PRIME SPLITTING IN ABELIAN NUMBER FIELDS AND LINEAR COMBINATIONS OF DIRICHLET CHARACTERS

PAUL POLLACK

Abstract. Let $\mathbb{X}$ be a finite group of primitive Dirichlet characters. Let $\xi = \sum_{\chi\in\mathbb{X}} a_\chi \chi$ be a nonzero element of the group ring $\mathbb{Z}[\mathbb{X}]$. We investigate the smallest prime q that is coprime to the conductor of each $\chi \in \mathbb{X}$ and that satisfies

$$\sum_{\chi\in\mathbb{X}} a_\chi \chi(q) \neq 0.$$

Our main result is a nontrivial upper bound on q valid for certain special forms ξ. From this, we deduce upper bounds on the smallest unramified prime with a given splitting type in an abelian number field. For example:

- Let p be a prime, and let χ be a Dirichlet character modulo p. Suppose that χ has order n and that d is a divisor of n with $d > 1$. The least prime q for which $\chi(q)$ is a primitive dth root of unity satisfies
$$q \ll_{n,\varepsilon} p^{\lambda+\varepsilon}, \quad \text{where} \quad \lambda = \frac{n}{8d}\cdot 2^{\omega(d)}.$$
- Let $K/\mathbb{Q}$ be an abelian number field of degree n and conductor f. Let g be a proper divisor of n. If there is any unramified rational prime q that splits into g distinct prime ideals in $\mathcal{O}_K$, then the least such q satisfies
$$q \ll_{n,\varepsilon} f^{\frac{n}{8}+\varepsilon}.$$

Our estimate also allows us to recover the upper bounds of Vinogradov–Linnik, Elliott, and the present author on the least split-completely prime in an abelian number field.

1. Introduction

1.1. **Statement of the main result.** In this paper, we study the smallest prime outside of a small finite set at which a given linear combination of Dirichlet characters is nonvanishing. Via class field theory for $\mathbb{Q}$, results of this nature have applications to the study of prime splitting in abelian number fields. To facilitate a precise statement of both the problem and the results, we begin by reviewing some notation and terminology.

If χ_1 and χ_2 are primitive Dirichlet characters, we define their product $\chi_1\chi_2$ as the primitive Dirichlet character which induces the function $n \mapsto \chi_1(n)\chi_2(n)$. With this definition, the conductor of $\chi_1\chi_2$ always divides the least common multiple of the conductors of χ_1 and χ_2, but is often smaller. By a *group of Dirichlet characters*, we mean a collection of primitive characters that forms a group with this notion of multiplication.

For each Dirichlet character χ, we let f_χ denote the conductor of χ. If $\mathbb{X}$ is a finite group of Dirichlet characters, we define the *conductor* $f_{\mathbb{X}}$ *of* $\mathbb{X}$ as the least common multiple of the conductors f_χ, for $\chi \in \mathbb{X}$. We say that $\mathbb{X}$ *is ramified at the prime* q if q divides $f_{\mathbb{X}}$. By a *form on* $\mathbb{X}$, we mean an element

$$\xi = \sum_{\chi\in\mathbb{X}} a_\chi \chi \tag{1.1}$$

2010 *Mathematics Subject Classification.* Primary 11L40, Secondary 11R42, 11R44.

of the group ring $\mathbb{Z}[\mathbb{X}]$. For each integer m and each form ξ, we define the evaluation of ξ at m in the obvious way, that is, $\xi(m) := \sum_{\chi\in\mathbb{X}} a_\chi \chi(m)$. Then $\xi(0) = a_{\mathbb{1}}$, where $\mathbb{1}$ denotes the unique primitive principal character (of conductor 1). It is important for the sequel to observe that $(\xi_1\xi_2)(m)$ need not equal $\xi_1(m)\xi_2(m)$ — indeed, this can fail even if ξ_1 and ξ_2 are characters themselves. However, equality does hold whenever m is coprime to $f_{\mathbb{X}}$.

It will be seen (see Proposition 1.5 below) that the least rational prime that splits completely in a given abelian number field $K/\mathbb{Q}$ is precisely the smallest unramified prime q having $\sum_\chi \chi(q) \neq 0$; here the sum runs over a certain finite set of characters that is canonically associated to K (see Proposition 2.1). It will turn out that the nonvanishing of other $\mathbb{Z}$-linear combinations of characters also yields useful arithmetic information. This leads us to the following problem:

Problem 1.1. Given a nonzero form $\xi \in \mathbb{Z}[\mathbb{X}]$, estimate the smallest prime q where $\xi(q) \neq 0$ (possibly satisfying certain other ramification-related restrictions).

It is not immediately obvious that this problem is well-posed; why must there be any such q? In fact, $\xi(q) \neq 0$ for infinitely many primes q. To see this, first observe that distinct $\chi \in \mathbb{X}$ induce distinct characters modulo $f_{\mathbb{X}}$. Since ξ is not identically zero, the Artin–Dedekind theorem on linear independence of characters (see, e.g., [10, Theorem 4.1, p. 283]) shows that $\xi(m) \neq 0$ for all m belonging to a certain coprime residue class modulo $f_{\mathbb{X}}$. Appealing now to Dirichlet's theorem on primes in progressions, we see that this residue class contains infinitely many primes q.

The argument of the last paragraph shows that an upper bound in Problem 1.1 follows from an upper bound on the least prime in a prescribed arithmetic progression. A bound of the latter type is given in a celebrated theorem of Linnik [11, 12]:

Proposition 1.2. *There is an absolute constant $\mathcal{L}$ with the following property: Whenever A and M are coprime, the smallest prime $q \equiv A \pmod{M}$ satisfies*

$$q \ll M^{\mathcal{L}}.$$

Combined with the above remarks, Proposition 1.2 shows that the smallest prime $q \nmid f_{\mathbb{X}}$ for which $\xi(q) \neq 0$ is $O(f_{\mathbb{X}}^{\mathcal{L}})$. Recent work of Xylouris [19] (improving on earlier results of Heath-Brown [7]) allows us to take $\mathcal{L} = 5.18$ in Proposition 1.2.

The purpose of this paper is to present an alternative upper bound for the prime q described in Problem 1.1, valid for certain special forms. There is no loss of generality in assuming that the coefficient $a_{\mathbb{1}}$ of ξ is nonzero; if $a_{\mathbb{1}}$ vanishes, we can replace ξ by $\chi^{-1}\xi$ for any χ in the support of ξ. (Here and below, the *support of* ξ refers to the set of $\chi \in \mathbb{X}$ with $a_\chi \neq 0$.) Our main theorem applies when the coefficient $a_{\mathbb{1}}$ of ξ is ± 1. When ξ is 'short', in the sense that ξ is a linear combination with small coefficients of only a few characters, the resulting upper bound on q is smaller than the naive bound from Linnik's theorem.

We need a few more definitions before we can state our result.

Definition 1.3. Suppose that ξ is a form on $\mathbb{X}$, written as (1.1). We define

- the *weight* of ξ, denoted W_ξ, as $\prod_{\chi\in\mathbb{X}} f_\chi^{a_\chi}$,
- the *length* of ξ, denoted $\|\xi\|$, as $\sum_{\chi\in\mathbb{X}} |a_\chi|$.
- the *positive part* of ξ, denoted ξ^+, as $\sum_{\chi\in\mathbb{X}:\ a_\chi>0} a_\chi\chi$; similarly, the *negative part of* ξ, denoted ξ^-, is defined as $-\sum_{\chi\in\mathbb{X}:\ a_\chi<0} a_\chi\chi$.

Our main result is the following. The proof is presented in §4, following preparatory work given in §3.

Theorem 1.4. *Let $\mathbb{X}$ be a finite group of Dirichlet characters with conductor f and exponent dividing the positive integer n. Let $\xi \in \mathbb{Z}[\mathbb{X}]$, and suppose that $\xi(0) = \pm 1$. Let*

$$W := \max\{W_{\xi^+}, W_{\xi^-}\},$$

and let L be an upper bound on the length of ξ. For each $\varepsilon > 0$, the smallest prime $q \nmid f$ for which $\xi(q) \neq 0$ satisfies

$$q \ll W^{1/4} f^{\varepsilon}.$$

Here the implied constant depends at most on n, ε, and L.

Remark. It is perhaps more natural to state the theorem with n equal to the (precise) exponent of $\mathbb{X}$ and L equal to the length of ξ. However, the looser definitions of n and L used above will be convenient in the proof.

1.2. **Consequences.** We now discuss applications. We begin by quoting the main result of [16], which we show in §2.1 to be a simple consequence of Theorem 1.4.

Proposition 1.5. *Let $K/\mathbb{Q}$ be an abelian extension of degree n and discriminant D. The smallest rational prime q that splits completely in K satisfies*

$$q \ll_{n,\varepsilon} |D|^{\frac{1}{4}+\varepsilon}$$

for each $\varepsilon > 0$.

If we specialize Proposition 1.5 to the case of a cyclic extension of prime conductor, we immediately obtain the following result (due to Vinogradov and Linnik [17] when $n = 2$ and Elliott [5] when $n > 2$):

Proposition 1.6. *Let p be a prime, and let χ be a Dirichlet character modulo p of order n. The smallest prime q for which $\chi(q) = 1$ satisfies*

$$q \ll_{n,\varepsilon} p^{\frac{n-1}{4}+\varepsilon},$$

for each $\varepsilon > 0$.

Next, we turn to our new results. The statement of the next theorem assumes familiarity with the correspondence between abelian extensions of $\mathbb{Q}$ and groups of Dirichlet characters (which is reviewed at the start of §2.1). The proof is given in §2.2. We remind the reader that $\omega(d)$ denotes the number of distinct primes dividing d.

Theorem 1.7. *Let $K/\mathbb{Q}$ be an abelian extension of degree n and conductor f. Choose a basis $\chi_1, \dots, \chi_k$ for the group of characters $\mathbb{X}$ associated to K. Suppose that each χ_i has order n_i. For all $1 \leq i \leq k$, choose a divisor d_i of n_i, and suppose that at least one $d_i > 1$. The smallest prime q for which $\chi_i(q)$ is a primitive d_ith root of unity, for every $1 \leq i \leq k$, satisfies*

$$q \ll f^{\lambda+\varepsilon}, \quad \textit{where} \quad \lambda = \frac{1}{8}\left(\prod_{i=1}^{k} n_i\right)\left(\prod_{i=1}^{k} \frac{2^{\omega(d_i)}}{d_i}\right).$$

Here the implied constant depends at most on n and ε.

Theorem 1.7 is perhaps a bit difficult to appreciate in itself. So we record two consequences here that seem of independent interest. The first complements Elliott's Proposition 1.6; we omit the proof, since it follows immediately from Theorem 1.7 upon restricting to extensions of prime conductor.

Corollary 1.8. *Let p be a prime, and let χ be a Dirichlet character modulo p of order n. Suppose that d divides n and $d > 1$. Then the least prime q for which $\chi(q)$ is a primitive dth root of unity satisfies*

$$q \ll_{n,\varepsilon} p^{\lambda+\varepsilon}, \quad \textit{where} \quad \lambda = \frac{n}{8d} \cdot 2^{\omega(d)}.$$

Our next result, proved in §2.3, complements Proposition 1.5.

Corollary 1.9. *Let $K/\mathbb{Q}$ be an abelian extension of degree n and conductor f. Let g be a divisor of n with $g < n$. Assume that there is at least one rational prime that does not ramify in K and that has g distinct prime ideal factors in $\mathcal{O}_K$. Then the smallest prime q of this type satisfies*

$$q \ll_{n,\varepsilon} f^{\frac{n}{8}+\varepsilon}.$$

Remark. For each abelian extension $K/\mathbb{Q}$ of degree n, one has $|D| \geq f^{n/2}$ (compare with [3, Lemma 9.2.1, p. 431]). Hence, $f^{\frac{n}{8}+\varepsilon} \leq |D|^{\frac{1}{4}} f^{\varepsilon} \leq |D|^{\frac{1}{4}+\varepsilon}$. So combining Corollary 1.9 with the result of Proposition 1.5, we see that the smallest unramified prime that splits into g distinct prime ideals in $\mathcal{O}_K$ is $O_{n,\varepsilon}(|D|^{\frac{1}{4}+\varepsilon})$, uniformly in g, provided that at least one prime of this kind exists.

1.3. **Sketch of the proof of Theorem 1.4.** We conclude the introduction with a brief sketch of the proof of Theorem 1.4. We freely omit details at this point in order to give the flavor of the argument. In addition, we tell some 'white lies'; for instance, in the actual proof, our partial sums of Dirichlet coefficients are weighted conveniently.

Write $\xi^+ = \sum_{\chi \in \mathbb{X}} a_{\chi,+}\chi$ and $\xi^- = \sum_{\chi \in \mathbb{X}} a_{\chi,-}\chi$. Since $\xi(0) = \pm 1$, either $a_{\mathbb{1},+} = 1$ or $a_{\mathbb{1},-} = 1$; we can assume it is the former (replace ξ with $-\xi$ otherwise). Since $\xi = \xi^+ - \xi^-$, whenever $\xi(q) = 0$, we have

$$\sum_{\chi \in \mathbb{X}} a_{\chi,+}\chi(q) = \sum_{\chi \in \mathbb{X}} a_{\chi,-}\chi(q). \tag{1.2}$$

Let us suppose that we were to have $\xi(q) = 0$ for **all** primes q. (We already know that this impossible, but it is insightful to see where this assumption leads us.) Define a Dirichlet series G by setting $\prod_{\chi \in \mathbb{X}} L(s,\chi)^{a_{\chi,+}} = G(s) \prod_{\chi \in \mathbb{X}} L(s,\chi)^{a_{\chi,-}}$. Taking Euler-product expansions of both sides and appealing to (1.2), we find that G represents a function that is analytic and nonzero for $\Re(s) > \frac{1}{2}$.

Define arithmetic functions f^+ and f^- by setting

$$\prod_{\chi \in \mathbb{X}} L(s,\chi)^{a_{\chi,+}} = \sum_{m=1}^{\infty} \frac{f^+(m)}{m^s} \quad \text{and} \quad \prod_{\chi \in \mathbb{X}} L(s,\chi)^{a_{\chi,-}} = \sum_{m=1}^{\infty} \frac{f^-(m)}{m^s}.$$

Writing $G(s) = \sum_{m \geq 1} g(m) m^{-s}$, and using $\star$ to denote Dirichlet convolution, the definition of G shows that

$$\sum_{m \leq y} f^+(m) = \sum_{m \leq y} (g \star f^-)(m) \tag{1.3}$$

for all y. But this cannot be: Since $a_{\mathbb{1},+} = 1$ and $a_{\mathbb{1},-} = 0$, the product $\prod_{\chi \in \mathbb{X}} L(s,\chi)^{a_{\chi,+}}$ has a simple pole at $s = 1$ from the factor $L(s,\mathbb{1}) = \zeta(s)$, whereas $G(s) \prod_{\chi \in \mathbb{X}} L(s,\chi)^{a_{\chi,-}}$ is analytic at $s = 1$. Applying Perron's formula, one derives from these facts that $\sum_{m \leq y} f^+(m)$ grows linearly with y while $\sum_{m \leq y} (g \star f^-)(m) = o(y)$, as $y \to \infty$. This contradiction proves (again) that $\xi(q)$ is nonzero for some prime q.

To obtain a bound on the smallest such q, we replace the extravagant assumption that $\xi(q)$ always vanishes with the more modest assumption that $\xi(q) = 0$ for all primes

$q \le y$. Keeping track of the dependencies in the error terms, Perron's formula shows that the right-hand side of (1.3) is much smaller than the left once y is a little larger than W. To derive this, one uses the trivial bound of f_χ on the partial sums of each nontrivial character χ. If one replaces the trivial bound with the Burgess bound, one can replace W here with $W^{1/4}$. These ideas suffice to prove Theorem 1.4, modulo technical work necessary to handle the extra condition that q not divide $f_{\mathbb{X}}$.

Remark. The ideas that go into the proof of Theorem 1.4 can be found in nascent form in the works of Vinogradov–Linnik [17] and Elliott [5] already alluded to. In the language of the present paper, those authors considered only cyclic groups $\mathbb{X}$ of prime conductor and the particular form $\xi = \sum_{\chi \in \mathbb{X}} \chi$. (Thus, $\xi^+ = \xi$ and $\xi^- = 0$, and the product $\prod_{\chi \in \mathbb{X}} L(s,\chi)^{a_{\chi,+}}$ is the Dedekind zeta function of the number field corresponding to $\mathbb{X}$. This allows for small technical simplifications over what is seen below.) The raison d'être of the present work is to place these earlier papers in a suitable general context.

Additional notation. We continue to 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 letters p and q are reserved for prime variables. We write

$$\tau_k(n) = \sum_{d_1 \cdots d_k = n} 1$$

for the k-fold Piltz divisor function. Thus, $\tau_2(n)$ is the usual number-of-divisors function, which we write simply as $\tau(n)$.

2. Proofs of the corollaries

2.1. **Proof of Proposition 1.5.**

For the convenience of the reader, we summarize the correspondence between finite groups of Dirichlet characters and finite abelian extensions of $\mathbb{Q}$. For much more, see [18, Chapter 3].

Proposition 2.1. *Let $\mathbb{X}$ be a finite group of characters of conductor f. Identify each $\chi \in \mathbb{X}$ with the induced character modulo f, and let $H = \cap_{\chi \in \mathbb{X}} \ker \chi \trianglelefteq (\mathbb{Z}/f\mathbb{Z})^\times = \mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q})$. Associate to $\mathbb{X}$ the fixed field $\mathbb{Q}(\zeta_f)^H$. Then $K/\mathbb{Q}$ is an abelian extension of degree $\#\mathbb{X}$ and conductor f. Conversely, each abelian extension $K/\mathbb{Q}$ arises in this way from a unique character group $\mathbb{X}$.*

Suppose now that $\mathbb{X}$ is a finite group of characters and that K is the corresponding field. If q is any rational prime, then

(i) q ramifies in K precisely when $q \mid f_\chi$ for some $\chi \in \mathbb{X}$,
(ii) the number of distinct prime ideal factors of q in $\mathcal{O}_K$ is equal to the number of $\chi \in \mathbb{X}$ for which $\chi(q) = 1$.

Proof of Proposition 1.5. Let $\mathbb{X}$ be the group of Dirichlet characters corresponding to K. Then the exponent of $\mathbb{X}$ divides $\#\mathbb{X} = [K : \mathbb{Q}] = n$. By Proposition 2.1, q splits completely in K precisely when $\chi(q) = 1$ for all $\chi \in \mathbb{X}$. To detect this condition, we introduce the form $\xi = \sum_{\chi \in \mathbb{X}} \chi \in \mathbb{Z}[\mathbb{X}]$. We claim that if $\mathbb{X}$ is unramified at q, and q does not split completely in K, then $\xi(q) = 0$. Indeed, under these conditions, there is a $\psi \in \mathbb{X}$ with $\psi(q) \neq 1$. Since q is relatively prime to $f = \mathrm{lcm}_{\chi \in \mathbb{X}}[f_\chi]$, multiplication by $\psi(q)$ permutes $\sum_{\chi \in \mathbb{X}} \chi(q)$; this forces $\sum_{\chi \in \mathbb{X}} \chi(q) = 0$.

From the last paragraph, the smallest split-completely prime is bounded above by the smallest $q \nmid f_{\mathbb{X}}$ for which $\xi(q) \neq 0$. We estimate this using Theorem 1.4. In our case, $\xi^+ = \xi$ has weight $\prod_{\chi\in\mathbb{X}} f_\chi = |D|$ (from the conductor-discriminant formula [18, Theorem 3.11, p. 27]) and $\xi^- = 0$ has weight 1. Thus, $W = |D|$. We can take $L = \|\xi\| = n$. Now Theorem 1.4 shows that there is a suitable prime $q \ll_{n,\varepsilon} |D|^{1/4} f^\varepsilon \le |D|^{1/4+\varepsilon}$. □

2.2. **Proof of Theorem 1.7.** We need an easy lemma concerning the length of a product of two forms.

Lemma 2.2. *Length is submultiplicative. In other words, if ξ_1 and ξ_2 are two forms on $\mathbb{X}$, then $\|\xi_1\xi_2\| \le \|\xi_1\|\cdot\|\xi_2\|$.*

Proof. Suppose $\xi_1 = \sum_{\chi\in\mathbb{X}} a_{\chi,1}\chi$ and $\xi_2 = \sum_{\chi\in\mathbb{X}} a_{\chi,2}\chi$. Then

$$\begin{aligned}\|\xi_1\xi_2\| = \left\|\sum_{\chi\in\mathbb{X}}\left(\sum_{\substack{\psi,\rho\in\mathbb{X}\\ \psi\rho=\chi}} a_{\psi,1}a_{\rho,2}\right)\chi\right\| &= \sum_{\chi\in\mathbb{X}}\left|\sum_{\substack{\psi,\rho\in\mathbb{X}\\ \psi\rho=\chi}} a_{\psi,1}a_{\rho,2}\right|\\ &\le \left(\sum_{\psi\in\mathbb{X}}|a_{\psi,1}|\right)\left(\sum_{\rho\in\mathbb{X}}|a_{\rho,2}|\right) = \|\xi_1\|\cdot\|\xi_2\|. \quad \square\end{aligned}$$

Proof of Theorem 1.7. The proof is similar to that of Proposition 1.5. But for our 'detector' form, we now choose

$$\xi = \prod_{i=1}^{k}\left((1+\chi_i^{d_i}+\chi_i^{2d_i}+\dots+\chi_i^{n_i-d_i})\prod_{p\mid d_i}(\chi_i^{d_i/p}-1)\right). \tag{2.1}$$

To justify this choice, suppose that $\mathbb{X}$ does not ramify at q. If the order of $\chi_i(q)$ divides n_i but not d_i, then $\chi_i(q)$ is a root of $\frac{x^{n_i}-1}{x^{d_i}-1} = 1 + x^{d_i} + \dots + x^{n_i-d_i}$; thus, $\xi(q) = 0$. Also, if the order of $\chi_i(q)$ is a proper divisor of d_i, then $\chi_i(q)$ is a root of $x^{d_i/p}-1$ for some prime p dividing d_i, and again $\xi(q) = 0$. Combining these two observations, we see that $\xi(q)$ vanishes unless $\chi_i(q)$ has order d_i for each i.

Before we can apply Theorem 1.4, we must check that ξ has constant term $a_{\mathbb{1}} = \pm 1$. By hypothesis, $\mathbb{X}$ is the direct sum of the groups generated by $\chi_1, \dots, \chi_k$. So it is sufficient to show that for every i, each monomial appearing in the expansion of the product (taken in the polynomial ring $\mathbb{Z}[x]$)

$$(1+x^{d_i}+x^{2d_i}+\dots+x^{n_i-d_i})\prod_{p\mid d_i}(x^{d_i/p}-1)$$

has the form x^m where either $m = 0$ or $n_i \nmid m$. In fact, if x^m appears with a nonzero coefficient in this expansion, then either $m \le n_i - d_i < n_i$, or

$$m \equiv \sum_{p\in\mathscr{S}} d_i/p \pmod{d_i}$$

for some nonempty subset $\mathscr{S}$ of the primes dividing d_i. But the right-hand sum is not divisible by d_i, since $\sum_{p\in\mathscr{S}}\frac{1}{p}$ is not an integer (its lowest-terms denominator is divisible by every prime in $\mathscr{S}$). So $d_i \nmid m$, and a fortiori, $n_i \nmid m$.

We are now in a position to apply Theorem 1.4. Since ξ^+ and ξ^- have disjoint support, $\|\xi\| = \|\xi^+\| + \|\xi^-\|$. Moreover, since ξ^+ and ξ^- have nonnegative coefficients,

$$0 = \xi(1) = \xi^+(1) - \xi^-(1) = \|\xi^+\| - \|\xi^-\|.$$

(The first equality uses our assumption that some $d_i > 1$.) Hence,

$$\|\xi^+\| = \|\xi^-\| = \frac{1}{2}\|\xi\|.$$

Examining the factors appearing in the definition of ξ and using the submultiplicativity of the length, we find that

$$\|\xi\| \le \left(\prod_{i=1}^{k} \frac{n_i}{d_i}\right)\left(\prod_{i=1}^{k} 2^{\omega(d_i)}\right) = n\prod_{i=1}^{k}\frac{2^{\omega(d_i)}}{d_i} = 8\lambda.$$

(In particular, $\|\xi\| \le n$, since $2^{\omega(d_i)} \le \tau(d_i) \le d_i$ for each $1 \le i \le k$.) Since each $\chi \in \mathbb{X}$ has conductor dividing f, the weight of ξ^+ is bounded above by $f^{\|\xi^+\|} \le f^{4\lambda}$, and similarly for ξ^-. So $W^{1/4} \le f^{\lambda}$. Taking $L = n$, the bound claimed in Theorem 1.7 now follows from Theorem 1.4. □

2.3. **Proof of Corollary 1.9.** Choose a basis $\chi_1 \ldots, \chi_k$ for the character group $\mathbb{X}$ corresponding to K. Let n_i denote the order of χ_i. Suppose that K is unramified at q_0 and that q_0 splits into g distinct prime ideals in $\mathcal{O}_K$, where $g < n$. Since q_0 does not split completely, some $\chi_i(q_0) \ne 1$. So by Theorem 1.7, there is a prime $q \ll_{n,\varepsilon} f^{n/8+\varepsilon}$ with the property that $\chi_i(q)$ and $\chi_i(q_0)$ have the same multiplicative order for all $1 \le i \le k$. For this q, the multiset $\{\chi_i^0(q), \chi_i^1(q), \ldots, \chi_i^{n_i-1}(q)\}$ coincides with the multiset $\{\chi_i^0(q_0), \chi_i^1(q_0), \ldots, \chi_i^{n_i-1}(q_0)\}$ for all $1 \le i \le k$. Using that $\chi_1, \ldots, \chi_k$ are a basis for $\mathbb{X}$, we deduce that the multiset $\{\chi(q) : \chi \in \mathbb{X}\}$ coincides with the multiset $\{\chi(q_0) : \chi \in \mathbb{X}\}$. In particular, the number 1 appears in these two multisets with the same multiplicity. So by Proposition 2.1(ii), q is unramified in K and also splits into g distinct prime ideals in $\mathcal{O}_K$.

Remark. One can often improve the exponent $n/8$ in Corollary 1.9 by taking into account the factors $2^{\omega(d_i)}/d_i$ featuring in Theorem 1.7. We have not pursued such an improvement, since our objective was to obtain an entirely uniform bound.

2.4. **Remarks concerning the optimality of Theorem 1.7.** There are two points in the proof of Theorem 1.7 where one may wonder whether we are making optimal use of Theorem 1.4. The first is our crude estimation of W, where we pretend that all of the characters involved have conductor $f_{\mathbb{X}}$. This worst-case estimate is sharp only when one of ξ^+ or ξ^- is supported on characters of conductor $f_{\mathbb{X}}$. This does sometimes occur; for example, it holds whenever $f_{\mathbb{X}}$ is prime (as in the application to Corollary 1.8). But one can certainly construct families of pairs $(\mathbb{X}, \xi)$ where our worst-case assumption on the weights is indeed lossy. In such cases, a more careful application of Theorem 1.4 may be advantageous.

The second concern is with our choice of the detector form ξ. There are many other possible candidates for ξ besides (2.1). For example, if we set $P_{n,d}(x) := (x^n - 1)/\Phi_d(x)$ (where $\Phi_d(x)$ is the dth cyclotomic polynomial), then the form

$$\xi = \prod_{i=1}^{k} P_{n_i,d_i}(\chi_i) \in \mathbb{Z}[\mathbb{X}] \tag{2.2}$$

will also detect when each $\chi_i(q)$ has order d_i. This is arguably a more intuitively appealing choice than (2.1). It turns out, however, that the choice (2.2) has larger length than (2.1). Since W is bounded in terms of the length of ξ in the proof of Theorem 1.7, the choice (2.1) is better. Perhaps surprisingly, the choice (2.1) is not only better than (2.2) but is in fact best possible. We prove this here for the special case when $\mathbb{X}$ is cyclic.

Theorem 2.3. *Let $\mathbb{X}$ be a cyclic group of characters with generator χ. Suppose that $\mathbb{X}$ has order n and that d is a divisor of n. Finally, suppose that the form $\xi \in \mathbb{Z}[\mathbb{X}]$ has the following 'detector' property: For all primes q, with at most finitely many exceptions,*

$$\chi(q) \text{ has order } d \Longleftrightarrow \xi(q) \neq 0. \tag{2.3}$$

Then

$$\|\xi\| \geq n \cdot \frac{2^{\omega(d)}}{d}.$$

The proof depends on two lemmas. The first is the dual form of the usual Möbius inversion formula of elementary number theory. For a proof, see, for example, [14, Theorem A.22, p. 320].

Lemma 2.4. *Let $\mathscr{D}$ be a finite set of natural numbers that is* divisor-closed*, meaning that every divisor of an element of $\mathscr{D}$ also belongs to $\mathscr{D}$. Suppose that the two functions $f, g\colon \mathscr{D} \to \mathbb{C}$ have the property that for all $s \in \mathscr{D}$,*

$$f(s) = \sum_{\substack{r \in \mathscr{D} \\ s \mid r}} g(r).$$

Then for all $r \in \mathscr{D}$,

$$g(r) = \sum_{\substack{s \in \mathscr{D} \\ r \mid s}} f(s)\mu(s/r).$$

The next lemma is a polynomial version of Theorem 2.3, possibly of independent interest.

Lemma 2.5. *Let $A(x) = \sum_{0 \leq k < n} a_k x^k \in \mathbb{Z}[x]$ be a polynomial of degree smaller than n that vanishes at all nth roots of unity with the exception of those of order d, where d divides n. Then*

$$\sum_{0 \leq k < n} |a_k| \geq n \cdot \frac{2^{\omega(d)}}{d}.$$

Proof. After dividing by a suitable power of x, we can assume that $a_0 \neq 0$. Let $\mathscr{D}$ denote the set of divisors of d. For each $r \in \mathscr{D}$, set $A_r(x) := \sum_{\substack{0 \leq k < n \\ \gcd(k,d) = r}} a_k x^k$. Then $A(x) = \sum_{r \mid d} A_r(x)$. Moreover, if $s \in \mathscr{D}$, then

$$\sum_{\zeta^s = 1} A(\zeta) = \sum_{0 \leq k < n} a_k \sum_{\zeta^s = 1} \zeta^k = s \sum_{\substack{0 \leq k < n \\ s \mid k}} a_k = s \sum_{\substack{r \in \mathscr{D} \\ s \mid r}} A_r(1). \tag{2.4}$$

Now if s is a *proper* divisor of d, then A vanishes at all of the sth roots of unity, and so $\sum_{\zeta^s = 1} A(\zeta) = 0$. Also, since A vanishes at all nth roots of unity except those of order d,

$$\sum_{\zeta^d = 1} A(\zeta) = \sum_{\zeta^n = 1} A(\zeta) = n \sum_{\substack{0 \leq k < n \\ n \mid k}} a_k = a_0 n.$$

So from (2.4), we find that for $s \in \mathscr{D}$,

$$\sum_{\substack{r \in \mathscr{D} \\ s \mid r}} A_r(1) = \begin{cases} 0 & \text{if } s \text{ is a proper divisor of } d, \\ a_0 n/d & \text{if } s = d. \end{cases}$$

By the dual form of the Möbius inversion formula, we deduce that for every $r \in \mathscr{D}$,

$$A_r(1) = a_0 \mu(d/r) \frac{n}{d}.$$

Using that $|\mu| = \mu^2$, we see that

$$\begin{aligned} |a_0| + |a_1| + \cdots + |a_{n-1}| &\geq \sum_{r \mid d} |A_r(1)| \\ &= |a_0| \frac{n}{d} \sum_{r \mid d} \mu^2(d/r) = |a_0| \frac{n}{d} \sum_{r \mid d} \mu^2(r) = |a_0| n \cdot \frac{2^{\omega(d)}}{d}. \end{aligned}$$

Since $|a_0| \geq 1$, the lemma follows. □

Proof of Theorem 2.3. Since χ has order n, each nth root of unity is the value of $\chi(q)$ for infinitely many primes q (for example, by Dirichlet's theorem). Write $\xi = \sum_{k=0}^{n-1} a_k \chi^k$. Then ξ is not the zero element of $\mathbb{Z}[\mathbb{X}]$. (Otherwise, the detection property (2.3) implies that $\chi(q)$ has order d only finitely many times.) If q is a prime not dividing f_χ, then $\xi(q) = A(\chi(q))$, where $A(x) := \sum_{0 \leq k < n} a_k x^k \in \mathbb{Z}[x]$. Since each nth root of unity is the value of $\chi(q)$ for infinitely many primes q not dividing f_χ, condition (2.3) shows that A vanishes at all of the nth roots of unity with the exception of those of exact order d. Since $\|\xi\| = \sum_{0 \leq k < n} |a_k|$, the desired lower bound on $\|\xi\|$ follows from Lemma 2.5. □

Remark. The proof of the non-cyclic analogue of Theorem 2.3 is entirely analogous, but the notation is much more unwieldy.

3. Preliminaries for the proof of Theorem 1.4

In this section, we present several results needed for the proof of Theorem 1.4. The first is a variant of Burgess's character sum estimates [1, 2], due to Heath-Brown (see [7, Lemma 2.4] for a more precise statement). In this version of Burgess's estimates, the restriction to characters of cubefree conductor present in Burgess's work is replaced by a bound on the order of χ.

Proposition 3.1. *Suppose that χ is a primitive character of conductor $f_\chi > 1$ whose order divides the natural number n. Let $\varepsilon > 0$, and let r be a positive integer. Then for every pair of integers M and N with $N > 0$, we have*

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

The next lemma gives an application of Proposition 3.1 that will be required below.

Lemma 3.2. *Let $\mathbb{X}$ be a finite group of characters of exponent dividing n. Let $\xi = \sum_{\chi \in \mathbb{X}} a_\chi \chi$ be a form on $\mathbb{X}$ with each $a_\chi \geq 0$ and $a_{\mathbb{1}} = 0$. Let W be an upper bound on the weight W_ξ and let L be an upper bound on the length $\|\xi\|$. Let $0 < \eta < 1$, and let*

$$\sigma = 1 - \frac{1}{1 + \lceil 1/\eta \rceil}. \tag{3.1}$$

(Thus, $\frac{2}{3} \leq \sigma < 1$.) If $y \geq W^{\frac{1}{4}+\eta}$, then for every s on the line $\Re(s) = \sigma$,

$$\prod_{\chi \in \mathbb{X}} \left(\sum_{m \leq y} \frac{\chi(m)}{m^s} \right)^{a_\chi} \ll_{n,\eta,L} |s|^L y^{1-\sigma-\frac{\eta^2}{80}}.$$

Proof. We introduce two parameters, a positive integer r and a positive real number ε, both of whose values will be specified in the course of the argument. For each χ in the support of ξ and each $u \geq 1$, Proposition 3.1 shows that

$$\sum_{m \leq u} \chi(m) \ll_{r,n,\varepsilon} u^{1-1/r} f_\chi^{\frac{r+1}{4r^2}+\varepsilon}.$$

We now apply partial summation. Using σ for the real part of s, we find that

$$\begin{aligned}\sum_{m \leq y} \frac{\chi(m)}{m^s} &= \frac{1}{y^s} \sum_{m \leq y} \chi(m) + s \int_1^y \frac{1}{u^{s+1}} \sum_{m \leq u} \frac{\chi(m)}{m} \,\mathrm{d}u \\ &\ll_{r,n,\varepsilon} y^{1-1/r-\sigma} f_\chi^{\frac{r+1}{4r^2}+\varepsilon} + |s| f_\chi^{\frac{r+1}{4r^2}+\varepsilon} \int_1^y u^{-\sigma-1/r} \,\mathrm{d}u.\end{aligned}$$

Provided that $\sigma + 1/r > 1$, this last expression does not exceed

$$f_\chi^{\frac{r+1}{4r^2}+\varepsilon} \left(1 + |s| \int_1^\infty u^{-\sigma-1/r} \,\mathrm{d}u\right) = f_\chi^{\frac{r+1}{4r^2}+\varepsilon} (1 + |s|(\sigma + 1/r - 1)^{-1}).$$

Now take $r := \lceil 1/\eta \rceil$ (so that $r \geq 2$) and $\sigma := 1 - \frac{1}{r+1}$. (This choice of σ is the same as that specified in the lemma statement.) We find that on the line $\Re(s) = \sigma$,

$$\sum_{m \leq y} \frac{\chi(m)}{m^s} \ll_{\eta,n,\varepsilon} |s| f_\chi^{\frac{r+1}{4r^2}+\varepsilon}.$$

Multiplying over those $\chi \in \mathbb{X}$, each taken with multiplicity a_χ, gives

$$\begin{aligned}\prod_{\chi \in \mathbb{X}} \left(\sum_{m \leq y} \frac{\chi(m)}{m^s}\right)^{a_\chi} &\ll_{\eta,n,\varepsilon,L} |s|^L W^{\frac{r+1}{4r^2}+\varepsilon} \\ &= |s|^L y^{1-\sigma} \left(W^{\frac{r+1}{4r^2}+\varepsilon} y^{\sigma-1}\right).\end{aligned}$$

To complete the proof, it suffices to show that the final parenthesized expression is bounded by $y^{-\eta^2/80}$. Since $y \geq W^{\frac{1}{4}+\eta}$, we have that

$$\begin{aligned}W^{\frac{r+1}{4r^2}+\varepsilon} y^{\sigma-1} &\leq (y^{\frac{4}{1+4\eta}})^{\frac{r+1}{4r^2}+\varepsilon} y^{-\frac{1}{r+1}} \\ &= y^{\frac{-4\eta r^2+4\varepsilon(r^2+r^3)+2r+1}{(4\eta+1)r^2(r+1)}} \leq y^{\frac{1-2r+8\varepsilon r^3}{(4\eta+1)r^2(r+1)}},\end{aligned}$$

where in the last step we used the bound $\eta \geq 1/r$ coming from our definition of r. Now select $\varepsilon := \frac{1}{8r^2}$; then

$$\begin{aligned}\frac{1-2r+8\varepsilon r^3}{(4\eta+1)r^2(r+1)} &= \frac{1-r}{(4\eta+1)r^2(r+1)} \leq \frac{-r/2}{(4\eta+1)r^2(r+1)} \\ &= -\frac{1}{2r(r+1)(4\eta+1)} \leq -\frac{1}{(2r)\cdot(2r)\cdot 5} = -\frac{1}{20r^2}.\end{aligned}$$

Since $r \leq 2/\eta$, this last expression is at most $-\eta^2/80$, which finishes the proof. □

The next two lemmas collect well-known results on $L(1,\chi)$.

Proposition 3.3. *Let χ be a primitive character with conductor $f_\chi > 1$. Let $\varepsilon > 0$. Then*

$$f_\chi^{-\varepsilon} \ll_\varepsilon |L(1,\chi)| \ll \log f_\chi.$$

Proof. For the upper bound, see (e.g.) [13, Lemma 10.15, p. 350]. For non-real characters χ, we have $|L(1,\chi)| \gg 1/\log f_\chi$ (see [13, Theorem 11.4, pp. 362–363]), which is stronger than the lower bound claimed above. Finally, for real χ, the lower bound $|L(1,\chi)| \gg_\varepsilon f_\chi^{-\varepsilon}$ is the celebrated theorem of Siegel [13, Theorem 11.14, p. 372]. □

Lemma 3.4. *Let χ be a primitive character of conductor $f_\chi > 1$, with order dividing n. Suppose that $0 < \eta \le 1/3$. If $y \ge f_\chi^{\frac{1}{4}+\eta}$, then*

$$\sum_{m\le y} \frac{\chi(m)}{m} = L(1,\chi)\left(1 + O_{n,\eta}(y^{-\eta^2/2})\right).$$

Proof. Under the hypotheses on χ and η appearing in the lemma statement, one can show that for all real numbers $u \ge f_\chi^{1/4+\eta}$,

$$\sum_{m\le u} \chi(m) \ll_{n,\eta} u^{1-\eta^2}.$$

(See [16, Lemma 3], and compare with [9, eq. (12.57), p. 326].) So for $y \ge f_\chi^{1/4+\eta}$,

$$\begin{aligned} L(1,\chi) - \sum_{m\le y}\frac{\chi(m)}{m} &= \sum_{m>y}\frac{\chi(m)}{m} \\ &= -\frac{1}{y}\sum_{m\le y}\chi(m) + \int_y^\infty \left(\sum_{m\le u}\chi(m)\right)\frac{\mathrm{d}u}{u^2} \ll_{n,\eta} y^{-\eta^2}. \end{aligned}$$

By Proposition 3.3, we have $|L(1,\chi)| \gg_\eta f_\chi^{-\eta^2/8} \ge y^{-\eta^2/2}$, and so

$$\begin{aligned} \sum_{m\le y}\frac{\chi(m)}{m} &= L(1,\chi) + O_{\eta,n}(y^{-\eta^2}) \\ &= L(1,\chi)(1 + O_{\eta,n}(y^{-\eta^2/2})). \end{aligned}$$

This completes the proof of the lemma. □

As in Elliott's work [5], our argument invokes a standard variant of Perron's theorem (proved, for instance, in [8, pp. 486–487]).

Lemma 3.5. *Let $F(s) = \sum_{n=1}^\infty f(n)n^{-s}$ be a Dirichlet series that converges absolutely in the half-plane $\Re(s) > 1$, and let ℓ be a positive integer. Then*

$$\frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty} F(s)\frac{x^s}{s^{\ell+1}}\,\mathrm{d}s = \frac{1}{\ell!}\sum_{n\le x} f(n)\left(\log\frac{x}{n}\right)^\ell$$

for any choice of $\sigma > 1$.

4. Proof of Theorem 1.4

We may assume that $0 < \varepsilon < 1/3$. Let $y := W^{1/4}f^\varepsilon$. Our strategy is as follows: We suppose that the smallest $q \nmid f$ with $\xi(q) \neq 0$ exceeds y, and we prove that f is bounded (in terms of L, n, and ε). Consequently, Theorem 1.4 holds with an implied constant of 1 once f is large enough. On the other hand, since $\xi(q)$ is nonvanishing for all primes q from a certain coprime progression modulo f, the smallest q in Theorem 1.4 is bounded by a function of f. Thus, if $f \ll_{L,n,\varepsilon} 1$, then $q \ll_{L,n,\varepsilon} 1$. So enlarging the implied constant if necessary, the estimate of Theorem 1.4 holds in every case.

Write $\xi^+ = \sum_{\chi\in\mathbb{X}} a_{\chi,+}\chi$ and $\xi^- = \sum_{\chi\in\mathbb{X}} a_{\chi,-}\chi$. Since $\xi(0) = \pm 1$, either $a_{\mathbb{1},+} = 1$ or $a_{\mathbb{1},-} = 1$. Without loss of generality, we can assume that $a_{\mathbb{1},+} = 1$. (Otherwise, replace ξ with $-\xi$). Let $G(s)$ be the Dirichlet series determined by the formal identity

$$\prod_{\chi\in\mathbb{X}} L(s,\chi)^{a_{\chi,+}} = G(s)\prod_{\chi\in\mathbb{X}} L(s,\chi)^{a_{\chi,-}}. \tag{4.1}$$

Lemma 4.1. *Write $G(s) = \sum_{m=1}^{\infty} g(m)m^{-s}$. Then all of the following hold:*

(i) The function $g(\cdot)$ is multiplicative.
(ii) If $g(m)\neq 0$ for the natural number $m\leq y$, then each prime dividing m appears to the second power or higher, except possibly for those primes dividing f.
(iii) For each natural number m,

$$|g(m)| \leq \tau_{\|\xi\|}(m).$$

Proof. Expanding each $L(s,\chi)$ as an Euler product, we find that

$$G(s) = \prod_p \prod_{\chi\in\mathbb{X}} \left((1+\chi(p)p^{-s}+\chi(p^2)p^{-2s}+\dots)^{a_{\chi,+}}(1-\chi(p)p^{-s})^{a_{\chi,-}}\right). \tag{4.2}$$

Since $G(s)$ has an Euler-product expansion, (i) immediate. We can read off from (4.2) that for each prime p,

$$g(p) = \sum_{\chi\in\mathbb{X}} (a_{\chi,+}-a_{\chi,-})\chi(p) = \xi^+(p)-\xi^-(p) = \xi(p).$$

By assumption, $\xi(p) = 0$ for all $p\leq y$, except possibly for those primes dividing f. So (ii) follows from the multiplicativity of $g(\cdot)$. Finally, (4.2) shows that each coefficient of $G(s)$ is bounded in absolute value by the corresponding coefficient of

$$\prod_p \prod_{\chi\in\mathbb{X}} \left((1+p^{-s}+p^{-2s}+\dots)^{a_{\chi,+}+a_{\chi,-}}\right) = \zeta(s)^{\|\xi\|}.$$

In other words, $|g(m)|\leq \tau_{\|\xi\|}(m)$, which is (iii). □

We have arranged matters so that $L(s,\mathbb{1}) = \zeta(s)$ appears in the left-hand side of (4.1) to the power $a_{\mathbb{1},+} = 1$. So from (4.1), the two Dirichlet series

$$\zeta(s)\prod_{\substack{\chi\in\mathbb{X}\\ \chi\neq\mathbb{1}}}\left(\sum_{m\leq y}\frac{\chi(m)}{m^s}\right)^{a_{\chi,+}} \quad\text{and}\quad \left(\sum_{m\leq y}\frac{g(m)}{m^s}\right)\prod_{\chi\in\mathbb{X}}\left(\sum_{m\leq y}\frac{\chi(m)}{m^s}\right)^{a_{\chi,-}}$$

share the same initial $\lfloor y\rfloor$ coefficients. Lemma 3.5 now implies that for any integer $\ell\geq 1$,

$$\begin{aligned}\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}&\left(\zeta(s)\prod_{\substack{\chi\in\mathbb{X}\\ \chi\neq\mathbb{1}}}\left(\sum_{m\leq y}\frac{\chi(m)}{m^s}\right)^{a_{\chi,+}}\right)\frac{y^s}{s^{\ell+1}}\,\mathrm{d}s\\ &= \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\left(\sum_{m\leq y}\frac{g(m)}{m^s}\prod_{\chi\in\mathbb{X}}\left(\sum_{m\leq y}\frac{\chi(m)}{m^s}\right)^{a_{\chi,-}}\right)\frac{y^s}{s^{\ell+1}}\,\mathrm{d}s.\end{aligned} \tag{4.3}$$

For technical reasons related to issues of convergence, in what follows we fix the choice

$$\ell := L+2.$$

Having fixed ℓ, we proceed to estimate both sides of (4.3).

Lemma 4.2. *We have*

$$\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\left(\zeta(s)\prod_{\substack{\chi\in\mathbb{X}\\ \chi\neq\mathbb{1}}}\left(\sum_{m\le y}\frac{\chi(m)}{m^s}\right)^{a_{\chi,+}}\right)\frac{y^s}{s^{\ell+1}}\,\mathrm{d}s = y\prod_{\substack{\chi\in\mathbb{X}\\ \chi\neq\mathbb{1}}}L(1,\chi)^{a_{\chi,+}} + O_{n,\varepsilon,L}(y^{1-\frac{\varepsilon^2}{80L^2}}). \tag{4.4}$$

Proof. Since $\mathbb{X}$ has conductor f, it is clear that $W_{\xi^+} = \prod_{\chi\in\mathbb{X}} f_\chi^{a_{\chi,+}} \le f^{\sum_{\chi\in\mathbb{X}} a_{\chi,+}} \le f^{\|\xi\|}$, and similarly for W_{ξ^-}. Thus, $W \le f^{\|\xi\|} \le f^L$, and our choice of y satisfies

$$y = W^{1/4} f^{\varepsilon} \ge W^{\frac{1}{4}+\eta}, \quad \text{where} \quad \eta := \varepsilon/L.$$

Shift the line of integration to $\Re(s) = \sigma$, where σ is defined in terms of η by (3.1). We pick up a residue from the pole at $s = 1$, which contributes (recall Lemma 3.4)

$$y\prod_{\substack{\chi\in\mathbb{X}\\ \chi\neq\mathbb{1}}}\left(\sum_{m\le y}\frac{\chi(m)}{m}\right)^{a_{\chi,+}} = \left(y\prod_{\substack{\chi\in\mathbb{X}\\ \chi\neq\mathbb{1}}}L(1,\chi)^{a_{\chi,+}}\right)\left(1 + O_{n,\eta,L}(y^{-\eta^2/2})\right). \tag{4.5}$$

By Proposition 3.3, for each nonprincipal χ with $a_{\chi,+} > 0$, we have

$$L(1,\chi) \ll \log f_\chi \le \log W \ll \log y,$$

and so the expression (4.5) is

$$y\prod_{\substack{\chi\in\mathbb{X}\\ \chi\neq\mathbb{1}}}L(1,\chi)^{a_{\chi,+}} + O_{n,\eta,L}(y^{1-\frac{\eta^2}{4}}).$$

It remains to estimate the size of the integral after the shift to the line $\Re(s) = \sigma$. Apply Lemma 3.2 to the form $\xi^+ - \mathbb{1}$. Note that the weight of $\xi^+ - \mathbb{1}$ is the same as that of ξ^+ (which is bounded by W) and that the length of $\xi^+ - \mathbb{1}$ is bounded by L. So Lemma 3.2 shows that the integral along the line $\Re(s) = \sigma$ is

$$\begin{aligned} &\ll_{n,\eta,L} \int_{\sigma-i\infty}^{\sigma+i\infty} |\zeta(s)|\cdot(|s|^L y^{1-\sigma-\eta^2/80})\cdot\frac{y^\sigma}{|s|^{\ell+1}}\,|\mathrm{d}s| \\ &\qquad = y^{1-\frac{\eta^2}{80}}\int_{\sigma-i\infty}^{\sigma+i\infty}|\zeta(s)|\cdot|s|^{L-\ell-1}\,|\mathrm{d}s|. \end{aligned} \tag{4.6}$$

Recall that for $\Re(s) \ge \frac{1}{2}$, one has $\zeta(s) \ll |s|(1 + 1/|s-1|)$ (see [4, p. 79]). When $\Re(s) = \sigma$, we have $|s-1| \ge |\sigma-1| \gg_\eta 1$; thus, $\zeta(s) \ll_\eta |s|$ on the entire line $\Re(s) = \sigma$. By this estimate and our choice of ℓ,

$$\int_{\sigma-i\infty}^{\sigma+i\infty}|\zeta(s)|\cdot|s|^{L-\ell-1}\,|\mathrm{d}s| \ll_\eta \int_{\sigma-i\infty}^{\sigma+i\infty}|s|^{L-\ell}\,|\mathrm{d}s| = \int_{\sigma-i\infty}^{\sigma+i\infty}\frac{|\mathrm{d}s|}{|s|^2} \ll_\eta 1.$$

Putting this back into (4.6), we get an upper bound of $O_{n,\eta,L}(y^{1-\frac{\eta^2}{80}})$.

Piecing the above estimates together, we find that the left-hand side of (4.4) is

$$y\prod_{\substack{\chi\in\mathbb{X}\\ \chi\neq\mathbb{1}}}L(1,\chi)^{a_{\chi,+}} + O_{n,\eta,L}(y^{1-\frac{\eta^2}{80}}).$$

Since $\eta = \varepsilon/L$, the lemma follows. □

Lemma 4.3. *We have*

$$\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\left(\sum_{m\le y}\frac{g(m)}{m^s}\prod_{\chi\in\mathbb{X}}\left(\sum_{m\le y}\frac{\chi(m)}{m^s}\right)^{a_{\chi,-}}\right)\frac{y^s}{s^{\ell+1}}\,\mathrm{d}s \ll_{n,\varepsilon,L} \tau(f)\cdot y^{1-\frac{\varepsilon^2}{80L^2}}.$$

Proof. As in the proof of Lemma 4.2, we begin by shifting the line of integration to $\Re(s)=\sigma$, where σ is defined by (3.1) with $\eta=\varepsilon/L$. In contrast to the previous case, the present integrand is defined and analytic for $\Re(s)>0$, and so we do not pick up any residues; thus, shifting the contour does not change the value of the integral. Proceeding as in the proof of Lemma 4.2 (but with Lemma 3.2 now applied to ξ^-), we see that the value of the shifted integral is

$$\ll_{n,\varepsilon,L} y^{1-\frac{\eta^2}{80}}\sum_{m\le y}\frac{|g(m)|}{m^\sigma}. \tag{4.7}$$

To estimate the sum on m, we use the results of Lemma 4.1 along with partial summation. We begin by showing that for $u\le y$, we have $S(u):=\sum_{m\le u}|g(m)|\ll_L \tau(f)u^{3/5}$. By Lemma 4.1(ii), every $m\le u$ for which $g(m)$ is nonvanishing can be written as the product of a divisor of f and a squarefull integer. Since the number of squarefull numbers in $[1,u]$ is $O(u^{1/2})$, the number of $m\le u$ with $g(m)\neq 0$ is $O(\tau(f)u^{1/2})$. Lemma 4.1(iii) implies that for every $m\le u$,

$$|g(m)|\le \tau_{\|\xi\|}(m)\le \tau(m)^{\|\xi\|-1}\le\tau(m)^{L-1}\ll_L u^{1/10}.$$

(In the last step, we have used the well-known estimate $\tau(m)\ll_\beta m^\beta$ for all $\beta>0$; see, for example, [6, Theorem 315, p. 343].) Thus,

$$|S(u)|\le\left(\max_{m\le u}|g(m)|\right)\sum_{\substack{m\le u\\ g(m)\neq 0}}1\ll_L u^{1/10}\cdot\tau(f)u^{1/2}=\tau(f)u^{3/5},$$

as claimed. Recalling that $\sigma\ge\frac{2}{3}$, we find that

$$\begin{aligned}\sum_{m\le y}|g(m)|m^{-\sigma}\le\int_{1^-}^{y}u^{-2/3}\,\mathrm{d}S(u)&=S(y)y^{-2/3}+\frac{2}{3}\int_1^y S(u)u^{-5/3}\,\mathrm{d}u\\ &\ll_L \tau(f)\left(y^{-1/15}+\int_1^y u^{-16/15}\,\mathrm{d}u\right)\ll\tau(f).\end{aligned}$$

Substituting this estimate into (4.7) completes the proof. □

Setting the estimates of Lemmas 4.2 and 4.3 equal to each other, we get the upper bound $\prod_{\chi\in\mathbb{X},\ \chi\neq\mathbb{1}}L(1,\chi)^{a_{\chi,+}}\ll_{n,\varepsilon,L}\tau(f)\cdot y^{-\varepsilon^2/80L^2}$. On the other hand, Proposition 3.3 shows that $\prod_{\chi\in\mathbb{X},\ \chi\neq\mathbb{1}}L(1,\chi)^{a_{\chi,+}}\gg_{\varepsilon,L}W^{-\varepsilon^2/640L^2}$ (say). Comparing these estimates, we get the lower bound

$$\begin{aligned}\tau(f)&\gg_{n,\varepsilon,L}y^{\varepsilon^2/80L^2}\cdot W^{-\varepsilon^2/640L^2}\\ &\ge y^{\varepsilon^2/80L^2}\cdot(y^4)^{-\varepsilon^2/640L^2}=y^{\varepsilon^2/160L^2},\end{aligned}$$

using that $y\ge W^{1/4}$. Since also $y\ge f^\varepsilon$, another appeal to the maximal order of the divisor function gives

$$\tau(f)\ll_{\varepsilon,L}y^{\varepsilon^2/320L^2}.$$

Comparing the last two displayed estimates shows that y is bounded in terms of n,ε, and L. So f is also bounded. The remarks at the start of this section now finish the proof of Theorem 1.4.

Remark. The use of contour integration in the proof of Theorem 1.4 can be avoided, as was shown by Pintz [15] in a closely related context. Indeed, Pintz's approach was followed by the author in [16]. However, it seems that the arrangement we have chosen above better highlights the similarities between our arguments and those of Elliott [5].

Acknowledgements

The author thanks Carl Pomerance for useful discussions. He is also grateful to Enrique Treviño and the referees for carefully reading through earlier drafts and proposing a number of corrections, clarifications, and simplifications.

References

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

[2] ———, *The character sum estimate with* $r = 3$, J. London Math. Soc. (2) **33** (1986), 219–226.

[3] H. Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000.

[4] H. Davenport, *Multiplicative number theory*, third ed., Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York, 2000.

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

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

[7] 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), 265–338.

[8] A. Ivić, *The Riemann zeta-function*, Dover Publications Inc., Mineola, NY, 2003.

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

[10] S. Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[11] U. V. Linnik, *On the least prime in an arithmetic progression. I. The basic theorem*, Rec. Math. (Mat. Sbornik) N.S. **15** (**57**) (1944), 139–178.

[12] ———, *On the least prime in an arithmetic progression. II. The Deuring-Heilbronn phenomenon*, Rec. Math. (Mat. Sbornik) N.S. **15** (**57**) (1944), 347–368.

[13] 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.

[14] M. B. Nathanson, *Additive number theory: the classical bases*, Graduate Texts in Mathematics, vol. 164, Springer-Verlag, New York, 1996.

[15] J. Pintz, *Elementary methods in the theory of L-functions. VI. On the least prime quadratic residue* (mod p), Acta Arith. **32** (1977), 173–178.

[16] P. Pollack, *The smallest prime that splits completely in an abelian number field*, Proc. Amer. Math. Soc. (to appear).

[17] A. I. Vinogradov and U. V. Linnik, *Hyperelliptic curves and the least prime quadratic residue*, Dokl. Akad. Nauk SSSR **168** (1966), 259–261 (Russian).

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

[19] T. Xylouris, *On the least prime in an arithmetic progression and estimates for the zeros of Dirichlet L-functions*, Acta Arith. **150** (2011), 65–91.

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