FURTHER VARIATIONS ON A THEME OF ERDŐS

GREG MARTIN AND PAUL POLLACK

Abstract. For each nonprincipal Dirichlet character χ, let n_χ be the least n with $\chi(n) \notin \{0,1\}$. For each prime p, let $\chi_p(\cdot) := \left(\frac{\cdot}{p}\right)$ be the quadratic character modulo p. In 1961, Erdős showed that n_{χ_p} possesses a finite mean value as p runs over the odd primes in increasing order. We show that as $q \to \infty$, the average of n_χ over *all* nonprincipal characters χ modulo q is $\ell(q) + o(1)$, where $\ell(q)$ denotes the least prime not dividing q. Moreover, if one averages over all nonprincipal characters of moduli $\le x$, the average approaches (as $x \to \infty$) the limiting value

$$\sum_{\ell} \frac{\ell^2}{\prod_{p \le \ell}(p+1)} = 2.5350541803\ldots,$$

where the sum is over primes ℓ and the product is over primes $p \le \ell$.

One can also view Erdős's theorem as giving the average size of the least non-split prime in the quadratic field of conductor p, where again p runs over odd primes. Similar results with the average taken over all quadratic fields were recently proved by the second author. In this paper, we prove a result of this type for cubic number fields: If one averages over all cubic fields K, ordered by discriminant, then the mean value of the least rational prime that does not split completely in K is

$$\sum_{r} \frac{r(5/6 + 1/r + 1/r^2)}{1 + 1/r + 1/r^2} \prod_{p<r} \frac{1/6}{1 + 1/p + 1/p^2} = 2.1211027268\ldots,$$

where the sum is over all primes r.

1. Introduction

For χ a nonprincipal Dirichlet character modulo q, let n_χ denote the least positive integer n with $\chi(n) \notin \{0,1\}$. If $q = p$ is prime, then χ is a kth power residue character for some k dividing $p-1$, and the study of the maximal order of n_χ goes back to Vinogradov and Linnik in the early part of the twentieth century. Assuming the Riemann Hypothesis for Dirichlet L-functions, we know that

$$\max_{\substack{\chi \bmod q \\ \chi \ne \chi_0}} n_\chi \le 3(\log q)^2. \tag{1.1}$$

(The first result of this kind is due to Ankeny [Ank52]; as stated here, the result is due to Bach [Bac90, Theorem 3].) The best unconditional result in this direction, due to Norton (see [Nor98, eq. (1.22)]), asserts that the maximum in (1.1) is $\ll_\epsilon q^{\frac{1}{4\sqrt{e}}+\epsilon}$.

Short of a completely satisfactory "pointwise" result, one can study n_χ on average. The first to adopt this viewpoint was Erdős [Erd61], who treated quadratic characters modulo p: He showed that as $x \to \infty$,

$$\frac{1}{\pi(x)} \sum_{\substack{2<p\le x \\ \chi(\cdot)=\left(\frac{\cdot}{p}\right)}} n_\chi \to \sum_{k=1}^{\infty} \frac{p_k}{2^k}, \tag{1.2}$$

where p_k denotes the kth prime in increasing order. This result was extended to all real primitive characters by the second author [Pol11], who showed that

$$\frac{\sum_{|D|\le x,\ \chi(\cdot)=\left(\frac{D}{\cdot}\right)} n_\chi}{\sum_{|D|\le x} 1} \to \sum_{k=1}^{\infty} \frac{p_k^2}{2(p_k+1)}, \tag{1.3}$$

where the sum on D is over fundamental discriminants of absolute value $\le x$. Our first goal in this paper is to understand the average of n_χ taken over all nonprincipal characters χ.

Let $\ell(q)$ denote the least prime not dividing q. If χ is any character modulo q, then $\chi(n) = 0$ whenever $1 < n < \ell(q)$. Hence, $n_\chi \ge \ell(q)$ for all nonprincipal χ. We prove that the average of n_χ is always very close to $\ell(q)$:

Theorem 1.1. *For $q \ge 3$, we have*

$$\frac{1}{\phi(q)-1} \sum_{\chi\ne\chi_0} n_\chi = \ell(q) + O((\log\log q)^2/\log q),$$

where χ runs over all nonprincipal characters modulo q.

One consequence of Theorem 1.1 is an analogue of (1.2) and (1.3) for all nonprincipal characters χ to moduli $\le x$:

Corollary 1.2. *As $x \to \infty$,*

$$\frac{\sum_{q\le x} \sum_{\substack{\chi \bmod q\\ \chi\ne\chi_0}} n_\chi}{\sum_{q\le x} \sum_{\substack{\chi \bmod q\\ \chi\ne\chi_0}} 1} \to \Delta, \quad \textit{where} \quad \Delta := \sum_{\ell} \frac{\ell^2}{\prod_{p\le \ell}(p+1)}. \tag{1.4}$$

Here the right-hand sum is over all primes ℓ and the product in the denominator is over primes $p \le \ell$.

Remark. A quick calculation with Mathematica shows that

$$\Delta = 2.5350541803604388301655300071859083508611780138537 0\ldots$$

One can also view (1.2) and (1.3) as results in algebraic number theory. If χ is the quadratic character modulo p, then n_χ is the least prime that does not split in the quadratic field of conductor p (equivalently, of discriminant $p^* := (-1)^{(p-1)/2}p$). Thus, Erdős's theorem gives the average least non-split prime in a quadratic extension, where the average is restricted to quadratic fields of prime conductor. Similarly, (1.3) is an estimate for the average least inert prime, where now the average is taken over all quadratic fields, ordered by discriminant.

For a prime $p \equiv 1 \pmod 3$, define $n_3(p)$ as the least cubic nonresidue modulo p. Elliott [Ell68] showed that $n_3(p)$ possesses a finite mean-value. (In fact, he showed the analogous result for kth power nonresidues, for all k.) We can interpret Elliott's result on $n_3(p)$ as the determination of the average least non-split prime, with the average restricted to cyclic cubic extensions of prime conductor. Our second theorem gives the average least non-split prime, with the average taken over *all* cubic extensions of $\mathbf{Q}$, ordered by discriminant. In what follows, we write D_K for the discriminant of the number field K.

Theorem 1.3. *For a cubic number field K, let n_K denote the least rational prime which does not split completely in K. As $x \to \infty$,*

$$\frac{\sum_{|D_K|\le x} n_K}{\sum_{|D_K|\le x} 1} \to \sum_{r} \frac{r(5/6+1/r+1/r^2)}{1+1/r+1/r^2} \prod_{p<r} \frac{1/6}{1+1/p+1/p^2}. \tag{1.5}$$

Here the left-hand sums are over all cubic fields K, up to isomorphism, for which $|D_K| \le x$, and the right-hand sum is over all primes r.

Remark. The numerical value of the right-hand sum is $2.1211027268\ldots$. As a reality check, we sampled fields with discriminant $\approx -10^{12}$. Using K. Belabas's `cubics` package (see [Bel97, Bel04]) and `PARI/GP`, we found that the average of n_K over fields with $|D_K - X| \le 250000$ is $2.1206494717\ldots$.

The proofs of our theorems, while similar in flavor to the arguments of [Erd61, Pol11], employ different tools. For the proof of Theorem 1.1, our primary inspiration was a paper of Burthe [Bur97], which uses zero-density estimates and a theorem of Montgomery (Proposition 2.2 below) to prove that

$$\frac{1}{x}\sum_{q\le x}\max_{\substack{\chi \bmod q\\ \chi\neq\chi_0}} n_\chi \ll (\log x)^{97};$$

note that Burthe's result shows unconditionally that a bound of the same flavor as (1.1) holds on average. The proof of Theorem 1.3 involves a few different ingredients; perhaps most crucial is the recent work of Taniguchi and Thorne [TT11] on counting cubic fields with prescribed local conditions (see Proposition 4.2 below).

Notation. The letters ℓ, p, and r are reserved for prime variables. We write $P(n)$ for the largest prime factor of n. We say that n is *y-friable* (or *y-smooth*) if $P(n) \le y$, and we let $\Psi(x, y)$ denote the number of y-friable $n \le x$. We write $\omega(n) := \sum_{p|n} 1$ for the number of distinct prime factors of n and $\Omega(n) := \sum_{p^k|n} 1$ for the number of prime factors of n counted with multiplicity. We use $c_1, c_2, \ldots$ for absolute positive constants. We write $\log_1 x = \max\{1, \log x\}$, and we use $\log_k$ for the kth iterate of $\log_1$.

2. Proof of Theorem 1.1

We begin by quoting two theorems from the literature. The first, due to Baker and Harman [BH96, BH98], asserts that many shifted primes possess a large prime factor.

Proposition 2.1. *For each positive real number $\theta \le 0.677$, there is a constant $c_\theta > 0$ with the following property: For all large x, say $x > x_0(\theta)$, the number of primes $p \le x$ with $P(p-1) > x^\theta$ is $> c_\theta x/\log x$.*

The next result, due to Montgomery (see [Mon94, Theorem 1, p. 164], and cf. [LMO79]), relates the size of n_χ to a zero-free region for $L(s, \chi)$ near $s = 1$. Define $N(\sigma, T, \chi)$ as the number of zeros $s = \beta + i\gamma$ of $L(s, \chi)$ with $\sigma \le \beta \le 1$ and $|\gamma| \le T$.

Proposition 2.2. *Let χ be a nonprincipal Dirichlet character modulo q. If $\frac{1}{\log q} < \delta \le 1/2$ and $N(1-\delta, \delta^2 \log q, \chi) = 0$, then $n_\chi < (c_1\delta \log q)^{1/\delta}$. Here c_1 is an absolute positive constant.*

Proposition 2.2 allows us to establish the next lemma, which will eventually be used to show that characters χ with n_χ larger than about $(\log q)^5$ do not significantly affect the average of n_χ.

Lemma 2.3. *The number of nonprincipal characters χ modulo q with $n_\chi \ge (\frac{c_1}{5}\log q)^5$ is $\ll q^{9/20}$. Here c_1 has the same meaning as in Proposition 2.2.*

Proof. The proof uses Proposition 2.2 and the following zero-density estimate due to Jutila (see [Jut77, Theorem 1]): Let $\epsilon > 0$. For $4/5 \le \alpha \le 1$ and $T \ge 1$, we have

$$\sum_{\chi \bmod q} N(\alpha, T, \chi) \ll_\epsilon (qT)^{(2+\epsilon)(1-\alpha)}. \tag{2.1}$$

For the proof of the lemma, we may assume that q is large. By Proposition 2.2 (with $\delta = 1/5$), the number of nonprincipal χ with $n_\chi \ge (\frac{c_1}{5}\log q)^5$ is bounded above by

$$\sum_{\chi \bmod q} N\left(\frac{4}{5}, \frac{1}{25}\log q, \chi\right).$$

From (2.1) with $\epsilon = \frac{1}{10}$, this sum is $\ll (q\log q)^{21/50}$, which is crudely $\ll q^{9/20}$. □

Lemma 2.4. *Assume $q > 1$, and write $\ell = \ell(q)$. Then*

$$\frac{1}{\phi(q)-1}\sum_{\substack{\chi\ne\chi_0\\ n_\chi=\ell}} n_\chi = \ell + O(\ell/f), \tag{2.2}$$

while

$$\frac{1}{\phi(q)-1}\sum_{\substack{\chi\ne\chi_0\\ n_\chi>\ell}} n_\chi \ll q^{-1/50} + \frac{1}{\phi(q)}\sum_{\substack{\chi\ne\chi_0\\ \ell<n_\chi\le(\frac{c_1}{5}\log q)^5}} n_\chi. \tag{2.3}$$

Lemma 2.4, once shown, reduces the proof of Theorem 1.1 to the task of showing that both the O-term in (2.2) and the right-hand side of (2.3) are $\ll (\log_2 q)^2/\log q$.

Proof. A character χ mod q has $\chi(\ell) = 1$ precisely when χ descends to a character on the quotient $(\mathbf{Z}/q\mathbf{Z})^\times/\langle\ell\rangle$. Hence, the proportion of characters χ mod q with $\chi(\ell) = 1$ is $\frac{1}{f}$, where f is the order of ℓ modulo q. So the contribution to the average of n_χ from those χ with $n_\chi = \ell$ is

$$\frac{\phi(q)-\phi(q)/f}{\phi(q)-1}\ell = \ell + O(\ell/f).$$

Turning to the contribution from the remaining χ, we have

$$\begin{aligned}\frac{1}{\phi(q)-1}\sum_{\substack{\chi\ne\chi_0\\ n_\chi>\ell}} n_\chi &= \frac{1}{\phi(q)-1}\sum_{\substack{\chi\ne\chi_0\\ \ell<n_\chi\le(\frac{c_1}{5}\log q)^5}} n_\chi + \frac{1}{\phi(q)-1}\sum_{\substack{\chi\ne\chi_0\\ n_\chi>(\frac{c_1}{5}\log q)^5}} n_\chi \\ &= \frac{1}{\phi(q)-1}\sum_{\substack{\chi\ne\chi_0\\ \ell<n_\chi\le(\frac{c_1}{5}\log q)^5}} n_\chi + O\left(\frac{\max_{\chi\ne\chi_0} n_\chi}{\phi(q)}\sum_{\substack{\chi\ne\chi_0\\ n_\chi>(\frac{c_1}{5}\log q)^5}} 1\right).\end{aligned}$$

By the Polya–Vinogradov inequality, the maximum over χ appearing here is $\ll q^{21/40}$, say. (Norton's sharper result, quoted in the introduction, would not be any better for our purposes.) Using this in conjunction with Lemma 2.3, we find that the O-term term here is $\ll q^{39/40}/\phi(q) \ll q^{-1/50}$. □

Proof of Theorem 1.1. We can assume that q is large. We first prove the theorem when $\ell > X$, where

$$X := (\log_2 q)^2/\log_3 q.$$

Fix $\theta := 2/3$. By Proposition 2.1, there are $\gg X/\log X$ primes $p \le X$ with $P(p-1) > X^\theta$. We claim that for almost all of these primes p, the order of ℓ modulo p is divisible by $P(p-1)$. To see this, note that if p does not have this property, then the order of ℓ modulo p is a divisor of $(p-1)/P(p-1)$ and so is less than $X^{1-\theta}$; hence,

$$p \mid \prod_{1\le j<X^{1-\theta}} (\ell^j - 1).$$

Now $\Omega(\ell^j - 1) \ll j \log \ell$, and so summing over j, we see there are only $\ll X^{2(1-\theta)} \log \ell \ll X^{3/4}$ such exceptional p, and this number is $o(X/\log X)$.

Let S be the set of non-exceptional p constructed above, so that $\#S \gg X/\log X$. If $q > X^\theta$, the number of $p \in S$ for which $q = P(p-1)$ is clearly $\leq \pi(x; q, 1) < X/q < X^{1-\theta}$. Hence, the number of distinct values $P(p-1)$, as p ranges over S, is $\gg X^\theta/\log X$. Since f, which is the order of $\ell \bmod q$, is divisible by all these values $P(p-1)$, it follows that

$$f \geq (X^\theta)^{c_2 X^\theta/\log X} \geq \exp(c_3 X^\theta)$$

for some $c_2, c_3 > 0$.

Now $\ell < 2 \log q$, by the prime number theorem. Consequently, for the O-term in (2.2), we have the estimate

$$\ell/f \leq \ell/\exp(c_3(\log_2 q)^{2\theta}/(\log_3 q)^\theta) < 2\log q/\exp((\log_2 q)^{1.3}) < 1/\log q.$$

Moreover, the right-hand side of (2.3) is

$$\ll q^{-1/50} + \frac{(\log q)^5}{\phi(q)} \sum_{\substack{\chi \neq \chi_0 \\ n_\chi > \ell}} 1 < q^{-1/50} + \frac{(\log q)^5}{f} < \frac{1}{\log q}.$$

So in the case when $\ell > X$, the average of n_χ is $\ell + O(1/\log q)$, which is sharper than what is claimed in the theorem.

In the above reasoning, it was not necessary to assume that q is divisible by *all* primes up to X; the same arguments apply if, in the notation of Proposition 2.1, q is divisible by all but at most $\frac{1}{2}c_\theta X/\log X$ primes $p \leq X$. So in what follows, we assume not only that $\ell \leq X$, but that there are more than $\frac{1}{2}c_\theta X/\log X$ primes $p \leq X$ not dividing q. Under these hypotheses, the error term ℓ/f in (2.2) is trivially bounded. Indeed, from $q \mid \ell^f - 1$, it follows that

$$f \geq \log q/\log \ell, \tag{2.4}$$

and so

$$\ell/f \leq \ell \log \ell/\log q \leq X \log X/\log q \ll (\log_2 q)^2/\log q,$$

which is acceptable. Also, the right-hand side of (2.3) is

$$\ll q^{-1/50} + \frac{1}{\phi(q)} \sum_{\substack{\chi \neq \chi_0 \\ \ell < n_\chi \leq X}} n_\chi + \frac{1}{\phi(q)} \sum_{\substack{\chi \neq \chi_0 \\ X < n_\chi \leq (\frac{c_1}{5}\log q)^5}} n_\chi \ll q^{-1/50} + \frac{X}{f} + \frac{(\log q)^5}{\phi(q)} \sum_{\substack{\chi \neq \chi_0 \\ n_\chi > X}} 1.$$

By our hypotheses, we may pick six primes $p_1, \dots, p_6 \leq X$ not dividing q. If $n_\chi > X$, then χ vanishes on the subgroup H (say) of $(\mathbf{Z}/q\mathbf{Z})^\times$ generated by (the images of) the p_i. The order of H is not less than the number of $n \leq q$ which factor as a product of the p_i, which is $\gg (\log q/\log X)^6 \gg (\log q/\log_3 q)^6$. It follows that

$$\frac{1}{\phi(q)} \sum_{\substack{\chi \neq \chi_0 \\ n_\chi > X}} 1 \leq \frac{\#\{\chi \bmod q : H \subset \ker \chi\}}{\phi(q)} = \frac{1}{\#H} \ll \frac{(\log_3 q)^6}{(\log q)^6}.$$

With (2.4), this gives that the right-hand side of (2.3) is $\ll (\log_2 q)^2/\log q$ and completes the proof of the theorem. □

Remark. For almost all q (in the sense of asympotic density), one has $f > q^{1/2}$. (This, and a bit more, follows from [KP05, Theorem 1].) For such q, we deduce quickly from Lemma 2.4 that the average of n_χ is $\ell + O(q^{-1/50})$. Thus, the estimate of Theorem 1.1 is only interesting for integers q for which f is abnormally small. Our proof of

Theorem 1.1 can be modified to show that (with notation as above) the average of n_χ is always $\ell + O(X/f) + O(\exp(-(\log_2 q)^{1.3}))$, and that the first O-term can be omitted when $\ell > X$.

3. Proof of Corollary 1.2

Lemma 3.1. *Let m be a natural number. For $x \ge 1$, we have that*

$$\sum_{\substack{n\le x\\ \gcd(n,m)=1}} \phi(n) = \frac{3x^2}{\pi^2}\prod_{p\mid m}(1+1/p)^{-1} + O(2^{\omega(m)}x\log(ex)),$$

uniformly in m.

Proof. Let χ_0 be the principal character modulo m, so that we seek to estimate the partial sums of $\phi\chi_0$. For each natural number d, let $h(d)$ denote the largest divisor of d coprime to m. One checks easily that $\frac{\phi(n)}{n}\chi_0(n) = \sum_{d\mid n}\mu(d)/h(d)$, so that

$$\sum_{\substack{n\le x\\ \gcd(n,m)=1}} \phi(n) = \sum_{n\le x} n \sum_{d\mid n}\mu(d)/h(d) = \sum_{d\le x}\frac{\mu(d)}{h(d)}\sum_{e\le x/d}(de)$$

$$= \sum_{d\le x}\frac{\mu(d)}{h(d)}\left(\frac{x^2}{2d}+O(x)\right) = \frac{x^2}{2}\sum_{d\le x}\frac{\mu(d)}{h(d)d} + O\left(x\sum_{\substack{d\le x\\ d \text{ squarefree}}}\frac{1}{h(d)}\right).$$

Now the infinite sum

$$\sum_{d}\frac{\mu(d)}{h(d)d} = \left(\prod_{p\nmid m}\left(1-\frac{1}{p^2}\right)\right)\left(\prod_{p\mid m}\left(1-\frac{1}{p}\right)\right)$$

$$= \left(\prod_{p}\left(1-\frac{1}{p^2}\right)\right)\prod_{p\mid m}\left(1+\frac{1}{p}\right)^{-1} = \frac{6}{\pi^2}\prod_{p\mid m}\left(1+\frac{1}{p}\right)^{-1},$$

and so
(3.1)

$$\sum_{\substack{n\le x\\ \gcd(n,m)=1}} \phi(n) = \frac{3x^2}{\pi^2}\prod_{p\mid m}\left(1+\frac{1}{p}\right)^{-1} + O\left(x^2\sum_{\substack{d>x\\ d \text{ squarefree}}}\frac{1}{dh(d)}\right) + O\left(x\sum_{\substack{d\le x\\ d \text{ squarefree}}}\frac{1}{h(d)}\right).$$

For each $y \ge 1$, we have

$$S(y) := \sum_{\substack{d\le y\\ d \text{ squarefree}}}\frac{1}{h(d)} \le \prod_{p\le y}\left(1+\frac{1}{h(p)}\right) \le 2^{\omega(m)}\prod_{p\le y}\left(1+\frac{1}{p}\right) \ll 2^{\omega(m)}\log(ey).$$

This shows immediately that the second O-term in (3.1) is acceptable for us. By partial summation, $\sum_{d>x,\text{ squarefree}}\frac{1}{dh(d)} = \int_x^\infty t^{-1}dS(t) \le \int_x^\infty S(t)/t^2\,dt \ll 2^{\omega(m)}x^{-1}\log(ex)$. Hence, the first O-term in (3.1) is $\ll 2^{\omega(m)}x\log(ex)$, which is again acceptable. This completes the proof of the lemma. □

Proof of Corollary 1.2. By Lemma 3.1, the denominator in (1.4) is

$$\sum_{q\le x}\sum_{\substack{\chi \bmod q\\ \chi\neq\chi_0}} 1 = \sum_{q\le x}(\phi(q)-1) = \frac{3x^2}{\pi^2} + O(x\log x),$$

and so it suffices to show that the numerator in (1.4) is $\sim \frac{3}{\pi^2}\Delta x^2$ as $x\to\infty$. By Theorem 1.1, we have that as $x\to\infty$,

$$\sum_{q\le x}\sum_{\substack{\chi \bmod q\\ \chi\neq\chi_0}} n_\chi = \sum_{q\le x}(\phi(q)-1)(\ell(q)+O((\log_2 q)^2/\log q))$$

$$= \sum_{1<q\le x}\phi(q)\ell(q) + O\left(\sum_{1<q\le x}\left(\ell(q)+\phi(q)\frac{(\log_2 q)^2}{\log q}\right)\right).$$

Put $y := 2\log x$, and notice that $\ell(q)\le y$ uniformly for $q\le x$ (assuming x is large). It follows that the O-term is $\ll x\log x + x^2(\log_2 x)^2/\log x$. In particular, as $x\to\infty$,

$$\sum_{q\le x}\sum_{\substack{\chi \bmod q\\ \chi\neq\chi_0}} n_\chi = \sum_{1<q\le x}\phi(q)\ell(q) + o(x^2).$$

To estimate the remaining right-hand sum, we let M be the y-friable part of q and partition the sum according to the value of M. Observe that since $q>1$, we have that $M>1$ and $\ell(q)=\ell(M)$.

We can assume that $M\le x^{1/2}$. Indeed, the number of $q\le x$ divisible by a y-friable number $M>x^{1/2}$ is at most

$$x\sum_{\substack{M>x^{1/2}\\ p\mid M\Rightarrow p\le y}}\frac{1}{M} = x\int_{x^{1/2}}^{\infty}\frac{d\Psi(t,y)}{t} \le x\int_{x^{1/2}}^{\infty}\frac{\Psi(t,y)}{t^2}\,dt \le x^{2/3},$$

say, once x is large. (We use here that $\Psi(t,y)\le\Psi(t,4\log t)$ once $t\ge x^{1/2}$, and that $\Psi(t,4\log t)\le t^{o(1)}$ as $t\to\infty$; see, e.g., [Ten95, Theorem 2, p. 359].) Since $\phi(q)\ell(q)\le xy$ for all $q\le x$, those q corresponding to values $M>x^{1/2}$ contribute $\le x^{5/3}y = o(x^2)$, which is negligible.

Again invoking Lemma 3.1, we find that each remaining value of $M>1$ contributes

$$\ell(M)\sum_{\substack{1<q\le x\\ \ell(q)=M}}\phi(q) = \ell(M)\phi(M)\sum_{\substack{q'\le x/M\\ \gcd(q',\prod_{p\le y}p)=1}}\phi(q')$$

$$= \frac{3x^2}{\pi^2}\frac{\ell(M)\phi(M)}{M^2}\prod_{p\le y}\left(1+\frac{1}{p}\right)^{-1} + O\left(2^{\pi(y)}\frac{\ell(M)\phi(M)}{M}x\log(ex)\right).$$

Now sum this estimate over y-friable M from the interval $(1,x^{1/2}]$. Since $\phi(M)/M\le 1$ and $\ell(M)\le y$, the O-error is

$$\ll 2^{\pi(y)}\sum_{M\le x^{1/2}}(yx\log(ex)) \ll x^{3/2}(\log x)^2\exp(O(\log x/\log\log x)),$$

which is $o(x^2)$. The main term is given by

$$\frac{3x^2}{\pi^2}\left(\prod_{p\le y}\left(1+\frac{1}{p}\right)^{-1}\right)\sum_{\ell\le y}\ell\sum_{\substack{M\le x^{1/2},\ y\text{-friable}\\ \ell(M)=\ell}}\frac{\phi(M)}{M^2}. \tag{3.2}$$

Extending the inner sum over all M, we find that

$$\sum_{\substack{M\ y\text{-friable} \\ \ell(M)=\ell}} \frac{\phi(M)}{M^2} = \prod_{p<\ell}\left(\frac{\phi(p)}{p^2}+\frac{\phi(p^2)}{p^4}+\dots\right)\prod_{\ell<p\le y}\left(1+\frac{\phi(p)}{p^2}+\frac{\phi(p^2)}{p^4}+\dots\right)$$
$$= \left(\prod_{p<\ell}\frac{1}{p}\right)\left(\prod_{\ell<p\le y}\left(1+\frac{1}{p}\right)\right);$$

moreover, the error incurred by extending the sum is (for large x) smaller than

$$\sum_{\substack{M\ y\text{-friable} \\ M>x^{1/2}}} \frac{1}{M} = \int_{x^{1/2}}^{\infty}\frac{d\Psi(t,y)}{t} < \frac{1}{x^{1/3}}.$$

This shows that (3.2) is

$$\frac{3x^2}{\pi^2}\sum_{\ell\le y}\frac{\ell^2}{\prod_{p\le\ell}(p+1)} + O\left(x^2\sum_{\ell\le y}\ell x^{-1/3}\right).$$

The O-error here is $\ll x^{5/3}y^2$, and so is again $o(x^2)$. Since the sum over ℓ appearing in the main term tends to Δ as $x\to\infty$, collecting our estimates we find that the numerator in (1.4) is indeed $\sim \frac{3}{\pi^2}\Delta x^2$ as $x\to\infty$, as desired. □

Remark. Let $q>1$, let $\ell=\ell(q)$, and let $\mathscr{X}(q)$ be a nonempty collection of nonprincipal Dirichlet characters mod q. The set of $\chi\in\mathscr{X}(q)$ with $n_\chi>\ell$ is obviously a subset of the set of all nonprincipal χ mod q with $n_\chi>\ell$. This triviality, taken together with the estimates occurring in the proof of Theorem 1.1, shows that

$$\frac{\sum_{\chi\in\mathscr{X}(q)} n_\chi}{\sum_{\chi\in\mathscr{X}(q)} 1} = \ell + O\left(\frac{\phi(q)}{\#\mathscr{X}(q)}(\log_2 q)^2/\log q\right). \tag{3.3}$$

To take an example of special interest, let $\mathscr{X}(q)$ be the set of primitive characters modulo q, and let $\phi'(q) := \#\mathscr{X}(q)$. From Möbius inversion applied to the relation $\sum_{d|q}\phi'(d)=\phi(q)$, we find that

$$\phi'(q) = q\prod_{p\|q}\left(1-\frac{2}{q}\right)\prod_{p^2|q}\left(1-\frac{1}{q}\right)^2.$$

Hence, $\phi'(q)>0$ precisely when $q\not\equiv 2 \pmod 4$, and whenever $\phi'(q)$ is nonvanishing, we have

$$\phi'(q) \gg \phi(q)\prod_{p|q}(1-1/p) \gg \phi(q)/\log_2 q.$$

So when $q\not\equiv 2 \pmod 4$, estimate (3.3) shows that the average of n_χ taken over primitive characters χ modulo q is $\ell(q)+O((\log_2 q)^3/\log q)$. From this, one can deduce a corollary similar to Corollary 1.2. One replaces Lemma 3.1 with the following estimate, which can be proved by a similar argument:

Lemma 3.2. *Let m be a natural number. For $x\ge 1$, we have that*

$$\sum_{\substack{n\le x \\ \gcd(n,m)=1}} \phi'(n) = \frac{18x^2}{\pi^4}\left(\prod_{p|m}\frac{p^3}{(p+1)(p^2-1)}\right) + O(2^{\omega(m)}x(\log(\mathrm{e}x))^2),$$

uniformly in m.

Imitating the proof of Corollary 1.2 but using Lemma 3.2 as input, one eventually finds that as $x \to \infty$,

$$\frac{\sum_{1<q\le x} \sum^{*}_{\chi} n_\chi}{\sum_{1<q\le x} \sum^{*}_{\chi} 1} \to \sum_{\ell} \frac{\ell^4}{(\ell+1)(\ell^2-1)} \prod_{p<\ell} \frac{p^2-p-1}{(p+1)(p^2-1)},$$

where $\sum^*$ indicates a sum over primitive characters modulo q. MATHEMATICA evaluates the right-hand sum as

$$2.1514351056861465486242810050965840532633045718584 5\ldots.$$

4. Proof of Theorem 1.3

The first ingredient of the proof of Theorem 1.3 is a now classical theorem of Davenport and Heilbronn [DH71]:

Proposition 4.1. *As $x \to \infty$, the number of cubic fields K with $|D_K| \le x$ is $\sim \frac{x}{3\zeta(3)}$, as $x \to \infty$.*

A refined version of the Davenport–Heilbronn theorem was proposed by Roberts [Rob01] and recently confirmed by Taniguchi and Thorne [TT11] (See also the independent work of Bhargava, Shankar, and Tsimerman [BST10].) One consequence of their work is the following estimate (see [TT11, Theorem 1.3]):

Proposition 4.2. *Let $x \ge 1$, and let $y = \frac{1}{50}\log x$. For each prime $p \le y$, we define local factors c_p and c'_p, depending on the desired splitting type of p, as follows:*

$$c_p := \begin{cases} 1/6 & \text{if } p \text{ is to split completely,} \\ 1/2 & \text{if } p \text{ is to split partially,} \\ 1/3 & \text{if } p \text{ is to be inert,} \\ 1/p & \text{if } p \text{ is to partially ramify,} \\ 1/p^2 & \text{if } p \text{ is to ramify completely,} \end{cases}$$

and

$$c'_p = \frac{c_p}{1+1/p+1/p^2}.$$

The number of cubic number fields K (up to isomorphism) with $|D_K| \le x$ and which satisfy these conditions is

$$\frac{x}{3\zeta(3)} \prod_{p\le y} c'_p + O(x^{5/6}),$$

uniformly in the choice of splitting conditions.

If K is a cubic field with non-cyclic Galois group, then the normal closure of $K/\mathbf{Q}$ contains a unique quadratic subfield, called the *quadratic resolvent* of K. If K is cyclic, we adopt the convention that K has quadratic resolvent $\mathbf{Q}$; in both cases, the quadratic resolvent is $\mathbf{Q}(\sqrt{D_K})$. The next lemma provides an upper bound on the number of cubic fields with a given quadratic resolvent. It should be noted that Cohen and Morra [CM11] have asymptotic results for this problem for a *fixed* quadratic resolvent, but in our application we require some uniformity.

Lemma 4.3. *As $x \to \infty$, the number of cubic fields of discriminant $\le x$ with a prescribed quadratic resolvent L is at most $x^{5/6+o(1)}$, uniformly in L.*

Proof. Suppose that K has quadratic resolvent L and that $|D_K| \le x$. Then $D_K = f^2 D_L$ for some positive integer f. Clearly, $f \le x^{1/2}$. So the number of choices for D_K is also $\le x^{1/2}$. Ellenberg and Venkatesh [EV07] have shown that the number of cubic fields with discriminant D is $\ll_\epsilon |D|^{1/3+\epsilon}$, and so the lemma follows upon summing over the possibilities for $D = D_K$. □

To handle the contribution to the average from fields K for which n_K is large, we need two results. The first is a universal upper bound on n_K, due to Li [Li11]:

Proposition 4.4. *If K is a cubic field, then the least non-split prime in K is $\ll |D_K|^{1/7.39}$.*

As discussed by Li, it is much simpler to prove Proposition 4.4 with the larger exponent $\frac{1}{4\sqrt{e}} + \epsilon$, which would also suffice for our purposes.

The next result, in slightly stronger form, appears without proof in a paper of Duke and Kowalski [DK00] (for details, see the proof of Lemma 5.3 in [Pol11]). Baier [Bai06] has a sharper result allowing one to replace $2/A$ below with $1/(A-1)$, but we shall not need this.

Lemma 4.5. *Fix $A > 2$. The number of primitive Dirichlet characters χ of conductor $\le x$ with $\chi(p) = 1$ for all primes $p \le (\log x)^A$ is at most at most $x^{2/A+o(1)}$, as $x \to \infty$.*

Proof of Theorem 1.3. Set $y := \frac{1}{50}\log x$, and set $z := (\log x)^{100}$. Denoting n_K by r, we consider the contribution to the average from three ranges of n_K:

(i) $r \le y$,
(ii) $y < r \le z$,
(iii) $r > z$.

For the contribution of those r in range (i), Proposition 4.2 shows that

$$\sum_{\substack{|D_K|\le x\\ n_K \le y}} n_K = \frac{x}{3\zeta(3)} \sum_{r \le y} \frac{r(5/6 + 1/r + 1/r^2)}{1 + 1/r + 1/r^2} \prod_{p<r} \frac{1/6}{1 + 1/p + 1/p^2} + O(x^{9/10})$$

$$= \left(\frac{1}{3\zeta(3)} + o(1)\right) x \sum_{r} \frac{r(5/6 + 1/r + 1/r^2)}{1 + 1/r + 1/r^2} \prod_{p<r} \frac{1/6}{1 + 1/p + 1/p^2}.$$

By the same proposition, the number of cubic fields K with $|D_K| \le x$ for which every prime $p \le y$ splits completely is

$$\ll x/6^{\pi(y)} + x^{5/6} \ll x/\exp\left(\frac{\log x}{30\log\log x}\right),$$

and so

$$\sum_{\substack{|D_K|\le x\\ y<n_K \le z}} n_K \ll z \cdot x/\exp\left(\frac{\log x}{30\log\log x}\right) \ll x/\exp\left(\frac{\log x}{31\log\log x}\right),$$

say. In particular, this contribution is $o(x)$.

Finally, suppose that $r > z$. Then every prime $p \le z$ splits completely in the normal closure of K, and so also splits in the quadratic resolvent L of K. But the number of quadratic fields of discriminant $\le x$ in which every prime $p \le z$ splits is $\le x^{1/50+o(1)}$. To see this, note that if L is a quadratic field with this property, then $\chi(\cdot) := \left(\frac{D_L}{\cdot}\right)$ is a primitive character of conductor $\le x$ with $\chi(p) = 1$ for all $p \le z$. The stated estimate now follows from Lemma 4.5. By Lemma 4.3, the number of corresponding cubic extensions K is at most

$$x^{1/50+5/6+o(1)}.$$

Finally, for each such K, Proposition (4.4) shows that $n_K \ll x^{1/7.39}$. So as $x \to \infty$,

$$\sum_{\substack{|D_K| \le x \\ n_K > z}} n_K \le x^{1/7.39+1/50+5/6+o(1)}.$$

The exponent here is < 0.99 for large x, and so this contribution is $o(x)$. Recalling that the denominator in (1.5) is $\sim \frac{1}{3\zeta(3)}x$, Theorem 1.3 follows. □

Remark. For each natural number k and each prime $p \equiv 1 \pmod{k}$, let $r_k(p)$ denote the least prime kth power residue modulo p. Elliott [Ell71] has shown that for each of $k = 2, 3$, and 4, the function $r_k(p)$ possesses a finite mean value. When $k = 3$, Elliott's result gives the average smallest split prime in cubic extensions of prime conductor.

Motivated by Elliott's work, one might wonder if it is possible dto obtain the average least split prime, taken over all cubic extensions of $\mathbf{Q}$ (ordered as in Theorem 1.3). One could ask the same question for the least partially split or inert prime. Following the proof of Theorem 1.3, one can establish the following:

Theorem 4.6. *Assume the Riemann Hypothesis for Dedekind zeta functions. For each prime p, define*

$$c'_{p,\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} = \frac{1/6}{1+1/p+1/p^2}, \quad c'_{p,\mathfrak{p}_1\mathfrak{p}_2} = \frac{1/2}{1+1/p+1/p^2}, \quad \textit{and} \quad c'_{p,\mathfrak{p}_1} = \frac{1/3}{1+1/p+1/p^2}.$$

The average least totally split prime in a cubic field is given by

$$\sum_r r c'_{r,\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} \prod_{p<r} (1 - c'_{p,\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3}) = 19.7952216366\ldots.$$

The average least inert prime is given by

$$\sum_r r c'_{r,\mathfrak{p}_1} \prod_{p<r} (1 - c'_{p,\mathfrak{p}_1}) = 8.5447294614\ldots.$$

Finally, if the average is restricted now to non-Galois cubic fields, the average least partially split prime is given by

$$\sum_r r c'_{r,\mathfrak{p}_1\mathfrak{p}_2} \prod_{p<r} (1 - c'_{p,\mathfrak{p}_1\mathfrak{p}_2}) = 5.3680248421\ldots.$$

The proofs mimic that of Theorem 4.6. However, the most difficult range of r, namely range (iii), can now be ignored. Indeed, under GRH, the least unramified prime p with a prescribed splitting type is $\ll \log^2 |D_K|$ (see [LO77], [LMO79]). It would be interesting to find an unconditional proof for any of the assertions of Theorem 4.6.

Acknowledgements

The authors thank Carl Pomerance for helpful conversations and Mits Kobayashi for technical assistance with Karim Belabas's `cubics` package.

References

[Ank52] N. C. Ankeny, *The least quadratic non residue*, Ann. of Math. (2) **55** (1952), 65–72.

[Bac90] E. Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), no. 191, 355–380.

[Bai06] S. Baier, *On the least n with $\chi(n) \neq 1$*, Q. J. Math. **57** (2006), no. 3, 279–283.

[Bel97] K. Belabas, *A fast algorithm to compute cubic fields*, Math. Comp. **66** (1997), no. 219, 1213–1237, software package `cubics` available from `http://www.math.u-bordeaux1.fr/~belabas/research/`.

[Bel04] ———, *On quadratic fields with large 3-rank*, Math. Comp. **73** (2004), no. 248, 2061–2074.

[BH96] R. C. Baker and G. Harman, *The Brun-Titchmarsh theorem on average*, Analytic number theory, Vol. 1 (Allerton Park, IL, 1995), Progr. Math., vol. 138, Birkhäuser Boston, Boston, MA, 1996, pp. 39–103.

[BH98] ———, *Shifted primes without large prime factors*, Acta Arith. **83** (1998), no. 4, 331–361.

[BST10] M. Bhargava, A. Shankar, and J. Tsimerman, *On the Davenport-Heilbronn theorem and second order terms*, e-print at `arXiv:1005.0672 [math.NT]`.

[Bur97] R. J. Burthe, Jr., *The average least witness is* 2, Acta Arith. **80** (1997), no. 4, 327–341.

[CM11] H. Cohen and A. Morra, *Counting cubic extensions with given quadratic resolvent*, J. Algebra **325** (2011), 461–478.

[DH71] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A **322** (1971), no. 1551, 405–420.

[DK00] 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.

[Ell68] P. D. T. A. Elliott, *A problem of Erdős concerning power residue sums*, Acta Arith. **13** (1967/1968), 131–149.

[Ell71] ———, *The least prime k-th-power residue*, J. London Math. Soc. (2) **3** (1971), 205–210.

[Erd61] P. Erdős, *Remarks on number theory. I*, Mat. Lapok **12** (1961), 10–17 (Hungarian).

[EV07] J. S. Ellenberg and A. Venkatesh, *Reflection principles and bounds for class group torsion*, Int. Math. Res. Not. IMRN (2007), no. 1, Art. ID rnm002, 18 pp.

[Jut77] M. Jutila, *On Linnik's constant*, Math. Scand. **41** (1977), no. 1, 45–62.

[KP05] P. Kurlberg and C. Pomerance, *On the periods of the linear congruential and power generators*, Acta Arith. **119** (2005), no. 2, 149–169.

[Li11] X. Li, *The smallest prime that does not split completely in a number field*, Algebra and Number Theory (2011), to appear, e-print at `arXiv:1003.5718 [math.NT]`.

[LMO79] J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Invent. Math. **54** (1979), no. 3, 271–296.

[LO77] 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.

[Mon94] H. L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, CBMS Regional Conference Series in Mathematics, vol. 84, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1994.

[Nor98] K. K. Norton, *A character-sum estimate and applications*, Acta Arith. **85** (1998), no. 1, 51–78.

[Pol11] P. Pollack, *The average least quadratic nonresidue modulo m and other variations on a theme of Erdős*, submitted, available from `http://www.math.ubc.ca/~pollack/work.html`.

[Rob01] D. P. Roberts, *Density of cubic field discriminants*, Math. Comp. **70** (2001), no. 236, 1699–1705 (electronic).

[Ten95] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics, vol. 46, Cambridge University Press, Cambridge, 1995.

[TT11] T. Taniguchi and F. Thorne, *Secondary terms in counting functions for cubic fields*, submitted, e-print at `arXiv:1102.2914 [math.NT]`.

University of British Columbia, Department of Mathematics, Room 121, 1984 Mathematics Road, Vancouver, BC Canada V6T 1Z2

E-mail address: `gerg@math.ubc.ca`

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