A VARIANT OF THE BOMBIERI-VINOGRADOV THEOREM IN SHORT INTERVALS WITH APPLICATIONS

JESSE THORNER

Abstract. We generalize the classical Bombieri-Vinogradov theorem to a short interval, non-abelian setting. This leads to variants of the prime number theorem for short intervals where the primes lie in arithmetic progressions that are "twisted" by a splitting condition in a Galois extension $L/K$ of number fields. Using this result in conjunction with recent work of Maynard, we prove that rational primes in short intervals with a given splitting condition in a Galois extension $L/\mathbb{Q}$ exhibit dense clusters in short intervals. We explore several arithmetic applications related to questions of Serre regarding the nonvanishing Fourier coefficients of cuspidal modular forms, including finding dense clusters of fundamental discriminants $d$ in short intervals for which the central values of $d$-quadratic twists of modular $L$-functions are non-vanishing.

1. Introduction and Statement of Results

Let $\mathbb{N}$ denote the set of positive integers, and let $a, q \in \mathbb{N}$ satisfy $(a, q) = 1$. Define

$$\psi(x; q, a) = \sum_{n \leq x \atop n \equiv a \mod{q}} \Lambda(n),$$

where $\Lambda(n)$ is the von Mangoldt function. The prime number theorem for arithmetic progressions states that if $q \leq (\log x)^D$ for any constant $D > 0$, then

$$(1.1) \quad \psi(2x; q, a) - \psi(x; q, a) \sim \frac{x}{\varphi(q)}.$$

where $\varphi$ denotes Euler’s totient function. Understanding both the error term and the range of $q$ for (1.1) is important for a wide variety of arithmetic problems. The generalized Riemann hypothesis (GRH) for Dirichlet $L$-functions implies that if $q \leq x^{1/2-\epsilon}$ for any $\epsilon > 0$, then

$$(1.2) \quad \psi(2x; q, a) - \psi(x; q, a) - \frac{x}{\varphi(q)} \ll \sqrt{x} (\log qx)^2.$$ 

While this is beyond the reach of current methods, it is known that the mean value of (1.2) is about as small as predicted by GRH when we average over moduli $q$. Specifically, for constants $0 < \theta < \frac{1}{2}$ and $D > 0$, Bombieri and Vinogradov proved [11] Theorem 15.1 that

$$(1.3) \quad \sum_{q \leq x^\theta} \max_{(a, q) = 1} \max_{N \leq x} \left| \psi(2N; q, a) - \psi(N; q, a) - \frac{N}{\varphi(q)} \right| \ll \frac{x}{(\log x)^D}.$$ 

We call $\theta$ the level of distribution of the primes.

A more difficult problem asks for the distribution of primes in arithmetic progressions when the interval $[x, 2x]$ is replaced with $[x, x + h]$, where $h \geq x^{1-\delta}$ for some $\delta > 0$. Using
deep analytic properties of Dirichlet $L$-functions, one can produce a short interval analogue of the Bombieri-Vinogradov estimate (1.3) of the form

\[(1.4) \sum_{q \leq x} \max_{(a,q)=1} \max_{y \leq h} \max_{\frac{1}{2}x \leq N \leq x} \left| \psi(N + y; q, a) - \psi(N; q, a) - \frac{y}{\varphi(q)} \right| \ll \frac{h}{(\log x)^{1+\delta}},\]

where $\delta > 0$ and $\theta > 0$ are certain constants, $D > 0$ is fixed, and $h \geq x^{1-\delta}$. The density hypothesis for Dirichlet $L$-functions, which follows from GRH, predicts that (1.4) holds when $0 \leq \delta < \frac{1}{2}$ and $0 \leq \theta < \frac{1}{2} - \delta$ [11, Chapter 12]. There has been much progress toward this conjectured estimate; see [18] and the sources contained therein. Currently, the sharpest version of (1.4) is due to Timofeev [23], who proved that (1.4) holds when

\[0 \leq \delta < \frac{5}{12}, \quad \frac{1}{2} - \delta \quad \text{if } 0 \leq \delta < \frac{2}{5}, \quad \frac{9}{20} - \delta \quad \text{if } \frac{2}{5} \leq \delta < \frac{5}{12}.\]

Most of these results have been extended to a broader context. Let $L/K$ be a Galois extension of number fields with Galois group $G$, let $a, q \in \mathbb{N}$ with $(a,q) = 1$, and let $N = N_{K/\mathbb{Q}}$ denote the absolute field norm of $K$. For a prime ideal $p$ of $K$ which is unramified in $L$, there corresponds a certain conjugacy class $C \subset G$ consisting of the set of Frobenius automorphisms attached to the prime ideals of $L$ which lie over $p$. We denote this conjugacy class by the Artin symbol $[L/K]_p$.

For a fixed conjugacy class $C$ and an integral ideal $a$ of $K$, define

\[\Lambda_C(a) := \begin{cases} \log Np & \text{if } a = p^m \text{ with } m \geq 1, p \text{ unramified in } L, \text{ and } \left[\frac{L/K}{p}\right]^m = C, \\ 0 & \text{otherwise} \end{cases}\]

and

\[(1.5) \psi_C(x; q, a) = \psi_C(x, L/K; q, a) := \sum_{\substack{N \leq x \\mod q}} \Lambda_C(a).\]

The Chebotarev density theorem asserts that if $q \leq (\log x)^D$, then

\[(1.6) \psi_C(2x; q, a) - \psi_C(x; q, a) \sim d(C; q, a)x\]

for some density $d(C; q, a) \geq 0$. If $\zeta_q = e^{2\pi i/q}$ and $L \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$, then

\[d(C; q, a) = \left| \frac{C}{|G|} \right| \frac{\varphi(q)}{\varphi(q)}\]

Building on the work of M. R. Murty and V. K. Murty [12], M. R. Murty and Petersen [13] proved that if $H \subset G$ is a largest abelian subgroup of $G$ such that $H \cap C$ is nonempty, $E$ is the fixed field of $H$, and $0 \leq \theta < 1/\max\{[E : \mathbb{Q}] - 2, 2\}$ is fixed, then

\[(1.7) \sum_{q \leq x} \max_{(a,q)=1} \max_{1 \leq N \leq x} \left| \psi_C(2N; q, a) - \psi_C(N; q, a) - \frac{|C| N}{|G| \varphi(q)} \right| \ll \frac{x}{(\log x)^D},\]

where $\sum'$ denotes summing over moduli $q$ satisfying $L \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$. This extends (1.3) to a nonabelian setting; in fact, (1.3) is recovered when $E = \mathbb{Q}$.

2
In the case of \( q = 1 \), Balog and Ono \cite{1} extended (1.6) to a short interval setting using Heath-Brown’s zero density estimate for Dedekind zeta functions \cite{5}. Balog and Ono proved that if

\[
0 < \delta < \begin{cases} 
1/[L : \mathbb{Q}] & \text{if } [L : \mathbb{Q}] \geq 3, \\
3/8 & \text{if } [L : \mathbb{Q}] = 2, \\
5/12 & \text{if } [L : \mathbb{Q}] = 1 
\end{cases}
\]

and \( h \geq x^{1-\delta} \), then

\[
\psi_C(x + h; 1, 1) - \psi_C(x; 1, 1) \sim |C| |\mathcal{G}| h.
\]

Our main result is a short interval variant of (1.7).

**Theorem 1.1.** Let \( L/K \) be a Galois extension of number fields with Galois group \( G \), and let \( C \subset G \) be a fixed conjugacy class. Let \( H \subset G \) be a largest abelian subgroup of \( G \) such that \( H \cap C \) is nonempty, and let \( E \) be the fixed field of \( H \). Let \( 0 \leq \delta < \frac{2}{5[E:Q]} \) and \( 0 \leq \theta < \frac{1}{3}(\frac{2}{5[E:Q]} - \delta) \). If \( h \geq x^{1-\delta} \), then for any fixed \( D > 0 \),

\[
\sum'_{q \leq x^D} \max_{(a,q) = 1} \max_{\frac{1}{2}x \leq N \leq x} \left| \psi_C(N + y; q, a) - \psi_C(N; q, a) - \frac{|C|}{|G| \varphi(q)} y \right| \ll \frac{h}{(\log x)^D},
\]

where \( \sum' \) denotes summing over moduli \( q \) satisfying \( L \cap \mathbb{Q}(\zeta_q) = \mathbb{Q} \).

When \( |H| = [L : E] \geq 3 \), Theorem 1.1 immediately yields an improvement to the range of \( \delta \) in (1.8) for Balog and Ono’s short interval variant of the Chebotarev density theorem.

**Corollary 1.2.** Let \( L/K \) be a Galois extension of number fields with Galois group \( G \), and let \( C \subset G \) be a fixed conjugacy class. Let \( H \subset G \) be a largest abelian subgroup of \( G \) such that \( H \cap C \) is nonempty, and let \( E \) be the fixed field of \( H \), and suppose that \( |H| \geq 3 \). Suppose that \( q \leq (\log x)^D \) satisfies \( L \cap \mathbb{Q}(\zeta_q) = \mathbb{Q} \) and \( (a,q) = 1 \). If \( 0 \leq \delta < \frac{2}{5[E:Q]} \) and \( h \geq x^{1-\delta} \), then

\[
\psi_C(x + h; q, a) - \psi_C(x; q, a) \sim \frac{|C|}{|G| \varphi(q)} h.
\]

Much like the results of \cite{12,13}, nonabelian analogues of the Bombieri-Vinogradov theorem in short intervals can have interesting arithmetic consequences. In this paper, we will focus on consequences related to recent advances toward the Hardy-Littlewood prime \( k \)-tuples conjecture. For these applications, we consider a Galois extension \( L/\mathbb{Q} \) with Galois group \( G \) and absolute discriminant \( d_L \), and we consider a fixed conjugacy class \( C \subset G \). In this setting, (1.5) counts primes in Chebotarev sets of the form

\[
P = \left\{ p : p \mid d_L, \left[ \frac{L/\mathbb{Q}}{p} \right] = C \right\}
\]

We establish some additional notation. Let \( \mathbb{P} \) denote the set of all primes, and let \( h_i \) denote a nonnegative integer. We call a collection of nonnegative integers \( \mathcal{H}_k = \{ h_1, \ldots, h_k \} \) admissible if \( \prod_{i=1}^k (n + h_i) \) has no fixed prime divisor. (We could consider more general admissible sets, but this sometimes hinders the applications we consider.)
Conjecture (Hardy-Littlewood). If $\mathcal{H}_k$ is admissible, then as $x \to \infty$, we have

$$
\# \{ n \in [x, 2x] : \#(\{ n + h_1, \ldots, n + h_k \} \cap \mathbb{P}) = k \} \sim \mathbb{S} \frac{x}{(\log x)^k},
$$

where $\mathbb{S}$ is a certain positive constant depending on $\mathcal{H}_k$.

Choosing $\mathcal{H}_2 = \{0, 2\}$, the Hardy-Littlewood conjecture implies the elusive twin prime conjecture, that there are infinitely many pairs of primes whose difference is 2.

In [10], Maynard developed a significant improvement to the Selberg sieve. Using this improvement and (1.3), Maynard proved that if $\mathcal{H}_k$ is admissible, then there are infinitely many integers $N \geq 1$ such that for some $n \in [N, 2N]$, we have

$$
\#(\{ n + h_1, \ldots, n + h_k \} \cap \mathbb{P}) \geq (1/4 + o_{k \to \infty}(1)) \log k,
$$

(Tao independently derived the same sieve improvement, but arrived at slightly different conclusions.) Using Maynard’s improvement to the Selberg sieve and (1.7), the author [22] proved that if $\mathcal{H}_k$ is admissible, then there are infinitely many integers $N \geq 1$ such that for some $n \in [N, 2N]$, we have

$$
(1.11) \quad \#(\{ n + h_1, \ldots, n + h_k \} \cap \mathcal{P}) \geq \left( \frac{1}{2 \max\{[E : Q] - 2, 2\}} \frac{|C| \varphi(d_L)}{d_L} + o_{k \to \infty}(1) \right) \log k,
$$

where $\mathcal{P}$ is a Chebotarev set given by (1.10). (In [22], $1/\max\{[E : Q] - 2, 2\}$ was replaced by $\min\{1/2, 2/|G|\}$, which is a sharp lower bound.) The author explored applications of (1.11) to ranks of quadratic twists of elliptic curves, congruence conditions on the Fourier coefficients of newforms, and representations of primes by binary quadratic forms.

In [9], Maynard generalized his methods to prove weak forms of the Hardy-Littlewood conjecture with specializations to primes in short intervals and primes in Chebotarev sets. More specifically, given $0 \leq \delta < \frac{5}{12}$ and $h \geq x^{1-\delta}$, Maynard proved that there exists an absolute constant $C > 0$ such that if $k \geq C$ and $\mathcal{H}_k$ is an admissible set, then

$$
(1.12) \quad \# \{ n \in [x, x+h] : \#(\{ n + h_1, \ldots, n + h_k \} \cap \mathcal{P}) \geq C^{-1} \log k \} \gg \frac{h}{(\log x)^k}
$$

Furthermore, if $\mathcal{P}$ is given by (1.10), then Maynard also proved that there exists a constant $C_L > 0$ such that if $k \geq C_L$ and $\mathcal{H}_k$ is admissible, then

$$
(1.13) \quad \# \{ n \in [x, 2x] : \#(\{ n + h_1, \ldots, n + h_k \} \cap \mathcal{P}) \geq C_L^{-1} \log k \} \gg \frac{x}{(\log x)^k}.
$$

(The subscript $L$ in $C_L$ denotes that the constant $C$ depends on at most $L$, and the dependence is effectively computable. We will use this convention henceforth.)

Using Theorem [1.1] we prove the following mutual refinement of (1.12) and (1.13), which extends the author’s applications in [22] to a short interval setting.

**Theorem 1.3.** Let $L/Q$ be a Galois extension of number fields, let $\mathcal{P}$ be as in (1.10), and choose $h$ as in Theorem [1.1]. There exists a constant $C_L \in \mathbb{N}$ such that if $k \geq C_L$ and $\mathcal{H}_k$ is admissible, then

$$
\# \{ n \in [x, x+h] : \#(\{ n + h_1, \ldots, n + h_k \} \cap \mathcal{P}) \geq C_L^{-1} \log k \} \gg \frac{h}{(\log x)^k}.
$$
Remark. Some of the parameters in the statement of Theorem 1.3 can have some uniformity in \( x \) by appealing to the arguments in \( [9] \). In what follows, we will assume that all parameters are constant with respect to \( x \).

We now consider arithmetic consequences of Theorem 1.3 in the theory of elliptic curves, modular forms, and modular \( L \)-functions; for an introduction to the relevant definitions and ideas, we refer the reader to [16]. We consider the following question of Serre [19], which may be seen as an automorphic analogue of Bertrand’s postulate on the existence of primes in every dyadic interval \([x, 2x]\).

**Serre’s Question.** Let \( q = e^{2\pi i z} \), and let \( S_\ell(\Gamma_0(N), \chi) \) be the space of weight \( \ell \), level \( N \) cusp forms. For a nonzero cusp form \( f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_\ell(\Gamma_0(N), \chi) \), let

\[
I_f(n) = \max\{i : a_f(n+j) = 0 \text{ for all } 0 \leq j \leq i\}.
\]

(1) Suppose that \( f \) is of weight \( \ell \geq 2 \), and is not a linear combination of forms with complex multiplication. Is \( I_f(n) \ll n^\delta \) for some \( 0 \leq \delta < 1 \)?

(2) More generally, are there analogous results for forms with non-integral weights, or forms with respect to other Fuchsian groups?

Motivated by the second part of Serre’s question, Balog and Ono [1] used (1.9) to prove that if \( f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_\ell(\Gamma_0(N), \chi) \) is a cusp form of weight \( \ell \in \frac{1}{2} \mathbb{N} - \{\frac{1}{2}\} \) which is not a linear combination of weight \( \frac{3}{2} \) theta functions, then there exists \( \nu_f \in \mathbb{N} \) such that if \( 0 \leq \delta < \frac{1}{\nu_f} \) and \( h \geq x^{1-\delta} \), then

\[(1.14) \quad \#\{n \in [x, x+h] : a_f(n) \neq 0\} \gg \frac{h}{\log x}.
\]

For such a cusp form \( f \), it follows that \( I_f(n) \ll n^{1-\frac{1}{\nu_f}+\epsilon} \) for any \( \epsilon > 0 \), affirmatively answering Serre’s question. By using Theorem 1.3 instead of (1.9) in Balog and Ono’s proof, we immediately obtain dense clusters of integers \( n \) in short intervals for which \( a_f(n) \neq 0 \). Specifically, we have the following.

**Theorem 1.4.** Let \( f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_\ell(\Gamma_0(N), \chi) \) be a nonzero cusp form of weight \( \ell \in \frac{1}{2} \mathbb{N} - \{\frac{1}{2}\} \) which is not a linear combination of weight \( \frac{3}{2} \) theta functions. There exist constants \( C_f, \nu_f, k \in \mathbb{N} \) such that if \( 0 \leq \delta < \frac{1}{\nu_f} \), \( h \geq x^{1-\delta} \), \( k \geq C_f^2 \) and \( H_k \) is admissible, then

\[
\#\{n \in [x, x+h] : \#\{h_i \in H_k : a_f(n+h_i) \neq 0\} \geq C_f^{-1} \log k\} \gg \frac{h}{(\log x)^k}.
\]

We address two corollaries of Theorem 1.4 regarding central values of modular \( L \)-functions and ranks of elliptic curves. Let \( \mathcal{D} \) be the set of all fundamental discriminants, and let \( f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_\ell(\Gamma_0(N)) \) be a newform (i.e., a holomorphic cuspidal normalized Hecke eigenform) of weight \( \ell \in 2\mathbb{N} \). Given \( d \in \mathcal{D} \), let \( L(s, f_d) \) denote the \( L \)-function given by

\[
L(s, f_d) = \sum_{n=1}^{\infty} \frac{a_f(n)\chi_d(n)}{n^{s+(\ell-1)/2}},
\]

where \( \chi_d \) is the Kronecker character for \( \mathbb{Q}(\sqrt{d}) \). Goldfeld [4] conjectured that the density of \( d \in \mathcal{D} \) for which \( L(1/2, f_d) \neq 0 \) is 1/2.
By the work of Shimura [20] and Waldspurger [24], Fourier coefficients of half-integer weight cusp forms \( g \) that satisfy the hypotheses of Theorem 1.4 interpolate central values of quadratic twists of modular \( L \)-functions associated to the Shimura correspondent of \( g \). Despite the fact that the Shimura correspondence is not surjective, Ono and Skinner [17] proved that such central values can be obtained in this fashion for the \( L \)-function of an even-integer weight newform with trivial nebentypus. Using this observation along with (1.14), Balog and Ono [1] proved that there exists \( \nu_f \in \mathbb{N} \) such that if \( 0 \leq \delta < \frac{1}{\nu_f} \) and \( h \geq x^{1-\delta} \), then

\[
\#\{ |d| \in [x, x + h] : d \in \mathcal{D}, L(1/2, f_d) \neq 0 \} \gg \frac{h}{\log x}.
\]

This is the sharpest result in the direction of Goldfeld’s conjecture which is valid for all newforms \( f \); slight improvements exist for certain classes of newforms [15]. By using Theorem 1.4 instead of (1.14) in Balog and Ono’s proof, we immediately obtain dense clusters of fundamental discriminants \( d \) in short intervals for which \( L(1/2, f_d) \neq 0 \).

**Corollary 1.5.** Let \( f \in S_2(\Gamma_0(N)) \) be a newform with \( \ell \in \mathbb{N} \). There exist an arithmetic progression \( a \mod q \) (depending explicitly on \( f \)) and constants \( \nu_f, C_f \in \mathbb{N} \) such that if \( 0 \leq \delta < \frac{1}{\nu_f} \), \( h \geq x^{1-\delta}, k \geq C_f, \mathcal{H}_k \) is admissible, and

\[
N_f(k, n) = \{ h_i \in \mathcal{H}_k : n + qh_i \in \mathcal{D}, L(1/2, f_{n+qh_i}) \neq 0 \},
\]

then

\[
\#\{ |n| \in [x, x + h] : n \equiv a \pmod{q}, \#N_f(k, n) \geq C_f^{-1} \log k \} \gg \frac{h}{(\log x)^{k}}.
\]

**Remark.** We need to restrict to the arithmetic progression \( a \mod q \) for technical reasons; see [17] for details. We accomplish this by combining the arguments of Freiburg [3]. Proof of Theorem 1] with Maynard’s proofs in [9], which is straightforward to do.

Let \( f \) be the newform associated to an elliptic curve \( E/\mathbb{Q} \) of conductor \( N \). If \( (d, 4N) = 1 \), then \( L(s, f_d) \) is the \( L \)-function of the \( d \)-quadratic twist \( E_d/\mathbb{Q} \). By the work of Kolyvagin [8], if \( L(1/2, f_d) \neq 0 \), then the rank \( \text{rk}(E_d(\mathbb{Q})) \) of the Mordell-Weil group \( E_d(\mathbb{Q}) \) is zero. Thus Corollary 1.5 immediately implies the existence of dense clusters of fundamental discriminants \( d \) in short intervals such that \( \text{rk}(E_d) = 0 \).

**Corollary 1.6.** Let \( E/\mathbb{Q} \) be an elliptic curve. There exist an arithmetic progression \( a \mod q \) (depending explicitly on \( E \)) and constants \( \nu_E, C_E \in \mathbb{N} \) such that if \( 0 \leq \delta < \frac{1}{\nu_E}, h \geq x^{1-\delta}, k \geq C_E, \mathcal{H}_k \) is admissible, and

\[
N_E(k, n) = \{ h_i \in \mathcal{H}_k : n + qh_i \in \mathcal{D}, \text{rk}(E_{n+qh_i}(\mathbb{Q})) = 0 \},
\]

then

\[
\#\{ |n| \in [x, x + h] : n \equiv a \pmod{q}, \#N_E(k, n) \geq C_E^{-1} \log k \} \gg \frac{h}{(\log x)^{k}}.
\]

For our final application, consider an elliptic curve \( E/\mathbb{Q} \). In [14], the distribution of the quantity \( a_E(p) := p + 1 - \#E(\mathbb{F}_p) \) is studied. We apply our results to study the distribution of \( a_E(p) \pmod{m} \) in short intervals, where \( m \) is a given integer. It follows from the work of Shiu [21] that if \( E/\mathbb{Q} \) has a rational point of order \( m \), then for every \( j \in \mathbb{N} \) and every \( i \neq 1 \pmod{m} \), there exists an \( n \in \mathbb{N} \) such that

\[
a_E(p_n) \equiv a_E(p_{n+1}) \equiv a_E(p_{n+2}) \equiv \cdots \equiv a_E(p_{n+j}) \equiv i \pmod{m},
\]
where the primes are indexed in increasing order. Using \([1.9]\) and the definition of the action of Galois on the torsion points of \(E\), Balog and Ono \([1]\) proved that if \(m \in \mathbb{N}\) and \(i \mod m\) is a residue class for which there is a prime of good reduction \(p_0\) with \(a_E(p_0) \equiv i \pmod{m}\), then there exists \(\nu_{E,m} \in \mathbb{N}\) such that if \(0 \leq \delta < \frac{1}{\nu_{E,m}}\) and \(h \geq x^{1-\delta}\), then

\[
(1.16) \quad \#\{p \in [x, x + h] : a_E(p) \equiv i \pmod{m}\} \gg \frac{h}{\log x}.
\]

By using Theorem \([1.3]\) instead of \([1.9]\) in Balog and Ono’s proof, we immediately obtain dense clusters of primes \(p\) in short intervals for which \(a_E(p) \equiv i \pmod{m}\).

**Corollary 1.7.** Let \(E/\mathbb{Q}\) be an elliptic curve, let \(m \in \mathbb{N}\), and let \(i \mod m\) be a residue class for which there is a prime of good reduction \(p_0\) with \(a_E(p_0) \equiv i \pmod{m}\). There exist constants \(\nu_{E,m}, C_{E,m} \in \mathbb{N}\) such that if \(0 \leq \delta < \frac{1}{\nu_{E,m}}\), \(h \geq x^{1-\delta}\), \(k \geq C_{E,m}\), and \(H_k\) is admissible, then

\[
\#\{n \in [x, x + h] : \#\{h_j \in H_k : n + h_j \in \mathbb{P}, a_E(n + h_j) \equiv i \pmod{m}\} \geq C_{E,m}^{-1}\log k\} \gg \frac{h}{(\log x)^k}.
\]

We prove Theorem \([1.1]\) in Section \([2]\) and then we prove Theorem \([1.3]\) in Section \([3]\).

**Acknowledgments**

The author thanks James Maynard, Robert Lemke Oliver, Ken Ono, Jeremy Rouse, Kannan Soundararajan, and the anonymous referees for their comments and suggestions.

## 2. Proof of Theorem \([1.1]\)

For a number field \(F\), we let \(n_F = [F : \mathbb{Q}]\) and \(d_F\) equal the absolute discriminant of \(F\). Let \(L/K\) be a Galois extension of number fields with Galois group \(G\), and let \(C \subset G\) be a fixed conjugacy class. Unless otherwise specified, all implied constants in the asymptotic notation \(\ll\) or \(O(\cdot)\) will depend in an effectively computable way on at most \(d_L\).

Let \(H\) be a largest abelian subgroup of \(G\) such that \(H \cap C\) is nonempty, and let \(E\) be the fixed field of \(H\). If \(L \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}\), then \(L(\zeta_q)/E\) is an abelian extension with Galois group \(H_q \cong H \oplus (\mathbb{Z}/q\mathbb{Z})^\times\). Let \(\chi\) be a Dirichlet character modulo \(q\), and let \(\xi\) be a Hecke character in the dual group \(\hat{H}\). Since \(L \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}\), the characters \(\omega\) in the dual group \(\hat{H}_q\) are of the form \(\xi \otimes \chi\), and the conductor \(f_\omega\) of \(\omega\) satisfies \(Nf_\omega \ll q^{n_\mathbb{Z}}\), where \(N\) is the absolute field norm of \(E\) (cf. \([13\text{, Sections 0-1]}\)).

Let \(\mathcal{R}(T) = \{s = \sigma + it \in \mathbb{C} : \frac{1}{2} \leq \sigma < 1, |t| \leq T\}\). If \(T \leq \sqrt{x}\), then by \([1\text{, Equation 3.2]}\) and the functional equation for Hecke \(L\)-functions,

\[
\max_{y \leq h} \left| \psi_C(N + y; q, a) - \psi_C(N; q, a) - \frac{|C|}{|G|} \frac{y}{\varphi(q)} \right| \ll \frac{h}{\varphi(q)} \sum_{\omega \in \hat{H}_q} \sum_{\rho = \beta + i\gamma} x^{\beta - 1} + \frac{x(\log x)^2}{T},
\]
where $\rho$ is a nontrivial zero of $L(s, \omega)$ and $\hat{\omega}$ is the primitive character which induces $\omega$. Thus Theorem 1.1 will follow from proving that for any fixed $D > 0$, we have that

$$\sum_{q \leq Q} \varphi(q) \prod_{\rho_{\omega} = \beta_{\omega} + i\gamma_{\omega}} x^{\beta_{\omega} - 1} \leq Q x (\log x)^2 + \frac{Q x (\log x)^2}{T} \ll \frac{h}{(\log x)^D},$$

where $\rho_{\omega}$ is a nontrivial zero of $L(s, \omega)$ and $\sum^*$ denotes summing over primitive characters $\omega$. (See also [13, Section 1] for a similar reduction.)

We now decompose the interval $[1, Q]$ into dyadic intervals of the form $[2^n, 2^{n+1}]$, where $0 \leq n \leq \lceil\log_2 Q\rceil$. Since there are $O(\log Q)$ such intervals and $\varphi(q)^{-1} \ll q^{-1} \log \log q$, the left side of (2.1) is

$$\ll h(\log Q)(\log \log Q) \max_{1 \leq Q_1 \leq Q} \frac{1}{Q_1} \sum_{Q_1} \sum_{\omega} x^{\beta_{\omega} - 1} \frac{Q x (\log x)^2}{T}.$$  

If $\omega$ is primitive, then $f_\omega$ is also the modulus of $\omega$. Since $Nf_\omega \ll q^{nE}$, (2.2) is

$$\ll h(\log Q)(\log \log Q) \max_{1 \leq Q_1 \leq Q} \frac{1}{Q_1} \sum_{Q_1} \sum_{\beta_{\omega}} x^{\beta_{\omega} - 1} + \frac{Q x (\log x)^2}{T}.$$  

For $\frac{1}{2} \leq \sigma \leq 1$, let $N_{\omega}(\sigma, T) := \#\{\rho = \beta + i\gamma : L(\rho, \omega) = 0, \sigma \leq \beta, |\gamma| \leq T\}$ and

$N(\sigma, R, T) := \sum_{N \leq R} \sum_{\omega} N_{\omega}(\sigma, T).$

**Proposition 2.1.** If $T \geq 2$, $R \geq 1$, and $\frac{1}{2} \leq \sigma \leq 1$, then

$$N(\sigma, R, T) \ll (R^2 T^{nE})^{\frac{1}{2}(1-\sigma)} (\log QT)^9 n^{nE + 10}.$$  

**Proof.** This follows directly from the work Montgomery [11, Theorem 12.2] for $n_E = 1$ and Hinz [6, Satz A and B] for $n_E \geq 2$. It is weaker than either Montgomery’s or Hinz’s results, but it is far more convenient for our purposes. \hfill $\square$

**Proof of Theorem 1.1** Let $D, \delta,$ and $h$ be as in the statement of Theorem 1.1. Let $0 < \epsilon < 1 - 5nE\delta/2$, and set $Q = x^{2(1-\epsilon-5nE\delta)/15nE} (\log x)^{-D+2}$ and $T = x^{2(1-\epsilon+5nE\delta)/15nE} (\log x)^{-2(D+1)/3}$. With $1 \leq Q_1 \leq Q$, we have

$$\sum_{N \leq Q_1^{nE}} \sum_{\omega} x^{\beta_{\omega} - 1} \ll \log x \max_{\frac{1}{2} \leq \sigma < 1} x^{\sigma - 1} N(\sigma, Q_1^{nE}, T).$$

By the zero-free region for Hecke $L$-functions proven by Bartz [2] and the fact that we restrict $q$ so that $L(\zeta_q) = 0$, there exists a constant $b_L > 0$ such that if

$$1 - \eta(Q_1, x) < \sigma \leq 1, \quad \eta(Q_1, x) := \frac{b_L}{\max\{\log Q_1, (\log x)^{3/4}\}},$$

then $N(\sigma, Q_1^{nE}, T)$ is either 0 or 1. If $N(\sigma, Q_1^{nE}, T) = 1$, then the zero $\beta_1$ which is counted is a Landau-Siegel zero associated to an exceptional modulus $q_1$ and an exceptional real quadratic character in $\tilde{H}_{q_1}$. Just as in [13, Section 2], a field-uniform version of Siegel’s
theorem for Hecke $L$-functions implies that \( x^{\delta_1-1} \ll (\log x)^{-D-3} \) with an ineffective implied constant.

Since \((Q^2T)^{5n_E/2} = x^{1-\epsilon}\), it follows from Proposition 2.1 that

\[
\max_{\frac{1}{2} \leq \sigma \leq 1-\eta(Q_1,T)} x^{\sigma-1} N(\sigma, Q_1^{n_E}, T) \ll (\log x)^{9n_E+10} \max_{\frac{1}{2} \leq \sigma \leq 1-\eta(Q_1,T)} ((Q^2T)^{5n_E/2}/x)^{1-\sigma} \ll (\log x)^{9n_E+10} x^{-\epsilon \eta(Q_1,x)}.
\]

By our definition of \( \eta(Q_1, x) \), we have that \( x^{-\epsilon \eta(Q_1,x)} \ll (\log x)^{-9n_E+14+D} \) when \( 1 \leq Q_1 \leq \exp((\log x)^{3/4}) \), and \( x^{-\epsilon \eta(Q_1,x)} \ll 1 \) when \( \exp((\log x)^{3/4}) < Q_1 \leq Q \). We have now bounded (2.4), and so (2.3) is bounded by

\[
h(Q)(\log Q)(\log \log Q)(\log x) \max_{Q_1 \leq Q} \frac{1}{Q_1} ((\log x)^{-D-3} + (\log x)^{9n_E+11} x^{-\epsilon \eta(Q_1,x)}) + \frac{Qx(\log x)^2}{T}.
\]

For our choice of \( h, Q, \) and \( T \), this is bounded by \( h(Q)(\log x)^{-D} \), proving (2.1). \[ \square \]

One can use the full strength of Montgomery and Hinz’s work [6,11] instead of Proposition 2.1 to improve the ranges of \( \delta \) and \( \theta \) in Theorem 1.1 by following the proofs of Huxley and Iwaniec [7], but the improvement is very small, and the ensuing dependence of \( \theta \) on \( \delta \) and \( n_E \) is very complicated. Ultimately, our proof of Theorem 1.1 cannot produce values of \( \delta \) and \( \theta \) comparable to those in [7] because we sum over primitive Hecke characters whose conductor has norm \( \ll Q^{n_E} \), which seems unavoidable at this time.

3. PROOF OF THEOREM 1.3

We will use Theorem 1.1 to prove Theorem 1.3. Given a set of integers \( \mathfrak{A} \), a set of primes \( \mathfrak{P} \subset \mathfrak{A} \), and a linear form \( L(n) = n + h \), define

\[
\mathfrak{A}(x) = \{ n \in \mathfrak{A} : x < n \leq 2x \}, \quad \mathfrak{A}(x; q, a) = \{ n \in \mathfrak{A}(x) : n \equiv a \pmod{q} \},
\]

\[
L(\mathfrak{A}) = \{ L(n) : n \in \mathfrak{A} \}, \quad \varphi_L(q) = \varphi(hq)/\varphi(h),
\]

\[
\mathfrak{P}_{L,\mathfrak{A}}(x, y) = L(\mathfrak{A}(x)) \cap \mathfrak{P}, \quad \mathfrak{P}_{L,\mathfrak{A}}(x; q, a) = L(\mathfrak{A}(x; q, a)) \cap \mathfrak{P}.
\]

We consider the 6-tuple \( (\mathfrak{A}, \mathfrak{H}_k, \mathfrak{P}, B, x, \theta) \), where \( \mathfrak{H}_k \) is admissible, \( \mathfrak{L}_k = \{ L_i(n) = n + h_i : h_i \in \mathfrak{H}_k \} \), \( B \in \mathbb{N} \) is constant, \( x \) is a large real number, and \( 0 \leq \theta < 1 \). We present a very general hypothesis that Maynard states in Section 2 of [9].

Hypothesis 3.1. With the above notation, consider the 6-tuple \( (\mathfrak{A}, \mathfrak{H}_k, \mathfrak{P}, B, x, \theta) \).

(1) We have

\[
\sum_{q \leq x^{\theta}} \max_a \left| \frac{\# \mathfrak{A}(x; q, a) - \# \mathfrak{A}(x)}{q} \right| \ll \frac{\# \mathfrak{A}(x)}{(\log x)^{100k^2}}.
\]

(2) For any \( L \in \mathfrak{H}_k \), we have

\[
\sum_{q \leq x^{\theta}, (q,B)=1} \max_{(L(a),q)=1} \left| \frac{\# \mathfrak{P}_{L,\mathfrak{A}}(x; q, a) - \# \mathfrak{P}_{L,\mathfrak{A}}(x)}{\varphi_L(q)} \right| \ll \frac{\# \mathfrak{P}_{L,\mathfrak{A}}(x)}{(\log x)^{100k^2}}.
\]

(3) For any \( q \leq x^{\theta} \), we have \( \# \mathfrak{A}(x; q, a) \ll \# \mathfrak{A}(x)/q \).

For \( (\mathfrak{A}, \mathfrak{H}_k, \mathfrak{P}, B, x, \theta) \) satisfying Hypothesis 3.1, Maynard proves the following in [9].
Theorem 3.2. Let $\alpha > 0$ and $0 \leq \theta < 1$. There is a constant $C$ depending only on $\theta$ and $\alpha$ so that the following holds. Let $(\mathfrak{A}, \mathcal{H}_k, \mathfrak{P}, B, x, \theta)$ satisfy Hypothesis 3.1. Assume that $k \geq C$. If $\delta > (\log k)^{-1}$ is such that
\[
\frac{1}{k} \frac{\varphi(B)}{B} \sum_{L_i \in \mathcal{H}_k} \# \mathfrak{P}_{L_i, \mathfrak{A}}(x) \geq \delta \frac{\# \mathfrak{A}(x)}{\log x},
\]
then
\[
\# \{ n \in \mathfrak{A}(x) : \# (\mathcal{H}_k(n) \cap \mathfrak{P}) \geq C^{-1} \delta \log k \} \gg \frac{\# \mathfrak{A}(x)}{(\log x)^k \exp(C/k)}.
\]

Proof of Theorem 1.3. The proof is essentially the same as Theorems 3.4 and 3.5 in [9]. Let $\delta, h, \text{ and } \theta$ be as in Theorem 1.1. Let $\mathfrak{A} = N \cap [x, x + h]$, $B = d_L$, and $\mathfrak{P} = \mathcal{P}$ (as in (1.10)). Parts (i) and (iii) of Hypothesis 3.1 are trivial to check for the 6-tuple $(\mathbb{N} \cap [x, x + h], \mathcal{H}_k, \mathcal{P}, d_L, x, \theta/2)$. By Theorem 1.1, partial summation, and the fact that $(q, d_L) = 1$ implies $L \cap \mathbb{Q}(q) = \mathbb{Q}$, all of Hypothesis 3.1 holds when $D$ and $x$ are sufficiently large in terms of $k$ and $\theta$. Given a suitable constant $C_L > 0$ (computed as in [10, 22]), we let $k \geq C_L$. For our choice of $\mathfrak{A}$ and $\mathfrak{P}$, we have
\[
\frac{1}{k} \frac{\varphi(d_L)}{d_L} \sum_{L_i \in \mathcal{H}_k} \# \mathfrak{P}_{L_i, \mathfrak{A}}(x) \geq (1 + o(1)) \frac{\varphi(d_L)}{d_L} \frac{C}{|G|} \frac{\# \mathfrak{A}(x)}{\log x}
\]
for all sufficiently large $x$, where the implied constant in $1 + o(1)$ depends only on $L$. Theorem 1.3 now follows directly from Theorem 3.2. \hfill \Box

References