BOUNDS ON SHORT CHARACTER SUMS AND L-FUNCTIONS WITH CHARACTERS TO A POWERFUL MODULUS

By

WILLIAM D. BANKS AND IGOR E. SHPARLINSKI

Abstract. We combine a classical idea of Postnikov (1956) with the method of Korobov (1974) for estimating double Weyl sums, deriving new bounds on short character sums when the modulus q has a small core $\prod_{p|q} p$. Using this estimate, we improve certain bounds of Gallagher (1972) and Iwaniec (1974) for the corresponding L-functions. In turn, this allows us to improve the error term in the asymptotic formula for primes in short arithmetic progressions modulo a power of a fixed prime. As yet another application of our bounds, we substantially extend the classical zero-free region (which might include Siegel zeros). Finally, we improve the previous best value $L = \frac{12}{5} = 2.2$ of the Linnik constant for primes in arithmetic progressions modulo powers of a fixed prime to $L < 2.1115$.

1 Introduction

1.1 Background. The core (or kernel) of a positive integer q is the product $\mathfrak{q}_\sharp$ of the distinct prime divisors p of q, that is,

$$\mathfrak{q}_\sharp = \prod_{p|q} p.$$

For a modulus q with a small core $\mathfrak{q}_\sharp$, a nonprincipal character χ modulo q, and integers M and $N \ge 1$, we study the character sum $S_\chi(M, N)$ defined by

$$S_\chi(M, N) = \sum_{n=M+1}^{M+N} \chi(n).$$

In the case of a prime power modulus $q = p^\gamma$, where $\mathfrak{q}_\sharp = p$ is prime and γ is a large integer, it has been known since the work of Postnikov [16, 17] that these sums satisfy bounds that are superior to those which can be established for arbitrary moduli (in full generality, the Burgess bound still gives the strongest known results; see, e.g., Iwaniec and Kowalski [12, Theorem 12.6]). Further advances and modifications have been achieved by Gallagher [5] along with applications to L-functions and to the distribution of primes in progressions modulo p^γ. Iwaniec [11]

JOURNAL D'ANALYSE MATHÉMATIQUE, Vol. 139 (2019)
DOI 10.1007/s11854-019-0060-4

has extended those results to any moduli q that have a small core $\mathfrak{q}_\sharp$. Both Gallagher [5] and Iwaniec [11] also give estimates for Dirichlet L-functions $L(s, \chi)$ (where $s = \sigma + it \in \mathbb{C}$ with $\sigma = \Re s$ and $t = \Im s$) when σ is close to one and χ is a primitive character modulo q; their estimates are uniform in the parameters q and t, where $q = p^\nu$ (in [5]) or q has a small core (in [11]). Further results in this direction have been obtained by Chang [2].

1.2 Outline of results. In this paper we combine the method of Postnikov [16, 17] with a different approach to estimating exponential sums with polynomials which is due to Korobov [14]. This allows us to improve known bounds on character sums and Dirichlet polynomials, which in turn leads to new bounds on Dirichlet L-functions and their zero-free regions. In particular, we improve some of the main results of Gallagher [5] and Iwaniec [11] and substantially extend the classical zero-free region (which might include Siegel zeros). See Sections 2 and 3 below for a precise description of our results and techniques.

Furthermore, as an application of our results on Dirichlet L-functions, in Section 3.3 we give a new asymptotic formula for the number of primes in arithmetic progressions relative to a large prime power modulus.

Finally, we give an improvement of the Linnik exponent L for the least prime in an arithmetic progression in the special case of progressions modulo powers of a fixed prime number. In this situation, our results on the zero-free region can be combined with a result of Harman [8] to improve the previous best value $L = \frac{12}{5} = 2.2$ to a value $L < 2.1115$. Unfortunately, our results do not yield an improvement of L for the entire class of progressions considered in this paper (that is, moduli with a small core; see [2, 11] for the latest results in this direction) since we are unable to exploit the specific form of the bound (3.2) below to strengthen existing zero density estimates.

1.3 Further applications. We remark that our results imply a rich profusion of primes p such that $p - 1$ contains a very large power of a small prime. Such primes appear in some algorithmic applications; see [13, 23]. Furthermore, for the cryptographic construction of [3] one needs the existence of primes p with any given bit size such that $p - 1$ contains very large powers of two distinct small primes; this is also guaranteed by our results.

It is likely that Theorem 3.2 and other results of this work will find other interesting applications in number theory and beyond.

2 Bounds of character sums

2.1 New bounds on short character sums. For a given prime p, let v_p denote the standard p-adic valuation; in other words, if $n \neq 0$ and $v_p(n) = \nu$, then ν is the largest integer for which $p^\nu \mid n$. In this paper, we show that there are absolute, effectively computable constants $\gamma_0, \xi_0 > 0$ with the following property. For any modulus q satisfying

$$\min_{p|q}\{v_p(q)\} \geq 0.7\gamma \quad \text{with } \gamma = \max_{p|q}\{v_p(q)\} \geq \gamma_0, \tag{2.1}$$

the bound

$$S_\chi(M, N) \leq AN^{1-\xi_0/\varrho^2} \quad (M, N \in \mathbb{Z},\ N \geq \mathfrak{q}_\sharp^{\gamma_0}) \tag{2.2}$$

holds, where ϱ is determined via the relation $N^\varrho = q$, and A is an absolute and effective constant.

In earlier versions of this result, all bounds have been of the somewhat weaker form

$$S_\chi(M, N) \leq \exp(a\varrho(1 + \log \varrho)^2)N^{1-\xi_0/(\varrho^2 \log \varrho)} \tag{2.3}$$

with an absolute constant a (see, e.g., [12, Theorem 12.16]). One advantage of (2.2) over (2.3) is the absence of $\log \varrho$ in the denominator of the "savings" term in the exponent of N. A more crucial advantage, however, is that our bound (2.2) has an absolute constant A instead of the superexponential function of ϱ that appears in (2.3); this ultimately accounts for our improvement of the exponent $3/4$ in (2.5) down to $2/3$ in (2.4) below.

We note that the recent work of Chang [2] also extends the class of moduli q to which the method of Postnikov [16, 17] applies but provides weaker bounds than ours.

Milićević [15] also uses the method of Postnikov [16, 17]. However, the main goal of [15] is to estimate L-functions $L(s, \chi)$ in the different extreme case in which $s = 1/2$, as opposed to the case $s = 1$ (or more generally, σ close to one) which is the case considered here. It turns out that for applications to $L(1/2, \chi)$ the strength of the bound of the character sums is more important than its range. Thus, Milićević [15] works in a different regime of long character sums, whereas we are mainly interested in short sums that are decisive for estimating $L(s, \chi)$ when σ is close to one.

To give a brief comparison of the strengths of our bound (2.2), which stems from our approach via double sums, and of (2.3), which is based on standard Weyl

sums, we note that (2.2) is nontrivial for

$$N \ge \exp((\log q)^{2/3+\varepsilon}) \tag{2.4}$$

whereas (2.3) requires that

$$N \ge \exp((\log q)^{3/4+\varepsilon}). \tag{2.5}$$

Our approach to (2.2) relies on an idea of Korobov [14] coupled with the use of Vinogradov's mean value theorem in the explicit form given by Ford [4]. Specifically, we employ a precise bound on the quantity $N_{k,d}(P)$ that is defined to be the number of solutions to the system of equations

$$y_1^r + \cdots y_k^r = z_1^r + \cdots + z_k^r \quad (1 \le r \le d,\ 1 \le y_r, z_r \le P). \tag{2.6}$$

It is worth remarking that subsequent improvements of Vinogradov's mean value theorem due to Wooley [20, 21, 22], and more recently, to Bourgain, Demeter and Guth [1] (the latter providing a bound that is essentially optimal with respect to P), are not suitable for our purposes here as they contain implicit constants that depend on k and d, whereas our methods require that k and d be permitted to grow with P.

Bearing in mind potential applications to L-functions (some of which are given below) we establish the following generalization of the bound (2.2). For a given polynomial $G(x)$ with real coefficients, let

$$S_\chi(M, N; G) = \sum_{n=M+1}^{M+N} \chi(n)\mathrm{e}(G(n)),$$

where $\mathrm{e}(t) = e^{2\pi i t}$ for all $t \in \mathbb{R}$.

For given functions U and V, the notations $U \ll V$, $V \gg U$ and $U = O(V)$ are all equivalent to the statement that the inequality $|U| \le c|V|$ holds with some constant $c > 0$. Throughout the paper, we indicate explicitly the parameters on which the implied constants may depend.

Theorem 2.1. *For any real number $C > 0$ there are effectively computable constants $\gamma_0, \xi_0 > 0$ that depend only on C and have the following property. For any modulus q satisfying* (2.1) *and any primitive character χ modulo q, the bound*

$$S_\chi(M, N; G) \ll N^{1-\xi_0/\varrho^2} \tag{2.7}$$

holds uniformly for all $M, N \in \mathbb{Z}$ and $G \in \mathbb{R}[x]$ subject to the conditions

$$q \ge N \ge \mathfrak{q}_\sharp^{\gamma_0} \quad \text{and} \quad \deg G \le C\varrho, \tag{2.8}$$

where $\varrho = (\log q)/\log N$ and implied constant in (2.7) *is effective and depends only on C.*

As an application of Theorem 2.1, we also study Dirichlet polynomials of the form

$$T_\chi(M, N; t) = \sum_{n=M+1}^{M+N} \chi(n) n^{it} \quad (t \in \mathbb{R}).$$

Approximating $T_\chi(M, N; t)$ by sums $S_\chi(M, N; G)$ with appropriately chosen polynomials G, we derive the following bound.

Theorem 2.2. *For any real number $C > 0$ there are effectively computable constants $\gamma_0, \xi_0 > 0$ that depend only on C and have the following property. For any modulus q satisfying* (2.1) *and any primitive character χ modulo q, the bound*

$$T_\chi(M, N; t) \ll M^{1-\xi_0/\varrho^2} \tag{2.9}$$

holds uniformly for all $M, N \in \mathbb{Z}$ and $t \in \mathbb{R}$ subject to the conditions

$$M \geq N, \quad q \geq N \geq \mathfrak{q}_\sharp^{\gamma_0} \quad \text{and} \quad |t| \leq q^C, \tag{2.10}$$

where $\varrho = (\log q)/\log N$ and implied constant in (2.9) *is effective and depends only on C.*

Theorem 2.2 improves [5, Lemma 5] in the special case that $|t|$ is bounded by a fixed power of the modulus of the character χ. For larger values of $|t|$, our approach incorporating ideas of Korobov (Lemma 4.2) breaks down, and in this case the method of Gallagher (which relies only on general estimates of Vinogradov [18, 19]) yields the best known result.

3 Applications

3.1 Bounds on L-functions. As in [5, 11], we can apply our bound on the sums $T_\chi(M, N; t)$ to estimate the size of L-functions inside the critical strip.

Theorem 3.1. *Fix $C > 0$ and $\eta \in (0, \frac{1}{3})$. There is an effectively computable constant $\gamma_0 > 0$ that depends only on C and has the following property. Let q be a modulus satisfying* (2.1) *and χ a primitive character modulo q. If the inequalities $\sigma > 1 - \eta$ and $|t| \leq q^C$ hold, then for $s = \sigma + it$ with $\sigma = \Re s$ and $t = \Im s$, we have*

$$|L(s, \chi)| \leq \eta^{-1} \exp(O(\max\{\eta \log \mathfrak{q}_\sharp, \eta^{3/2}\ell, \eta\ell^{2/3}(\log \ell)^{1/3}\})),$$

where $\ell = \log q(|t| + 3)$ and the implied constant depends only on C.

To illustrate the strength of the bound, we note that with the specific choice

$$\eta = \frac{1}{\ell^{1/2}(\log \ell)^{3/4}}$$

considered by Iwaniec [11], our Theorem 3.1 yields the bound

$$|L(s,\chi)| \le \mathfrak{q}_\sharp^{o(1)} \exp(O(\ell^{1/4}(\log \ell)^{-9/8}))$$

for $\sigma > 1 - \eta$ provided that $|t|$ is polynomially bounded in terms of q, where $o(1)$ is a function that tends to zero as $q \to \infty$. In particular, this improves the bound of [11, Theorem 1], i.e.,

$$|L(s,\chi)| \le \mathfrak{q}_\sharp^{o(1)} \exp(100\ell^{1/4}),$$

under the same condition on t (we point out, however, that the Iwaniec bound also holds for all larger values of t). It is important to note that for all known applications to the distribution of primes, only values of $s = \sigma + it$ with t bounded by a small power of q (typically, $|t| \le q$) play an important rôle; see Section 3.3 where we give one application of this type.

Taking η somewhat smaller, namely

$$\eta = \frac{(\log \ell)^{2/3}}{\ell^{2/3}}$$

(in other words, taking values of s that lie closer to the edge of the critical strip), Theorem 3.1 yields the bound

$$|L(s,\chi)| \le \mathfrak{q}_\sharp^{o(1)} (\log q)^{O(1)}$$

for $\sigma > 1 - \eta$ provided that $|t|$ is polynomially bounded in terms of q.

Choosing η even smaller, namely

$$\eta = \frac{1}{\ell^{2/3}(\log \ell)^{1/3}},$$

we obtain the following attractive bound:

$$|L(s,\chi)| \le \mathfrak{q}_\sharp^{o(1)} (\log q)^{2/3} (\log\log q)^{1/3} \tag{3.1}$$

for $\sigma > 1 - \eta$ provided that $|t|$ is polynomially bounded in terms of q. In particular, the bound (3.1) applies to $L(1, \chi)$ and is therefore of special interest as it is presently unknown whether the estimate

$$L(1,\chi) = o(\log q)$$

holds for general moduli q (although the bound $L(1,\chi) \ll \log\log q$ is implied by the GRH); for the strongest unconditional upper bounds on $|L(1,\chi)|$, see Granville and Soundararajan [6].

We conclude this subsection with the remark that, in our setting, one can define ℓ more simply as $\ell = \log q$. In Theorem 3.1 and in the above examples, we have used the definition $\ell = \log q(|t|+3)$ solely for the purpose of comparing our results to those of [11, Theorem 1].

3.2 The zero-free region. We apply our new bounds on L-functions to extend the zero-free region on low-lying zeros. Note that we formulate the results of this section only for primitive characters χ modulo q satisfying (2.1); for other characters, our results can be formulated in terms of the conductor of χ.

Theorem 3.2. *For every $C > 0$, there is an effectively computable constant $\gamma_0 > 0$ that depends only on C and has the following property. Let q be a modulus satisfying* (2.1). *There is a constant $A > 0$, which depends only on C and $\mathfrak{q}_\sharp$, such that if*

$$\vartheta = \frac{A}{(\log q)^{2/3}(\log\log q)^{1/3}}, \tag{3.2}$$

then there exists at most one primitive character χ modulo q such that $L(s,\chi)$ has a zero in the region $\{s \in \mathbb{C} : \sigma > 1-\vartheta,\ |t| \le q^C\}$, where $\sigma = \Re s$ and $t = \Im s$. If such a character exists, then it is a real character, and the zero is unique, real and simple.

It is worth mentioning that, under the same conditions as in Theorem 3.2, the previous result of Iwaniec [11, Theorem 2] yields a similar bound with $(\log q(|t|+3))^{3/4}(\log\log q(|t|+3))^{3/4}$ in the denominator of ϑ instead of our $(\log q)^{2/3}(\log\log q)^{1/3}$, but with no restriction on $|t|$. Of course, for applications to exceptional characters the restriction on $|t|$ is irrelevant as any Siegel zero must lie on the real axis, and thus Theorem 3.2 reveals a substantially larger portion of the real interval $[0,1]$ that is zero-free with at most one exception.

Corollary 3.3. *Let q be a modulus satisfying* (2.1). *There is a constant $A > 0$, which depends only on $\mathfrak{q}_\sharp$, with the following property. Let ϑ be given by* (3.2). *Then there exists at most one primitive real character χ modulo q such that $L(\sigma,\chi)$ has a zero in the region $1 \ge \sigma > 1-\vartheta$, and any such zero must be simple.*

We remark that, in the most interesting case in which $q = p^\gamma$ is a power of a fixed prime p, the condition (2.1) is satisfied automatically once $\gamma \ge \gamma_0$, and thus Theorem 3.2 yields the following statement for all characters modulo a prime power $q = p^\gamma$.

Corollary 3.4. *Let $q = p^\gamma$ with a prime p and $\gamma \in \mathbb{N}$. There is a constant $A_0 > 0$, which depends only on p, such that for any character χ modulo q, the function $L(s,\chi)$ does not vanish in the region*

$$\mathcal{R}_0 = \{s \in \mathbb{C} : \sigma > 1-\vartheta_0,\ |t| \le T_0\},$$

where

$$\vartheta_0 = \frac{A_0}{(\log q)^{2/3}(\log\log q)^{3/4}} \quad \text{and} \quad T_0 = \exp((\log q)^{8/9}).$$

3.3 Primes in arithmetic progressions and the Linnik constant. As usual we use Λ to denote the von Mangoldt function, which is given by

$$\Lambda(n) = \begin{cases} \log r & \text{if } n \text{ is a power of the prime } r, \\ 0 & \text{if } n \text{ is not a prime power,} \end{cases}$$

and we set

$$\psi(x; q, a) = \sum_{\substack{n \le x \\ n \equiv a \bmod q}} \Lambda(n).$$

The asymptotic formula in Theorem 3.5 below has a smaller error term than that which appears in any other asymptotic formula of this type. As in [5, 11] our result depends on density estimates for the zeros of Dirichlet L-functions. More specifically, let $N_q(\alpha, T)$ be the total number of zeros $s = \sigma + it$ for all L-functions modulo q that occur in the rectangle $\alpha < \sigma < 1$, $|t| \le T$. In order to state a general result suitable for further advances, we assume that for some constant $b > 1$ the uniform bound

$$N_q(\alpha, T) \ll (qT)^{b(1-\alpha)} \ell^{O(1)} \tag{3.3}$$

holds, where $\ell = \log q(|t| + 3)$ as before. By a result of Huxley [10] we can take $b = \frac{12}{5}$ in (3.3); see also [12, Equation (18.13)].

Theorem 3.5. *Suppose that* (3.3) *holds with the constant $b > 1$. Fix a prime p and a real number $\varepsilon > 0$. There is a constant $c_0 > 0$, which depends only on b, ε and p, such that the following holds. For any modulus $q = p^\gamma$ with $\gamma \in \mathbb{N}$, any integer a coprime to p, and any positive real number x in the range*

$$qx^{1-1/b+\varepsilon} \le x \le q^{1/\varepsilon},$$

we have

$$\psi(x; q, a) = \frac{x}{\varphi(q)}(1 + O_\varepsilon(\exp(-c_0(\log x)^{1/3}(\log\log x)^{-3/4}))),$$

where φ is the Euler totient function.

In particular, using the value $b = \frac{12}{5}$ we see that Theorem 3.5 can be applied throughout the range $q^A \ge x \ge q^{12/5+\varepsilon}$ for any fixed positive A and ε.

Our proof of Theorem 3.5 closely follows that of Gallagher [5, Theorem 2], however we apply Corollary 3.4 at an appropriate place. We remark that the results of Gallagher [5] and Iwaniec [11] imply a weaker form of Theorem 3.5 with the error term $O(x\exp(-c_0(\log x)^{1/4}(\log\log x)^{3/4}))$; on the other hand, the results of [5, 11] also apply to short intervals, that is, to $\psi(x + h; q, a) - \psi(x; q, a)$.

Furthermore, combining our bound on the zero-free region with the result of Harman [8] we obtain a new bound on the Linnik constant for prime power moduli $q = p^\gamma$ with a fixed prime p, improving the previously known bound $\frac{12}{5}$. In fact the following value

$$L = \frac{1}{0.4736} < 2.1115 \tag{3.4}$$

seems to be the lowest value known for any infinite family of moduli.

Theorem 3.6. *For any modulus $q = p^\gamma$ with an integer $\gamma > \gamma_0(p)$, where $\gamma_0(p)$ depends only on p, any integer a coprime to p, and any positive real number*

$$x > q^L$$

with L given by (3.4)*, we have*

$$\psi(x; q, a) \gg \frac{x}{\varphi(q)},$$

where φ is the Euler totient function.

4 Preliminaries

4.1 Notation. For a real number $t > 0$, $\lfloor t \rfloor$ denotes the greatest integer not exceeding t, and $\lceil t \rceil$ denotes the least integer that is not less than t.

Throughout the paper, we use the symbols O, $\ll$, $\gg$ and $\asymp$ along with their standard meanings; any constants or functions implied by these symbols are absolute unless specified otherwise.

4.2 Polynomial representation of characters. Following Gallagher [5], for an integer $d \geq 1$ we use F_d to denote the polynomial approximation to $\log(1+x)$ given by

$$F_d(x) = \sum_{r=1}^{d} (-1)^{r-1} \frac{x^r}{r}. \tag{4.1}$$

The earliest version of the following result is due to Postnikov [16, 17]. The present form is due to Iwaniec [11, Lemma 2]; it extends an earlier result of Gallagher [5, Lemma 2].

Lemma 4.1. *Let χ be a primitive character modulo q. Let d be an integer such that $q^2 \mid \mathfrak{q}_\sharp^d$, and put*

$$\tau = \begin{cases} 2, & \text{if } 4 \mid q, \\ 1, & \text{otherwise.} \end{cases}$$

Then $\chi(1 + \tau \mathfrak{q}_\sharp x) = \mathrm{e}(f(x))$*, where* f *is a polynomial of the form*

$$f(x) = q^{-1} m \cdot F_d(\tau \mathfrak{q}_\sharp x)$$

with an integer m *for which* $\gcd(m, q) = 1$*, and* $r \mid m$ *for every integer* $r \in [1, d]$ *coprime to* q*.*

4.3 Bounds of exponential sums. Suppose $d \geq 2$, and

$$g(x) = \alpha_1 x + \cdots + \alpha_d x^d$$

with each $\alpha_r \in \mathbb{R}$. Suppose further that each α_r has a rational approximation of the form

$$\alpha_r = \frac{a_r}{b_r} + \frac{\vartheta_r}{b_r^2}, \quad a_r \in \mathbb{Z}, \quad b_r \in \mathbb{N}, \quad \gcd(a_r, b_r) = 1, \quad |\vartheta_r| \leq 1.$$

Let S denote the double exponential sum

$$S = \sum_{y,z=1}^{P} \mathrm{e}(g(yz)). \tag{4.2}$$

The next result is due to Korobov [14, Lemma 3]; it provides a bound on S in terms of $N_{k,d}(P)$ (the number of solutions to (2.6)) and a product involving the denominators of the coefficients of g.

Lemma 4.2. *For any natural number* k*, the sum* (4.2) *admits the upper bound*

$$|S|^{2k^2} \leq (64k^2 \log(3Q))^{d/2} W P^{2k(2k-1)} N_{k,d}(P),$$

where

$$Q = \max\{b_r : 1 \leq r \leq d\} \quad \textit{and} \quad W = \prod_{r=1}^{d} \min\{P^r, P^r b_r^{-1/2} + b_r^{1/2}\}.$$

We also use the following weakened and simplified version of a result of Ford [4, Theorem 3].

Lemma 4.3. *For every integer* $d \geq 129$ *there is an integer* $k \in [2d^2, 4d^2]$ *such that*

$$N_{k,d}(P) \leq d^{3d^3} P^{2k - 0.499d^2} \quad (P \geq 1).$$

5 Proof of bounds of character sums

5.1 Simple character sums: Proof of Theorem 2.1. Let γ_0 and ε be positive constants such that

$$\gamma_0 \geq e^{200}, \quad \varepsilon \leq 1/200 \quad \text{and} \quad \varepsilon\gamma_0 \geq 2. \tag{5.1}$$

Put $d_0 = 2\gamma$. Since $\gamma = \max_{p|q}\{v_p(q)\}$, the condition $q^2 \mid \mathfrak{q}_\sharp^{d_0}$ of Lemma 4.1 is clearly met. Also, the parameter ϱ lies in $[1, \gamma/\gamma_0]$ since

$$\log q = \sum_{p|q} v_p(q)\log p \leq \gamma \sum_{p|q} \log p = \gamma \log \mathfrak{q}_\sharp,$$

whereas by (2.8) we have

$$\log N \geq \gamma_0 \log \mathfrak{q}_\sharp.$$

Put $s = \lfloor \varepsilon\gamma/\varrho \rfloor$. Since $\varepsilon\gamma/\varrho \geq \varepsilon\gamma_0 \geq 2$, it follows that

$$\frac{1}{2}\varepsilon\gamma/\varrho \leq \varepsilon\gamma/\varrho - 1 < s \leq \varepsilon\gamma/\varrho, \tag{5.2}$$

and thus $s \asymp \gamma/\varrho$. Using (5.1) and (5.2) we deduce that

$$\log\gamma \geq 200 \quad \text{and} \quad 2 \leq s \leq \gamma/200. \tag{5.3}$$

Finally, we record the simple inequality

$$t \leq e^{t/1250} \quad (t \geq \gamma_0). \tag{5.4}$$

Let $\mathcal{N}$ be the set of integers coprime to q in the interval $[M+1, M+N]$. Shifting the interval $[M+1, M+N]$ by the amount $\mathfrak{q}_\sharp^s yz$, where $1 \leq y, z \leq \mathfrak{q}_\sharp^s$, we have the uniform estimate

$$S_\chi(M, N; G) = \sum_{n=M+1}^{M+N} \chi(n)\mathrm{e}(G(n)) = \sum_{n=M+1}^{M+N} \chi(n + \mathfrak{q}_\sharp^s yz)\mathrm{e}(G(n + \mathfrak{q}_\sharp^s yz)) + O(\mathfrak{q}_\sharp^{3s}).$$

Averaging over all such y and z, it follows that

$$S_\chi(M, N; G) = \mathfrak{q}_\sharp^{-2s} V + O(\mathfrak{q}_\sharp^{3s}), \tag{5.5}$$

where

$$V = \sum_{y,z=1}^{\mathfrak{q}_\sharp^s} \sum_{n\in\mathcal{N}} \chi(n + \mathfrak{q}_\sharp^s yz)\mathrm{e}(H_n(yz))$$

and H_n is the polynomial given by

$$H_n(x) = G(n + \mathfrak{q}_\sharp^s x).$$

For every $n \in \mathcal{N}$, let $\overline{n}$ be an integer such that $n\overline{n} \equiv 1 \bmod q$. Using the multiplicativity of χ, we have

$$V = \sum_{n \in \mathcal{N}} \chi(n) \sum_{y,z=1}^{\mathfrak{q}_\sharp^s} \chi(1 + \mathfrak{q}_\sharp^s \overline{n} yz) \mathrm{e}(H_n(yz)).$$

Applying Lemma 4.1 (noting that $s \ge 2$ and thus $\tau \mathfrak{q}_\sharp \mid \mathfrak{q}_\sharp^s$) we see that

$$V = \sum_{n \in \mathcal{N}} \chi(n) \sum_{y,z=1}^{\mathfrak{q}_\sharp^s} \mathrm{e}(f_n(yz) + H_n(yz)), \tag{5.6}$$

where f_n is a polynomial of the form

$$f_n(x) = q^{-1} m \cdot F_{d_0}(\mathfrak{q}_\sharp^s \overline{n} x)$$

with some integer m such that $\gcd(m, q) = 1$ and $r \mid m$ for any integer $r \in [1, d_0]$ coprime to q. To apply Lemma 4.2, we need to control the denominators of the coefficients of $f_n + H_n$ for each $n \in \mathcal{N}$.

Using (4.1) we see that the r-th coefficient of f_n is the rational number

$$\alpha_r = (-1)^{r-1} \mathfrak{q}_\sharp^{rs} q^{-1} m \overline{n}^r r^{-1}.$$

Write

$$\alpha_r = \frac{a_r}{b_r}, \quad a_r \in \mathbb{Z}, \quad b_r \in \mathbb{N}, \quad \gcd(a_r, b_r) = 1 \quad (1 \le r \le d_0).$$

Since $r \mid m$ for every integer $r \in [1, d_0]$ coprime to q, and $\gcd(m\overline{n}, q) = 1$, it follows that b_r is the numerator of the rational number

$$q \mathfrak{q}_\sharp^{-rs} \prod_{p \mid \gcd(r,q)} p^{v_p(r)}$$

when the latter is expressed in reduced form (in particular, b_r is composed solely of primes that divide q). Consequently,

$$v_p(b_r) = \max\{0, v_p(q) - rs + v_p(r)\}$$

for every prime p dividing q.

Let us denote

$$\mathscr{L} = \left\lfloor \frac{3}{2} \log d_0 \right\rfloor = \left\lfloor \frac{3}{2} \log 2\gamma \right\rfloor.$$

As the inequality $v_p(r) \le \mathscr{L}$ holds for every positive integer $r \le d_0$, we have

$$\max\{0, v_p(q) - rs\} \le v_p(b_r) \le \max\{0, v_p(q) - rs + \mathscr{L}\} \tag{5.7}$$

for any prime $p \mid q$.

Now put

$$d = \max_{p|q} \left\lfloor \frac{v_p(q) + \mathscr{L}}{s} \right\rfloor = \left\lfloor \frac{\gamma + \mathscr{L}}{s} \right\rfloor. \tag{5.8}$$

Note that $d \geq 200$ since $\gamma/s \geq 200$ by (5.3); in particular, we are able to apply Lemma 4.3 above with this choice of d.

For any integer $r \geq d$, it follows from (5.7) that $b_r = 1$; in other words, $\alpha_r \in \mathbb{Z}$. Therefore, defining

$$g_n(x) = q^{-1}m \cdot F_d(\mathfrak{q}_\sharp^s \overline{n} x) \quad (n \in \mathcal{N}),$$

the polynomial $f_n - g_n$ lies in $\mathbb{Z}[x]$ for every $n \in \mathcal{N}$; therefore, in view of (5.6) we have

$$V = \sum_{n \in \mathcal{N}} \chi(n) \sum_{y,z=1}^{\mathfrak{q}_\sharp^s} \mathrm{e}(h_n(yz)), \tag{5.9}$$

where

$$h_n(x) = g_n(x) + H_n(x).$$

Suppose that ε is initially chosen to be small enough, depending on C, so that $C \leq (3\varepsilon)^{-1}$. In view of (5.2), the second inequality in (2.8) implies

$$\deg G \leq \gamma/(3s). \tag{5.10}$$

We now use approximations with denominators $\mathfrak{b}_r = 1$ for the initial $\lfloor \gamma/(3s) \rfloor$ coefficients of h_n (i.e., for $1 \leq r \leq \gamma/(3s)$) and with the denominators $\mathfrak{b}_r = b_r$ considered above for remaining coefficients of h_n (i.e., for $r > \gamma/(3s)$), which by (5.10) are the same as the coefficients of $g_n(x)$.

Put

$$Q = \max\{\mathfrak{b}_r : 1 \leq r \leq d\} \quad \text{and} \quad W = \prod_{r=1}^{d} \min\{\mathfrak{q}_\sharp^{rs}, \mathfrak{q}_\sharp^{rs}\mathfrak{b}_r^{-1/2} + \mathfrak{b}_r^{1/2}\}.$$

Applying Lemma 4.2 with $P = \mathfrak{q}_\sharp^s$ we derive the bound

$$\left| \sum_{y,z=1}^{\mathfrak{q}_\sharp^s} \mathrm{e}(h_n(yz)) \right|^{2k^2} \leq (64k^2 \log(3Q))^{d/2} W \mathfrak{q}_\sharp^{2sk(2k-1)} N_{k,d}(\mathfrak{q}_\sharp^s) \tag{5.11}$$

with any natural number k. Using (5.7) we have that

$$q\mathfrak{q}_\sharp^{-rs} \leq b_r \leq q\mathfrak{q}_\sharp^{-rs+\mathscr{L}} \quad (1 \leq r \leq d). \tag{5.12}$$

In particular, $Q \le q\mathfrak{q}_\sharp^{\mathscr{L}}$, which implies (since $q \le \mathfrak{q}_\sharp^{\gamma}$)

$$\log(3Q) \le 2\gamma \log \mathfrak{q}_\sharp. \tag{5.13}$$

Next, note that the hypothesis (2.1) immediately yields the bound

$$\log q = \sum_{p \mid q} v_p(q) \log p \ge 0.7\gamma \sum_{p \mid q} \log p = 0.7\gamma \log \mathfrak{q}_\sharp,$$

hence $q = \mathfrak{q}_\sharp^{\mu\gamma}$ with some $\mu \in [0.7, 1]$. To estimate W, we use (5.12) to derive the bound

$$\min\{\mathfrak{q}_\sharp^{rs}, \mathfrak{q}_\sharp^{rs}\mathfrak{b}_r^{-1/2} + \mathfrak{b}_r^{1/2}\} \le \begin{cases} \mathfrak{q}_\sharp^{rs} & \text{if } r \le \gamma/(3s); \\ 2\mathfrak{q}_\sharp^{(\mu\gamma - rs + \mathscr{L})/2} & \text{if } \gamma/(3s) < r \le \mu\gamma/(2s); \\ 2\mathfrak{q}_\sharp^{(3rs - \mu\gamma)/2} & \text{if } \mu\gamma/(2s) < r \le \gamma/s; \\ \mathfrak{q}_\sharp^{rs} & \text{if } \gamma/s < r \le d. \end{cases}$$

To simplify the notation, let $\lambda = \gamma/s$ for the moment. Using the preceding bound, we have

$$W \le \prod_{r \le \lambda/3} \mathfrak{q}_\sharp^{rs} \prod_{\lambda/3 < r \le \mu\lambda/2} (2\mathfrak{q}_\sharp^{(\mu\gamma - rs + \mathscr{L})/2}) \prod_{\mu\lambda/2 < r \le \lambda} (2\mathfrak{q}_\sharp^{(3rs - \mu\gamma)/2}) \prod_{\lambda < r \le d} \mathfrak{q}_\sharp^{rs} \le 2^d \mathfrak{q}_\sharp^{\Delta},$$

where

$$\Delta = \sum_{r \le \lambda/3} rs + \sum_{\lambda/3 < r \le \mu\lambda/2} \frac{\mu\gamma - rs + \mathscr{L}}{2} + \sum_{\mu\lambda/2 < r \le \lambda} \frac{3rs - \mu\gamma}{2} + \sum_{\lambda < r \le d} rs.$$

We write

$$\begin{aligned} \Delta &= s\Sigma + \frac{\mu\gamma}{2}\Big(\frac{\mu\lambda}{2} - \frac{\lambda}{3} + O(1)\Big) - \frac{\mu\gamma}{2}\Big(\lambda - \frac{\mu\lambda}{2} + O(1)\Big) + O(\mathscr{L}\lambda) \\ &= s\Sigma + \mu\gamma\Big(\frac{\mu\lambda}{2} - \frac{2\lambda}{3}\Big) + O(\gamma + \mathscr{L}\lambda) \end{aligned} \tag{5.14}$$

(recall our convention that all implied constants are absolute), with

$$\begin{aligned} \Sigma &= \sum_{r \le \lambda/3} r - \frac{1}{2} \sum_{\lambda/3 < r \le \mu\lambda/2} r + \frac{3}{2} \sum_{\mu\lambda/2 < r \le \lambda} r + \sum_{\lambda < r \le d} r \\ &\le \frac{1}{2}\Big(\frac{\lambda}{3}\Big)^2 - \frac{1}{4}\Big(\Big(\frac{\mu\lambda}{2}\Big)^2 - \Big(\frac{\lambda}{3}\Big)^2\Big) + \frac{3}{4}\Big(\lambda^2 - \Big(\frac{\mu\lambda}{2}\Big)^2\Big) + \frac{1}{2}(d^2 - \lambda^2) + O(d). \end{aligned}$$

Since $d = \lambda + O(1)$ and thus $d^2 - \lambda^2 = O(\lambda)$, we derive that

$$\Sigma = \Big(\frac{5}{6} - \frac{\mu^2}{4}\Big)\lambda^2 + O(\lambda).$$

Inserting this result into (5.14), recalling that $\lambda = \gamma/s$ and $\mu \in [0.7, 1]$, and using (5.8), it follows that

$$\Delta = \Big(\frac{5}{6} + \frac{\mu^2}{4} - \frac{2\mu}{3}\Big)\frac{\gamma^2}{s} + O\Big(\gamma + \frac{\gamma\mathscr{L}}{s}\Big) \le 0.49sd^2 + O(sd\log d).$$

Therefore, if ε is small enough initially (depending on the absolute implied constant in the preceding bound), then we have

$$\Delta \le 0.495sd^2,$$

and thus

$$W \le 2^d \mathfrak{q}_\sharp^{0.495sd^2}. \tag{5.15}$$

Now, combining the bounds (5.11), (5.13) and (5.15), and using Lemma 4.3 to bound $N_{k,d}(\mathfrak{q}_\sharp^s)$, we deduce that

$$\Big|\sum_{y,z=1}^{\mathfrak{q}_\sharp^s} \mathrm{e}(h_n(yz))\Big|^{2k^2} \le A\mathfrak{q}_\sharp^B$$

holds with

$$A = (128k^2\gamma\log\mathfrak{q}_\sharp)^{d/2}2^d d^{3d^3}$$

and

$$B = 4sk^2 - 0.004sd^2$$

for some integer $k \in [2d^2, 4d^2]$.

Since $k \in [2d^2, 4d^2]$ we clearly have $A \le d^{cd^3}(\gamma\log\mathfrak{q}_\sharp)^{d/2}$ with some absolute (effective) constant $c > 0$. As $\gamma\log\mathfrak{q}_\sharp \ge \gamma_0$, using (5.4) and taking into account the definition (5.8), which implies that $\gamma \le 2sd$, it follows that

$$(\gamma\log\mathfrak{q}_\sharp)^{d/2} \le \mathfrak{q}_\sharp^{0.0004\gamma d} \le \mathfrak{q}_\sharp^{0.0008sd^2}.$$

Putting everything together, we find that

$$\Big|\sum_{y,z=1}^{\mathfrak{q}_\sharp^s} \mathrm{e}(h_n(yz))\Big|^{2k^2} \le d^{cd^3}\mathfrak{q}_\sharp^{4sk^2-0.0032sd^2}.$$

Raise both sides to the power $1/(2k^2)$. Since $k \in [2d^2, 4d^2]$ we have

$$d^{cd^3/(2k^2)} \le d^{c/(8d)} \ll 1 \quad \text{and} \quad sd^2/(2k^2) \ge s/(32d^2);$$

consequently,

$$\sum_{y,z=1}^{\mathfrak{q}_\sharp^s} \mathrm{e}(h_n(yz)) \ll \mathfrak{q}_\sharp^{2s-0.0001s/d^2}.$$

Finally, using (5.2) and (5.3) we see that

$$\frac{s}{d^2} \asymp \frac{s}{(\gamma/s)^2} = \frac{s^3}{\gamma^2} \asymp \frac{(\gamma/\varrho)^3}{\gamma^2} = \frac{\gamma}{\varrho^3} \asymp \frac{\mu\gamma}{\varrho^3},$$

and therefore

$$\sum_{y,z=1}^{\mathfrak{q}_\sharp^s} \mathrm{e}(g_n(yz)) \ll \mathfrak{q}_\sharp^{2s-\xi_0\mu\gamma/\varrho^3} = \mathfrak{q}_\sharp^{2s} N^{-\xi_0/\varrho^2}$$

with some absolute constant $\xi_0 > 0$.

Inserting the previous bound into (5.9) we derive that

$$V \ll \mathfrak{q}_\sharp^{2s} N^{1-\xi_0/\varrho^2}$$

and combining this result with (5.5) we obtain that

$$S_\chi(M, N; G) \ll N^{1-\xi_0/\varrho^2} + \mathfrak{q}_\sharp^{3s}. \tag{5.16}$$

The second term on the right side of (5.16) is negligible (indeed, using (5.2) we have $\mathfrak{q}_\sharp^s \le N^{\varepsilon/\mu}$, hence $\mathfrak{q}_\sharp^{3s} \le N^{5\varepsilon}$, which is insignificant compared to $N^{1-\xi_0/\varrho^2}$ if one makes suitable initial choices of the absolute constants γ_0, ξ_0 and ε). This completes the proof.

5.2 Dirichlet polynomials: Proof of Theorem 2.2. We continue to use the notation of §5.1. We denote $\nu = \lceil \gamma/(3s) \rceil$. For any real number x, we have the estimate

$$(1+x)^{it} = \mathrm{e}(tG(x))(1 + O(|t||x|^\nu)),$$

where $G(x) = (2\pi)^{-1} F_{\nu-1}(x)$ in the notation of (4.1) (note that $G(x)$ is a polynomial of degree $\nu - 1$ with real coefficients). Hence, for all $n \in [M+1, M+N]$ and $y, z \in [1, \mathfrak{q}_\sharp^s]$ we have

$$(n + \mathfrak{q}_\sharp^s yz)^{it} = n^{it}(1 + \mathfrak{q}_\sharp^s yz/n)^{it} = n^{it}\mathrm{e}(tG(\mathfrak{q}_\sharp^s yz/n)) + O(M^{-\nu}|t|\mathfrak{q}_\sharp^{3s\nu}).$$

Using this estimate and following the proof of Theorem 2.1, in place of (5.5) we derive that

$$T_\chi(M, N; t) = \mathfrak{q}_\sharp^{-2s}\widetilde{V} + O(\mathfrak{q}_\sharp^{3s} + M^{1-\nu}|t|\mathfrak{q}_\sharp^{3s\nu}),$$

where

$$\widetilde{V} = \sum_{n \in \mathcal{N}} \chi(n) n^{it} \sum_{y,z=1}^{\mathfrak{q}_\sharp^s} \chi(1 + \mathfrak{q}_\sharp^s \overline{n} yz)\mathrm{e}(tG(\mathfrak{q}_\sharp^s yz/n)).$$

Since $\deg G < \gamma/(3s)$, at this point the proof parallels that of Theorem 2.1, leading to the bound

$$T_\chi(M,N;t) \ll M^{1-\xi_0/\varrho^2} + \mathfrak{q}_\sharp^{3s} + M^{1-\nu}|t|\mathfrak{q}_\sharp^{3s\nu} \tag{5.17}$$

in place of (5.16). As before, the term $\mathfrak{q}_\sharp^{3s}$ in (5.17) does not exceed $N^{5\varepsilon}$ and can thus be disregarded if one makes suitable initial choices of γ_0, ξ_0 and ε.

To finish the proof, it remains to bound the last term in (5.17). Let τ be such that $N^\tau = |t|+3$. Since $\nu = \lceil \gamma/(3s)\rceil$, it follows that $3s\nu \le \gamma + 3s$, and by (5.2) we have $\nu \ge \gamma/(3s) \ge \varrho/(3\varepsilon)$; therefore,

$$M^{1-\nu}|t|\mathfrak{q}_\sharp^{3s\nu} \ll M^{1-\varrho/(3\varepsilon)+\tau}\mathfrak{q}_\sharp^{\gamma+3s}.$$

We have $\mathfrak{q}_\sharp^{3s} \le N^{5\varepsilon} \le M^{5\varepsilon}$, and by (2.1) it follows that $\mathfrak{q}_\sharp^{\gamma} \le N^{2\varrho} \le M^{2\varrho}$. We get that

$$M^{1-\nu}|t|\mathfrak{q}_\sharp^{3s\nu} \ll M^{1-\varrho/(3\varepsilon)+\tau+2\varrho+5\varepsilon}.$$

Inserting this bound into (5.17), the theorem is a consequence of the inequality

$$\tau \le \varrho((3\varepsilon)^{-1} - 2) - \xi_0/\varrho^2 - 5\varepsilon,$$

which follows from the last inequality in (2.10) (which implies, $\tau \le C\varrho + o(1)$) assuming that ε and ξ_0 are sufficiently small in terms of C.

6 Proofs of results for L-functions and distribution of primes in progressions

6.1 Bounds on L-functions and zero-free regions: Proof of Theorem 3.1. We begin with a general statement involving two parameters η and Y.

Lemma 6.1. *For any real number $C > 0$ there are effectively computable constants $\gamma_0, \xi_0, c_0 > 0$ that depend only on C and have the following property. Let q be a modulus satisfying* (2.1) *and χ a primitive character modulo q. If Y and η satisfy*

$$Y \ge \mathfrak{q}_\sharp^{\gamma_0}, \quad \eta \in (0, \frac{1}{3}) \quad \text{and} \quad \eta \le \xi_0(\log Y)^2/\ell^2 - c_0(\log \ell)/\log Y, \tag{6.1}$$

where $\ell = \log q(|t|+3)$, and the inequalities $\sigma > 1-\eta$ and $|t| \le q^C$ hold, then for $s = \sigma + it$ we have

$$|L(s,\chi)| \le \eta^{-1}Y^\eta.$$

Proof. Fix $C > 0$, and let $\gamma_0, \xi_0 > 0$ have the property described in Theorem 2.2. Let q be a modulus satisfying (2.1) and χ a primitive character modulo q. By Theorem 2.2 and partial summation, the bound

$$\sum_{N<n\le 2N} \chi(n) n^{-s} \ll N^{1-\sigma-\xi_0/\varrho^2} \quad (N \ge \mathfrak{q}_\sharp^{\gamma_0}) \tag{6.2}$$

holds, where $\varrho = (\log q)/\log N$ and the implied constant depends only on C.

Put $Z = e^{2\ell}$. Arguing as in the proof of [11, Lemma 8], the bound

$$\left| \sum_{n>Z} \chi(n) n^{-s} \right| \le 1 \tag{6.3}$$

holds since $\sigma > \frac{1}{2}$. On the other hand, let Y and η be real numbers that satisfy (6.1) with some constant $c_0 > 0$ that depends only on C. Assuming that $\sigma > 1 - \eta$, the bounds (6.1) and (6.2) imply

$$\sum_{N<n\le 2N} \chi(n) n^{-s} \ll N^{\eta-\xi_0/\varrho^2} \le Y^{\eta-\xi_0/\varrho^2} \le \ell^{-c_0} \quad (N \ge Y).$$

Hence, if c_0 is sufficiently large in terms of C, then for $\sigma > 1 - \eta$ we have

$$\left| \sum_{N<n\le 2N} \chi(n) n^{-s} \right| \le (3\ell)^{-1} \quad (N \ge Y),$$

which by a standard splitting argument yields the bound

$$\left| \sum_{n\le Z} \chi(n) n^{-s} \right| \le 1 + \left| \sum_{n\le Y} \chi(n) n^{-s} \right| \le 1 + \sum_{n\le Y} n^{\eta-1} \le 2 + \eta^{-1}(Y^\eta - 1).$$

Combining this with (6.3), and taking into account that $\eta \le \frac{1}{3}$, it follows that

$$|L(s, \chi)| \le \eta^{-1} Y^\eta$$

holds when $\sigma > 1 - \eta$. □

We now turn to the proof of Theorem 3.1. Let the notation be the same as in Lemma 6.1. The first inequality in (6.1) is

$$\log Y \ge \gamma_0 \log \mathfrak{q}_\sharp. \tag{6.4}$$

If Y also satisfies the inequality

$$\log Y \ge (2c_0/\xi_0)^{1/3} \ell^{2/3} (\log \ell)^{1/3}, \tag{6.5}$$

then it follows that

$$\xi_0 (\log Y)^2/\ell^2 - c_0 (\log \ell)/\log Y \ge 0.5 \xi_0 (\log Y)^2/\ell^2;$$

hence the second inequality in (6.1) is satisfied provided that the lower bound

$$\log Y \geq 2^{1/2}\xi_0^{-1/2}\eta^{1/2}\ell \tag{6.6}$$

also holds. Consequently, defining Y by the equation

$$\log Y = A\max\{\log \mathfrak{q}_\sharp, \eta^{1/2}\ell, \ell^{2/3}(\log \ell)^{1/3}\}$$

with a suitably large absolute constant $A > 0$ (depending only on γ_0, ξ_0, c_0), we see that the inequalities (6.4), (6.5) and (6.6) all hold, hence the condition (6.1) is met. Applying Lemma 6.1 we obtain the stated bound.

6.2 The zero-free region: Proof of Theorem 3.2. We start with a technical result contained in Iwaniec [11], which we present in a generic form suitable for further applications.

Lemma 6.2. *Let q be a fixed modulus. Let $\eta \in (0, \frac{1}{3})$, $T \geq 1$ and $M \geq e$ be numbers that can depend on q. Put*

$$\vartheta = \frac{\eta}{400\log M}, \tag{6.7}$$

and suppose that

$$8\log(5\log 3q) + \frac{24}{\eta}\log(2M/5\vartheta) \leq \frac{1}{15\vartheta}. \tag{6.8}$$

Suppose that $|L(s,\chi)| \leq M$ for all primitive characters χ modulo q and all s in the region $\{s \in \mathbb{C} : \sigma > 1-\eta,\ |t| \leq 3T\}$. There is at most one primitive character χ modulo q such that $L(s,\chi)$ has a zero in the region $\{s \in \mathbb{C} : \sigma > 1-\vartheta,\ |t| \leq T\}$. If such a character exists, then it is a real character, and the zero is unique, real and simple.

Proof. The first part of the proof of [11, Lemma 11] shows that $L(s,\chi) \neq 0$ throughout the region

$$\Gamma = \begin{cases} \{s \in \mathbb{C} : \sigma > 1-\vartheta,\ |t| \leq T\} & \text{if } \chi^2 \neq \chi_0, \\ \{s \in \mathbb{C} : \sigma > 1-\vartheta,\ \eta/4 < |t| \leq T\} & \text{if } \chi^2 = \chi_0, \end{cases}$$

provided that

$$6\log(5\log 3q) + \frac{16}{\eta}\log(M/5\vartheta) + \frac{8}{\eta}\log(2M/5\vartheta) \leq \frac{1}{15\vartheta},$$

which follows from (6.8). The second part of the proof of [11, Lemma 11] then shows that if $L(s, \chi) = 0$ for some s in the region $\{s \in \mathbb{C} : \sigma > 1 - \vartheta,\ |t| \le \eta/4\}$, then the zero is unique, real and simple provided that

$$8 \log(5 \log 3q) + \frac{16}{\eta} \log(M/5\vartheta) \le \frac{1}{15\vartheta}, \tag{6.9}$$

which also follows from (6.8). Finally, [11, Lemma 12] shows that there is at most one nonprincipal character χ modulo q for which $L(s, \chi)$ has a real zero $\beta > 1 - \vartheta$, provided that

$$2 \log(5 \log 3q) + \frac{12}{\eta} \log(M/5\vartheta) \le \frac{2}{15\vartheta},$$

which is also a consequence of (6.9). The result now follows. □

Turning now to the proof of Theorem 3.2, we note that with the choice

$$\eta = \frac{(\log \log q)^{2/3}}{(\log q)^{2/3}}$$

Theorem 3.1 shows that $|L(s, \chi)| \le M$ for all primitive characters χ modulo q and all s in the region $\{s \in \mathbb{C} : \sigma > 1 - \eta,\ |t| \le 3q^C\}$, where

$$M = (\log q)^B$$

for some constant B that depends only on C and $\mathfrak{q}_\sharp$. Using (6.7) to define ϑ, we obtain (3.2) with $A = 1/(400B)$. Taking B larger (and A smaller) if necessary, we can guarantee that $M \ge e$ and that the condition (6.8) is met. Applying Lemma 6.2, we obtain the statement of Theorem 3.2.

6.3 The zero-free region: Proof of Corollary 3.4. Corollary 3.4 concerns only those moduli q of the form $q = p^\gamma$, where p is a fixed prime and $\gamma \in \mathbb{N}$; note that $\mathfrak{q}_\sharp = p$ in this situation. Let γ_0, A and ϑ be the numbers supplied by Theorem 3.2 with the constant $C = 1$, and let

$$\mathcal{R} = \{s \in \mathbb{C} \ :\ \sigma > 1 - \vartheta,\ |t| \le q\}.$$

Clearly,

$$\vartheta_0 \ll \frac{\vartheta}{(\log \log q)^{5/12}},$$

hence adjusting the constant A_0 (if necessary) we have $\mathcal{R}_0 \subseteq \mathcal{R}$.

For a fixed prime p there are only finitely many primitive characters χ of conductor p^γ with $\gamma < \gamma_0$. Consequently, after replacing A with a smaller number (depending only on p), we can ensure that $L(s, \chi)$ does not vanish in $\mathcal{R}$ for any such primitive character. Thus, from now on, we assume $\gamma \ge \gamma_0$.

Given an arbitrary character χ modulo $q = p^\gamma$, let $q^* = p^{\gamma^*}$ be its conductor. Since $\gcd(n, q) = 1$ if and only if $\gcd(n, q^*) = 1$, the character χ is primitive when regarded as a character modulo q^*.

If $\gamma^* < \gamma_0$, $L(s, \chi)$ does not vanish in $\mathcal{R}$ by our choice of A. In particular, this holds true if χ is a real character. Indeed, for an odd p, if χ is real, then χ is either the principal character modulo p or the Legendre symbol modulo p, since $(\mathbb{Z}/p^\gamma\mathbb{Z})^\times$ is cyclic for odd p and therefore admits only two real characters. If $p = 2$, then $(\mathbb{Z}/2^\gamma\mathbb{Z})^\times$ is of rank at most two and a similar argument implies that there are at most four real characters. In each case, the conductors of these characters depend only on p.

Now suppose that $\gamma^* \geq \gamma_0$ and that χ is not real. We consider two cases.

If $q^* \geq T_0$, then using Theorem 3.2 (with $C = 1$) $L(s, \chi)$ does not vanish in $\mathcal{R}$, hence it is nonzero in $\mathcal{R}_0$ ($\subseteq \mathcal{R}$).

If $q^* < T_0$, we use a result of Gallagher [5, Equation (15)] which asserts that the corresponding L-function does not vanish in the region

$$\mathcal{Q} = \left\{ s \in \mathbb{C} \,:\, \sigma > 1 - \frac{B}{(\log(q^*|t|) \log\log(q^*|t|))^{3/4}} \right\}$$

for some constant B that depends only on p. For $t \leq T_0$ we obtain that

$$\begin{aligned} \frac{1}{(\log(q^*|t|) \log\log(q^*|t|))^{3/4}} &\geq \frac{1}{(\log(T_0^2) \log\log(T_0^2))^{3/4}} \\ &\gg \frac{1}{(\log T_0 \log\log T_0)^{3/4}} \gg \frac{1}{(\log q)^{2/3} (\log\log q)^{3/4}}. \end{aligned}$$

Hence, for an appropriate choice of the constant A_0 we have $\mathcal{R}_0 \subseteq \mathcal{Q}$.

6.4 Primes in arithmetic progressions: Proof of Theorem 3.5. We again put

$$T_0 = \exp((\log q)^{8/9})$$

to allow an application of Corollary 3.4. More precisely, since $\log q \asymp \log x$ holds with implied constants that depend only on b and ε, an application of Corollary 3.4 shows that there is a constant $a > 0$ depending only on b, ε and p such that $N_q(\alpha, T_0) = 0$ for all $\alpha \geq \vartheta$, where

$$\vartheta = \frac{a}{(\log x)^{2/3} (\log\log x)^{3/4}}. \tag{6.10}$$

We now follow the proof of [5, Theorem 2], with the parameters h and x there being replaced by x and 2, respectively.

Using (3.3) together with the "trivial" bound (see [12, Theorem 5.24])

$$N_q(\alpha, T_0) \ll qT_0\ell,$$

the first double sum in [5, Equation (16)] is bounded by the following precise version of [5, Equation (17)]:

$$\begin{aligned}\int_0^{1-\vartheta} x^{\alpha-1}N_q(\alpha, T_0)(\log x)\,d\alpha + x^{-1}N_q(0, T_0) &\\ \ll (\log x)^{O(1)} \int_0^{1-\vartheta} ((qT_0)^b x^{-1})^{1-\alpha}\,d\alpha + qT_0x^{-1}(\log x)^{O(1)} &\\ = (\log x)^{O(1)} \int_0^{1-\vartheta} x^{-\varepsilon(1-\alpha)}\,d\alpha + x^{(1-\varepsilon)/b-1+o(1)} &\\ \ll_\varepsilon x^{-\varepsilon\vartheta}(\log x)^{O(1)} + x^{(1-\varepsilon)/b-1+o(1)}, &\end{aligned}$$

where the symbol $\ll_\varepsilon$ indicates that the implied constant may depend on ε.

Since $b > 1$ implies that $(1-\varepsilon)/b - 1 < 0$, using (6.10) we see that the first term of the preceding bound dominates, and so we obtain that

$$\int_0^{1-\vartheta} x^{\alpha-1}N_q(\alpha, T_0)\log x\,d\alpha + x^{-1}N_q(0, T_0) \ll_\varepsilon \exp(-c_0(\log x)^{1/3}(\log\log x)^{-3/4})$$

holds with any fixed $c_0 < \varepsilon a$. We also use [5, Equation (18)] to bound the second double sum in [5, Equation (16)]. Putting everything together, we have

$$\psi(x; q, a) - \frac{x}{\varphi(q)} \ll_\varepsilon \frac{x}{\varphi(q)} \exp(-c_0(\log x)^{1/3}(\log\log x)^{-3/4}) + \frac{x}{T_0\varphi(q)}(\log x)^{O(1)}.$$

Recalling the choice of T_0, we conclude the proof.

6.5 Primes in arithmetic progressions: Proof of Theorem 3.6. We recall the following result of Harman [8, Theorem 1.2], which we present in an equivalent form in terms of the functions $\psi(x; q, a)$.

Lemma 6.3. *There is a value $\delta > 0$ such that the following statement is true. Given $\varepsilon > 0$, there are constants $K(\varepsilon) \ge 2$ and $c > 0$, such that if $q > K$ is such that each prime divisor $p \mid q$ satisfies $p < q^\delta$ and for every $d \mid q$ and a primitive character χ modulo d we have $L(s, \chi) = 0$ for $s = \sigma + it$ with*

$$\sigma > 1 - \frac{1}{(\log q)^{3/4}} \quad \text{and} \quad |t| \le \exp(\varepsilon(\log q)^{3/4}),$$

then

$$\psi(x; q, a) \gg \frac{x}{\varphi(q)},$$

whenever $x^{0.4736} > q$.

Recalling Corollary 3.4 and assuming that γ is large enough, by Lemma 6.3 we conclude the proof.

7 Comments

Our results can be extended to more general classes of moduli. For example, suppose that $q = rs$ with coprime positive integers r and s, and instead of (2.1) we have

$$\min_{p|s}\{v_p(s)\} \geq 0.7\gamma \quad \text{with } \gamma = \max_{p|s}\{v_p(s)\} \geq \gamma_0.$$

For any primitive character χ modulo q, we write

$$S_\chi(M,N) = \sum_{k=0}^{r-1} \sum_{(M-k)/r<m\leq(M+N-k)/r} \chi(k+rm) + O(r).$$

Defining $\chi^*(m) = \chi(k+rm)$, we see that χ^* is a primitive character modulo s, hence Theorem 2.1 applies to the inner sum over m. Consequently, if r is not too large (say, $r = N^{o(1)}$), then we obtain a result of roughly the same strength as Theorem 2.1. This applies to the other results of this paper as well.

We also remark that splitting the sums in the argument of §6.1 into intervals which are shorter than dyadic, one can extend the range of t in Theorem 3.1 and then in turn in Theorem 3.2 (with slightly weaker bounds). This leads to a version of Theorem 3.5 for longer progressions (with a weaker error term).

Harman and Kátai [9, Lemma 6] give an asymptotic formula for primes in an arithmetic progression modulo a very smooth number. Their result applies to progressions that are much longer than those covered by Theorem 3.5, but are much shorter than those that can be treated nowadays for generic moduli.

Finally, we note that Green [7, Theorem 4.1] has established the bound

$$\sum_{n=1}^{N} \mu(n)\chi(n) \ll N\exp(-c_0(\log N)^{1/2}),$$

where $\mu(n)$ is the Möbius function and $\chi(n)$ is a multiplicative character modulo $q = 2^\gamma$ (with integer $\gamma > 0$) for which $q \leq \exp(c_0(\log N)^{1/2})$, where $c_0 > 0$ is an absolute constant. Using our bounds, in particular Theorem 3.5 and the potential modifications mentioned above, one can obtain nontrivial bounds for sums of this form with much larger and more general moduli.

Acknowledgements. The authors are very grateful to Glyn Harman for various discussions concerning [8, Theorem 1.2]. We also thank the anonymous referee for numerous important comments and suggestions.

The first author was supported in part by a grant from the University of Missouri Research Board. The second author was supported by ARC Grant DP170100786.

References

[1] J. Bourgain, C. Demeter and L. Guth, *Proof of the main conjecture in Vinogradov's mean value theorem for degrees higher than three*, Ann. of Math. (2) **184** (2016), 633–682.

[2] M.-C. Chang, *Short character sums for composite moduli*, J. Anal. Math. **123** (2014), 1–33.

[3] L. De Feo, D. Jao and J. Plût, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, J. Math. Cryptol. **8** (2014), 209–247.

[4] K. Ford, *Vinogradov's integral and bounds for the Riemann zeta function*, Proc. Lond. Math. Soc. (3) **85** (2002), 565–633.

[5] P. X. Gallagher, *Primes in progressions to prime-power modulus*, Invent. Math. **16** (1972), 191–201.

[6] A. Granville and K. Soundararajan, *Upper bounds for* $|L(1, \chi)|$, Q. J. Math. **53** (2002), 265–284.

[7] B. Green, *On (not) computing the Möbius function using bounded depth circuits*, Combin. Probab. Comput. **21** (2012), 942–951.

[8] G. Harman, *Watt's mean value theorem and Carmichael numbers*, Int. J. Number Theory **4** (2008), 41–248.

[9] G. Harman and I. Kátai, *Primes with preassigned digits, II*, Acta Arith. **133** (2008), 171–184.

[10] M. N. Huxley, *Large values of Dirichlet polynomials, III*, Acta Arith. **26** (1974), 435–444.

[11] H. Iwaniec, *On zeros of Dirichlet's L series*, Invent. Math. **23** (1974), 97–104.

[12] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, American Mathematical Society, Providence, RI, 2004.

[13] S. Konyagin and C. Pomerance, *On primes recognizable in deterministic polynomial time*, in *The Mathematics of Paul Erdős, Vol. 1*, Springer, New York, 2013, pp. 159–186.

[14] N. M. Korobov, *The distribution of digits in periodic fractions*, Math. USSR-Sb. **18** (1974), 659–676.

[15] D. Milićević, *Sub-Weyl subconvexity for Dirichlet L-functions to powerful moduli*, Compos. Math. **152** (2016), 825–875.

[16] A. G. Postnikov, *On the sum of characters with respect to a modulus equal to a power of a prime number*, Izv. Akad. Nauk SSSR. Ser. Mat. **19** (1955), 11–16.

[17] A. G. Postnikov, *On Dirichlet L-series with the character modulus equal to the power of a prime number*, J. Indian Math. Soc. **20** (1956), 217–226.

[18] I. M. Vinogradov, *The upper bound of the modulus of a trigonometric sum*, Izv. Akad. Nauk SSSR. Ser. Mat. **14** (1950), 199–214.

[19] I. M. Vinogradov, *General theorems on the upper bound of the modulus of a trigonometric sum*, Izv. Akad. Nauk SSSR. Ser. Mat. **15** (1951), 109–130.

[20] T. D. Wooley, *Vinogradov's mean value theorem via efficient congruencing*, Ann. of Math. (2) **175** (2012), 1575–1627.

[21] T. D. Wooley, *Vinogradov's mean value theorem via efficient congruencing, II*, Duke Math. J. **162** (2013), 673–730.

[22] T. D. Wooley, *Multigrade efficient congruencing and Vinogradov's mean value theorem*, Proc. Lond. Math. Soc. (3) **111** (2015), 519–560.

[23] B. Źrałek, *Using partial smoothness of* $p - 1$ *for factoring polynomials modulo* p, Math. Comp. **79** (2010), 2353–2359.

William D. Banks
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF MISSOURI
COLUMBIA, 65211 MO, USA
email: bankswd@missouri.edu

Igor E. Shparlinski
DEPARTMENT OF PURE MATHEMATICS
UNIVERSITY OF NEW SOUTH WALES
SYDNEY, NSW 2052, AUSTRALIA
email: igor.shparlinski@unsw.edu.au

(Received February 14, 2017 and in revised form November 13, 2017)