ACTA ARITHMETICA
168.1 (2015)

On invariants of elliptic curves on average

by

Amir Akbary and Adam Tyler Felix (Lethbridge)

1. Introduction and results. Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N. For a prime p of good reduction (i.e. $p \nmid N$), let E_p be the reduction mod p of E. It is known that $E_p(\mathbb{F}_p)$, the group of rational points of E over the finite field $\mathbb{F}_p$, is the product of at most two cyclic groups, namely

$$E_p(\mathbb{F}_p) \cong (\mathbb{Z}/i_E(p)\mathbb{Z}) \times (\mathbb{Z}/e_E(p)\mathbb{Z}),$$

where $i_E(p)$ divides $e_E(p)$. Thus, $e_E(p)$ is the exponent of $E_p(\mathbb{F}_p)$ and $i_E(p)$ is the index of the largest cyclic subgroup of $E_p(\mathbb{F}_p)$. In recent years there has been a lot of interest in studying the distribution of the invariants $i_E(p)$ and $e_E(p)$.

Borosh, Moreno, and Porta [8] were the first to study $i_E(p)$ computationally and conjectured that, for some elliptic curves, $i_E(p) = 1$ occurs often. We note that $i_E(p) = 1$ if and only if $E_p(\mathbb{F}_p)$ is cyclic. Let

$$N_E(x) = \#\{p \leq x;\ p \nmid N \text{ and } E_p(\mathbb{F}_p) \text{ is cyclic}\}. \tag{1.1}$$

Then Serre [29], under the assumption of the generalized Riemann hypothesis (GRH) for division fields $\mathbb{Q}(E[k])$, proved that $N_E(x) \sim c_E \operatorname{li}(x)$ as $x \to \infty$, where $c_E > 0$ if and only if $\mathbb{Q}(E[2]) \neq \mathbb{Q}$. Here $\operatorname{li}(x) = \int_2^x dt/\log t$. For the curves with complex multiplication (CM), Murty [28] removed the assumption of the GRH. Also, he showed that under GRH one can obtain the estimate $O(x \log\log x/(\log x)^2)$ for the error term in the asymptotic formula for $N_E(x)$ for any elliptic curve E. The value of the error term is improved to $O(x^{5/6}(\log x)^{2/3})$ in [10]. In [3], following the method of [28] in the CM case, the error term $O(x/(\log x)^A)$ for any $A > 1$ is established.

Another problem closely related to cyclicity is finding the average value of the number of divisors of $i_E(p)$ as p varies over primes. Let $\tau(n)$ denote

2010 *Mathematics Subject Classification*: 11G05, 11G20.
Key words and phrases: reduction mod p of elliptic curves, invariants of elliptic curves, average results.

DOI: 10.4064/aa168-1-3 © Instytut Matematyczny PAN, 2015

the number of divisors of n. In [1], Akbary and Ghioca proved that

$$\sum_{p\le x}\tau(i_E(p)) = c_E\,\mathrm{li}(x) + O(x^{5/6}(\log x)^{2/3})$$

if GRH holds, and

$$\sum_{p\le x}\tau(i_E(p)) = c_E\,\mathrm{li}(x) + O\left(\frac{x}{(\log x)^A}\right),$$

for $A>1$, if E has CM. In the above asymptotic formulas, c_E is a positive constant which depends only on E.

The average value of $i_E(p)$ is a more challenging problem. In [26], Kowalski proposed this problem and proved unconditionally that the lower bound $\log\log x$ holds for

$$\frac{1}{x/\log x}\sum_{p\le x} i_E(p)$$

if E has CM. He also showed that, for a non-CM curve, the above quantity is bounded from below.

A more approachable problem is finding the average value of $e_E(p)$. Freiberg and Kurlberg [16] were the first to consider this problem and established conditional (unconditional in the CM case) asymptotic formulas for $\sum_{p\le x} e_E(p)$. Felix and Murty [14] proved, for k a fixed positive integer, the following more general asymptotic formula:

$$\sum_{p\le x} e_E^k(p) = c_{E,k}\,\mathrm{li}(x^{k+1}) + O(x^k\mathcal{E}(x)),$$

where

$$\mathcal{E}(x) = \begin{cases} x/(\log x)^A & \text{if } E \text{ has CM},\\ x^{5/6}(\log x)^2 & \text{if GRH holds},\end{cases}$$

and $c_{E,k}$ is a positive constant depending on E and k. (For $k=1$ and a non-CM curve E, Wu [33] has obtained a slightly better error term under GRH.) Felix and Murty derived their result as a consequence of a more general theorem on asymptotic distribution of $i_E(p)$'s. Their general theorem also implies the best known results on the cyclicity, the Titchmarsh divisor problem, and several other similar problems. To state their result, let $g(n)$ be an arithmetic function such that

$$\sum_{n\le x}|g(n)| \ll x^{1+\beta}(\log x)^\gamma, \tag{1.2}$$

where β and γ are arbitrary, and let

$$f(n) = \sum_{d\mid n} g(d). \tag{1.3}$$

Then the following is proved in [14, Theorem 1.1(c)].

Theorem 1.1 (Felix and Murty). *Under the assumption of GRH and the bound* (1.2) *for* $\beta < 1/2$ *and arbitrary* γ, *we have*

$$\sum_{p\le x} f(i_E(p)) = c_E(f)\,\mathrm{li}(x) + O\big(x^{\frac{5+2\beta}{6}}(\log x)^{\frac{(2-\beta)(1+\gamma)}{3}}\big),$$

where $c_E(f)$ *is a constant depending only on* E *and* f.

They also proved an unconditional version of the above theorem for CM elliptic curves (see [14, Theorem 1.1(a)]).

Our goal in this paper is to prove that Theorem 1.1 holds unconditionally on average over the family of all elliptic curves in a box. More precisely, we consider the family $\mathcal{C}$ of elliptic curves

$$E_{a,b} : y^2 = x^3 + ax + b,$$

where $|a| \le A$ and $|b| \le B$. It is not that difficult to prove a version of Theorem 1.1 on average over a large box. However it is a challenging problem to establish the same over a thin box. By a *thin* box we mean that, as a function of x, either A or B can be as small as x^{ϵ} for any $\epsilon > 0$. Here we prove a stronger result in which one of A and B can be as small as $\exp(c_1(\log x)^{1/2})$ for a suitably chosen constant $c_1 > 0$. Before stating our main theorem, we note that, at the expense of replacing β and γ by larger non-negative values, we can assume that β and γ are non-negative.

Theorem 1.2. *Let* $c > 1$ *be a positive constant and let* f *be the summatory function* (1.3) *of a function* g *that satisfies* (1.2) *for certain non-negative values of* β *and* γ. *Assume that* $AB > x(\log x)^{4+2c}$ *if* $0 \le \beta < 1/2$ *and* $AB > x^{1/2+\beta}(\log x)^{2\gamma+6+2c}(\log\log x)^2$ *if* $1/2 \le \beta < 1$. *Then there is a positive constant* $c_1 > 0$ *such that if* $A, B > \exp(c_1(\log x)^{1/2})$, *we have*

$$\frac{1}{|\mathcal{C}|}\sum_{E_{a,b}\in\mathcal{C}}\sum_{p\le x} f(i_{E_{a,b}}(p)) = c_0(f)\,\mathrm{li}(x) + O\bigg(\frac{x}{(\log x)^c}\bigg),$$

where

$$c_0(f) := \sum_{d\ge 1}\frac{g(d)}{d\psi(d)\varphi(d)^2}. \tag{1.4}$$

The implied constant depends on g, β, γ, *and* c. *Here* $\varphi(n) = n\prod_{p\mid n}(1-1/p)$ *and* $\psi(n) = n\prod_{p\mid n}(1+1/p)$.

Remark 1.3. We note that if f is a non-zero multiplicative function, then the constant $c_0(f)$ has an Euler product. More precisely, for multiplicative f we have

$$c_0(f) = \prod_{\ell\ \mathrm{prime}}\bigg(1 - \frac{1}{(\ell^2-1)(\ell^2-\ell)} + \frac{(\ell^4-1)}{(\ell^2-1)(\ell^2-\ell)}\sum_{\alpha\ge 1}\frac{f(\ell)}{\ell^{4\alpha}}\bigg).$$

Moreover, if f is completely multiplicative, then

$$c_0(f)=\prod_{\ell\text{ prime}}\left(1-\frac{\ell^4(1-f(\ell))}{(\ell^2-1)(\ell^2-\ell)(\ell^4-f(\ell))}\right).$$

If $f(n)\ll n$, then $c_0(f)=0$ if and only if

$$f(\ell)=\frac{\ell^3(1-\ell+\ell^2+\ell^3-\ell^4)}{\ell^2+\ell-1}$$

for some prime ℓ. One can verify that the right hand side of the above expression is less than or equal to $-\ell^3$. Thus we can conclude that if f is completely multiplicative and $f(n)\ll n$, then $c_0(f)\neq 0$.

Observe that it is possible that $c_0(f)=0$ for f multiplicative but not completely multiplicative. For example, let $f:\mathbb{N}\to\mathbb{C}$ be a multiplicative function such that $f(2)=-16/3$, $f(2^\alpha)=0$ for $\alpha\geq 2$, and $f(\ell^\alpha)=0$ for $\ell\geq 3$ and $\alpha\geq 1$. Then from the above expression for $c_0(f)$ we conclude that $c_0(f)=0$.

We would also like to point out that, following [16, Section 7], for an elliptic curve E and a multiplicative function f there exists a constant $\kappa_E(f)$ that can be expressed in terms of data associated to Galois representations on the torsion points of E, such that $c_E(f)=\kappa_E(f)c_0(f)$, where $c_E(f)$ is the constant given in Theorem 1.1. In particular, if $f(n)$ is completely multiplicative and $f(\mathbb{N})\subset\mathbb{Q}$, then $\kappa_E(f)\in\mathbb{Q}$. This phenomenon also occurs in Artin's conjecture and its related problems (see [27]). It would be interesting to know whether

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}c_E(f)\to c_0(f)\qquad\text{as } x\to\infty.$$

The work of Jones [24, Notation 4 and Corollary 8] establishes, under certain conditions, this relation in the case $f(n)=\sum_{d\mid n}\mu(d)$.

Theorem 1.2 is comparable to Stephens's average result on Artin's primitive root conjecture. Let a be a positive integer and let $A_a(x)$ be the number of primes not exceeding x and for which a is a primitive root. The following result has been proved in [31] and [32].

Theorem 1.4 (Stephens). *There exists a constant $c_1>0$ such that, if $N>\exp(c_1(\log x)^{1/2})$, then*

$$\frac{1}{N}\sum_{a\leq N}A_a(x)=A\,\mathrm{li}(x)+O\left(\frac{x}{(\log x)^c}\right),$$

where $A=\prod_{\ell\text{ prime}}(1-1/\ell(\ell-1))$ and c is an arbitrary constant greater than 1.

The line of research on Artin's primitive root conjecture on average started with the work of Goldfeld [19], who used multiplicative character sums and the large sieve inequality to establish a weaker version of Theorem 1.4. The extension of the method of character sums to the average questions on a two-parameter family, in the case of elliptic curves inside a box, was pioneered by the work of Fouvry and Murty [15] on the average Lang–Trotter conjecture for supersingular primes. This was extended to the general Lang–Trotter conjecture by David and Pappalardi [13]. The best result on the size of the box ($|a| \leq A$ and $|b| \leq B$) is due to Baier [4] who established the Lang–Trotter conjecture on average under the condition

$$A, B > x^{1/2+\epsilon} \quad \text{and} \quad AB > x^{3/2+\epsilon}, \tag{1.5}$$

where $\epsilon > 0$. The supersingular case of this result is due to Fouvry and Murty [15, Theorem 6]. Baier [5] also established an average result for the Lang–Trotter conjecture in the range

$$A, B > (\log x)^{60+\epsilon} \quad \text{and} \quad x^{3/2}(\log x)^{10+\epsilon} < AB < e^{x^{1/8-\epsilon}}, \tag{1.6}$$

where $\epsilon > 0$. Note that (1.6) is superior to (1.5) if A and B are not very large. Another notable result is due to James [23] who proved the Lang–Trotter conjecture on averages over elliptic curves with given fixed torsion.

There are also average results for other distribution problems for elliptic curves. Banks and Shparlinski [7] considered such average problems in a very general setting by employing multiplicative characters, and consequently proved average results for the cyclicity problem, the Sato–Tate conjecture, and the divisibility problem on a box $|a| \leq A$, $|b| \leq B$ satisfying the conditions

$$A, B \leq x^{1-\epsilon} \quad \text{and} \quad AB \geq x^{1+\epsilon}, \tag{1.7}$$

where $\epsilon > 0$. Another notable result is related to the Koblitz conjecture. Let

$$\pi_E^{\text{twin}}(x) := \#\{p \leq x;\ \#E_p(\mathbb{F}_p) \text{ is prime}\}.$$

A conjecture of Koblitz [25] predicts that

$$\pi_E^{\text{twin}}(x) \sim c_E \frac{x}{(\log x)^2}$$

as $x \to \infty$, where c_E is a constant depending on E. Balog, Cojocaru, and David [6] proved the following result on Koblitz conjecture on average over the family $\mathcal{C}$.

Theorem 1.5 (Balog, Cojocaru, and David [6, Theorem 1]). *Let $A, B > x^\epsilon$ and $AB > x(\log x)^{10}$. Then, as $x \to \infty$,*

$$\frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \pi_E^{\text{twin}}(x) = \prod_{\text{prime } \ell} \left(1 - \frac{\ell^2 - \ell - 1}{(\ell-1)^3(\ell+1)}\right) \frac{x}{(\log x)^2} + O\left(\frac{x}{(\log x)^3}\right).$$

The error term in the above theorem is estimated by a careful analysis of some multiplicative character sums. We prove our Theorem 1.2 by a generalization of a modified version of [6, Lemma 6] (see our Lemma 3.1). We have used some results of Stephens [32] to sharpen the estimates given in [6, Lemma 6], and thus we could establish our results, for $\beta < 1/2$, on a box of size

$$A, B > \exp(c_1(\log x)^{1/2}) \quad \text{and} \quad AB > x(\log x)^{\delta}, \tag{1.8}$$

for appropriate positive constants c_1 and δ. As far as we know, this is the thinnest box used for an elliptic curve average problem.

Our Theorem 1.2 has many applications. Here we mention some direct consequences of it to the cyclicity problem, the Titchmarsh divisor problem for elliptic curves, and computation of the kth power moment of the exponent $e_E(p)$.

Corollary 1.6. *Let $c > 1$ and $AB > x(\log x)^{4+2c}$. There is $c_1 > 0$ such that if $A, B > \exp(c_1(\log x)^{1/2})$, then, as $x \to \infty$, the following statements hold:*

(i) *We have*

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}} N_E(x) = \prod_{\ell \text{ prime}}\left(1 - \frac{1}{(\ell^2-1)(\ell^2-\ell)}\right)\mathrm{li}(x) + O\left(\frac{x}{(\log x)^c}\right),$$

where $N_E(x)$ is the cyclicity counting function and $\mu(d)$ is the Möbius function.

(ii) *We have*

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\sum_{p\le x}\tau(i_E(p)) = \prod_{\ell \text{ prime}}\left(1 + \frac{\ell^3}{(\ell-1)(\ell^2-1)(\ell^4-1)}\right)\mathrm{li}(x) + O\left(\frac{x}{(\log x)^c}\right).$$

(iii) *For $k \in \mathbb{N}$ we have*

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\sum_{p\le x} e_E^k(p) = \prod_{\ell \text{ prime}}\left(1 - \frac{\ell^3(\ell^k-1)}{(\ell-1)(\ell^2-1)(\ell^{k+4}-1)}\right)\mathrm{li}(x^{k+1}) + O\left(\frac{x^{k+1}}{(\log x)^c}\right).$$

Part (i) of the above corollary gives a strengthening of a result of Banks and Shparlinski [7, Theorem 18] where the asymptotic formula in (i) was proved in the weaker range (1.7). Parts (ii) and (iii) establish unconditional average versions of some results given in [1] and [14]. In (iii), if $k = 1$, then we obtain the universal constant in [16].

REMARKS 1.7. (i) As corollaries of Theorem 1.2, we can also establish unconditional average results for $f(i_E(p))$, where $f(n)$ is one of the functions $(\log n)^\alpha$, $\omega(n)^k$, $\Omega(n)^k$, $2^{k\omega(n)}$, or $\tau_k(n)^r$. Here α is an arbitrary positive real number and k and r are fixed non-negative integers. See [14, p. 276] for conditional results related to these functions in the case of a single elliptic curve.

(ii) Under the conditions of Theorem 1.2 one can also obtain average results for $f(n) = n^\beta$ and $f(n) = \sigma_\beta(n) = \sum_{m|n} m^\beta$ as long as $\beta < 1$. More precisely, for A and B satisfying the conditions of Theorem 1.2 we have, for $c > 1$,

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\sum_{p\le x} i_E^\beta(p) = \biggl(\sum_{d\ge 1}\frac{g(d)}{d\psi(d)\varphi(d)^2}\biggr)\operatorname{li}(x) + O\biggl(\frac{x}{(\log x)^c}\biggr),$$

where g is the unique arithmetic function satisfying

$$n^\beta = \sum_{m|n} g(m).$$

This stops short of providing an answer on average to a problem proposed by Kowalski [26, Problem 3.1] that asks about the asymptotic behavior of $\sum_{p\le x} i_E(p)$.

(iii) Following the proof of Theorem 1.2, one can improve the condition $A, B > x^\epsilon$ in Theorem 1.5 to $A, B > \exp(c_1(\log x)^{1/2})$ for some suitably chosen constant c_1.

(iv) Lemma 3.1 is the difficult part of the proof of Theorem 1.2. The proof of Lemma 3.1 follows the method used in the proof of [6, Lemma 6] (which itself is based on [7]) and combines it with some devices from [32]. A new ingredient is an asymptotic estimate due to Howe (see Lemma 2.1) for the number of elliptic curves over $\mathbb{F}_p$ which have d-torsion subgroup over $\mathbb{F}_p$ isomorphic to two copies of $\mathbb{Z}/d\mathbb{Z}$. Another new feature is a successful application of Burgess's bound (see Lemma 2.6) in handling terms obtained from the error term of Howe's estimate.

(v) One other novel feature of the proof of Theorem 1.2 is sharp estimates of the error terms arising from the curves of j-invariant 0 or 1728, which are estimated using some results from the theory of CM curves (see Lemma 2.3). A trivial estimate of these terms will result in unsatisfactory bounds on admissible values of A and B in Theorem 1.2.

Following the ideas of the proof of Theorem 1.2 and by a careful analysis of some character sums one can show that $c_0(f)\operatorname{li}(x)$ closely approximates $\sum_{p\le x} f(i_E(p))$ for almost all curves $E \in \mathcal{C}$. Here we prove the following more general theorem.

Theorem 1.8. *Let* $0 \le \beta < 1/2$ *and* $\gamma \ge 0$. *Let* $f(n) = \sum_{d|n} g(d)$ *be an arithmetic function satisfying*

$$f(n) \ll n^{\beta}(\log n)^{\gamma}. \tag{1.9}$$

Suppose $AB > x^2(\log x)^6$ *if* $0 \le \beta < 1/4$ *and* $AB > x^{3/2+2\beta}(\log x)^{4\gamma+14} \times (\log\log x)^4$ *if* $1/4 \le \beta < 1/2$. *Then there is a positive constant* $c_1 > 0$ *such that, if* $A, B > \exp(c_1(\log x)^{1/2})$, *we have*

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\Big(\sum_{p\le x} f(i_E(p)) - c_0(f)\operatorname{li}(x)\Big)^2 = O\Big(\frac{x^2}{(\log x)^2}\Big),$$

where $c_0(f)$ *is defined by* (1.4).

The following is a direct consequence of Theorem 1.8.

Corollary 1.9. *Let* $h(x)$ *be a positive real function such that* $\lim_{x\to\infty} h(x) = 0$. *Under the assumptions of Theorem* 1.8, *for any* $x > 1$ *we have*

$$\Big|\sum_{p\le x} f(i_E(p)) - c_0(f)\operatorname{li}(x)\Big| \le \frac{x}{h(x)\log x} \tag{1.10}$$

for almost all $E \in \mathcal{C}$. *More precisely,* (1.10) *holds except possibly for* $O(h(x)^2|\mathcal{C}|)$ *of curves in* $\mathcal{C}$.

We note that one can take f to be any of the functions mentioned in Corollary 1.6(i), (ii), and Remarks 1.7(i), (ii). For Corollary 1.6(i), the corresponding function $f(n)$ is the characteristic function of the singleton set $\{1\}$.

Remarks 1.10. It is possible to establish a version of Theorem 1.8 using the bound

$$\sum_{n\le x}|g(n)|^2 \ll x^{1+2\beta}(\log x)^{2\gamma}$$

instead of (1.9). However, we find that (1.9) will make the presentation of the proof more convenient. Note that if

$$f(n) = \sum_{d|n} g(d) \ll n^{\beta}(\log n)^{\gamma},$$

then, by the Möbius inversion formula, we have

$$\sum_{n\le x}|g(n)|^2 \ll x^{1+2\beta}(\log x)^{2\gamma+1}.$$

The structure of the paper is as follows. In Section 2 we summarize results that will be used in the proof of our two theorems. Section 3 is dedicated to a detailed proof of Theorem 1.2 and Corollary 1.6. In Section 4 we briefly summarize the proof of a technical lemma, which is a two-dimensional version of Lemma 3.1. The proof is tedious and divided into several subcases. We treat some cases and briefly comment on the remaining ones. Finally in Section 5 we prove Theorem 1.8.

NOTATION 1.11. Throughout the paper p and q denote primes (for simplicity in most cases we assume that $p, q \neq 2, 3$), $\varphi(n)$ is the Euler function, $\omega(n)$ is the number of distinct prime divisors of n, $\Omega(n)$ is the total number of prime divisors of n, $\tau(n)$ is the total number of divisors of n, $p(n)$ is the largest prime factor of n, $\tau_k(n)$ is the number of representations of n as a product of k natural numbers, $\mu(n)$ is the Möbius function, $\psi(n) = n\prod_{p\mid n}(1+1/p)$, and $\pi(x; d, a)$ is the number of primes not exceeding x that are congruent to a modulo d. Moreover, K is an imaginary quadratic number field of class number 1, $N(\mathfrak{a})$ is the norm of an ideal $\mathfrak{a}$ of K, $N(\alpha)$ is the norm of an element α in K, $\mathfrak{p}$ always denotes a degree 1 prime ideal of K with $N(\mathfrak{p}) = p$, and d_{sp} is the largest divisor of d composed of primes that split completely in K. We denote the finite field of p elements by $\mathbb{F}_p$ and its multiplicative group by $\mathbb{F}_p^\times$. For two functions $f(x)$ and $g(x) \neq 0$, we use the notation $f(x) = O(g(x))$, or alternatively $f(x) \ll g(x)$, if $|f(x)/g(x)|$ is bounded as $x \to \infty$.

2. Lemmas. Let $E_{s,t}$ denote an elliptic curve over $\mathbb{F}_p$ (with $p \neq 2, 3$) given by the equation

$$y^2 = x^3 + sx + t, \qquad s, t \in \mathbb{F}_p,$$

where at least one of s or t is non-zero. Let $E_{s,t}[d](\mathbb{F}_p)$ denote the set of d-torsion points of $E_{s,t}$ with coordinates in $\mathbb{F}_p$. The following lemma is essentially due to Howe (see [21, p. 245]).

LEMMA 2.1.

(i) *For $d \in \mathbb{N}$ and a fixed prime p, let*

$$\mathcal{S}_d(p) := \{(s,t) \in \mathbb{F}_p \times \mathbb{F}_p;\ 4s^3+27t^2 \neq 0 \text{ and } E_{s,t}[d](\mathbb{F}_p) \cong \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}\}.$$

For $d \mid p-1$, we have

$$\#\mathcal{S}_d(p) = \frac{p(p-1)}{d\psi(d)\varphi(d)} + O(p^{3/2}).$$

Moreover, if $d \nmid p-1$ or $d > \sqrt{p}+1$, then $\#\mathcal{S}_d(p) = 0$.

(ii) *The assertions in* (i) *hold if we replace $\mathcal{S}_d(p)$ with $\tilde{\mathcal{S}}_d(p)$, where*

$$\tilde{\mathcal{S}}_d(p) := \{(s,t) \in \mathbb{F}_p^\times \times \mathbb{F}_p^\times;\ 4s^3+27t^2 \neq 0 \text{ and } E_{s,t}[d](\mathbb{F}_p) \cong \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}\}.$$

Proof. (i) We know that elliptic curves isomorphic (over $\mathbb{F}_p$) to $E_{s,t}$ are of the form E_{su^4,tu^6}, where $u \in \mathbb{F}_p^\times$. Let $\mathrm{Aut}_{\mathbb{F}_p}(E_{s,t})$ be the group of automorphisms (over $\mathbb{F}_p$) of the elliptic curve $E_{s,t}$. So the number of elliptic curves isomorphic to $E_{s,t}$ (over $\mathbb{F}_p$) is $(p-1)/|\mathrm{Aut}_{\mathbb{F}_p}(E_{s,t})|$. Let $[E_{s,t}]$ denote the class of all elliptic curves over $\mathbb{F}_p$ that are isomorphic over $\mathbb{F}_p$ to $E_{s,t}$.

We have

$$\#\mathcal{S}_d(p) = \sum_{[E_{s,t}]\subset\mathcal{S}_d(p)} \frac{p-1}{|\mathrm{Aut}_{\mathbb{F}_p}(E_{s,t})|}.$$

Now the result follows since by [21, p. 245] we have, for $d \mid p-1$,

$$\sum_{[E_{s,t}]\subset\mathcal{S}_d(p)} \frac{1}{|\mathrm{Aut}_{\mathbb{F}_p}(E_{s,t})|} = \frac{p}{d\psi(d)\varphi(d)} + O(p^{1/2}). \tag{2.1}$$

Moreover, by [30, Corollary III.8.1.1], if $d \nmid p-1$ then $(\mathbb{Z}/d\mathbb{Z})^2 \not\cong E_{s,t}(\mathbb{F}_p)[d]$, and so $\#\mathcal{S}_d(p) = 0$. Also if $d > \sqrt{p}+1$ and $(\mathbb{Z}/d\mathbb{Z})^2 \cong E_{s,t}(\mathbb{F}_p)[d] \subseteq E_{s,t}(\mathbb{F}_p)$, then $p + 2\sqrt{p} + 1 < d^2 \le \#E_{s,t}(\mathbb{F}_p)$. On the other hand $\#E_{s,t}(\mathbb{F}_p) \le p + 2\sqrt{p} + 1$, by Hasse's theorem. This is a clear contradiction.

(ii) We can deduce this by following the proof of part (i) and observing that there are $O(1)$ isomorphism classes over $\mathbb{F}_p$ containing a curve of the form $E_{0,t}$ or $E_{s,0}$. ∎

Remark 2.2. (i) For any prime p, we know that $|\mathrm{Aut}_{\mathbb{F}_p}(E_{s,t})| = O(1)$. In fact, for $p \ne 2,3$, from [30, Theorem III.10.1] we know that

$$|\mathrm{Aut}_{\mathbb{F}_p}(E_{s,t})| = \begin{cases} 6 & \text{if } s = 0 \text{ and } p \equiv 1 \pmod 6,\\ 4 & \text{if } t = 0 \text{ and } p \equiv 1 \pmod 4,\\ 2 & \text{otherwise.}\end{cases}$$

(ii) We note that, using Howe's notation [21, p. 245], we have

$$\sum_{[E_{s,t}]\subset\mathcal{S}_d(p)} \frac{1}{|\mathrm{Aut}_{\mathbb{F}_p}(E_{s,t})|} = \frac{p}{d\psi(d)\varphi(d)} + O(\psi(d/d)2^{\omega(d)}\sqrt{p}),$$

where the implied constant is absolute. However, the term $2^{\omega(d)}$ is a bound for $\sum_{j\mid\gcd(d,p-1)/d} \mu(j)$. In our case, $\gcd(d,p-1)/d = 1$, since $d \mid p-1$. Thus, the term $2^{\omega(d)}$ can be removed. Also, $\psi(d/d) = 1$, and thus (2.1) is correct.

Let K be an imaginary quadratic number field of class number 1. Let $\mathfrak{p}$ be a degree 1 prime ideal of K with $N(\mathfrak{p}) = p$. Let π_p be the unique generator of $\mathfrak{p}$. Note that if $\mathfrak{p}$ is unramified, then π_p is unique up to units, and if it is ramified, then π_p is unique up to units and complex conjugation. We have $N(\mathfrak{p}) = N(\pi_p) = p$.

Lemma 2.3. *Suppose that d_{sp} is the largest divisor of a positive integer d composed of primes that split completely in K.*

(i) *For $d^2 \le x/\log x$ we have*

$$\sum_{\substack{N(\mathfrak{p})\le x\\ d\mid(\pi_p-1)(\bar{\pi}_p-1)}} 1 \ll \frac{2^{\omega(d_{\mathrm{sp}})}\tau(d_{\mathrm{sp}})}{\varphi(d)}\,\frac{x}{\log(x/d^2)}.$$

(ii) *For all positive integers d, we have*

$$\sum_{\substack{N(\mathfrak{p})\le x\\ d\mid(\pi_p-1)(\bar{\pi}_p-1)}} 1 \ll \frac{\tau(d_{\mathrm{sp}})x}{d}.$$

(iii) *Let $E_{s,t}: y^2 = x^3+sx+t$ be an elliptic curve over $\mathbb{F}_p$ with $st=0$. Then $\#E_{s,t}(\mathbb{F}_p) = p+1$ or $\#E_{s,t}(\mathbb{F}_p) = (\pi_p-1)(\bar{\pi}_p-1)$ and $N(\pi_p)=p$, where $\pi_p\in\mathbb{Z}[(1+i\sqrt{3})/2]$ or $\mathbb{Z}[i]$.*

(iv) *Let $g(d)$ be an arithmetic function satisfying* (1.2) *with $\beta<1$. Then*

$$\sum_{p\le x}\frac{1}{p}\sum_{\substack{s,t\in\mathbb{F}_p\\ st=0}}\ \sum_{\substack{d\mid p-1\\ E_{s,t}(\mathbb{F}_p)[d]\cong(\mathbb{Z}/d\mathbb{Z})^2}} |g(d)| \ll \frac{x}{\log x}.$$

Proof. The proofs of (i) and (ii) are identical to the proofs of [2, Propositions 2.2 and 2.3].

(iii) See [22, Chapter 18, Theorems 4 and 5].

(iv) We observe that the condition $E_{s,t}(\mathbb{F}_p)[d]\cong(\mathbb{Z}/d\mathbb{Z})^2$ implies that $d\mid p-1$ and $d^2\mid\#E_{s,t}(\mathbb{F}_p)$. By part (iii), we know the possibilities for $\#E_{s,t}(\mathbb{F}_p)$. Now if $\#E_{s,t}(\mathbb{F}_p)=p+1$, then we conclude that $d=2$ (since $d\mid p-1$ and $d\mid p+1$). On the other hand, if $\#E_{s,t}(\mathbb{F}_p)=(\pi_p-1)(\bar{\pi}_p-1)$ where $\pi_p\in\mathbb{Z}[(1+i\sqrt{3})/2]$ or $\mathbb{Z}[i]$, we let $0<\epsilon<1-\beta$. So by employing (i) and (ii), the sum in (iv) is bounded by

$$\sum_{\substack{p\le x\\ p\equiv-1\ (\mathrm{mod}\ 4)}} 1 + \sum_{d\le\sqrt{x}+1}|g(d)| \sum_{\substack{N(\mathfrak{p})\le x\\ d\mid(\pi_p-1)(\bar{\pi}_p-1)}} 1$$
$$\ll \frac{x}{\log x}+\frac{x}{\log x}\sum_{d\le x^{1/5}}\frac{|g(d)|}{d^{2-\epsilon}}+x\sum_{d>x^{1/5}}\frac{|g(d)|}{d^{2-\epsilon}} \ll \frac{x}{\log x}. \qquad\blacksquare$$

We next recall a version of the large sieve inequality for multiplicative characters.

Lemma 2.4 (Gallagher [18, p. 16]). *Let M and N be positive integers and $(a_n)_{n=M+1}^{M+N}$ be a sequence of complex numbers. Then*

$$\sum_{q\le Q}\frac{q}{\varphi(q)}\sideset{}{^*}\sum_{\chi\,(\mathrm{mod}\,q)}\Big|\sum_{n=M+1}^{M+N} a_n\chi(n)\Big|^2 \ll (N+Q^2)\sum_{n=M+1}^{M+N}|a_n|^2,$$

where Q is any positive real number, and $\sum^*_{\chi\,(\mathrm{mod}\,q)}$ denotes a sum over all primitive Dirichlet characters χ modulo q.

To state the next lemma, we need some notation. Let

$$\tau_{k,B}(n) := \#\{(a_1,\ldots,a_k)\in[1,B]^k\cap\mathbb{N}^k;\ n=a_1\cdots a_k\}.$$

We also set

$$\Psi(X,Y) := \sum_{\substack{n\le X\\ p(n)\le Y}} 1,$$

where $p(m)$ is the largest prime factor of m. Note that we define $p(0) = p(\pm 1) = \infty$.

LEMMA 2.5 (Stephens [32, Lemmas 8–10]).

(i) *For $k \in \mathbb{N}$, if $B^k \le x^8$, then*
$$\sum_{b\le B^k} \tau_{k,B}(n)^2 < B^k(\Psi(B, 9\log x))^k.$$

(ii) *For a sufficiently large constant $c_1 > 0$ there exists $c_2 > 0$ such that, if $\exp(c_1(\log x)^{1/2}) < B \le x^8$, then*
$$x^{-1/2k}(\Psi(B, 9\log x))^{1/2} \ll \exp\bigl(-c_2(\log x)^{1/2}/\log\log x\bigr),$$
where
$$k = [2\log x/\log B] + 1.$$

(iii) *For a sufficiently large constant $c_1 > 0$ there exists $c_3 > 0$ such that, if $\exp(c_1(\log x)^{1/2}) < B \le x^4$, then*
$$x^{-1/k}(\Psi(B, 9\log x))^{1/2} \ll \exp\bigl(-c_3(\log x)^{1/2}/\log\log x\bigr),$$
where
$$k = [4\log x/\log B] + 1.$$

LEMMA 2.6 (Burgess [9, Theorems 1 and 2]).

(i) *For any prime p, non-principal character χ, $r \in \mathbb{N}$, and $B \ge 1$,*
$$\sum_{b\le B} \chi(b) \ll B^{1-1/r} p^{\frac{r+1}{4r^2}} \log p,$$
where the implied constant is absolute.

(ii) *Let $\epsilon > 0$, $n > 1$, χ be a non-principal character, $r \in \mathbb{N}$, and $B \ge 1$. Then, if n is cube-free or $r = 2$, we have*
$$\sum_{b\le B} \chi(b) \ll B^{1-1/r} n^{\frac{r+1}{4r^2}+\epsilon},$$
where the implied constant may depend on ϵ and r.

LEMMA 2.7.

(i) (Friedlander and Iwaniec [17, Lemma 3]) *Let Q and N be positive integers. Then*
$$\sideset{}{^*}\sum_{\chi\,(\mathrm{mod}\,Q)} \Bigl|\sum_{n\le N} \chi(n)\Bigr|^4 \ll N^2 Q \log^6 Q,$$
where $*$ denotes a sum over all primitive Dirichlet characters modulo Q.

(ii) *Suppose that Q is the product of two distinct primes. Then*

$$\sum_{\substack{\chi \,(\mathrm{mod}\, Q)\\ \chi\neq\chi_0}} \Big|\sum_{n\le N}\chi(n)\Big|^4 \ll N^2 Q\log^6 Q.$$

Proof. (ii) Let $Q = pq$ with $p \neq q$. To see that the result is true if the summation is over all non-principal characters, we need to consider the inequality for imprimitive characters. The only non-principal imprimitive characters modulo pq are of the form $\chi'\chi_0''$ or $\chi_0'\chi''$, where χ_0' and χ_0'' are the principal characters modulo p and q, respectively, and χ' and χ'' are primitive characters modulo p and q, respectively. Then partition the summation over all characters into a summation over primitive characters modulo pq, primitive characters modulo p, and primitive characters modulo q. Hence, the assertion can be obtained by using the triangle inequality and the result for primitive characters in part (i). ∎

We summarize several elementary estimations that are used in the proofs in the next sections.

Lemma 2.8.

(i) (Brun–Titchmarsh inequality) *Let $\epsilon > 0$. Then, for $1 \le d \le x^{1-\epsilon}$, we have*

$$\pi(x; d, a) \ll \frac{x}{\varphi(d)\log x}.$$

(ii) *Let $\theta < 1$ and $\epsilon > 0$. Then, for $1 \le d \le x^{1-\epsilon}$, we have*

$$\sum_{\substack{p\le x\\ p\equiv 1\,(\mathrm{mod}\, d)}} \frac{1}{p^\theta} \ll \frac{x^{1-\theta}}{\varphi(d)\log x}.$$

(iii) *For $x \ge 3$ and $d \ge 1$ we have*

$$\sum_{\substack{p\le x\\ p\equiv 1\,(\mathrm{mod}\, d)}} \frac{1}{p} \ll \frac{\log\log x + \log d}{\varphi(d)}.$$

(iv) *We have*

$$\frac{1}{\varphi(d)} \ll \frac{\log\log d}{d}.$$

(v) *Under the assumption of the bound* (1.2), *for any real θ, we have*

$$\sum_{d\le y} \frac{|g(d)|}{d^\theta} \ll 1 + y^{1+\beta-\theta}(\log y)^{\gamma+1}.$$

Proof. For (i), see [11, Theorem 7.3.1]; (ii) is a consequence of partial summation and (i); for (iii), see [11, Section 13.1, Exercise 9]; for (iv), see

[20, p. 267, Theorem 328]; and (v) comes by straightforward applications of partial summation and (1.2). ■

3. Proofs of Theorem 1.2 and Corollary 1.6

3.1. Basic set up. Let $\mathcal{C}$ be the family of elliptic curves

$$E_{a,b} : y^2 = x^3 + ax + b,$$

where $|a| \le A$, $|b| \le B$, and at least one of a or b is non-zero. Note that

$$|\mathcal{C}| = 4AB + O(A+B).$$

Let

$$f(n) = \sum_{d|n} g(d)$$

for all $n \in \mathbb{N}$. We have

$$\frac{1}{|\mathcal{C}|}\sum_{E_{a,b}\in\mathcal{C}}\sum_{p\le x} f(i_{E_{a,b}}(p)) = \frac{1}{|\mathcal{C}|}\sum_{p\le x}\sum_{s,t\in\mathbb{F}_p}\frac{|\mathrm{Aut}_{\mathbb{F}_p}(E_{s,t})| f(i_{E_{s,t}}(p))}{p-1}\sum_{\substack{|a|\le A,\,|b|\le B\colon \exists 1\le u<p\\ a\equiv su^4 \,(\mathrm{mod}\,p)\\ b\equiv tu^6\,(\mathrm{mod}\,p)}} 1.$$

Next, by applying Remark 2.2(i) in the above identity (recall that $p\neq 2,3$), we have

$$\frac{1}{|\mathcal{C}|}\sum_{E_{a,b}\in\mathcal{C}}\sum_{p\le x} f(i_{E_{a,b}}(p)) = \frac{2}{|\mathcal{C}|}\sum_{p\le x}\sum_{s,t\in\mathbb{F}_p^\times}\frac{f(i_{E_{s,t}}(p))}{p-1}\sum_{\substack{|a|\le A,\,|b|\le B\colon \exists 1\le u<p\\ a\equiv su^4 \,(\mathrm{mod}\,p)\\ b\equiv tu^6\,(\mathrm{mod}\,p)}} 1 + \text{Error Term 1},$$

where

$$\text{Error Term 1} = \frac{1}{|\mathcal{C}|}\sum_{p\le x}\sum_{\substack{s,t\in\mathbb{F}_p\\ st=0}}\frac{|\mathrm{Aut}_{\mathbb{F}_p}(E_{s,t})| f(i_{E_{s,t}}(p))}{p-1}\sum_{\substack{|a|\le A,\,|b|\le B\\ ab\equiv 0\,(\mathrm{mod}\,p)}} 1. \tag{3.1}$$

Now, by considering

$$\sum_{\substack{|a|\le A,\,|b|\le B\colon \exists 1\le u<p\\ a\equiv su^4 \,(\mathrm{mod}\,p)\\ b\equiv tu^6\,(\mathrm{mod}\,p)}} 1 = \frac{2AB}{p} + \Bigg(\sum_{\substack{|a|\le A,\,|b|\le B\colon \exists 1\le u<p\\ a\equiv su^4 \,(\mathrm{mod}\,p)\\ b\equiv tu^6\,(\mathrm{mod}\,p)}} 1 - \frac{2AB}{p}\Bigg)$$

and applying it in the previous identity, we arrive at

$$\frac{1}{|\mathcal{C}|}\sum_{E_{a,b}\in\mathcal{C}}\sum_{p\le x} f(i_{E_{a,b}}(p)) = \text{Main Term} + \text{Error Term 1} + \text{Error Term 2},$$

where

$$\text{Main Term} = \frac{4AB}{|\mathcal{C}|}\sum_{p\le x}\sum_{s,t\in\mathbb{F}_p^\times}\frac{f(i_{E_{s,t}}(p))}{p(p-1)},$$

$$\text{Error Term 2} = \frac{2}{|\mathcal{C}|}\sum_{p\le x}\sum_{s,t\in\mathbb{F}_p^\times}\frac{f(i_{E_{s,t}}(p))}{p-1}\Bigg(\sum_{\substack{|a|\le A,\,|b|\le B\colon \exists 1\le u<p\\ a\equiv su^4 \pmod p\\ b\equiv tu^6 \pmod p}} 1 - \frac{2AB}{p}\Bigg).$$

3.2. The Main Term. We have

$$\begin{aligned}\text{Main Term} &= \frac{4AB}{|\mathcal{C}|}\sum_{p\le x}\sum_{s,t\in\mathbb{F}_p^\times}\frac{f(i_{E_{s,t}}(p))}{p(p-1)}\\ &= \frac{4AB}{|\mathcal{C}|}\sum_{p\le x}\frac{1}{p(p-1)}\sum_{s,t\in\mathbb{F}_p^\times}\sum_{d\mid i_{E_{s,t}}(p)} g(d)\\ &= \frac{4AB}{|\mathcal{C}|}\sum_{p\le x}\frac{1}{p(p-1)}\sum_{d\mid p-1} g(d)\#\tilde{\mathcal{S}}_d(p).\end{aligned}$$

Let

$$G_1(p) = \sum_{\substack{d\mid p-1\\ d\le\sqrt{p}+1}}\frac{g(d)}{d\psi(d)\varphi(d)} \quad\text{and}\quad G_2(p) = \sum_{\substack{d\mid p-1\\ d\le\sqrt{p}+1}} |g(d)|.$$

By using these notations and employing Lemma 2.1, we obtain

$$\text{Main Term} = \frac{4AB}{|\mathcal{C}|}\Bigg(\sum_{p\le x} G_1(p) + O\Bigg(\sum_{p\le x}\frac{G_2(p)}{\sqrt{p}}\Bigg)\Bigg) = \frac{4AB}{|\mathcal{C}|}(\mathscr{S}_1 + O(\mathscr{S}_2)).$$

3.2.1. *Estimation of* $\mathscr{S}_1$. Let $\alpha\in\mathbb{R}_{>0}$ be fixed. The Siegel–Walfisz Theorem implies

$$\pi(x;d,1) = \frac{\mathrm{li}(x)}{\varphi(d)} + O\bigg(\frac{x}{(\log x)^C}\bigg)$$

for any $d\le(\log x)^\alpha$ and any $C>0$. Then, by the Brun–Titchmarsh inequality (Lemma 2.8(i)), the fact that $\psi(d)\ge d$, and (1.2), we have

$$\begin{aligned}
\mathscr{S}_1 &= \sum_{d\le(\log x)^\alpha}\frac{g(d)\pi(x;d,1)}{d\psi(d)\varphi(d)} + \sum_{(\log x)^\alpha<d\le\sqrt{x}+1}\frac{g(d)\pi(x;d,1)}{d\psi(d)\varphi(d)}\\
&= \mathrm{li}(x)\sum_{d\ge1}\frac{g(d)}{d\psi(d)\varphi(d)^2} + O\bigg(\frac{x}{(\log x)^C}\sum_{d\ge1}\frac{|g(d)|}{d\psi(d)\varphi(d)}\bigg)\\
&\quad + O\bigg(\frac{x}{\log x}\sum_{d>(\log x)^\alpha}\frac{|g(d)|}{d\psi(d)\varphi(d)^2}\bigg).
\end{aligned}$$

Note that, for any $\varepsilon>0$, we have

$$\sum_{d>y}\frac{|g(d)|}{d\psi(d)\varphi(d)} \ll \sum_{d>y}\frac{|g(d)|}{d^{3-\varepsilon/2}} \ll \frac{1}{y^{2-\beta-\varepsilon}}.$$

Thus, for $\beta<2$,

$$c_0(f) := \sum_{d\ge1}\frac{g(d)}{d\psi(d)\varphi(d)^2}$$

is a constant and

$$\mathscr{S}_1 = c_0(f)\,\mathrm{li}(x) + O\bigg(\frac{x}{(\log x)^{C'}}\bigg),$$

where $C' := C'(C,\alpha,\beta,\varepsilon)$ is an appropriate positive constant. Since α is arbitrary, we can choose α so that C' is any constant greater than 1. So

$$\mathscr{S}_1 = c_0(f)\,\mathrm{li}(x) + O\bigg(\frac{x}{(\log x)^{c}}\bigg), \tag{3.2}$$

where c can be chosen as any number greater than 1.

3.2.2. *Estimation of* $\mathscr{S}_2$. We first employ the Brun–Titchmarsh inequality (Lemma 2.8(i)) and (1.2) to deduce

$$\begin{aligned}
\sum_{p\le x}G_2(p) &= \sum_{d\le\sqrt{x}+1}|g(d)|\pi(x;d,1)\\
&\ll \begin{cases} x^{1+\beta/2}(\log x)^{\gamma-1}\log\log x & \text{if } \beta\ne0,\\ x^{1+\beta/2}(\log x)^{\gamma}\log\log x & \text{if } \beta=0.\end{cases}
\end{aligned} \tag{3.3}$$

By partial summation and (3.3), we have

$$\mathscr{S}_2 = \sum_{p\le x}\frac{G_2(p)}{\sqrt{p}} \ll x^{\frac{1+\beta}{2}}(\log x)^\gamma\log\log x. \tag{3.4}$$

In conclusion, since $\beta<1$,

$$\text{Main Term} = \frac{4AB}{|\mathcal{C}|}\bigg(c_0(f)\,\mathrm{li}(x) + O\bigg(\frac{x}{(\log x)^c}\bigg)\bigg), \tag{3.5}$$

where c can be taken as any number greater than 1.

3.3. Error Term 1. Recall expression (3.1) for Error Term 1. We have

$$\begin{aligned}\text{Error Term 1} &\ll \frac{1}{|\mathcal{C}|}\sum_{p\le x}\sum_{\substack{s,t\in\mathbb{F}_p\\ st=0}}\frac{|f(i_{E_{s,t}}(p))|}{p}\left(\frac{AB}{p}+A+B\right)\\ &\ll \sum_{p\le x}\frac{1}{p^2}\sum_{\substack{s,t\in\mathbb{F}_p\\ st=0}}\sum_{\substack{d\mid p-1\\ E_{s,t}(\mathbb{F}_p)[d]\cong(\mathbb{Z}/d\mathbb{Z})^2}}|g(d)|\\ &\quad+\left(\frac{1}{A}+\frac{1}{B}\right)\sum_{p\le x}\frac{1}{p}\sum_{\substack{s,t\in\mathbb{F}_p\\ st=0}}\sum_{\substack{d\mid p-1\\ E_{s,t}(\mathbb{F}_p)[d]\cong(\mathbb{Z}/d\mathbb{Z})^2}}|g(d)|.\end{aligned}$$

An application of Lemma 2.3(iv) in the latter sum yields

$$\text{Error Term 1} \ll \sum_{p\le x}\frac{1}{p}\sum_{\substack{d\mid p-1\\ d\le\sqrt{p}+1}}|g(d)| + \left(\frac{1}{A}+\frac{1}{B}\right)\frac{x}{\log x}. \tag{3.6}$$

By employing Lemma 2.8(iii), (iv) and usual estimates, the first of these summations is bounded as follows:

$$\begin{aligned}\sum_{p\le x}\frac{1}{p}\sum_{\substack{d\mid p-1\\ d\le\sqrt{p}+1}}|g(d)| &= \sum_{d\le\sqrt{x}+1}|g(d)|\sum_{\substack{p\le x\\ p\equiv 1\ (\mathrm{mod}\ d)}}\frac{1}{p}\\ &\ll (\log\log x)(\log x)\sum_{d\le\sqrt{x}+1}\frac{|g(d)|}{d}.\end{aligned} \tag{3.7}$$

By applying Lemma 2.8(v) in (3.7), we obtain

$$\text{Error Term 1} \ll x^{\beta/2}(\log x)^{\gamma+2}(\log\log x) + \left(\frac{1}{A}+\frac{1}{B}\right)\frac{x}{\log x}. \tag{3.8}$$

3.4. Error Term 2. We summarize the main result of this section in the following lemma, which can be considered as a generalization and an improvement of [6, Lemma 6].

LEMMA 3.1. *Let $r\in\mathbb{N}$, $0\le\beta<3/2$, $\gamma\in\mathbb{R}_{\ge 0}$, and $g:\mathbb{N}\to\mathbb{C}$ be a function such that*

$$\sum_{d\le x}|g(d)| \ll x^{1+\beta}(\log x)^{\gamma}.$$

Then there are positive constants c_1 and c_2 such that, if $A,B > \exp(c_1(\log x)^{1/2})$, we have

$$\frac{2}{|\mathcal{C}|}\sum_{p\le x}\sum_{d\mid p-1} g(d) \sum_{\substack{1\le s,t<p\\ E_{s,t}(\mathbb{F}_p)[d]\cong(\mathbb{Z}/d\mathbb{Z})^2}} \frac{1}{p-1}\Bigg(\sum_{\substack{|a|\le A,\, |b|\le B\colon \exists 1\le u<p\\ a\equiv su^4 \,(\mathrm{mod}\, p)\\ b\equiv tu^6 \,(\mathrm{mod}\, p)}} 1-\frac{2AB}{p}\Bigg)$$

$$\begin{aligned}
&\ll x^{\frac{\beta-1}{2}}(\log x)^{\gamma+1}\log\log x+(\log x)^{\gamma}\log\log x+x\exp\left(-c_2\frac{(\log x)^{1/2}}{\log\log x}\right)\\
&\quad+\left(\frac{1}{A}+\frac{1}{B}\right)\left(\frac{x}{\log x}+x^{\frac{1+\beta}{2}}(\log x)^{\gamma}\log\log x\right)\\
&\quad+\left(\frac{1}{A^{1/r}}+\frac{1}{B^{1/r}}\right)x^{\frac{1+\beta}{2}+\frac{r+1}{4r^2}}(\log x)^{\gamma+1}\log\log x+\frac{x^{3/2}(\log x)^2}{\sqrt{AB}}\\
&\quad+\frac{1}{\sqrt{AB}}\left(x^{1+\beta/2}(\log x)^{\gamma+3}(\log\log x)^{5/4}+x^{\frac{5+2\beta}{4}}(\log x)^{\gamma+3}\log\log x\right).
\end{aligned}$$

Proof. Throughout, χ, with or without subscript, will denote a character modulo p. As usual, χ_0 will be the principal character modulo p. Let p be a fixed prime, and let $s,t\in\mathbb{F}_p^\times$ be fixed. By [6, Equation (12)], we have

$$\sum_{\substack{|a|\le A,\, |b|\le B\colon \exists 1\le u<p\\ a\equiv su^4 \,(\mathrm{mod}\, p)\\ b\equiv tu^6 \,(\mathrm{mod}\, p)}} 1=\frac{1}{2(p-1)}\sum_{\substack{\chi_1,\chi_2\\ \chi_1^4\chi_2^6=\chi_0}}\chi_1(s)\chi_2(t)\mathcal{A}(\overline{\chi_1})\mathcal{B}(\overline{\chi_2}),$$

where

$$\mathcal{A}(\chi):=\sum_{|a|\le A}\chi(a)\quad\text{and}\quad \mathcal{B}(\chi):=\sum_{|b|\le B}\chi(b).$$

We use the identity

$$\begin{aligned}
&\frac{1}{2(p-1)}\sum_{\substack{\chi_1,\chi_2\\ \chi_1^4\chi_2^6=\chi_0}}\chi_1(s)\chi_2(t)\mathcal{A}(\overline{\chi_1})\mathcal{B}(\overline{\chi_2})\\
&\quad=\frac{1}{2(p-1)}\chi_0(s)\chi_0(t)\mathcal{A}(\overline{\chi_0})\mathcal{B}(\overline{\chi_0})+\frac{1}{2(p-1)}\sum_{\substack{\chi_0\neq\chi_2\\ \chi_2^6=\chi_0}}\chi_0(s)\chi_2(t)\mathcal{A}(\overline{\chi_0})\mathcal{B}(\overline{\chi_2})\\
&\qquad+\frac{1}{2(p-1)}\sum_{\substack{\chi_1\neq\chi_0\\ \chi_1^4=\chi_0}}\chi_1(s)\chi_0(t)\mathcal{A}(\overline{\chi_1})\mathcal{B}(\overline{\chi_0})\\
&\qquad+\frac{1}{2(p-1)}\sum_{\substack{\chi_1\neq\chi_0\\ \chi_2\neq\chi_0\\ \chi_1^4\chi_2^6=\chi_0}}\chi_1(s)\chi_2(t)\mathcal{A}(\overline{\chi_1})\mathcal{B}(\overline{\chi_2})
\end{aligned}$$

and note that

$$\frac{1}{2(p-1)}\chi_0(s)\chi_0(t)\mathcal{A}(\overline{\chi_0})\mathcal{B}(\overline{\chi_0}) = \frac{1}{2(p-1)}\sum_{|a|\le A}\chi_0(a)\sum_{|b|\le B}\chi_0(b) = \frac{2AB}{p} + O\left(\frac{AB}{p^2} + \frac{A+B}{p}\right).$$

Therefore,

$$\frac{2}{|\mathcal{C}|}\sum_{p\le x}\sum_{d|p-1} g(d) \sum_{\substack{1\le s,t<p\\ E_{s,t}(\mathbb{F}_p)[d]\cong(\mathbb{Z}/d\mathbb{Z})^2}} \frac{1}{p-1}\left(\sum_{\substack{|a|\le A,\, |b|\le B:\, \exists 1\le u<p\\ a\equiv su^4 \,(\mathrm{mod}\, p)\\ b\equiv tu^6 \,(\mathrm{mod}\, p)}} 1 - \frac{2AB}{p}\right)$$

$$= \frac{2}{|\mathcal{C}|}\sum_{p\le x}\sum_{d|p-1} g(d) \sum_{\substack{1\le s,t<p\\ E_{s,t}(\mathbb{F}_p)[d]\cong(\mathbb{Z}/d\mathbb{Z})^2}} \frac{1}{p-1}O\left(\frac{AB}{p^2} + \frac{A+B}{p}\right)$$

$$+ \frac{2}{|\mathcal{C}|}\sum_{p\le x}\sum_{d|p-1} g(d) \sum_{\substack{1\le s,t<p\\ E_{s,t}(\mathbb{F}_p)[d]\cong(\mathbb{Z}/d\mathbb{Z})^2}} \frac{1}{2(p-1)^2}\sum_{\substack{\chi_2\ne\chi_0\\ \chi_2^6=\chi_0}}\chi_0(s)\chi_2(t)\mathcal{A}(\overline{\chi_0})\mathcal{B}(\overline{\chi_2})$$

$$+ \frac{2}{|\mathcal{C}|}\sum_{p\le x}\sum_{d|p-1} g(d) \sum_{\substack{1\le s,t<p\\ E_{s,t}(\mathbb{F}_p)[d]\cong(\mathbb{Z}/d\mathbb{Z})^2}} \frac{1}{2(p-1)^2}\sum_{\substack{\chi_1\ne\chi_0\\ \chi_1^4=\chi_0}}\chi_1(s)\chi_0(t)\mathcal{A}(\overline{\chi_1})\mathcal{B}(\overline{\chi_0})$$

$$+ \frac{2}{|\mathcal{C}|}\sum_{p\le x}\sum_{d|p-1} g(d) \sum_{\substack{1\le s,t<p\\ E_{s,t}(\mathbb{F}_p)[d]\cong(\mathbb{Z}/d\mathbb{Z})^2}} \frac{1}{2(p-1)^2}\sum_{\substack{\chi_1\ne\chi_0\\ \chi_2\ne\chi_0\\ \chi_1^4\chi_2^6=\chi_0}}\chi_1(s)\chi_2(t)\mathcal{A}(\overline{\chi_1})\mathcal{B}(\overline{\chi_2})$$

$$=: \varSigma_1 + \varSigma_2 + \varSigma_3 + \varSigma_4.$$

We will evaluate each sum separately.

3.4.1. *Estimation of $\varSigma_1$.* We have

$$\varSigma_1 := \frac{2}{|\mathcal{C}|}\sum_{p\le x}\sum_{d|p-1} g(d) \sum_{\substack{1\le s,t<p\\ E_{s,t}(\mathbb{F}_p)[d]\cong(\mathbb{Z}/d\mathbb{Z})^2}} \frac{1}{p-1}O\left(\frac{AB}{p^2} + \frac{A+B}{p}\right)$$

$$\ll \frac{1}{|\mathcal{C}|}\sum_{p\le x}\left(\frac{AB}{p^3} + \frac{A+B}{p^2}\right)\sum_{d|p-1}|g(d)| \sum_{\substack{1\le s,t<p\\ E_{s,t}(\mathbb{F}_p)[d]\cong(\mathbb{Z}/d\mathbb{Z})^2}} 1$$

$$\ll \frac{AB}{|\mathcal{C}|}\sum_{p\le x}\frac{1}{p^3}\sum_{\substack{d|p-1\\ d\le\sqrt{p}+1}}|g(d)|\left(\frac{p(p-1)}{d\psi(d)\varphi(d)} + O(p^{3/2})\right)$$

$$+ \frac{A+B}{|\mathcal{C}|}\sum_{p\le x}\frac{1}{p^2}\sum_{\substack{d|p-1\\ d\le\sqrt{p}+1}}|g(d)|\left(\frac{p(p-1)}{d\psi(d)\varphi(d)} + O(p^{3/2})\right).$$

We denote the first sum by $\Sigma_{1,1}$ and the second by $\Sigma_{1,2}$. By partial summation and (3.3), we have

$$\Sigma_{1,1} \ll x^{\frac{\beta-1}{2}} (\log x)^{\gamma+1} \log\log x + (\log x)^{\gamma} \log\log x \tag{3.9}$$

as $\beta < 3/2$. By (3.2) and (3.4), we have

(3.10)
$$\begin{aligned}\Sigma_{1,2} &\ll \left(\frac{1}{A}+\frac{1}{B}\right)\Bigg(\sum_{p\le x}\sum_{\substack{d\mid p-1\\ d\le\sqrt{p}+1}} \frac{|g(d)|}{d\psi(d)\varphi(d)} + \sum_{p\le x}\frac{1}{p^{1/2}}\sum_{\substack{d\mid p-1\\ d\le\sqrt{p}+1}} |g(d)|\Bigg)\\ &\ll \left(\frac{1}{A}+\frac{1}{B}\right)\left(\frac{x}{\log x} + x^{\frac{1+\beta}{2}}(\log x)^{\gamma}\log\log x\right).\end{aligned}$$

Therefore, Σ_1 is bounded by the error terms in the lemma.

3.4.2. *Estimations of Σ_2 and Σ_3.* For Σ_2, we see that

$$\begin{aligned}\Sigma_2 &:= \frac{1}{|\mathcal{C}|}\sum_{p\le x}\sum_{\substack{d\mid p-1\\ d\le\sqrt{p}+1}} g(d) \sum_{\substack{1\le s,t<p\\ E_{s,t}(\mathbb{F}_p)[d]\cong(\mathbb{Z}/d\mathbb{Z})^2}} \frac{1}{(p-1)^2}\sum_{\substack{\chi_2\ne\chi_0\\ \chi_2^6=\chi_0}} \chi_0(s)\chi_2(t)\mathcal{A}(\overline{\chi_0})\mathcal{B}(\overline{\chi_2})\\ &\ll \frac{1}{|\mathcal{C}|}\sum_{p\le x}\sum_{\substack{d\mid p-1\\ d\le\sqrt{p}+1}} |g(d)| \sum_{\substack{1\le s,t<p\\ E_{s,t}(\mathbb{F}_p)[d]\cong(\mathbb{Z}/d\mathbb{Z})^2}} \frac{1}{p^2}\sum_{\substack{\chi_2\ne\chi_0\\ \chi_2^6=\chi_0}} |\mathcal{B}(\overline{\chi_2})| \sum_{\substack{-A\le a\le A\\ p\nmid a}} 1\\ &\ll \frac{A}{|\mathcal{C}|}\sum_{p\le x}\frac{1}{p^2}\sum_{\substack{d\mid p-1\\ d\le\sqrt{p}+1}} |g(d)| \sum_{\substack{\chi_2\ne\chi_0\\ \chi_2^6=\chi_0}} |\mathcal{B}(\overline{\chi_2})| \sum_{\substack{1\le s,t<p\\ E_{s,t}(\mathbb{F}_p)[d]\cong(\mathbb{Z}/d\mathbb{Z})^2}} 1.\end{aligned}$$

By Lemma 2.1, we have

$$\begin{aligned}\Sigma_2 &\ll \frac{1}{B}\sum_{p\le x}\frac{1}{p^2}\sum_{\substack{d\mid p-1\\ d\le\sqrt{p}+1}} |g(d)| \sum_{\substack{\chi_2\ne\chi_0\\ \chi_2^6=\chi_0}} |\mathcal{B}(\overline{\chi_2})|\left(\frac{p(p-1)}{d\psi(d)\varphi(d)} + O(p^{3/2})\right)\\ &\ll \frac{1}{B}\sum_{p\le x}\sum_{\substack{d\mid p-1\\ d\le\sqrt{p}+1}} \frac{|g(d)|}{d\psi(d)\varphi(d)} \sum_{\substack{\chi_2\ne\chi_0\\ \chi_2^6=\chi_0}} |\mathcal{B}(\overline{\chi_2})|\\ &\quad + \frac{1}{B}\sum_{p\le x}\frac{1}{p^{1/2}}\sum_{\substack{d\mid p-1\\ d\le\sqrt{p}+1}} |g(d)| \sum_{\substack{\chi_2\ne\chi_0\\ \chi_2^6=\chi_0}} |\mathcal{B}(\overline{\chi_2})|\\ &=: \Sigma_{2,1} + \Sigma_{2.2}.\end{aligned}$$

Now,

$$\Sigma_{2,1} = \frac{1}{B}\sum_{d\le\sqrt{x}+1} \frac{|g(d)|}{d\psi(d)\varphi(d)} \sum_{\substack{p\le x\\ p\equiv 1 \pmod{d}}} \sum_{\substack{\chi_2\ne\chi_0\\ \chi_2^6=\chi_0}} |\mathcal{B}(\overline{\chi_2})|. \tag{3.11}$$

Let $k = [2\log x/\log B] + 1$. By Hölder's inequality we deduce

$$\sum_{\substack{p\le x\\ p\equiv 1\,(\mathrm{mod}\,d)}} \sum_{\substack{\chi_2\ne\chi_0\\ \chi_2^6=\chi_0}} |\mathcal{B}(\overline{\chi_2})| \tag{3.12}$$

$$\le \Bigg(\sum_{\substack{p\le x\\ p\equiv 1\,(\mathrm{mod}\,d)}} \sum_{\substack{\chi_2\ne\chi_0\\ \chi_2^6=\chi_0}} 1\Bigg)^{1-\frac{1}{2k}} \Bigg(\sum_{\substack{p\le x\\ p\equiv 1\,(\mathrm{mod}\,d)}} \sum_{\substack{\chi_2\ne\chi_0\\ \chi_2^6=\chi_0}} \Big|\sum_{b\le B}\chi_2(b)\Big|^{2k}\Bigg)^{\frac{1}{2k}}$$

$$\ll (\pi(x;d,1))^{1-\frac{1}{2k}} \Big(\sum_{p\le x}\sum_{\chi_2\ne\chi_0}\Big|\sum_{b\le B^k}\tau_{k,B}(b)\chi_2(b)\Big|^2\Big)^{\frac{1}{2k}},$$

where $\tau_{k,B}(n) := \#\{(a_1,\dots,a_k)\in[1,B]^k\cap\mathbb{N}^k;\ n = a_1\cdots a_k\}$. By Lemma 2.4, we have

$$\sum_{p\le x}\sum_{\chi\ne\chi_0}\Big|\sum_{b\le B^k}\tau_{k,B}(b)\chi(b)\Big|^2 \ll (x^2+B^k)\sum_{b\le B^k}\tau_{k,B}(b)^2. \tag{3.13}$$

Suppose $k=1$, that is, $B > x^2$. Then

$$\sum_{p\le x}\sum_{\chi_2\ne\chi_0}\Big|\sum_{b\le B^k}\tau_1^B(b)\chi_2(b)\Big|^2 \ll B^2.$$

Therefore from (3.12) we get

$$\sum_{\substack{p\le x\\ p\equiv 1\,(\mathrm{mod}\,d)}} \sum_{\substack{\chi_2\ne\chi_0\\ \chi_2^6=\chi_0}} |\mathcal{B}(\overline{\chi_2})| \ll B\frac{x^{1/2}}{\varphi(d)^{1/2}(\log x)^{1/2}}$$

after using Lemma 2.8(i). Substituting this inequality into (3.11), we obtain

$$\Sigma_{2,1} \ll \frac{x^{1/2}}{(\log x)^{1/2}}\sum_{d\le x}\frac{|g(d)|}{d\psi(d)\varphi(d)^{3/2}} \ll \frac{x^{1/2}}{(\log x)^{1/2}},$$

as $\beta < 3/2$.

Now suppose $k = [2\log x/\log B] + 1 > 1$. Then $B \le x^2$ and $x^2 < B^k \le Bx^2 \le x^4$. Therefore, by Lemma 2.5(i), (ii), (3.12), (3.13), and the trivial bound for $\pi(x;d,1)$, we have

(3.14)

$$\sum_{\substack{p\le x\\ p\equiv 1\,(\mathrm{mod}\,d)}} \sum_{\substack{\chi_2\ne\chi_0\\ \chi_2^6=\chi_0}} |\mathcal{B}(\overline{\chi_2})| \ll \Big(\frac{x}{d}\Big)^{1-\frac{1}{2k}}\Big((x^2+B^k)B^k(\Psi(B,9\log x))^k\Big)^{\frac{1}{2k}}$$

$$\ll B\frac{x}{d^{3/4}}x^{-\frac{1}{2k}}\Big(\Psi(B,9\log x)\Big)^{1/2}$$

$$\ll B\frac{x}{d^{3/4}}\exp\Big(-c_2\frac{(\log x)^{1/2}}{\log\log x}\Big),$$

where $c_2 > 0$, if $B > \exp(c_1(\log x)^{1/2})$ for sufficiently large c_1. Substituting (3.14) into (3.11), we obtain

$$\Sigma_{2,1} \ll x \exp\left(-c_2 \frac{(\log x)^{1/2}}{\log\log x}\right) \sum_{d \leq x} \frac{|g(d)|}{d^{7/4}\psi(d)\varphi(d)} \ll x \exp\left(-c_2 \frac{(\log x)^{1/2}}{\log\log x}\right),$$

as $\beta < 3/2$.

For $\Sigma_{2,2}$, by Lemma 2.6(i), (1.2) and Lemma 2.8(i), (ii), (v), we have

$$\begin{aligned}
\Sigma_{2,2} &= \frac{1}{B} \sum_{p \leq x} \frac{1}{p^{1/2}} \sum_{\substack{d \mid p-1 \\ d \leq \sqrt{p}+1}} |g(d)| \sum_{\substack{\chi_2 \neq \chi_0 \\ \chi_2^6 = \chi_0}} |\mathcal{B}(\overline{\chi_2})(b)| \\
&\ll \frac{1}{B} \sum_{d \leq \sqrt{x}+1} |g(d)| \sum_{\substack{p \leq x \\ p \equiv 1 \,(\mathrm{mod}\, d)}} \frac{1}{p^{1/2}} \sum_{\substack{\chi_2 \neq \chi_0 \\ \chi_2^6 = \chi_0}} \Big| \sum_{b \leq B} \chi_2(b) \Big| \\
&\ll \frac{1}{B^{1/r}} \sum_{d \leq \sqrt{x}+1} |g(d)| \sum_{\substack{p \leq x \\ p \equiv 1 \,(\mathrm{mod}\, d)}} p^{\frac{-2r^2+r+1}{4r^2}} \log p \sum_{\substack{\chi_2 \neq \chi_0 \\ \chi_2^6 = \chi_0}} 1 \\
&\ll \frac{x^{\frac{1}{2}+\frac{r+1}{4r^2}} \log\log x}{B^{1/r}} \sum_{d \leq \sqrt{x}+1} \frac{|g(d)|}{d} \ll \frac{x^{\frac{1+\beta}{2}+\frac{r+1}{4r^2}} (\log x)^{\gamma+1} \log\log x}{B^{1/r}}.
\end{aligned}$$

The proof of the bound for Σ_2 gives us the same bound for Σ_3, *mutatis mutandis*.

3.4.3. *Estimation of Σ_4.* For Σ_4, we have

$$\begin{aligned}
\Sigma_4 &= \frac{2}{|\mathcal{C}|} \sum_{p \leq x} \sum_{\substack{d \mid p-1 \\ d \leq \sqrt{p}+1}} g(d) \sum_{\substack{1 \leq s,t < p \\ E_{s,t}(\mathbb{F}_p)[d] \cong (\mathbb{Z}/d\mathbb{Z})^2}} \frac{1}{2(p-1)^2} \sum_{\substack{\chi_1 \neq \chi_0 \\ \chi_2 \neq \chi_0 \\ \chi_1^4 \chi_2^6 = \chi_0}} \chi_1(s)\chi_2(t)\mathcal{A}(\overline{\chi_1})\mathcal{B}(\overline{\chi_2}) \\
&= \frac{1}{|\mathcal{C}|} \sum_{d \leq \sqrt{x}+1} g(d) \sum_{\substack{p \leq x \\ p \equiv 1 \,(\mathrm{mod}\, d)}} \frac{1}{(p-1)^2} \sum_{\substack{\chi_1 \neq \chi_0 \\ \chi_2 \neq \chi_0 \\ \chi_1^4 \chi_2^6 = \chi_0}} \mathcal{A}(\overline{\chi_1})\mathcal{B}(\overline{\chi_2}) \sum_{\substack{1 \leq s,t < p \\ E_{s,t}(\mathbb{F}_p)[d] \cong (\mathbb{Z}/d\mathbb{Z})^2}} \chi_1(s)\chi_2(t) \\
&= \frac{1}{|\mathcal{C}|} \sum_{d \leq \sqrt{x}+1} g(d) \sum_{\substack{p \leq x \\ p \equiv 1 \,(\mathrm{mod}\, d)}} \frac{1}{(p-1)^2} \sum_{\substack{\chi_1 \neq \chi_0 \\ \chi_2 \neq \chi_0 \\ \chi_1^4 \chi_2^6 = \chi_0}} \mathcal{A}(\overline{\chi_1})\mathcal{B}(\overline{\chi_2})\mathcal{W}_{p,d}(\chi_1,\chi_2),
\end{aligned}$$

where

$$\mathcal{W}_{p,d}(\chi_1,\chi_2) := \sum_{\substack{1 \leq s,t < p \\ E_{s,t}(\mathbb{F}_p)[d] \cong (\mathbb{Z}/d\mathbb{Z})^2}} \chi_1(s)\chi_2(t).$$

Applying the Cauchy–Schwarz inequality twice, we obtain

$$\Big| \sum_{\substack{\chi_1 \neq \chi_0 \\ \chi_2 \neq \chi_0 \\ \chi_1^4\chi_2^6 = \chi_0}} \mathcal{A}(\overline{\chi_1})\mathcal{B}(\overline{\chi_2})\mathcal{W}_{p,d}(\chi_1,\chi_2)\Big|^4$$

$$\leq \bigg(\sum_{\substack{\chi_1 \neq \chi_0 \\ \chi_2 \neq \chi_0 \\ \chi_1^4\chi_2^6 = \chi_0}} \big|\mathcal{W}_{p,d}(\chi_1,\chi_2)\big|^2 \bigg)^2 \bigg(\sum_{\substack{\chi_1 \neq \chi_0 \\ \chi_2 \neq \chi_0 \\ \chi_1^4\chi_2^6 = \chi_0}} |\mathcal{A}(\chi_1)|^4 \bigg)\bigg(\sum_{\substack{\chi_1 \neq \chi_0 \\ \chi_2 \neq \chi_0 \\ \chi_1^4\chi_2^6 = \chi_0}} |\mathcal{B}(\chi_2)|^4 \bigg).$$

By Lemma 2.7, we have

$$\sum_{\chi_1 \neq \chi_0} \Big| \sum_{a \leq A} \chi_1(a) \Big|^4 \ll A^2 p (\log p)^6.$$

Hence,

$$\sum_{\substack{\chi_1 \neq \chi_0 \\ \chi_2 \neq \chi_0 \\ \chi_1^4\chi_2^6 = \chi_0}} |\mathcal{A}(\chi_1)|^4 = \sum_{\substack{\chi_1 \neq \chi_0 \\ \chi_2 \neq \chi_0 \\ \chi_1^4\chi_2^6 = \chi_0}} \Big| \sum_{|a| \leq A} \chi_1(a) \Big|^4 \leq 16 \sum_{\chi_1 \neq \chi_0} \Big| \sum_{a \leq A} \chi_1(a) \Big|^4 \sum_{\substack{\chi_2 \neq \chi_0 \\ \chi_1^4\chi_2^6 = \chi_0}} 1$$

$$\ll \sum_{\chi_1 \neq \chi_0} \Big| \sum_{a \leq A} \chi_1(a) \Big|^4 \ll A^2 p (\log p)^6.$$

Similarly,

$$\sum_{\substack{\chi_1 \neq \chi_0 \\ \chi_2 \neq \chi_0 \\ \chi_1^4\chi_2^6 = \chi_0}} |\mathcal{B}(\chi_2)|^4 \ll B^2 p (\log p)^6.$$

Also,

$$\begin{aligned}
(3.15) \qquad & \sum_{\chi_1,\chi_2} \big|\mathcal{W}_{p,d}(\chi_1,\chi_2)\big|^2 \\
&= \sum_{\chi_1,\chi_2} \sum_{\substack{1 \leq s,t < p \\ E_{s,t}(\mathbb{F}_p)[d] \cong (\mathbb{Z}/d\mathbb{Z})^2}} \chi_1(s)\chi_2(t) \sum_{\substack{1 \leq s',t' < p \\ E_{s',t'}(\mathbb{F}_p)[d] \cong (\mathbb{Z}/d\mathbb{Z})^2}} \overline{\chi_1}(s')\overline{\chi_2}(t') \\
&= \sum_{\substack{1 \leq s,t < p \\ E_{s,t}(\mathbb{F}_p)[d] \cong (\mathbb{Z}/d\mathbb{Z})^2}} \sum_{\substack{1 \leq s',t' < p \\ E_{s',t'}(\mathbb{F}_p)[d] \cong (\mathbb{Z}/d\mathbb{Z})^2}} \sum_{\chi_1} \chi_1(s)\overline{\chi_1}(s') \sum_{\chi_2} \chi_2(t)\overline{\chi_2}(t') \\
&= (p-1)^2 \sum_{\substack{1 \leq s,t < p \\ E_{s,t}(\mathbb{F}_p)[d] \cong (\mathbb{Z}/d\mathbb{Z})^2}} 1 \ll \frac{p^4}{d\psi(d)\varphi(d)} + p^{7/2}
\end{aligned}$$

by Lemma 2.1. Putting all this information together, we obtain

$$\Bigg|\sum_{\substack{\chi_1\neq\chi_0\\ \chi_2\neq\chi_0\\ \chi_1^4\chi_2^6=\chi_0}} \mathcal{A}(\overline{\chi_1})\mathcal{B}(\overline{\chi_2})\mathcal{W}_{p,d}(\chi_1,\chi_2)\Bigg|^4$$
$$\ll \frac{(AB)^2p^{10}(\log p)^{12}}{d^2\psi(d)^2\varphi(d)^2} + \frac{(AB)^2p^{19/2}(\log p)^{12}}{d\psi(d)\varphi(d)} + (AB)^2p^9(\log p)^{12}.$$

Hence,

$$\begin{aligned}\Sigma_4 &\ll \frac{1}{|\mathcal{C}|}\sum_{d\leq\sqrt{x}+1}|g(d)|\sum_{\substack{p\leq x\\ p\equiv 1\ (\mathrm{mod}\ d)}}\sqrt{AB}(\log p)^3\\
&\qquad\times\bigg(\frac{p^{1/2}}{d^{1/2}\psi(d)^{1/2}\varphi(d)^{1/2}} + \frac{p^{3/8}}{d^{1/4}\psi(d)^{1/4}\varphi(d)^{1/4}} + p^{1/4}\bigg)\\
&\ll \frac{1}{\sqrt{AB}}\big(x^{3/2}(\log x)^2 + x^{1+\beta/2}(\log x)^{\gamma+3}(\log\log x)^{5/4}\\
&\qquad + x^{\frac{5+2\beta}{4}}(\log x)^{\gamma+3}\log\log x\big),\end{aligned}$$

as $\beta < 3/2$.

This completes the proof of Lemma 3.1. ∎

3.5. Proof of Theorem 1.2. By combining (3.5), (3.8), and Lemma 3.1, we obtain

$$\frac{1}{|\mathcal{C}|}\sum_{E_{a,b}\in\mathcal{C}}\sum_{p\leq x} f(i_{E_{a,b}}(p)) = \bigg(\sum_{d\geq 1}\frac{g(d)}{d\psi(d)\varphi(d)^2}\bigg)\,\mathrm{li}(x) + E,$$

where

$$\begin{aligned}E &\ll \frac{x}{(\log x)^c} + \left(\frac{1}{A}+\frac{1}{B}\right)\left(\frac{x}{\log x} + x^{\frac{1+\beta}{2}}(\log x)^{\gamma+2}\right)\\
&\quad + \left(\frac{1}{A^{1/r}}+\frac{1}{B^{1/r}}\right)x^{\frac{1+\beta}{2}+\frac{r+1}{4r^2}}(\log x)^{\gamma+1}\log\log x + \frac{x^{3/2}(\log x)^2}{\sqrt{AB}}\\
&\quad + \frac{1}{\sqrt{AB}}(x^{1+\beta/2}(\log x)^{\gamma+3}(\log\log x)^{5/4} + x^{\frac{5+2\beta}{4}}(\log x)^{\gamma+3}\log\log x)\end{aligned}$$

for given $c > 1$ and $A, B > \exp(c_1(\log x)^{1/2})$. Now we choose r large enough so that $\frac{1+\beta}{2} + \frac{r+1}{4r^2} < 1$. (Note that we can do this if $\beta < 1$.) So we arrive at the upper bound

$$\begin{aligned}E &\ll \frac{x}{(\log x)^c} + x\exp\left(-\frac{c_1}{r}(\log x)^{1/2}\right)\\
&\quad + \frac{1}{\sqrt{AB}}(x^{3/2}(\log x)^2 + x^{\frac{5+2\beta}{4}}(\log x)^{\gamma+3}\log\log x).\end{aligned}$$

Now the result follows by choosing $AB \geq x(\log x)^{4+2c}$ if $\beta < 1/2$, and $AB \geq x^{1/2+\beta}(\log x)^{2\gamma+6+2c}(\log\log x)^2$ if $1/2 \leq \beta < 1$.

3.6. Proof of Corollary 1.6. Parts (i) and (ii) hold since the characteristic function of $\{1\}$ can be written as

$$\sum_{d|n} \mu(d)$$

and the divisor function can be written as

$$\tau(n) = \sum_{d|n} 1.$$

Thus, $g(d) = \mu(d)$ and $g(d) = 1$ both satisfy (1.2) with $\beta = 0$ and $\gamma = 1$.

For (iii), let $f(n) = 1/n^k$, where $k \in \mathbb{N}$. Then writing

$$f(n) = \sum_{d|n} g(d)$$

gives us

$$|g(n)| = \sum_{d|n} |\mu(n/d) f(d)| \leq \sum_{d|n} 1 = \tau(n).$$

Therefore, by Theorem 1.2, we have

$$\frac{1}{|\mathcal{C}|} \sum_{E\in\mathcal{C}} \sum_{p\leq x} \frac{1}{i_E(p)^k} = C_k \operatorname{li}(x) + O\biggl(\frac{x}{(\log x)^c}\biggr), \tag{3.16}$$

where C_k is defined in the corollary. Let $a_p(E)$ be defined by $\#E_p(\mathbb{F}_p) = p + 1 - a_p(E)$. Hasse's Theorem says that $|a_p(E)| \leq 2\sqrt{p}$. Note that

$$\begin{aligned}
\sum_{E\in\mathcal{C}} \sum_{p\leq x} e_E(p)^k &= \sum_{E\in\mathcal{C}} \sum_{p\leq x} \biggl(\frac{p+1-a_E(p)}{i_E(p)}\biggr)^k \\
&= \sum_{E\in\mathcal{C}} \sum_{p\leq x} \biggl(\frac{p^k}{i_E(p)^k} + \sum_{j=1}^{k} \binom{k}{j} \frac{p^{k-j}(1-a_p(E))^j}{i_E(p)^k}\biggr) \\
&= \sum_{E\in\mathcal{C}} \sum_{p\leq x} \frac{p^k}{i_E(p)^k} + O_k\biggl(x^{k-1/2} \sum_{E\in\mathcal{C}} \sum_{p\leq x} \frac{1}{i_p(E)^k}\biggr) \\
&= \sum_{E\in\mathcal{C}} \sum_{p\leq x} \frac{p^k}{i_E(p)^k} + O_k\biggl(\frac{|\mathcal{C}| x^{k+1/2}}{\log x}\biggr).
\end{aligned}$$

For the first part in the above, by (3.16), we have

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\sum_{p\le x}\frac{p^k}{i_E(p)^k} = C_k x^k \operatorname{li}(x) + O\left(\frac{x^{k+1}}{(\log x)^c}\right)$$
$$- C_k k\int_2^x t^{k-1}\operatorname{li}(t)\,dt + O_k\left(\int_2^x \frac{t^k}{(\log t)^c}\,dt\right)$$
$$= C_k x^k \operatorname{li}(x) - C_k k\int_2^x t^{k-1}\operatorname{li}(t)\,dt + O\left(\frac{x^{k+1}}{(\log x)^c}\right).$$

Then the result holds since there exists a constant C such that

$$\operatorname{li}(x^{k+1}) + C = x^k\operatorname{li}(x) - k\int_2^x t^{k-1}\operatorname{li}(t)\,dt.$$

4. A technical lemma

Lemma 4.1. *Let $r\in\mathbb{N}$ and $\varepsilon>0$ be fixed. Let $g:\mathbb{N}\to\mathbb{C}$ be a function such that*

$$\sum_{d\le x}|g(d)| \ll x^{1+\beta}(\log x)^{\gamma},$$

where $0\le\beta<3/4$ and $\gamma\in\mathbb{R}_{\ge 0}$. Then there are positive constants c_1 and c_3 such that if

$$A, B > \exp(c_1(\log x)^{1/2}),$$

we have

$$\frac{4}{|\mathcal{C}|}\sum_{\substack{p,q\le x\\ p\ne q}}\frac{1}{(p-1)(q-1)}$$
$$\times \sum_{\substack{s,t\in\mathbb{F}_p^\times\\ s',t'\in\mathbb{F}_q^\times}}\ \sum_{\substack{d\mid i_{E_{s,t}}(p)\\ d'\mid i_{E_{s',t'}}(q)}} g(d)g(d')\Bigg(\sum_{\substack{|a|\le A,\,|b|\le B\colon \exists 1\le u<p,\,1\le u'<q\\ a\equiv su^4 \,(\mathrm{mod}\,p),\, a\equiv s'(u')^4 \,(\mathrm{mod}\,q)\\ b\equiv tu^6 \,(\mathrm{mod}\,p),\, b\equiv t'(u')^6 \,(\mathrm{mod}\,q)}} 1 - \frac{AB}{pq}\Bigg)$$
$$\ll x(\log x)^{\gamma-1}(\log\log x) + \left(\frac{1}{A}+\frac{1}{B}\right)\frac{x^2}{(\log x)^2} + x^2\exp\left(-c_3\frac{(\log x)^{1/2}}{\log\log x}\right)$$
$$+\left(\frac{1}{A^{1/r}}+\frac{1}{B^{1/r}}\right)x^{\frac{3+\beta}{2}+\frac{r+1}{2r^2}+2\varepsilon}(\log x)^{\gamma}\log\log x$$
$$+\frac{1}{\sqrt{AB}}\left(x^3(\log x) + x^{\frac{11+2\beta}{4}}(\log x)^{2\gamma+3}(\log\log x)^2\right).$$

Proof. Throughout, a prime $'$ will denote that the underlying object is related to the prime q. Note that, for p,q prime, $s,t\in\mathbb{F}_p^\times$ and $s',t'\in\mathbb{F}_q^\times$ fixed, by orthogonality relations, we have

$$\sum_{\substack{|a|\le A,\,|b|\le B:\,\exists 1\le u<p,\,1\le u'<q\\ a\equiv su^4\,(\mathrm{mod}\,p),\,a\equiv s'(u')^4\,(\mathrm{mod}\,q)\\ b\equiv tu^6\,(\mathrm{mod}\,p),\,b\equiv t'(u')^6\,(\mathrm{mod}\,q)}} 1$$
$$= \frac{1}{4}\sum_{1\le u<p}\ \sum_{1\le u'<q}\ \sum_{|a|\le A}\ \sum_{|b|\le B}\left(\frac{1}{p-1}\sum_{\chi_1\,(\mathrm{mod}\,p)}\chi_1(su^4)\overline{\chi_1}(a)\right)$$
$$\times\left(\frac{1}{p-1}\sum_{\chi_2\,(\mathrm{mod}\,p)}\chi_2(tu^6)\overline{\chi_2}(b)\right)\left(\frac{1}{q-1}\sum_{\chi_1'\,(\mathrm{mod}\,q)}\chi_1'(s'(u')^4)\overline{\chi_1'}(a)\right)$$
$$\times\left(\frac{1}{q-1}\sum_{\chi_2'\,(\mathrm{mod}\,q)}\chi_2'(t'(u')^6)\overline{\chi_2'}(b)\right)$$
$$= \frac{1}{4(p-1)(q-1)}\sum_{\substack{\chi_1,\chi_2\,(\mathrm{mod}\,p)\\ \chi_1^4\chi_2^6=\chi_0}}\chi_1(s)\chi_2(t)$$
$$\times\sum_{\substack{\chi_1',\chi_2'\,(\mathrm{mod}\,q)\\ (\chi_1')^4(\chi_2')^6=\chi_0'}}\chi_1'(s')\chi_2'(t')\mathcal{A}(\overline{\chi_1\chi_1'})\mathcal{B}(\overline{\chi_2\chi_2'}),$$

where

$$\mathcal{A}(\chi) := \sum_{|a|\le A}\chi(a)\quad\text{and}\quad \mathcal{B}(\chi) := \sum_{|b|\le B}\chi(b).$$

Thus,

$$\sum_{\substack{|a|\le A,\,|b|\le B:\,\exists 1\le u<p,\,1\le u'<q\\ a\equiv su^4\,(\mathrm{mod}\,p),\,a\equiv s'(u')^4\,(\mathrm{mod}\,q)\\ b\equiv tu^6\,(\mathrm{mod}\,p),\,b\equiv t'(u')^6\,(\mathrm{mod}\,q)}} 1 = \sum_{j=1}^{16} S_j(p,q,s,t,s',t'),$$

where S_j corresponds to one of the cases arising from choices of each of the following conditions:

$$\left\{\begin{matrix}\chi_1=\chi_0,\ \chi_2=\chi_0\\ \chi_1=\chi_0,\ \chi_2\ne\chi_0:\chi_2^6=\chi_0\\ \chi_1\ne\chi_0,\ \chi_2=\chi_0:\chi_1^4=\chi_0\\ \chi_1\ne\chi_0,\ \chi_2\ne\chi_0:\chi_1^4\chi_2^6=\chi_0\end{matrix}\right\}\times\left\{\begin{matrix}\chi_1'=\chi_0',\ \chi_2'=\chi_0'\\ \chi_1'=\chi_0',\ \chi_2'\ne\chi_0':(\chi_2')^6=\chi_0'\\ \chi_1'\ne\chi_0',\ \chi_2'=\chi_0':(\chi_1')^4=\chi_0'\\ \chi_1'\ne\chi_0',\ \chi_2'\ne\chi_0':(\chi_1')^4(\chi_2')^6=\chi_0'\end{matrix}\right\}.$$

From these 16 cases, there are essentially five different cases to handle.

Case 1: All four of $\chi_1,\chi_2,\chi_1',\chi_2'$ are principal. Let this correspond to $j=1$. Then, for $p\ne q$, we have

$$S_1(p,q,s,t,s',t') = \frac{AB}{pq} + O\left(\frac{AB}{p^2q}\right) + O\left(\frac{AB}{pq^2}\right) + O\left(\frac{A+B}{pq}\right).$$

Thus,

$$\frac{4}{|\mathcal{C}|}\sum_{\substack{p,q\le x\\ p\neq q}}\frac{1}{(p-1)(q-1)}$$

$$\times\sum_{\substack{s,t\in\mathbb{F}_p^\times\\ s',t'\in\mathbb{F}_q^\times}}\sum_{\substack{d|i_{E_{s,t}}(p)\\ d'|i_{E_{s',t'}}(q)}} g(d)g(d')\Bigg(\sum_{\substack{|a|\le A,\,|b|\le B:\,\exists 1\le u<p,\,1\le u'<q\\ a\equiv su^4\,(\mathrm{mod}\,p),\,a\equiv s'(u')^4\,(\mathrm{mod}\,q)\\ b\equiv tu^6\,(\mathrm{mod}\,p),\,b\equiv t'(u')^6\,(\mathrm{mod}\,q)}} 1-\frac{AB}{pq}\Bigg)$$

$$=\frac{4}{|\mathcal{C}|}\sum_{\substack{p,q\le x\\ p\neq q}}\frac{1}{(p-1)(q-1)}\sum_{\substack{s,t\in\mathbb{F}_p^\times\\ s',t'\in\mathbb{F}_q^\times}}\sum_{\substack{d|i_{E_{s,t}}(p)\\ d'|i_{E_{s',t'}}(q)}} g(d)g(d')$$

$$\times\Bigg(\sum_{j=2}^{16}S(p,q,s,t,s',t')+O\Bigg(\frac{AB}{p^2q}+\frac{AB}{pq^2}+\frac{A+B}{pq}\Bigg)\Bigg).$$

The sums corresponding to $j=2,\dots,16$ are dealt with in Cases 2–5. Here, we will bound the sums corresponding to the error terms above. We have

$$\frac{4}{|\mathcal{C}|}\sum_{\substack{p,q\le x\\ p\neq q}}\frac{1}{(p-1)(q-1)}\sum_{\substack{s,t\in\mathbb{F}_p^\times\\ s',t'\in\mathbb{F}_q^\times}}\sum_{\substack{d|i_{E_{s,t}}(p)\\ d'|i_{E_{s',t'}}(q)}} g(d)g(d')\frac{AB}{p^2q}$$

$$\ll\Bigg(\sum_{p\le x}\frac{1}{p^3}\sum_{s,t\in\mathbb{F}_p^\times}\sum_{d|i_{E_{s,t}}(p)}|g(d)|\Bigg)\Bigg(\sum_{q\le x}\frac{1}{q^2}\sum_{s',t'\in\mathbb{F}_q^\times}\sum_{d|i_{E_{s',t'}}(q)}|g(d')|\Bigg).$$

The first sum can be bounded just as $\Sigma_{1,1}$ in Subsection 3.4.1, and the second as $\Sigma_{1,2}$ in Subsection 3.4.1. That is, by (3.9), (3.10), and $\beta<3/4$, we have

$$\frac{4}{|\mathcal{C}|}\sum_{p,q\le x}\frac{1}{(p-1)(q-1)}\sum_{\substack{s,t\in\mathbb{F}_p^\times\\ s',t'\in\mathbb{F}_q^\times}}\sum_{\substack{d|i_{E_{s,t}}(p)\\ d'|i_{E_{s',t'}}(q)}} g(d)g(d')\frac{AB}{p^2q}\ll x(\log x)^{\gamma-1}\log\log x.$$

The same bound holds for the term coming from $O(AB/(pq^2))$. For the last error term, by (3.10), we have

$$\frac{4}{|\mathcal{C}|}\sum_{\substack{p,q\le x\\ p\neq q}}\frac{1}{(p-1)(q-1)}\sum_{\substack{s,t\in\mathbb{F}_p^\times\\ s',t'\in\mathbb{F}_q^\times}}\sum_{\substack{d|i_{E_{s,t}}(p)\\ d'|i_{E_{s',t'}}(q)}} g(d)g(d')\frac{A+B}{pq}$$

$$\ll\Big(\frac{1}{A}+\frac{1}{B}\Big)\Bigg(\sum_{p\le x}\frac{1}{p^2}\sum_{s,t\in\mathbb{F}_p^\times}\sum_{d|i_{E_{s,t}}(p)}|g(d)|\Bigg)\Bigg(\sum_{q\le x}\frac{1}{q^2}\sum_{s',t'\in\mathbb{F}_q^\times}\sum_{d|i_{E_{s',t'}}(q)}|g(d')|\Bigg)$$

$$\ll\Big(\frac{1}{A}+\frac{1}{B}\Big)\frac{x^2}{(\log x)^2}.$$

CASE 2: Exactly two of $\chi_1, \chi_2, \chi_1', \chi_2'$ are principal. We have two subcases to consider.

SUBCASE 2a: Exactly one of χ_1 or χ_2 is principal and exactly one of χ_1' or χ_2' is principal. We will bound the sum when $\chi_1 = \chi_0$ and $\chi_1' = \chi_0'$. The bound when $\chi_1 = \chi_0$ and $\chi_2' = \chi_0'$ is similar.

The estimation is analogous to those of Σ_2 and Σ_3 in Subsection 3.4.2. We note that $\chi_0\chi_0'$ is the principal character modulo pq since $p \neq q$. Hence, $|\mathcal{A}(\chi_0\chi_0')| \ll A$. Thus,

$$
\begin{aligned}
(4.1)\qquad & \frac{4}{|\mathcal{C}|}\sum_{\substack{p,q\le x\\ p\neq q}} \frac{1}{(p-1)(q-1)} \sum_{\substack{s,t\in\mathbb{F}_p^\times\\ s',t'\in\mathbb{F}_q^\times}} \sum_{\substack{d\mid i_{E_{s,t}}(p)\\ d'\mid i_{E_{s',t'}}(q)}} g(d)g(d')\frac{1}{4(p-1)(q-1)} \\
&\qquad \times \sum_{\substack{\chi_2\neq\chi_0,\,\chi_2'\neq\chi_0'\\ \chi_2^6=\chi_0,\,(\chi_2')^6=\chi_0'}} \chi_2(t)\chi_2'(t')\mathcal{A}(\overline{\chi_0\chi_0'})\mathcal{B}(\overline{\chi_2\chi_2'}) \\
&\ll \frac{1}{B}\sum_{\substack{p,q\le x\\ p\neq q}} \frac{1}{p^2q^2} \sum_{\substack{d\mid p-1\\ d\le\sqrt{p}+1\\ d'\mid q-1\\ d\le\sqrt{q}+1}} |g(d)|\cdot|g(d')| \sum_{\substack{s,t\in\mathbb{F}_p^\times\\ E_{s,t}(\mathbb{F}_p)[d]\cong(\mathbb{Z}/d\mathbb{Z})^2\\ s',t'\in\mathbb{F}_p^\times\\ E_{s',t'}(\mathbb{F}_q)[d']\cong(\mathbb{Z}/d'\mathbb{Z})^2}} \sum_{\substack{\chi_2\neq\chi_0,\,\chi_2'\neq\chi_0'\\ \chi_2^6=\chi_0,\,(\chi_2')^6=\chi_0'}} |\mathcal{B}(\overline{\chi_2\chi_2'})| \\
&\ll \frac{1}{B}\sum_{d\le\sqrt{x}+1} |g(d)| \sum_{d'\le\sqrt{x}+1} |g(d')| \sum_{\substack{p\le x\\ p\equiv 1 \,(\mathrm{mod}\, d)}} \frac{1}{p^2} \sum_{\substack{q\le x\\ q\equiv 1 \,(\mathrm{mod}\, d')}} \frac{1}{q^2} \sum_{\substack{\chi_2\neq\chi_0,\,\chi_2'\neq\chi_0'\\ \chi_2^6=\chi_0,\,(\chi_2')^6=\chi_0'}} |\mathcal{B}(\overline{\chi_2\chi_2'})| \\
&\qquad \times \left(\frac{p(p-1)}{d\psi(d)\varphi(d)} + O(p^{3/2})\right)\left(\frac{q(q-1)}{d'\psi(d')\varphi(d')} + O(q^{3/2})\right) \\
&= \sigma_1+\sigma_2+\sigma_3+\sigma_4,
\end{aligned}
$$

where σ_1 is the sum corresponding to the product of the main terms in (4.1), σ_4 corresponds to the product of the error terms in (4.1), and σ_2, σ_3 correspond to the mixed terms. We will evaluate each of these sums separately.

For the first sum we have

$$
(4.2)\qquad \sigma_1 = \frac{1}{B}\sum_{d\le\sqrt{x}+1} \frac{|g(d)|}{d\psi(d)\varphi(d)} \sum_{d'\le\sqrt{x}+1} \frac{|g(d')|}{d'\psi(d')\varphi(d')} \sum_{\substack{p,q\le x\\ p\equiv 1\,(\mathrm{mod}\, d)\\ q\equiv 1\,(\mathrm{mod}\, d')}} \sum_{\substack{\chi_2\neq\chi_0,\,\chi_2'\neq\chi_0'\\ \chi_2^6=\chi_0,\,(\chi_2')^6=\chi_0'}} |\mathcal{B}(\overline{\chi_2\chi_2'})|.
$$

Let $k = [4\log x/\log B] + 1$. By Hölder's inequality, we have

(4.3)
$$\sum_{\substack{p,q\le x\\ p\equiv 1\,(\mathrm{mod}\,d)\\ q\equiv 1\,(\mathrm{mod}\,d')}}\ \sum_{\substack{\chi_2\neq\chi_0,\,\chi_2'\neq\chi_0'\\ \chi_2^6=\chi_0,\,(\chi_2')^6=\chi_0'}} |\mathcal{B}(\overline{\chi_2\chi_2'})| \le \Bigg(\sum_{\substack{p,q\le x\\ p\equiv 1\,(\mathrm{mod}\,d)\\ q\equiv 1\,(\mathrm{mod}\,d')}}\ \sum_{\substack{\chi_2\neq\chi_0,\,\chi_2'\neq\chi_0'\\ \chi_2^6=\chi_0,\,(\chi_2')^6=\chi_0'}} 1\Bigg)^{1-\frac{1}{2k}}$$
$$\times\Bigg(\sum_{\substack{p,q\le x\\ p\equiv 1\,(\mathrm{mod}\,d)\\ q\equiv 1\,(\mathrm{mod}\,d')}}\ \sum_{\substack{\chi_2\neq\chi_0,\,\chi_2'\neq\chi_0'\\ \chi_2^6=\chi_0,\,(\chi_2')^6=\chi_0'}} \Big|\sum_{b\le B}\chi_2\chi_2'(b)\Big|^{2k}\Bigg)^{\frac{1}{2k}}$$
$$\ll (\pi(x;d,1)\pi(x;d',1))^{1-\frac{1}{2k}}\Bigg(\sum_{p,q\le x}\ \sum_{\chi_2\neq\chi_0,\,\chi_2'\neq\chi_0'}\Big|\sum_{b\le B^k}\tau_{k,B}(b)\chi_2\chi_2'(b)\Big|^2\Bigg)^{\frac{1}{2k}},$$

where $\tau_{k,B}(n) := \#\{(a_1,\ldots,a_k)\in[1,B]^k\cap\mathbb{N}^k;\ n=a_1\cdots a_k\}$. By Lemma 2.4, we have

$$\sum_{p,q\le x}\sideset{}{^*}\sum_{\chi\neq\chi_0}\Big|\sum_{b\le B^k}\tau_{k,B}(b)\chi(b)\Big|^2 \ll (x^4+B^k)\sum_{b\le B^k}\tau_{k,B}(b)^2. \tag{4.4}$$

Suppose $k=1$. That is, $B>x^4$. Then

$$\sum_{p,q\le x}\ \sum_{\substack{\chi_2\neq\chi_0\\ \chi_2'\neq\chi_0'}}\Big|\sum_{b\le B^k}\tau_{1,B}(b)\chi_2\chi_2'(b)\Big|^2 \ll B^2.$$

Therefore by employing Lemma 2.8(i) in (4.3), we have

$$\sum_{\substack{p,q\le x\\ p\equiv 1\,(\mathrm{mod}\,d)\\ q\equiv 1\,(\mathrm{mod}\,d')}}\ \sum_{\substack{\chi_2\neq\chi_0,\,\chi_2'\neq\chi_0'\\ \chi_2^6=\chi_0,\,(\chi_2')^6=\chi_0'}} |\mathcal{B}(\overline{\chi_2\chi_2'})| \ll B\frac{x}{\varphi(d)^{1/2}\varphi(d')^{1/2}(\log x)}.$$

Substituting this into (4.2), we obtain

$$\sigma_1 \ll \frac{x}{\log x}\sum_{d\le x}\frac{|g(d)|}{d\psi(d)\varphi(d)^{3/2}}\sum_{d'\le x}\frac{|g(d')|}{d'\psi(d')\varphi(d')^{3/2}} \ll \frac{x}{\log x},$$

as $\beta<3/4$.

Now suppose $k=[4\log x/\log B]+1>1$. Then $B\le x^4$ and $x^4<B^k\le Bx^4\le x^8$. Then, by Lemma 2.5(i), (iii), (4.3), (4.4), and the trivial bounds for $\pi(x;d,1)$ and $\pi(x;d',1)$, we have

$$(4.5)\qquad \sum_{\substack{p\le x\\ p\equiv 1 \,(\mathrm{mod}\, d)\\ q\equiv 1\,(\mathrm{mod}\, d')}} \sum_{\substack{\chi_2\ne\chi_0,\, \chi_2'\ne\chi_0'\\ \chi_2^6=\chi_0,\, (\chi_2')^6=\chi_0'}} |\mathcal{B}(\overline{\chi_2\chi_2'})|$$
$$\ll \left(\frac{x^2}{dd'}\right)^{1-\frac{1}{2k}} \left((x^4+B^k)B^k(\Psi(B,9\log x))^k\right)^{\frac{1}{2k}}$$
$$\ll B\frac{x^2}{(dd')^{3/4}} x^{-1/k}(\Psi(B,9\log x))^{1/2}$$
$$\ll B\frac{x^2}{(dd')^{3/4}} \exp\biggl(-c_3\frac{(\log x)^{1/2}}{\log\log x}\biggr),$$

where $c_3>0$, if $B>\exp(c_1(\log x)^{1/2})$ for sufficiently large c_1. Substituting (4.5) into (4.2), we obtain

$$\sigma_1 \ll x^2\exp\biggl(-c_3\frac{(\log x)^{1/2}}{\log\log x}\biggr)\sum_{d\le x}\frac{|g(d)|}{d^{7/4}\psi(d)\varphi(d)}\sum_{d'\le x}\frac{|g(d')|}{(d')^{7/4}\psi(d')\varphi(d')}$$
$$\ll x^2\exp\biggl(-c_3\frac{(\log x)^{1/2}}{\log\log x}\biggr),$$

as $\beta<3/4$.

By Lemma 2.6(ii), for any $r\in\mathbb{N}$ and $\varepsilon>0$, our second sum σ_2 is

$$\ll \frac{1}{B}\sum_{d,d'\le\sqrt{x}+1}\frac{|g(d)|}{d\psi(d)\varphi(d)}|g(d')| \sum_{\substack{p,q\le x\\ p\equiv 1 \,(\mathrm{mod}\, d)\\ q\equiv 1\,(\mathrm{mod}\, d')}} \frac{1}{q^{1/2}} \sum_{\substack{\chi_2\ne\chi_0,\, \chi_2'\ne\chi_0'\\ \chi_2^6=\chi_0,\, (\chi_2')^6=\chi_0'}} \Bigl|\sum_{b\le B}\chi_2\chi_2'(b)\Bigr|$$
$$\ll_{r,\varepsilon} \frac{1}{B}\sum_{d,d'\le\sqrt{x}+1}\frac{|g(d)|}{d\psi(d)\varphi(d)}|g(d')| \sum_{\substack{p,q\le x\\ p\equiv 1 \,(\mathrm{mod}\, d)\\ q\equiv 1\,(\mathrm{mod}\, d')}} \frac{1}{q^{1/2}} \sum_{\substack{\chi_2\ne\chi_0,\, \chi_2'\ne\chi_0'\\ \chi_2^6=\chi_0,\, (\chi_2')^6=\chi_0'}} B^{1-1/r}(pq)^{\frac{r+1}{4r^2}+\varepsilon}$$
$$\ll \frac{x^{1+\frac{r+1}{4r^2}+\varepsilon}}{B^{1/r}\log x}\sum_{d\le\sqrt{x}+1}\frac{|g(d)|}{d\psi(d)\varphi(d)^2}\sum_{d'\le\sqrt{x}+1}|g(d')|\sum_{\substack{q\le x\\ q\equiv 1\,(\mathrm{mod}\, d')}} q^{\frac{-2r^2+r+1}{4r^2}+\varepsilon}$$
$$\ll \frac{x^{\frac{3}{2}+\frac{r+1}{2r^2}+2\varepsilon}(\log\log x)}{B^{1/r}(\log x)^2}\sum_{d'\le\sqrt{x}+1}\frac{|g(d')|}{d'}$$
$$\ll \frac{1}{B^{1/r}}x^{\frac{3+\beta}{2}+\frac{r+1}{2r^2}+2\varepsilon}(\log x)^{\gamma-1}\log\log x.$$

In the above estimations we employed Lemma 2.8(v) and the fact that $\beta<3/4$.

We obtain a similar bound for σ_3.

Finally, by Lemmas 2.6(ii) and 2.8(v), for any $r \in \mathbb{N}$ and $\varepsilon > 0$, we find that our fourth sum σ_4 is

$$\ll \frac{1}{B} \sum_{d,d' \le \sqrt{x}+1} |g(d)| \cdot |g(d')| \sum_{\substack{p,q \le x \\ p \equiv 1 \, (\mathrm{mod}\, d) \\ q \equiv 1 \, (\mathrm{mod}\, d')}} \frac{1}{p^{1/2}q^{1/2}} \sum_{\substack{\chi_2 \ne \chi_0,\, \chi_2' \ne \chi_0' \\ \chi_2^6 = \chi_0,\, (\chi_2')^6 = \chi_0'}} \Big| \sum_{b \le B} \chi_2 \chi_0'(b) \Big|$$

$$\ll \frac{1}{B^{1/r}} \sum_{d,d' \le \sqrt{x}+1} |g(d)| \cdot |g(d')| \sum_{\substack{p \le x \\ p \equiv 1 \, (\mathrm{mod}\, d)}} \sum_{\substack{q \le x \\ q \equiv 1 \, (\mathrm{mod}\, d')}} (pq)^{\frac{-2r^2+r+1}{4r^2}+\varepsilon}$$

$$\ll \frac{x^{1+\frac{r+1}{2r^2}+2\varepsilon} (\log\log x)^2}{B^{1/r} (\log x)^2} \sum_{d \le \sqrt{x}+1} \frac{|g(d)|}{d} \sum_{d' \le \sqrt{x}+1} \frac{|g(d')|}{d'}$$

$$\ll \frac{1}{B^{1/r}} x^{1+\beta+\frac{r+1}{2r^2}+2\varepsilon} (\log x)^{2\gamma} (\log\log x)^2.$$

Adding the above bounds for σ_1, σ_2, σ_3, σ_4 concludes Subcase 2a.

Subcase 2b: Either both χ_1 and χ_2 are principal or both χ_1' and χ_2' are principal. Without loss of generality we assume that $\chi_1' = \chi_0'$ and $\chi_2' = \chi_0'$. We have

$$\begin{aligned} &\frac{4}{|\mathcal{C}|} \sum_{\substack{p,q \le x \\ p \ne q}} \frac{1}{(p-1)(q-1)} \sum_{\substack{s,t \in \mathbb{F}_p^\times \\ s',t' \in \mathbb{F}_q^\times}} \sum_{\substack{d \mid i_{E_{s,t}}(p) \\ d' \mid i_{E_{s',t'}}(q)}} g(d) g(d') \frac{1}{4(p-1)(q-1)} \\ &\qquad \times \sum_{\substack{\chi_1 \ne \chi_0 \\ \chi_2 \ne \chi_0 \\ \chi_1^4 \chi_2^6 = \chi_0}} \chi_1(s) \chi_2(t) \mathcal{A}(\overline{\chi_1 \chi_0'}) \mathcal{B}(\overline{\chi_2 \chi_0'}) \\ &= \frac{1}{|\mathcal{C}|} \sum_{d \le \sqrt{x}+1} g(d) \sum_{d' \le \sqrt{x}+1} g(d') \sum_{\substack{p,q \le x \\ p \ne q \\ p \equiv 1 \, (\mathrm{mod}\, d) \\ q \equiv 1 \, (\mathrm{mod}\, d')}} \frac{1}{(p-1)^2 (q-1)^2} \\ &\qquad \times \sum_{\substack{\chi_1 \ne \chi_0 \\ \chi_2 \ne \chi_0 \\ \chi_1^4 \chi_2^6 = \chi_0}} \mathcal{A}(\overline{\chi_1 \chi_0'}) \mathcal{B}(\overline{\chi_2 \chi_0'}) \mathcal{W}_{p,q}(\chi_1, \chi_2), \end{aligned} \tag{4.6}$$

where

$$\mathcal{W}_{p,q}(\chi_1, \chi_2) := \sum_{\substack{s,t \in \mathbb{F}_p^\times \\ E_{s,t}(\mathbb{F}_p)[d] \cong (\mathbb{Z}/d\mathbb{Z})^2}} \sum_{\substack{s',t' \in \mathbb{F}_q^\times \\ E_{s',t'}(\mathbb{F}_q)[d'] \cong (\mathbb{Z}/d'\mathbb{Z})^2}} \chi_1(s) \chi_2(t).$$

By applying the Cauchy–Schwarz inequality twice, we obtain

$$\Big| \sum_{\substack{\chi_1\neq\chi_0\\ \chi_2\neq\chi_0\\ \chi_1^4\chi_2^6=\chi_0}} \mathcal{A}(\overline{\chi_1\chi_0'})\mathcal{B}(\overline{\chi_2\chi_0'})\mathcal{W}_{p,q}(\chi_1,\chi_2)\Big|^4$$

$$\leq \Big(\sum_{\substack{\chi_1\neq\chi_0\\ \chi_2\neq\chi_0\\ \chi_1^4\chi_2^6=\chi_0}} |\mathcal{W}_{p,q}(\chi_1,\chi_2)|^2\Big)^2 \Big(\sum_{\substack{\chi_1\neq\chi_0\\ \chi_2\neq\chi_0\\ \chi_1^4\chi_2^6=\chi_0}} |\mathcal{A}(\overline{\chi_1\chi_0'})|^4\Big)\Big(\sum_{\substack{\chi_1\neq\chi_0\\ \chi_2\neq\chi_0\\ \chi_1^4\chi_2^6=\chi_0}} |\mathcal{B}(\overline{\chi_2\chi_0'})|^4\Big).$$

From Lemma 2.7 we deduce

$$\sum_{\substack{\chi_1\neq\chi_0\\ \chi_2\neq\chi_0\\ \chi_1^4\chi_2^6=\chi_0}} |\mathcal{A}(\overline{\chi_1\chi_0'})|^4 \ll A^2pq(\log pq)^6, \qquad \sum_{\substack{\chi_1\neq\chi_0\\ \chi_2\neq\chi_0\\ \chi_1^4\chi_2^6=\chi_0}} |\mathcal{B}(\overline{\chi_2\chi_0'})|^4 \ll B^2pq(\log pq)^6.$$

We have

$$\sum_{\substack{\chi_1\neq\chi_0\\ \chi_2\neq\chi_0\\ \chi_1^4\chi_2^6=\chi_0}} |\mathcal{W}_{p,q}(\chi_1,\chi_2)|^2 \leq \sum_{\chi_1,\chi_2} \mathcal{W}_{p,q}(\chi_1,\chi_2)\overline{\mathcal{W}_{p,q}(\chi_1,\chi_2)}$$

$$= \sum_{\chi_1,\chi_2} \sum_{\substack{s,t\in\mathbb{F}_p^\times,\, s',t'\in\mathbb{F}_q^\times\\ E_{s,t}(\mathbb{F}_p)[d]\cong(\mathbb{Z}/d\mathbb{Z})^2\\ E_{s',t'}(\mathbb{F}_q)[d']\cong(\mathbb{Z}/d'\mathbb{Z})^2}} \chi_1(s)\chi_2(t) \sum_{\substack{u,v\in\mathbb{F}_p^\times,\, u',v'\in\mathbb{F}_q^\times\\ E_{u,v}(\mathbb{F}_p)[d]\cong(\mathbb{Z}/d\mathbb{Z})^2\\ E_{u',v'}(\mathbb{F}_q)[d']\cong(\mathbb{Z}/d'\mathbb{Z})^2}} \overline{\chi_1(u)}\,\overline{\chi_2(v)}$$

$$= \sum_{\substack{s,t\in\mathbb{F}_p^\times,\, s',t'\in\mathbb{F}_q^\times\\ E_{s,t}(\mathbb{F}_p)[d]\cong(\mathbb{Z}/d\mathbb{Z})^2\\ E_{s',t'}(\mathbb{F}_q)[d']\cong(\mathbb{Z}/d'\mathbb{Z})^2}} \sum_{\substack{u,v\in\mathbb{F}_p^\times,\, u',v'\in\mathbb{F}_q^\times\\ E_{u,v}(\mathbb{F}_p)[d]\cong(\mathbb{Z}/d\mathbb{Z})^2\\ E_{u',v'}(\mathbb{F}_q)[d']\cong(\mathbb{Z}/d'\mathbb{Z})^2}} \sum_{\chi_1}\chi_1(s)\overline{\chi_1(u)}\sum_{\chi_2}\chi_2(t)\overline{\chi_2(v)}.$$

Thus,

$$\sum_{\substack{\chi_1\neq\chi_0\\ \chi_2\neq\chi_0\\ \chi_1^4\chi_2^6=\chi_0}} |\mathcal{W}_{p,q}(\chi_1,\chi_2)|^2 \leq \sum_{\substack{s,t\in\mathbb{F}_p^\times,\, s',t',u',v'\in\mathbb{F}_q^\times\\ E_{s,t}(\mathbb{F}_p)[d]\cong(\mathbb{Z}/d\mathbb{Z})^2\\ E_{s',t'}(\mathbb{F}_q)[d']\cong(\mathbb{Z}/d'\mathbb{Z})^2\\ E_{u',v'}(\mathbb{F}_q)[d']\cong(\mathbb{Z}/d'\mathbb{Z})^2}} (p-1)(q-1)$$

$$\ll pq\Big(\frac{p^2}{d\psi(d)\varphi(d)}+p^{3/2}\Big)\Big(\frac{q^4}{(d'\psi(d')\varphi(d'))^2}+q^3\Big)$$

$$\ll \frac{p^3q^5}{d(d')^2\psi(d)\psi(d')^2\varphi(d)\varphi(d')^2}+\frac{p^3q^4}{d\psi(d)\varphi(d)} + \frac{p^{5/2}q^5}{(d'\psi(d')\varphi(d'))^2}+p^{5/2}q^4,$$

which implies

$$\left| \sum_{\substack{\chi_1\neq\chi_0 \\ \chi_2\neq\chi_0 \\ \chi_1^4\chi_2^6=\chi_0}} \mathcal{A}(\overline{\chi_1\chi_0'})\mathcal{B}(\overline{\chi_2\chi_0'})\mathcal{W}_{p,q}(\chi_1,\chi_2) \right| \tag{4.7}$$

$$\ll \sqrt{AB}(\log pq)^3 \frac{p^2q^3}{(d\psi(d)\varphi(d))^{1/2}d'\psi(d')\varphi(d')} + \sqrt{AB}(\log pq)^3 \frac{p^2q^{5/2}}{(d\psi(d)\varphi(d))^{1/2}} + \frac{p^{7/4}q^3}{d'\psi(d')\varphi(d')} + \sqrt{AB}(\log pq)^3 p^{7/4}q^{5/2}.$$

In the above inequalities, we have used the facts that $(a+b+c+d)^2 \ll a^2+b^2+c^2+d^2$ and $(a+b+c+d)^{1/4} \ll a^{1/4}+b^{1/4}+c^{1/4}+d^{1/4}$, where the implied constants are absolute.

Substituting the first term in (4.7) into the original sum in (4.6), we obtain

$$\frac{1}{\sqrt{AB}} \sum_{d\leq\sqrt{x}+1} \frac{|g(d)|}{d^{1/2}\psi(d)^{1/2}\varphi(d)^{1/2}} \sum_{d'\leq\sqrt{x}+1} \frac{|g(d')|}{d'\psi(d')\varphi(d')} \sum_{\substack{p,q\leq x \\ p\equiv 1 \ (\mathrm{mod}\, d) \\ q\equiv 1 \ (\mathrm{mod}\, d')}} q(\log pq)^3 \tag{4.8}$$

$$\ll \frac{1}{\sqrt{AB}} x^3(\log x) \sum_{d\leq\sqrt{x}+1} \frac{|g(d)|}{d^{1/2}\psi(d)^{1/2}\varphi(d)^{3/2}} \sum_{d'\leq\sqrt{x}+1} \frac{|g(d')|}{(d')\psi(d')\varphi(d')^2}$$

$$\ll \frac{1}{\sqrt{AB}} x^3(\log x),$$

as $\beta < 3/4$. Similarly by substituting the second, third, and fourth terms in (4.7) into the original summation in (4.6), we obtain

$$\frac{1}{\sqrt{AB}}\big(x^{(5+\beta)/2}(\log x)^{\gamma+2}(\log\log x) + x^{(11+2\beta)/4}(\log x)^{\gamma+2}(\log\log x)\big) + \frac{x^{(9+4\beta)/4}(\log x)^{2\gamma+3}(\log\log x)^2}{\sqrt{AB}}. \tag{4.9}$$

Adding (4.8) to (4.9) concludes Subcase 2b.

Case 3: Exactly three of χ_1, χ_2, χ_1', χ_2' are principal. Then by following the method of Subcase 2a, we conclude that the sum in question is bounded by the same bound as in that subcase.

Case 4: Exactly one of $\chi_1, \chi_2, \chi_1', \chi_2'$ is principal. Then follow the method of Subcase 2b.

Case 5: All four of $\chi_1, \chi_2, \chi_1', \chi_2'$ are non-principal. Again we follow the method of Subcase 2b. ■

5. Proof of Theorem 1.8. We will evaluate the following sum:

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\sum_{p\le x}\big(f(i_E(p))-c_0(f)\,\mathrm{li}(x)\big)^2=\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\sum_{\substack{p,q\le x\\ p\ne q}} f(i_E(p))f(i_E(q)) \tag{5.1}$$
$$+\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\Big(\sum_{p\le x} f(i_E(p))^2-2c_0(f)\,\mathrm{li}(x)\sum_{p\le x} f(i_E(p))+c_0(f)^2\,\mathrm{li}(x)^2\Big).$$

For the first sum in (5.1) we have

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\sum_{\substack{p,q\le x\\ p\ne q}} f(i_E(p))f(i_E(q)) \tag{5.2}$$
$$=\frac{4}{|\mathcal{C}|}\sum_{\substack{p,q\le x\\ p\ne q}}\frac{1}{(p-1)(q-1)}$$
$$\times\sum_{\substack{s,t\in\mathbb{F}_p^\times\\ s',t'\in\mathbb{F}_q^\times}}\ \sum_{\substack{d\mid i_{E_{s,t}}(p)\\ d'\mid i_{E_{s',t'}}(q)}} g(d)g(d')\sum_{\substack{|a|\le A,\,|b|\le B:\,\exists 1\le u<p,\,1\le u'<q\\ a\equiv su^4\ (\mathrm{mod}\,p),\,a\equiv s'(u')^4\ (\mathrm{mod}\,q)\\ b\equiv tu^6\ (\mathrm{mod}\,p),\,b\equiv t'(u')^6\ (\mathrm{mod}\,q)}} 1$$
$$+\frac{1}{|\mathcal{C}|}\sum_{\substack{p,q\le x\\ p\ne q}}\frac{|\mathrm{Aut}_{\mathbb{F}_p}(E_{s,t})|\cdot|\mathrm{Aut}_{\mathbb{F}_q}(E_{s',t'})|}{(p-1)(q-1)}$$
$$\times\sum_{\substack{s,t\in\mathbb{F}_p\\ st=0\\ s',t'\in\mathbb{F}_q^\times}}\ \sum_{\substack{d\mid i_{E_{s,t}}(p)\\ d'\mid i_{E_{s',t'}}(q)}} g(d)g(d')\sum_{\substack{|a|\le A,\,|b|\le B:\,\exists 1\le u<p,\,1\le u'<q\\ a\equiv su^4\ (\mathrm{mod}\,p),\,a\equiv s'(u')^4\ (\mathrm{mod}\,q)\\ b\equiv tu^6\ (\mathrm{mod}\,p),\,b\equiv t'(u')^6\ (\mathrm{mod}\,q)}} 1$$
$$+\frac{1}{|\mathcal{C}|}\sum_{\substack{p,q\le x\\ p\ne q}}\frac{|\mathrm{Aut}_{\mathbb{F}_p}(E_{s,t})|\cdot|\mathrm{Aut}_{\mathbb{F}_q}(E_{s',t'})|}{(p-1)(q-1)}$$
$$\times\sum_{\substack{s,t\in\mathbb{F}_p^\times\\ s',t'\in\mathbb{F}_q\\ s't'=0}}\ \sum_{\substack{d\mid i_{E_{s,t}}(p)\\ d'\mid i_{E_{s',t'}}(q)}} g(d)g(d')\sum_{\substack{|a|\le A,\,|b|\le B:\,\exists 1\le u<p,\,1\le u'<q\\ a\equiv su^4\ (\mathrm{mod}\,p),\,a\equiv s'(u')^4\ (\mathrm{mod}\,q)\\ b\equiv tu^6\ (\mathrm{mod}\,p),\,b\equiv t'(u')^6\ (\mathrm{mod}\,q)}} 1$$
$$+\frac{1}{|\mathcal{C}|}\sum_{\substack{p,q\le x\\ p\ne q}}\frac{|\mathrm{Aut}_{\mathbb{F}_p}(E_{s,t})|\cdot|\mathrm{Aut}_{\mathbb{F}_q}(E_{s',t'})|}{(p-1)(q-1)}$$
$$\times\sum_{\substack{s,t\in\mathbb{F}_p\\ st=0\\ s',t'\in\mathbb{F}_q\\ s't'=0}}\ \sum_{\substack{d\mid i_{E_{s,t}}(p)\\ d'\mid i_{E_{s',t'}}(q)}} g(d)g(d')\sum_{\substack{|a|\le A,\,|b|\le B:\,\exists 1\le u<p,\,1\le u'<q\\ a\equiv su^4\ (\mathrm{mod}\,p),\,a\equiv s'(u')^4\ (\mathrm{mod}\,q)\\ b\equiv tu^6\ (\mathrm{mod}\,p),\,b\equiv t'(u')^6\ (\mathrm{mod}\,q)}} 1$$
$$=S_1+S_2+S_3+S_4.$$

Let S be the bound in Lemma 4.1 corresponding to a function $g(n)$ satisfying

$$\sum_{n\leq x}|g(n)| \ll x^{1+\beta}(\log x)^{\gamma+1}.$$

We have

$$\begin{aligned}(5.3)\quad S_1 &= O(S)+\frac{4AB}{|\mathcal{C}|}\sum_{\substack{p,q\leq x\\ p\neq q}}\frac{1}{p(p-1)q(q-1)}\sum_{\substack{s,t\in\mathbb{F}_p^\times\\ s',t'\in\mathbb{F}_q^\times}} f(i_{E_{s,t}}(p))f(i_{E_{s',t'}}(q))\\ &= O(S)+\frac{4AB}{|\mathcal{C}|}\bigg(\sum_{p\leq x}\frac{1}{p(p-1)}\sum_{s,t\in\mathbb{F}_p^\times} f(i_{E_{s,t}}(p))\bigg)^2\\ &\quad-\frac{4AB}{|\mathcal{C}|}\sum_{p\leq x}\frac{1}{p^2(p-1)^2}\Big(\sum_{s,t\in\mathbb{F}_p^\times} f(i_{E_{s,t}}(p))\Big)^2.\end{aligned}$$

From the calculation of the Main Term in Section 3.2, we have

$$(5.4)\qquad \sum_{p\leq x}\frac{1}{p(p-1)}\sum_{s,t\in\mathbb{F}_p^\times} f(i_{E_{s,t}}(p)) = c_0(f)\,\mathrm{li}(x)+O\bigg(\frac{x}{(\log x)^{c'}}\bigg)$$

for any $c'>1$. Since $i_{E_{s,t}}(p)\leq\sqrt{p}+1$ and $f(n)\ll n^\beta(\log n)^\gamma$, we see that

$$(5.5)\qquad \sum_{p\leq x}\frac{1}{p^2(p-1)^2}\Big(\sum_{s,t\in\mathbb{F}_p^\times} f(i_{E_{s,t}}(p))\Big)^2 \ll x^{1+\beta}(\log x)^{2\gamma-1}.$$

As $\beta<3/4$, applying (5.3) and (5.4) in (5.5) yields

$$(5.6)\qquad S_1 = c_0(f)^2\,\mathrm{li}(x)^2+O(S)+O\bigg(\frac{x^2}{(\log x)^{2c'}}\bigg)$$

for any $c'>1$.

We will next bound S_2 (and a similar argument will deal with S_3). We have

$$\begin{aligned}(5.7)\quad S_2 &\ll \frac{1}{|\mathcal{C}|}\sum_{\substack{p,q\leq x\\ p\neq q}}\frac{|\mathrm{Aut}_{\mathbb{F}_p}(E_{s,t})|\cdot|\mathrm{Aut}_{\mathbb{F}_q}(E_{s',t'})|}{(p-1)(q-1)}\\ &\quad\times\sum_{\substack{s,t\in\mathbb{F}_p\\ st=0\\ s',t'\in\mathbb{F}_q^\times}}\ \sum_{\substack{d\mid i_{E_{s,t}}(p)\\ d'\mid i_{E_{s',t'}}(q)}}|g(d)|\,|g(d')|\sum_{\substack{|a|\leq A,\,|b|\leq B:\,\exists 1\leq u<p,\,1\leq u'<q\\ a\equiv su^4\ (\mathrm{mod}\,p),\,a\equiv s'(u')^4\ (\mathrm{mod}\,q)\\ b\equiv tu^6\ (\mathrm{mod}\,p),\,b\equiv t'(u')^6\ (\mathrm{mod}\,q)}}1\\ &\ll \frac{1}{|\mathcal{C}|}\sum_{\substack{p,q\leq x\\ p\neq q}}\frac{|\mathrm{Aut}_{\mathbb{F}_p}(E_{s,t})|\cdot|\mathrm{Aut}_{\mathbb{F}_q}(E_{s',t'})|}{(p-1)(q-1)}\\ &\quad\times\sum_{\substack{s,t\in\mathbb{F}_p\\ st=0\\ s',t'\in\mathbb{F}_q^\times}}\ \sum_{\substack{d\mid i_{E_{s,t}}(p)\\ d'\mid i_{E_{s',t'}}(q)}}|g(d)|\,|g(d')|\sum_{\substack{|a|\leq A,\,|b|\leq B:\,\exists 1\leq u'<q\\ a\equiv s'(u')^4\ (\mathrm{mod}\,q)\\ b\equiv t'(u')^6\ (\mathrm{mod}\,q)}}1\end{aligned}$$

$$\ll \Bigg(\sum_{p\le x}\frac{1}{p}\sum_{\substack{s,t\in\mathbb{F}_p\\ st=0}}\sum_{d\mid i_{E_{s,t}}(p)}|g(d)|\Bigg)$$

$$\times\Bigg(\frac{1}{|\mathcal{C}|}\sum_{q\le x}\sum_{s',t'\in\mathbb{F}_q^\times}\frac{|\mathrm{Aut}_{\mathbb{F}_q}(E_{s',t'})|}{q-1}\sum_{d'\mid i_{E_{s',t'}}(q)}|g(d')|\sum_{\substack{|a|\le A,\,|b|\le B:\,\exists 1\le u'<q\\ a\equiv s'(u')^4\ (\mathrm{mod}\, q)\\ b\equiv t'(u')^6\ (\mathrm{mod}\, q)}}1\Bigg).$$

By Lemma 2.3(iv), the first term in the above product is bounded by $x/\log x$. The second term can be bounded by

$$\ll \frac{1}{|\mathcal{C}|}\sum_{q\le x}\frac{1}{q}\sum_{s',t'\in\mathbb{F}_q^\times}\sum_{d'\mid i_{E_{s',t'}}(q)}|g(d')|\Bigg(\sum_{\substack{|a|\le A,\,|b|\le B:\,\exists 1\le u'<q\\ a\equiv s'(u')^4\ (\mathrm{mod}\ )/q\\ b\equiv t'(u')^6\ (\mathrm{mod}\ )/q}}1-\frac{2AB}{q}\Bigg)$$

$$+\frac{1}{|\mathcal{C}|}\sum_{q\le x}\frac{1}{q}\sum_{s',t'\in\mathbb{F}_q^\times}\sum_{d'\mid i_{E_{s',t'}}(q)}|g(d')|\frac{2AB}{q}.$$

Following the computations in Section 3.2, we conclude that

$$\sum_{q\le x}\frac{1}{q}\sum_{s',t'\in\mathbb{F}_q^\times}\sum_{d'\mid i_{E_{s',t'}}(q)}|g(d')|\frac{2AB}{q}\ll AB\frac{x}{\log x}.$$

This together with Lemma 3.1 implies that, under the assumptions of Theorem 1.8, the second term of the product in (5.7) is also bounded by $x/\log x$. Thus,

$$S_2\ll\frac{x^2}{(\log x)^2}. \tag{5.8}$$

For S_4, we have

$$S_4\ll\frac{1}{|\mathcal{C}|}\sum_{\substack{p,q\le x\\ p\ne q}}\frac{1}{pq}\sum_{\substack{s,t\in\mathbb{F}_p\\ st=0\\ s',t'\in\mathbb{F}_q\\ s't'=0}}\sum_{\substack{d\mid i_{E_{s,t}}(p)\\ d'\mid i_{E_{s',t'}}(q)}}|g(d)|\,|g(d')|\sum_{\substack{|a|\le A,\,|b|\le B\\ ab\equiv 0\ (\mathrm{mod}\, p)\\ ab\equiv 0\ (\mathrm{mod}\, q)}}1.$$

Note that

$$\sum_{\substack{|a|\le A,\,|b|\le B\\ ab\equiv 0\ (\mathrm{mod}\, pq)}}1\ll\frac{AB}{pq}+O\bigg(A+B+\frac{B}{q}+\frac{B}{p}+\frac{B}{pq}\bigg)\ll\frac{AB}{pq}+O(A+B).$$

Thus,

$$S_4\ll\frac{1}{|\mathcal{C}|}\sum_{\substack{p,q\le x\\ p\ne q}}\frac{1}{pq}\sum_{\substack{s,t\in\mathbb{F}_p\\ st=0\\ s',t'\in\mathbb{F}_q\\ s't'=0}}\sum_{\substack{d\mid i_{E_{s,t}}(p)\\ d'\mid i_{E_{s',t'}}(q)}}|g(d)|\,|g(d')|\bigg(\frac{AB}{pq}+A+B\bigg). \tag{5.9}$$

The sum in (5.9) corresponding to $AB/(pq)$ can be bounded by

$$\Big(\sum_{d\leq\sqrt{x}+1}|g(d)|\sum_{\substack{p\leq x\\ p\equiv 1\,(\mathrm{mod}\,d)}}\frac{1}{p}\Big)^2\ll(\log\log x)^2(\log x)^2\Big(\sum_{d\leq\sqrt{x}+1}\frac{|g(d)|}{d}\Big)^2$$
$$\ll x^{\beta}(\log\log x)^2(\log x)^{2\gamma+4}.$$

By employing Lemma 2.3(iv), the sum in (5.9) corresponding to $A+B$ can in turn be bounded by

$$\ll\left(\frac{1}{A}+\frac{1}{B}\right)\Big(\sum_{p\leq x}\frac{1}{p}\sum_{\substack{s,t\in\mathbb{F}_p\\ st=0}}\sum_{d\mid i_{E_{s,t}}(p)}|g(d)|\Big)^2\ll\left(\frac{1}{A}+\frac{1}{B}\right)\frac{x^2}{(\log x)^2}.$$

In conclusion we have

$$S_4\ll x^{\beta}(\log\log x)^2(\log x)^{2\gamma+4}+\left(\frac{1}{A}+\frac{1}{B}\right)\frac{x^2}{(\log x)^2}. \tag{5.10}$$

Thus, under the assumptions of Theorem 1.8, by applying (5.6), (5.8), and (5.10) in (5.2), we obtain

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\sum_{\substack{p,q\leq x\\ p\neq q}}f(i_E(p))f(i_E(q))=c_0(f)^2\,\mathrm{li}(x)^2+O(S)+O\left(\frac{x^2}{(\log x)^2}\right). \tag{5.11}$$

Next we bound $\sum_{p\leq x}f(i_E(p))^2$. Let $G:\mathbb{N}\to\mathbb{C}$ be defined by

$$f(n)^2=\sum_{d\mid n}G(d).$$

Then

$$\sum_{n\leq x}|G(n)|\leq\sum_{d\leq x}|f(d)|^2\sum_{\substack{n\leq x\\ d\mid n}}1\leq x\sum_{d\leq x}\frac{|f(d)|^2}{d}\ll x^{1+2\beta}(\log x)^{2\gamma+1}.$$

The proof of Theorem 1.2 for G and f^2 yields

$$\begin{aligned}\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\sum_{p\leq x}f(i_E(p))^2\ll{}&\frac{x}{\log x}+\left(\frac{1}{A}+\frac{1}{B}\right)\left(\frac{x}{\log x}+x^{\frac{1+2\beta}{2}}(\log x)^{2\gamma+3}\right)\\&+\left(\frac{1}{A^{1/r}}+\frac{1}{B^{1/r}}\right)x^{\frac{1+2\beta}{2}+\frac{r+1}{4r^2}}(\log x)^{2\gamma+2}\log\log x\\&+\frac{1}{\sqrt{AB}}\big(x^{3/2}(\log x)^2+x^{1+\beta}(\log x)^{2\gamma+4}(\log\log x)^{5/4}\big)\\&+\frac{1}{\sqrt{AB}}\big(x^{\frac{5+4\beta}{4}}(\log x)^{2\gamma+4}\log\log x\big).\end{aligned}$$

Therefore

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\sum_{p\leq x}f(i_E(p))^2=O(S). \tag{5.12}$$

Now by applying (5.11) and (5.12) to (5.1), we conclude that, under the assumptions of Theorem 1.8, we have

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\Big(\sum_{p\le x} f(i_E(p)) - c_0(f)\,\mathrm{li}(x)\Big)^2 = O(S) + O\bigg(\frac{x^2}{(\log x)^2}\bigg).$$

Since $S = O(x^2/(\log x)^2)$ the result follows.

Acknowledgements. The authors would like to thank Chantal David and Igor Shparlinski for correspondence on an earlier version of this paper. They would also like to thank the referee for thorough reading of the manuscript and providing many helpful comments.

Research of the first author is partially supported by NSERC. Research of the second author is supported by a PIMS postdoctoral fellowship.

References

[1] A. Akbary and D. Ghioca, *A geometric variant of Titchmarsh divisor problem*, Int. J. Number Theory 8 (2012), 53–69.

[2] A. Akbary and V. K. Murty, *Reduction mod p of subgroups of the Mordell–Weil group of an elliptic curve*, Int. J. Number Theory 5 (2009), 465–487.

[3] A. Akbary and V. K. Murty, *An analogue of the Siegel–Walfisz theorem for the cyclicity of CM elliptic curves mod p*, Indian J. Pure Appl. Math. 41 (2010), 25–37.

[4] S. Baier, *The Lang–Trotter conjecture on average*, J. Ramanujan Math. Soc. 22 (2007), 299–314.

[5] S. Baier, *A remark on the Lang–Trotter conjecture*, in: New Directions in Value-Distribution Theory of Zeta and L-functions, Ber. Math., Shaker, Aachen, 2009, 11–18.

[6] A. Balog, A. C. Cojocaru, and C. David, *Average twin prime conjecture for elliptic curves*, Amer. J. Math. 133 (2011), 1179–1229.

[7] W. D. Banks and I. E. Shparlinski, *Sato–Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height*, Israel J. Math. 173 (2009), 253–277.

[8] I. Borosh, C. J. Moreno, and H. Porta, *Elliptic curves over finite fields. II*, Math. Comp. 29 (1975), 951–964.

[9] D. A. Burgess, *On character sums and L-series, II*, Proc. London Math. Soc. (3) 13 (1963), 524–536.

[10] A. C. Cojocaru and M. R. Murty, *Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem*, Math. Ann. 330 (2004), 601–625.

[11] A. C. Cojocaru and M. R. Murty, *An Introduction to Sieve Methods and their Applications*, Cambridge Univ. Press, 2006.

[12] H. Davenport, *Multiplicative Number Theory*, 3rd ed., Springer, 2000.

[13] C. David and F. Pappalardi, *Average Frobenius distribution of elliptic curves*, Int. Math. Res. Notices 1999, no. 4, 165–183.

[14] A. Felix and M. R. Murty, *On the asymptotics for invariants of elliptic curves modulo p*, J. Ramanujan Math. Soc. 28 (2013), 271–298.

[15] É. Fouvry and M. R. Murty, *On the distribution of supersingular primes*, Canad. J. Math. 48 (1996), 81–104.

[16] T. Freiberg and P. Kurlberg, *On the average exponent of elliptic curves modulo p*, Int. Math. Res. Notices 2014, no. 8, 2265–2293.
[17] J. B. Friedlander and H. Iwaniec, *The divisor problem for arithmetic progressions*, Acta Arith. 45 (1985), 273–277.
[18] P. X. Gallagher, *The large sieve*, Mathematika 14 (1967), 14–20.
[19] M. Goldfeld, *Artin's conjecture on average*, Mathematika 15 (1968), 223–226.
[20] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford Univ. Press, 1979.
[21] E. W. Howe, *On the group orders of elliptic curves over finite fields*, Compos. Math. 85 (1993), 229–247.
[22] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer, 1990.
[23] K. James, *Average Frobenius distributions for elliptic curves with 3-torsion*, J. Number Theory 109 (2004), 278–298.
[24] N. Jones, *Averages of elliptic curve constants*, Math. Ann. 345 (2009), 685–710.
[25] N. Koblitz, *Primality of the number of points on an elliptic curve over a finite field*, Pacific J. Math. 131 (1988), 157–165.
[26] E. Kowalski, *Analytic problems for elliptic curves*, J. Ramanujan Math. Soc. 21 (2006), 19–114.
[27] H. W. Lenstra, Jr., P. Stevenhagen, and P. Moree, *Character sums for primitive root densities*, Math. Proc. Cambridge Philos. Soc. 157 (2014), 489–511.
[28] M. R. Murty, *On Artin's conjecture*, J. Number Theory 16 (1983), 147–168.
[29] J.-P. Serre, *Résumé des cours de 1977–1978*, Ann. Collège de France (1978), 67–70.
[30] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 1986.
[31] P. J. Stephens, *An average result for Artin's conjecture*, Mathematika 16 (1969), 178–188.
[32] P. J. Stephens, *Prime divisors of second-order linear recurrences. II*, J. Number Theory 8 (1976), 333–345.
[33] J. Wu, *The average exponent of elliptic curves modulo p*, J. Number Theory 135 (2014), 28–35.

Amir Akbary, Adam Tyler Felix
Department of Mathematics and Computer Science
University of Lethbridge
4401 University Drive
Lethbridge, AB, T1K 3M4, Canada
E-mail: amir.akbary@uleth.ca
adam.felix@uleth.ca

Received on 17.4.2014
and in revised form on 25.11.2014 (7778)