PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 142, Number 6, June 2014, Pages 1925–1934
S 0002-9939(2014)12199-X
Article electronically published on March 5, 2014

THE SMALLEST PRIME THAT SPLITS COMPLETELY IN AN ABELIAN NUMBER FIELD

PAUL POLLACK

(Communicated by Ken Ono)

Abstract. Let $K/\mathbf{Q}$ be an abelian extension and let D be the absolute value of the discriminant of K. We show that for each $\varepsilon > 0$, the smallest rational prime that splits completely in K is $O(D^{\frac{1}{4}+\varepsilon})$. Here the implied constant depends only on ε and the degree of K. This generalizes a theorem of Elliott, who treated the case when $K/\mathbf{Q}$ has prime conductor.

1. Introduction

Let K be a number field. Kronecker conjectured that the proportion of rational primes p which split completely in K is well-defined and given exactly by $1/[L : \mathbf{Q}]$, where L is the normal closure of $K/\mathbf{Q}$. This conjecture, and much more, follows from the Frobenius (or Chebotarev) density theorem (see, e.g., [9]). Since split-completely primes are plentiful in this sense, it is natural to ask for an estimate of the least rational prime p that splits completely in K.

Suppose that $K/\mathbf{Q}$ is Galois, and let D denote the absolute value of the discriminant of K. If one assumes the Generalized Riemann Hypothesis, then work of Lagarias and Odlyzko on effective versions of the Chebotarev density theorem [11] shows that there is a split-completely prime $p \ll \log^2(2|D|)$ (see also [1], which makes this numerically explicit in the abelian case). Unconditionally, we have only much weaker results. From a general theorem of Lagarias, Montgomery, and Odlyzko [10, Theorem 1.1], we know that there is a prime $p \ll D^A$ which splits completely in K, for a certain absolute constant A (left unspecified in [10]). In this note, we consider the special case when $K/\mathbf{Q}$ is abelian of fixed degree and we show that one can take any $A > \frac{1}{4}$.

Theorem 1. *Let K be an abelian extension of $\mathbf{Q}$ and let $\varepsilon > 0$. The least prime p which splits completely in K satisfies*

$$p \ll D^{\frac{1}{4}+\varepsilon}.$$

Here D is the absolute value of the discriminant of K, and the implied constant depends only on ε and the degree of $K/\mathbf{Q}$.

Special cases of Theorem 1 are already in the literature in the guise of estimates for the least prime kth power residue to a prime modulus. When $K/\mathbf{Q}$ is a quadratic field of prime conductor, Theorem 1 reduces to an earlier result of Linnik and Vinogradov [24]. An elementary version of their proof was later discovered by Pintz [21]. More generally, if we restrict to extensions $K/\mathbf{Q}$ of prime conductor (which

Received by the editors July 9, 2012.
2010 *Mathematics Subject Classification.* Primary 11R44; Secondary 11L40, 11R42.

are necessarily cyclic), then Theorem 1 reduces to a theorem of Elliott [5]. Our proof of Theorem 1 employs the same general strategy as these earlier papers, but we have to modify the argument to account for the fact that the nontrivial Dirichlet characters attached to K need not share the same conductor. As in Pintz's work, we arrange the details to avoid contour integration.

We discuss some preliminaries for the proof of Theorem 1 in §2. The proof itself is presented in §3. In the final section, we compare Theorem 1 with what one obtains from a direct application of the known results on the least prime in an arithmetic progression.

The reader may wish to compare our results with those known for the complementary problem of estimating the least prime that does not split completely. For this, see the papers of K. Murty [20], Vaaler and Voloch [23], and Li [13].

Notation. We employ the Landau–Bachmann o and O notations, as well as the associated Vinogradov symbols $\ll$ and $\gg$, with their usual meanings. Any dependence of implied constants is indicated explicitly, usually with subscripts. Throughout, the letter p is reserved for a prime variable. We use $\star$ for Dirichlet convolution, so that $(f \star g)(n) := \sum_{de=n} f(d)g(e)$. We let $\mathbf{1}$ denote the arithmetic function which is identically 1. We write $\tau_k(n)$ for the k-fold Piltz divisor function, which is the k-fold convolution of the function $\mathbf{1}$ with itself. Thus, $\tau_2(n)$ is the usual number-of-divisors function, which we write simply as $\tau(n)$. The fractional part of the real number x is denoted $\{x\}$.

2. Preliminaries

The appearance of the exponent $\frac{1}{4}$ in Theorem 1 suggests, correctly, that Burgess's estimates for short character sums ([2, Theorem 2] and [3]) will play a key role in our proofs. In the original formulation of Burgess, these bounds achieve their full strength only when the conductor of the character χ is cubefree. In our problem, this translates into the requirement that $K/\mathbf{Q}$ have cubefree conductor. To avoid imposing this restriction, we use a variant of Burgess's bounds, due to Heath-Brown (see [8, Lemma 2.4]), which is effective whenever χ has small order.

Proposition 2 (Heath-Brown)**.** *Let $q > 1$, and suppose that χ is a primitive character mod q whose order divides the natural number k. Let $\varepsilon > 0$, and let r be a positive integer. Then for every pair of integers M and N with $N > 0$, we have*

$$\left| \sum_{M<n\le M+N} \chi(n) \right| \ll_{r,\varepsilon} k^{\frac{3}{2r}} N^{1-1/r} q^{\frac{r+1}{4r^2}+\varepsilon}.$$

Rather than work directly with Proposition 2, it will be more convenient for us to use the following consequence of that result.

Lemma 3. *Let $q > 1$, and let χ be a primitive character modulo q of order dividing k. Suppose that $0 < \delta \le \frac{1}{3}$. For $N \ge q^{\frac{1}{4}+\delta}$, we have*

$$\sum_{n\le N} \chi(n) \ll_{\delta,k} N^{1-\delta^2}.$$

Proof. Suppose that $N \geq q^{\frac{1}{4}+\delta}$. Then with r and ε still to be determined, Proposition 2 (with $M = 0$) gives

$$\sum_{n \leq N} \chi(n) \ll_{r,\varepsilon,k} N^{1-1/r} q^{\frac{r+1}{4r^2}+\varepsilon} \leq N^{1-1/r} \cdot N^{\frac{(r+1)/(4r^2)+\varepsilon}{1/4+\delta}} = N \cdot N^{\frac{1/(4r^2)+\varepsilon-\delta/r}{1/4+\delta}}. \tag{2.1}$$

We choose $r = \lceil \frac{1}{2\delta} \rceil$ and $\varepsilon = \frac{\delta^2}{60}$. Using that $0 < \delta \leq \frac{1}{3}$, we see that

$$\frac{1}{2\delta} \leq r < \frac{1}{2\delta} + 1 = \frac{1}{\delta}\left(\frac{1}{2} + \delta\right) \leq \frac{5}{6\delta},$$

so that

$$\frac{1}{4r^2} - \frac{\delta}{r} = \frac{1}{r}\left(\frac{1}{4r} - \delta\right) \leq -\frac{\delta}{2r} \leq -\frac{3}{5}\delta^2.$$

Since $\varepsilon = \frac{\delta^2}{60}$, the numerator in the final exponent on N in (2.1) is at most $-7\delta^2/12$. But the denominator in (2.1) is $\frac{1}{4} + \delta$, which is at most $\frac{7}{12}$. This proves the lemma. □

The second essential component in our argument is a lower bound on the absolute value of $L(1, \chi)$.

Proposition 4. *Let $q > 1$, and let χ be a primitive character modulo q. Let $\varepsilon > 0$. Then*

$$|L(1, \chi)| \gg_\varepsilon q^{-\varepsilon}.$$

For quadratic characters, the assertion of Proposition 4 is "Siegel's theorem" (proved as [19, Theorem 11.14, p. 372]). For nonreal χ, one has the much sharper estimate $|L(1, \chi)| \gg 1/\log q$ (a special case of [19, Theorem 11.4, pp. 362–363]), originally due to Landau [12].

3. Proof of Theorem 1

Since Theorem 1 is trivial when $K = \mathbf{Q}$, we will assume that $K/\mathbf{Q}$ is a nontrivial extension, so that $D > 1$. Let $\zeta_K(s)$ denote the Dedekind zeta function of K, and let $k := [K : \mathbf{Q}]$. By class field theory, there is a group of primitive Dirichlet characters $\chi_0 = \mathbf{1}, \chi_1, \ldots, \chi_{k-1}$ of conductors $q_0 = 1$, q_1, $\ldots$, q_{k-1}, respectively, with

$$\zeta_K(s) = \zeta(s) \prod_{i=1}^{k-1} L(s, \chi_i). \tag{3.1}$$

For future applications of Lemma 3, note that each of the χ_i has order dividing k. By the conductor-discriminant formula [25, Theorem 3.11, p. 27],

$$D = q_1 \cdots q_{k-1}. \tag{3.2}$$

We can (and do) assume in the sequel that the ε in Theorem 1 satisfies $0 < \varepsilon < \frac{2}{3}$.

We now introduce some convenient notation. For each $1 \leq i \leq k-1$, put

$$y_i := \max\{q_i^{\frac{1}{4}+\frac{\varepsilon}{2}}, D^{\frac{\varepsilon}{2k}}\}, \tag{3.3}$$

and set

$$y := \prod_{i=1}^{k-1} y_i. \tag{3.4}$$

Note that from (3.2), we have

$$D^{\frac{1}{4}+\frac{\varepsilon}{2}} \le y < D^{\frac{1}{4}+\varepsilon}. \tag{3.5}$$

By definition, we can write $\zeta_K(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$, where a_n counts the number of (integral) ideals of K of norm n. To prove Theorem 1, we will show that if no prime up to $D^{\frac{1}{4}+\varepsilon}$ splits completely in K, then K has "too few" ideals of norm bounded by y.

Lemma 5. *Assume that every prime that splits completely in K exceeds $D^{\frac{1}{4}+\varepsilon}$. Then with y defined as in* (3.4),

$$\sum_{n\le y} a_n \ll_k y^{3/4}.$$

Proof. Exploiting the Euler-factorization of $\zeta_K(s)$, we see that

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_p (1-p^{-f_p s})^{-g_p}, \tag{3.6}$$

where f_p is the inertial degree of any prime ideal $\mathfrak{p}$ of K lying above p and g_p is the number of such prime ideals. Let p be a prime with $p \le y$. Since p does not split completely in K, either $p \mid D$ or $f_p > 1$. It follows from (3.6) that if $n \le y$ and $a_n \ne 0$, then one can write $n = n_1 n_2$, where n_1 is a squarefree divisor of D and n_2 is squarefull. Since the number of squarefull $n_2 \le y$ is $\ll y^{1/2}$ (see, e.g., [6]) while $\tau(D) \ll D^{1/32}$ (in fact, $\tau(D) \ll_\varepsilon D^\varepsilon$; see [7, Theorem 315, p. 343]), the number of $n \le y$ with a_n nonvanishing is

$$\ll y^{1/2} D^{1/32} < y^{1/2} y^{1/8} = y^{5/8}.$$

On the other hand, (3.1) shows that for every natural number n,

$$a_n = (\mathbf{1} \star \chi_1 \star \chi_2 \star \cdots \star \chi_{k-1})(n) \le \tau_k(n).$$

Since $\tau_k(n) \le \tau(n)^{k-1} \ll_k n^{1/8}$, we find that $\sum_{n\le y} a_n \ll_k y^{5/8} \cdot y^{1/8} = y^{3/4}$, as claimed. □

We proceed to estimate $\sum_{n\le y} a_n$ in a different way. Using the convolution identity $a_n = (\mathbf{1} \star \chi_1 \star \chi_2 \star \cdots \star \chi_{k-1})(n)$, we can write $\sum_{n\le y} a_n$ as

$$\begin{aligned} &\sum_{d_1\cdots d_{k-1}\le y} \chi_1(d_1)\chi_2(d_2)\cdots\chi_{k-1}(d_{k-1}) \left\lfloor \frac{y}{d_1\cdots d_{k-1}} \right\rfloor \\ &\quad = y \sum_{d_1\cdots d_{k-1}\le y} \frac{\chi_1(d_1)}{d_1}\cdots\frac{\chi_{k-1}(d_{k-1})}{d_{k-1}} \\ &\qquad - \sum_{d_1\cdots d_{k-1}\le y} \chi_1(d_1)\cdots\chi_{k-1}(d_{k-1}) \left\{ \frac{y}{d_1\cdots d_{k-1}} \right\}. \end{aligned} \tag{3.7}$$

We estimate the two right-hand-side terms in the next two lemmas.

Lemma 6. *We have*

$$\sum_{d_1\cdots d_{k-1}\le y} \frac{\chi_1(d_1)}{d_1}\cdots\frac{\chi_{k-1}(d_{k-1})}{d_{k-1}} = L(1,\chi_1)L(1,\chi_2)\cdots L(1,\chi_{k-1}) + O_{\varepsilon,k}(D^{-\frac{\varepsilon^2}{20k}}).$$

Proof. We partition the sum on the left-hand side according to the sizes of the d_i. For each $(k-1)$-tuple $(d_1,\dots,d_{k-1})$ with $d_1\cdots d_{k-1}\le y$, let $\mathscr{S}_{(d_1,\dots,d_{k-1})}=\{1\le i\le k-1: d_i>y_i\}$. For each subset $\mathscr{S}\subset\{1,2,\dots,k-1\}$, let $\mathscr{I}(\mathscr{S})=\{(d_1,\dots,d_{k-1}):\mathscr{S}_{(d_1,\dots,d_{k-1})}=\mathscr{S}\}$. Clearly,

(3.8)
$$\sum_{d_1\cdots d_{k-1}\le y}\frac{\chi_1(d_1)}{d_1}\cdots\frac{\chi_{k-1}(d_{k-1})}{d_{k-1}}=\sum_{\mathscr{S}}\sum_{(d_1,\dots,d_{k-1})\in\mathscr{I}(\mathscr{S})}\frac{\chi_1(d_1)}{d_1}\cdots\frac{\chi_{k-1}(d_{k-1})}{d_{k-1}}.$$

We first estimate the contribution to the right-hand side of (3.8) from $\mathscr{S}=\emptyset$. Since $y=\prod y_i$, we have

$$\sum_{(d_1,\dots,d_{k-1})\in\mathscr{I}(\emptyset)}\frac{\chi_1(d_1)}{d_1}\cdots\frac{\chi_{k-1}(d_{k-1})}{d_{k-1}}=\prod_{i=1}^{k-1}\sum_{d_i\le y_i}\frac{\chi_i(d_i)}{d_i}.$$

For each $1\le i\le k-1$, put $S_i(t):=\sum_{n\le t}\chi_i(n)$. From Lemma 3 and the definition (3.3) of y_i, we have that $S_i(t)\ll_{\varepsilon,k}t^{1-\frac14\varepsilon^2}$ for $t\ge y_i$. Thus,

$$\begin{aligned}L(1,\chi_i)-\sum_{d_i\le y_i}\frac{\chi_i(d_i)}{d_i}&=-\frac{S_i(y_i)}{y_i}+\int_{y_i}^{\infty}\frac{S_i(t)}{t^2}\,\mathrm{d}t\\&\ll_{\varepsilon,k}y_i^{-\frac{\varepsilon^2}{4}}\le D^{-\frac{\varepsilon^3}{8k}}.\end{aligned}$$

(We use here that $y_i\ge D^{\frac{\varepsilon}{2k}}$.) So by Proposition 4 (with ε taken as $\frac{\varepsilon^3}{16k}$), we see that

$$\sum_{d_i\le y_i}\frac{\chi_i(d_i)}{d_i}=L(1,\chi_i)(1+O_{\varepsilon,k}(q_i^{\frac{\varepsilon^3}{16k}}D^{-\frac{\varepsilon^3}{8k}}))=L(1,\chi_i)(1+O_{\varepsilon,k}(D^{-\frac{\varepsilon^3}{16k}})).$$

Thus,

$$\begin{aligned}\prod_{i=1}^{k-1}\sum_{d_i\le y_i}\frac{\chi_i(d_i)}{d_i}&=L(1,\chi_1)\cdots L(1,\chi_{k-1})\left(1+O_{\varepsilon,k}(D^{-\frac{\varepsilon^3}{16k}})\right)\\&=L(1,\chi_1)\cdots L(1,\chi_{k-1})+O_{\varepsilon,k}(D^{-\frac{\varepsilon^3}{20k}}),\end{aligned}$$

using in the second line the crude upper bound $L(1,\chi_i)\ll\log q_i\le\log D$ (see, for example, [19, Lemma 10.15, p. 350]).

Now we study the contribution to the right-hand side of (3.8) from those sets $\mathscr{S}\ne\emptyset$. Fix such an $\mathscr{S}$. Then $i_0\in\mathscr{S}$ for some $1\le i_0\le k-1$. By the triangle inequality,

$$\begin{aligned}&\left|\sum_{(d_1,\dots,d_{k-1})\in\mathscr{I}(\mathscr{S})}\frac{\chi_1(d_1)}{d_1}\cdots\frac{\chi_{k-1}(d_{k-1})}{d_{k-1}}\right|\\&\qquad\le\sum_{d_i:\ i\ne i_0}\frac{1}{\prod_{i\ne i_0}d_i}\left|\sum_{y_{i_0}<d_{i_0}\le\frac{y}{\prod_{i\ne i_0}d_i}}\frac{\chi_{i_0}(d_{i_0})}{d_{i_0}}\right|;\end{aligned}$$

here the outer sum is over all tuples $\{d_i\}_{i\ne i_0}$ with the property that $(d_1,\dots,d_{k-1})\in\mathscr{I}(\mathscr{S})$ for some d_{i_0}. Writing $\Pi=\prod_{i\ne i_0}d_i$ and using S_i with the same meaning

as above,

$$\sum_{y_{i_0}<d_{i_0}\le y/\Pi}\frac{\chi_{i_0}(d_{i_0})}{d_{i_0}}=\frac{S_{i_0}(y/\Pi)}{y/\Pi}-\frac{S_{i_0}(y_{i_0})}{y_{i_0}}+\int_{y_{i_0}}^{y/\Pi}\frac{S_{i_0}(t)}{t^2}\,\mathrm{d}t$$
$$\ll_{\varepsilon,k}(y/\Pi)^{-\varepsilon^2/4}+y_{i_0}^{-\varepsilon^2/4}\ll y_{i_0}^{-\varepsilon^2/4}.$$

Thus,

$$\sum_{d_i:\ i\neq i_0}\frac{1}{\Pi}\left|\sum_{y_{i_0}<d_{i_0}\le y/\Pi}\frac{\chi_{i_0}(d_{i_0})}{d_{i_0}}\right|\ll_{\varepsilon,k} y_{i_0}^{-\frac{\varepsilon^2}{4}}\sum_{d_i:\ i\neq i_0}\frac{1}{\Pi}$$
$$\le D^{-\frac{\varepsilon^3}{8k}}\left(\sum_{d\le y}\frac{1}{d}\right)^{k-2}$$
$$\le D^{-\frac{\varepsilon^3}{8k}}(1+\log y)^{k-2}\ll_{\varepsilon,k} D^{-\frac{\varepsilon^3}{10k}}.$$

(Recall that each $y_i\ge D^{\varepsilon/2k}$ and that $y<D$.)

Adding our bound for $\mathscr{S}=\emptyset$ to our bounds for those $\mathscr{S}\neq\emptyset$ completes the proof of Lemma 6. □

Lemma 7. *We have*

$$\sum_{d_1\cdots d_{k-1}\le y}\chi_1(d_1)\cdots\chi_{k-1}(d_{k-1})\left\{\frac{y}{d_1\cdots d_{k-1}}\right\}\ll_{\varepsilon,k} yD^{-\frac{\varepsilon^3}{600k}}.$$

Proof. We start by throwing away those tuples for which $d_1\cdots d_{k-1}\le y'$, where $y':=y/D^{\varepsilon/4}$. Such tuples make a contribution bounded in absolute value by

$$\sum_{d_1\cdots d_{k-1}\le y'}1\le y'\left(\sum_{d\le y'}\frac{1}{d}\right)^{k-2}\le y'(1+\log y')^{k-2}$$
$$<yD^{-\varepsilon/4}(1+\log D)^{k-2}\ll_{\varepsilon,k} yD^{-\varepsilon/5}.$$

This is negligible compared to our target upper bound, and so we may restrict our attention to bounding that portion of the initial sum where $y'<d_1\cdots d_{k-1}\le y$. From (3.5), we have $y'\ge D^{\frac14+\frac{\varepsilon}{4}}$. Thus, if $d_1\cdots d_{k-1}>y'$, then some $d_i>y_i'$, where

$$y_i':=\max\{q_i^{\frac14+\frac{\varepsilon}{8}},D^{\frac{\varepsilon}{8k}}\}.$$

Also, if $d_1\cdots d_{k-1}>y'$, then clearly

$$\left\lfloor\frac{y}{d_1\cdots d_{k-1}}\right\rfloor<\frac{y}{y'}.$$

These observations suggest a convenient sorting of the remaining tuples $(d_1,\dots,d_{k-1})$. For each tuple $(d_1,\dots,d_{k-1})$ with $y'<d_1\cdots d_{k-1}\le y$, let $\mathscr{S}_{(d_1,\dots,d_{k-1})}=\{1\le i\le k-1: d_i>y_i'\}$. Since some $d_i>y_i'$, the set $\mathscr{S}_{(d_1,\dots,d_{k-1})}$ is always nonempty. For each nonempty subset $\mathscr{S}\subset\{1,2,\dots,k-1\}$ and each positive integer $m<y/y'$, let

$$\mathscr{I}(\mathscr{S},m):=\left\{(d_1,\dots,d_{k-1}):\mathscr{S}_{(d_1,\dots,d_{k-1})}=\mathscr{S},\ \left\lfloor\frac{y}{d_1\cdots d_k}\right\rfloor=m\right\}.$$

Then

$$\sum_{y'<d_1\cdots d_{k-1}\le y} \chi_1(d_1)\cdots\chi_{k-1}(d_{k-1})\left\{\frac{y}{d_1\cdots d_{k-1}}\right\}$$
$$= \sum_{\mathscr{S},m}\ \sum_{(d_1,\dots,d_{k-1})\in\mathscr{I}(\mathscr{S},m)} \chi_1(d_1)\cdots\chi_{k-1}(d_{k-1})\left\{\frac{y}{d_1\cdots d_{k-1}}\right\}.$$

We proceed to bound the contribution to the right-hand side from each pair $\mathscr{S}, m$.

Fix a pair $\mathscr{S}$ and m, and fix an $i_0\in\mathscr{S}$. Suppose we are given a tuple $\{d_i\}_{i\ne i_0}$ for which $(d_1,\dots,d_{k-1})\in\mathscr{I}(\mathscr{S},m)$ for some d_{i_0}. Then the set of d_{i_0} with this property consists exactly of those integers satisfying

$$M < d_{i_0} \le \frac{y}{m\Pi}, \quad \text{where} \quad M := \max\left\{y'_{i_0}, \frac{y}{(m+1)\Pi}, \frac{y'}{\Pi}\right\} \quad \text{and} \quad \Pi := \prod_{i\ne i_0} d_i.$$

(Of course, M and Π depend on the tuple $\{d_i\}_{i\ne i_0}$, but we suppress this for the sake of readability.) Thus,

$$\left|\sum_{(d_1,\dots,d_{k-1})\in\mathscr{I}(\mathscr{S},m)} \chi_1(d_1)\cdots\chi_{k-1}(d_{k-1})\left\{\frac{y}{d_1\cdots d_{k-1}}\right\}\right| \le \sum_{d_i:\ i\ne i_0}\left|\sum_{M<d_{i_0}\le\frac{y}{m\Pi}} \chi_{i_0}(d_{i_0})\left\{\frac{y}{d_{i_0}\Pi}\right\}\right|. \tag{3.9}$$

In the new inner sum, $\lfloor\frac{y}{d_{i_0}\Pi}\rfloor = m$ is constant, so that $\{\frac{y}{d_{i_0}\Pi}\}$ is a decreasing function of d_{i_0}; now using Abel's inequality, we find that

$$\left|\sum_{M<d_{i_0}\le\frac{y}{m\Pi}} \chi_{i_0}(d_{i_0})\left\{\frac{y}{d_{i_0}\Pi}\right\}\right| \le \max_{M<u\le\frac{y}{m\Pi}}\left|\sum_{M<d_{i_0}\le u}\chi_{i_0}(d_{i_0})\right|.$$

Since $M\ge y'_{i_0}\ge q^{\frac14+\frac{\varepsilon}{8}}$, Lemma 3 gives that the final sum is $\ll_{\varepsilon,k} u^{1-\frac{\varepsilon^2}{64}}$, and thus the maximum over u is

$$\ll_{\varepsilon,k} \frac{y}{m\Pi}\left(\frac{y}{m\Pi}\right)^{-\varepsilon^2/64} \le \left(\frac{y}{m\Pi}\right)M^{-\frac{\varepsilon^2}{64}} \le \frac{y}{m\Pi}D^{-\frac{\varepsilon^3}{512k}}.$$

(We use that $M\ge y'_{i_0}\ge D^{\frac{\varepsilon}{8k}}$.) Substituting back into (3.9), we find that the contribution from the pair $\mathscr{S}$ and m is

$$\ll_{\varepsilon,k} \frac{y}{m}D^{-\frac{\varepsilon^3}{512k}}\sum_{d_i:\ i\ne i_0}\frac{1}{\Pi} \le \frac{y}{m}D^{-\frac{\varepsilon^3}{512k}}\left(\sum_{d\le y}\frac{1}{d}\right)^{k-2} \le \frac{y}{m}D^{-\frac{\varepsilon^3}{512k}}(1+\log y)^{k-2}.$$

Now summing over all $m<y/y'$ and over all $O_k(1)$ possibilities for $\mathscr{S}$, we obtain an upper bound that is

$$\ll_{\varepsilon,k} yD^{-\frac{\varepsilon^3}{512k}}(1+\log y)^{k-1} \ll_{\varepsilon,k} yD^{-\frac{\varepsilon^3}{600k}},$$

as desired. □

Proof of Theorem 1. By (3.7) and Lemmas 6 and 7, we have that

$$\sum_{n\le y} a_n = yL(1,\chi_1)\cdots L(1,\chi_{k-1}) + O_{\varepsilon,k}(yD^{-\frac{\varepsilon^3}{600k}}).$$

Now suppose that the least split-completely prime in K exceeds $D^{\frac{1}{4}+\varepsilon}$. Then from Lemma 5, we get that $\sum_{n\le y} a_n \ll_k y^{3/4}$. Putting these last two estimates together shows that

$$\begin{aligned} L(1,\chi_1)\cdots L(1,\chi_{k-1}) &\ll_{\varepsilon,k} y^{-1/4} + D^{-\frac{\varepsilon^3}{600k}} \\ &\le D^{-1/16} + D^{-\frac{\varepsilon^3}{600k}} \ll D^{-\frac{\varepsilon^3}{600k}}. \end{aligned}$$

But by Proposition 4, we have $|L(1,\chi_i)| \gg_{\varepsilon,k} q_i^{-\frac{\varepsilon^3}{700k}}$ (say) for each i, so that (3.2) gives

$$|L(1,\chi_1)\cdots L(1,\chi_{k-1})| \gg_{\varepsilon,k} D^{-\frac{\varepsilon^3}{700k}}.$$

Hence, $D \ll_{\varepsilon,k} 1$; that is, D is bounded (in terms of ε and k). This proves Theorem 1 for large D, with an implied constant of 1. If D is bounded, then there are only finitely many possibilities for the field K (for example, by Hermite's theorem [22, Theorem 3, p. 59]), and Theorem 1 still holds after adjusting the value of the implied constant. □

Remark. The implied constant in Theorem 1 is in general ineffective because of the appeal to Siegel's theorem. However, if $[K:\mathbf{Q}]$ is odd, then all of the characters χ appearing in the factorization (3.1) of $\zeta_K(s)$ have odd order and so are nonreal. For nonreal χ, one has an effective lower bound $|L(1,\chi)| \gg 1/\log q$. (In fact, if χ has small odd order, one can get effective lower bounds that are significantly larger than $1/\log q$; see [19, Exercise 4, p. 366] and compare with [5, Lemma 2(ii)].) Since the implied constants in Burgess's bounds are also effective, the estimate of Theorem 1 can be made effective when $K/\mathbf{Q}$ has odd degree.

4. Comparison with Linnik's theorem

For an abelian extension $K/\mathbf{Q}$, the splitting behavior of a prime p is governed by the residue class of p modulo f, where f is the conductor of K. We conclude this note by comparing our Theorem 1 with what one obtains from Linnik's celebrated theorem [14, 15] on the least prime in an arithmetic progression:

Proposition 8 (Linnik)**.** *There is an absolute constant C with the following property: For every pair of coprime integers a and q with $q > 0$, the smallest prime $p \equiv a \pmod q$ satisfies $p \ll q^C$.*

Theorem 1 is superseded by Proposition 8 once the degree of $K/\mathbf{Q}$ is large. To see this, observe that if $K/\mathbf{Q}$ is abelian with conductor f, then any prime $p \equiv 1 \pmod f$ splits completely in K, and the least such p is $O(f^C)$. One can show that for each abelian extension, $D \ge f^{[K:\mathbf{Q}]/2}$ (compare with [4, Lemma 9.2.1, p. 431]). Thus, the least prime that splits completely in K is $O(D^{2C/[K:\mathbf{Q}]})$, which is superior to the estimate of Theorem 1 once $[K:\mathbf{Q}] \ge 8C$. In the opposite direction, the conductor f of K satisfies (in the notation of §3)

$$f = \operatorname{lcm}[q_1,\dots,q_{k-1}], \tag{4.1}$$

so that

$$D = \prod_{i=1}^{k-1} q_i \le f^{[K:\mathbf{Q}]-1}.$$

This shows that Theorem 1 does better than a naive application of Linnik's result if $[K:\mathbf{Q}] < 4C+1$.

Xylouris [26] has shown that $C = 5.18$ is allowable in Proposition 8. For q prime, Meng has shown that $C = 4.5$ is permissible [16], and he has claimed the same result for all q with an absolutely bounded cubefull part ([17], with a correction in [18]). Now if $K/\mathbf{Q}$ is abelian of degree k, then the cubefull part of f divides $(2k)^2$. Indeed, Heath-Brown has observed (see the bottom of [8, p. 271]) that if χ is any primitive character of order dividing k, then its conductor q has a cubefull part dividing $(2k)^2$; now apply (4.1). Thus, Meng's claim would yield the existence of a split-completely prime $p \ll_k f^{4.5}$. This is certainly better than Theorem 1 once $[K : \mathbf{Q}] \geq 36$.

Acknowledgements

The author thanks Enrique Treviño and the anonymous referee for their careful readings of the manuscript.

References

[1] Eric Bach and Jonathan Sorenson, *Explicit bounds for primes in residue classes*, Math. Comp. **65** (1996), no. 216, 1717–1735, DOI 10.1090/S0025-5718-96-00763-6. MR1355006 (97a:11143)

[2] D. A. Burgess, *On character sums and L-series. II*, Proc. London Math. Soc. (3) **13** (1963), 524–536. MR0148626 (26 #6133)

[3] D. A. Burgess, *The character sum estimate with $r = 3$*, J. London Math. Soc. (2) **33** (1986), no. 2, 219–226, DOI 10.1112/jlms/s2-33.2.219. MR838632 (87g:11098)

[4] Henri Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000. MR1728313 (2000k:11144)

[5] P. D. T. A. Elliott, *The least prime $k-$th-power residue*, J. London Math. Soc. (2) **3** (1971), 205–210. MR0281686 (43 #7401)

[6] S. W. Golomb, *Powerful numbers*, Amer. Math. Monthly **77** (1970), 848–855. MR0266878 (42 #1780)

[7] G. H. Hardy and E. M. Wright, *An introduction to the theory of number,* 6th ed., revised by D. R. Heath-Brown and J. H. Silverman, with a foreword by Andrew Wiles. Oxford University Press, Oxford, 2008. MR2445243 (2009i:11001)

[8] D. R. Heath-Brown, *Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression*, Proc. London Math. Soc. (3) **64** (1992), no. 2, 265–338, DOI 10.1112/plms/s3-64.2.265. MR1143227 (93a:11075)

[9] H. Heilbronn, *Zeta-functions and L-functions*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 204–230. MR0218327 (36 #1414)

[10] 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, DOI 10.1007/BF01390234. MR553223 (81b:12013)

[11] 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. MR0447191 (56 #5506)

[12] E. Landau, *Über Dirichletsche Reihen mit komplexen Charakteren*, J. Reine Angew. Math. **157** (1926), 26–32.

[13] Xiannan Li, *The smallest prime that does not split completely in a number field*, Algebra Number Theory **6** (2012), no. 6, 1061–1096, DOI 10.2140/ant.2012.6.1061. MR2968634

[14] U. V. Linnik, *On the least prime in an arithmetic progression. I. The basic theorem* (English, with Russian summary), Rec. Math. [Mat. Sbornik] N.S. **15(57)** (1944), 139–178. MR0012111 (6,260b)

[15] U. V. Linnik, *On the least prime in an arithmetic progression. II. The Deuring-Heilbronn phenomenon* (English, with Russian summary), Rec. Math. [Mat. Sbornik] N.S. **15(57)** (1944), 347–368. MR0012112 (6,260c)

[16] Zaizhao Meng, *The distribution of the zeros of L-functions and the least prime in some arithmetic progression*, Sci. China Ser. A **43** (2000), no. 9, 937–944, DOI 10.1007/BF02879799. MR1804045 (2001k:11178)

[17] Zaizhao Meng, *A note on the least prime in an arithmetic progression* (English, with English and Chinese summaries), Beijing Daxue Xuebao Ziran Kexue Ban **37** (2001), no. 1, 20–22. MR1841920

[18] Zaizhao Meng, *A note on the Linnik's constant*, `arXiv:1010.3544v1 [math.NT]`.

[19] Hugh L. Montgomery and Robert C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007. MR2378655 (2009b:11001)

[20] V. Kumar Murty, *The least prime which does not split completely*, Forum Math. **6** (1994), no. 5, 555–565, DOI 10.1515/form.1994.6.555. MR1295152 (95h:11131)

[21] J. Pintz, *Elementary methods in the theory of L-functions. VI. On the least prime quadratic residue* (mod ρ), Acta Arith. **32** (1977), no. 2, 173–178. MR0485735 (58 #5551e)

[22] Pierre Samuel, *Algebraic theory of numbers*, translated from the French by Allan J. Silberger, Houghton Mifflin Co., Boston, Mass., 1970. MR0265266 (42 #177)

[23] Jeffrey D. Vaaler and José Felipe Voloch, *The least nonsplit prime in Galois extensions of* $\mathbf{Q}$, J. Number Theory **85** (2000), no. 2, 320–335, DOI 10.1006/jnth.2000.2551. MR1802720 (2002a:11129)

[24] A. I. Vinogradov and Ju. V. Linnik, *Hypoelliptic curves and the least prime quadratic residue* (Russian), Dokl. Akad. Nauk SSSR **168** (1966), 259–261. MR0209223 (35 #125)

[25] Lawrence C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR1421575 (97h:11130)

[26] Triantafyllos Xylouris, *On the least prime in an arithmetic progression and estimates for the zeros of Dirichlet L-functions*, Acta Arith. **150** (2011), no. 1, 65–91, DOI 10.4064/aa150-1-4. MR2825574 (2012m:11129)

Department of Mathematics, University of Georgia, Athens, Georgia 30602
E-mail address: `pollack@uga.edu`