Canad. J. Math. Vol. 62 (5), 2010 pp. 1099–1115
doi:10.4153/CJM-2010-047-9

Character Sums to Smooth Moduli are Small

Leo Goldmakher

Abstract. Recently, Granville and Soundararajan have made fundamental breakthroughs in the study of character sums. Building on their work and using estimates on short character sums developed by Graham–Ringrose and Iwaniec, we improve the Pólya–Vinogradov inequality for characters with smooth conductor.

1 Introduction

Introduced by Dirichlet to prove his celebrated theorem on primes in arithmetic progressions (see [1]), Dirichlet characters have proved to be a fundamental tool in number theory. In particular, character sums of the form

$$S_\chi(x) := \sum_{n\le x} \chi(n)$$

(where $\chi(\operatorname{mod} q)$ is a Dirichlet character) arise naturally in many classical problems of analytic number theory, from estimating the least quadratic nonresidue (mod p) to bounding L-functions. Recall that for any character $\chi(\operatorname{mod} q)$, $|S_\chi(x)|$ is trivially bounded above by $\varphi(q)$. A folklore conjecture (which is a consequence of the Generalized Riemann Hypothesis) predicts that for non-principal characters the true bound should look like[1]

$$|S_\chi(x)| \ll_\epsilon \sqrt{x}\cdot q^\epsilon.$$

Although we are currently very far from being able to prove such a statement, there have been some significant improvements over the trivial estimate. The first such is due (independently) to Pólya and Vinogradov. They proved that

$$|S_\chi(x)| \ll \sqrt{q}\log q$$

(see [1, pp. 135–137]). Almost 60 years later, Montgomery and Vaughan [10] showed that, conditionally on the Generalized Riemann Hypothesis (GRH), one can improve Pólya–Vinogradov to

$$|S_\chi(x)| \ll \sqrt{q}\log\log q.$$

Received by the editors December 19, 2007.
Published electronically June 14, 2010.
AMS subject classification: **11L40**, 11M06.

[1]Here and throughout we use Vinogradov's notation $f \ll g$ to mean $f = O(g)$, with variables in subscript to indicate dependence of the implicit constant.

This is a best possible result, since in 1932 Paley [12] gave an unconditional construction of an infinite class of quadratic characters for which the magnitude of the character sum could be made $\gg \sqrt{q}\log\log q$.

In their recent work, Granville and Soundararajan [4] gave a characterization of when a character sum can be large. From this they were able to deduce a number of new results, including an improvement of Pólya–Vinogradov (unconditionally) and of Montgomery–Vaughan (on GRH) for characters of small odd order. In the present paper we explore a different application of their characterization. Recall that a positive integer N is said to be *smooth* if its prime factors are all small relative to N; if in addition the product of all its prime factors is small, N is *powerful*. Building on the work of Granville and Soundararajan and using a striking estimate developed by Graham and Ringrose, we will obtain (in Section 5) the following improvement of Pólya–Vinogradov for characters of smooth conductor.

Theorem 1 *Given $\chi(\operatorname{mod} q)$ a primitive character, with q squarefree. For any integer n, denote its largest prime factor by $\mathcal{P}(n)$. Then*

$$|S_\chi(x)| \ll \sqrt{q}(\log q)\Big(\Big(\frac{\log\log\log q}{\log\log q}\Big)^{\frac{1}{2}} + \Big(\frac{(\log\log\log q)^2\log(\mathcal{P}(q)d(q))}{\log q}\Big)^{1/4}\Big)$$

where $d(q)$ is the number of divisors of q, and the implied constant is absolute.

From the well-known upper bound $\log d(q) \ll \frac{\log q}{\log\log q}$ (see, for example, [11, Ex. 1.3.3]), we immediately deduce the following weaker but more concrete bound.

Corollary *Given $\chi(\operatorname{mod} q)$ primitive, with q squarefree. Then*

$$|S_\chi(x)| \ll \sqrt{q}(\log q)\Big(\frac{(\log\log\log q)^2}{\log\log q} + \frac{(\log\log\log q)^2\log\mathcal{P}(q)}{\log q}\Big)^{\frac{1}{4}}$$

where the implied constant is absolute.

For characters with powerful conductor, we can do better by appealing to the work of Iwaniec [9]. We prove the following.

Theorem 2 *Given $\chi(\operatorname{mod} q)$ a primitive Dirichlet character with q large and*

$$\operatorname{rad}(q) \le \exp\big((\log q)^{3/4}\big),$$

where the radical of q is defined

$$\operatorname{rad}(q) := \prod_{p|q} p.$$

Then

$$|S_\chi(x)| \ll_\epsilon \sqrt{q}(\log q)^{7/8+\epsilon}.$$

https://doi.org/10.4153/CJM-2010-047-9 Published online by Cambridge University Press

The key ingredient in the proofs of Theorems 1 and 2 is also at the heart of [4]. In that paper, Granville and Soundararajan introduce a notion of 'distance' on the set of characters, and then show that $|S_\chi(x)|$ is large if and only if χ is close (with respect to their distance) to a primitive character of small conductor and opposite parity. (Ideas along these lines had been earlier considered by Hildebrand in [8], and—in the context of mean values of arithmetic functions—by Halász in [6, 7].) More precisely, given characters χ, ψ, let

$$\mathbb{D}(\chi, \psi; y) := \left(\sum_{p \le y} \frac{1 - \operatorname{Re} \chi(p)\overline{\psi}(p)}{p} \right)^{\frac{1}{2}}.$$

Although it is possible for $\mathbb{D}(\chi, \chi; y) \neq 0$, all the other properties of a distance function are satisfied; in particular, a triangle inequality holds:

$$\mathbb{D}(\chi_1, \psi_1; y) + \mathbb{D}(\chi_2, \psi_2; y) \ge \mathbb{D}(\chi_1\chi_2, \psi_1\psi_2; y).$$

See [5] for a more general form of this 'distance' and its role in number theory. Granville and Soundararajan's characterization of large character sums comes in the form of the following two theorems.

Theorem A ([4, Theorem 2.1]) *Given $\chi(\operatorname{mod} q)$ primitive, let $\xi(\operatorname{mod} m)$ be any primitive character of conductor less than $(\log q)^{\frac{1}{3}}$ which minimizes the quantity $\mathbb{D}(\chi, \xi; q)$. Then*

$$|S_\chi(x)| \ll (1 - \chi(-1)\xi(-1)) \frac{\sqrt{m}}{\varphi(m)} \sqrt{q} \log q \exp\Big(-\frac{1}{2}\mathbb{D}(\chi, \xi; q)^2\Big) + \sqrt{q}(\log q)^{\frac{6}{7}}.$$

Theorem B ([4, Theorem 2.2]) *Given $\chi(\operatorname{mod} q)$ a primitive character, let $\xi(\operatorname{mod} m)$ be any primitive character of opposite parity. Then*

$$\max_x |S_\chi(x)| + \frac{\sqrt{m}}{\varphi(m)} \sqrt{q} \log\log q \gg \frac{\sqrt{m}}{\varphi(m)} \sqrt{q} \log q \exp(-\mathbb{D}(\chi, \xi; q)^2).$$

Roughly, the first theorem says that $|S_\chi(x)|$ is small (*i.e.*, $\ll \sqrt{q}(\log q)^{6/7}$) unless there exists a primitive character ξ of small conductor and opposite parity, whose distance from χ is small (*i.e.*, $\mathbb{D}(\chi, \xi; q)^2 \le \frac{2}{7} \log\log q$). The second theorem says that if there exists a primitive character $\xi(\operatorname{mod} m)$ of small conductor and of opposite parity, whose distance from χ is small, then $|S_\chi(x)|$ gets large. In particular, to improve Pólya–Vinogradov for a primitive character $\chi(\operatorname{mod} q)$, it suffices (by Theorem A) to find a lower bound on the distance from χ to primitive characters of small conductor and opposite parity. For example, if one can find a positive constant δ, independent of q, for which

$$\mathbb{D}(\chi, \xi; q)^2 \ge (\delta + o(1)) \log\log q, \tag{1.1}$$

then Theorem A would immediately yield an improvement of Pólya–Vinogradov:

$$\max_x |S_\chi(x)| \ll \sqrt{q}(\log q)^{1 - \frac{\delta}{2} + o(1)}.$$

As it turns out (see [4, Lemma 3.2]), it is not too difficult to show that (1.1) holds for χ a character of odd order g, with $\delta = \delta_g = 1 - \frac{g}{\pi} \sin \frac{\pi}{g}$.

Thus, to derive bounds on character sums from Theorem A, one must understand the magnitude of $\mathbb{D}(\chi, \xi; q)$. This is the problem we take up in Section 2. Since $\mathbb{D}(\chi, \xi; q) = \mathbb{D}(\chi\overline{\xi}, 1; q)$, we are naturally led to study lower bounds on distances of the form $\mathbb{D}(\chi, 1; y)$, for χ a primitive character and y a parameter with some flexibility. By definition,

$$\mathbb{D}(\chi, 1; y)^2 = \sum_{p \leq y} \frac{1}{p} - \operatorname{Re} \sum_{p \leq y} \frac{\chi(p)}{p}.$$

The first sum on the right hand side is well approximated by $\log \log y$ (a classical estimate due to Mertens, see [1, pp. 56–57]). We will show that the second sum is comparable to $|L(s_y, \chi)|$, where

$$s_y := 1 + \frac{1}{\log y}.$$

To be precise, in Section 2 we prove the following.

Lemma 3 *For all $y \geq 2$,*

$$\mathbb{D}(\chi, 1; y)^2 = \log \left| \frac{\log y}{L(s_y, \chi)} \right| + O(1).$$

Our problem is now reduced to finding upper bounds on $|L(s, \chi)|$ for s slightly larger than 1. This is a classical subject, and many bounds are available. Thanks to the remarkable work of Graham and Ringrose [3] on short character sums, a particularly strong upper bound on L-functions is known when the character has smooth modulus. From a slight generalization of their result, we will deduce the following (in Section 3).

Lemma 4 *Given a primitive character χ (mod Q), let r be any positive number such that for all $p \geq r$, $\operatorname{ord}_p Q \leq 1$. Let*

$$q' = q'_r := \prod_{p<r} p^{\operatorname{ord}_p Q}$$

and denote by $\mathcal{P}(Q)$ the largest prime factor of Q. Then for all $y > 3$,

$$|L(s_y, \chi)| \ll \log q' + \frac{\log Q}{\log \log Q} + \sqrt{(\log Q)\big(\log \mathcal{P}(Q) + \log d(Q)\big)},$$

where the implied constant is absolute.

Using the bound $\log d(Q) \ll \frac{\log Q}{\log \log Q}$, one deduces the weaker but more concrete bound

$$|L(s_y, \chi)| \ll \log q' + \frac{\log Q}{(\log \log Q)^{1/2}} + \sqrt{(\log Q)\big(\log \mathcal{P}(Q)\big)}.$$

Lemma 4 will enable us to prove Theorem 1. For the proof of Theorem 2, we need a corresponding bound for $L(s_y, \chi)$ when the conductor of χ is powerful. In Section 4, we will prove the following using a potent estimate of Iwaniec [9].

Lemma 5 *Given χ (mod Q) a primitive Dirichlet character with Q large and*

$$\mathrm{rad}(Q) \le \exp(2(\log Q)^{3/4}).$$

Then for all $y > 3$, $|L(s_y, \chi)| \ll_\epsilon (\log Q)^{3/4+\epsilon}$.

In the final section of the paper, we synthesize our results and prove Theorems 1 and 2.

2 The Size of $\mathbb{D}(\chi, 1; y)$

How large should one expect $\mathbb{D}(\chi, 1; y)$ to be? Before proving Lemma 3 we gain intuition by exploring what can be deduced from GRH.

Proposition 2.1 *Assume GRH. For any non-principal character χ (mod Q) we have*

$$\mathbb{D}(\chi, 1; y)^2 = \log\log y + O(\log\log\log Q).$$

Proof Since

$$\sum_{p \le y} \frac{1}{p} = \log\log y + O(1)$$

by Mertens' well-known estimate, we need only show that

$$\sum_{p \le y} \frac{\chi(p)}{p} = O(\log\log\log Q).$$

We may assume that $y > (\log Q)^6$, else the estimate is trivial. Recall that on GRH, for all $x > (\log Q)^6$ we have:

$$\theta(x, \chi) := \sum_{p \le x} \chi(p) \log p \ll \sqrt{x} (\log Qx)^2 \ll x^{5/6}.$$

(Such a bound may be deduced from the first formula appearing on page 125 of [1].) Partial summation now gives

$$\sum_{(\log Q)^6 < p \le y} \frac{\chi(p)}{p} = \int_{(\log Q)^6}^{y} \frac{1}{t \log t}\, d\theta(t, \chi) \ll \frac{1}{\log Q} \ll 1$$

and the proposition follows. ∎

We now return to unconditional results. Recall that the prime number theorem gives $\theta(x) := \sum_{p \le x} \log p \sim x$.

Proof of Lemma 3 As before, by Mertens' estimate it suffices to show that

$$\operatorname{Re}\sum_{p\le y}\frac{\chi(p)}{p}=\log|L(s_y,\chi)|+O(1), \tag{2.1}$$

where $s_y := 1+(\log y)^{-1}$. From the Euler product we know

$$\log|L(s_y,\chi)|=\operatorname{Re}\sum_p\sum_{k=1}^{\infty}\frac{\chi(p)^k}{kp^{ks_y}}=\operatorname{Re}\sum_p\frac{\chi(p)}{p^{s_y}}+O(1),$$

so that (2.1) would follow from

$$\sum_{p\le y}\Big(\frac{1}{p}-\frac{1}{p^{s_y}}\Big)+\sum_{p>y}\frac{1}{p^{s_y}}\ll 1.$$

The first term above is

$$\sum_{p\le y}\Big(\frac{1}{p}-\frac{1}{p^{s_y}}\Big)=\sum_{p\le y}\frac{1-\exp\big(-\frac{\log p}{\log y}\big)}{p}\le\frac{1}{\log y}\sum_{p\le y}\frac{\log p}{p}=$$
$$\frac{1}{\log y}\int_1^y\frac{1}{t}\,d\theta(t)\ll 1$$

by partial summation and the prime number theorem. A second application of partial summation and the prime number theorem yields

$$\sum_{p>y}\frac{1}{p^{s_y}}=\int_y^{\infty}\frac{1}{t^{s_y}\log t}\,d\theta(t)\ll 1.$$

The lemma follows. ■

For a clearer picture of where we are heading, we work out a simple consequence of this result. Let $\chi \pmod q$ and $\xi \pmod m$ be as in Theorem A. By Lemma 3,

$$\mathbb{D}(\chi,\xi;q)^2=\mathbb{D}(\chi\overline{\xi},1;q)^2=\log\Big|\frac{\log q}{L(s_q,\chi\overline{\xi})}\Big|+O(1),$$

and Theorem A immediately yields the following.

Proposition 2.2 *Let $\chi \pmod q$ be a primitive character, and ξ a character as in Theorem A. Then*

$$|S_\chi(x)|\ll\sqrt{q}\sqrt{(\log q)|L(s_q,\chi\overline{\xi})|}+\sqrt{q}(\log q)^{6/7}.$$

Thus, to improve Pólya–Vinogradov, it suffices to prove $L(s_q,\chi\overline{\xi})=o(\log q)$. This is the problem we explore in the next two sections.

3 Proof of Lemma 4

We ultimately wish to bound $|L(s_q, \chi\overline{\xi})|$. In this section we explore the more general quantity $|L(s_y, \chi)|$, where throughout y will be assumed to be at least 3, and Q will denote the conductor of χ.

By partial summation (see [1, (8), p. 33]),

$$L(s_y, \chi) = s_y \int_1^\infty \frac{1}{t^{s_y+1}} \Big(\sum_{n \le t} \chi(n) \Big) \, dt.$$

When $t > Q$, the character sum is trivially bounded by Q, so that this portion of the integral contributes an amount $\ll 1$. For $t \le T$ (a suitable parameter to be chosen later), we may bound our character sum by t, and therefore this portion of the integral contributes an amount $\ll \log T$. Thus,

$$|L(s_y, \chi)| \ll \Big| \int_T^Q \frac{1}{t^2} \Big(\sum_{n \le t} \chi(n) \Big) \, dt \Big| + 1 + \log T. \tag{3.1}$$

To bound the character sum in this range, we invoke a powerful estimate of Graham and Ringrose [3]. For technical reasons, we need a slight generalization of their theorem.

Theorem 3.1 (Compare [3, Lemma 5.4]) *Given a primitive character χ (mod Q), with q' and $\mathcal{P}(Q)$ defined as in Lemma 4. Then for any $k \in \mathbb{N}$, writing $K := 2^k$, we have*

$$\Big| \sum_{M < n \le M+N} \chi(n) \Big| \ll N^{1 - \frac{k+3}{8K-2}} \mathcal{P}(Q)^{\frac{k^2+3k+4}{32K-8}} Q^{\frac{1}{8K-2}} (q')^{\frac{k+1}{4K-1}} d(Q)^{\frac{3k^2+11k+8}{16K-4}} (\log Q)^{\frac{k+3}{8K-2}}$$

where $d(Q)$ is the number of divisors of Q, and the implicit constant is absolute.

Our proof of this is a straightforward extension of the arguments given in [3]. For the sake of completeness, we write out all the necessary modifications explicitly in the appendix.

Armed with Theorem 3.1, we deduce Lemma 4 in short order. Set

$$T := \mathcal{P}(Q)^{3k} Q^{\frac{1}{k}} (q')^2 d(Q)^{3k} (\log Q)^{\frac{16K}{k}}.$$

If $T \le Q$, then for all $t \ge T$, Theorem 3.1 implies

$$\Big| \sum_{n \le t} \chi(n) \Big| \ll \frac{t}{\log Q}$$

whence

$$\Big| \int_T^Q \frac{1}{t^2} \Big(\sum_{n \le t} \chi(n) \Big) \, dt \Big| \ll 1.$$

https://doi.org/10.4153/CJM-2010-047-9 Published online by Cambridge University Press

From the bound (3.1), we deduce that for $T \le Q$, $|L(s_y,\chi)| \ll \log T$. But for $T > Q$ such a bound holds trivially (irrespective of our choice of T). Therefore

$$|L(s_y,\chi)| \ll \log T \ll k\log \mathcal{P}(Q) + \frac{1}{k}\log Q + \log q' + k\log d(Q) + \frac{K}{k}\log\log Q.$$

It remains to choose k appropriately. Let

$$k' := \min\left\{\frac{1}{10}\log\log Q, \sqrt{\frac{\log Q}{\log\mathcal{P}(Q) + \log d(Q)}}\right\},$$

and set $k = [k'] + 1$. Writing $K' = 2^{k'}$ we have

$$k'\log\mathcal{P}(Q) + k'\log d(Q) \ll \sqrt{(\log Q)\big(\log\mathcal{P}(Q) + \log d(Q)\big)} \ll \frac{1}{k'}\log Q$$

and

$$\frac{K'}{k'}\log\log Q \ll (\log Q)^{\frac{\log 2}{10}}(\log\log Q) \ll (\log Q)^{\frac{1}{10}} \ll \frac{1}{k'}\log Q.$$

Finally, since $K \ll K'$ and $k \asymp k'$ (*i.e.*, $k \ll k' \ll k$) for all Q sufficiently large, we deduce:

$$|L(s_y,\chi)| \ll \log q' + \frac{1}{k}\log Q \ll \log q' + \frac{\log Q}{\log\log Q} + \sqrt{(\log Q)\big(\log\mathcal{P}(Q) + \log d(Q)\big)}.$$

The proof of Lemma 4 is now complete. ■

4 Proof of Lemma 5

Iwaniec, inspired by Postnikov [13] and Gallagher [2], proved the following.

Theorem 4.1 ([9, Lemma 6]) *Given χ (mod Q) a primitive Dirichlet character. Then for all N, N' satisfying $(\mathrm{rad}\, Q)^{100} < N < 9Q^2$ and $N < N' < 2N$,*

$$\Big|\sum_{N\le n\le N'}\chi(n)\Big| < \gamma_N N^{1-\epsilon_N},$$

where

$$\gamma_x := \exp(C_1 z_x \log^2 C_2 z_x) \qquad \epsilon_x := \frac{1}{C_3 z_x^2 \log C_4 z_x} \qquad z_x := \frac{\log 3Q}{\log x}$$

and the C_i are effective positive constants independent of Q.

In fact, Lemma 6 of [9] is more general (bounding sums of $\chi(n)n^{it}$), and provides explicit choices of the constants C_i.

https://doi.org/10.4153/CJM-2010-047-9 Published online by Cambridge University Press

Proof of Lemma 5
Recall the bound (3.1):

$$|L(s_y, \chi)| \ll \left| \int_T^Q \frac{1}{t^2} \Big(\sum_{n \le t} \chi(n) \Big) \, dt \right| + 1 + \log T.$$

Writing

$$|\sum_{n \le t} \chi(n)| \le \sqrt{t} + |\sum_{\sqrt{t} < n \le t} \chi(n)|,$$

partitioning the latter sum into dyadic intervals, and applying Iwaniec's result to each of these, we deduce that, so long as $\sqrt{t} > (\operatorname{rad} Q)^{100}$,

$$|\sum_{n \le t} \chi(n)| \ll (\log t) \gamma_t t^{1-\epsilon_t}$$

with $C_1 = 400, C_2 = 2400, C_3 = 4 \cdot 1800^2, C_4 = 7200$ in the definitions of γ_t and ϵ_t. Choosing $T = \exp((\log Q)^\alpha)$ for some $\alpha \in (0, 1)$ to be determined later, and assuming that $T > (\operatorname{rad} Q)^{200}$, our bound becomes

$$|L(s_y, \chi)| \ll (\log Q)^\alpha + \int_{\exp((\log Q)^\alpha)}^Q \frac{\log t}{t^2} \gamma_t t^{1-\epsilon_t} \, dt \tag{4.1}$$

Denote by $\int$ the integral in (4.1), and set $\delta_Q = \frac{\log 3}{\log Q}$. Making the substitution $z = \frac{\log 3Q}{\log t}$ and simplifying, one finds

$$\begin{aligned} \int &= (\log^2 3Q) \int_{1+\delta_Q}^{(1+\delta_Q)(\log Q)^{1-\alpha}} \frac{1}{z^3} \exp\Big(C_1 z \log^2 C_2 z - \frac{\log 3Q}{C_3 z^3 \log C_4 z} \Big) \, dz \\ &\ll \exp\Big(2 \log\log 3Q + C_1 (\log Q)^{1-\alpha} (\log\log Q)^2 - \frac{(\log Q)^{3\alpha - 2}}{C_3 \log\log Q} \Big) \\ &\quad \times \int_{1+\delta_Q}^{(1+\delta_Q)(\log Q)^{1-\alpha}} \frac{dz}{z^3} \\ &\ll 1 \end{aligned}$$

upon choosing $\alpha = \frac{3}{4} + \epsilon$. Plugging this back into (4.1), we conclude. ■

It is plausible that with a more refined upper bound on the integral in (4.1) one could take a smaller value of α, thus improving the exponents in both Lemma 5 and Theorem 2.

5 Upper Bounds on Character Sums

Given a primitive character $\chi (\operatorname{mod} q)$, recall from Proposition 2.2 the bound

$$|S_\chi(x)| \ll \sqrt{q} \sqrt{(\log q) |L(s_q, \chi \overline{\xi})|} + \sqrt{q} (\log q)^{6/7},$$

https://doi.org/10.4153/CJM-2010-047-9 Published online by Cambridge University Press

where $\xi \pmod m$ is the primitive character with $m < (\log q)^{1/3}$ that χ is closest to, and $s_q := 1 + \frac{1}{\log q}$.

To prove Theorems 1 and 2, we would like to apply Lemmas 4 and 5 (respectively) to derive a bound on $|L(s_q, \chi\overline{\xi})|$. An immediate difficulty is that both lemmas require the character to be primitive, which is not necessarily true of $\chi\overline{\xi}$. Instead, we will apply the lemmas to the primitive character which induces $\chi\overline{\xi}$; thus, we must understand the size of the conductor of $\chi\overline{\xi}$. This is the goal of the following simple lemma, which is surely well known to the experts but which the author could not find in the literature. We write $[a, b]$ to denote the least common multiple of a and b, and $\mathrm{cond}(\psi)$ to denote the conductor of a character ψ.

Lemma 5.1 *For any non-principal Dirichlet characters $\chi_1 \pmod{q_1}$ and $\chi_2 \pmod{q_2}$,*

$$\mathrm{cond}(\chi_1\chi_2) \mid [\mathrm{cond}(\chi_1), \mathrm{cond}(\chi_2)]$$

Proof First, observe that $\chi_1\chi_2$ is a character modulo $[q_1, q_2]$. One needs only check that it is completely multiplicative, periodic with period $[q_1, q_2]$, and that $\chi_1\chi_2(n) = 0$ if and only if $(n, [q_1, q_2]) > 1$. Since the conductor of a character divides its modulus, the lemma is proved in the case that both χ_1 and χ_2 are primitive.

Now suppose that χ_1 and χ_2 are not necessarily primitive. Denote by $\tilde{\chi}_i \pmod{\tilde{q}_i}$ the primitive character which induces χ_i. By the argument above, we know that

$$\mathrm{cond}(\tilde{\chi}_1\tilde{\chi}_2) \mid [\tilde{q}_1, \tilde{q}_2]. \tag{5.1}$$

Next we note that the character $\tilde{\chi}_1\tilde{\chi}_2$, while not necessarily primitive, does induce $\chi_1\chi_2$ (*i.e.*, $\chi_1\chi_2 = \tilde{\chi}_1\tilde{\chi}_2\chi_0$ for χ_0 the trivial character modulo $[q_1, q_2]$), whence $\mathrm{cond}(\tilde{\chi}_1\tilde{\chi}_2) = \mathrm{cond}(\chi_1\chi_2)$. Plugging this into (5.1) we immediately deduce the lemma. ■

Given $\chi \pmod q$ and $\xi \pmod m$ as at the start of the section, denote by $\psi \pmod Q$ the primitive character inducing $\chi\overline{\xi}$. Taking $\chi_1 = \chi$ and $\chi_2 = \overline{\xi}$ in Lemma 5.1, we see that $Q \mid [q, m]$; in particular, $Q \le qm$. On the other hand, making the choice $\chi_1 = \chi\overline{\xi}$ and $\chi_2 = \xi$ yields $q \mid [Q, m]$, so $q \le Qm$. Combining these two estimates, we conclude that

$$\frac{q}{m} \le Q \le qm. \tag{5.2}$$

Since we will be working with both $L(s, \chi\overline{\xi})$ and $L(s, \psi)$, the following estimate will be useful.

Lemma 5.2 *Given $\chi \pmod q$ and $\xi \pmod m$ primitive characters, let $\psi \pmod Q$ be the primitive character which induces $\chi\overline{\xi}$. Then for all s with $Re(s) > 1$,*

$$\left| \frac{L(s, \chi\overline{\xi})}{L(s, \psi)} \right| \ll 1 + \log\log m.$$

https://doi.org/10.4153/CJM-2010-047-9 Published online by Cambridge University Press

Proof For $\mathrm{Re}(s) > 1$ we have

$$\frac{L(s,\chi\overline{\xi})}{L(s,\psi)} = \prod_{\substack{p\mid[q,m]\\ p\nmid Q}} \Big(1 - \frac{\psi(p)}{p^s}\Big)$$

whence

$$\Big|\frac{L(s,\chi\overline{\xi})}{L(s,\psi)}\Big| \le \prod_{\substack{p\mid[q,m]\\ p\nmid Q}} \Big(1 + \frac{1}{p}\Big).$$

From Lemma 5.1, we know $q \mid [Q,m]$. It follows that if $p \mid [q,m]$ and $p \nmid Q$, then p must divide m. Thus,

$$\prod_{\substack{p\mid[q,m]\\ p\nmid Q}} \Big(1 + \frac{1}{p}\Big) \le \prod_{p\mid m} \Big(1 + \frac{1}{p}\Big).$$

Since

$$\log \prod_{p\mid m} \Big(1 + \frac{1}{p}\Big) = \sum_{p\mid m} \log\Big(1 + \frac{1}{p}\Big) \le \sum_{p\mid m} \frac{1}{p},$$

to prove the lemma it suffices to show that for all m sufficiently large,

$$\sum_{p\mid m} \frac{1}{p} \le \log\log\log m + O(1). \tag{5.3}$$

Let $P = P(m)$ denote the largest prime such that $\prod_{p\le P} p \le m$. Then $\omega(m) \le \pi(P)$ (otherwise we would have $m \ge \mathrm{rad}(m) > \prod_{p\le P} p$, contradicting the maximality of P); therefore,

$$\sum_{p\mid m} \frac{1}{p} \le \sum_{p\le P} \frac{1}{p} = \log\log P + O(1).$$

Finally from the prime number theorem, we know that for all m sufficiently large, $\theta(P) \ge \frac{1}{2}P$, whence $P \le 2\log m$ and the bound (5.3) follows. ■

With these lemmas in hand we can now prove Theorems 1 and 2 without too much difficulty.

Proof of Theorem 1 Given $\chi(\mathrm{mod}\, q)$ primitive with q squarefree, define the character $\xi(\mathrm{mod}\, m)$ as in Theorem A, and let $\psi(\mathrm{mod}\, Q)$ be the primitive character inducing $\chi\overline{\xi}$. Recall that we denote the largest prime factor of n by $\mathcal{P}(n)$.

From Proposition 2.2 we have

$$|S_\chi(x)| \ll \sqrt{q}\sqrt{(\log q)|L(s_q,\chi\overline{\xi})|} + \sqrt{q}(\log q)^{6/7}, \tag{5.4}$$

and Lemma 5.2 yields the bound

$$|L(s_q,\chi\overline{\xi})| \ll |L(s_q,\psi)| \log\log\log q. \tag{5.5}$$

https://doi.org/10.4153/CJM-2010-047-9 Published online by Cambridge University Press

Lemma 5.1 tells us that $Q \mid [q, m]$, whence for all primes $p > m$ we have

$$\operatorname{ord}_p Q \leq \max(\operatorname{ord}_p q, \operatorname{ord}_p m) = \operatorname{ord}_p q \leq 1$$

since q is squarefree. Therefore we may apply Lemma 4 to the character ψ, taking $y = q$ and

$$q' = \prod_{p \leq m} p^{\operatorname{ord}_p Q};$$

this gives the bound

$$|L(s_q, \psi)| \ll \log q' + \frac{\log Q}{\log\log Q} + \sqrt{(\log Q) \log\big(\mathcal{P}(Q) d(Q)\big)}.$$

It remains only to bound the right hand side in terms of q, which we do term by term. The first term is small:

$$\begin{aligned}
\log q' &= \sum_{p \leq m} (\operatorname{ord}_p Q) \log p \\
&\leq \sum_{p \leq m} (\operatorname{ord}_p q) \log p + \sum_{p \leq m} (\operatorname{ord}_p m) \log p \\
&\leq \theta(m) + \log m \\
&\ll (\log q)^{\frac{1}{3}}.
\end{aligned}$$

From (5.2) we deduce

$$\frac{\log Q}{\log\log Q} \ll \frac{\log q}{\log\log q}.$$

For the last term, Lemma 5.1 yields

$$d(Q) \leq d(qm) \leq d(q)d(m) \leq d(q)(\log q)^{\frac{1}{3}}$$

and

$$\mathcal{P}(Q) \leq \max\big(\mathcal{P}(q), \mathcal{P}(m)\big) \leq \mathcal{P}(q)\mathcal{P}(m) \leq \mathcal{P}(q)(\log q)^{\frac{1}{3}},$$

while (5.2) gives $\log Q \ll \log q$. Putting this all together, we find

$$|L(s_q, \psi)| \ll \frac{\log q}{\log\log q} + \sqrt{(\log q) \log\big(\mathcal{P}(q) d(q)\big)}.$$

Plugging this into (5.5) and (5.4), we deduce the theorem. ■

Proof of Theorem 2 Given $\chi (\bmod\, q)$ with q large and $\operatorname{rad}(q) \leq \exp\big((\log q)^{\frac{3}{4}}\big)$, let $\xi (\bmod\, m)$ be defined as in Theorem A, and let $\psi (\bmod\, Q)$ denote the primitive character which induces $\chi\overline{\xi}$. We have $\operatorname{rad}(m) \leq \exp\big(\theta(m)\big)$, whence by the prime number theorem there exists $C > 0$ with

$$\begin{aligned}
\operatorname{rad}(Q) &\leq \operatorname{rad}(q) \operatorname{rad}(m) \\
&\leq \exp\Big((\log q)^{3/4} + C(\log q)^{1/3}\Big) \\
&\leq \exp\Big(\frac{4}{3}(\log q)^{3/4}\Big)
\end{aligned}$$

for all q sufficiently large. From (5.2) we deduce

$$\left(\frac{\log Q}{\log q}\right)^{\frac{3}{4}} \geq \left(\frac{\log \frac{q}{m}}{\log q}\right)^{\frac{3}{4}} \geq \left(1 - \frac{\log\log q}{\log q}\right) \geq \frac{2}{3}$$

for q sufficiently large, whence $\operatorname{rad}(Q) \leq \exp(2(\log Q)^{3/4})$. Combining Lemma 5 with (5.5) and (5.2), we obtain

$$\begin{aligned}|L(s_q, \chi\overline{\xi})| &\ll_\epsilon (\log\log\log q)(\log Q)^{3/4+\epsilon} \\ &\leq (\log\log\log q)(\log qm)^{3/4+\epsilon} \ll_\epsilon (\log q)^{3/4+\epsilon}.\end{aligned}$$

Plugging this into Proposition 2.2 yields Theorem 2. ■

A Appendix: Proof of Theorem 3.1

We follow the original proof of Graham and Ringrose very closely; indeed, we will only explicitly write down those parts of their arguments which must be modified to obtain our version of the result. We refer the reader to [3, Sections 3–5]. Set $S := \sum_{M<n\leq M+N} \chi(n)$.

We begin by restating Lemma 3.1 of [3], but skimming off some of the unnecessary hypotheses given there.

Lemma A.1 (Compare [3, Lemma 3.1]) *Let $k \geq 0$ be an integer, and set $K := 2^k$. Let $q_0, \dots, q_k$ be arbitrary positive integers, and let $H_i := N/q_i$ for all i. Then*

$$|S|^{2K} \leq 8^{2K-1}\Big(\max_{0\leq j\leq k}\big(N^{2K-K/J} q_j^{K/J}\big) + \frac{N^{2K-1}}{H_0 \cdots H_k} \sum_{h_0\leq H_0} \cdots \sum_{h_k \leq H_k} |S_k(\mathbf{h})|\Big), \tag{A.1}$$

where $J = 2^j$ and $S_k(\mathbf{h})$ satisfies the bound given below.

A bound on $S_k(\mathbf{h})$ is given by (3.4) of [3]:

$$|S_k(\mathbf{h})| \ll NQ^{-1}|S(Q;\chi, f_k, g_k, 0)| + \sum_{0<|s|\leq Q/2} \frac{1}{|s|}|S(Q;\chi, f_k, g_k, s)|. \tag{A.2}$$

See [3, pp. 279–280] for the definitions of f_k, g_k, and $S(Q;\chi, f_k, g_k, s)$.

Let $q := Q/q'$. We have $(q, q') = 1$, whence from Lemma 4.1 of [3] we deduce

$$S(Q;\chi, f_k, g_k, s) = S(q';\chi', f_k, g_k, s\overline{q})S(q;\eta, f_k, g_k, s\overline{q'})$$

for some primitive characters χ' (mod q') and η (mod q), where $q\overline{q} \equiv 1$ (mod q') and $q'\overline{q'} \equiv 1$ (mod q). By construction, q is squarefree, so Lemmas 4.1–4.3 of [3] apply to give

$$|S(q;\eta, f_k, g_k, s\overline{q'})| \leq d(q)^{k+1}\left(\frac{q}{(q, Q_k)}\right)^{1/2}(q, Q_k, |s\overline{q'}|)$$

where $Q_k := \prod_{i\leq k} h_i q_i$. Combining this with the trivial estimate

$$|S(q';\chi', f_k, g_k, s\overline{q})| \leq q'$$

yields the following.

https://doi.org/10.4153/CJM-2010-047-9 Published online by Cambridge University Press

Lemma A.2 (Compare [3, Lemma 4.4]) *Keep the notation as above. Then for any positive integers $q_1, \dots, q_k$,*

$$|S(Q;\chi, f_k, g_k, s)| \le q' d(q)^{k+1} \Big(\frac{q}{(q, Q_k)}\Big)^{1/2} (q, Q_k, |s\overline{q'}|).$$

We shall need the following simple lemma (versions of which appear implicitly in [3]).

Lemma A.3 *Given q, $\overline{q'}$ be as above; let x and H be arbitrary. Then*

$$\text{(i)} \quad \sum_{0<|s|\le x} \frac{(q, |s\overline{q'}|)}{|s|} \ll d(q) \log x, \tag{A.3}$$

$$\text{(ii)} \quad \sum_{h \le H} (q, h)^{\frac{1}{2}} \le d(q) H. \tag{A.4}$$

Proof

(i) Since $(q, q') = 1$, we have $(q, \overline{q'}) = 1$, whence

$$\sum_{0<|s|\le x} \frac{(q, |s\overline{q'}|)}{|s|} = 2 \sum_{1\le s\le x} \frac{(q, s\overline{q'})}{s} = 2 \sum_{1\le s\le x} \frac{(q, s)}{s} = 2 \sum_{n\ge 1} \frac{a_n}{n},$$

where $a_n := \#\{s \le x : n = \frac{s}{(q,s)}\}$. Note that $a_n = 0$ for all $n > x$, and that

$$a_n = \#\{s \le x : s = (q, s)n\} \le \#\{s \le x : s = dn, d \mid q\} \le d(q).$$

Therefore

$$\sum_{0<|s|\le x} \frac{(q, |s\overline{q'}|)}{|s|} \ll \sum_{n\ge 1} \frac{a_n}{n} \le d(q) \sum_{n\le x} \frac{1}{n} \ll d(q) \log x.$$

(ii) Write

$$\sum_{h\le H} (q, h)^{\frac{1}{2}} = \sum_{n\ge 1} a_n \sqrt{n},$$

where $a_n := \#\{h \le H : n = (q, h)\}$. It is clear that $a_n = 0$ whenever $n \nmid q$. Also, if $(q, h) = n$ then $n \mid h$, whence

$$a_n \le \#\{h \le H : n \mid h\} \le \frac{H}{n}.$$

Therefore

$$\sum_{h\le H} (q, h)^{\frac{1}{2}} = \sum_{n\ge 1} a_n \sqrt{n} \le \sum_{n\mid q} \frac{H}{\sqrt{n}} \le d(q) H. \qquad \blacksquare$$

Lemma A.4 (Compare [3, Lemma 4.5]) *Keep the notation from above. For any real number $A_0 \geq 1$,*

$$|S|^{4K} \ll 8^{4K-2}\left(AA_0^{2K} + BA_0^{-2K+1}(q')^2 + CA_0^{2K-1}(q')^2\right),$$

where

$$A = N^{2K}$$
$$B = N^{6K-k-4}P^{k+1}Qd(Q)^{2k+4}\log^2 Q$$
$$C = N^{2K+k+2}Q^{-1}d(Q)^{4k+4}$$

and the implied constant is independent of k.

Proof Following the proof of Lemma 4.5 in [3] and applying (A.3) with $x = Q/2$ yields the following analogue of equation (4.5) from that paper:

$$\text{(A.5)} \qquad \sum_{h_k \leq H_k} \sum_{0<|s|\leq Q/2} \frac{1}{|s|}|S(Q;\chi, f_k, g_k, s)| \ll q'\sqrt{q}d(q)^{k+2}H_kR_k^{-\frac{1}{2}}\log Q.$$

Setting $S_j := h_0 \cdots h_j$, one deduces the following analogue of equation (4.6) of [3]:

$$NQ^{-1}\sum_{h_k \leq H_k}|S(Q;\chi, f_k, g_k, 0)| \leq Nq'\frac{\sqrt{qR_k}}{Q}d(Q)^{k+2}H_k\sqrt{(q, S_{k-1})}.$$

From (A.4) and the bound $(q, S_j) \leq (q, S_{j-1})(q, h_j)$, one sees that

$$\text{(A.6)} \qquad \sum_{h_0 \leq H_0} \cdots \sum_{h_{k-1} \leq H_{k-1}} \sqrt{(q, S_{k-1})} \leq d(q)^k H_0 \cdots H_{k-1}.$$

Plugging (A.2) into (A.1) and applying (A.5) and (A.6), one obtains

$$|S|^{2K} \ll 8^{2K-1}\max_{0\leq j\leq k}\left(N^{2K-K/J}q_j^{K/J}\right) + 8^{2K-1}q'N^{2K-1}d(q)^{k+2}(\log Q)\sqrt{\frac{q}{R_k}} + 8^{2K-1}q'N^{2K}d(q)^{2k+2}\frac{\sqrt{q}}{Q}\sqrt{R_k}.$$

Since $q \mid Q$, we have that $q \leq Q$ and $d(q) \leq d(Q)$. Therefore from the above we deduce the following analogue of (4.7) in [3]:

$$|S|^{2K} \ll 8^{2K-1}\max_{0\leq j\leq k}\left(N^{2K-K/J}q_j^{K/J}\right) + 8^{2K-1}q'N^{2K-1}d(Q)^{k+2}(\log Q)\sqrt{\frac{Q}{R_k}} + 8^{2K-1}q'N^{2K}d(Q)^{2k+2}\sqrt{\frac{R_k}{Q}}.$$

The rest of the proof given in [3] can now be copied exactly to yield our claim. ■

https://doi.org/10.4153/CJM-2010-047-9 Published online by Cambridge University Press

Chasing through the arguments in [3] gives this analogue of Lemma 5.3, which we record for reference.

Lemma A.5 (Compare [3, Lemma 5.3])

$$|S| \ll N^{1-\frac{k+3}{8K-2}} P^{\frac{k+1}{8K-2}} Q^{\frac{1}{8K-2}} d(Q)^{\frac{k+2}{4K-1}} (\log Q)^{\frac{1}{4K-1}} (q')^{\frac{1}{4K-1}} + N^{1-\frac{1}{4K}} P^{\frac{k+1}{8K}} d(Q)^{\frac{3k+4}{4K}} (\log Q)^{\frac{1}{4K}} (q')^{\frac{1}{2K}}.$$

Finally, we arrive at the following.

Proof of Theorem 3.1 Let E_k be the right hand side of the bound claimed in the statement of the theorem. The rest of the proof given in [3] now goes through almost verbatim. ■

This concludes the proof of Theorem 3.1. Note that one can extend this to a bound on all non-principal characters by following the argument given directly after Lemma 5.4 in [3]; however, for our applications the narrower result suffices.

Acknowledgments I am indebted to Professor Soundararajan for suggesting the problem, for encouraging me throughout, and for making innumerable improvements to my exposition. I am also grateful to the referee for meticulously reading the manuscript and catching an important error in the original proofs of Theorems 1 and 2, to Denis Trotabas and Bob Hough for some helpful discussions, and to the Stanford Mathematics Department, where the bulk of this project was completed.

References

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

[2] P. X. Gallagher, *Primes in progressions to prime-power modulus.* Invent. Math. **16**(1972), 191–201. doi:10.1007/BF01425492

[3] S. W. Graham and C. J. Ringrose, *Lower bounds for least quadratic nonresidues.* In: Analytic number theory (Allerton Park, IL, 1989), Progr. Math., 85, Birkhäuser, Boston, MA, 1990, pp. 269–309.

[4] A. Granville and K. Soundararajan, *Large character sums: pretentious characters and the Pólya–Vinogradov theorem.* J. Amer. Math. Soc. **20**(2007), no. 2, 357–384. doi:10.1090/S0894-0347-06-00536-4

[5] ———, *Pretentious multiplicative functions and an inequality for the zeta-function.* In: Anatomy of integers, CRM Proc. Lecture Notes, 46, American Mathematical Society, Providence, RI, 2008, pp. 191–197.

[6] G. Halász, *On the distribution of additive and mean values of multiplicative arithmetic functions.* Studia Sci. Math. Hungar. **6**(1971), 211–233.

[7] ———, *On the distribution of additive arithmetic functions.* Acta Arith. **27**(1975), 143–152.

[8] A. Hildebrand, *Large values of character sums.* J. Number Theory **29**(1988), no. 3, 271–296. doi:10.1016/0022-314X(88)90106-0

[9] H. Iwaniec, *On zeros of Dirichlet's L series.* Invent. Math. **23**(1974), 97–104. doi:10.1007/BF01405163

[10] H. L. Montgomery and R. C. Vaughan, *Exponential sums with multiplicative coefficients.* Invent. Math. **43**(1977), no. 1, 69–82. doi:10.1007/BF01390204

[11] M. Ram Murty, *Problems in analytic number theory*, Graduate Texts in Mathematics, 206, Springer-Verlag, New York, 2001.

[12] R. E. A. C. Paley, *A theorem on characters.* J. London Math. Soc. **7**(1932), no. 1, 28–32.
[13] A. G. Postnikov, *On Dirichlet L-series with the character modulus equal to the power of a prime number.* J. Indian Math. Soc. (N.S.) **20**(1956), 217–226.

Department of Mathematics, University of Toronto, Toronto, ON
e-mail: leo.goldmakher@utoronto.ca