Short character sums for composite moduli *†

Mei-Chu Chang‡
Department of Mathematics
University of California, Riverside
mcc@math.ucr.edu

Abstract

We establish new estimates on short character sums for arbitrary composite moduli with small prime factors. Our main result improves on the Graham-Ringrose bound for square-free moduli and also on the result due to Gallagher and Iwaniec when the core $q' = \prod_{p|q} p$ of the modulus q satisfies $\log q' \sim \log q$. Some applications to zero free regions of Dirichlet L-functions and the Pólya and Vinogradov inequalities are indicated.

Introduction.

In this paper we will discuss short character sums for moduli with small prime factors. In particular, we will revisit the arguments of Graham-Ringrose [GR] and Postnikov [P]. Our main result is an estimate valid for general moduli, which improves on the known estimates in certain situations.

It is well known that non-trivial estimates on short character sums are important to many number theoretical issues. In particular, they are relevant in establishing density theorems for the corresponding Dirichlet L-functions.

In the literature, several bounds on short incomplete character sums to some modulus q may be found, depending on the nature of q. Burgess' bound applies for moduli q that are cube free, provided the summation interval I has size $N \gg q^{\frac{1}{4}+\epsilon}$. Assuming q has small prime factors, nontrivial estimates may

*2000 *Mathematics Subject Classification.* 11L40, 11M06.
†*Key words.* character sums, zero free regions
‡Research partially financed by the National Science Foundation.

be obtained under weaker assumptions on N. There are two classical results in this aspect, based on quite different arguments. Citing from [IK], the Graham-Rignrose theorem (see [IK], Corollary 12.15) makes the assumptions that q is square-free and

$$N \geq q^{\frac{4}{\sqrt{\log\log q}}} + \mathcal{P}^9 \tag{0.1}$$

with $\mathcal{P}$ the largest prime factor of q. On the other hand, Iwaniec's generalization of Postnikov's theorem (see [IK], Theorem 12.16) comes with a condition of the form

$$N > (q')^{100} + e^{(\log q)^{3/4}\log\log q} \tag{0.2}$$

with $q' = \prod_{p|q} p$ the core of q.

The main purpose of this work is to formulate a condition on N as weak as possible, for general modulus q with small prime factors, providing at least subpower savings. That this is possible (assuming $\log N > \phi(\log q)$ for some function ϕ satisfying $\frac{\phi(x)}{x} \to 0$ as $x \to \infty$) was probably known to experts, though no result of this kind seems to appear in the literature.

More specifically, we prove the following.

Theorem 5. *Assume N satisfies*

$$q > N > \max_{p|q} p^{10^3}$$

and

$$\log N > (\log q)^{1-c} + C\log\Big(2\frac{\log q}{\log q'}\Big)\,\frac{\log q'}{\log\log q}\,, \tag{0.3}$$

where $C, c > 0$ are some constants, (e.g. we may take $c = 10^{-3}$ and $C \sim 10^3$) and $q' = \prod_{p|q} p$.

Let χ be a primitive multiplicative character modulo q and I an interval of size N. Then

$$\Big|\sum_{x\in I}\chi(x)\Big| \ll Ne^{-(\log N)^{3/5}}. \tag{0.4}$$

Note that assumption (0.3) of Theorem 5 is implied by the stronger and friendlier assumption

$$\log N > C\Big(\log\mathcal{P} + \frac{\log q}{\log\log q}\Big), \tag{0.5}$$

where $\mathcal{P} = \max_{p|q} p$. Assumption (0.5) is weaker than Graham-Ringrose's condition

$$\log N > C\Big(\log \mathcal{P} \ + \ \frac{\log q}{\sqrt{\log\log q}}\Big) \ ,$$

which moreover assumes q square-free.

Many techniques used in the paper are just elaborations of known arguments. In addition to the basic techniques introduced in the work of Graham-Ringrose and Postnikov, we introduce one further ingredient which is a (new) mixed character sum estimate (see Theorem 1). It allows to merge more efficiently Postnikov's procedure of replacing multiplicative characters to a powerful modulus by additive characters with a polynomial argument and the Weyl differencing scheme which is the basis of the Graham-Ringrose analysis. Note that the replacement of $(\log\log q)^{\frac{1}{2}}$ in (0.1) by $\log\log q$ is achieved by a more economical variant of the Graham-Ringrose argument (based on a notion of 'admissible pair' (f, q) with $f \in \mathbb{Z}[x]$, $q \in \mathbb{Z}$). But this is a technical point with no essentially new ideas.

The condition (0.3) in Theorem 5 is the best we could do. But we did not try to optimize the power $1 - c$ in the first term nor the saving in (0.4). The main interest of (0.3) compared with (0.2) is that the assumption

$$\log N > C \log q'$$

is weakened to

$$\log N > C \frac{\log(2\frac{\log q}{\log q'})}{\log\log q} \ \log q'$$

leading to an improvement when q' is relatively large.

This is the place where the mixed character sum (Theorem 1) comes into play.

Next, we turn to some consequences of Theorem 5 that are elaborated in the last section of the paper.

Following well-known arguments (cf. [I]), Theorem 5 implies the following zero-free regions for the corresponding Dirichlet L-functions.

Theorem 10. *Let χ be a primitive multiplicative character with modulus q, $\mathcal{P} = \max_{p|q} p$, $q' = \prod_{p|q} p$, and $K = \frac{\log q}{\log q'}$. For $T > 0$, let*

$$\theta = c \min\Big(\frac{1}{\log \mathcal{P}}, \frac{\log\log q'}{(\log q')\log 2K}, \frac{1}{(\log qT)^{1-c'}}\Big).$$

Then the Dirichlet L-function $L(s,\chi) = \sum_n \chi(n)n^{-s}$, $s = \rho + it$ has no zeros in the region $\rho > 1 - \theta$, $|t| < T$, except for possible Siegel zeros.

In the theorem above, one may take $c' = 1/10$. In certain ranges of q', Theorem 10 improves upon Iwaniec's condition [I]

$$\theta = \min\left\{ c\frac{1}{(\log qT)^{\frac{2}{3}}(\log\log qT)^{\frac{1}{3}}}\ , \frac{1}{\log q'}\right\}.$$

Using the zero-free region above and the result from [HB2] on the effect of a possible Siegel zero, we obtain the following.

Corollary 11. *Assume q satisfies that $\log p = o(\log q)$ for any $p|q$. If $(a,q) = 1$, then there is a prime $P \equiv a \pmod q$ such that $P < q^{\frac{12}{5}+o(1)}$.*

Using Theorem 5, we may also obtain a slight improvement of the following result by Goldmakher ([G], corollary to Theorem 1) on the Pólya-Vinogradov inequality.

(Goldmakher) *Given $\chi \pmod q$ primitive, with q square-free. Then*

$$\Big|\sum_{n<x}\chi(n)\Big| \ll \sqrt{q}\ \log q\ \sqrt{\log\log\log q}\left(\frac{1}{\log\log q} + \frac{\log\mathcal{P}}{\log q}\right)^{\frac{1}{4}}. \tag{0.6}$$

What we obtain is the following.

Theorem 12. *Let χ be a primitive multiplicative character with modulus q, and let $\mathcal{P}$ be the largest prime divisor of q, $q' = \prod_{p|q} p$ and $K = \frac{\log q}{\log q'}$. Let $M = (\log q)^{1-c} + \frac{\log q'}{\log\log q'}\log 2K + \log\mathcal{P}$. Then*

$$\Big|\sum_{n<x}\chi(n)\Big| \ll \sqrt{q}\sqrt{\log q}\ \sqrt{M}\sqrt{\log\log\log q}.$$

In particular, Theorem 12 gives the bound

$$\sqrt{q}\ \log q\ \sqrt{\log\log\log q}\left(\frac{1}{\sqrt{\log\log q}} + \frac{\sqrt{\log\mathcal{P}}}{\sqrt{\log q}}\right) \quad \text{for arbitrary } q. \tag{0.7}$$

Clearly, (0.7) is a stronger bound than (0.6).

The paper is organized as follows. In Section 1, we state the mixed character sum theorem with square-free modulus and indicate where the changes are in the proof for prime modulus. In Section 2, we give a version of Postnikov's Theorem, using it to derive a non-trivial character sum bound for the modulus $q_0^m q_1$, q_1 square-free. Section 3 contains the notion of admissible pair and an improved version of Graham-Ringrose Theorem. Section 4 is the Graham-Ringrose version of mixed character sum estimate. Section 5 contains our main theorem, discussion of our assumption and comparison of it with the assumptions in known results. The proof of the main theorem is in Section 6 and Section 7, its applications in Section 8.

Notations and Conventions.

1. $e(\theta) = e^{2\pi i\theta}$, $e_p(\theta) = e(\frac{\theta}{p})$.
2. $\omega(q)$ = the number of prime divisors of q.
3. $\tau(q)$ = the number of divisors of q.
4. $q' = \prod_{p|q} p$, the core of q.
5. $\mathcal{P} = \mathcal{P}(q) = \max_{p|q} p$.
6. When there is no ambiguity, $p^{\,\varepsilon} = [p^{\,\varepsilon}] \in \mathbb{Z}$.
7. Modulus q is always sufficiently large.
8. ϵ, c, C = various constants, and ϵ is particularly small.
9. All characters are non-principal.
10. For polynomials $f(x)$ and $g(x)$ with no common factors, the *degree* of $\frac{f(x)}{g(x)}$ is $\deg f(x) + \deg g(x)$.
11. $A \ll B$ and $A = O(B)$ are each equivalent to that $|A| \leq cB$ for some constant c. If the constant c depends on a parameter ρ, we use $\ll_\rho$. Otherwise, c is absolute.

1 Mixed character sums.

Theorem 1. *Let $P(x) \in \mathbb{R}[x]$ be an arbitrary polynomial of degree $d \geq 1$, p a sufficiently large prime, $I \subset [1,p]$ an interval of size*

$$|I| > p^{\frac{1}{4}+\kappa} \tag{1.1}$$

(for some $\kappa > 0$) and χ a multiplicative character (mod p)*. Then*

$$\Big|\sum_{n\in I} \chi(n) e^{iP(n)}\Big| < c(\kappa)(d+1)^2\ |I|\ p^{-\frac{\kappa^2}{10(d^2+2d+3)}}. \tag{1.2}$$

In the proof of Theorem 1, the assumption that p is a prime is only used in order to apply Weil's bound on complete exponential sums. (For the Weil's estimate below, see Theorem 11.23 in [IK])

Weil's Theorem. *Let p be a prime, $f \in \mathbb{Z}[x]$ a polynomial of degree d, and χ a multiplicative character* (mod p) *of order $r > 1$. Suppose f*(mod p) *is not an r-th power. Then we have*

$$\Big|\sum_{x=1}^{p} \chi(f(x))\Big| \leq d\ \sqrt{p}.$$

The assumption of f(mod p) in Weil's Theorem holds if f(mod p) has a simple root or a simple pole. For q square-free, one can derive the following theorem.

Weil's Theorem'. *Let $q = p_1 \cdots p_k$ be square-free, $f \in \mathbb{Z}[x]$ a polynomial of degree d, and χ a multiplicative character* (mod q)*. Let $q_1|q$ be such that for any prime $p|q_1$, f*(mod p) *has a simple root or a simple pole. Then*

$$\Big|\sum_{x=1}^{q} \chi(f(x))\Big| \leq d^{\,\omega(q_1)} \frac{q}{\sqrt{q_1}}.$$

Proof. Let χ_i be a multiplicative character (mod p_i). Then

$$\Big|\sum_{x=1}^{q} \chi(f(x))\Big| \leq \prod_{i=1}^{k} \Big|\sum_{x=1}^{p_i} \chi_i(f(x))\Big| \leq \prod_{p_i|q_1} d\sqrt{p_i} \prod_{p_i\nmid q_1} p_i = d^{\,\omega(q_1)} \frac{q}{\sqrt{q_1}}.$$

Therefore, we have the following.

Theorem 1'. *Let $P(x) \in \mathbb{R}[x]$ be an arbitrary polynomial of degree $d \geq 1$, $q \in \mathbb{Z}$ square-free and sufficiently large, $I \subset [1, q]$ an interval of size*

$$|I| > q^{\frac{1}{4}+\kappa} \tag{1.3}$$

(for some $\kappa > 0$) and χ a multiplicative character (mod q)*. Then*

$$\Big| \sum_{n \in I} \chi(n) e^{iP(n)} \Big| < c(\kappa)|I|\ q^{-c\kappa^2 d^{-2}} \tau(q)^{4(\log d) d^{-2}}. \tag{1.4}$$

Here c is an absolute constant.

Remark. In the proof of Theorem 1 in [C1], the assumption that p is a prime is only used to derive display (14) from display (13) by applying Weil's Theorem. For q square-free, the same argument works if Weil's Theorem is replaced by Weil's Theorem'.

2 Postnikov's Theorem.

An immediate application is obtained by combining Theorem 1' with Postnikov's method (See [P], [Ga], [I], and [IK] §12.6).

Postnikov's Theorem. *Let χ be a primitive multiplicative character* (mod q)*, $q = q_0^m$. Then*

$$\chi(1 + q_0 u) = e_q\big(F(q_0 u)\big).$$

Here $F(x) \in \mathbb{Q}[x]$ is a polynomial of the form

$$F(x) = BD\Big(x - \frac{x^2}{2} + \cdots \pm \frac{x^{m'}}{m'}\Big) \tag{2.1}$$

with

$$D = \prod_{\substack{k \leq m' \\ (k, q_0)=1}} k, \quad m' = 2m$$

and $B \in \mathbb{Z}, (B, q_0) = 1$. (Note that $F(q_0 x) \in \mathbb{Z}[x]$.)

Remark. In [IK] the above theorem was proved for $\chi(1 + q'u) = e_q(F(q'u))$, where $q' = \prod_{p|q} p$ is the core of q. That argument works verbatim for our case.

Theorem 2. *Let $q = q_0^m q_1$ with $(q_0, q_1) = 1$ and q_1 square-free.*

Assume $I \subset [1, q]$ an interval of size

$$|I| > q_0 q_1^{\frac{1}{4}+\kappa}. \tag{2.2}$$

Let χ be a multiplicative character (mod q) *of the form*

$$\chi = \chi_0 \chi_1$$

with χ_0(mod q_0^m) *arbitrary and χ_1*(mod q_1) *primitive. Then*

$$\Big| \sum_{n \in I} \chi(n) \Big| \ll |I| q_1^{-c\kappa^2 m^{-2}} \tau(q_1)^{c(\log m) m^{-2}}. \tag{2.3}$$

Proof. For $a \in [1, q_0], (a, q_0) = 1$ fixed, using Postnikov's Theorem, we write

$$\chi_0(a + q_0 x) = \chi_0(a)\chi_0(1 + q_0 \bar{a} x) = \chi_0(a) e_{q_0^m}\big(F(q_0 \bar{a} x)\big), \tag{2.4}$$

where

$$a\bar{a} = 1 \pmod{q_0^m}.$$

Hence

$$\Big| \sum_{n \in I} \chi(n) \Big| \leq \sum_{(a, q_0)=1} \Big| \sum_{a + q_0 x \in I} e_{q_0^m}\big(F(q_0 \bar{a} x)\big) \chi_1(a + q_0 x) \Big|. \tag{2.5}$$

Writing $\chi_1(a + q_0 x) = \chi_1(q_0)\chi_1(a\bar{q}_0 + x), q_0 \bar{q}_0 \equiv 1 (\text{mod } q_1)$, the inner sum in (2.5) is a sum over an interval $J = J_a$ of size $\sim \frac{|I|}{q_0}$, and Theorem 1' applies. □

3 Graham-Ringrose Theorem.

As a warm up, in this section we will reproduce Graham-Ringrose's argument. With some careful counting of the *bad* set, we are able to improve their condition on the size of the interval from $q^{1/\sqrt{\log \log q}}$ to $q^{C/\log \log q}$.

Theorem 3. *Let $q \in \mathbb{Z}$ be square-free, χ a primitive multiplicative character* (mod q)*, and $N < q$. Assume*

1. *For all* $p|q$, $p < N^{\frac{1}{10}}$.

2. $\log N > C\frac{\log q}{\log\log q}$.

Then

$$\Big|\sum_{x=1}^{N}\chi(x)\Big| \ll Ne^{-\sqrt{\log N}}.$$

We will prove the following stronger and more technically stated theorem.

Theorem 3' *Assume* $q = q_1 \dots q_r$ *with* $(q_i, q_j) = 1$ *for* $i \neq j$, *and* q_r *square-free. Factor*

$$\chi = \chi_1 \cdots \chi_r,$$

where $\chi_i(\mathrm{mod}\ q_i)$ *is arbitrary for* $i < r$, *and primitive for* $i = r$. *We further assume*

(i). *For all* $p|q_r, p > \sqrt{\log q_r}$.

(ii). *For all* i, $q_i < N^{\frac{1}{3}}$.

(iii). $r < c\log\log q$ for some $c < 1/4 - \epsilon$.

Then

$$\Big|\sum_{x=1}^{N}\chi(x)\Big| \ll Ne^{-\sqrt{\log q_r}}.$$

Remark 3.1. Instead of proving Theorem 3, we will prove Theorem 3'. To see that Theorem 3' implies Theorem 3, we write

$$q = \bar{p}_1 \cdots \bar{p}_\ell \cdot p_1 \cdot p_2 \cdots,$$

where

$$\bar{p}_1, \dots, \bar{p}_\ell < \sqrt{\log q}, \quad \text{and} \quad p_1 > p_2 > \cdots \geq \sqrt{\log q}.$$

Hence

$$\prod_{i=1}^{\ell}\bar{p}_i < e^{2\sqrt{\log q}} < q^{\frac{1}{10}}. \tag{3.1}$$

Let $q_1 = \prod_{i=1}^{k} p_i$, where we let k be maximum as to ensure that $q_1 < N^{\frac{1}{3}}$.

Therefore, $p_{k+1}q_1 > N^{\frac{1}{3}}$. By (1), $q_1 > N^{\frac{1}{3}-\frac{1}{10}} > N^{\frac{1}{5}}$.

We repeat this process on $\frac{q}{q_1}$ to get q_2 such that $N^{\frac{1}{3}} > q_2 > N^{\frac{1}{5}}$. Then, we repeat it on $\frac{q}{q_1 q_2}$ etc. After re-indexing, we have

$$q_r > q_{r-1} > \cdots > q_2 > N^{\frac{1}{5}}.$$

Hence $q > \left(N^{\frac{1}{5}}\right)^{r-1}$, which together with (2) gives (iii). $\square$

Remark 3.2. It follows from (ii) and the argument in Remark 3.1 that in the proof of Theorem3, one may choose q_r satisfying $N^{1/5} < q_r < N^{1/3}$. Hence $\log N \sim \log q_r$.

The following definition will be used frequently throughout the rest of the paper.

Definition. Let p be a prime and $f \in \mathbb{Z}[x]$. We say p is *good* or f is *p-good*, if f mod p has a simple root or a simple pole. Otherwise it is called *bad* or *p-bad*. For $\bar{q}|q_r$ satisfying $\bar{q} > \sqrt{q_r}$, the pair $(f, \bar{q})$ is called q_r-*admissible* (or *admissible* when there is no ambiguity) if

$$p > \sqrt{\log q_r} \quad \text{for all} \quad p|\bar{q},$$

and

$$\prod_{\substack{p|\bar{q} \\ p \text{ is good}}} p \; > \; \frac{\bar{q}}{q_r^{\tau}}, \qquad \text{where } \tau = \frac{10}{\log\log q_r}.$$

Remark 3.3. Let $(f, \bar{q})$ be admissible, and let χ be primitive mod $\tilde{\tilde{q}}$, where $\tilde{\tilde{q}}$ is square-free and a multiple of $\bar{q}$. Assume

$$\log d < \frac{1}{\tau} = \frac{\log\log q_r}{10}, \text{ where } d = \deg f. \tag{3.2}$$

Then we have a bound on the complete sum

$$\left| \sum_{x=1}^{\tilde{\tilde{q}}} \chi(f(x)) \right| < \tilde{\tilde{q}} \, (\hat{q})^{-\frac{3}{10}} < \tilde{\tilde{q}} (\bar{q})^{-\frac{3}{10}} q_r^{\frac{3}{10}\tau},$$

where $\hat{q}$ is the product of the good primes $p|\bar{q}$.

Proof of Remark 3.3. For $p|\bar{q}|q_r$, our assumptions imply

$$p^{1/5} > (\log q_r)^{1/10} > d. \tag{3.3}$$

To prove the remark, we factor $\chi = \chi_1\chi_2$, where χ_1 (respectively, χ_2) is a character mod $\bar{q}$ (resp. mod $\frac{\tilde{\tilde{q}}}{\bar{q}}$). Weil's estimate gives a bound on the complete sum of χ_1 in the following estimate.

$$\begin{aligned} &\left|\sum_{x=1}^{\tilde{\tilde{q}}} \chi(f(x))\right| \\ &\leq \left|\sum_{x=1}^{\bar{q}} \chi_1(f(x))\right| \left|\sum_{x=1}^{\frac{\tilde{\tilde{q}}}{\bar{q}}} \chi_2(f(x))\right| < \frac{\bar{q}}{\sqrt{\hat{q}}}\, d^{\,\omega(\hat{q})}\, \frac{\tilde{\tilde{q}}}{\bar{q}} = \frac{\tilde{\tilde{q}}}{\sqrt{\hat{q}}}\, d^{\,\omega(\hat{q})}. \end{aligned} \tag{3.4}$$

where $\hat{q}$ is the product of the good primes $p|\bar{q}$. Using (3.3), we bound the character sum above by

$$\tilde{\tilde{q}} \prod_{p|\hat{q}} \frac{d}{\sqrt{p}} < \tilde{\tilde{q}} \prod_{p|\hat{q}} p^{-3/10} = \tilde{\tilde{q}}\hat{q}^{\,-3/10}.$$

Since $(f, \bar{q})$ is admissible, we have

$$\left|\sum_{x=1}^{\tilde{\tilde{q}}} \chi(f(x))\right| < \tilde{\tilde{q}}\hat{q}^{\,-\frac{3}{10}} < \tilde{\tilde{q}}(\bar{q})^{-\frac{3}{10}} q_r^{\frac{3}{10}\tau}. \qquad \square$$

Proof of Theorem 3'. We will use Weyl differencing.

Take $M = \left[\sqrt{N}\,\right]$. Shifting the interval $[1, N]$ by yq_i for any $1 \leq y \leq M$, we get

$$\Big|\sum_{x=1}^{N} \chi(x) - \sum_{x=1}^{N} \chi(x + yq_1)\Big| \leq 2yq_1 \ll Mq_1.$$

Averaging over the shifts gives

$$\frac{1}{N}\Big|\sum_{x=1}^{N} \chi(x)\Big| \leq \frac{1}{NM} \sum_{x=1}^{N} \Big|\sum_{y=1}^{M} \chi(x + yq_1)\Big| + O\left(\frac{Mq_1}{N}\right). \tag{3.5}$$

Let

$$\chi_1' = \chi_2 \cdots \chi_r.$$

Using the q_1-periodicity of χ_1 and Cauchy-Schwarz inequality on the double sum in (3.5), we have

$$\frac{1}{NM}\sum_{x=1}^{N}\Big|\sum_{y=1}^{M}\chi(x+yq_1)\Big| \le \left[\frac{1}{NM^2}\sum_{y,\,y'=1}^{M}\Big|\sum_{x=1}^{N}\chi_1'\left(\frac{x+q_1y}{x+q_1y'}\right)\Big|\right]^{1/2}. \quad (3.6)$$

For given (y, y'), we consider

$$f_{y,y'}(x) = \frac{x+q_1y}{x+q_1y'}$$

and distinguish among the pairs $(f_{y,y'}, q_r)$ by whether or not they are q_r-admissible. Note that if $(f_{y,y'}, q_r)$ is not admissible, then the product of *bad* prime factors of q_r is at least q_r^τ and this product must divide $y-y'$. We will estimate the size of the set of bad (y, y') and use trivial bound for the inner sum in (3.6) corresponding to such bad (y, y').

$$\begin{aligned}
&\Big|\big\{(y,y')\in[1,M]^2 : (f_{y,y'},q_r) \text{ is not admissible }\big\}\Big| \\
&\le \sum_{\substack{Q|q_r\\ Q\ge q_r^\tau}}\Big|\big\{(y,y')\in[1,M]^2 : Q|\ y-y'\ \big\}\Big| \\
&\le \sum_{\substack{Q|q_r\\ Q\ge q_r^\tau}}\frac{M^2}{Q} < 2^{\omega(q_r)}\frac{M^2}{q_r^\tau} < M^2 q_r^{-\frac{7}{10}\tau}.
\end{aligned} \quad (3.7)$$

(For the second inequality, we note that $M > Q$.)

Hence (3.6) is bounded by

$$q_r^{-\frac{7}{20}\tau} + \Big|\frac{1}{N}\sum_{x=1}^{N}\chi_1'(f_1(x))\Big|^{\frac{1}{2}}, \quad (3.8)$$

where f_1 is the $f_{y,y'}$ with the maximal character sum among all admissible pairs. i.e.

$$\Big|\sum_{x=1}^{N}\chi_1'(f_1(x))\Big| = \max_{\substack{f_{y,y'}\\ (f_{y,y'},q_r)\text{ admissible}}}\left|\sum_{x=1}^{N}\chi_1'(f_{y,y'}(x))\right|. \quad (3.9)$$

Thus, there exists $\bar{q}_1|q_r$, $\bar{q}_1 > q_r^{1-\tau}$ and for any $p|\bar{q}_1$, f_1 is p-good.

To bound the second term in (3.8), we will do induction on the number of characters in the factorization of χ and first prove the following.

Claim. For $s = 1, \cdots, r-1$, denote $\chi'_s = \chi_{s+1} \cdots \chi_r$. Let $f_s(x)$ be of the form $f_s(x) = \prod_j (x - b_j)^{c_j}$, where $b_j, c_j \in \mathbb{Z}$ and $\deg f_s \le 2^s$.
Denote $\bar{q}_0 = q_r$. Assume there is $\bar{q}_{s-1}|q_r$ such that $\bar{q}_{s-1} > q_r^{1-(s-1)\tau}$ and $(f_s, \bar{q}_{s-1})$ is admissible. Then

$$\frac{1}{N}\left|\sum_{x=1}^{N} \chi'_s(f_s(x))\right| \le q_r^{-\frac{\tau}{5}\cdot\frac{1}{2}} + \left|\frac{1}{N}\sum_{x=1}^{N} \chi'_{s+1}(f_{s+1}(x))\right|^{\frac{1}{2}}, \tag{3.10}$$

where f_{s+1} is of the same form as f_s with $\deg f_{s+1} \le 2^{s+1}$, and there is $\bar{q}_s|q_r$ such that $\bar{q}_s > q_r^{1-s\tau}$ and $(f_{s+1}, \bar{q}_s)$ is admissible.

Proof of Claim.

As before, the q_{s+1}-periodicity of χ_{s+1} and Cauchy-Schwarz inequality give a bound on the character sum in the left-hand-side of (3.10) by

$$\left[\frac{1}{NM^2}\sum_{y,\,y'=1}^{M}\left|\sum_{x=1}^{N}\chi'_{s+1}\left(\frac{f_s(x+q_{s+1}y)}{f_s(x+q_{s+1}y')}\right)\right|\right]^{1/2}. \tag{3.11}$$

Set

$$f_{s+1}(x) = \frac{f_s(x+q_{s+1}y)}{f_s(x+q_{s+1}y')}\,,$$

where (y, y') is chosen among all good pairs as in (3.9), such that the inner character sum in (3.11) is the maximum.

We want to bound the set of bad (y, y'). For $p|\bar{q}_s$,

$$f_s(x) = (x-a)^{\epsilon}\prod_j (x-b_j)^{c_j} \quad \text{for some } \epsilon \in \{-1, 1\}, \text{ where } a \neq b_j \bmod p.$$

Hence

$$f_{s+1}(x) = \left(\frac{x+q_{s+1}y-a}{x+q_{s+1}y'-a}\right)^{\epsilon}\prod_j\left(\frac{x+q_{s+1}y-b_j}{x+q_{s+1}y'-b_j}\right)^{c_j}.$$

For $y \neq y' \bmod p$, if $a - q_{s+1}y$ is not a simple root or pole, then

$$a - q_{s+1}y = b_j - q_{s+1}y' \mod p$$

for some j. Therefore, by the same reasoning as for (3.7),

$$\begin{aligned}
&\Big|\big\{(y,y')\in[1,M]^2 : (f_{s+1},\bar{q}_s) \text{ is not admissible }\big\}\Big| \\
&\leq \sum_{\substack{Q|\bar{q}_s \\ Q>q_r^\tau}} \Big|\big\{(y,y')\in[1,M]^2 : \forall p|Q, f_{s+1} \text{ is } p\text{-bad }\big\}\Big| \\
&\leq \sum_{\substack{Q|\bar{q}_s \\ Q>q_r^\tau}} \frac{M^2}{Q}\left(2^s\right)^{\omega(Q)} = M^2 \sum_{\substack{Q|\bar{q}_s \\ Q>q_r^\tau}} \frac{\left(2^s\right)^{\omega(Q)}}{Q}\,.
\end{aligned} \tag{3.12}$$

(In the above bound, the factor 2^s comes from the choices of b_j.)

By assumptions (i) and (iii),

$$\frac{\left(2^s\right)^{\omega(Q)}}{Q} \leq \prod_{p|Q}\frac{2^r}{p} < \prod_{p|Q}\frac{1}{\sqrt{p}} = \frac{1}{\sqrt{Q}} < {q_r}^{-\frac{\tau}{2}}, \tag{3.13}$$

and (3.12) is bounded by

$$M^2\,\frac{2^{\omega(q_r)}}{q_r^{\tau/2}} < M^2 q_r^{-\tau/5},$$

and the claim is proved. $\square$

At the last step of our induction, we are bounding

$$\Big|\sum_{x=1}^{N}\chi_r(f_{r-1}(x))\Big|, \tag{3.14}$$

where f_{r-1} is of the form as in the claim with $\deg f_{r-1}\leq 2^{r-1}$ and there is $\bar{q}_{r-2}|q_r$ such that $\bar{q}_{r-2} > q_r^{1-(r-2)\tau} > \sqrt{q}_r$ and $\forall p|\bar{q}_{r-2}$ is good. In particular, $(f_{r-1},\bar{q}_{r-2})$ is admissible and Remark 3.3 applies. $\big($Note that ${\bar{q}_{r-2}}^{-\frac{3}{10}}\ {q_r}^{\frac{3}{10}\tau} < {\bar{q}_{r-2}}^{-(\frac{3}{10}-\frac{3}{5}\tau)} < {\bar{q}_{r-2}}^{-\frac{1}{4}}$.$\big)$ Hence, we have

$$\Big|\sum_{x=1}^{N}\chi_r(f_{r-1}(x))\Big| < N{\bar{q}_{r-2}}^{-\frac{1}{4}} < N{q_r}^{-\frac{1}{8}},$$

and we reach the final bound

$$\begin{aligned}
&\frac{1}{N}\Big|\sum_{x=1}^{N}\chi(x)\Big| \\
&\leq q_r^{-7\tau/20} + q_r^{-\tau/10} + \cdots + \left(q_r^{-\tau/5}\right)^{1/2^{r-1}} + \left(q_r^{-1/8}\right)^{1/2^{r-1}} + O\left(\frac{Mq_1}{N}\right) \\
&\ll \left(q_r^{-\tau/5}\right)^{1/2^{r-1}} + \left(q_r^{-1/8}\right)^{1/2^{r-1}} \\
&\ll q_r^{-\frac{2}{\log\log q_r}\cdot\frac{1}{2^c\log\log q_r}} \\
&= e^{-\frac{\log q_r}{\log\log q_r\ (\log q_r)^c}} \\
&< e^{-\sqrt{\log q_r}}.
\end{aligned} \tag{3.15}$$

□

The proof of Theorem 3' also gives an argument for the following theorem.

Remark 3.4. Since in (iii) we assume that $c < 1/4-\epsilon$, from the last inequality in (3.15), we have proved the theorem for a better saving of $e^{(\log q_r)^{3/4}}$ instead of $e^{\sqrt{\log q_r}}$.

Theorem 3" *Assume $q = q_1 \dots q_r$ with $(q_i, q_j) = 1$ for $i \neq j$, and q_r square-free. Factor $\chi = \chi_1 \dots \chi_r$, where $\chi_i \pmod{q_i}$ is arbitrary for $i < r$, and primitive for $i = r$.*
We further assume

(i). *For all $p|q_r, p > \sqrt{\log q_r}$.*

(ii). For all i, $q_i < N^{1/3}$.

(iii). $r < c \log\log q$ for some $c < 1/4 - \epsilon$.

Let

$$f(x) = \prod_j (x - b_j)^{c_j}, \quad c_1 \in \{-1, 1\}, \ \ d = \deg f = \sum |c_j|.$$

Suppose that (f, q_r) is admissible (*as defined after the statement of Theorem 3'). Furthermore, assume*

(iv). $d = \deg f < \left(\log q_r\right)^{\frac{1}{8}}$.

Then

$$\Big|\sum_{x=1}^{N}\chi(f(x))\Big| \ll Ne^{-\sqrt{\log q_r}}.$$

Remark 3.5. To prove Theorem 3", one only needs to modify the proof of Theorem 3' slightly by multiplying $\frac{M^2}{Q}$ by $d^{\omega(Q)}$ in (3.7) and replacing 2^s (respectively, 2^r) by $2^{s-1}d$ (resp. $2^{r-1}d$) in (3.12) (resp. (3.13)).

4 Graham-Ringrose for mixed character sums.

The technique used to prove Theorem 1' may be combined with the method of Graham-Ringrose for Theorem 3' to bound short mixed character sums with highly composite modulus (see also [IK] p. 330–334).

Let $q = q_1 \dots q_r$ with $(q_i, q_j) = 1$ for $i \neq j$, and q_r square-free, such that (i) and (iii) of Theorem 3' hold .

Let

$$\chi = \chi_1 \cdots \chi_r,$$

where $\chi_i (\mathrm{mod}\ q_i)$ is arbitrary for $i < r$, and primitive for $i = r$.

Let $I \subset [1, q]$ be an interval of size $N < q$, and let $f(x) = \alpha_d x^d + \cdots + \alpha_0 \in \mathbb{R}[x]$ be an arbitrary polynomial of degree d.

Assuming (ii) of Theorem 3' and an appropriate assumption on d, we establish a bound on

$$\sum_{x\in I}\chi(x)e^{if(x)}. \tag{4.1}$$

The case $f = 0$ corresponds to Theorem 3'. The main idea to bound (4.1) is as follows. First, we repeat part of the proof of Theorem 3' in order to remove the factor $e^{if(x)}$ at the cost of obtaining a character sum with polynomial argument. Next, we invoke Theorem 3" to estimate these sums.

Write $q = q_1 Q_1$ with $Q_1 = q_2 \dots q_r$, and denote $\mathcal{Y}_1 = \chi_2 \dots \chi_r$.

Choose $M \in \mathbb{Z}$ such that

$$M \cdot \max q_i < N, \quad \text{and} \quad M < \sqrt{N}. \tag{4.2}$$

Using shifted product method as in (3.5), we have

$$\sum_{x\in I}\chi(x)e^{if(x)}=\frac{1}{M}\sum_{\substack{x\in I\\0\le y<M}}\chi(x+q_1y)e^{if(x+q_1y)}+O(q_1M), \tag{4.3}$$

$$\begin{aligned}\frac{1}{M}\Big|\sum_{\substack{x\in I\\0\le y<M}}\chi(x+q_1y)e^{if(x+q_1y)}\Big|&=\frac{1}{M}\Big|\sum_{\substack{x\in I\\0\le y<M}}\chi_1(x)\mathcal{Y}_1(x+q_1y)e^{if(x+q_1y)}\Big|\\&\le\frac{1}{M}\sum_{x\in I}\Big|\sum_{0\le y<M}\mathcal{Y}_1(x+q_1y)e^{if(x+q_1y)}\Big|.\end{aligned} \tag{4.4}$$

Next, we write

$$f(x+q_1y)=f_0(x)+f_1(x)y+\cdots+f_d(x)y^d.$$

Subdivide the unit cube $\mathbb{T}^{d+1}$ into cells $U_\alpha=B\big(\xi_\alpha,\frac{1}{M^{d+1}}\big)\subset\mathbb{T}^{d+1}$, $\xi_\alpha\in\mathbb{T}^{d+1}$.

Denote

$$\Omega_\alpha=\{x\in I:\big(f_0(x),\dots,f_d(x)\big)\in U_\alpha\ \bmod 1\}.$$

Hence, for $x\in\Omega_\alpha$

$$\begin{aligned}f(x+q_1y)&=\xi_{\alpha,0}+\xi_{\alpha,1}y+\cdots+\xi_{\alpha,d}y^d+O\Big(\frac{1}{M}\Big)\\e^{if(x+q_1y)}&=e^{i(\xi_{\alpha,0}+\cdots+\xi_{\alpha,d}y^d)}+O\Big(\frac{1}{M}\Big).\end{aligned} \tag{4.5}$$

The number of cells is

$$\sim\big(M^{d+1}\big)^{d+1}. \tag{4.6}$$

Substituting (4.5) in (4.4) gives

$$\begin{aligned}&\frac{1}{M}\sum_{x\in I}\Big|\sum_{0\le y<M}\mathcal{Y}_1(x+q_1y)e^{if(x+q_1y)}\Big|\\=&\frac{1}{M}\sum_{\alpha}\sum_{x\in\Omega_\alpha}\Big|\sum_{0\le y\le M}C_\alpha(y)\mathcal{Y}_1(x+q_1y)\Big|+O\Big(\frac{N}{M}\Big),\end{aligned} \tag{4.7}$$

where $|C_\alpha(y)| = 1$.

Next, applying Hölder's inequality to the triple sum in (4.7) with $k \in \mathbb{N}$, we have

$$\begin{aligned}&\sum_\alpha \sum_{x\in\Omega_\alpha} \Big| \sum_{0\le y\le M} C_\alpha(y)\mathcal{Y}_1(x+q_1y)\Big| \\ \le& N^{1-\frac{1}{2k}}\Big(\sum_\alpha\sum_{x\in I}\Big|\sum_{0\le y\le M} C_\alpha(y)\mathcal{Y}_1(x+q_1y)\Big|^{2k}\Big)^{\frac{1}{2k}}.\end{aligned}$$

Therefore, up to an error of $O(\frac{N}{M})$, (4.7) is bounded by

$$\begin{aligned}&N\left[\frac{1}{NM^{2k}}\left(M^{d+1}\right)^{d+1}\sum_{0\le y_1,\dots y_{2k}<M}\Big|\sum_{x\in I}\mathcal{Y}_1\Big(\frac{(x+q_1y_1)\cdots(x+q_1y_k)}{(x+q_1y_{k+1})\cdots(x+q_1y_{2k})}\Big)\Big|\right]^{\frac{1}{2k}} \\ =& N\left(M^{d+1}\right)^{\frac{d+1}{2k}}\left[\frac{1}{NM^{2k}}\sum_{0\le y_1,\dots,y_{2k}<M}\Big|\sum_{x\in I}\mathcal{Y}_1\big(R_{y_1,\dots,y_{2k}}(x)\big)\Big|\right]^{\frac{1}{2k}}, \qquad (4.8)\end{aligned}$$

where

$$R_{y_1,\dots,y_{2k}}(x) = \frac{(x+q_1y_1)\cdots(x+q_1y_k)}{(x+q_1y_{k+1})\cdots(x+q_1y_{2k})}.$$

To bound the double sum in (4.8), we apply Theorem 3" with $f(x) = R_{y_1,\dots,y_{2k}}(x)$ for those tuples $(y_1,\dots,y_{2k}) \in [0, M-1]^{2k}$ for which $(R_{y_1,\dots,y_{2k}}, q_r)$ is admissible. For the other tuples, we use the trivial bound. If $(R_{y_1,\dots,y_{2k}}, q_r)$ is not admissible, then there is a divisor $Q|q_r$, $Q > q_r^\tau$, such that for each $p|Q$, the set $\{\pi_p(y_1),\cdots,\pi_p(y_{2k})\}$ has at most k elements. Here π_p is the natural projection from $\mathbb{Z}$ to $\mathbb{Z}/p\mathbb{Z}$. We will estimate the contributions of $(y_1,\dots,y_{2k})$ for which $(R_{y_1,\dots,y_{2k}}, q_r)$ is not admissible by distinguishing the tuples $(y_1,\dots,y_{2k})$ according to the relative size of Q and its prime factors.

(a). *Suppose that there is $p|Q$ with $p > \sqrt{M}$.*

Then the number of p-bad tuples $(y_1,\dots,y_{2k})$ is bounded by

$$\binom{2k}{k} M^k k^k\Big(1+\frac{M}{p}\Big)^k < (4k)^k M^{\frac{3}{2}k}.$$

Indeed, one chooses a set I of k indices and specify the corresponding y_j; for the other indices, $\pi_p(y_j)$ is taken within $\{\pi_p(y_j) : j \in I\}$, and summing over the prime divisors of q_r gives

$$\omega(q_r)(4k)^k M^{\frac{3}{2}k} < M^{\frac{7}{4}k}, \qquad (4.9)$$

provided

$$50 \le k < M^{\frac{1}{5}}, \tag{4.10}$$

and

$$\log q_r < M. \tag{4.11}$$

(b). *Suppose $Q > M$ and $p \le \sqrt{M}$ for each $p|Q$.*

Take $Q_1|Q$ such that $\sqrt{M} < Q_1 \le M$. The number of tuples $(y_1, \dots, y_{2k})$ that are p-bad for each $p|Q_1$ is at most

$$\begin{aligned} &\Big(\frac{M}{Q_1}\Big)^{2k} \prod_{p|Q_1} \binom{2k}{k}\ p^k\ k^k \\ &< \Big(\frac{M}{Q_1}\Big)^{2k} \prod_{p|Q_1} (4kp)^k < \ (ck)^{k\omega(Q_1)} \frac{M^{2k}}{Q_1^k} < \ \frac{M^{2k}}{Q_1^{\frac{k}{3}}} < \ M^{\frac{11}{6}k}, \end{aligned}$$

provided

$$k < \min_{p|q_r} p^{\frac{1}{3}}. \tag{4.12}$$

Summing over all Q_1 as above gives the contribution

$$M^{\frac{11}{6}k+1} < M^{\frac{15}{8}k}. \tag{4.13}$$

(c). *Suppose $q_r^\tau < Q < M$.*

The number of tuples $(y_1, \dots, y_{2k})$ that are p-bad for all $p|Q$ is at most $M^{2k}/Q^{\frac{k}{3}}$, and summation over these Q gives the contribution

$$2^{\omega(q_r)}\ \frac{M^{2k}}{Q^{\frac{k}{3}}} < \frac{M^{2k}}{q_r\ ^{\frac{1}{4}k\tau}}. \tag{4.14}$$

Hence, in summary, the number of $(y_1, \dots, y_{2k})$ for which $(R_{y_1,\dots,y_{2k}}, q_r)$ is not admissible is at most

$$M^{2k}(M^{-\frac{k}{8}} + q_r^{\ -\frac{1}{4}k\tau}).$$

From (4.3)-(4.4) and (4.7)-(4.8) we obtain the estimate

$$\sum_{x\in I} \chi(x) e^{if(x)} < N\big(M^{d+1}\big)^{\frac{d+1}{2k}} \Big[M^{-\frac{k}{8}} + q_r^{\ -\frac{1}{4}k\tau} + e^{-\sqrt{\log q_r}}\ \Big]^{\frac{1}{2k}}$$

using Theorem 3" for the contribution of *good* tuples $(y_1, \dots, y_{2k})$. Here we need to assume

$$2k < \big(\log q_r\big)^{\frac{1}{8}}, \tag{4.15}$$

which also implies (4.10) and (4.12), under assumption (i) and if (4.11) holds.

Take $k = 50d^2$, assuming

$$d < \frac{1}{10}\Big(\log q_r\Big)^{\frac{1}{16}}, \tag{4.16}$$

(which implies (4.15),) then

$$\begin{aligned}\sum_{x\in I}\chi(x)e^{if(x)} &< NM^{\frac{(d+1)^2}{2k}}\Big(M^{-\frac{1}{16}} + e^{-\frac{\sqrt{\log q_r}}{2k}}\Big)\\ &< N\bigg(M^{-\frac{1}{1600}} + \bigg(\frac{M^{(d+1)^2}}{e^{\sqrt{\log q_r}}}\bigg)^{\frac{1}{100d^2}}\bigg).\end{aligned}$$

Choose

$$M = \Big[\exp\Big(\frac{\sqrt{\log q_r}}{2(d+1)^2}\Big)\Big].$$

(So (4.11) is also satisfied.) We have

$$\sum_{x\in I}\chi(x)e^{if(x)} < Ne^{-\frac{\sqrt{\log q_r}}{200d^2}}.$$

Thus we proved

Theorem 4. *Assume $q = q_1 \dots q_r$ with $(q_i, q_j) = 1$ for $i \neq j$, and q_r square-free. Factor $\chi = \chi_1 \dots \chi_r$, where $\chi_i (\mathrm{mod}\ q_i)$ is arbitrary for $i < r$, and primitive for $i = r$.*

We further assume

(i). *For all $p|q_r, p > \sqrt{\log q_r}$.*

(ii). *For all i, $q_i < N^{1/3}$.*

(iii). *$r < c \log\log q$ for some $c < 1/4 - \epsilon$.*

Let $f(x) \in \mathbb{R}[x]$ be an arbitrary polynomial of degree d. Assume

$$d < \frac{1}{10}\Big(\log q_r\Big)^{\frac{1}{16}}.$$

Then

$$\Big|\sum_{n\in I} e^{if(n)}\chi(n)\Big| < CNe^{-\frac{\sqrt{\log q_r}}{200d^2}}, \tag{4.17}$$

where I is an interval of size N.

Combined with Postnikov (as in the proof of Theorem 2), Theorem 4 then implies

Theorem 4' *Suppose $q = q_0 \dots q_r$ with $(q_i, q_j) = 1$ for $i \neq j$, and q_r square-free. Assume $\bar{q}_0 | q_0$ and $q_0 | (\bar{q}_0)^m$ for some $m \in \mathbb{N}$, and*

$$m < \frac{1}{20}\Big(\log q_r\Big)^{\frac{1}{16}}.$$

Factor $\chi = \chi_0 \dots \chi_r$, where $\chi_i (\mathrm{mod}\ q_i)$ is arbitrary for $i < r$, and primitive for $i = r$.

We further assume

(i). *For all $p | q_r, p > \sqrt{\log q_r}$.*

(ii). *For all i, $q_i < \big(N/\bar{q}_0\big)^{1/3}$.*

(iii). *$r < c \log\log q$ for some $c < 1/4 - \epsilon$.*

Then

$$\Big|\sum_{n\in I} \chi(n)\Big| < CNe^{-\frac{\sqrt{\log q_r}}{800m^2}}, \tag{4.18}$$

where I is an interval of size N.

Note that for Theorem 4' to provide a nontrivial estimate, we should assume at least

$$r \ll \log\log q_r$$

and

$$\log m \ll \log\log q_r.$$

5 The main theorem.

Theorem 4' as a consequence of Theorem 4 was stated mainly for expository reason. (cf. §7. Proposition 7.) Our goal is to develop this approach further in order to prove the following stronger result.

Theorem 5. *Assume N satisfies*

$$q > N > \max_{p|q} p^{10^3} \tag{5.1}$$

and

$$\log N > (\log q)^{1-c} + C \log\left(2\frac{\log q}{\log q'}\right) \frac{\log q'}{\log\log q}\ , \tag{5.2}$$

where $C, c > 0$ are some constants, (e.g. we may take $c = 10^{-3}$ and $C \sim 10^3$) and $q' = \prod_{p|q} p$.

Let χ be primitive (mod q) *and I an interval of size N. Then*

$$\Big|\sum_{x\in I} \chi(x)\Big| \ll N e^{-(\log N)^{3/5}}. \tag{5.3}$$

We will prove Theorem 5 in the next two sections. In this section, we make some further technical specifications which will be important in the proof. Also, we discuss assumption (5.2) and compare it with the assumptions in known results. Some of the remarks at the end of this section (Remarks 5.2 and 5.3) will be used in the proof as well.

Claim. We may make the following assumptions.

(1.) $q' > N^{\frac{1}{200}}$

(2.) $q = Q\ q_r = Q_1 \cdots Q_{r-1}\ q_r$, where $(Q_i, Q_j) = (Q_i, q_r) = 1$, (5.4)

$$r = 1 + 10\left[\frac{\log Q'}{\log N}\right], \tag{5.5}$$

(where Q' is the core of Q,) and

$$q_r = q_0^m,\ \ q_0 \text{ square-free} \tag{5.6}$$

with

$$e^{(\log N)^{\frac{3}{4}}} < q_0 < N^{\frac{1}{10}}, \tag{5.7}$$

$$m \le (\log N)^{3c}. \tag{5.8}$$

Also, the core of Q_s satisfies

$$Q_s' < N^{\frac{1}{5}} \ \text{ for } s = 1, \ldots, r-1. \tag{5.9}$$

Moreover, we may assume

$$\forall p|q_r, \;\; p > \sqrt{\log q_r}. \tag{5.10}$$

(3.) There exist $q_1, \cdots, q_{r-1}$, $(q_i, q_j) = (q_i, q_r) = 1$,

$$\max_i q_i < N^{1/2}, \tag{5.11}$$

such that

$$q = Q_1 \cdots Q_{r-1} q_r \mid q_1^{m_1} \cdots q_{r-1}^{m_{r-1}} q_r, \tag{5.12}$$

with

$$m_s = 10 \left[\frac{\log Q_s}{\log N} \right]. \tag{5.13}$$

Proof of Claim.

To verify Assumption (1), we will obtain the bound (5.3) for the case $q' \leq N^{\frac{1}{200}}$ by using Theorem 12.16 in [IK]. The latter provides the following bound

$$\Big| \sum_{M < x \leq \widetilde{M}} \chi(x) \Big| < C^{s(\log s)^2} M^{1 - \frac{c}{s^2 \log s}} \tag{5.14}$$

with $s = \frac{\log q}{\log M}$, assuming that $q'^{100} < M < \widetilde{M} \leq 2M$. This gives a nontrivial bound $M^{1-\frac{c}{s^2 \log s}}$ provided $\log M \gtrsim (\log q)^{\frac{3}{4}+\epsilon}$. We will use this result by dividing our interval $[1, N]$ dyadically.

Let $M_1 = Ne^{-\sqrt{\log N}}$, $M_i = 2^{i-1} M_1$ and $s_i = \frac{\log q}{\log M_i}$, for $i = 2, \cdots, m = \sqrt{\log N}$.

We divide $[1, N]$ into subintervals

$$[1, N] = [1, M_1] \bigcup_{i=1}^{m-1} (M_i, M_{i+1}],$$

and note that $M_i > N^{1/2} > q'^{100}$, and $\log M_i \sim \log N$. Hence $s_i \sim \frac{\log q}{\log N} := r$ for $i \geq 1$.

We bound the character sum $\sum_{i=1}^{N} \chi(x)$ by bounding subsum over each subinterval, using the trivial bound for the interval $[1, M_1]$ and Theorem

12.16 in [IK] for the intervals $(M_i, M_{i+1}]$. It is straightforward to check that the sum of all bounds is bounded by

$$Ne^{-\sqrt{\log N}} + m\ M_m^{1-\frac{c}{r^2\log r}} \ll Ne^{-\sqrt{\log N}},$$

if $\log N \gtrsim (\log q)^{\frac{4}{5}+\epsilon}$, which follows from (5.2).

To see Assumption (2), we first note that

$$\prod_{\nu_p > (\log N)^{3c}} p < q^{(\log N)^{-3c}} < e^{(\log N)^{1-c}} < q'^{\frac{1}{200}}, \tag{5.15}$$

where ν_p is the exponent of p in the prime factorization of q. In the display above, the second inequality follows from (5.2) (which implies that $\log q < (\log N)^{1+2c}$), and the last inequality follows from Assumption (1) in the claim and provided $\log q'$ is sufficiently large.

From

$$\prod_{m=1}^{(\log N)^{3c}} \Big(\prod_{\nu_p = m} p\Big) > q'^{\frac{99}{100}}, \tag{5.16}$$

there exists $m \le (\log N)^{3c}$ such that

$$\prod_{\nu_p = m} p > (q')^{\frac{1}{2}(\log N)^{-3c}} > e^{\frac{1}{400}(\log N)^{1-3c}} > e^{(\log N)^{\frac{3}{4}}}.$$

The second inequality in Assumption (5.1) ensures that we may take

$$q_0 \Big| \prod_{\nu_p = m} p \quad \text{such that} \quad q_0 < N^{\frac{1}{10}}.$$

Therefore, there exists a q_r which satisfies (5.6)-(5.8).

To see (5.10), we note that in the inner product in (5.16), we may impose the condition that $p > \sqrt{\log q_r}$, because

$$\prod_{p < \sqrt{\log q_r}} p < e^{2\sqrt{\log q_r}} < e^{(\log N)^{\frac{2}{3}}} < q'^{\frac{1}{200}}. \tag{5.17}$$

(The second inequality follows from (5.6)-(5.8).)

Write $q = Q\, q_r$, and

$$Q = \prod p_i^{\nu_i}, \quad \text{where } \nu_i := \nu_{p_i} \text{ and } \nu_1 \geq \nu_2 \geq \cdots .$$

Let $Q' = \prod_{\nu_i \geq 1} p_i$ be the core of Q, and factor

$$Q' = Q'_1 \cdots Q'_{r-1} \text{ such that } Q'_s < N^{\frac{1}{5}} \text{ and } r = 1 + 10\left[\frac{\log Q'}{\log N}\right].$$

For each s, define $Q_s = \prod_{p|Q'_s} p^{\,\nu_p}$ and $q_s = \prod_{p|Q'_s} p^{\,\bar{\nu}_p}$ as follows

$$\bar{\nu}_p = \begin{cases} \left[\frac{\nu_p}{m_s}\right] + 1, \text{ if } \nu_p > m_s \\ 1, \quad \text{otherwise} \end{cases} \tag{5.18}$$

Denote

$$m_s = 10\frac{\log Q_s}{\log N}.$$

It follows that $Q_s | (q_s)^{m_s}$ and $q_s < Q'_s Q_s^{\frac{2}{m_s}} < N^{\frac{1}{2}}$, which are (5.11)-(5.12).

Remark 5.1. Assumption (5.2) can be reformulated as

$$\Big(3\,\frac{\log q}{\log q' N}\Big)^{10\frac{\log Nq'}{\log N}} < (\log N)^c. \tag{5.19}$$

Remark 5.2. Using (5.4), (5.19) and the inequality of arithmetic and geometric means, one can show that

$$\prod_{i=1}^{r-1} m_i < \big(\log q_0\big)^{\frac{1}{75}}. \tag{5.20}$$

Remark 5.3. It is easy to check that (5.2) and (5.7) imply

$$r < 10^{-3} \log\log q_0. \tag{5.21}$$

Remark 5.4. If $\log q' \leq \log N$, (5.19) becomes

$$\log N > (\log q)^{1-c},$$

which is similar to Theorem 12.16 in [IK].

Remark 5.5. If $q = q'$ (i.e. q is square-free), condition (5.19) becomes

$$\frac{\log q}{\log\log q} < c \log N.$$

This is slightly better than Corollary 12.15 in [IK] and essentially optimal in view of the Graham-Ringrose argument.

6 The proof of Theorem 5.

The following lemma is the technical part of the inductive step. It is based on the techniques proving Theorem 2 and Theorem 4, which are shifting product and averaging (Graham-Ringrose), replacing χ_i by an additive character of a polynomial(Postnikov), and the mixed character technique to drop the additive character.

Lemma 6. *Assume*

(*a*). $q = q_1^m \hat{q}$, *where* $\hat{q} = \hat{\hat{q}} q_r$, *with* $q_1, \hat{\hat{q}}, q_r$ *mutually coprime.*

(*b*). $\chi = \chi_1 \hat{\chi}$, *with* $\chi_1 (\mathrm{mod}\ q_1^m)$ *and* $\hat{\chi} (\mathrm{mod}\ \hat{q})$.

(*c*). $f(x) = \prod_{\alpha=1}^{\beta} (x - a_\alpha)^{d_\alpha}$, $d = \sum |d_\alpha|$, *with* $a_\alpha \in \mathbb{Z}$ *distinct and* $d_\alpha \in \mathbb{Z} \backslash \{0\}$.

(*d*). *there exists* $\bar{q} | q_r$ *such that for each* $p | \bar{q}$, $p > \sqrt{\log q_r}$ *and* f *is* p*-good.*

(*e*). I *an interval of length* N, $q_1^2 < N < q$, $1440 \cdot m^2 d < (\log N)^{\frac{1}{5}}$.

(*f*). $M \in \mathbb{Z}$, $\log N + \log \bar{q} < M < N^{\frac{1}{10}}$, $M < \bar{q}^{\,\tau}$.

Then

$$\frac{1}{N} \Big| \sum_{x \in I} \chi\big(f(x)\big) \Big| < M^{-1/15} + M^{\frac{1}{60}} \Big| \frac{1}{N} \sum_{x \in I} \hat{\chi}\big(f_1(x)\big) \Big|^{\frac{1}{60m^2}}, \tag{6.1}$$

where $f_1(x)$ *is of the form*

$$f_1(x) = \frac{\prod_{\nu=1}^{k} f(x + q_1 t_\nu)}{\prod_{\nu=k+1}^{2k} f(x + q_1 t_\nu)} = \prod_{\alpha'=1}^{\beta'} (x - b_{\alpha'})^{d_{\alpha'}} \tag{6.2}$$

with $b_{\alpha'}, d_{\alpha'} \in \mathbb{Z}$, $2k = 60m^2$ *and*

$$d^{(1)} := \sum |\ d_{\alpha'}\ | \leq 60\ d\ m^2. \tag{6.3}$$

Furthermore, $(f_1, \bar{q})$ *is admissible.*

Proof. Take $t \in [1, M]$. Clearly,

$$\chi\big(f(x + tq_1)\big) = \chi_1\big(f(x)\big) \chi_1\bigg(1 + \frac{f(x + tq_1) - f(x)}{f(x)}\bigg) \hat{\chi}\big(f(x + tq_1)\big). \tag{6.4}$$

Hence, as in the proof of Theorem 2,

$$\chi\big(f(x+tq_1)\big) = \chi_1\big(f(x)\big)\hat{\chi}\big(f(x+tq_1)\big)e_{q_1^m}\Big(\sum_{j=1}^{m-1} Q_j(x)\ q_1^j\ t^j\Big), \tag{6.5}$$

where

$$Q_j(x) = \frac{1}{j!}\frac{d^j}{dt^j}\Big\{F\Big(\frac{f(x+t)-f(x)}{f(x)}\Big)\Big\}\Big|_{t=0} \tag{6.6}$$

with

$$F(x) = \sum_{s=1}^{2m}(-1)^{s-1}\frac{1}{s}x^s \qquad \text{(up to a factor)}. \tag{6.7}$$

We estimate $\sum_{x\in I}\chi(f(x))$ by the same technique as used in the proof of Theorem 4 with $d = m-1$ (see (4.3)-(4.8)). After averaging and summing over $t \in M$, and applying Hölder's inequality, we remove the last factor in (6.5) and obtain

$$\frac{1}{N}\left|\sum_{x\in I}\chi(f(x))\right| \ll \left[\frac{M^{\,m^2}}{NM^{2k}}\sum_{0\le t_1,\dots,t_{2k}<M}\Big|\sum_{x\in I}\hat{\chi}\big(R_{t_1,\dots,t_{2k}}(x)\big)\Big|\right]^{\frac{1}{2k}}. \tag{6.8}$$

Here

$$R_{\underline{t}}(x) := R_{t_1,\dots,t_{2k}}(x) = \frac{f(x+q_1t_1)\cdots f(x+q_1t_k)}{f(x+q_1t_{k+1})\cdots f(x+q_1t_{2k})}.$$

Choose $\underline{t} = (t_1,\cdots,t_{2k}) \in [1,M]^{2k}$ such that $f_1(x) = R_{\underline{t}}(x)$ maximizes the inner character sum in the right-hand-side of (6.8) among all admissible $(R_{\underline{t}},\bar{q})$. Let $\mathcal{B}$ be the set of $\underline{t}$ such that $(R_{\underline{t}},\bar{q})$ is not admissible. Since in (f), we assume $2k = 60m^2$, (6.8) gives

$$\frac{1}{N}\Big|\sum_{x\in I}\chi(f(x))\Big| \ll M^{\frac{1}{60}-1}|\mathcal{B}|^{\frac{1}{2k}} + M^{\frac{1}{60}}\Big|\frac{1}{N}\sum_{x\in I}\hat{\chi}\big(f_1(x)\big)\Big|^{\frac{1}{60m^2}}. \tag{6.9}$$

We want to give an upper bound on $|\mathcal{B}|$.

Claim. $|\mathcal{B}| \ll M^{2k-\frac{k}{6}}$..

Proof of Claim. First, we observe that the zeros or poles of $R_{\underline{t}}(x)$ are of the form

$$b_{\alpha'} := a_\alpha - t_\nu q_1 \ \text{ with } t_\nu \in [1,M]. \tag{6.10}$$

Second, we note that while applying Hölder's inequality to obtain (6.8), we take $k \in \mathbb{Z}^+$ satisfying

$$48kd < \big(\log N\big)^{\frac{1}{10}} \text{ and } k > 30. \tag{6.11}$$

To bound $|\mathcal{B}|$, we fix $p|\bar{q}$. In $R_{\underline{t}}(x) = \prod_{\alpha'=1}^{\beta'}(x - b_{\alpha'})^{d_{\alpha'}}$, we may assume $d_1 = 1$ and $a_1 \neq a_\alpha \pmod p$ for any $\alpha > 1$. Recalling (6.10), assume that none of the $a_1 - t_\nu q_1, 1 \leq \nu \leq 2k$, is simple (mod p). This means that for each ν there is a pair $(\alpha(\nu), \sigma(\nu))$ in $\{1, \dots, \beta\} \times \{1, \dots, 2k\}$ such that $\alpha(\nu) \neq 1$, $\sigma(\nu) \neq \nu$ and

$$a_1 - t_\nu q_1 \equiv a_{\alpha(\nu)} - t_{\sigma(\nu)} q_1 \pmod p. \tag{6.12}$$

The important point is that $\sigma(\nu) \neq \nu$ for all ν, by assumption on a_1. One may therefore obtain a subset $S \subset \{1, \dots, 2k\}$ with $|S| = k$ such that there exists $S_1 \subset S$ with $|S_1| = \frac{k}{2}$ and

$$S_1 = \{\nu \in S : \sigma(\nu) \notin S_1\}. \tag{6.13}$$

(The existence of S and S_1 satisfying this property is justified in Fact 6.1 following the proof of this lemma.)

Specifying the values of $t_{\nu'}$ for those $\nu' \in \{1, \cdots, 2k\} \backslash S_1$, equations (6.12) will determine the remaining values, after specification of $\alpha(\nu)$ and $\sigma(\nu)$. An easy count shows that

$$\begin{aligned} &\big|\{\pi_p(\underline{t}) : \ R_{\underline{t}} \ \text{ is } p\text{-bad } \}\big| \\ &\leq \binom{2k}{k} \ \binom{k}{\frac{k}{2}} \left(\frac{3}{2}\, k\right)^{\frac{k}{2}} \left(\frac{\beta}{2}\right)^{\frac{k}{2}} \big(\mathcal{M}\big)^{\frac{3k}{2}} < (48kd)^{\frac{k}{2}} \big(\mathcal{M}\big)^{\frac{3k}{2}}, \end{aligned} \tag{6.14}$$

where $\mathcal{M} = \min(M, p)$. The first factor counts the number of sets S, the second the number of sets S_1, and the third and the forth the numbers of maps $\sigma|_{S_1}$ and $\alpha|_{S_1}$.

Applying assumptions (e)-(f) to (6.14), we obtain

$$\big|\{\pi_p(\underline{t}) : \ R_{\underline{t}} \ \text{ is } p\text{-bad } \}\big| < \big(\mathcal{M}\big)^{\frac{8}{5}k}. \tag{6.15}$$

If $(R_{\underline{t}}, \bar{q})$ is not admissible, there is some $Q|\bar{q}$, $Q > q_r^\tau > \bar{q}^{\,\tau}$ such that for each $p|Q$, $R_{\underline{t}}$ is p-bad. As in the proof of Theorem 4, we distinguish several cases.

(*a*). *There is* $p|Q$ *with* $p > M$.

Hence, $\big|\{\underline{t} \in [1,M]^{2k} : R_{\underline{t}} \text{ is } p\text{-bad }\}\big| < M^{\frac{8}{5}k}$ and summing over p gives the contribution $M^{\frac{8}{5}k}\log\bar{q}$.

(*b*). $\sqrt{M} < \max\limits_{p|Q} p < M$.

Then

$$\begin{aligned}&\big|\{\underline{t} \in [1,M]^{2k} : R_{\underline{t}} \text{ is } p\text{-bad }\}\big|\\ \le&\Big(\frac{M}{p}+1\Big)^{2k}\big|\{\pi_p(\underline{t}) : R_{\underline{t}} \text{ is } p\text{-bad }\}\big|\\ \le&\Big(\frac{M}{p}+1\Big)^{2k}p^{\frac{8}{5}k} < M^{2k}\Big(\frac{p}{32}\Big)^{-\frac{2}{5}k} < (4M)^{\frac{9}{5}k}.\end{aligned}$$

Summing over p gives the contribution $(4M)^{\frac{9}{5}k}\log\bar{q}$.

(*c*). $\max\limits_{p|Q} p \le \sqrt{M}$ *and* $Q > M$.

Take $Q_1|Q$ such that $\sqrt{M} < Q_1 < M$. Then

$$\begin{aligned}&\big|\{\underline{t} \in [1,M]^{2k} : R_{\underline{t}} \text{ is } p\text{-bad for each } p|Q_1\}\big|\\ \le&\Big(\frac{M}{Q_1}+1\Big)^{2k}\big|\{\pi_{Q_1}(\underline{t}) : R_{\underline{t}} \text{ is } p\text{-bad for each } p|Q_1\}\big|\\ \le&\Big(\frac{M}{Q_1}+1\Big)^{2k}\prod_{p|Q_1}p^{\frac{8}{5}k} < M^{2k}\Big(\frac{Q_1}{32}\Big)^{-\frac{2}{5}k} < (4M)^{\frac{9}{5}k}.\end{aligned}$$

Summing over Q_1 gives the contribution $(4M)^{\frac{9}{5}k+1}$.

Summing up cases (a)-(c) and recalling assumption (f), we conclude that

$$\begin{aligned}|\mathcal{B}| &= \big|\{\underline{t} \in [1,M]^{2k} : (R_{\underline{t}},\bar{q}) \text{ is not admissible }\}\big|\\ &< M^{2k}\big(M^{-\frac{k}{6}} + \bar{q}^{\,\frac{-\tau k}{5}}\big) \ll M^{2k-\frac{k}{6}}. \quad \square\end{aligned} \tag{6.16}$$

Putting (6.9) and (6.16) together, we obtain (6.1) and the lemma is proved.

Fact 6.1. *Let* $\mathcal{K} = \{1,\cdots,2k\}$ *and* $\sigma : \mathcal{K} \to \mathcal{K}$ *be a function such that* $\sigma(\nu) \neq \nu$ *for all* $\nu \in \mathcal{K}$. *Then there exist subsets* $S_1 \subset S \subset \mathcal{K}$ *with* $|S_1| = \frac{k}{2}$, $|S| = k$ *and* $\sigma(\nu) \notin S_1$ *for any* $\nu \in S$.

Proof. Since the subset of elements of $\mathcal{K}$ with more than one pre-image of σ has size $\leq k$, there exists a subset $S \subset \mathcal{K}$ with $|S| = k$ such that every $\nu \in S$ has at most one pre-image. To construct $S_1 \subset S$, we choose $\nu_i \in S$ inductively, such that $\nu_i \notin \{\nu_1, \dots, \nu_{i-1}, \sigma(\nu_1), \dots, \sigma(\nu_{i-1})\} \bigcup \sigma^{-1}(\{\nu_1, \dots, \nu_{i-1}\})$ and $\sigma(\nu_i) \notin S_1$. $\square$

Proof of Theorem 5.

Following the claim in §5, we will prove the theorem for $\chi = \chi_1 \cdots \chi_r$, where $\chi_i (\mathrm{mod}\ q_i^{m_i})$ is arbitrary for $i < r$, and primitive for $i = r$, and $q = q_1^{m_1} \cdots q_{r-1}^{m_{r-1}} q_r$ satisfies (3) of the claim. We will apply lemma 6 repeatedly. First, we choose $M_1 < M_2 < \cdots < M_{r-1}$ a sequence of values of M, which will satisfy condition (6.19). Then we will iterate (6.1), losing a factor χ_i in χ and adding an error term $M_i^{-1/12}$ in the bound each time.

In order to satisfy Assumption (e), we assume

$$1440 \cdot 60^{r-1} \prod_{i=1}^{r} (m_i^2) < \big(\log N\big)^{\frac{1}{5}}, \tag{6.17}$$

which follows from (5.20) and (5.21).

Let

$$M = e^{(\log q_r)^{9/10}}, \tag{6.18}$$

and for $s = 1, \cdots, r-1$, take M_s, such that

$$\begin{aligned} M_1^{-\frac{1}{15}} &= M^{-1} \\ M_1^{\frac{1}{60}} M_2^{\frac{1}{60^2 m_1^2}} \cdots M_{s-1}^{\frac{1}{60^{s-1} m_1^2 \cdots m_{s-2}^2}} M_s^{-\frac{1}{15 \cdot 60^{s-1} m_1^2 \cdots m_{s-1}^2}} &= M_1^{-\frac{1}{15}}. \end{aligned} \tag{6.19}$$

One checks recursively that

$$M_s \leq M^{5^{s-1} \cdot 15^s m_1^2 \cdots m_{s-1}^2}. \tag{6.20}$$

Indeed, from (6.19),

$$M_{s-1}^{\frac{1}{15 \cdot 60^{s-2} m_1^2 \cdots m_{s-2}^2}} = M_{s-1}^{\frac{-1}{60^{s-1} m_1^2 \cdots m_{s-2}^2}} M_s^{\frac{1}{15 \cdot 60^{s-1} m_1^2 \cdots m_{s-1}^2}}.$$

Therefore, by induction

$$M_s = M_{s-1}^{75 m_{s-1}^2} \leq M^{5^{s-2} \cdot 15^{s-1} m_1^2 \cdots m_{s-2}^2 (75 m_{s-1}^2)} = M^{5^{s-1} \cdot 15^s m_1^2 \cdots m_{s-1}^2}.$$

In order to satisfy the last condition in Assumption (f) of Lemma 6, we assume

$$\sum_{i=1}^{r-1} \log m_i < \frac{1}{40} \log\log q_r, \tag{6.21}$$

(Clearly, this follows from (5.20).) and note that

$$M^{(5\cdot 15)^{r-1} m_1^2 \cdots m_{r-2}^2} < q_r^{\tau} = q_r^{\frac{10}{\log\log q_r}}. \tag{6.22}$$

(Since by (5.21), $r < 10^{-3} \log\log q_r$.)

By (6.1) and iteration, $\frac{1}{N}\big|\sum_{x=1}^{N} \chi(x)\big|$ is bounded by

$$\begin{aligned} M_1^{-\frac{1}{15}} + M_1^{\frac{1}{60}} M_2^{-\frac{1}{15\cdot 60 m_1^2}} + M_1^{\frac{1}{60}} M_2^{\frac{1}{60^2 m_1^2}} M_3^{-\frac{1}{15\cdot 60^2 m_1^2 m_2^2}} + \cdots \\ + M_1^{\frac{1}{60}} M_2^{\frac{1}{60^2 m_1^2}} \cdots M_{r-2}^{\frac{1}{60^{r-2} m_1^2 \cdots m_{r-3}^2}} M_{r-1}^{-\frac{1}{15\cdot 60^{r-2} m_1^2 \cdots m_{r-2}^2}} \\ + M_1^{\frac{1}{60}} M_2^{\frac{1}{60^2 m_1^2}} \cdots M_{r-1}^{\frac{1}{60^{r-1} m_1^2 \cdots m_{r-2}^2}} \mathcal{S}^{\frac{1}{60^{r-1} m_1^2 \cdots m_{r-1}^2}}, \end{aligned} \tag{6.23}$$

where $\mathcal{S}$ is of the form

$$\mathcal{S} = \frac{1}{N}\Big|\sum_{x=1}^{N} \chi_r(f(x))\Big|, \tag{6.24}$$

with χ_r primitive modulo q_r, and

$$\begin{aligned} f(x) = \prod_{\alpha=1}^{\beta} (x - a_\alpha)^{d_\alpha}, a_\alpha, d_\alpha \in \mathbb{Z}, \\ d = \sum \mid d_\alpha \mid < 60^r m_1^2 \ldots m_r^2, \end{aligned} \tag{6.25}$$

and $(f, \bar{q})$ admissible for some $\bar{q} | q_r$, $\bar{q} > \sqrt{q_r}$.

Condition (6.19) ensures that each of the $r-1$ fist terms in (6.23) is bounded by $\frac{1}{M}$.

Applying (6.20) to (6.23) gives

$$\frac{1}{N}\big|\sum_{x=1}^{N} \chi(x)\big| < \frac{r-1}{M} + M^{(\frac{5}{4})^{r-1}-1} \mathcal{S}^{\frac{1}{60^{r-1} m_1^2 \cdots m_{r-1}^2}}. \tag{6.26}$$

We will continue the proof of the theorem in the next section by distinguishing two cases.

7 The two cases.

To finish the proof of Theorem 5, we need to bound $\mathcal{S}$ in (6.26). We will use Claim (2) in §5. Recall (5.6) that

$$q_r = q_0^m, \quad q_0 \text{ square-free .}$$

We will do induction on m.

Case 1. $m = 1$.

Since $(f, \bar{q})$ is admissible and $\bar{q}$ is square-free, we may apply Remark 3.3 to bound $\mathcal{S}$. Therefore,

$$\mathcal{S} < \bar{q}^{-\frac{3}{10}} q_r^{\frac{3}{10}\tau} < q_r^{-\frac{1}{7}}, \tag{7.1}$$

and by (6.26)

$$\frac{1}{N}\Big|\sum_{x=1}^{N}\chi(x)\Big| < \frac{r-1}{M} + M^{(\frac{5}{4})^{r-1}-1} q_r^{-\frac{1}{7\cdot 60^{r-1} m_1^2 \cdots m_{r-1}^2}} < \frac{r}{M}. \tag{7.2}$$

The last inequality is by (5.20) in Remark 5.2 and (6.22).

Now we use (6.18) and (5.21) to bound (7.2) and (5.6)-(5.8) to obtain (5.3). $\square$

We state the above case as a proposition for its own interest.

Proposition 7. *Assume* $q = q_1^{m_1} \dots q_{r-1}^{m_{r-1}} q_r$ *with* $(q_i, q_j) = 1$ *for* $i \neq j$, q_r *square-free and*

$$\prod_{i=1}^{r-1} m_i < \Big(\log q_r\Big)^{\frac{1}{75}}. \tag{7.3}$$

Factor $\chi = \chi_1 \dots \chi_r$, *where* $\chi_i (\mathrm{mod}\ q_i^{m_i})$ *is arbitrary for* $i < r$, *and primitive for* $i = r$.

We further assume

(i). *For all* $p | q_r, p > \sqrt{\log q_r}$.

(ii). *For all* i, $q_i^2 < N < q$.

(iii). $r < 10^{-3} \log\log q_r$.

Then

$$\Big|\sum_{x\in I}\chi(x)\Big| < Ne^{-(\log q_r)^{4/5}}, \tag{7.4}$$

where I is an interval of size N.

Case 2. $m > 1$.

In this situation, we follow the analysis in the proof of Lemma 6. (Particularly, see (6.4)-(6.7).) To bound $\mathcal{S}$ in (6.23), we will use Postnikov's theorem and Vinogradov's lemma ([Ga], Lemma 4) rather than Weil's estimate (Remark 3.3) as we did in Case 1. Recall

$$\mathcal{S} = \frac{1}{N}\Big|\sum_{n=1}^{N}\chi_r(f(n))\Big|,$$

with χ_r primitive modulo q_r, and

$$f(x) = \prod_{\alpha=1}^{\beta}(x-a_\alpha)^{d_\alpha} \quad \text{with } d \le 60^r m_1^2\dots m_r^2, \tag{7.5}$$

where $f(x)$ satisfies the property that for all $p|q_0$, $f(x)$ is p-good.

Write $n \in [1,N]$ as $n = x + tq_0$, with $1 \le x \le q_0$ and $1 \le t \le \frac{N}{q_0}$. Then as in (6.4) and (6.6),

$$\begin{aligned} N\cdot\mathcal{S} &= \sum_{x=1}^{q_0}\sum_{t=1}^{N/q_0}\chi_r\big(f(x)\big)e_{q_0^m}\Big(\sum_{j=1}^{m-1}Q_j(x)q_0^jt^j\Big) \\ &\le \sum_{x=1}^{q_0}\Big|\sum_{t=1}^{N/q_0}e_{q_0^m}\Big(\sum_{j=1}^{m-1}Q_j(x)q_0^jt^j\Big)\Big|. \end{aligned} \tag{7.6}$$

We want to find some information on the coefficients Q_j in (6.5). We may assume in (7.5) that $a_1 = 0$ is a simple zero or pole of f; replacing f by $\frac{1}{f}$ (which we may by replacement of χ by $\bar{\chi}$), hence

$$f(x) = xg(x) = x\prod_{a_\alpha\neq 0}(x-a_\alpha)^{d_\alpha} \qquad \bmod p \tag{7.7}$$

with $g(0)$ defined and non-vanishing (mod p).

From (6.6), (6.7), and (7.7), we have

$$j!Q_j(x) = \sum_s (-1)^{s-1} \frac{1}{s(xg(x))^s} \frac{d^j}{dt^j} \big[\big((x+t)g(x+t) - xg(x) \big)^s \big] \Big|_{t=0}. \quad (7.8)$$

Let $G(t) = (x+t)g(x+t) - xg(x)$. Since $G(t)$ divides $\frac{d^j}{dt^j} G(t)^s$ for $s > j$, and $G(0) = 0$, in (7.8) only the terms $s \leq j$ contribute and Q_j has a pole at 0 of order j. Write

$$C \cdot Q_j(x) = \frac{1}{x^j} + \frac{A_j(x)}{B_j(x)} \quad (7.9)$$

with $A_j(x), B_j(x) \in \mathbb{Z}[x]$ and $B_j(x) = x^k \hat{B}_j(x), k < j$. Here

$$\hat{B}_j(0) \not\equiv 0 (\text{mod } p), \quad (7.10)$$

since $B_j(x)$ is a product of monomials of the form $x - a_\alpha$ and $a_\alpha \not\equiv 0 (\text{mod } p)$ for $\alpha \neq 1$. Thus

$$C \cdot Q_j(x) = \frac{P_j(x)}{x^j \hat{B}_j(x)} \quad (7.11)$$

where $P_j(x) \in \mathbb{Z}[x]$ is of degree at most dj, $P_j(0) \not\equiv 0 \pmod p$. It follows that

$$\big| \{ 1 \leq x \leq p : Q_j(x) \equiv 0 \pmod p \} \big| \leq dj, \quad (7.12)$$

and

$$\big| \{ 1 \leq x \leq q_0 : Q_j(x) \equiv 0 \pmod{\bar{q}_0} \} \big| \leq (dj)^{\omega(\bar{q}_0)} \frac{q_0}{\bar{q}_0}, \quad (7.13)$$

whenever $\bar{q}_0 | q_0$. Taking $j = m - 1$ and fixing x, we will apply Vinogradov's lemma ([Ga], Lemma 4) to bound the following inner double sum in (7.6).

$$\Big| \sum_{t=1}^{N/q_0} e_{q_0^m} \Big(\sum_{j=1}^{m-1} Q_j(x) q_0^j t^j \Big) \Big|. \quad (7.14)$$

Lemma (Vinogradov). *Let $f(t) = a_1 t + \cdots + a_k t^k \in \mathbb{R}[t], k \geq 2$ and $P \in \mathbb{Z}_+$ large.*
Assume a_k rational, $a_k = \frac{a}{b}, (a,b) = 1$ such that

$$2 < P \leq b \leq P^{k-1} \quad (7.15)$$

Then

$$\Big|\sum_{n\in I} e(f(n))\Big| < C^{k(\log k)^2} P^{1-\frac{c}{k^2\log k}} \tag{7.16}$$

for any interval I of size P (c, C are constants).

Since the dominating saving in (7.16) is $P^{\frac{c}{k^2\log k}}$, we want the denominator of the leading coefficient $a_{m-1} = \frac{Q_{m-1}(x)}{q_0^m} q_0^{m-1}$ in (7.14) big.

Let $\bar{q}_0 = \big(Q_{m-1}(x), q_0\big)$. Write $Q_{m-1}(x) \equiv \bar{q}_0 \bar{a} \in \mathbb{Z} (\mathrm{mod}\ q_0)$. Therefore

$$a_{m-1} = \frac{Q_{m-1}(x)}{q_0} = \frac{\bar{a}}{\bar{\bar{q}}_0}, \ \text{ with } \bar{\bar{q}}_0 = \frac{q_0}{\bar{q}_0} \ \text{ and } (\bar{a}, \bar{\bar{q}}_0) = 1.$$

To sum $x \in [1, q_0]$ in (7.6), we distinguish the cases according to $\big(Q_{m-1}(x), q_0\big)$.

Case (i). $\bar{q}_0 = \bar{q}_0(x) = (Q_{m-1}(x), q_0) \le \sqrt{q_0}$. Hence $\bar{\bar{q}}_0 > \sqrt{q_0}$.

Divide the interval $[1, N/q_0]$ into subintervals of length $\sqrt{q_0}$ each. Applying (7.16) with $P = \sqrt{q_0}$ to the subsum over each subinterval and summing up the subsums give

$$\Big|\sum_{t=1}^{N/q_0} e_{q_0^m}\Big(\sum_{j=1}^{m-1} Q_j(x) q_0^j t^j\Big)\Big| < \frac{N}{q_0}\ C^{m(\log m)^2} q_0^{-\frac{c}{2m^2(\log m)}}. \tag{7.17}$$

The last inequality follows from (5.6)-(5.8).

Case (ii). $\bar{q}_0 = \bar{q}_0(x) = (Q_{m-1}(x), q_0) > \sqrt{q_0}$. We will use the trivial bound N/q_0 on (7.14). It remains to estimate the number of those $1 \le x \le q_0$ such that $Q_{m-1}(x) \equiv 0$ in $\mathbb{Z}/\bar{q}_0\mathbb{Z}$ for some $\bar{q}_0 > \sqrt{q_0}$. This number is by (7.13) at most

$$\sum_{\substack{\bar{q}_0 | q_0 \\ \bar{q}_0 > \sqrt{q_0}}} (dm)^{\omega(\bar{q}_0)} \frac{q_0}{\bar{q}_0} < 2^{\omega(q_0)} (dm)^{\omega(q_0)} \sqrt{q_0} < (2dm)^{\frac{2\log q_0}{\log\log N}} \sqrt{q_0}, \tag{7.18}$$

since all prime divisors of q_0 are at least $(\log N)^{\frac{1}{2}}$. Note that the degree d of $f(x)$ is bounded by (6.25). Applying (5.8) and (5.20), we have

$$dm < 60^r \big(\log q_r\big)^{\frac{2}{75}} \big(\log N\big)^{3c} < \big(\log N\big)^{15c}. \tag{7.19}$$

In particular, (7.19) will ensure that (7.18) is bounded by $q_0^{3/4}$.

Applying Case (i) and Case (ii) to (7.6), we have

$$\begin{aligned}
&\sum_{x=1}^{q_0}\Big|\sum_{t=1}^{N/q_0} e_{q_0^m}\Big(\sum_{j=1}^{m-1} Q_j(x)q_0^j t^j\Big)\Big| \\
&= \sum_{\bar{q}_0(x)\le\sqrt{q_0}}\Big|\sum_{t=1}^{N/q_0} e_{q_0^m}\Big(\sum_{j=1}^{m-1} Q_j(x)q_0^j t^j\Big)\Big| + \sum_{\bar{q}_0(x)>\sqrt{q_0}}\Big|\sum_{t=1}^{N/q_0} e_{q_0^m}\Big(\sum_{j=1}^{m-1} Q_j(x)q_0^j t^j\Big)\Big| \\
&\le\ q_0\ \frac{N}{q_0}C^{m(\log m)^2}q_0^{-\frac{c}{2m^2(\log m)}} + q_0^{\frac{3}{4}}\ \frac{N}{q_0} \\
&<\ NC^{m\log m)^2}q_0^{-\frac{c}{2m^2(\log m)}}.
\end{aligned} \tag{7.20}$$

Therefore $\mathcal{S} < C^{m\log m)^2}q_0^{-\frac{c}{2m^2(\log m)}}$. Together with (6.26), (5.21), (6.18) and (5.20), we have

$$\frac{1}{N}\Big|\sum_{x=1}^{N}\chi(x)\Big| < \frac{r-1}{M} + e^{(\log q_r)^{9/10+\epsilon}}\ q_0^{-(\log q_r)^{-\epsilon}} < e^{-(\log q_r)^{9/10}}. \tag{7.21}$$

This proves the theorem. □

8 Applications.

Repeating the argument in deducing Theorem 4 from Theorem 3' and Theorem 3", we obtain the following mixed character sum estimate from the proof of Theorem 5.

There is the following mixed character sum version of Theorem 5.

Theorem 8. *Under the assumptions of Theorem 5,*

$$\Big|\sum_{x\in I}\chi(x)e^{if(x)}\Big| < Ne^{-\sqrt{\log N}} \tag{8.1}$$

assuming $f(x)\in\mathbb{R}[x]$ of degree at most $(\log N)^c$ for some $c>0$.

A more precise statement is again possible, but the above one is all we need for what follows. To prove Theorem 8, simply go back to the opening

argument in Theorem 4 which removes the factor $e^{if(x)}$ at the cost of replacing $\chi(x)$ by $\chi(R(x))$ with $R(x)$ a certain rational function of x. Note that this step is already part of the proof of Lemma 6. At this point, proceed further with §6 and §7 as in proving Theorem 5.

Corollary 9. *Assume N satisfies*

$$q > N > \max_{p|q} p^{10^3}$$

and q satisfies

$$\log N > (\log qT)^{1-c} + C \log\Big(2\frac{\log q}{\log q'}\Big)\ \frac{\log q'}{\log\log q}\ . \tag{8.2}$$

Then for χ primitive, we have

$$\Big|\sum_{n\in I} \chi(n) n^{it}\Big| < Ne^{-\sqrt{\log N}}. \tag{8.3}$$

From Corollary 9, one derives bounds on the Dirichlet L-function $L(s,\chi)$ and zero-free regions the usual way. See for instance Lemmas 8-11 in [*I*]. This leads to the following theorem.

Theorem 10. *Let χ be a primitive multiplicative character with modulus q, $\mathcal{P} = \max_{p|q} p$, $q' = \prod_{p|q} p$, and $K = \frac{\log q}{\log q'}$. For $T > 0$, let*

$$\theta = c \min\Big(\frac{1}{\log \mathcal{P}}, \frac{\log\log q'}{(\log q')\log 2K}, \frac{1}{(\log qT)^{1-c'}}\Big).$$

Then the Dirichlet L-function $L(s,\chi) = \sum_n \chi(n) n^{-s}$, $s = \rho + it$ has no zeros in the region $\rho > 1 - \theta$, $|t| < T$, except for possible Siegel zeros.

It follows in particular that $\theta \log qT \to \infty$ if $\frac{\log \mathcal{P}}{\log q} \to 0$.

From Theorem 10, we have the following.

Corollary 11. *Assume q satisfies that $\log p = o(\log q)$ for any $p|q$. If $(a,q) = 1$, then there is a prime $P \equiv a \pmod q$ such that $P < q^{\frac{12}{5}+o(1)}$.*

To deduce Corollary 11, we follow the exposition of Linnik's theorem in [IK] (see p.440). Define

$$\psi(x,q,a)=\frac{1}{\phi(q)}\sum_{\chi \bmod q}\bar{\chi}(a)\sum_{n\le x}\Lambda(n)\chi(n),$$

where Λ is the von Mangoldt function. Assuming $x>q^{\frac{12}{5}+\epsilon}$, we have

$$\begin{aligned}&\psi(x,q,a)\\&=\frac{x}{\phi(q)}\left\{1-\sigma\frac{x^{\beta_1-1}}{\beta_1}+O\left(\frac{x^{-c\epsilon}}{\epsilon}\right)+O\left(\frac{x^{-c\eta}}{\epsilon}\right)+O\left(\frac{\log q}{q}\right)\right\}\end{aligned}\tag{8.4}$$

with

$$\eta>c\min\left(\frac{1}{\log\mathcal{P}},\frac{\log\log q}{\log q}\right),\quad \mathcal{P}=\max_{p|q}p.\tag{8.5}$$

Here, on the right hand side of (8.4), the second term accounts for a possible Siegel zero $s=\beta_1$ in Theorem 10 (in which case $\sigma=1$, otherwise $\sigma=0$), while the third term is from Huxley's density estimate [H], and the fourth term from the zero-free region given by (8.5). Certainly, $x^{-c\eta}\to 0$, if $\frac{\log\mathcal{P}}{\log q}\to 0$ (with ϵ fixed). Also,

$$1-\frac{x^{\beta_1-1}}{\beta_1}\ge\beta_1-q^{-(1-\beta_1)}=1-\frac{\gamma}{\log q}-e^{-\gamma}$$

with $\gamma=(1-\beta_1)\log q$.

We distinguish two cases. If γ is sufficiently small, then Corollary 2 in [HB2] applies. In this case there is a prime $P\equiv a \pmod q$ with $P<q^{2+\delta}<q^{\frac{12}{5}}$. Otherwise, the right hand side of (8.4) is greater than zero. Hence the conclusion in Corollary 11 holds in either case.

Next, following Goldmakher's work [G], we will derive from Theorem 5 the following theorem.

Theorem 12. *Let χ be a primitive multiplicative character with modulus q, $\mathcal{P}=\max_{p|q}p$, $q'=\prod_{p|q}p$ and $K=\frac{\log q}{\log q'}$.*
Let $M=(\log q)^{1-c}+\frac{\log q'}{\log\log q'}\log 2K+\log\mathcal{P}$. Then

$$\left|\sum_{n<x}\chi(n)\right|\ll\sqrt{q}\sqrt{\log q}\,\sqrt{M}\sqrt{\log\log\log q}.$$

We will sketch the argument and refer to [G] for more details. Denoting

$$\mathcal{S}_\chi(x) = \sum_{n<x} \chi(n)$$

with χ primitive modulo q. Proposition 2.2 in [G] states that

$$|\mathcal{S}_\chi(x)| \ll \sqrt{q}\,(\log q)^{\frac{1}{2}} \left| L(1+\frac{1}{\log q}, \chi\bar{\xi}) \right|^{\frac{1}{2}} + \sqrt{q}\,(\log q)^{\frac{6}{7}} \tag{8.6}$$

for some primitive character $\xi \pmod m$ of conductor less than $(\log q)^{1/3}$. This result uses crucially the work of Granville and Soundararajan [GS]. Let $\psi \pmod Q$ be the primitive character which induces $\chi\xi$. Then, by [G], Lemma 5.1 and Lemma 5.2,

$$\frac{q}{m} \le Q \le qm \tag{8.7}$$

and

$$\left| \frac{L(s, \chi\bar{\xi})}{L(s,\psi)} \right| \ll 1 + \log\log m. \tag{8.8}$$

Taking $s = 1 + \frac{1}{\log q}$, we get by partial summation that

$$L(s,\psi) = s\int_1^\infty \frac{1}{t^{s+1}} \left(\sum_{n\le t} \psi(n) \right) dt. \tag{8.9}$$

For $t > Q$, estimate $|\sum_{n\le t} \psi(n)|$ trivially by Q, which contributes in (8.9) for $O(1)$. Next,

$$\int_1^Q \frac{1}{t^{s+1}} \left| \sum_{n\le t} \psi(n) \right| dt \ll \log T + \int_T^Q \frac{1}{t^2} \left| \sum_{n\le t} \psi(n) \right| dt \tag{8.10}$$

and we apply Theorem 5 to bound $\sum_{n\le t} \psi(n)$ in the second term of the right hand side of (8.10). Note that by (8.7) the expression (0.3) in Theorem 5 is essentially preserved, if Q is replaced by q. Thus $T = N$ has to be chosen to satisfy (0.3) and Theorem 12 follows from (8.6), (8.8), and (8.10).

Acknowledgement. The author would like to thank the referee for very careful reading of the paper, which greatly improved its presentation. The author would also like to thank I. Shparlinski for helpful comments and the mathematics department of University of California at Berkeley for hospitality.

References

[C1] M.-C. Chang, *An Estimate of Incomplete Mixed Character Sums*, in *An Irregular Mind*. Editors: Brny, Imre, Solymosi, Jozsef . Bolyai Society Mathematical Studies. Budapest. Vol. 21, (2010), 243-250.

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

[Go] L. Goldmakher, *Character sums to smooth moduli are small*, Can J. Math. 62 (2010), 1099.

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

[GS] A. Granville, K. Soundararajan, *Large Character Sums: Pretentious Characters and the Pólya-Vinogradov Theorem*, J. Amer. Math. Soc. 20 (2007), 357-384.

[HB1] 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, no. 2 (1992), 265338.

[HB2] D.R. Heath-Brown, *Siegel zeros and the least prime in an arithmetic progression*, Quart. J. Math. Oxford Ser. (2), 41 (1990), 405-418.

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

[IK] H. Iwaniec, E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence RI, (2004).

[I] H. Iwaniec, *On zeros of Dirichlets L series*, Invent. Math. 23 (1974), 97-104.

[P] 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.