Short average distribution of a prime counting function over families of elliptic curves

Sumit Giri

Abstract

Let $E$ be an elliptic curve defined over $\mathbb{Q}$ and let $N$ be a positive integer. Now, $M_E(N)$ counts the number of primes $p$ such that the group $E_p(\mathbb{F}_p)$ is of order $N$. In an earlier joint work with Balasubramanian, we showed that $M_E(N)$ follows Poisson distribution when an average is taken over a family of elliptic curve with parameters $A$ and $B$ where $A, B \geq N^{\frac{\ell^2}{2}} (\log N)^{1+\gamma}$ and $AB > N^{\frac{3\ell^2}{2}} (\log N)^{2+\gamma}$ for a fixed integer $\ell$ and any $\gamma > 0$. In this paper we show that for sufficiently large $N$, the same result holds even if we take $A$ and $B$ in the range $\exp(N^{\frac{\epsilon^2}{20}}) \geq A, B > N^{\epsilon}$ and $AB > N^{\frac{3\ell^2}{2}} (\log N)^{6+\gamma}$ for any $\epsilon > 0$.

1. Introduction

Let $E$ be an elliptic curve defined over the field of rationals $\mathbb{Q}$ with discriminant $\Delta_E$. For a prime $p$ where $E$ has good reduction, i.e. $p \nmid \Delta_E$, we denote by $E_p$ the reduction of $E$ modulo $p$. Let $\mathbb{F}_p$ be the finite field with $p$ elements and $E_p(\mathbb{F}_p)$ be the group of $\mathbb{F}_p$ points over $E_p$.

For $p \nmid \Delta_E$, we know $|E_p(\mathbb{F}_p)| = p + 1 - a_p(E)$ where $a_p(E)$ is the trace of the Frobenius morphism at $p$. By Hasse’s theorem we know $|a_p(E)| < 2\sqrt{p}$. For a fixed positive integer $N$, we define the following prime counting function

$$M_E(N) := \# \{ p \text{ prime : } E \text{ has good reduction over } p \text{ and } |E_p(\mathbb{F}_p)| = N \}. \quad (1.1)$$

Now, for a pair of integers $(a, b)$, let $E_{a,b}$ be the elliptic curve defined by the Weierstrass equation

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

Also, for $A, B > 0$, we define the family of curves $\mathcal{C}(A, B)$ by

$$\mathcal{C}(A, B) := \{ E_{a,b} : |a| \leq A, |b| \leq B, \Delta(E_{a,b}) \neq 0 \}. \quad (1.2)$$

Now, let us recall Barban-Davenport-Halberstam conjecture for primes in arithmetic progression in short interval.

Conjecture 1. (Barban-Davenport-Halberstam) Let $\theta(x; q, a) = \sum_{\substack{p \leq x, p \equiv a \pmod{q}}} \log p$. Let $0 < \eta \leq 1$ and $\beta > 0$ be real numbers. Suppose that $X$, $Y$, and $Q$ are positive real numbers satisfying $X^\eta \leq Y \leq X$ and $Y/(\log X)^\beta \leq Q \leq Y$. Then

$$\sum_{q \leq Q} \sum_{1 \leq a \leq q \atop (a, q) = 1} |\theta(X + Y; q, a) - \theta(X; q, a) - \frac{Y}{\phi(q)}|^2 \ll_{\eta, \beta} YQ \log X.$$
Under the above conjecture, David and Smith proved that

**Theorem A.** Let Conjecture 1 be true for some $0 < \eta < \frac{1}{2}$. If $A, B \geq \sqrt{N} (\log N)^{1+\gamma} \log \log N$ and that $AB \geq N^\frac{2}{3} (\log N)^{2+\gamma} \log \log N$, then for any odd integer $N$, we have

$$\frac{1}{\#C(A, B)} \sum_{E \in C(A, B)} M_E(N) = \frac{K(N)N}{\phi(N) \log N} + O\left(\frac{1}{(\log N)^{1+\gamma}}\right),$$

with

$$K(N) := \prod_{p \mid N} \left(1 - \frac{(N-1)^2p + 1}{(p-1)^2(p+1)}\right) \prod_{p \mid N} \left(1 - \frac{1}{p^{\nu_p}(N)(p-1)}\right),$$

where $\nu_p$ denotes the usual $p$-adic valuation where $\nu_p(n)$ and $(\frac{n-1}{p})$ is the Kronecker symbol.

Also, by taking another average over $N \leq x$, a similar result was unconditionally proven by Chandee, David, Koukoulopoulos and Smith [CDKS14]. Improving a result of Martin, Pollack and Smith [MPS14], in a work with Balasubramanian [BG14], we showed that the function $K(N)$ is 1 on an average and the average approaches 1 reasonably fast.

Using an approach first used by Banks and Shparlinski [BS09], Balog, Cojocaru and David [BCD11], Akbary and Felix [AF15], in [Par16] Parks proved that the average result in **Theorem A** is true even if we significantly relax the lower bound conditions on $A$ and $B$. To be precise, he proved

**Theorem B.** Let $\epsilon, \gamma > 0$ and assume for intervals of length $N^\eta$ that the Barban- Davenport- Halberstam Conjecture holds for

$$\eta = \frac{1}{2} - (\gamma + 2) \frac{\log \log N}{\log N}.$$

Suppose further that

$$\exp\left(N^{\frac{2}{\alpha}}\right) \gg A, B > N^\epsilon \text{ and } AB \geq N^\frac{3}{2} (\log N)^{2+\gamma} \log \log N.$$

Then, for any odd integer $N$,

$$\frac{1}{C(A, B)} \sum_{E \in C(A, B)} M_E(N) = \frac{K(N)N}{\phi(N) \log N} + O\left(\frac{1}{(\log N)^{1+\gamma}}\right),$$

where $K(N)$ is given in (1.4).

In an earlier work with Balasubramanian [BG15], we proved results related to distribution of the function $M_E(N)$. More precisely, we proved that

**Theorem C.** Let $C(A, B)$ be as defined as in (1.2) and $N$ be a positive integer greater than 7. If $L$ be a positive integer such that $A, B > N^{L/2}(\log N)^{1+\gamma}$ and $AB > N^{3L/2}(\log N)^{2+\gamma}$ for some $\gamma > 0$, then for $1 \leq \ell \leq L - 1$

$$\frac{1}{\#C(A, B)} \sum_{E \in C(A, B), M_E(N) = \ell} 1 = \frac{1}{\ell!} \left(\frac{1}{\#C(A, B)} \sum_{E \in C(A, B)} M_E(N)\right) \ell + O\left(\frac{N}{\phi(N) \log N}\right) + O\left(\frac{1}{N^{1/2}(\log N)^\gamma}\right),$$
where the ‘O’-constant in the last error term is independent of \( \gamma \).

Using an approach similar to Parks [Par15, Par16], in this paper, we improve Theorem \( \mathcal{C} \) as follows:

**Theorem 1.** Let \( 0 < \epsilon < 1 \) be a small positive number and \( \ell \) be a positive integer. Suppose \( \frac{\log N}{\log \log N} \geq \frac{20\epsilon}{\log 2} \) and \( \exp \left( N^\frac{2}{3\epsilon} \right) \gg A, B > N^\epsilon \) and \( AB > N^3 \gamma (\log N)^{6+2\gamma} (\log \log N)^{\frac{1}{2}} \), then

\[
\frac{1}{\mathcal{C}(A, B)} \sum_{E \in \mathcal{C}(A, B)} M_E(N)^\ell \left( 1 + O \left( \frac{N}{\phi(N) \log N} \right) \right) + O \left( \frac{1}{(\log N)^{\ell+\gamma}} \right),
\]

where the ‘O’-constant in the last error term is independent of \( \gamma \).

Alternatively, under Conjecture \( \mathcal{I} \) we can state the above theorem in the following form:

**Theorem 2.** Suppose Conjecture \( \mathcal{I} \) is true for some \( \eta < \frac{1}{2} \). Let \( \gamma_1 \) be a non negative integer and \( \gamma_2 > 0 \). Also let \( \exp \left( N^\frac{2}{20(\ell+\gamma_1)} \right) \gg A, B > N^\epsilon \) and \( AB > N^3 \gamma_1 (\log N)^{6+2\gamma_2} (\log \log N)^{\frac{1}{2}} \) for a odd positive integer \( N \) with \( \frac{\log N}{\log \log N} \geq \frac{20(\ell+\gamma_1)}{\log 2} \). Then, for \( r \leq \ell \)

\[
\frac{1}{\#\mathcal{C}(A, B)} \sum_{E \in \mathcal{C}(A, B)} \sum_{M_E(N) \geq \ell} M_E(N)^r = \sum_{m=\ell}^{\ell+\gamma_1} d_{\ell,r}(m) \left( \frac{K(N)N}{\phi(N) \log N} \right)^m + O \left( \frac{N}{\phi(N) \log N} \right)^{1+\ell+\gamma_1} + O \left( \frac{1}{(\log N)^{\ell+\gamma_2}} \right),
\]

where \( \mathcal{C}(A, B) \) is as before and

\[
d_{\ell,r}(m) = \sum_{k=\ell}^{m} \frac{k^r (-1)^{m-k}}{k! (m-k)!}.
\]  

**Remark:** Although, in [Par16], Theorem \( \mathcal{B} \) is claimed to hold for \( \exp(N^\epsilon) \gg A, B > N^\epsilon \), the correct upper bound for \( A \) and \( B \) should be of the order \( \exp(N^{O(\epsilon^2)}) \).

The crucial difference between proof of Theorem \( \mathcal{I} \) and Theorem \( \mathcal{C} \) is Proposition \( \mathcal{I} \) which is stated in Section 3. In this proposition, we have better estimate of the number of curves of the form \( E_{a,b} : y^2 = x^3 + ax + b \) with \( a, b \in \mathbb{Z} \), which simultaneously reduces modulo a given set of distinct primes \( p_1, p_2, \ldots, p_\ell \) to fixed set of curves of the form \( E_{s_1,t_1}/\mathbb{F}_{p_1}, E_{s_2,t_2}/\mathbb{F}_{p_2}, \ldots, E_{s_\ell,t_\ell}/\mathbb{F}_{p_\ell} \) for \( (s_1, s_2, \ldots, s_\ell), (t_1, t_2, \ldots, t_\ell) \in \mathbb{F}_{p_1}^\times \times \cdots \times \mathbb{F}_{p_\ell}^\times \).

In our previous paper with Balasubramanian [BG15], we estimated number of curves satisfying above conditions using a technique essentially due to Fouvry and Murty [FM96], which involves partitioning a rectangle of size \( A \times B \) into boxes of size \( p_1 p_2 \cdots p_\ell \times p_1 p_2 \cdots p_\ell \) and using Chinese reminder theorem to merge congruence condition over different primes together. While in Proposition \( \mathcal{I} \) we use estimates of sums of suitable multiplicative characters.

**Acknowledgements:** I would like to thank Chantal David, Dimitris Koukoulopoulos and Amir Akbary for their useful advices. I also thank James Parks for spending time in clarifying some of my doubts that were essential for completing the work.

**Funding:** This work was done while working as a Postdoctoral Fellow at Centre de Recherches Mathématiques, Université de Montréal.
2. Preliminaries

Let $D$ be a negative discriminant. Using the class number formula [p. 515, [IK]], the Kronecker class number for a discriminant $D$ can be written as

$$H(D) := \sum_{f^2 \mid D} \frac{\sqrt{|D|}}{2\pi f} L(1, \chi_{D/f^2})$$

(2.1)

where $\chi_d$ is the Kronecker symbol $(d)$ and $L(s, \chi_d) := \sum_{n=1}^{\infty} \frac{\chi_d(n)}{n^s}$.

Using Deuring’s theorem [Deu41] we get

$$H(t^2 - 4p) = \sum_{E \mid \mathbb{F}_p} \# \text{Aut}(E),$$

(2.2)

where the sum is over the $\mathbb{F}_p$-isomorphism classes of elliptic curves.

Define,

$$D_N(p) := (p + 1 - N)^2 - 4p = (N + 1 - p)^2 - 4N,$$

(2.3)

$$N^+ := (\sqrt{N} + 1)^2; \quad N^- := (\sqrt{N} - 1)^2$$

$$d_{N,f}(p) := \frac{D_N(p)}{f^2} \text{ for } f^2 \mid D_N(p).$$

With these notations defined, we recall the following lemma from [Lemma 2.1, [BG15]].

**Lemma 1.** Let $N$ be a positive integers and $N^-$ and $N^+$ are defined as above. Also let $H(D_N(p))$ be defined by (2.1) and (2.3). Then

(a) $$\sum_{N^- < p < N^+} H(D_N(p)) \ll \frac{N^2}{\phi(N) \log N}.$$  

(b) For $k \geq 2$,

$$\sum_{N^- < p < N^+} H(D_N(p))^k \ll N \frac{1}{\log(N)} (\log N)^{k-2} (\log \log N)^k.$$  

We also need the following two theorems:

**Theorem 3.** Let $M, N, Q$ be positive integers and let $\{a_n\} \mod q$ is a sequence of complex numbers. For a fixed $q \leq Q$, we let $\chi$ be a Dirichlet character modulo $q$. Then

$$\sum_{q \leq Q} \frac{\phi(q)}{\chi \mod q} \sum_{\chi \text{ primitive}} \left| \sum_{M < n \leq M+N} a_n \chi(n) \right|^2 \leq (N + 3Q^2) \sum_{M < n \leq M+N} |a_n|^2.$$  

For the proof of the above theorem, see [Chapter 27, [Dav00]].

The second theorem is due to Friedlander and Iwaniec [FI2], which bounds the fourth power moment of Dirichlet characters.
ELLiptic curve short average

Theorem 4. *(Friedlander-Iwaniec)* Let $q$ and $N$ be positive integers. Let $\chi$ denote a Dirichlet character modulo $q$, with $\chi_0$ denoting the principal character. Then

$$\sum_{\chi \neq \chi_0} \left| \sum_{n \leq N} \chi(n) \right|^4 \ll N^2 q \log^6 q.$$ 

3. Proof of Theorems

Let $r \geq 1$ be a positive integer. We have,

$$\frac{1}{\#C(A,B)} \sum_{E \in C(A,B), M_E(N) \geq \ell} M_E(N)^r = \frac{1}{\#C(A,B)} \sum_{E \in C(A,B), M_E(N) \geq \ell} \left( \sum_{N-\ell < p < N+} \ell^{r-1} \right) \left( \sum_{E \in C(A,B), M_E(N) \geq \ell} \right)^r = \frac{1}{\#C(A,B)} \sum_{E \in C(A,B), M_E(N) \geq \ell} \sum_{N-\ell < p < N+} 1.$$

For any non-negative integer $\gamma_1$, breaking the sum into two parts, the right hand side can be written as

$$\frac{1}{\#C(A,B)} \sum_{N-\ell \leq p < N+} \sum_{1 \leq i \leq r} \sum_{E \in C(A,B), \ell \leq M_E(N) \leq \ell + \gamma_1} 1 + \frac{1}{\#C(A,B)} \sum_{E \in C(A,B), 1 \leq i \leq r} \sum_{E \in C(A,B), 1 \leq i \leq r} 1$$

(3.1)

For $r \leq \ell$, consider the expression

$$\frac{1}{\#C(A,B)} \sum_{N-\ell \leq p < N+} \sum_{1 \leq i \leq r} 1$$

(3.2)

Now, for a curve $E$ with $M_E(N) = L \geq \ell + 1$, the curve $E$ is counted $L^r$ times in (3.2). While, the same $E$ is counted $\frac{L^r}{(L-\ell-1)!}$ times if we consider the expression

$$\frac{1}{\#C(A,B)} \sum_{N-\ell \leq p < N+} \sum_{1 \leq i \leq r} 1$$

(3.3)

Using Stirling’s approximation, is easy to see that $\frac{L^r(\ell-\ell-1)!}{L^r} \ll e^\ell$ for $r \leq \ell$. Thus

$$\frac{1}{\#C(A,B)} \sum_{N-\ell \leq p < N+} \sum_{1 \leq i \leq r} 1 \ll \ell, \gamma_1 \frac{1}{\#C(A,B)} \sum_{N-\ell \leq p < N+} \sum_{1 \leq i \leq r} 1$$

(3.4)
For \( r \leq \ell \leq j \leq \ell + \gamma_1 \), using a similar argument, one can also show that
\[
\frac{1}{\#C(A, B)} \sum_{N^- < p_i < N^+ \atop 1 \leq i \leq r} \sum_{M_E(N) = j} \frac{1}{j! \#C(A, B)} \sum_{E \in C(A, B), 1 \leq i \leq r} \sum_{M_E(N) = j} 1
\]  
(3.5)

Also, for \( r \leq \ell \leq j \leq \ell + \gamma_1 \),
\[
\sum_{N^- < p_i < N^+ \atop 1 \leq i \leq r} \sum_{E \in C(A, B), M_E(N) = j} 1 = \frac{1}{(j - r)!} \sum_{N^- < p_i < N^+ \atop 1 \leq i \leq r} \sum_{E \in C(A, B), M_E(N) = j} 1
\]  
(3.6)

We now consider the first term of (3.1). Note that, the primes in the range of summations in (3.1) are not distinct. Recalling the definition of \( S(n, m) \), the Stirling number of the second kind, which equals to the number of ways of partitioning a set of \( n \) elements into \( m \) non empty sets, we get
\[
\sum_{N^- < p_i < N^+ \atop 1 \leq i \leq r} \sum_{E \in C, M_E(N) = j} 1 = \left( \sum_{m=1}^{r} \frac{S(r, m)}{(j - m)!} \right) \sum_{N^- < p_i < N^+ \atop 1 \leq i \leq r} \sum_{E \in C(A, B), M_E(N) = j} 1.
\]  
(3.7)

To simplify the first factor on the right hand side, we use the equality \( \sum_{m=1}^{r} \frac{S(r, m)!}{(j - m)!} = j^r \). See [(4.1.3), p. 60, [Rom84]].

With this,
\[
\sum_{N^- < p_i < N^+ \atop 1 \leq i \leq r} \sum_{E \in \mathbb{C}, M_E(N) = j} 1 = \sum_{N^- < p_i < N^+ \atop 1 \leq i \leq r} \sum_{E \in \mathbb{C}(A, B), M_E(N) = j} 1
\]  
(3.8)

Now we denote the left hand side of (3.6) by \( \omega(r, j) \) and the first term of the right hand side of (3.8) by \( \Omega(j, j) \). Also we call the left hand side of (3.7) by \( \Upsilon(r, j) \). Then, in view of (3.6) and (3.7), we get the following set of relations
\[
\begin{align*}
\Upsilon(r, j) &= \frac{j^r}{r} \omega(j, j), \\
\Omega(t, s) &= \sum_{t \leq s} \omega(t, n) \quad \text{for} \ t \leq s, \\
\omega(t, n) &= \frac{1}{(n-t)!} \omega(n, n) \quad \text{for} \ t \leq n.
\end{align*}
\]  
(3.9)

Now, we state the following Proposition, whose proof will be completed in Section 4.

**Proposition 1.** Let \( C(A, B) \) be as above. Let \( 0 < \epsilon < 1 \) be a small positive number. Suppose \( N \) be a positive integer such that \( \frac{\log N}{\log \log N} \geq \frac{20\ell}{\epsilon} \) with \( \exp \left( \left( \frac{N}{\log N} \right)^{\frac{20\ell}{\epsilon}} \right) \gg A, B > N^\epsilon \) and
Elliptic curve short average

\[ AB > N^{3\frac{1}{2}} (\log N)^{6+2\gamma_2} (\log \log N)^{\frac{\ell}{2}}, \]  then

\[
\frac{1}{\#C(A, B)} \sum_{N^{-\epsilon} < p < N^+ \atop \text{gcd}(p, m) = 1 \text{ or } m \mid n} \sum_{1 \leq i \leq \ell} 1 = \left( \sum_{N^{-\epsilon} < p < N^+} \frac{H(D_N(p))}{p} \right)^\ell + O \left( \frac{1}{(\log N)^{\ell+\gamma_2}} \right).
\]

Now, by Proposition 1

\[
\frac{1}{\#C(A, B)} \Omega(j, j) = \left( \sum_{N^{-\epsilon} < p < N^+} \frac{H(D_N(p))}{p} \right)^j + O \left( \frac{1}{(\log N)^{j+\gamma_2}} \right),
\]

whenever \( \exp \left( \left( \frac{N}{\log N} \right)^{2\gamma_2} \right) \gg A, B > N^\epsilon \) and \( AB > N^{\frac{3}{2}} (\log N)^{6+2\gamma_2} \).

Now, we replace \( \sum_{j=\ell}^{\ell+\gamma_1} \Upsilon(r, j) \) by \( \sum_{j=\ell}^{\ell+\gamma_1} z_{\ell, r}(j) \Omega(j, j) + O(\Omega(\ell + \gamma_1, \ell + \gamma_1 + 1)) \) where \( \{z_{\ell, r}(j)\} \) are some constants to be determined later using (3.9). Also note that \( \Omega(\ell + \gamma_1, \ell + \gamma_1 + 1) \ll AB \left[ \left( \sum_p \frac{H(D_N(p))}{p} \right)^{\ell+\gamma_1} + \frac{1}{(\log N)^{\ell+\gamma_2}} \right] \).

Then, in view of (3.4) and Proposition 1 the expression in (3.1) equals to

\[
\sum_{j=\ell}^{\ell+\gamma_1} z_{\ell, r}(j) \left( \sum_{N^{-\epsilon} < p < N^+} \frac{H(D_N(p))}{p} \right)^j + O \left( \sum_{N^{-\epsilon} < p < N^+} \frac{H(D_N(p))}{p} \right)^{\ell+\gamma_1+1} + O \left( \frac{1}{(\log N)^{\ell+\gamma_2}} \right)
\]

(3.10)

for some real numbers \( \{z_{\ell, r}(j)\}_{j=\ell}^{\ell+\gamma_1} \)

Only thing that remains to be shown is that \( \{z_{\ell, r}(j)\}_j \) are equals to \( \{d_{\ell, r}(j)\}_j \), as defined in (1.5). For that, we have the following lemma.

**Lemma 2.** Consider \( \omega, \Omega \) as variables satisfying the identities in (3.9). Then, the solution of the equation

\[
\sum_{j=\ell}^\infty j^r \frac{\omega(j, j)}{j!} = \sum_{j=\ell}^\infty z_{\ell, r}(j) \Omega(j, j)
\]

in variables \( z_{\ell, r}(j) \) are given by

\[
z_{\ell, r}(j) = \sum_{k=\ell}^{j} \frac{k^r (-1)^{j-k}}{k! (j-k)!} = d_{\ell, r}(j).
\]

**Proof.** See [Lemma 3.2, [BG15]] for the proof of the above lemma. \( \square \)
Finally, combining (3.2), (3.10) and Lemma 2 we have

\[
\frac{1}{\# C(A, B)} \sum_{E \in C(A, B)} M_E(N)^r = \sum_{j=\ell}^{\ell+\gamma_1} \sum_{N^{-}<p<N^{+}} d_{\ell, r}(j) \left( \sum_{N^{-}<p<N^{+}} \frac{H(D_N(p))}{p} \right)^j + O \left( \sum_{N^{-}<p<N^{+}} \frac{H(D_N(p))}{p} \right)^{\ell+\gamma_1+1} + O \left( \frac{1}{(\log N)^{\ell+\gamma_2}} \right) \tag{3.11}
\]

for \( \exp \left( \left( \frac{N}{\log N} \right)^{\frac{20}{\log \epsilon}} \right) \gg A, B > N^\epsilon \) and \( AB > N^{3\frac{\ell+\gamma_1}{2}}(\log N)^{6+\gamma_2} \).

Putting \( \ell = 1, r = 1 \) and \( \gamma_1 = 0, \gamma_2 = \gamma \), from (3.11) we get,

\[
\frac{1}{\# C(A, B)} \sum_{E \in C(A, B)} M_E(N) = \sum_{N^{-}<p<N^{+}} \frac{H(D_N(p))}{p} + O \left( \left( \sum_{N^{-}<p<N^{+}} \frac{H(D_N(p))}{p} \right)^2 \right) + O \left( \frac{1}{(\log N)^{\ell+\gamma}} \right) \tag{3.12}
\]

for \( \exp \left( \left( \frac{N}{\log N} \right)^{\frac{20}{\log \epsilon}} \right) \gg A, B > N^\epsilon \) and \( AB > N^{3\frac{\ell+\gamma_1}{2}}(\log N)^{6+\gamma} \)

Also, for \( \gamma_1 = 0, \gamma_2 = \gamma \), from (3.11) we have

\[
\frac{1}{\# C(A, B)} \sum_{E \in C(A, B) \atop M_E(N) = \ell} M_E(N)^r = d_{\ell, r}(\ell) \left( \sum_{N^{-}<p<N^{+}} \frac{H(D_N(p))}{p} \right)^{\ell} + O \left( \left( \sum_{N^{-}<p<N^{+}} \frac{H(D_N(p))}{p} \right)^{\ell+1} \right) + O \left( \frac{1}{(\log N)^{\ell+\gamma}} \right)
\]
\[
\text{or,}
\]

\[
\frac{1}{\# C(A, B)} \sum_{E \in C(A, B) \atop M_E(N) = \ell} \frac{1}{\ell^r} d_{\ell, r}(\ell) \left( \sum_{N^{-}<p<N^{+}} \frac{H(D_N(p))}{p} \right)^{\ell} + O \left( \left( \sum_{N^{-}<p<N^{+}} \frac{H(D_N(p))}{p} \right)^{\ell+1} \right) + O \left( \frac{1}{(\log N)^{\ell+\gamma}} \right) \tag{3.13}
\]

for \( \exp \left( \left( \frac{N}{\log N} \right)^{\frac{20}{\log \epsilon}} \right) \gg A, B > N^\epsilon \) and \( AB > N^{3\frac{\ell+\gamma_1}{2}}(\log N)^{6+\gamma} \).

We use (3.12) and (3.13) to replace \( \sum_{N^{-}<p<N^{+}} \frac{H(D_N(p))}{p} \) in the right hand side of (3.13) by
Elliptic curve short average

\[
\frac{1}{\#C(A,B)} \sum_{E \in C(A,B)} M_E(N) \text{.} \quad \text{Now, using Lemma 1a, we get}
\]

\[
1 \sum_{E \in C(A,B)} 1 = \frac{d_{\ell, r}(\ell)}{\ell} \left( \frac{1}{\#C(A,B)} \sum_{E \in C(A,B)} M_E(N) \right)^\ell \left( 1 + O \left( \frac{N}{\varphi(N) \log N} \right) \right) + O \left( \frac{1}{(\log N)^{\ell + \gamma}} \right)
\]

for \( \exp \left( \frac{N}{\log N} \right)^{\frac{2}{3\pi}} \gg A, B > N^{\epsilon} \) and \( AB > N \frac{\log N}{\varphi(N) \log N} \). Further, we recall that \( d_{\ell, r}(\ell) = \frac{\ell}{r} \). This proves Theorem 1.

Assuming Conjecture 1 and the proof of [Theorem 3, [DS13]], we have that

\[
\sum_{N^{-\epsilon} < p < N^{\epsilon}} \frac{H(D_N(p))}{p} = K(N) N + O \left( \frac{1}{(\log N)^{1+\gamma}} \right)
\]

for odd integer \( N \), where \( K(N) \) is given by (1.4). Combining (3.14) with (3.11), we complete the proof of Theorem 2.

4. Proof of Proposition 1

Before proceeding with the proof of the proposition, we define some standard notations.

Let \( P := (p_1, \ldots, p_{\ell}) \) be a vector of \( \ell \) distinct primes such that \((\sqrt{N} - 1)^2 < p_i < (\sqrt{N} + 1)^2\) for \( 1 \leq i \leq \ell \). So, the primes in question are effectively of the order \( N \).

Let \( S := (s_1, \ldots, s_{\ell}) \) and \( T := (t_1, \ldots, t_{\ell}) \) be elements of \( \mathbb{F}_{p_1}^* \times \mathbb{F}_{p_2}^* \times \cdots \times \mathbb{F}_{p_{\ell}}^* \). For such \( S \) and \( T \) as above, define the following indicator function

\[
h(P, N, S, T) := \begin{cases} 
1 & \text{if } \#E_{s_i, t_i}(\mathbb{F}_{p_i}) = N \text{ for } 1 \leq i \leq \ell, \\
0 & \text{otherwise.} \end{cases}
\]

Also,

\[
\sum_{S, T \in \mathbb{F}(P)} 1 = \sum_{1 \leq s_1 \leq p_1} \cdots \sum_{1 \leq s_{\ell} \leq p_{\ell}} 1 \quad \text{and} \quad \sum_{S, T \in \mathbb{F}(P)^*} 1 = \sum_{1 \leq s_1 < p_1} \cdots \sum_{1 \leq s_{\ell} < p_{\ell}} 1.
\]

Throughout the rest of the proof, \( E_{s, t} : y^2 = x^3 + sx + t \) denotes a curve over a finite field \( \mathbb{F}_p \). Also \( E_{a, b} \) denotes curve over \( \mathbb{Q} \) as defined in (1.2).

Further, we know, two elliptic curves \( E_{s, t} \) and \( E_{s', t'} \) are isomorphic over \( \mathbb{F}_p \) if and only if there exists a \( u \in \mathbb{F}_p^* \) such that \( s' = su^4 \) and \( t' = tu^6 \). Hence, the number of elliptic curves over \( \mathbb{F}_p \) isomorphic to \( E_{s, t} \) is

\[
\frac{\#\mathbb{F}_p^*}{\#\text{Aut}(E_{s, t})} = \frac{p - 1}{\#\text{Aut}(E_{a, b})}.
\]

Further,

\[
\#\text{Aut}(E_{s, t}) = \begin{cases} 
6 & \text{if } s = 0 \text{ and } p \equiv 1 \pmod{3}, \\
4 & \text{if } t = 0 \text{ and } p \equiv 1 \pmod{4}, \\
2 & \text{otherwise.}
\end{cases}
\]
For $1 \leq i \leq \ell$,
\[
\sum_{1 \leq s_i, t_i \leq p_i} 1 = \sum_{\#E_{p_i, s_i, t_i}(F_{p_i}) = N} \frac{p_i - 1}{\#\text{Aut}(E_{p_i, s_i, t_i}(F_{p_i}))},
\tag{4.2}
\]
where the summation in the right hand side of (4.2) runs over isomorphism classes of elliptic curve $E_{p_i, s_i, t_i}(F_{p_i})$. Further, using (2.2), from (4.2) we get
\[
\sum_{1 \leq s_i, t_i \leq p_i} 1 = (p_i - 1)H(D_N(p_i))
\tag{4.3}
\]
Now, the left hand side of the proposition 1 is equal to
\[
\frac{1}{\#C(A, B)} \sum_{N^{-1} < p_i < N^+} \sum_{E \in C(A, B) \atop \#E_{p_i}(F_{p_i}) = N} 1 \sum_{1 \leq i \leq \ell} h(P, N, S, T) \sum_{|a| \leq A, |b| \leq B \atop a \equiv s_i (mod p_i), \atop b \equiv t_i (mod p_i)} 1 \prod_{j=1}^\ell \frac{\#\text{Aut}(E_{p_j, s_j, t_j})}{(p_j - 1)}.
\tag{4.4}
\]
We plan to count the number of curves $E_{a, b} \in C(A, B)$ whose reductions modulo $p_i$ are $E_{s_i, t_i}$ for all $p_i$. Then, the inner summation on left hand side of (4.4) can be written as
\[
\frac{1}{\#C(A, B)} \sum_{E \in C(A, B) \atop \#E_{p_i}(F_{p_i}) = N} 1 \sum_{S, T \in F(P)} h(P, N, S, T) \prod_{j=1}^\ell \frac{\#\text{Aut}(E_{p_j, s_j, t_j})}{(p_j - 1)} \sum_{|a| \leq A, |b| \leq B \atop \exists (u_1, \ldots, u_\ell) \in F(P)^* \atop a \equiv s_i u_i^4 (mod p_i), \atop b \equiv t_i u_i^6 (mod p_i)} 1
\prod_{j=1}^\ell \frac{\#\text{Aut}(E_{p_j, s_j, t_j})}{(p_j - 1)},
\tag{4.5}
\]
where $Z(P, S, T)$ denotes the number of integers $|a| \leq A, |b| \leq B$ such that $\exists (u_1, \ldots, u_\ell) \in F(P)^*$ such that
\[
a \equiv s_i u_i^4 (mod p_i), \quad b \equiv t_i u_i^6 (mod p_i) \quad \text{for } 1 \leq i \leq \ell.
\]
Now, \( \#\text{Aut}(E_{s,t}) = 2 \) most of the times and in particular when \( st \neq 0 \). So, we write (4.3) as

\[
\frac{2^\ell}{\#\mathcal{C}(A,B)} \sum_{N < p_i < N^+} \sum_{1 \leq i \leq \ell \atop p_m \neq p_n, \forall m \neq n} \frac{1}{p_i(p_i - 1)} h(P,N,S,T)Z(P,S,T) \prod_{j=1}^{\ell} \frac{\#\text{Aut}(E_{p_j,s_j,t_j})}{(p_j - 1)}.
\]

(4.6)

Define

\[
\Sigma_1 := \frac{2^\ell}{\#\mathcal{C}(A,B)} \sum_{N < p_i < N^+} \sum_{1 \leq i \leq \ell \atop p_m \neq p_n, \forall m \neq n} \frac{1}{p_i(p_i - 1)} h(P,N,S,T)Z(P,S,T) \prod_{j=1}^{\ell} \frac{\#\text{Aut}(E_{p_j,s_j,t_j})}{(p_j - 1)}.
\]

(4.7)

\[
\Sigma_2 := \frac{1}{\#\mathcal{C}(A,B)} \sum_{N < p_i < N^+} \sum_{1 \leq i \leq \ell \atop p_m \neq p_n, \forall m \neq n} h(P,N,S,T)Z(P,S,T) \prod_{j=1}^{\ell} \frac{\#\text{Aut}(E_{p_j,s_j,t_j})}{(p_j - 1)}.
\]

(4.8)

We plan to complete the estimation of \( \Sigma_1 \) first. Later, we show that the same estimation technique can be modified suitably to give required upper bound to \( \Sigma_2 \).

For this part of the proof related to the estimation of \( \Sigma_1 \), we are essentially going to follow the approach of Parks [Par15], except possibly the different range of summation over primes.

Separating the expected main term from the expected error term in \( \Sigma_1 \), we write

\[
\Sigma_1 := \frac{4AB}{\#\mathcal{C}(A,B)} \sum_{N < p_i < N^+} \prod_{1 \leq i \leq \ell \atop p_m \neq p_n, \forall m \neq n} \frac{1}{p_j(p_j - 1)} \sum_{S,T \in \mathbb{F}(P)^*} h(P,N,S,T)
\]

\[
+ \frac{2^\ell}{\#\mathcal{C}(A,B)} \sum_{N < p_i < N^+} \prod_{1 \leq i \leq \ell \atop p_m \neq p_n, \forall m \neq n} \frac{1}{(p_j - 1)} \sum_{S,T \in \mathbb{F}(P)^*} h(P,N,S,T) \left( Z(P,S,T) - \frac{AB}{2^\ell p_1 \cdots p_\ell} \right).
\]

(4.9)

In order to bound the second summation on the right hand side of (4.9), we use the following lemma

**Lemma 3.** Let \( \ell, A, B, h(\cdot), Z(\cdot) \) as defined before. Then, as \( N \to \infty \), we have

\[
\sum_{N < p_i < N^+} \frac{1}{p_1 \cdots p_\ell} \sum_{S,T \in \mathbb{F}(P)^*} h(P,N,S,T) \left( Z(P,S,T) - \frac{AB}{2^\ell p_1 \cdots p_\ell} \right)
\]

\[
\ll_k,\ell ABN^{-\frac{2k}{k+1}} (\log N)^{\frac{k^2-1}{2k}} \left( \log A \right)^{\frac{k^2+\ell+1}{2k}} + (\log B)^{\frac{k^2-1}{2k}} \left( \log log N \right)^\ell + \sqrt{ABN^{\frac{2k}{k+1}}} (\log N)^{3-\ell} (\log log N)^\ell,
\]

(4.10)
Using \((4.12)\), the first term in \((4.9)\) can be written as
\[ E \]
for any positive integer \(k\).

We give a proof of the above lemma later in this section.

Now, using \((4.3)\), we write the inner summation in the first sum in \((4.9)\) as
\[
\sum_{S,T \in \mathbb{F}(P)^*} h(P, N, S, T) = \prod_{i=1}^{\ell} \left( \sum_{\substack{p_i-1 \geq \#E_{p_i, s_i, t_i}(F_{p_i}) = N \atop \#E_{p_i, s_i, t_i}(F_{p_i}) = N}} \frac{p_i - 1}{\# \Aut(E_{p_i, s_i, t_i}(F_{p_i})) + O(p_i)} \right)
\]
\[
= \prod_{i=1}^{\ell} \left( (p_i - 1) H(D_N(p_i)) + O(p_i) \right). \tag{4.11}
\]

Using the bound \(L(1, \chi_{dN, f}(p)) \ll \log N\), one can show that \(H(D_N(p_i)) \ll \sqrt{N} \log N \log \log N\) for \(1 \leq i \leq \ell\). This together with \((4.11)\) gives

\[
\sum_{S,T \in \mathbb{F}(P)^*} h(P, N, S, T) = \prod_{i=1}^{\ell} (p_i - 1) H(D_N(p_i)) + O_\ell \left( N^{\frac{3\ell}{4} + \frac{1}{2}} (\log N)^{\ell-1} (\log \log N)^{\ell-1} \right). \tag{4.12}
\]

Using \((4.12)\), the first term in \((4.9)\) can be written as
\[
\frac{4AB}{\#C(A, B)} \sum_{N^- < p_i < N^+} \prod_{1 \leq i < j \leq \ell} \frac{1}{p_j(p_j - 1)} \sum_{S,T \in \mathbb{F}(P)^*} h(P, N, S, T)
\]
\[
= \frac{4AB}{\#C(A, B)} \sum_{N^- < p_i < N^+} \left( \prod_{j=1}^{\ell} \frac{H(D_N(p_j))}{p_j} + O_\ell \left( \frac{1}{N^{2\ell}} \cdot N^{\frac{3\ell}{4} + \frac{1}{2}} (\log N)^{\ell-1} (\log \log N)^{\ell-1} \right) \right)
\]
\[
= \left( \sum_{N^- < p_i < N^+} \prod_{1 \leq i < j \leq \ell} \frac{H(D_N(p_j))}{p_j} + O_\ell \left( \frac{(\log \log N)^{\ell-1}}{\sqrt{N} \log N} \right) \right) \left( 1 + O_\ell \left( \frac{1}{A} + \frac{1}{B} + \frac{1}{AB} \right) \right). \tag{4.13}
\]

Combining \((4.13)\) and Lemma 4, together with Lemma 3, we can write \((4.9)\) as
\[
\Sigma_1 = \left( \sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^\ell + \mathcal{E}_1(N, A, B, \ell)
\]
where
\[
\mathcal{E}_1(N, A, B, \ell) \ll_{\ell,k} N^{-\frac{k}{2}} (\log N)^{\frac{k}{2} + \frac{1}{2}} (\log \log N)^{\ell} \left( (\log A)^{\frac{k}{2} + \frac{1}{2}} + (\log B)^{\frac{k}{2} + \frac{1}{2}} \right) \frac{1}{\sqrt{AB}} N^{\frac{3\ell}{4}} (\log N)^{3-\ell} (\log \log N)^{\frac{3}{2}}
\]
\[+ \left( \frac{1}{\sqrt{B}} + \frac{1}{\sqrt{A}} \right) N^{\frac{1}{4}} (\log \log N)^{\ell} (\log N)^{\frac{3\ell}{2} - 1} + \left( \frac{\log \log N}{\log N} \right)^{\ell} \left( \frac{1}{A} + \frac{1}{B} + \frac{1}{AB} \right) + O_\ell (N^{-\frac{1}{2}}). \tag{4.14}\]
For the time being, we assume that $\Sigma_2$ is significantly small compared to $E_1(N, A, B, \ell)$ under the condition that $A, B \geq N^\varepsilon$.

Choose $k = \frac{2\ell}{\varepsilon}$. Now, if

$$N^\varepsilon \leq A, B \leq \exp\left(\frac{N^{2\ell}}{\pi^2}\right)$$

$$AB \geq N^{\frac{4\ell}{\varepsilon}}(\log N)^{6+2\gamma_2}(\log \log N)^{\frac{\ell}{2}}$$

$$\frac{\log \log N}{\log N} \geq \frac{20\ell}{e^2}$$

one can check that

$$E_1(N, A, B, \ell) \ll O\left(\frac{1}{(\log N)\ell + \gamma_2}\right).$$

Before we proceed with estimating $\Sigma_2$ as defined in (4.8), we give a proof of Lemma 3. Later we are going to use the same proof and the discussions above to give a bound on $\Sigma_2$.

### 4.1 Proof of Lemma 3

Let $\chi_i$ and $\chi'_i$ be Dirichlet characters modulo $p_i$ for $1 \leq i \leq \ell$ and let $\chi_0$ denote the principal character modulo $n$ for any integer $n$. Let

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

For $U := (u_1, \ldots, u_\ell) \in \mathbb{F}_{p_1}^* \times \cdots \times \mathbb{F}_{p_\ell}^* = \mathbb{F}(P)^*$,

$$Z(P, S, T) = \sum_{\substack{|a| \leq A, |b| \leq B \\exists U \in \mathbb{F}(P)^* \\chi_i(s_i u_i^4) \chi'_i(t_i u_i^6) \ (\text{mod } p_i) \\prod_{1 \leq i \leq \ell} (p_i - 1)}} 1$$

$$= \frac{1}{2^\ell} \sum_{|a| \leq A} \sum_{U \in \mathbb{F}(P)^*} \prod_{1 \leq i \leq \ell} \frac{1}{(p_i - 1)^2} \sum_{|b| \leq B} \chi_i(s_i u_i^4) \chi'_i(t_i u_i^6) \sum_{\chi_i (\text{mod } p_i)} \chi_i(s_i u_i^4) \chi'_i(t_i u_i^6) \chi_i(a) \chi'_i(b).$$

By the orthogonality relations of Dirichlet characters, we have

$$\prod_{i=1}^\ell \sum_{U \in \mathbb{F}_{p_i}^*} \chi_i(u_i^4) \chi'_i(u_i^6) = \begin{cases} \prod_{i=1}^\ell (p_i - 1) & \text{if } \chi_i^6(\chi'_i)^6 = \chi_0 \ (\text{mod } p_i) \text{ for } 1 \leq i \leq \ell, \\ 0 & \text{otherwise.} \end{cases}$$

(4.16)

Then combining (4.15) and (4.16), we get
In this case, consequently, and
\[ Z(P, S, T) = \frac{1}{2^\ell} \sum_{\chi_1, \ldots, \chi_\ell \in \chi} \prod_{i=1}^{\ell} \left( \frac{\chi_i(s_i)\chi_i'(t_i)}{p_i - 1} \right) A(\chi_1 \cdots \chi_\ell) B(\chi_1' \cdots \chi_\ell') \]

Then, the LHS of (4.10), can be written as,
\[
\begin{align*}
&= \frac{1}{2^\ell} \left[ \sum_{\chi_i = \chi_i' = \chi_0 \ (\text{mod} \ p_i) \ \text{for} \ 1 \leq i \leq \ell} + \sum_{\chi_i = \chi_i' = \chi_0 \ (\text{mod} \ p_i) \ \text{for} \ 1 \leq i \leq \ell \ \text{and} \ \exists 1 \leq j \leq \ell \ \text{s.t.} \ \chi_j' \neq \chi_0 \ (\text{mod} \ p_j)} + \sum_{\chi_i' = \chi_0 \ (\text{mod} \ p_i) \ \text{for} \ 1 \leq i \leq \ell} + \sum_{\chi_i' = \chi_0 \ (\text{mod} \ p_i) \ \text{for} \ 1 \leq i \leq \ell \ \text{and} \ \exists 1 \leq j \leq \ell \ \text{s.t.} \ \chi_j \neq \chi_0 \ (\text{mod} \ p_j)} \right] \\
&= Z_1(P, S, T) + Z_2(P, S, T) + Z_3(P, S, T) + Z_4(P, S, T) \quad (4.17)
\end{align*}
\]

Then, the LHS of (4.10), can be written as,
\[
\begin{align*}
&\sum_{\frac{N^- - p_1 < N^+}{1 \leq i \leq \ell}} \prod_{i=1}^{\ell} \frac{1}{p_i} \sum_{S, T \in \mathbb{F}(P)^*} h(P, N, S, T) \left( Z(P, S, T) - \frac{AB}{2^{\ell-2} p_1 \cdots p_\ell} \right) \\
&= \sum_{\frac{N^- - p_1 < N^+}{1 \leq i \leq \ell}} \prod_{i=1}^{\ell} \frac{1}{p_i} \sum_{S, T \in \mathbb{F}(P)^*} h(P, N, S, T) \left( \sum_{j=1}^{4} Z_j(P, S, T) - \frac{AB}{2^{\ell-2} p_1 \cdots p_\ell} \right) .
\end{align*}
\]

**Case 1:** \( \chi_i = \chi_i' = \chi_0 \ (\text{mod} \ p_i) \) for \( 1 \leq i \leq \ell \).

In this case,
\[
A(\chi_1 \cdots \chi_\ell) = \sum_{|a| \leq A} \chi_0(a) = \sum_{|a| \leq A, (a, p_1, \ldots, p_\ell) = 1} 1 = 2A \frac{\varphi(p_1 \cdots p_\ell)}{p_1 \cdots p_\ell} + O(\tau(p_1 \cdots p_\ell))
\]

\[
= 2A \left( \frac{(p_1 - 1) \cdots (p_\ell - 1)}{p_1 \cdots p_\ell} \right) + O(1) \quad (4.19)
\]

and
\[
B(\chi_1' \cdots \chi_\ell') = 2B \left( \frac{(p_1 - 1) \cdots (p_\ell - 1)}{p_1 \cdots p_\ell} \right) + O(1) .
\]

Consequently,
\[
Z_1(P, S, T) = \frac{1}{2^\ell} \prod_{j=1}^{\ell} \frac{1}{p_j - 1} \left( \frac{2A(p_1 - 1) \cdots (p_\ell - 1)}{p_1 \cdots p_\ell} + O(1) \left( \frac{2B(p_1 - 1) \cdots (p_\ell - 1)}{p_1 \cdots p_\ell} + O(1) \right) \right) + O(1) \\
= \frac{AB}{2^{\ell-2} p_1 \cdots p_\ell} + O_\ell \left( \frac{AB}{N^{\ell+1}} + \frac{A + B + 1}{N^{\ell}} \right) .
\]

Combining (4.12) with (4.20) and using Lemma 1, we get
\[
\sum_{1 \leq i \leq \ell} \frac{1}{p_i} \sum_{S, T \in \mathbb{F}(P)^*} h(P, S, T) \left( Z_1(P, S, T) - \frac{AB}{2^{\ell-2}p_1 \cdots p_{\ell}} \right) \\
\ll \ell \sum_{N^{-\infty} < p_i < N^+} \frac{1}{p_i} \left( \frac{AB}{N^{\ell+1}} + \frac{A + B + 1}{N^{\ell}} \right) \left( \prod_{j=1}^{\ell} (p_j - 1) H(D_N(p_j)) + N^{\frac{\ell - 1}{2}} (\log N)^{\ell-1} (\log \log N)^{\ell-1} \right) \\
\ll \ell \frac{AB (\log \log N)}{N (\log N)^{\ell}} + \frac{(A + B + 1)}{(\log N)^{\ell}}. \tag{4.21}
\]

Now,

\[
Z_2(P, S, T) = \frac{1}{2^{\ell}} \sum_{\chi_i = (\chi'_i)^{p_i} = \chi_0 \mod p_i} \prod_{i=1}^{\ell} \left( \frac{\chi_i(s_i)\chi'_i(t_i)}{p_i - 1} \right) A(\chi_1 \cdots \chi_\ell) B(\chi'_1 \cdots \chi'_{\ell}) \\
= \frac{1}{2^{\ell}} \sum_{(\chi'_i)^{p_i} = \chi_0 \mod p_i} \prod_{j=1}^{\ell} \frac{\chi'_j(t_j)}{(p_j - 1)} \left( 2A \prod_{i=1}^{\ell} \frac{(p_i - 1)}{p_i} + O(1) \right) B(\chi'_1 \cdots \chi'_{\ell}) \\
\ll \ell \frac{A}{p_1 \cdots p_{\ell}} \sum_{(\chi'_i)^{p_i} = \chi_0 \mod p_i} |B(\chi'_1 \cdots \chi'_{\ell})|. 
\]
Using (4.11) and Hölder's inequality, we get

\[
\sum_{N^{-}<p_i<N^+ \atop \text{pm} \neq p_n, \forall m \neq n} \prod_{i=1}^{\ell} \frac{1}{p_i} \sum_{S, T \in \mathbb{F}(P)^*} h(P, N, S, T)(Z_2(P, S, T))
\]

\[
\ll_{\ell} A \sum_{N^{-}<p_i<N^+ \atop \text{pm} \neq p_n, \forall m \neq n} \prod_{j=1}^{\ell} \frac{H(D_N(p_j))}{p_j} \sum_{(\chi_j^i)^{\ell}=\chi_0 \text{ (mod } p_i)} |B(\chi_1^{\cdot} \cdots \chi_\ell^{\cdot})| \]

\[
\ll_{\ell} A \left( \sum_{N^{-}<p_i<N^+ \atop \text{pm} \neq p_n, \forall m \neq n} \prod_{j=1}^{\ell} \frac{H(D_N(p_j))}{p_j} \right)^{2k} \frac{1}{2k} \]

\[
\times \left( \sum_{N^{-}<p_i<N^+ \atop p_i \neq p_j, \forall i \neq j} (\log p_i)^{\ell}(\log \log p_i)^{\ell} \right)^{2k} \frac{1}{2k} \]

\[
\ll_{\ell} N^{-\ell} (\log N)^{\ell} (\log \log N)^{\ell} \left( \sum_{N^{-}<p_i<N^+ \atop \text{pm} \neq p_n, \forall m \neq n} \sum_{(\chi_j^i)^{\ell}=\chi_0 \text{ (mod } p_i)} |B(\chi_1^{\cdot} \cdots \chi_\ell^{\cdot})|^{2k} \right)^{1/\ell} \]

(4.22)

Now, for a fixed prime \( \ell \)-tuple \((p_1, p_2, \cdots, p_\ell)\), the second product in \([1.22]\), let \( J \subseteq \{1, \ldots, \ell\} \) be the set of positive integers such that \( \chi_j^{\cdot} \neq \chi_0 \) (mod \( p_j\)) for \( j \in J \). Thus,

\[
|B(\chi_1^{\cdot} \cdots \chi_\ell^{\cdot})| = \left| \sum_{|b| \leq B} \chi_j^{\cdot}(b) \cdots \chi_\ell^{\cdot}(b) \right| = \sum_{|b| \leq B} \prod_{j \in J} \chi_j^{\cdot}(b) \prod_{j \notin J} \chi_j^{\cdot}(b) = \left| \sum_{|b| \leq B} \prod_{j \notin J} \chi_j^{\cdot}(b) \right|.
\]

Let \( \tau_k(b; B) \) denote the number of representation of \( b \) as a product of \( k \) positive \( B \) smooth
Elliptic curve short average

integers. Then,

\[ \left| \sum_{b \leq B} \prod_{j \in J} \chi_j(b) \right|^{2k} \ll \ell \left| \sum_{b \leq B^k} \tau_k(b; B) \prod_{j \in J} \chi_j(b) \right|^2. \]

Thus,

\[
\left( \sum_{N^{-1} \leq p_i \leq N^+} \sum_{1 \leq i \leq \ell} \sum_{\chi_i \neq \chi_0 \pmod{p_i}} \left| B \left( \chi_1 \cdots \chi_\ell \right)^{2k} \right| \right)^{\frac{1}{2k}} \ll \ell \left( \sum_{N^{-1} \leq p_i \leq N^+} \sum_{1 \leq i \leq \ell} \sum_{\chi_i \neq \chi_0 \pmod{p_i}} \left| \sum_{b \leq B^k} \tau_k(b; B) \prod_{j \in J} \chi_j(b) \right|^2 \right)^{\frac{1}{2k}}. \quad (4.23)
\]

Now, \( \left( \prod_{j \in J} \chi_j(b) \right) \) is a primitive character modulo \( \prod_{j \in J} p_j \leq N^\ell \). Now we extend the sum in \( (1.23) \) to a sum over all primitive characters modulo \( d \) for all modulus \( d \leq N^\ell \). Using Theorem 3, we get

\[
\left( \sum_{N^{-1} \leq p_i \leq N^+} \sum_{1 \leq i \leq \ell} \sum_{\chi_i \neq \chi_0 \pmod{p_i}} \left| B \left( \chi_1 \cdots \chi_\ell \right)^{2k} \right| \right)^{\frac{1}{2k}} \ll \ell \left( \sum_{\chi \text{ primitive}} \left| \sum_{d \leq N^\ell} \sum_{b \leq B^k} \tau_k(b; \chi(b)) \right|^2 \right)^{\frac{1}{2k}}
\]

\[
\ll \ell \left( \sum_{\chi \text{ primitive}} \left| \sum_{d \leq N^\ell} \left| \sum_{b \leq B^k} \tau_k(b; \chi(b)) \right|^2 \right)^{\frac{1}{2k}}
\]

\[
\ll \ell \left( (B^k + N^{2\ell}) \sum_{b \leq B^k} |\tau_k(b)|^2 \right)^{\frac{1}{2k}}
\]

\[
\ll \ell \left( (B^k + N^{2\ell}) B^k \log^k - 1(B^k) \right)^{\frac{1}{2k}} \quad (4.24)
\]
Combining (4.22) and (4.24), we get

\[
\sum_{N^- < p_i < N^+} \prod_{1 \leq i \leq \ell} \frac{1}{p_i} \sum_{S,T \in \mathbb{F}(P)^*} h(P, N, S, T) Z_2(P, S, T)
\]

\[\ll_{\ell} A \sum_{N^- < p_i < N^+} \prod_{1 \leq i \leq \ell} \frac{1}{p_i} \prod_{j=1}^\ell H(D_N(p_j)) \sum_{\chi_i^j \equiv \chi_0 \pmod{p_i}} |B(\chi_1^j \cdots \chi_{\ell}^j)| \]

\[\ll_{\ell} A \left( (B^k + N^{2\ell}) B^k \log k^2 - 1 (B^k) \right) \frac{1}{k^8} N^{-\frac{1}{18}} (\log N)^{\frac{1}{2}} (\log \log N)^{\ell} \]

\[\ll_{k, \ell} ABN^{-\frac{1}{72}} (\log N)^{\frac{1}{8}} (\log \log N)^{\ell} \log \frac{k^2 - 1}{2k} + A \sqrt{B} \frac{N^{\frac{3}{2k}}}{\mathbb{N}(N)} (\log N)^{\frac{k^2 - 1}{2k}} (\log \log N)^{\ell}. \]

(4.25)

Following almost similar arguments,

\[Z_3(P, S, T) \ll_{\ell} \frac{B}{p_1 \cdots p_\ell} \sum_{\chi_1^j \equiv \chi_0 \pmod{p_i}} |A(\chi_1^j \cdots \chi_{\ell}^j)|.\]

and

\[\sum_{N^- < p_i < N^+} \prod_{1 \leq i \leq \ell} \frac{1}{p_i} \sum_{S,T \in \mathbb{F}(P)^*} h(P, N, S, T) Z_3(P, S, T)
\]

\[\ll_{\ell} A \sum_{N^- < p_i < N^+} \prod_{1 \leq i \leq \ell} \frac{1}{p_i} \prod_{j=1}^\ell H(D_N(p_j)) \sum_{\chi_i^j \equiv \chi_0 \pmod{p_i}} |A(\chi_1^j \cdots \chi_{\ell}^j)| \]

\[\ll_{k, \ell} ABN^{-\frac{1}{72}} (\log N)^{\frac{1}{8}} (\log \log N)^{\ell} \log \frac{k^2 - 1}{2k} + A \sqrt{B} \frac{N^{\frac{3}{2k}}}{\mathbb{N}(N)} (\log N)^{\frac{k^2 - 1}{2k}} (\log \log N)^{\ell}. \]

(4.26)

for a positive real number \( k > \frac{1}{2} \). Hence,

\[\sum_{N^- < p_i < N^+} \prod_{1 \leq i \leq \ell} \frac{1}{p_i} \sum_{S,T \in \mathbb{F}(P)^*} h(P, N, S, T) (Z_2(P, S, T) + Z_3(P, S, T))
\]

\[\ll_{k, \ell} ABN^{-\frac{1}{72}} (\log N)^{\frac{1}{8}} (\log \log N)^{\ell} \log \frac{k^2 - 1}{2k} + (A \sqrt{B} + B \sqrt{A}) \frac{N^{\frac{3}{2k}}}{\mathbb{N}(N)} (\log N)^{\frac{k^2 - 1}{2k}} (\log \log N)^{\ell}. \]

(4.27)

Finally, for \( Z_4(P, S, T) \), define

\[g(P, \chi_i, \chi_i^j) := \sum_{1 \leq s_i, t_i < p_i \atop 1 \leq i \leq \ell} h(P, N, S, T) \chi_i(s_i) \chi_i^j(t_i).\]
Applying Hölder's inequality again, we have
\[
\sum_{N^e < p_i < N^+ \atop 1 \leq i \leq \ell} \frac{1}{p_i} \sum_{S,T \in \mathcal{F}(P)^*} h(P, N, S, T) Z_4(P, S, T) \prod_{1 \leq i \leq \ell} p_j (p_j - 1) \sum_{\chi_i(\chi'_j)^6 = \chi_0 \pmod{p_i}} g(P, \chi_i, \chi'_j) \mathcal{A}(\chi_1 \cdots \chi_\ell) \mathcal{B}(\chi'_1 \cdots \chi'_\ell).
\]
(4.28)

Applying Hölder’s inequality again, we have
\[
\left| \sum_{\chi_i(\chi'_j)^6 = \chi_0 \pmod{p_i}} g(P, \chi_i, \chi'_j) \mathcal{A}(\chi_1 \cdots \chi_\ell) \mathcal{B}(\chi'_1 \cdots \chi'_\ell) \right|^\frac{1}{2} \left( \sum_{\chi_i(\chi'_j)^6 = \chi_0 \pmod{p_i}} |\mathcal{A}(\chi_1 \cdots \chi_\ell)|^4 \right)^{\frac{1}{4}} \times \left( \sum_{\chi_i(\chi'_j)^6 = \chi_0 \pmod{p_i}} |\mathcal{B}(\chi'_1 \cdots \chi'_\ell)|^4 \right)^{\frac{1}{4}}.
\]
(4.29)

Now, extending the sum over all non-principal characters modulo $N^\ell$, from Theorem [4], we have
\[
\sum_{\chi_i(\chi'_j)^6 = \chi_0 \pmod{p_i}} |\mathcal{A}(\chi_1 \cdots \chi_\ell)|^4 \ll_\ell \sum_{\chi \neq \chi_0 \pmod{N^\ell}} \sum_{|a| \leq A} \chi(a)^4 \ll_\ell A^2 N^\ell (\log(N^\ell))^6 \ll_\ell A^2 N^\ell (\log N)^6
\]
(4.30)

Similarly,
\[
\sum_{\chi_i(\chi'_j)^6 = \chi_0 \pmod{p_i}} |\mathcal{B}(\chi'_1 \cdots \chi'_\ell)|^4 \ll_\ell \left( \sum_{\chi \neq \chi_0 \pmod{N^\ell}} \sum_{|b| \leq B} \chi'(b)^4 \right) \ll_\ell B^2 N^\ell (\log(N^\ell))^6 \ll_\ell B^2 N^\ell (\log N)^6
\]
(4.31)
Further, from (4.29), we have
\[
\sum_{\chi_i' \equiv \chi_0 \pmod{p_i} \text{ for } 1 \leq i \leq \ell} \sum_{1 \leq r, s \leq \ell \text{ s.t. } \chi_r \neq \chi_0 \pmod{p_r},} |g(P, \chi_i, \chi_i')|^2 \leq \sum_{\chi_i' \equiv \chi_0 \pmod{p_i} \text{ for } 1 \leq i \leq \ell} |g(P, \chi_i, \chi_i')|^2
\]
\[
\leq \sum_{S, T \in \mathbb{P}(P)^*} \sum_{S', T' \in \mathbb{P}(P)^*} h(P, N, S, T)h(P, N, S', T') \sum_{\chi_i \pmod{p_i}} \chi_i(s_i)\overline{\chi_i(t_i)} \sum_{\chi_i' \pmod{p_i}} \chi_i'(t_i)\overline{\chi_i'(t_i)}
\]
\[
= \prod_{i=1}^{\ell} (p_i - 1)^2 \sum_{S, T \in \mathbb{P}(P)^*} |h(P, N, S, T)|
\]
\[
= \prod_{i=1}^{\ell} (p_i - 1)^2 \sum_{S, T \in \mathbb{P}(P)^*} |h(P, N, S, T)|^2
\]
\[
= N^{3\ell} \prod_{i=1}^{\ell} H(D_N(p_i)) + O_\ell \left(N^{\frac{\ell - 1}{2}} (\log N)^{\ell} (\log \log N)^{\ell}\right),
\]
\[
(4.32)
\]
Combining (4.29), (4.30), (4.31) and (4.32), we have
\[
\left| \sum_{\chi_i' \equiv \chi_0 \pmod{p_i} \text{ for } 1 \leq i \leq \ell} \sum_{1 \leq r, s \leq \ell \text{ s.t. } \chi_r \neq \chi_0 \pmod{p_r},} g(P, \chi_i, \chi_i')A(\chi_1 \cdots \chi_\ell)B(\chi_1' \cdots \chi_\ell') \right|
\]
\[
\ll_\ell \sqrt{ABN^2(\log N)^3} \prod_{i=1}^{\ell} \left(\sum_{N^- < p_i < N^+} \sum_{1 \leq s, t \leq \ell \text{ s.t. } p_{m_i} \neq p_{n_i}, \forall m \neq n} h(P, N, S, T)Z_4(P, S, T) \right)
\]
\[
(4.33)
\]
Thus (4.33) and (4.28) gives
\[
\left| \sum_{N^- < p_i < N^+} \prod_{i=1}^{\ell} \frac{1}{p_i} \sum_{1 \leq s, t \leq \ell \text{ s.t. } p_{m_i} \neq p_{n_i}, \forall m \neq n} h(P, N, S, T)Z_4(P, S, T) \right|
\]
\[
\ll_\ell \sqrt{AB(\log N)^3} \sum_{N^- < p_i < N^+} \prod_{i=1}^{\ell} \sqrt{H(D_N(p_j))}
\]
\[
(4.34)
\]
Using Lemma [1] and Cauchy-Schwarz inequality, we get
\[
\sum_{N^- < p_i < N^+} \prod_{i=1}^{\ell} \sqrt{H(D_N(p_j))} \ll_\ell \left( \sum_{N^- < p_i < N^+} \prod_{i=1}^{\ell} H(D_N(p_i)) \right)^{\frac{1}{2}} \left( \sum_{N^- < p_i < N^+} \prod_{i=1}^{\ell} 1 \right)^{\frac{1}{2}}
\]
\[
\ll_\ell N^{3\ell} (\log N)^{\frac{3\ell}{2}}
\]
\[
(4.35)
\]
In that case, the contribution corresponding to the set \(I\)

\[
\sum_{N^{-1} < p_i < N^+ \atop 1 \leq i \leq \ell} \prod_{p_m \neq p_n, \forall m \neq n} \frac{1}{p_i} \sum_{S,T \in \mathbb{F}(P)} h(P, N, S, T) Z_4(P, S, T) \ll_{\ell} \sqrt{AB} N^\frac{3\ell}{2} (\log N)^{3-\ell} (\log \log N)^\frac{\ell}{2} \tag{4.36}
\]

Finally, combining (4.21), (4.27) and (4.36), we complete the proof of Lemma 3.

4.2 Bound on \(\Sigma_2\):

Next, we plan to modify the previous proof of Lemma 3 to give a upper bound on \(\Sigma_2\).

Recall,

\[
\Sigma_2 = \frac{1}{\#\mathcal{C}(A, B)} \sum_{N^{-1} < p_i < N^+ \atop 1 \leq i \leq \ell} \sum_{S,T \in \mathbb{F}(P)} h(P, N, S, T) Z(P, S, T) \prod_{j=1}^\ell \frac{\# \text{Aut}(E_{p_j s_j t_j})}{p_j - 1} \tag{4.37}
\]

**Case 1:** \(s_i t_i = 0\) for all \(i\).

Then the corresponding rational curves look like \(E_{a,b}\) where \(p_1 p_2 \cdots p_{\ell} \mid a\) or \(p_1 p_2 \cdots p_{\ell} \mid b\).

In that case, the contribution corresponding to \(a b = 0\) is bounded by

\[
\frac{1}{4AB} \sum_{N^{-1} < p_i < N^+ \atop 1 \leq i \leq \ell} \frac{AB}{p_1 p_2 \cdots p_{\ell}} \ll_{\ell} N^{-\frac{\ell}{2}} \tag{4.38}
\]

If, either \(a = 0\) or \(b = 0\), then the curve has complex multiplication. Hence, by Kowalski [Kow06], there are only \(O_{\ell, \ell}(N^{\frac{3\ell}{2}})\) many primes such that \(#E_p(\mathbb{F}_p) = N\). So, the contribution corresponding to \(a b = 0\) is bounded by

\[
O_{\ell, \ell}\left(N^{\frac{3\ell}{2}} \left(\frac{N^{\frac{3\ell}{2}}}{A} + \frac{1}{B}\right)\right) \tag{4.39}
\]

**Case 2:** \(s_{j_1} s_{j_2} \neq 0\) for some \(j_1\) and \(s_{j_2} s_{j_2} = 0\) for some \(j_2\).

The number of possible subsets \(I\) of \(\{1, 2, \cdots \ell\}\) such that \(s_i t_i = 0\) for all \(i \in I\) is bounded by \(O_{\ell}(1)\). Take one such subset \(I\) and without loss of generality, assume that \(#I = e + f\) with

\[
s_1 = s_2 = \cdots = s_e = 0, \quad t_{e+1} = t_{e+2} = \cdots = t_{e+f} = 0, \quad \text{and} \quad s_i t_i \neq 0 \text{ for } e + f + 1 \leq i \leq \ell.
\]

In that case, the contribution corresponding to the set \(I\) in (4.37) is bounded by

\[
\frac{1}{4AB} \left(\sum_{N^{-1} < p_i < N^+ \atop 1 \leq i \leq e+f} \prod_{i=1}^{e+f} \frac{1}{(p_i - 1)}\right) \sum_{N^{-1} < p_i < N^+ \atop e+f+1 \leq i \leq \ell} \prod_{i=e+f+1}^\ell \frac{1}{p_i - 1} \sum_{S,T \in \mathbb{F}(P)} h(\hat{P}, N, \hat{S}, \hat{T}) \hat{Z}(\hat{P}, \hat{S}, \hat{T}) \tag{4.40}
\]

21
where

\[
\hat{P} := (p_{e+f+1}, p_{e+f+2}, \ldots, p_{\ell})
\]
\[
\hat{S} := (s_{e+f+1}, s_{e+f+2}, \ldots, s_{\ell})
\]
\[
\hat{T} := (t_{e+f+1}, t_{e+f+2}, \ldots, t_{\ell})
\]
\[
\hat{h}(\hat{P}, N, \hat{S}, \hat{T}) := \begin{cases} 
1 & \text{if } \#E_{p_i, s_i, t_i}(F_{p_i}) = N \text{ for } e + f + 1 \leq i \leq \ell, \\
0 & \text{otherwise.}
\end{cases}
\]

Then, (4.40) is bounded by

\[
\frac{1}{4AB} \sum_{N^- < p_i < N^+} \prod_{i=1}^{e+f} \frac{1}{p_i - 1} \hat{E}_1(N, A, B, e + f + 1, \ell) = O\left(\frac{\hat{E}_1(N, A, B, e + f + 1, \ell)}{ABN^{\frac{e+f}{2}}}\right) \tag{4.41}
\]

where

\[
\hat{E}_1(N, A, B, e + f + 1, \ell) = \sum_{N^- < p_i < N^+} \prod_{\substack{i = e+f+1 \leq i \leq \ell \\
p_i \neq p_m, \forall m \neq n}} \frac{1}{p_i - 1} \sum_{\hat{S}, \hat{T} \in \mathbb{F}(\hat{P})^*} \hat{h}(\hat{P}, N, \hat{S}, \hat{T}) \hat{Z}(\hat{P}, \hat{S}, \hat{T})
\]
Elliptic curve short average

We proceed with an argument almost similar to the proof of Lemma 3 to estimate

\[ \hat{E}_1(N, A, B, e + f + 1, \ell) = \sum_{N' < p_i < N^+ \atop e + f + 1 \leq \ell \atop p_m \neq p_n, \forall m \neq n} \left( \prod_{i=e+f+1}^{\ell} \frac{1}{p_i - 1} \right) \sum_{\hat{S}, \hat{T} \in \mathbb{F}(P)^*} \hat{h}(\hat{P}, N, \hat{S}, \hat{T}) \hat{Z}(\hat{P}, \hat{S}, \hat{T}) \]

\[ = \sum_{N' < p_i < N^+ \atop e + f + 1 \leq \ell \atop p_m \neq p_n, \forall m \neq n} \left( \prod_{i=e+f+1}^{\ell} \frac{1}{p_i - 1} \right) \sum_{\hat{S}, \hat{T} \in \mathbb{F}(P)^*} \hat{h}(\hat{P}, N, \hat{S}, \hat{T}) \frac{AB/p_1p_2\cdots p_{e+f}}{2^{e-f}2^{p_{e+f}+1}\cdots p_{\ell}} \]

\[ + \sum_{N' < p_i < N^+ \atop e + f + 1 \leq \ell \atop p_m \neq p_n, \forall m \neq n} \left( \prod_{i=e+f+1}^{\ell} \frac{1}{p_i - 1} \right) \sum_{\hat{S}, \hat{T} \in \mathbb{F}(P)^*} \hat{h}(\hat{P}, N, \hat{S}, \hat{T}) \left( \hat{Z}(\hat{P}, \hat{S}, \hat{T}) - \frac{AB/p_1p_2\cdots p_{e+f}}{2^{e-f}2^{p_{e+f}+1}\cdots p_{\ell}} \right) \]

(4.42)

Define \( \hat{A}(\chi_{e+f+1}\cdots \chi_{\ell}) \) and \( \hat{B}(\chi'_{e+f+1}\cdots \chi'_{\ell}) \), by

\[ \hat{A}(\chi_{e+f+1}\cdots \chi_{\ell}) = \sum_{|a| \leq A/p_1\cdots p_{e}} \chi_{e+f+1}\cdots \chi_{\ell}(p_1, p_2, \cdots p_{e}a) \]

\[ = \chi_{e+f+1}\cdots \chi_{\ell}(p_1, \cdots p_{e}) \sum_{|a| \leq A/p_1\cdots p_{e}} \chi_{e+f+1}\cdots \chi_{\ell}(a) \]

\[ \hat{B}(\chi'_{e+f+1}\cdots \chi'_{\ell}) = \sum_{|b| \leq B/p_{e+1}\cdots p_{e+f}} \chi'_{e+f+1}\cdots \chi'_{\ell}(p_{e+1}, \cdots p_{e+f}b) \]

\[ = \chi'_{e+f+1}\cdots \chi'_{\ell}(p_{e+1}, \cdots p_{e+f}) \sum_{|b| \leq B/p_{e+1}\cdots p_{e+f}} \chi'_{e+f+1}\cdots \chi'_{\ell}(b) \]

First of all, using (4.11), note that the first summation on the right hand side of (4.42) is bounded by

\[ O_\ell \left( ABN^{-e-f} \left( \sum_{N' < p < N^+} \frac{H(D_N(p))}{p} \right)^{\ell-e-f} \right) = O_\ell \left( \frac{AB}{N^{e+f}} \left( \frac{\log \log N}{\log N} \right)^{\ell-e-f} \right) \]

Again, we write \( \hat{Z}(\hat{P}, \hat{S}, \hat{T}) \) as

\[ \hat{Z}(\hat{P}, \hat{S}, \hat{T}) = \sum_{j=1}^{4} \hat{Z}_j(\hat{P}, \hat{S}, \hat{T}) \]

23
where

\[
\tilde{Z}_1(\hat{P}, \hat{S}, \hat{T}) = \frac{1}{2^e} \sum_{\substack{\chi_i = \chi'_i = \chi_0 \mod (p_i) \\
\text{for } 1 \leq i \leq \ell}} \prod_{i = e + f + 1}^{\ell} \left( \frac{\chi_i(s_i)\chi'_i(t_i)}{p_i - 1} \right) \hat{A}(x_{e+f+1} \cdots x_{\ell}) \hat{B}(x'_{e+f+1} \cdots x'_{\ell})
\]

\[
\tilde{Z}_2(\hat{P}, \hat{S}, \hat{T}) = \frac{1}{2^e} \sum_{\substack{\chi_i = \chi'_i = \chi_0 \mod (p_i) \\
\text{for } 1 \leq i \leq \ell \text{ and } \\
\exists 1 \leq j \leq \ell \text{ s.t. } \chi'_j \neq \chi_0 \mod (p_j)}} \prod_{i = e + f + 1}^{\ell} \left( \frac{\chi_i(s_i)\chi'_i(t_i)}{p_i - 1} \right) \hat{A}(x_{e+f+1} \cdots x_{\ell}) \hat{B}(x'_{e+f+1} \cdots x'_{\ell})
\]

\[
\tilde{Z}_3(\hat{P}, \hat{S}, \hat{T}) = \frac{1}{2^e} \sum_{\substack{\chi'_i = \chi_0 \mod (p_i) \\
\text{for } 1 \leq i \leq \ell \text{ and } \\
\exists 1 \leq j \leq \ell \text{ s.t. } \chi'_j \neq \chi_0 \mod (p_j), \\
\chi'_s \neq \chi_0 \mod (p_s)}} \prod_{i = e + f + 1}^{\ell} \left( \frac{\chi_i(s_i)\chi'_i(t_i)}{p_i - 1} \right) \hat{A}(x_{e+f+1} \cdots x_{\ell}) \hat{B}(x'_{e+f+1} \cdots x'_{\ell})
\]

\[
\tilde{Z}_4(\hat{P}, \hat{S}, \hat{T}) = \frac{1}{2^e} \sum_{\substack{\chi'_i = \chi_0 \mod (p_i) \\
\text{for } 1 \leq i \leq \ell \text{ and } \\
\exists 1 \leq r, s \leq \ell \text{ s.t. } \chi'_r \neq \chi_0 \mod (p_r), \\
\chi'_s \neq \chi_0 \mod (p_s), \\
\chi'_r \neq \chi_0 \mod (p_s)}} \prod_{i = e + f + 1}^{\ell} \left( \frac{\chi_i(s_i)\chi'_i(t_i)}{p_i - 1} \right) \hat{A}(x_{e+f+1} \cdots x_{\ell}) \hat{B}(x'_{e+f+1} \cdots x'_{\ell})
\]

Now, let us denote \( \hat{A} = \frac{A}{p_{e+1} \cdots p_e} \) and \( \hat{B} = \frac{B}{p_{e+1} \cdots p_{e+f}} \).

Then, following the same argument as the one we used to prove \((4.21)\), we should get

\[
\sum_{N^{-c} < p_i < N^{+c}} \left( \prod_{i = e + f + 1}^{\ell} \frac{1}{p_i - 1} \right) \sum_{\hat{S}, T \in \mathcal{F}(\hat{P})} \hat{h}(\hat{P}, N, \hat{S}, \hat{T}) \left( \hat{Z}_1(\hat{P}, \hat{S}, \hat{T}) - \frac{AB/p_{1}p_{2} \cdots p_{e+f}}{2^{e+f-2}p_{e+f+1} \cdots p_{\ell}} \right) \ll_{\ell} \frac{\hat{A}\hat{B}(\log \log N)}{N^{(e+f-1)}} + \frac{(\hat{A} + \hat{B} + 1)}{(\log N)^{e+f-2}} \quad (4.43)
\]

Since, the primes \( p_i \)'s are distinct, we also have

\[
\left| \chi_{m+n+1} \cdots \chi_{\ell}(p_1, \ldots p_m) \right| = 1 \\
\left| \chi_{m+n+1} \cdots \chi_{\ell}(p_{m+1}, \ldots p_{m+n}) \right| = 1, \quad (4.44)
\]

Hence,

\[
\tilde{Z}_2(\hat{P}, \hat{S}, \hat{T}) \ll_{\ell} \frac{\hat{A}}{p_{e+f+1} \cdots p_{\ell}} \sum_{\substack{\chi'_i = \chi_0 \mod (p_i) \\
\text{for } e+f+1 \leq i \leq \ell \text{ and } \\
\exists e+f+1 \leq j \leq \ell \text{ s.t. } \chi'_j \neq \chi_0 \mod (p_j)}} \left| \hat{B}(x'_{e+f+1} \cdots x'_{\ell}) \right|
\]

\[
\ll_{\ell} \frac{A}{N^{\ell}} \sum_{\substack{\chi'_i = \chi_0 \mod (p_i) \\
\text{for } e+f+1 \leq i \leq \ell \text{ and } \\
\exists e+f+1 \leq j \leq \ell \text{ s.t. } \chi'_j \neq \chi_0 \mod (p_j)}} \left| B(x'_{e+f+1} \cdots x'_{\ell}(b)) \right|
\]

24
and
\[ \hat{Z}_3(\hat{P}, \hat{S}, \hat{T}) \ll_{\ell} \frac{B}{N^\ell} \sum_{\chi_i^4 = \chi_0 \mod p_i} \sum_{\chi_{e+f+1} \cdots \chi_{\ell}} |\sum a|_{p_1 \cdots p_\ell} \chi_{e+f+1} \cdot \cdots \chi(\ell)(a)| \]

Replacing \( A, B \) and \( \ell \) by \( \hat{A}, \hat{B} \) and \( \ell - e - f \) respectively in the proof of (4.27), we get the following inequality
\[
\sum_{N^e < p_i < N^{e+f+1}} \left( \prod_{i=e+f+1}^{\ell} \frac{1}{p_i - 1} \right) \sum_{\hat{S}, T \in \mathbb{F}(\hat{P})^*} \hat{h}(\hat{P}, N, \hat{S}, \hat{T}) \left( \hat{Z}_2(\hat{P}, \hat{S}, \hat{T}) + \hat{Z}_3(\hat{P}, \hat{S}, \hat{T}) \right) 
\]
\[ \ll_{k, \ell} \hat{A}\hat{B}N^{-\frac{e-f}{4k}}(\log N)^{\frac{\ell-e-f}{2k}}(\log \log N)^{\ell-e-f}(\log \frac{k^2+1}{2\hat{A}} + \log \frac{k^2+1}{2\hat{B}}) 
\]
\[ + (\hat{A}\sqrt{\hat{B}} + \hat{B}\sqrt{\hat{A}})N^\frac{3(\ell-e-f)}{4k}(\log N)^{\frac{k^2+e-f}{2k}}(\log \log N)^{\ell-e-f} \tag{4.45} \]

for some \( k > \frac{1}{2} \).

Again, using (4.44) and replacing \( A, B \) and \( \ell \) by \( \hat{A}, \hat{B} \) and \( \ell - e - f \) respectively in the proof of (4.36), we get
\[
\sum_{N^e < p_i < N^{e+f+1}} \left( \prod_{i=e+f+1}^{\ell} \frac{1}{p_i - 1} \right) \sum_{\hat{S}, T \in \mathbb{F}(\hat{P})^*} \hat{h}(\hat{P}, N, \hat{S}, \hat{T}) \hat{Z}_4(\hat{P}, \hat{S}, \hat{T}) 
\]
\[ \ll \sqrt{\hat{A}\hat{B}}N^{\frac{3(\ell-e-f)}{4k}}(\log N)^{3-(\ell-e-f)}(\log \log N)^{\frac{\ell-e-f}{2}} \tag{4.46} \]

Since \( e + f \geq 1 \), observe that we get a savings of a factor of \( \frac{1}{\sqrt{N}} \) in (4.43), (4.45) and (4.46) compared to the upper bounds for corresponding expressions in the proof of Lemma 3. Also, in view of (4.39), we need to assume \( A, B \geq N^e \) to make the corresponding error term sufficiently small in Proposition I.

As a conclusion, it is safe to claim that \( \Sigma_2 \) is small enough compared to the the error term in Proposition I. This completes the proof of Proposition I. \( \square \)

References

AF15 A. Akbary and A. T. Felix, On invariants of elliptic curves on average. Acta Arith. 168 (2015), no. 1, 31-70.

BG14 R. Balasubramanian and S. Giri, The mean-value of a product of shifted multiplicative functions and the average number of points of elliptic curves. J. Number Theory 157 (2015), 37-53.

BG15 R. Balasubramanian and S. Giri, Poisson Distribution of a Prime Counting Function Corresponding to Elliptic Curves, to appear in Internat. Math. Res. Notices. arXiv:1503.01018 [math.NT].

BCD11 A. Balog, A.-C. Cojocaru and C. David, Average twin prime conjecture for elliptic curves, Amer. J. Math. 133 (2011), no. 5, 1179-1229.

BS09 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.
CDKS14 V. Chandee, C. David, D. Koukoulopoulos and E. Smith, The Frequency of Elliptic Curve Groups Over Prime Finite Fields. Canad. J. Math. 68 (2016), no. 4, 721-761.

Dav00 H. Davenport, Multiplicative number theory. Third edition. Revised and with a preface by Hugh L. Montgomery. Graduate Texts in Mathematics, 74. Springer-Verlag, New York, 2000.

DS13 C. David and E. Smith, Elliptic curves with a given number of points over finite fields, Compositio Math. 149 (2013), 175203.

DS14 C. David and E. Smith, Corrigendum to Elliptic curves with a given number of points over finite fields, Compositio Math. 150 (2014), no. 8, 13471348.

Deu41 M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Univ. Hamburg, 14 (1941), no. 1, 197-272.

FM96 E. Fouvry and M. R. Murty, On the distribution of supersingular primes, Canad. J. Math. 48 (1996), 81104.

FI2 J. Friedlander and H. Iwaniec, The divisor problem for arithmetic progressions. Acta Arith. 45 (1985), 273-277.

IK H. Iwaniec and E. Kowalski, Analytic number theory, colloquium publications, vol. 53, American Mathematical Society.

Kow06 E. Kowalski, Analytic problems for elliptic curves, J. Ramanujan Math. Soc. 21 (2006), 19114.

MPS14 G. Martin, P. Pollack and E. Smith, Averages of the number of points on elliptic curves. Algebra Number Theory 8 (2014), no. 4, 813836.

Par15 J. Parks, Amicable pairs and aliquot cycles on average. Int. J. Number Theory 11 (2015), no. 6, 1751-1790.

Par16 J. Parks, A remark on elliptic curves with a given number of points over finite fields. SCHOLARa scientific celebration highlighting open lines of arithmetic research, 165-179, Contemp. Math., 655, Amer. Math. Soc., Providence, RI, 2015.

Rom84 S. Roman, The Umbral Calculus. New York: Academic Press, pp. 59-63, 1984.

Sumit Giri sumit.giri199@gmail.com
School of Mathematics, Tel Aviv University, P.O.B. 39040, Ramat Aviv, Tel Aviv 69978, Israel.