# THE SMALLEST INERT PRIME IN A CYCLIC NUMBER FIELD OF PRIME DEGREE

PAUL POLLACK

ABSTRACT. Fix an odd prime $\ell$. For each cyclic extension $K/\mathbf{Q}$ of degree $\ell$, let $n_K$ denote the least rational prime which is inert in $K$, and let $r_K$ be the least rational prime which is split in $K$. We show that $n_K$ possesses a finite mean value, where the average is taken over all such $K$ ordered by conductor. As an example ($\ell = 3$), the average least inert prime in a cyclic cubic field is approximately 2.870.

We conjecture that $r_K$ also has a finite mean value, and we prove this assuming the Generalized Riemann Hypothesis. For the case $\ell = 3$, we give an unconditional proof that the average of $r_K$ exists and is about 6.862.

## 1. INTRODUCTION

For each odd prime $p$, let $n_2(p)$ denote the least quadratic nonresidue modulo $p$. In 1961, Erdős [9] showed that $n_2(p)$ possesses a finite mean value. More precisely, with $p_k$ denoting the $k$th prime in the usual increasing order, Erdős proved that

$$\frac{1}{\pi(x)} \sum_{2<p\le x} n_2(p) \to \sum_{k=1}^{\infty} \frac{p_k}{2^k}, \quad \text{as } x \to \infty.$$

The infinite series on the right-hand side converges rapidly to about 3.675. Erdős's result was generalized by Elliott: For each prime $p \equiv 1 \pmod{k}$, let $n_k(p)$ denote the least $k$th power nonresidue modulo $p$; for $p \not\equiv 1 \pmod{k}$, set $n_k(p) = 0$. Answering a question of Erdős, Elliott showed [6] that $n_k(p)$ possesses a finite mean value for every $k$. If one is interested in power residues instead of nonresidues, the corresponding object of study is the function $r_k(p)$, defined for $p \equiv 1 \pmod{k}$ as the least prime $k$th power residue modulo $p$. (Again, we set $r_k(p) = 0$ if $p \not\equiv 1 \pmod{k}$.) Elliott also proved [8] that $r_k(p)$ has a finite mean value for each of $k = 2, 3$, and 4.

These results of Erdős and Elliott can be viewed as describing statistical properties of number fields. This is simplest to see when $k = 2$. For each quadratic number field $K$, let $n_K$ denote the least rational prime $p$ which is inert in $K$, and let $r_K$ be the least rational prime which is split in $K$. Then Erdős's result gives the average value of $n_K$ as $K$ runs over quadratic fields of *prime* conductor, and Elliott's result on $r_2(p)$ gives the corresponding average of $r_K$. (Recall that the *conductor* of an abelian extension $K/\mathbf{Q}$ may be defined as the least $f$ for which $K \subset \mathbf{Q}(\zeta_f)$.) This suggests the question of whether analogous mean value theorems can be proved for other classes of number fields.

In [20], the present author determined the average of $n_K$ and $r_K$ over all quadratic number fields $K$, ordered by conductor. Both averages have the same value, approximately 4.981. For the class of cubic number fields, the average least prime with a given splitting type is investigated in recent work of the author with Greg Martin [17]. While

2010 *Mathematics Subject Classification.* Primary 11A15, Secondary 11L40, 11R47.

many of the results of that paper are conditional on the Generalized Riemann Hypothesis, it is proved there without any assumption that the average value of the smallest non-completely-split prime in a cubic field is $\approx 2.121$.

The purpose of this paper is to study corresponding averages for cyclic number fields of degree $\ell$, where $\ell$ is a fixed odd prime. In each such number field $K$, an unramified rational prime $p$ is either inert or splits completely. We let $n_K$ denote the least inert prime, and we let $r_K$ be the least split-completely prime. Our main theorem is the following determination of the average value of $n_K$.

⟨thm:main⟩ **Theorem 1.1.** *Fix a prime $\ell \geq 3$. Then $n_K$ has a finite mean value taken over all cyclic extensions $K/\mathbf{Q}$ of degree $\ell$. We describe this average value explicitly: For each rational prime $q$, set*

$$c_{\mathrm{ni}}(q) = \begin{cases} \frac{2\ell-1}{\ell^2+\ell-1} & \text{if } q = \ell, \\ \frac{1}{\ell} \cdot \frac{q+\ell(\ell-1)}{q+\ell-1} & \text{if } q \equiv 1 \pmod{\ell}, \\ \frac{1}{\ell} & \text{if } q \neq \ell \text{ and } q \not\equiv 1 \pmod{\ell}. \end{cases} \tag{1.1}$$

*Then as $x \to \infty$,*

$$\left( \sum_{f_K \leq x} 1 \right)^{-1} \left( \sum_{f_K \leq x} n_K \right) \to \Gamma_\ell, \tag{1.2}$$

*where*

$$\Gamma_\ell := \sum_p p(1 - c_{\mathrm{ni}}(p)) \prod_{q<p} c_{\mathrm{ni}}(q). \tag{1.3}$$

*In (1.2), as in the rest of this paper, the condition "$f_K \leq x$" indicates a sum over cyclic degree $\ell$ extensions $K/\mathbf{Q}$ with conductor $f_K \leq x$. In (1.3), $p$ and $q$ run over rational primes.*

**Remark.** By the conductor-discriminant formula [26, Theorem 3.11, p. 27], the discriminant of a cyclic, degree $\ell$ number field $K$ is $f_K^{\ell-1}$. So for average value results such as Theorem 1.1, it makes no difference whether we order by conductor or by discriminant.

We can also find the average value of $r_K$, but this time we need to assume certain generalizations of the Riemann Hypothesis.

⟨thm:mainsplit⟩ **Theorem 1.2.** *Fix a prime $\ell \geq 3$. Assume that the Riemann Hypothesis holds for the Riemann zeta function $\zeta(s)$ as well as for all $L$-functions associated to Dirichlet characters of order $\ell$. Then $r_K$ has a finite mean value taken over all cyclic extensions $K/\mathbf{Q}$ of degree $\ell$. We describe this average value explicitly: For each rational prime $q$, set*

$$c_{\mathrm{ns}}(q) = \begin{cases} \frac{\ell^2-1}{\ell^2+\ell-1} & \text{if } q = \ell, \\ \frac{\ell-1}{\ell} \cdot \frac{q+\ell}{q+\ell-1} & \text{if } q \equiv 1 \pmod{\ell}, \\ \frac{\ell-1}{\ell} & \text{if } q \neq \ell \text{ and } q \not\equiv 1 \pmod{\ell}. \end{cases} \tag{1.4}$$

*Then as $x \to \infty$,*

$$\left( \sum_{f_K \leq x} 1 \right)^{-1} \left( \sum_{f_K \leq x} r_K \right) \to \Delta_\ell, \tag{1.5}$$

*where*

$$\Delta_\ell := \sum_p p(1 - c_{\mathrm{ns}}(p)) \prod_{q<p} c_{\mathrm{ns}}(q).$$

TABLE 1. The first several odd primes $\ell$ together with the average least inert prime $\Gamma_\ell$ and the conjectured average least split prime $\Delta_\ell$. One can show (proof omitted) that $\Gamma_\ell = 2+1/\ell+O(1/\ell^2)$ and that $\Delta_\ell$ is asymptotic to the $\ell$th prime $p_\ell$, as $\ell \to \infty$.

| | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 |
|---|---|---|---|---|---|---|---|---|
| inert | 2.8698 | 2.3178 | 2.1925 | 2.1092 | 2.0898 | 2.0662 | 2.0585 | 2.0474 |
| split | 6.8616 | 13.2766 | 20.4056 | 37.5746 | 46.2243 | 65.1005 | 74.8968 | 96.5967 |

Drawing inspiration from Elliott's study of the functions $r_k(p)$, we can remove the unproved hypotheses in the case when $\ell = 3$.

⟨thm:mainsplit3⟩ **Theorem 1.3.** *The conclusion of Theorem 1.2 holds unconditionally when $\ell = 3$. In other words, the average least split prime in a cyclic cubic field is $\Delta_3$.*

**Notation and conventions.** All number fields are considered subfields of the complex numbers. The symbol $\zeta_m$ stands for $e^{2\pi i/m}$. In what follows, $\ell$ always denotes a fixed odd prime. For the rest of this paper, every field denoted by $K$ is understood to be a cyclic, degree $\ell$ number field. The letters $p$ and $q$ are reserved for rational primes. We define $n_K$ and $r_K$ as in the introduction. We write $f_K$ for the conductor of $K$. If $\chi$ is a Dirichlet character, we write $f_\chi$ for the conductor of $\chi$. We also use $n_\chi$ to denote the least prime $p$ with $\chi(p) \notin \{0, 1\}$ (sometimes called the *least character nonresidue*), and we write $r_\chi$ for the least prime $p$ with $\chi(p) = 1$.

We use $\omega(m) := \sum_{p|m} 1$ to denote the number of distinct prime factors of $m$ and $\Omega(m) := \sum_{p^k|m} 1$ to denote its total number of prime factors, counted with multiplicity.

We employ the Landau–Bachmann $o$ and $O$ notation, as well as the associated Vinogradov symbols $\ll$ and $\gg$, with their usual meaning. Implied constants may depend on $\ell$ without further mention, but any additional dependence will be indicated explicitly (for example, with subscripts).

## 2. The least inert prime: Proof of Theorem 1.1

2.1. **Outline.** In this section, we prove that $n_K$ possesses a finite mean value, contingent on certain auxiliary results to be established later. We adopt a strategy similar to that of Erdős [9]. We start by showing that the average value $\Gamma_\ell$ claimed in Theorem 1.1 is essentially accounted for by those fields $K$ where $n_K$ is small. (The notion of 'small' that will be convenient for us is that of lying below a fixed large number $z$; the bound $z$ will eventually be sent to infinity at the end of the proof.) It then remains to argue that those $K$ where $n_K$ is large make a negligible contribution to the average.

We require a series of lemmas to carry out this plan, some of which are drawn from the literature and others of which are proved later in this paper. The first of these gives an estimate for the size of the set over which the average in (1.2) is taken. This result goes back to Urazbaev [25]; since the method is useful for us, we also include a sketch of the proof in §2.2 below.

⟨lem:fieldcount⟩ **Lemma 2.1.** *The number of cyclic, degree $\ell$-number fields $K$ with $f_K \le x$ is asymptotic to a nonzero constant multiple of $x$, as $x \to \infty$.*

The next result, also discussed in §2.2, will be used to estimate the contribution to the average from those fields $K$ where $n_K$ is bounded. Recall the definition of the constants $c_{\mathrm{ni}}(q)$ from (1.1).

⟨lem:finitecase⟩ **Lemma 2.2.** *Let $\mathscr{Q}$ be a finite set of primes. The proportion of fields $K$ in which no $q \in \mathscr{Q}$ is inert is $\prod_{q\in\mathscr{Q}} c_{\mathrm{ni}}(q)$. More precisely,*

$$\Big(\sum_{f_K\le x} 1\Big)^{-1}\Big(\sum_{\substack{f_K\le x\\ \text{all } q\in\mathscr{Q} \text{ non-inert}}} 1\Big) \to \prod_{q\in\mathscr{Q}} c_{\mathrm{ni}}(q), \quad \text{as } x\to\infty.$$

The remaining lemmas will be used to show that the contribution from those $K$ where $n_K$ is large is essentially nil. The statements of the subsequent lemmas are in terms of Dirichlet characters. We remind the reader that there is a conductor-preserving correspondence between primitive Dirichlet characters of order $\ell$ and cyclic, degree $\ell$ number fields $K$. Here $\chi$ corresponds to the fixed field $K$ of $\ker\chi \subset (\mathbf{Z}/f_\chi\mathbf{Z})^\times = \mathrm{Gal}(\mathbf{Q}(\zeta_{f_\chi})/\mathbf{Q})$. The correspondence is $(\ell-1)$-to-1; in fact, two such $\chi$ correspond to the same field $K$ precisely when they generate the same group of Dirichlet characters. Moreover, for any prime $q$,

$$\chi(q)=0 \iff q \text{ ramifies in } K, \quad \text{and} \quad \chi(q)=1 \iff q \text{ splits in } K.$$

(The details of this correspondence, in greater generality than that needed here, are worked out in [26, Chapter 3].) This correspondence allows us to go back and forth between counting $K$ with prescribed prime splitting behavior and counting characters with specified values at certain primes.

Lemma 2.3, to be proved in §2.3, will be used to bound the contribution from those fields $K$ where $n_K$ is a medium-sized prime; here "medium-sized" means that $n_K$ exceeds a large, fixed parameter $z$ but is bounded above by $(\log x)^{1000}$.

em:mediumprimes⟩ **Lemma 2.3.** *Let $2 \le z \le \frac{1}{10\ell^2}\log x$. The number of primitive, order $\ell$ Dirichlet characters $\chi$ of conductor not exceeding $x$ for which $n_\chi \ge z$ is*

(2.1) eq:mediumprimebound $\qquad \ll x\exp(-cz/\log z),$

*where $c = c(\ell)$ is a positive constant depending on $\ell$.*

The next two lemmas, taken from the literature, will be used in the large prime range, where $n_K > (\log x)^{1000}$. The first of the lemmas below was proved by Norton [19, Theorem 1.20, eq. (1.22)], using Burgess's character sum bounds.

⟨lem:norton⟩ **Lemma 2.4.** *Let $\chi$ be any nontrivial Dirichlet character mod $m$. For each $\epsilon > 0$, we have $n_\chi \ll_\epsilon m^{\frac{1}{4\sqrt{e}}+\epsilon}$.*

The next lemma is due to Duke and Kowalski [5, eq. (1)] and is proved using the multiplicative large sieve (quoted as Lemma 3.7 below). For a detailed proof, see [20, Lemma 5.3].

⟨lem:DB⟩ **Lemma 2.5.** *Fix $A > 2$. The number of primitive characters $\chi$ of conductor not exceeding $x$ for which $n_\chi > (\log x)^A$ is at most $x^{\frac{2}{A}+o(1)}$, as $x\to\infty$.*

Assuming all of these auxiliary results, we can now prove our main theorem.

*Proof of Theorem 1.1.* Let $z$ be a large, fixed real parameter. Re-organizing the left-hand side of (1.2) as a sum over $n_K = p$, the contribution to the average from those $K$ with $n_K \le z$ assumes the form

(2.2) eq:fromsmallcases $\qquad \displaystyle\sum_{p\le z} p\cdot\frac{\#\{K : f_K\le x, n_K = p\}}{\#\{K : f_K\le x\}}.$

In order to have $n_K = p$, it must be that $p$ is inert in $K$ but that every prime $q < p$ is not inert. Making two applications of Lemma 2.2, we see that the limiting proportion of fields $K$ with $n_K = p$ is $(1 - c_{\mathrm{ni}}(p)) \prod_{q<p} c_{\mathrm{ni}}(q)$. Thus, as $x \to \infty$, the right-hand side of (2.2) is asymptotic to

$$\sum_{p \le z} p(1 - c_{\mathrm{ni}}(p)) \prod_{q<p} c_{\mathrm{ni}}(q).$$

This expression is almost the same as $\Gamma_\ell$ defined in (1.3), the only difference being that the sum on $p$ is truncated at the finite point $z$.

Now let us study the contribution to the average from those $K$ with $n_K > z$. We first deal with the range where $n_K \le \frac{1}{10\ell^2} \log x$. Using Lemmas 2.1 and 2.3, we find that

$$\begin{aligned}\sum_{z<p\le \frac{1}{10\ell^2}\log x} p \cdot \frac{\#\{K : f_K \le x, n_K = p\}}{\#\{K : f_K \le x\}} &\le \sum_{z<p\le \frac{1}{10\ell^2}\log x} p \cdot \frac{\#\{K : f_K \le x, n_K \ge p\}}{\#\{K : f_K \le x\}} \\ &\ll \sum_{p>z} p \cdot \exp(-cp/\log p) \ll z^{-1}.\end{aligned}$$

(To see the final estimate, observe that $p \cdot \exp(-cp/\log p) \ll p^{-2}$.) Next, consider the range where $\frac{1}{10\ell^2 \log x} < n_K \le (\log x)^{1000}$. We apply Lemma 2.3 again to find that

$$\begin{aligned}\sum_{\frac{1}{10\ell^2}\log x<p\le(\log x)^{1000}} p \cdot \frac{\#\{K : f_K \le x, n_K = p\}}{\#\{K : f_K \le x\}} &\le \frac{\#\{K : f_K \le x, n_K > \frac{1}{10\ell^2}\log x\}}{\#\{K : f_K \le x\}} \sum_p p \\ &\ll \exp(-c' \log x/\log\log x) \cdot (\log x)^{2000},\end{aligned}$$

where $c' = c'(\ell) > 0$. This final expression goes to zero. We conclude that those fields $K$ with $z < n_K \le (\log x)^{1000}$ make a total contribution of $O(1/z) + o(1)$.

Finally, we deal with those $K$ where $n_K > (\log x)^{1000}$. Since $1/4\sqrt{e} < 0.2$, Lemma 2.4 shows that $n_K < x^{0.2}$ for all $K$ with $f_K \le x$, once $x$ is large. Moreover, from Lemma 2.5, the number of $K$ with $n_K > (\log x)^{1000}$ is smaller than $x^{1/499}$ for large $x$, and so is certainly smaller than $x^{0.1}$. Hence,

$$\sum_{f_K\le x:\ n_K>(\log x)^{1000}} n_K \le \Big(\max_{f_K\le x} n_K\Big)\Big(\sum_{f_K\le x:\ n_K>(\log x)^{1000}} 1\Big) < x^{0.2} \cdot x^{0.1} = x^{0.3}.$$

To determine the contribution of these $K$ to the average, we divide by the total number of fields $K$ with $f_K \le x$, which was estimated in Lemma 2.1. We find that these $K$ contribute $\ll x^{-0.7} = o(1)$ to our average (1.2).

Piecing everything together, we have shown that the average of $n_K$ over those $K$ with $f_K \le x$ has the form $\sum_{p\le z}(1 - c_{\mathrm{ni}}(p)) \prod_{q<p} c_{\mathrm{ni}}(q) + O(1/z) + o(1)$, as $x \to \infty$. Now let $x \to \infty$ and then let $z \to \infty$ to complete the proof of the theorem. □

⟨sec:finitecase⟩ 2.2. **Proof of Lemma 2.2.** For use below, we quickly review how one establishes an asymptotic formula for the number of cyclic, degree $\ell$ number fields $K$ with bounded conductor. As already mentioned above, this result goes back to Urazbaev [24] (but the $\ell = 3$ case is sometimes attributed to Cohn [4], who worked independently).

In view of the $(\ell - 1)$-to-1 correspondence between primitive Dirichlet characters $\chi$ of order $\ell$ and fields $K$, it suffices to estimate the number of such $\chi$ with $f_\chi \le x$. If $\chi$ is a primitive, order $\ell$ Dirichlet character, then $f := f_\chi > 1$, and $f$ is either a squarefree product of primes $p \equiv 1 \pmod{\ell}$ or is $\ell^2$ multiplied by such a product (compare with

[23]). Given an $f$ of this form, the number of primitive characters $\chi$ mod $f$ of order $\ell$ is precisely $(\ell-1)^{\omega(f)}$ (cf. [25]). Now set

$$U(x) := \sum_{\substack{f \le x \\ f \text{ squarefree} \\ p \mid f \Rightarrow p \equiv 1 \pmod{\ell}}} (\ell-1)^{\omega(f)}. \tag{2.3}$$

Then the number of primitive, order $\ell$ characters $\chi$ with $f_\chi \le x$ and $(f_\chi, \ell) = 1$ is

$$U(x) - 1, \tag{2.4}$$

and the number of primitive, order $\ell$ characters $\chi$ where $f_\chi \le x$ and $\ell^2 \mid f_\chi$ is

$$(\ell-1) \cdot U(x/\ell^2). \tag{2.5}$$

(The '$-1$' in (2.4) is explained by the fact that there are no primitive, order $\ell$ characters modulo 1.) This reduces the problem of counting $K$ with $f_K \le x$ to that of obtaining an asymptotic formula for $U$.

To get a handle on the growth rate of $U$, one introduces the Dirichlet series defined by the Euler product

$$F(s) = \prod_{p \equiv 1 \pmod{\ell}} \left(1 + \frac{\ell-1}{p^s}\right), \tag{2.6}$$

noting that $U(x)$ is the summatory function of the coefficients of $F$. Let $L = \mathbf{Q}(\zeta_\ell)$. A prime-by-prime comparison of the Euler product defining $F(s)$ with that of the Dedekind zeta function $\zeta_L(s)$ reveals that $\zeta_L(s) = F(s)G(s)$, where $G$ is analytic and nonzero for $\Re(s) > \frac{1}{2}$. In particular, since $\zeta_L(s)$ is analytic for $\Re(s) > \frac{1}{2}$ but for a simple pole at $s = 1$, the same is true for $F(s)$. So we may apply the Tauberian theorem of Wiener–Ikehara [18, Corollary 8.8, p. 261] to find that

$$\sum_{\substack{f \le x \\ p \mid f \Rightarrow p \equiv 1 \pmod{\ell} \\ f \text{ squarefree}}} (\ell-1)^{\omega(f)} \sim \kappa_\ell x \quad \text{as } x \to \infty, \quad \text{where} \quad \kappa_\ell := \operatorname{Res}_{s=1} F(s).$$

It follows that our count (2.4) of $\chi$ with $(f_\chi, \ell) = 1$ is $\sim \kappa_\ell x$ (as $x \to \infty$), while the corresponding count of $\chi$ where $\ell^2 \mid f_\chi$ is $\sim \frac{\ell-1}{\ell^2}\kappa_\ell x$. Adding these estimates and dividing by $\ell - 1$, we find that the total number of $K$ with $f_K \le x$ is asymptotic to

$$\kappa_\ell \left(\frac{1}{\ell-1} + \frac{1}{\ell^2}\right) x. \tag{2.7}$$

This vindicates the claim of Lemma 2.1. As shown in [3, Corollary 2], one can express the coefficient of $x$ in (2.7) rather more explicitly; however, we will not need this.

We now return to the proof of Lemma 2.2. It is enlightening to reformulate that lemma in probabilistic terms. If $P$ is a property which a cyclic, degree $\ell$ field $K$ might have, we define the "probability" of $P$ by the expression

$$\mathbf{Prob}(\mathrm{P}) := \lim_{x \to \infty} \left( \sum_{f_K \le x} 1 \right)^{-1} \left( \sum_{\substack{f_K \le x \\ K \text{ has } P}} 1 \right).$$

(The term "probability" is used loosely here, since not all of Kolmogorov's axioms are satisfied.) In this notation, Lemma 2.2 is an assertion about the probability that all primes in a given finite set $\mathscr{Q}$ are non-inert. As a prelude, we determine the probability that a given rational prime $q$ ramifies in a random $K$.

⟨lem:probramify⟩ **Lemma 2.6.** *For each rational prime $q$,*

$$\mathbf{Prob}(q \text{ ramifies}) = \begin{cases} \frac{\ell-1}{\ell^2+\ell-1} & \text{if } q = \ell, \\ \frac{\ell-1}{q+\ell-1} & \text{if } q \equiv 1 \pmod{\ell}, \\ 0 & \text{if } q \neq \ell \text{ and } q \not\equiv 1 \pmod{\ell}. \end{cases}$$

*Proof.* We make use of the field-counting argument given at the start of this section. That argument shows (cf. (2.5)) that the number of $K$ for which $f_K$ is a multiple of $\ell$ belonging to $[1, x]$ is asymptotically $\kappa_\ell x/\ell^2$, as $x \to \infty$. Comparing with (2.7), we see that the probability that $\ell$ ramifies in a random $K$ is

$$\frac{1/\ell^2}{1/(\ell-1) + 1/\ell^2} = \frac{\ell-1}{\ell^2+\ell-1},$$

which establishes the first case of the lemma.

Suppose next that $q \equiv 1 \pmod{\ell}$. Then $q$ ramifies precisely when $f_K = qf'$, where $f' \leq x/q$ and $f'$ is prime to $q$. So the number of $K$ with $f_K \leq x$ where $q$ is ramified is

$$\frac{1}{\ell-1} \sum_{f'} (\ell-1)^{\omega(qf')} = \sum_{f'} (\ell-1)^{\omega(f')} = U'\left(\frac{x}{q}\right) + (\ell-1)U'\left(\frac{x}{\ell^2 q}\right), \tag{2.8}$$

where

$$U'(t) := \sum_{\substack{f' \leq t \\ f' \text{ squarefree, prime to } q \\ p \mid f \Rightarrow p \equiv 1 \pmod{\ell}}} (\ell-1)^{\omega(f')}.$$

The function $U'$ has the same form as the function $U$ defined in (2.3), except for the extra restriction that $q \nmid f'$. So to study the asymptotic behavior of $U'(t)$, we remove the factor $1 + (\ell-1)/q^s$ from the generating function $F(s)$ appearing in (2.6). This changes the residue at $s = 1$ from $\kappa_\ell$ to $\kappa_\ell(1 + (\ell-1)/q)^{-1}$. Now following our previous argument, we find that as $t \to \infty$,

$$U'(t) \sim \kappa_\ell \left(1 + \frac{\ell-1}{q}\right)^{-1} t.$$

Inserting this estimate back into (2.8) and simplifying, we find that the number of $K$ where $q$ is ramified and $f_K \leq x$ is asymptotic, as $x \to \infty$, to

$$\left(\kappa_\ell \left(\frac{1}{\ell-1} + \frac{1}{\ell^2}\right) x\right) \cdot \frac{\ell-1}{q+\ell-1}.$$

Comparing this estimate with (2.7) gives the second case of the lemma.

Finally, if $q \neq \ell$ and $q \not\equiv 1 \pmod{\ell}$, then $q$ never divides any conductor $f_K$, and so $q$ is always unramified. □

We are now in a position to prove Lemma 2.2. In addition to Lemma 2.6, we make use of some powerful, recent theorems of Wood. These are taken from her study [27] of probabilities of prime splitting configurations in abelian extensions.

*Proof of Lemma 2.2.* We first invoke the independence result [27, Theorem 1.3], which shows that distinct primes split independently of one another in a random $K$. Thus, it suffices to prove Lemma 2.2 in the case when $\mathscr{Q}$ consists of a single prime $q$. Next, we appeal to [27, Corollary 1.2]. A special case of that result shows that the probability

that $q$ splits, given that $q$ is unramified, is $1/\ell$. (For the present application, we could also have cited an earlier theorem of Taylor [22, Theorem 2].) Thus,

$$\begin{aligned}\mathbf{Prob}(q \text{ non-inert}) &= \mathbf{Prob}(q \text{ splits}) + \mathbf{Prob}(q \text{ ramifies}) \\ &= \frac{1}{\ell} \cdot \mathbf{Prob}(q \text{ unramified}) + \mathbf{Prob}(q \text{ ramifies}) \\ &= \frac{1}{\ell} + \left(1 - \frac{1}{\ell}\right) \cdot \mathbf{Prob}(q \text{ ramifies}).\end{aligned}$$

To complete the proof, we now substitute the ramification probabilities given in Lemma 2.6 and check that the result coincides with the value $c_{\mathrm{ni}}(q)$ specified in (1.1). □

ec:mediumprimes⟩ 2.3. **Proof of Lemma 2.3.** The proof of Lemma 2.3 has two components. First, we exhibit a bijection between certain primitive Dirichlet characters of order $\ell$ and certain power-residue symbols associated with ideals of $\mathbf{Z}[\zeta_\ell]$. This paves the way for an application of higher reciprocity laws. These laws reduce the proof of Lemma 2.3 to the problem of quantitatively understanding the equidistribution of ideals in strict ray class groups, for which we can appeal to known results.

We begin by reviewing the definition of the $\ell$th power residue symbol. (For complete details, see [12, Chapter 14, §2].) Suppose that $\mathfrak{p}$ is a prime ideal of $\mathbf{Z}[\zeta_\ell]$ not containing $\ell$, and let $\alpha$ be an element of $\mathbf{Z}[\zeta_\ell]$. Then the $\ell$th power residue symbol $\left(\frac{\alpha}{\mathfrak{p}}\right)_\ell$ is either 0 or an $\ell$th root of unity, and is uniquely specified by the congruence

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_\ell \equiv \alpha^{\frac{\mathbf{Nm}(\mathfrak{p})-1}{\ell}} \pmod{\mathfrak{p}}.$$

It is customary to extend this definition to allow non-prime ideals in the "denominator": If $\mathfrak{m}$ is any ideal of $\mathbf{Z}[\zeta_\ell]$ prime to $\ell$, we write $\mathfrak{m} = \prod_i \mathfrak{p}_i$, and we set $\left(\frac{\alpha}{\mathfrak{m}}\right)_\ell = \prod \left(\frac{\alpha}{\mathfrak{p}_i}\right)_\ell$.

The next lemma should be compared with the results discussed on [7, pp. 71–72].

:correspondence⟩ **Lemma 2.7.** *Suppose that $f$ is a squarefree product of primes $p \equiv 1 \pmod{\ell}$. There is a one-to-one correspondence between primitive, order $\ell$ characters $\chi$ of conductor $f$ and ideals $\mathfrak{m}$ of $\mathbf{Z}[\zeta_\ell]$ with norm $f$. More precisely: Given any $\mathfrak{m}$ of norm $f$, the map $\chi\colon \mathbf{Z} \to \mathbf{C}$ given by*

(2.9) eq:charideal

$$\chi(a) = \left(\frac{a}{\mathfrak{m}}\right)_\ell$$

*is a primitive Dirichlet character of order $\ell$ and conductor $f$; conversely, every such Dirichlet character arises in this way from a unique $\mathfrak{m}$.*

*Proof.* We start by showing that (2.9) defines a character of conductor $f$ and order $\ell$. Factor $\mathfrak{m} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$, and put $p_i = \mathbf{Nm}(\mathfrak{p}_i)$. Then the $p_i$ are distinct rational primes, each $p_i \equiv 1 \pmod{\ell}$, and $\prod_i p_i = f$. Define $\chi_{p_i}\colon \mathbf{Z} \to \mathbf{C}$ by setting $\chi_{p_i}(a) = \left(\frac{a}{\mathfrak{p}_i}\right)_\ell$. With $\chi$ defined by (2.9), we see that $\chi = \prod_i \chi_{p_i}$. So if we show that each $\chi_{p_i}$ is a character of order $\ell$ modulo $p_i$, it will follow (for example, from [18, Lemma 9.3]) that $\chi$ is a primitive character of order $\ell$ and conductor $\prod_i p_i = f$, as desired.

Each $\chi_{p_i}$ is totally multiplicative in $a$, is periodic modulo $p_i$, and vanishes precisely when $p_i \mid a$; thus, $\chi_{p_i}$ is a Dirichlet character modulo $p_i$. Clearly, the order of $\chi_{p_i}$ divides $\ell$. To see that the order of $\chi_{p_i}$ is $\ell$ and not 1, choose a rational integer $\eta$ which is not an $\ell$th power modulo $p_i$. Since $\mathbf{Z}[\zeta_\ell]/\mathfrak{p}_i \cong \mathbf{Z}/p_i\mathbf{Z}$, it follows that $\eta$ is not an $\ell$th power modulo $\mathfrak{p}_i$, and so $\chi_{p_i}(\eta) \neq 1$. So $\chi_{p_i}$ is nontrivial and therefore has order $\ell$.

It remains to show that each primitive Dirichlet character of order $\ell$ and conductor $f$ arises in this way from a unique $\mathfrak{m}$. Write $f = p_1 \cdots p_k$, with the $p_i$ distinct and each

$p_i \equiv 1 \pmod{\ell}$. If $\chi$ is a primitive Dirichlet character modulo $f$, then $\chi$ has a unique decomposition as a product $\prod_i \chi_{p_i}$, where each $\chi_{p_i}$ is a Dirichlet character modulo $p_i$ of order $\ell$. So we may assume that $f = p$ is prime, where $p \equiv 1 \pmod{\ell}$.

Let $\mathfrak{p}$ be a prime above $p$, and let $\chi_p$ be the order $\ell$ Dirichlet character corresponding to $\mathfrak{p}$, so that $\chi_p(a) = \left(\frac{a}{\mathfrak{p}}\right)_\ell$. The group of characters mod $p$ is cyclic, and so every Dirichlet character modulo $p$ of order $\ell$ can be written uniquely in the form $\chi_p^j$, where $1 \le j < \ell$. If $\sigma_j$ is the automorphism of $\mathbf{Q}(\zeta_\ell)$ sending $\zeta_\ell \to \zeta_\ell^j$, then (see [12, Proposition 14.2.4])

$$\chi_p^j(a) = \sigma_j(\chi_p(a)) = \sigma_j\left(\left(\frac{a}{\mathfrak{p}}\right)_\ell\right) = \left(\frac{a}{\sigma_j(\mathfrak{p})}\right)_\ell;$$

thus, $\chi_p^j$ is the order $\ell$ Dirichlet character corresponding to the prime $\sigma(\mathfrak{p})$. Now the distinct primes above $p$ are precisely the ideals $\sigma_j(\mathfrak{p})$, for $1 \le j < \ell$. Thus, every character mod $p$ of order $\ell$ arises, in a unique way, from the construction detailed in the first half of the proof. □

For the next few lemmas, we let $L$ denote a fixed number field. We also let $\mathrm{Cl} = \mathcal{I}_L/\mathcal{P}_L$ denote the class group of $L$, and for each (nonzero) ideal $\mathfrak{f}$ of $L$, we write $\mathrm{Cl}(\mathfrak{f}) = \mathcal{I}_L(\mathfrak{f})/\mathcal{P}_{L,\mathfrak{f}}^+$ for the strict ray class group modulo $\mathfrak{f}$. When we speak of *ideal classes modulo* $\mathfrak{f}$ below, we always mean classes of the strict ray class group mod $\mathfrak{f}$. Let $h := \#\mathrm{Cl}$ denote the class number of $L$ and write $h(\mathfrak{f}) := \#\mathrm{Cl}(\mathfrak{f})$ for the strict ray class number modulo $\mathfrak{f}$. It is known that if $r_1$ denotes the number of real embeddings of $L$, then

$$h(\mathfrak{f}) \mid h \cdot 2^{r_1} \cdot \#(\mathcal{O}_L/\mathfrak{f})^\times.$$

(See, for example, [2, Proposition 2.1, p. 50].) In particular, since $h$ and $r_1$ depend only on $L$,

(2.10) eq:classgroupbound $$h(\mathfrak{f}) \ll_L \mathbf{Nm}(\mathfrak{f}).$$

The next lemma, due to Rieger [21, Hauptsatz and p. 465], is a precise form of the elementary result that integral ideals prime to $\mathfrak{f}$ equidistribute mod $\mathfrak{f}$.

⟨lem:rieger⟩ **Lemma 2.8.** *Let $L$ be a fixed number field, and let $\mathfrak{f}$ be a nonzero ideal of $\mathcal{O}_L$. For $x \ge 1$, every element of the strict ray class group modulo $\mathfrak{f}$ contains*

(2.11) eq:numideals $$C(\mathfrak{f})x + O_L(\mathbf{Nm}(\mathfrak{f})^{2-1/[L:\mathbf{Q}]}x^{1-1/[L:\mathbf{Q}]})$$

*ideals of norm not exceeding $x$. Here $C(\mathfrak{f})$ is a constant depending only on $\mathfrak{f}$.*

As shown by Dedekind, the total number of integral ideals of norm not exceeding $x$ is asymptotic to $\mathrm{Res}_{s=1}\zeta_L(s) \cdot x$, as $x \to \infty$. Comparing this with the result of summing (2.11) over all $h(\mathfrak{f})$ classes, we find that $h(\mathfrak{f})C(\mathfrak{f}) \le \mathrm{Res}_{s=1}\zeta_L(s)$. So Lemma 2.8 implies the following crude upper bound:

cor:riegercrude⟩ **Corollary 2.9.** *Let $L$ be a fixed number field, and let $\mathfrak{f}$ be a nonzero ideal of $\mathcal{O}_L$. For $x \ge 1$, every element of the strict ray class group modulo $\mathfrak{f}$ contains*

$$\ll_L \frac{1}{h(\mathfrak{f})}x + \mathbf{Nm}(f)^2 x^{1-1/[L:\mathbf{Q}]}.$$

*ideals of norm not exceeding $x$.*

The application of higher reciprocity laws is made in the following two lemmas. The first is a special case of [7, Lemma 28].

lem:reciprocity⟩ **Lemma 2.10.** *Let $q_1, q_2, \dots, q_k$ be distinct rational primes. Let $\mathfrak{f}$ be the principal ideal of $\mathbf{Z}[\zeta_\ell]$ generated by $\ell^2 q_1 q_2 \cdots q_k$. For integral ideals $\mathfrak{m}$ of $\mathbf{Z}[\zeta_\ell]$ prime to $\mathfrak{f}$, the sequence of values*

$$\left(\frac{q_i}{\mathfrak{m}}\right)_\ell, \qquad i = 1, 2, 3, \dots, k,$$

*depends only on the ideal class modulo $\mathfrak{f}$ to which $\mathfrak{m}$ belongs.*

em:reciprocity2⟩ **Lemma 2.11.** *In the notation of Lemma 2.10, the proportion of ideal classes of $\mathfrak{m}$ modulo $\mathfrak{f}$ which make each $\left(\frac{q_i}{\mathfrak{m}}\right)_\ell = 1$ is precisely $\ell^{-k}$.*

*Proof.* For each $1 \le i \le k$, let $F_i = \mathbf{Q}(\zeta_\ell, \sqrt[\ell]{q_i})$. Let $F = \mathbf{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \dots, \sqrt[\ell]{q_k})$ be the compositum of the $F_i$. By [6, Lemma 3], the $F_i$ are linearly disjoint over $\mathbf{Q}(\zeta_\ell)$, and $[F : \mathbf{Q}(\zeta_\ell)] = \ell^k$. We now apply the splitting criterion of Dedekind–Kummer to see that (with finitely many exceptions)

$$\left(\frac{q_i}{\mathfrak{p}}\right)_\ell = 1 \iff \mathfrak{p} \text{ splits in } F_i \iff \left(\frac{F_i/\mathbf{Q}(\zeta_\ell)}{\mathfrak{p}}\right) \text{ is the identity in } \mathrm{Gal}(F_i/\mathbf{Q}(\zeta_\ell)).$$

So all $\left(\frac{q_i}{\mathfrak{p}}\right)_\ell = 1$ precisely when $\mathfrak{p}$ splits in $F$ (again, with finitely many exceptions). By the Chebotarev density theorem (see, for instance, [11]), the set of such $\mathfrak{p}$ has density

$$\frac{1}{[F : \mathbf{Q}(\zeta_\ell)]} = \frac{1}{\ell^k}.$$

It is now simple to conclude: Since prime ideals are equidistributed in ray class groups (a result of Landau [16]), the proportion of allowable classes mod $\mathfrak{f}$ in the lemma statement must also be $\ell^{-k}$. (This argument is essentially the same as that given by Elliott [6, p. 144] in a related context.) □

We can now prove Lemma 2.3.

*Proof of Lemma 2.3.* Let $q_1, \dots, q_k$ be a list of the primes smaller than $z$ belonging to the congruence class $-1 \pmod{\ell^2}$. Rather than use the full strength of the condition that $n_\chi \ge z$, we will deduce the upper bound (2.1) using only that each $\chi(q_i) \in \{0, 1\}$.

For any primitive character $\chi$ of order $\ell$, we have seen already that the conductor $f_\chi$ is composed only of primes from the congruence classes $0, 1 \pmod{\ell}$. So automatically, $\chi(q_i) \ne 0$. Thus, it suffices to prove the upper bound (2.1) for the count of primitive, order $\ell$ characters $\chi$ of conductor not exceeding $x$ with $\chi(q_i) = 1$ for all $1 \le i \le k$.

We start by counting the $\chi$ of this type for which $\ell \nmid f_\chi$. By Lemmas 2.7, 2.10, and 2.11, the count of such $\chi$ does not exceed the number of ideals of norm $\le x$ from a certain collection of $\ell^{-k} h(\mathfrak{f})$ ideal classes modulo $\mathfrak{f}$, where $\mathfrak{f} = (\ell^2 q_1 q_2 \cdots q_k)$. By Corollary 2.9, this last count is

(2.12) eq:numbound $$\frac{x}{\ell^k} + \frac{1}{\ell^k} h(\mathfrak{f}) \cdot \mathbf{Nm}(f)^2 x^{1-1/\ell} \ll \frac{x}{\ell^k} \left(1 + \mathbf{Nm}(f)^3 x^{-1/\ell}\right),$$

using the upper bound (2.10) for $h(\mathfrak{f})$ in the last step. Since the product of all of the primes in $[2, z]$ is bounded by $4^z$ [10, Theorem 415, p. 453], we have

$$\mathbf{Nm}(f)^3 = \ell^{6\ell} (q_1 \cdots q_k)^{3\ell} \ll 4^{3\ell z} \le 4^{\frac{3}{10\ell} \log x} < x^{\frac{1}{2\ell}},$$

and so our upper bound (2.12) is $\ll x/\ell^k$. Now if $z$ is large (as we may assume), then $k \gg z/\log z$, and so

$$x/\ell^k \le x/\exp(cz/\log z)$$

for a certain $c = c(\ell) > 0$, which confirms the bound (2.1).

Now suppose that the conductor of $\chi$ is divisible by $\ell$. Write $\chi = \chi_1\chi_2$, where $\chi_1$ is a primitive character of conductor $\ell^2$ and $\chi_2$ is a primitive character of conductor prime to $\ell$. For each $1 \le i \le k$, we have $\chi_1(q_i) = \chi_1(-1) = \chi(-1)^\ell = 1$, using that $q_i \equiv -1 \pmod{\ell^2}$ and $-1 = (-1)^\ell$. So

$$\chi_2(q_i) = \chi_1(q_i)\chi_2(q_i) = \chi(q_i) = 1 \quad \text{for all } 1 \le i \le k.$$

The analysis of the last paragraph shows that the number of possibilities for $\chi_2$ is bounded by (2.1). But there are only $\ell - 1 = O(1)$ possibilities for $\chi_1$. So the number of possible values of $\chi = \chi_1\chi_2$ also satisfies the upper bound (2.1). □

## 3. The least split prime

With a few notable exceptions, the proofs of Theorems 1.2 and 1.3 closely parallel our demonstration of Theorem 1.1. So we only sketch them here, focusing on those steps which require a substantial departure from earlier arguments.

3.1. **Proof of Theorem 1.2.** In agreement with our earlier strategy, we re-organize the finite average in (1.5) according to the value of $p = n_K$. We then consider separately the contribution from those $p$ in the same three ranges as before: the small primes $p \le z$, the medium-sized primes $z < p \le (\log x)^{1000}$, and the large primes $p > (\log x)^{1000}$. The small primes are handled by the following lemma. As the proof is essentially identical to that given for Lemma 2.2, we omit it.

initecasesplit⟩? **Lemma 3.1.** *Let $\mathscr{Q}$ be a finite set of primes. The proportion of cyclic, degree $\ell$ number fields in which no $q \in \mathscr{Q}$ is split is $\prod_{q\in\mathscr{Q}} c_{\mathrm{ns}}(q)$. More precisely,*

$$\Big(\sum_{f_K \le x} 1\Big)^{-1} \Big(\sum_{\substack{f_K \le x \\ \text{all } q\in\mathscr{Q} \text{ non-split}}} 1\Big) \to \prod_{q\in\mathscr{Q}} c_{\mathrm{ns}}(q), \quad \text{as } x \to \infty.$$

*Here the constants $c_{\mathrm{ns}}(q)$ are those defined in* (1.4).

The treatment of the medium primes goes through the following lemma, which differs from Lemma 2.3 only in the replacement of $n_\chi$ with $r_\chi$.

diumprimessplit⟩ **Lemma 3.2.** *Let $2 \le z \le \frac{1}{10\ell^2}\log x$. The number of primitive, order $\ell$ Dirichlet characters $\chi$ of conductor not exceeding $x$ for which $r_\chi \ge z$ is*

$$\ll x\exp(-cz/\log z),$$

*where $c = c(\ell)$ is a positive constant depending on $\ell$.*

Lemma 3.2 is established in exactly the same way as Lemma 2.3, except that we replace Lemma 2.11 with the following result (which, like Lemma 2.11, is proved by applying the Chebotarev density theorem to $\mathbf{Q}(\zeta_\ell, \sqrt[\ell]{q_1}, \dots, \sqrt[\ell]{q_k})$).

m:reciprocity3⟩? **Lemma 3.3.** *In the notation of Lemma 2.10, the proportion of ideal classes of $\mathfrak{m}$ modulo $\mathfrak{f}$ which make each $\left(\frac{q_i}{\mathfrak{m}}\right)_\ell \ne 1$ is precisely $(\frac{\ell-1}{\ell})^k$.*

It remains to treat the contribution of the large primes. Tracing through our argument for Theorem 1.1, we find that the proof of Theorem 1.2 will be completed once we show that (as $x \to \infty$)

(3.1) eq:largerk

$$\sum_{\substack{f_K \le x \\ r_K > (\log x)^{1000}}} r_K = o(x).$$

So far, all of our work has been unconditional. It is the proof of (3.1) which requires the Riemann Hypothesis assumptions in Theorem 1.2. Specifically, these assumptions make possible an application of the following result, taken from Lagarias and Odlyzko's study [15] of effective versions of the Chebotarev density theorem.

:leastsplitcheb⟩ **Lemma 3.4.** *Let $L/\mathbf{Q}$ be a nontrivial Galois extension with discriminant $D_L$. Suppose that the Riemann Hypothesis holds for the Dedekind zeta function $\zeta_L(s)$. Then for each conjugacy class $\mathscr{C}$ of $\mathrm{Gal}(L/\mathbf{Q})$, one can find a rational prime $p$ unramified in $L$ with $\left(\frac{L/\mathbf{Q}}{p}\right) = \mathscr{C}$ for which*

$$p \ll (\log |D_L|)^2.$$

*Here the implied constant is absolute.*

Let $K$ be any cyclic, degree $\ell$ number field. By [26, Theorem 4.3, p. 33], $\zeta_K(s)$ factors as the product of $\zeta(s)$ and the $L$-functions $L(s,\chi)$, where $\chi$ runs over the $\ell - 1$ characters $\chi$ corresponding to $K$. Since we are assuming in Theorem 1.2 that each of these factors obeys the Riemann Hypothesis, so does $\zeta_K(s)$. Applying Lemma 3.4 with $L = K$ and $\mathscr{C}$ the identity element of $\mathrm{Gal}(K/\mathbf{Q})$, we obtain that

$$r_K \ll (\log |D_K|)^2 = (\log f_K^{\ell-1})^2 \ll (\log f_K)^2.$$

This shows that the left-hand side of (3.1) is empty for large $x$, making the $o$-estimate trivial. This completes the proof of Theorem 1.2.

3.2. **Proof of Theorem 1.3.** It is sufficient to prove (3.1) unconditionally in the case when $\ell = 3$. In the proof of Theorem 1.2, the sum analogous to (3.1) was handled in two steps: We bounded the maximum size of an individual term via Lemma 2.4 and bounded the total number of terms by Lemma 2.5. The same strategy can be used here. The total number of terms in (3.1) is bounded in the following lemma, proved below in §3.3.

⟨lem:largerchi⟩ **Lemma 3.5.** *Fix $A > 1$. The number of primitive, order $\ell$ characters $\chi$ of conductor not exceeding $x$ for which $r_\chi > (\log x)^A$ is at most $x^{\frac{4}{A}+o(1)}$, as $x \to \infty$.*

Taking $A = 1000$, we see that the number of terms in the sum (3.1) is at most $x^{1/249}$ for large $x$, and so certainly at most $x^{0.1}$. To bound the size of the terms in (3.1), we use the following theorem of Elliott, which is the main result of [8].[1]

⟨lem:elliottmax⟩ **Lemma 3.6.** *Let $\chi$ be a primitive Dirichlet character of order $k \geq 2$, and assume that the conductor $f$ of $\chi$ is cube-free. Let $\epsilon > 0$. Then the smallest prime $p$ for which $\chi(p) = 1$ is*

$$\ll f^{\frac{k-1}{4}+\epsilon},$$

*where the implied constant depends only on $\epsilon$ and $k$.*

**Remark.** Elliott states Lemma 3.6 for characters of prime conductor. The only significant change required to prove the general statement is that [8, Lemma 3], which is Burgess's bound on character sums to a prime modulus, must be replaced with a more general version of Burgess's bounds (such as [13, Theorem 12.4], valid for arbitrary primitive characters to cubefree moduli).

By Lemma 3.6 with $k = 3$, each term of the sum (3.1) is bounded by $x^{0.51}$ once $x$ is large. Since $x^{0.51} \cdot x^{0.1} = o(x)$, we have the $o$-result asserted in (3.1). This completes the proof of Theorem 1.3.

[1]We take this opportunity to correct what appears to be a minor inaccuracy in Elliott's paper: The estimate of [8, Lemma 4] should be asserted only on the line $\sigma = 1 - \alpha$ and not uniformly for all $\sigma \geq 1 - \alpha$.

⟨sec:largerchi⟩ 3.3. **Proof of Lemma 3.5.** Let $\mathscr{X}(Q)$ be the set of primitive Dirichlet characters of conductor not exceeding $Q$, and recall the statement of Gallagher's multiplicative large sieve (see, for instance, [13, Theorem 7.13, p. 179]):

⟨lem:BDS⟩ **Lemma 3.7** (Multiplicative large sieve)**.** *Let $Q, N \geq 1$. If $\{a_n\}_{n\leq N}$ is any sequence of complex numbers, then*

$$\sum_{\chi\in\mathscr{X}(Q)}\left|\sum_{n\leq N} a_n\chi(n)\right|^2 \ll (N+Q^2)\sum_{n\leq N}|a_n|^2$$

⟨lem:EB⟩ **Lemma 3.8.** *Suppose $Q \geq 1$ and that $2 \leq z \leq Q^2$. Let $\mathscr{Q}$ be any set of primes contained in $[2, z]$. The number of $\chi \in \mathscr{X}(Q)$ with*

$$\left|\sum_{q\in\mathscr{Q}}\chi(q)\right| > z/(\log z)^2 \tag{3.2}$$

*is*

$$\ll (\log Q)^2 \exp\left(4\frac{\log Q}{\log z}\log(4\log Q)\right).$$

*Proof.* We adapt a method of Elliott and Burgess (compare with [1, Lemmas 1 and 2] and [7, Lemma 9]). Let $m$ be a positive integer parameter to be specified later. For each $\chi \in \mathscr{X}(Q)$, we have

$$\left(\sum_{q\in\mathscr{Q}}\chi(q)\right)^m = \sum_{n\leq z^m}\chi(n)\sum_{\substack{q_1q_2\cdots q_m=n\\ q\in\mathscr{Q}}} 1.$$

So by the multiplicative large sieve,

$$\sum_{\chi\in\mathscr{X}(Q)}\left|\sum_{q\in\mathscr{Q}}\chi(q)\right|^{2m} \ll (z^m+Q^2)\sum_{n\leq z^m}\left(\sum_{\substack{q_1q_2\cdots q_m=n\\ q_i\in\mathscr{Q}}} 1\right)^2. \tag{3.3}$$

By unique factorization, the right-hand inner sum is uniformly bounded by $m! \leq m^m$. Hence, the right-hand side of (3.3) is $O((z^m+Q^2)(zm^2)^m)$. It follows that the number of $\chi \in \mathscr{X}(Q)$ satisfying (3.2) is

$$\ll ((\log z)^{2m}z^{-2m})\cdot((z^m+Q^2)(zm^2)^m) = (1+Q^2z^{-m})(m\log z)^{2m}.$$

We choose $m = \lceil 2\log Q/\log z\rceil$, so that $Q^2 \leq z^m < zQ^2$. This gives an upper bound that is

$$\begin{aligned}\ll (m\log z)^{2m} &\leq \exp(2m\log(4\log Q))\\ &\leq \exp\left(\left(\frac{4\log Q}{\log z}+2\right)\log(4\log Q)\right)\\ &\ll (\log Q)^2\exp\left(4\frac{\log Q}{\log z}\log(4\log Q)\right),\end{aligned}$$

as desired. □

*Proof of Lemma 3.5.* Let $z := (\log x)^A$. Suppose that $\chi$ is a primitive, order $\ell$ character of conductor $f := f_\chi \leq x$ for which $r_\chi > z$. Let $\mathscr{Q}$ be the set of primes not exceeding

$z$; then for every $q \in \mathscr{Q}$, either $q \mid f$ or $\chi(q)$ is a primitive $\ell$th root of unity. Thus, $\sum_{q\in\mathscr{Q}} \sum_{j=0}^{\ell-1} \chi^j(q) = 0$. By the triangle inequality, there is a $j \in [1, \ell-1]$ for which

$$\left|\sum_{q\in\mathscr{Q}} \chi^j(q)\right| \geq \frac{1}{\ell-1} \sum_{q\in\mathscr{Q}} \chi^0(q) \geq \frac{\pi(z)-\omega(f)}{\ell-1}.$$

Now $\pi(z) \gg \frac{z}{\log z} = \frac{(\log x)^A}{A \log\log x}$ while $\omega(f) \leq \Omega(f) < 2\log x$; hence, $\omega(f) < \frac{1}{2}\pi(z)$ for large $x$, and

$$\frac{\pi(z)-\omega(f)}{\ell-1} \geq \frac{\pi(z)/2}{\ell-1} > \frac{z}{(\log z)^2}.$$

So $\chi^j$ is counted in Lemma 3.8 with $Q = x$ and $z = (\log x)^A$. Substituting in these values of $Q$ and $z$, we find that the number of possibilities for $\chi^j$ at most $x^{4/A+o(1)}$. Since $\chi$ belongs to the $\ell$-element subgroup generated by $\chi^j$, this upper bound also holds for the number of possibilities for $\chi$. □

**Remark.** We have not said anything so far about the smallest ramified prime in $K$, say $q_K$. The trivial observation that $q_K$ is the smallest prime factor of $f_K$ allows one to show, rather easily, that $\sum_{f_K\leq x} q_K \sim \frac{x^2}{2(\ell-1)\log x}$ as $x \to \infty$. In fact, the sum is dominated by those $K$ with prime conductor, in the sense that the asymptotic formula is unaffected even if the sum is restricted to such $K$. (Compare with Kalecki's determination [14] of the average least prime factor of an integer.) By Lemma 2.1, the average of $q_K$, taken over all $K$ with $f_K \leq x$, is thus asymptotic to a constant multiple of $x/\log x$.

## Acknowledgements

The impetus for this paper was a question posed to the author by Ralph Greenberg at the 2012 Pacific Northwest Number Theory Conference. The author thanks Professor Greenberg for the question and the conference organizers for the invitation. This paper was written while the author was visiting Dartmouth College. He is grateful for the hospitality shown by the members of the mathematics department, especially his hosts Lola Thompson and Ben Linowitz. Finally, he thanks Dino Lorenzini, Greg Martin, Carl Pomerance, and Enrique Treviño for helpful comments on earlier versions of the manuscript.

## References

BE68 [1] D. A. Burgess and P. D. T. A. Elliott, *The average of the least primitive root*, Mathematika **15** (1968), 39–50.

childress09 [2] N. Childress, *Class field theory*, Universitext, Springer, New York, 2009.

CDF00 [3] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Densité des discriminants des extensions cycliques de degré premier*, C. R. Acad. Sci. Paris Sér. I Math. **330** (2000), no. 2, 61–66.

cohn54 [4] H. Cohn, *The density of abelian cubic fields*, Proc. Amer. Math. Soc. **5** (1954), 476–477.

DK00 [5] W. Duke and E. Kowalski, *A problem of Linnik for elliptic curves and mean-value estimates for automorphic representations*, Invent. Math. **139** (2000), no. 1, 1–39.

elliott68 [6] P. D. T. A. Elliott, *A problem of Erdős concerning power residue sums*, Acta Arith. **13** (1967/1968), 131–149, corrigendum in **14** (1967/1968), p. 437.

elliott70 [7] ———, *On the mean value of $f(p)$*, Proc. London Math. Soc. (3) **21** (1970), 28–96.

elliott71 [8] ———, *The least prime $k$-th-power residue*, J. London Math. Soc. (2) **3** (1971), 205–210.

erdos61 [9] P. Erdős, *Remarks on number theory. I*, Mat. Lapok **12** (1961), 10–17 (Hungarian).

HW08 [10] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, sixth ed., Oxford University Press, Oxford, 2008.

heilbronn67 [11] H. Heilbronn, *Zeta-functions and L-functions*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 204–230.

IR90 [12] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.

IK04 [13] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004.

kalecki63 [14] M. Kalecki, *On certain sums extended over primes or prime factors*, Prace Mat. **8** (1963/1964), 121–129 (Polish).

LO77 [15] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic number fields: $L$-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 409–464.

landau18 [16] E. Landau, *Über Ideale und Primideale in Idealklassen*, Math. Zeit. **2** (1918), 52–154.

MP [17] G. Martin and P. Pollack, *The average least character nonresidue and further variations on a theme of Erdős*, J. London Math. Soc. (2012), to appear.

MV07 [18] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007.

norton98 [19] K. K. Norton, *A character-sum estimate and applications*, Acta Arith. **85** (1998), no. 1, 51–78.

pollack11 [20] P. Pollack, *The average least quadratic nonresidue modulo $m$ and other variations on a theme of Erdős*, J. Number Theory **132** (2012), 1185–1202.

rieger58 [21] G. J. Rieger, *Über die Anzahl der Ideale in einer Idealklasse mod $\mathfrak{f}$ eines algebraischen Zahlkörpers*, Math. Ann. **135** (1958), 444–466.

taylor84 [22] M. J. Taylor, *On the equidistribution of Frobenius in cyclic extensions of a number field*, J. London Math. Soc. (2) **29** (1984), no. 2, 211–223.

urazbaev50 [23] B. M. Urazbaev, *On the discriminant of a cyclic field of prime degree*, Izvestiya Akad. Nauk Kazah. SSR Ser. Mat. Meh. **4** (1950), no. 97, 19–32 (Russian).

urazbaev51d [24] ———, *On the density of distribution of cyclic fields of prime degree*, Izvestiya Akad. Nauk Kazah. SSR Ser. Mat. Meh. **5** (1951), no. 62, 37–52 (Russian).

urazbaev51 [25] ———, *On the number of cyclic fields of prime degree with given discriminant*, Izvestiya Akad. Nauk Kazah. SSR Ser. Mat. Meh. **5** (1951), no. 62, 53–67 (Russian).

washington97 [26] L. C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.

wood10 [27] M. M. Wood, *On the probabilities of local behaviors in abelian field extensions*, Compos. Math. **146** (2010), no. 1, 102–128.

Department of Mathematics, University of British Columbia, Vancouver, BC, Canada V6T 1Z2; and Department of Mathematics, University of Georgia, Athens, GA, USA 30602

*E-mail address*: pollack@math.ubc.ca