PAIR CORRELATION OF TORSION POINTS ON ELLIPTIC CURVES

EMRE ALKAN, MAOSHENG XIONG, AND ALEXANDRU ZAHARESCU

ABSTRACT. We prove the existence of the pair correlation measure associated to torsion points on the real locus $E(\mathbb{R})$ of an elliptic curve E and provide an explicit formula for the limiting pair correlation function.

1. INTRODUCTION

The statistics of local spacings shed light on the structure of sequences improving on the classical uniform distribution result of Weyl [12]. Their study was proposed first by physicists (see Wigner [13] and Dyson [4], [5], [6]) in order to approach the problem concerning the spectra of high energies. Recently the authors [1] studied the local spacings problem for a sequence of points on piecewise smooth curves in the plane (see also [14]). We investigated how the spacing distribution function deforms via smooth maps between curves. In this way we provided explicit formulas for the nearest neighbor spacing distribution function of torsion points on elliptic curves over \mathbb{R} . Surprisingly it turns out that the nearest neighbor spacing distribution function detects a strong repulsion between torsion points of E. The reason behind this repulsion phenomenon comes from the fact that the distribution of torsion points coincides locally with the distribution of Farey fractions. In this sequel paper we complement the results of [1] by obtaining the pair

²⁰⁰⁰ Mathematics Subject Classification. 11K06, 11L07.

Key words and phrases. Pair correlation, Elliptic curves, torsion points.

First author is supported in part by TUBITAK Career Award and Distinguished Young Scholar Award, TUBA-GEBIP of Turkish Academy of Sciences. Third author is supported in part by National Science Foundation Grant DMS-0456615.

correlation function of torsion points on an elliptic curve E defined over \mathbb{R} . We should remark that, due to the fundamental properties of Farey fractions, the pair correlation problem of Farey fractions is more subtle than the distribution of spacings between Farey fractions. The pair correlation problem for Farey fractions was settled recently by Boca and one of the authors [3]. To study the pair correlation of torsion points, we need to improve on the techniques of [3] and first obtain the pair correlation of Farey fractions in short intervals. This is crucial for the transfer of the desired type of information from Farey fractions to torsion points along a given elliptic curve.

More specifically, let us fix an elliptic curve E defined over the real numbers, take an arc \mathcal{J} on the real locus $E(\mathbb{R})$ of E, and for each large positive integer Q, consider the pair correlation measure of the set $\mathscr{M}_{E,\mathcal{J},Q}$ of torsion points on $E(\mathbb{R})$ of order $\leq Q$ which lie in \mathcal{J} . Here the distance between elements of $\mathscr{M}_{E,\mathcal{J},Q}$, which is used in the definition of the pair correlation measure, is defined as the arclength along the curve, and we are interested to see whether for any E and \mathcal{J} as above, one has a limiting pair correlation measure as $Q \to \infty$. Our main result shows the existence of the limiting pair correlation measure associated to $\mathscr{M}_{E,\mathcal{J},Q}$, as $Q \to \infty$. We work with finite arcs \mathcal{J} contained in the unbounded component $E_U(\mathbb{R})$ of the real locus $E(\mathbb{R})$ of E.

Theorem 1. (i) For any elliptic curve E defined over \mathbb{R} and any finite arc $\mathcal{J} \subset E_U(\mathbb{R})$, the pair correlation measures associated to the sets $(\mathscr{M}_{E,\mathcal{J},Q})_{Q\in\mathbb{N}}$ of torsion points on \mathcal{J} of order $\leq Q$ converge weakly, as $Q \to \infty$, to a measure $\mu_{E,\mathcal{J}}$ which is absolutely continuous with respect to the Lebesgue measure.

(ii) For any E and \mathcal{J} as above, denote by $g_{E,\mathcal{J}}$ the density of the measure $\mu_{E,\mathcal{J}}$. Then for any point $P \in E_U(\mathbb{R})$, and any sequence $(\mathcal{J}_n)_{n\in\mathbb{N}}$ of arcs on $E_U(\mathbb{R})$ containing P with $\lim_{n\to\infty} length(\mathcal{J}_n) = 0$, the sequence of functions $(g_{E,\mathcal{J}_n})_{n\in\mathbb{N}}$ converges to a function $g_{E,P}$. Moreover, the function $g_{E,P}$ is independent of P and E, and is given by

$$g_{E,P}(\lambda) = \frac{6}{\pi^2 \lambda^2} \sum_{1 \le k \le \frac{\pi^2 \lambda}{3}} \varphi(k) \log \frac{\pi^2 \lambda}{3k},$$

for any $\lambda > 0$, where φ is Euler's totient function.

To establish Theorem 1, we make use of the Weierstrass parametrization in order to move the problem from the elliptic curve to \mathbb{R}/\mathbb{Z} . The pair correlation measure of torsion points on \mathbb{R}/\mathbb{Z} of order $\leq Q$ was proved convergent as $Q \to \infty$, and the corresponding limiting pair correlation function was explicitly computed by Boca and one of the authors in [3]. Here we need to provide a local version of this result, and then analyze how the limiting pair correlation measure is deformed via the Weierstrass parametrization when one moves the problem back to the elliptic curve. A precise description of the corresponding limiting pair correlation function $g_{E,\mathcal{J}}$ is given in equation (4) from Section 3 below.

2. PAIR CORRELATION ON CURVES

As mentioned in the Introduction, we begin by moving the problem, via the Weierstrass parametrization, from the real locus of the elliptic curve to the real line. For this purpose, we have to study how pair correlations are deformed by a general parametrization. First we set some notation and terminology. Let \mathcal{C} be a connected, piecewise smooth, compact curve in \mathbb{R}^k and let $\mathcal{M} = \{x_n \in \mathcal{C} : 1 \leq n \leq N\}$ be a finite sequence of points on \mathcal{C} . Let \mathcal{J} be a connected subarc of \mathcal{C} with length $l(\mathcal{J})$. Denote by $\mathcal{M}(\mathcal{J}) = \{1 \leq j \leq N : x_j \in \mathcal{J}\}$ and for $x, y \in \mathcal{C}$, denote by $l(\widetilde{xy})$ the length of the subarc \widetilde{xy} on the curve \mathcal{C} . Then define the pair correlation measure $R^{(2)}_{\mathcal{J},\mathcal{M}}$ by letting

$$R^{(2)}_{\mathcal{J},\mathcal{M}}(\mathbf{I}) = \frac{1}{2\#\mathcal{M}(\mathcal{J})} \# \left\{ (x,y) \in \mathcal{M}(\mathcal{J})^2 : \begin{array}{c} x \neq y, \\ \frac{\#\mathcal{U}(\mathcal{J})}{l(\mathcal{J})} l(\widetilde{xy}) \in \mathbf{I} \end{array} \right\} \,,$$

for any interval $\mathbf{I} \subset [0, \infty)$. Here the factor 2 appears in the denominator because each pair (x, y) is counted twice. Let us denote for any $\lambda > 0$,

$$G_{\mathcal{J},\mathcal{M}}(\lambda) = R^{(2)}_{\mathcal{J},\mathcal{M}}([0,\lambda]).$$

Suppose that $\mathscr{M} = (\mathscr{M}_Q)_{Q \in \mathbb{N}}$ is an increasing sequence of finite sequences of points of \mathcal{C} . If the sequence of pair correlation measures $\left(R^{(2)}_{\mathcal{J},\mathscr{M}_Q}\right)_{Q \in \mathbb{N}}$ converges weakly, we denote the limiting measure by $R^{(2)}_{\mathcal{J},\mathscr{M}}$ and call it the pair correlation measure of \mathscr{M} . Corresponding to the limiting measure $R^{(2)}_{\mathcal{J},\mathscr{M}}$ we also have an associated function $G_{\mathcal{J},\mathscr{M}}$ given by

$$G_{\mathcal{J},\mathcal{M}}(\lambda) = R^{(2)}_{\mathcal{J},\mathcal{M}}([0,\lambda]) = \lim_{Q \to \infty} G_{\mathcal{J},\mathcal{M}_Q}(\lambda).$$

In case this measure is absolutely continuous with respect to the Lebesgue measure, we denote its density by $g_{\mathcal{J},\mathcal{M}}$ and call it the pair correlation function of \mathcal{M} . The functions $G_{\mathcal{J},\mathcal{M}}$ and $g_{\mathcal{J},\mathcal{M}_{Q}}$ are related by

$$G_{\mathcal{J},\mathcal{M}}(\lambda) = \int_0^\lambda g_{\mathcal{J},\mathcal{M}}(x) \,\mathrm{d}x$$

A natural question that arises is how these functions deform via smooth maps between two curves. While there is no essential difficulty to deal with the general situation, for the sake of our applications here it suffices to consider a curve and an interval on the real line.

Let **I** be a closed interval with length $|\mathbf{I}|$ and $\mathcal{C} \subset \mathbb{R}^k$ a curve with parametrization f: $\mathbf{I} \longrightarrow \mathcal{C}$, where the function f is continuous, piecewise continuously differentiable, and f' does not vanish in **I**. Suppose $\mathscr{F} = (\mathscr{F}_Q)_{Q \in \mathbb{N}}$ is a sequence of finite sequences of points on **I** with $\mathscr{F}_Q = \{t_j^Q : 1 \leq j \leq N_Q\}$. Denoting $x_j^Q = f(t_j^Q)$, we form a sequence of finite sequences of points on \mathcal{C} by letting $\mathscr{M}_Q = \{x_j^Q : 1 \leq j \leq N_Q\}$ and $\mathscr{M} = (\mathscr{M}_Q)_{Q \in \mathbb{N}}$. We need the following result.

Theorem 2. Let $\mathcal{C}, \mathbf{I}, f, \mathcal{M}, \mathcal{F}$ be as above. Suppose that \mathcal{F} is uniformly distributed on \mathbf{I} and for any subinterval \mathbf{J} of \mathbf{I} , the sequence of functions $\left(G_{\mathbf{J}, \mathcal{F}_Q}\right)_{Q \in \mathbb{N}}$ converges pointwise as $Q \to \infty$ to a continuous function $G_{\mathbf{J}, \mathcal{F}}$ which is independent of the interval \mathbf{J} . Then the limiting pair correlation measure $R_{\mathcal{C}, \mathcal{M}}^{(2)}$ exists. Moreover, the corresponding limiting function $G_{\mathcal{C}, \mathcal{M}}$ is given by

$$G_{\mathcal{C},\mathscr{M}}(\lambda) = \frac{1}{|\mathbf{I}|} \cdot \int_{\mathbf{I}} G_{\mathbf{I},\mathscr{F}}\left(\frac{l(\mathcal{C})}{|\mathbf{I}||f'(t)|} \cdot \lambda\right) dt,$$

for any $\lambda > 0$.

Proof of Theorem 2. We adapt the method of proof of Theorem 1 in [1] with necessary modifications to obtain the limiting pair correlation function. For $\lambda > 0$, it suffices to study the behavior of the quantity

$$G_{\mathcal{C},N_Q}(\lambda) = \frac{1}{2N_Q} \#\{(x,y) \in \mathscr{M}_Q : x \neq y, l(\widetilde{xy}) \leq \frac{\lambda l(\mathcal{C})}{N_Q}\}$$

as $Q \to \infty$. For this purpose, we make a partition of **I**,

$$\pi: a = a_0 < a_1 < a_2 < \dots < a_L = b.$$

Denote $B_i = f(a_i)$ for i = 0, 1, ..., L, and $\mathbf{I}_i = [a_i, a_{i+1}], \mathcal{J}_i = \widetilde{B_i B_{i+1}}$ as subintervals of \mathbf{I} and subarcs of \mathcal{C} respectively for i = 0, ..., L - 1. Then

$$\mathbf{I} = \bigcup_{i=0}^{L-1} \mathbf{I}_i, \quad \mathcal{C} = \bigcup_{i=0}^{L-1} \mathcal{J}_i.$$

Moreover, for $i = 0, 1, \ldots, L - 1$ define

$$\mathscr{F}_{Q}(\mathbf{I}_{i}) = \{t_{j}^{Q} \in \mathbf{I}_{i} : 1 \leq j \leq N_{Q}\},\$$
$$\mathscr{M}_{Q}(\mathcal{J}_{i}) = \{x_{j}^{Q} \in \mathcal{J}_{i} : 1 \leq j \leq N_{Q}\},\$$

and denote

$$N_{Q,i} = \#\mathscr{F}_Q(\mathbf{I}_i) = \#\mathscr{M}_Q(\mathcal{J}_i).$$

Let

$$H_i = \frac{1}{2N_{Q,i}} \#\{(x,y) \in \mathscr{M}_Q(\mathcal{J}_i)^2 : x \neq y, l(\widetilde{xy}) \le \frac{\lambda l(\mathcal{C})}{N_Q}\}.$$

It is easy to see that

$$\sum_{i=0}^{L-1} N_{Q,i} H_i \le N_Q G_{\mathcal{C},N_Q}(\lambda).$$

For any $\epsilon > 0$, and each point $B_i, i = 1, ..., L - 1$, we draw a subarc \mathcal{J}'_i of \mathcal{C} centered at B_i with length ϵ . Let $\mathbf{I}'_i = f^{-1}(\mathcal{J}'_i)$ and denote

$$N'_{Q,i} = \#\mathscr{F}_Q(\mathbf{I}'_i) = \#\mathscr{M}_Q(\mathcal{J}'_i),$$
$$H'_i = \frac{1}{2N'_{Q,i}} \#\{(x,y) \in \mathscr{M}_Q(\mathcal{J}'_i)^2 : x \neq y, l(\widetilde{xy}) \le \frac{\lambda l(\mathcal{C})}{N_Q}\}.$$

For any $x \in \mathcal{J}_i, y \in \mathcal{J}_{i+1}$ with $x \neq y, l(\widetilde{xy}) \leq \frac{\lambda l(\mathcal{C})}{N_Q}$, thus we must have $x, y \in \mathcal{J}'_i$ when Q is sufficiently large, since $N_Q \to \infty$ as $Q \to \infty$. Therefore

$$N_Q G_{\mathcal{C}, N_Q}(\lambda) \le \sum_{i=0}^{L-1} N_{Q,i} H_i + \sum_{i=0}^{L-1} N'_{Q,i} H'_i.$$

One has

(1)
$$\sum_{i=0}^{L-1} \frac{N_{Q,i}}{N_Q} H_i \le G_{\mathcal{C},N_Q}(\lambda) \le \sum_{i=0}^{L-1} \frac{N_{Q,i}}{N_Q} H_i + \sum_{i=1}^{L-1} \frac{N'_{Q,i}}{N_Q} H'_i.$$

Note that

$$m = \min_{t \in \mathbf{I}} \{ |f'(t)| \} > 0,$$

and let

$$M_i = \max_{t \in \mathbf{I}_i} \{ |f'(t)| \}, \qquad m_i = \min_{t \in \mathbf{I}_i} \{ |f'(t)| \} \ge m.$$

When $x, y \in \mathbf{I}_i$, assuming x < y, we have

$$m_i(y-x) \le l(\widetilde{f(x)f(y)}) = \int_x^y |f'(t)| \mathrm{d}t \le M_i(y-x).$$

Define the quantities

$$\begin{split} L_i &= \frac{1}{2N_{Q,i}} \# \left\{ (x,y) \in \mathscr{F}_Q(\mathbf{I}_i)^2 : 0 < |x-y| \le \frac{\lambda l(\mathcal{C})}{N_Q M_i} \right\}, \\ U_i &= \frac{1}{2N_{Q,i}} \# \left\{ (x,y) \in \mathscr{F}_Q(\mathbf{I}_i)^2 : 0 < |x-y| \le \frac{\lambda l(\mathcal{C})}{N_Q m_i} \right\}, \\ U'_i &= \frac{1}{2N'_{Q,i}} \# \left\{ (x,y) \in \mathscr{F}_Q(\mathbf{I}'_i)^2 : 0 < |x-y| \le \frac{\lambda l(\mathcal{C})}{N_Q m} \right\}. \end{split}$$

Using the definition and the inequalities above, we have

$$L_i \le H_i \le U_i, \qquad H'_i \le U'_i.$$

Taking (1) into account we have

$$\sum_{i=0}^{L-1} \frac{N_{Q,i}}{N_Q} \cdot L_i \le G_{\mathcal{C},N_Q}(\lambda) \le \sum_{i=0}^{L-1} \frac{N_{Q,i}}{N_Q} \cdot U_i + \sum_{i=1}^{L-1} \frac{N'_{Q,i}}{N_Q} U'_i.$$

Since $\mathscr{F} = (\mathscr{F}_Q)_Q$ is uniformly distributed along the interval \mathbf{I} ,

$$\lim_{Q \to \infty} \frac{N_{Q,i}}{N_Q} = \frac{|\mathbf{I}_i|}{|\mathbf{I}|}, \qquad \lim_{Q \to \infty} \frac{N'_{Q,i}}{N_Q} = \frac{|\mathbf{I}'_i|}{|\mathbf{I}|} \le \frac{\epsilon}{m|\mathbf{I}|}$$

Denote

$$\delta_i = \frac{l(\mathcal{C})}{|\mathbf{I}|M_i}, \quad \delta'_i = \frac{l(\mathcal{C})}{|\mathbf{I}|m_i}, \quad \delta = \frac{l(\mathcal{C})}{|\mathbf{I}|m}.$$

Since the limiting functions $G_{\mathbf{I}_i,\mathscr{F}}, G_{\mathbf{I}'_i,\mathscr{F}}$ exist and coincide with $G_{\mathbf{I},\mathscr{F}}$, we have

$$\begin{array}{rcl} L_i & \longrightarrow & G_{\mathbf{I},\mathscr{F}}(\delta_i \cdot \lambda), \\ \\ U_i & \longrightarrow & G_{\mathbf{I},\mathscr{F}}(\delta_i' \cdot \lambda) & Q \to \infty \\ \\ U_i' & \longrightarrow & G_{\mathbf{I},\mathscr{F}}(\delta \cdot \lambda), \end{array}$$

Therefore

$$L_{\pi} = \lim_{Q \to \infty} \sum_{i=0}^{L-1} \frac{N_{Q,i}}{N_Q} \cdot L_i = \frac{1}{|\mathbf{I}|} \cdot \sum_{i=0}^{L-1} G_{\mathbf{I},\mathscr{F}}(\delta_i \lambda) \cdot |\mathbf{I}_i|,$$
$$U_{\pi} = \lim_{Q \to \infty} \sum_{i=0}^{L-1} \frac{N_{Q,i}}{N_Q} \cdot U_i = \frac{1}{|\mathbf{I}|} \cdot \sum_{i=0}^{L-1} G_{\mathbf{I},\mathscr{F}}(\delta'_i \lambda) \cdot |\mathbf{I}_i|,$$

and

$$\lim_{Q \to \infty} \sum_{i=1}^{L-1} \frac{N'_{Q,i}}{N_Q} \cdot U'_i \le \frac{\epsilon}{m|\mathbf{I}|} (L-1) G_{\mathbf{I},\mathscr{F}}(\delta\lambda).$$

Letting $Q \to \infty$ and $\epsilon \to 0$ we conclude that, for any partition π of **I**,

$$L_{\pi} \leq \liminf_{Q \to \infty} G_{\mathcal{C}, \mathscr{M}_{Q}}(\lambda) \leq \limsup_{Q \to \infty} G_{\mathcal{C}, \mathscr{M}_{Q}}(\lambda) \leq U_{\pi}.$$

Since the functions $G_{\mathbf{I},\mathscr{F}}(\lambda)$ and $\frac{1}{|f'(t)|}$ are continuous, we have

$$\lim_{|\pi|\to 0} L_{\pi} = \lim_{|\pi|\to 0} U_{\pi} = \frac{1}{|\mathbf{I}|} \int_{\mathbf{I}} G_{\mathbf{I},\mathscr{F}} \left(\frac{l(\mathcal{C})}{|\mathbf{I}| |f'(t)|} \cdot \lambda \right) dt$$

This gives the formula for $G_{\mathcal{C},\mathcal{M}}$ as in the statement of Theorem 2. It follows that the sequence of pair correlation measures $R_{\mathcal{C},\mathcal{M}_Q}^{(2)}$ converges weakly as $Q \to \infty$, and this completes the proof of Theorem 2.

ALKAN, XIONG, AND ZAHARESCU

3. PAIR CORRELATION OF TORSION POINTS

For each positive integer Q, let $\mathscr{F}_Q = \{\gamma_1, \ldots, \gamma_{N(Q)}\}$ denote the Farey sequence of order Q with $1/Q = \gamma_1 < \gamma_2 < \cdots < \gamma_{N(Q)} = 1$ and $\mathscr{F} = (\mathscr{F}_Q)_{Q \in \mathbb{N}}$ (for basic properties of the Farey sequence see [9]). The pair correlation measure of \mathscr{F} on [0,1] was established by Boca and one of the authors in [3]. Here we will need a short interval version of this result in order to obtain the pair correlation measure of torsion points on elliptic curves by using the Weierstrass parametrization and Theorem 2. We adapt the method of [3] with some necessary modifications. The formula ([7], formula (1), pp. 246)

$$\sum_{\gamma \in \mathscr{F}_Q} e(r\gamma) = \sum_{\substack{d \geq 1 \\ d \mid r}} dM\left(\frac{Q}{d}\right), \quad r, Q \in \mathbb{Z}, Q \geq 1,$$

where

$$M(x) = \sum_{n \le x} \mu(n)$$

where μ is the Möbius function, plays an important role in the sequel.

Let **I** be a subinterval of [0, 1]. We denote by $\mathscr{F}_{\mathbf{I}}(Q) := \mathscr{F}_{Q} \cap \mathbf{I}$ and by $N_{\mathbf{I}}(Q)$ the cardinality of $\mathscr{F}_{\mathbf{I}}(Q)$. It is known that

(2)
$$N = \frac{N_{\mathbf{I}}(Q)}{|\mathbf{I}|} = \frac{3Q^2}{\pi^2} + O(Q\log Q).$$

Our objective is to estimate, for any positive real number \wedge , the quantity

$$S_{Q,\mathbf{I}}(\wedge) := \# \left\{ (x,y) \in \mathscr{F}_{\mathbf{I}}(Q)^2 : x \neq y, x - y \in \frac{(0,\wedge)}{N} + \mathbb{Z} \right\},\$$

as $Q \to \infty$. Indeed we prove a more general result. We use Supp f to denote the support of a function f.

Lemma 1. Suppose $H, G \in C^1(\mathbb{R})$ with Supp $G \subset (0,1)$ and Supp $H \subset (0, \wedge)$ for some $\wedge > 0$. Define

$$h(y) = \sum_{n \in \mathbb{Z}} H(N(y+n)), \quad g(y) = \sum_{n \in \mathbb{Z}} G(y+n),$$

and

$$S_{Q,\mathbf{I},H,G} = \sum_{\gamma,\gamma' \in \mathscr{F}_Q} h(\gamma - \gamma')g(\gamma)g(\gamma').$$

Then

$$S_{Q,\mathbf{I},H,G} = \frac{3Q^2}{\pi^2} \left(\int_0^1 G(z)^2 \, \mathrm{d}z \right) \int_0^{\wedge} H(x) g_1(x) \, \mathrm{d}x + E_{Q,\mathbf{I},H,G},$$

where

(3)
$$g_1(x) = \frac{6}{\pi^2 x^2} \sum_{1 \le k \le \frac{\pi^2 x}{3}} \varphi(k) \log \frac{\pi^2 x}{3k}$$

for x > 0, φ is the Euler totient function and for any $\sigma > 0$,

$$E_{Q,\mathbf{I},H,G} \ll_{\mathbf{I},H,G,\sigma} Q^{2-\frac{1}{4}+\sigma}.$$

Note that assuming Lemma 1 and using the fact that the error term is $Q^{2-\frac{1}{4}+\sigma}$, we have for $0 < \sigma < \frac{1}{4}$,

$$\lim_{Q \to \infty} \frac{S_{Q,\mathbf{I},H,G}}{N_{\mathbf{I}}(Q)} = \lim_{Q \to \infty} \frac{S_{Q,\mathbf{I},H,G}}{\frac{3|\mathbf{I}|}{\pi^2}Q^2}$$
$$= \frac{\int_0^1 G(z)^2 \mathrm{d}z}{|\mathbf{I}|} \cdot \int_0^{\wedge} H(x)g_1(x) \,\mathrm{d}x.$$

Letting the smooth function G approach $\chi_{\mathbf{I}},$ the characteristic function of the interval $\mathbf{I},$ we have

$$\frac{\int_0^1 G(z)^2 \mathrm{d}z}{|\mathbf{I}|} \to 1,$$

and letting the smooth function H approach $\chi_{(0,\wedge)}$, the characteristic function of the interval $(0, \wedge)$, by a standard approximation argument, we see that the pair correlation function of \mathscr{F} on the subinterval \mathbf{I} exists, is independent of the location and length of the subinterval, and is equal to the pair correlation function of \mathscr{F} on [0, 1] which was determined in [3]. More precisely we have,

Theorem 3. The pair correlation function of $\mathscr{F} = (\mathscr{F}_Q)_{Q \in \mathbb{N}}$ on any subinterval $\mathbf{I} \subset [0, 1]$ exists and is given by

$$g_1(x) = \frac{6}{\pi^2 x^2} \sum_{1 \le k \le \frac{\pi^2 x}{3}} \varphi(k) \log \frac{\pi^2 x}{3k},$$

for any x > 0.

We now turn to our problem of studying the correlation of torsion points on an elliptic curve over \mathbb{R} (for the general theory of elliptic curves see [10]). Let *E* be an elliptic curve defined over \mathbb{R} , given by the equation

$$E: y^2 = 4x^3 - g_2x - g_3,$$

where $g_2, g_3 \in \mathbb{R}$ and $g_2^3 - 27g_3^2 \neq 0$. The set $E(\mathbb{R})$ of real points of E has a natural group structure which makes $E(\mathbb{R})$ an abelian group. Recall that there is a complex analytic isomorphism of complex Lie groups (see [10])

$$\exp: \ \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}) \subseteq P^2(\mathbb{C})$$
$$z \longmapsto (\wp(z), \wp'(z)),$$

where Λ is a lattice in \mathbb{C} associated to $E(\mathbb{C})$, and $\wp(z)$ is the Weierstrass \wp -function associated to Λ . Here $E(\mathbb{R})$ may have one or two connected components. The unbounded one $E_U(\mathbb{R})$ is isomorphic under exp to $\mathcal{S}^1 \simeq \mathbb{R}/\mathbb{Z}$ as real Lie groups. Identifying \mathbb{R}/\mathbb{Z} with [0, 1), this gives us in turn a C^{∞} map $\phi : [0, 1) \longrightarrow E_U(\mathbb{R})$ such that $\phi(0) = \mathcal{O}$ is the point at infinity and for any $t \in [0, 1)$, any integer n,

$$\phi(nt \pmod{1}) = [n]\phi(t) \in E_U(\mathbb{R}).$$

For any finite arc $\mathcal{J} \subset E_U(\mathbb{R})$, let $\mathbf{I} = \phi^{-1}(\mathcal{J}) \subset [0, 1)$. The set $\mathscr{M}_{E,\mathcal{J},Q}$ of torsion points of Eon \mathcal{J} corresponds to the set $\mathscr{F}_{\mathbf{I}}(Q)$ via the parametrization ϕ . Hence by combining Theorem 2 and Theorem 3 we obtain that, **Corollary 1.** The pair correlation function of $(\mathscr{M}_{E,\mathcal{J},Q})_{Q\in\mathbb{N}}$ exists for any elliptic curve E over \mathbb{R} and any finite arc $\mathcal{J} \subset E_U(\mathbb{R})$ and is given by

(4)
$$g_{E,\mathcal{J}}(\lambda) = \frac{l(\mathcal{J})}{|\mathbf{I}|^2} \cdot \int_{\mathbf{I}} g_1\left(\frac{l(\mathcal{J})}{|\mathbf{I}||\phi'(t)|} \cdot \lambda\right) \frac{\mathrm{d}t}{|\phi'(t)|},$$

for any $\lambda > 0$.

It follows from Corollary 1 that for any $P \in E_U(\mathbb{R}), P \neq \mathcal{O}$, one has

$$g_{E,P}(\lambda) = \lim_{\substack{l(\mathcal{J}) \to 0, \\ P \in \mathcal{J} \subset E_U(\mathbb{R}),}} g_{\mathcal{J},\mathscr{M}}(\lambda) = g_1(\lambda).$$

Proof of Lemma 1. The proof of this lemma will require several steps. All the constants in the proof implied by the big "O" or " \ll " notations may depend on the functions H and G.

3.1. Fourier series expansion and Poisson summation formula. Suppose that the Fourier series expansion of functions h and g are given by

$$h(y) = \sum_{n \in \mathbb{Z}} c_n e(ny)$$

and

$$g(y) = \sum_{n \in \mathbb{Z}} a_n e(ny)$$

for $y \in \mathbb{R}$, where $e(ny) = \exp(2\pi i ny)$. Then we have

$$S_{Q,\mathbf{I},H,G} = \sum_{\gamma,\gamma'\in\mathscr{F}_Q} \sum_m c_m e(m(\gamma-\gamma')) \sum_n a_n e(n\gamma)) \sum_r a_r e(r\gamma')$$

$$= \sum_{m,n,r} c_m a_n a_r \sum_{\gamma\in\mathscr{F}_Q} e((m+n)\gamma) \sum_{\gamma'\in\mathscr{F}_Q} e((r-m)\gamma')$$

$$= \sum_{m,n,r} c_m a_n a_r \left(\sum_{\substack{1\leq d\leq Q, \\ d|m+n}} dM\left(\frac{Q}{d}\right)\right) \left(\sum_{\substack{1\leq d\leq Q, \\ d|r-m}} dM\left(\frac{Q}{d}\right)\right).$$

Changing the summation index as m + n = m', r - m = n', m = r', we have m = r', n = m' - r', r = n' + r', and

$$S_{Q,\mathbf{I},H,G} = \sum_{m',n',r'} c_{r'} a_{m'-r'} a_{n'+r'} \left(\sum_{\substack{1 \le d \le Q, \\ d|m'}} dM\left(\frac{Q}{d}\right) \right) \left(\sum_{\substack{1 \le d \le Q, \\ d|n'}} dM\left(\frac{Q}{d}\right) \right)$$
$$= \sum_{1 \le d_1, d_2 \le Q} d_1 d_2 M\left(\frac{Q}{d_1}\right) M\left(\frac{Q}{d_2}\right) \sum_{\substack{r',m',n' \in \mathbb{Z}, \\ d_1|m', d_2|n',}} c_{r'} a_{m'-r'} a_{n'+r'}$$
$$= \sum_{1 \le d_1, d_2 \le Q} d_1 d_2 M\left(\frac{Q}{d_1}\right) M\left(\frac{Q}{d_2}\right) \sum_{r \in \mathbb{Z}} c_r \sum_{m \in \mathbb{Z}} a_{d_1m-r} \sum_{n \in \mathbb{Z}} a_{d_2n+r}.$$

Consider for each d > 0 and real number r the function

$$G_{r,d}(x) = \frac{1}{d} G\left(\frac{x}{d}\right) e\left(\frac{rx}{d}\right), \quad x \in \mathbb{R}.$$

Using the Fourier transform and a simple change of variable we obtain that for any $m \in \mathbb{Z}$,

$$\begin{aligned} \widehat{G}_{r,d}(m) &= \int_{\mathbb{R}} G_{r,d}(t) e(-mt) \, \mathrm{d}t = \int_{\mathbb{R}} \frac{1}{d} G\left(\frac{t}{d}\right) e\left(\frac{rt}{d}\right) e(-mt) \, \mathrm{d}t \\ &= \int_{\mathbb{R}} G(t') e(rt') e(-mdt') \, \mathrm{d}t' = \int_{\mathbb{R}} G(t) e(-(md-r)t) \, \mathrm{d}t \\ &= \widehat{G}(md-r) = a_{dm-r}. \end{aligned}$$

Applying the Poisson summation formula one has

$$\sum_{m \in \mathbb{Z}} a_{d_1m-r} = \sum_{m \in \mathbb{Z}} \widehat{G}_{r,d_1}(m) = \sum_{m \in \mathbb{Z}} G_{r,d_1}(m) = \sum_{m \in \mathbb{Z}} \frac{1}{d_1} G\left(\frac{m}{d_1}\right) e\left(\frac{rm}{d_1}\right),$$

and similarly

$$\sum_{n \in \mathbb{Z}} a_{d_2 n + r} = \sum_{n \in \mathbb{Z}} \frac{1}{d_2} G\left(\frac{n}{d_2}\right) e\left(\frac{-rn}{d_2}\right).$$

It follows that

$$\sum_{r \in \mathbb{Z}} c_r \sum_{m \in \mathbb{Z}} a_{d_1 m - r} \sum_{n \in \mathbb{Z}} a_{d_2 n + r}$$

$$= \sum_{r \in \mathbb{Z}} c_r \sum_{m \in \mathbb{Z}} \frac{1}{d_1} G\left(\frac{m}{d_1}\right) e\left(\frac{rm}{d_1}\right) \sum_{n \in \mathbb{Z}} \frac{1}{d_2} G\left(\frac{n}{d_2}\right) e\left(\frac{-rn}{d_2}\right)$$

$$= \frac{1}{d_1 d_2} \sum_{m,n} G\left(\frac{m}{d_1}\right) G\left(\frac{n}{d_2}\right) \sum_r c_r e\left(\left(\frac{m}{d_1} - \frac{n}{d_2}\right)r\right).$$

The Fourier expansion of h(y) gives us that

$$\sum_{r} c_r e\left(\left(\frac{m}{d_1} - \frac{n}{d_2}\right)r\right) = h\left(\frac{m}{d_1} - \frac{n}{d_2}\right) = \sum_{r} H\left(N\left(r + \frac{m}{d_1} - \frac{n}{d_2}\right)\right).$$

Using this in the above formula for $S_{Q,\mathbf{I},H,G}$ we deduce in conclusion that

$$S_{Q,\mathbf{I},H,G} = \sum_{1 \le d_1, d_2 \le Q} M\left(\frac{Q}{d_1}\right) M\left(\frac{Q}{d_2}\right) \times \\ \sum_{m,n,r \in \mathbb{Z}} G\left(\frac{m}{d_1}\right) G\left(\frac{n}{d_2}\right) H\left(N\left(r + \frac{m}{d_1} - \frac{n}{d_2}\right)\right) \\ = \sum_{1 \le G_1, r_2 \le Q} \mu(r_1)\mu(r_2) \sum_{\substack{d_1 \le Q/r_1, \\ d_2 \le Q/r_2,}} \times \\ \sum_{m,n,r \in \mathbb{Z}} G\left(\frac{m}{d_1}\right) G\left(\frac{n}{d_2}\right) H\left(N\left(r + \frac{m}{d_1} - \frac{n}{d_2}\right)\right).$$

3.2. Further Reductions. First, using the facts that Supp $G \subset (0,1)$, Supp $H \subset (0, \wedge)$, $d_1, d_2 \leq Q$ and $N \sim \frac{3}{\pi^2}Q^2$, we have for $r \neq 0$, $H\left(N\left(r + \frac{m}{d_1} - \frac{n}{d_2}\right)\right) = 0$ when Q is sufficiently large. For positive integers d_1, d_2 , let

$$\delta = (d_1, d_2), \quad d_1 = q_1 \delta, \quad d_2 = q_2 \delta,$$

Clearly $(q_1, q_2) = 1$, and there is a unique integer \bar{q}_2 such that $0 < \bar{q}_2 < q_1, \bar{q}_2 q_2 \equiv 1 \pmod{q_1}$. Take $\tilde{a}_1 = (1 - \bar{q}_2 q_2)/q_1$, so that $\tilde{a}_1 q_1 + \bar{q}_2 q_2 = 1$. Changing the summation index as

$$m' = q_2m - q_1n, \quad n' = \widetilde{a}_1m + \overline{q}_2n,$$

we have

$$m = \overline{q}_2 m' + q_1 n', \quad n = -\widetilde{a}_1 m' + q_2 n'.$$

Hence by taking r = 0, the inner sum on m, n, r in the formula of $S_{Q,\mathbf{I},H,G}$ above can be written as

$$\sum_{m,n\in\mathbb{Z}} G\left(\frac{m}{d_1}\right) G\left(\frac{n}{d_2}\right) H\left(N\left(\frac{m}{d_1}-\frac{n}{d_2}\right)\right)$$
$$= \sum_{m,n\in\mathbb{Z}} G\left(\frac{\bar{q}_2m}{q_1\delta}+\frac{n}{\delta}\right) G\left(\frac{-\tilde{a}_1m}{q_2\delta}+\frac{n}{\delta}\right) H\left(\frac{Nm}{q_1q_2\delta}\right)$$
$$= \sum_{m,n\in\mathbb{Z}} G\left(\frac{1}{\delta}\left(\frac{\bar{q}_2m}{q_1}+n\right)\right) G\left(\frac{1}{\delta}\left(\frac{\bar{q}_2m}{q_1}+n-\frac{m}{q_1q_2}\right)\right) H\left(\frac{Nm}{q_1q_2\delta}\right).$$

Combining this with the above formula for $S_{Q,\mathbf{I},H,G}$ we obtain

$$S_{Q,\mathbf{I},H,G} = \sum_{1 \le r_1, r_2 \le Q} \mu(r_1)\mu(r_2) \sum_{\substack{q_1\delta \le Q/r_1, \ m,n \in \mathbb{Z} \\ q_2\delta \le Q/r_2, \ (q_1,q_2)=1}} \sum_{\substack{q_1\sigma_1 \le Q/r_2, \ (q_1,q_2)=1}} \times G\left(\frac{1}{\delta}\left(\frac{\bar{q}_2m}{q_1}+n\right)\right) G\left(\frac{1}{\delta}\left(\frac{\bar{q}_2m}{q_1}+n-\frac{m}{q_1q_2}\right)\right) H\left(\frac{Nm}{q_1q_2\delta}\right).$$

Next for any $0 < \epsilon < \frac{1}{2}$, when Q is sufficiently large, we have

(5)
$$\frac{3Q^2}{2\pi^2} < \frac{3Q^2}{\pi^2}(1-\epsilon) < N < \frac{3Q^2}{\pi^2}(1+\epsilon) < \frac{9Q^2}{2\pi^2}.$$

Since Supp $H \subset (0, \wedge)$, to get a non-zero contribution from H, we must have

$$0 < m\delta r_1 r_2 \frac{3}{\pi^2} (1 - \epsilon) < m\delta r_1 r_2 \frac{N}{Q^2}$$

$$\leq m\delta r_1 r_2 \frac{N}{(q_1 \delta r_1)(q_2 \delta r_2)}$$

$$= \frac{Nm}{q_1 q_2 \delta} < \wedge.$$

That is

$$mr_1r_2\delta < \frac{\pi^2\wedge}{3(1-\epsilon)}.$$

14

Denoting

$$C_{\wedge} = \frac{\pi^2 \wedge}{3},$$

and choosing ϵ sufficiently small we obtain that

$$1 \le mr_1 r_2 \delta \le C_{\wedge}.$$

We fix m, r_1, r_2 and δ bounded by C_{\wedge} . Since Supp $G \subset (0, 1)$, to get a non-zero contribution from G, we need

$$0 < \frac{1}{\delta} \left(\frac{\bar{q}_2 m}{q_1} + n \right) < 1.$$

Clearly there are only finitely many integers n satisfying this inequality. Denote by \mathcal{A} the finite set consisting of all possible values of such n. By changing the order of summation we can simplify $S_{Q,\mathbf{I},H,G}$ as

$$S_{Q,\mathbf{I},H,G} = \sum_{\substack{mr_1r_2\delta \leq C_{\wedge}, \\ n \in \mathcal{A}, \\ m \in \mathcal{A}, \\ m \in \mathcal{A}, \\ G\left(\frac{1}{\delta}\left(\frac{\bar{q}_2m}{q_1} + n - \frac{m}{q_1q_2}\right)\right) H\left(\frac{Nm}{\delta q_1q_2}\right).$$

Since

$$G\left(\frac{1}{\delta}\left(\frac{\bar{q}_2m}{q_1}+n-\frac{m}{q_1q_2}\right)\right) = G\left(\frac{1}{\delta}\left(\frac{\bar{q}_2m}{q_1}+n\right)\right) + O\left(\frac{m}{\delta q_1q_2}\right),$$

one has

$$S_{Q,\mathbf{I},H,G} = \sum_{\substack{mr_1r_2\delta \leq C_{\wedge}, \\ n \in \mathcal{A},}} \mu(r_1)\mu(r_2) \sum_{\substack{q_1 \leq Q/\delta r_1, \\ q_2 \leq Q/\delta r_2, \\ (q_1,q_2)=1,}} G\left(\frac{1}{\delta}\left(\frac{\bar{q}_2m}{q_1}+n\right)\right)^2 \times H\left(\frac{Nm}{\delta q_1 q_2}\right) + E_0,$$

where for any $\sigma > 0$,

$$E_0 \ll \sum_{\substack{mr_1r_2\delta \le C_{\wedge}, q_1 \le Q/\delta r_1, \\ n \in \mathcal{A}, \\ (q_1, q_2) = 1,}} \frac{m}{\delta q_1 q_2} \ll (\log Q)^2 \ll_{\sigma} Q^{\sigma}.$$

For fixed m, r_1, r_2, δ, n , let us define the functions

(6)
$$f_n(x) := G\left(\frac{1}{\delta}(mx+n)\right)^2, \quad h(x,y) := H\left(\frac{Nm}{\delta xy}\right).$$

Then the inner sum of the main term of $S_{Q,\mathbf{I},H,G}$ on q_1,q_2 can be written as

(7)
$$\sum = \sum_{\substack{q_1 \le Q/\delta r_1, \\ q_2 \le Q/\delta r_2, \\ (q_1, q_2) = 1,}} f_n\left(\frac{\bar{q}_2}{q_1}\right) h(q_1, q_2),$$

where \bar{q}_2 is the unique integer such that $0 < \bar{q}_2 < q_1, \bar{q}_2 q_2 \equiv 1 \pmod{q_1}$.

3.3. Auxiliary Estimations. We will need some additional estimations to complete the proof. First of all we know that f_n and f'_n are uniformly bounded. Also, since Supp $H \subset (0, \wedge)$, for $0 < x \le Q/\delta r_1, 0 < y \le Q/\delta r_2$, if $h(x, y) \ne 0$, then we must have $0 < \frac{N\lambda}{xy} < \wedge$. Using (5), this implies that

$$\frac{Q}{\delta r_1} \ge x > \frac{N\lambda}{\wedge y} \ge \frac{\frac{3Q^2m}{2\pi^2\delta}}{\frac{Q}{\delta r_2}\wedge} = \frac{3m\delta r_1r_2}{2\pi^2\wedge}\frac{Q}{\delta r_1}$$

A similar inequality holds for y. Therefore denoting

$$c_{\wedge} = \frac{3m\delta r_1 r_2}{2\pi^2 \wedge},$$

we have,

(8)
$$h(x,y) \neq 0 \implies \frac{c_{\wedge}Q/\delta r_1 \leq x \leq Q/\delta r_1,}{c_{\wedge}Q/\delta r_2 \leq y \leq Q/\delta r_2.}$$

Clearly h is uniformly bounded and

$$\left|\frac{\partial h}{\partial x}(x,y)\right| = \left|H'\left(\frac{N\lambda}{xy}\right)\right| \cdot \frac{N\lambda}{xy} \cdot \frac{1}{x} \le ||DH||_{\infty} \cdot \wedge \cdot \frac{\delta r_1}{c_{\wedge}Q} \ll \frac{1}{Q}.$$

A similar inequality holds for $\frac{\partial h}{\partial y}(x, y)$, and gives that

$$||Dh||_{\infty} = \left| \left| \frac{\partial h}{\partial x} \right| \right|_{\infty} + \left| \left| \frac{\partial h}{\partial y} \right| \right|_{\infty} \ll \frac{1}{Q},$$

where $||.||_{\infty}$ denotes the supremum norm.

3.4. Completion of the Proof of Lemma 1. Let K be a large positive integer which will be chosen later. Then (7) can be written as

$$\sum = \sum_{i=0}^{K-1} \sum_{\substack{q_1 \le Q/\delta r_1, \\ q_2 \le Q/\delta r_2, \\ (q_1,q_2)=1, \\ \bar{q}_2 \in [\frac{i}{K}q_1, \frac{i+1}{K}q_1)}} f_n\left(\frac{\bar{q}_2}{q_1}\right) h(q_1, q_2)$$

$$= \sum_{i=0}^{K-1} \sum_{\substack{q_1 \le Q/\delta r_1, \\ q_2 \le Q/\delta r_2, \\ (q_1,q_2)=1, \\ \bar{q}_2 \in [\frac{i}{K}q_1, \frac{i+1}{K}q_1)}} \left(f_n\left(\frac{i}{K}\right) + O\left(\frac{1}{K}\right)\right) h(q_1, q_2)$$

$$= \sum_{i=0}^{K-1} f_n\left(\frac{i}{K}\right) \sum_{\substack{q_1 \le Q/\delta r_1, \\ q_2 \le Q/\delta r_2, \\ (q_1,q_2)=1, \\ q_2 \in [\frac{i}{K}q_1, \frac{i+1}{K}q_1)}} h(q_1, q_2) + O\left(\frac{Q^2}{K}\right).$$

We need the following variations of results from [2]. Recall that for each region Ω in \mathbb{R}^2 and each C^1 function $f: \Omega \longrightarrow \mathbb{C}$, we denote by

$$||f||_{\infty,\Omega} = \sup_{(x,y)\in\Omega} |f(x,y)|,$$

and

$$||Df||_{\infty,\Omega} = \sup_{(x,y)\in\Omega} \left(\left| \frac{\partial f}{\partial x}(x,y) \right| + \left| \frac{\partial f}{\partial y}(x,y) \right| \right).$$

For any subinterval $\mathbf{I} = [\alpha, \beta]$ of [0, 1], denote by $\mathbf{I}_a = [(1 - \beta)a, (1 - \alpha)a]$.

Lemma 2. Let $\Omega \subset [1, R] \times [1, R]$ be a convex region and let f be a C^1 function on Ω . For any subinterval $\mathbf{I} \subset [0, 1]$ one has

$$\sum_{\substack{(a,b)\in\Omega\cap\mathbb{Z}^2_{pr},\\\bar{b}\in\mathbf{I}_a}} f(a,b) = \frac{6|\mathbf{I}|}{\pi^2} \iint_{\Omega} f(x,y) \,\mathrm{d}x \mathrm{d}y + \mathscr{F}_{R,\Omega,f,\mathbf{I}},$$

where

$$\mathcal{F}_{R,\Omega,f,\mathbf{I}} \ll_{\delta} m_{f} ||f||_{\infty,\Omega} R^{3/2+\delta} + ||f||_{\infty,\Omega} R \log R$$
$$+ ||Df||_{\infty,\Omega} Area(\Omega) \log R,$$

for any $\delta > 0$, where \bar{b} denotes the multiplicative inverse of $b \pmod{a}$, i.e., $1 \le \bar{b} \le a, b\bar{b} \equiv 1 \pmod{a}$, m_f is an upper bound for the number of intervals of monotonicity of each of the functions $y \mapsto f(x, y)$.

This is Lemma 8 in [2], where Weil type estimates ([11], [8]) for certain weighted incomplete Kloosterman sums play a crucial role in its proof. Using the fact that h is uniformly bounded and $||Dh||_{\infty} \ll \frac{1}{Q}$ and applying Lemma 2, we have

$$\begin{split} \sum_{\substack{q_1 \leq Q/\delta r_1, \\ q_2 \leq Q/\delta r_2, \\ (q_1,q_2) = 1, \\ \bar{q}_2 \in [\frac{i}{K}q_1, \frac{i+1}{K}q_1)} } h(q_1, q_2) &= \frac{6}{\pi^2 K} \int_0^{\frac{Q}{\delta r_1}} \int_0^{\frac{Q}{\delta r_2}} h(x, y) \mathrm{d}x \mathrm{d}y + O_\sigma \left(Q^{\frac{3}{2} + \sigma}\right) \\ &= \frac{6Q^2}{\pi^2 K \delta^2 r_1 r_2} \iint_{[0,1]^2} h\left(\frac{Qx}{\delta r_1}, \frac{Qy}{\delta r_2}\right) \mathrm{d}x \mathrm{d}y + O_\sigma \left(Q^{\frac{3}{2} + \sigma}\right). \end{split}$$

Using the definition of h(x, y) from (6) we have,

$$h\left(x\frac{Q}{\delta_1}, y\frac{Q}{\delta_2}\right) := H\left(\frac{N\frac{m}{\delta}}{\frac{Q\cdot Q}{\delta r_1\delta r_2}xy}\right) = H\left(\frac{Nm\delta r_1r_2}{Q^2xy}\right).$$

Finally using (8),

$$h\left(x\frac{Q}{\delta_1}, y\frac{Q}{\delta_2}\right) \neq 0 \implies c_{\wedge} \leq x, y \leq 1,$$

we obtain by (2) that,

$$\left| H\left(\frac{Nm\delta r_1 r_2}{Q^2 x y}\right) - H\left(\frac{3m\delta r_1 r_2}{\pi^2 x y}\right) \right| \leq ||DH||_{\infty} \frac{m\delta r_1 r_2}{x y} \left| \frac{N}{Q^2} - \frac{3}{\pi^2} \right|$$
$$\ll \frac{\log Q}{Q} \ll_{\sigma} Q^{-1+\sigma}.$$

It follows that

$$\sum_{\substack{q_1 \le Q/\delta r_1, \\ q_2 \le Q/\delta r_2, \\ (q_1,q_2) = 1, \\ \bar{q}_2 \in [\frac{i}{K}q_1, \frac{i+1}{K}q_1)}} h(q_1, q_2) = \frac{6Q^2}{\pi^2 K \delta^2 r_1 r_2} \iint_{[0,1]^2} H\left(\frac{3m\delta r_1 r_2}{\pi^2 xy}\right) \mathrm{d}x \mathrm{d}y + O_\sigma\left(Q^{\frac{3}{2}+\sigma}\right).$$

Returning to the sum \sum above, we obtain that

$$\sum = \sum_{i=0}^{K-1} f_n\left(\frac{i}{K}\right) \frac{6Q^2}{\pi^2 K \delta^2 r_1 r_2} \iint_{[0,1]^2} H\left(\frac{3m\delta r_1 r_2}{\pi^2 x y}\right) \mathrm{d}x \mathrm{d}y + O_{\sigma}\left(KQ^{\frac{3}{2}+\sigma}\right) + O\left(\frac{Q^2}{K}\right) = \frac{6}{\pi^2} \frac{Q^2}{\delta^2 r_1 r_2} \left(\int_0^1 f_n(x) \mathrm{d}x\right) \left(\iint_{[0,1]^2} h\left(x\frac{Q}{\delta_1}, y\frac{Q}{\delta_2}\right) \mathrm{d}x \mathrm{d}y\right) + O_{\sigma}\left(KQ^{\frac{3}{2}+\sigma}\right) + O\left(\frac{Q^2}{K}\right).$$

We may choose

$$K = [Q^{\frac{1}{4}}] \asymp Q^{\frac{1}{4}},$$

to see that the error term is $E_1 \ll_{\sigma} Q^{2-\frac{1}{4}+\sigma}$ for $\sigma > 0$. Using the definition of f_n from (6),

$$\int_0^1 f_n(x) dx = \int_0^1 G\left(\frac{1}{\delta}(mx+n)\right)^2 dx = \frac{\delta}{m} \int_{\frac{n}{\delta}}^{\frac{m+n}{\delta}} G(z)^2 dz$$
$$= \frac{\delta}{m} \left(\int_{\frac{n}{\delta}}^{\frac{n+1}{\delta}} G(z)^2 dz + \dots + \int_{\frac{n+m-1}{\delta}}^{\frac{n+m}{\delta}} G(z)^2 dz\right).$$

Consequently,

$$\sum_{n \in \mathbb{Z}} \int_0^1 f_n(x) dx = \frac{\delta}{m} \sum_{n \in \mathbb{Z}} \left(\int_{\frac{n}{\delta}}^{\frac{n+1}{\delta}} G(z)^2 dz + \dots + \int_{\frac{n+m-1}{\delta}}^{\frac{n+m}{\delta}} G(z)^2 dz \right)$$
$$= \delta \cdot \int_0^1 G(z)^2 dz.$$

Finally, we conclude that

$$S_{Q,\mathbf{I},H,G} = \sum_{mr_1r_2\delta \leq C_{\wedge},} \mu(r_1)\mu(r_2) \left(\sum_{n \in \mathcal{A}} \sum\right) + E_0$$

$$= \frac{6}{\pi^2} Q^2 \left(\int_0^1 G(z)^2 dz\right) \sum_{1 \leq r_1r_2m\delta \leq \frac{\pi^2}{3}\wedge} \frac{\mu(r_1)\mu(r_2)}{\delta r_1r_2} \times \int_{[0,1]^2} H\left(\frac{3m\delta r_1r_2}{\pi^2 xy}\right) dx \, dy + E_{Q,\mathbf{I},H,G},$$

where the error term is

$$E_{Q,\mathbf{I},H,G} \ll E_0 + E_1 \ll_{\sigma} Q^{2-\frac{1}{4}+\sigma}.$$

Now following the computation of S_2 in [3] we have

$$\sum_{1 \le r_1 r_2 m \delta \le \frac{\pi^2}{3} \land} \frac{\mu(r_1)\mu(r_2)}{\delta r_1 r_2} \iint_{[0,1]^2} H\left(\frac{3m\delta r_1 r_2}{\pi^2 x y}\right) = \frac{1}{2} \int_0^{\land} H(x)g_1(x) \,\mathrm{d}x,$$

where the function g_1 is defined as in (3). This completes the proof of Lemma 1.

References

- [1] E. Alkan, M. Xiong, A. Zaharescu, Local spacings along curves, J. Math. Anal. Appl. 329 (2007), 721–735.
- [2] F. Boca, C. Cobeli, A. Zaharescu, A conjecture of R. R. Hall on Farey points, J. Reine Angew. Math. 535(2001), 207–236.
- [3] F. P. Boca, A. Zaharescu, The Correlations of Farey Fractions, J. London Math. Soc. (2) 72(2005), 25–39.
- [4] F. J. Dyson, Statistical theory of the energy levels of complex systems, I. J. Mathematical Phys. 3(1962), 140–156.
- [5] F. J. Dyson, Statistical theory of the energy levels of complex systems, II. J. Mathematical Phys. 3(1962), 157–165.

- [6] F. J. Dyson, Statistical theory of the energy levels of complex systems, III. J. Mathematical Phys. 3(1962), 166–175.
- [7] H. M. Edwards, "Riemann's zeta function", Dover, Mineola, NY 2001.
- [8] T. Esterman, On Kloosterman's sums, Mathematika 8(1961), 83–86.
- [9] G.H. Hardy, E.M. Wright, An Introduction to the Theory of Numbers, Oxford, Clarendon Press, 1938 (fourth edition 1960).
- [10] J. H. Silverman, "The arithmetic of elliptic curves", Springer-Verlag, New York, GTM 106, 1986.
- [11] A. Weil, On some exponential sums, Proc. Nat. Acad. Sci.USA 34(1948), 204-207.
- [12] H. Weyl, Über die Gleichverteilung von Zahlen mod eins, Math. Ann. 77(1916), no. 3, 313–352.
- [13] E. Wigner, Random matrices in physics, SIAM Review 9(1967), 1–23.
- [14] A. Zaharescu, Spacing distribution along curves, Adv. Stud. Contemp. Math. 7(2003), 61–67.

Department of Mathematics, Koc University, Rumelifeneri Yolu, 34450, Sariyer, Istanbul, TURKEY

E-mail address: ealkan@ku.edu.tr

DEPARTMENT OF MATHEMATICS, EBERLY COLLEGE OF SCIENCE, PENNSYLVANIA STATE UNIVERSITY, MCALLISTER BUILDING, UNIVERSITY PARK, PA 16802 USA

E-mail address: xiong@math.psu.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, 273 ALTGELD HALL, MC-382, 1049 W. GREEN STREET, URBANA, ILLINOIS 61801-2975, USA

E-mail address: zaharesc@math.uiuc.edu