A variant of the Bombieri–Vinogradov theorem in short intervals and some questions of Serre

BY JESSE THORNER

Department of Mathematics and Computer Science, Emory University, Atlanta, Georgia, U.S.A.
e-mail: jesse.thorner@gmail.com

(Received 22 October 2014; revised 21 December 2015)

Abstract

We generalise the classical Bombieri–Vinogradov theorem for short intervals to a 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 of number fields. Using this result in conjunction with the recent work of Maynard, we prove that rational primes with a given splitting condition in a Galois extension $L/\mathbb{Q}$ exhibit bounded gaps in short intervals. We explore several arithmetic applications related to questions of Serre regarding the non-vanishing Fourier coefficients of cuspidal modular forms. One such application is that for a given modular $L$-function $L(s, f)$, the fundamental discriminants $d$ for which the $d$-quadratic twist of $L(s, f)$ has a non-vanishing central critical value exhibit bounded gaps in short intervals.

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

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

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

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

(1.1)

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

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

(1.2)

While this is currently out of reach, we know that the mean value of the left-hand side of (1.2) is about as small as predicted by GRH when we average over moduli $q$. Specifically, for constants $0 < \theta < 1/2$ and $D > 0$, Bombieri and Vinogradov [12, theorem 15.1] proved
that
\[
\sum \max_{q \leq x^\delta} \max_{(a, q) = 1} \max_{N \leq x} \left| \psi(2N; q, a) - \psi(N; q, a) - \frac{N}{\varphi(q)} \right| \lesssim \frac{x}{(\log x)^D}, \tag{1.3}
\]

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) in the form
\[
\sum \max_{q \leq x^\delta} \max_{(a, q) = 1} \max_{\frac{1}{2}x \leq N \leq x} \left| \psi(N + y; q, a) - \psi(N; q, a) - \frac{y}{\varphi(q)} \right| \lesssim \frac{h}{(\log x)^D}, \tag{1.4}
\]
where \(\delta > 0\) and \(\theta > 0\) are certain constants, \(D > 0\), and \(h \geq x^{1-\delta}\). It follows from GRH that (1.4) holds when \(0 \leq \delta < 1/2\) and \(0 \leq \theta < 1/2 - \delta\). In spite of the fact that we are far from proving GRH, there has been much progress toward this conjectured estimate; see [20] and the sources contained therein. As of now, the sharpest version of (1.4) is due to Timofeev [25], who proved that (1.4) holds when
\[
0 \leq \delta < \frac{5}{12}, \quad 0 \leq \theta < \begin{cases} \frac{1}{2} - \delta & \text{if } 0 \leq \delta < \frac{2}{5}, \\ \frac{9}{20} - \delta & \text{if } \frac{2}{5} \leq \delta < \frac{5}{12}. \end{cases}
\]

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 \(N_{K/\mathbb{Q}}\) 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 \(C \subset G\) 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
\[
\Lambda_C(a) := \begin{cases} \log N_{K/\mathbb{Q}}p & \text{if } a = p^m \text{ with } m \geq 1, p \text{ unramified in } L, \text{ and } \left[\frac{L/K}{p}\right]^m = C, \\ 0 & \text{otherwise}. \end{cases}
\]
and
\[
\psi_C(x; q, a) = \psi_C(x, L/K; q, a) := \sum_{N_{K/\mathbb{Q}}a \equiv a \pmod{q}} \Lambda_C(a). \tag{1.5}
\]
The Chebotarev density theorem asserts that if \(q \leq (\log x)^D\) for some constant \(D > 0\), then
\[
\psi_C(2x; q, a) - \psi_C(x; q, a) \sim d(C; q, a)x \tag{1.6}
\]
for some rational density \(d(C; q, a) \geq 0\). If \(\xi_q = e^{2\pi i/q}\) and \(L \cap \mathbb{Q}(\xi_q) = \mathbb{Q}\), then
\[
d(C; q, a) = \frac{|C|}{|G| \varphi(q)}. \]

Building on the work of M. R. Murty and V. K. Murty [13], M. R. Murty and Petersen [15] 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 \(0 \leq \theta < 1/\max(|E: \mathbb{Q}| - 2, 2)\), then for any constant \(D > 0\),
\[
\sum_{q \leq x^\delta} \max_{(a, q) = 1} \max_{N \leq x} \left| \psi_C(2N; q, a) - \psi_C(N; q, a) - \frac{|C|}{|G| \varphi(q)} \right| \lesssim \frac{x}{(\log x)^D}. \tag{1.7}
\]
A variant of the Bombieri–Vinogradov theorem in short intervals

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

When $q = 1$, Balog and Ono [1] extended (1.6) to a short interval setting using Heath–Brown’s zero density estimate for Dedekind zeta functions [5]. Specifically, if

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

(1.8)

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

$$\psi_C(x + h; 1, 1) - \psi_C(x; 1, 1) \sim \frac{|C|}{|G|} h.$$ 

(1.9)

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 $H \subset C$ be a largest abelian subgroup of $G$ such that $H \cap C$ is nonempty, and let $E$ be the fixed field of $H$. Let $0 \leq \delta < 2/[E : \mathbb{Q}]$ and $0 \leq \theta < (2/[E : \mathbb{Q}] - \delta)/3$. If $h \geq x^{1-\delta}$, then for any constant $D > 0$,

$$\sum_{\mathcal{Q}(\psi)} \max_{y \leq h} \max_{\frac{1}{x} \leq N \leq x} \left| \psi_C(N + y; q, a) - \psi_C(N; q, a) - \frac{|C|}{|G|} \psi(q) \right| \leq \frac{h}{(\log x)^D},$$

(1.10)

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

When $|H| \geq 3$, 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. This improvement holds for the vast majority of choices of $L/K$ and $C$. Examples of such situations include when $C$ has an element of order at least 3 or when $[L : K] \geq 3$ is odd.

**Corollary 1.1.** Let $L/K$, $G$, $C$, $H$, and $E$ be as in Theorem 1.1, and suppose that $|H| \geq 3$. Let $a, q \in \mathbb{N}$ satisfy $L \cap \mathbb{Q}(\xi_q) = \mathbb{Q}$ and $(a, q) = 1$; furthermore, for some constant $D > 0$, let $q \leq (\log x)^D$. If $0 \leq \delta < 2/[E : \mathbb{Q}]$ and $h \geq x^{1-\delta}$, then

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

Much like the results of [13, 15], 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 sets of the form

$$\mathcal{P} = \left\{ p : p \neq d_L, \left[ \frac{L/\mathbb{Q}}{p} \right] = C \right\}.$$ 

(1.11)

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.)
Furthermore, if $\mathcal{H}_k$ is admissible, then as $x \to \infty$, we have
\[
\#\{n \in [x, 2x] : \#(\{n + h_1, \ldots, n + h_k\} \cap \mathcal{P}) = k\} \sim \mathcal{G} \frac{x}{(\log x)^k},
\]
where $\mathcal{G}$ 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 [11], 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
\[
\#(\{n + h_1, \ldots, n + h_k\} \cap \mathcal{P}) \geq (1/4 + o_{k \to \infty}(1)) \log k.
\]
(Tao independently developed similar ideas, but arrived at slightly different conclusions.)

Using Maynard’s improvement to the Selberg sieve and (1.7), the author [24] proved a similar result for Chebotarev sets; the proof is easily generalised to show that if $\mathcal{H}_k$ is admissible, then there are infinitely many integers $N \geq 1$ such that for some $n \in [N, 2N]$,
\[
\#(\{n + h_1, \ldots, n + h_k\} \cap \mathcal{P}) \geq \left(\frac{1}{2 \max\{|E : \mathbb{Q}| - 2, 2\}} \frac{|C| \varphi(d_L)}{|G|} + o_{k \to \infty}(1)\right) \log k,
\]
(1.12)
where $\mathcal{P}$ is given by (1.11). (In [24], $1/\max\{|E : \mathbb{Q}| - 2, 2\}$ was replaced by $\min\{1/2, 2/|G|\}$, which is a convenient lower bound. This lower bound is close to sharp, considering that $|E : \mathbb{Q}|$ divides $|G| = [L : \mathbb{Q}]$ in this case.)

The author explored applications of (1.12) to ranks of quadratic twists of elliptic curves, congruences for the Fourier coefficients of newforms, and representations of primes by binary quadratic forms.

In [10], Maynard generalised his methods to prove weak forms of the Hardy–Littlewood conjecture with specialisations to primes in short intervals and primes in Chebotarev sets. More specifically, given $0 \leq \delta < 5/12$ 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
\[
\#\{n \in [x, x+h] : \#(\{n + h_1, \ldots, n + h_k\} \cap \mathcal{P}) \geq C^{-1} \log k\} \geq \frac{h}{(\log x)^k}.
\]
(1.13)
Furthermore, if $\mathcal{P}$ is given by (1.11), 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
\[
\#\{n \in [x, 2x] : \#(\{n + h_1, \ldots, n + h_k\} \cap \mathcal{P}) \geq C_L^{-1} \log k\} \geq \frac{x}{(\log x)^k}.
\]
(1.14)
(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 (1.13) and (1.14), which extends the author’s applications in [24] to a short interval setting.

**Theorem 1.2.** Let $L/\mathbb{Q}$ be a Galois extension of number fields, let $\mathcal{P}$ be as in (1.11), 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 $\mathcal{H}_k = \{h_1, \ldots, h_k\}$ is admissible, then
\[
\#\{n \in [x, x+h] : \#(\{n + h_1, \ldots, n + h_k\} \cap \mathcal{P}) \geq C_L^{-1} \log k\} \geq \frac{h}{(\log x)^k}.
\]
Remark. Some of the parameters in the statement of Theorem 1-2 can have some uniformity in \( x \) by appealing to the arguments in [10]. In what follows, we will assume that all parameters are constant with respect to \( x \).

We now consider arithmetic consequences of Theorem 1-2 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 [18]. We consider the following questions of Serre [21], 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 Questions.** 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 of nebentypus \( \chi \). For a nonzero cusp form \( f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_\ell(\Gamma_0(N), \chi) \), let

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

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

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

Motivated by Serre’s questions, 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 \( \ell \in \frac{1}{2} \mathbb{Z} \setminus \{1/2\} \) which is not a linear combination of weight 3/2 theta functions, then there exists \( \nu_f \in \mathbb{N} \) such that if \( 0 \leq \delta < 1/\nu_f \) and \( h \geq x^{1-\delta} \), then

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

For such a cusp form \( f \), it follows that \( I_f(n) \leq n^{1-\frac{1}{\nu_f} + \epsilon} \) for any \( \epsilon > 0 \), affirmatively answering Serre’s questions. By using Theorem 1-2 instead of (1.9) in Balog and Ono’s proof, we immediately conclude that the integers \( n \) for which \( a_f(n) \neq 0 \) exhibit bounded gaps in short intervals. More specifically, we have the following.

**Theorem 1.3.** 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 \( \ell \in \mathbb{N}/2 \setminus \{1/2\} \) which is not a linear combination of weight 3/2 theta functions. There exist constants \( C_f, \nu_f \in \mathbb{N} \) such that if \( 0 \leq \delta < 1/\nu_f \), \( h \geq x^{1-\delta} \), \( k \geq C_f \) and \( \mathcal{H}_k = \{h_1, \ldots, h_k\} \) is admissible, then

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

We use Theorem 1.3 to study the central critical values of modular \( L \)-functions and ranks of elliptic curves. Let \( f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_\ell(\Gamma_0(N), \chi) \) be a cusp form such that \( \ell \geq 2 \) is an integer, \( a_f(1) = 1 \), and \( f \) is an eigenform of the Hecke operators \( T_p \) for \( p \nmid N \) and \( U_p \) for \( p \mid N \); we call such a cusp form \( f \) a newform. Let \( \mathcal{D} \) be the set of all fundamental discriminants; given \( d \in \mathcal{D} \), we consider the twisted \( L \)-function

\[
L(s, f_d) = \sum_{n=1}^{\infty} \frac{a_f(n)\chi_d(n)}{n^{s+(\ell-1)/2}},
\]
where $\chi_d$ is the Kronecker character for $\mathbb{Q}(\sqrt{d})$. For newforms of weight $\ell \in 2\mathbb{N}$ and trivial nebentypus $\chi$, Goldfeld [4] conjectured that the proportion of $d \in \mathcal{D}$ for which $L(1/2, f_d) \neq 0$ is $1/2$.

If $g$ is a half-integer weight cusp form satisfying the hypotheses of Theorem 1.3, then by the work of Shimura [22] and Waldspurger [26], the Fourier coefficients $a_\nu(n)$ interpolate the central critical values $L(1/2, f_d)$ as $d$ varies, where $f$ is the Shimura correspondent of $g$. Despite the fact that the Shimura correspondence is not surjective, Ono and Skinner [19] proved that such central critical values can be obtained in this fashion when $f$ is a newform of even weight and trivial nebentypus $\chi$. Using this observation along with (1.15), Balog and Ono [1] proved that there exists $v_f \in \mathbb{N}$ such that if $0 \leq \delta < 1/v_f$ and $h \geq x^{1-\delta}$, then

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

(1.16)

This is the sharpest result in the direction of Goldfeld’s conjecture which is valid for all newforms $f$ of even weight and trivial nebentypus; for most such newforms, the power of $\log x$ can be improved [17]. By using Theorem 1.3 instead of (1.15) in Balog and Ono’s proof, we immediately conclude that fundamental discriminants $d$ for which $L(1/2, f_d) \neq 0$ exhibit bounded gaps in short intervals.

**Corollary 1.2.** Let $f \in S_{2\ell}(\Gamma_0(N), \chi_{\text{triv}})$ be a newform with $\ell \in \mathbb{N}$. There exists an arithmetic progression $a \mod q$ (depending on $f$) and there exist constants $v_f, C_f \in \mathbb{N}$ such that if $0 \leq \delta < 1/v_f$, $h \geq x^{1-\delta}$, $k \geq C_f$, $\mathcal{H}_k = \{h_1, \ldots, h_k\}$ is admissible, and

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

then

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

Remark. We need to restrict to the arithmetic progression $a \mod q$ for technical reasons; see [19] for details. We accomplish this by combining the arguments of Freiburg [3, proof of theorem 1] with Maynard’s proofs in [10], which is straightforward to do.

Let $f$ be the newform associated to an elliptic curve $E/\mathbb{Q}$ of conductor $N$ with Weierstrass equation $y^2 = x^3 + ax^2 + bx + c$. If $(d, 4N) = 1$, then $L(s, f_d)$ is the $L$-function of the $d$-quadratic twist $E_d/\mathbb{Q}$, whose Weierstrass equation is given by $y^2 = x^3 + adx^2 + bd^2x + cd^3$.

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 1.2 immediately implies the following result.

**Corollary 1.3.** Let $E/\mathbb{Q}$ be an elliptic curve. There exists an arithmetic progression $a \mod q$ (depending explicitly on $E$) and there exist constants $v_E, C_E \in \mathbb{N}$ such that if $0 \leq \delta < 1/v_E$, $h \geq x^{1-\delta}$, $k \geq C_E$, $\mathcal{H}_k = \{h_1, \ldots, h_k\}$ is admissible, and

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

then

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

For our final application, consider an elliptic curve $E/\mathbb{Q}$. The distribution of the quantity $a_E(p) := p + 1 - #E(\mathbb{F}_p)$ is well-studied [14, 16, 21, 27]; we apply our results to study the distribution of $a_E(p) \pmod{m}$ in short intervals. It follows from the work of Shiu [23]
that if \( E/\mathbb{Q} \) has a rational point of order \( m \), then for every \( j \in \mathbb{N} \) and every \( i \not\equiv 1 \pmod{m} \), 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 for any \( m \in \mathbb{N} \) and any residue class \( i \pmod{m} \) for which there is a prime of good reduction \( p_0 \) with \( a_E(p_0) \equiv i \pmod{m} \), there exists \( v_{E,m} \in \mathbb{N} \) such that if \( 0 \leq \delta < 1/v_{E,m} \) and \( h \geq x^{1-\delta} \), then

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

By using Theorem 1.2 instead of (1.9) in Balog and Ono’s proof, we immediately conclude the following result.

**Corollary 1.4.** Let \( E/\mathbb{Q} \) be an elliptic curve, let \( m \in \mathbb{N} \), and let \( i \pmod{m} \) 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 \( v_{E,m}, C_{E,m} \in \mathbb{N} \) such that if \( 0 \leq \delta < 1/v_{E,m} \), \( h \geq x^{1-\delta} \), \( k \geq C_{E,m} \), and \( \mathcal{H}_k = \{ h_1, \ldots, h_k \} \) is admissible, then

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

First, we give some necessary setup and background on the Chebotarev density theorem in Section 2. We then prove Theorem 1.1 in Section 3 and Theorem 1.2 in Section 4.

### 2. Preliminary setup

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 \( C \subseteq G \) 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 \( d_L \).

The setup in this section is essentially the same as in [9, 15]. To single out those \( p^n \) in \( K \) such that both \( [(L/K)/p]^n = C \) and \( N_{K/\mathbb{Q}}p^n \equiv a \pmod{q} \), we will use the characters \( \eta = \phi \otimes \chi \) of the Galois group \( \text{Gal}(L(\zeta_q)/K) \), where \( \phi \) is an irreducible character of \( G \) and \( \chi \) (mod \( q \)) is a Dirichlet character. We work under the assumption that \( L \cap \mathbb{Q}(\zeta_q) = \mathbb{Q} \) so that \( \text{Gal}(L(\zeta_q)/K) \cong G \times (\mathbb{Z}/q\mathbb{Z})^\times \) and \( \eta(a) = \phi(a)\chi(N_{K/\mathbb{Q}}a) \) for any integral ideal \( a \) of \( K \). Let

\[
F_C(s) = -\frac{|C|}{|G|} \frac{1}{\varphi(q)} \sum_\eta \frac{L'}{L}(s, \eta, L(\zeta_q)/K),
\]

where \( L(s, \eta, L(\zeta_q)/K) \) is the Artin \( L \)-function associated to \( \eta \). For \( \text{Re}(s) > 1 \), we have the Dirichlet series expansion

\[
F_C(s) = \sum_p \sum_{m=1}^{\infty} \theta(p^m)(\log N_{K/\mathbb{Q}}p)N_{K/\mathbb{Q}}p^{-ms}.
\]

If \( p \) is unramified in \( L \), then \( \theta(p^m) = 1 \) if \( [(L/K)/p]^n = C \) and \( N_{K/\mathbb{Q}}p \equiv a \pmod{q} \); otherwise, \( \theta(p^m) = 0 \). If \( p \) ramifies in \( L \) or \( \mathbb{Q}(\zeta_q) \), then \( |\theta(p^m)| \leq 1 \). Therefore, apart from ramified primes, \( \psi_C(x; q, a) \) is a partial sum of the coefficients of \( F_C(s) \).
Unfortunately, \( \theta(p^n) \) is expressed in terms of Artin L-functions corresponding to the (usually nonabelian) characters of \( G \times (\mathbb{Z}/q\mathbb{Z})^\times \). Fortunately, \( F_C(s) \) can be written in terms of L-functions associated to abelian characters, which are Hecke L-functions by abelian reciprocity. Let \( H \subset G \) be a largest abelian subgroup such that \( H \cap C \) is nonempty, let \( E \) be the fixed field of \( H \), and let \( \xi \) denote the irreducible characters of \( H \). Since \( H \) is abelian, the characters \( \omega = \xi \otimes \chi \) of the Galois group \( H_q = \text{Gal}(L(\zeta_q)/E) \cong H \times (\mathbb{Z}/q\mathbb{Z})^\times \) are one-dimensional. Because \( L \cap \mathbb{Q}(\zeta_q) = \mathbb{Q} \), we have that \( \omega(a) = \xi(a)\chi(N_{E/\mathbb{Q}}a) \); furthermore, if \( f_\omega \) is the conductor of \( \omega \), then \( N_{E/\mathbb{Q}}f_\omega \ll q^{n_E} \). (We let \( N = N_{E/\mathbb{Q}} \) henceforth.)

By the same arguments as in [9, lemma 4.1], we may write

\[
F_C(s) = -\frac{|C|}{|G|} \frac{1}{\varphi(q)} \sum_{\omega \in \hat{H}_q} \tilde{\omega}(C) \frac{L'}{L}(s, \omega, L(\zeta_q)/E).
\]

Repeating the analysis leading up to [9, theorem 7.1], we find that if \( 2 \leq T \leq x \), then

\[
\psi_C(x; q, a) = \frac{|C|}{|G|} \frac{1}{\varphi(q)} \left( x - \sum_{\omega \in \hat{H}_q} \tilde{\omega}(C) \left( \sum_{\rho = \beta + iy, |\gamma| \leq T} \frac{x^\rho}{\rho} - \sum_{|\rho| \leq 1/2} \frac{1}{\rho} \right) \right) \ll \frac{x(\log x)^2}{T},
\]

where \( \rho \) is a nontrivial zero of \( L(s, \omega, L(\zeta_q)/E) \) and \( \tilde{\omega} \) is the primitive character which induces \( \omega \). Now, suppose \( y \leq h \) and \( \frac{1}{2}x \leq N \leq x \). Using the bound

\[
\left| \left( N + y \right)^\rho - N^\rho \right| = \left| \int_N^{N+y} t^{\rho-1} dt \right| \leq \int_N^{N+y} t^{\Re(\rho)-1} dt \leq yN^{\Re(\rho)-1} \ll hx^{\Re(\rho)-1},
\]

we find that

\[
\max_{\frac{1}{2}x \leq N \leq x} \left| \psi_C(N + y; q, a) - \psi_C(N; q, a) \right| = \frac{|C|}{|G|} \frac{y}{\varphi(q)} \sum_{\omega \in \hat{H}_q} \sum_{\rho = \beta + iy, |\gamma| \leq T} x^{\beta-1} + \frac{x(\log x)^2}{T}.
\]

Therefore, the left-hand side of (1.10) is

\[
\ll h \sum_{q \leq Q} \frac{1}{\varphi(q)} \sum_{\omega \in \hat{H}_q} \sum_{\rho = \beta + iy, |\gamma| \leq T} x^{\beta-1} + \frac{Qx(\log x)^2}{T}, \tag{2.1}
\]

where \( \rho \) is a nontrivial zero of \( L(s, \omega, L(\zeta_q)/E) \) and \( \sum^* \) denotes summing over primitive characters \( \omega \).

Theorem 1.1 will follow immediately from proving that for any fixed \( D > 0 \), we have

\[
h \sum_{q \leq Q} \frac{1}{\varphi(q)} \sum_{\omega \in \hat{H}_q} \sum_{\rho = \beta + iy, |\gamma| \leq T} x^{\beta-1} + \frac{Qx(\log x)^2}{T} \ll \frac{h}{(\log x)^D}, \tag{2.2}
\]

where \( Q = x^\theta, \ h \geq x^{1-\delta} \), and \( \delta \) and \( \theta \) are given in the statement of Theorem 1.1.

3. Proof of Theorem 1.1

Decompose the interval \([1, Q]\) into the dyadic intervals \([2^n, 2^{n+1}]\), where \( 0 \leq n \leq \lfloor \log_2 Q \rfloor \). Since \( \varphi(q)^{-1} \ll q^{-1} \log \log q \), (2.1) is

\[
\ll h(\log Q)(\log \log Q) \max_{1 \leq R \leq Q} \frac{1}{R} \sum_{q \leq R} \sum_{\omega \in \hat{H}_q} \sum_{\rho = \beta + iy, |\gamma| \leq T} x^{\beta-1} + \frac{Qx(\log x)^2}{T}. \tag{3.1}
\]
A variant of the Bombieri–Vinogradov theorem in short intervals  

If \( \omega = \eta \otimes \chi \) is primitive, then \( f_\omega \) is also the modulus of \( \omega \). Since \( N f_\omega \ll q^{n_E} \), where \( q \) is the modulus of \( \chi \), (3.1) is

\[
\ll h(\log Q)(\log \log Q) \max_{1 \leq R \leq Q} \frac{1}{R} \sum_{N \alpha \leq R} \sum_{\omega \mod a} x^{\beta-1} + \frac{Qx(\log x)^2}{T}. 
\]  

(3.2)

For \( 1/2 \leq \sigma \leq 1 \), let \( N_\omega(\sigma, T) := \#\{ \rho = \beta + iy : L(\rho, \omega, L(\xi_q)/E) = 0, \sigma \leq \beta, |y| \leq T \} \) and

\[
N(\sigma, R, T) := \sum_{N \alpha \leq R} \sum_{\omega \mod a} N_\omega(\sigma, T).
\]

**PROPOSITION 3.1.** If \( T \geq 2, R \geq 1 \), and \( 1/2 \leq \sigma \leq 1 \), then

\[
N(\sigma, R, T) \ll (R^2 T^{n_E})^{1/(1-\sigma)} (\log RT)^{9n_E+10}.
\]

**Proof.** This follows directly from the work Montgomery [12, 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.

**Proof of Theorem 1.1.** Let \( D > 0 \), let \( 0 \leq \delta < 2/5n_E \), and let \( h \geq x^{1-\delta} \). Let

\[
Q = x^{1/(\frac{1}{5} - \delta) - \frac{2}{5n_E} \epsilon} (\log x)^{-\frac{11}{6}} \quad \text{and} \quad T = x^{\frac{2}{5n_E} (1 + 5n_E \delta - \epsilon)} (\log x)^{\frac{2D + 11}{5}},
\]

where \( 0 < \epsilon < 1 - 5n_E \delta/2 \) is fixed. With \( 1 \leq R \leq Q \), we have

\[
\sum_{N \alpha \leq R} \sum_{\omega \mod a} x^{\beta-1} \ll \log x \max_{\frac{1}{7} \leq \sigma < 1} x^{\sigma-1} N(\sigma, R^{n_E}, T).
\]  

(3.3)

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

\[
1 - \alpha(R, x) < \sigma \leq 1, \quad \alpha(R, x) := \frac{b_L}{\max[\log R, (\log x)^{3/4}]},
\]  

(3.4)

then \( N(\sigma, R^{n_E}, T) \) is either 0 or 1. If \( N(\sigma, R^{n_E}, T) = 1 \), then the counted zero \( \beta_1 \) is a Landau–Siegel zero associated to an exceptional modulus \( q_1 \) and an exceptional real quadratic character in \( \mathcal{H}_{q_1} \). Just as in [15, section 2], a field-uniform version of Siegel’s theorem implies that \( x^{\beta_1-1} \ll (\log x)^{-D-3} \) with an ineffective implied constant.

Since \( (Q^2 T)^{5n_E/2} = x^{1-\epsilon} \), it follows from Proposition 3.1 that

\[
\max_{\frac{1}{7} \leq \sigma \leq 1 - \alpha(R, x)} x^{\sigma-1} N(\sigma, R^{n_E}, T) \ll (\log x)^{9n_E+10} \max_{\frac{1}{7} \leq \sigma \leq 1 - \alpha(R, x)} ((Q^2 T)^{5n_E/2} / x)^{1-\sigma} \ll (\log x)^{9n_E+10} x^{-\varepsilon(R, x)}.
\]

By our definition of \( \alpha(R, x) \), we have that \( x^{-\varepsilon(R, x)} \ll (\log x)^{-9n_E+14+D} \) when \( 1 \leq R \leq \exp((\log x)^{3/4}) \), and \( x^{-\varepsilon(R, x)} \ll 1 \) when \( \exp((\log x)^{3/4}) < R \leq Q \). We have now bounded (3.3), and so (3.2) is bounded by

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

For our choice of \( h \), \( Q \), and \( T \), this is \( \ll (\log x)^{-D} \), proving (2.2).

Using the full strength of Montgomery and Hinz’s work [6, 12] instead of Proposition 3.1, one can improve the ranges of \( \delta \) and \( \theta \) in Theorem 1.1 by following Huxley and Iwaniec [7].
The improvement is very small, and the ensuing dependence of $\theta$ on $\delta$ and $n_E$ is cumbersome. Ultimately, our proof of Theorem 1.1 cannot produce values of $\delta$ and $\theta$ comparable to those in [7] because we sum over primitive characters $\omega$ with $Nf_\omega \ll Q^{\alpha_2}$ instead of $\ll Q$, which seems unavoidable at this time.

4. Proof of Theorem 1.2

We will use Theorem 1.1 to prove Theorem 1.2. 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

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

$$L(\mathfrak{A}) = \{ L(n) : n \in \mathfrak{A} \}, \quad \varphi_L(q) = \varphi(c) / \varphi(h),$$

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

We consider the 6-tuple $(\mathfrak{A}, L_k, \mathfrak{P}, B, x, \theta)$, where $H_k$ is admissible, $L_k = \{ L(n) = n + h_i : h_i \in H_k \}, B \in \mathbb{N}$ is constant, $x$ is a large real number, and $0 \leq \theta < 1$. We present a very general hypothesis that Maynard states in [10, section 2].

**Hypothesis 4.1.** With the above notation, consider the 6-tuple $(\mathfrak{A}, L_k, \mathfrak{P}, B, x, \theta)$.

(i) We have

$$\sum_{q \leq x^\theta} \max_a \left| \frac{\#\mathfrak{A}(x; q, a) - \#\mathfrak{A}(x)}{q} \right| \ll \frac{\#\mathfrak{A}(x)}{(\log x)^{100\alpha_2}}.$$

(ii) For any $L \in L_k$, we have

$$\sum_{q \leq x^\theta, (q, B) = 1} \max_{L(n), a = 1} \left| \frac{\#\mathfrak{P}_{L, \mathfrak{A}}(x; q, a) - \#\mathfrak{P}_{L, \mathfrak{A}}(x)}{\varphi_L(q)} \right| \ll \frac{\#\mathfrak{P}_{L, \mathfrak{A}}(x)}{(\log x)^{100\alpha_2}}.$$

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

For $(\mathfrak{A}, L_k, \mathfrak{P}, B, x, \theta)$ satisfying Hypothesis 4.1, Maynard proves the following in [10].

**Theorem 4.1.** Let $(\mathfrak{A}, L_k, \mathfrak{P}, B, x, \theta)$ satisfy Hypothesis 4.1 with $0 \leq \theta < 1$. There is a constant $C > 0$, depending only on $\theta$, such that if $k \geq C$ and $\eta > (\log k)^{-1}$ satisfies

$$\frac{1}{k} \frac{\varphi(B)}{B} \sum_{L \in L_k} \#\mathfrak{P}_{L, \mathfrak{A}}(x) \geq \eta \frac{\#\mathfrak{A}(x)}{\log x},$$

then

$$\#\{ n \in \mathfrak{A}(x) : \#\{ L_i \in L_k : L_i(n) \in \mathfrak{P} \} \geq C^{-1} \eta \log k \} \geq \frac{\#\mathfrak{A}(x)}{(\log x)^e \exp(Ck)}.$$

**Proof of Theorem 1.2.** Let $\delta$, $h$, and $\theta$ be as in Theorem 1.1. Let $\mathfrak{A} = \mathbb{N} \cap [x, x + h]$, $B = d_L$, and $\mathfrak{P} = \mathcal{P}$ (as in (1.11)). The proof is the same as in [10, theorems 3.4 and 3.5]: we show that the 6-tuple $\mathfrak{A} \cap [x, x + h]$, $L_k$, $\mathfrak{P}$, $d_L$, $x$, $\theta/2$ satisfies Theorem 4.1.

Parts (i) and (iii) of Hypothesis 4.1 are trivial to check. For Part (ii), note that if $(d_L, q) = 1$, then $L \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$. Thus by Theorem 1.1 and partial summation, all of Hypothesis 4.1 holds when $D$ and $x$ are sufficiently large in terms of $k$ and $\theta$. Given a suitable constant $C_L > 0$ (computed as in [11, 24]), we let $k \geq C_L$. W have

$$\frac{1}{k} \frac{\varphi(d_L)}{d_L} \sum_{L \in L_k} \#\mathfrak{P}_{L, \mathfrak{A}}(x) \geq \left( 1 + o(1) \right) \frac{\varphi(d_L)}{d_L} \frac{|C| \#\mathfrak{A}(x)}{|G| \log x}$$

for all sufficiently large $x$, where the $o(1)$ implied constant depends only on $L$. 


A variant of the Bombieri–Vinogradov theorem in short intervals

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

REFERENCES

[1] A. BALOG and K. ONO. The Chebotarev density theorem in short intervals and some questions of Serre. J. Number Theory. 91 (2001), no. 2, 356–371.
[2] K. M. BARTZ. An effective order of Hecke-Landau zeta functions near the line $\sigma = 1$. II. (Some applications). Acta Arith. 52 (1989), no. 2, 163–170.
[3] T. FREIBERG. A Note on the Theorem of Maynard and Tao. Advances in the Theory of Numbers. Proc. Thirteenth Conference of the Canadian Number Theory Association. (2015), pp. 87–103.
[4] D. GOLDFELD. Conjectures on Elliptic Curves Over Quadratic Fields. Number Theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979). (1979), pp. 108–118. Berlin.
[5] D. R. HEATH–BROWN. On the density of the zeros of the Dedekind zeta-function. Acta Arith. 33 (1977), no. 2, 169–181.
[6] J. Hinz. Über Nullstellen der Heckeschen Zetafunctionen in algebraischen Zahlkörpern. Acta Arith. 31 (1976), no. 2, 167–193.
[7] M. N. HUXLEY and H. IWANIEC. Bombieri’s theorem in short intervals. Mathematika 22 (1975), no. 2, 188–194.
[8] V. A. KOLYVAGIN. Finiteness of $E(\mathbb{Q})$ and SH $(E, \mathbb{Q})$ for a subclass of Weil curves. Izv. Akad. Nauk SSSR Ser. Mat. 52 (1988), no. 3, 522–540, 670–671.
[9] J. C. LAGARIAS and A. M. ODLYZKO. Effective Versions of the Chebotarev Density Theorem. Algebraic Number Fields: $L$-functions and Galois properties (Proc. Sympos., University Durham, Durham, 1975), (1977), pp. 409–464.
[10] J. MAYNARD. Dense clusters of primes in subsets. arxiv.org/abs/1405.2593.
[11] J. MAYNARD. Small gaps between primes. Ann. of Math. (2) 181 (2015), no. 1, 383–413.
[12] H. L. MONTGOMERY. Topics in multiplicative number theory. Lecture Notes in Math., Vol. 227. (Springer-Verlag, Berlin-New York, 1971).
[13] M. R. MURTY and V. K. MURTY. A variant of the Bombieri–Vinogradov theorem. Number Theory (Montreal, Que., 1985), (1987), pp. 243–272.
[14] M. R. MURTY, V. K. MURTY and N. SARADHA. Modular forms and the Chebotarev density theorem. Amer. J. Math. 110(1988), no. 2, 253–281.
[15] M. R. MURTY and K. L. PETERSEN. A Bombieri–Vinogradov theorem for all number fields. Trans. Amer. Math. Soc. 365 (2013), no. 9, 4987–5032.
[16] V. K. MURTY. Modular forms and the Chebotarev density theorem. II. Analytic Number Theory (Kyoto, 1996), (1997), pp. 287–308.
[17] K. ONO. Nonvanishing of quadratic twists of modular $L$-functions and applications to elliptic curves. J. Reine Angew. Math. 533 (2001), 81–97.
[18] K. ONO. The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and $q$-Series. CBMS Regional Conference Series in Mathematics. vol. 102. Published for the Conference Board of the Mathematical Sciences, Washington, DC (American Mathematical Society, Providence, RI, 2004).
[19] K. ONO and C. SKINNER. Non-vanishing of quadratic twists of modular $L$-functions. Invent. Math. 134 (1998), no. 3, 651–660.
[20] A. PERELLI, J. PINTZ and S. SALERNO. Bombieri’s theorem in short intervals. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) 11 (1984), no. 4, 529–539.
[21] J.–P. SERRE. Quelques applications du thêorème de densité de Chebotarev. Inst. Hautes Études Sci. Publ. Math., (54) (1981), 323–401.
[22] G. SHIMURA. On modular forms of half integral weight. Ann. of Math. (2) 97 (1973), 440–481.
[23] D. K. L. SHIU. Strings of congruent primes. J. London Math. Soc. (2) 61 (2000), no. 2, 359–373.
[24] J. THORNER. Bounded gaps between primes in Chebotarev sets. Res. Math. Sci. 1 (2014), Art. 4, 16.
[25] N. M. TIMOFEEV. Distribution of arithmetic functions in short intervals in the mean with respect to progressions. Izv. Akad. Nauk SSSR Ser. Mat. 51 (1987), no. 2, 341–362, 447.
[26] J.–L. WALDSPURGER. Sur les coefficients de Fourier des formes modulaires de poids demi-entier. J. Math. Pures Appl. (9) 60 (1981), no. 4, 375–484.
[27] D. Q. WAN. On the Lang–Trotter conjecture. J. Number Theory. 35 (1990), no. 3, 247–268.