ON THE AVERAGE ANALYTIC RANKS OF ELLIPTIC CURVES

PETER JAEHYUN CHO
ULSAN NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY

1. Introduction

This article reviews the paper "The average analytic rank of elliptic curves with prescribed torsion" [CJ23] by the author and Jeong. In [CJ23], we study the distribution of analytic ranks of elliptic curves with prescribed torsion. Let us start with our model for elliptic curves. Our elliptic curves defined over $\mathbb{Q}$ are represented by for a pair (A, B) of integers with $4A^3+27B^2 \neq 0$

$$E_{A,B} : y^2 = x^2 + Ax + B$$

such that there is no prime p with $p^4 \mid A$ and $p^6 \mid B$. Let $\mathcal{E}$ be the set of all such pairs. A bijection exists between $\mathcal{E}$ and the set of $\mathbb{Q}$-isomorphism classes of elliptic curves over $\mathbb{Q}$. Then, we can order elliptic curves by the naive height:

$$\mathcal{E}(X) = \left\{ E_{A,B} \in \mathcal{E} : |A| \leq X^{\frac{1}{3}}, |B| \leq X^{\frac{1}{2}} \right\}.$$

We can define the average rank of elliptic curves as the limit of the average rank over $\mathcal{E}(X)$ as X goes to infinity if it exists. It was Brumer [Bru92] who first showed that the average analytic rank of elliptic curves is bounded. His bound was 2.3 under GRH for elliptic curve L-functions, which was lowered to 2 and $\frac{25}{14}$ by Heath-Brown [Hea04] and Young [You06] respectively, under GRH for elliptic curve L-functions.

On the other hand, Harron and Snowden [HS14] counted elliptic curves with prescribed torsion G. We say that an elliptic curve E over $\mathbb{Q}$ has torsion G if $E(\mathbb{Q})$ contains a subgroup isomorphic to G.

By a work of Mazur, G is one of the groups

$$\mathbb{Z}/n\mathbb{Z}, \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$$

for $n \in \{1, 2, \cdots 10, 12\}$ and $m \in \{1, 2, 3, 4\}$. Let

$$\mathcal{G}_{\leq 4} := \{\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\}$$

and $\mathcal{G}_{\geq 5}$ be the set of torsion groups of order ≥ 5. We remark that elliptic curves with torsion G in $\mathcal{G}_{\geq 5}$ can be parametrized by Tate's normal form. We often use n and $2 \times 2m$ in place of $G = \mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ to ease the notation.

Let

$$\mathcal{E}_G(X) = \{E_{A,B} \in \mathcal{E}(X) : E(\mathbb{Q}) \geq G\}.$$

Harron and Snowden showed that

$$\lim_{X \to \infty} \frac{\log |\mathcal{E}_G(X)|}{\log X} = \frac{1}{d(G)},$$

TABLE 1.

G	$d(G)$	G	$d(G)$	G	$d(G)$
0	6/5	$\mathbb{Z}/6\mathbb{Z}$	6	$\mathbb{Z}/12\mathbb{Z}$	24
$\mathbb{Z}/2\mathbb{Z}$	2	$\mathbb{Z}/7\mathbb{Z}$	12	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$	3
$\mathbb{Z}/3\mathbb{Z}$	3	$\mathbb{Z}/8\mathbb{Z}$	12	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$	6
$\mathbb{Z}/4\mathbb{Z}$	4	$\mathbb{Z}/9\mathbb{Z}$	18	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$	12
$\mathbb{Z}/5\mathbb{Z}$	6	$\mathbb{Z}/10\mathbb{Z}$	18	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$	24

where $d(G)$ is given in Table 1.

We define the average analytic rank over $\mathcal{E}_G$ to be

$$\lim_{X\to\infty}\frac{1}{|\mathcal{E}_G(X)|}\sum_{E\in\mathcal{E}_G(X)} r_E$$

where r_E is the analytic rank of E. We show that the average analytic rank over any $\mathcal{E}_G$ is bounded.

Theorem 1. Let G be a torsion group. For $G=\mathbb{Z}/n\mathbb{Z}$, $n=7,8,9,10,12$ and $G=\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2m\mathbb{Z}$, $m=3,4$, we assume the moment conditions (5), (6). Under GRH for elliptic curve L-functions, the average analytic rank over $\mathcal{E}_G$ is bounded. In particular when $|G|\geq 5$, we have a bound $\frac{1}{2}+5d(G)$.

For elliptic curves with torsion group $G=\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, we can show that there are fewer elliptic curves with large analytic rank. To ease the notation let $G_1=\mathbb{Z}/2\mathbb{Z}$ and $G_2=\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Let $P_G(r_E\geq a)$ denote the proportion of elliptic curves analytic rank $r_E\geq a$ among the elliptic curves with torsion G. We show a few elliptic curves with torsion G_i, $i=1,2$ with large ranks.

Theorem 2. Assume GRH for elliptic curve L-functions. Let C be a positive constant and n be a positive integer. We have

$$P_{G_i}\left(r_E\geq c_i(1+C)n\right)\leq\frac{\sum_{k=0}^{n}\binom{2n}{2k}\left(\frac{1}{2}\right)^{2n-2k}(2k)!\left(\frac{1}{6}\right)^{k}}{(c_iCn)^{2n}}.$$

where $c_i=18$ and 20 when $i=1,2$ respectively. In particular, the proportions $P_{G_1}(r_E\geq 23)$ and $P_{G_2}(r_E\geq 25)$ are both at most 0.0234.

Many other interesting results and discussions in [CJ23] are not mentioned here. For those who are interested, we recommend looking at it.

2. Counting elliptic curves with torsion points and local conditions

When we count the elliptic curves containing a torsion group G, we divide G into the two classes. Let

$$\mathcal{G}_{\leq 4}:=\{\mathbb{Z}/2\mathbb{Z},\mathbb{Z}/3\mathbb{Z},\mathbb{Z}/4\mathbb{Z},\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\}$$

and $\mathcal{G}_{\geq 5}$ be the set of torsion groups of order ≥ 5. For simplicity, we focus on the case when G is in $\mathcal{G}_{\leq 4}$. Let us recall the result of [GT12, Theorem 1.1], which says that $E_{A,B} : y^2 = x^3 + Ax + B$ for $A, B \in \mathbb{Z}$ has a G as a torsion subgroup if and only if

$$(A, B) = \Phi_G(a, b)$$

for some $a, b \in \mathbb{Z}$, where $\Phi_G = (f_G, g_G)$ for

$$\begin{array}{ll} f_2(a,b) = a, & g_2(a,b) = b^3 + ab, \\ f_3(a,b) = 6ab + 27a^4, & g_3(a,b) = b^2 - 27a^6, \\ f_4(a,b) = -3a^2 + 6ab^2 - 2b^4, & g_4(a,b) = (2a - b^2)(a^2 + 2ab^2 - b^4), \\ f_{2\times 2}(a,b) = -(a^2 + 3b^2)/4, & g_{2\times 2}(a,b) = (b^3 - a^2 b)/4. \end{array} \tag{1}$$

The set

$$\mathcal{E}(X) = \left\{ (A,B) \in \mathbb{Z}^2 : \begin{array}{c} |A| \leq X^{\frac{1}{3}}, |B| \leq X^{\frac{1}{2}}, 4A^3 + 27B^2 \neq 0, \\ \text{if } p^4 \text{ divides } A, \text{ then } p^6 \text{ does not divide } B. \end{array} \right\}$$

parametrizes all elliptic curves $E_{A,B}$ whose height is less than X, and each isomorphism class appears only once by the minimality condition. (i.e. there is no prime p such that $p^4 \mid A$ and $p^6 \mid B$.)

We define a height $h(A, B)$ of an integer pair (A, B) by $\max(|A|^3, |B|^2)$. Let

$$\begin{aligned} M_G(X) &= \left\{ (a,b) \in \mathbb{Z}^2 : (a,b) = 1, h(\Phi_G(a,b)) \leq X \right\}, \\ R_G(X) &= \left\{ (a,b) \in \mathbb{R}^2 : |f_G(a,b)| \leq X^{\frac{1}{3}}, |g_G(a,b)| \leq X^{\frac{1}{2}} \right\}, \\ \mathcal{D}_G(X) &= \left\{ (A,B) \in \mathbb{Z}^2 : (A,B) = \Phi_G(a,b) \text{ for some } (a,b) \in R_G(X) \cap \mathbb{Z}^2 \right\}, \\ \mathcal{M}_G(X) &= \left\{ (A,B) \in \mathcal{D}_G(X) : \text{ if } p^4 \mid A, \text{ then } p^6 \nmid B \right\}, \end{aligned}$$

and

$$\begin{aligned} \mathcal{E}_G(X) &= \left\{ (A,B) \in \mathcal{M}_G(X) : 4A^3 + 27B^2 \neq 0 \right\}, \\ \mathcal{S}_G(X) &= \left\{ (A,B) \in \mathcal{M}_G(X) : 4A^3 + 27B^2 = 0 \right\}, \end{aligned}$$

where $\mathcal{E}_G(X)$ represents elliptic curves with G torsion and $\mathcal{S}_G(X)$ takes up singular curves.

For the reader's convenience, it is good to remember that (a, b) denotes an element in the domain of Φ_G or R_G and (A, B) does in the range of Φ_G. Also, $\mathcal{D}_G, \mathcal{M}_G, \mathcal{E}_G$, and $\mathcal{S}_G$ are sets on the range side. For pairs $I, J \in (\mathbb{Z}/p\mathbb{Z})^2$, the subscripts $-_{G,I}(X)$ or $-_{G,J}(X)$ means that this is the subset of the original set consisting of elements $(a, b) \equiv I \pmod p$ or $(A, B) \equiv J \pmod p$ respectively. We often drop the subscript G to ease the notation.

Lemma 2.1. *For a torsion subgroup G, the number of integer points in $R_G(X)$ is*

$$\mathrm{Area}(R_G(1)) X^{\frac{1}{d(G)}} + O(X^{\frac{1}{e(G)}}).$$

Proof. We note that [HS14, Lemma 5.2] proves this lemma for $G = \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$. Since $f_4(a, b) = X^{\frac{1}{3}}, g_4(a, b) = X^{\frac{1}{2}}$ are equivalent to $f_4(a/X^{\frac{1}{6}}, b/X^{\frac{1}{12}}) = 1, g_4(a/X^{\frac{1}{6}}, b/X^{\frac{1}{12}}) = 1$, by change of variables we have

$$\mathrm{Area}(R_4(X)) = X^{\frac{1}{4}} \mathrm{Area}(R_4(1)).$$

Then, the claim follows from the Principle of Lipschitz, [HS14, (5.3)] since $X^{\frac{1}{e(G)}}$ is the longer length of the projection of $R_G(X)$ to the axes. The same idea works for $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

By the Principle of Lipschitz, we have

Corollary 2.2. *For a prime $p \geq 5$, I an element in $(\mathbb{Z}/p\mathbb{Z})^2$, and a torsion subgroup G, we have*

$$|R_{G,I}(X)| = \mathrm{Area}(R_G(1))p^{-2}X^{\frac{1}{d(G)}} + O(1 + p^{-1}X^{\frac{1}{e(G)}}).$$

The map Φ_G is not one-to-one. We prove some elementary but not simple properties of Φ_G. We put

(2)

G	$\{0\}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	G in $\mathcal{G}_{\geq 5}$
$e(G)$	2	3	4	6	6	$2d(G)$

Lemma 2.3. *For a group G in $\mathcal{G}_{\leq 4}$, there is a positive integer $r(G)$ such that the number of the preimages of Φ_G is $r(G)$ except for $O(X^{\frac{1}{e(G)}})$ points.*

Proof. We show the case of $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. For a given $(A, B) = \left(-\frac{a^2+3b^2}{4}, \frac{b^3-ba^2}{4}\right)$, we find all the pairs (a', b') such that

$$\left(-\frac{a^2+3b^2}{4}, \frac{b^3-ba^2}{4}\right) = \left(-\frac{a'^2+3b'^2}{4}, \frac{b'^3-b'a'^2}{4}\right),$$

and

$$\left\{\frac{a+b}{2}, \frac{b-a}{2}, -b\right\} = \left\{\frac{a'+b'}{2}, \frac{b'-a'}{2}, -b'\right\}.$$

Since A and B are integers, a and b should have the same parity. The set equality determines six pairs (a', b') and all the pairs satisfy the first relation. Hence, (a', b') has the same image as (a, b) if and only if one of the following six linear systems holds

$$\begin{pmatrix} a' \\ b' \end{pmatrix} = A_i \begin{pmatrix} a \\ b \end{pmatrix},$$

for $A_0 = I$, and

$$A_1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} \frac{1}{2} & -\frac{3}{2} \\ -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}, A_3 = \begin{pmatrix} -\frac{1}{2} & \frac{3}{2} \\ -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}, A_4 = \begin{pmatrix} \frac{1}{2} & \frac{3}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix}, A_5 = \begin{pmatrix} -\frac{1}{2} & -\frac{3}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix}.$$

Consequently, for (a, b) satisfying $a \equiv b \pmod 2$, the (not necessarily distinct) six points

$$(a, b), (-a, b), \left(\frac{a-3b}{2}, \frac{-a-b}{2}\right), \left(\frac{-a+3b}{2}, \frac{-a-b}{2}\right), \left(\frac{a+3b}{2}, \frac{a-b}{2}\right), \text{ and } \left(\frac{-a-3b}{2}, \frac{a-b}{2}\right)$$

corresponds to the same (A, B). We find a domain for the representatives for the above (not necessarily distinct) six points. □

For $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we consider only the pairs (a, b) with $a \equiv b \pmod 2$. By Lemma 2.1, Lemma 2.3, and Möbius inversion argument, we have the following corollary, which is a complement of [HS14, Theorem 5.6].

Corollary 2.4. *For a group G in $\mathcal{G}_{\leq 4}$ and $r(G)$ defined in Lemma 2.3, let*

$$c(G) := \frac{\mathrm{Area}(R_G(1))}{2^{\delta_{G=2\times 2}} r(G)\zeta(\frac{12}{d(G)})}.$$

Then,

$$|\mathcal{E}_G(X)| = c(G)X^{\frac{1}{d(G)}} + O(X^{\frac{1}{e(G)}}).$$

Similarly, we can count elliptic curves $E_{A,B}$ in $\mathcal{E}(X)$ satisfying the local restriction $(A,B) \equiv J \pmod p$. Let $W_{G,J}$ be the set of pairs $I \in (\mathbb{Z}/p\mathbb{Z})^2$ with $(f_G, g_G)(I) \equiv J$ modulo p.

Proposition 2.5. *For a prime $p \geq 5$, a non-zero pair $J \in (\mathbb{Z}/p\mathbb{Z})^2$ and a group G in $\mathcal{G}_{\leq 4}$, we have*

$$|\mathcal{E}_{G,J}(X)| = c(G)\frac{|W_{G,J}|}{p^2}\frac{p^{\frac{12}{d(G)}}}{p^{\frac{12}{d(G)}}-1}X^{\frac{1}{d(G)}} + O(p^{-1}X^{\frac{1}{e(G)}} + X^{\frac{1}{12}}).$$

For $J = (0,0)$, we have

$$|\mathcal{E}_{G,J}(X)| = c(G)\left(\frac{1}{p^2} - \frac{1}{p^{\frac{12}{d(G)}}}\right)\frac{p^{\frac{12}{d(G)}}}{p^{\frac{12}{d(G)}}-1}X^{\frac{1}{d(G)}} + O(pX^{\frac{1}{e(G)}} + p^2X^{\frac{1}{12}}).$$

3. Moments of traces of the Frobenius

We define a class number weighted by $|W_{G,J}|$.

Definition. We define

$$H_G(a,p) := \sum_{\substack{J=(A,B)\in(\mathbb{Z}/p\mathbb{Z})^2 \\ a_p(E_J)=a \\ 4A^3+27B^2\not\equiv 0 \pmod p}} |W_{G,J}|, \tag{3}$$

where $a_p(E)$ is the trace of the Frobenius of an elliptic curve E at p.

We claim that the following relations are true.

$$\sum_{|a|<2\sqrt{p}} H_G(a,p) = p^2 + O_G(p), \tag{4}$$

$$\sum_{|a|<2\sqrt{p}} aH_G(a,p) = O_G(p^{\frac{3}{2}}), \tag{5}$$

$$\sum_{|a|<2\sqrt{p}} a^2H_G(a,p) = p^3 + O_G(p^{\frac{5}{2}}). \tag{6}$$

We remark that (4) holds for all torsion groups. In [CJ23], we were able to show that the equations (5) and (6) holds when torsion group G is small, for example, when $|G| \leq 6$. (See Proposition 3.2.) The primary tool was the Eichler–Selberg trace formula [KP17]. We introduce some notations first. The Chebyshev polynomials of the second kind are defined as

$$U_0(t) = 1, \quad U_1(t) = 2t, \quad U_{j+1}(t) = 2tU_j(t) - U_{j-1}(t).$$

We define normalized Chebyshev polynomials to be

$$U_{k-2}(t,q) := q^{k/2-1}U_{k-2}\left(\frac{t}{2\sqrt{q}}\right) = \frac{\alpha^{k-1}-\overline{\alpha}^{k-1}}{\alpha-\overline{\alpha}} \in \mathbb{Z}[q,t],$$

where $\alpha, \overline{\alpha}$ are the two roots in $\mathbb{C}$ of $X^2 - tX + q = 0$. Let

$$C_{R,j} := \begin{cases} a_{\frac{R}{2},j} & \text{if } R \text{ is even} \\ a_{\frac{R-1}{2},j} + a_{\frac{R-1}{2},j-1} & \text{if } R \text{ is odd} \end{cases} \qquad \text{for } a_{R,j} := \binom{2R}{j} - \binom{2R}{j-1}$$

be the Chebyshev coefficients. We have

$$t^R = \sum_{j=0}^{\lfloor R/2 \rfloor} C_{R,j} q^j U_{R-2j}(t,q)$$

which is [KP17, (1.3)]. In particular, we have

$$t^0 = U_0(t,q), \quad t = U_1(t,q), \quad t^2 = U_2(t,q) + qU_0(t,q). \tag{7}$$

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ with q elements, $\mathfrak{C}$ be the set of all the isomorphism classes of elliptic curves over $\mathbb{F}_q$. Let A denote a finite abelian group and let Φ_A be

$$\Phi_A(E) = \begin{cases} 1 & \text{if there exists an injective homomorphism } A \hookrightarrow E(\mathbb{F}_p) \\ 0 & \text{otherwise.} \end{cases}$$

We define

$$\mathbb{E}_q(a^R\Phi_A) := \frac{1}{q} \sum_{\substack{E \in \mathfrak{C} \\ A \hookrightarrow E(\mathbb{F}_q)}} \frac{a_q(E)^R}{|\mathrm{Aut}_{\mathbb{F}_q}(E)|}.$$

From now on, we assume that $q = p$. For a finite abelian group A, let $n_1 = n_1(A)$ and $n_2 = n_2(A)$ be its first and second invariant factors, respectively. We denote $\psi(n) = n\prod_{p|n}(1+1/p)$, $\varphi(n) = n\prod_{p|n}(1-1/p)$ and $\phi(n) = n\prod_{p|n}(-\varphi(p))$.

For $\lambda \mid (p-1, n_1)$, let

$$T_{n_1,\lambda}(p,1) := \frac{\psi(n_1^2/\lambda^2)\varphi(n_1/\lambda)}{\psi(n_1^2)}(-T_{\mathrm{trace}} - T_{\mathrm{hyp}} + T_{\mathrm{dual}}),$$

with

$$T_{\mathrm{trace}} := \frac{1}{\varphi(n_1)}\,\mathrm{Tr}(T_p | S_k(\Gamma(n_1,\lambda))),$$

$$T_{\mathrm{hyp}} := \frac{1}{4}\sum_{i=0}^{1}\sum_{\substack{\tau | n_1\lambda \\ g | p-1}} \frac{\varphi(g)\varphi(n_1(n_1(\lambda,g)/g)}{\varphi(n_1)}\left(\delta_{n_1(\lambda,g)/g}(y_i,1) + (-1)^k\delta_{n_1(\lambda,g)/g}(y_i,-1)\right),$$

$$T_{\mathrm{dual}} := \frac{p+1}{\varphi(n_1)}\delta(k,2),$$

where $g = (\tau, n_1\lambda/\tau)$, y_i is the unique element of $(\mathbb{Z}/(n_1\lambda/g)\mathbb{Z})^\times$ such that $y_i \equiv p^i \pmod{\tau}$ and $y_i \equiv p^{1-i} \pmod{n_1\lambda/\tau}$, $\delta(a,b)$ is the indicator function of $a = b$, and $\delta_c(a,b)$ is the indicator function of the congruence $a \equiv b \pmod{c}$.

Theorem 3.1. [KP17, Theorem 3, when $q = p$] *Let A be a finite abelian group of rank at most 2. Suppose $(p, |A|) = 1$ and $k \geq 2$. If $p \equiv 1 \pmod{n_2(A)}$ we have*

$$\mathbb{E}_p(U_{k-2}(t,p)\Phi_A) = \frac{1}{\varphi(n_1/n_2)} \sum_{\nu \mid \frac{(p-1,n_1)}{n_2}} \phi(\nu) T_{n_1, n_2\nu}(p,1) \tag{8}$$

and if $p \not\equiv 1 \pmod{n_2(A)}$, then $\mathbb{E}_p(U_{k-2}(t,p)\Phi_A) = 0$.

Using Theorem 3.1, we show

Proposition 3.2. *Let G be one of the groups $\mathbb{Z}/n\mathbb{Z}$ for $2 \leq n \leq 6$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$. Then, the moment conditions (5) and (6) hold.*

Proof. For each group G, we denote n_1 be its first invariant factor. We define $A_{G,i}$ be abelian groups satisfying $G \leq A_{G,i} \leq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1\mathbb{Z}$, and $j < i$ if and only if $A_{G,j} < A_{G,i}$. We define $\widetilde{\omega}_{G,i}$ to be $|W_{G,I}|$ if $E_I[n_1](\mathbb{F}_p) \cong A_{G,i}$. Let

$$\omega_{G,i} := \widetilde{\omega}_{G,i} - \sum_{j<i} \omega_{G,j}.$$

Then, one can obtain that

$$\sum_{|a|<2\sqrt{p}} a^R H_G(a,p) = p(p-1) \sum_i \omega_{G,i} \mathbb{E}_p(a^R \Phi_{A_{G,i}}).$$

By (4),

$$\sum_i \omega_{G,i} \mathbb{E}_p(\Phi_{A_{G,i}}) = 1 + O\left(\frac{1}{p}\right). \tag{9}$$

Since $t^2 = U_2(t,p) + pU_0(t,p)$, we have the identity

$$\mathbb{E}_p(t^2\Phi_A) = \mathbb{E}_p(U_2(t,p)\Phi_A) + p\mathbb{E}_p(U_0(t,p)\Phi_A),$$

and this together with (9) implies

$$\sum_{|a|<2\sqrt{p}} a^2 H_G(a,p) = p(p-1)(p+O(1)) + O(p^{2.5}) = p^3 + O(p^{2.5})$$

because $\mathbb{E}_p(U_2(t,p)\Phi_A) \ll_G \frac{p^{1.5}}{p} \ll_G p^{0.5}$ by Theorem 3.1 and the Deligne bound.

Using the identity $t = U_1(t,p)$ and $\mathbb{E}_p(U_1(t,p)\Phi_A) \ll_G p^{-0.5}$, it is easy to see that

$$\sum_{|a|<2\sqrt{p}} a H_G(a,p) = O_G(p^{1.5})$$

by Theorem 3.1 and the Deligne bound. □

When $G = \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we can obtain the $2R+1$-th moments.

Proposition 3.3. *For $G = \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we have*

$$\sum_{|a|<2\sqrt{p}} a^{2R+1} H_G(a,p) = 0$$

for $R \geq 0$.

Proposition 3.3 will be used for the Frobenius trace formula for elliptic curves in Section 4.

4. Proofs of the Main Theorems

4.1. **Proof of Theorem 1.** Let ϕ be an even non-negative Schwartz class function with its Fourier transform $\widehat{\phi}$ compactly supported. Let γ_E denote the imaginary part of a non-trivial zero $\rho_E = \frac{1}{2} + i\gamma_E$ of an elliptic curve L-function $L(s, E)$. By the explicit formula [RS, Proposition 2.1] and Ogg's formula [CJ, §4] we have

$$\begin{aligned}\frac{1}{|\mathcal{E}_G(X)|}\sum_{E\in\mathcal{E}_G(X)}\sum_{\gamma_E}\phi\left(\gamma_E\frac{\log X}{2\pi}\right) &= \frac{\widehat{\phi}(0)}{|\mathcal{E}_G(X)|}\sum_{E\in\mathcal{E}_G(X)}\frac{\log N_E}{\log X} + \frac{2}{\pi}\int_{-\infty}^{\infty}\phi\left(\frac{\log X\cdot r}{2\pi}\right)\mathrm{Re}\,\frac{\Gamma_E'}{\Gamma_E}(\frac{1}{2}+ir)dr \\ &\quad - \frac{2}{\log X\,|\mathcal{E}_G(X)|}\sum_{n=1}^{\infty}\frac{\Lambda(n)}{\sqrt{n}}\widehat{\phi}\left(\frac{\log n}{\log X}\right)\sum_{E\in\mathcal{E}_G(X)}\hat{a}_E(n) \\ &\le \widehat{\phi}(0) - \frac{2}{\log X\,|\mathcal{E}_G(X)|}\sum_{n=1}^{\infty}\frac{\Lambda(n)}{\sqrt{n}}\widehat{\phi}\left(\frac{\log n}{\log X}\right)\sum_{E\in\mathcal{E}_G(X)}\hat{a}_E(n) + O\left(\frac{1}{\log X}\right) \\ &\le \widehat{\phi}(0) - S_1 - S_2 + O\left(\frac{1}{\log X}\right),\end{aligned}$$

where

$$S_1 = \frac{2}{\log X\,|\mathcal{E}_G(X)|}\sum_{p}\frac{\log p}{\sqrt{p}}\widehat{\phi}\left(\frac{\log p}{\log X}\right)\sum_{E\in\mathcal{E}_G(X)}\hat{a}_E(p),$$

$$S_2 = \frac{2}{\log X\,|\mathcal{E}_G(X)|}\sum_{p}\frac{\log p}{p}\widehat{\phi}\left(\frac{2\log p}{\log X}\right)\sum_{E\in\mathcal{E}_G(X)}\hat{a}_E(p^2),$$

and $\hat{a}_E(n)$'s come from the logarithmic derivative of $L(s, E)$

$$-\frac{L'}{L}(s, E) = \sum_{n=1}^{\infty}\frac{\hat{a}_E(n)\Lambda(n)}{n^s}.$$

From now on, for a positive constant σ, we specify the test function ϕ and $\widehat{\phi}$:

$$\widehat{\phi}(u) = \frac{1}{2}\left(\frac{1}{2}\sigma - \frac{1}{2}|u|\right) \text{ for } |u|\le\sigma, \quad \text{and} \quad \phi(x) = \frac{\sin^2(2\pi\frac{1}{2}\sigma x)}{(2\pi x)^2}.$$

Note that $\phi(0) = \frac{\sigma^2}{4}$ and $\widehat{\phi}_n(0) = \frac{\sigma}{4}$.

If we show

$$-S_1 - S_2 = \frac{1}{2}\phi(0) + o(1), \tag{10}$$

by the positivity of ϕ, we have

$$\frac{1}{|\mathcal{E}_G(X)|}\sum_{E\in\mathcal{E}_G(X)} r_E \le \frac{1}{2} + \frac{\widehat{\phi}(0)}{\phi(0)} + o(1) \le \frac{1}{2} + \frac{1}{\sigma} + o(1). \tag{11}$$

Hence, it is left to show that (10) holds for each torsion group G with some explicit σ. For this purpose, we need the following lemmas.

Lemma 4.1. *For $G = \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$,*

$$\sum_{E\in\mathcal{E}_G(X)}\hat{a}_E(p) \ll p^{-1}X^{\frac{1}{d(G)}} + pX^{\frac{1}{e(G)}} + p^2X^{\frac{1}{12}}.$$

Lemma 4.2. *For $G = \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$,*

$$\sum_{E\in\mathcal{E}_G(X)} \hat{a}_E(p^2) = -c(G)X^{\frac{1}{d(G)}} + O\left(p^{-\frac{1}{2}}X^{\frac{1}{d(G)}} + pX^{\frac{1}{e(G)}} + p^2X^{\frac{1}{12}}\right).$$

By Lemma 4.1, for $G = \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$,

$$\begin{aligned} S_1 &\ll \frac{1}{\log X}\sum_p \frac{\log p}{\sqrt{p}}\widehat{\phi}\left(\frac{\log p}{\log X}\right)\left(\frac{1}{p} + pX^{\frac{1}{e(G)}-\frac{1}{d(G)}} + p^2X^{\frac{1}{12}-\frac{1}{d(G)}}\right) \\ &\ll X^{-\frac{1}{d(G)}}\sum_{p\le X^\sigma}\left(p^{\frac{1}{2}}\log pX^{\frac{1}{e(G)}} + p^{\frac{3}{2}}\log pX^{\frac{1}{12}}\right) \ll X^{-\frac{1}{d(G)}}\left(X^{\frac{1}{e(G)}+\frac{3\sigma}{2}} + X^{\frac{1}{12}+\frac{5\sigma}{2}}\right). \end{aligned} \tag{12}$$

By Lemma 4.2, for $G = \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$,

$$\begin{aligned} S_2 &= \frac{2}{\log X}\sum_p \frac{\log p}{p}\widehat{\phi}\left(\frac{2\log p}{\log X}\right)\left(-1 + O\left(p^{-\frac{1}{2}} + pX^{\frac{1}{e(G)}-\frac{1}{d(G)}} + p^2X^{\frac{1}{12}-\frac{1}{d(G)}}\right)\right) \\ &= -\frac{2}{\log X}\sum_p \frac{\log p}{p}\widehat{\phi}\left(\frac{2\log p}{\log X}\right) + O\left(\sum_{p\le X^{\frac{\sigma}{2}}} \log pX^{\frac{1}{e(G)}-\frac{1}{d(G)}} + p\log pX^{\frac{1}{12}-\frac{1}{d(G)}}\right) \\ &= -\frac{1}{2}\phi(0) + O\left(X^{\frac{1}{e(G)}-\frac{1}{d(G)}+\frac{\sigma}{2}} + X^{\frac{1}{12}-\frac{1}{d(G)}+\sigma}\right). \end{aligned}$$

From our computation, if we take $\sigma = \frac{1}{18}, \frac{1}{18}$, and $\frac{1}{5d(G)}$ for $G = \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ and G in $\mathcal{G}_{\ge 5}$ respectively then (10) and (11) hold. Therefore, the average analytic ranks for $G = \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ are bounded by 18.5. For the case for $G = \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, we omit the proof.

4.2. **Proof of Theorem 2.** This section assumes that $G = \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. In Theorem 2, we claim that there are not so many elliptic curves in $\mathcal{E}_G$ with large ranks. We need two technical propositions. For their proof, the following trace formula is required.

Theorem 4.3. *[Frobenius Trace Formula for Elliptic Curves] Let $G = \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, k be a fixed positive integer. Assume $e_i = 1$ or 2, r_i is odd or 2 if $e_i = 1$, and $r_i = 1$ if $e_i = 2$ for $i = 1,\dots,k$. Then,*

$$\begin{aligned} \sum_{E\in\mathcal{E}_G(X)} \widehat{a_E}(p_1^{e_1})^{r_1}\widehat{a_E}(p_2^{e_2})^{r_2}\cdots\widehat{a_E}(p_k^{e_k})^{r_k} &= c\frac{c(G)}{\zeta(12/d(G))}X^{\frac{1}{d(G)}} + O_k\left(\left(\sum_{i=1}^k\frac{1}{p_i}\right)X^{\frac{1}{d(G)}}\right) \\ &\quad + O_k\left(\left(\prod_{i=1}^k p_i\right)X^{\frac{1}{e(G)}} + \left(\prod_{i=1}^k p_i\right)^2X^{\frac{1}{12}}\right) \end{aligned}$$

where

$$c = \begin{cases} 0 & \text{if } e_j = 1 \text{ and } r_j \text{ is odd for some } j, \\ -1 & \text{if } r_j = 2 \text{ for all } j \text{ with } e_j = 1, \text{ and the number of } j\text{'s with } e_j = 2 \text{ is odd}, \\ 1 & \text{otherwise.} \end{cases}$$

and the first error term exists only if $e_i = 1$ and $r_i = 2$ or $e_i = 2$ for all i.

Let γ_E denote the imaginary part of a non-trivial zero of $L(s,E)$. We index them using the natural order in real numbers:

$$\cdots \gamma_{E,-3} \le \gamma_{E,-2} \le \gamma_{E,-1} \le \gamma_{E,0} \le \gamma_{E,1} \le \gamma_{E,2} \le \gamma_{E,3} \cdots$$

if analytic rank r_E is odd,

$$\cdots \gamma_{E,-3} \le \gamma_{E,-2} \le \gamma_{E,-1} \le 0 \le \gamma_{E,1} \le \gamma_{E,2} \le \gamma_{E,3} \cdots$$

otherwise.

We specify the test function for Weil's explicit formula as follows.

$$\widehat{\phi}_n(u) = \frac{1}{2}\left(\frac{1}{2}\sigma_n - \frac{1}{2}|u|\right) \text{ for } |u| \le \sigma_n, \quad \text{and} \quad \phi_n(x) = \frac{\sin^2(2\pi\frac{1}{2}\sigma_n x)}{(2\pi x)^2}.$$

Note that $\phi_n(0) = \frac{\sigma_n^2}{4}$, $\widehat{\phi}_n(0) = \frac{\sigma_n}{4}$ and

$$\int_{\mathbb{R}} |u|\widehat{\phi}_n(u)^2 du = \frac{1}{6}\phi_n(0)^2. \tag{13}$$

We prove the following two propositions using the Frobenius trace formula (Theorem 4.3).

Proposition 4.4. *Let $\widehat{\phi}_n$ be as above with $\sigma_n = \frac{1}{9n}$ and $\frac{1}{10n}$ for $G = \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ respectively. Then, we have*

$$\sum_{E\in\mathcal{E}_G(X)} \sum_{m_{i_1}m_{i_2}\cdots m_{i_k}\neq\square} \frac{\Lambda(m_{i_1})\cdots\Lambda(m_{i_k})\widehat{a}_E(m_{i_1})\cdots\widehat{a}_E(m_{i_k})}{\sqrt{m_{i_1}m_{i_2}\cdots m_{i_k}}} \widehat{\phi}_n\left(\frac{\log m_{i_1}}{\log X}\right)\cdots\widehat{\phi}_n\left(\frac{\log m_{i_k}}{\log X}\right)$$
$$\ll |\mathcal{E}_G(X)|.$$

Proposition 4.5. *Let $\widehat{\phi}_n$ be as above with $\sigma_n = \frac{1}{9n}$ and $\frac{1}{10n}$ for $G = \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ respectively. For a subset $S = \{i_1, i_2, \ldots, i_k\}$ of $\{1, 2, \ldots, n\}$,*

$$\frac{1}{|\mathcal{E}_G(X)|}\left(\frac{-2}{\log X}\right)^{|S|} \sum_{E\in\mathcal{E}_G(X)} \sum_{m_{i_1}m_{i_2}\cdots m_{i_k}=\square} \left(\prod_{j=1}^{|S|} \frac{\Lambda(m_{i_j})\widehat{a}_E(m_{i_j})}{\sqrt{m_{i_j}}}\widehat{\phi}_n\left(\frac{\log m_{i_j}}{\log X}\right)\right)$$
$$= \sum_{\substack{S_2\subset S \\ |S_2| even}} \left(\frac{1}{2}\phi_n(0)\right)^{|S_2^c|} |S_2|! \left(\int_{\mathbb{R}} |u|\widehat{\phi}_n(u)^2 du\right)^{\frac{|S_2|}{2}} + O\left(\frac{1}{\log X}\right).$$

Now, let's prove Theorem 2. By Weil's explicit formula, we have

$$r_E\phi_{2n}(0) \le \widehat{\phi}_{2n}(0) - \frac{2}{\log X}\sum_{m_i} \frac{\widehat{a}_E(m_i)\Lambda(m_i)}{\sqrt{m_i}}\widehat{\phi}_{2n}\left(\frac{\log m_i}{\log X}\right) + O\left(\frac{1}{\log X}\right),$$

hence

$$r_E \le \frac{1}{\sigma_{2n}} + \frac{4}{\sigma_{2n}^2}\left(-\frac{2}{\log X}\sum_{m_i} \frac{\widehat{a}_E(m_i)\Lambda(m_i)}{\sqrt{m_i}}\widehat{\phi}_{2n}\left(\frac{\log m_i}{\log X}\right)\right) + O\left(\frac{1}{\sigma_{2n}^2\log X}\right).$$

Now assume that $r_E \ge \frac{1+C}{\sigma_{2n}}$ with some positive constant C. Then, for sufficiently large X,

$$-\frac{2}{\log X}\sum_{m_i} \frac{\widehat{a}_E(m_i)\Lambda(m_i)}{\sqrt{m_i}}\widehat{\phi}_{2n}\left(\frac{\log m_i}{\log X}\right) \ge \frac{C\sigma_{2n}}{4}.$$

Therefore,

$$\left|\{E \in \mathcal{E}_G(X) | r_E \geq \frac{1+C}{\sigma_{2n}}\}\right| \left(\frac{C\sigma_{2n}}{4}\right)^{2n} \leq \sum_{E \in \mathcal{E}_G(X)} \left(-\frac{2}{\log X} \sum_{m_i} \frac{\widehat{a}_E(m_i)\Lambda(m_i)}{\sqrt{m_i}} \widehat{\phi}_{2n}\left(\frac{\log m_i}{\log X}\right)\right)^{2n}$$

$$\leq \left(\frac{\sigma_{2n}^2}{4}\right)^{2n} \sum_{S_2 \subset \{1,2,3,\ldots,2n\}} \left(\frac{1}{2}\right)^{|S_2^c|} |S_2|! \left(\frac{1}{6}\right)^{\frac{|S_2|}{2}} |\mathcal{E}_G(X)| + O\left(\frac{X^{\frac{1}{d(G)}}}{\log X}\right)$$

where the second inequality is justified by Proposition 4.4 and Proposition 4.5, and Theorem 2 follows.

References

[Bru92] A. Brumer, The average rank of elliptic curves I, *Invent. Math.* **109** (1992), no. 3, pp.445–472. 1

[CJ] P. J. Cho, K. Jeong, On the distribution of analytic ranks of elliptic curves, preprint. 8

[CJ23] The average analytic rank of elliptic curves with prescribed torsion. J. London Math. Soc., 107: 616-657. https://doi.org/10.1112/jlms.12693 1, 2, 5

[GT12] I. Gracía-Selfa, J. M. Tornero, A complete Diophantine characterization of the rational torsion of an elliptic curve. *Acta Math. Sin. (Engl. Ser.)* **28** (2012), no. 1, pp.83–96. 3

[HS14] R. Harron, A. Snowden, Counting elliptic curves with prescribed torsion, *J. Reine Angew. Math.* **729** (2017), pp.151–170. 1, 3, 4

[Hea04] D. R. Heath-Brown, The average analytic rank of elliptic curves, *Duke Math. J.* **122** (2004), no. 3, pp.591–623. 1

[KP17] N. Kaplan, I. Petrow, Elliptic curves over a finite field and the trace formula, *Proc. Lond. Math. Soc.* (3) **115** (2017), no. 6, pp.1317–1372. 5, 6, 7

[RS] Z. Rudnick, P. Sarnak, Zeros of principal L-functions and random matrix theory. *Duke Math. J.* **81** (1996), no. 2, 269–322. 8

[You06] M. P. Young, Low-lying zeros of families of elliptic curves, *J. Amer. Math. Soc.* **19** (2006), no. 1, pp.205–250. 1

Department of Mathematical Sciences, Ulsan National Institute of Science and Technology, UNIST-gil 50, Ulsan 44919, Korea

Email address: petercho@unist.ac.kr