A NOTE ON THE LEAST PRIME THAT SPLITS COMPLETELY IN A NONABELIAN GALOIS NUMBER FIELD

ZHENCHAO GE, MICAH B. MILINOVICH, AND PAUL POLLACK

Abstract. We prove a nontrivial estimate for the size of the least rational prime that splits completely in the ring of integers of certain families of nonabelian Galois number fields. Our result complements results of Linnik and Vinogradov and of Pollack who studied this problem in the quadratic and abelian number field settings, respectively.

1. Introduction

One of the classical problems in number theory is to study the distribution of quadratic residues and non-residues modulo a prime p. I. M. Vinogradov conjectured that the least quadratic non-residue modulo p is $O_\varepsilon(p^\varepsilon)$ for any $\varepsilon > 0$. Recall that the least quadratic non-residue (mod p) is always a prime. Analogously, Vinogradov conjectured that the least prime quadratic residue modulo p is $O_\varepsilon(p^\varepsilon)$ as well. Neither of these conjectures has been established.

In this paper we study a generalization of the second problem, bounding the least prime quadratic residue modulo p. The Pólya-Vinogradov inequality and Siegel's theorem for exceptional zeros of Dirichlet L-functions imply that the least prime quadratic residue (mod p) is $O_\varepsilon(p^{1/2+\varepsilon})$ for any $\varepsilon > 0$. Yu. V. Linnik and A. I. Vinogradov [22] improved this estimate to $O_\varepsilon(p^{1/4+\varepsilon})$ using Burgess's estimates for character sums in place of the Pólya-Vinogradov inequality. Due to the use of Siegel's theorem, the implied constant in this estimate is ineffective. Pintz [14] later developed an elementary proof of the same bound using similar tools.

Since the least prime quadratic residue modulo an odd prime p is the smallest prime that splits completely in a quadratic number field with a discriminant of either p or $4p$ (depending on the residue class of p modulo 4), this problem generalizes to number fields. Let K be a Galois extension of $\mathbb{Q}$ with discriminant D_K and ring of integers $\mathcal{O}_K$. We aim to bound the least rational prime that splits completely in $\mathcal{O}_K$, denoted henceforth as q_K, in terms of $|D_K|$. As we show below, there is always a bound of the form $q_K \ll |D_K|^{1/2+\varepsilon}$ with an implied constant depending on ε and the degree $[K:\mathbb{Q}]$ of K over $\mathbb{Q}$. We refer to this as the *trivial bound* for this problem. For abelian extensions K over $\mathbb{Q}$, Pollack [15] recently proved the nontrivial estimate that $q_K \ll_{[K:\mathbb{Q}],\varepsilon} |D_K|^{1/4+\varepsilon}$ (see also [16]). This generalizes Linnik and Vinogradov's estimate for the quadratic extensions of $\mathbb{Q}$ and the proof uses similar

2000 *Mathematics Subject Classification.* 11R42, 11R44, 11F66, 11M20.

Key words and phrases. primes, split completely, number fields, Dedekind zeta-function, subconvexity.

Research of the second author was partially supported by the NSA Young Investigator Grants H98230-15-1-0231 and H98230-16-1-0311. Research of the third author was partly supported by NSF award DMS-1402268.

methods. Pollack's proof relies on essentially three ingredients: the factorization of the Dedekind zeta-function $\zeta_K(s)$ into Dirichlet L-functions, Burgess's estimates for character sums, and Siegel's theorem for exceptional zeros.

In this note, for certain nonabelian Galois extensions K over $\mathbb{Q}$, we prove nontrivial estimates for the size of the least prime that splits completely in $\mathcal{O}_K$. The methods in [22] and [15], mentioned above, do not immediately generalize to this setting. There is a generalization of Siegel's theorem for exceptional zeros known as the Brauer-Siegel theorem [2]. However, when a Galois extension $K/\mathbb{Q}$ is nonabelian, the Dedekind zeta-function $\zeta_K(s)$ does not factor into a product of Dirichlet L-functions and so we cannot use Burgess's estimates for character sums to estimate coefficients of $\zeta_K(s)$. In place of Burgess's estimates, we invoke subconvexity estimates for $\zeta_K(s)$ in the discriminant aspect. Such estimates are known when $\zeta_K(s)$ can be expressed in terms of product of automorphic L-functions for which level-aspect subconvexity bounds have been established. We give some examples of families of nonabelian number fields for which this is the case in the next section. To keep things slightly more general, we state our main theorem in terms of the following subconvexity hypothesis.

Hypothesis 1. *Let K be a number field of fixed degree m. There exist constants $\vartheta, A \geq 0$ (depending at most on m) such that for $\mathrm{Re}(s) = 1/2$, we have*

$$\zeta_K(s) \ll_m |s|^A |D_K|^{1/4-\vartheta}. \tag{1.1}$$

This hypothesis is stated by Einsiedler, Lindenstrauss, Michel, and Venkatesh in [6] where examples of families of number fields satisfying Hypothesis 1 are listed. In particular, they note that by results in [1, 3, 4, 7, 8, 11, 21] this hypothesis holds when $K/\mathbb{Q}$ is contained in a ring class field of an arbitrary quadratic extension of an arbitrary but fixed ground field F.

Assuming this Hypothesis 1, we prove the following theorem.

Theorem 1. *Let $K/\mathbb{Q}$ be a Galois extension of degree m, and let q_K denote the least prime that splits completely in $\mathcal{O}_K$. Assuming Hypothesis 1, we have*

$$q_K \ll |D_K|^{1/2-2\vartheta+\varepsilon} \tag{1.2}$$

for any $\varepsilon > 0$. Here the implied constant depends at most on ε and m.

The Phragmén-Lindelöf convexity principle implies that Hypothesis 1 always holds with $\vartheta = 0$. Therefore Theorem 1 implies that $q_K \ll_{\varepsilon,m} |D_K|^{1/2+\varepsilon}$. As mentioned above, we refer to this as the trivial bound for the least rational prime that splits completely in $\mathcal{O}_K$. The generalized Lindelöf hypothesis (GLH) implies that Hypothesis 1 holds with $\vartheta = 1/4$. Therefore, assuming GLH, Theorem 1 implies that $q_K \ll_{\varepsilon,m} |D_K|^{\varepsilon}$ for any $\varepsilon > 0$. This is the number field analogue of Vinogradov's conjecture for the least prime quadratic residue.

For abelian extensions $K/\mathbb{Q}$, the generalized Burgess method for estimating Dirichlet L-functions (e.g. [7, 8]) implies that $\vartheta = 3/8$ is admissible in Hypothesis 1 and hence, via Theorem 1, that $q_K \ll_{\varepsilon,m} |D_K|^{3/8+\varepsilon}$. Analogously, the stronger subconvexity estimate of Conrey and Iwaniec [4] for quadratic Dirichlet L-functions implies that $q_K \ll_{\varepsilon,m} |D_K|^{1/3+\varepsilon}$ for multiquadratic extensions $K/\mathbb{Q}$. While these estimates are nontrivial, they are weaker than the results of Vinogradov and Linnik [22] and of Pollack [15]. In the next section, we use Theorem 1 to give examples of nonabelian Galois number fields where the results in [22] and [15] do not apply.

If a Galois number field $K/\mathbb{Q}$ has a quadratic subfield, then the implied constant in Theorem 1 is ineffective (due to the application of the Brauer-Siegel Theorem). This is true even for the trivial bound $q_K \ll_\varepsilon |D_K|^{1/2+\varepsilon}$ for any $\varepsilon > 0$. Using classical work of Stark [18] and more recent work of Soundararajan [17], our proof of Theorem 1 can be modified to give the following effective estimate for q_K for a large class of number fields.

Theorem 2. *Let K be a solvable Galois number field of degree m over $\mathbb{Q}$ with no quadratic subfield. Then*

$$q_K \ll_{\varepsilon,m} |D_K|^{1/2}(\log |D_K|)^{\varepsilon}$$

for any $\varepsilon > 0$ where the implied constant is effectively computable.

It would be equally natural to ask for bounds on the least prime that does *not* split completely in a number field K. This problem, which is a generalization of the classical problem of bounding the least quadratic non-residue, is of a somewhat different nature than the one discussed in this paper and has been investigated by Murty [12], Vaaler and Voloch [20], Li [9], Murty and Patankar [13], and Zaman [23]. As an example of what is known, Li shows in [9] that for an arbitrary number field K (not necessarily Galois over $\mathbb{Q}$) of degree m, there is a nonsplit prime $\ll_\varepsilon |D_K|^{1/(4(m-1))+\varepsilon}$ for any $\varepsilon > 0$ when m is sufficiently large; more precisely, it is shown that there is a nonsplit prime

$$\ll_\varepsilon |D_K|^{(1+\varepsilon)/(4A_m(m-1))},$$

where $A_m \geq 1 - \sqrt{2}\,(m-1)^{-1/2}$. As a corollary of a more general result, this more precise bound was recently improved slightly by Zaman in [23]. The Brauer-Siegel Theorem is not needed in this setting, so the estimates in [9] and [23] are effective.

2. Examples

In this section, we exhibit explicit examples of families of nonabelian Galois extensions $K/\mathbb{Q}$ for which nontrivial estimates for the size of the least prime that splits completely in $\mathcal{O}_K$ can be established using Theorem 1 and the following subconvexity estimates.

Lemma 1. *Let $L(s,\rho)$ be an Artin L-function of degree two over $\mathbb{Q}$ not of icosahedral type with conductor D such that the determinant character χ is primitive modulo D. Then, for $\mathrm{Re}(s) = 1/2$, we have*

$$L(s,\rho) \ll |s|^A |D|^{1/4-1/1889+\varepsilon}$$

for any $\varepsilon > 0$ where A is an absolute constant.

Proof. This is due to Blomer, Harcos, and Michel [1] improving upon the earlier work of Duke, Friedlander, and Iwaniec [5]. □

Lemma 2. *Let χ be a primitive Dirichlet character modulo D. Then, for $\mathrm{Re}(s) = 1/2$, we have*

$$L(s,\chi) \ll |s|^A |D|^{\eta+\varepsilon},$$

for any $\varepsilon > 0$ where A is an absolute constant, $\eta = 1/6$ if χ is quadratic, and $\eta = 3/16$ otherwise.

Proof. The case for quadratic Dirichlet L-functions is due to Conrey and Iwaniec [4], while the result for general characters is due to Heath-Brown [7, 8] extending work of Burgess [3]. □

Example 1. *Let $K/\mathbb{Q}$ be a degree $2n$ Galois extension whose Galois group is isomorphic to the dihedral group D_n, the group of symmetries of the regular n-gon. Then we have that*

$$q_K \ll_{n,\varepsilon} |D_K|^{1/2-2/1889+\varepsilon} \tag{2.1}$$

for any $\varepsilon > 0$ where the implied constant is ineffective.

When n is odd, the dihedral group D_n has 2 degree one irreducible characters, denoted χ_0 and χ_1, and $(n-1)/2$ degree two irreducible characters, denoted $\psi_1, \psi_2, \dots, \psi_{\frac{n-1}{2}}$. Hence the induced character for K over $\mathbb{Q}$ can be decomposed as

$$\chi_0 + \chi_1 + 2\psi_1 + 2\psi_2 + \cdots + 2\psi_{\frac{n-1}{2}}.$$

From this decomposition, it follows that

$$\zeta_K(s) = \zeta(s) L(s, \chi_1) \prod_{j=1}^{(n-1)/2} L(s, \psi_j)^2 \tag{2.2}$$

where $\zeta(s)$ is the Riemann zeta-function, $L(s, \chi_1)$ is a quadratic Dirichlet L-function, and the $L(s, \psi_j)$ for $1 \le j \le (n-1)/2$ are degree two Artin L-functions over $\mathbb{Q}$ of dihedral type.

When n is even, the dihedral group D_n has 4 degree one irreducible characters, denoted χ_0, χ_1, χ_2, and χ_3, and $(n-2)/2$ degree two irreducible characters, denoted $\psi_1, \psi_2, \dots, \psi_{\frac{n-2}{2}}$. In this case, the induced character for K over $\mathbb{Q}$ can be decomposed as

$$\chi_0 + \chi_1 + \chi_2 + \chi_3 + 2\psi_1 + 2\psi_2 + \cdots + 2\psi_{\frac{n-2}{2}}$$

and we have

$$\zeta_K(s) = \zeta(s) L(s, \chi_1) L(s, \chi_2) L(s, \chi_3) \prod_{j=1}^{(n-2)/2} L(s, \psi_j)^2$$

where the $L(s, \chi_i)$ for $i = 1, 2, 3$ are quadratic Dirichlet L-functions and the $L(s, \psi_j)$ for $1 \le j \le (n-2)/2$ are degree two Artin L-functions over $\mathbb{Q}$ of dihedral type.

We now apply the above subconvexity estimates to both cases simultaneously. Let D_{χ_i} denote the conductor of each Dirichlet L-function $L(s, \chi_i)$ and let D_{ψ_j} denote the conductor of each Artin L-function $L(s, \psi_j)$. Then, by Lemma 1 and Lemma 2, we have

$$\begin{aligned} \zeta_K(s) &\ll |s|^A \left(\prod_i |D_{\chi_i}| \prod_j |D_{\psi_j}|^2 \right)^{1/4-1/1889+\varepsilon} \\ &\ll |s|^A |D_K|^{1/4-1/1889+\varepsilon} \end{aligned}$$

for $\mathrm{Re}(s) = 1/2$ and $\varepsilon > 0$ arbitrary by the Führerdiskriminantenproduktformel (conductor–discriminant formula). Hence Hypothesis 1 holds with $\vartheta = 1/1889 - \varepsilon$ and therefore the estimate in (2.1) follows from Theorem 1.

Example 1 is a special case of generalized dihedral (Galois) extensions of $\mathbb{Q}$. We say a group G of order $2n$ is a finite generalized dihedral group if $G = A \rtimes (\mathbb{Z}/2\mathbb{Z})$ where A is a finite abelian group and $\mathbb{Z}/2\mathbb{Z}$ acts on A by $\tau a \tau = a^{-1}$ for any $a \in A$ where τ is the generator of $\mathbb{Z}/2\mathbb{Z}$. By classical representation theory, if s denotes the number of squares in A, then there are $2n/s$ one dimensional representations χ_i of G and $(n - n/s)/2$ inequivalent two-dimensional irreducible representations ρ_j of G. This accounts for all irreducible representations of G.

Now if a Galois extension K over $\mathbb{Q}$ with $[K : \mathbb{Q}] = 2n$ has $\mathrm{Gal}(K/\mathbb{Q}) \cong G$, then

$$\zeta_K(s) = \zeta(s) \prod_{i=1}^{2n/s-1} L(s, \chi_i) \prod_{j=1}^{(n-n/s)/2} L(s, \rho_j)^2$$

where the $L(s, \chi_i)$ are Dirichlet L-functions and the $L(s, \rho_j)$ are degree two Artin L-functions over $\mathbb{Q}$ of dihedral type (as can be seen by considering intermediate dihedral fields between K and $\mathbb{Q}$). Again applying Lemma 1 and Lemma 2 as in Example 1, we are led to the following conclusion.

Example 2. *Let $K/\mathbb{Q}$ be a generalized dihedral Galois extension of $\mathbb{Q}$. Then we have that*

$$q_K \ll_\varepsilon |D_K|^{1/2-2/1889+\varepsilon}$$

for any $\varepsilon > 0$, where the implied constant is ineffective.

Quaternion octic extensions of $\mathbb{Q}$ are an example of a family of Galois number fields that are not generalized dihedral Galois extensions of $\mathbb{Q}$.

Example 3. *Let $K/\mathbb{Q}$ be a (Galois) quaternion octic number field. Then for any $\varepsilon > 0$ we have*

$$q_K \ll_\varepsilon |D_K|^{1/2-2/1889+\varepsilon}, \tag{2.3}$$

where the implicit constant is ineffective.

As in the previous examples, we need only verify Hypothesis 1 for the Dedekind zeta-function $\zeta_K(s)$. In this case, we have

$$\zeta_K(s) = \zeta(s) L(s, \chi_1) L(s, \chi_2) L(s, \chi_3) L(s, \psi)^2, \tag{2.4}$$

where $L(s, \chi_i)$ for $i = 1, 2, 3$ are quadratic Dirichlet L-functions and $L(s, \psi)$ is a degree two Artin L-function over $\mathbb{Q}$ of dihedral type. For details, see [10, Section 1]. Again, applying Lemma 1 and Lemma 2 to each L-function, we obtain the desired result from the conductor–discriminant formula.

The estimates in Examples 1 and 2 can be improved when the degree $[K : \mathbb{Q}]$ is large enough using explicit bounds for the least prime ideal in the Chebotarev density theorem. For instance, if K is a degree $2n$ dihedral Galois extension of $\mathbb{Q}$, then we can use the recent work of Thorner and Zaman [19, Theorem 1.1] to deduce an estimate of the form

$$q_K \ll |D_K|^{173/n+521/\varphi(n)} \tag{2.5}$$

where $\varphi(n)$ is the Euler φ-function. Their theorem is more precise and we have used a number of inequalities to deduce this slightly weaker estimate for q_K. If

we assume n is prime, then the effective bound in (2.5) is better than (2.1) when $n \geq 1399$. If n is composite, using explicit lower bounds for $\varphi(n)$, we can show that (2.5) is stronger than the bound in Example 1 when $n \geq 5814$. On the other hand, we can show that if $[K : \mathbb{Q}] \leq 2088$, then it is always better to use the bounds in Examples 1 or 2 than the actual version [19, Theorem 1.1]. We have not tried to optimize all of these values.

3. Lemmas

In this section, we establish some lemmas that are used to prove Theorem 1.

Lemma 3. *Let D be a positive integer and $D^\infty = \{n \in \mathbb{N} : p \mid n \text{ implies } p \mid D\}$ for primes p. Then, for any $\varepsilon > 0$, we have*

$$\sum_{n \in D^\infty} \frac{1}{\sqrt{n}} \ll_\varepsilon D^\varepsilon. \tag{3.1}$$

Proof. Since every $n \in D^\infty$ is a product of the prime divisors of D, it follows that

$$\sum_{n \in D^\infty} \frac{1}{\sqrt{n}} = \prod_{p \mid D} \left(1 - \frac{1}{\sqrt{p}}\right)^{-1} = \prod_{p \mid D} \left(1 + \frac{1}{\sqrt{p} - 1}\right) \leq \left(1 + \frac{1}{\sqrt{2} - 1}\right)^{\omega(D)}. \tag{3.2}$$

Here, as usual, $\omega(D)$ denotes the number of distinct prime divisors of D. Since $\omega(D) \ll \log D / \log\log D$, the result follows. □

Lemma 4. *Let $K/\mathbb{Q}$ be a Galois extension of degree m and let $\zeta_K(s)$ denote the corresponding Dedekind zeta-function. For $\mathrm{Re}(s) > 1$, write*

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{r_K(n)}{n^s}. \tag{3.3}$$

Then

$$\sum_{n < q_K} r_K(n) \ll q_K^{1/2+\varepsilon} |D_K|^\varepsilon \tag{3.4}$$

for any $\varepsilon > 0$, where the implied constant depends only on ε and m.

Proof. Since $K/\mathbb{Q}$ is a Galois extension, we have

$$p\mathcal{O}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^e$$

for every rational prime p where $g \cdot e \cdot f = m$ and f is the relative degree of each of the prime ideals $\mathfrak{p}_i$ over p. A prime p splits completely if and only if $g = m$ and $f = e = 1$. Hence any rational prime p that does not split completely in $\mathcal{O}_K$ must fall into one the following cases:

(i) p is ramified with $e \geq 2$ and $p \mid D_K$;
(ii) $e = 1$ and $f \geq 2$.

Recalling that q_K is the least prime that splits completely in $\mathcal{O}_K$, we see that every prime p less than q_K falls into either case (i) or (ii). Since the primes in case (i) and case (ii) are disjoint, every positive integer n less than q_K has a unique factorization $n = uv$, where u is a product of primes in case (ii) and v is a product of primes in case (i). Clearly $v \in |D_K|^\infty$. We claim that u is power-full whenever $r_K(n) \neq 0$.[1] To see this, first notice that $r_K(\cdot)$ is multiplicative, being the coefficients in a Dirichlet

[1]We say an integer n is *power-full* or *square-full* if $p \mid n$ implies that $p^2 \mid n$ for any prime p.

series with an Euler product. If p is a prime of type (ii), then $r_K(p) = 0$, since $f \geq 2$. So if $p \parallel n$ where p is of type (ii), then $r_K(n) = 0$. Hence, if $r_K(n) \neq 0$, then u is power-full.

Using the factorization $n = uv$ described above, we have

$$\sum_{n<q_K} r_K(n) \leq \sum_{\substack{v<q_K \\ v\in|D_K|^\infty}} r_K(v) \sum_{\substack{u<q_K/v \\ u \text{ power-full}}} r_K(u).$$

Since the number of power-full integers less than x is $O(x^{1/2})$ and the coefficients $r_K(n) \ll_\varepsilon n^\varepsilon$ for any $\varepsilon > 0$, it follows from Lemma 3 that

$$\sum_{n<q_K} r_K(n) \ll_\varepsilon q_K^{1/2+\varepsilon} \sum_{\substack{v<q_K \\ v\in|D_K|^\infty}} v^{-1/2} \ll_\varepsilon q_K^{1/2+\varepsilon}|D_K|^\varepsilon.$$

This completes the proof of the lemma. □

Lemma 5. *Let $K/\mathbb{Q}$ be a finite extension of degree m (not necessarily Galois). Then, assuming Hypothesis 1, we have*

$$\sum_{n=1}^{\infty} r_K(n)\, e^{-n/x} = x \operatorname*{Res}_{s=1} \zeta_K(s) + O_m\Big(\sqrt{x}\,|D_K|^{1/4-\vartheta}\Big). \tag{3.5}$$

Proof. Using the inverse Mellin transform identity

$$e^{-y} = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \Gamma(s)\, y^{-s}\,\mathrm{d}s \tag{3.6}$$

which is valid for $c > 0$ and $y > 0$, we deduce that

$$\begin{aligned}\sum_{n=1}^{\infty} r_K(n)\, e^{-n/x} &= \sum_{n=1}^{\infty} r_K(n) \left\{\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \Gamma(s)\left(\frac{x}{n}\right)^s \mathrm{d}s\right\} \\ &= \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \sum_{n=1}^{\infty} \frac{r_K(n)}{n^s}\,\Gamma(s)\, x^s\,\mathrm{d}s \\ &= \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \zeta_K(s)\,\Gamma(s)\, x^s\,\mathrm{d}s\end{aligned} \tag{3.7}$$

for any $x > 0$. Here the interchange of summation and integration is justified by the absolute convergence of the series in (3.3) when $\mathrm{Re}(s) = 2$. Next, we shift the line of integration in the third integral on the right-hand side left from $\mathrm{Re}(s) = 2$ to $\mathrm{Re}(s) = 1/2$. (To justify the contour shift, we use that $\zeta_K(s)$ is polynomially bounded in the vertical strip $1/2 \leq \sigma \leq 2$, while $|\Gamma(\sigma + it)|$ decays exponentially in t there.) In doing so, we pass over the simple pole of $\zeta_K(s)$ at $s = 1$ and no other singularities of the integrand. Since

$$\operatorname*{Res}_{s=1}\Big(\zeta_K(s)\,\Gamma(s)\, x^s\Big) = x \operatorname*{Res}_{s=1} \zeta_K(s),$$

we deduce that

$$\sum_{n=1}^{\infty} r_K(n)\, e^{-n/x} = x \operatorname*{Res}_{s=1} \zeta_K(s) + \frac{1}{2\pi i}\int_{\frac{1}{2}-i\infty}^{\frac{1}{2}+i\infty} \zeta_K(s)\,\Gamma(s)\, x^s\,\mathrm{d}s. \tag{3.8}$$

Stirling's formula for the gamma function and Hypothesis 1 imply that the integral on the right-hand side is

$$\ll_m \sqrt{x}\,|D_K|^{1/4-\vartheta}\int_{-\infty}^{\infty}(1+|t|)^A\left|\Gamma(\tfrac{1}{2}+it)\right|\mathrm{d}t \ \ll_m \sqrt{x}\,|D_K|^{1/4-\vartheta}.$$

Inserting this estimate into (3.8), the lemma follows. □

4. Proof of Theorem 1

We may suppose that $|D_K|$ is sufficiently large in terms of ε, since otherwise there are only finitely many fields K in question, and the estimate of Theorem 1 is trivial. We prove Theorem 1 by contrasting the fact that the algebraic estimate in Lemma 4 indicates that the sum $\sum_{n<q_K} r_K(n)$ is small while the combination of the Brauer-Siegel theorem and the analytic estimate in Lemma 5 tell us that this sum must be large if q_K is sufficiently large in terms of $|D_K|$.

Fix $\varepsilon > 0$. Lemma 4 states that

$$\sum_{n<q_K} r_K(n) \ll q_K^{1/2+\varepsilon}|D_K|^{\varepsilon}. \tag{4.1}$$

On the other hand, by Lemma 5, we have

$$\begin{aligned}\sum_{n\le x\log x} r_K(n) &\ge \sum_{n=1}^{\infty} r_K(n)\,e^{-n/x} + O\big((x\log x)^{\varepsilon}\big)\\ &\ge x\operatorname*{Res}_{s=1}\zeta_K(s) + O_m\Big(\sqrt{x}\,|D_K|^{1/4-\vartheta}\Big).\end{aligned} \tag{4.2}$$

Here we bounded the tail of the infinite sum as follows:

$$\sum_{n>x\log x} r_K(n)\,e^{-n/x} \ll \sum_{n>x\log x} n^{\varepsilon}\,e^{-n/x} \ll (x\log x)^{\varepsilon}.$$

(To see the last estimate, put n into intervals $(x\log x + jx, x\log x + (j+1)x]$, and note that the contribution from the jth interval is $\ll ((x\log x)^{\varepsilon} + j^{\varepsilon}x^{\varepsilon})e^{-j}$.) We now argue that (4.1) and (4.2) are incompatible if $q_K \ge |D_K|^{1/2-2\vartheta+3\varepsilon}$. Since the Brauer-Siegel theorem [2] states that

$$\operatorname*{Res}_{s=1}\zeta_K(s) \gg |D_K|^{-\varepsilon}, \tag{4.3}$$

by choosing x with $q_K = x\log x$ it follows from (4.2) that

$$\sum_{n\le q_K} r_K(n) \gg \frac{q_K}{\log q_K}\,|D_K|^{-\varepsilon} \tag{4.4}$$

if $q_K \ge |D_K|^{1/2-2\vartheta+3\varepsilon}$. Hence, if $q_K \ge |D_K|^{1/2-2\vartheta+3\varepsilon}$, by combining (4.1) and (4.4) we see that

$$\frac{q_K}{\log q_K}\,|D_K|^{-\varepsilon} \ll \sum_{n\le q_K} r_K(n) \ll q_K^{1/2+\varepsilon}|D_K|^{\varepsilon},$$

which is not possible if $|D_K|$ is sufficiently large. Therefore it must be the case that $q_K \ll |D_K|^{1/2-2\vartheta+3\varepsilon}$. Theorem 1 now follows by replacing 3ε with ε.

5. Proof of Theorem 2

In this section, we indicate what changes need to be made to our proof of Theorem 1 in order to prove Theorem 2.

Sketch of the Proof. In place of Hypothesis 1, we use the very general weak subconvexity result of Soundararajan [17] which, for Galois extensions of $\mathbb{Q}$, implies that

$$\zeta_K(s) \ll_{m,\varepsilon} |s|^{m/4} \frac{|D_K|^{1/4}}{(\log |D_K|)^{1-\varepsilon}}$$

for $\mathrm{Re}(s) = 1/2$ and any $\varepsilon > 0$.[2] Using this estimate in the proof of Lemma 5, we deduce that

$$\sum_{n=1}^{\infty} r_K(n)\, e^{-n/x} = x \operatorname*{Res}_{s=1} \zeta_K(s) + O_{m,\varepsilon}\left(\sqrt{x}\, \frac{|D_K|^{1/4}}{(\log |D_K|)^{1-\varepsilon}}\right). \tag{5.1}$$

If $K/\mathbb{Q}$ is a solvable Galois number field with no quadratic subfield, then Stark [18] proved an effective version of the Brauer-Siegel Theorem which states that

$$\operatorname*{Res}_{s=1} \zeta_K(s) \gg \frac{1}{\log |D_K|} \tag{5.2}$$

where the implied constant is effectively computable. Theorem 2 now follows by using (5.1) and (5.2) in place of Lemma 4 and (4.3) in the proof of Theorem 1. □

Acknowledgments

This project began as a result of an SEC Faculty Travel Grant that allowed the second author to visit the University of Georgia. We thank the Southeastern Conference for its support. We also thank Caroline Turnage-Butterbaugh, Jesse Thorner, and the anonymous referee for a number of useful comments.

References

1. V. Blomer, G. Harcos, and P. Michel, *Bounds for modular L-functions in the level aspect*, Ann. Sci. Écol Norm. Sup. (4), **40(5)** (2007), 697–740.
2. R. Brauer, *On the zeta-function of algebraic number fields*, Amer. J. Math., **69** (1947), 243–250.
3. D. A. Burgess, *On character sums and L-series. II*, Proc. London Math. Soc. (3), **13** (1963), 524–536.
4. J. B. Conrey, and H. Iwaniec, *The cubic moment of central values of automorphic L-functions*, Ann. of Math. (2), **151** (2000), 1175–1216.
5. W. Duke, J. B. Friedlander, and H. Iwaniec, *The subconvexity problem for Artin L-functions*, Invent. Math., **149(3)** (2002), 489–577.
6. M. Einsiedler, E. Lindenstrauss, P. Michel, and A. Venkatesh, *Distribution of the periodic torus orbits and Duke's theorem for cubic fields*, Ann. of Math. (2), **173(2)** (2011), 815–885.
7. D. R. Heath-Brown, *Hybrid bounds for Dirichlet L-functions*, Invent. Math., **47** (1978), no. 2, 149–170.
8. ———, *Hybrid bounds for Dirichlet L-functions. II*, Quart. J. Math. Oxford Ser. (2), **31** (1980), no. 122, 157–167.
9. X. Li, *The smallest prime that does not split completely in a number field*, Algebra Number Theory, **6** (2012), no. 6, 1061–1096.
10. S. Louboutin, *Determination of all quaternion octic CM-fields with class number 2*, J. London Math. Soc. (2), **54** (1996), 227–238.

[2] To deduce this bound, we apply [17, Theorem 1] to the L-function $L(s) = \zeta_K(s)/\zeta(s)$ which satisfies conditions (1.5a)-(1.5e) and (1.6a)-(1.6c) in that paper if $K/\mathbb{Q}$ is a Galois extension.

11. P. Michel and A. Venkatesh, *The subconvexity problem for* GL_2, Publ. Math. Inst. Hautes Études Sci., **111** (2010), 171–271.
12. V. K. Murty, *The least prime which does not split completely*, Forum Math., **6** (1994), no. 5, 555–565.
13. V. K. Murty and V. M. Patankar, *Tate cycles on Abelian varieties with complex multiplication*, Canad. J. Math., **67** (2015), no. 1, 198–213.
14. J. Pintz, *Elementary methods in the theory of L-functions. VI. On the least prime quadratic residue* (mod p), Acta Arith., **32(2)** (1977), 173–178.
15. P. Pollack, *The smallest prime that splits completely in an abelian number field*, Proc. Amer. Math. Soc., **142(6)** (2014), 1925–1934.
16. ———, *Prime splitting in abelian number fields and linear combinations of Dirichlet characters*, Int. J. Number Theory, **10(4)** (2014), 885–903.
17. K. Soundararajan, *Weak subconvexity for central values of L-functions*, Ann. of Math. (2), **172** (2010), no. 2, 1469–1498.
18. H. M. Stark, *Some effective cases of the Brauer-Siegel theorem*, Invent. Math., **23** (1974), 135–152.
19. J. Thorner and A. Zaman, *An explicit bound for the least prime ideal in the Chebotarev density theorem*, Algebra Number Theory, **11** (2017), no. 5, 1135–1197.
20. J. D. Vaaler and J. F. Voloch, *The least nonsplit prime in Galois extensions of* $\mathbb{Q}$, J. Number Theory, **85** (2000), no. 2, 320–335.
21. A. Venkatesh, *Sparse equidistribution problems, period bounds and subconvexity*, Ann. of Math. (2), **172** (2010), 989–1094.
22. A. I. Vinogradov and Ju. V. Linnik, *Hypoelliptic curves and the least prime quadratic residue*, Dokl. Akad. Nauk SSSR., **168** (1966), 258–261.
23. A. Zaman, *The least unramified prime which does not split completely*, Forum. Math., to appear.

Department of Mathematics, University of Mississippi, University, MS 38677, USA
E-mail address: zge@olemiss.edu
E-mail address: mbmilino@olemiss.edu

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