit. Hence $\phi(\beta) = \beta^{-1}$. The same reasoning for roots of unity gives $\phi = c$ on the field generators.

Conversely, if $\phi = c$, it restricts to the nonidentity automorphism of K, so p is inert. The residues of the roots and roots of unity satisfy $x^p = x^{-1}$. Thus $x^{p^2} = x$, which puts them in $\mathbb{F}_{p^2}$, and $x^{p+1} = 1$ puts them in T_p. The n distinct reduced roots of unity give $n \mid |T_p| = p+1$, and the roots of the generators give $\Gamma_{(p)} \subset T_p^n$. This proves the converse. Chebotarev applied to the singleton class $\{c\}$ now gives density $1/[K_n : \mathbb{Q}]$ among all rational primes.

Truncate $j_p = \sum_{n \mid j_p} \varphi(n)$ at $n \leq n_{\max}$. After discarding $p \leq T+1$, multiply by $p-1$, so every term comes from an ideal with $I_{(p)} > T$. For a fixed n, the density just proved and Lemma 4.2 with $\beta = 1$ give

$$\sum_{\substack{p \leq Y \text{ good inert} \\ n \mid j_p}} (p-1) = \left(\frac{1}{2[K_n : \mathbb{Q}]} + o(1)\right) \frac{Y^2}{\log Y} = \left(\frac{1}{[K_n : \mathbb{Q}]} + o(1)\right) \frac{X}{\log X}, \qquad Y = \sqrt{X}.$$

The subtraction of one per prime costs $O(Y)$, and deleting the fixed initial segment costs $O_T(1)$. Sum the finite truncation, divide by $\pi_K(X)$, then let $n_{\max} \to \infty$. Since $[K_n : \mathbb{Q}] = 2[K_n : K]$ and $b(n) = 1/[K_n : K]$, the resulting coefficient is

$$\sum_{n\geq 1} \frac{\varphi(n)}{[K_n : \mathbb{Q}]} = \frac{1}{2} \sum_{n\geq 1} \varphi(n) b(n) = \frac{M_1}{2}.$$

The last equality is the convergent model-moment identity in Corollary 1.2 with $s = 1 < r$. The degree-one estimate in Section 4.2 applies to this group over K. Adding its lower bound M_1 to the disjoint inert bound $M_1/2$ gives $3M_1/2$. The assertion for V_1 follows by subtracting the first-moment tail of ν and sending $T \to \infty$.

For the explicit generators $g_j = \varpi_j^2/q_j$, where $q_j = 5, 13, 17$, one square root is $\varpi_j/\sqrt{q_j}$. Adjoining the three roots to K is therefore equivalent to adjoining $\sqrt{5}, \sqrt{13}, \sqrt{17}$. A product $5^{e_1}13^{e_2}17^{e_3}$ can be a rational square only if all three exponents are even, by their respective valuations. Kummer theory at $n = 2$ gives $[\mathbb{Q}(\sqrt{5}, \sqrt{13}, \sqrt{17}) : \mathbb{Q}] = 2^3$. This field is real and $\mathbb{Q}(i) \cap \mathbb{R} = \mathbb{Q}$, so $[K_2 : \mathbb{Q}] = 2 \cdot 2^3 = 16$.

At level three the base $K(\mu_3) = \mathbb{Q}(\mu_{12})$ has degree $\varphi(12) = 4$ and is unramified over $5, 13, 17$. At a prime of this base above (ϖ_j), the valuation of $\prod_k g_k^{e_k}$ is e_j, because the ramification index is one and $v_{(\varpi_j)}(g_k) = \delta_{jk}$. If the product is a cube then $3 \mid e_j$ for each j. The radical classes thus generate a group of order 3^3, giving $[K_3 : \mathbb{Q}] = 4 \cdot 3^3 = 108$ by Kummer theory [5, v5.10, Theorem 5.30].

Since $[K_1 : \mathbb{Q}] = 2$, the densities at $n = 1, 2, 3$ are $1/2, 1/16, 1/108$. Weighting by $1, 1, 2$ gives $1/2+1/16+2/108 = 251/432$. At order two, use $j_p^2 = \sum_{n|j_p} J_2(n)$ and $I_{(p)}^2 = (p-1)^2 j_p^2$. For each of these three levels the cost of replacing $(p-1)^2$ by p^2 is at most $2Y\pi(Y) = O(Y^2) = o(Y^3/\log Y)$. Lemma 4.2 with $\beta = 2$ weights the level density by $1/3$, and $Y^3/\log Y = 2X^{3/2}/\log X$. Thus the three Jordan weights $1, 3, 8$ give the lower coefficient $\frac{2}{3}(1/2 + 3/16 + 8/108) = 329/648$, already for the inert sum.

□

An asymptotic below weight one requires an additional mean-value hypothesis on j_p. For $0 < s < 1$, suppose $\sum_{p\leq y}^{\text{in}} j_p^s = (b + o(1))y/\log y$ with $b > 0$, where the sum is over good inert rational primes. Lemma 4.2 with $\beta = s$ gives $(b/(1+s) + o(1))Y^{1+s}/\log Y$ for the sum with weight $p^s j_p^s$. Since $(p-1)^s/p^s \to 1$ and the summands are nonnegative, the same asymptotic holds with $p-1$ in place of p. With $Y = \sqrt{X}$ this gives the conditional formula

$$\frac{1}{\pi_K(X)} \sum_{p\leq\sqrt{X}}^{\text{in}} I_{(p)}^s = \left(\frac{2b}{1+s} + o(1)\right) X^{-(1-s)/2},$$

where the factor two comes from $\log Y = (\log X)/2$.

Generators in a proper subfield. The subfield mechanism in Section 4.1 also extends to a tower of number fields $K/K_0/\mathbb{Q}$ without a normality assumption. Let $\Gamma \subset K_0^\times$ be fixed and finitely generated of positive rank. Consider a rational prime p unramified in K and good for Γ at every prime above it, with ideals $\mathfrak{p} \mid \mathfrak{q} \mid p$ in $K, K_0, \mathbb{Q}$, respectively. Let $k_\mathfrak{q} = \mathcal{O}_{K_0}/\mathfrak{q}$, and write $I_\mathfrak{q} = [k_\mathfrak{q}^\times : \mathrm{red}_\mathfrak{q}(\Gamma)]$ for the residual index over K_0. Write $f = \deg(\mathfrak{p})$ and $e = \deg(\mathfrak{q})$ for their absolute residue degrees. Then $k_\mathfrak{q} \hookrightarrow k_\mathfrak{p}$ gives $f = e[k_\mathfrak{p} : k_\mathfrak{q}]$. Reduction at $\mathfrak{p}$ factors through this injection, so the two images of Γ have the same order. By (1),

$$I_\mathfrak{p} = \frac{p^f - 1}{p^e - 1} I_\mathfrak{q}.$$

If $K_0 \subsetneq K$, a set of rational primes of positive density realizes $e = 1$ and a fixed $f > 1$. To see this, let $\widetilde{K}$ be a Galois closure of $K/\mathbb{Q}$, and put

$$G_{\mathrm{cl}} = \mathrm{Gal}(\widetilde{K}/\mathbb{Q}), \qquad H = \mathrm{Gal}(\widetilde{K}/K) \subsetneq H_0 = \mathrm{Gal}(\widetilde{K}/K_0).$$

Choose $g \in H_0 \setminus H$. Chebotarev gives positive density for its conjugacy class, and deleting the finitely many bad primes preserves this density. For each remaining unramified prime in that class, choose a prime $\mathfrak{R}$ of $\widetilde{K}$ with Frobenius exactly g, and let $\mathfrak{p}, \mathfrak{q}$ be its restrictions. The decomposition group at $\mathfrak{R}$ over $\mathbb{Q}$ is $\langle g \rangle$. Over K and K_0 its subgroups are $\langle g \rangle \cap H$ and $\langle g \rangle \cap H_0$, respectively. Unramifiedness makes their orders equal to the corresponding residue degrees [2, Ch. 8]. By the tower formula for residue fields,

$$[k_{\mathfrak{p}} : \mathbb{F}_p] = \frac{|\langle g \rangle|}{|\langle g \rangle \cap H|} = f > 1, \qquad [k_{\mathfrak{q}} : \mathbb{F}_p] = \frac{|\langle g \rangle|}{|\langle g \rangle \cap H_0|} = 1.$$

The strict inequality follows from $g \notin H$, and the second equality from $g \in H_0$. Each such rational p therefore supplies at least one ideal of norm p^f with $I_{\mathfrak{p}} \geq (p^f - 1)/(p - 1) \geq p^{f-1}$. Counting those p in $X^{1/f}/2 < p \leq X^{1/f}$ gives the exponent $a_f(s)$ of (8). The all-class coefficient $c_K^\sharp$ above is stated for rational generators and Galois $K/\mathbb{Q}$.

5 Admissible ranks and the weight-one obstruction

Theorem 1.1 gives a convergence range in terms of r, θ and σ, while Section 4 exhibits arithmetic obstructions at larger weights. We now turn the parameter range into a criterion for the least rank needed at a prescribed weight, illustrate the effect of different common zero bounds, and distinguish the limit of the estimate from the obstruction at weight one.

5.1 The rank required for a prescribed weight

Dividing the two fractions in (4) gives

$$\sigma_* = \frac{r(1-\theta) - \theta}{r(1-\theta) + 1} = 1 - \frac{1 + \theta}{r(1-\theta) + 1}. \tag{54}$$

Fix $1/2 \leq \theta < 1$ and $0 \leq \sigma < 1$. The saving in (5), before its arbitrarily small loss, is

$$\delta_* - u\sigma = \frac{r(1-\theta)(1-\sigma) - \theta - \sigma}{2r + 1}.$$

It is positive exactly when $r(1-\theta)(1-\sigma) > \theta + \sigma$, which also implies $\theta < r/(r+1)$. Thus, assuming $\mathcal{Z}(\theta)$, the least rank for which Theorem 1.1 gives a power saving at weight σ is

$$r_{\min}(\theta, \sigma) = 1 + \left\lfloor \frac{\theta + \sigma}{(1-\theta)(1-\sigma)} \right\rfloor. \tag{55}$$

The strict inequality excludes the endpoint. Under GRH the condition becomes $r > (1+2\sigma)/(1-\sigma)$, equivalently $\sigma < (r-1)/(r+2)$. At zero weight it is $r > \theta/(1-\theta)$. For a single prescribed index over $\mathbb{Q}$ without an additional filter, Pappalardi and Susa [19, p. 322] had identified the corresponding threshold $\theta < r/(r+1)$. Here (55) applies to the full weighted norm.

In rank one the hypotheses would require $1/2 \leq \theta < 1/2$. Substituting $r = 1, \theta = 1/2$ in the balance gives $\delta_* = 0$ even at zero weight. This is a limitation of the present power-saving estimate. The logarithmic distribution estimate of Moree, Perucca and Sgobba includes torsion-free groups of rank one [40, Theorem 1], and Hooley's theorem gives the primitive-root density for an admissible fixed rational integer under its own GRH hypotheses [9]. A power-saving estimate for all sets of indices of a single rational generator requires an additional input.

5.2 Illustrations with common zero bounds

At $\sigma = 0$, the rank criterion gives the following values. The last two rows take the statements of the cited preprints as additional hypotheses. In the third row, θ_{Liu} denotes the bound called θ_G in that source.

Common upper bound	Least rank	Source of the input
$1/2$	2	GRH for all composita E_n
$7/8$	8	Hu, v2, Theorem 1.2 [63]
$\theta_{\mathrm{Liu}} \approx 0.87333$	7	Liu, v1, Theorem 7.33 [64]

Both cited statements cover the trivial unitary Hecke character of every number field. Its L-function over E_n is ζ_{E_n}, so a boundary common to all number fields would supply $\mathcal{Z}(\theta)$ for every level n. These are illustrations of the family hypothesis in Theorem 1.1; we use the preprints as stated, without an independent verification of their analytic proofs.

For $r = 8$ and $\theta = 7/8$, (4) gives $u = 2/17$, $\delta_* = 1/136$ and $\sigma_* = 1/16$. For the Liu input, the stated enclosure is

$$0.8733326374459049352 < \theta_{\mathrm{Liu}} < 0.8733326374459051924.$$

Substituting this enclosure into (55) gives $r_{\min}(\theta_{\mathrm{Liu}}, 0) = 7$. At $r = 7$,

$$u = \frac{8 - 7\theta}{15}, \qquad \delta_* = \frac{7 - 8\theta}{15}, \qquad \sigma_* = \frac{7 - 8\theta}{8 - 7\theta}.$$

At $\theta = \theta_{\mathrm{Liu}}$, these are approximately 0.12577810, 0.00088926 and 0.00707007, respectively. Thus this least rank permits a positive but narrow weight range; the rank criterion alone does not describe the size of the saving.

5.3 The method's ceiling and the arithmetic obstruction

For every fixed $\theta < 1$, (54) gives $\sigma_* \to 1$ as $r \to \infty$. Nevertheless, the estimate cannot be extended to weight one uniformly over the groups and fields in the theorem. For any $r \geq 2$, take r distinct rational primes as generators in $K = \mathbb{Q}(i)$ and use the unrestricted count. Their valuations give rank r, and (6) gives a finite first moment for D. Theorem 1.3 and Corollary 4.4, with $\nu = D$, give

$$\liminf_{X \to \infty} \sum_{t \geq 1} t |P_X(t) - D(t)| \geq \frac{(1 - 2^{-r})\zeta(r)}{2} > \frac{1}{2}.$$

With weight t^σ, the discrepancy tends to $+\infty$ for every $\sigma > 1$. This is an arithmetic obstruction supplied by higher-degree ideals.

The earlier ceiling σ_* comes from the balance (40) between the single-level error and Lemma 2.2, whose exponent is $\kappa_r = 1 + 1/r$. The argument does not decide the interval $\sigma_* \leq \sigma < 1$. For $K = \mathbb{Q}$, every prime ideal has degree one, so the higher-degree mechanism is absent. Sections 4.3 and 4.4 describe the classwise scales below one and the additional moment hypotheses needed for asymptotics. The parameter ceiling and the weight-one obstruction therefore mark different limits: the former belongs to the estimate, while the latter prevents a general convergence theorem at the first moment.

6 Conclusions

The two main results distinguish quantitative control of a fixed group's index distribution from control of its positive moments. We obtain a power saving for the full weighted distribution

and unconditional counterexamples to the all-prime-ideal formulation of Ambrose's moment heuristic. Under GRH, the Gaussian examples have convergent index distributions while their normalized means remain separated from the finite model first moment.

The quantitative advance over the distribution theorem of Moree, Perucca and Sgobba [40, Theorem 1] is the combination of a power-saving rate and positive power weights. Their uniform estimate for arbitrary sets of indices gives an unweighted normalized error $O((\log X)^{-r/(r+1)})$. Under GRH, Theorem 1.1 gives

$$\sum_{t\geq 1} t^{\sigma}|P_{X,C}(t) - D_C(t)| \ll_{K,F,\Gamma,\sigma,\varepsilon} X^{-\frac{r-1-(r+2)\sigma}{2(2r+1)}+\varepsilon}, \qquad r \geq 2, \quad 0 \leq \sigma < \frac{r-1}{r+2}.$$

Section 5 makes this range explicit as the least-rank criterion (55); under GRH it is $r > (1+2\sigma)/(1-\sigma)$. For example, at rank three and zero weight the respective rates are $O((\log X)^{-3/4})$ and $O(X^{-1/7+\varepsilon})$; the new estimate also controls positive weights below $2/5$. It is uniform in the Frobenius filter and permits torsion. The earlier theorem includes rank one, which remains outside our power-saving range.

The algebraic coefficients agree with the earlier model for torsion-free groups. The common-half-plane threshold $\theta < r/(r+1)$ and the cutoff by divisor size also have rational precedents [19, 23]. The additional conclusion here is control of the sum of all absolute errors with an increasing power weight, over a general number field. Corollary 1.2 turns this estimate into convergent empirical moments with explicit Jordan-series constants. The model moments are finite unconditionally for $0 < s < r$; empirical convergence is established in the smaller conditional range $0 < s < \sigma_*$.

The unconditional result rules out several of the proposed moment scales. For rational generators of rank $r > 1$ in a nontrivial finite Galois extension of $\mathbb{Q}$, each occurring residue degree $f > 1$ gives

$$S_s(X) \gg \frac{X^{a_f(s)}}{\log X}, \qquad a_f(s) = \frac{1+(f-1)s}{f}.$$

Comparison with the three proposed scales disproves Ambrose's heuristic [4, §4.2, (4.2)] throughout $1 < s < 1 + f(r-1)$, when prime ideals of every residue degree are counted. In both Gaussian rank-three examples this interval is $1 < s < 5$. This concerns fixed groups; Ambrose's theorems on averages over generating tuples [44] have different quantifiers.

At weight one the conclusion concerns the coefficient of the mean. Section 4.2 proves, for any fixed group of rank greater than one over any number field, that the degree-one part has normalized lower limit at least M_1. Under the rational-generator hypotheses above, Theorem 4.3 adds the disjoint higher-degree contribution and gives

$$\liminf_{X\to\infty} \frac{S_1(X)}{\pi_K(X)} \geq M_1 + c_K^{\sharp}(\Gamma) > M_1.$$

The constant $c_K^{\sharp}(\Gamma)$ is finite for $r > 1$ and infinite for $r = 1$. More generally, Theorem 4.3 gives an explicit Jordan-series lower coefficient in each Frobenius class for every positive moment order. This retains the joint dependence of the rational index and Frobenius through the coefficients $b_U^{\mathbb{Q}}(n)$. Thus a finite model moment does not force convergence of the empirical mean to that moment. The scale $\mathrm{Li}(X)$ at $s = 1 < r$ is not excluded by this lower bound.

The explicit coefficients quantify the effect. For $\Gamma = \langle 2, 3, 5\rangle$ over $\mathbb{Q}(i)$, Corollary 4.4 evaluates the first-moment lower-bound constant as $(5887/12000)\zeta(3)$. Its second-moment coefficient is $655\zeta(3)/(14\pi^4) = 0.577349508443\ldots$ at the scale $X^{3/2}/\log X$. These are exact values of coefficients in proved lower bounds. Proposition 4.5 supplies a separate Frobenius criterion for the explicit norm-one group that generates $\mathbb{Q}(i)$ as a field. The density $1/[K_n : \mathbb{Q}]$ gives an inert mean contribution of at least $M_1/2 \geq 251/432$, a full-mean lower limit of at least

$3M_1/2$, and a second-moment coefficient at least $329/648$. The final argument of Section 4.4 also extends the growth mechanism to generators in a proper subfield, without requiring $K/\mathbb{Q}$ to be Galois.

The weight ceiling σ_* belongs to the present large-index estimate. The obstruction at weight one is arithmetic: in these examples it prevents convergence in first-moment weighted variation, and the discrepancy diverges at every larger weight against any nonnegative measure of finite first moment. The interval $\sigma_* \le \sigma < 1$, power-saving rates at rank one, and classwise asymptotics beyond the conditional moment range require further large-index control. Improving that control could enlarge the convergence range, but cannot remove the first-moment defect proved here.

Use of artificial intelligence

The author directed the investigation, selected the questions and requested revisions and detailed checks of the arguments. OpenAI ChatGPT and Codex were used extensively for mathematical exploration, the development and checking of arguments, drafting and revising the manuscript, checking references, and preparing computational checks. The author used Anthropic's Claude for several rounds of independent review of the arguments and computations.

References

[1] Günther Frei and Peter Roquette, editors. *Emil Artin und Helmut Hasse. Die Korrespondenz 1923–1934*. Universitätsverlag Göttingen, 2008. With contributions by Franz Lemmermeyer. DOI 10.17875/gup2008-61.

[2] James S. Milne. Algebraic number theory. Course notes, version 3.08, 2020. Author's text.

[3] Samuel S. Wagstaff, Jr. Pseudoprimes and a generalization of Artin's conjecture. *Acta Arithmetica*, 41(2):141–150, 1982. DOI 10.4064/aa-41-2-141-150.

[4] Christopher Daniel Ambrose. *On Artin's Primitive Root Conjecture*. PhD thesis, Georg-August-Universität Göttingen, 2014. DOI 10.53846/goediss-4538.

[5] James S. Milne. Fields and Galois theory. Course notes, version 5.10, 2022. Author's text.

[6] Tom M. Apostol. *Introduction to Analytic Number Theory*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1976. DOI 10.1007/978-1-4757-5579-4.

[7] James S. Milne. Class field theory. Course notes, version 4.03, 2020. Author's text.

[8] Jeffrey C. Lagarias and Andrew M. Odlyzko. Effective versions of the Chebotarev density theorem. In Albrecht Fröhlich, editor, *Algebraic Number Fields: L-Functions and Galois Properties*, pages 409–464. Academic Press, 1977. Online text.

[9] Christopher Hooley. On Artin's conjecture. *Journal für die reine und angewandte Mathematik*, 225:209–220, 1967. DOI 10.1515/crll.1967.225.209.

[10] George Cooke and Peter J. Weinberger. On the construction of division chains in algebraic number rings, with applications to SL_2. *Communications in Algebra*, 3(6):481–524, 1975. DOI 10.1080/00927877508822057.

[11] Hendrik W. Lenstra, Jr. On Artin's conjecture and Euclid's algorithm in global fields. *Inventiones mathematicae*, 42(1):201–224, 1977. DOI 10.1007/bf01389788.

[12] Leo Murata. A problem analogous to Artin's conjecture for primitive roots and its applications. *Archiv der Mathematik*, 57(6):555–565, 1991. DOI 10.1007/bf01199060.

[13] Pieter Moree. Artin's primitive root conjecture: a survey. *Integers*, 12(6):1305–1416, 2012. DOI 10.1515/integers-2012-0043.

[14] Francesco Pappalardi. On the order of finitely generated subgroups of $\mathbb{Q}^*$ (mod p) and divisors of $p-1$. *Journal of Number Theory*, 57(2):207–222, 1996. DOI 10.1006/jnth.1996.0044.

[15] Francesco Pappalardi. On the r-rank Artin conjecture. *Mathematics of Computation*, 66(218):853–868, 1997. DOI 10.1090/s0025-5718-97-00805-3.

[16] Leonardo Cangelmi and Francesco Pappalardi. On the r-rank Artin conjecture, II. *Journal of Number Theory*, 75(1):120–132, 1999. DOI 10.1006/jnth.1998.2319.

[17] Rajiv Gupta and M. Ram Murty. A remark on Artin's conjecture. *Inventiones Mathematicae*, 78(1):127–130, 1984. DOI 10.1007/bf01388719.

[18] D. R. Heath-Brown. Artin's conjecture for primitive roots. *The Quarterly Journal of Mathematics*, 37(1):27–38, 1986. DOI 10.1093/qmath/37.1.27.

[19] Francesco Pappalardi and Andrea Susa. An analogue of Artin's conjecture for multiplicative subgroups of the rationals. *Archiv der Mathematik*, 101(4):319–330, 2013. DOI 10.1007/s00013-013-0563-7.

[20] Herish Abdullah, Andam Ali Mustafa, and Francesco Pappalardi. Density of the quasi r-rank Artin problem. *Functiones et Approximatio Commentarii Mathematici*, 65(1):73–93, 2021. DOI 10.7169/facm/1902.

[21] Pieter Moree and Peter Stevenhagen. Computing higher rank primitive root densities. *Acta Arithmetica*, 163(1):15–32, 2014. DOI 10.4064/aa163-1-2.

[22] Amir Akbary and Milad Fakhari. Constants for Artin-like problems in Kummer and division fields. *Research in Number Theory*, 10:article 22, 2024. DOI 10.1007/s40993-024-00509-6.

[23] Adam Tyler Felix. *Variations on Artin's Primitive Root Conjecture*. PhD thesis, Queen's University, 2011. Queen's University repository.

[24] Francesco Pappalardi. On Hooley's theorem with weights. *Rendiconti del Seminario Matematico, Università e Politecnico di Torino*, 53(4):375–388, 1995. Journal text.

[25] Eric Bach, Richard Lukes, Jeffrey Shallit, and H. C. Williams. Results and estimates on pseudopowers. *Mathematics of Computation*, 65(216):1737–1747, 1996. DOI 10.1090/S0025-5718-96-00762-4.

[26] O. M. Fomenko. Class numbers of indefinite binary quadratic forms and the residual indices of integers modulo p. *Journal of Mathematical Sciences*, 122(6):3685–3698, 2004. DOI 10.1023/b:joth.0000035245.77356.76.

[27] Adam Tyler Felix and M. Ram Murty. A problem of Fomenko's related to Artin's conjecture. *International Journal of Number Theory*, 8(7):1687–1723, 2012. DOI 10.1142/s1793042112500984.

[28] Adam Tyler Felix. Higher rank generalizations of Fomenko's conjecture. *Journal of Number Theory*, 133(5):1738–1751, 2013. DOI 10.1016/j.jnt.2012.09.008.

[29] Pieter Moree. On the distribution of the order and index of g mod p over residue classes, I. *Journal of Number Theory*, 114(2):238–271, 2005. DOI 10.1016/j.jnt.2004.09.004.

[30] Pieter Moree. On the distribution of the order and index of g mod p over residue classes, II. *Journal of Number Theory*, 117(2):330–354, 2006. DOI 10.1016/j.jnt.2005.06.006.

[31] Pieter Moree. On the distribution of the order and index of g mod p over residue classes, III. *Journal of Number Theory*, 120(1):132–160, 2006. DOI 10.1016/j.jnt.2005.11.005.

[32] Adam Tyler Felix. The index of a modulo p. In *SCHOLAR: A Scientific Celebration Highlighting Open Lines of Arithmetic Research*, volume 655 of *Contemporary Mathematics*, pages 83–96. American Mathematical Society, 2015. DOI 10.1090/conm/655/13228.

[33] Volker Ziegler. On the distribution of the order of number field elements modulo prime ideals. *Uniform Distribution Theory*, 1(1):65–85, 2006. Journal text.

[34] Pietro Sgobba. On the distribution of the order and index for the reductions of algebraic numbers. *Journal of Number Theory*, 223:132–152, 2021. DOI 10.1016/j.jnt.2020.11.008.

[35] Olli Järviniemi and Antonella Perucca. Unified treatment of Artin-type problems. *Research in Number Theory*, 9:article 10, 2023. DOI 10.1007/s40993-022-00418-6.

[36] Olli Järviniemi, Antonella Perucca, and Pietro Sgobba. Unified treatment of Artin-type problems II. *Research in Number Theory*, 11:article 42, 2025. DOI 10.1007/s40993-025-00620-2.

[37] Antonella Perucca and Igor E. Shparlinski. Uniform bounds for the density in Artin's conjecture on primitive roots. *Bulletin of the London Mathematical Society*, 57(3):978–991, 2025. DOI 10.1112/blms.70011.

[38] Antonella Perucca. A closed formula for the density in Artin's primitive root conjecture over number fields. *Bulletin of the London Mathematical Society*, 58(7):article e70448, 2026. DOI 10.1112/blms.70448.

[39] Chi Wa Chan. Uniform bounds for the density in Artin's conjecture for quadratic number fields. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 96:29–72, 2026. DOI 10.1007/s12188-026-00300-7.

[40] Pieter Moree, Antonella Perucca, and Pietro Sgobba. The distribution of the multiplicative index of algebraic numbers over residue classes. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 94(1):1–17, 2024. DOI 10.1007/s12188-024-00276-2.

[41] Pietro Sgobba. Unconditional results for Artin-type problems over number fields. arXiv:2508.08996v1, 2025. DOI 10.48550/arXiv.2508.08996.

[42] Morris Goldfeld. Artin's conjecture on the average. *Mathematika*, 15(2):223–226, 1968. DOI 10.1112/s0025579300002606.

[43] P. J. Stephens. An average result for Artin's conjecture. *Mathematika*, 16(2):178–188, 1969. DOI 10.1112/S0025579300008159.

[44] Christopher Ambrose. Artin's primitive root conjecture and a problem of Rohrlich. *Mathematical Proceedings of the Cambridge Philosophical Society*, 157(1):79–99, 2014. DOI 10.1017/s0305004114000206.

[45] Amir Akbary and Adam Tyler Felix. On the average value of a function of the residual index. In *Geometry, Algebra, Number Theory, and Their Information Technology Applications*, volume 251 of *Springer Proceedings in Mathematics and Statistics*, pages 19–37. Springer, 2018. DOI 10.1007/978-3-319-97379-1_2.

[46] Lorenzo Menici and Cihan Pehlivan. Average r-rank Artin conjecture. *Acta Arithmetica*, 174(3):255–276, 2016. DOI 10.4064/aa8258-4-2016.

[47] Pär Kurlberg and Carl Pomerance. On a problem of Arnold: the average multiplicative order of a given integer. *Algebra & Number Theory*, 7(4):981–999, 2013. DOI 10.2140/ant.2013.7.981.

[48] Cihan Pehlivan. The average multiplicative order of a finitely generated subgroup of the rationals modulo primes. *International Journal of Number Theory*, 12(8):2147–2158, 2016. DOI 10.1142/s1793042116501281, arXiv:1504.01550v2.

[49] Masaru Ishikawa and Yoshiyuki Kitaoka. On the distribution of units modulo prime ideals in real quadratic fields. *Journal für die reine und angewandte Mathematik*, 494:65–72, 1998. DOI 10.1515/crll.1998.011.

[50] Yen-Mei J. Chen, Yoshiyuki Kitaoka, and Jing Yu. Distribution of units of real quadratic number fields. *Nagoya Mathematical Journal*, 158:167–184, 2000. DOI 10.1017/s0027763000007364.

[51] Hans Roskam. Artin's primitive root conjecture for quadratic fields. *Journal de théorie des nombres de Bordeaux*, 14(1):287–324, 2002. DOI 10.5802/jtnb.360.

[52] Joseph Cohen. Primitive roots in quadratic fields, II. *Journal of Number Theory*, 124(2):429–441, 2007. DOI 10.1016/j.jnt.2006.10.001, arXiv:math/0501120.

[53] Noam Kimmel. Artin's primitive root conjecture in number fields and for matrices. *Acta Arithmetica*, 216(4):329–348, 2024. DOI 10.4064/aa230810-29-6.

[54] Antonella Perucca and Pietro Sgobba. Kummer theory for number fields and the reductions of algebraic numbers. *International Journal of Number Theory*, 15(8):1617–1633, 2019. DOI 10.1142/s179304211950091x.

[55] Pietro Sgobba. Divisibility conditions on the order of the reductions of algebraic numbers. *Mathematics of Computation*, 92(343):2281–2305, 2023. DOI 10.1090/mcom/3848.

[56] C. R. Matthews. Counting points modulo p for some finitely generated subgroups of algebraic groups. *Bulletin of the London Mathematical Society*, 14(2):149–154, 1982. DOI 10.1112/blms/14.2.149.

[57] Władysław Narkiewicz. A note on Artin's conjecture in algebraic number fields. *Journal für die reine und angewandte Mathematik*, 381:110–115, 1987. DOI 10.1515/crll.1987.381.110.

[58] Hester Graves. Growth results and Euclidean ideals. *Journal of Number Theory*, 133(8):2756–2769, 2013. DOI 10.1016/j.jnt.2012.12.016, arXiv:1008.2479v1.

[59] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Publications Mathématiques de l'IHÉS*, 54:123–201, 1981. DOI 10.1007/BF02698692.

[60] Alina Carmen Cojocaru. Questions about the reductions modulo primes of an elliptic curve. In Hershy Kisilevsky and Eyal Z. Goren, editors, *Number Theory*, volume 36 of *CRM Proceedings and Lecture Notes*, pages 61–79. American Mathematical Society, 2004. DOI 10.1090/crmp/036/05.

[61] Joseph Cohen. *Primitive Roots in Algebraic Number Fields*. PhD thesis, Technion–Israel Institute of Technology, 2004. Thesis.

[62] Lawrence C. Washington. *Introduction to Cyclotomic Fields*, volume 83 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 1997. Chapter 3, Dirichlet Characters.

[63] Boyang Hu. A seven-eighths zero-free half-plane for unitary Weil L-functions. Hexagon preprint 2610.00216v2, November 7, 2026. Version cited.

[64] Baiying Liu. Mixed character moments and a zero-free half-plane for unitary Hecke L-functions. Hexagon preprint 2611.00741v1, November 20, 2026. Version cited.