Algebra & Number Theory

Volume 9
2015
No. 4

The Elliott–Halberstam conjecture implies the Vinogradov least quadratic nonresidue conjecture

Terence Tao

msp

ALGEBRA AND NUMBER THEORY 9:4 (2015)
dx.doi.org/10.2140/ant.2015.9.1005

The Elliott–Halberstam conjecture implies the Vinogradov least quadratic nonresidue conjecture

Terence Tao

For each prime p, let $n(p)$ denote the least quadratic nonresidue modulo p. Vinogradov conjectured that $n(p) = O(p^\varepsilon)$ for every fixed $\varepsilon > 0$. This conjecture follows from the generalized Riemann hypothesis and is known to hold for almost all primes p but remains open in general. In this paper, we show that Vinogradov's conjecture also follows from the Elliott–Halberstam conjecture on the distribution of primes in arithmetic progressions, thus providing a potential "nonmultiplicative" route to the Vinogradov conjecture. We also give a variant of this argument that obtains bounds on short centered character sums from "Type II" estimates of the type introduced recently by Zhang and improved upon by the Polymath project or from bounds on the level of distribution on variants of the higher-order divisor function. In particular, an improvement over the Burgess bound would be obtained if one had Type II estimates with level of distribution above $\frac{2}{3}$ (when the conductor is not cube-free) or $\frac{3}{4}$ (if the conductor is cube-free); morally, one would also obtain such a gain if one had distributional estimates on the third or fourth divisor functions τ_3 or τ_4 at level above $\frac{2}{3}$ or $\frac{3}{4}$, respectively. Some applications to the least primitive root are also given.

1. Introduction

For each prime p, let $n(p)$ denote the least natural number that is not a quadratic residue modulo p. Vinogradov [1985] established the asymptotic bound

$$n(p) \ll p^{1/2\sqrt{e}} \log^2 p \tag{1-1}$$

for all primes p and made the following conjecture:

Conjecture 1.1 (Vinogradov's conjecture). *For any fixed $\varepsilon > 0$, we have $n(p) \ll p^\varepsilon$.*

MSC2010: primary 11L40; secondary 11L20.
Keywords: quadratic nonresidue, Elliott–Halberstam conjecture, character sums, Burgess bound.

(See the end of the section for our conventions on asymptotic notation.) Linnik [1942] showed that this conjecture follows[1] from the generalized Riemann hypothesis; Ankeny [1952] improved the bound further to

$$n(p) \ll \log^2 p$$

on this hypothesis. However, Conjecture 1.1 remains open unconditionally; the best bound available (up to logarithmic factors) for general primes p is

$$n(p) \ll p^{1/4\sqrt{e}+\varepsilon} \tag{1-2}$$

for any fixed $\varepsilon > 0$, a well-known result of Burgess [1957]. It was also shown by Linnik [1942] unconditionally that, for any fixed $\varepsilon > 0$, the number of $p \le x$ with $n(p) > x^{\varepsilon}$ is bounded uniformly in x, and hence, the number of exceptions to the inequality $n(p) > p^{\varepsilon}$ with $p \le x$ is bounded by $O(\log\log x)$.

In this paper, we connect Vinogradov's conjecture to a standard conjecture in sieve theory, the *Elliott–Halberstam conjecture* [1970], as well as to a restricted fragment of this conjecture recently introduced by Zhang [2014]. The basic phenomenon being exploited here is that distribution estimates such as those given by the Elliott–Halberstam conjecture allow one to control correlations of the form[2]

$$\sum_n (\alpha * \beta)(n)(\gamma * \delta)(n+h) \tag{1-3}$$

for various arithmetic sequences α, β, γ, and δ and nontrivial shifts h, as long as all of the sequences α, β, γ, and δ vanish for very small values of n and provided that at least one of the sequences α, β, γ, or δ is "smooth" (e.g., if one of these sequences is an indicator function such as $1_{[N,2N]}$). On the other hand, by combining the multiplicativity and periodicity properties of Dirichlet characters with a hypothesis that the least quadratic residue is large (or that a character sum is large), we will be able to construct sums of the form (1-3) that deviate substantially from its expected value, giving the required contradiction. It is the periodicity of Dirichlet characters χ that allow us to introduce the shift h, thus transferring the problem from a multiplicative number theory problem (in which hypotheses

[1] In fact, the conjecture follows from even very weak fragments of this hypothesis; see, e.g., [Bateman and Diamond 2004, Theorem 10.6]. (Thanks to Kevin Ford for this reference.) The strongest result in this direction comes from a very recent work of Granville and Soundararajan [2015] (see also [Banks and Makarov 2014]), who showed (roughly speaking) that the only way this conjecture can fail is if a positive proportion of low-lying zeros of an L-function lies extremely close to the line $\operatorname{Re} s = 1$.

[2] If only the original Elliott–Halberstam conjecture is available, rather than its variants, then one of the convolutions $\alpha * \beta$ or $\gamma * \delta$ needs to be replaced by the von Mangoldt function Λ. Also, for technical reasons, it is convenient to ensure that one of the factors α, β, γ, or δ is supported on numbers coprime to the shift h.

such as the generalized Riemann hypothesis are useful) to a sieve theory problem (in which hypotheses such as the Elliott–Halberstam conjecture are useful). The arguments share some similarities with that of Burgess [1957] (which also relies heavily on the multiplicativity and periodicity properties of Dirichlet characters) but is ultimately powered by a somewhat different source of cancellation, namely the equidistribution assumptions of Elliott–Halberstam type rather[3] than the Weil exponential sum estimates.

To describe the results more precisely, we need some notation. For any function $\alpha : \mathbb{N} \to \mathbb{C}$ with finite support (that is, α is nonzero only on a finite set) and any primitive residue class $a\ (r)$, we define the (signed) *discrepancy* $\Delta(\alpha; a\ (r))$ to be the quantity

$$\Delta(\alpha; a\ (r)) := \sum_{n=a\ (r)} \alpha(n) - \frac{1}{\varphi(r)} \sum_{(n,r)=1} \alpha(n), \tag{1-4}$$

where φ is the Euler totient function.

Conjecture 1.2 (Elliott–Halberstam conjecture). *Let $0 < \vartheta < 1$ be fixed. Then*

$$\sum_{r<x^{\vartheta}} \sup_{a\in(\mathbb{Z}/r\mathbb{Z})^{\times}} |\Delta(\Lambda 1_{[1,x]}; a\ (r))| \ll x \log^{-A} x \tag{1-5}$$

for any fixed $A > 1$, where Λ is the von Mangoldt function. Equivalently, from the prime number theorem, one has

$$\sum_{r<x^{\vartheta}} \sup_{a\in(\mathbb{Z}/r\mathbb{Z})^{\times}} \left| \sum_{n\le x: n=a\ (r)} \Lambda(n) - \frac{x}{\varphi(r)} \right| \ll x \log^{-A} x$$

for any fixed $A > 1$.

The case $\vartheta < \frac{1}{2}$ of this conjecture is of course (a slightly weakened form of) the Bombieri–Vinogradov theorem [Bombieri 1965; Vinogradov 1965].

Our first theorem is then:

Theorem 1.3 (Elliott–Halberstam implies Vinogradov). *Conjecture 1.2 implies Conjecture 1.1.*

We prove this theorem in Section 2. The basic idea is to observe (from the general theory of mean values of multiplicative functions) that, if $n(q) > q^{\varepsilon}$ for some large prime q, then the character sum $\sum_{n\le x} \chi(n)\Lambda(n)$ will be anomalously large for

[3]It is worth noting however that much of the recent partial progress on the Elliott–Halberstam conjecture has proceeded by using Weil exponential sum estimates, although the precise estimates used there are different from those used in the Burgess argument. In Section 5, though, we sketch a version of the argument that allows for an improvement over the original bound (1-1) of Vinogradov using only the elementary bound on Kloosterman sums [1927] and does not require the full strength of the Weil conjectures.

some large $x = O(q^{O(1)})$, where χ is the quadratic character modulo q. As χ is periodic modulo q, this forces $\sum_{n\le x} \chi(n)\Lambda(n+q)$ to be large also. But one can use the Elliott–Halberstam conjecture (and an expansion of χ into divisor sums, using once again the largeness of $n(q)$) to obtain good bounds for $\sum_{n\le x} \chi(n)\Lambda(n+q)$ and obtain a contradiction.

With some additional combinatorial argument, we can obtain a similar implication[4] concerning the least primitive root modulo p, provided that $p-1$ has only boundedly many factors:

Theorem 1.4 (Elliott–Halberstam bounds least primitive roots). *Assume Conjecture 1.2. Then for any fixed $d \ge 1$ and fixed $\varepsilon > 0$ and any prime p for which $p-1$ is the product of at most d primes (counting multiplicity), the least primitive residue modulo p is $O(p^{\varepsilon})$.*

We prove this theorem in Section 3.

Our proof of Theorem 1.3 does not easily allow one to convert partial progress on the Elliott–Halberstam conjecture to partial progress on Vinogradov's conjecture. We now present a different argument that replaces the Elliott–Halberstam conjecture by a conjecture on "Type II sums" of the type introduced[5] by Zhang [2014] with the feature that partial progress on the Type II conjecture implies partial progress on Vinogradov's conjecture. In particular, the Type II estimates in [Polymath 2014a] can be used to improve slightly upon the Vinogradov bound (1-1) by a method different from the Burgess argument, although the numerical exponent obtained is inferior to that in [Burgess 1957].

Let us first state the Type II conjecture, in a formulation suited for the current application.

Conjecture 1.5 (Type II conjecture). *Let $0 < \varpi < \frac{1}{4}$, and let $\delta > 0$ be a sufficiently small fixed quantity depending on ϑ. Let x be an asymptotic parameter going to infinity. Let P be any number that is the product of some subset of the primes in $[1, x^{\delta}]$; equivalently, let P be a square-free number all of whose prime factors are at most x^{δ}. Let N and M be quantities such that*

$$x^{1/2-2\varpi} \ll N \ll M \ll x^{1/2+2\varpi}$$

with $NM \asymp x$, and let $\alpha, \beta : \mathbb{N} \to \mathbb{R}$ be sequences supported on $[M, 2M]$ and $[N, 2N]$, respectively, such that one has the pointwise bounds

$$|\alpha(n)| \ll 1 \tag{1-6}$$

[4] We are indebted to Felipe Voloch for suggesting this variant.

[5] Zhang also considered "Type I" and "Type III" sums, which will not be of direct relevance in this paper, although the τ_3 distribution estimates mentioned in Section 5 are related to the Type III sums. Similar sums had also been previously considered by Bombieri, Fouvry, Friedlander, and Iwaniec [Bombieri et al. 1986; 1987; 1989; Fouvry 1984; 1985; Fouvry and Iwaniec 1980; 1983; 1992].

for all natural numbers n. We also assume that β is simply the indicator function

$$\beta = 1_{[N,2N]}.$$

Then one has

$$\sup_{1\le a\le x:(a,P)=1} \sum_{r\ll x^{1/2+2\varpi}:r|P} |\Delta(\alpha\star\beta; a\ (r))| \ll x\log^{-A} x \tag{1-7}$$

for any fixed $A > 0$.

This conjecture is implied by the generalized Elliott–Halberstam conjecture in [Polymath 2014b], which was in turn inspired by a similar conjecture in [Bombieri et al. 1986]. In [Motohashi 1976] (see also [Gallagher 1968]), a generalization of the Bombieri–Vinogradov theorem is obtained that roughly speaking implies (up to logarithmic factors) the $\varpi = 0$ endpoint of this conjecture. The arguments in [Zhang 2014] implicitly establish the above conjecture for $0 < \varpi < \frac{1}{1168}$, and more explicitly, the estimate in [Polymath 2014a, Theorem 5.1(iv)] establishes the conjecture for $0 < \varpi < \frac{1}{68}$. The estimates in those papers allow for more general values of a and r and more general sequences α and β than those considered here; however, the restricted version of Conjecture 1.5 stated above will suffice for our application. It is likely that the additional restrictions imposed here (particularly the requirement that β be the indicator function of an interval) allow for some improvement in the exponent $\frac{1}{68}$ obtained in [Polymath 2014a]; see also Section 5 below for a slightly different way to improve upon this exponent, from $\frac{1}{68}$ to $\frac{1}{28}$.

Our next main result is then:

Theorem 1.6 (Type II sums bound character sums). *Suppose that Conjecture 1.5 holds for a fixed choice of $0 < \varpi < \frac{1}{4}$. Then one has*

$$\left|\sum_{n<q^{1/2-2\varpi+\varepsilon}} \chi(n)\right| \ll q^{1/2-2\varpi+\varepsilon}\log^{-A} q \tag{1-8}$$

for any sufficiently small fixed $\varepsilon > 0$, any fixed $A > 0$, and any natural number q (not necessarily prime) whenever χ is a nonprincipal primitive Dirichlet character of conductor q.

By the usual argument of Vinogradov, this gives:

Corollary 1.7. *Suppose that Conjecture 1.5 holds for a fixed choice of $0 < \varpi < \frac{1}{4}$. Then one has*

$$n(q) \ll q^{(1/\sqrt{e})(1/2-2\varpi)+\varepsilon}$$

for any fixed $\varepsilon > 0$ and any prime q.

Proof. From the pointwise estimate

$$\chi(n) \geq 1 - 2 \sum_{p|n: p > n(q)} 1$$

for the quadratic character $\chi(n) := \left(\frac{n}{q}\right)$, we see that

$$\sum_{n<x} \chi(n) \geq x - 1 - 2 \sum_{n(q)<p\leq x} \left(\frac{x}{p} + 1\right)$$

for any $x > 1$. Setting $x := q^{1/2-2\varpi+\varepsilon}$ for some $\varepsilon > 0$ and using Theorem 1.6, we see that

$$x - 2x \sum_{n(q)<p\leq x} \frac{1}{p} \leq o(x)$$

as $q \to \infty$. From Mertens' theorem, this implies that

$$\log \frac{\log x}{\log n(q)} \geq \tfrac{1}{2} + o(1),$$

and the claim follows. □

In particular, the Type II estimates in [Polymath 2014a] give the improvement

$$n(p) \ll p^{(1/\sqrt{e})(1/2-1/34)+\varepsilon}$$

to (1-1) for any fixed $\varepsilon > 0$. This is well short of the improvement in (1-2); however, it represents a slightly different way to break the "square root barrier" from the Burgess argument; for instance, the arguments can extend to more general moduli than primes p without much difficulty, whereas the Burgess argument encounters some additional technical issues when the modulus is not cube-free. One will be able to surpass the Burgess bound as soon as one can establish a Type II estimate for some $\varpi > \frac{1}{8}$ (or $\varpi > \frac{1}{12}$ in the non-cube-free case); thus, one needs to improve the Type II exponents in [Polymath 2014a] by a factor of roughly eight. Interestingly, it was noted in [Bombieri et al. 1986, Conjecture 3] that, if one assumed square root cancellation in certain exponential sums, one could obtain Type II estimates for all $\varpi < \frac{1}{8}$, thus falling barely short of being able to improve upon the Burgess bound.

Theorem 1.6, when combined with the Type II estimates in [Polymath 2014a], establishes the short character sum bounds

$$\sum_{n<q^{1/2-1/34+\varepsilon}} \chi(n) = q^{1/2-1/34+\varepsilon} \log^{-A} q \tag{1-9}$$

for any primitive character χ of conductor q. This bound is inferior to that of Burgess [1957; 1963; 1986], which establishes

$$\sum_{M\leq n\leq M+N} \chi(n) = N^{1-\delta(\varepsilon)}$$

for arbitrary M when $N \gg q^{1/3+\varepsilon}$ (if q is not cube-free) or $N \gg q^{1/4+\varepsilon}$ (if q is cube-free), and $\delta(\varepsilon) > 0$ depends only on ε. With our methods, one would need Type II estimates at level of distribution at least $\frac{2}{3}$ (thus $\varpi > \frac{1}{12}$) to improve upon the Burgess bound in the non-cube-free setting or at least $\frac{3}{4}$ (thus $\varpi > 1/8$) in the cube-free setting. Note also the Burgess bound has also been improved for certain types of modulus q, such as smooth numbers (see, e.g., [Graham and Ringrose 1990; Goldmakher 2010]) or prime powers (see, e.g., [Postnikov 1956]).

Remark 1.8. If one had the Type II estimates for all $0 < \varpi < \frac{1}{4}$, then (by combining Corollary 1.7 with the Burgess bound) we would have

$$\sum_{n \le x} \chi(n) \ll x \log^{-A} x$$

for all $x \ge q^{\varepsilon}$ and fixed $A, \varepsilon > 0$, and hence (by summation by parts), one would obtain a very slight improvement $L(1, \chi) = o(\log q)$ to the standard upper bound $L(1, \chi) = O(\log q)$ for the sum $L(1, \chi) = \sum_n \chi(n)/n$. Furthermore, one obtains the bound $L(s, \chi) = O(\log^2 q)$ (say) when $|s - 1| \le A \log\log q / \log q$ for any fixed A. Using this and standard arguments (see, e.g., [Iwaniec and Kowalski 2004, Chapter 8]), one can enlarge[6] the classical zero-free region of $L(s, \chi)$ to include the region $|s - 1| \le A/\log q$ for any fixed $A > 0$, except possibly for a Siegel zero. This in turn can be used to improve the prime number theorem of Gallagher [1970] and hence also the constant in Linnik's theorem on primes in an arithmetic progression, assuming the Type II estimates and possibly excluding an exceptional modulus; we omit the details.

Remark 1.9. By standard arguments (see, e.g., [Montgomery and Vaughan 2007, Corollary 9.20]) starting from the observation that the sum

$$\sum_{d|Q} \frac{\varphi(Q/d)\mu(d)}{Q} \sum_{\substack{\chi(Q) \\ \operatorname{ord} \chi = d}} \sum_{n \le x} \chi(n)$$

counts the number of primitive roots modulo a prime p up to x, where Q is the product of all the primes dividing $p - 1$, we see that Theorem 1.6 implies that, if one has Type II estimates for a given $0 < \varpi < \frac{1}{4}$, then the least primitive root of $\mathbb{Z}/p\mathbb{Z}$ is $O(p^{1/2-2\varpi+\varepsilon})$ for any fixed ε and any prime p, provided that $p - 1$ has at most $O(\log\log p)$ prime factors; we leave the details to the interested reader. In particular, we can strengthen the conclusion of Theorem 1.4 slightly if we replace the Elliott–Halberstam conjecture by the Type II conjecture for ϖ arbitrarily close to $\frac{1}{4}$. It may be possible[7] to remove the requirement on the number of prime factors

[6] We thank James Maynard for this remark.

[7] We thank the anonymous referee for this suggestion.

of $p-1$ by using zero-density estimates (together with a result of Rodosskiĭ [1956] linking L-function zeros with character sums; see also the recent preprints [Banks and Makarov 2014; Granville and Soundararajan 2015]) to show that $\sum_{n\le x}\chi(n)$ is small for most characters χ; we will not pursue this in detail here.

Remark 1.10. Suppose Conjecture 1.5 holds for some fixed $0<\varpi<\frac{1}{4}$, and suppose that q is a large prime such that the least prime quadratic *residue* is at least[8] $q^{1/2-2\varpi+\varepsilon}$. Then, letting χ be the quadratic character of conductor q, one has $\chi(n)=\lambda(n)$ for all $n\le q^{1/2-2\varpi+\varepsilon}$, where λ is the Liouville function. From the prime number theorem (for $n\le q^{1/2-2\varpi+\varepsilon}$) and Theorem 1.6, we conclude that $\sum_n \chi(n)/n \ll \log^{-A} q$ and $\sum_n \chi(n)\log n/n \gg 1$, so $|L'(1,\chi)/L(1,\chi)| \gg \log^A q$ for any fixed A. From standard arguments, this implies that one has a Siegel zero $L(\sigma,\chi)=0$ with $1-\sigma \ll \log^{-A} q$ for any fixed A. Thus, if one could rule out Siegel zeros, one could use Type II estimates to bound the least prime quadratic residue. If one could improve the $\log^{-A} q$ gain in (1-8) to a power saving $q^{-\varepsilon}$, then Siegel's theorem could be used to remove the need to consider Siegel zeros; for instance, this argument recovers the standard bound of $q^{1/4+o(1)}$ for the least prime quadratic residue coming from the Burgess bound. However, our arguments would require a similar power saving in the Type II estimates to achieve this, which may be an overly ambitious hypothesis.

We prove Theorem 1.6 in Section 4. The idea here is to exploit the fact that, if $\sum_{n\in[N/2,N]}\chi(n)$ is large, then on an interval $[1,x]$ with $x=q^{1+O(\varepsilon)}$, $\chi(n)$ will exhibit large correlation with $\alpha*\beta(n+jq)$ for any $j=O(q^\varepsilon)$, where $\beta:=1_{[N/2,N]}$ and α is the restriction of χ to smooth square-free numbers of magnitude close to x/N and that are coprime to q. This is because of the multiplicativity and periodicity properties of χ. An application of Cauchy–Schwarz (i.e., the dispersion method) then shows that $\alpha*\beta(n+jq)$ and $\alpha*\beta(n+j'q)$ correlate with each other for some distinct j and j', but one can use Type II estimates to prevent this scenario from occurring.

Remark 1.11. The above argument shares many similarities with the argument of Burgess [1957]. Both arguments rely heavily on the periodicity and multiplicativity of the Dirichlet character χ, which allows one to start with a hypothesis that a single character sum $\sum_{n\le x}\chi(n)$ is large and deduce that χ is biased on many arithmetic progressions. In the current argument, one exploits the bias of χ on medium-length arithmetic progressions (of length about $q^{1/2-2\varpi}$) and varying modulus; in contrast, the argument of Burgess exploits the bias of χ on many (close to $q^{1/2}$) very short progressions (of length q^ε for some small ε) and fixed modulus. Unfortunately, the author was not able to combine the two methods together to obtain any improvement

[8] We thank John Friedlander for suggesting this problem.

on (1-2) without assuming a large portion of the Elliott–Halberstam or Type II conjectures.

Remark 1.12. The proof of Theorem 1.6 may possibly extend to cover the shifted character sums $\sum_{M\le n\le M+N}\chi(n)$ appearing in the work of Burgess; however, the way the argument is currently presented, this would require a shifted version of a Type II estimate in which the convolution $\alpha*\beta$ is replaced by a shifted convolution. As such, one can no longer directly quote the results from [Polymath 2014a] to obtain a result for such shifted sums; however, it is plausible that some modification of the *proof* of the Type II estimate in [Polymath 2014a] can still be adapted to this shifted setting. We do not pursue this matter here (as with the centered sums, we do not seem to directly improve upon the Burgess bounds at the current level of technology for equidistribution estimates).

A variant of the argument used to prove Theorem 1.6, which we discuss in Section 5 below, allows one to use distributional estimates for the higher divisor functions

$$\tau_k(n) := \sum_{n_1,\dots,n_k:n_1\cdots n_k=n} 1 \tag{1-10}$$

(or more precisely, from dyadic components of such functions) in place of Type II estimates to obtain similar results. Roughly speaking, a distributional estimate on τ_k at level θ implies a bound of the form (1-8) with $\frac{1}{2}-2\varpi$ replaced by $\max(1-\theta, 1/(k\theta+1))$; thus, for instance, the classical distribution estimate of τ_2 at $\theta=\frac{2}{3}$ gives (1-8) with $\varpi=\frac{1}{28}$, slightly improving upon (1-9) though still short of the Burgess bounds in both cube-free and non-cube-free cases. More recently, a level of distribution $\frac{4}{7}$ has been established (in a restricted averaged sense) for τ_3 in [Fouvry et al. 2014], which (morally at least) also recovers (1-8) with $\varpi=\frac{1}{28}$. To improve upon the Burgess bound, one would need τ_k at level of distribution above $\frac{2}{3}$ for some $k\ge 3$ (in the non-cube-free case) or above $\frac{3}{4}$ for some $k\ge 4$ (in the cube-free case). Both results seem unfortunately to be out of reach of current methods.

A similar analysis, again discussed in Section 5 below, suggests that one should be able to improve the exponent $\frac{1}{2}-2\varpi$ in (1-8) to $1/k-c$ for some $c>0$ provided that one can obtain good asymptotics for sums such as

$$\sum_{n\le x}\tau_k(n)\tau_k(n+q)$$

with $q=o(x)$. In particular, controlling such sums for $k=3$ would (morally, at least) improve upon the non-cube-free Burgess bound and for $k=4$ would improve upon the cube-free Burgess bound. Unfortunately, rigorous asymptotics for these sums have only been established for $k=2$.

Notation. We use the following asymptotic notation. We allow for an asymptotic parameter (e.g., x or q) to go to infinity; quantities in this paper may depend on this parameter unless they are explicitly labeled as *fixed*. We then write $X \ll Y$, $X = O(Y)$, or $Y \gg X$ if one has $|X| \leq CY$ for some fixed C (in particular, C can depend on other parameters as long as they are also fixed). We also write $X = o(Y)$ if we have $|X| \leq cY$ for some quantity c that goes to zero as the asymptotic parameter goes to infinity and write $X \asymp Y$ for $X \ll Y \ll X$.

Sums over p are understood to be over primes, and all other sums are over the natural numbers $\mathbb{N} = \{1, 2, 3, \dots\}$ unless otherwise indicated.

Given two functions $f, g : \mathbb{N} \to \mathbb{C}$, their Dirichlet convolution $f * g$ is defined by

$$f * g(n) := \sum_{d|n} f(d) g\Big(\frac{n}{d}\Big),$$

where $d \mid n$ denotes the assertion that d divides n.

Given two natural numbers a and b, we use (a, b) to denote the greatest common divisor of a and b and $a\ (b)$ to denote the residue class of integers equal to a modulo b. Given a natural number r, we use $(\mathbb{Z}/r\mathbb{Z})^\times = \{a\ (r) : (a, r) = 1\}$ to denote the primitive residue classes modulo r.

We use 1_E to denote the indicator function of E; thus, $1_E(n)$ equals 1 when $n \in E$ and equals 0 otherwise. Similarly, if S is a sentence, we write 1_S to equal 1 when S is true and 0 otherwise; thus, for instance, $1_E(n) = 1_{n \in E}$.

2. Vinogradov from Elliott–Halberstam

We now prove Theorem 1.3. We will in fact prove a slightly stronger implication, in which Conjecture 1.1 is replaced by:

Conjecture 2.1. *For any Dirichlet character χ, let n_χ be the first natural number with $\chi(n_\chi) \neq 1$. For any fixed $\varepsilon > 0$, we have $n_\chi \ll q^\varepsilon$ for any primitive Dirichlet character χ of prime conductor q.*

Clearly, Conjecture 1.1 is the special case of Conjecture 2.1 in which χ is a quadratic character.

Assume the Elliott–Halberstam conjecture. Suppose for sake of contradiction that Conjecture 1.1 failed; then we can find a fixed $\kappa > 0$ and a sequence q of primes going to infinity, as well as a character χ of modulus q, such that

$$n_\chi > q^\kappa.$$

Without loss of generality, we may take κ to be small, e.g., $\kappa < \frac{1}{2}$. We view q as an asymptotic parameter for the purposes of asymptotic notation and reserve the right to refine q to subsequences as necessary.

We will need some basic results from the theory of mean values of multiplicative functions in order to produce some anomalous distribution for $\chi(n)\Lambda(n)$ at large scales. This could be accomplished using the results of Granville and Soundararajan [2001] (or even the earlier work of Wirsing [1967]), but we do not need the full strength of their theory here since we will be satisfied with an analysis of logarithmic densities such as $(1/\log x)\sum_{n\le x}\chi(n)/n$ instead of natural densities such as $(1/x)\sum_{n\le x}\chi(n)$. As such, we give a self-contained treatment here.

It will be technically convenient to work in the asymptotic limit in which we extract the mean value after sending q to infinity (this is a luxury available in the logarithmic density setting that is not easily achievable for natural densities, at least if one is not willing to use the tools of nonstandard analysis). For any fixed $t \ge 0$, we consider the logarithmic densities

$$A_q(t) := \frac{1}{\log q}\sum_{n<q^t}\frac{\chi(n)}{n},$$

$$B_q(t) := \frac{1}{\log q}\sum_{n<q^t}\frac{\chi(n)\Lambda(n)}{n}.$$

From Mertens' theorem, we have the Lipschitz bounds

$$|A_q(t) - A_q(s)|, |B_q(t) - B_q(s)| \le |t-s| + o(1) \tag{2-1}$$

for all fixed $t, s \ge 0$; also we clearly have $A_q(0) = B_q(0) = 0$. From the Arzelà–Ascoli theorem, and refining q to a subsequence as necessary, we may thus find *fixed* Lipschitz functions $A, B : [0,+\infty) \to \mathbb{C}$ such that

$$A_q(t) = A(t) + o(1), \qquad B_q(t) = B(t) + o(1) \tag{2-2}$$

for all fixed $t \ge 0$; that is to say that A_q and B_q converge locally uniformly to A and B, respectively. (The traditional form of the Arzelà–Ascoli theorem allows one to pass to a subsequence on which one has uniform convergence on $[0,n]$ for each natural number n, and then a further diagonalization gives locally uniform convergence on $[0,+\infty)$.) From (2-1), we have

$$|A(t) - A(s)|, |B(t) - B(s)| \le |t-s|$$

for all fixed $t, s \ge 0$. By the Rademacher differentiation theorem, we can thus find Lebesgue-measurable functions $a, b : [0,+\infty) \to \mathbb{C}$ bounded in magnitude by 1, defined up to almost-everywhere equivalence, such that

$$A(t) = \int_0^t a(u)\,du, \qquad B(t) = \int_0^t b(u)\,du$$

for all $t \in [0,+\infty)$.

We now establish some bounds on A and B. Since χ has mean zero on intervals of length q, it is easy to see that

$$A_q(t) = A_q(t') + o(1)$$

for all fixed $t, t' > 1$; in fact, one can extend this to $t, t' > \frac{1}{4}$ using the Burgess bound [1957], but we will not need to do so here. This implies that a is supported on $[0, 1]$ (modulo null sets).

Next, since $\chi(n) = 1$ for $n \le q^\kappa$, we have from Mertens' theorem that

$$A_q(t), B_q(t) = t + o(1)$$

for $t < \kappa$. Thus, $A(t) = B(t) = t$ for $t < \kappa$, and so $a(t) = b(t) = 1$ for $t < \kappa$ (again up to null sets).

Next, we claim that a and b obey the integral equation of Wirsing [1967]:

Lemma 2.2 (Wirsing equation). *We have*

$$ta(t) = \int_0^t a(u)b(t-u)\,du$$

for almost all $t > 0$.

This equation also holds for means other than logarithmic densities (replacing a and b by suitable substitutes, such as the functions $t \mapsto (1/q^t)\sum_{n\le q^t}\chi(n)$ and $t \mapsto (1/q^t)\sum_{n\le q^t}\chi(n)\Lambda(n)$, respectively), but the arguments are more complicated, and one has to work nonasymptotically and admit some $o(1)$ errors; see [Wirsing 1967; Granville and Soundararajan 2001].

Proof. We start with the Dirichlet convolution identity

$$\chi(n)\log n = (\chi\Lambda) * \chi(n)$$

and conclude for any fixed $t > 0$ that

$$\frac{1}{\log^2 q}\sum_{n\le q^t}\frac{\chi(n)\log n}{n} = \frac{1}{\log q}\sum_{d\le q^t}\frac{\chi(d)\Lambda(d)}{d}\frac{1}{\log q}\sum_{m\le q^t/d}\frac{\chi(m)}{m}. \tag{2-3}$$

To estimate this expression, we use a Riemann sum argument. Let $J > 0$ be a large fixed natural number. If $q^{(j-1)t/J} \le d < q^{jt/J}$ for some $1 \le j \le J$, then $(1/\log q)\sum_{m\le q^t/d}\chi(m)/m = A(t - jt/J) + O(1/J) + o(1)$ (with implied constant uniform in J), and so the expression (2-3) may be written (after using Mertens' theorem to estimate error terms) as

$$\left(\sum_{j=1}^{J} A\left(t - \frac{jt}{J}\right)\frac{1}{\log q}\sum_{q^{(j-1)t/J}\le d<q^{jt/J}}\frac{\chi(d)\Lambda(d)}{d}\right) + O\left(\frac{1}{J}\right) + o(1).$$

One has

$$\frac{1}{\log q}\sum_{q^{(j-1)t/J}\le d<q^{jt/J}}\frac{\chi(d)\Lambda(d)}{d} = B(jt/J) - B((j-1)t/J) + o(1)$$
$$= \int_{(j-1)t/J}^{jt/J} b(u)\,du + o(1),$$

and so (by the Lipschitz nature of A), the previous expression becomes

$$\int_0^1 A(t-u)b(u)\,du + O\left(\frac{1}{J}\right) + o(1).$$

As J can be arbitrarily large, we conclude that

$$\frac{1}{\log^2 q}\sum_{n\le q^t}\frac{\chi(n)\log n}{n} = \int_0^t A(t-u)b(u)\,du + o(1).$$

On the other hand, from the identity $\log n/\log q = t - \int_0^t 1_{n\le q^u}\,du$ and (2-2), we see (after a Riemann sum argument as before) that

$$\frac{1}{\log^2 q}\sum_{n\le q^t}\frac{\chi(n)\log n}{n} = tA(t) - \int_0^t A(u)\,du + o(1)$$

and hence

$$tA(t) - \int_0^t A(u)\,du = \int_0^t A(t-u)b(u)\,du$$

for all t. Differentiating using the Lebesgue differentiation theorem, we conclude that

$$ta(t) = \int_0^t a(t-u)b(u)\,du$$

almost everywhere, as desired. □

We will use this equation, together with some complex analysis and the previously established compact support of a, to derive the following consequence:

Corollary 2.3. *b is not compactly supported (up to null sets).*

Proof. Suppose for contradiction that b is compactly supported (modulo null sets). Now consider the Fourier–Laplace transforms

$$\mathcal{L}a(s) := \int_0^\infty a(t)e^{-ts}\,dt,$$
$$\mathcal{L}b(s) := \int_0^\infty b(t)e^{-ts}\,dt;$$

as a and b are both bounded and compactly supported, the functions $\mathcal{L}a$ and $\mathcal{L}b$ are entire and of at most exponential growth and are not identically zero since a

and b are not identically zero. On the other hand, from Lemma 2.2 and standard computations, we have

$$-\frac{d}{ds}\mathcal{L}a = \mathcal{L}a \times \mathcal{L}b. \tag{2-4}$$

As $\mathcal{L}b$ has no poles, $\mathcal{L}a$ cannot have any zeros; in particular, $\log \mathcal{L}a$ is entire and grows at most linearly and must therefore be a linear function so that $\mathcal{L}a$ is an exponential function, and hence, by (2-4), $\mathcal{L}b$ is a constant function. But this is absurd (it contradicts the Riemann–Lebesgue lemma). □

Remark 2.4. The above argument shows that a and b cannot both be compactly supported while still obeying Lemma 2.2, except in trivial cases. A stronger result in this regard, in which a and b are allowed to decay exponentially, can be found in [Granville and Soundararajan 2007]. Note that the argument used to establish this corollary would have been significantly messier if one had to contend with $o(1)$ errors in the Wirsing integral equation as one would need quantitative approximate versions of various basic qualitative facts about entire functions. This is the main reason why we took the asymptotic limit $q \to \infty$ previously. However, Andrew Granville (private communication) has informed me that such an approximate version of this observation was obtained in an unpublished work of Granville and Soundararajan. (See also the recent paper [Granville and Soundararajan 2015] for some related results.)

From the above corollary and the Lebesgue differentiation theorem, we can find fixed $1 < t_1 < t_2$ such that $|B(t_2) - B(t_1)| > 0$, and so

$$\left| \frac{1}{\log q} \sum_{q^{t_1} < n < q^{t_2}} \frac{\chi(n)\Lambda(n)}{n} \right| \gg 1$$

for q sufficiently large. By the pigeonhole principle, we may thus find $q^{t_1} \ll x \ll q^{t_2}$ such that

$$\left| \sum_{n \in [x/2, x]} \chi(n)\Lambda(n) \right| \gg x.$$

Of course, x will depend on q. Since $q = o(x)$, we may shift n by q, using the periodicity of χ, to conclude that

$$\left| \sum_{n \in [x/2, x]} \chi(n)\Lambda(n+q) \right| \gg x.$$

On the other hand, as χ has mean zero on intervals of length q, we have

$$\sum_{n \in [x/2, x]} \chi(n) = o(x).$$

Thus, if we let

$$X := \sum_{n\in[x/2,x]} \chi(n)(\Lambda(n+q)-1),$$

then we have

$$|X| \gg x \tag{2-5}$$

for sufficiently large q.

We now upper-bound X in order to contradict (2-5). The first step is to expand out χ in terms of Dirichlet convolutions. By Möbius inversion, we can express

$$\chi = 1 * f = 1 + 1 * \tilde{f},$$

where

$$\tilde{f}(n) := f(n) - 1_{n=1}$$

and

$$f = \chi * \mu;$$

in other words, f is the multiplicative function with

$$f(p^j) = \chi(p)^{j-1}(\chi(p)-1)$$

whenever p is a prime and $j \geq 1$, with the convention that $0^0 = 1$. In particular, we see that $f(n)$ is only nonzero when n is q^κ*-rough*, by which we mean that n has no prime factor less than or equal to q^κ; this implies furthermore that $\tilde{f}(n)$ vanishes unless $n > q^\kappa$ and that

$$|\tilde{f}(n)| \ll 1 \tag{2-6}$$

whenever $n = O(q^{O(1)})$.

Let $\nu > 0$ be a small fixed constant to be chosen later. We expand X using the identity

$$\chi 1_{[x/2,x]} = 1_{[x/2,x]} + (1_{[1,x^\nu)} * \tilde{f})1_{[x/2,x]} + (1_{[x^\nu,q^{-\kappa}x]} * \tilde{f})1_{[x/2,x]}, \tag{2-7}$$

where we have used the fact that $\tilde{f}(n)$ vanishes for $n < q^\kappa$. This gives the splitting

$$X = X_1 + X_2 + X_3$$

where

$$X_1 = \sum_{n\in[x/2,x]} (\Lambda(n+q)-1),$$

$$X_2 = \sum_{n\in[x/2,x]} (1_{[1,x^\nu)} * \tilde{f})(n)(\Lambda(n+q)-1),$$

$$X_3 = \sum_{n\in[x/2,x]} (1_{[x^\nu,q^{-\kappa}x]} * \tilde{f})(n)(\Lambda(n+q)-1).$$

From the prime number theorem, we have

$$X_1 = o(x).$$

For X_2, we use the triangle inequality to bound

$$|X_2| \leq \sum_{d<x^\nu} \sum_{x/2d\leq m\leq x/d} |\tilde{f}(m)|(\Lambda(dm+q)+1).$$

We claim that

$$\sum_{x/2d\leq m\leq x/d} |\tilde{f}(m)|\Lambda(dm+q) \ll \frac{x}{\varphi(d)\log x} \tag{2-8}$$

and

$$\sum_{x/2d\leq m\leq x/d} |\tilde{f}(m)| \ll \frac{x}{d\log x} \tag{2-9}$$

for all $d < x^\nu$, and hence,

$$X_2 \ll \nu x$$

with implied constant independent of ν.

We first prove (2-8). From (2-6), we have $|\tilde{f}(m)|\Lambda(dm+q) = O(\log x)$, and this expression vanishes unless m and $dm+q$ are both q^κ-rough, except for a small exceptional contribution (coming from when $dm+q$ is the power of a small prime) that can easily be seen to be negligible. Removing this exceptional contribution, we see that we are removing two residue classes modulus p from the interval of m for each prime $p < x^\kappa$ not dividing d. Using a standard upper-bound sieve (see, e.g., [Friedlander and Iwaniec 2010]), we conclude that the number of surviving summands m is $O(x/(\varphi(d)\log^2 x))$, and the claim follows. The bound (2-9) is established similarly, except now we bound $|\tilde{f}(m)| = O(1)$ and we remove just a single residue class for each prime p, rather than two.

Finally we turn to X_3. We expand

$$X_3 = \sum_{q^\kappa \ll r \ll x^{1-\nu}} \tilde{f}(r) \sum_{m\in[x/2r,x/r]\cap[x^\nu,q^{-\kappa}x]} (\Lambda(rm+q)-1).$$

The contribution when $r \asymp q^\kappa$ or $r \asymp x^{1-\nu}$ can be seen to be $O(x/\log x)$ using the Brun–Titchmarsh inequality (and upper-bound sieve bounds on q^κ-rough numbers, as in the estimation of X_2). The contribution when r is divisible by q can be treated similarly (in fact one has the better bound of $O(x/q)$ in this case). So we may write

$$X_3 = \sum_{2q^\kappa<r<x^{1-\nu}/2;(r,q)=1} \tilde{f}(r) \sum_{x/2r\leq m\leq x/r} (\Lambda(rm+q)-1) + o(x)$$

or equivalently (since q is significantly smaller than x)

$$X_3 = \sum_{2q^\kappa<r<x^{1-\nu}/2;(r,q)=1} \tilde{f}(r) \sum_{n\in[x/2,x]:n=q\ (r)} (\Lambda(n)-1) + o(x).$$

Invoking the Elliott–Halberstam conjecture and the prime number theorem, we then have

$$X_3 = \sum_{2q^\kappa < r < x^{1-\nu}/2; (r,q)=1} \tilde{f}(r)\left(\frac{1}{\varphi(r)}\frac{x}{2} - \frac{1}{r}\frac{x}{2}\right) + o(x).$$

If r contributes to the above sum, then it is the product of $O(1)$ primes of size at least q^κ, and so $1/\varphi(r) = 1/r + O(q^{-\kappa}/r)$. From this, we see that

$$X_3 = o(x).$$

Putting all this together, we conclude that

$$|X| \ll (\nu + o(1))x,$$

contradicting (2-5) for ν small enough. This completes the proof of Theorem 1.3.

Remark 2.5. Our arguments here do not easily give any effective quantitative bound on $n(p)$ due to our use of asymptotic limits; in particular, the fixed quantities t_1 and t_2 appearing above were obtained by what is essentially a compactness argument and thus not obviously effective. It is likely that a more carefully quantitative version of the above argument (perhaps using the estimates from [Granville and Soundararajan 2001]) can make this portion of the argument effective, thus allowing one to derive partial progress on the Vinogradov conjecture from sufficiently strong partial progress on the Elliott–Halberstam conjecture; however, the dependence of constants will be far worse than in Theorem 1.6. We will not pursue this question further here.

Remark 2.6. Suppose the Burgess bound (1-2) was sharp up to epsilon factors, in the sense that one could find a sequence of primes q going to infinity with $n(q) = q^{1/4\sqrt{e}+o(1)}$. Then by extracting a limit to obtain the functions a and b as above, we see that $a(t) = b(t) = 1$ for $t \le 1/4\sqrt{e}$ and (from the Burgess character sum bounds) $a(t) = 0$ for $t > \frac{1}{4}$. As was first observed by Heath-Brown (see, e.g., Appendix 2 of [Diamond et al. 2006]), this information allows one in this case to determine the functions a and b completely. Indeed, in the range $1/4\sqrt{e} \le t < 1/2\sqrt{e}$, one has from Lemma 2.2 that

$$ta(t) = \int_0^t a(u)\,du - \int_0^{t-1/4\sqrt{e}} (1 - b(t-u))\,du.$$

Bounding $1 - b(t-u)$ by 2, we thus have

$$ta(t) \ge \int_0^t a(u)\,du - 2(t - 1/4\sqrt{e})$$

and thus by Gronwall's inequality

$$a(t) \ge 1 - 2\log(4\sqrt{e}t).$$

(Indeed, one can verify that the difference $f(t) := a(t) - 1 + 2\log(4\sqrt{e}t)$ obeys the inequality $tf(t) \geq \int_{1/4\sqrt{e}}^{t} f(u)\,du$ for $1/4\sqrt{e} \leq t < 1/2\sqrt{e}$ with $f(1/4\sqrt{e}) = 0$.) Since equality is attained for $t = \frac{1}{4}$ (note from Lemma 2.2 that a is continuous), we must have $1 - b(t-u) = 2$ whenever $t \leq \frac{1}{4}$ and $0 \leq u < t - 1/4\sqrt{e}$; that is to say $b(t) = -1$ for $1/4\sqrt{e} < t \leq \frac{1}{4}$; also $a(t) = 1 - 2\log(4\sqrt{e}t)$ in this range. For $t > \frac{1}{4}$, Lemma 2.2 gives

$$0 = \int_0^t a(t-u)b(u)\,du,$$

which on differentiation gives the integral equation

$$b(t) = 2\int_{1/4\sqrt{e}}^{1/4} b(t-u)\,\frac{du}{u},$$

which can then be used to complete the description of b, for instance via Laplace transforms. For instance, we see that $b(t) = 1$ for $\frac{1}{4} < t \leq 1/2\sqrt{e}$. One can compute that b does not vanish near $t = 1$, in which case the argument above shows that some improvement upon (1-2) can be made provided one can establish the Elliott–Halberstam conjecture for some $\vartheta > 1 - 1/4\sqrt{e} \approx 0.8484$.

3. From Elliott–Halberstam to the least primitive root

We now prove Theorem 1.4. The key new tool is the following combinatorial statement. Given a subset A of an additive group $G = (G, +)$ and a natural number k, define the iterated sumset kA to be the set of all sums $a_1 + \cdots + a_k$, where $a_1, \ldots, a_k$ are elements in A (allowing repetition).

Proposition 3.1 (escape from cosets). *Let $d, m \geq 1$ be fixed integers. Then there exists a natural number k with the following property: whenever G is a finite additive group whose order is the product of at most d primes (counting multiplicity) and A is a subset of G containing 0 for which one has inclusions of the form*

$$kA \subset \bigcup_{i=1}^{m} x_i + H_i \subsetneq G$$

for some cosets $x_i + H_i$ of subgroups H_i of G, then A is contained in a proper subgroup of G.

In the contrapositive, Proposition 3.1 asserts that, if A generates G and contains 0, then the iterated sumsets kA for k large enough cannot be covered by a small number of cosets of subgroups of G, unless these cosets of subgroups already covered all of G. Thus, the sumsets kA "escape" all nontrivial unions of boundedly many cosets. This result can be viewed as a simple abelian variant of the nonabelian "escape from subvarieties" lemma that first appeared in [Eskin et al. 2005].

Let us assume this proposition for the moment and see how it implies Theorem 1.4. Assume the Elliott–Halberstam conjecture, and assume for sake of contradiction that the conclusion of Theorem 1.4 failed. Carefully negating the quantifiers, this means that we can find a sequence of primes p going off to infinity, with $p-1$ being the product of $O(1)$ primes, and a fixed $\kappa > 0$, with the property that the least primitive root of $\mathbb{Z}/p\mathbb{Z}$ is at least p^κ.

Using a discrete logarithm, we have an isomorphism $\log : (\mathbb{Z}/p\mathbb{Z})^\times \to G$ from the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ to the additive cyclic group $G := \mathbb{Z}/(p-1)\mathbb{Z}$. If n is a natural number less than p^κ, then by hypothesis n is not a primitive root of $(\mathbb{Z}/p\mathbb{Z})^\times$, which implies that

$$\log(n) \subset \bigcup_{r|p-1:r<p-1} \{x \in G : rx = 0\} \subsetneq G.$$

In particular, for any natural number k, if we set $A := \{\log(n) : 1 \leq n < p^{\kappa/k}\}$, then

$$kA \subset \bigcup_{r|p-1:r<p-1} \{x \in G : rx = 0\} \subsetneq G.$$

Since $\log(1) = 0$, A contains 0. Applying Proposition 3.1 (and using the hypothesis that $p-1$ is the product of $O(1)$ primes), we conclude (for k large enough) that A is contained in a proper subgroup of G. Equivalently, A lies in the kernel of a primitive character χ of conductor p; thus, $\chi(n) = 1$ for all $n < p^{\kappa/k}$. But this contradicts Conjecture 2.1, which as we saw in the previous section was a consequence of the Elliott–Halberstam conjecture.

It remains to prove Proposition 3.1. To illustrate the proposition, let us first give a simple case when G is a direct product $H_1 \times H_2$ and we are given that $0 \in A$ and

$$2A \subset (H_1 \times \{0\}) \cup (\{0\} \times H_2).$$

We claim that this forces either $A \subset H_1 \times \{0\}$ or $A \subset \{0\} \times H_2$. Indeed, if neither of these statements were true, then either there would exist $a \in A$ that was outside both $H_1 \times \{0\}$ and $\{0\} \times H_2$ or else there would exist $a_1, a_2 \in A$ with $a_1 \in H_1 \times \{0\}$, $a_2 \in \{0\} \times H_2$, and $a_1, a_2 \neq 0$. In either case, we could find an element of $2A$ ($a+0$ or a_1+a_2, respectively) that was outside of $(H_1 \times \{0\}) \cup (\{0\} \times H_2)$, giving the desired contradiction. This simple special case is already sufficient to handle the case of Theorem 1.4 in which $p-1$ is the product of just two primes (that is, $p-1 = 2q$ for some prime q) although in this case it turns out that the least primitive root is also the least quadratic nonresidue (for p large enough, at least), so the claim in this case is already immediate from Theorem 1.3.

The general case can be obtained by a rather complicated induction on the "complexity" of the covering set $\bigcup_{i=1}^m x_i + H_i$, as follows. Fix a natural number d.

Define a *configuration* to be a tuple

$$(k, G, A, m, (x_i + H_i)_{i=1}^m), \tag{3-1}$$

where k and m are natural numbers, G is a finite additive group with $|G|$ the product of d primes, A is a subset of G containing 0 and not contained in any proper subgroup of G, and the $x_i + H_i$ are distinct cosets in G, such that

$$kA \subset \bigcup_{i=1}^m x_i + H_i \subsetneq G. \tag{3-2}$$

In particular, this implies that $H_i \neq G$ for each i. Our task is to show that, for any configuration (3-1), k is bounded by a quantity depending only on d and m.

Suppose for contradiction that this claim failed. Then we can find a sequence of configurations (3-1) in which m stays constant but k goes to infinity. (The other data G, A, x_i, and H_i in the sequence may vary arbitrarily.)

Now we define a measure of complexity of a configuration (3-1). Given a subgroup H of G, define the *dimension* $\dim H$ of H to be the quantity such that the order $|H|$ of H is the product of $\dim H$ primes (counting multiplicity). This is a natural number between 0 and d, and any proper subgroup of G has dimension at most $d-1$.

Given a configuration (3-1), define the *complexity* of the configuration to be the tuple $(m_0, \dots, m_{d-1})$, where, for each $j = 0, \dots, d-1$, m_j is the number of cosets $x_i + H_i$ in the configuration such that H_i has dimension j. Since all the H_i have dimensions between 0 and $d-1$, we see that the $m_0, \dots, m_{d-1}$ are natural numbers that sum to m. In particular, if m is constant, there are only finitely many possible complexities. Thus, by passing to a subsequence if necessary, we can find a sequence of configurations (3-1) whose complexity $(m_0, \dots, m_{d-1})$ stays constant, but k goes to infinity.

We give the space of tuples $(m_0, \dots, m_{d-1}) \in \mathbb{N}^d$ the lexicographical ordering: we write $(m_0, \dots, m_{d-1}) < (n_0, \dots, n_{d-1})$ if there exists $0 \leq i \leq d-1$ such that $m_i < n_i$ and $m_j = n_j$ for $i < j \leq d-1$. As is well-known, this makes $\mathbb{N}^d$ a well-ordered set.

Call a tuple $(m_0, \dots, m_{d-1})$ *good* if there exists a sequence of configurations (3-1) with constant complexity $(m_0, \dots, m_{d-1})$, for which k goes to infinity. We have seen that there is at least one good tuple; by the well-ordering of $\mathbb{N}^d$, we may thus find a minimal good tuple $(m_0, \dots, m_{d-1})$.

By rounding k down to an even number and then dividing by two, we may thus find a sequence of configurations

$$(2k, G, A, m, (x_i + H_i)_{i=1}^m) \tag{3-3}$$

of complexity $(m_0, \dots, m_{d-1})$ with k going to infinity.

Let d_* be the largest j for which m_j is nonzero; thus, $0 \le d_* \le d-1$ (note that at least one of the m_j must be nonzero; otherwise, the first inclusion in (3-2) could not hold). By relabeling, we may assume without loss of generality that H_1 has dimension d_* for any configuration (3-3) in the above sequence.

Consider a configuration (3-3) in the above sequence; then

$$2kA \subset \bigcup_{i=1}^{m} x_i + H_i.$$

In particular, for any $y \in kA$, we have

$$kA \subset 2kA \cap (2kA - y) \subset \bigcup_{i=1}^{m} \bigcup_{j=1}^{m} (x_i + H_i) \cap (x_j - y + H_j).$$

Note that the set $(x_i + H_i) \cap (x_j - y + H_j)$ is either empty or a coset of $H_i \cap H_j$, which has dimension at most d_*, with equality if and only if $H_i = H_j$ has dimension d_*. In particular, since all the cosets $x_j + H_j$ are assumed distinct, we see that, if H_i has dimension d_*, there is at most one set $(x_i + H_i) \cap (x_j - y + H_j)$ that is a coset of a d_*-dimensional subgroup. In particular, at most m_{d_*} of the $(x_i + H_i) \cap (x_j - y + H_j)$ arise as cosets of d_*-dimensional subgroups.

Now suppose that we can find $y \in kA$ such that

$$y \notin \bigcup_{1 \le j \le m : H_j = H_1} x_j - x_1 + H_1. \tag{3-4}$$

Then we see that $x_1 + H_1 \ne x_j - y + H_j$ for any $j = 1, \dots, m$. As such, now at most $m_{d_*} - 1$ of the $(x_i + H_i) \cap (x_j - y + H_j)$ arise as cosets of d_*-dimensional subgroups. Collecting all the cosets of the form $(x_i + H_i) \cap (x_j - y + H_j)$ and eliminating duplicates, we obtain a new configuration

$$(k, G, A, m', (x_i' + H_i')_{i=1}^{m'}),$$

which has strictly lower complexity than $(m_0, \dots, m_{d-1})$. By the minimality of $(m_0, \dots, m_{d-1})$, this situation can only occur for finitely many of the sequence of configurations (3-3). Thus, after discarding finitely many terms, we may assume that the situation (3-4) does not occur for any $y \in kA$; that is to say, we have

$$kA \subset \bigcup_{1 \le j \le m : H_j = H_1} x_j - x_1 + H_1.$$

This gives rise to a configuration of strictly lower complexity than $(m_0, \dots, m_{d-1})$, unless $(m_0, \dots, m_{d-1}) = (0, \dots, 0, m, 0, \dots, 0)$ (with m in the d_* position), and all of the H_j are equal to H_1. Thus, after discarding finitely many terms in the

sequence, we may assume that $H_j = H_1$ for all j, and so

$$kA \subset \bigcup_{j=1}^{m} x_j - x_1 + H_1.$$

Intersecting this with the inclusion $kA \subset \bigcup_{j=1}^m x_j + H_1$, we again obtain a configuration of lower complexity, unless the set of cosets $\{x_j + H_1 : 1 \le j \le m\}$ is invariant with respect to translation by x_1; so by discarding another finite number of terms in the sequence, we may assume that this is the case. By permuting indices, we can then assume that $\{x_j + H_1 : 1 \le j \le m\}$ is invariant under translation by x_i for any $1 \le i \le m$. In other words, $\{x_j + H_1 : 1 \le j \le m\}$ is a subgroup of the quotient group G/H_1, so $\bigcup_{j=1}^m x_j + H_1$ is a subgroup of G. But this has to be a proper subgroup by (3-2), and so A is in a proper subgroup of G, a contradiction.

4. Character sums from Type II sums

We now prove Theorem 1.6. Suppose that Conjecture 1.5 holds for a fixed choice of $0 < \varpi < \frac{1}{4}$. Let $\delta > 0$ be as in Conjecture 1.5; we may assume that δ is small, e.g., $\delta < \frac{1}{4}$. Let $\varepsilon > 0$ be a sufficiently small fixed quantity depending on δ. If the claim (1-8) failed, then we could find a sequence of nonprincipal primitive characters χ with conductor q going to infinity such that

$$\left| \sum_{n < q^{1/2-2\varpi+\varepsilon}} \chi(n) \right| \gg q^{1/2-2\varpi+\varepsilon} \log^{-A} q$$

for some fixed $A > 0$. From the pigeonhole principle, we have

$$\left| \sum_{n \in [N/2, N]} \chi(n) \right| \gg N \log^{-A} q \tag{4-1}$$

for some $N = q^{1/2-2\varpi+\varepsilon} \log^{-O(A)} q$ (of course, N will depend on q).

Set $x := N^{1/(1/2-2\varpi)}$ and $M := x/N$; thus,

$$N = x^{1/2-2\varpi}, \qquad M = x^{1/2+2\varpi}$$

and

$$x \ge q^{1+2\varepsilon}. \tag{4-2}$$

Let $\mathcal{D}$ be the set of square-free natural numbers in $[(1-\log^{-10A-10} x)M, M]$ whose prime factors all lie in $[q^\varepsilon, x^\delta]$ not dividing q. Note that the number of primes dividing q may be crudely bounded by $O(\log q)$ and are thus a negligible proportion of the primes in $[q^\varepsilon, x^\delta]$. If ε is small enough, then the prime number theorem gives the cardinality bound

$$|\mathcal{D}| \asymp M \log^{-10A-11} x. \tag{4-3}$$

(We allow implied constants to depend on the fixed quantities ε, δ, and A.)

We now set

$$\alpha(m) := 1_{\mathcal{D}}(m)\overline{\chi(m)}$$

and

$$\beta(n) := 1_{[N/2,N]}(n) \tag{4-4}$$

and consider the quantity

$$\sum_{j\le q^{\varepsilon}}\sum_{n\le x}\chi(n)\alpha*\beta(n+jq).$$

Shifting n by jq and using the periodicity of χ, we may write this as

$$\sum_{j\le q^{\varepsilon}}\sum_{jq<n\le x+jq}\chi(n)\alpha*\beta(n).$$

Since $\alpha*\beta$ is supported on $[MN/4, MN] = [x/4, x]$, this is equal (by (4-2)) to

$$\sum_{j\le q^{\varepsilon}}\sum_{n}\chi(n)\alpha*\beta(n),$$

which factorizes as

$$\sum_{j\le q^{\varepsilon}}\Big(\sum_{m}\chi(m)\alpha(m)\Big)\Big(\sum_{n}\chi(n)\beta(n)\Big),$$

and hence, by (4-1) and (4-3), we have

$$\Big|\sum_{n\le x}\chi(n)\sum_{j\le q^{\varepsilon}}\alpha*\beta(n+jq)\Big| \gg xq^{\varepsilon}\log^{-11A-11}x.$$

We now "disperse" the $\alpha*\beta$ factors and eliminate the χ factors by a Cauchy–Schwarz argument. Let γ denote the quantity

$$\gamma := \frac{1}{x/2}\sum_{n}\alpha*\beta(n), \tag{4-5}$$

which (since $\sum_n \beta(n) = (1+o(1))N/2$) factorizes as

$$\gamma = \frac{1+o(1)}{M}\sum_{m}\alpha(m). \tag{4-6}$$

In particular, from (4-3) we have

$$\gamma = O(\log^{-10A-11}x). \tag{4-7}$$

Since χ has mean 0 on intervals of length q, we have

$$\Big|\sum_{n\le x}\chi(n)\sum_{j\le q^{\varepsilon}}\gamma 1_{[x/2,x]}(n+jq)\Big| \ll \gamma q q^{\varepsilon} = o(xq^{\varepsilon}\log^{-11A-11}x)$$

and thus

$$\left|\sum_{n\le x}\chi(n)\sum_{j\le q^{\varepsilon}}(\alpha*\beta-\gamma 1_{[x/2,x]})(n+jq)\right|\gg xq^{\varepsilon}\log^{-11A-11}x.$$

Applying the Cauchy–Schwarz inequality, we conclude that

$$\sum_{n\le x}\left|\sum_{j\le q^{\varepsilon}}(\alpha*\beta-\gamma 1_{[x/2,x]})(n+jq)\right|^2\gg xq^{2\varepsilon}\log^{-22A-22}x,$$

which we rearrange (using the support of $\alpha*\beta-\gamma 1_{[x/2,x]}$ to remove the restriction $n\le x$) as

$$\left|\sum_{j,j'\le q^{\varepsilon}}\sum_{n}(\alpha*\beta-\gamma 1_{[x/2,x]})(n)(\alpha*\beta-\gamma 1_{[x/2,x]})(n+(j'-j)q)\right|\gg xq^{2\varepsilon}\log^{-22A-22}x. \quad (4\text{-}8)$$

From the divisor bound, we have $\alpha*\beta=x^{o(1)}$, and the inner sum

$$\sum_{n}(\alpha*\beta-\gamma 1_{[x/2,x]})(n)(\alpha*\beta-\gamma 1_{[x/2,x]})(n+(j'-j)q)$$

may then be crudely bounded as $x^{1+o(1)}$. From this, we may remove the diagonal contribution $j=j'$ from (4-8); by symmetry, we may then reduce to the case $j'<j$. By the pigeonhole principle, we thus have

$$\left|\sum_{n}(\alpha*\beta-\gamma 1_{[x/2,x]})(n)(\alpha*\beta-\gamma 1_{[x/2,x]})(n-jq)\right|\gg x\log^{-22A-22}x \quad (4\text{-}9)$$

for some $1\le j\le q^{\varepsilon}$.

Let j be as above. We have

$$\sum_{n}\gamma 1_{[x/2,x]}(n)\times\gamma 1_{[x/2,x]}(n-jq)=\gamma^2\frac{x}{2}+o(x\log^{-22A-22}x).$$

Also, the quantity $\alpha*\beta$ is supported in $[(1-\log^{-10A-10}x)x/2,x]$. Standard divisor sum calculations using (4-3) give

$$\sum_{n}|\alpha*\beta(n)|1_{[(1-O(\log^{-10A-10}x))x/2,x/2]}(n)=O(x\log^{-20A-21}x) \quad (4\text{-}10)$$

and similarly

$$\sum_{n}|\alpha*\beta(n)|1_{[x,x(1+O(\log^{-10A-10}x))]}(n)=O(x\log^{-20A-21}x) \quad (4\text{-}11)$$

while from (4-5) one has

$$\sum_n \alpha * \beta(n)\gamma = \gamma^2 \frac{x}{2}.$$

We conclude (using (4-7)) that

$$\sum_n \alpha * \beta(n) \times \gamma 1_{[x/2,x]}(n - jq) = \gamma^2 \frac{x}{2} + o(x \log^{-22A-22} x).$$

A similar argument gives

$$\sum_n \gamma 1_{[x/2,x]}(n) \times \alpha * \beta(n - jq) = \gamma^2 \frac{x}{2} + o(x \log^{-22A-22} x).$$

Inserting these bounds into (4-9), we conclude that, if X denotes the quantity

$$X := \sum_n \alpha * \beta(n)\alpha * \beta(n - jq), \tag{4-12}$$

then we have

$$\left| X - \gamma^2 \frac{x}{2} \right| \gg x \log^{-22A-22} x \tag{4-13}$$

for q large enough.

Now we estimate X using Type II estimates in order to contradict (4-13). Expanding out the convolution $\alpha * \beta(n)$, we have

$$X = \sum_r \alpha(r) \sum_{N/2 \le m \le N} \alpha * \beta(rm - jq)$$

or equivalently

$$X = \sum_r \alpha(r) \sum_{\substack{rN/2 - jq \le n \le rN - jq \\ n = jq\ (r)}} \alpha * \beta(n).$$

Note from the support of α that $rN/2 - jq = x/2 + O(x \log^{-10A-10} x)$ and $rN - jq = x + O(x \log^{-10A-10} x)$ if $\alpha(r)$ is nonzero. A modification of (4-10) and (4-11) then shows that

$$\sum_{\substack{rN/2 + jq \le n \le rN + jq \\ n = jq\ (r)}} \alpha * \beta(n) = \sum_{n : n = jq\ (r)} \alpha * \beta(n) + O\left(\frac{x}{r} \log^{-20A-21} x\right),$$

and thus (by (4-3)),

$$X = \sum_r \alpha(r) \sum_{n : n = jq\ (r)} \alpha * \beta(n) + o(x \log^{-22A-22} x).$$

From construction, we see that jq is coprime to every prime between x^ε and x^δ that does not divide q and is in particular coprime to r. From the Type II estimate

hypothesis, we have

$$\sum_r |\alpha(r)| \Big| \sum_{n:n=jq\ (r)} \alpha * \beta(n) - \frac{1}{\varphi(r)} \sum_{n:(n,r)=1} \alpha * \beta(n) \Big| \ll x \log^{-A'} x$$

for any fixed $A' > 0$. We conclude that

$$X = \sum_r \frac{\alpha(r)}{\varphi(r)} \sum_{n:(n,r)=1} \alpha * \beta(n) + o(x \log^{-22A-22} x).$$

If $\alpha(r)$ is nonzero, then r is the product of $O(1)$ primes between q^ε and x^δ, and so $1/\varphi(r) = 1/r + O(q^{-\varepsilon}/r)$; the contribution of the error $O(q^{-\varepsilon}/r)$ is then $o(x \log^{-22A-22} x)$ by (4-7). Also, from standard divisor bound bounds, one has

$$\sum_{n:p|n} \alpha * \beta(n) \ll \frac{x}{p}$$

for any prime p between q^ε and x^δ, and so

$$\sum_{n:(n,r)\neq 1} \alpha * \beta(n) \ll q^{-\varepsilon} x.$$

We conclude that

$$X = \sum_r \frac{\alpha(r)}{r} \sum_n \alpha * \beta(n) + o(x \log^{-22A-22} x),$$

and hence, by (4-5), (4-6), (4-7), and the estimate $1/r = 1/M + O((\log^{-10A-10} x)/M)$ on the support of α, one has

$$X = \gamma^2 \frac{x}{2} + o(x \log^{-22A-22} x),$$

which contradicts (4-13) for x large enough. This concludes the proof of Theorem 1.6.

Remark 4.1. If we have $n(q) > x^\delta$, then the sequence α in the above argument is simply $\alpha = 1_{\mathcal{D}}$. Thus, for the purposes of establishing Vinogradov's conjecture, it suffices to consider Type II sums when α is a sequence of the form $1_{\mathcal{D}}$; there is also considerable flexibility in how to choose the set $\mathcal{D}$, and other choices than the one given here are available. For similar reasons, one can relax (1-7) by moving the absolute values outside of the r summation. This leads to some further numerical improvements in the $\frac{1}{68}$ exponent in [Polymath 2014a] for the purposes of the applications to Vinogradov's conjecture; see Section 5 below.

5. A variant of the method

In this section, we sketch how to modify the arguments in Section 4 to be able to utilize distributional estimates for (components of) the divisor functions τ_k.

We start with a setup similar to that in Section 4; namely, (4-1) holds for some N (and some character χ of conductor q going off to infinity) and some fixed $A \geq 1$. We set $x := q^{1+2\varepsilon}$ for some small fixed $\varepsilon > 0$. Let $k \geq 2$ be a fixed natural number, and suppose first that $N \leq x^{1/k}$. Then the quantity $M := \lfloor x/N^k \rfloor$ is at least 1. If we set $\alpha(m) := \overline{\chi(m)} 1_{[(1-\log^{10A} x)M, M]}(m)$ and $\beta(n) := 1_{[N/2,N]}(n)$, a brief calculation similar to that in the previous section reveals that

$$\left| \sum_{j \leq q^\varepsilon} \sum_{n \leq x} \chi(n) \alpha * \beta^{*k}(n + jq) \right| \gg x q^\varepsilon \log^{-(10+k)A} x,$$

where β^{*k} denotes the Dirichlet convolution of k copies of β; one should think of β^{*k} here as a component of the divisor function $\tau_k = 1^{*k}$ defined on (1-10). We then approximate $\alpha * \beta^{*k}$ by $\gamma \psi(n/x)$, where

$$\psi(t) := \int_{t_1 \cdots t_k = t} 1_{[1/2,1]}(t_1) \cdots 1_{[1/2,1]}(t_k) \frac{dt_1 \cdots dt_{k-1}}{t_1 \cdots t_k}$$

is the multiplicative convolution of k copies of $1_{[1/2,1]}$ and

$$\gamma := \frac{1}{M(N/2)^k} \sum_n \alpha * \beta^{*k}(n).$$

A repetition of the arguments of the previous section (with $\alpha * \beta^{*(k-1)}$ playing the role of α) then shows that there is $1 \leq j \leq q^\varepsilon$ for which one has

$$\left| X - \gamma^2 x \int_{\mathbb{R}} \psi^2(t)\, dt \right| \gg x \log^{-(20+2k)A} x,$$

where

$$X := \sum_n \alpha * \beta^{*k}(n) \alpha * \beta^{*k}(n - jq).$$

However, a somewhat tedious calculation (similar to that in the preceding section) shows that, if one has an Elliott–Halberstam-type distributional estimate for β^{*k} on residue classes to moduli up to $MN^{k-1} \asymp q^{1+2\varepsilon}/N$, one can obtain an asymptotic of the form

$$X = \gamma^2 x \int_{\mathbb{R}} \psi^2(t)\, dt + o(x \log^{-(20+2k)A} x)$$

giving the desired contradiction. If τ_k has a level of distribution θ for some $0 < \theta < 1$, this suggests we can establish cancellation in sums such as $\sum_{n \leq N} \chi(n)$ whenever $N \leq q^{1/k}$ and $q^{1+2\varepsilon}/N \leq (N^k)^{\theta-\varepsilon}$, which suggests that N can be as low as $q^{1/(1+k\theta)+\varepsilon}$ if $\theta > 1 - 1/k$. For instance, using the well-known level of

distribution $\theta = \frac{2}{3}$ for the divisor function τ_2 or for the variant $\beta * \beta$ (an old observation of Linnik and Selberg, arising from the Weil bound on Kloosterman sums), this argument gives (1-8) with $\varpi = \frac{1}{28}$ (in fact, one can replace $\log^{-A} q$ by a power savings because the Linnik–Selberg argument provides such a savings in the equidistribution estimate). Using only the elementary bound of Kloosterman [1927], one gets a level of distribution $\theta = \frac{4}{7}$, corresponding to the value $\varpi = \frac{1}{60}$, thus giving a slight improvement over the Pólya–Vinogradov bound (or even the currently best known consequence of Theorem 1.6) that requires no knowledge of the Weil conjectures.

If instead $N < q^{1/k}$, one can repeat the above analysis with the convolution $\alpha * \beta^{*k}$ replaced by $\beta_1 * \cdots * \beta_k$, where $\beta_i = 1_{[N_i/2, N_i]}$ and $N_1, \dots, N_k \geq 1$ are quantities with $N = N_1 \geq N_2, \dots, N_k$ and $N_1 \cdots N_k = x$. If (4-1) holds for all $N_1, \dots, N_k$, then the above analysis again leads to a contradiction if $q^{1+2\varepsilon}/N \leq x^{\theta-\varepsilon}$, which suggests that N can be as low as $q^{1-\theta+\varepsilon}$ if $\theta \leq 1 - 1/k$. By a numerical coincidence, the best known distribution results (at $\theta = \frac{4}{7}$) on τ_3, due to Fouvry, Kowalski, and Michel, correspond to the same value of ϖ, namely $\frac{1}{28}$, as the Linnik–Selberg distribution result discussed above.

In the endpoint case $N = x^{1/k}$, α becomes trivial and the quantity X discussed above is analogous to the sum

$$\sum_{n \leq x} \tau_k(n) \tau_k(n + jq),$$

with jq being slightly smaller than x. Thus, if one were able to obtain good asymptotics for such sums (with error terms that were smaller than the main term by an arbitrary power of the logarithm), one would expect to be able to obtain bounds such as (1-8) with $q^{1/2-2\varpi+\varepsilon}$ replaced by a quantity slightly smaller than $q^{1/k}$. Unfortunately, asymptotics for such sums are currently only known for $k = 2$.

Acknowledgments

The author was supported by a Simons Investigator grant, the James and Carol Collins Chair, the Mathematical Analysis and Application Research Fund Endowment, and NSF grant DMS-1266164. He also thanks John Friedlander, Andrew Granville, James Maynard, Lillian Pierce, and Felipe Voloch for several useful discussions and the anonymous referee for many valuable comments and suggestions.

References

[Ankeny 1952] N. C. Ankeny, "The least quadratic non residue", *Ann. of Math.* (2) **55** (1952), 65–72. MR 13,538c Zbl 0046.04006

[Banks and Makarov 2014] W. D. Banks and K. A. Makarov, "Convolutions with probability distributions, zeros of L-functions, and the least quadratic nonresidue", preprint, 2014. arXiv 1411.2009v1

[Bateman and Diamond 2004] P. T. Bateman and H. G. Diamond, *Analytic number theory: an introductory course*, Monographs in Number Theory **1**, World Scientific, Hackensack, NJ, 2004. MR 2005h:11208 Zbl 1074.11001

[Bombieri 1965] E. Bombieri, "On the large sieve", *Mathematika* **12** (1965), 201–225. MR 33 #5590 Zbl 0136.33004

[Bombieri et al. 1986] E. Bombieri, J. B. Friedlander, and H. Iwaniec, "Primes in arithmetic progressions to large moduli", *Acta Math.* **156**:3–4 (1986), 203–251. MR 88b:11058 Zbl 0588.10042

[Bombieri et al. 1987] E. Bombieri, J. B. Friedlander, and H. Iwaniec, "Primes in arithmetic progressions to large moduli, II", *Math. Ann.* **277**:3 (1987), 361–393. MR 88f:11085 Zbl 0625.10036

[Bombieri et al. 1989] E. Bombieri, J. B. Friedlander, and H. Iwaniec, "Primes in arithmetic progressions to large moduli, III", *J. Amer. Math. Soc.* **2**:2 (1989), 215–224. MR 89m:11087 Zbl 0674.10036

[Burgess 1957] D. A. Burgess, "The distribution of quadratic residues and non-residues", *Mathematika* **4** (1957), 106–112. MR 20 #28 Zbl 0081.27101

[Burgess 1963] D. A. Burgess, "On character sums and L-series, II", *Proc. London Math. Soc.* (3) **13** (1963), 524–536. MR 26 #6133 Zbl 0123.04404

[Burgess 1986] D. A. Burgess, "The character sum estimate with $r = 3$", *J. London Math. Soc.* (2) **33**:2 (1986), 219–226. MR 87g:11098 Zbl 0593.10033

[Diamond et al. 2006] H. G. Diamond, H. L. Montgomery, and U. M. A. Vorhauer, "Beurling primes with large oscillation", *Math. Ann.* **334**:1 (2006), 1–36. MR 2006j:11131 Zbl 1207.11105

[Elliott and Halberstam 1970] P. D. T. A. Elliott and H. Halberstam, "A conjecture in prime number theory", pp. 59–72 in *Symposia mathematica IV* (Istituto Nazionale di Alta Matematica, Rome, 1968–1969), Academic Press, London, 1970. MR 43 #1943 Zbl 0238.10030

[Eskin et al. 2005] A. Eskin, S. Mozes, and H. Oh, "On uniform exponential growth for linear groups", *Invent. Math.* **160**:1 (2005), 1–30. MR 2006a:20081 Zbl 1137.20024

[Fouvry 1984] É. Fouvry, "Autour du théorème de Bombieri–Vinogradov", *Acta Math.* **152**:3–4 (1984), 219–244. MR 85m:11052 Zbl 0552.10024

[Fouvry 1985] É. Fouvry, "Sur le problème des diviseurs de Titchmarsh", *J. Reine Angew. Math.* **357** (1985), 51–76. MR 87b:11090 Zbl 0547.10039

[Fouvry and Iwaniec 1980] E. Fouvry and H. Iwaniec, "On a theorem of Bombieri–Vinogradov type", *Mathematika* **27**:2 (1980), 135–152. MR 82h:10057 Zbl 0469.10027

[Fouvry and Iwaniec 1983] E. Fouvry and H. Iwaniec, "Primes in arithmetic progressions", *Acta Arith.* **42**:2 (1983), 197–218. MR 84k:10035 Zbl 0517.10045

[Fouvry and Iwaniec 1992] É. Fouvry and H. Iwaniec, "The divisor function over arithmetic progressions", *Acta Arith.* **61**:3 (1992), 271–287. MR 93g:11089 Zbl 0764.11040

[Fouvry et al. 2014] E. Fouvry, E. Kowalski, and P. Michel, "On the exponent of distribution of the ternary divisor function", preprint, 2014. arXiv 1304.3199v2

[Friedlander and Iwaniec 2010] J. Friedlander and H. Iwaniec, *Opera de cribro*, Colloquium Publications **57**, American Mathematical Society, Providence, RI, 2010. MR 2011d:11227 Zbl 1226.11099

[Gallagher 1968] P. X. Gallagher, "Bombieri's mean value theorem", *Mathematika* **15** (1968), 1–6. MR 38 #5724 Zbl 0174.08103

[Gallagher 1970] P. X. Gallagher, "A large sieve density estimate near $\sigma = 1$", *Invent. Math.* **11** (1970), 329–339. MR 43 #4775 Zbl 0219.10048

[Goldmakher 2010] L. Goldmakher, "Character sums to smooth moduli are small", *Canad. J. Math.* **62**:5 (2010), 1099–1115. MR 2011k:11108 Zbl 1273.11125

[Graham and Ringrose 1990] S. W. Graham and C. J. Ringrose, "Lower bounds for least quadratic non-residues", pp. 269–309 in *Analytic number theory* (Allerton Park, IL, 1989), edited by B. C. Berndt et al., Progr. Math. **85**, Birkhäuser, Boston, 1990. MR 92d:11108 Zbl 0719.11006

[Granville and Soundararajan 2001] A. Granville and K. Soundararajan, "The spectrum of multiplicative functions", *Ann. of Math.* (2) **153**:2 (2001), 407–470. MR 2002g:11127 Zbl 1036.11042

[Granville and Soundararajan 2007] A. Granville and K. Soundararajan, "An uncertainty principle for arithmetic sequences", *Ann. of Math.* (2) **165**:2 (2007), 593–635. MR 2008g:11165 Zbl 1139.11040

[Granville and Soundararajan 2015] A. Granville and K. Soundararajan, "Large character sums: Burgess's theorem and zeros of L-functions", preprint, 2015. arXiv 1501.01804v1

[Iwaniec and Kowalski 2004] H. Iwaniec and E. Kowalski, *Analytic number theory*, Colloquium Publications **53**, American Mathematical Society, Providence, RI, 2004. MR 2005h:11005 Zbl 1059.11001

[Kloosterman 1927] H. D. Kloosterman, "On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$", *Acta Math.* **49**:3–4 (1927), 407–464. MR 1555249 Zbl 53.0155.01

[Linnik 1942] U. V. Linnik, "A remark on the least quadratic non-residue", *C. R.* (*Doklady*) *Acad. Sci. URSS* (*N.S.*) **36** (1942), 119–120. MR 4,189a Zbl 0063.03570

[Montgomery and Vaughan 2007] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory, I: Classical theory*, Cambridge Studies in Advanced Mathematics **97**, Cambridge University, 2007. MR 2009b:11001 Zbl 1142.11001

[Motohashi 1976] Y. Motohashi, "An induction principle for the generalization of Bombieri's prime number theorem", *Proc. Japan Acad.* **52**:6 (1976), 273–275. MR 54 #10171 Zbl 0355.10035

[Polymath 2014a] D. H. J. Polymath, "New equidistribution estimates of Zhang type", *Algebra Number Theory* **8**:9 (2014), 2067–2199. MR 3294387 Zbl 06387014

[Polymath 2014b] D. H. J. Polymath, "Variants of the Selberg sieve, and bounded intervals containing many primes", *Res. Math. Sci.* **1**:12 (2014).

[Postnikov 1956] 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. MR 18,793a Zbl 0072.27304

[Rodosskiĭ 1956] K. A. Rodosskiĭ, "On non-residues and zeros of L-functions", *Izv. Akad. Nauk SSSR. Ser. Mat.* **20** (1956), 303–306. In Russian. MR 18,564b Zbl 0071.04501

[Vinogradov 1965] A. I. Vinogradov, "The density hypothesis for Dirichet L-series", *Izv. Akad. Nauk SSSR Ser. Mat.* **29** (1965), 903–934. In Russian. MR 33 #5579 Zbl 0128.04205

[Vinogradov 1985] I. M. Vinogradov, *Selected works*, edited by L. D. Faddeev et al., Springer, Berlin, 1985. MR 87a:01042 Zbl 0577.01049

[Wirsing 1967] E. Wirsing, "Das asymptotische Verhalten von Summen über multiplikative Funktionen, II", *Acta Math. Acad. Sci. Hungar.* **18** (1967), 411–467. MR 36 #6366 Zbl 0165.05901

[Zhang 2014] Y. Zhang, "Bounded gaps between primes", *Ann. of Math.* (2) **179**:3 (2014), 1121–1174. MR 3171761 Zbl 1290.11128

Communicated by Andrew Granville
Received 2014-10-26 Revised 2015-01-12 Accepted 2015-03-18

tao@math.ucla.edu *Department of Mathematics, University of California, Los Angeles, 405 Hilgard Avenue, Los Angeles, CA 90095-1555, United States*

Algebra & Number Theory

msp.org/ant

EDITORS

MANAGING EDITOR

Bjorn Poonen
Massachusetts Institute of Technology
Cambridge, USA

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Georgia Benkart	University of Wisconsin, Madison, USA	Susan Montgomery	University of Southern California, USA
Dave Benson	University of Aberdeen, Scotland	Shigefumi Mori	RIMS, Kyoto University, Japan
Richard E. Borcherds	University of California, Berkeley, USA	Raman Parimala	Emory University, USA
John H. Coates	University of Cambridge, UK	Jonathan Pila	University of Oxford, UK
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Anand Pillay	University of Notre Dame, USA
Brian D. Conrad	Stanford University, USA	Victor Reiner	University of Minnesota, USA
Hélène Esnault	Freie Universität Berlin, Germany	Peter Sarnak	Princeton University, USA
Hubert Flenner	Ruhr-Universität, Germany	Joseph H. Silverman	Brown University, USA
Edward Frenkel	University of California, Berkeley, USA	Michael Singer	North Carolina State University, USA
Andrew Granville	Université de Montréal, Canada	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Joseph Gubeladze	San Francisco State University, USA	J. Toby Stafford	University of Michigan, USA
Roger Heath-Brown	Oxford University, UK	Ravi Vakil	Stanford University, USA
Craig Huneke	University of Virginia, USA	Michel van den Bergh	Hasselt University, Belgium
Kiran S. Kedlaya	Univ. of California, San Diego, USA	Marie-France Vignéras	Université Paris VII, France
János Kollár	Princeton University, USA	Kei-Ichi Watanabe	Nihon University, Japan
Yuri Manin	Northwestern University, USA	Efim Zelmanov	University of California, San Diego, USA
Barry Mazur	Harvard University, USA	Shou-Wu Zhang	Princeton University, USA
Philippe Michel	École Polytechnique Fédérale de Lausanne		

PRODUCTION

production@msp.org

Silvio Levy, Scientific Editor

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2015 is US $255/year for the electronic version, and $440/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

© 2015 Mathematical Sciences Publishers

Algebra & Number Theory

Volume 9 No. 4 2015