TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 373, Number 12, December 2020, Pages 8725–8749
https://doi.org/10.1090/tran/8197
Article electronically published on September 29, 2020

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 $\bar{E}(\mathbb{F}_p) = \langle P(\mathrm{mod}\, p)\rangle$ 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

$$\pi_c(x, E) = \#\{p \le x \mid p \nmid N_E \text{ and } \bar{E}(\mathbb{F}_p) \text{ is cyclic}\}, \tag{1.1}$$

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

$$\pi_c(x, E) = \mathfrak{c}_E \operatorname{Li}(x) + o\Big(\frac{x}{\log x}\Big),$$

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.

where $\mathrm{Li}(x)$ is the logarithmic integral function,

$$\mathfrak{c}_E = \sum_{m=1}^{\infty} \frac{\mu(m)}{[\mathbb{Q}(E[m]) : \mathbb{Q}]},$$

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

$$\pi_c(x, E) = \mathfrak{c}_E \,\mathrm{Li}(x) + O\Big(\frac{x \log\log x}{(\log x)^2}\Big).$$

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,

$$\pi_c(x, E) = \mathfrak{c}_E \,\mathrm{Li}(x) + O(x^{3/4}(\log(N_E x))^{1/2}), \tag{1.2}$$

where the implied constant is absolute. Also, Cojocaru and M. R. Murty [10, Sec. 6] showed that, unconditionally, $\mathfrak{c}_E$ 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 $\bar{E}(\mathbb{F}_p)$ 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 $E/\mathbb{Q}$,

$$\pi_c(x, E) = \mathfrak{c}_E \,\mathrm{Li}(x) + O\Big(\frac{x}{(\log x)(\log\log((\log x)/N_E^2))} \frac{\log\log x}{\log((\log x)/N_E^2)}\Big).$$

More recently, based on M. R. Murty's argument [37] with an insert of Huxley's Bombieri–Vinogradov theorem for number fields [23] (see also Theorem 2.1 in Section 2), Akbary and V. K. Murty [1] improved the error term in the above asymptotic formula by showing that if $E/\mathbb{Q}$ is an elliptic curve of conductor N_E and with complex multiplication by $\mathcal{O}_K$, then for any $A, D > 0$, one has

$$\pi_c(x, E) = \mathfrak{c}_E \,\mathrm{Li}(x) + O_{A,D}\Big(\frac{x}{(\log x)^A}\Big) \tag{1.3}$$

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 $A > 0$,

$$\pi(x) = \mathrm{Li}(x) + O\Big(\frac{x}{(\log x)^A}\Big),$$

which implies that for any $A > 0$,

$$\pi(2x) - \pi(x) = \mathrm{Li}(2x) - \mathrm{Li}(x) + O\Big(\frac{x}{(\log x)^A}\Big).$$

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

$$\pi_c(2x, E) - \pi_c(x, E) = \mathfrak{c}_E(\mathrm{Li}(2x) - \mathrm{Li}(x)) + O_A\Big(\frac{x}{(\log x)^A}\Big),$$

we see that

$$\frac{\pi_c(2x,E)-\pi_c(x,E)}{\pi(2x)-\pi(x)} \sim \mathfrak{c}_E$$

as $x \to \infty$. In other words, the "density" of primes p with cyclic $\bar{E}(\mathbb{F}_p)$ in $(x, 2x]$ is $\mathfrak{c}_E$.

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 $x^{1-\delta} \le h \le x$ with $\delta \in [0, 1)$. Assuming the Riemann hypothesis, one can show that for any $A > 0$,

$$\pi(x+h)-\pi(x) = \mathrm{Li}(x+h)-\mathrm{Li}(x)+O\Big(\frac{h}{(\log x)^A}\Big) \tag{1.4}$$

whenever $x^{1-\delta} \le h \le x$ 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 $x^{1-\delta} \le h \le x$ 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 $\delta \in [0, \frac{1}{4})$ and $x^{1-\delta} \le h \le x$, one has

$$\pi_c(x+h,E)-\pi_c(x,E) = \mathfrak{c}_E(\mathrm{Li}(x+h)-\mathrm{Li}(x))+O\Big((\log N_E)^{1/2}\frac{h}{(\log x)^A}\Big)$$

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 $0 \le \delta < \frac{1}{25}$. Then for any $x^{1-\delta} \le h \le x$, we have*

$$\pi_c(x+h,E)-\pi_c(x,E) = \mathfrak{c}_E(\mathrm{Li}(x+h)-\mathrm{Li}(x))+O\Big(N_E(\log N_E)\frac{h}{(\log x)^A}\Big),$$

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

$$\pi_e(x,E) = \sum_{p \le x} e_p \tag{1.5}$$

and showed that under GRH,

$$\pi_e(x,E) = \mathfrak{e}_E\,\mathrm{Li}(x^2)+O(x^{19/10}(\log x)^{6/5}),$$

where

$$\mathfrak{e}_E = \sum_{m=1}^{\infty} \frac{1}{[\mathbb{Q}(E[m]) : \mathbb{Q}]} \sum_{de|m} \frac{\mu(d)}{e},$$

and that

$$\pi_e(x, E) = \mathfrak{e}_E \operatorname{Li}(x^2) + O\Big(\frac{x^2 \log\log\log x}{(\log x)(\log\log x)}\Big),$$

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 $A, D > 0$,

$$\pi_e(x, E) = \mathfrak{e}_E \operatorname{Li}(x^2) + O_{A,D}\Big(\frac{x^2}{(\log x)^A}\Big), \tag{1.6}$$

uniformly in $N_E \le (\log x)^D$, 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 e_p in short intervals. By (1.6), we know that

$$\pi_e(2x, E) - \pi_e(x, E) = \mathfrak{e}_E(\operatorname{Li}((2x)^2) - \operatorname{Li}(x^2)) + O_{A,D}\Big(\frac{x^2}{(\log x)^A}\Big)$$

if E is with CM. Also, by the above-mentioned result of Wu, assuming GRH, one has

$$\pi_e(x+h, E) - \pi_e(x, E) = \mathfrak{e}_E(\operatorname{Li}((x+h)^2) - \operatorname{Li}(x^2)) + O\Big(\frac{xh}{(\log x)^A}\Big)$$

for any $A > 0$ and $x^{1-\delta} \le h \le x$ with $\delta \in [0, \frac{1}{6})$. 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 $0 \le \delta < \frac{1}{25}$. Then for any $x^{1-\delta} \le h \le x$, we have*

$$\pi_e(x+h, E) - \pi_e(x, E) = \mathfrak{e}_E(\operatorname{Li}((x+h)^2) - \operatorname{Li}(x^2)) + O\Big(\frac{xh}{(\log x)^A}\Big),$$

where $\pi_e(x, E)$ is defined as in (1.5)*, and the implied constant depends on $\mathbb{Q}(E[2])$ and A.*

Furthermore, one may study the prime divisors of $|\bar{E}(\mathbb{F}_p)|$ and e_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

$$\sum_{n \le x} (\omega(n) - \log\log x)^2 = O(x \log\log x),$$

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

$$\sum_{p \le x} (\omega(p-1) - \log\log x)^2 = O\Big(\frac{x}{\log x}(\log\log x)\Big).$$

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 $E/\mathbb{Q}$,

$$\sum_{p\le x}(\omega(|\bar{E}(\mathbb{F}_p)|)-\log\log x)^2 = O\Big(\frac{x}{\log x}(\log\log x)\Big). \tag{1.7}$$

As $d_p \mid e_p$, it follows that

$$\sum_{p\le x}(\omega(e_p)-\log\log x)^2 = O\Big(\frac{x}{\log x}(\log\log x)\Big).$$

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

$$\sum_{x<p\le 2x}(\omega(|\bar{E}(\mathbb{F}_p)|)-\log\log x)^2 = O\Big(\frac{x}{\log x}(\log\log x)\Big)$$

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 $x^{1-\delta} \le h \le x$, we have*

$$\sum_{x<p\le x+h}(\omega(|\bar{E}(\mathbb{F}_p)|)-\log\log x)^2 = O\Big(\frac{h}{\log x}(\log\log x)\Big),$$

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 $x^{1-\delta} \le h \le x$, we have*

$$\sum_{x<p\le x+h}(\omega(e_p)-\log\log x)^2 = O\Big(\frac{h}{\log x}(\log\log x)\Big),$$

where the implied constant is independent of E.

The proofs of our theorems are adaptions 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 $1 \le m \le 2\sqrt{x}$ 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 $\mathfrak{a}$ and $\mathfrak{q}$ of F, we set

$$\pi(x,\mathfrak{q},\mathfrak{a}) = \#\{\mathfrak{p}\subset\mathcal{O}_F \mid \mathrm{N}(\mathfrak{p})\le x \text{ and } \mathfrak{p}\sim\mathfrak{a} \pmod{\mathfrak{q}}\},$$

where $\mathfrak{p}\sim\mathfrak{a} \pmod{\mathfrak{q}}$ means that $\mathfrak{p}$ and $\mathfrak{a}$ belong to the same ray class of the ray class group modulo $\mathfrak{q}$.)

Theorem 1.4. *Let F be a number field of degree n_F. For $0 \le \delta < \frac{2}{5n_F}$, we fix $0 \le \theta < \frac{1}{5n_F+10}(2-5n_F\delta)$. Then for any $x^{1-\delta} \le h \le x$ and $A > 0$, we have*

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

where, as later, $h(\mathfrak{q})$ denotes the cardinality of the ray class group modulo $\mathfrak{q}$, $\phi(\mathfrak{q})$ is the number field analogue of Euler's totient function, and $N \sim x$ means that $\frac{1}{2}x \le N \le x$, 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 Sokolovskiĭ [46] on the prime ideal theorem in short intervals.

Remark 1.5. It may be possible that the dependence of $\mathbb{Q}(E[2])$ 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 δ and θ 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

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

The celebrated Bombieri–Vinogradov theorem states that for any $A > 0$, there exists $B = B(A) > 0$ such that for $Q \le x^{1/2}/(\log x)^B$,

$$\sum_{q\le Q} \max_{(a,q)=1} \max_{y\le x} \left|\pi(y,q,a) - \frac{1}{\phi(q)}\mathrm{Li}(y)\right| \ll_A \frac{x}{(\log x)^A}, \tag{2.1}$$

where $\phi(q)$ and $\mathrm{Li}(x)$ denote Euler's totient function and the logarithmic integral function, respectively. After the work of Bombieri and Vinogradov, Gallagher [16] and Vaughan [50] gave different proofs for (2.1), and Bombieri, Friedlander, and Iwaniec [4–6] improved (2.1) by extending the valid range of Q with a proviso. Besides, several variants have been derived by Huxley [23] and Wilson [51] for prime ideals, M. R. Murty-V. K. Murty [39] and M. R. Murty-Petersen [40] for primes with

Chebotarev conditions, Coleman-Swallow [11] and Hinz [22] for algebraic integers, and Johnson [26] for ideal numbers.

We shall recall Huxley's Bombieri–Vinogradov theorem for number fields. For any coprime ideals $\mathfrak{a}$ and $\mathfrak{q}$ in $\mathcal{O}_F$, we set

$$\pi(x,\mathfrak{q},\mathfrak{a}) = \#\{\mathfrak{p} \subset \mathcal{O}_F \mid \mathrm{N}(\mathfrak{p}) \le x \text{ and } \mathfrak{p} \sim \mathfrak{a} \pmod{\mathfrak{q}}\},$$

where $\mathfrak{p} \sim \mathfrak{a} \pmod{\mathfrak{q}}$ means that $\mathfrak{p}$ and $\mathfrak{a}$ belong to the same ray class of the ray class group modulo $\mathfrak{q}$. (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 $Q \le x^{1/2}/(\log x)^B$, one has*

$$\sum_{\mathrm{N}(\mathfrak{q}) \le Q} \frac{h(\mathfrak{q})}{\phi(\mathfrak{q})} \max_{(\mathfrak{a},\mathfrak{q})=1} \max_{y \le x} \left| \pi(y,\mathfrak{q},\mathfrak{a}) - \frac{1}{h(\mathfrak{q})} \mathrm{Li}(y) \right| \ll_{F,A} \frac{x}{(\log x)^A},$$

where $h(\mathfrak{q})$ is the cardinality of the ray class group modulo $\mathfrak{q}$, and $\phi(\mathfrak{q})$ 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

$$h(\mathfrak{q}) = \frac{h_F 2^{r_1} \phi(\mathfrak{q})}{T(\mathfrak{q})},$$

where $T(\mathfrak{q})$ is the number of residue classes $(\mathrm{mod}\, \mathfrak{q})$ that contain a unit (see [51, Eq. (7)]), one can replace $\frac{h(\mathfrak{q})}{\phi(\mathfrak{q})}$ in the estimate by $\frac{1}{T(\mathfrak{q})}$. Also, if F is an imaginary quadratic field, then $T(\mathfrak{q}) \le 6$, and hence the factor $\frac{h(\mathfrak{q})}{\phi(\mathfrak{q})}$ 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 $H \cap C \ne \varnothing$, 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 $\epsilon, A > 0$,

$$\sum_{\substack{q \le Q \\ (q, d_L)=1}} \max_{(a,q)=1} \max_{y \le x} \left| \pi_C(y,q,a) - \frac{1}{\phi(q)} \frac{|C|}{|G|} \mathrm{Li}(y) \right| \ll_{\epsilon,L,A} \frac{x}{(\log x)^A}, \tag{2.2}$$

where $Q = x^{\theta-\epsilon}$, $\theta = \theta(G) = \min\{\frac{1}{|n_E-2|}, \frac{1}{2}\}$,

$$\pi_C(x,q,a) = \sum_{\substack{\mathrm{N}(\mathfrak{p}) \le x \\ \mathrm{N}(\mathfrak{p}) \equiv a (\mathrm{mod}\, q)}} \delta_C(\mathfrak{p}),$$

δ_C denotes the indicator function for the unramified primes $\mathfrak{p}$ of L/F with Artin symbol $\sigma_{\mathfrak{p}} = C$, and the implied constant depends on ϵ, 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 $0 \le \delta < \frac{5}{12}$, and let*

$$0 \le \theta < \begin{cases} \frac{1}{2} - \delta & \text{if } 0 \le \delta < \frac{2}{5}, \\ \frac{9}{20} - \delta & \text{if } \frac{2}{5} \le \delta < \frac{5}{12}. \end{cases} \tag{2.3}$$

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

$$\sum_{q \le x^{\theta}} \max_{\substack{(a,q)=1 \\ y \le h \\ N \sim x}} \left| \pi(N+y,q,a) - \pi(N,q,a) - \frac{1}{\phi(q)} (\mathrm{Li}(N+y) - \mathrm{Li}(N)) \right| \ll_A \frac{h}{(\log x)^A},$$

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

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

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

$$\pi_C(x+h,1,1) - \pi_C(x,1,1) \sim \frac{|C|}{|G|} (\mathrm{Li}(x+h) - \mathrm{Li}(x)).$$

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

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

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 [3], 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 $\mathfrak{a}$ and $\mathfrak{q}$ in $\mathcal{O}_F$, we consider the prime-counting function

$$\tilde{\psi}(x, \mathfrak{q}, \mathfrak{a}) = \sum_{\substack{\mathrm{N}(\mathfrak{p}) \le x \\ \mathfrak{p} \sim \mathfrak{a}}} \log \mathrm{N}(\mathfrak{p}),$$

where $\mathfrak{p} \sim \mathfrak{a} \pmod{\mathfrak{q}}$ means that $\mathfrak{p}$ and $\mathfrak{a}$ belong to the same ray class of the ray class group modulo $\mathfrak{q}$. By Abel's summation, to prove Theorem 1.4, it suffices to show that for any $x^{1-\delta} \le h \le x$ and $A > 0$, one has

(2.4)
$$\sum_{\mathrm{N}(\mathfrak{q}) \le x^{\theta}} \frac{h(\mathfrak{q})}{\phi(\mathfrak{q})} \max_{(\mathfrak{a},\mathfrak{q})=1} \max_{y \le h} \max_{N \sim x} \left| \tilde{\psi}(N+y,\mathfrak{q},\mathfrak{a}) - \tilde{\psi}(N,\mathfrak{q},\mathfrak{a}) - \frac{1}{h(\mathfrak{q})} y \right| \ll \frac{h}{(\log x)^A}$$

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

For any Hecke character $\chi \pmod{\mathfrak{q}}$, we define

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

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

$$\psi(x,\mathfrak{q},\mathfrak{a}) = \frac{1}{h(\mathfrak{q})} \sum_{\chi \pmod{\mathfrak{q}}} \overline{\chi}(\mathfrak{a}) \psi(x,\chi). \tag{2.5}$$

A direct calculation shows that

$$\psi(x,\mathfrak{q},\mathfrak{a}) - \tilde{\psi}(x,\mathfrak{q},\mathfrak{a}) \ll \sum_{\substack{\mathrm{N}(\mathfrak{p}) \le x \\ (\mathfrak{p},\mathfrak{q}) \ne 1}} \log \mathrm{N}(\mathfrak{p}) + \sum_{\substack{\mathrm{N}(\mathfrak{p}^m) \le x \\ m \ge 2}} \log \mathrm{N}(\mathfrak{p}) \ll (\log x)(\log \mathrm{N}(\mathfrak{q}) + x^{\frac{1}{2}}).$$

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

$$\sum_{\mathrm{N}(\mathfrak{q}) \le x^{\theta}} \frac{h(\mathfrak{q})}{\phi(\mathfrak{q})} \max_{(\mathfrak{a},\mathfrak{q})=1} \max_{y \le h} \max_{N \sim x} \left| \psi(N+y,\mathfrak{q},\mathfrak{a}) - \psi(N,\mathfrak{q},\mathfrak{a}) - \frac{1}{h(\mathfrak{q})} y \right| \ll \frac{h}{(\log x)^A}.$$

Note that by (2.5), we have

$$\begin{aligned} &\left| \psi(N+y,\mathfrak{q},\mathfrak{a}) - \psi(N,\mathfrak{q},\mathfrak{a}) - \frac{1}{h(\mathfrak{q})} y \right| \\ &\le \frac{1}{h(\mathfrak{q})} \Big(|\psi(N+y,\chi_0) - \psi(N,\chi_0) - y| + \sum_{\chi \ne \chi_0} |\psi(N+y,\chi) - \psi(N,\chi)| \Big), \end{aligned} \tag{2.6}$$

where χ_0 denotes the trivial character, and the second sum is over the nontrivial character χ modulo $\mathfrak{q}$. Let $\chi^* \pmod{\mathfrak{q}^*}$ be the Hecke character inducing $\chi \pmod{\mathfrak{q}}$. Then

$$\psi(x,\chi) - \psi(x,\chi^*) \ll \sum_{\substack{\mathrm{N}(\mathfrak{p}^m) \le x \\ \mathfrak{p} \mid \mathfrak{q}}} \log \mathrm{N}(\mathfrak{p}) \ll (\log x) \log \mathrm{N}(\mathfrak{q}),$$

and hence for any fixed modulus $\mathfrak{q}$ with $\mathrm{N}(\mathfrak{q}) \le x$,

$$\begin{aligned} &\frac{1}{h(\mathfrak{q})} \sum_{\chi \ne \chi_0} \max_{y \le h} \max_{N \sim x} |\psi(N+y,\chi) - \psi(N,\chi)| \\ &= \frac{1}{h(\mathfrak{q})} \sum_{\chi \ne \chi_0} \max_{y \le h} \max_{N \sim x} |\psi(N+y,\chi^*) - \psi(N,\chi^*)| + O\Big((\log x)^2 \sum_{\chi}^{\circ} \frac{1}{h(\mathfrak{q})} \Big), \end{aligned} \tag{2.7}$$

where $\circ$ indicates that the sum is only over imprimitive characters modulo $\mathfrak{q}$.

Let $0 \le Q_1 \le x$, and set

$$S(Q_1) = \sum_{\mathrm{N}(\mathfrak{q}) \le Q_1} \frac{h(\mathfrak{q})}{\phi(\mathfrak{q})} \frac{1}{h(\mathfrak{q})} \sum_{\chi \ne \chi_0} \max_{y \le h} \max_{N \sim x} |\psi(N+y, \chi) - \psi(N, \chi)|.$$

From (2.7), it follows that

$$\begin{aligned} S(Q_1) = & \sum_{\mathrm{N}(\mathfrak{q}) \le Q_1} \frac{1}{\phi(\mathfrak{q})} \sum_{\chi \ne \chi_0} \max_{y \le h} \max_{N \sim x} |\psi(N+y, \chi^*) - \psi(N, \chi^*)| \\ & + O\Big((\log x)^2 \sum_{\mathrm{N}(\mathfrak{q}) \le Q_1} \sideset{}{^\circ}\sum_{\chi} \frac{1}{\phi(\mathfrak{q})}\Big). \end{aligned}$$

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

$$\begin{aligned} S(Q_1) = & \sum_{1 < \mathrm{N}(\mathfrak{q}^*) \le Q_1} \sideset{}{'}\sum_{\chi^* (\mathrm{mod}\, \mathfrak{q}^*)} \max_{y \le h} \max_{N \sim x} |\psi(N+y, \chi^*) - \psi(N, \chi^*)| \sum_{\substack{\mathrm{N}(\mathfrak{q}) \le Q_1 \\ \mathfrak{q}^* \mid \mathfrak{q}}} \frac{1}{\phi(\mathfrak{q})} \\ & + O\Big((\log x)^2 \sum_{\mathrm{N}(\mathfrak{q}^*) \le Q_1} \sideset{}{'}\sum_{\chi^* (\mathrm{mod}\, \mathfrak{q}^*)} \sum_{\substack{\mathrm{N}(\mathfrak{q}) \le Q_1 \\ \mathfrak{q}^* \mid \mathfrak{q}}} \frac{1}{\phi(\mathfrak{q})}\Big), \end{aligned}$$

where the primed sums are over the primitive characters. Since there are $h(\mathfrak{q})$ Hecke characters modulo $\mathfrak{q}$, $h(\mathfrak{q}) \ll_F \phi(\mathfrak{q})$, and

$$\sum_{\substack{\mathrm{N}(\mathfrak{q}) \le Q_1 \\ \mathfrak{q}^* \mid \mathfrak{q}}} \frac{1}{\phi(\mathfrak{q})} \ll \frac{\log Q_1}{\phi(\mathfrak{q}^*)}$$

(see [51, pp. 199–200]), we derive

(2.8)

$$\begin{aligned} S(Q_1) \ll & (\log Q_1) \sum_{1 < \mathrm{N}(\mathfrak{q}^*) \le Q_1} \frac{1}{\phi(\mathfrak{q}^*)} \sideset{}{'}\sum_{\chi^* (\mathrm{mod}\, \mathfrak{q}^*)} \max_{y \le h} \max_{N \sim x} |\psi(N+y, \chi^*) - \psi(N, \chi^*)| \\ & + O((\log x)^3 Q_1). \end{aligned}$$

Thus, upon replacing $\mathfrak{q}^*$ and χ^* by $\mathfrak{q}$ and χ for the sums in (2.8), respectively, putting (2.6) and (2.8) together, we obtain

$$\begin{aligned} & \sum_{\mathrm{N}(\mathfrak{q}) \le Q_1} \frac{h(\mathfrak{q})}{\phi(\mathfrak{q})} \max_{(\mathfrak{a}, \mathfrak{q}) = 1} \max_{y \le h} \max_{N \sim x} \Big|\psi(N+y, \mathfrak{q}, \mathfrak{a}) - \psi(N, \mathfrak{q}, \mathfrak{a}) - \frac{1}{h(\mathfrak{q})} y\Big| \\ & \ll \sum_{\mathrm{N}(\mathfrak{q}) \le Q_1} \frac{1}{\phi(\mathfrak{q})} \max_{y \le h} \max_{N \sim x} |\psi(N+y, \chi_0) - \psi(N, \chi_0) - y| + S(Q_1) \\ & \ll (\log Q_1) \sum_{\mathrm{N}(\mathfrak{q}) \le Q_1} \frac{1}{\phi(\mathfrak{q})} \sideset{}{'}\sum_{\chi (\mathrm{mod}\, \mathfrak{q})} \max_{y \le h} \max_{N \sim x} |\psi(N+y, \chi) - \psi(N, \chi) - \delta(\chi) y| \\ & + O((\log x)^3 Q_1), \end{aligned} \tag{2.9}$$

where $\delta(\chi)$ is the indicator function of the trivial character χ_0.

By [28, Eq. (5.53)], for $2 \le T \le x$ and $\chi \pmod{\mathfrak{q}}$ with $\mathrm{N}(\mathfrak{q}) \le Q_1 \le x$, we have

$$\psi(N+y,\chi)-\psi(N,\chi)-\delta(\chi)y \ll \sum_{\substack{\rho=\beta+i\gamma\\ |\gamma|\le T}} \Big|\frac{(N+y)^\rho - N^\rho}{\rho}\Big| + O\Big(\frac{x(\log x)^2}{T}\Big),$$

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

$$\Big|\frac{(N+y)^\rho - N^\rho}{\rho}\Big| = \Big|\int_N^{N+y} t^{\rho-1}dt\Big| \le \int_N^{N+y} t^{\beta-1}dt \le yN^{\beta-1} \ll hx^{\beta-1},$$

we have

$$\psi(N+y,\chi)-\psi(N,\chi)-\delta(\chi)y \ll h \sum_{\substack{\rho=\beta+i\gamma\\ |\gamma|\le T}} x^{\beta-1} + O\Big(\frac{x(\log x)^2}{T}\Big).$$

Hence, we obtain the estimate

$$\begin{aligned}(2.10)\qquad &\sum_{\mathrm{N}(\mathfrak{q})\le Q_1} \frac{1}{\phi(\mathfrak{q})} \sideset{}{'}\sum_{\chi \pmod{\mathfrak{q}}} \max_{y\le h} \max_{N\sim x} |\psi(N+y,\chi)-\psi(N,\chi)-\delta(\chi)y| \\ &\ll h \sum_{\mathrm{N}(\mathfrak{q})\le Q_1} \frac{1}{\phi(\mathfrak{q})} \sideset{}{'}\sum_{\chi \pmod{\mathfrak{q}}} \sum_{\substack{\rho=\beta+i\gamma\\ |\gamma|\le T}} x^{\beta-1} + \frac{Q_1 x(\log x)^2}{T}.\end{aligned}$$

Now we are in a position to proceed with the "dyadic argument" as in [40, Lemma 1.7], which requires the estimate

$$(2.11)\qquad \frac{1}{\phi(\mathfrak{q})} \ll \frac{\log\log \mathrm{N}(\mathfrak{q})}{\mathrm{N}(\mathfrak{q})}.$$

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 $\mathfrak{q}$. Let $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_{r-k}$ be the primes which divide $\mathfrak{q}$ and are with norm not exceeding $\log \mathrm{N}(\mathfrak{q})$, and let $\mathfrak{p}_{r-k+1}, \dots, \mathfrak{p}_r$ be those which divide $\mathfrak{q}$ and are with norm greater than $\log \mathrm{N}(\mathfrak{q})$. Then we have

$$(\log \mathrm{N}(\mathfrak{q}))^k \le \mathrm{N}(\mathfrak{p}_{r-k+1}) \cdots \mathrm{N}(\mathfrak{p}_r) \le \mathrm{N}(\mathfrak{q})$$

and hence

$$k \le \log \mathrm{N}(\mathfrak{q}) / \log\log \mathrm{N}(\mathfrak{q}).$$

Thus, we have

$$\frac{\phi(\mathfrak{q})}{\mathrm{N}(\mathfrak{q})} = \prod_{i=1}^{r}\Big(1-\frac{1}{\mathrm{N}(\mathfrak{p}_i)}\Big) \ge \Big(1-\frac{1}{\log \mathrm{N}(\mathfrak{q})}\Big)^{\log \mathrm{N}(\mathfrak{q})/\log\log \mathrm{N}(\mathfrak{q})} \prod_{\mathrm{N}(\mathfrak{p})\le \log \mathrm{N}(\mathfrak{q})}\Big(1-\frac{1}{\mathrm{N}(\mathfrak{p})}\Big).$$

As $(1-x^{-1})^{x/\log x} \sim 1$, and Rosen's generalisation of Mertens's theorem asserts that

$$\prod_{\mathrm{N}(\mathfrak{p})\le x}\Big(1-\frac{1}{\mathrm{N}(\mathfrak{p})}\Big)^{-1} \sim \alpha_F \log x$$

for some (explicit) constant α_F depending on F (see [44, Theorem 2]), we obtain (2.11). □

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 $m \in \{0, \dots, \lceil \log_2 Q_1 \rceil\}$. This dyadic consideration and (2.11) majorise the triple sum in (2.10) by

$$\begin{aligned}(\log Q_1) \max_{Q \le Q_1} \sum_{\mathrm{N}(\mathfrak{q}) \in [\frac{Q}{2}, Q)} \frac{\log\log \mathrm{N}(\mathfrak{q})}{\mathrm{N}(\mathfrak{q})} \sideset{}{'}\sum_{\chi \,(\mathrm{mod}\, \mathfrak{q})} \sum_{\substack{\rho = \beta + i\gamma \\ |\gamma| \le T}} x^{\beta - 1} \\ \ll (\log Q_1)(\log\log Q_1) \max_{Q \le Q_1} \frac{1}{Q} \sum_{\mathrm{N}(\mathfrak{q}) \le Q} \sideset{}{'}\sum_{\chi \,(\mathrm{mod}\, \mathfrak{q})} \sum_{\substack{\rho = \beta + i\gamma \\ |\gamma| \le T}} x^{\beta - 1},\end{aligned} \tag{2.12}$$

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

For $\sigma \in [\frac{1}{2}, 1]$, we set $N_\chi(\sigma, T) = \#\{\rho = \beta + i\gamma \mid L(\rho, \chi) = 0, \sigma \le \beta, |\gamma| \le T\}$, and for $Q \le Q_1$, we let

$$N(\sigma, Q, T) = \sum_{\mathrm{N}(\mathfrak{q}) \le Q} \sideset{}{'}\sum_{\chi \,(\mathrm{mod}\, \mathfrak{q})} N_\chi(\sigma, T).$$

We recall that by the zero-free region for Hecke L-functions established by Bartz [3], there is a constant c_F, depending on F, such that $N(\sigma, Q, T)$ is either 0 or 1 whenever

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

where

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

We note that for $1 - C_F(x, Q) < \sigma \le 1$, if $N(\sigma, Q, T) = 1$, then it is contributed by the Siegel zero β_1 of an exceptional Hecke L-function attached to a real Hecke character modulo $\mathfrak{q}_1$ (with $\mathrm{N}(\mathfrak{q}_1) \le Q$). Invoking Siegel's theorem for number fields established by Mitsui [33, Sec. 1, Lemma 12] to bound β_1, one has

$$\frac{1}{Q} x^{\beta_1 - 1} \ll \begin{cases} (\log x)^{-(A+4)} & \text{if } 1 \le Q < (\log x)^{A+4}, \\ (\log x)^{-(A+4)} x^0 & \text{if } (\log x)^{A+4} \le Q \end{cases} \tag{2.13}$$

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

$$\sum_{\mathrm{N}(\mathfrak{q}) \le Q} \sideset{}{'}\sum_{\chi \,(\mathrm{mod}\, \mathfrak{q})} \sum_{\substack{\rho = \beta + i\gamma \\ |\gamma| \le T \\ \frac{1}{2} \le \beta \le 1 - C_F(x, Q)}} x^{\beta - 1} \ll (\log x) \max_{\frac{1}{2} \le \sigma \le 1 - C_F(x, Q)} x^{\sigma - 1} N(\sigma, Q, T). \tag{2.14}$$

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 $2 \le T \le x$, $1 \le Q \le Q_1$, and $\frac{1}{2} \le \sigma \le 1$,

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

which implies that

$$\max_{\frac{1}{2} \le \sigma \le 1 - C_F(x, Q)} x^{\sigma - 1} N(\sigma, Q, T) \ll (\log x)^{9n_F + 10} \max_{\frac{1}{2} \le \sigma \le 1 - C_F(x, Q)} (x^{-1} Q_1^5 T^{\frac{5}{2} n_F})^{1 - \sigma}.$$

Now, for $0 \le \delta < \frac{2}{5n_F}$ and sufficiently small $\epsilon > 0$, we choose

$$Q_1 = x^{\frac{1}{5n_F+10}(2-5n_F\delta-2\epsilon)}(\log x)^{-n_F\frac{A+3}{n_F+2}} \text{ and } T = x^{\frac{2}{5n_F+10}(1+5\delta-\epsilon)}(\log x)^{\frac{2(A+3)}{n_F+2}},$$

which give

$$Q_1^5 T^{\frac{5}{2}n_F} = x^{1-\epsilon}.$$

From the definition of $C_F(x,Q)$, it follows that $x^{-\epsilon C_F(x,Q)} \ll (\log x)^{-(9n_F+14+A)}$ if $1 \le Q \le \exp((\log x)^{3/4})$ and that $x^{-\epsilon C_F(x,Q)} \ll 1$ if $\exp((\log x)^{3/4}) < Q \le Q_1$. Therefore, we deduce

(2.15)
$$\begin{aligned}\max_{Q\le Q_1}\frac{1}{Q}\max_{\frac{1}{2}\le\sigma\le 1-C_F(x,Q)} x^{\sigma-1}N(\sigma,Q,T) &\ll (\log x)^{9n_F+10}\max_{Q\le Q_1}\frac{1}{Q}x^{-\epsilon C_F(x,Q)}\\ &\ll (\log x)^{-A-4}.\end{aligned}$$

Putting (2.10), (2.12), (2.13), (2.14), and (2.15) together, we obtain

(2.16)
$$\begin{aligned}&\sum_{\mathrm{N}(\mathfrak{q})\le Q_1}\frac{1}{\phi(\mathfrak{q})}\sideset{}{'}\sum_{\chi(\mathrm{mod}\,\mathfrak{q})}\max_{y\le h}\max_{N\sim x}|\psi(N+y,\chi)-\psi(N,\chi)-\delta(\chi)y|\\ &\ll h(\log Q_1)(\log\log Q_1)(\log x)(\log x)^{-A-4}+\frac{Q_1 x(\log x)^2}{T}\\ &\ll \frac{h}{(\log x)^{A+1}}+\frac{x^{1-\delta}}{(\log x)^{A+1}}.\end{aligned}$$

Finally, for $x^{1-\delta} \le h \le x$ with $0 \le \delta < \frac{2}{5n_F}$, combining (2.9) and (2.16) yields

$$\sum_{\mathrm{N}(\mathfrak{q})\le x^\theta}\frac{h(\mathfrak{q})}{\phi(\mathfrak{q})}\max_{(\mathfrak{a},\mathfrak{q})=1}\max_{y\le h}\max_{N\sim x}\left|\psi(N+y,\mathfrak{q},\mathfrak{a})-\psi(N,\mathfrak{q},\mathfrak{a})-\frac{1}{h(\mathfrak{q})}y\right| \ll \frac{h}{(\log x)^A}$$

whenever $0 \le \theta < \frac{1}{5n_F+10}(2-5n_F\delta)$, which concludes the proof. □

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 $H \cap C \ne \varnothing$, 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 $F_\mathfrak{q}$ denote the ray class field corresponding to the ray class group modulo $\mathfrak{q}$.

Assume $L \cap F_\mathfrak{q} = \varnothing$. As argued in [40, Sec. 0.5-0.7], by Mackey's induction theorem, for any Hecke character χ modulo $\mathfrak{q}$, one has

$$L(s,\delta_C\times\chi,L/F) = L(s,\delta_{C_H}\times\chi,L/E)^\lambda,$$

where δ_C and δ_{C_H} are the indicator functions of C and C_H, respectively, and $\lambda = \frac{|C||H|}{|G||C_H|}$, and thus one can deduce

(2.17)
$$\sum_{\substack{\mathrm{N}(\mathfrak{p}^m)\le x\\ \mathfrak{p}\sim\mathfrak{a}(\mathrm{mod}\,\mathfrak{q})\\ \sigma_\mathfrak{p}=C}}\log\mathrm{N}(\mathfrak{p}) = \frac{-1}{2\pi i}\frac{1}{h(\mathfrak{q})}\frac{|C|}{|G|}\sum_{\substack{\chi(\mathrm{mod}\,\mathfrak{q})\\ \eta\in\mathrm{Irr}(H)}}\bar\chi(\mathfrak{a})\bar\eta(h_C)\int_{(2)}\frac{L'}{L}(s,\eta\times\chi)\frac{x^s}{s}ds$$

(cf. [40, Eq. (0.7.1) and (1.0.4)]). Moreover, for fixed $\chi \pmod{\mathfrak{q}}$ and $\eta \in \mathrm{Irr}(H)$, via Artin reciprocity, setting

$$\omega(\mathfrak{A}) = \eta(\mathfrak{A})\chi(\mathrm{N}_{E/F}(\mathfrak{A})),$$

for $\mathfrak{A} \subseteq \mathcal{O}_E$, we see that ω is a Hecke character (over E) of modulus $\mathfrak{Q}$ for some $\mathfrak{Q} \subseteq \mathcal{O}_E$ with $\mathrm{N}_{E/F}(\mathfrak{Q}) \ll_L \mathrm{N}(\mathfrak{q})^{n_{E/F}}$ (where $n_{E/F} = [E : F]$), and we have the identification

$$L(s, \omega) = L(s, \eta \times \chi),$$

where $L(s, \omega)$ the Hecke L-function attached to ω. Herein, the proof of Theorem 1.4 goes through verbatim for $L(s, \omega)$; the only proviso is that now we sum over Hecke characters ω (over E) of modulus $\mathfrak{Q}$ for which $\mathrm{N}_{E/F}(\mathfrak{Q}) \ll_L Q_1^{n_{E/F}}$. Hence, denoting the sum on the left of (2.17) by $\psi_C(x, \mathfrak{q}, \mathfrak{a})$, one can bound

$$\left|\psi_C(N + y, \mathfrak{q}, \mathfrak{a}) - \psi_C(N, \mathfrak{q}, \mathfrak{a}) - \frac{1}{h(\mathfrak{q})}\frac{|C|}{|G|}y\right|$$

similarly and then establish the following Chebotarev variant of the Bombieri–Vinogradov theorem in short intervals.

Theorem 2.5. *For $0 \le \delta < \frac{2}{5n_E}$, let $0 \le \theta < \frac{1}{5n_E+10n_{E/F}}(2 - 5n_E\delta)$. Then for any $x^{1-\delta} \le h \le x$ and $A > 0$, one has*

$$\sum_{\mathrm{N}(\mathfrak{q}) \le x^\theta} \max_{(\mathfrak{a},\mathfrak{q})=1} \max_{\substack{y \le h \\ N \sim x}} \left|\pi_C(N + y, \mathfrak{q}, \mathfrak{a}) - \pi_C(N, \mathfrak{q}, \mathfrak{a}) - \frac{1}{h(\mathfrak{q})}\frac{|C|}{|G|}(\mathrm{Li}(N + y) - \mathrm{Li}(N))\right| \ll \frac{h}{(\log x)^A},$$

where the sum is over $\mathfrak{q}$ with $L \cap F_{\mathfrak{q}} = \varnothing$, $\pi_C(x, \mathfrak{q}, \mathfrak{a})$ is the number of primes $\mathfrak{p}$ of F with $\mathrm{N}(\mathfrak{p}) \le x$, $\mathfrak{p} \sim \mathfrak{a} \pmod{\mathfrak{q}}$, and $\sigma_{\mathfrak{p}} = C$, and the implied constant depends on L and A.

3. Preliminaries on CM elliptic curves and associated prime-counting functions

In this section, we shall collect some results for CM elliptic curves and associated prime-counting functions. 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 $E[m]$ 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 $\mathfrak{f} = \mathfrak{f}_E$ such that

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

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

Lemma 3.1. [37, Lemma 6] *If $m \ge 3$, 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 $\bar{E}(\mathbb{F}_p)$ 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

$$\pi_E(x, m) = \#\{p \le x \mid p \nmid N_E \text{ splits completely in } \mathbb{Q}(E[m])\}$$

and $\pi_E(x, 1) = \#\{p \le x \mid p \nmid N_E\}$. We recall that for any square-free $3 \le m \le 2\sqrt{x}$, 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

$$\mathcal{E}(x, m) = \pi_E(x, m) - \frac{1}{n(m)} \operatorname{Li}(x).$$

It follows from the prime number theorem and (2.2) that for any $A > 0$,

$$\mathcal{E}(x, 1) = O\Big(\frac{x}{(\log x)^A}\Big) \tag{3.2}$$

and

$$\mathcal{E}(x, 2) = O_{\mathbb{Q}(E[2]),A}\Big(\frac{x}{(\log x)^A}\Big), \tag{3.3}$$

where the implied constant depends at most on $\mathbb{Q}(E[2])$ and A. Moreover, by Theorem 2.2, for any $x^{1-\delta} \le h \le x$ with $0 \le \delta < \frac{5}{12}$ and $A > 0$, one has

$$\mathcal{E}(x + h, 1) - \mathcal{E}(x, 1) = O\Big(\frac{h}{(\log x)^A}\Big). \tag{3.4}$$

In addition, from Theorem 2.3, it follows that for any $0 \le \delta < \frac{1}{5}$, $x^{1-\delta} \le h \le x$, and $A > 0$,

$$\mathcal{E}(x + h, 2) - \mathcal{E}(x, 2) = O\Big(\frac{h}{(\log x)^A}\Big), \tag{3.5}$$

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 $\operatorname{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$ is a subgroup of $\operatorname{GL}_2(\mathbb{Z}/2\mathbb{Z})$. Hence, $\operatorname{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$ 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 [37, p. 159], respectively).

Lemma 3.3. *If $m \ge 3$ 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 $m \ge 3$, the lemma above yields that

$$\pi_E(x, m) = \frac{1}{2}\tilde{\pi}_E(x, m) + O\Big(\frac{x^{1/2}}{\log x} + \log N_E\Big), \tag{3.6}$$

where

$$\tilde{\pi}_E(x, m) = \#\{\mathfrak{p} \subset \mathcal{O}_K \mid \mathrm{N}(\mathfrak{p}) \le x \text{ and } \mathfrak{p} \nmid \mathfrak{f}\mathfrak{m} \text{ splits completely in } K(E[m])\}.$$

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

$$t(m)[K(E[m]) : K] = h(\mathfrak{f}\mathfrak{m})$$

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 $\pi_c(x,E) = \#\{p \le x \mid p \nmid N_E \text{ and } \bar{E}(\mathbb{F}_p) \text{ is cyclic}\}$. 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 $\mathrm{N}(\mathfrak{f}) \le N_E$, we then obtain

$$\begin{aligned}\pi_c(x,E) &= \sum_{1\le m\le z/\mathrm{N}(\mathfrak{f})^{1/2}} \mu(m)\pi_E(x,m) + O\Big(\sum_{z/\mathrm{N}(\mathfrak{f})^{1/2}\le m\le 2\sqrt{x}} \frac{x}{m^2}\Big)\\ &= \sum_{1\le m\le z/\mathrm{N}(\mathfrak{f})^{1/2}} \mu(m)\pi_E(x,m) + O(N_E^{1/2}xz^{-1}),\end{aligned} \tag{4.1}$$

where $z = z(x)$ is a parameter, satisfying $3 \le z/\mathrm{N}(\mathfrak{f})^{1/2} \le 2\sqrt{x}$, to be chosen later. Thus, by (3.4), (3.5), and (4.1), we can express $\pi_c(x+h,E) - \pi_c(x,E)$ as

$$\begin{aligned}&\pi_E(x+h,1) - \pi_E(x,1) - (\pi_E(x+h,2) - \pi_E(x,2))\\ &\quad + \sum_{3\le m\le z/\mathrm{N}(\mathfrak{f})^{1/2}} \mu(m)(\pi_E(x+h,m) - \pi_E(x,m)) + O(N_E^{1/2}xz^{-1})\\ &= \Big(1 - \frac{1}{n(2)}\Big)(\mathrm{Li}(x+h) - \mathrm{Li}(x)) + O_{\mathbb{Q}(E[2]),A}\Big(\frac{h}{(\log x)^A}\Big)\\ &\quad + \sum_{3\le m\le z/\mathrm{N}(\mathfrak{f})^{1/2}} \mu(m)(\pi_E(x+h,m) - \pi_E(x,m)) + O(N_E^{1/2}xz^{-1})\end{aligned} \tag{4.2}$$

whenever $x^{1-\delta} \le h \le x$ with $\delta \in [0, \frac{1}{5})$. Also, by (3.6), we have

$$\begin{aligned}&\sum_{3\le m\le z/\mathrm{N}(\mathfrak{f})^{1/2}} \mu(m)\pi_E(x,m)\\ &= \sum_{3\le m\le z/\mathrm{N}(\mathfrak{f})^{1/2}} \mu(m)\Big(\frac{1}{2}\tilde{\pi}_E(x,m) + O\Big(\frac{x^{1/2}}{\log x} + \log N_E\Big)\Big)\\ &= \frac{1}{2}\sum_{3\le m\le z/\mathrm{N}(\mathfrak{f})^{1/2}} \mu(m)\frac{\mathrm{Li}(x)}{[K(E[m]):K]} + \frac{1}{2}\sum_{3\le m\le z/\mathrm{N}(\mathfrak{f})^{1/2}} \mu(m)\tilde{\mathcal{E}}(x,m)\\ &\quad + O\Big(\frac{x^{1/2}z}{\log x} + (\log N_E)z\Big),\end{aligned} \tag{4.3}$$

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

$$\tilde{\mathcal{E}}(x,m) = \tilde{\pi}_E(x,m) - \frac{\mathrm{Li}(x)}{[K(E[m]):K]}.$$

Note that it follows from Lemma 3.4 that

$$\tilde{\mathcal{E}}(x,m)=\tilde{\pi}_E(x,m)-\frac{\mathrm{Li}(x)}{[K(E[m]):K]}=\sum_{i=1}^{t(m)}\Big(\pi(x,\mathfrak{fm},\mathfrak{m}_i)-\frac{\mathrm{Li}(x)}{h(\mathfrak{fm})}\Big).$$

Thus, by Theorem 1.4 (for $z^2\le x^\theta$ with $0\le\theta<\frac{1}{10}(1-5\delta)$ and $0\le\delta<\frac{1}{5}$), the fact that $T(\mathfrak{q})\le 6$ in our consideration, and Lemma 3.4, for any $A>0$, we derive

(4.4)

$$\begin{aligned}
&\sum_{3\le m\le z/\,\mathrm{N}(\mathfrak{f})^{1/2}}\big|\tilde{\mathcal{E}}(x+h,m)-\tilde{\mathcal{E}}(x,m)\big|\\
&\le\sum_{3\le\mathrm{N}(\mathfrak{fm})\le z^2}\sum_{i=1}^{t(m)}\Big|\pi(x+h,\mathfrak{fm},\mathfrak{m}_i)-\pi(x,\mathfrak{fm},\mathfrak{m}_i)-\frac{\mathrm{Li}(x+h)-\mathrm{Li}(x)}{h(\mathfrak{fm})}\Big|\\
&\ll N_E(\log N_E)\sum_{\mathrm{N}(\mathfrak{q})\le z^2}\max_{(\mathfrak{a},\mathfrak{q})=1}\Big|\pi(x+h,\mathfrak{q},\mathfrak{a})-\pi(x,\mathfrak{q},\mathfrak{a})-\frac{\mathrm{Li}(x+h)-\mathrm{Li}(x)}{h(\mathfrak{q})}\Big|\\
&\ll_A N_E(\log N_E)\frac{h}{(\log x)^A}.
\end{aligned}$$

(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

$$\begin{aligned}
&\sum_{1\le m\le z/\,\mathrm{N}(\mathfrak{f})^{1/2}}\frac{\mu(m)}{n(m)}(\mathrm{Li}(x+h)-\mathrm{Li}(x))\\
&+O\Big(N_E^{1/2}xz^{-1}+N_E(\log N_E)\frac{h}{(\log x)^A}+\frac{x^{1/2}z}{\log x}+(\log N_E)z\Big)
\end{aligned}$$

whenever $z^2\le x^\theta$ and $x^{1-\delta}\le h\le x$ with $0\le\theta<\frac{1}{10}(1-5\delta)$ and $0\le\delta<\frac{1}{5}$. Finally, as $n(m)=[\mathbb{Q}(E[m]):\mathbb{Q}]\gg\phi(m)^2\gg\frac{m^2}{(\log\log m)^2}$ and L'Hôpital's rule gives

$$\lim_{z\to\infty}\Big(\int_z^\infty\frac{(\log\log t)^2}{t^2}dt\Big)/\Big(\frac{\log z}{z}\Big)=0,$$

one has

$$\sum_{m>z/\,\mathrm{N}(\mathfrak{f})^{1/2}}\frac{\mu(m)}{n(m)}(\mathrm{Li}(x+h)-\mathrm{Li}(x))\ll\sum_{m>z/\,\mathrm{N}(\mathfrak{f})^{1/2}}\frac{(\log\log m)^2}{m^2}\frac{h}{\log x}\ll\frac{N_E^{1/2}h}{z}.$$

Herein, for any $0\le\delta<\frac{1}{25}$ and $x^{1-\delta}\le h\le x$, we have

$$\pi_c(x+h,E)-\pi_c(x,E)=\mathfrak{c}_E(\mathrm{Li}(x+h)-\mathrm{Li}(x))+O\Big(N_E(\log N_E)\frac{h}{(\log x)^A}\Big),$$

which completes the proof.

5. Proof of Theorem 1.2

Throughout this section, we let p denote a rational prime coprime to N_E. Recall that by Weil's bound, one has

$$\pi_e(x,E)=\sum_{p\le x}e_p=\sum_{p\le x}\frac{p}{d_p}+O\Big(\frac{x^{3/2}}{\log x}\Big).$$

As argued in [15] and [52], by the identity

$$\frac{1}{m}=\sum_{de|m}\frac{\mu(d)}{e},$$

one has

$$\sum_{p\le x}\frac{p}{d_p}=\sum_{p\le x}p\sum_{de|d_p}\frac{\mu(d)}{e}=\sum_{m\le 2\sqrt{x}}\sum_{de|m}\frac{\mu(d)}{e}\sum_{\substack{p\le x\\ m|d_p}}p.$$

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

$$\sum_{m\le z/N(\mathfrak{f})^{1/2}}\sum_{de|m}\frac{\mu(d)}{e}\sum_{\substack{p\le x\\ m|d_p}}p+\sum_{z/N(\mathfrak{f})^{1/2}\le m\le 2\sqrt{x}}\sum_{de|m}\frac{\mu(d)}{e}\sum_{\substack{p\le x\\ m|d_p}}p+O\Big(\frac{x^{3/2}}{\log x}\Big),\tag{5.1}$$

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

$$\Big|\sum_{de|m}\frac{\mu(d)}{e}\Big|\le 1,$$

Lemma 3.5, combined with (3.1), yields that the last triple sum in (5.1) is

$$\ll\sum_{z/N(\mathfrak{f})^{1/2}\le m\le 2\sqrt{x}}\frac{x^2}{m^2}\ll\frac{N_E^{1/2}x^2}{z}.$$

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

$$\begin{aligned}&(x+h)\pi_E(x+h,m)-\int_2^{x+h}\pi_E(t,m)dt-\Big(x\pi_E(x,m)-\int_2^x\pi_E(t,m)dt\Big)\\&=x(\pi_E(x+h,m)-\pi_E(x,m))+h\pi_E(x+h,m)\\&-\int_2^{x+h}\pi_E(t,m)dt+\int_2^x\pi_E(t,m)dt.\end{aligned}$$

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

$$\begin{aligned}&x\Big(\frac{1}{n(m)}(\operatorname{Li}(x+h)-\operatorname{Li}(x))+\mathcal{E}(x+h,m)-\mathcal{E}(x,m)\Big)\\&+h\Big(\frac{1}{n(m)}\operatorname{Li}(x+h)+\mathcal{E}(x+h,m)\Big)-\int_2^{x+h}\frac{1}{n(m)}\operatorname{Li}(t)dt+\int_2^x\frac{1}{n(m)}\operatorname{Li}(t)dt\\&-\int_2^{x+h}\mathcal{E}(t,m)dt+\int_2^x\mathcal{E}(t,m)dt.\end{aligned}$$

Thus, as $\mathrm{Li}(x^2) = x\,\mathrm{Li}(x) - \int_2^x \mathrm{Li}(t)dt + O(1)$, we have

$$\sum_{\substack{p\le x+h\\ m\mid d_p}} p - \sum_{\substack{p\le x\\ m\mid d_p}} p = \frac{1}{n(m)}(\mathrm{Li}((x+h)^2) - \mathrm{Li}(x^2)) + O(1) \tag{5.2}$$
$$+ O\Big(x|\mathcal{E}(x+h,m) - \mathcal{E}(x,m)| + h\max_{x\le t\le x+h}|\mathcal{E}(t,m)|\Big).$$

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

$$\sum_{3\le m\le z/\,\mathrm{N}(\mathfrak{f})^{1/2}} \max_{x\le t\le x+h}\Big|\tilde{\pi}_E(t,m) - \frac{1}{[K(E[m]):K]}\,\mathrm{Li}(t)\Big| \ll_A N_E(\log N_E)\frac{x}{(\log x)^A}$$

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

$$\sum_{3\le m\le z/N(\mathfrak{f})^{1/2}} \Big(x|\mathcal{E}(x+h,m) - \mathcal{E}(x,m)| + h\max_{x\le t\le x+h}|\mathcal{E}(t,m)|\Big) \tag{5.3}$$
$$\ll N_E(\log N_E)\frac{xh}{(\log x)^A} + \frac{x^{3/2}z}{\log x} + (\log N_E)(xz),$$

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

$$\sum_{m\le z/N(\mathfrak{f})^{1/2}}\sum_{de\mid m}\frac{\mu(d)}{e}\sum_{\substack{p\le x+h\\ m\mid d_p}} p - \sum_{m\le z/N(\mathfrak{f})^{1/2}}\sum_{de\mid m}\frac{\mu(d)}{e}\sum_{\substack{p\le x\\ m\mid d_p}} p$$

is equal to

$$\sum_{1\le m\le z/N(\mathfrak{f})^{1/2}}\sum_{de\mid m}\frac{\mu(d)}{e}\frac{1}{n(m)}(\mathrm{Li}((x+h)^2) - \mathrm{Li}(x^2))$$
$$+ O\Big(\frac{xh}{(\log x)^A}\Big) + O\Big(N_E(\log N_E)\frac{xh}{(\log x)^A} + \frac{x^{3/2}z}{\log x} + (\log N_E)(xz)\Big),$$

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

$$\sum_{m>z/N(\mathfrak{f})^{1/2}}\sum_{de\mid m}\frac{\mu(d)}{e}\frac{1}{n(m)}(\mathrm{Li}((x+h)^2) - \mathrm{Li}(x^2)) \ll \frac{N_E^{1/2}xh}{z},$$

and hence

$$\pi_e(x+h,E) - \pi_e(x,E) = \mathfrak{e}_E(\mathrm{Li}((x+h)^2) - \mathrm{Li}(x^2))$$
$$+ O\Big(N_E(\log N_E)\frac{xh}{(\log x)^A} + \frac{x^{3/2}z}{\log x} + \frac{N_E^{1/2}x^2}{z}\Big)$$

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

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

for any $x^{1-\delta} \le h \le x$. 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 ℓ 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 ℓ of $n\in\mathbb{N}$ for which $\ell\le y$.

We consider

$$\begin{aligned}&\sum_{x<p\le x+h}(\omega(|\bar{E}(\mathbb{F}_p)|)-\log\log x)^2\\&=\sum_{x<p\le x+h}\omega^2(|\bar{E}(\mathbb{F}_p)|)-2(\log\log x)\sum_{x<p\le x+h}\omega(|\bar{E}(\mathbb{F}_p)|)+(\log\log x)^2\sum_{x<p\le x+h}1.\end{aligned}$$

By the prime number theorem in short intervals established by Huxley [24], the last term is

$$(\mathrm{Li}(x+h)-\mathrm{Li}(x))(\log\log x)^2+O\Big(\frac{h}{(\log x)^2}(\log\log x)^2\Big)$$

for $x^{1-\delta}\le h\le x$ with $\delta\in[0,\frac{5}{12})$. Observing that for $p\le x+h$,

$$|\bar{E}(\mathbb{F}_p)|\le p+2\sqrt{p}+1\le 6x,$$

and that the number of prime divisors ℓ of any $n\le 6x$ for which $\ell>y$ is at most $\frac{2}{\eta}$ (for $x\ge 6$), we may write the second-to-last sum of the equation above as

$$\begin{aligned}\sum_{x<p\le x+h}\omega(|\bar{E}(\mathbb{F}_p)|)&=\sum_{x<p\le x+h}\omega_y(|\bar{E}(\mathbb{F}_p)|)+\sum_{x<p\le x+h}O(1)\\&=\sum_{x<p\le x+h}\omega_y(|\bar{E}(\mathbb{F}_p)|)+O\Big(\frac{h}{\log x}\Big).\end{aligned}$$

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 $p\ne 2$ is inert in K, then the Legendre symbol $(\frac{-D}{p})=-1$, and $|\bar{E}(\mathbb{F}_p)|=p+1$. Let $a_1,\dots,a_{r(\ell)}\in(\mathbb{Z}/\ell D\mathbb{Z})^\times$ be integers for which $a_i\equiv -1 \pmod{\ell}$ and $(\frac{-D}{a_i})=-1$. Then it follows from Theorem 2.2 and the estimate $r(\ell)\ll 1$ that for any $\delta\in[0,\frac{5}{12})$ and $x^{1-\delta}\le h\le x$,

$$\begin{aligned}\sum_{\substack{x<p\le x+h\\ p\text{ supersingular}}}\omega_y(|\bar{E}(\mathbb{F}_p)|)&=\sum_{\ell\le y}\sum_{\substack{x<p\le x+h\\ p\text{ supersingular}\\ \ell\mid|\bar{E}(\mathbb{F}_p)|}}1+O(y)\\&=\sum_{\ell\le y}\sum_{i=1}^{r(\ell)}\sum_{\substack{x<p\le x+h\\ p\equiv a_i\,(\mathrm{mod}\,\ell D)}}1+O(y)\\&=\sum_{\ell\le y}\frac{r(\ell)}{\phi(\ell D)}(\mathrm{Li}(x+h)-\mathrm{Li}(x))+O\Big(\frac{h}{(\log x)^2}\Big)\end{aligned}$$

whenever $\eta < \theta$, with θ satisfying condition (2.3). As $\frac{r(\ell)}{\phi(\ell D)} = \frac{1}{2(\ell-1)}$, by Mertens's theorem (see, e.g., [12, Ch. 7]), we see that

$$\sum_{\substack{x<p\le x+h\\ p \text{ supersingular}}} \omega_y(|\bar{E}(\mathbb{F}_p)|) = \frac{1}{2}(\mathrm{Li}(x+h)-\mathrm{Li}(x))(\log\log x) + O\Big(\frac{h}{\log x}\Big).$$

Now we consider ordinary primes p. We let π_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 ℓ ramified in K, we can only consider the unramified primes ℓ and divide them into two groups, namely, ℓ is inert or ℓ splits.

For ℓ 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 $x^{1-\delta}\le h\le x$,

$$\begin{aligned}\sum_{\substack{\ell\le y\\ \ell \text{ inert}}}\sum_{\substack{x<p\le x+h\\ p \text{ ordinary}\\ \ell\mid|\bar{E}(\mathbb{F}_p)|}} 1 &\ll \sum_{\substack{\mathrm{N}((\ell))=\ell^2\le y^2\\ \ell \text{ inert}}}\sum_{\substack{x<p\le x+h\\ p \text{ ordinary}\\ (\pi_p)\sim(1)\,(\mathrm{mod}(\ell))}} 1\\ &\ll \sum_{\substack{\mathrm{N}((\ell))=\ell^2\le y^2\\ \ell \text{ inert}}} \frac{1}{h((\ell))}(\mathrm{Li}(x+h)-\mathrm{Li}(x)) + O\Big(\frac{h}{(\log x)^2}\Big),\end{aligned}$$

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

$$h((\ell)) \ge \frac{\phi(\ell^2)}{6},$$

and thus

$$\sum_{\substack{\ell\le y\\ \ell \text{ inert}}}\sum_{\substack{x<p\le x+h\\ p \text{ ordinary}\\ \ell\mid|\bar{E}(\mathbb{F}_p)|}} 1 \ll \frac{h}{\log x}.$$

For ℓ splitting in K, we write $(\ell)=\mathfrak{l}_1\mathfrak{l}_2$. Now the condition $\ell \mid |\bar{E}(\mathbb{F}_p)|$ tells us that $\pi_p \equiv 1 \pmod{\mathfrak{l}_1}$ or $\pi_p \equiv 1 \pmod{\mathfrak{l}_2}$. Therefore, letting $\mathfrak{l}$ stand for $\mathfrak{l}_1$ or $\mathfrak{l}_2$ (depending on the pertinent congruence condition) and applying Theorem 1.4, for any $\delta \in [0,\frac{1}{5})$ and $x^{1-\delta}\le h\le x$, we have

$$\begin{aligned}\sum_{\substack{\ell\le y\\ \ell \text{ splits}}}\sum_{\substack{x<p\le x+h\\ p \text{ ordinary}\\ \ell\mid|\bar{E}(\mathbb{F}_p)|}} 1 &= \frac{1}{2}\sum_{\substack{\mathrm{N}(\mathfrak{l})=\ell\le y\\ \ell \text{ splits}}}\sum_{\substack{x<p\le x+h\\ p \text{ ordinary}\\ \pi_p\equiv 1 \,(\mathrm{mod}\,\mathfrak{l})}} 1\\ &= \frac{1}{2}\sum_{\substack{\mathrm{N}(\mathfrak{l})=\ell\le y\\ \ell \text{ splits}}}\frac{1}{T(\mathfrak{l})}\sum_{\substack{x<\mathrm{N}((\pi_p))=p\le x+h\\ p \text{ ordinary}\\ (\pi_p)\sim(1)\,(\mathrm{mod}\,\mathfrak{l})}} 1\\ &= \frac{1}{2}\sum_{\substack{\mathrm{N}(\mathfrak{l})=\ell\le y\\ \ell \text{ splits}}}\frac{1}{\phi(\mathfrak{l})}(\mathrm{Li}(x+h)-\mathrm{Li}(x)) + O\Big(\frac{h}{(\log x)^2}\Big),\end{aligned}$$

provided that $\eta < \frac{1}{10}(1-5\delta)$. As $(\ell) = \mathfrak{l}_1\mathfrak{l}_2$, we derive

$$\sum_{\substack{\ell\le y\\ \ell \text{ splits}}}\sum_{\substack{x<p\le x+h\\ p \text{ ordinary}\\ \ell\mid\mid \bar{E}(\mathbb{F}_p)|}} 1 = \frac{1}{2}\cdot 2\sum_{\substack{\ell\le y\\ \ell \text{ splits}}}\frac{1}{\phi(\ell)}(\mathrm{Li}(x+h)-\mathrm{Li}(x)) + O\Big(\frac{h}{(\log x)^2}\Big)$$
$$= \frac{1}{2}(\mathrm{Li}(x+h)-\mathrm{Li}(x))(\log\log x) + O\Big(\frac{h}{\log x}\Big),$$

where the last estimate follows form Mertens's theorem and the fact that $\ell \neq 2$ splits in K if and only if $(\frac{-D}{p}) = 1$. Finally, for any $\delta \in [0, \frac{1}{5})$, choosing $\eta < \frac{1}{20}(1-5\delta)$, we arrive at

$$\sum_{x<p\le x+h}\omega(|\bar{E}(\mathbb{F}_p)|) = (\mathrm{Li}(x+h)-\mathrm{Li}(x))(\log\log x) + O\Big(\frac{h}{\log x}\Big)$$

whenever $x^{1-\delta} \le h \le x$. Moreover, by an analogous argument, for any $\delta \in [0, \frac{1}{5})$, choosing $\eta < \frac{1}{40}(1-5\delta)$, we have

$$\sum_{x<p\le x+h}\omega^2(|\bar{E}(\mathbb{F}_p)|) = (\mathrm{Li}(x+h)-\mathrm{Li}(x))(\log\log x)^2 + O\Big(\frac{h(\log\log x)}{\log x}\Big).$$

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

$$\sum_{x<n\le x+h}\omega(n) = \sum_{x<n\le x+h}\omega_y(n) + \sum_{x<n\le x+h}O(1) = \sum_{x<n\le x+h}\omega_y(n) + O(h)$$

and

$$\sum_{x<n\le x+h}\omega_y(n) = \sum_{x<n\le x+h}\sum_{\substack{\ell\mid n\\ \ell\le y}}1 = \sum_{\ell\le y}\sum_{\substack{x<n\le x+h\\ \ell\mid n}}1 = \sum_{\ell\le y}\Big(\Big\lfloor\frac{x+h}{\ell}\Big\rfloor - \Big\lfloor\frac{x}{\ell}\Big\rfloor\Big),$$

observing that the last sum is

$$\sum_{\ell\le y}\frac{h}{\ell} + O(y) = h\log\log x + O(h+y),$$

and then choosing $\eta \le 1-\delta$, one has $\sum_{x<n\le x+h}\omega(n) = h\log\log x + O(h)$. Similarly, one can show that $\sum_{x<n\le x+h}\omega^2(n) = h(\log\log x)^2 + O(h(\log\log x))$ and conclude the following.

Theorem 6.2. *Let $\delta \in [0,1)$. Then for any $x^{1-\delta} \le h \le x$, one has*

$$\sum_{x<n\le x+h}(\omega(n)-\log\log x)^2 = O(h(\log\log x)).$$

Furthermore, in much the same spirit, as one can write

$$\sum_{x<p\le x+h}\omega_y(p-a) = \sum_{x<p\le x+h}\sum_{\substack{\ell\mid p-a\\ \ell\le y}}1 = \sum_{\ell\le y}\sum_{\substack{x<p\le x+h\\ p\equiv a \pmod\ell}}1,$$

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 $\delta \in [0, \frac{5}{12})$. Then for any $x^{1-\delta} \le h \le x$, one has*

$$\sum_{x<p\le x+h} (\omega(p-a) - \log\log x)^2 = O\Big(\frac{h}{\log x}(\log\log x)\Big),$$

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

[1] Amir Akbary and V. Kumar Murty, *An analogue of the Siegel-Walfisz theorem for the cyclicity of CM elliptic curves mod p*, Indian J. Pure Appl. Math. **41** (2010), no. 1, 25–37, DOI 10.1007/s13226-010-0002-4. MR2650098

[2] Antal Balog and Ken Ono, *The Chebotarev density theorem in short intervals and some questions of Serre*, J. Number Theory **91** (2001), no. 2, 356–371, DOI 10.1006/jnth.2001.2694. MR1876282

[3] 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, DOI 10.4064/aa-52-2-163-170. MR1005602

[4] E. Bombieri, J. B. Friedlander, and H. Iwaniec, *Primes in arithmetic progressions to large moduli*, Acta Math. **156** (1986), no. 3-4, 203–251, DOI 10.1007/BF02399204. MR834613

[5] E. Bombieri, J. B. Friedlander, and H. Iwaniec, *Primes in arithmetic progressions to large moduli. II*, Math. Ann. **277** (1987), no. 3, 361–393, DOI 10.1007/BF01458321. MR891581

[6] E. Bombieri, J. B. Friedlander, and H. Iwaniec, *Primes in arithmetic progressions to large moduli. III*, J. Amer. Math. Soc. **2** (1989), no. 2, 215–224, DOI 10.2307/1990976. MR976723

[7] Nancy Childress, *Class field theory*, Universitext, Springer, New York, 2009. MR2462595

[8] Alina Carmen Cojocaro, *Cyclicity of elliptic curves modulo p*, ProQuest LLC, Ann Arbor, MI, 2002. Thesis (Ph.D.)–Queen's University (Canada). MR2703535

[9] Alina Carmen Cojocaru, *Cyclicity of CM elliptic curves modulo p*, Trans. Amer. Math. Soc. **355** (2003), no. 7, 2651–2662, DOI 10.1090/S0002-9947-03-03283-5. MR1975393

[10] Alina Carmen Cojocaru and M. Ram Murty, *Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem*, Math. Ann. **330** (2004), no. 3, 601–625, DOI 10.1007/s00208-004-0562-x. MR2099195

[11] Mark Coleman and Andrew Swallow, *Localised Bombieri–Vinogradov theorems in imaginary quadratic fields*, Acta Arith. **120** (2005), no. 4, 349–377, DOI 10.4064/aa120-4-3. MR2190070

[12] Harold Davenport, *Multiplicative number theory*, 3rd ed., Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York, 2000. Revised and with a preface by Hugh L. Montgomery. MR1790423

[13] Max Deuring, *Über den Tschebotareffschen Dichtigkeitssatz*, Math. Ann. **110** (1935), no. 1, 414–415, DOI 10.1007/BF01448036. MR1512947

[14] P. Erdős, *On the normal order of prime factors of $p-1$ and some related problems concerning Euler's ϕ-functions*, Q. J. Math. (Oxford) **6** (1935), 205–213.

[15] Tristan Freiberg and Pär Kurlberg, *On the average exponent of elliptic curves modulo p*, Int. Math. Res. Not. IMRN **8** (2014), 2265–2293, DOI 10.1093/imrn/rns280. MR3194018

[16] P. X. Gallagher, *Bombieri's mean value theorem*, Mathematika **15** (1968), 1–6, DOI 10.1112/S002557930000231X. MR237442

[17] Rajiv Gupta and M. Ram Murty, *Cyclicity and generation of points mod p on elliptic curves*, Invent. Math. **101** (1990), no. 1, 225–235, DOI 10.1007/BF01231502. MR1055716

[18] G. H. Hardy and S. Ramanujan, *The normal number of prime factors of a number n*, Quart. J. Pure. Appl. Math. **48** (1917), 76–97.

[19] G. H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, fourth ed., Oxford, at the Clarendon Press, 1960.
[20] D. R. Heath-Brown, *On the density of the zeros of the Dedekind zeta-function*, Acta Arith. **33** (1977), no. 2, 169–181, DOI 10.4064/aa-33-2-169-181. MR434988
[21] Jürgen Hinz, *Über Nullstellen der Heckeschen Zetafunctionen in algebraischen Zahlkörpern*, Acta Arith. **31** (1976), no. 2, 167–193, DOI 10.4064/aa-31-2-167-193. MR424756
[22] Jürgen G. Hinz, *A generalization of Bombieri's prime number theorem to algebraic number fields*, Acta Arith. **51** (1988), no. 2, 173–193, DOI 10.4064/aa-51-2-173-193. MR975109
[23] M. N. Huxley, *The large sieve inequality for algebraic number fields. III. Zero-density results*, J. London Math. Soc. (2) **3** (1971), 233–240, DOI 10.1112/jlms/s2-3.2.233. MR276196
[24] M. N. Huxley, *On the difference between consecutive primes*, Invent. Math. **15** (1972), 164–170, DOI 10.1007/BF01418933. MR292774
[25] M. N. Huxley and H. Iwaniec, *Bombieri's theorem in short intervals*, Mathematika **22** (1975), no. 2, 188–194, DOI 10.1112/S0025579300006069. MR389790
[26] David Johnson, *Mean values of Hecke L-functions*, J. Reine Angew. Math. **305** (1979), 195–205, DOI 10.1515/crll.1979.305.195. MR518861
[27] Matti Jutila, *A statistical density theorem for L-functions with applications*, Acta Arith. **16** (1969/70), 207–216, DOI 10.4064/aa-16-2-207-216. MR252336
[28] Henryk Iwaniec and Emmanuel Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004. MR2061214
[29] Sungjin Kim, *Average behaviors of invariant factors in Mordell-Weil groups of CM elliptic curves modulo p*, Finite Fields Appl. **30** (2014), 178–190, DOI 10.1016/j.ffa.2014.07.003. MR3249828
[30] Edmund Landau, *Über Ideale und Primideale in Idealklassen* (German), Math. Z. **2** (1918), no. 1-2, 52–154, DOI 10.1007/BF01212899. MR1544310
[31] S. Lang and H. Trotter, *Primitive points on elliptic curves*, Bull. Amer. Math. Soc. **83** (1977), no. 2, 289–292, DOI 10.1090/S0002-9904-1977-14310-3. MR427273
[32] Yu-Ru Liu, *Prime divisors of the number of rational points on elliptic curves with complex multiplication*, Bull. London Math. Soc. **37** (2005), no. 5, 658–664, DOI 10.1112/S0024609305004558. MR2164827
[33] Takayoshi Mitsui, *Generalized prime number theorem*, Jpn. J. Math. **26** (1956), 1–42, DOI 10.4099/jjm1924.26.0_1. MR92814
[34] Takayoshi Mitsui, *On the prime ideal theorem*, J. Math. Soc. Japan **20** (1968), 233–247, DOI 10.2969/jmsj/02010233. MR223314
[35] S. Ali Miri and V. Kumar Murty, *An application of sieve methods to elliptic curves*, Progress in cryptology—INDOCRYPT 2001 (Chennai), Lecture Notes in Comput. Sci., vol. 2247, Springer, Berlin, 2001, pp. 91–98, DOI 10.1007/3-540-45311-3_9. MR1934487
[36] Hugh L. Montgomery, *Topics in multiplicative number theory*, Lecture Notes in Mathematics, Vol. 227, Springer-Verlag, Berlin-New York, 1971. MR0337847
[37] M. Ram Murty, *On Artin's conjecture*, J. Number Theory **16** (1983), no. 2, 147–168, DOI 10.1016/0022-314X(83)90039-2. MR698163
[38] M. Ram Murty and V. Kumar Murty, *Prime divisors of Fourier coefficients of modular forms*, Duke Math. J. **51** (1984), no. 1, 57–76, DOI 10.1215/S0012-7094-84-05104-4. MR744288
[39] M. Ram Murty and V. Kumar Murty, *A variant of the Bombieri–Vinogradov theorem*, Number theory (Montreal, Que., 1985), CMS Conf. Proc., vol. 7, Amer. Math. Soc., Providence, RI, 1987, pp. 243–272. MR894326
[40] M. Ram Murty and Kathleen L. Petersen, *A Bombieri–Vinogradov theorem for all number fields*, Trans. Amer. Math. Soc. **365** (2013), no. 9, 4987–5032, DOI 10.1090/S0002-9947-2012-05805-3. MR3066777
[41] 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. MR808422
[42] A. Perelli, J. Pintz, and S. Salerno, *Bombieri's theorem in short intervals. II*, Invent. Math. **79** (1985), no. 1, 1–9, DOI 10.1007/BF01388653. MR774526
[43] S. J. Ricci, *Mean-value theorems for primes in short intervals*, Proc. London Math. Soc. (3) **37** (1978), no. 2, 230–242, DOI 10.1112/plms/s3-37.2.230. MR507605
[44] Michael Rosen, *A generalization of Mertens' theorem*, J. Ramanujan Math. Soc. **14** (1999), no. 1, 1–19. MR1700882

[45] J.-P. Serre, *Résumé des cours de l'année scolaire 1977-1978*, Annuaire du Collège de France, 1978, 67-70, in Collected Papers, volume III, Springer-Verlag, 1985.
[46] A. V. Sokolovskiĭ, *A theorem on the zeros of Dedekind's zeta-function and the distance between "neighboring" prime ideals* (Russian), Acta Arith. **13** (1967/68), 321–334. MR223332
[47] Jesse Thorner, *A variant of the Bombieri–Vinogradov theorem in short intervals and some questions of Serre*, Math. Proc. Cambridge Philos. Soc. **161** (2016), no. 1, 53–63, DOI 10.1017/S0305004116000050. MR3505669
[48] N. M. Timofeev, *Distribution of arithmetic functions in short intervals in the mean with respect to progressions* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **51** (1987), no. 2, 341–362, 447, DOI 10.1070/IM1988v030n02ABEH001013; English transl., Math. USSR-Izv. **30** (1988), no. 2, 315–335. MR897001
[49] Paul Turán, *On a Theorem of Hardy and Ramanujan*, J. London Math. Soc. **9** (1934), no. 4, 274–276, DOI 10.1112/jlms/s1-9.4.274. MR1574877
[50] R. C. Vaughan, *Mean value theorems in prime number theory*, J. London Math Soc. (2) **10** (1975), 153–162, DOI 10.1112/jlms/s2-10.2.153. MR0376567
[51] Robin J. Wilson, *The large sieve in algebraic number fields*, Mathematika **16** (1969), 189–204, DOI 10.1112/S0025579300008160. MR263774
[52] J. Wu, *The average exponent of elliptic curves modulo p*, J. Number Theory **135** (2014), 28–35, DOI 10.1016/j.jnt.2013.08.009. MR3128449
[53] Tao Zhan, *Bombieri's theorem in short intervals*, Acta Math. Sinica (N.S.) **5** (1989), no. 1, 37–47, DOI 10.1007/BF02107621. A Chinese summary appears in Acta Math. Scinica **33** (1989), no. 2, 287. MR998386

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

Email address: pengjie.wong@uleth.ca