CYCLICITY AND EXPONENTS OF CM ELLIPTIC CURVES
MODULO \( p \) IN SHORT INTERVALS

PENG-JIE WONG

Abstract. Let \( E \) be a CM elliptic curve defined over \( \mathbb{Q} \). We establish an asymptotic formula for the number of primes \( p \) for which the reduction modulo \( p \) of \( E \) is cyclic over short intervals. This extends previous work of Akbary, Cojocaru, M. R. Murty, V. K. Murty, and Serre. Also, in light of the work of Freiberg, Kim, Kurlberg, Liu, and Wu, we estimate the average exponent of \( E \) and the second moment of the number of distinct prime divisors of exponents of \( E \) in short intervals. The key new idea is the use of our short interval generalisation of the work of Huxley and Wilson on the Bombieri–Vinogradov theorem for number fields.

1. Introduction

Let \( E \) be an elliptic curve defined over \( \mathbb{Q} \) and of conductor \( N_E \). For a prime \( p \) of good reduction, we let \( \bar{E} \) be the reduction of \( E \) modulo \( p \) and \( \bar{E}(\mathbb{F}_p) \) be the group of rational points of \( \bar{E} \) over \( \mathbb{F}_p \). In 1977, Lang and Trotter [31] formulated an elliptic curve analogue of Artin’s primitive root conjecture asserting that if \( P \) is a rational point of \( E/\mathbb{Q} \) of infinite order, then the density of the primes \( p \nmid N_E \) for which \( \bar{E}(\mathbb{F}_p) = \langle P(\textrm{mod } p) \rangle \) exists. Naturally, this led to the subquestion of finding the density of the primes \( p \nmid N_E \) with cyclic \( \bar{E}(\mathbb{F}_p) \). (We remark that there is also an elliptic curve analogue of the twin prime conjecture due to Koblitz of determining the density of \( p \) for which the cardinality of \( \bar{E}(\mathbb{F}_p) \) is prime.) The study of these questions is still one of the major problems in the “analytic part” of the theory of elliptic curves.

In this paper, we shall consider

\[ \pi_c(x, E) = \# \{ p \leq x \mid p \nmid N_E \text{ and } \bar{E}(\mathbb{F}_p) \text{ is cyclic} \}, \]

and let GRH stand for the generalised Riemann hypothesis for the Dedekind zeta functions of the division fields \( \mathbb{Q}(E[m])/\mathbb{Q} \) of \( E \), where \( E[m] \) is the group of \( m \)-torsion points of \( E \) for square-free \( m \).

Adapting Hooley’s conditional proof of Artin’s primitive root conjecture, Serre [45] proved that under the assumption of GRH, if \( \mathbb{Q}(E[2]) \neq \mathbb{Q} \), then one has

\[ \pi_c(x, E) = c_E \text{Li}(x) + o\left( \frac{x}{\log x} \right), \]

Received by the editors September 18, 2019, and, in revised form, April 1, 2020.
2010 Mathematics Subject Classification. Primary 11G05, 11N36, 11G15, 11R45, 11R44.
Key words and phrases. CM elliptic curves, cyclicity problem, exponents of elliptic curves, Bombieri–Vinogradov theorem in short intervals.

The author is currently a PIMS Post-Doctoral Fellow at the University of Lethbridge.

©2020 Peng-Jie Wong

8725
where \( \text{Li}(x) \) is the logarithmic integral function,

\[
c_E = \sum_{m=1}^{\infty} \frac{\mu(m)}{[Q(E[m]) : Q]},
\]

and \( \mu(m) \) is the Möbius function. After the work of Serre, M. R. Murty [37] Theorem 2] showed that under GRH,

\[
\pi_c(x, E) = c_E \text{Li}(x) + O\left(\frac{x \log \log x}{(\log x)^2}\right).
\]

Furthermore, the error term in the above estimate was considerably improved by Cojocaru and M. R. Murty [10]. For instance, for any elliptic curve \( E/\mathbb{Q} \) of conductor \( N_E \) and with complex multiplication by the ring of integers \( \mathcal{O}_K \) of an imaginary quadratic field \( K \), they showed that under GRH,

\[
\pi_c(x, E) = c_E \text{Li}(x) + O(x^{3/4}(\log(N_E x))^{1/2}),
\]

where the implied constant is absolute. Also, Cojocaru and M. R. Murty [10, Sec. 6] showed that, unconditionally, \( c_E \) is positive if and only if \( \mathbb{Q}(E[2]) \neq \mathbb{Q} \).

There are several unconditional estimates for \( \pi_c(x, E) \). For any elliptic curve \( E/\mathbb{Q} \), in [17], Gupta and M. R. Murty proved that the number of primes \( p \leq x \) with cyclic \( E(F_p) \) is \( \gg x/(\log x)^2 \). Also, in [37], M. R. Murty removed the assumption of GRH in Serre’s theorem for CM elliptic curves by invoking Wilson’s Bombieri–Vinogradov theorem for number fields [51] (without giving an error term). Moreover, by a more elementary sieve method (particularly, without using Wilson’s theorem), Cojocaru [9] established that for any CM elliptic curve \( E/\mathbb{Q} \),

\[
\pi_c(x, E) = c_E \text{Li}(x) + O\left(\frac{x \log \log x}{(\log x) \log((\log x)/N_E^2)}\right),
\]

uniformly in \( N_E \leq (\log x)^D \), where the implied constant only depends on \( A \) and \( D \).

The main theme of this paper is to study the above-discussed “cyclicity problem” of elliptic curves for “short intervals”. To motivate and state this properly, we shall recall that a strong form of the prime number theorem asserts that for any \( A > 0 \),

\[
\pi(x) = \text{Li}(x) + O\left(\frac{x}{(\log x)^A}\right),
\]

which implies that for any \( A > 0 \),

\[
\pi(2x) - \pi(x) = \text{Li}(2x) - \text{Li}(x) + O\left(\frac{x}{(\log x)^A}\right).
\]

In much the same spirit, observing that from (1.3), it follows that for \( A > 0 \),

\[
\pi_c(2x, E) - \pi_c(x, E) = c_E (\text{Li}(2x) - \text{Li}(x)) + O_A\left(\frac{x}{(\log x)^A}\right),
\]

where the implied constant is absolute.

This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.
we see that
\[ \frac{\pi_c(2x, E) - \pi_c(x, E)}{\pi(2x) - \pi(x)} \sim c_E \]
as \( x \to \infty \). In other words, the “density” of primes \( p \) with cyclic \( \bar{E}(\mathbb{F}_p) \) in \((x, 2x] \)
is \( c_E \).

There is a more difficult question concerning the distribution of primes in short intervals when \((x, 2x] \)
is replaced by \((x, x + h] \) for some \( x^{1-\delta} \leq h \leq x \) with \( \delta \in [0, 1) \). Assuming the Riemann hypothesis, one can show that for any \( A > 0 \),
\[ (1.4) \quad \pi(x + h) - \pi(x) = \text{Li}(x + h) - \text{Li}(x) + O\left( \frac{h}{(\log x)^A} \right) \]
whenever \( x^{1-\delta} \leq h \leq x \) with \( \delta \in [0, \frac{1}{2}) \). While the Riemann hypothesis is currently out of reach, a result of M. N. Huxley [24] shows that (1.4) is valid for \( x^{1-\delta} \leq h \leq x \) with \( \delta \in [0, \frac{5}{12}] \) (see Section 2 for a more detailed discussion and references therein).

A natural question, regarding the density of primes \( p \) with cyclic \( \bar{E}(\mathbb{F}_p) \) in short intervals, then arises. By the virtue of (1.2), if one is willing to assume GRH, then for any \( \delta \in [0, \frac{1}{2}) \) and \( x^{1-\delta} \leq h \leq x \), one has
\[ \pi_c(x + h, E) - \pi_c(x, E) = c_E(\text{Li}(x + h) - \text{Li}(x)) + O\left( (\log N_E)^{1/2} \frac{h}{(\log x)^A} \right) \]
for any \( A > 0 \). As it is apparent that we are far from proving GRH, the object of this paper is to prove the following unconditional estimate for the cyclicity of CM elliptic curves modulo \( p \) in short intervals.

**Theorem 1.1.** Let \( E \) be an elliptic curve defined over \( \mathbb{Q} \) of conductor \( N_E \) and with complex multiplication by the ring of integers \( \mathcal{O}_K \) of an imaginary quadratic field \( K \). Let \( A > 0 \), and let \( 0 \leq \delta < \frac{1}{25} \). Then for any \( x^{1-\delta} \leq h \leq x \), we have
\[ \pi_c(x + h, E) - \pi_c(x, E) = c_E(\text{Li}(x + h) - \text{Li}(x)) + O\left( N_E(\log N_E) \frac{h}{(\log x)^A} \right), \]
where \( \pi_c(x, E) \) is defined as in (1.1), the implied constant depends on \( \mathbb{Q}(E[2]) \) and \( A \).

In a slightly different vein, there is a question closely related to the cyclicity problem of elliptic curves. We recall that for any prime \( p \) of good reduction, it is known that
\[ \bar{E}(\mathbb{F}_p) \simeq \mathbb{Z}/d_p \mathbb{Z} \oplus \mathbb{Z}/e_p \mathbb{Z} \]
with \( d_p \mid e_p \). (The integer \( e_p \) is often called the exponent of \( \bar{E}(\mathbb{F}_p) \), which is the largest possible order of points on \( \bar{E}(\mathbb{F}_p) \).) In light of studying the cyclicity of \( \bar{E}(\mathbb{F}_p) \), one may be curious about the behaviours of \( d_p \) and \( e_p \). For instance, in [15], Freiberg and Kurlberg started the investigation of the average order of \( e_p \). More precisely, they considered
\[ (1.5) \quad \pi_c(x, E) = \sum_{p \leq x} e_p \]
and showed that under GRH,
\[ \pi_c(x, E) = c_E \text{Li}(x^2) + O(x^{19/10}(\log x)^{6/5}), \]
where
\[ \epsilon_E = \sum_{m=1}^{\infty} \frac{1}{[Q(E[m]) : Q]} \sum_{d|m} \frac{\mu(d)}{e}, \]
and that
\[ \pi_e(x, E) = \epsilon_E \text{Li}(x^2) + O\left(\frac{x^2 \log \log \log x}{(\log x)(\log \log x)}\right), \]
unconditionally, if \( E/\mathbb{Q} \) is a CM elliptic curve. These estimates have been improved by Wu [52], who shows that the errors in the above estimates can be reduced to \( O(x^{11/6}(\log x)^{1/3}) \) and \( O(x^2/(\log x)^{15/14}) \), respectively. After the work of Freiberg, Kurlberg, and Wu, by invoking Huxley’s Bombieri–Vinogradov theorem for number fields [23] as in [1], Kim [29] derived that if \( E/\mathbb{Q} \) is a CM elliptic curve with complex multiplication by \( \mathcal{O}_K \), then for any \( A, D > 0 \),
\[ (1.6) \]
\[ \pi_e(x, E) = \epsilon_E \text{Li}(x^2) + O_{A,D}\left(\frac{x^2}{(\log x)^A}\right), \]
uniformly in \( N_E \leq (\log x)^D \), where the implied constant only depends on \( A \) and \( D \). Similar to the cyclicity problem of elliptic curves for short intervals, one may also study the average order of \( \epsilon_p \) in short intervals. By (1.6), we know that
\[ \pi_e(2x, E) - \pi_e(x, E) = \epsilon_E(\text{Li}((2x)^2) - \text{Li}(x^2)) + O_{A,D}\left(\frac{x^2}{(\log x)^A}\right) \]
if \( E \) is with CM. Also, by the above-mentioned result of Wu, assuming GRH, one has
\[ \pi_e(x+h, E) - \pi_e(x, E) = \epsilon_E(\text{Li}((x+h)^2) - \text{Li}(x^2)) + O\left(\frac{xh}{(\log x)^A}\right) \]
for any \( A > 0 \) and \( x^{1-\delta} \leq h \leq x \) with \( \delta \leq [0, \frac{1}{6}] \). In this article, we shall prove the following unconditional estimate for the average exponent of CM elliptic curves modulo \( p \) in short intervals.

**Theorem 1.2.** Let \( E \) be an elliptic curve defined over \( \mathbb{Q} \) of conductor \( N_E \) and with complex multiplication by \( \mathcal{O}_K \). Let \( A > 0 \), and let \( 0 \leq \delta < \frac{1}{29} \). Then for any \( x^{1-\delta} \leq h \leq x \), we have
\[ \pi_e(x+h, E) - \pi_e(x, E) = \epsilon_E(\text{Li}((x+h)^2) - \text{Li}(x^2)) + O\left(\frac{xh}{(\log x)^A}\right), \]
where \( \pi_e(x, E) \) is defined as in (1.3), and the implied constant depends on \( \mathbb{Q}(E[2]) \) and \( A \).

Furthermore, one may study the prime divisors of \( |\tilde{E}(\mathbb{F}_p)| \) and \( \epsilon_p \) as follows. Let \( \omega(n) \) be the number of distinct prime divisors of \( n \in \mathbb{N} \). We recall that a theorem of Turán [49] states that
\[ \sum_{n \leq x} (\omega(n) - \log \log x)^2 = O(x \log \log x), \]
which implies a theorem of Hardy and Ramanujan [18] asserting that the normal order of \( \omega(n) \) is \( \log \log n \). In 1935, Erdős [14] obtained a prime analogue of Turán’s theorem by showing that
\[ \sum_{p \leq x} (\omega(p-1) - \log \log x)^2 = O\left(\frac{x}{\log x}(\log \log x)\right). \]
Moreover, several “non-abelian” analogues were studied by M. R. Murty-V. K. Murty [38] for Fourier coefficients of modular forms and by Liu [32] and Miri-V. K. Murty [35] for elliptic curves. In particular, Liu showed that for any CM elliptic curve $E/\mathbb{Q}$,

\begin{equation}
\sum_{p \leq x} (\omega(|\bar{E}(\mathbb{F}_p)|) - \log \log x)^2 = O\left(\frac{x}{\log x} (\log \log x)\right) .
\end{equation}

As $d_p | e_p$, it follows that

\begin{equation}
\sum_{p \leq x} (\omega(e_p) - \log \log x)^2 = O\left(\frac{x}{\log x} (\log \log x)\right).
\end{equation}

Similar to the cyclicity problem of elliptic curves in short intervals, one may rewrite (1.7) as

\begin{equation}
\sum_{x < p \leq 2x} (\omega(|\bar{E}(\mathbb{F}_p)|) - \log \log x)^2 = O\left(\frac{h}{\log x} (\log \log x)\right),
\end{equation}

and ask for the validity for such an estimate over short intervals. In Section 6, we shall prove the following short interval variant of Liu’s result.

**Theorem 1.3.** Let $E$ be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by $\mathcal{O}_K$. Let $\delta \in [0, \frac{1}{5})$. Then for any $x^{1-\delta} \leq h \leq x$, we have

\begin{equation}
\sum_{x < p \leq x+h} (\omega(|\bar{E}(\mathbb{F}_p)|) - \log \log x)^2 = O\left(\frac{h}{\log x} (\log \log x)\right),
\end{equation}

where the implied constant is independent of $E$.

**Corollary 1.3.1.** Let $E$ be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by $\mathcal{O}_K$. Let $\delta \in [0, \frac{1}{5})$. Then for any $x^{1-\delta} \leq h \leq x$, we have

\begin{equation}
\sum_{x < p \leq x+h} (\omega(e_p) - \log \log x)^2 = O\left(\frac{h}{\log x} (\log \log x)\right),
\end{equation}

where the implied constant is independent of $E$.

The proofs of our theorems are adaptations of the arguments of Akbary-V. K. Murty [1], Kim [29], Liu [32], and M. R. Murty [37]. While the original arguments rely on the Bombieri–Vinogradov theorems for number fields of Huxley [23] and Wilson [51], we require the following short interval variant of the work of Huxley and Wilson to control the “initial range” of the splitting of $1 \leq m \leq 2\sqrt{x}$ of Cojocaru and M. R. Murty [10, Eq. (10)] as adapted by Wu [52] (see also (4.1) and (5.1) in Sections 4 and 5, respectively), as well as bounding the contribution of “small” prime divisors in Section 6. (Let $F$ be a number field, and let $\mathcal{O}_F$ be its ring of integers. Throughout our discussion, for any coprime integral ideals $a$ and $q$ of $F$, we set

\begin{equation}
\pi(x, q, a) = \# \{ p \subset \mathcal{O}_F \mid N(p) \leq x \text{ and } p \sim a \pmod{q}\},
\end{equation}

where $p \sim a \pmod{q}$ means that $p$ and $a$ belong to the same ray class of the ray class group modulo $q$.)
Theorem 1.4. Let $F$ be a number field of degree $n_F$. For $0 \leq \delta < \frac{2}{5n_F}$, we fix $0 \leq \theta < \frac{1}{5n_F+10}(2 - 5n_F\delta)$. Then for any $x^{1-\delta} \leq h \leq x$ and $A > 0$, we have

$$\sum_{N(q) \leq x^\theta} \frac{h(q)}{\phi(q)} \max_{(a,q) = 1} \max_{y \leq h} \left| \pi(N + y, q, a) - \pi(N, q, a) - \frac{1}{h(q)}(\text{Li}(N + y) - \text{Li}(N)) \right| \ll \frac{h}{(\log x)^A},$$

where, as later, $h(q)$ denotes the cardinality of the ray class group modulo $q$, $\phi(q)$ is the number field analogue of Euler’s totient function, and $N \sim x$ means that $\frac{1}{2}x \leq N \leq x$, and the implied constant depends on $F$ and $A$.

We note that this theorem gives a version, generalised to ray class groups, of the previous work of Heath-Brown [20] and Sokolovskii [46] on the prime ideal theorem in short intervals.

Remark 1.5. It may be possible that the dependence of $Q(E[2])$ in Theorems 1.1 and 1.2 can be made explicit and that unconditional estimates of the cyclicity and average exponent of non-CM elliptic curves modulo $p$ in short intervals can be derived. Also, the ranges of $\delta$ and $\theta$ in Theorem 1.4 (and thus Theorems 1.1, 1.2, and 1.3) may be improved by adapting Timofeev’s method [48], and the dependence of $F$ in Theorem 1.4 may be tracked. However, it is apparent that these directions involve more sophisticated methods than the ones presented in the article. Nonetheless, as the work of Huxley [23] and Wilson [51] have been utilised to study certain “prime-counting problems” related to CM elliptic curves, and several applications of the Bombieri–Vinogradov type estimates in short intervals have been obtained (see, e.g., [25] and [47]), it shall be reasonable to expect that Theorem 1.4 has more applications to arithmetic. We reserve these studies to future research.

This paper is arranged as follows. In Section 2, we will discuss the Bombieri–Vinogradov theorem in short intervals and its variants and then prove Theorem 1.4. Preliminaries on CM elliptic curves will be given in Section 3. We will prove Theorems 1.1, 1.2, and 1.3 in Sections 4, 5, and 6, respectively.

2. A variant of the Bombieri–Vinogradov theorem in short intervals

For any $(a, q) = 1$, we set

$$\pi(x, q, a) = \# \{p \leq x \mid p \equiv a \pmod{q} \}.$$

We shall recall Huxley’s Bombieri–Vinogradov theorem for number fields. For any coprime ideals \( a \) and \( q \) in \( \mathcal{O}_F \), we set
\[
\pi(x, q, a) = \# \{ p \in \mathcal{O}_F \mid N(p) \leq x \text{ and } p \sim a \pmod{q} \},
\]
where \( p \sim a \pmod{q} \) means that \( p \) and \( a \) belong to the same ray class of the ray class group modulo \( q \). (For the background on ray class groups, we refer the reader to Landau’s classical paper [30] and Childress’s book [7, Ch. 3].) In [23], Huxley proved the following Bombieri–Vinogradov theorem for number fields, which improves the previous result of Wilson [51].

**Theorem 2.1** (Huxley). Let \( F \) be a number field. Then for any \( A > 0 \), there is \( B = B(A) > 0 \) such that for \( Q \leq x^{1/2}/(\log x)^B \), one has
\[
\sum_{N(q) \leq Q} \frac{h(q)}{\phi(q)} \max_{a,q = 1} \max_{y \leq x} \left| \pi(y, q, a) - \frac{1}{h(q)} \operatorname{Li}(y) \right| \ll_{F,A} \frac{x}{(\log x)^A},
\]
where \( h(q) \) is the cardinality of the ray class group modulo \( q \), and \( \phi(q) \) is the number field analogue of Euler’s totient function.

Let \( h_F \) denote the class number of \( F \), and let \( r_1 \) be the number of real places of \( F \). We note that as
\[
h(q) = \frac{h_F^{2r_1} \phi(q)}{T(q)},
\]
where \( T(q) \) is the number of residue classes \(( \text{mod } q) \) that contain a unit (see [51, Eq. (7)]), one can replace \( \frac{h(q)}{\phi(q)} \) in the estimate by \( \frac{1}{T(q)} \). Also, if \( F \) is an imaginary quadratic field, then \( T(q) \leq 6 \), and hence the factor \( \frac{h(q)}{\phi(q)} \) can be removed from the estimate in this case.

Let \( L/F \) be a Galois extension of number fields with Galois group \( G \) and absolute discriminant \( d_K \). Let \( C \) be a conjugacy class in \( G \). Let \( H \) be the largest abelian subgroup of \( G \) satisfying \( H \cap C \neq \emptyset \), and let \( E = L^H \) be the fixed field of \( H \). M. R. Murty and Petersen [40] extended previous work of M. R. Murty-V. K. Murty [39] by showing that for any \( \epsilon, A > 0 \),
\[
(2.2) \quad \sum_{q \leq Q} \max_{(a,q) = 1} \max_{y \leq x} \left| \pi_C(y, q, a) - \frac{1}{\phi(q)} \left( \frac{|C|}{|G|} \right) \operatorname{Li}(y) \right| \ll_{\epsilon,L,A} \frac{x}{(\log x)^A},
\]
where \( Q = x^{\theta - \epsilon} \), \( \theta = \theta(G) = \min\left\{ \frac{1}{|n_E - 1|}, \frac{1}{2} \right\} \),
\[
\pi_C(x, q, a) = \sum_{N(p) \leq x} \delta_C(p),
\]
\( \delta_C \) denotes the indicator function for the unramified primes \( p \) of \( L/F \) with Artin symbol \( \sigma_p = C \), and the implied constant depends on \( \epsilon \), \( L \), and \( A \). (See [39,40] for a discussion of Artin symbols and the Chebotarev density theorem.)

As mentioned in the introduction, a sharp form of the prime number theorem in short intervals was established by Huxley [24]. This has been further extended by Timofeev [48], who proved the following Bombieri–Vinogradov theorem in short intervals. (We note that such a theorem has been studied by Jutila [27], Huxley-Iwaniec [25], Ricci [43], Perelli-Pintz-Salerno [41,42], and Zhan [53].)
Theorem 2.2 (Timofeev). Let $0 \leq \delta < \frac{5}{12}$, and let

\begin{equation}
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}
\end{equation}

Then for any $x^{1-\delta} \leq h \leq x$ and $A > 0$, one has

\[
\sum_{q \leq x^{\theta}} \max_{(a,q)=1} \max_{y \leq h \sim x} \left| \pi(N + y, q, a) - \pi(N, q, a) - \frac{1}{\phi(q)}(\text{Li}(N + y) - \text{Li}(N)) \right| \ll A \frac{h}{(\log x)^A},
\]

where the implied constant depends on $A$.

We further recall that by the zero density estimates and zero-free regions for Dedekind zeta functions due to Heath-Brown [20] and Mitsui [34], Balog and Ono [2] showed that if $0 \leq \delta < \begin{cases} \frac{3}{8} & \text{if } [L : \mathbb{Q}] = 2, \\ 1/[L : \mathbb{Q}] & \text{if } [L : \mathbb{Q}] \geq 3, \end{cases}$ and $x^{1-\delta} \leq h \leq x$, then

\[
\pi_C(x + h, 1, 1) - \pi_C(x, 1, 1) \sim \frac{|C|}{|G|} (\text{Li}(x + h) - \text{Li}(x)).
\]

(Note that by Theorem 2.2 if $[L : \mathbb{Q}] = 1$, then any $\delta \in [0, \frac{5}{12})$ is admissible.) Recently, Thorner [47] obtained the following common generalisation of the work of Balog-Ono [2] and M. R. Murty-Petersen [40].

Theorem 2.3 (Thorner). For $0 \leq \delta < \frac{2}{5n_E}$, let $0 \leq \theta < \frac{1}{15n_E} (2 - 5n_E \delta)$. Then for any $x^{1-\delta} \leq h \leq x$ and $A > 0$, one has

\[
\sum_{q \leq x^{\theta}} \max_{(a,q)=1} \max_{y \leq h \sim x} \left| \pi_C(N + y, q, a) - \pi_C(N, q, a) - \frac{1}{\phi(q)} \frac{|C|}{|G|} (\text{Li}(N + y) - \text{Li}(N)) \right| \ll \frac{h}{(\log x)^A},
\]

where the sum is over $q$ coprime to $d_L$, and the implied constant depends on $L$ and $A$.

Now we shall prove our variant of Bombieri–Vinogradov theorem in short intervals, i.e., Theorem 1.4. As shall be seen, our argument consists of two parts. We shall first remove the contribution of the imprimitive Hecke characters by adapting the reduction methods used by Gallagher [16], Murty-Petersen [40], and Wilson [51]. After the reduction, similar to the argument of Huxley-Iwaniec [25] and Thorner [47], we will invoke the zero-free region for Hecke L-functions derived by Bartz [2], Siegel’s theorem for number fields established by Mitsui [33], and the zero-density estimates for Hecke L-functions derived by Hinz [21] and Montgomery [36] to deduce Theorem 1.4.

Proof of Theorem 1.4 For any coprime ideals $a$ and $q$ in $\mathcal{O}_F$, we consider the prime-counting function

\[
\tilde{\psi}(x, q, a) = \sum_{\substack{N(p) \leq x \\ p \sim a}} \log N(p),
\]
where \( p \sim a \pmod{q} \) means that \( p \) and \( a \) belong to the same ray class of the ray class group modulo \( q \). By Abel’s summation, to prove Theorem 1.3, it suffices to show that for any \( x^{1-\delta} \leq h \leq x \) and \( A > 0 \), one has

\[
(2.4) \quad \sum_{N(q) \leq x^\theta} \frac{h(q)}{\phi(q)} \max_{(a,q)=1} \max_{y \leq h} \max_{N \sim x} \left| \psi(N + y, q, a) - \psi(N, q, a) - \frac{1}{h(q)}y \right| \ll \frac{h}{(\log x)^A}
\]

whenever \( 0 \leq \theta < \frac{1}{5n_F+10}(2 - 5n_F\delta) \) and \( \delta \in [0, \frac{2}{5n_F}) \).

For any Hecke character \( \chi \pmod{q} \), we define

\[
\psi(x, \chi) = \frac{1}{2\pi i} \int_{(2)} \frac{L'(s)}{L(s, \chi)} x^s ds,
\]

where the integral is over the line \( \Re(s) = 2 \), and \( L(s, \chi) \) is the Hecke L-function attached to \( \chi \). We further set

\[
(2.5) \quad \psi(x, q, a) = \frac{1}{h(q)} \sum_{\chi \pmod{q}} \overline{\chi}(a) \psi(x, \chi).
\]

A direct calculation shows that

\[
\psi(x, q, a) - \psi(x, q, a) \ll \sum_{N(p) \leq x \atop (p, q) \neq 1} \log N(p) + \sum_{N(p^m) \leq x \atop m \geq 2} \log N(p) \ll (\log x)(\log N(q) + x^{\frac{1}{2}}).
\]

Therefore, to derive (2.4), it suffices to show that

\[
(2.7) \quad \sum_{N(q) \leq x^\theta} \frac{h(q)}{\phi(q)} \max_{(a,q)=1} \max_{y \leq h} \max_{N \sim x} \left| \psi(N + y, q, a) - \psi(N, q, a) - \frac{1}{h(q)}y \right| \ll \frac{h}{(\log x)^A}.
\]

Note that by (2.3), we have

\[
(2.6) \quad \left| \psi(N + y, q, a) - \psi(N, q, a) - \frac{1}{h(q)}y \right| \leq \frac{1}{h(q)} \left( \left| \psi(N + y, \chi_0) - \psi(N, \chi_0) - y \right| + \sum_{\chi \neq \chi_0} \left| \psi(N + y, \chi) - \psi(N, \chi) \right| \right),
\]

where \( \chi_0 \) denotes the trivial character, and the second sum is over the nontrivial character \( \chi \pmod{q} \). Let \( \chi^* \pmod{q^*} \) be the Hecke character inducing \( \chi \pmod{q} \). Then

\[
\psi(x, \chi) - \psi(x, \chi^*) \ll \sum_{N(p^m) \leq x \atop p | q} \log N(p) \ll (\log x) \log N(q),
\]

and hence for any fixed modulus \( q \) with \( N(q) \leq x \),

\[
(2.7) \quad \frac{1}{h(q)} \sum_{\chi \neq \chi_0} \max_{y \leq h} \max_{N \sim x} \left| \psi(N + y, \chi) - \psi(N, \chi) \right| \ll \frac{1}{h(q)} \sum_{\chi \neq \chi_0} \max_{y \leq h} \max_{N \sim x} \left| \psi(N + y, \chi^*) - \psi(N, \chi^*) \right| + O\left((\log x)^2 \sum_{\chi} \frac{1}{h(q)}\right),
\]

where \( \circ \) indicates that the sum is only over imprimitive characters modulo \( q \).
Let \( 0 \leq Q_1 \leq x \), and set

\[
S(Q_1) = \sum_{N(q) \leq Q_1} \frac{h(q)}{\phi(q)} \frac{1}{h(q)} \sum_{\chi \neq \chi_0} \max_{y \leq h} \max_{N \sim x} |\psi(N + y, \chi) - \psi(N, \chi)|.
\]

From (2.7), it follows that

\[
S(Q_1) = \sum_{N(q) \leq Q_1} \frac{1}{\phi(q)} \sum_{\chi \neq \chi_0} \max_{y \leq h} \max_{N \sim x} |\psi(N + y, \chi^*) - \psi(N, \chi^*)| \sum_{N(q) \leq Q_1} \frac{1}{\phi(q)}
\]

\[+ O\left( (\log x)^2 \sum_{N(q) \leq Q_1} \sum_{\chi \neq \chi_0} \max_{y \leq h} \max_{N \sim x} \frac{1}{\phi(q)} \right),
\]

Rewriting this as sums over the conductors of \( \chi \) (instead of over the moduli of imprimitive characters), we have

\[
S(Q_1) = \sum_{1 < N(q^*) \leq Q_1} \sum'_{\chi^* \pmod{q^*}} \max_{y \leq h} \max_{N \sim x} |\psi(N + y, \chi^*) - \psi(N, \chi^*)| \sum_{N(q) \leq Q_1} \frac{1}{\phi(q)}
\]

\[+ O\left( (\log x)^2 \sum_{N(q^*) \leq Q_1} \sum'_{\chi^* \pmod{q^*}} \sum_{N(q) \leq Q_1} \frac{1}{\phi(q)} \right),
\]

where the primed sums are over the primitive characters. Since there are \( h(q) \) Hecke characters modulo \( q \), \( h(q) \ll \phi(q) \), and

\[
\sum_{N(q) \leq Q_1} \frac{1}{\phi(q)} \ll \frac{\log Q_1}{\phi(q^*)}
\]

(see [51] pp. 199–200), we derive

\[
S(Q_1) \ll (\log Q_1) \sum_{1 < N(q^*) \leq Q_1} \frac{1}{\phi(q^*)} \sum'_{\chi^* \pmod{q^*}} \max_{y \leq h} \max_{N \sim x} |\psi(N + y, \chi^*) - \psi(N, \chi^*)|
\]

\[+ O((\log x)^3 Q_1).
\]

Thus, upon replacing \( q^* \) and \( \chi^* \) by \( q \) and \( \chi \) for the sums in (2.8), respectively, putting (2.6) and (2.8) together, we obtain

\[
\sum_{N(q) \leq Q_1} \frac{h(q)}{\phi(q)} \max_{(a,q) = 1} \max_{y \leq h} \max_{N \sim x} |\psi(N + y, q, a) - \psi(N, q, a) - \frac{1}{h(q)} y|
\]

\[\ll \sum_{N(q) \leq Q_1} \frac{1}{\phi(q)} \max_{y \leq h} \max_{N \sim x} |\psi(N + y, \chi_0) - \psi(N, \chi_0) - y| + S(Q_1)
\]

\[
\ll (\log Q_1) \sum_{N(q) \leq Q_1} \frac{1}{\phi(q)} \sum'_{\chi \pmod{q}} \max_{y \leq h} \max_{N \sim x} |\psi(N + y, \chi) - \psi(N, \chi) - \delta(\chi) y|
\]

\[+ O((\log x)^3 Q_1),
\]

where \( \delta(\chi) \) is the indicator function of the trivial character \( \chi_0 \).
By [28, Eq. (5.53)], for $2 \leq T \leq x$ and $\chi \pmod{q}$ with $N(q) \leq Q_1 \leq x$, we have
\[
\psi(N + y, \chi) - \psi(N, \chi) - \delta(\chi)y \ll \sum_{\rho = \beta + i\gamma \atop |\gamma| \leq T} \left| \frac{(N + y)^\rho - N^\rho}{\rho} \right| + O\left(\frac{x(\log x)^2}{T}\right),
\]
where the sum is over nontrivial zeros $\rho$ of $L(s, \chi)$. Since
\[
\left| \frac{(N + y)^\rho - N^\rho}{\rho} \right| = \left| \int_N^{N+y} t^{\rho-1} dt \right| \leq \int_N^{N+y} t^{\beta-1} dt \leq yN^{\beta-1} \ll hx^{\beta-1},
\]
we have
\[
\psi(N + y, \chi) - \psi(N, \chi) - \delta(\chi)y \ll h \sum_{\rho = \beta + i\gamma \atop |\gamma| \leq T} x^{\beta-1} + O\left(\frac{x(\log x)^2}{T}\right).
\]
Hence, we obtain the estimate
\[
\sum_{N(q) \leq Q_1} \frac{1}{\phi(q)} \sum_{\chi \pmod{q}}' \max_{y \leq h} \max_{N \sim x} |\psi(N + y, \chi) - \psi(N, \chi) - \delta(\chi)y| 
\ll h \sum_{N(q) \leq Q_1} \frac{1}{\phi(q)} \sum_{\chi \pmod{q}}' \sum_{\rho = \beta + i\gamma \atop |\gamma| \leq T} x^{\beta-1} + \frac{Q_1x(\log x)^2}{T}.
\]

Now we are in a position to proceed with the “dyadic argument” as in [40, Lemma 1.7], which requires the estimate
\[
\frac{1}{\phi(q)} \ll \frac{\log \log N(q)}{N(q)}.
\]
As it seems hard to find such an estimate in the literature, we shall give a proof here (which, in fact, follows from the argument in [19, Sec. 22.9] and a result of Rosen [44]).

**Proof of the estimate (2.11).** Fix $q$. Let $p_1, p_2, \ldots, p_{r-k}$ be the primes which divide $q$ and are with norm not exceeding $\log N(q)$, and let $p_{r-k+1}, \ldots, p_r$ be those which divide $q$ and are with norm greater than $\log N(q)$. Then we have
\[
(\log N(q))^k \leq N(p_{r-k+1}) \cdots N(p_r) \leq N(q)
\]
and hence
\[
k \leq \log N(q)/\log \log N(q).
\]
Thus, we have
\[
\frac{\phi(q)}{N(q)} = \prod_{i=1}^r \left(1 - \frac{1}{N(p_i)}\right) \geq \left(1 - \frac{1}{\log N(q)}\right)^{\log N(q)/\log \log N(q)} \prod_{N(p) \leq \log N(q)} \left(1 - \frac{1}{N(p)}\right).
\]
As $(1 - x^{-1})x/\log x \sim 1$, and Rosen’s generalisation of Mertens’s theorem asserts that
\[
\prod_{N(p) \leq x} \left(1 - \frac{1}{N(p)}\right)^{-1} \sim \alpha_F(\log x)
\]
for some (explicit) constant $\alpha_F$ depending on $F$ (see [44, Theorem 2]), we obtain (2.11). \qed
Following the argument of [40, Lemma 1.7], we split $[1, Q_1]$ into intervals of the form $[\frac{Q}{2}, Q]$ that $Q = 2^{m+1}$ and $m \in \{0, \ldots, \lfloor \log_2 Q_1 \rfloor \}$. This dyadic consideration and (2.11) majorise the triple sum in (2.10) by

$$
(\log Q_1) \max_{Q \leq Q_1} \sum_{\frac{Q}{2} \leq N(q) \leq Q} \frac{\log \log N(q)}{N(q)} \sum_{\chi \mod q}^' \sum_{\rho = \beta + i\gamma \atop |\gamma| \leq T} x^{\beta - 1} \ll (\log Q_1)(\log \log Q_1) \max_{Q \leq Q_1} \frac{1}{Q} \sum_{\frac{Q}{2} \leq N(q) \leq Q} \sum_{\chi \mod q}^' \sum_{\rho = \beta + i\gamma \atop |\gamma| \leq T} x^{\beta - 1},
$$

(2.12)

where the last sum is over nontrivial zeros $\rho$ of $L(s, \chi)$.

For $\sigma \in [\frac{3}{4}, 1]$, we set $N_\chi(\sigma) = \# \{\rho = \beta + i\gamma \mid L(\rho, \chi) = 0, \sigma \leq \beta, |\gamma| \leq T\}$, and for $Q \leq Q_1$, we let

$$
N(\sigma, Q, T) = \sum_{N(q) \leq Q, \chi \mod q} \sum_{\rho = \beta + i\gamma \atop |\gamma| \leq T} N_\chi(\sigma, T).
$$

We recall that by the zero-free region for Hecke L-functions established by Bartz [33], there is a constant $c_F$, depending on $F$, such that $N(\sigma, Q, T)$ is either 0 or 1 whenever

$$
1 - C_F(x, Q) < \sigma \leq 1,
$$

where

$$
C_F(x, Q) = \frac{c_F}{\max \{\log Q, (\log x)^{3/4}\}}.
$$

We note that for $1 - C_F(x, Q) < \sigma \leq 1$, if $N(\sigma, Q, T) = 1$, then it is contributed by the Siegel zero $\beta_1$ of an exceptional Hecke L-function attached to a real Hecke character modulo $q_1$ (with $N(q_1) \leq Q$). Invoking Siegel’s theorem for number fields established by Mitsui [33] Sec. 1, Lemma 12] to bound $\beta_1$, one has

$$
\frac{1}{Q} x^{\beta_1 - 1} \ll \begin{cases} 
(\log x)^{-A+4} & \text{if } 1 \leq Q < (\log x)^{A+4}, \\
(\log x)^{-A+4} x^0 & \text{if } (\log x)^{A+4} \leq Q 
\end{cases}
$$

(2.13)

(here we use the trivial bounds $1/Q \leq 1$ and $\beta_1 - 1 \leq 0$ for the first and second estimates, respectively). Thus, to bound the last triple sum in (2.12), it suffices to consider

$$
\sum_{N(q) \leq Q} \sum_{\chi \mod q}^' \sum_{\rho = \beta + i\gamma \atop |\gamma| \leq T} x^{\beta - 1} \ll (\log x) \max_{\frac{1}{2} \leq \sigma \leq 1 - C_F(x, Q)} x^{\sigma - 1} N(\sigma, Q, T).
$$

Furthermore, we recall that from the work of Hinz [21] Sätze A und B] (for general $F$) and Montgomery [36 Theorem 12.2] (for $n_F = 1$), it follows that for $2 \leq T \leq x$, $1 \leq Q \leq Q_1$, and $\frac{1}{2} \leq \sigma \leq 1$,

$$
N(\sigma, Q, T) \ll (Q^2 T^{n_F})^{\frac{5}{2} (1 - \sigma)} (\log QT)^{9n_F + 10},
$$

which implies that

$$
\max_{\frac{1}{2} \leq \sigma \leq 1 - C_F(x, Q)} x^{\sigma - 1} N(\sigma, Q, T) \ll (\log x)^{9n_F + 10} \max_{\frac{1}{2} \leq \sigma \leq 1 - C_F(x, Q)} (x^{-1} Q_1^n T^{\frac{5}{2} n_F})^{1 - \sigma}.
$$
Now, for $0 \leq \delta < \frac{2}{5n_F}$ and sufficiently small $\epsilon > 0$, we choose
\[ Q_1 = x^{\frac{1}{m_F + m} (2 - 5n_F \delta - 2\epsilon)} (\log x)^{-n_F \frac{A+3}{p+2}} \] and $T = x^{\frac{2}{m_F + m} (1 + 5\delta - \epsilon)} (\log x)^{\frac{2(A+3)}{p+2}}$, which give
\[ Q_1^{5T} T^2 n_F = x^{1-\epsilon}. \]
From the definition of $C_F(x, Q)$, it follows that $x^{-\epsilon C_F(x, Q)} \ll (\log x)^{-\left(9n_F + 14 + \epsilon\right)}$ if $1 \leq Q \leq \exp((\log x)^{3/4})$ and that $x^{-\epsilon C_F(x, Q)} \ll 1$ if $\exp((\log x)^{3/4}) < Q \leq Q_1$. Therefore, we deduce
\[ \max_{Q \leq Q_1} \frac{1}{Q} \max_{\frac{1}{2} \leq \sigma \leq 1-C_F(x, Q)} x^{\sigma - 1} N(\sigma, Q, T) \ll (\log x)^{9n_F + 10} \max_{Q \leq Q_1} \frac{1}{Q} x^{-\epsilon C_F(x, Q)} \ll (\log x)^{-A-4}. \]
Putting (2.10), (2.12), (2.13), (2.14), and (2.15) together, we obtain
\[ \sum_{N(q) \leq Q_1} \frac{1}{\phi(q)} \sum_{\chi \mod q} \max_{y \leq h} \max_{N \sim x} |\psi(N + y, \chi) - \psi(N, \chi) - \delta(\chi)y| \]
\[ \ll h(\log Q_1)(\log \log Q_1)(\log x)(\log x)^{-A-4} + \frac{Q_1 x(\log x)^2}{T} \]
\[ \ll \frac{h}{(\log x)^{A+1}} + \frac{x^{1-\delta}}{(\log x)^{A+1}}. \]
Finally, for $x^{1-\delta} \leq h \leq x$ with $0 \leq \delta < \frac{2}{5n_F}$, combining (2.9) and (2.16) yields
\[ \sum_{N(q) \leq x^{\theta}} \frac{h(q)}{\phi(q)} \max_{(a, q) = 1} \max_{y \leq h} \max_{N \sim x} |\psi(N + y, q, a) - \psi(N, q, a) - \frac{1}{h(q)} y| \ll \frac{h}{(\log x)^A} \]
whenever $0 \leq \theta < \frac{1}{5n_F + 10}(2 - 5n_F \delta)$, which concludes the proof. \(\square\)

**Remark 2.4.** We note that the proof presented above can be adjusted to derive a variant of the above-mentioned theorem of Thorner, Theorem 2.3, via the reduction method of Deuring [13] (which was rediscovered by MacCluer) as follows.

Let $L/F$ be a Galois extension with Galois group $G$, and let $C$ be a fixed conjugacy class in $G$. Let $H$ be the largest abelian subgroup of $G$ satisfying $H \cap C \neq \emptyset$, and let $E = L^H$ be the fixed field of $H$. For $h_C \in H \cap C$, we let $C_H$ be the conjugacy class of $h_C$ in $H$. Let $F_q$ denote the ray class field corresponding to the ray class group modulo $q$.

Assume $L \cap F_q = \emptyset$. As argued in [10] Sec. 0.5-0.7, by Mackey’s induction theorem, for any Hecke character $\chi$ modulo $q$, one has
\[ L(s, \delta_C \times \chi, L/F) = L(s, \delta_{C_H} \times \chi, L/E)^\lambda, \]
where $\delta_C$ and $\delta_{C_H}$ are the indicator functions of $C$ and $C_H$, respectively, and $\lambda = \frac{|C|}{|H|}$, and thus one can deduce
\[ \sum_{N(p^n) \leq x} \log N(p) = \frac{-1}{2\pi i} \frac{1}{h(q)} \frac{|C|}{|G|} \sum_{\chi \mod q} \chi(a) \eta(h_C) \int \frac{L'}{L}(s, \eta \times \chi) \frac{x^s}{s} ds \]
Suppose that \( N \) be an elliptic curve defined over \( \mathbb{Q} \) of conductor \( N_E \) and with complex multiplication by the ring of integers \( \mathcal{O}_K \) of an imaginary quadratic field \( K \). Let \( E[m] \) denote the set of \( m \)-torsion points of \( E \), and let \( n(m) = [\mathbb{Q}(E[m]) : \mathbb{Q}] \). By the theory of complex multiplication, M. R. Murty [37] Lemma 4] showed that there exists an ideal \( f = f_E \) such that

\[ K_m \subseteq K(E[m]) \subseteq K_{fm}, \]

where \( K_m \) and \( K_{fm} \) are the ray class fields of \( K \) of levels \( m = m\mathcal{O}_K \) and \( fm \), respectively. (As remarked in [1], \( f \) above can be taken as the conductor of the Hecke character associated to \( E \) (see [37] p. 163), and hence \( N_E = N(f)d_K \), where \( d_K \) is the absolute discriminant of \( K \). This implies that \( \phi(f) \leq N(f) \leq N_E \).) Also, M. R. Murty proved the following lemma.

**Lemma 3.1.** [37] Lemma 6] If \( m \geq 3 \), then \( K(E[m]) = \mathbb{Q}(E[m]) \).

We also require the following cyclicity criterion for elliptic curves.

**Lemma 3.2.** Suppose that \( p \nmid N_E \). Then \( E(\mathbb{F}_p) \) is cyclic if and only if \( p \) does not split completely in \( \mathbb{Q}(E[m]) \) for any square-free \( m \).
In light of this lemma, for square-free $m > 1$, we set
\[ \pi_E(x, m) = \# \{ p \leq x \mid p \nmid N_E \text{ splits completely in } \mathbb{Q}(E[m]) \} \]
and $\pi_E(x, 1) = \# \{ p \leq x \mid p \nmid N_E \}$. We recall that for any square-free $3 \leq m \leq 2\sqrt{x}$, one has
\[ \pi_E(x, m) \ll \frac{x}{m^2}, \tag{3.1} \]
where the implied constant is absolute. For the sake of convenience, we further set
\[ \mathcal{E}(x, m) = \pi_E(x, m) - \frac{1}{n(m)} \text{Li}(x). \]
It follows from the prime number theorem and (2.2) that for any $A > 0$,
\[ \mathcal{E}(x, 1) = O\left(\frac{x}{(\log x)^A}\right) \tag{3.2} \]
and
\[ \mathcal{E}(x, 2) = O_{\mathbb{Q}(E[2]), A}\left(\frac{x}{(\log x)^A}\right), \tag{3.3} \]
where the implied constant depends at most on $\mathbb{Q}(E[2])$ and $A$. Moreover, by Theorem 2.2 for any $x^{1-\delta} \leq h \leq x$ with $0 \leq \delta < \frac{5}{12}$ and $A > 0$, one has
\[ \mathcal{E}(x + h, 1) - \mathcal{E}(x, 1) = O\left(\frac{h}{(\log x)^A}\right). \tag{3.4} \]
In addition, from Theorem 2.3 it follows that for any $0 \leq \delta < \frac{1}{5}$, $x^{1-\delta} \leq h \leq x$, and $A > 0$,
\[ \mathcal{E}(x + h, 2) - \mathcal{E}(x, 2) = O\left(\frac{h}{(\log x)^A}\right), \tag{3.5} \]
where the implied constant depends on $\mathbb{Q}(E[2])$ and $A$. (Note that $[\mathbb{Q}(E[2]) : \mathbb{Q}]$ is either 1, 2, 3, or 6, as $\text{Gal}(\mathbb{Q}(E[2]) / \mathbb{Q})$ is a subgroup of $\text{GL}_2(\mathbb{Z}/2\mathbb{Z})$. Hence, $\text{Gal}(\mathbb{Q}(E[2]) / \mathbb{Q})$ is either abelian or isomorphic to $S_3$, which has an abelian subgroup of order 3.)

Lastly, we recall the following three lemmata concerning the primes that split completely in division fields of $E$ (see [1] Lemma 2.4, Lemma 2.7, and pp. 35–36 and [27] p. 159, respectively).

**Lemma 3.3.** If $m \geq 3$ is square-free, and $p \nmid 6N_E$ is a prime that splits completely in $\mathbb{Q}(E[m])$, then $p$ is ordinary.

We note that as Lemma 3.1 tells us that $K(E[m]) = \mathbb{Q}(E[m])$ for every $m \geq 3$, the lemma above yields that
\[ \pi_E(x, m) = \frac{1}{2} \bar{\pi}_E(x, m) + O\left(\frac{x^{1/2}}{\log x} + \log N_E\right), \tag{3.6} \]
where
\[ \bar{\pi}_E(x, m) = \# \{ p \subset O_K \mid N(p) \leq x \text{ and } p \nmid fm \text{ splits completely in } K(E[m]) \}. \]

**Lemma 3.4.** Let $E / \mathbb{Q}$ be of conductor $N_E$ and with CM by $O_K$. Then there exist an ideal $\mathfrak{f} = \mathfrak{f}_E$ of $O_K$ and $t(m)$ ray classes modulo $fm$ so that for any prime $p$ of $K$ with $p \nmid fm$, $p$ splits completely in $K(E[m])$ if and only if $p \sim m_i (\mod fm)$ for some $1 \leq i \leq t(m)$. Moreover, one has
\[ t(m)[K(E[m]) : K] = h(fm) \]
and

\[ t(m) \ll_K N_E(\log N_E), \]

where the implied constant depends only on \( K \).

**Lemma 3.5.** Let \( E/\mathbb{Q} \) be an elliptic curve, and let \( p \) be a prime of good reduction. Then \( p \) splits completely in \( \mathbb{Q}(E[m]) \) if and only if \( m \mid d_p \).

4. PROOF OF THEOREM 1.1

With the results stated in Sections 2 and 3 in hand, we are now in a position to prove Theorem 1.1.

Let \( \pi_c(x, E) = \# \{ p \leq x \mid p \nmid N_E \text{ and } E(\mathbb{F}_p) \text{ is cyclic} \} \). By Lemma 3.2 and the inclusion-exclusion principle, as argued in [10, Sec. 2], we have

\[ \pi_c(x, E) = \sum_{m=1}^{2\sqrt{x}} \mu(m)\pi_E(x, m). \]

By (3.1) and the fact that \( N(f) \leq N_E \), we then obtain

\[
\begin{aligned}
\pi_c(x, E) &= \sum_{1 \leq m \leq z/N(f)^{1/2}} \mu(m)\pi_E(x, m) + O \left( \sum_{z/N(f)^{1/2} \leq m \leq 2\sqrt{x}} \frac{x}{m^2} \right) \\
&= \sum_{1 \leq m \leq z/N(f)^{1/2}} \mu(m)\pi_E(x, m) + O(N_E^{1/2}xz^{-1}),
\end{aligned}
\]

where \( z = z(x) \) is a parameter, satisfying \( 3 \leq z/N(f)^{1/2} \leq 2\sqrt{x} \), to be chosen later. Thus, by (3.1), (3.3), and (4.1), we can express \( \pi_c(x + h, E) - \pi_c(x, E) \) as

\[
\begin{aligned}
\pi_E(x + h, 1) - \pi_E(x, 1) &= (\pi_E(x + h, 2) - \pi_E(x, 2)) \\
&+ \sum_{3 \leq m \leq z/N(f)^{1/2}} \mu(m)(\pi_E(x + h, m) - \pi_E(x, m)) + O(N_E^{1/2}xz^{-1}) \\
&= \left( 1 - \frac{1}{n(2)} \right)(\text{Li}(x + h) - \text{Li}(x)) + O_{Q(E[2]), A}(\frac{h}{(\log x)^A}) \\
&+ \sum_{3 \leq m \leq z/N(f)^{1/2}} \mu(m)(\pi_E(x + h, m) - \pi_E(x, m)) + O(N_E^{1/2}xz^{-1})
\end{aligned}
\]

whenever \( x^{1-\delta} \leq h \leq x \) with \( \delta \in [0, \frac{1}{2}) \). Also, by (3.6), we have

\[
\begin{aligned}
&\sum_{3 \leq m \leq z/N(f)^{1/2}} \mu(m)\pi_E(x, m) \\
&= \sum_{3 \leq m \leq z/N(f)^{1/2}} \mu(m)\left( \frac{1}{2} \bar{\pi}_E(x, m) + O\left( \frac{x^{1/2}}{\log x} + \log N_E \right) \right) \\
&= \frac{1}{2} \sum_{3 \leq m \leq z/N(f)^{1/2}} \mu(m)\left( \text{Li}(x) / [K(E[m]) : K] + \frac{1}{2} \sum_{3 \leq m \leq z/N(f)^{1/2}} \mu(m)\bar{\pi}(x, m) \right) \\
&+ O\left( \frac{x^{1/2}}{\log x} + (\log N_E)z \right),
\end{aligned}
\]

where, by Lemma 3.1, \( 2[K(E[m]) : K] = [\mathbb{Q}(E[m]) : \mathbb{Q}] \), and

\[ \bar{\pi}(x, m) = \pi_E(x, m) - \frac{\text{Li}(x)}{[K(E[m]) : K]} . \]
Note that it follows from Lemma 3.4 that
\[ \tilde{\xi}(x, m) = \pi_E(x, m) - \frac{\text{Li}(x)}{[K(E[m]) : K]} = \sum_{i=1}^{t(m)} \left( \pi(x, fm, m_i) - \frac{\text{Li}(x)}{h(fm)} \right). \]

Thus, by Theorem 1.4 (for \( z^2 \leq x^\theta \) with \( 0 \leq \theta < \frac{1}{10} (1 - 5\delta) \) and \( 0 \leq \delta < \frac{1}{5} \)), the fact that \( T(q) \leq 6 \) in our consideration, and Lemma 3.4 for any \( A > 0 \), we derive
\[ (4.4) \]
\[ \sum_{3 \leq m \leq z / N(f)^{1/2}} \left| \tilde{\xi}(x + h, m) - \tilde{\xi}(x, m) \right| \leq \sum_{3 \leq N(fm) \leq z^2} \sum_{i=1}^{t(m)} \left| \pi(x + h, fm, m_i) - \pi(x, fm, m_i) - \frac{\text{Li}(x + h) - \text{Li}(x)}{h(fm)} \right| \ll N_E(\log N_E) \sum_{N(q) \leq z^2} \max_{(a,q)=1} \left| \pi(x + h, q, a) - \pi(x, q, a) - \frac{\text{Li}(x + h) - \text{Li}(x)}{h(q)} \right| \ll A N_E(\log N_E) \frac{h}{(\log x)^A}. \]

(Since there are only nine imaginary quadratic fields \( K \) of class number 1, we may take the implied constant independent of \( K \).)

To summarise, via (4.2), (4.3), and (4.4), we have shown that \( \pi_c(x + h, E) - \pi_c(x, E) \) equals
\[ \sum_{1 \leq m \leq z / N(f)^{1/2}} \frac{\mu(m)}{n(m)} (\text{Li}(x + h) - \text{Li}(x)) + O \left( N_E^{1/2} x z^{-1} + N_E(\log N_E) \frac{h}{(\log x)^A} + \frac{x^{1/2} z}{\log x} + (\log N_E) z \right) \]
whenever \( z^2 \leq x^\theta \) and \( x^{1-\delta} \leq h \leq x \) with \( 0 \leq \theta < \frac{1}{10} (1 - 5\delta) \) and \( 0 \leq \delta < \frac{1}{5} \).

Finally, as \( n(m) = |Q(E|m)| : \mathbb{Q}| \gg \phi(m)^2 \gg \frac{m^2}{(\log \log m)^2} \) and L'Hôpital's rule gives
\[ \lim_{z \to \infty} \left( \int_{z}^{\infty} \frac{(\log t)^2}{t^2} dt \right) \left( \frac{\log z}{z} \right) = 0, \]
one has
\[ \sum_{m > z / N(f)^{1/2}} \frac{\mu(m)}{n(m)} (\text{Li}(x + h) - \text{Li}(x)) \ll \sum_{m > z / N(f)^{1/2}} \frac{(\log \log m)^2}{m^2} \frac{h}{\log x} \ll \frac{N_E^{1/2} h}{z}. \]

Herein, for any \( 0 \leq \delta < \frac{1}{25} \) and \( x^{1-\delta} \leq h \leq x \), we have
\[ \pi_c(x + h, E) - \pi_c(x, E) = \epsilon_E (\text{Li}(x + h) - \text{Li}(x)) + O \left( N_E(\log N_E) \frac{h}{(\log x)^A} \right), \]
which completes the proof.
Since Lemma 3.5, combined with (3.1), yields that the last triple sum in (5.1) is

\[
\sum \frac{1}{m} = \sum_{d|m} \frac{\mu(d)}{e},
\]

one has

\[
\sum_{p \leq x} \frac{p}{d_p} = \sum_{p \leq x} p \sum_{d|p} \frac{\mu(d)}{e} = \sum_{m \leq 2\sqrt{x}} \sum_{d|m} \frac{\mu(d)}{e} \sum_{p \leq x} \frac{p}{d_p}.
\]

Similar to [52], we consider the splitting \( m \leq z/N(f)^{1/2} \) and \( z/N(f)^{1/2} < m \leq 2\sqrt{x} \) and deduce that \( \pi_e(x, E) \) equals

\[
(5.1) \quad \sum_{m \leq z/N(f)^{1/2}} \frac{\mu(d)}{e} \sum_{p \leq x, m|d_p} p + \sum_{z/N(f)^{1/2} \leq m \leq 2\sqrt{x}} \frac{\mu(d)}{e} \sum_{p \leq x, m|d_p} p + O\left(\frac{x^{3/2}}{\log x}\right),
\]

where \( z = z(x) \) is a parameter, satisfying \( 3 \leq z/N(f)^{1/2} \leq 2\sqrt{x} \), to be chosen later.

Since

\[
\left| \sum_{d|m} \frac{\mu(d)}{e} \right| \leq 1,
\]

Lemma 8.5 combined with (5.1), yields that the last triple sum in (5.1) is

\[
\ll \sum_{z/N(f)^{1/2} \leq m \leq 2\sqrt{x}} \frac{x^2}{m^2} \ll \frac{N_E^{1/2} x^2}{z}.
\]

Let \( x^{1-\delta} \leq h \leq x \) with \( \delta \in [0, \frac{1}{5}] \). To bound the first triple sum in (5.1), we apply partial summation to express \( \sum_{p \leq x+h} p - \sum_{p \leq x} p \) as

\[
(x + h) \pi_E(x + h, m) - \int_2^{x+h} \pi_E(t, m) dt = (x \pi_E(x, m) - \int_2^x \pi_E(t, m) dt) + h \pi_E(x + h, m)
\]

\[
- \int_2^{x+h} \pi_E(t, m) dt + \int_2^x \pi_E(t, m) dt.
\]

Recalling we set \( n(m) = \lfloor Q(E[m]) : \mathbb{Q} \rfloor \) and \( \mathcal{E}(x, m) = \pi_E(x, m) - \frac{1}{n(m)} \text{Li}(x) \), we see that the expression above is equal to

\[
x \left( \frac{1}{n(m)} (\text{Li}(x + h) - \text{Li}(x)) + \mathcal{E}(x + h, m) - \mathcal{E}(x, m) \right)
\]

\[
+ h \left( \frac{1}{n(m)} \text{Li}(x + h) + \mathcal{E}(x + h, m) \right) - \int_2^{x+h} \frac{1}{n(m)} \text{Li}(t) dt + \int_2^x \frac{1}{n(m)} \text{Li}(t) dt
\]

\[
- \int_2^{x+h} \mathcal{E}(t, m) dt + \int_2^x \mathcal{E}(t, m) dt.
\]
Thus, as $\text{Li}(x^2) = x \text{Li}(x) - \int_x^z \text{Li}(t) dt + O(1)$, we have

$$
\sum_{p \leq x+h, m | d_p} p - \sum_{p \leq x, m | d_p} p = \frac{1}{n(m)} (\text{Li}((x+h)^2) - \text{Li}(x^2)) + O(1)
$$

\[ (5.2) \]

$$
+ O \left( x |\mathcal{E}(x+h, m) - \mathcal{E}(x, m) | + h \max_{x \leq t \leq x+h} |\mathcal{E}(t, m)| \right).
$$

Similar to the argument for obtaining (4.4), by Huxley’s theorem, Theorem 2.1, we have

$$
\sum_{3 \leq m \leq z / (N(f))^{1/2}} \max_{x \leq t \leq x+h} \left| \pi_E(t, m) - \frac{1}{[K(E[m]) : K]} \text{Li}(t) \right| \ll_A N_E (\log N_E) \frac{x}{(\log x)^A}
$$

whenever $z^2 \leq x^\theta$ for some $\theta \in (0, \frac{1}{2})$. This, together with (3.6) and (4.4), gives

$$
\sum_{3 \leq m \leq z / (N(f))^{1/2}} \left( x |\mathcal{E}(x+h, m) - \mathcal{E}(x, m) | + h \max_{x \leq t \leq x+h} |\mathcal{E}(t, m)| \right)
$$

\[ (5.3) \]

$$
\ll N_E (\log N_E) \frac{xh}{(\log x)^A} + \frac{x^{3/2}z}{\log x} + (\log N_E)(xz),
$$

where the implied constant depends on $A$. Therefore, by (5.2) and (5.3),

$$
\sum_{m \leq z / (N(f))^{1/2}} \sum_{d | m} \frac{\mu(d)}{e} \sum_{p \leq x+h, m | d_p} p - \sum_{m \leq z / (N(f))^{1/2}} \sum_{d | m} \frac{\mu(d)}{e} \sum_{p \leq x, m | d_p} p
$$

is equal to

$$
\sum_{1 \leq m \leq z / (N(f))^{1/2}} \sum_{d | m} \frac{\mu(d)}{e} \frac{1}{n(m)} (\text{Li}((x+h)^2) - \text{Li}(x^2))
$$

$$
+ O \left( \frac{xh}{(\log x)^A} \right) + O \left( N_E (\log N_E) \frac{xh}{(\log x)^A} + \frac{x^{3/2}z}{\log x} + (\log N_E)(xz) \right),
$$

where the first big-O term is due to (3.2), (3.3), (3.4), and (3.5). As argued in the previous section, we have

$$
\sum_{m \geq z / (N(f))^{1/2}} \sum_{d | m} \frac{\mu(d)}{e} \frac{1}{n(m)} (\text{Li}((x+h)^2) - \text{Li}(x^2)) \ll \frac{N_E^{1/2}xh}{z},
$$

and hence

$$
\pi_e(x+h, E) - \pi_e(x, E) = \epsilon_E (\text{Li}((x+h)^2) - \text{Li}(x^2))
$$

$$
+ O \left( N_E (\log N_E) \frac{xh}{(\log x)^A} + \frac{x^{3/2}z}{\log x} + \frac{N_E^{1/2}x^2}{z} \right)
$$

whenever $z^2 \leq x^\theta$ and $x^{1-\delta} \leq h \leq x$ with $0 \leq \theta < \frac{1}{10} (1 - 5\delta)$ and $0 \leq \delta < \frac{1}{5}$. To balance the errors, we take $0 \leq \delta < \frac{1}{25}$ and bound the big-O term above by

$$
\ll N_E (\log N_E) \frac{xh}{(\log x)^A}
$$

for any $x^{1-\delta} \leq h \leq x$. Herein, we conclude the proof.
6. Proof of Theorem 1.3

Let $E$ be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by $\mathcal{O}_K$. Throughout our discussion, $p$ will denote a prime of good reduction of $E$, and $\ell$ will stand for a (rational) prime. We write $K = \mathbb{Q}(\sqrt{-D})$ for some square-free $D > 0$. Also, we shall let $y = y(x) = x^\eta$ for some $\eta \in (0, 1)$ (which will be chosen later), and let $\omega_y(n)$ denote the number of distinct prime divisors $\ell$ of $n \in \mathbb{N}$ for which $\ell \leq y$.

We consider
\[
\sum_{x < p \leq x + h} (\omega(|\bar{E}(\mathbb{F}_p)|) - \log \log x)^2
\]
\[
= \sum_{x < p \leq x + h} \omega^2(|\bar{E}(\mathbb{F}_p)|) - 2(\log \log x) \sum_{x < p \leq x + h} \omega(|\bar{E}(\mathbb{F}_p)|) + (\log \log x)^2 \sum_{x < p \leq x + h} 1.
\]
By the prime number theorem in short intervals established by Huxley \[24\], the last term is
\[
(Li(x + h) - Li(x))(\log \log x)^2 + O\left(\frac{h}{(\log x)^2} (\log \log x)^2\right)
\]
for $x^{1-\delta} \leq h \leq x$ with $\delta \in [0, \frac{5}{12})$. Observing that for $p \leq x + h$,
\[
|\bar{E}(\mathbb{F}_p)| \leq p + 2\sqrt{p} + 1 \leq 6x,
\]
and that the number of prime divisors $\ell$ of any $n \leq 6x$ for which $\ell > y$ is at most $\frac{2}{\eta}$ (for $x \geq 6$), we may write the second-to-last sum of the equation above as
\[
\sum_{x < p \leq x + h} \omega(|\bar{E}(\mathbb{F}_p)|) = \sum_{x < p \leq x + h} \omega_y(|\bar{E}(\mathbb{F}_p)|) + \sum_{x < p \leq x + h} O(1)
\]
\[
= \sum_{x < p \leq x + h} \omega_y(|\bar{E}(\mathbb{F}_p)|) + O\left(\frac{h}{\log x}\right).
\]

Following Liu \[32\], we divide primes $p$ into two groups depending on whether $p$ is supersingular or ordinary. Recall that $p$ is supersingular if and only if $p$ is ramified or inert in $K$ and that there are only finitely many ramified primes $p$ in $K/\mathbb{Q}$. Moreover, if $p \neq 2$ is inert in $K$, then the Legendre symbol $\left(\frac{-D}{p}\right) = -1$, and $|\bar{E}(\mathbb{F}_p)| = p + 1$. Let $a_1, \ldots, a_r(\ell) \in (\mathbb{Z}/\ell D\mathbb{Z})^\times$ be integers for which $a_i \equiv -1 \pmod{\ell}$ and $\left(\frac{-D}{a_i}\right) = -1$. Then it follows from Theorem 2.2 and the estimate $r(\ell) \ll 1$ that for any $\delta \in [0, \frac{5}{12})$ and $x^{1-\delta} \leq h \leq x$,
\[
\begin{align*}
\sum_{x < p \leq x + h} & \omega_y(|\bar{E}(\mathbb{F}_p)|) = \sum_{\ell \leq y} \sum_{\substack{x < p \leq x + h \ \ell | \bar{E}(\mathbb{F}_p)| \ \ell \text{supersingular}}} 1 + O(y) \\
& = \sum_{\ell \leq y} \sum_{i=1}^{r(\ell)} \sum_{\substack{x < p \leq x + h \ \ell \equiv a_i(\mod{\ell D})}} 1 + O(y) \\
& = \sum_{\ell \leq y} \frac{r(\ell)}{\phi(\ell D)} (Li(x + h) - Li(x)) + O\left(\frac{h}{(\log x)^2}\right)
\end{align*}
\]
whenever \( \eta < \theta \), with \( \theta \) satisfying condition (2.3). As \( \frac{r(\ell)}{\omega(\ell)} = \frac{1}{2(\ell-1)} \), by Mertens’s theorem (see, e.g., [12, Ch. 7]), we see that

\[
\sum_{x<p\leq x+h \atop p \text{ supersingular}} \omega_y(|\bar{E}(\mathbb{F}_p)|) = \frac{1}{2} (\text{Li}(x+h) - \text{Li}(x)) (\log \log x) + O\left(\frac{h}{\log x}\right).
\]

Now we consider ordinary primes \( p \). We let \( \pi_p \) and \( \bar{\pi}_p \) be the conjugate roots of \( x^2 - (p + 1 - |\bar{E}(\mathbb{F}_p)|) + p \), and note that \( \mathbb{Q}(\pi_p) = K \) (see [8, Lemma 5.1.2]). As there are only finitely many primes \( \ell \) ramified in \( K \), we can only consider the unramified primes \( \ell \) and divide them into two groups, namely, \( \ell \) is inert or \( \ell \) splits.

For \( \ell \) inert in \( K \), we let \( (\ell) = \ell \mathcal{O}_K \). As

\[
|\bar{E}(\mathbb{F}_p)| = (\pi_p - 1)(\bar{\pi}_p - 1),
\]

the condition \( \ell \mid |\bar{E}(\mathbb{F}_p)| \) implies that \( \pi_p \equiv 1 \pmod{\ell} \). Thus, it follows from Theorem [1.4] that for any \( \delta \in [0, \frac{1}{5}] \) and \( x^{1-\delta} \leq h \leq x \),

\[
\sum_{\ell \leq y \atop \ell \text{ inert}} \sum_{x<p\leq x+h \atop \ell \mid |\bar{E}(\mathbb{F}_p)|} 1 \ll \sum_{\ell \leq y \atop \ell \text{ inert}} \sum_{x<p\leq x+h \atop \ell \text{ ordinary}} \frac{1}{h((\ell))} (\text{Li}(x+h) - \text{Li}(x)) + O\left(\frac{h}{(\log x)^2}\right),
\]

provided that \( 2\eta < \frac{1}{10}(1-5\delta) \). Since \( K \) is of class number 1 and \( r_1 = r_1(K) = 0 \),

\[
h((\ell)) \geq \frac{\phi(\ell^2)}{6},
\]

and thus

\[
\sum_{\ell \leq y \atop \ell \text{ inert}} \sum_{x<p\leq x+h \atop \ell \mid |\bar{E}(\mathbb{F}_p)|} 1 \ll \frac{h}{\log x}.
\]

For \( \ell \) splitting in \( K \), we write \( (\ell) = \ell_1 \ell_2 \). Now the condition \( \ell \mid |\bar{E}(\mathbb{F}_p)| \) tells us that \( \pi_p \equiv 1 \pmod{\ell_1} \) or \( \pi_p \equiv 1 \pmod{\ell_2} \). Therefore, letting \( I \) stand for \( I_1 \) or \( I_2 \) (depending on the pertinent congruence condition) and applying Theorem [1.4] for any \( \delta \in [0, \frac{1}{5}] \) and \( x^{1-\delta} \leq h \leq x \), we have

\[
\sum_{\ell \leq y \atop \ell \text{ splits}} \sum_{x<p\leq x+h \atop \ell \mid |\bar{E}(\mathbb{F}_p)|} 1 = \frac{1}{2} \sum_{\ell \leq y \atop \ell \text{ splits}} \sum_{x<p\leq x+h \atop \ell \mid |\bar{E}(\mathbb{F}_p)|} 1
\]

\[
= \frac{1}{2} \sum_{\ell \leq y \atop \ell \text{ splits}} \frac{1}{T(\ell)} \sum_{x<p\leq x+h \atop \ell \text{ ordinary}} \sum_{\pi_p \equiv 1 \pmod{\ell} \atop (\pi_p) \sim (1) \pmod{\ell}} 1
\]

\[
= \frac{1}{2} \sum_{\ell \leq y \atop \ell \text{ splits}} \frac{1}{\phi(\ell)} (\text{Li}(x+h) - \text{Li}(x)) + O\left(\frac{h}{(\log x)^2}\right),
\]
provided that $\eta < \frac{1}{10}(1 - 5\delta)$. As $\ell = I_1I_2$, we derive
\[
\sum_{\ell \leq y} \sum_{x < p \leq x + h \atop \ell \text{ splits } p \text{ ordinary } \ell \mid |E(F_p)|} 1 = \frac{1}{2} \cdot 2 \sum_{\ell \leq y} \frac{1}{\phi(\ell)} (\text{Li}(x + h) - \text{Li}(x)) + O\left(\frac{h}{(\log x)^2}\right)
\]
\[
= \frac{1}{2}(\text{Li}(x + h) - \text{Li}(x))(\log \log x) + O\left(\frac{h}{\log x}\right),
\]
where the last estimate follows from Mertens’s theorem and the fact that $\ell \neq 2$ splits in $K$ if and only if $\frac{1}{\phi(\ell)} = 1$. Finally, for any $\delta \in [0, \frac{1}{5})$, choosing $\eta < \frac{1}{20}(1 - 5\delta)$, we arrive at
\[
\sum_{x < p \leq x + h} \omega(|E(F_p)|) = (\text{Li}(x + h) - \text{Li}(x))(\log \log x) + O\left(\frac{h}{\log x}\right)
\]
whenever $x^{1-\delta} \leq h \leq x$. Moreover, by an analogous argument, for any $\delta \in [0, \frac{1}{5})$, choosing $\eta < \frac{1}{20}(1 - 5\delta)$, we have
\[
\sum_{x < p \leq x + h} \omega^2(|E(F_p)|) = (\text{Li}(x + h) - \text{Li}(x))(\log \log x)^2 + O\left(\frac{h(\log \log x)^2}{\log x}\right).
\]
Putting everything together, we obtain Theorem 1.3.

**Remark 6.1.** If one would like to apply the argument above to $\omega(n)$, then one would obtain a short interval version of Turán’s theorem. More precisely, since
\[
\sum_{x < n \leq x + h} \omega(n) = \sum_{x < n \leq x + h} \omega_y(n) + \sum_{x < n \leq x + h} O(1) = \sum_{x < n \leq x + h} \omega_y(n) + O(h)
\]
and
\[
\sum_{x < n \leq x + h} \omega_y(n) = \sum_{x < n \leq x + h} \sum_{\ell \mid n} 1 = \sum_{\ell \leq y} \left\lfloor \frac{x + h}{\ell} \right\rfloor - 
\left\lfloor \frac{x}{\ell} \right\rfloor,
\]
observing that the last sum is
\[
\sum_{\ell \leq y} \frac{h}{\ell} + O(y) = h \log \log x + O(h + y),
\]
and then choosing $\eta \leq 1 - \delta$, one has $\sum_{x < n \leq x + h} \omega(n) = h \log \log x + O(h)$. Similarly, one can show that $\sum_{x < n \leq x + h} \omega^2(n) = h(\log \log x)^2 + O(h(\log \log x))$ and conclude the following.

**Theorem 6.2.** Let $\delta \in [0, 1)$. Then for any $x^{1-\delta} \leq h \leq x$, one has
\[
\sum_{x < n \leq x + h} (\omega(n) - \log \log x)^2 = O(h(\log \log x)).
\]
Furthermore, in much the same spirit, as one can write
\[
\sum_{x < p \leq x + h} \omega_y(p - a) = \sum_{x < p \leq x + h} \sum_{\ell \mid p - a} 1 = \sum_{\ell \leq y} \sum_{p \equiv a(\mod \ell)} 1,
\]
arguing similarly as above, one may apply Theorem 2.2 to deduce the following variant of the earlier-mentioned theorem of Erdős.
Theorem 6.3. Let $a$ be an integer, and let $\delta \in \left[0, \frac{5}{12}\right)$. Then for any $x^{1-\delta} \leq h \leq x$, one has
\[
\sum_{x < p \leq x + h} (\omega(p - a) - \log \log x)^2 = O\left(\frac{h}{\log x} (\log \log x)\right),
\]
where the sum is over primes $p$ coprime to $a$, and the implied constant is independent of $a$.

Acknowledgments

The author would like to thank Professors Wen-Ching Winnie Li and Ram Murty for their comments on the previous versions of the manuscript as well as thanking Jesse Thorner for the discussion. He is also grateful to the referee for the careful reading and helpful comments.

References


This is a free offprint provided to the author by the publisher. Copyright restrictions may apply.


Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, Alberta T1K 3M4, Canada

Email address: pengjie.wong@uleth.ca