hexagon:2611.00956v1

Weighted distribution of residual indices and the contribution of higher-degree primes

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

Abstract

The residual index at a prime ideal of good reduction counts the cosets of the reduced subgroup in the multiplicative residue group. For a fixed finitely generated group of rank r in a number field, we estimate index frequencies up to norm X, uniformly over conditions on the Frobenius action on residue fields in a fixed finite Galois extension. Adjoin roots of unity and radicals of the generators to this extension. If the nontrivial zeta zeros of the resulting fields have real parts uniformly below $r/(r+1)$, the sum of absolute frequency errors weighted by small powers of the index admits a power saving. Model moments are finite for positive orders below r. Under the generalized Riemann hypothesis, empirical moments converge to them for positive orders below $(r-1)/(r+2)$.

For rational generators in a nontrivial finite Galois extension of the rationals, we give an unconditional lower bound for the contribution of higher-degree ideals to the mean above any fixed index cutoff. This contribution diverges in rank one. For two rank-three groups over the Gaussian rationals, the sum of squared indices divided by $X^{3/2}/\log X$ has lower limit at least $329/648$. This growth exceeds the scale in the literal form of Ambrose's prime-ideal heuristic.

1 Introduction

Artin's primitive root problem, formulated in his correspondence with Hasse [1, §17.2], asks how often a fixed rational number is a primitive root modulo a prime. Knowing the density for each index leaves open how often large indices occur and how much they contribute to the mean. Even a set of density zero can determine the growth of a sum of positive powers of the index.

1.1 The fixed-group moment problem

Let K be a number field with ring of integers $\mathcal{O}_K$, and let $\Gamma \subset K^\times$ be finitely generated with torsion subgroup Γ_{tor} and free rank $r \geq 1$. Write N for the absolute ideal norm. For $\mathfrak{p} \mid p$ put $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$, $\deg(\mathfrak{p}) = [k_\mathfrak{p} : \mathbb{F}_p]$ and $q_\mathfrak{p} = \mathrm{N}\mathfrak{p} = p^{\deg(\mathfrak{p})}$. Higher-degree primes are those with $\deg(\mathfrak{p}) > 1$.

Write $v_\mathfrak{p}(a)$ for the exponent of $\mathfrak{p}$ in the principal fractional ideal $a\mathcal{O}_K$. For a fixed list of m_Γ generators $\gamma_1, \ldots, \gamma_{m_\Gamma}$ the set of primes of bad reduction is

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

At a good prime $\mathfrak{p} \notin S_\Gamma$, let $\Gamma_\mathfrak{p} = \mathrm{red}_\mathfrak{p}(\Gamma) \subset k_\mathfrak{p}^\times$ be the reduction of Γ [2, Chs. 3–4]. Its residual index is

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

Arithmetic Frobenius and the prime filter. Fix a finite Galois extension F/K with group $G_F = \mathrm{Gal}(F/K)$. A prime is *admissible* if it lies outside $S_{\mathrm{exc}} = S_\Gamma \cup \{\mathfrak{p} : \mathfrak{p} \mid \mathfrak{d}_{F/K}\}$, where $\mathfrak{d}_{F/K}$ is the relative discriminant. For admissible $\mathfrak{p}$ and $\mathfrak{P} \mid \mathfrak{p}$ in F, the arithmetic Frobenius is the element of the decomposition group inducing $x \mapsto x^{q_\mathfrak{p}}$ on $k_\mathfrak{P} = \mathcal{O}_F/\mathfrak{P}$. Its conjugacy class $\mathrm{Frob}_{\mathfrak{p},F/K}$ is independent of $\mathfrak{P}$. Its elements have order $[k_\mathfrak{P} : k_\mathfrak{p}]$, and the identity class corresponds to complete splitting [2, Ch. 8, pp. 139–143].

A *Frobenius filter* is a union C of conjugacy classes in G_F. For $X \geq 2$, write $\mathcal{P}_C(X)$ for the admissible primes with $q_\mathfrak{p} \leq X$ and $\mathrm{Frob}_{\mathfrak{p},F/K} \subseteq C$. For $F/K = \mathbb{Q}(i)/\mathbb{Q}$, the identity selects the split primes $p \equiv 1 \pmod 4$, and complex conjugation the inert primes $p \equiv 3 \pmod 4$. We take $F = K,\ C = \{1\}$ for the unrestricted count, including admissible prime ideals of every absolute residue degree.

For real $s > 0$, the (unnormalized) moment is $S_{s,C}(X) = \sum_{\mathfrak{p} \in \mathcal{P}_C(X)} I_\mathfrak{p}^s$. We normalize by the count of all prime ideals up to norm X, and 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 his formula (4.2) predicts, for a fixed group and nonempty C, positive constants $\mathcal{A}_j$ depending on the data and on s, with

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

A fixed subgroup of $K^\times$ can satisfy the same algebraic constraint at every prime of a given splitting type. This distinction from averaging over generators is essential in the examples below.

We address the first line of (2) in a range of small positive exponents, with a rate and a formula for the constant. We also exhibit two fixed groups for which that same line fails at a larger exponent. The two assertions apply to the same prime-ideal convention.

1.2 The distribution theorem

Let $\mathbb{N} = \{1, 2, \ldots\}$, and let $\pi_K(X)$ count all prime ideals of K of norm at most X. Write $\pi(X) = \pi_\mathbb{Q}(X)$. For $\Gamma \subset \mathbb{Q}^\times$ and a good rational prime p, write $I_p^\mathbb{Q} = [\mathbb{F}_p^\times : \Gamma \bmod p]$. For a measure ν on $\mathbb{N}$ we write $\nu(t) = \nu(\{t\})$. When $\pi_K(X) > 0$, define the empirical measure by

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

With this normalization, Chebotarev's theorem gives $\sum_t P_{X,C}(t) = |\mathcal{P}_C(X)|/\pi_K(X) \to |C|/|G_F|$ [2, Theorem 8.31].

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 all n-th roots of elements of Γ. For each $n \geq 1$ form the division field K_n and its compositum E_n with F. Set

$$K_n = K(\mu_n, \Gamma^{1/n}), \quad E_n = FK_n, \quad k_n = [K_n : K], \quad H_n = \mathrm{Gal}(E_n/K_n).$$

Both fields are finite Galois over K [5, Chs. 3 and 5]. With μ the Möbius function [6, Ch. 2], define

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

The notation B_n suppresses the fixed filter C. Section 2.1 shows that (3) converges absolutely and defines a nonnegative model measure D_C of mass $|C|/|G_F|$.

Write ζ_L for the Dedekind zeta function of L and $\zeta = \zeta_{\mathbb{Q}}$. By a nontrivial zero of ζ_L we mean a zero in $0 < \Re z < 1$ [7, Ch. VI, §1 and Ch. VIII, §10]. For the completed function see [8, §5, (5.5)–(5.8)]. For $1/2 \le \theta < 1$, write $\mathcal{Z}(\theta)$ for the assumption that all nontrivial zeros of the Dedekind zeta functions ζ_{E_n}, for every $n \ge 1$, have real part at most θ. The generalized Riemann hypothesis (GRH) for this family asserts that each such zero has real part $1/2$, and hence gives $\mathcal{Z}(1/2)$.

Theorem 1.1 (Weighted distribution)**.** *Suppose $\mathcal{Z}(\theta)$ holds with $1/2 \le \theta < r/(r+1)$. 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 $0 \le \sigma < \sigma_*$ and $\varepsilon > 0$, uniformly over the unions C in G_F,

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

Our weighted total variation norm is the full sum in (5). It measures the largest possible error in the mean of a function of the index bounded by t^{σ}, even for functions that vary with X. In particular, at $\sigma = 0$ it bounds the discrepancy on every set of indices. Since $\theta < r/(r+1)$ and $\theta \ge 1/2$, one has $r \ge 2$ and $\delta_* > 0$. Equation (5) gives a power saving for every $\sigma < \sigma_*$ in this range.

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 $M_{s,C} = \sum_{n \ge 1} J_s(n) b_C(n)$ converges, and unconditionally

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

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

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

In particular the first line of (2) holds in this interval for nonempty C. Under GRH this includes every $0 < s < (r-1)/(r+2)$.

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

1.3 The contribution of higher-degree primes

Even in the unrestricted count $F = K$, the splitting of rational primes in $K/\mathbb{Q}$ matters. Suppose $K/\mathbb{Q}$ is finite Galois and p is unramified in it. The order of Frobenius at p in this extension is the absolute residue degree $f = \deg(\mathfrak{p})$ of each ideal $\mathfrak{p}$ above p. If the generators of Γ are rational, they all reduce into $\mathbb{F}_p^{\times}$, even when $k_{\mathfrak{p}}$ is much larger. This simple restriction supplies an unconditional lower bound. For rational Γ, write $b_U^{\mathbb{Q}}(n)$ for (3) over $\mathbb{Q}$, with auxiliary extension $K/\mathbb{Q}$ and conjugacy class $U \subset G = \operatorname{Gal}(K/\mathbb{Q})$. This is the density of rational primes in U at which n divides the rational residual index. If $d = |G|$ and f_U is the order of an element of U, define the extended real number

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

Here φ denotes Euler's totient. 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 $\Gamma \subset \mathbb{Q}^\times \subset K^\times$ be fixed, finitely generated and of positive rank. Write* $\mathrm{ord}(g)$ *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).

In $K = \mathbb{Q}(i)$, take $\Gamma = \langle 2, 3, 5\rangle$. Then $r = 3$, $c_K = 1/2$ and $a_2(2) = 3/2$. Section 4 exhibits a second rank-three group whose generators generate K as a field. For each of these groups we obtain

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

For the rational group, Corollary 4.4 improves this coefficient to $655\zeta(3)/(14\pi^4)$. For $s = 2 < r$, the literal all-ideal sum in (2) has predicted scale $\mathrm{Li}(X)$. In both examples the inert ideals have density zero. Their contribution to every fixed first-moment tail has lower limit at least $(5887/12000)\zeta(3)$ for the rational generators, and at least $251/432$ for the second group. Sections 4.3 and 4.4 give the computations.

1.4 Antecedents and the proof

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].

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].

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.

Write $\Delta_\Phi = \mu * \Phi$ for the Möbius transform and τ_k for the k-fold divisor function [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.

Ambrose's fixed-group prediction [4, §4.2, (4.2)] extends Wagstaff's heuristic to positive moments and Frobenius restrictions. 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 $I_p^{\mathbb{Q}} \geq L$ by $O_\Gamma(\pi(X)L^{-r})$, for $1 \leq L \leq \log X$ under GRH [48, Theorem 9 of the preprint version].

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 below 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].

A divisibility level n means the condition $n \mid I_{\mathfrak{p}}$. The cutoff in our proof is on the whole integer $n = tv$ in (3). At small levels a Chebotarev estimate must retain its constant as the division field varies. Above the cutoff, every divisor of an index belongs to a prime with a large index. Charging the omitted divisors to that prime makes the estimate summable over all exact indices and gives the same bound for all functions of the index bounded in absolute value by t^σ at index t.

These choices can be compared directly with three earlier estimates. 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 comparison above.

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 quantifies the contribution of higher-degree primes to the first and higher moments.

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.
$\mathfrak{d}_{L/K_n},\ d_L$	Relative discriminant ideal and absolute value of the field discriminant of L over $\mathbb{Q}$.
$\mu_n,\ \mu(n)$	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

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. The subsequent estimates for the coefficients will allow us to sum over all n.

Division fields and restriction of automorphisms. Use the fixed generators $\gamma_1, \ldots, \gamma_{m_\Gamma}$ of the whole group Γ. In a fixed algebraic closure, choose β_j 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. The compositum $E_n = FK_n$ is finite Galois over K 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 $H_n = \mathrm{Gal}(E_n/K_n)$ 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). An element counted by B_n corresponds to a pair $(a, 1)$. Compatibility means that $a \in C$ fixes $F \cap K_n$, and each such a occurs once. The tower formula gives the denominator, so

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

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, put $q = q_{\mathfrak{p}}$, and write p for its rational residue characteristic. 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

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

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 $\mathfrak{p}$, inertia therefore fixes 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. Write $\tau(n) = \tau_2(n)$ for the number of positive divisors of n. 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 $\Gamma = \Gamma_{\mathrm{tor}} \times \Gamma_0$. *Kummer degree theorem (Perucca–Sgobba).* 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 $n \ge 1$

$$\frac{n^a}{[P(\mu_n, \Lambda^{1/n}) : P(\mu_n)]} \quad \text{is an integer dividing } c(P, \Lambda) \qquad [54, \text{Theorem 1.1}].$$

Applying this with $(P, \Lambda) = (K, \Gamma_0)$ gives the lower bound $n^r/c(K, \Gamma_0)$ for the relative degree. The larger field K_n contains this free-part field even when n and $|\Gamma_{\mathrm{tor}}|$ have a common factor. Moreover,

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

Multiplying these degree estimates and applying (13) gives, with $c_1 = [K : \mathbb{Q}]c(K, \Gamma_0)$,

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

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

We use the standard divisor bounds, for every $\lambda > 0$,

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

Fix $0 \le s < r$ 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 $t^s|\mu(v)| \le n^s$. Using (14) and then (15) gives

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

In particular $\sum_t t^s |D_C(t)|$ is bounded by the left side of (16). This proves absolute convergence of (3) and will justify interchanging its sums.

Nonnegativity and total mass. For $t \geq 1$ and $z \geq 2$ let Q_z be the product of the rational primes $\ell \leq z$. Write $\mathbf{1}_A$ for the indicator of A. For every positive integer I,

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

For $I = tm$ this is inclusion–exclusion on the primes dividing (m, Q_z), including those that also divide t.

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 $\sum_{v|Q_z} \mu(v) b_C(tv)$ 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

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

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

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

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 $C = G_F$.

2.2 A uniform estimate at a single level

Under GRH, Sgobba's cyclotomic–Kummer count already 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]. This uses the effective Chebotarev theorem of Serre [59, §2.4, Theorem 4, formula (14R) and Remark 1]. For a Galois extension of $\mathbb{Q}$, Cojocaru states a version under a bound θ for the real parts of the nontrivial zeros of the Dedekind zeta function of the extension field [60, Lemma 3(2)]. Here the base number field in the explicit formula varies, and we keep its degree visible.

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. The base field and its root discriminant. Fix n for the moment. Put $L = E_n$, $H = \mathrm{Gal}(L/K_n)$, $h = |H|$, and write $n_M = [M : \mathbb{Q}]$, $d_M = |\operatorname{disc}(M/\mathbb{Q})|$ for any number field M. Its root discriminant is d_M^{1/n_M}. An element of H fixing F fixes both fields generating $L = FK_n$. Restriction is therefore injective on H, and

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

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 $(w, n) > 1$. *Discriminant bound (Sgobba).* Let P be any number field, let $\Lambda \subset P^\times$ be fixed, finitely generated and torsion-free of rank $a > 0$, and let $1 \le n \mid m$. Write $W = P(\mu_m, \Lambda^{1/n})$ and let s_Λ be the product of the rational primes below the primes of bad reduction of Λ in P, with empty product one. Then [55, Proposition 9]

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

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 $d_L = 1$.

Explicit formula over K_n. For a conjugacy class U of H, choose $g \in U$ and put $a = |U|/h$. Let $H_g = \langle g \rangle$, $h_g = |H_g|$ and $P_g = L^{H_g}$. 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 $\mathfrak{f}_\chi$ 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. To induce the indicator from H_g to H, extend it by zero and sum over conjugates. At $x \in H$ this gives

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

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 complex representation ϱ on V, the Artin L-function has Euler factors $\det(1 - q^{-z}\varrho(\phi) \mid V^{\mathcal{I}})^{-1}$, where q is the norm of the prime, ϕ lifts its residue Frobenius, and $V^{\mathcal{I}}$ is the subspace fixed by inertia. 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].

Explicit formula (Lagarias–Odlyzko). For every finite Galois extension of number fields, every single conjugacy class of its Galois group, and all real $y, T \ge 2$, Theorem 7.1, (7.4)–(7.5) of [8]

applies with their base field, extension field and cyclic fixed field equal to K_n, L, P_g, respectively. Its zero sum and remainder bound are

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

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

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 $an_L = |U| n_{K_n} \geq n_{K_n}$.

Ramified primes in the counting function. 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. 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)].

Euler factors and zeros over the cyclic subfield. 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

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

Put $A(\chi) = d_{P_g}\mathrm{N}\mathfrak{f}_\chi$, using the finite conductor of χ. 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 $L/P_g/\mathbb{Q}$,

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

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

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

From prime powers to primes. 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 $\theta \ge 1/2$. 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 $h \le [F:K]$ 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 $|B_n|/h \le 1$, 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 $y \ge 2$ and $\int_2^X y^{\theta-1}dy \le X^\theta/\theta$. In this integration the field is fixed at the chosen level n, including when $y < n$.

Descent to K. Write $\omega(n)$ for the number of distinct prime divisors of n. Discard primes of K_n above 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 $2^{\omega(n)} \le n$ 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 $\mathrm{N}\mathfrak{P} \ge (\mathrm{N}\mathfrak{p})^2$. The number of all such $\mathfrak{P}$ with norm at most X is consequently bounded by $k_n\pi_K(\sqrt{X}) \le k_n[K:\mathbb{Q}]\sqrt{X}$ 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

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

In particular $0 \le \Pi_{B_n}(X)/k_n - A_n(X) \le |S_{\mathrm{exc}}| + [K:\mathbb{Q}]\omega(n) + \pi_K(\sqrt{X})$. 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), $\omega(n) \le \log n/\log 2$ and $\pi_K(\sqrt{X}) \le [K:\mathbb{Q}]\sqrt{X}$ 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 $\pi_K(X) - \mathrm{Li}(X) \ll_{K,F,\Gamma,\theta} X^\theta \log^2(3X)$. Since $0 \le b_C(n) \le 1$, (27) also holds with $\pi_K(X)$ as the main-term normalization. Finally, for $1 \le n \le X$, $\log(2n)\log^2(3X) \le \log^3(3X) \ll_\lambda X^\lambda$. 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. □

2.3 Primes with small reduction groups

We next bound the number of primes which can supply a large index. Cohen's small-image estimate applies to independent algebraic numbers and prime ideals of a number field [61, Lemma 5.7]. In the preprint of [52] this is Lemma 1.7, with the strict threshold $|\Gamma_\mathfrak{p}| < y$. Taking $y = T + 1 \le 2T$ for $T \ge 1$ gives the same power as the weak threshold below. We give the proof to exhibit the constants and the treatment of all prime ideals.

Lemma 2.2 (Small reduction groups)**.** *For any finitely generated $\Gamma \subset K^\times$ of rank $r \ge 1$, 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 independent elements $g_1, \dots, g_r$ of Γ, for instance the free basis chosen above, 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 ideal divisors of $\prod_j (a_j b_j)$. A prime in S_{frac} can be good if the valuations in a numerator and denominator cancel. We count the good primes in S_{frac} by $|S_{\mathrm{frac}}|$, and use 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 $\prod_j g_j^{v_j} \equiv 1 \bmod \mathfrak{p}$.

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 $U_v/W_v = \prod_j g_j^{v_j}$. Since W_v is a unit at $\mathfrak{p} \notin S_{\mathrm{frac}}$, the congruence implies $h_v \in \mathfrak{p}$. If $h_v = 0$, the same identity in $K^\times$ would give a nonzero multiplicative relation on $g_1, \dots, g_r$. Thus $h_v \ne 0$ for every nonzero v. 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.

Put $d = [K : \mathbb{Q}]$. Take $H_\infty \ge 2$ at least as large as $|\iota(a_j)|$ and $|\iota(b_j)|$ for all j and embeddings $\iota : K \hookrightarrow \mathbb{C}$. Each monomial in (29) has total exponent $\sum_j (v_j^+ + v_j^-) = \sum_j |v_j|$. For every such embedding,

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

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

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

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

Every counted $\mathfrak{p} \notin S_{\mathrm{frac}}$ divides at least one (h_v). Since all h_v are nonzero algebraic integers,

$$v_\mathfrak{p}\left(\prod_{v\in\mathcal{V}_B} h_v\right) = \sum_{v\in\mathcal{V}_B} v_\mathfrak{p}(h_v) \ge 1$$

at each such $\mathfrak{p}$. Indeed, factorization of the product of the principal ideals gives

$$\log \mathrm{N}\left(\prod_{v\in\mathcal{V}_B} (h_v)\right) = \sum_{\mathfrak{p}} \left(\sum_{v\in\mathcal{V}_B} v_\mathfrak{p}(h_v)\right) \log \mathrm{N}\mathfrak{p}.$$

The inner multiplicity is nonnegative at every prime and at least one at every prime being counted, even when several vectors give the same congruence. Applying (30) gives, for $B \ge 1$,

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

Dividing by $\log 2$, adding $|S_{\mathrm{frac}}|$, and substituting $B \le 2T^{1/r}$ 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 $\mathrm{N}\mathfrak{p} \le X$ and $I_\mathfrak{p} > T_0$ give

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

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

3 Proof of the distribution and moment estimates

3.1 Möbius inversion and the three errors

We truncate Möbius inversion [6, Ch. 2] at a common divisibility level and sum the errors over the exact indices.

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

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

The second identity sums the first over $\mathfrak{p} \in \mathcal{P}_C(X)$. The sum of counts is finite because $tv \mid I_\mathfrak{p}$ implies $tv \le I_\mathfrak{p} \le \mathrm{N}\mathfrak{p} - 1 < X$.

The hypotheses give $r \geq 2$. The numerator of $\sigma_* = (r-(r+1)\theta)/(r+1-r\theta)$ is positive and the denominator exceeds it by $1+\theta$. In particular, $0 \leq \sigma < \sigma_* < 1 < \kappa_r = 1+1/r$ and $\sigma < r$. The absolute convergence in (16) therefore holds 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 $v \mid n$.

Let $1 \leq Y \leq X$ be real. For each t, subtract $\pi_K(X) D_C(t)$ from (32). With all sums below taken over $v \geq 1$, the difference is

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

Take absolute values, multiply by t^σ, and sum over t. After the triangle inequality the summands are nonnegative, so we may group them by $n = tv$. As t ranges over the divisors of n, the resulting inner sum is precisely $w_\sigma(n)$. This gives the unnormalized inequality

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

Small divisibility levels. Fix $\lambda > 0$, to be chosen below. Choose C_λ such that $\tau(n) \leq C_\lambda n^\lambda$ by (15). In $\mathcal{E}_1$, every n is at most $Y \leq X$, so Lemma 2.1 gives the same bound $O_{K,F,\Gamma,\theta,\lambda}(X^{\theta+\lambda})$ for each absolute difference. By (33),

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

Large divisors at the counted primes. In the empirical term of (34), insert $A_n(X) = \sum_{\mathfrak{p} \in \mathcal{P}_C(X)} \mathbf{1}_{n|I_\mathfrak{p}}$. All terms with $n \geq X$ vanish because $I_\mathfrak{p} < X$. Interchanging these two finite sums 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 $I > Y$ write $I = \prod_{\ell|I} \ell^{\alpha_\ell}$, with ℓ prime. Summing over all choices of exponents for a divisor gives

$$\sum_{n|I} \tau(n) = \prod_{\ell|I} \sum_{b=0}^{\alpha_\ell} (b+1) = \prod_{\ell|I} \frac{(\alpha_\ell+1)(\alpha_\ell+2)}{2} \leq \prod_{\ell|I} (\alpha_\ell+1)^2 = \tau(I)^2.$$

Using $n^\sigma \leq I^\sigma$ for $n \mid I$ and recalling $I < X$, we obtain

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

We may now include all good prime ideals in the upper bound. Partition the indices above Y into dyadic bands $Y_j < I_\mathfrak{p} \leq 2Y_j$, with $Y_j = 2^j Y$ for $j \geq 0$. Each prime in the j-th band has

weight at most $(2Y_j)^\sigma$. If the band contributes, $Y_j < X$, and Lemma 2.2 bounds their number by $c_{K,\Gamma}(X/Y_j)^{\kappa_r}$, where $c_{K,\Gamma}$ is the implied constant in (28). We conclude that

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

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.

Tail of the algebraic coefficients. The bound (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

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

Choose $2\lambda < r-\sigma$, and put $\beta = r-\sigma-2\lambda > 0$. Since $\lfloor Y \rfloor \ge Y/2$ for $Y \ge 1$,

$$\sum_{n>Y} n^{-1-\beta} \le \int_{\lfloor Y \rfloor}^\infty z^{-1-\beta}\, dz = \frac{\lfloor Y \rfloor^{-\beta}}{\beta} \le \frac{2^\beta}{\beta} Y^{-\beta}.$$

There are at most $[K:\mathbb{Q}]$ prime ideals above each rational prime $p \le X$, so $\pi_K(X) \le [K:\mathbb{Q}]X$. With $Y^{2\lambda} \le X^{2\lambda}$ we obtain

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

Choice of the cutoff. Given $\eta > 0$, take $\lambda = \min\{\eta/4, (r-\sigma)/4\}$. Then $2\lambda \le \eta$ and $\beta > 0$. Inserting (35), (38) and (39) into (34) gives

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

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 every allowed $r \ge 2$. At this crossing e_3 is strictly smaller. To its left e_2 is larger than its value at the crossing, and to its right e_1 is larger. This explains why balancing the first two terms also minimizes the largest of all three exponents. The right side of (40) is therefore $O_{K,F,\Gamma,\theta,\sigma,\eta}(X^{1-\delta_*+u\sigma+\eta})$.

For normalization apply Lemma 2.1 at level one with the full filter, for which the excluded set is fixed and finite. Choosing $0 < \lambda < 1 - \theta$ in that lemma gives $\pi_K(X) \sim \mathrm{Li}(X) \sim X/\log X$. Divide the raw bound by $\pi_K(X) \gg_K X/\log X$ for sufficiently large X, and take $\eta = \varepsilon/2$. Then $\log X \ll_\varepsilon X^{\varepsilon/2}$ proves (5). All estimates are independent of 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

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

The real-valued function $\Phi(t) = t^\sigma \operatorname{sgn}(a_t)$ attains equality even if the supremum permits complex values. It can be chosen afresh for every X, C. In particular, at $\sigma = 0$ every indicator of a set $S_X \subseteq \mathbb{N}$ is allowed. The absolute discrepancy on S_X is bounded by (5) with the same constant for every choice of S_X.

3.2 The moment constant and an example

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

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

Here and below ℓ in a product denotes a prime. For every $0 < s < r$, (16) justifies regrouping the signed double sum over (t, v). With $n = tv$ and $e = n/t$, the computation is

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

Every factor $1 - \ell^{-s}$ in $J_s(n)$ is positive and $J_s(1) = 1$. Since $0 \le b_C(n) \le 1/k_n$, retaining the term $n = 1$ and bounding $J_s(n) \le n^s$ give

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

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, again at level one with the full filter, gives $\pi_K(X) = \mathrm{Li}(X) + O_{K,F,\Gamma,\theta,\varepsilon}(X^{\theta+\varepsilon})$. By (45) this replacement produces a uniform error of that same order. Since $1-\delta_*+us = \theta+u(1+s) > \theta$, it is absorbed in (7). For nonempty C, $M_{s,C} \geq 1/|G_F|$ and $\mathrm{Li}(X) \asymp X/\log X$. Hence the relative error is $O_{K,F,\Gamma,\theta,s,\varepsilon}(X^{-\delta_*+us+\varepsilon}\log X)$. Choose $0 < \varepsilon < \delta_* - us$, possible precisely for $s < \sigma_*$, to conclude the asserted relative asymptotic. 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 use only the algebraic coefficients. Under GRH for the division fields, $u = 2/5$, $\delta_* = 1/10$, and the empirical moment conclusion holds for $0 < s < 1/4$. At $s = 1/8$, the saving is $1/10 - (2/5)(1/8) = 1/20$, giving the raw error $O_\varepsilon(X^{19/20+\varepsilon})$.

4 The contribution of higher-degree prime ideals

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

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

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

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

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

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

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

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

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

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. The stronger coefficient and its rank dependence follow from Theorem 4.3 below, using fixed-level counts. For $\sigma > 1$ the right-hand side tends to $+\infty$, giving the second. □

4.1 Two groups over the Gaussian field

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 $\operatorname{Li}(X)$ 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 $\sigma > 1$. Proposition 4.5 in Section 4.4 strengthens the weight-one bound to $M_1/2 \geq 251/432$ for these generators.

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. Keeping three divisibility levels gives $329/648$ for both groups. Corollary 4.4 sums all levels for the rational group, and Proposition 4.5 treats the norm-one group.

4.2 The first-moment coefficient and comparison with Ambrose

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. For the following 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 $I_\mathfrak{p} = \sum_{n|I_\mathfrak{p}} \varphi(n) \geq \sum_{n\leq B,\, n|I_\mathfrak{p}} \varphi(n)$. 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. Taking the supremum over B on the right gives $\liminf_{X\to\infty} S_1^{(1)}(X)/\pi_K(X) \geq M_1$ by positivity and convergence of the model series.

Now impose the hypotheses of Theorem 1.3, including rational generators. The sum $S_1(X)$ contains both the degree-one contribution and the disjoint higher-degree tail above any fixed cutoff. Its lower limit after normalization is at least the sum of the two lower limits. Applying Theorem 4.3 to the latter tail 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, Proposition 4.5 gives $3M_1/2$ by a separate splitting criterion.

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 $\gamma = r$. All three predicted scales appear 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.

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.

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.

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 write $I_p^{\mathbb{Q}} = [\mathbb{F}_p^\times : \Gamma \bmod p]$. If p is unramified in K with Frobenius class U, of order $f = f_U$, its d/f prime ideals 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, and let $S_{s,U}^{\mathrm{high}}(X)$ be the sum over ideals above the good unramified rational primes in U up to X^{1/f_U}. Indeed, $\mathrm{N}\mathfrak{p} = p^{f_U} \leq X$ is equivalent to $p \leq X^{1/f_U}$, and each such p occurs d/f_U times. 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.

Lemma 4.1 (Fixed joint density)**.** *Let U be a conjugacy class in* $\mathrm{Gal}(K/\mathbb{Q})$*, let $n \geq 1$, and put $Q_n = \mathbb{Q}(\mu_n, \Gamma^{1/n})$. 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 $\sum_{p \leq y} w_p = (b + o(1))y/\log y$ with $b \geq 0$, then for each fixed $\beta \geq 0$*

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

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

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

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 $U \neq \{1\}$, $f = f_U$, $s > 0$, and fixed index cutoff $T \geq 1$, let $S_{s,U}^{\mathrm{high}}(X;T)$ be the part of $S_{s,U}^{\mathrm{high}}(X)$ with $I_{\mathfrak{p}} > T$. Then*

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

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 $m_U = \alpha_U^{-1} \sum_{n \geq 1} \varphi(n) b_U^{\mathbb{Q}}(n)$, this coefficient is $\sum_{U \neq \{1\}} |U| m_U / f_U$.

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

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

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. Each term at a fixed level n has by the two lemmas

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

Insert the truncated divisor sum into $S^{\mathrm{high}}_{s,U}(X;T)$. 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. An automorphism of Q_n fixing Ω_n multiplies each chosen generator root by an element of μ_n. These multipliers form an injective homomorphism into μ_n^r, since the roots generate Q_n/Ω_n and 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). □

What would give a classwise asymptotic. 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 $S^{\mathrm{high}}_{s,U}(X)\sim d\mathcal{L}_{s,U}X^{a_f(s)}/((1+(f-1)s)\log X)$. 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 $r > 1$,*

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

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

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

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

For the field-generating group in Section 4, the factor left in the residual index is an index inside the norm-one group. Let $K = \mathbb{Q}(i)$, and let $\Gamma \subset K^\times$ be a fixed finitely generated group of rank $r > 1$ with $\gamma\bar{\gamma} = 1$ for every $\gamma \in \Gamma$. 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 cyclic of order $p+1$. The following calculation uses the division field over K of the norm-one group.

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

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

Here M_1 is the unrestricted model moment for this group over K. The lower limit of the full mean is at least $3M_1/2$, and $\liminf_{X\to\infty} V_1(X,\nu) \geq M_1/2$ for every nonnegative measure ν of finite first moment. For the three Gaussian generators above, $M_1/2 \geq 251/432$, and the second-moment lower bound is $\liminf_{X\to\infty}(\log X)S_2(X)/X^{3/2} \geq 329/648$.

Proof. Fix the embedding $K = \mathbb{Q}(i) \subset \mathbb{C}$. 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

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

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.

For $0 < s < 1$, suppose $\sum_{p\leq y}^{\text{in}} j_p^s = (b + o(1))y/\log y$ with $b > 0$, using the 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. There is also a local form of the growth obstruction for a tower $K/K_0/\mathbb{Q}$, without a normality assumption. Let $\Gamma \subset K_0^\times$ and consider a good unramified rational prime with ideals $\mathfrak{p} \mid \mathfrak{q} \mid p$ in $K, K_0, \mathbb{Q}$, respectively. If their absolute residue degrees at $\mathfrak{p}, \mathfrak{q}$ are f, e, then $k_\mathfrak{q} \hookrightarrow k_\mathfrak{p}$ gives $f = e[k_\mathfrak{p} : k_\mathfrak{q}]$. Reduction at $\mathfrak{p}$ is reduction at $\mathfrak{q}$ followed by 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, take a Galois closure of $K/\mathbb{Q}$ with group G_{cl}. Let $H \subsetneq H_0$ fix K and K_0, respectively, and 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 the closure 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 The range of weights and the rank-one question

The admissible weight in Theorem 1.1 depends on the rank and the common bound on the real parts of zeta zeros. 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 $0 \leq \sigma < 1$. Then $\sigma < \sigma_*$ is equivalent to $r(1-\theta)(1-\sigma) > \theta + \sigma$, which also implies $\theta < r/(r+1)$. The strict inequality gives the least admissible rank

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

Under GRH, $r > (1 + 2\sigma)/(1 - \sigma)$ suffices. For each fixed $\theta < 1$, the upper endpoint σ_* in (54) tends to one as $r \to \infty$. To see what happens at and above one, take any $r \geq 2$ distinct rational primes as generators in $\mathbb{Q}(i)$. Their valuations give rank r, and (6) gives a finite first moment for D. With $\nu = D$, Theorem 1.3 and Corollary 4.4 give a lower limit of at least $(1 - 2^{-r})\zeta(r)/2 > 1/2$ for the discrepancy at $\sigma = 1$. The discrepancy diverges to $+\infty$ for every $\sigma > 1$. The endpoint σ_* comes from balancing the single-level error with the large-index count of Lemma 2.2, whose exponent is $\kappa_r = 1 + 1/r$. It is a limit of this estimate. For $K = \mathbb{Q}$ every prime ideal has degree one. In the Gaussian examples the proven higher-degree obstruction starts at weight one. Sections 4.3 and 4.4 give the classwise scales below one and the additional moment conditions for the corresponding asymptotics.

For the unweighted case, (55) requires $r > \theta/(1 - \theta)$. The last two rows of the table are conditional on the respective preprint.

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

Here θ_{Liu} is the bound denoted by θ_G in Liu, enclosed by

$$.8733326374459049352 < \theta_{\text{Liu}} < .8733326374459051924.$$

For these two conditional illustrations we use the preprints as stated, without an independent verification of their analytic proofs. Both statements cover the trivial unitary Hecke character of every number field. Its L-function over E_n is ζ_{E_n}. Applying the asserted bound for every n would therefore give the family hypothesis of Theorem 1.1.

For $r = 8$ and $\theta = 7/8$, (4) gives $u = 2/17$, $\delta_* = 1/136$ and $\sigma_* = 1/16$. For the third row,

$$6 \le \frac{\theta}{1-\theta} < 7 \quad \Longleftrightarrow \quad \frac{6}{7} \le \theta < \frac{7}{8}.$$

The stated interval for θ_{Liu} lies inside this range, so seven is the first rank. At $r = 7$, one has $u = (8 - 7\theta)/15$ and $\delta_* = (7 - 8\theta)/15$. These give $u \simeq 0.12577810$, $\delta_* \simeq 0.00088926$ and their ratio $\sigma_* \simeq 0.00707007$ at $\theta = \theta_{\mathrm{Liu}}$. For a single prescribed index over $\mathbb{Q}$ without an additional filter, Pappalardi and Susa [19, p. 322] had identified the same strict threshold for θ. The rate in (5) applies to the full weighted norm.

In rank one the hypotheses would require $1/2 \le \theta < 1/2$. In the balancing calculation, setting $\theta = 1/2$ and $r = 1$ gives $\delta_* = 0$ even at zero weight. Hooley's conditional density theorem for the primitive-root event of an admissible fixed rational integer [9] remains applicable under its own GRH hypotheses. A power-saving rate here for all sets of indices of a single rational generator would require an additional estimate.

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.