

LARGE CHARACTER SUMS

ANDREW GRANVILLE AND K. SOUNDARARAJAN

Dedicated to John Friedlander on the occasion of his 48th birthday by the first author, and on the occasion of his 58th birthday by the second author

INTRODUCTION

A central problem in analytic number theory is to gain an understanding of character sums

$$\sum_{n \leq x} \chi(n),$$

where χ is a non-principal Dirichlet character $\chi \pmod{q}$. It is easy to show that such characters sums are always $\leq q$ in absolute value, while G. Pólya and I.M. Vinogradov [3] improved this to $\leq \sqrt{q} \log q$ around 1919, and H.L. Montgomery and R.C. Vaughan [13] to $\ll \sqrt{q} \log \log q$ assuming the Generalized Riemann Hypothesis (GRH), in 1977. Up to the constant this is “best possible” since R.E.A.C. Paley [14] had shown, in 1932, that there exist characters sums (with real, quadratic characters), that are $\gg \sqrt{q} \log \log q$.

In many applications one is interested in when the above character sum is $o(x)$ with x substantially smaller than $q^{\frac{1}{2}+o(1)}$, that is

$$(1) \quad \left| \sum_{n \leq x} \chi(n) \right| = o(x).$$

In 1957, Burgess [2] used ingenious combinatorial methods together with the “Riemann Hypothesis for hyperelliptic curves” to establish (1) whenever $x > q^{\frac{1}{4}+o(1)}$, for any quadratic character mod q , with q prime (and subsequently generalized this to any non-principal character $\chi \pmod{q}$ when q is cubefree; with the smaller range $x > q^{\frac{3}{8}+o(1)}$ otherwise). Recently Friedlander and Iwaniec [4] have supplied a different proof of Burgess’s result, and Hildebrand [9] observed that one can “extrapolate” Burgess’s bound to the range $x > q^{\frac{1}{4}-o(1)}$. However, Burgess’s range has not been substantially improved over the last forty years although it is widely believed that such an estimate should hold for $x \gg_{\epsilon} q^{\epsilon}$.

In this paper we investigate the distribution of the size of character sums, and in particular in what range the estimate (1) should hold. For example on this question we prove:

The first author is a Presidential Faculty Fellow. He is also supported, in part, by the National Science Foundation. The second author is partially supported by the American Institute of Mathematics (AIM).

Corollary A. *Assuming that the Riemann Hypothesis is true for $L(s, \chi)$, the estimate (1) holds if $\log x / \log \log q \rightarrow \infty$ as $q \rightarrow \infty$. This is “best possible” in the sense that, for any given $A > 0$, for every prime q there exists a non-principal character $\chi \pmod{q}$ such $|\sum_{n \leq x} \chi(n)| \gg_A x$ where $x = \log^A q$.*

The proof of the first part of this result is inspired by Montgomery and Vaughan’s paper mentioned above. In fact, modifying and refining their argument we will get upper bounds on character sums in all ranges, assuming GRH, which we believe are close to the truth — we will discuss a more refined conjecture below.

To believe one’s upper bounds are close to the truth, one wants to show that there are character sums of comparable magnitude. Previous arguments to show that such sums exist, as in Paley’s work described above, have relied in part on using the law of quadratic reciprocity and Dirichlet’s theorem for primes in arithmetic progression to find discriminants for which many of the small primes are quadratic residues. Such an argument seems unlikely to generalize to characters of high order, and might make one suspicious that perhaps one can only obtain particularly large character sums (for instance, $\gg \sqrt{q} \log \log q$) when the character is real and quadratic. However this is not so, as we shall show below with a very different proof, involving high moments of character sums.

In the large character sums that we exhibited to prove Corollary A, we showed that they are large by establishing, for those characters, that the character sum over “smooth integers” is particularly large. Here “smooth” refers to integers with only small prime factors, and we define

$$\Psi(x, y; f) := \sum_{\substack{n \leq x \\ p|n \implies p \leq y}} f(n),$$

for any arithmetic function f . Our work on upper and lower bounds motivates our belief that character sums can only be large because of extraordinary behaviour of the values of $\chi(p)$ for small primes p . We formalize this as the following conjecture:

Conjecture 1. *There exists a constant $A > 0$ such that for any non-principal character $\chi \pmod{q}$, and for any $1 \leq x \leq q$ we have, uniformly,*

$$\sum_{n \leq x} \chi(n) = \Psi(x, y; \chi) + o(\Psi(x, y; \chi_0)),$$

where $y = (\log q + \log^2 x)(\log \log q)^A$.

The function $\Psi(x, y) := \Psi(x, y; 1)$, the well-known counting function for smooth numbers, has been extensively investigated. For any fixed $u > 0$, we know that $\lim_{x \rightarrow \infty} \Psi(x, x^{1/u})/x$ exists, and equals $\rho(u)$, where $\rho(u) = 1$ for $0 \leq u \leq 1$ and is the real continuous function satisfying the differential-delay equation $\rho'(u) = -\rho(u-1)/u$ for all $u > 1$. We note that $\rho(u) = 1/u^{u+o(u)}$ as $u \rightarrow \infty$. In §3b we will discuss several further estimates for $\Psi(x, y)$, though see [10] for a survey.

Note that Conjecture 1 implies the results of Corollary A, and, in fact, further that if

$$\Delta(x, q) := \max_{\chi \neq \chi_0} \left| \sum_{n \leq x} \chi(n) \right|$$

then $\Delta(x, q) \sim \Psi(x, \log q)$ whenever $\log x = o((\log \log q / \log \log \log q)^2)$, for any prime q .

Assuming the GRH it is known that there exists $n \ll \log^2 q$ with $(n, q) = 1$ for which $\chi(n) \neq 1$; assuming Conjecture 1 this would be improved to $n \leq \log^{1+o(1)} q$ (see [5] for the latest unconditional work on this problem).

In the wider range $x \leq \exp(\sqrt{\log q})$, Conjecture 1 implies that

$$(2) \quad \left| \sum_{n \leq x} \chi(n) \right| \leq \Psi(x, (\log q)^{1+o(1)}) = \frac{x}{u^{u+o(u)}}, \quad \text{where} \quad u = \frac{\log x}{\log \log q}.$$

for any non-principal character $\chi \pmod{q}$.

We shall establish lower bounds on character sums by various different methods in this paper (and in [6] and [7]). These will imply that, in most ranges of x , the value of y needs to be at least roughly as large as the value for y given in Conjecture 1.

We shall establish that Conjecture 1 holds with $y = \log^2 q \log^2 x (\log \log q)^{O(1)}$, assuming GRH, by extending the method of [13]. This implies the upper bound $\ll x/u^{u/4+o(u)}$ in (2), as well as the first part of Corollary A.

We shall also establish that Conjecture 1 holds for “almost all” characters $\chi \pmod{q}$ when $x \leq \exp((\log \log q)^{O(1)})$. More generally we shall show that Conjecture 1 with $y = \log q \log x (\log \log q)^{O(1)}$ holds for almost all non-principal characters $\chi \pmod{q}$.

Rather than the size distribution, one might be interested in the “angle distribution” of large character sums \pmod{q} . For example, if a character sum is “large”, in what directions can it point? Below we show, unconditionally, that for any fixed $A > 0$, for any given angle θ , there are non-principal characters χ modulo any prime q for which the character sum up to $\log^A q$ equals $\{e^{i\theta} + o(1)\} \rho(A) \log^A q$. In [7] we show the complementary result that there are non-principal characters χ modulo any prime q for which the character sum up to $q/2$ equals $\{e^{i\theta} + o(1)\} (e^\gamma/\pi) \sqrt{q} \log \log q$.

We shall also consider analogues of our results for real characters, when appropriate; that is,

$$\Delta_{\mathbb{R}}(x, q) = \max_{q \leq |D| \leq 2q} \left| \sum_{n \leq x} \left(\frac{D}{n} \right) \right|,$$

where D runs over fundamental discriminants. We establish similar and, in some cases, stronger versions of the results for $\Delta(x, q)$.

In the next section we give a more technical description of our results. In particular our results mostly apply to characters modulo any integer q , not just primes, and with various complicated error terms.

1. STATEMENT OF RESULTS

We begin with a unconditional, weak version of Conjecture 1 which works for “almost all” characters $\chi \pmod{q}$.

Theorem 1. *Let $1 \leq x \leq q$ be given. For all but at most $q^{1-\frac{1}{\log x}}$ characters $\chi \pmod{q}$ we have*

$$\sum_{n \leq x} \chi(n) = \Psi(x, y; \chi) + O\left(\frac{\Psi(x, y)}{(\log \log q)^2}\right), \quad \text{whenever} \quad y \geq \log q \log x (\log \log q)^5.$$

For all but at most $q^{1-\frac{1}{(\log \log q)^2}}$ characters $\chi \pmod{q}$ we have

$$\left| \sum_{n \leq x} \chi(n) \right| \leq \Psi(x, (\log q + \log^2 x)(\log \log q)^5).$$

Remark. Let $\omega(q)$ denote the number of distinct prime factors of q . Tenenbaum [16] showed that $\Psi(x, y, \chi_0) \asymp (\varphi(q)/q)\Psi(x, y)$ whenever $\log y \gg (\log 2\omega(q))(\log \log x)$. Since $1 \geq \varphi(q)/q \gg 1/\log \log q$ we see that the error term in Theorem 1 can be rewritten as $O(\Psi(x, y, \chi_0)/\log \log q)$ in this range.

Assuming the GRH we can establish results similar to (but weaker than) Theorem 1, but valid for all non-principal characters. The prototype for our result appears as Lemma 2 in [13]. There, Montgomery and Vaughan show that if $\chi \pmod{q}$ is non-principal and the GRH holds then

$$\sum_{n \leq x} \chi(n) = \Psi(x, y, \chi) + O(xy^{-\frac{1}{2}} \log^4 q),$$

when $\log^4 q \leq y \leq x \leq q$. Their objective was not to establish this in as wide a range as possible; however, ours is, so we modify and refine their method to obtain the following result.

Theorem 2. *Let χ be any non-principal character \pmod{q} , and assume the Riemann Hypothesis for $L(s, \chi)$. If $1 \leq x \leq q$ and $y \geq \log^2 q \log^2 x (\log \log q)^{12}$ then*

$$\sum_{n \leq x} \chi(n) = \Psi(x, y; \chi) + O\left(\frac{\Psi(x, y)}{(\log \log q)^2}\right).$$

Further

$$\left| \sum_{n \leq x} \chi(n) \right| \ll \Psi(x, \log^2 q (\log \log q)^{20}),$$

and so the estimate (1) holds when $\log x / \log \log q \rightarrow \infty$ as $q \rightarrow \infty$.

Remarks. To compare this with Montgomery and Vaughan's result, the error term in the first part of Theorem 2 could have been written as the rather more complicated $O(\Psi(x, y) \log q \log x (\log \log q)^4 / \sqrt{y})$. Similarly, the error term in the first part of Theorem 1 can be considerably sharpened.

As in Theorem 1 the error term can be rewritten as $O(\Psi(x, y, \chi_0)/\log \log q)$ when $\log y \gg (\log 2\omega(q))(\log \log x)$.

We now proceed to the problem of finding large character sums, beginning with the range $x \leq \exp((\log \log q)^{2-\epsilon})$. Here we get large character sums, pointing in any given direction.

Theorem 3. *Let q be large, and suppose $\log x \leq \frac{(\log \log q)^2}{(\log \log \log q)^2}$. For all $|\theta| \leq \pi$ there are at least $q^{1 - \frac{2}{\log x}}$ characters $\chi \pmod{q}$ for which*

$$\sum_{n \leq x} \chi(n) = e^{i\theta} \Psi(x, \log q; \chi_0) + O\left(\Psi(x, \log q) \left(\frac{1}{\log x} + \frac{\log x (\log \log \log q)^2}{(\log \log q)^2}\right)\right).$$

If q has no prime factors less than $\log q$ then we may write the above as

$$\sum_{n \leq x} \chi(n) = x e^{i\theta} \rho\left(\frac{\log x}{\log \log q}\right) \left(1 + O\left(\frac{1}{\log x} + \frac{\log x (\log \log \log q)^2}{(\log \log q)^2}\right)\right).$$

This implies the second part of Corollary A.

Theorem 3 is not useful when q has many prime factors less than $\log q$. We next deduce, by a very different method, lower bounds of more or less the same strength for these cases.

Theorem 4. *Suppose $x = (10 \log q)^B = q^{o(1)}$ for some $B \geq 1$. Then*

$$\max_{\chi \neq \chi_0} \left| \sum_{n \leq x} \chi(n) \right| \gg \frac{x^{\frac{1}{2} + \frac{|B|}{2B}}}{(4 \log x)^{|B|}}.$$

If, in addition, q has less than $(\log q)^{B/(B+1)-\epsilon}$ distinct prime factors then

$$\max_{\chi \neq \chi_0} \left| \sum_{n \leq x} \chi(n) \right| \gg \frac{x}{(4 \log x)^{|B|+1}}.$$

Applying Theorem 4 appropriately, we can deduce the following corollaries.

Corollary 1. *If $\log x \geq (\log \log q)^2$ then*

$$\max_{\chi \neq \chi_0} \left| \sum_{n \leq x} \chi(n) \right| \gg x \exp\left(- (1 + o(1)) \log x \frac{\log \log x}{\log \log q}\right).$$

If, in addition, q has less than $(\log q)^{1-\epsilon}$ distinct prime factors then this bound holds in the extended range $\log x / \log \log q \rightarrow \infty$.

Remark. There are $\ll q / \exp((\log q)^{1-\epsilon})$ integers $q \leq x$ failing the restriction “ q has less than $(\log q)^{1-\epsilon}$ distinct prime factors”.

Corollary 2. *Fix σ in the range $\frac{1}{2} \leq \sigma < 1$. If $(\log q)^{\frac{1}{1-\sigma}} \leq x \leq \exp((\log q)^{1-\sigma+o(1)})$ then*

$$\max_{\chi \neq \chi_0} \left| \sum_{n \leq x} \chi(n) \right| \gg x^\sigma.$$

If, in addition, $\omega(q) \leq (\log q)^{\frac{1}{2}-\epsilon}$ then this bound holds whenever $x \geq (\log q)^{1+\epsilon}$. In any case we have

$$\max_{x \geq 1} \max_{\chi \neq \chi_0} \frac{1}{x^\sigma} \left| \sum_{n \leq x} \chi(n) \right| \gg \exp\left(\frac{(\log q)^{1-\sigma}}{14 \log \log q}\right).$$

So far we have dealt with the range $x \leq \exp((\log q)^{\frac{1}{2}-\epsilon})$. We now proceed to the range when x is larger, dealing first with the range $\log \log x = (\frac{1}{2} + o(1)) \log \log q$.

Theorem 5. *Suppose that $\log x = \tau\sqrt{\log q \log \log q}$ with $\tau = (\log \log q)^{O(1)}$, and let $\eta = \tau + 1/\tau$. There exists a constant $c > 0$ such that for any sufficiently large q , there exists a non-principal character $\chi \pmod{q}$ for which*

$$\frac{1}{\sqrt{x}} \left| \sum_{n \leq x} \chi(n) \right| \gg \exp\left(c \frac{1 + \log(\eta\tau)}{\eta} \sqrt{\frac{\log q}{\log \log q}}\right).$$

As a consequence we get Corollary 3 below, which improves Corollary 2 in the case $\sigma = \frac{1}{2}$.

Corollary 3. *There exists a constant $c > 0$ such that for all integers q*

$$\max_{\chi \neq \chi_0} \max_{x \geq 1} \frac{1}{\sqrt{x}} \left| \sum_{n \leq x} \chi(n) \right| \gg \exp\left(c \sqrt{\frac{\log q}{\log \log q}}\right).$$

Next we consider the range when $\log x/\sqrt{\log q \log \log q}$ is large, but x is smaller than q^ϵ .

Theorem 6. *Suppose both $\log q/\log x$ and $\log x/\sqrt{\log q \log \log q} \rightarrow \infty$. There exists a non-principal character $\chi \pmod{q}$ for which*

$$\frac{1}{\sqrt{x}} \left| \sum_{n \leq x} \chi(n) \right| \gg \left(\frac{\log x}{\sqrt{\log q \log \log q}} \right)^{(1+o(1))\frac{\log q}{\log x}}.$$

When x is as large as a power of q we obtain:

Theorem 7. *Let $k \geq 2$ be an integer and suppose $\exp(\frac{\log q}{\log \log q}) \leq x < q^{\frac{1}{k}}$. Then there exists a non-principal character $\chi \pmod{q}$ for which*

$$\frac{1}{\sqrt{x}} \left| \sum_{n \leq x} \chi(n) \right| \gg_k (\log q)^{\frac{(k-1)^2}{2k} + o(1)}.$$

Once $x \geq q^{\frac{1}{2}}$ Theorem 7 reduces to the bound $\Delta(x, q) \geq \sqrt{x}(\log q)^{o(1)}$ which follows immediately from the mean square of $\sum_{n \leq x} \chi(n)$. However it is possible to obtain non-trivial information here by appealing to (essentially) the Poisson summation formula. We quote Pólya's Fourier expansion (see Lemma 1 of [13])

$$(3) \quad \sum_{n \leq x} \chi(n) = \frac{\tau(\chi)}{2\pi i} \sum_{\substack{h=-H \\ h \neq 0}}^H \frac{\bar{\chi}(h)}{h} (1 - e(-\frac{hx}{q})) + O(1 + qH^{-1} \log q),$$

where χ is primitive, and $\tau(\chi)$ is the usual Gauss sum. Since $|\tau(\bar{\chi})| = \sqrt{q}$, (3) suggests a relation of the type $\Delta(x, q) \asymp \frac{x}{\sqrt{q}} \Delta(\frac{q}{x}, q)$; now $\frac{q}{x} \leq q^{\frac{1}{2}}$ so that applying the ideas behind our earlier Theorems should lead to a good lower bound for $\Delta(x, q)$. While we cannot show such a result for every x , using (3) we can obtain good bounds for $\Delta(t, q)$ for some $t \leq x$. Naturally one would expect $\Delta(t, q)$ to be an increasing function of t (at least most of the time) but we don't know how to prove this. For convenience, we state this result only for primes q , so that every non-principal character is primitive.

Theorem 8. *Let q be a large prime. Given $\exp(c\sqrt{\log q}) \geq N \geq 2$ (for a small positive constant c) we have*

$$\max_{t \leq q/N} \max_{\chi \neq \chi_0 \pmod{q}} \left| \sum_{n \leq t} \chi(n) \right| \gg \sqrt{q} \frac{1}{N} \Psi \left(N, \frac{\log q}{(\log \log q)^{10}} \right).$$

When $\log N = \tau \sqrt{\log q \log \log q}$ with $\tau = (\log \log q)^{O(1)}$ we have (for a small positive constant c and $\eta = \tau + 1/\tau$)

$$\max_{t \leq q/N} \max_{\chi \neq \chi_0 \pmod{q}} \left| \sum_{n \leq t} \chi(n) \right| \gg \sqrt{q/N} \exp \left(c \frac{1 + \log(\eta\tau)}{\eta} \sqrt{\frac{\log q}{\log \log q}} \right).$$

If both $\log q / \log N$ and $\log N / \sqrt{\log q \log \log q} \rightarrow \infty$ then

$$\max_{t \leq q/N} \max_{\chi \neq \chi_0 \pmod{q}} \left| \sum_{n \leq t} \chi(n) \right| \gg \sqrt{q/N} \left(\frac{\log N}{\sqrt{\log q \log \log q}} \right)^{(1+o(1)) \frac{\log q}{\log N}}.$$

Lastly if $\exp(\frac{\log q}{\log \log q}) \leq N \leq q^{\frac{1}{k}-\epsilon}$ for an integer $k \geq 2$ then

$$\max_{t \leq q/N} \max_{\chi \neq \chi_0 \pmod{q}} \left| \sum_{n \leq t} \chi(n) \right| \gg_k \sqrt{q/N} (\log q)^{\frac{(k-1)^2}{2k} + o(1)}.$$

Several different authors (for example [1]) gave the same explicit version of Paley's result: There are infinitely many non-square, positive integers q , and integers $x = x_q$ for which

$$(4) \quad \left| \sum_{1 \leq n \leq x} \left(\frac{q}{n} \right) \right| \gtrsim \frac{e^\gamma}{\pi} \sqrt{q} \log \log q,$$

where $\gamma \approx 0.5772156649\dots$ is the Euler-Mascheroni constant. We can prove that there are many characters $\chi \pmod{q}$ for which $\sum_{n \leq q/2} \chi(n)$ is of such large magnitude, and points in any given direction, for any given prime q . Further, whenever $q(\log q)^{-A} \leq x \leq q$ we can show that $\Delta(x, q) \gg \rho_A \sqrt{q} \log \log q$, where $\rho_A = 1/A^{A+o(A)}$ as $A \rightarrow \infty$. The proofs of these results will appear in [7], because they are more closely related to the methods of that paper. Note, though, in Theorem 11 below we obtain some results of this type for real characters.

We now turn our attention to getting bounds for $\Delta_{\mathbb{R}}(x, q)$: that is, exhibiting large character sums for real characters. We begin by showing that the lower bound implicit in Conjecture 1 holds in a very wide range for real characters.

Theorem 9. *Suppose q is large, and that $1 \leq x \leq \exp(\sqrt{\log q})$. Then*

$$\max_{q \leq |D| \leq 2q} \left| \sum_{n \leq x} \left(\frac{D}{n} \right) \right| \geq \Psi(x, \frac{1}{3} \log q).$$

Consequently for a fixed real number B there are fundamental discriminants D in the range $q \leq |D| \leq 2q$ with

$$\sum_{n \leq x} \left(\frac{D}{n} \right) \geq (\rho(B) + o(1))x \gg_B x, \quad \text{where } x = \left(\frac{1}{3} \log q \right)^B$$

Theorem 9 is the analogue of Theorems 3 and 4 above. From Theorem 9 we can deduce the analogues of Corollaries 1 and 2 for real characters.

It seems to have been widely believed that $\sum_{N < n \leq N+x} \left(\frac{D}{n} \right) = o(x)$ when $x / \log^2 D \rightarrow \infty$ (see, for instance, page 379 of [11]), perhaps in analogy with the known result $\sum_{p \leq x} \left(\frac{D}{p} \right) = o(\pi(x))$ in this range, assuming GRH. However Theorem 9 shows that this widely held view is false. It seems safe to hazard the guess that, for all non-principal characters $\chi \pmod{q}$ we have, uniformly,

$$\sum_{n=N}^{N+x} \chi(n) \ll x^{1-1/\log \log q}.$$

Set

$$\alpha(B) = \limsup_{|D| \rightarrow \infty} \frac{1}{(\log |D|)^B} \sum_{n \leq (\log |D|)^B} \left(\frac{D}{n} \right).$$

Clearly $\alpha(B) = 1$ for $0 \leq B \leq 1$, and from Theorem 9, we know that $\alpha(B) \geq \rho(B)$. If the GRH is true then $\alpha(B) \leq \rho(\frac{B}{2})$, by Theorem 2. Conjecture 1 predicts that $\alpha(B) = \rho(B)$ but this is not known for any $B > 1$. In Theorem 3 we obtained large character sums pointing in any given direction. Mark Watkins asked us if the analogue for real character sums holds: that is, can one get real character sums to be large and negative? Precisely, what can one say about

$$\beta(B) := \liminf_{|D| \rightarrow \infty} \frac{1}{(\log |D|)^B} \sum_{n \leq (\log |D|)^B} \left(\frac{D}{n} \right).$$

Interestingly $\beta(B)$ can never be as small as -1 . Indeed in [6] we have shown that $\beta(B) \geq \delta_1 = -0.656999\dots$ (see Theorem 1 of [6] for a definition of δ_1) for all B , and in fact $\beta(B) = \delta_1$ for $0 \leq B \leq 1$. Answering Watkins' question we also show there that $\beta(B) < 0$ for all B , but it is an open problem to determine $\beta(B)$ and $\alpha(B)$ for $B > 1$.

We obtain the following analogue of Theorems 5, 6 and 7, but in a much wider range.

Theorem 10. *Suppose that q is large, and $\exp((\log q)^{\frac{1}{2}}) \leq x \leq q / \exp((\log q)^{\frac{1}{2}})$. Then there exist fundamental discriminants D in the range $q \leq |D| \leq 2q$ with*

$$\frac{1}{\sqrt{x}} \sum_{n \leq x} \left(\frac{D}{n} \right) \gg \exp\left((1 + o(1)) \frac{\sqrt{\log q}}{\log \log q} \right).$$

Notice that Theorem 10 is much stronger than the bounds of Theorems 6 and 7, as soon as $\log x \geq \sqrt{\log q} (\log \log q)^2$. This difference is especially noticeable when

x is like a small power of q , and suggests that Theorems 6 and 7 are unlikely to be “best possible.”

In the next result we use Poisson summation (as discussed after (3)) to get lower bounds for character sums when x is very large, in terms of smooth numbers. This suggests that we should be able to make another conjecture like Conjecture 1 for large x , which takes this natural symmetry into account. We have not yet felt able to formulate this appropriately.

Theorem 11. *Let q be large. For any $\exp(\sqrt{\log q}) \geq N \geq 2$ there exists a fundamental discriminant D with $q \leq |D| \leq 2q$ such that*

$$\left| \sum_{n \leq |D|/N} \left(\frac{D}{n} \right) \right| \gg \sqrt{q} \frac{1}{N} \Psi \left(N, \frac{1}{9} \log q \right) \left\{ 1 + \frac{\log \log q}{\log(A+2)} \right\},$$

where $N = (\frac{1}{9} \log q)^A$. In particular if $\exp((\log \log q)^2) \geq N \geq 2$ then there exists a fundamental discriminant D with $q \leq |D| \leq 2q$ such that

$$\left| \sum_{n \leq |D|/N} \left(\frac{D}{n} \right) \right| \gg \frac{\rho(A)}{\log(A+2)} \sqrt{|D|} \log \log |D|.$$

2. THE PLAN OF ATTACK

We define complex, multiplicative random variables X_n as follows: X_n is multiplicative: that is, if $n = \prod_i p_i^{a_i}$ then $X_n = \prod_i X_{p_i}^{a_i}$. For primes p , X_p is equidistributed on the unit circle, and for different primes p and q , X_p and X_q are independent. Thus $\mathbb{E}(X_m \overline{X_n}) = 1$ if $m = n$, and $\mathbb{E}(X_m \overline{X_n}) = 0$ otherwise. Here, and below, $\mathbb{E}(\cdot)$ denotes the expectation.

Let f be any arithmetical function, and k and n be integers. Below we shall put

$$d_{k,f}(n, x) = \sum_{\substack{m_1 \dots m_k = n \\ m_i \leq x}} f(m_1) \dots f(m_k),$$

so that

$$\left(\sum_{n \leq x} \chi(n) f(n) \right)^k = \sum_{n \leq x^k} d_{k,f}(n, x) \chi(n), \quad \text{and} \quad \left(\sum_{n \leq x} X_n f(n) \right)^k = \sum_{n \leq x^k} d_{k,f}(n, x) X_n.$$

We shall abbreviate $d_{k,f}(n, x)$ to $d_k(n, x)$ when f is the function $f(n) = 1$.

Lemma 2.1. *Let x , q , and k be integers with $x^k \leq q$; and let f be any arithmetic function. Then*

$$\frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left| \sum_{n \leq x} \chi(n) f(n) \right|^{2k} = \sum_{\substack{n \leq x^k \\ (n, q) = 1}} |d_{k,f}(n, x)|^2 = \mathbb{E} \left(\left| \sum_{\substack{n \leq x \\ (n, q) = 1}} X_n f(n) \right|^{2k} \right).$$

Proof. This is immediate from the definition of X_n , and the orthogonality of the characters $(\bmod q)$:

$$\frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \chi(a) \overline{\chi}(b) = \begin{cases} 1 & \text{if } a \equiv b \pmod{q}, \quad (ab, q) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Our plan (see §4, and §6) is to obtain large lower bounds for the quantity in Lemma 2.1 (in the case $f(n) = 1$) so as to obtain large non-trivial character sums. In order to do this, we need to eliminate the principal character term (which is often large for trivial reasons) which is included in the sum in Lemma 2.1.

For any arithmetic function f we define

$$\Delta_f(x, q) := \max_{\chi \neq \chi_0 \pmod{q}} \left| \sum_{n \leq x} \chi(n) f(n) \right|.$$

Proposition 2.2. *Let q be large, $x \geq \log q$, and suppose k is an integer with $x^k \leq q$. For any arithmetic function f we have*

$$\Delta_f(x, q)^{2k} \gg \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left| \sum_{n \leq x} \chi(n) f(n) \right|^{2k}.$$

Proof. Write $\Delta = \Delta_f(x, q)$, and define

$$\Delta_0 := \sum_{n \leq x} \chi_0(n), \quad \Delta_1 := \left| \sum_{n \leq x} \chi_0(n) f(n) \right| \quad \text{and} \quad \Delta_2 := \sum_{n \leq x} \chi_0(n) |f(n)|^2.$$

Note that the Cauchy-Schwarz inequality gives $\Delta_1^2 \leq \Delta_0 \Delta_2$. A straightforward computation, using the orthogonality relations for characters, gives that

$$\Delta_2 = \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left| \sum_{n \leq x} \chi(n) f(n) \right|^2,$$

and thus

$$\left(\Delta_2 - \frac{\Delta_1^2}{\varphi(q)} \right)^k \leq \left(\frac{1}{\varphi(q)} \sum_{\substack{\chi \pmod{q} \\ \chi \neq \chi_0}} \left| \sum_{n \leq x} \chi(n) f(n) \right|^{2k} \right) \left(\frac{1}{\varphi(q)} \sum_{\substack{\chi \pmod{q} \\ \chi \neq \chi_0}} 1 \right)^{k-1} \leq \Delta^{2k},$$

by Hölder's inequality. This then implies

$$\Delta_1^2 \left(1 - \frac{\Delta_0}{\varphi(q)} \right) = \Delta_1^2 - \frac{\Delta_0 \Delta_1^2}{\varphi(q)} \leq \Delta_0 \left(\Delta_2 - \frac{\Delta_1^2}{\varphi(q)} \right) \leq \Delta_0 \Delta^2.$$

If $k \geq 2$ then $x \leq \sqrt{q}$ and so $(1 - \Delta_0/\varphi(q))^k = 1 + o(1)$, which, combined with the line above, implies that $\Delta_1^{2k} \lesssim \Delta_0^k \Delta^{2k}$. Therefore

$$(2.1) \quad \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left| \sum_{n \leq x} \chi(n) f(n) \right|^{2k} \leq \frac{\Delta_1^{2k}}{\varphi(q)} + \frac{(\varphi(q) - 1) \Delta^{2k}}{\varphi(q)} \lesssim \Delta^{2k} \left(\frac{\Delta_0^k}{\varphi(q)} + 1 \right).$$

By the small sieve we know that for $x \geq \log q$

$$\Delta_0 = \sum_{\substack{n \leq x \\ (n, q) = 1}} 1 \leq c \frac{\varphi(q)}{q} x$$

for some absolute constant $c > 0$. Hence

$$\Delta_0^k \leq x^{k-1} \Delta_0 \leq c \frac{\varphi(q)}{q} x^k \leq c \varphi(q)$$

and the Proposition follows upon inserting this estimate in (2.1).

We cannot expect to get good lower bounds for $\Delta_f(x, q)$ for all arithmetic functions f , since there may be a good deal of cancellation in determining the sum $d_{k,f}(n, x)$, making $\sum_n |d_{k,f}(n, x)|^2$ small. We shall focus on a large class \mathcal{F} of arithmetic functions defined as follows: $f \in \mathcal{F}$ if $f(n) = g(n)h(n)$ where g is a multiplicative function with $|g(n)| = 1$ for all n , and $h(n) \geq 0$ for all n . Note that \mathcal{F} includes $\mu(n)$ (the Möbius function), $\omega(n)$ (the number of distinct prime divisors of n), $d(n)$ (the divisor function), n^{it} (for a real number t) among others.

Lemma 2.3. *Suppose f and g are arithmetic functions with $f(n) \geq g(n) \geq 0$ for all n . Then for all integers $k \geq 1$*

$$\mathbb{E} \left(\left| \sum_{n \leq x} X_n f(n) \right|^{2k} \right) \geq \mathbb{E} \left(\left| \sum_{n \leq x} X_n g(n) \right|^{2k} \right).$$

If $f \in \mathcal{F}$ with $|f(n)| \geq \theta$ for all square-free n then

$$\mathbb{E} \left(\left| \sum_{n \leq x} X_n f(n) \right|^{2k} \right) \geq \theta^{2k} \sum_{N \leq x^k} \mu(N)^2 d_k(N, x)^2.$$

Proof. If $f(n) \geq g(n) \geq 0$ then $d_{k,f}(n, x) \geq d_{k,g}(n, x)$ and so the first assertion follows from Lemma 2.1. If $f \in \mathcal{F}$ and $|f(n)| \geq \theta$ for all n , then for squarefree N we have $|d_{k,f}(N, x)| \geq \theta^k d_k(N, x)$ and so the second statement follows from the first part of the lemma.

In §3 we collect together several results from multiplicative number theory; chiefly on smooth numbers (integers not having large prime factors), and round numbers (integers having many prime factors). We shall use these in §4 to estimate the $2k$ -th moments of $\sum_{n \leq x}^b X_n$ where the flat “b” indicates that the sum is over squarefree n coprime to q ; and in §6 to get good estimates for large moments of $\sum_{n \leq x} X_n$. We show in §5 how the estimates of §4 lead to the large character sums given in Theorems 4 through 7, and Corollaries 1, 2, and 3. We note that these results depend only on the lower bounds for $\sum_{N \leq x^k}^b d_k(N, x)^2$ given in Theorems 4.1, and 4.2. In view of Lemma 2.3 we may thus generalize these results for Δ_f when $f \in \mathcal{F}$ with $|f(n)| \geq 1$.

Theorems 4-7, Corollaries 1-3 Revisited. *Let $f \in \mathcal{F}$ be any arithmetic function with $|f(n)| \geq 1$ for all n . Then Theorem 4-7 and Corollaries 1-3 all hold for $\Delta_f(x, q)$ in place of $\Delta(x, q)$.*

In §7 we derive Theorems 1 and 3 as consequences of the analysis of §6. In §8 we obtain the conditional result Theorem 2. The case of real characters (Theorems 9-11) are dealt with in §9. Lastly, Theorem 8, which is a consequence of the “Fourier flip” $x \rightarrow \frac{q}{x}$, is proved in §10.

3. SMOOTH AND ROUND NUMBERS

3a. Integers with a specified number of prime factors.

Estimating $\pi(x, y)$, the number of integers up to x with exactly y distinct prime factors, has long been a central topic of additive number theory. Hardy and Ramanujan [8] established the famous upper bound

$$\pi(x, y) \ll \frac{x}{\log x} \frac{(\log \log x + O(1))^{y-1}}{(y-1)!},$$

uniformly for all y . However good lower bounds, even on the order of magnitude for $\pi(x, y)$, when $y \gg \log \log x$ were not known until recently. In 1984, Pomerance [15] made an important breakthrough in showing that

$$(3.1) \quad \pi(x, y) = \frac{x}{\log x} \frac{L^{y+O(\frac{y}{L})}}{y!}, \quad \text{where } L = \log \left(\frac{\log x}{y \log y} \right),$$

in the range

$$(3.2) \quad \log \log x \leq y \leq \frac{\log x}{3 \log \log x}.$$

Pomerance only claimed to have proved this result in the narrower range with $y \geq (\log \log x)^2$. However he gives a slightly worse error term in one place in his proof than is necessary, with the resulting loss in the range of applicability. This mistake is corrected in the proof of Theorem 3.1 below; taking $m = 1$ there implies the lower bound in (3.1). The upper bound in the missing range follows from Hardy and Ramanujan’s result.

Although it appears that we have imposed some rather severe extra restrictions, it turns out that we can obtain the following result with minor modifications to Pomerance’s proof. Here \sum^b indicates that the sum is over squarefree arguments.

Theorem 3.1. *Given integers x, y and m , let $z = \max(y^2, \omega(m))$. If (3.2) holds and, in addition,*

$$(3.3) \quad y^2 \leq z \leq x^{\frac{2}{3y}}$$

then

$$(3.4) \quad \sum_{\substack{n \leq x, \omega(n)=y \\ (n,m)=1}}^b 1 \geq \frac{x}{\log x} \frac{L^{y+O(\frac{y}{L})}}{y!}, \quad \text{where } L = L(x, y, z) := \log \left(\frac{\log x}{y \log \sqrt{z}} \right).$$

To prove this Theorem we require the following lemma.

Lemma 3.2. *Let I be any interval, and let $s \geq 2$ be an integer. Then*

$$\left(\sum_{p \in I} \frac{1}{p}\right)^s - \frac{s(s-1)}{2} \left(\sum_{p \in I} \frac{1}{p^2}\right) \left(\sum_{p \in I} \frac{1}{p}\right)^{s-2} \leq \sum_{\substack{p_1, p_2, \dots, p_s \in I \\ p_i \text{ distinct}}} \frac{1}{p_1 \cdots p_s} \leq \left(\sum_{p \in I} \frac{1}{p}\right)^s.$$

Proof. The upper bound is immediate, and the lower bound follows by induction on s , after noting that

$$\begin{aligned} \sum_{\substack{p_1, \dots, p_s \in I \\ p_i \text{ distinct}}} \frac{1}{p_1 \cdots p_s} &= \sum_{\substack{p_1 \cdots p_{s-1} \\ p_i \text{ distinct}}} \frac{1}{p_1 \cdots p_{s-1}} \left(\sum_{p \in I} \frac{1}{p} - \frac{1}{p_1} - \cdots - \frac{1}{p_{s-1}} \right) \\ &\geq \left(\sum_{p \in I} \frac{1}{p} \right) \sum_{\substack{p_1 \cdots p_{s-1} \\ p_i \text{ distinct}}} \frac{1}{p_1 \cdots p_{s-1}} - (s-1) \sum_{p \in I} \frac{1}{p^2} \sum_{\substack{p_1 \cdots p_{s-2} \\ p_i \text{ distinct}}} \frac{1}{p_1 \cdots p_{s-2}}. \end{aligned}$$

Proof of Theorem 3.1. If m is an integer with exactly k distinct prime factors, and p_k is the k th smallest prime, then

$$(3.5) \quad \sum_{\substack{n \leq x, \omega(n)=y \\ (n,m)=1}}^b 1 \geq \sum_{\substack{n \leq x, \omega(n)=y \\ p|n \implies p > p_k}}^b 1.$$

This is evident from noting that if q_1, \dots, q_l are the distinct prime factors of m that are $> p_k$, and r_1, \dots, r_l are the primes $\leq p_k$ that do not divide m , then each integer $q_1 q_2 \cdots q_l t$ counted in the sum on the right side of (3.5), corresponds to a distinct integer $r_1 r_2 \cdots r_l t$ counted in the sum on the left side.

Note that $L \geq \log 3$, and put $s = \lfloor \frac{y-1}{L+20} \rfloor$ and $J = \lfloor \log(L+20) \rfloor - 2$. We define the intervals $I_{-1} = (z, x^{\frac{2}{e^y}}]$, and (for $0 \leq j \leq J-1$) $I_j = (x^{\frac{2e^{j-1}}{y}}, x^{\frac{2e^j}{y}}]$. We get a lower bound on the right side of (3.5) by counting only those integers n of the form $n = n_{-1} n_0 \cdots n_{J-1} p$ where n_{-1} consists of exactly $y-1-sJ$ distinct primes from I_{-1} , and (for $0 \leq j \leq J-1$) n_j consists of exactly s distinct primes from I_j , and $x^{\frac{2e^{J-1}}{y}} < p \leq \frac{x}{n_{-1} n_0 \cdots n_{J-1}}$ is prime. Hence using the prime number theorem

$$(3.5) \geq \sum_{n_{-1}, n_0, \dots, n_{J-1}} \sum_{x^{\frac{2e^{J-1}}{y}} \leq p \leq \frac{x}{n_{-1} n_0 \cdots n_{J-1}}} 1 \geq \frac{x}{2 \log x} \prod_{j=-1}^{J-1} \left(\sum_{n_j} \frac{1}{n_j} \right).$$

Appealing to Lemma 3.2 we determine that

$$\sum_{n_{-1}} \frac{1}{n_{-1}} = \frac{(L + O(1))^{y-1-sJ}}{(y-1-sJ)!} \left(1 + O\left(\frac{y^2}{z \log z} \right) \right),$$

and that for $0 \leq j \leq J-1$

$$\sum_{n_j} \frac{1}{n_j} = \frac{(1 + O(L^{-1}))^s}{s!} \left(1 + O\left(\frac{s^2}{x^{\frac{2e^{j-1}}{y}} \log z} \right) \right).$$

It follows that

$$(3.5) \geq \frac{x}{2 \log x} \frac{L^{y-1-sJ}}{(y-1-sJ)!s!^J} e^{O(\frac{y}{L} + \frac{1}{\log y})},$$

and Theorem 3.1 follows upon using Stirling's formula, keeping in mind that $y \geq L$ in our range.

Lemma 3.3. *Let ℓ be a positive integer, and suppose $y \geq 2\ell^2$. For all $x \geq y^\ell$,*

$$\sum_{\substack{n \leq x, \Omega(n) = \ell \\ p|n \implies p > y}} 1 \ll \frac{x}{\log y} \frac{(\log \log x + O(1))^{\ell-1}}{(\ell-1)!}.$$

Proof. Given a squarefree integer m with exactly $j (\leq \ell)$ distinct prime factors all larger than y , there are $\leq j^{\ell-j}$ integers n with $\Omega(n) = \ell$ and having exactly the same prime factors as m . Moreover if $n \leq x$ then $m \leq n/y^{\ell-j} \leq x/y^{\ell-j}$. Thus the sum we seek is

$$\leq \sum_{j=1}^{\ell} j^{\ell-j} \sum_{\substack{m \leq x/y^{\ell-j} \\ \omega(m) = j}} \mu(m)^2.$$

By the Hardy-Ramanujan upper bound this is

$$\ll \frac{x}{\log y} \sum_{j=1}^{\ell} \frac{j^{\ell-j}}{y^{\ell-j}} \frac{(\log \log x + O(1))^{j-1}}{(j-1)!} \leq \frac{x}{\log y} \frac{(\log \log x + O(1))^{\ell-1}}{(\ell-1)!} \sum_{j=1}^{\ell} \frac{(j\ell)^{\ell-j}}{y^{\ell-j}},$$

and the result follows as $y \geq 2\ell^2$.

3b. Smooth numbers.

Given real numbers $x \geq y \geq 1$, and an integer ℓ we define $\mathcal{S}_\ell(x, y)$ to be the set of integers $\leq x$ having exactly ℓ prime factors (counted with multiplicity) larger than y . We denote the cardinality of $\mathcal{S}_\ell(x, y)$ by $\Psi_\ell(x, y)$. The case $\ell = 0$ gives rise to smooth numbers: that is, integers free of large prime factors, and we write $\mathcal{S}(x, y)$, $\Psi(x, y)$ in place of $\mathcal{S}_0(x, y)$, $\Psi_0(x, y)$. Estimating $\Psi(x, y)$ has been the focus of much attention, and we quote below the best results known.

Theorem 3.4. *Let $x \geq y \geq 2$ be real numbers and put $u = \frac{\log x}{\log y}$. For any fixed $\epsilon > 0$ the asymptotic formula*

$$(3.6) \quad \Psi(x, y) = x \rho(u) \left(1 + O\left(\frac{\log(u+1)}{\log y} \right) \right),$$

holds uniformly in the range $1 \leq u \leq \exp((\log y)^{\frac{3}{5}-\epsilon})$. The weaker relation

$$(3.7) \quad \log \frac{\Psi(x, y)}{x} = \left(1 + O\left(\exp(-(\log u)^{\frac{3}{5}-\epsilon}) \right) \right) \log \rho(u)$$

holds uniformly in the range $1 \leq u \leq y^{1-\epsilon}$. Lastly, as $u \rightarrow \infty$

$$(3.8) \quad \log \rho(u) = -u \left(\log u + \log \log(u+2) - 1 + O\left(\frac{\log \log(u+2)}{\log(u+2)} \right) \right).$$

Proof. See Theorems 1.1, 1.2, and Corollary 2.3 of [10].

We next give a bound for $\Psi(x/z, y)$ in terms of $\Psi(x, y)$.

Proposition 3.5. *There is an absolute constant c such that for all $1 \leq z \leq x$ and $y \geq 2$,*

$$\Psi\left(\frac{x}{z}, y\right) \ll (c \log x)^{\frac{\log z}{\log y}} \frac{\Psi(x, y)}{z}.$$

Proof. We prove this when $1 \leq z \leq y$; the general case follows by repeated application of this result. From Corollary 1.7 of [10] we obtain $\Psi\left(\frac{x}{z}, y\right) \leq c_1 \Psi(x, y) z^{-\alpha(x/z, y)}$ where $c_1 > 0$ is some absolute constant, and $\alpha = \alpha(x/z, y)$ is the unique positive solution to $\log(x/z) = \sum_{p \leq y} \log p / (p^\alpha - 1)$. Notice that

$$\log x \geq \log(x/z) \geq \sum_{n \leq y} \frac{\Lambda(n)}{n^\alpha} \geq \frac{1}{y^\alpha} \sum_{n \leq y} \Lambda(n) \geq \frac{y}{4y^\alpha}.$$

This shows that $y^{-\alpha} \leq 4(\log x)/y$ so that $z^{-\alpha} \leq (4 \log x)^{\frac{\log z}{\log y}}/z$. The result $\Psi(x/z, y) \leq c_1 (4 \log x)^{\log z / \log y} \Psi(x, y)/z$ follows for $1 \leq z \leq y$, and repeated applications of this result give $\Psi(x/z, y) \leq c_1 (4c_1 \log x)^{\log z / \log y} \Psi(x, y)/z$ in general.

We note here a useful corollary of this result:

Corollary 3.6. *Let $0 \leq \kappa < 1$, and let c be as in Proposition 3.5. Suppose $y \geq e(c \log x)^{\frac{1}{1-\kappa}}$. Then*

$$\sum_{n \in \mathcal{S}(x, y)} \frac{1}{n^\kappa} \ll \frac{\log y}{1-\kappa} \frac{\Psi(x, y)}{x^\kappa}, \quad \text{and} \quad \sum_{n \in \mathcal{S}(x, y)} \frac{1}{n^\kappa} \log \frac{x}{n} \ll \frac{\log y}{(1-\kappa)^2} \frac{\Psi(x, y)}{x^\kappa}.$$

If $y \geq (c \log x)^2$ then

$$\sum_{n \in \mathcal{S}(x, y)} \log \frac{x}{n} \ll \Psi(x, y).$$

Proof. By partial summation

$$\sum_{n \in \mathcal{S}(x, y)} \frac{1}{n^\kappa} = \int_{1-}^x \frac{1}{t^\kappa} d\Psi(t, y) = \frac{\Psi(x, y)}{x^\kappa} + \kappa \int_1^x \frac{\Psi(t, y)}{t^{1+\kappa}} dt.$$

Using Proposition 3.5 the second term above is

$$\ll \kappa \frac{\Psi(x, y)}{x} \int_1^x \frac{1}{t^\kappa} (c \log x)^{\frac{\log(x/t)}{\log y}} dt = \kappa \frac{\Psi(x, y)}{x} \int_1^x \frac{x^{\frac{\log(c \log x)}{\log y}}}{t^{\kappa + \frac{\log(c \log x)}{\log y}}} dt,$$

and using our hypothesis on y this is

$$\leq \frac{\kappa \log y}{1-\kappa} \frac{\Psi(x, y)}{x^\kappa}.$$

The first part of the corollary follows. The other two assertions are proved similarly.

Lemma 3.7. *Let $x \geq y \geq (\log x)^{1+\epsilon}$, and put $u = \frac{\log x}{\log y}$. Then*

$$\frac{\Psi(x, y \log y)}{\Psi(x, y)} = \exp\left(u \frac{\log \log y}{\log(y \log y)} (\log u + O(\log \log(u+2)))\right).$$

Proof. By Lemma 2.2 and Corollary 2.4 of [10] we get

$$\frac{\rho\left(\frac{\log x}{\log(y \log y)}\right)}{\rho\left(\frac{\log x}{\log y}\right)} = \exp\left(u \frac{\log \log y}{\log(y \log y)} (\log u + O(\log \log(u+2)))\right).$$

The lemma follows upon combining this with (3.6) when $u \leq \exp((\log y)^{\frac{3}{5}-\epsilon})$, and (3.7) for larger u .

Lemma 3.8. *Suppose $y \geq (\log x)^{\frac{3}{2}}$ and that $x \geq z \geq xy^{-\frac{1}{3}}$. Then*

$$\Psi(x+z, y) - \Psi(x, y) \gg z \frac{\Psi(x, y)}{x}.$$

This follows from Theorems 5.1 and 5.2 of [10]. The next result is an immediate consequence of Corollary 2.4 of [10].

Lemma 3.9. $\rho(u-v) \asymp \rho(u)$ if $|v| \ll 1/\log 2u$, for $u, u-v \geq 1$.

4. THE $2k$ -TH MOMENT OF $\sum_{n \leq x}^{\flat} X_n$

In this section we prove upper and lower bounds on the $2k$ -th moment of $\sum_{n \leq x}^{\flat} X_n$, where (throughout this section) the \flat indicates that the sum is over squarefree n coprime to q . These bounds will be useful in deducing many of our large character sums results.

Theorem 4.1. *Let $k \geq 1$ be an integer, and put $K = \max(k, \omega(q))$. Uniformly for all $x \geq K^{ek}$ we have*

$$(4.1) \quad \mathbb{E}\left(\left|\sum_{n \leq x}^{\flat} X_n\right|^{2k}\right)^{\frac{1}{2k}} \leq \mathbb{E}\left(\left|\sum_{n \leq x} X_n\right|^{2k}\right)^{\frac{1}{2k}} \leq x^{\frac{1}{2}} \left(\frac{\log x}{k}\right)^{\frac{(k-1)^2}{2k}} e^{O(k)},$$

and

$$(4.2) \quad \begin{aligned} \mathbb{E}\left(\left|\sum_{n \leq x}^{\flat} X_n\right|^{2k}\right)^{\frac{1}{2k}} &\geq \left(\sum_{N \leq x^k}^{\flat} d_k(N, x)^2\right)^{\frac{1}{2k}} \\ &\geq \frac{x^{\frac{1}{2}}}{(\log x)^{1-\frac{1}{2k}}} \left(\frac{\log x}{k \log K}\right)^{\frac{k}{2}} \left(\log\left(\frac{\log x}{k \log K}\right)\right)^{O(k)}. \end{aligned}$$

Proof of the upper bound (4.1). Observe that

$$\begin{aligned} \mathbb{E}\left(\left|\sum_{n \leq x} X_n\right|^{2k}\right) &= \sum_{N \leq x^k} d_k(N, x)^2 \\ &= \#\{b_1, b_2, \dots, b_k, B_1, B_2, \dots, B_k \leq x : b_1 \dots b_k = B_1 \dots B_k\}. \end{aligned}$$

To each solution above we associate a $k \times k$ “g.c.d.-matrix” of integers $A = (a_{i,j})$ defined as follows: Put $a_{1,1} = (b_1, B_1)$, and then define (using induction on $i + j$)

$$a_{i,j} = \left(\frac{b_i}{\prod_{\ell < j} a_{i,\ell}}, \frac{B_j}{\prod_{\ell < i} a_{\ell,j}} \right),$$

so that, for $1 \leq i \leq k$,

$$b_i = \prod_{\ell=1}^k a_{i,\ell}, \quad \text{and} \quad B_i = \prod_{\ell=1}^k a_{\ell,i}.$$

We will bound the number of $k \times k$ integer matrices $A = (a_{i,j})$ with all row and column products $\prod_{\ell=1}^k a_{i,\ell}$, $\prod_{\ell=1}^k a_{\ell,i}$ less than x , which thus implies an upper bound in our original problem. The number of choices for $a_{k,k}$ is

$$\leq \min \left(\frac{x}{\prod_{i=1}^{k-1} a_{i,k}}, \frac{x}{\prod_{i=1}^{k-1} a_{k,i}} \right) \leq \frac{x}{\prod_{i=1}^{k-1} (a_{i,k} a_{k,i})^{\frac{1}{2}}}.$$

Next we sum over the possibilities for $a_{i,k}$, $a_{k,i}$ ($1 \leq i \leq k-1$). Notice that $a_{i,k} \leq x / \prod_{j=1}^{k-1} a_{i,j}$ and $a_{k,i} \leq x / \prod_{j=1}^{k-1} a_{j,i}$, and so

$$\sum_{a_{i,k}} \frac{1}{\sqrt{a_{i,k}}} \leq \frac{2\sqrt{x}}{\prod_{j=1}^{k-1} a_{i,j}^{\frac{1}{2}}}, \quad \sum_{a_{k,i}} \frac{1}{\sqrt{a_{k,i}}} \leq \frac{2\sqrt{x}}{\prod_{j=1}^{k-1} a_{j,i}^{\frac{1}{2}}}.$$

Thus given $a_{i,j}$ ($1 \leq i, j \leq k-1$), the number of possibilities for the last row and column of A is

$$\leq \frac{2^{2k-2} x^k}{\prod_{1 \leq i, j \leq k-1} a_{i,j}}.$$

We now sum this over all the possibilities for $a_{i,j}$ ($1 \leq i, j \leq k-1$). Keeping in mind that $\prod_{j=1}^{k-1} a_{i,j} \leq x$ for all $1 \leq i \leq k-1$, we see that this is

$$\leq 2^{2k-2} x^k \prod_{i=1}^{k-1} \left(\sum_{a_{i,1} \dots a_{i,k-1} \leq x} \frac{1}{a_{i,1} \dots a_{i,k-1}} \right) = 2^{2k-2} x^k \left(\sum_{n \leq x} \frac{d_{k-1}(n)}{n} \right)^{k-1}.$$

Now for any $\alpha > 0$

$$\sum_{n \leq x} \frac{d_{k-1}(n)}{n} \leq x^\alpha \sum_{n \leq x} \frac{d_{k-1}(n)}{n^{1+\alpha}} \leq x^\alpha \zeta(1+\alpha)^{k-1} = x^\alpha \left(\frac{1}{\alpha} + O(1) \right)^{k-1}.$$

Choosing (optimally) $\alpha = k / \log x$ we obtain (since $k \leq \log x$)

$$\sum_{n \leq x} \frac{d_{k-1}(n)}{n} \leq \left(\frac{\log x}{k} \right)^{k-1} e^{O(k)}.$$

To sum up, we have shown that

$$\mathbb{E}\left(\left|\sum_{n \leq x} X_n\right|^{2k}\right) \leq 2^{2k-2} x^k \left(\sum_{n \leq x} \frac{d_{k-1}(n)}{n}\right)^{k-1} \leq x^k \left(\frac{\log x}{k}\right)^{(k-1)^2} e^{O(k^2)},$$

and (4.1) follows.

Proof of the lower bound (4.2). We bound

$$\mathbb{E}\left(\left|\sum_{n \leq x} X_n\right|^{2k}\right) \geq \sum_{N \leq x^k} d_k(N, x)^2$$

by focussing only on special values of N for which we expect $d_k(N, x)$ to be large. Specifically, we let y denote an integer parameter to be chosen later, and consider only those $N \leq x^k$ which are square-free, coprime to q , and have ky distinct prime factors. Using Cauchy's inequality, we find that

$$(4.3) \quad \sum_{N \leq x^k} d_k(N, x)^2 \geq \left(\sum_{\substack{N \leq x^k \\ \omega(N)=ky}} d_k(N, x)\right)^2 \frac{1}{\pi(x^k, ky)}.$$

We shall choose $y = [kL_0]$ where $L_0 = \log\left(\frac{\log x}{k \log K}\right)$. Using (3.1) (after checking that the constraint (3.2) is met) we find that

$$\pi(x^k, ky) = \frac{x^k}{k \log x} \frac{L^{ky+O(\frac{ky}{L})}}{(ky)!} \quad \text{where } L = \log\left(\frac{\log x}{y \log(ky)}\right).$$

Since $L_0 - L = \log \frac{y}{k} + \log \frac{\log(ky)}{\log K} \ll \log L_0$ we conclude that

$$(4.4) \quad \pi(x^k, ky) = \frac{x^k}{k \log x} \frac{L_0^{ky}}{(ky)!} \exp\left(O\left(ky \frac{\log L_0}{L_0}\right)\right).$$

Next observe that

$$\sum_{\substack{N \leq x^k \\ \omega(N)=ky}} d_k(N, x) \geq \sum_{\substack{m_1, \dots, m_k \leq x \\ \omega(m_i)=y}}^* 1$$

where the $*$ indicates that the sum is over squarefree m_1 coprime to q , and pairwise coprime. We deduce from (3.5) that this is

$$\geq \left(\sum_{\substack{n \leq x, \\ p|n \implies p > p_\ell}} \mu(n)^2\right)^k \quad \text{where } \ell = (k-1)y + \omega(q).$$

Now we use Theorem 3.1 to bound this quantity. Our assumption that $k \log K \leq e^{-1} \log x$ ensures that the criteria (3.2) and (3.3) are met. Hence, with $z = \max(\ell, y^2)$,

$$\sum_{\substack{n \leq x, \\ p|n \implies p > p_\ell}} \mu(n)^2 \geq \frac{x}{\log x} \frac{L_1^{y+O(\frac{y}{L_1})}}{y!} \quad \text{where } L_1 = \log\left(\frac{\log x}{y \log \sqrt{z}}\right).$$

Since $L_0 - L_1 \ll \log L_0$ we obtain

$$(4.5) \quad \sum_{\substack{N \leq x^k \\ \omega(N) = ky}}^b d_k(N, x) \geq \frac{x^k}{(\log x)^k} \frac{L_0^{ky}}{y!^k} \exp\left(O\left(ky \frac{\log L_0}{L_0}\right)\right).$$

Using (4.4) and (4.5) in (4.3) we deduce

$$\left(\sum_{N \leq x^k}^b d_k(N, x)^2\right)^{\frac{1}{2k}} \geq \frac{x^{\frac{1}{2}}}{(\log x)^{1 - \frac{1}{2k}}} \frac{L_0^{\frac{y}{2}} (ky)!^{\frac{1}{2k}}}{y!} \exp\left(O\left(\frac{y \log L_0}{L_0}\right)\right),$$

and the lower bound (4.2) follows upon using Stirling's formula, and recalling the definitions of y and L_0 .

Next we give lower bounds on the $2k$ -th moment of $\sum_{n \leq x}^b X_n$ when x is small (roughly, $x = K^A$ for some integer A).

Theorem 4.2. *Let k, A be positive integers, and put $K = \max(k, \omega(q))$. For all $x \geq (4(Ak + K) \log(Ak + K))^A$ we have, uniformly,*

$$(4.6) \quad \mathbb{E}\left(\left|\sum_{n \leq x}^b X_n\right|^{2k}\right)^{\frac{1}{2k}} \geq \left(\sum_{N \leq x^k}^b d_k(N, x)^2\right)^{\frac{1}{2k}} \gg x^{\frac{1}{2}} \left(\frac{k}{\log x}\right)^{\frac{A}{2}}.$$

Proof. Plainly

$$\mathbb{E}\left(\left|\sum_{n \leq x}^b X_n\right|^{2k}\right) = \sum_{N \leq x^k}^b d_k(N, x)^2 \geq \sum_{\substack{N \leq x^k \\ (N, q) = 1}}^* d_k(N, x)^2$$

where the $*$ indicates that we sum over only those N that are square-free and composed of exactly Ak prime factors, all less than $x^{1/A}$. Note that for such N , $d_k(N, x)$ is at least the number of k -tuples m_1, \dots, m_k whose product is N , where each m_i is the product of exactly A primes. Thus $d_k(N, x) \geq (Ak)!/A!^k$, and so

$$(4.7) \quad \begin{aligned} \sum_{N \leq x^k}^b d_k(N, x)^2 &\geq \frac{(Ak)!}{(A!)^k} \sum_{\substack{N \leq x^k \\ (N, q) = 1}}^* d_k(N, x) \geq \frac{(Ak)!}{(A!)^k} \frac{1}{(A!)^k} \sum_{\substack{p_1, \dots, p_{Ak} \leq x^{\frac{1}{A}} \\ p_i \neq p_j, p_i \nmid q}} 1 \\ &\geq \frac{(Ak)!}{(A!)^{2k}} \prod_{j=1}^{Ak} \left(\pi\left(x^{\frac{1}{A}}\right) - \sum_{\substack{p|q \\ p \leq x^{\frac{1}{A}}}} 1 - j + 1\right). \end{aligned}$$

By the prime number theorem, and our lower bound for x , we get

$$\pi\left(x^{\frac{1}{A}}\right) - \sum_{\substack{p|q \\ p \leq x^{\frac{1}{A}}}} 1 - Ak \geq \pi\left(x^{\frac{1}{A}}\right) - Ak - K \geq \frac{Ax^{\frac{1}{A}}}{\log x} - Ak - K \geq \frac{Ax^{\frac{1}{A}}}{2 \log x}.$$

Using this, and Stirling's formula, in (4.7) we get Theorem 4.2.

5. APPLICATIONS TO LARGE CHARACTER SUMS

In this section, we use Theorems 4.1 and 4.2 to deduce many of our results on large character sums. We split these results in two parts: when $\log \log x \leq (\frac{1}{2} + o(1)) \log \log q$ where we use Theorem 4.2, and when $\log \log x \geq (\frac{1}{2} + o(1)) \log \log q$ where Theorem 4.1 is most useful.

5a. Large character sums when $\log \log x \leq (\frac{1}{2} + o(1)) \log \log q$.

Proof of Theorem 4. Recall that $x = (10 \log q)^B$ for some $B \geq 1$. We take $k = \lfloor \frac{\log q}{\log x} \rfloor$ and $A = \lfloor B \rfloor$. Notice that $K = \max(k, \omega(q)) \leq (1 + o(1)) \frac{\log q}{\log \log q}$, and so $kA + K \leq \frac{5}{2} \frac{\log q}{\log \log q}$. We check now that the condition of Theorem 4.2 is met, and so

$$\Delta \gg x^{\frac{1}{2}} \left(\frac{k}{\log x} \right)^{\frac{\lfloor B \rfloor}{2}} \geq \frac{x^{\frac{1}{2} + \frac{\lfloor B \rfloor}{2B}}}{(4 \log x)^{\lfloor B \rfloor}}.$$

This gives the portion of Theorem 4 not having any restriction on q .

For our next application we suppose that $\omega(q) \leq (\log q)^{\frac{B}{B+1} - \epsilon}$. Here, we take $A = \lfloor B \rfloor + 1$, and $k = \lfloor x^{\frac{1}{A}} / (10 \log x) \rfloor$. Our bound on $\omega(q)$ ensures that the condition of Theorem 4.2 is met, and so

$$\Delta \gg x^{1/2} \left(\frac{k}{\log x} \right)^{\frac{\lfloor B \rfloor + 1}{2}} \geq \frac{x}{(4 \log x)^{\lfloor B \rfloor + 1}}.$$

This gives the second part of Theorem 4. Corollaries 1 and 2 are immediate consequences.

5b. Large character sums when $\log \log x \geq (\frac{1}{2} + o(1)) \log \log q$.

Proof of Theorem 5. We take $k = \lfloor \frac{c}{\eta} \sqrt{\frac{\log q}{\log \log q}} \rfloor$ for a fixed, but sufficiently small positive constant c . Since $K \leq \log q$, one can verify that the condition $x \geq K^{ek}$ of Theorem 4.1 is met. Hence by (4.2) we get

$$\Delta \gg \frac{x^{\frac{1}{2}}}{(\log x)^{1 - \frac{1}{2k}}} \left(\frac{\log x}{k \log \log q} \right)^{\frac{k}{2}} \left(\log \frac{\log x}{k \log \log q} \right)^{O(k)} = \frac{x^{\frac{1}{2}}}{(\log x)^{1 - \frac{1}{2k}}} \left(\frac{\eta \tau}{c} \right)^{\frac{k}{2}} \left(\log \frac{\eta \tau}{c} \right)^{O(k)}.$$

The result follows if c is sufficiently small.

Proofs of Theorems 6 and 7. Both these results follow upon using (4.2) with $k = \lfloor \frac{\log q}{\log x} \rfloor$: the hypotheses in the Theorems ensure that $x \geq (\log q)^{ek} \geq K^{ek}$.

6. THE $2k$ -TH MOMENT OF $\sum_{n \leq x} X_n$

Here we explore more finely the $2k$ -th moment of $\sum_{n \leq x} X_n$. Put

$$\Psi_\ell(x, y; X_n) = \sum_{n \in \mathcal{S}_\ell(x, y)} X_n.$$

Our aim in this section is to show that $\sum_{n \leq x} X_n$ behaves like $\Psi_0(x, y; X_n)$ most of the time, for an appropriately chosen y .

Theorem 6.1. *Suppose $k \geq 2$ is an integer, and that $y \geq C \log^2 x$ for a large absolute constant C . Then*

$$\mathbb{E} \left(\left| \sum_{n \leq x} X_n - \Psi_0(x, y; X_n) \right|^{2k} \right)^{\frac{1}{2k}} \ll \Psi(x, y) \left(\frac{k \log y \log^2 x}{y} \right)^{\frac{1}{2}} \exp \left(O \left(\frac{k \log^2 x \log \log x}{y} \right) \right).$$

Proof. Put $u = \frac{\log x}{\log y}$. By Minkowski's inequality

$$(6.1) \quad \mathbb{E} \left(\left| \sum_{n \leq x} X_n - \Psi_0(x, y; X_n) \right|^{2k} \right)^{\frac{1}{2k}} = \mathbb{E} \left(\left| \sum_{\ell=1}^{[u]} \Psi_\ell(x, y; X_n) \right|^{2k} \right)^{\frac{1}{2k}} \\ \leq \sum_{\ell=1}^{[u]} \mathbb{E} (|\Psi_\ell(x, y; X_n)|^{2k})^{\frac{1}{2k}}.$$

Observe that

$$\mathbb{E} (|\Psi_\ell(x, y; X_n)|^{2k}) = \sum_{\substack{m_1 \dots m_k = m'_1 \dots m'_k \\ m_i, m'_i \in \mathcal{S}(x/y^\ell, y)}} \sum_{\substack{n_1 \dots n_k = n'_1 \dots n'_k \\ n_i \leq x/m_i, n'_i \leq x/m'_i \\ \Omega(n_i) = \Omega(n'_i) = \ell \\ p|n_i, n'_i \implies p > y}} 1.$$

Now, given $N = n_1 \dots n_k$, the number of factorizations $N = n'_1 \dots n'_k$ with each $\Omega(n'_i) = \ell$ is $\leq (k\ell)!/\ell!^k$, and so the inner sum over n_i, n'_i is

$$\leq \sum_{\substack{n_1, \dots, n_k \\ n_i \leq x/m_i \\ \Omega(n_i) = \ell \\ p|n_i \implies p > y}} \frac{(k\ell)!}{\ell!^k} \ll \frac{k^{k\ell}}{\ell^{(k-1)/2}} \prod_{i=1}^k \sum_{\substack{n_i \leq x/m_i \\ \Omega(n_i) = \ell \\ p|n_i \implies p > y}} 1.$$

Using Lemma 3.3 (note that $y \geq C \log^2 x \geq 2\ell^2$) this is

$$\leq \frac{x^k k^{k\ell}}{m_1 \dots m_k} \frac{(\log \log x + O(1))^{k(\ell-1)}}{(\ell-1)!^k} \left(\frac{c}{\log y} \right)^k \frac{1}{\ell^{(k-1)/2}} \\ \ll \frac{x^k}{m_1 \dots m_k} \frac{(2k \log \log x)^{k\ell}}{(\ell! \log y \log \log x)^k}.$$

Now

$$\sum_{\substack{m_1 \dots m_k = m'_1 \dots m'_k \\ m_i, m'_i \in \mathcal{S}(x/y^\ell, y)}} \frac{1}{m_1 \dots m_k} = \mathbb{E} \left(\left| \sum_{n \in \mathcal{S}(x/y^\ell, y)} \frac{X_n}{\sqrt{n}} \right|^{2k} \right) \leq \left(\sum_{n \in \mathcal{S}(x/y^\ell, y)} \frac{1}{\sqrt{n}} \right)^{2k},$$

and, by Corollary 3.6 and Proposition 3.5

$$\sum_{n \in \mathcal{S}(x/y^\ell, y)} \frac{1}{\sqrt{n}} \ll \log y \frac{\Psi(x/y^\ell, y)}{(x/y^\ell)^{\frac{1}{2}}} \ll \log y (c \log x)^\ell \frac{\Psi(x, y)}{\sqrt{xy^\ell}}.$$

Therefore, combining the bounds above, we get

$$\mathbb{E} \left(|\Psi_\ell(x, y; X_n)|^{2k} \right)^{\frac{1}{2k}} \ll \Psi(x, y) \left(\frac{\log y}{\ell! \log \log x} \right)^{1/2} \left(\frac{ck \log^2 x \log \log x}{y} \right)^{\ell/2}$$

for some constant $c > 0$. Therefore, substituting this into (6.1), we get

$$\begin{aligned} \mathbb{E} \left(\left| \sum_{n \leq x} X_n - \Psi_0(x, y; X_n) \right|^{2k} \right)^{\frac{1}{2k}} &\ll \Psi(x, y) \left(\frac{\log y}{\log \log x} \right)^{1/2} \sum_{\ell=1}^{[u]} \frac{1}{\ell!^{1/2}} \left(\frac{ck \log^2 x \log \log x}{y} \right)^{\ell/2} \\ &\ll \Psi(x, y) \left(\frac{k \log^2 x \log y}{y} \right)^{\frac{1}{2}} \exp \left(O \left(\frac{k \log^2 x \log \log x}{y} \right) \right), \end{aligned}$$

since $\sum_{j=0}^{\infty} \xi^{\frac{j}{2}} / j!^{\frac{1}{2}} \ll e^\xi$ for all $\xi \geq 0$. This proves the theorem.

We now derive a good lower bound for the $2k$ -th moment of $\sum_{n \leq x} X_n$. This is a considerable refinement of Theorem 4.2, in the case that $q = 1$.

Theorem 6.2. *Let $k \geq 2$ be an integer. Then for all $y \geq 2$ we have*

$$\mathbb{E} \left(\left| \sum_{n \leq x} X_n \right|^{2k} \right)^{\frac{1}{2k}} \geq \Psi(x, y) \exp \left(-\frac{2y \log \log x}{k \log y} + O \left(\frac{1}{\log x} \right) \right).$$

Proof. Using Lemma 2.3 with $f(n) = 1$, and $g(n) =$ the characteristic function of $\mathcal{S}(x, y)$ we have

$$\mathbb{E} \left(\left| \sum_{n \leq x} X_n \right|^{2k} \right) \geq \mathbb{E} \left(\left| \sum_{n \in \mathcal{S}(x, y)} X_n \right|^{2k} \right).$$

We bound the right side above by picking only those X_n for which $|\arg(X_p)| \leq \pi(\log x)^{-2}$ for all $p \leq y$ (where \arg is defined to lie between $-\pi$ and π). The probability of this happening is clearly $(\log x)^{-2\pi(y)}$. For such a choice of X_p 's note that

$$\left| \sum_{n \in \mathcal{S}(x, y)} X_n - \Psi(x, y) \right| \leq \sum_{n \in \mathcal{S}(x, y)} |X_n - 1| \ll \sum_{n \in \mathcal{S}(x, y)} \frac{\Omega(n)}{\log^2 x} \ll \frac{\Psi(x, y)}{\log x}.$$

Hence

$$\mathbb{E} \left(\left| \sum_{n \in \mathcal{S}(x, y)} X_n \right|^{2k} \right) \geq \Psi(x, y)^{2k} \exp \left(-2\pi(y) \log \log x + O \left(\frac{k}{\log x} \right) \right),$$

and the result follows.

Combining Theorems 6.1 and 6.2 we get good upper and lower estimates for large moments of $\sum_{n \leq x} X_n$; and in fact, we get an asymptotic formula for very large k .

Corollary 6.3. *If $k \geq C \log x$ is an integer then*

$$(6.3) \quad \Psi(x, k \log^5 k \log x) \left(1 + O\left(\frac{1}{\log x}\right)\right) \geq \mathbb{E}\left(\left|\sum_{n \leq x} X_n\right|^{2k}\right)^{\frac{1}{2k}} \geq \Psi\left(x, \frac{k \log x}{\log^3 k}\right) \left(1 + O\left(\frac{1}{\log x}\right)\right).$$

If $\log k / \sqrt{\log x} \log \log x \rightarrow \infty$ then

$$(6.4) \quad \mathbb{E}\left(\left|\sum_{n \leq x} X_n\right|^{2k}\right)^{\frac{1}{2k}} = (1 + o(1))\Psi(x, k).$$

Proof. From Theorem 6.2 we get

$$\mathbb{E}\left(\left|\sum_{n \leq x} X_n\right|^{2k}\right)^{\frac{1}{2k}} \geq \Psi\left(x, \frac{k \log x}{\log^3 k}\right) \exp\left(O\left(\frac{1}{\log x} + \frac{\log x}{\log^3 k}\right)\right).$$

The lower bound of (6.3) now follows upon appealing to Lemma 3.7. Using Minkowski's inequality and Theorem 6.1 (with $y = k \log^4 k \log x$) we get, since $|\Psi_0(x, y; X_n)| \leq \Psi(x, y)$,

$$\begin{aligned} \mathbb{E}\left(\left|\sum_{n \leq x} X_n\right|^{2k}\right)^{\frac{1}{2k}} &\leq \mathbb{E}\left(|\Psi_0(x, y; X_n)|^{2k}\right)^{\frac{1}{2k}} + O\left(\Psi(x, y) \left(\frac{\log x}{\log^3 k}\right)^{\frac{1}{2}} \exp\left(O\left(\frac{\log x}{\log^3 k}\right)\right)\right) \\ &\leq \Psi(x, k \log^4 k \log x) \exp\left(O\left(\frac{\log x}{\log^3 k}\right)\right). \end{aligned}$$

The upper bound of (6.3) follows from this and Lemma 3.7. By Lemma 3.7 we deduce that if $k > \exp(\sqrt{\log x})$ then

$$\Psi(x, k(\log k)^{O(1)}) = \Psi(x, k) \exp\left(O\left(\log x \frac{(\log \log x)^2}{\log^2 k}\right)\right).$$

Therefore (6.4) follows from (6.3).

7. IMPLICATIONS FOR CHARACTER SUMS: PROOFS OF THEOREMS 1 AND 3

Observe that for any integer $k \leq \frac{\log q}{\log x}$, and any y , we have

$$\frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left| \sum_{n \leq x} \chi(n) - \Psi(x, y; \chi) \right|^{2k} \leq \mathbb{E}\left(\left|\sum_{n \leq x} X_n - \Psi(x, y; X_n)\right|^{2k}\right).$$

Using Theorem 6.1 we deduce that if $y \geq C \log^2 x$ then

$$(7.1) \quad \begin{aligned} &\frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left| \sum_{n \leq x} \chi(n) - \Psi(x, y; \chi) \right|^{2k} \\ &\leq c^k \Psi(x, y)^{2k} \left(\frac{k \log y \log^2 x}{y}\right)^k \exp\left(O\left(\frac{k^2 \log \log x \log^2 x}{y}\right)\right), \end{aligned}$$

for some constant $c > 0$.

Proof of Theorem 1. We choose $k = \lfloor \frac{\log q}{\log x} \rfloor$. It follows from (7.1) that for any $A > 1$ there are fewer than qA^{-2k} characters $\chi \pmod{q}$ not satisfying

$$\left| \sum_{n \leq x} \chi(n) - \Psi(x, y; \chi) \right| \ll A \Psi(x, y) \left(\frac{\log q \log x \log y}{y} \right)^{\frac{1}{2}} \exp \left(O \left(\frac{\log q \log x \log \log x}{y} \right) \right).$$

Taking $y \geq \log q \log x (\log \log q)^5$, and $A = 10$ above, we obtain the first assertion of Theorem 1.

Next, take $y = (\log q + \log^2 x)(\log \log q)^4$, and $A = \exp(\frac{\log x}{(\log \log q)^2})$. We deduce that with at most $q^{1 - \frac{1}{(\log \log q)^2}}$ exceptions

$$\left| \sum_{n \leq x} \chi(n) \right| \ll \Psi(x, y) \exp \left(O \left(\frac{\log x}{(\log \log q)^2} \right) \right) \ll \Psi(x, y \log y),$$

using Lemma 3.7. This gives the second part of Theorem 1.

We now move towards the proof of Theorem 3. We begin with a lemma which may be of independent interest.

Lemma 7.1. *Let $f(n)$ be any completely multiplicative function with $|f(n)| = 1$ for all n . Let $2 \leq x \leq \exp((\log q)^{\frac{1}{2}})$, and let $y = \log q / (\log x (\log \log q)^8)$. There are at least $q^{1 - \frac{1}{(\log \log q)^2}}$ characters $\chi \pmod{q}$ with*

$$\sum_{\substack{n \in \mathcal{S}(x, y) \\ (n, q) = 1}} \chi(n) = \sum_{\substack{n \in \mathcal{S}(x, y) \\ (n, q) = 1}} f(n) + O \left(\frac{\Psi(x, y; \chi_0)}{(\log \log q)^2} \right).$$

Proof. Note that for any integer $k \leq \frac{\log q}{\log x}$

$$(7.2) \quad \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left| \sum_{\substack{n \in \mathcal{S}(x, y) \\ (n, q) = 1}} \frac{\chi(n) \overline{f(n)} + 1}{2} \right|^{2k} = \mathbb{E} \left(\left| \sum_{\substack{n \in \mathcal{S}(x, y) \\ (n, q) = 1}} \frac{X_n + 1}{2} \right|^{2k} \right).$$

We give a lower bound for the right side of (7.2) by the argument of Theorem 6.2. We pick only those X_n with $|\arg(X_p)| \leq \frac{\pi}{\log q}$ for all $p \leq y$. This happens with probability $\geq (\log q)^{-\pi(y)} \geq \exp(-3y)$, and for such a choice

$$\sum_{\substack{n \in \mathcal{S}(x, y) \\ (n, q) = 1}} \frac{X_n + 1}{2} = \Psi(x, y; \chi_0) + O \left(\sum_{\substack{n \in \mathcal{S}(x, y) \\ (n, q) = 1}} \frac{\Omega(n)}{\log q} \right) = \Psi(x, y; \chi_0) \left(1 + O \left(\frac{\log x}{\log q} \right) \right).$$

It follows that

$$\frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \left| \sum_{\substack{n \in \mathcal{S}(x, y) \\ (n, q) = 1}} \frac{\chi(n) \overline{f(n)} + 1}{2} \right|^{2k} \geq \Psi(x, y; \chi_0)^{2k} e^{-3y} \left(1 + O \left(\frac{\log x}{\log q} \right) \right)^{2k}.$$

We deduce immediately that there are at least $\varphi(q)e^{-4y}(1 + O(\frac{\log x}{\log q}))^{2k}$ characters $\chi \pmod{q}$ with

$$\left| \sum_{\substack{n \in \mathcal{S}(x,y) \\ (n,q)=1}} \frac{\chi(n)\overline{f(n)} + 1}{2} \right| \geq \Psi(x, y; \chi_0) e^{-\frac{2y}{k}} \left(1 + O\left(\frac{\log x}{\log q}\right) \right).$$

Choosing $k = \lceil \log q / (\log x (\log \log q)^4) \rceil$ we conclude that there are $\geq q^{1 - \frac{1}{(\log \log q)^2}}$ characters $\chi \pmod{q}$ for which

$$(7.3) \quad \left| \sum_{\substack{n \in \mathcal{S}(x,y) \\ (n,q)=1}} \frac{\chi(n)\overline{f(n)} + 1}{2} \right| = \Psi(x, y; \chi_0) \left(1 + O\left(\frac{1}{(\log \log q)^4}\right) \right).$$

Let $\alpha = (\sum_{n \in \mathcal{S}(x,y), (n,q)=1} \chi(n)\overline{f(n)}) / \Psi(x, y; \chi_0)$, so that $|\alpha| \leq 1$, and (7.3) states that $|\alpha + 1| = 2 + O(1/L^4)$ where $L = \log \log q$. By the triangle inequality we have $2 \geq 1 + |\alpha| \geq |\alpha + 1| = 2 + O(1/L^4)$, and so $|1 - \alpha|^2 = 2(1 + |\alpha|^2) - |\alpha + 1|^2 = O(1/L^4)$. Thus $|1 - \alpha| = O(1/L^2)$ and the Lemma follows.

Proof of Theorem 3. We suppose that $\log x \leq \frac{(\log \log q)^2}{(\log \log \log q)^2}$. Let y be as in Lemma 7.1, and put $y_1 = \log q (\log \log q)^7$. Using Theorem 1 and Lemma 3.7, we get that with at most $q^{1 - \frac{1}{\log x}}$ exceptions

$$(7.4) \quad \begin{aligned} \sum_{n \leq x} \chi(n) &= \Psi(x, y_1; \chi) + O\left(\frac{\Psi(x, y_1)}{(\log \log q)^2}\right) \\ &= \Psi(x, y; \chi) + O(|\Psi(x, y_1) - \Psi(x, y)|) + O\left(\frac{\Psi(x, \log q)}{(\log \log q)^2}\right) \\ &= \Psi(x, y; \chi) + O\left(\Psi(x, \log q) \frac{\log x (\log \log \log q)^2}{(\log \log q)^2}\right). \end{aligned}$$

Given any angle θ , we take $f(n) = n^{\frac{i\theta}{\log x}}$ in Lemma 7.1. We deduce that there are at least $q^{1 - \frac{1}{\log x}}$ characters $\chi \pmod{q}$ with

$$\begin{aligned} \Psi(x, y; \chi) &= \sum_{\substack{n \in \mathcal{S}(x,y) \\ (n,q)=1}} n^{\frac{i\theta}{\log x}} + O\left(\frac{\Psi(x, y; \chi_0)}{(\log \log q)^2}\right) \\ &= e^{i\theta} \Psi(x, y; \chi_0) + O\left(\sum_{\substack{n \in \mathcal{S}(x,y) \\ (n,q)=1}} \frac{\log(x/n)}{\log x} + \frac{\Psi(x, y; \chi_0)}{(\log \log q)^2}\right) \\ &= e^{i\theta} \Psi(x, y; \chi_0) + O\left(\frac{\Psi(x, \log q)}{\log x}\right) \end{aligned}$$

by Corollary 3.6, and Lemma 3.7. Theorem 3 follows by combining this with (7.4).

8. RESULTS CONDITIONAL ON GRH: PROOF OF THEOREM 2

We begin with two standard lemmas which we shall use to prove the conditional Theorem 2.

Lemma 8.1. *Let $s = \sigma + it$ with $\sigma > \frac{1}{2}$ and $|t| \leq 3q$. Let $\frac{1}{2} \leq \sigma_0 < \sigma$, and suppose that there are no zeros of $L(z, \chi)$ inside the rectangle $\{z : \sigma_0 \leq \operatorname{Re}(z) \leq 1, |\operatorname{Im}(z) - t| \leq 3\}$. Then*

$$|\log L(s, \chi)| \ll \frac{\log q}{\sigma - \sigma_0}.$$

Proof. First note that if $\sigma \geq 2$ then $|\log L(s, \chi)| \ll 1$ and there is nothing to prove. We may hence assume that $\sigma < 2$. Consider the circles with centre $2 + it$ and radii $r := 2 - \sigma < R := 2 - \sigma_0$, so that the smaller circle passes through s . By our hypothesis $\log L(s, \chi)$ is analytic inside the larger circle. For a point z on the larger circle we use the estimate $|L(z, \chi)| \leq 2q|z| \leq q^3$, so that

$$\operatorname{Re} \log L(z, \chi) = \log |L(z, \chi)| \leq 3 \log q.$$

The Borel-Caratheodory theorem precisely states that for any point on the smaller circle (and so for s in particular) we have

$$\begin{aligned} |\log L(s, \chi)| &\leq \frac{2r}{R-r} \max_{|z-2-it|=R} \operatorname{Re} \log L(z, \chi) + \frac{R+r}{R-r} |\log L(2+it, \chi)| \\ &\ll \frac{1}{\sigma - \sigma_0} \log q + \frac{1}{\sigma - \sigma_0} \ll \frac{\log q}{\sigma - \sigma_0}. \end{aligned}$$

Lemma 8.2. *Let $s = \sigma + it$ with $\sigma > \frac{1}{2}$ and $|t| \leq 2q$. Let $y \geq 2$ be a real number, let $\frac{1}{2} \leq \sigma_0 < \sigma$. Suppose that there are no zeros of $L(z, \chi)$ inside the rectangle $\{z : \sigma_0 \leq \operatorname{Re}(z) \leq 1, |\operatorname{Im}(z) - t| \leq y + 3\}$. Put $\sigma_1 = \min(\frac{\sigma + \sigma_0}{2}, \sigma_0 + \frac{1}{\log y})$. Then*

$$\log L(s, \chi) = \sum_{n=2}^y \frac{\Lambda(n)\chi(n)}{n^s \log n} + O\left(\frac{\log q}{(\sigma_1 - \sigma_0)^2} y^{\sigma_1 - \sigma}\right).$$

Proof. Without loss of generality we may assume that $y \in \mathbb{Z} + \frac{1}{2}$. By Perron's formula (see [3]) we obtain, with $c = 1 - \sigma + \frac{1}{\log y}$,

$$\begin{aligned} \frac{1}{2\pi i} \int_{c-iy}^{c+iy} \log L(s+w, \chi) \frac{y^w}{w} dw &= \sum_{m=2}^y \frac{\Lambda(m)\chi(m)}{m^s \log m} + O\left(\frac{1}{y} \sum_{n=1}^{\infty} \frac{y^c}{n^{\sigma+c}} \frac{1}{|\log(y/n)|}\right) \\ (8.1) \qquad \qquad \qquad &= \sum_{m=2}^y \frac{\Lambda(m)\chi(m)}{m^s \log m} + O(y^{-\sigma} \log y). \end{aligned}$$

We move the line of integration from the line $\operatorname{Re}(w) = c$ to the line $\operatorname{Re}(w) = \sigma_1 - \sigma < 0$. Our hypothesis ensures that the integrand is regular over the region

where the line is moved, except for a simple pole at $w = 0$ with residue $\log L(s, \chi)$. Hence the left side of (8.1) equals $\log L(s, \chi)$ plus

$$\frac{1}{2\pi i} \left(\int_{c-iy}^{\sigma_1-\sigma-iy} + \int_{\sigma_1-\sigma-iy}^{\sigma_1-\sigma+iy} + \int_{\sigma_1-\sigma+iy}^{c+iy} \right) \log L(s+w, \chi) \frac{y^w}{w} dw \ll \frac{\log q}{(\sigma_1 - \sigma_0)^2} y^{\sigma_1 - \sigma},$$

using Lemma 8.1 to estimate $\log L(s+w, \chi)$ in the above integrals. The result follows

If we assume the GRH for $L(s, \chi)$ then the hypotheses of Lemmas 8.1 and 8.2 are met with $\sigma_0 = \frac{1}{2}$, and so the conclusions drawn there are valid. The advantage of these formulations is that they can be used unconditionally for many characters $\chi \pmod{q}$ by appealing to zero-density estimates; we exploit this to get large values of $L(\sigma, \chi)$ in [7].

We now assume the Riemann hypothesis for $L(s, \chi)$, and proceed to prove Theorem 2. Define

$$L(s, \chi; y) = L(s, \chi) \prod_{p \leq y} \left(1 - \frac{\chi(p)}{p^s} \right),$$

so that $L(s, \chi; y)$ is regular in the whole plane. Note that

$$\begin{aligned} \log L(s, \chi; y) &= \log L(s, \chi) + \sum_{p \leq y} \log \left(1 - \frac{\chi(p)}{p^s} \right) \\ &= \log L(s, \chi) - \sum_{m=2}^y \frac{\Lambda(m) \chi(m)}{m^s \log m} + O \left(\sum_{\substack{p \leq y \\ m \geq 2}} \frac{1}{mp^{m \operatorname{Re}(s)}} \right), \end{aligned}$$

and so if $\operatorname{Re}(s) \geq \frac{1}{2} + \frac{1}{\log y}$, and $|\operatorname{Im}(s)| \leq 2q$ we get by Lemma 8.2

$$(8.2) \quad |\log L(s, \chi; y)| \leq C \log q \log^2 y,$$

where $C > 0$ is some constant.

Assume, without loss of generality, that the fractional part of x is $\frac{1}{2}$. Let $u = \frac{\log x}{\log y}$ and put $c = 1 + \frac{1}{\log x}$. By Perron's formula

$$\begin{aligned} \sum_{n \leq x} \chi(n) - \Psi(x, y; \chi) &= \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \left(L(s, \chi) - \prod_{p \leq y} \left(1 - \frac{\chi(p)}{p^s} \right)^{-1} \right) \frac{x^s}{s} ds \\ &= \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \prod_{p \leq y} \left(1 - \frac{\chi(p)}{p^s} \right)^{-1} (\exp(\log L(s, \chi; y)) - 1) \frac{x^s}{s} ds \\ (8.3) \quad &= \sum_{\ell=1}^{[u]} \frac{1}{\ell!} \sum_{n \in \mathcal{S}(x/y^\ell, y)} \frac{\chi(n)}{2\pi i} \int_{c-i\infty}^{c+i\infty} (\log L(s, \chi; y))^\ell \left(\frac{x}{n} \right)^s \frac{ds}{s}. \end{aligned}$$

Now note that $(\log L(s, \chi; y))^\ell / \ell! = \sum_{m=1}^{\infty} a_\ell(m, y) m^{-s}$ where $|a(m, y)| \leq 1$ for all m . Hence, by the lemma of section 17 of [3],

$$\begin{aligned} \frac{1}{2\pi i \ell!} \int_{c-i\infty}^{c+i\infty} (\log L(s, \chi; y))^\ell \left(\frac{x}{n}\right)^s \frac{ds}{s} &= \frac{1}{2\pi i \ell!} \int_{c-ix/n}^{c+ix/n} (\log L(s, \chi; y))^\ell \left(\frac{x}{n}\right)^s \frac{ds}{s} \\ &\quad + O\left(\sum_{m=1}^{\infty} \frac{1}{m^c} \frac{1}{|\log(x/mn)|}\right) \\ &= \frac{1}{2\pi i \ell!} \int_{c-ix/n}^{c+ix/n} (\log L(s, \chi; y))^\ell \left(\frac{x}{n}\right)^s \frac{ds}{s} + O(\log x). \end{aligned}$$

We move the line of integration to the line segment from $\kappa - ix/n$ to $\kappa + ix/n$ where $\kappa := \frac{1}{2} + \frac{1}{\log y}$. Using (8.2) we obtain

$$\frac{1}{2\pi i \ell!} \int_{c-i\infty}^{c+i\infty} (\log L(s, \chi; y))^\ell \left(\frac{x}{n}\right)^s \frac{ds}{s} \ll \left(\frac{x}{n}\right)^\kappa \frac{(C \log q \log^2 y)^\ell}{\ell!} \log \frac{x}{n} + \log x.$$

Using this in (8.3) we obtain

$$\left| \sum_{n \leq x} \chi(n) - \Psi(x, y; \chi) \right| \ll \sum_{\ell=1}^{[u]} \frac{(C \log q \log^2 y)^\ell}{\ell!} \sum_{n \in \mathcal{S}(x/y^\ell, y)} \frac{x^\kappa}{n^\kappa} \log \frac{x}{n} + \sum_{\ell=1}^u \Psi\left(\frac{x}{y^\ell}, y\right) \log x.$$

Using Proposition 3.5 and Corollary 3.6 we deduce that (keeping in mind $y \gg \log^2 x$)

$$\Psi\left(\frac{x}{y^\ell}, y\right) \ll \left(\frac{c \log x}{y}\right)^\ell \Psi(x, y), \quad \text{and} \quad \sum_{n \in \mathcal{S}(x/y^\ell, y)} \frac{x^\kappa}{n^\kappa} \log \frac{x}{n} \ll \ell (c \log x)^\ell \log^2 y \frac{\Psi(x, y)}{y^{\ell(1-\kappa)}}.$$

Hence

$$\begin{aligned} \left| \sum_{n \leq x} \chi(n) - \Psi(x, y; \chi) \right| &\ll \Psi(x, y) \sum_{\ell=1}^{[u]} \left(\log^2 y \frac{(C \log q \log x \log^2 y)^\ell}{(\ell-1)! y^{\frac{\ell}{2}}} + \left(\frac{c \log x}{y}\right)^\ell \log x \right) \\ (8.4) \quad &\ll \Psi(x, y) \frac{\log q \log x \log^4 y}{y^{\frac{1}{2}}} \exp\left(O\left(\frac{\log q \log x \log^2 y}{y^{\frac{1}{2}}}\right)\right). \end{aligned}$$

It is of interest to compare (8.4) with the bound of Theorem 6.1.

Deduction of Theorem 2. The first assertion follows by taking $y = \log^2 q \log^2 x (\log \log q)^{12}$ in (8.4). Next, taking $y = \log^2 q (\log \log q)^{14}$ in (8.4) we get

$$\sum_{n \leq x} \chi(n) \ll \Psi(x, y) \exp\left(O\left(\frac{\log x}{(\log \log q)^3}\right)\right),$$

and using Lemma 3.7, this is $\ll \Psi(x, \log^2 q (\log \log q)^{20})$, as desired.

9. LARGE CHARACTER SUMS FOR REAL CHARACTERS

9a. Proofs of Theorem 9, and Theorem 10 for “small” x .

Let $y \geq 2$ be a parameter to be chosen later and put $b = b(y) = 4 \prod_{p \leq y} p$. Choose $a \pmod{b}$ such that $a \equiv 1 \pmod{8}$, and $\left(\frac{a}{p}\right) = 1$ for every odd $p \leq y$. Note that a squarefree integer $D \equiv a \pmod{b}$ is a fundamental discriminant satisfying $\left(\frac{D}{p}\right) = 1$ for all $p \leq y$. We obtain the lower bounds of Theorems 9 and 10 by averaging over fundamental discriminants of this special type, and choosing y appropriately.

Write $n \leq x$ as $n = rs$ where $p|r \implies p \leq y$, and $p|s \implies p > y$. Note that if $D \equiv a \pmod{b}$ then $\left(\frac{D}{n}\right) = \left(\frac{D}{s}\right)$. Thus

$$(9.1) \quad \sum_{\substack{q \leq D \leq 2q \\ D \equiv a \pmod{b}}} \mu(D)^2 \sum_{n \leq x} \left(\frac{D}{n}\right) = \sum_{r \in \mathcal{S}(x,y)} \sum_{\substack{s \leq x/r \\ p|s \implies p > y}} \sum_{\substack{q \leq D \leq 2q \\ D \equiv a \pmod{b}}} \mu(D)^2 \left(\frac{D}{s}\right).$$

If s is not a square then using $\mu(D)^2 = \sum_{\alpha^2 | D} \mu(\alpha)$

$$\sum_{\substack{q \leq D \leq 2q \\ D \equiv a \pmod{b}}} \mu(D)^2 \left(\frac{D}{s}\right) = \sum_{\substack{\alpha \leq A \\ (\alpha, b) = 1}} \mu(\alpha) \sum_{\substack{q \leq D \leq 2q \\ \alpha^2 | D \\ D \equiv a \pmod{b}}} \left(\frac{D}{s}\right) + O\left(\sum_{\sqrt{2q} > \alpha > A} \left(\frac{q}{\alpha^2 b} + 1\right)\right),$$

and by (a modification to the proof of) the Pólya-Vinogradov inequality this is

$$(9.2a) \quad \ll A\sqrt{s} \log s + \sqrt{q} + \frac{q}{Ab} \ll \sqrt{q} + \frac{\sqrt{q}}{\sqrt{b}} s^{\frac{1}{4}} \log s,$$

upon choosing $A = \sqrt{q}/(b^{\frac{1}{2}} s^{\frac{1}{4}})$. If s is a square, say $s = t^2$, then we see similarly that

$$(9.2b) \quad \sum_{\substack{q \leq D \leq 2q \\ D \equiv a \pmod{b}}} \mu(D)^2 \left(\frac{D}{s}\right) = \sum_{\substack{q \leq D \leq 2q \\ D \equiv a \pmod{b} \\ (d, t) = 1}} \mu(D)^2 = \frac{q}{b} \frac{\varphi(t)}{t} \prod_{\substack{p > y \\ p|t}} \left(1 - \frac{1}{p^2}\right) + O(\sqrt{qt}^\epsilon).$$

Note that (9.2b) with $s = t = 1$ counts the number of fundamental discriminants $q \leq D \leq 2q$ with $D \equiv a \pmod{b}$.

Using (9.2a,b) in (9.1) we deduce that

$$\sum_{\substack{q \leq D \leq 2q \\ D \equiv a \pmod{b}}} \mu(D)^2 \sum_{n \leq x} \left(\frac{D}{n}\right) = \frac{q}{b} \sum_{r \in \mathcal{S}(x,y)} \sum_{\substack{t^2 \leq x/r \\ p|t \implies p > y}} \frac{\varphi(t)}{t} \prod_{\substack{p > y \\ p|t}} \left(1 - \frac{1}{p^2}\right) + O\left(\sqrt{q}x^{1+\epsilon} + \frac{\sqrt{q}x^{\frac{5}{4}+\epsilon}}{\sqrt{b}}\right).$$

It follows that there is at least one fundamental discriminant $D \equiv a \pmod{b}$ between q and $2q$ with

$$(9.3) \quad \sum_{n \leq x} \left(\frac{D}{n}\right) \geq \sum_{r \in \mathcal{S}(x,y)} \sum_{\substack{t^2 \leq x/r \\ p|t \implies p > y}} \prod_{p|t} \frac{p}{p+1} + O\left(\frac{b}{\sqrt{q}}x^{1+\epsilon} + \frac{\sqrt{b}}{\sqrt{q}}x^{\frac{5}{4}+\epsilon}\right).$$

We first use (9.3) to prove Theorem 9. Take y to be the smallest prime $> \frac{1}{3} \log q$, so that $b(y) = q^{\frac{1}{3} + o(1)}$. Since $x \leq q^{o(1)}$ we see, by counting only the $t = 1$ terms on the right side of (9.3), that there is a fundamental discriminant $q \leq D \leq 2q$ with

$$\sum_{n \leq x} \left(\frac{D}{n} \right) \geq \sum_{r \in \mathcal{S}(x, y)} 1 + o(1) \geq \Psi(x, \frac{1}{3} \log q).$$

This proves Theorem 9.

To prove Theorem 10 in the range $\exp(\sqrt{\log q}) \leq x \leq q^{1/2}$, we take $y = (\frac{1}{2} - 2\epsilon) \log \frac{q}{x}$ so that $b(y) \leq (\frac{q}{x})^{\frac{1}{2} - \epsilon}$. By (9.3) there is a fundamental discriminant $q \leq D \leq 2q$ such that

$$(9.4) \quad \sum_{n \leq x} \left(\frac{D}{n} \right) \geq \sum_{r \in \mathcal{S}(x, y)} \sum_{\substack{t^2 \leq x/r \\ p|t \Rightarrow p > y}} \prod_{p|t} \frac{p}{p+1} + O(x^{\frac{1}{2}}).$$

We get a lower bound on the right side by counting only those $r \leq R (\leq \frac{x}{4y^2})$ for some parameter R to be chosen soon. The prime number theorem and the small sieve show that for such r the sum over t is $\gg \frac{\sqrt{x/r}}{\log y}$. Hence the right side of (9.4) is

$$\gg \frac{\sqrt{x}}{\log y} \sum_{r \in \mathcal{S}(R, y)} \frac{1}{\sqrt{r}} \gg \frac{\sqrt{x}}{\log y} \frac{\Psi(R, y)}{\sqrt{R}}.$$

Choose $R = \exp(2\sqrt{y})$ so that by Theorem 3.4 this is $\gg \sqrt{x} \exp((2 + o(1)) \frac{\sqrt{y}}{\log y})$, as needed.

9b. Proofs of Theorem 11, and Theorem 10 for “large” x .

We shall consider *negative* fundamental discriminants D , so that $(\frac{D}{-1}) = -1$, and $\tau(\chi_D) = i\sqrt{|D|}$. Pólya’s Fourier expansion (see (3)) gives

$$(9.5) \quad \begin{aligned} \frac{\pi}{2\sqrt{|D|}} \sum_{n \leq |D|/N} \left(\frac{D}{n} \right) &= \frac{1}{4} \sum_{\substack{h=-H \\ h \neq 0}}^H \frac{(\frac{D}{h})}{h} (1 - e(-h/N)) + O\left(\frac{1}{\sqrt{|D|}} + \frac{\sqrt{|D|}}{H} \log |D| \right) \\ &= \sum_{h=1}^H \frac{(\frac{D}{h})}{h} \sin^2(\pi h/N) + O\left(\frac{1}{\sqrt{|D|}} + \frac{\sqrt{|D|}}{H} \log |D| \right). \end{aligned}$$

Let y be a parameter to be chosen later, and let $b = b(y)$, and a be as in §9a. We average (9.5) over fundamental discriminants $q \leq -D \leq 2q$ with $D \equiv a \pmod{b}$. Arguing exactly as in the proof of (9.3), we deduce that there is a fundamental discriminant D with $q \leq -D \leq 2q$ such that

$$\begin{aligned} \frac{\pi}{2\sqrt{|D|}} \sum_{n \leq |D|/N} \left(\frac{D}{n} \right) &\geq \sum_{r \in \mathcal{S}(H, y)} \frac{1}{r} \sum_{\substack{t^2 \leq H/r \\ p|t \Rightarrow p > y}} \frac{\sin^2(\pi r t^2 / N)}{t^2} \prod_{p|t} \frac{p}{p+1} \\ &\quad + O\left(\frac{1}{\sqrt{q}} + \frac{\sqrt{q}}{H} \log q + \frac{b}{\sqrt{q}} H^\epsilon + \frac{\sqrt{b}}{\sqrt{q}} H^{\frac{1}{4} + \epsilon} \right). \end{aligned}$$

Choosing $H = q^{\frac{4}{5}}/b^{\frac{2}{5}}$ we deduce that for some fundamental discriminant D with $q \leq -D \leq 2q$ we have

$$(9.6) \quad \frac{\pi}{2\sqrt{|D|}} \sum_{n \leq |D|/N} \left(\frac{D}{n}\right) \geq \sum_{r \in \mathcal{S}(H,y)} \frac{1}{r} \sum_{\substack{t^2 \leq H/r \\ p|t \implies p > y}} \frac{\sin^2(\pi r t^2/N)}{t^2} \prod_{p|t} \frac{p}{p+1} + O\left(q^\epsilon \left(\frac{b}{\sqrt{q}} + \frac{b^{\frac{2}{5}}}{q^{\frac{3}{10}}}\right)\right).$$

We now get a bound on the right side of (9.6) for various ranges of N . Throughout we shall take $y = \frac{1}{3} \log q$ so that $b \leq q^{\frac{1}{3}+\epsilon}$. Then $H \geq \sqrt{q}$, and the error term in (9.6) is $O(q^{-\frac{1}{7}})$.

We begin with the range $\sqrt{\log q} \geq N \geq 2$. (Note that by taking $N = 2$, the right side above is $\gtrsim \sum_{r \leq H} 1/r$, where the sum is over those odd r whose prime factors are all $\leq y$, which is $\gtrsim (e^\gamma/2) \log y$, and we thus recover Paley's bound (4).)

We count only the terms for which $t = 1$, and $r \leq y$ with $\frac{1}{4} \leq \{r/N\} \leq \frac{3}{4}$ in (9.6). Thus

$$(9.6) \geq \sum_{r \leq y} \frac{\sin^2(\pi r/N)}{r} + O(q^{-\frac{1}{7}}) \geq \sum_{k=0}^{y/N} \sum_{(k+1/4)N \leq r \leq (k+3/4)N} \frac{\sin^2(\pi r/N)}{r} + O(1) \\ \geq \sum_{k=0}^{y/N} \frac{1}{N(k+1)} \frac{1}{2} \left\lfloor \frac{N}{2} \right\rfloor + O(1) \geq \frac{1}{8} \log(y/N) + O(1) \geq \frac{1}{16} \log \log q + O(1).$$

Next we consider the range $\exp(\sqrt{\log q}) \geq N \geq \sqrt{\log q}$. Here we bound (9.6) as follows: Let $\theta = 1/\log(6 \log N/\log y)$.

$$(9.6) \geq \sum_{r \in \mathcal{S}(Ny^\theta, y)} \frac{\sin^2(\pi r/N)}{r} + O(q^{-\frac{1}{7}}) \geq \sum_{k=0}^{y^\theta} \frac{1}{N(k+1)} \sum_{\substack{(k+1/4)N \leq n \leq (k+3/4)N \\ p|n \implies p \leq y}} \frac{1}{2} + O(q^{-\frac{1}{7}}).$$

First we focus on the range $N < \exp((\log \log q)^2)$. Appealing to the ‘‘smooth numbers in short intervals estimate’’, Lemma 3.8, and Theorem 3.4 this is

$$\gg \sum_{k=0}^{y^\theta} \frac{1}{N(k+1)} N \rho\left(\frac{\log(N(k+\frac{1}{4}))}{\log y}\right) \gg \theta \rho\left(\frac{\log N}{\log y} + \theta\right) \log y,$$

which gives the result since $\rho(u+1/\log(6u)) \asymp \rho(u)$ by Lemma 3.9.

Next if $\exp(\sqrt{\log q}) \geq N \geq \exp((\log \log q)^2)$ we use Lemma 3.8, and ignore all but the $k = 0$ term. This gives

$$(9.6) \gg \frac{1}{N} \Psi\left(\frac{N}{4}, y\right) \gg \frac{1}{N} \Psi(N, y).$$

The result follows from Lemma 3.9, completing the proof of Theorem 11.

To prove Theorem 10 in the range $q^{1/2} \leq x \leq q/\exp(\sqrt{\log q})$, we consider the range $\sqrt{q} \geq N \geq \exp(\sqrt{\log q})$. Let $R \leq N/(4y^2)$ be a parameter to be chosen

shortly. We bound (9.6) by considering only $r \in \mathcal{S}(R, y)$, and then summing over values where $t = p$ is prime in the range $\sqrt{N}/(2\sqrt{r}) \leq p \leq \sqrt{3N}/(2\sqrt{r})$. Thus, using the prime number theorem,

$$(9.6) \geq \sum_{r \in \mathcal{S}(R, y)} \frac{1}{r} \sum_{\frac{\sqrt{N}}{2\sqrt{r}} \leq p \leq \frac{\sqrt{3N}}{2\sqrt{r}}} \frac{\sin^2(\pi r/Np^2)}{p^2} \gg \sum_{r \in \mathcal{S}(R, y)} \frac{1}{r} \frac{\sqrt{r/N}}{\log q} \gg \frac{1}{\sqrt{N} \log q} \frac{\Psi(R, y)}{\sqrt{R}}.$$

Taking $R = \exp(2\sqrt{y})$ and using Theorem 3.4, this is $\gg (1/\sqrt{N}) \exp((2+o(1))\frac{\sqrt{y}}{\log y})$, as needed.

10. PROOF OF THEOREM 8

We consider only primitive characters χ with $\chi(-1) = 1$. Note that for a twice continuously differentiable function Φ the Poisson summation formula gives

$$\sum_{n=-\infty}^{\infty} \chi(n) \Phi\left(\frac{n}{X}\right) = \frac{X\tau(\chi)}{q} \sum_{a=-\infty}^{\infty} \bar{\chi}(a) \hat{\Phi}\left(\frac{aX}{q}\right).$$

Define Φ_1 to be the characteristic function of $[-1, 1]$, and let Φ_r be the r -fold convolution of Φ_1 . Note that $\Phi_r(t)$ is supported in $[-r, r]$, $\Phi_r(-t) = \Phi_r(t)$, and that $\Phi_r(t)$ increases for $t \in [-r, 0)$, and decreases for $t \in (0, r]$. Lastly, note that $\hat{\Phi}_r(\xi) = \hat{\Phi}_1(\xi)^r = \left(\frac{\sin(2\pi\xi)}{\pi\xi}\right)^r$ if $\xi \neq 0$, and $= 2^r$ if $\xi = 0$. We shall use the Poisson summation formula above with $X = q/(rN)$, and $\Phi = \Phi_r$ for an even value of $r \geq 4$, so that the Fourier transform $\hat{\Phi}_r$ is always non-negative.

On the one hand, we have

$$\begin{aligned} \sum_{n=-\infty}^{\infty} \chi(n) \Phi_r\left(\frac{n}{X}\right) &= 2 \sum_{n=1}^{q/N} \chi(n) \Phi_r\left(\frac{n}{X}\right) = -2 \int_0^{q/N} \frac{1}{X} \Phi_r'\left(\frac{t}{X}\right) \sum_{n \leq t} \chi(n) dt \\ (10.1) \quad &\leq 2\Phi_r(0) \max_{t \leq q/N} \left| \sum_{n \leq t} \chi(n) \right| \leq 2^r \max_{t \leq q/N} \left| \sum_{n \leq t} \chi(n) \right|. \end{aligned}$$

On the other hand, the right side of the Poisson sum formula has size (since $|\tau(\chi)| = \sqrt{q}$, and $\bar{\chi}(-1) = 1$)

$$\begin{aligned} \frac{2\sqrt{q}}{rN} \left| \sum_{a=1}^{\infty} \bar{\chi}(a) \hat{\Phi}_r\left(\frac{a}{rN}\right) \right| &= \frac{2\sqrt{q}}{rN} \left| \sum_{a=1}^{(rN)^{\frac{r}{r-1}}} \bar{\chi}(a) \left(\frac{\sin(2\pi\frac{a}{rN})}{\frac{\pi a}{rN}}\right)^r \right| + O\left(\frac{\sqrt{q}}{rN} \sum_{a > (rN)^{\frac{r}{r-1}}} \left(\frac{rN}{\pi a}\right)^r\right) \\ (10.2) \quad &= \frac{2\sqrt{q}}{rN} \left| \sum_{a=1}^{(rN)^{\frac{r}{r-1}}} \bar{\chi}(a) \left(\frac{\sin(2\pi\frac{a}{rN})}{\frac{\pi a}{rN}}\right)^r \right| + O\left(\frac{\sqrt{q}}{rN}\right). \end{aligned}$$

Now observe that for integers $k \leq \frac{(r-1)\log(q/2)}{r \log(rN)}$ we have

$$\frac{2}{\varphi(q)} \sum_{\substack{\chi \pmod{q} \\ \chi(-1)=1}} \left| \sum_{a=1}^{(rN)^{\frac{r}{r-1}}} \bar{\chi}(a) \left(\frac{\sin(2\pi\frac{a}{rN})}{\frac{\pi a}{rN}}\right)^r \right|^{2k} = \mathbb{E} \left(\left| \sum_{h=1}^{(rN)^{\frac{r}{r-1}}} X_h \left(\frac{\sin(2\pi\frac{h}{rN})}{\frac{\pi h}{rN}}\right)^r \right|^{2k} \right).$$

Since $r \geq 4$ is even, note that $\sin^r(2\pi \frac{a}{rN}) / (\frac{\pi a}{rN})^r \geq 0$ for all a , and $\geq c2^r$ for all $a \leq N$, for some absolute constant c . Hence we get from Lemma 2.3 that

$$\mathbb{E} \left(\left| \sum_{h=1}^{(rN)^{\frac{r}{r-1}}} X_h \left(\frac{\sin(2\pi \frac{h}{rN})}{\frac{\pi h}{rN}} \right)^r \right|^{2k} \right) \geq (c2^r)^{2k} \mathbb{E} \left(\left| \sum_{a=1}^N X_a \right|^{2k} \right).$$

Combining the above statements thus gives

$$(10.3) \quad \max_{t \leq q/N} \left| \sum_{n \leq t} \chi(n) \right| \gg \frac{\sqrt{q}}{rN} \left(\mathbb{E} \left(\left| \sum_{a=1}^N X_a \right|^{2k} \right)^{\frac{1}{2k}} + O(1) \right).$$

We may obtain a lower bound from this by appealing to the results of §4 and §6, taking $k = \lceil (r-1) \log(q/2) / r \log(rN) \rceil$ in the first three parts, choosing r appropriately and replacing x in those arguments by N here. Thus the first part of the theorem is a consequence of Corollary 6.3 with $r = 4$. The remaining parts of the theorem follow by choosing r to be an even integer around $\log \log q$, and then applying Theorem 4.1 as in the proofs of Theorems 5, 6, and 7.

Acknowledgements. Thanks are due to John Friedlander for his persistent encouragement, to Mark Watkins for the question discussed in the introduction, and to Carl Pomerance for several helpful questions.

REFERENCES

1. P.T. Bateman and S. Chowla, *Averages of character sums*, Proc. Amer. Math. Soc **1** (1950), 781-787.
2. D.A. Burgess, *The distribution of quadratic residues and non-residues*, Mathematika Soc **4** (1957), 106-112.
3. H. Davenport, *Multiplicative number theory*, Springer Verlag, New York, 1980.
4. J.B. Friedlander and H. Iwaniec, *A note on character sums*, Contemp. Math. J **166** (1994), 295-299.
5. S.W. Graham and C.J. Ringrose, *Lower bounds for least quadratic non-residues*, Prog. Math **85** (1990), Birkhäuser, Boston, 269-309.
6. A. Granville and K. Soundararajan, *The spectrum of multiplicative functions* (to appear).
7. A. Granville and K. Soundararajan, *The distribution of $L(1, \chi)$* (to appear).
8. G.H. Hardy and S. Ramanujan, *The normal number of prime factors of a number n* , Quart. J. Math **48** (1917), 76-92.
9. A. Hildebrand, *A note on Burgess's character sum estimate*, C.R. Acad. Sci. Roy. Soc. Canada **8** (1986), 35-37.
10. A. Hildebrand and G. Tenenbaum, *Integers without large prime factors*, J. Théorie des Nombres, Bordeaux **5** (1993), 411-484.
11. H.L. Montgomery, *An exponential polynomial formed with the Legendre symbol*, Acta Arithm. **37** (1980), 375-380.
12. H.L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, vol. 84, CBMS Regional Conference Series in Mathematics, AMS, 1994.
13. H.L. Montgomery and R.C. Vaughan, *Exponential sums with multiplicative coefficients*, Invent. Math **43** (1977), 69-82.
14. R.E.A.C. Paley, *A theorem on characters*, J. London Math. Soc **7** (1932), 28-32.
15. C. Pomerance, *On the distribution of round numbers*, Number Theory (Proc. Ootacamund, India), Springer Lecture Notes No. 1122, 1984, pp. 173-200.

16. G. Tenenbaum, *Criblez les entiers sans grand facteur premier*, Phil. Trans. Roy. Soc. **345** (1993), 377-384.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GEORGIA, ATHENS, GEORGIA 30602, USA
E-mail address: `andrew@math.uga.edu`

DEPARTMENT OF MATHEMATICS, PRINCETON UNIVERSITY, PRINCETON, NEW JERSEY 08544,
USA
E-mail address: `skannan@math.princeton.edu`