The average analytic rank of elliptic curves with prescribed torsion

Peter J. Cho 1  |  Keunyoung Jeong 2

1Department of Mathematical Sciences, Ulsan National Institute of Science and Technology, Ulsan, Korea
2Department of Mathematics Education, Chonnam National University, Gwangju, Korea

Correspondence
Peter J. Cho, Department of Mathematical Sciences, Ulsan National Institute of Science and Technology, UNIST-gil 50, Ulsan 44919, Korea.
Email: petercho@unist.ac.kr

Funding information
NRF, Grant/Award Numbers: 2019R1F1A1062599, 2019R1C1C1004264;
NRF, Basic Science Research Program, Grant/Award Number: 2020R1A4A1016649

Abstract
We show that the average analytic rank of elliptic curves with prescribed torsion $G$ is bounded for every torsion group $G$ under Generalized Riemann Hypothesis (GRH) for elliptic curve $L$-functions and, in addition, some moment conditions for $G = \mathbb{Z}/n\mathbb{Z}$, $n = 7, 8, 9, 10, 12$, and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$, $m = 3, 4$.

MSC 2020
11G05, 11M26 (primary), 11F72 (secondary)

1  |  INTRODUCTION

The distribution of (algebraic or analytic) ranks of elliptic curves defined over $\mathbb{Q}$ is one of the fascinating problems in number theory. One of the important features of the distribution is the average rank of elliptic curves. 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 $4A^3 + 27B^2 \neq 0$

$$E_{A,B} : y^2 = x^3 + Ax + B$$

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. There is a natural bijection 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 is widely believed that the following conjecture initially proposed by Goldfeld \[10\] would be true.

**Conjecture 1** (Minimalist conjecture). The proportions of elliptic curves with rank 0 and elliptic curves with rank 1 are both \( \frac{1}{2} \).

Recently, Park, Poonen, Voight, and Wood \[17\] have brought out a more refined conjecture \( \dagger \) which not only claims Conjecture 1 but also proposes the number of elliptic curves with algebraic rank \( r \) for \( 1 \leq r \leq 20 \).

**Conjecture 2** \[17, Corollary 7.2.6, Theorem 7.3.3\].

1. The proportion of elliptic curves with algebraic rank 0 and elliptic curves with algebraic rank 1 are both \( \frac{1}{2} \).
2. There are only finitely many elliptic curves with algebraic rank \( > 21 \).
3. For \( 1 \leq r \leq 20 \), the number of elliptic curves over \( \mathbb{Q} \) with algebraic rank \( \geq r \) and height \( \leq X \) is \( X^{-\frac{21r}{24} + o(1)} \).

Bhargava and Shankar \[2, 3\] made a breakthrough for Conjecture 1. They showed that the proportion of elliptic curves with algebraic rank \( \leq 1 \) is at least 0.8375, and with algebraic rank 0 is at least 0.2062. For the average analytic rank, Brumer \[4\] showed that it is bounded by 2.3 under Generalized Riemann Hypothesis (GRH) for elliptic curve \( L \)-functions. This bound was lowered to 2 and \( \frac{25}{14} \) by Heath-Brown \[13\] and Young \[23\], respectively, under GRH for elliptic curve \( L \)-functions.

On the other hand, Harron and Snowden \[12\] 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 \( \mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} \) for \( n \in \{1, 2, \ldots, 10, 12\} \) and \( m \in \{1, 2, 3, 4\} \). Let

\[
G_{\leq 4} := \{ \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \}
\]

and \( G_{\geq 5} \) be the set of torsion groups of order \( \geq 5 \). We remark that elliptic curves with torsion \( G \) in \( G_{\geq 5} \) can be parametrized by Tate’s normal form (see §2). 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

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

\( \dagger \) We note that Conjecture 2 is also suggested by \[21, 22\] through another heuristic method.


**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     |

Harron and Snowden showed that

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

where the constant $d(G)$ is given in Table 1. Furthermore, for $G = \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$, they obtained the cardinality of $\mathcal{E}_G(X)$ with a power-saving error term. We remark that Table 1 by Harron and Snowden implies that 100% of the elliptic curves in $\mathcal{E}_G$ has the torsion $G$ exactly.

Not much is known about the distribution of (algebraic or analytic) ranks of elliptic curves with prescribed torsion group $G$. In [17, §8.3], they give an upper bound of algebraic ranks of elliptic curves in $\mathcal{E}_G$ but do not give a statement on the distribution of ranks in $\mathcal{E}_G$ other than this. In their preprint, Bhargava and Ho [1, Theorem 1.1] obtained bounds for the average algebraic rank of the families of elliptic curves with marked torsion point $(0,0)$ of orders 2 and 3, respectively, which are $7/6$ and $3/2$. 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 (9), (10). 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 $\frac{1}{2} + 5d(G)$.

We remark that the moment conditions (9), (10) are verified in Proposition 2.8 when $|G| \leq 6$ and $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Furthermore, Theorem 1 remains true when we replace $\mathcal{E}_G$ by the set of elliptic curves with torsion $G$ exactly since the analytic rank of an elliptic curve is bounded by the logarithm of its conductor [13] and the number of elliptic curves with $E(\mathbb{Q}) > G$ is negligible by Table 1.

We want to know not only the average analytic rank but also other information on the analytic ranks. Heath-Brown [13, Theorem 2] showed that there are not so many elliptic curves with large analytic ranks. Let $P(r_E \geq a)$ denote the proportion of elliptic curves with analytic rank $r_E \geq a$. He showed that, under GRH for elliptic curve $L$-functions,

$$P(r_E \geq a) \ll \left( \frac{5a}{2} \right)^{-\frac{a}{20}}.$$

We obtain an analogue of Heath–Brown [13, Theorem 2] for elliptic curves with torsion groups $G = \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. 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
The average analytic rank of elliptic curves with prescribed torsion

\( P_G(r_E \geq a) \) denote the proportion of elliptic curves with analytic rank \( r_E \geq a \) among the elliptic curves with torsion \( G \). We show that there are 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

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

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.

We also give an explicit bound on the \( n \)th moment of analytic ranks of elliptic curves with torsion \( G_i, i = 1, 2 \).

**Theorem 3.** Assume GRH for elliptic curve \( L \)-functions. For every positive integer \( n \), we have

\[
\limsup_{X \to \infty} \frac{1}{|E_{G_i}(X)|} \sum_{E \in \mathcal{E}_{G_i}(X)} r_E^n \leq \sum_S (9n)^{|S^c|} \sum_{S_2 \subseteq S} \left( \frac{1}{2} \right)^{|S^c|} |S_2|! \left( \frac{1}{6} \right)^{|S^c|},
\]

where \( S \) runs over subsets of \( \{1, 2, 3, \ldots, n\} \), and \( S_2 \) runs over subsets of even cardinality of the set \( S \). In particular, the average analytic rank of \( \mathcal{E}_{G_1} \) and that of \( \mathcal{E}_{G_2} \) are at most 9.5 and 10.5, respectively.

Our rank results are obtained from the computation of one-level (or \( n \)-level) density for the family of elliptic \( L \)-functions arising from \( \mathcal{E}_G \). Katz and Sarnak’s philosophy claims that the one-level density holds for a test function with any compact support, and this philosophy, combined with our results, implies that the average analytic rank over \( \mathcal{E}_G \) for any \( G \) is bounded by \( \frac{1}{2} \). Since it is widely believed that the root numbers are evenly distributed in \( \mathcal{E}_G \), our one-level density results give small evidence for the following folklore conjecture.

**Conjecture 3.** Let \( G \) be a torsion group. The proportion of elliptic curves with rank 0 in \( \mathcal{E}_G \) and the proportion of elliptic curves with rank 1 in \( \mathcal{E}_G \) are both \( \frac{1}{2} \).

For some numerical data for \( G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \), we refer to a result of Chan, Hanselman, and Li [5]. Young [23, §8] also computed bounds for average analytic rank for families of elliptic curves with some prescribed torsion \( G \) under not only GRH for elliptic curve \( L \)-functions but also GRH for Dirichlet \( L \)-functions and some other assumptions.

Our approach gives a systematic frame to compute the one-level density for any \( G \) using a version of Eichler–Selberg trace formula by Kaplan and Petrow [15]. This version of Eichler–Selberg trace formula is indispensable for dealing with every torsion group \( G \). However, we need to count elliptic curves satisfying a local condition to bound the average rank. A local condition at prime \( p \) is a property of an elliptic curve \( E \) when reduced modulo \( p \). For example, we say that an elliptic curve \( E \) satisfies a local condition good, mult, addi, or \( a \) at a prime \( p \) if its reduction modulo \( p \) has good reduction, multiplicative reduction, additive reduction, or \( a_E(p) = p + 1 - |E(F_p)| = a \), respectively. For torsion groups \( G \) in \( \mathcal{G}_{\leq 4} \), we have the following.
Theorem 4 (Theorem 3.7). For a prime $p \geq 5$, a local condition $\mathcal{L}C$, and a group $G$ in $G_{\leq 4}$,

$$|E_{G,p}(X)| = c(G) \cdot c_{G,\mathcal{L}C}(p) \cdot \frac{p^{12} X^{\frac{1}{12}}}{p^{\frac{1}{12}}} + O(h_{G,\mathcal{L}C}(p, X)),$$

where $c_{G,\mathcal{L}C}(p)$ is a constant depending on $G, p$, and $\mathcal{L}C$, and $h_{G,\mathcal{L}C}(p, X)$ is a function whose order of magnitude is less than $pX^{\frac{1}{e(G)}} + p^2X^{\frac{1}{12}}$ for some $e(G) > d(G)$. The constant $e(G)$ is given in the table (6).

For torsion groups $G$ in $G_{\geq 5}$, we obtain Theorem 3.9, an analog of Theorem 4, based on the work of [7] which computes the cardinality of $E_G(X)$. As a result of Theorem 4 and Theorem 3.9, there are many interesting phenomena. One of our motivations in this article was to compare the probability for a local condition under no prescribed torsion with that for the local condition under prescribed torsion.

Corollary 5. For $p \geq 5$, $\mathcal{L}C \in \{\text{good}, \text{mult}, a\}$ and a torsion group $G$, we have

$$\lim_{X \to \infty} \frac{|E_{G,p}(X)|}{|E(X)|} \neq \lim_{X \to \infty} \frac{|E_{G,\mathcal{L}C}(X)|}{|E_G(X)|}.$$

In other words, the three local conditions above and torsion $G$ are not independent.

The constant $c_{G,\mathcal{L}C}(p)$ is essentially the probability for an elliptic curve with torsion $G$ to satisfy $\mathcal{L}C$ at $p$. When $\mathcal{L}C = \text{mult}$, we can give an interesting interpretation of $c_{G,\mathcal{L}C}(p)$.

Corollary 6 (Corollary 3.11). Let $p$ be a prime $\geq 5$ and $G$ be a group in $G_{\leq 4}$. Then, $c_{G,\text{mult}}(p)$ is proportional to the ratio of the number of the cusps of corresponding modular curve $X_1(N)$ and $X(2)$. For a group $G$ in $G_{\geq 5}$, there is a set of primes $p$ of positive density such that $c_{G,\text{mult}}(p)$ is proportional to the number of cusps of corresponding modular curves.

We recommend seeing Corollary 3.11 to Corollary 3.13 for details and other examples.

2  |  LOCAL DENSITY AND THE MOMENTS OF CLASS NUMBERS

2.1  |  Model

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

$$G_{\leq 4} := \{\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\}$$

and $G_{\geq 5}$ be the set of torsion groups of order $\geq 5$. 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.

For each torsion subgroup, we should clarify the model we use. When $G$ in $G_{\leq 4}$, we recall that the result of [11, Theorem 1.1] shows 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
\[
\begin{align*}
f_2(a, b) &= a, & g_2(a, b) &= b^3 + ab, \\
f_3(a, b) &= 6ab + 27a^4, & g_3(a, b) &= b^2 - 27a^6, \\
f_4(a, b) &= -3a^2 + 6ab^2 - 2b^4, & g_4(a, b) &= (2a - b^2)(a^2 + 2ab^2 - b^4), \\
f_{2 \times 2}(a, b) &= -(a^2 + 3b^2)/4, & g_{2 \times 2}(a, b) &= (b^3 - a^2b)/4. 
\end{align*}
\]

We recall that the set
\[
\mathcal{E}(X) = \left\{ (A, B) \in \mathbb{Z}^2 : |A| \leq X^{\frac{3}{2}}, |B| \leq X^{\frac{1}{2}}, 4A^3 + 27B^2 \neq 0, \text{ if } p^4 \text{ divides } A, \text{ then } p^6 \text{ does not divide } B. \right\}
\]

which parametrizes all elliptic curves \(E_{A,B}\) whose height is less than \(X\), and each isomorphism class appears only once by the minimality condition. (That is, there is no prime \(p\) such that \(p^4 \mid A\) and \(p^6 \mid B\).) When \(G\) is in \(G_{4,4}\), the set
\[
\mathcal{E}_G(X) = \{(A, B) \in \mathcal{E}(X) : (A, B) = \Phi_G(a, b) \text{ for some } a, b \in \mathbb{Z}\}
\]
parametrizes all elliptic curves with prescribed torsion subgroup \(G\).

For a group \(G\) in \(G_{5,5}\), we use Tate’s normal form
\[
E(u, v) : y^2 + (1 - v)xy - uy = x^3 - ux^2,
\]
which parametrizes all elliptic curves with prescribed torsion subgroup \(G\) of order \(\geq 4\). For each \(G\), parameters \(u\) and \(v\) can be expressed as a rational function of one variable \(t\). It can be summarized as follows: (for example, [14, Table 3])

| \(G\)   | \(u(t)\)   | \(v(t)\)   |
|--------|-------------|-------------|
| \(\mathbb{Z}/4\mathbb{Z}\) | \(t\)       | 0           |
| \(\mathbb{Z}/5\mathbb{Z}\) | \(t\)       | \(t\)       |
| \(\mathbb{Z}/6\mathbb{Z}\) | \(t + t^2\) | \(t\)       |
| \(\mathbb{Z}/7\mathbb{Z}\) | \(t^3 - t^2\) | \(t^2 - t\) |
| \(\mathbb{Z}/8\mathbb{Z}\) | \((2t - 1)(t - 1)\) | \((2t - 1)(t - 1)/t\) |
| \(\mathbb{Z}/9\mathbb{Z}\) | \(t^2(t - 1)(t^2 - t + 1)\) | \(t^2(t - 1)\) |
| \(\mathbb{Z}/10\mathbb{Z}\) | \(t^3(2t - 1)(t - 1)/(-t^2 + 3t - 1)^2\) | \(t(2t - 1)(t - 1)/(-t^2 + 3t - 1)\) |
| \(\mathbb{Z}/12\mathbb{Z}\) | \((3t^2 - 3t + 1)(t - 2t^2)(2t - 2t^2 - 1)/(t - 1)^4\) | \((3t^2 - 3t + 1)(t - 2t^2)/(t - 1)^3\) |
| \(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}\) | \(t^2 - 1/16\) | 0           |
| \(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}\) | \(v(t) + v(t)^2\) | \((10 - 2t)/(t^2 - 9)\) |
| \(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}\) | \((2t + 1)(8t^2 + 4t + 1)/(8t^2 - 1)^2\) | \((2t + 1)(8t^2 + 4t + 1)/(2t(4t + 1)(8t^2 - 1))\) |

For each torsion subgroup \(G\), we first obtain an equation over \(\mathbb{Z}[t]\) by clearing the denominator of each coefficient. After that we take the usual coordinate change and obtain an equation of the form \(y^2 = x^3 + f_G(t)x + g_G(t)\). For \(t = \frac{a}{b}\), the homogenization \(f_G(a, b) = b^{\deg f} f_G(a/b)\) and \(g_G(a, b) = b^{\deg g} g_G(a/b)\) of \(f_G\) and \(g_G\) and change of coordinate give...
\[ y^2 = x^3 + f_G(a, b)x + g_G(a, b). \] 

Since \( f_{2\times4}(a, 4b)/8^4, g_{2\times4}(a, 4b)/8^6 \), and \( f_{2\times6}(a + 3b, b), g_{2\times6}(a + 3b, b) \) represent all isomorphism classes of elliptic curves with the corresponding torsion, we use them for \( f_{2\times4}, g_{2\times4}, f_{2\times6}, g_{2\times6} \), respectively. In Appendix A, the table for \( f_G \) and \( g_G \) is provided for readers’ convenience.

For any torsion subgroup \( G \) in \( \mathcal{G}_{\geq 5} \) we have \( 3 \deg f_G = 2 \deg g_G \), and we define \( d(G) \) as

\[ 3 \deg f_G = 2 \deg g_G = 2d(G). \]

Note that \( d(G) \) coincides with \( d(G) \) given in the Table 1.

On the other hand, it is very crucial to recognize that the set

\[ \{(A, B) \in \mathcal{E}(X) : (A, B) = (f_G, g_G)(a, b) \text{ for some } a, b \in \mathbb{Z}\} \]

might not parametrize all isomorphism classes of elliptic curves with torsion subgroup \( G \) in \( \mathcal{G}_{\geq 5} \). The reason is as follows: The Tate normal form parametrizes all isomorphism classes of elliptic curves with prescribed torsion, but to parametrize all the curves, we need to consider all \( t \in \mathbb{Q} \), in other words, all relatively prime integer pairs \( (a, b) \). But if there is an integer \( e > 1 \) such that \( e^4 | f_G(a, b) \) and \( e^6 | g_G(a, b) \), then the minimal elliptic curve isomorphic to \( E_{f_G(a, b), g_G(a, b)} \) may not appear in the above set since it is removed by the minimality condition.

The problem is that the map \((f_G, g_G)\) does not care about the minimality condition. Following [7, Theorem 3.3.1], we define the defect of \((a, b)\) to be

\[ e(a, b) = e = \max_{e^4 | f_G(a, b), e^6 | g_G(a, b)} e'. \]

We slightly modify the definition of \( \Phi_G \) as follows:

\[ \Phi_G(a, b) = \left( \frac{f_G(a, b)}{e^4}, \frac{g_G(a, b)}{e^6} \right), \]

where \( e \) is the defect of \((a, b)\). We remark that the image of \( \Phi_G \) satisfies the minimality condition, so

\[ \mathcal{E}_G(X) = \{(A, B) \in \mathcal{E}(X) : (A, B) = \Phi_G(a, b) \text{ for relatively prime integers } a, b\} \]

parametrizes all isomorphism classes of elliptic curves with torsion subgroup \( G \). We define a height of an integer pair \((A, B)\) by \( \max(|A|^3, |B|^2) \) and

\[ M_G(X) = \{(a, b) \in \mathbb{Z}^2 : (a, b) = 1, h(\Phi_G(a, b)) \leq X\}. \]

Hence \( \Phi_G \) is a map from \( \mathbb{Z}^2 \) to \( \mathbb{Z}^2 \) when \( G \) is in \( \mathcal{G}_{\leq 4} \), and from the set of the pairs of relatively prime integers to \( \mathbb{Z}^2 \) when \( G \) is in \( \mathcal{G}_{\geq 5} \).

Also, we define \( M_G^e(X) \) as the subset of \( M_G(X) \) of elements with defect \( e \). Now we compute all defects for the torsion groups \( G \), except \( G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \) and \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \).

**Lemma 2.1.** Let \( G \) be a group in \( \mathcal{G}_{\geq 5} \setminus \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}\} \), and let \( e \) be the defect of a relatively prime integer pair \((a, b)\). Then, the defect \( e(a, b) \) is 1, 2, 3, or 6. Explicitly, we have
(i) $e$ has a prime divisor 2 if and only if
- $G = \mathbb{Z}/6\mathbb{Z}$ and $(a, b) \equiv (1, 1) \pmod{2}$ or,
- $G = \mathbb{Z}/8\mathbb{Z}$ and $(a, b) \equiv (1, 0) \pmod{2}$ or,
- $G = \mathbb{Z}/10\mathbb{Z}$ and $(a, b) \equiv (1, 0) \pmod{2}$ or,
- $G = \mathbb{Z}/12\mathbb{Z}$ and $(a, b) \equiv (1, 0) \pmod{2}$ or,
- $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and $(a, b) \equiv (1, 1) \pmod{2}$;
(ii) $e$ has a prime divisor 3 if and only if
- $G = \mathbb{Z}/7\mathbb{Z}$ and $(a, b) \equiv (1, 2)$ or $(2, 1) \pmod{3}$ or,
- $G = \mathbb{Z}/9\mathbb{Z}$ and $(a, b) \equiv (1, 2)$ or $(2, 1) \pmod{3}$ or,
- $G = \mathbb{Z}/12\mathbb{Z}$, $a \not\equiv 0$, and $b \equiv 0 \pmod{3}$.

**Proof.** By the argument [7, p. 17], the defect $e$ is a divisor of the least common multiplier of the two resultants $\text{Res}(f_G(a, 1), g_G(a, 1))$ and $\text{Res}(f_G(1, b), g_G(1, b))$. Sagemath [19] gives

| $G$ | lcm of resultants | $G$ | lcm of resultants |
|-----|-------------------|-----|-------------------|
| $\mathbb{Z}/5\mathbb{Z}$ | $2^{16}3^{15}5$ | $\mathbb{Z}/10\mathbb{Z}$ | $2^{72}3^{108}5^3$ |
| $\mathbb{Z}/6\mathbb{Z}$ | $-2^{24}3^{19}$ | $\mathbb{Z}/12\mathbb{Z}$ | $2^{96}3^{156}$ |
| $\mathbb{Z}/7\mathbb{Z}$ | $-2^{32}3^{27}7$ | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ | $2^{24}3^{36}$ |
| $\mathbb{Z}/8\mathbb{Z}$ | $2^{48}3^{22}$ | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ | $2^{192}3^{78}$ |
| $\mathbb{Z}/9\mathbb{Z}$ | $-2^{48}3^{117}$ | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ | $2^{576}3^{144}$ |

Hence any prime divisor of $e$ should divide $6|G|$.

First, for each prime divisor $p$ of $6|G|$, we find all the pairs $(a, b) \in (\mathbb{Z}/p^6\mathbb{Z})^2$ such that
- $a, b$ are relatively prime to $p$,
- $p^4 \mid f_G(a, b)$ and $p^6 \mid g_G(a, b)$.

Then, there is no such pair $(a, b)$ except for the following four cases:
- when $G = \mathbb{Z}/6\mathbb{Z}$ and $(a, b) \equiv (1, 1) \pmod{2}$, 2 exactly divides $e$;
- when $G = \mathbb{Z}/7\mathbb{Z}$ and $(a, b) \equiv (1, 2)$ or $(2, 1) \pmod{3}$, 3 exactly divides $e$;
- when $G = \mathbb{Z}/9\mathbb{Z}$ and $(a, b) \equiv (1, 2)$ or $(2, 1) \pmod{3}$, 3 exactly divides $e$;
- when $G = \mathbb{Z}/12\mathbb{Z}$, $a \not\equiv 0$, and $b \equiv 0 \pmod{3}$.

Now, we consider the pairs $(a, b)$ for which only one of $a$ and $b$ is a multiple of $p$. When $G = \mathbb{Z}/5\mathbb{Z}$ and $p = 2$, if only one of the $a$ or $b$ is divided by 2, then $2^4$ does not divide $f_5(a, b)$ because the coefficients of $a^4$ and $b^4$ are not divided by $2^4$. Hence we can conclude that 2 does not divide the defect $e$ for arbitrary $(a, b)$. Considering the coefficients of $f_G$ and $g_G$ (see Appendix A), the same argument shows that the possible prime divisors of defect are (with the previous four cases):
- when $G = \mathbb{Z}/8\mathbb{Z}$ and $(a, b) \equiv (1, 0) \pmod{2}$, 2 divides $e$;
- when $G = \mathbb{Z}/10\mathbb{Z}$ and $(a, b) \equiv (1, 0) \pmod{2}$, 2 divides $e$;
- when $G = \mathbb{Z}/12\mathbb{Z}$ and $(a, b) \equiv (1, 0) \pmod{2}$, 2 divides $e$;
- when $G = \mathbb{Z}/12\mathbb{Z}$, $a \not\equiv 0$, and $b \equiv 0 \pmod{3}$, 3 divides $e$.

For the first three cases we can check that there is no $(a, b) \in (\mathbb{Z}/2^6\mathbb{Z})^2$ such that $2^5 \mid f_G(a, b)$ and $2^6 \mid g_G(a, b)$, which implies that $2^5 \nmid e$. Similarly for the fourth case, we can check that there is no $(a, b) \in (\mathbb{Z}/3^6\mathbb{Z})^2$ such that $3^6 \mid f_G(a, b)$ and $3^6 \mid g_G(a, b)$.

□
Remark 1. We note that one may calculate the defects for the remaining two groups by following the proof of Lemma 2.1. For example for $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ when $a \equiv 0 \pmod{4}$ and $b \equiv 1 \pmod{2}$, $2^2$ exactly divides $e(a, b)$ and when $a \equiv 2 \pmod{4}$ and $b \equiv 1 \pmod{2}$, $2^3$ divides $e(a, b)$. It seems like the defect is $2^4$, but we need more computing power to check it. So, we omit $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ cases.

2.2 Weights for local conditions

We define a weight for a local condition as the number of preimages of $(f_G, g_G)$ modulo $p$.

**Definition.** For a prime $p \geq 5$ and a pair $J \in (\mathbb{Z}/p\mathbb{Z})^2$, let $W_{G, J}$ be the set of pairs $I \in (\mathbb{Z}/p\mathbb{Z})^2$ with $(f_G, g_G)(I) \equiv J \pmod{p}$.

For a given $J$, $|W_{G, J}|$ is morally a weight to determine the number of elliptic curves $E$ with mod $p$ reduction $E_J$ and $E(\mathbb{Q})_{\text{tor}} \geq G$. By the definition of $W_{G, J}$, the identity

$$\sum_{J \in (\mathbb{Z}/p\mathbb{Z})^2} |W_{G, J}| = p^2$$

follows directly.

**Proposition 2.2.** For a prime $p \geq 5$, the sums of $|W_{G, J}|$ over $J = (A, B) \in \mathbb{F}_p^2$ satisfying $4A^3 + 27B^2 \equiv 0 \pmod{p}$ are summarized as follows:

| $G$ | $p$ | $\Sigma |W_{G, J}|$ | $G$ | $p$ | $\Sigma |W_{G, J}|$ |
|-----|-----|-----------------|-----|-----|-----------------|
| $\mathbb{Z}/2\mathbb{Z}$ | $\cdot$ | $2p - 1$ | $\mathbb{Z}/9\mathbb{Z}$ | $1 \pmod{3}$, $y_9 \in (\mathbb{F}_p^\times)^3$ | $8p - 7$ |
| $\mathbb{Z}/3\mathbb{Z}$ | $\cdot$ | $2p - 1$ | $\mathbb{Z}/9\mathbb{Z}$ | $1 \pmod{3}$, $y_9 \notin (\mathbb{F}_p^\times)^3$ | $5p - 4$ |
| $\mathbb{Z}/4\mathbb{Z}$ | $\cdot$ | $3p - 2$ | $\mathbb{Z}/9\mathbb{Z}$ | $2 \pmod{3}$, $y_9 \in (\mathbb{F}_p[\sqrt{-3}]^\times)^3$ | $6p - 5$ |
| $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ | $\cdot$ | $3p - 2$ | $\mathbb{Z}/9\mathbb{Z}$ | $2 \pmod{3}$, $y_9 \notin (\mathbb{F}_p[\sqrt{-3}]^\times)^3$ | $3p - 2$ |
| $\mathbb{Z}/5\mathbb{Z}$ | $\pm 1 \pmod{5}$ | $4p - 3$ | $\mathbb{Z}/10\mathbb{Z}$ | $\pm 1 \pmod{5}$ | $8p - 7$ |
| $\mathbb{Z}/5\mathbb{Z}$ | $\pm 2 \pmod{5}$ | $2p - 1$ | $\mathbb{Z}/10\mathbb{Z}$ | $\pm 2 \pmod{5}$ | $4p - 3$ |
| $\mathbb{Z}/6\mathbb{Z}$ | $\cdot$ | $4p - 3$ | $\mathbb{Z}/12\mathbb{Z}$ | $1 \pmod{12}$ | $10p - 9$ |
| $\mathbb{Z}/7\mathbb{Z}$ | $\gamma_7 \in (\mathbb{F}_p[\sqrt{-3}]^\times)^3$ | $6p - 5$ | $\mathbb{Z}/12\mathbb{Z}$ | $5, 7, 11 \pmod{12}$ | $6p - 5$ |
| $\mathbb{Z}/7\mathbb{Z}$ | $\gamma_7 \notin (\mathbb{F}_p[\sqrt{-3}]^\times)^3$ | $3p - 2$ | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ | $\cdot$ | $4p - 3$ |
| $\mathbb{Z}/8\mathbb{Z}$ | $\pm 1 \pmod{8}$ | $6p - 5$ | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ | $\cdot$ | $6p - 5$ |
| $\mathbb{Z}/8\mathbb{Z}$ | $\pm 3 \pmod{8}$ | $4p - 3$ | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ | $1 \pmod{8}, \geq 11$ | $10p - 9$ |
| $\mathbb{Z}/8\mathbb{Z}$ | $\cdot$ | $7 \pmod{8}, \geq 11$ | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ | $\cdot$ | $8p - 7$ |
| $\mathbb{Z}/8\mathbb{Z}$ | $\cdot$ | $5 \pmod{8}, \geq 11$ | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ | $\cdot$ | $6p - 5$ |
| $\mathbb{Z}/8\mathbb{Z}$ | $\cdot$ | $3 \pmod{8}, \geq 11$ | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ | $\cdot$ | $4p - 3$ |

where $\gamma_7 = 4(637 + 147\sqrt{-3})$ and $\gamma_9 = 4(-9 \pm 3\sqrt{-3})$. Here $\cdot$ means that there is no condition on $p$. Furthermore, we have
\[
\sum_{\alpha=a^2 \in (\mathbb{Z}/p\mathbb{Z})^\times} |W_{3,(-3\alpha^2,2\alpha^3)}| = \begin{cases} 
2(p-1) & \text{for } p \equiv 1 \mod 12, \\
(p-1) & \text{for } p \equiv 5 \text{ or } 11 \mod 12, \\
0 & \text{for } p \equiv 7 \mod 12.
\end{cases}
\] (5)

Proof. We note that for \( p \geq 5 \), the pair \( I = (0,0) \) in \((\mathbb{Z}/p\mathbb{Z})^2\) is the only pair such that \((f_G, g_G)(I) \equiv (0,0) \) (mod \( p \)). For the groups \( G \) in \( G_{\leq 4} \), one can directly check the sum \( \sum |W_{G,I}| \). We show the case of \( G = \mathbb{Z}/3\mathbb{Z} \). We parametrize \((A, B)\) satisfying \(4A^3 + 27B^2 \equiv 0\) \((\mod \mathbb{Z}/p\mathbb{Z})\) for \( \alpha \in \mathbb{Z}/p\mathbb{Z} \).

Directly solving the equations \(\Phi_G(a, b) = (A, B)\), we know that \( |W_{3,(A,B)}| \) is equal to the number of distinct zeros of the polynomial
\[
h(x) = h_{A,B}(x) = 3^5 \cdot x^8 + 2 \cdot 3^3 \cdot A \cdot x^4 + 2^2 \cdot 3^2 \cdot B \cdot x^2 - A^2,
\]
when \( A \neq 0 \). Since \( h_{-3\alpha^2,2\alpha^3}(x) \) is factored into
\[
3^5\left(x^2 - \frac{\alpha}{3}\right)^3 (x^2 + \alpha),
\]
the number of distinct zeros of \( h_{-3\alpha^2,2\alpha^3}(x) \) is 4 if \(-\alpha\) and \( \alpha/3 \) are both quadratic residues modulo \( p \), 2 if either \(-\alpha\) or \( \alpha/3 \) is a quadratic residue, and 0 if neither \(-\alpha\) nor \( \alpha/3 \) is a quadratic residue. From this observation, it is easy to see that the sum of distinct zeros of \( h_{-3\alpha^2,2\alpha^3}(x) \) over \( \alpha \in \mathbb{Z}/p\mathbb{Z} \) is \( 2(p-1) + 1 = 2p - 1 \). If \( p \equiv 1 \) (mod 12), \(-1\) and \(3\) are both quadratic residues modulo \( p \). Hence, the sum of \( |W_{3,(-3\alpha^2,2\alpha^3)}| \) over quadratic residues \( \alpha \) in \( \mathbb{Z}/p\mathbb{Z} \) is equal to the sum of \( |W_{3,(-3\alpha^2,2\alpha^3)}| \) over all non-zero residues \( \alpha \) in \( \mathbb{Z}/p\mathbb{Z} \). By the similar argument, we can check the other two cases in Equation (5).

Now we treat the case that \( G \) are in \( G_{>5} \). Let \((a, b)\) be a pair such that \( 4f_{G}(a, b)^3 + 27g_{G}(a, b)^2 \equiv 0 \) (mod \( p \)). Then, \((a, b)\) determines \( \alpha \) in \( \mathbb{Z}/p\mathbb{Z} \) satisfying \((f_G, g_G)(a, b) \equiv (-3\alpha^2, 2\alpha^3)\). Hence, if we find all such pairs \((a, b)\) (including the \((0,0)\) pair), then the number of the pairs is the sum we want to know. We will consider the discriminant of \( E_{(f_G(a,b),g_G(a,b))} \), instead of \((f_G, g_G)(a, b)\).

Let \( \Delta_G(a, b) \) be the discriminant of \( E_{(f_G, g_G)(a,b)} \). Then, we have the following table.

| \( G \) | \( \Delta_G(a,b) \) |
|---|---|
| \( \mathbb{Z}/5\mathbb{Z} \) | \(2^{12}3^{12}a^5b^5(a^2 - 11ab - b^2)\) |
| \( \mathbb{Z}/6\mathbb{Z} \) | \(2^{12}3^{12}a^6b^2(9a + b)(a + b)^3\) |
| \( \mathbb{Z}/7\mathbb{Z} \) | \(\begin{cases} 2^{12}3^{12}a^8b^2(a - b)^8(a^3 - 8a^2b + 5ab^2 + b^3) & \text{for } \alpha \equiv 3, 6 \mod 7 \\
2^{12}3^{12}a^8b^2(-2a + b)^8(-a + b)^8(8a^2 - 8ab + b^2) & \text{for } \alpha \equiv 2, 4 \mod 7
\end{cases}\) |
| \( \mathbb{Z}/9\mathbb{Z} \) | \(\begin{cases} 2^{12}3^{12}a^9b^9(a - b)^9(a^2 - 3ab + b^2)^3(a^3 - 6a^2b + 3ab^2 + b^3) & \text{for } \alpha \equiv 3, 6 \mod 9 \\
2^{12}3^{12}a^9b^9(-a + b)^9(-a + b)^9(a^2 - 3ab + b^2)^3 & \text{for } \alpha \equiv 2, 4 \mod 9
\end{cases}\) |
| \( \mathbb{Z}/10\mathbb{Z} \) | \(\begin{cases} 2^{12}3^{12}a^5b^5(-a + b)^5(-a + b)^{10}(-4a^2 + 2ab + b^2)(a^2 - 3ab + b^2)^2 & \text{for } \alpha \equiv 3, 6 \mod 10 \\
2^{12}3^{12}a^5b^5(-a + b)^5(-a + b)^{10}(-a + b)^{12}(6a^2 - 6ab + b^2)(2a^2 - 2ab + b^2)^3 & \text{for } \alpha \equiv 2, 4 \mod 10
\end{cases}\) |
| \( \mathbb{Z}/12\mathbb{Z} \) | \(\begin{cases} 2^{12}3^{12}a^2b^2(-2a + b)^2(-a + b)^2(-4a^2 + 2ab + b^2)(a^2 - 3ab + b^2)^4 & \text{for } \alpha \equiv 3, 6 \mod 12 \\
2^{12}3^{12}a^2b^2(-a + b)^2(-a + b)^2(2a^2 - 2ab + b^2)^3 & \text{for } \alpha \equiv 2, 4 \mod 12
\end{cases}\) |
| \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \) | \(2^{12}3^{12}b^2a^2(a - b)^4(a + b)^4\) |
| \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \) | \(2^{12}3^{12}a^4(a - 6b)^2(a + 6b)^2b^8(a - 2b)^6(a + 2b)^6\) |
| \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \) | \(2^{20}3^{12}b^8a^8(8a^2 - b^2)^8(2a^2 + 4ab + b^2)^4\) |
First, let us treat the cases where $\Delta_G(a, b)$ is a product of linear polynomials and quadratic polynomials. For example, consider

$$\Delta_8(a, b) = 2^{12}3^{12}a^8b^2(-2a + b)^4(-a + b)^8(8a^2 - 8ab + b^2).$$

So in this case we have four types of $(a, b)$ satisfying the condition which are $a = 0, b = 0, 2a/b = 1, a/b = 1$, and $a/b$ is a zero of the quadratic polynomial $8t^2 - 8t + 1$. The first four cases give $4(p - 1)$ pairs, and the quadratic polynomial has two zeros in $\mathbb{F}_p$ when $p \equiv 1, 7 \pmod{8}$. Since the values of $8t^2 - 8t + 1$ at $t = 1$ and $1/2$ are $1$ and $-1$, respectively, there is no overlap among those solutions. Hence we verified the case of $G = \mathbb{Z}/8\mathbb{Z}$. The other cases can be handled similarly.

Let us verify the cases where $\Delta_G(a, b)$ contains a cubic polynomial. For this purpose, we need the following lemma.

**Lemma 2.3.** Let $f(t) = t^3 + at + b$ be a polynomial over $\mathbb{F}_p$ with the discriminant $\Delta = (-4a^3 - 27b^2)$. The number of zeros (without multiplicity) of $f(t)$ is

1. zero if and only if $\Delta = 81\mu^2$ is a square and $(-b + \mu\sqrt{-3})/2$ is not a cube in the field $\mathbb{F}_p[\sqrt{-3}]$;
2. one if and only if $\Delta$ is a non-square;
3. two if and only if $\Delta$ is zero;
4. three, otherwise.

**Proof.** The first, second, and fourth statements are shown in [8] and the third one follows from the fact that a monic cubic which has two zeros and has no term of degree two is parametrized by $(t - 2a)(t + a)^2$.

When $G = \mathbb{Z}/7\mathbb{Z}$, $\Delta_G(a, b)$ contains the polynomial $(a^3 - 8a^2b + 5ab^2 + b^3)$. By change of coordinate, we have the polynomial $f(t) = (t^3 - \frac{49}{3}t - \frac{637}{27})$. The discriminant of the polynomial $f(t)$ is $2401 = 7^4$. So when $p > 7$, the number of zeros is one of 0 or 3. Also, $\mu = 49/9$ and the number of zeros is determined by $\frac{1}{2}(-\frac{637}{27} + \frac{49}{9}\sqrt{-3})$ which is equal to $4(-637 + 147\sqrt{-3})$ up to a cube. By Lemma 2.3, the number of zeros of $f(t)$ is zero or three whether $4(-637 + 147\sqrt{-3})$ is a cube or not in $\mathbb{F}_p[\sqrt{-3}]$.

Since the 0 or 1 is not a solution of $f(t)$, there is no overlap with the pairs $(a, b)$ from $t = 0$ or 1. We have verified the case $G = \mathbb{Z}/7\mathbb{Z}$. When $G = \mathbb{Z}/9\mathbb{Z}$, we can show the claim similarly.

We prove some elementary but not simple properties of $\Phi_G$. We put

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

**Lemma 2.4.** For a group $G$ in $G_{\leq 4}$, there is a positive integer $r(G)$ such that the number of the preimages of $\Phi_G$ is $r(G)$ except for $O(\sqrt{e(G)})$ points.

**Proof.** The cases of $G = \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are essentially shown in [12, Lemma 5.5] with $r(\mathbb{Z}/2\mathbb{Z}) = 1$ and $r(\mathbb{Z}/3\mathbb{Z}) = 2$. For $G = \mathbb{Z}/4\mathbb{Z}$, assume that there is a pair $(a', b') \neq (a, \pm b)$ such that

$$(−3a'^2 + 6ab^2 − 2b^4, (2a − b^2)(a^2 + 2ab^2 − b^4))$$

$$= (−3a^2 + 6a'b'^2 − 2b'^4, (2a' − b'^2)(a'^2 + 2a'b'^2 − b'^4)).$$
The average analytic rank of elliptic curves with prescribed torsion

The elliptic curve $E_{\Phi_4(a,b)}$ has a 4-torsion point $(a, b(-b^2 + 3a))$. Since an elliptic curve over rational numbers does not have $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ as a subgroup, $(a, b)$ and $(a', b')$ satisfy the relation

$$(a, b(-b^2 + 3a)) = (a', \pm b'(-b'^2 + 3a')).$$

If $b^2 \neq b'^2$, we obtain $bb' = 0$. Without loss of generality we may assume that $b' = 0$, then we have $3a = b^2$. Then, a 4-torsion point $(a, b(-b^2 + 3a))$ becomes a 2-torsion point, which is a contradiction. Therefore, we have $r(\mathbb{Z}/4\mathbb{Z}) = 2$.

Let $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. For a given $(A, B) = (-\frac{a^2 + 3b^2}{4}, -\frac{b^3 - ba^2}{4})$, 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 with $(a, b)$ 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

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

$$A_4 = \begin{pmatrix} \frac{1}{2} & \frac{3}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix}, \quad A_5 = \begin{pmatrix} -\frac{1}{2} & -\frac{3}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix}.$$

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

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

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

correspond to the same $(A, B)$. We find a domain for the representatives for the above (not necessarily distinct) six points. We claim that the following set

$$X = \left\{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a \geq 0, b \geq \frac{a}{3}, a \equiv b \pmod{2}\right\}$$

is the collection of all the representatives of the above (not necessarily distinct) six points. On the other hand, the number of points \((A, B)\) with the number of their preimages is strictly less than six is \(O(X^{\frac{1}{6}})\).

Hence, we showed the claim with \(r(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) = 6\). \(\square\)

For a group \(G\) in \(G_{\geq 5}\), we can prove an analogous statement using the argument of [7].

**Lemma 2.5.** For a group \(G\) in \(G_{\geq 5}\), there is an integer \(r(G)\) such that the preimages of \(\Phi_G\) are \(r(G)\) except for \(O(X^{\frac{1}{6}})\) points.

**Proof.** Essentially it is proved in the proof of [7, Theorem 3.3.1], so we give a sketch. For a group \(G\) in \(G_{\geq 5}\) and its corresponding congruence subgroup \(\Gamma\), there is a bijection between the set of \(\mathbb{Q}\)-isomorphism classes of elliptic curves with \(\Gamma\)-structure and rational points of the modular curve \(Y_\Gamma\) (see [7, Proposition 3.1.1]). By choosing a coordinate that defines an embedding \(Y_\Gamma \to \mathbb{A}^1_{\mathbb{Q}}\), the proof of [7, Theorem 3.3.1] gives a bijection from

\[
\left\{ (a, b) \in \mathbb{Z}^2 : \left| \frac{f_G(a, b)}{e^4} \right| \leq X^{\frac{1}{6}}, \left| \frac{g_G(a, b)}{e^6} \right| \leq X^{\frac{1}{2}}, (a, b) = 1 \right\}
\]

to the set of elliptic curves with \(\Gamma\)-structure whose heights are less than or equal to \(X\). Note that the elliptic curve in the latter set can be identified with a pair of integers in

\[
\left\{ (A, B) \in \mathbb{Z}^2 : (A, B) = \Phi_G(a, b), |A| \leq X^{\frac{1}{3}}, |B| \leq X^{\frac{1}{2}} \right\}.
\]

Now, the natural map which forgets \(\Gamma\)-structure is \(r(G)\)-to-one map (cf. [7, Lemma 3.1.8, Theorem 3.3.1, Step 4]) except for the curves with \(\Gamma'\)-structure for \(\Gamma' \subset \Gamma\) and curves whose \(j\)-invariants is 0 or 1728. The size of the set of these curves is negligible. The composition of the bijection and the natural forget map is \(\Phi_G\), hence the result follows. \(\square\)

Let \(J\) be an element in \(\mathbb{Z}/p\mathbb{Z}\) such that \(E_J\) is an elliptic curve and \(W_{G,J}\) is non-empty. Then for each \((a, b) \in W_{G,J}\) we have a change of coordinate from \(E(u, v)\) of the form (2) to \(E_J: y^2 = x^3 + f_G(a, b)x + g_G(a, b)\). Since the change of coordinate gives an isomorphism between the groups of \(\mathbb{F}_p\)-points, the image of \((0, 0)\) of \(E(u, v)\) also goes to a torsion point of maximal order. When \(G\) is cyclic, it defines a map \(\Psi_{G,J}: W_{G,J} \to E_J(\mathbb{F}_p)\) whose image is in the set of points of maximal order in \(G\).

**Lemma 2.6.** Let \(G\) be a group in \(G_{\leq 4}\), \(G = \mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}\), or \(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}\), and \(J \in \mathbb{Z}/p\mathbb{Z}\) for \(p \geq 5\) such that \(E_J\) is an elliptic curve. Then,

\[
E_J(\mathbb{F}_p) \geq G \quad \text{if and only if} \quad J = \Phi_G(a, b)
\]

for some \((a, b)\). Furthermore, \(|W_{G,J}|\) is the number of embedding of \(G\) into \(E_J(\mathbb{F}_p)\).

**Proof.** When \(G\) is in \(G_{\leq 4}\), we use the computation of [11] for the first statement. For example when \(G = \mathbb{Z}/4\mathbb{Z}\), assume that \((x_1, w_1)\) is a point of order 4 of an elliptic curve \(E_{AB}/\mathbb{F}_p\). From the
computation of the first coordinate of \([3](x_1, w_1) = (x_1, -w_1)\) for \(w_1 \neq 0\), we have

\[
B = \frac{1}{4} \left( 5x_1^3 - Ax_1 \pm \sqrt{(3x_1^2 - 2A)(A + 3x_1^2)^2} \right).
\]

Hence, \(B\) is in \(\mathbb{F}_p\) if and only if there exists \(x_2 \in \mathbb{F}_p\) such that \(3x_1^2 - 2A = x_2^2\). The computation of the second coordinate gives that \(w_2^2 = (3x_1 - x_2)(x_2 + 3x_1)^2/8\), so we have \(x_2 \neq 3x_1\) and there exists \(x_3 \in \mathbb{F}_p^\times\) such that \(3x_2^2 = (3x_1 - x_2)/2\). By the change of variables \(a = x_1\) and \(b = x_3\), we have \((A, B) = \Phi_4(a, b)\) with points of order 4, \((x_1, w_1) = (a, \pm b(-b^2 + 3a))\). For the converse, we know that \((a, \pm b(-b^2 + 3a))\) are points of order 4 of \(E_{\Phi_4(a, b)}\). The other cases with order \(\leq 4\) can be proved similarly, but we remark that the first equation of \([11, p. 92]\) should be

\[(−z_2, 0), \left( \frac{1}{2} \left( z_2 \pm \sqrt{z_2^2 - 4z_1} \right), 0 \right)\).

Now we prove the second statement when \(G\) is in \(\mathcal{G}_{\leq 4}\). When \(G\) is cyclic, it suffices to prove that \(\Psi_{G, J}\) is bijective with the set of the points of order \(|G|\) in \(E_J\). For example, when \(G = \mathbb{Z}/4\mathbb{Z}\), we note that for \(J = \Phi_4(a, b)\), the pair \((a, -b)\) also corresponds to the same \(J\) but they both induce the two points \((a, \pm b(-b^2 + 3a))\) of order 4. The proof above shows that for any point \((x_1, w_1)\) of order 4, there is a pair \((a, b) \in W_1\) such that \((x_1, w_1)\) is nothing but \((a, b(-b^2 + 3a))\). Hence, \(\Psi_{G, J}\) is surjective. For injectivity, we suppose \(\Phi_4(a', b') = (A, B)\) and \((a', b'(-b'^2 + 3a')) = (a, b(-b^2 + 3a))\). If \(b \neq b'\), then we have \(a = a'\) and \(bb' = 0\). Hence, one of the points \((a', b'(-b'^2 + 3a'))\) and \((a, b(-b^2 + 3a))\) is of order 2, which is a contradiction. Cases \(G = \mathbb{Z}/2\mathbb{Z}\) and \(\mathbb{Z}/3\mathbb{Z}\) can be treated similarly.

Next, we treat the case \(G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\). We recall that \(E_J\) has a \(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\) torsion if and only if \(J = (f_{2x2}(a, b), g_{2x2}(a, b))\). Hence if \(E_J\) does not have the full 2-torsion, then \(|W_{2x2,J}|\) should be zero. If \(E_J\) has the full 2-torsions, then \(b^3 + Ab + B \equiv 0 \pmod{p}\) has three zeros and \(A = f_{2x2}(a, b) = -(a^2 + 3b^2)/4\) for some \(a\). This \(a\) is not zero since if so, then \(f_{2x2}(0, b) = -3b^2/4\) and \(g_{2x2}(0, b) = b^3/4\), and this implies that \(4f_{2x2}(0, b)^3 + 27g_{2x2}(0, b)^2 \equiv 0 \pmod{p}\). Hence, there are precisely six pairs \((a, b)\) such that

\[b^3 + Ab + B \equiv 0, \quad 4A \equiv -(a^2 + 3b^2) \pmod{p}.
\]

Since this equation is equivalent to the system of the equations \(J = (f_{2x2}(a, b), g_{2x2}(a, b))\), we conclude that if \(E_J(\mathbb{F}_p) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\), then \(|W_{2x2,J}| = 6\).

When \(G = \mathbb{Z}/5\mathbb{Z}\), by taking homogenization and computing the multiples of the points, we know that the points

\[(3a^2 - 18ab + 3b^2, \pm 108ab^2), \quad (3a^2 + 18ab + 3b^2, \pm 108a^2b)
\]

are points of order 5 in \(E_J\) where \(J = \Phi_G(a, b)\). When the pair \((a, b)\) gives one of the four points above, then other three come from the pairs \((-b, a), (b, -a)\) and \((-a, -b)\).

We claim that the four pairs are all the pairs \((c, d)\) such that \(\Phi_5(c, d) = J\) and

\[3a^2 - 18ab + 3b^2 = 3c^2 - 18cd + 3d^2, \quad 3a^2 + 18ab + 3b^2 = 3c^2 + 18cd + 3d^2,
\]
or

\[3a^2 - 18ab + 3b^2 = 3c^2 + 18cd + 3d^2, \quad 3a^2 + 18ab + 3b^2 = 3c^2 - 18cd + 3d^2.\]

A straightforward computation shows that both systems do not generate new pairs. Therefore, \(\Psi_5\) is injective, and \(|W_{G, J}|\) is less than or equal to the number of points of order 5 in \(E_J\).

Let \(P\) be a point of order 5 in \(E_J(F_p)\) and \(E_J: y^2 = x^3 + Ax + B\). Let \(x_1\) and \(x_2\) be the \(x\)-coordinates of \(P\) and \(2P\). Then by the duplication formula, we have

\[
\frac{x_1^4 - 2Ax_1^2 - 8Bx_1 + A^2}{4(x_1^3 + Ax_1 + B)} = x_2, \quad \frac{x_2^4 - 2Ax_2^2 - 8Bx_2 + A^2}{4(x_2^3 + Ax_2 + B)} = x_1.
\]

From the identity above, we can see that \(2x_1 + x_2\) and \(x_1 + 2x_2\) are squares in \(F_p\). Let \(\sqrt{2x_1 + x_2}\) and \(\sqrt{x_1 + 2x_2}\) be one of the square roots of \(2x_1 + x_2\) and \(x_1 + 2x_2\), respectively. Then, by putting

\[
a = \frac{\sqrt{2x_1 + x_2} + \sqrt{x_1 + 2x_2}}{6}, \quad b = \frac{\sqrt{2x_1 + x_2} - \sqrt{x_1 + 2x_2}}{6},
\]

we have

\[
x_1 = 3a^2 + 18ab + 3b^2, \quad x_2 = 3a^2 - 18ab + 3b^2,
\]

and one can check easily that \(A = f_G(a, b)\) and \(B = g_G(a, b)\). Hence for the point \(P\) of order 5, we found \((a, b) \in W_J\) such that \(P = (3a^2 - 18ab + 3b^2, 108ab^2)\), which shows the surjectivity of \(\Psi_5\).

Now, we consider the \(\mathbb{Z}/6\mathbb{Z}\)-case. As we did in the \(\mathbb{Z}/5\mathbb{Z}\)-case, we can show that

\[(-9a^2 - 18ab + 3b^2, \pm(108a^2b + 108ab^2))\]

are points of order 6 in elliptic curve \(E_J\) where \(J = \Phi_6(a, b)\) for some \(a, b \in F_p\).

We claim that \((c, d) = \pm(a, b)\) are all the pair such that \(\Phi_6(a, b) = \Phi_6(c, d)\) and \(\Psi_6(a, b) = \Psi_6(c, d)\). Considering the \(x\)-coordinates of multiplies of the point \(\Psi_6(a, b)\) we have

\[-9a^2 - 18ab + 3b^2 = -9c^2 - 18cd + 3d^2, \quad 27a^2 + 18ab + 3b^2 = 27c^2 + 18cd + 3d^2, \quad -9a^2 + 18ab + 3b^2 = -9c^2 + 18cd + 3d^2,\]

since the \(x\)-coordinate of \(2P\) and \(3P\) is \(27a^2 + 18ab + 3b^2, -9a^2 + 18ab + 3b^2\), respectively. This system does not generate a new pair. Therefore \(\Psi_6\) is injective.

Let \(P := (x_1, y_1)\) be a point of order 6 of \(E_J(F_p)\) and let \((x_2, y_2) := 2P\), and \((x_3, 0) := 3P\). By the duplication formula, we know that \(2x_1 + x_2\) is a square. Since \(2P\) is a point of order 3, then \(J = \Phi_3(a_3, b_3)\) for some \(a_3, b_3 \in F_p\) and \((3a_3^2, \pm(9a_3^3 + b_3))\) are 3-torsion point of \(E_J\). Especially, we note that \(x_2/3\) is square in \(F_p\). Now, we define

\[
a := \frac{3\sqrt{x_2/3} + \sqrt{2x_1 + x_2}}{12}, \quad b := \frac{\sqrt{x_2/3} - \sqrt{2x_1 + x_2}}{4}.
\]
Both are in \( \mathbb{F}_p \) and we have \( x_2 = 27a^2 + 18ab + 3b^2, x_1 = -9a^2 - 18ab + 3b^2 \). Using the result of the \( \mathbb{Z}/3\mathbb{Z} \) case, one can easily check that \((f_6(a, b), g_6(a, b)) = (A, B)\).

Let \( G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \) and assume that \( J = \Phi_{2 \times 4}(a, b) \) for some \( a, b \). We claim that

\[
|W_{2 \times 4, J}| = \begin{cases} 
24 & \text{if } E_J(\mathbb{F}_p)[4] \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \\
8 & \text{if } E_J(\mathbb{F}_p)[4] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.
\end{cases}
\]

Considering the six systems deduced by \( \Phi_{2 \times 4}(a, b) = \Phi_{2 \times 4}(c, d) \), we can see that \( |W_{2 \times 4, J}| \) is at least 8 and it is exactly 8 if either \( p \equiv 3 \pmod{4} \) or \( p \equiv 1 \pmod{4} \) and \( ab \) is non-square in \( \mathbb{F}_p \). If \( p \equiv 1 \pmod{4} \) and \( ab \) is a square in \( \mathbb{F}_p \), the six systems are all consistent and have 24 solutions and by direct computation, we can conclude that they are the preimages of \( \Phi_{2 \times 4}(a, b) \). Therefore,

\[
|W_{2 \times 4, J}| = \begin{cases} 
24 & \text{if } \sqrt{ab} \in \mathbb{F}_p \text{ and } p \equiv 1 \pmod{4}, \\
8 & \text{otherwise}.
\end{cases}
\]

We recall that \( E_J \) has three non-trivial 2-torsion points whose \( x \)-coordinates are \(-(3a^2 - 18ab + 3b^2), -(3a^2 + 18ab + 3b^2), (6a^2 + 6b^2)\), respectively. The points \( P \) with \( 2P = (6a^2 + 6b^2, 0) \) are already contained in the \( E_J(\mathbb{F}_p) \), and one can check that the two points

\[
(3a^2 + 18ab + 3b^2 \pm 18\sqrt{ab}(a + b), \sqrt{-1} \cdot 3^{3/2}\sqrt{ab}(\sqrt{a} \pm \sqrt{b})^2(a + b))
\]

and their inverses defined in \( \mathbb{F}_p[\sqrt{ab}, \sqrt{-1}] \) are the 4 points \( Q \) with \( 2Q = (-3a^2 + 18ab + 3b^2, 0) \). Therefore, \( p \equiv 1 \pmod{4} \) and \( ab \) is square if and only if \( E_J \) includes \( \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \) which is equivalent to \( |W_{2 \times 4, J}| = 24 \).

At last, we need to show that when \( E_J \) has \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \) as a subgroup, then there exists \( a, b \in \mathbb{F}_p \) such that \( J = \Phi_{2 \times 4}(a, b) \). Since we already showed the analogue for \( G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \) and \( \mathbb{Z}/4\mathbb{Z} \), there are \( u, v, s, t \in \mathbb{F}_p \) such that

\[
(A, B) = (-u^2 + 3v^2)/4, (v^3 - u^2v)/4 = (-3s^2 + 6st^2 - 2t^4, (2s - t^2)(s^2 + 2st^2 - t^4)).
\]

One can check that \( 5t^2 - 12s \) should be a square, say \( r^2 \). Then, \((A, B) = \Phi_{2 \times 4}(6^{-1}r, 6^{-1}t)\). \( \square \)

By Lemma 2.6, for example, we have

\[
|W_{6, J}| = \begin{cases} 
24 & \text{if } E_J(\mathbb{F}_p)[6] \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \\
8 & \text{if } E_J(\mathbb{F}_p)[6] \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \\
6 & \text{if } E_J(\mathbb{F}_p)[6] \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \\
2 & \text{if } E_J(\mathbb{F}_p)[6] \cong \mathbb{Z}/6\mathbb{Z}, \\
0 & \text{if } E_J(\mathbb{F}_p)[6] \not\cong \mathbb{Z}/6\mathbb{Z}.
\end{cases}
\]

Remark 2. In contrast to Lemma 2.5, we remark that Lemma 2.6 does not hold for all torsion groups. For example, let \( E_1 : y^2 = x^3 + 2x + 1 \) and \( E_2 : y^2 = x^3 + 2x + 4 \) be elliptic curves over \( \mathbb{F}_5 \). Then, \( E_1 \) and \( E_2 \) are isomorphic, and \( E_1(\mathbb{F}_5) \cong E_2(\mathbb{F}_5) \cong \mathbb{Z}/7\mathbb{Z} \). However, one can compute that \( |W_{7,(2,1)}| = 0 \) and \( |W_{7,(2,4)}| = 12 \). This phenomenon is the major obstacle to verifying the
moment conditions (9) and (9) using Kaplan and Petrow’s Eichler–Selberg trace formula. See Proposition 2.8.

2.3 Moments of traces of the Frobenius

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

**Definition.** We define

$$H_G(a, p) := \sum_{J=(A, B) \in (\mathbb{Z}/p\mathbb{Z})^2 \atop a_p(E_J) = a} |W_{G,J}|,$$

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

The goal of this section is to show

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

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

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

We remark that (8) holds for all torsion groups by Proposition 2.2.

The primary tool is the Eichler–Selberg trace formula [15]. 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

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

be the Chebyshev coefficients. We have

$$t^R = \sum_{j=0}^{\lfloor R/2 \rfloor} C_{R,j}q^jU_{R-2j}(t, q),$$
which is [15, (1.3)]. In particular, we have
\begin{equation}
    t^0 = U_0(t, q), \quad t = U_1(t, q), \quad t^2 = U_2(t, q) + qU_0(t, q).
\end{equation}  

Let $E$ be an elliptic curve defined over a finite field $\mathbb{F}_q$ with $q$ elements, $\mathcal{C}$ be the set of all the isomorphism classes of elliptic curves over $\mathbb{F}_q$. Let $A$ denote a finite abelian group and let $\Phi_A$ 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
\[
    E_q(a^R \Phi_A) = \frac{1}{q} \sum_{E \in \mathcal{C}} \frac{a_q(E)^R}{|Aut_{\mathbb{F}_q}(E)|}.
\]

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 $\psi(n) = n \prod_{p|n}(1 - 1/p)$ and $\phi(n) = n \prod_{p|n}(1 + 1/p)$.

For $\lambda \mid (p - 1, n_1)$, let
\[
    T_{n_1, \lambda}(p, 1) := \frac{\psi(n_1^2/\lambda^2)\phi(n_1/\lambda)}{\phi(n_1)} (-T_{\text{trace}} - T_{\text{hyp}} + T_{\text{dual}}),
\]

with
\[
    T_{\text{trace}} := \frac{1}{\phi(n_1)} \text{Tr}(T_p|S_k(G(\mathbb{F}_q))),
\]
\[
    T_{\text{hyp}} := \frac{1}{4} \sum_{i=0}^{1} \sum_{\tau|n_1 \lambda, g \not| p-1} \frac{\varphi(g)\varphi(n_1(\lambda, g)/\lambda)}{\varphi(n_1)} \left( \delta_{n_1(\lambda, g)/\lambda}(y_1, 1) + (-1)^k \delta_{n_1(\lambda, g)/\lambda}(y_1, -1) \right),
\]
\[
    T_{\text{dual}} := \frac{p+1}{\phi(n_1)} \delta(k, 2),
\]

where $g = (\tau, n_1 \lambda/\tau)$, $y_1$ is the unique element of $(\mathbb{Z}/(n_1 \lambda/g)\mathbb{Z})^\times$ such that $y_1 \equiv p^i \pmod{\tau}$ and $y_1 \equiv p^{i-1} \pmod{n_1 \lambda/\tau}$, $\delta(a, b)$ 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 2.7** [15, 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
\[
    E_p(U_{k-2}(t, p)\Phi_A) = \frac{1}{\phi(n_1/n_2)} \sum_{y \mid (p-1)n_1/n_2} \Phi(y)T_{n_1, n_2 y}(p, 1)
\]
and if $p \not\equiv 1 \pmod{n_2(A)}$, then $E_p(U_{k-2}(t, p)\Phi_A) = 0$.

**Proposition 2.8.** 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 (9) and (10) 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 $\tilde{\omega}_{G,i}$ to be $|W_{G,i}|$ if $E_i[n_1](\mathbb{F}_p) \cong A_{G,i}$. This is well defined by the second statement of Lemma 2.6. Let $$\omega_{G,i} := \tilde{\omega}_{G,i} - \sum_{j < i} \omega_{G,j}.$$ Then, one can obtain that $$\sum_{|a| < 2\sqrt{p}} a^R H_G(a, p) = p(p - 1) \sum_i \omega_{G,i} E_p(a^R \Phi_{A_{G,i}}).$$ By (8), $$\sum_i \omega_{G,i} E_p(\Phi_{A_{G,i}}) = 1 \pm O \left( \frac{1}{p} \right). \quad (13)$$ Since $t^2 = U_2(t, p) + pU_0(t, p)$, we have the identity $$E_p(t^2 \Phi_A) = E_p(U_2(t, p) \Phi_A) + pE_p(U_0(t, p) \Phi_A),$$ and this together with (13) implies $$\sum_{|a| < 2\sqrt{p}} a^{2R} H_G(a, p) = p(p - 1)(p + O(1)) + O(p^{2.5}) = p^3 + O(p^{2.5})$$ because $E_p(U_2(t, p) \Phi_A) \ll_G p^{1.5} \ll_G p^{0.5}$ by Theorem 2.7 and the Deligne bound.

Using the identity $t = U_1(t, p)$ and $E_p(U_1(t, p) \Phi_A) \ll_G p^{-0.5}$, it is easy to see that $$\sum_{|a| < 2\sqrt{p}} a^{2R} H_G(a, p) = O_G(p^{1.5})$$ by Theorem 2.7 and the Deligne bound. \hfill \Box

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 2.9.** 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 $R > 0$.

**Proof.** Let $N_n(a)$ (respectively, $N_{n \times n}(a)$) be the number of isomorphism classes of elliptic curves over $\mathbb{F}_p$ such that $E(\mathbb{F}_p)[n] \geq \mathbb{Z}/n\mathbb{Z}$ (respectively, $E(\mathbb{F}_p)[n] = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$) with weight $2/|Aut_{\mathbb{F}_p}(E)|$. Then, [20, Theorem 4.6, 4.9] shows that for a prime $p \geq 5$, an $a$ in the Weil bound, and a positive integer $n \geq 2$, $$N_n(a) = \begin{cases} H(a^2 - 4p) & \text{if } a \equiv p + 1 \pmod{n}, \\ 0 & \text{otherwise}, \end{cases}$$
and
\[ N_{n \chi n}(a) = \begin{cases} H\left(\frac{a^2 - 4p}{n}ight) & \text{if } p \equiv 1 \pmod{n} \text{ and } a \equiv p + 1 \pmod{n^2}, \\ 0 & \text{otherwise.} \end{cases} \]

By Lemma 2.6,
\[ H_2(a, p) = \frac{p - 1}{2}(N_2(a) + 2N_{2 \times 2}(a)), \quad H_{2 \times 2}(a, p) = 6 \cdot \frac{p - 1}{2}N_{2 \times 2}(a). \]

Since \( N_2(a) = N_2(-a) \) and \( N_{2 \times 2}(a) = N_{2 \times 2}(-a) \), the result follows.

Proposition 2.9 will be used for the Frobenius trace formula for elliptic curves in Section 4.

### 3. COUNTING ELLIPTIC CURVES WITH TORSION POINTS AND LOCAL CONDITIONS

We introduce some notations first. Let
\[ R_G(X) = \left\{ (a, b) \in \mathbb{R}^2 : |f_G(a, b)| \leq X^{\frac{1}{3}}, |g_G(a, b)| \leq X^{\frac{1}{2}} \right\}. \]

For a group \( G \) in \( G_{\leq 4} \) we define
\[ D_G(X) = \left\{ (A, B) \in \mathbb{Z}^2 : (A, B) = \Phi_G(a, b) \text{ for some } (a, b) \in R_G(X) \cap \mathbb{Z}^2 \right\}, \]
\[ M_G(X) = \left\{ (A, B) \in D_G(X) : \text{ if } p^4 \mid A, \text{ then } p^6 \nmid B \right\}, \]
and
\[ E_G(X) = \left\{ (A, B) \in M_G(X) : 4A^3 + 27B^2 \neq 0 \right\}, \]
\[ S_G(X) = \left\{ (A, B) \in M_G(X) : 4A^3 + 27B^2 = 0 \right\}, \]
where \( E_G(X) \) represents elliptic curves with \( G \) torsion and \( S_G(X) \) takes up singular curves. We note that \( E_G(X) \) coincides with the previous definition.

For a group \( G \) in \( G_{> 5} \), we recall that \( M_G(X) \) is the set of relatively prime pairs \((a, b)\) with \( h(\Phi_G(a, b)) \leq X \). We define
\[ \tilde{M}_G(X) = \left\{ (a, b) \in \mathbb{Z}^2 : (a, b) = 1, e = e(a, b), |f_G(a, b)| \leq X^{\frac{1}{3}}, |g_G(a, b)| \leq X^{\frac{1}{2}} \right\}, \]
and \( \tilde{M}_G(X) \) as the union of \( \tilde{M}_G^e(X) \) for all \( e \geq 1 \). Let \( M_G^e(X) \) be the subset of \( M_G(X) \) of elements with defect \( e \). We define \( E_G(X) \) as (4) and
\[ S_G(X) = \left\{ (A, B) \in S(X) : (A, B) = \Phi_G(a, b) \text{ for relatively prime } (a, b) \right\}, \]
where
\[ S(X) = \left\{ (A, B) \in \mathbb{Z}^2 : |A| \leq X^{\frac{1}{3}}, |B| \leq X^{\frac{1}{2}}, 4A^3 + 27B^2 = 0, \quad \text{if } p^4 \text{ divides } A, \text{ then } p^6 \text{ does not divide } B. \right\}. \]
For the reader’s convenience, it is good to remember that \((a, b)\) denotes an element in the domain of \(\Phi_G\) or \(R_G\) (respectively, \(M_G\) for a group \(G\) in \(\mathcal{G}_{\geq 5}\)) and \((A, B)\) does in the range of \(\Phi_G\). Also, \(D_G, M_G, E_G,\) and \(S_G\) 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 3.1.** For a torsion subgroup \(G\), the number of integer points in \(R_G(X)\) is

\[
\text{Area}(R_G(1))X^{\frac{1}{\sigma(G)}} + O(X^{\frac{1}{\sigma(G)}}).
\]

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

\[
\text{Area}(R_4(X)) = X^{\frac{1}{4}}\text{Area}(R_4(1)).
\]

Then, the claim follows from the Principle of Lipschitz, [12, (5.3)] since \(X^{\frac{1}{\sigma(G)}}\) is the longer length of the projection of \(R_G(X)\) to the axes. The same idea works for \(G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\). Also, we obtain the result for the groups \(G\) in \(\mathcal{G}_{\geq 5}\) since \(e(G) = 3 \deg f_G(a, b) = 2 \deg g_G(a, b) = 2d(G)\). \(\Box\)

By the Principle of Lipschitz, we have the following.

**Corollary 3.2.** For a prime \(p \geq 5\), an element in \((\mathbb{Z}/p\mathbb{Z})^2\), and a torsion subgroup \(G\), we have

\[
|R_G,I(X)| = \text{Area}(R_G(1))p^{-2}X^{\frac{1}{\sigma(G)}} + O(1 + p^{-1}X^{\frac{1}{\sigma(G)}}).
\]

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 3.1 and Möbius inversion argument gives the following corollary, which is a complement of [12, Theorem 5.6]. For details, we refer to the proof of Proposition 3.6.

**Corollary 3.3.** For a group \(G\) in \(\mathcal{G}_{\leq 4}\) and \(r(G)\) defined in Lemma 2.4, let

\[
c(G) := \frac{\text{Area}(R_G(1))}{2^5G=2\times r(G)\zeta\left(\frac{12}{d(G)}\right)}.
\]

Then,

\[
|E_G(X)| = c(G)X^{\frac{1}{\sigma(G)}} + O(X^{\frac{1}{\sigma(G)}}).
\]

**Lemma 3.4.** For a prime \(p \geq 5\), a non-zero pair \(J\) in \((\mathbb{Z}/p\mathbb{Z})^2\) and a group \(G\) in \(\mathcal{G}_{\leq 4}\),

\[
|D_G,J(X)| = \frac{|W_G,J|}{2^5G=2\times r(G)}|R_G,I(X)| + O(1 + p^{-1}X^{\frac{1}{\sigma(G)}}),
\]
where $I$ is an arbitrary pair in $W_{G,J}$. For $G$ in $G_{\geq 5}$, we have

$$|E_{G,J}(X)| = \frac{|W_{G,J}|}{r(G)} \sum_{l \in W_{G,J}} \sum_{e} |M_{l}^{e}(X)| + O(1 + p^{-1}X^{\frac{1}{\sigma(G)}}).$$

**Proof.** We fix a group $G$ and omit it in the subscript. For $G$ in $G_{\leq 4}$, $\Phi$ induces a surjective map

$$\bigsqcup_{I \in W_{J}} R_{I}(X) \rightarrow D_{J}(X), \quad (a, b) \rightarrow (A, B) = \Phi(a, b).$$

Let $h_{J}(X)$ be the number of the pairs $(A, B)$ for which its pre-image is not equal to $r(G)$. Then, $h_{J}(X)$ is bounded by $O(p^{-1}X^{\frac{1}{\sigma(G)}})$ by the proof of Lemma 2.4. We note that the number of solutions of the system of equations

$$f(a, b) = A \quad \text{and} \quad g(a, b) = B$$

is less than or equal to $\deg f \cdot \deg g$ by Bézout's theorem, and $|R_{I}(X)|$ does not depend on $I$ by Corollary 3.2. Therefore, we have

$$|D_{J}(X)| = \frac{|W_{J}|}{2^{\sigma_{G=2x2}} r(G)} |R_{J}(X)| + O(h_{J}(X)).$$

For a group $G$ in $G_{\geq 5}$, $\Phi$ induces a surjective map

$$\bigsqcup_{I \in W_{J}} \bigcup_{e} M_{l}^{e}(X) \rightarrow E_{J}(X) \bigcup S_{J}(X).$$

Hence, the above argument and an estimate of $S_{J}(X)$ give a similar result. 

For a pair $(A, B)$ of integers or elements of $\mathbb{Z}/p\mathbb{Z}$ and an integer $d$, we define an operation $\ast$ by

$$d \ast (A, B) = (d^{4}A, d^{6}B).$$

**Proposition 3.5.** For a prime $p \geq 5$, a non-zero pair $J \in (\mathbb{Z}/p\mathbb{Z})^{2}$ and a group $G$ in $G_{\leq 4}$,

$$|M_{G,J}(X)| = \sum_{1 \leq d \leq X^{\frac{1}{p}}} \frac{1}{\mu(d)} |D_{G,d^{-1}sJ}(d^{-12}X)|,$$

and $|S_{G,J}(X)| = O(p^{-1}X^{\frac{1}{\sigma}}).$

**Proof.** Let $(A, B) \in D_{G,J}(X)$ and let $d$ be the maximum of $d'$ satisfying $d'^{4} \mid A$ and $d'^{6} \mid B$. Since $J$ is non-zero, $p \nmid d$. By (1), the definition of $f_{G}$ and $g_{G}$, one can easily check that there are positive integers $m$ and $n$ depending $G$ such that

$$\frac{1}{d^{4}} f_{G}(a, b) = f_{G}\left(\frac{a}{d^{m}}, \frac{b}{d^{n}}\right), \quad \frac{1}{d^{6}} g_{G}(a, b) = g_{G}\left(\frac{a}{d^{m}}, \frac{b}{d^{n}}\right).$$
Furthermore, we can check that $a/d^m$ and $b/d^n$ are integers. Hence if $(A, B) = (f_G(a, b), g_G(a, b))$ for some $a, b \in \mathbb{Z}$, then

$$d^{-1} \ast (A, B) = \left( f_G\left(\frac{a}{d^m}, \frac{b}{d^n}\right), g_G\left(\frac{a}{d^m}, \frac{b}{d^n}\right) \right)$$

is an element of $\mathcal{M}_{G, d^{-1} \ast J}(d^{-12}X)$, and there is a bijection

$$(A, B) \rightarrow d^{-1} \ast (A, B), \quad D_{G, J}(X) \rightarrow \bigsqcup_{d \in X \frac{1}{12}} \mathcal{M}_{G, d^{-1} \ast J}(d^{-12}X).$$

By Möbius inversion argument, the first identity follows. The error term is easy to establish. □

**Proposition 3.6.** For a prime $p \geq 5$, a non-zero pair $J \in (\mathbb{Z}/p\mathbb{Z})^2$, and a group $G$ in $G_{\leq 4}$, we have

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

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

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

**Proof.** For $d$ not divisible by $p$, we note that $|W_{G, d^{-1} \ast J}| = |W_{G, J}|$ for all $p \nmid d$. Then,

$$|\mathcal{E}_{G, J}(X)| = |\mathcal{M}_{G, J}(X)| + O(S_{G, J}(X)) = \sum_{d \leq X \frac{1}{12}} \mu(d) |D_{G, d^{-1} \ast J}(X^{\frac{1}{d(G)}})| + O\left( \frac{X^{\frac{1}{6}}}{p} \right)$$

$$= \sum_{d \leq X \frac{1}{12}} \mu(d) \left( \frac{|W_{G, d^{-1} \ast J}|}{2^{5G=2\times2} r(G)} |R_{G, I}(X^{\frac{1}{d(G)}})| + O\left( 1 + p^{-1} X^{\frac{1}{d(G)}} \right) \right) + O\left( \frac{X^{\frac{1}{6}}}{p} \right)$$

$$= \frac{|W_{G, J}|}{2^{5G=2\times2} r(G)} \sum_{d \leq X \frac{1}{12}} \mu(d) |R_{G, J}(X^{\frac{1}{d(G)}})| + O\left( \frac{X^{\frac{1}{6}}}{p} + \frac{X^{\frac{1}{d(G)}}}{p} \right)$$

by Lemma 3.4. Here we also used that $|R_{G, J}(X)|$ does not depend on $I \in W_{J}$. Using Corollary 3.2, the sum is
By [12, Theorem 5.6] and Corollary 3.3, the main term of

$$|E_{G,(0,0)}(X)| = |E_G(X)| - \sum_{J \neq (0,0)} |E_{G,J}(X)|$$

is

$$c(G)X^{\frac{1}{d(G)}} - \sum_{J \neq (0,0)} c(G) \left| \frac{W_{G,J}}{p^2} \right| \frac{X^{\frac{1}{d(G)}}}{p^{\frac{12}{d(G)}} - 1} = c(G)X^{\frac{1}{d(G)}} \left( \frac{1}{p^2} - \frac{1}{p^{\frac{12}{d(G)}}} \right) \frac{X^{\frac{1}{d(G)}}}{p^{\frac{12}{d(G)}} - 1}.$$ 

The error term is easily checked. □

Now, we study the probability of a local condition when the probability space is the set of elliptic curves with torsion $G$. For a torsion group $G$, we define

$$c_{G,LC}(p) = \sum_{E_J \text{ satisfies } LC} \frac{|W_{G,J}|}{p^2}.$$ 

**Theorem 3.7.** For a prime $p \geq 5$, a local condition $LC$, and a group $G$ in $G_{\leq 4}$,

$$|E_{G,p}(X)| = c(G) \cdot c_{G,LC}(p) \cdot \frac{X^{\frac{1}{d(G)}}}{p^{\frac{12}{d(G)}} - 1} + O(h_{G,LC}(p,X)),$$

where $c_{G,LC}(p)$ is

|   | 2          | 3          | 4          | 2 × 2       |
|---|------------|------------|------------|-------------|
| good | $(p - 1)^2/p^2$ | $(p - 1)^2/p^2$ | $(p - 1)^2/(p - 2)/p^2$ | $(p - 1)(p - 2)/p^2$ |
| mult | $(2p - 2)/p^2$ | $(2p - 2)/p^2$ | $(3p - 3)/p^2$ | $(3p - 3)/p^2$ |
| addi | $1/p^2 - 1/p^6$ | $1/p^2 - 1/p^4$ | $1/p^2 - 1/p^3$ | $1/p^2 - 1/p^4$ |
| $a$ | $H_2(a, p)/p^2$ | $H_3(a, p)/p^2$ | $H_4(a, p)/p^2$ | $H_{2\times 2}(a, p)/p^2$ |
and
\[
c_{3,\text{split}}(p) = \begin{cases} 
2(p - 1)/p^2 & \text{for } p \equiv 1 \mod 12, \\
(p - 1)/p^2 & \text{for } p \equiv 5 \text{ or } 11 \mod 12, \\
0 & \text{for } p \equiv 7 \mod 12.
\end{cases}
\]

The error term \( h_{G,\mathcal{LC}}(p, X) \) is

| good/bad | \( h_{G,\mathcal{LC}}(p, X) \) |
|----------|--------------------------|
| mult     | \( pX^{1/2} + p^2X^{1/12} \) |
| split    | \( X^{1/2} + pX^{1/12} \) |
| addi     | \( pX^{1/2} + p^2X^{1/12} \) |
| a        | \( H_G(a, p)(p^{-1}X^{1/2(G)} + X^{1/12}) \) |

**Proof.** By Proposition 3.6,
\[
|\mathcal{E}_{G,p}^{\text{good}}(X)| = \sum_{J=(A,B)\in\mathbb{F}_p^2, 4A^3+27B^2\neq0} |\mathcal{E}_{G,J}(X)|
\]
\[
= \sum_{J=(A,B)\in\mathbb{F}_p^2, 4A^3+27B^2\neq0} c(G) \frac{|W_{G,J}|}{p^2} \frac{p^{12}}{p^{2d(G)}} X^{\frac{1}{d(G)}} + O\left(\frac{p(p-1)}{p} \left(\frac{X^{1/2(G)}}{p} + X^{1/12}\right)\right).
\]

By Propositions 2.2, we have
\[
\sum_{J=(A,B)\in\mathbb{F}_p^2, 4A^3+27B^2\neq0} |W_{2,J}| = \sum_{J=(A,B)\in\mathbb{F}_p^2, 4A^3+27B^2\neq0} |W_{3,J}| = (p-1)^2,
\]
\[
\sum_{J=(A,B)\in\mathbb{F}_p^2, 4A^3+27B^2\neq0} |W_{4,J}| = \sum_{J=(A,B)\in\mathbb{F}_p^2, 4A^3+27B^2\neq0} |W_{2\times2,J}| = (p-1)(p-2),
\]

which proves the good reduction case. The other cases can be shown similarly. \( \square \)

For a group \( G \) in \( G_{\geq 5} \), we note that
\[
|\tilde{M}_G(X)| = \frac{\text{Area}(R(1))}{\zeta(2)} X^{\frac{1}{d(G)}} + O(X^{\frac{1}{d(G)}} \log X)
\]

by the Möbius inversion and the Principle of Lipschitz. For details, we refer to the proof of the following lemma.
Lemma 3.8. For an arbitrary prime power $p^m$, $p \geq 5$, and a pair $I \in (\mathbb{Z}/p^m \mathbb{Z})^2$ whose coordinates are not divisible by $p$ simultaneously,

$$|\tilde{M}_{G,I}(X)| = \frac{1}{p^{3m} \mathbb{P}^2} \frac{\text{Area}(R(1))}{\kappa(2)} X^{\frac{1}{\text{dim}(G)}} + O(X^{\frac{1}{\text{dim}(G)}} + p^{-m}X^{\frac{1}{\text{dim}(G)}} \log X).$$

Proof. For a given $I$, we have a bijection

$$R_{G,I}(X) \cong \bigsqcup_{d \in X^{\frac{\text{dim}(G)}}{p|d}}} d \ast \tilde{M}_{G,d^{-1}I}(d^{-2d(G)}X), \quad (a, b) \rightarrow d \ast \left(\frac{a}{d}, \frac{b}{d}\right),$$

where $d$ is the gcd of $a$ and $b$. By Möbius inversion argument and the Principle of Lipschitz, we have

$$|\tilde{M}_{G,I}(X)| = \sum_{d \in X^{\frac{\text{dim}(G)}}{p|d}}} \mu(d)|R_{G,d^{-1}I}(d^{-2d(G)}X)|
= \sum_{d \in X^{\frac{\text{dim}(G)}}{p|d}}} \mu(d) \left(\frac{1}{p^{2m}} \frac{\text{Area}(R(1))}{d^2} X^{\frac{1}{\text{dim}(G)}} + O(p^{-m}d^{-1}X^{\frac{1}{\text{dim}(G)}})\right)
= \frac{1}{p^{2m}} \frac{\mathbb{P}^2}{\mathbb{P}^2 - 1} \frac{\text{Area}(R(1))}{\kappa(2)} X^{\frac{1}{\text{dim}(G)}} + O(X^{\frac{1}{\text{dim}(G)}} + p^{-m}X^{\frac{1}{\text{dim}(G)}} \log X).$$

□

Theorem 3.9. Let $G$ be a torsion group in $G_{\geq 5}$, $p \geq 5$ be a prime, and $J$ be a non-zero pair in $(\mathbb{Z}/p \mathbb{Z})^2$. Then, there is an absolute constant $c(G)$ such that

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

Proof. We use the strategy of [7, §3]. Let $\epsilon = \epsilon(G)$ be a positive integer which is the least common multiplier of the possible defects of $(f_G, g_G)$ which is well defined by Lemma 2.1. Since $M_G^\epsilon(X) = \tilde{M}_G^\epsilon(e^{12X}),$

$$|\mathcal{E}_{G,J}(X)| = \frac{1}{r(G)} \sum_{\ell \in W_J} \sum_{e \in \epsilon} |M^\epsilon_{G,J}(X)| + O(1 + p^{-1}X^{\frac{1}{\epsilon(G)}})
= \frac{1}{r(G)} \sum_{\ell \in W_{G,J}} \sum_{e \in \epsilon} |\tilde{M}^\epsilon_{G,J}(e^{12X})| + O(1 + p^{-1}X^{\frac{1}{\epsilon(G)}})$$

by Lemma 2.4, Lemma 2.5, and Lemma 3.4. We note that the defect of the given pair $(a, b)$ is determined by its reduction modulo $\epsilon$ by Lemma 2.1 for $G$ in $G_{\geq 5}$ except for $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, and modulo $\epsilon^6$ for $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. 
We consider the case of $\epsilon > 1$, and for simplicity, we assume that $\epsilon$ is prime. Let $I_\epsilon$ be the set of pairs $(\mathbb{Z}/\epsilon\mathbb{Z})^2$ which has a defect $e$. Then,

$$\tilde{M}_{\epsilon,G,J}(X) = \bigcup_{I' \in I_\epsilon} \tilde{M}_{G,I,I'}(X),$$

where $\tilde{M}_{G,I,I'}(X)$ is a subset of $\tilde{M}_{G,I}(X)$ where the additional condition $(a, b) \equiv I' \pmod{\epsilon}$ is imposed. Since $\epsilon$ is a prime, $e = 1$ or $\epsilon$. By Lemma 3.8 and Chinese Remainder Theorem,

$$|\tilde{M}_{\epsilon,G,I}(X)| = \frac{|I_\epsilon|}{(\epsilon^2 - 1)} \frac{1}{(p^2 - 1)} \frac{\text{Area}(R(1))}{\zeta(2)} X^{\frac{1}{\delta(G)}} + O(X^{\frac{1}{2\delta(G)}} + p^{-1}X^{\frac{1}{2\delta(G)}} \log X)$$

and

$$|\tilde{M}_{1,G,I}(X)| = \frac{(\epsilon^2 - 1 - |I_\epsilon|)}{(\epsilon^2 - 1)} \frac{1}{(p^2 - 1)} \frac{\text{Area}(R(1))}{\zeta(2)} X^{\frac{1}{\delta(G)}} + O(X^{\frac{1}{2\delta(G)}} + p^{-1}X^{\frac{1}{2\delta(G)}} \log X).$$

Therefore,

$$|E_{\epsilon,G,J}(X)| = \frac{|W_{G,I}|}{p^2 - 1} \frac{(\epsilon^{12(G)} - 1)|I_\epsilon| + \epsilon^2 - 1)}{(\epsilon^2 - 1)} \frac{1}{r(G)} \frac{\text{Area}(R(1))}{\zeta(2)} X^{\frac{1}{\delta(G)}} + O(X^{\frac{1}{2\delta(G)}} + p^{-1}X^{\frac{1}{2\delta(G)}} \log X).$$

Similarly, for the groups with no defect, we can show that

$$|E_{G,J}(X)| = \frac{|W_{G,I}|}{p^2 - 1} \frac{1}{r(G)} \frac{\text{Area}(R(1))}{\zeta(2)} X^{\frac{1}{\delta(G)}} + O(X^{\frac{1}{2\delta(G)}} + p^{-1}X^{\frac{1}{2\delta(G)}} \log X).$$

By taking $c(G) = \frac{(\epsilon^{12(G)} - 1)|I_\epsilon| + \epsilon^2 - 1)}{(\epsilon^2 - 1)} \frac{1}{r(G)} \frac{\text{Area}(R(1))}{\zeta(2)}$ where the first term exists only if $\epsilon \neq 1$, the claim follows. When $\epsilon$ is not prime (only appear when $G = \mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ by Lemma 2.1), we can compute $c(G)$ similarly.

Our proof gives $c(G)$ concretely except for $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Even for such $G$, if one knows the defects (see Remark 1), then one can calculate $c(G)$ precisely.

For the torsion subgroups $G$ in $G_{\geqslant 5}$, we have an analog of Theorem 3.7. Instead of listing them all, we record the results which will be used in the applications.

**Corollary 3.10.** For a group $G$ in $G_{\geqslant 5}$ and a prime $p \geqslant 5$,

$$|E_G(X)| = c(G)X^{\frac{1}{\delta(G)}} + O(X^{\frac{1}{\delta(G)}}),$$

$$|E_{G,p}^a(X)| = c(G) \frac{H_G(a, p)}{p^2 - 1} X^{\frac{1}{\delta(G)}} + O \left( H_G(a, p)X^{\frac{1}{\delta(G)}} + \frac{H_G(a, p)}{p} X^{\frac{1}{\delta(G)}} \log X \right),$$

$$|E_{G,p}^{\text{mult}}(X)| = O \left( p^{-1}X^{\frac{1}{\delta(G)}} + pX^{\frac{1}{\delta(G)}} + X^{\frac{1}{\delta(G)}} \log X \right).$$

Theorems 3.7 and 3.9 help to understand the probability for elliptic curves with a local condition. In particular, for $\mathcal{L}C = \text{mult}$, we observe an interesting phenomenon.
Corollary 3.11. The ratios of functions \( c_{G, \text{mult}}(p) \) for a group \( G \) in \( G_{\leq 4} \) and \( p \geq 5 \) are proportional to the number of cusps of the corresponding modular curves. Also, there is a set of primes \( S \) with a positive density such that, for \( p \) in \( S \), the ratios of functions \( c_{G, \text{mult}}(p) \) for a group \( G \) in \( G_{\geq 5} \) are proportional to the number of cusps of the corresponding modular curves.

Proof. One can easily compute that the numbers of cusps of modular curve \( X_1(N) \) for \( N = 1, 2, 3, 4 \) and \( X(2) \) are 1, 2, 2, 3, and 3, respectively (for example, see [9, §3.9]). So the claim for a group \( G \) in \( G_{\leq 4} \) follows from Proposition 2.2 and Theorem 3.7. Also, the number of cusps of \( X_1(N) \) for \( N = 5, 6, 7, 8, 9, 10, 12 \) and \( X_{\Gamma_1(M) \cap \Gamma(2)} \) for \( M = 4, 6, 8 \) is 4, 4, 6, 6, 8, 8, 10 and 4, 6, 10. The second statement follows from Proposition 2.2, Theorem 3.9, and Chebotarev density theorem. \( \square \)

It is well known that every elliptic curve with torsion \( G \) in \( G_{\geq 5} \) has semistable reduction at \( p \nmid |G| \). We can confirm this phenomenon with probability 1. Also, we have the analogous result for a group \( G \) in \( G_{\leq 4} \).

Corollary 3.12. For a group \( G \) in \( G_{\geq 5} \) and a prime \( p \nmid 6|G| \), we have

\[
\lim_{X \to \infty} \frac{|\mathcal{E}_{G, p}^{\text{ss}}(X)|}{|\mathcal{E}_G(X)|} = 1.
\]

For a torsion subgroup \( G \) in \( G_{\leq 4} \) and a prime \( p \geq 5 \),

\[
c_{G, \text{ss}}(p) = 1 - \frac{1}{p^2}.
\]

As we can see in the [6, Theorem 1.1], the number of elliptic curves with split reduction at \( p \) and that of elliptic curves with non-split reduction at \( p \) are the same. However, this property holds no more when we consider elliptic curves with torsion \( G \).

Corollary 3.13. For \( G = \mathbb{Z}/3\mathbb{Z} \) and a prime \( p \geq 5 \), we have

\[
\lim_{X \to \infty} \frac{|\mathcal{E}_{G, p}^{\text{split}}(X)|}{|\mathcal{E}_{G, p}^{\text{mult}}(X)|} = \begin{cases} 
\frac{1}{2} & \text{when } p \equiv 5, 11 \pmod{12}, \\
1 & \text{when } p \equiv 3 \pmod{4}, \\
0 & \text{when } p \equiv 7 \pmod{12}.
\end{cases}
\]

In Section 4, we establish the Frobenius trace formula for elliptic curves when \( G = \mathbb{Z}/2\mathbb{Z} \) and \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \). For this purpose, we need to count elliptic curves with finitely many local conditions. Since its proof is similar to that of [6, Theorem 8], we introduce the notations and state the results.

Let \( P = \{p_k\}_k \) be a finite set of primes such that \( p_k \geq 5 \), and \( J = J_p \) be a finite set of pairs \((A_k, B_k)\) for \( A_k, B_k \in \mathbb{Z}/p_k\mathbb{Z} \) such that \((A_k, B_k) \neq (0, 0) \pmod{p_k}\). We define analogously \( \mathcal{M}_{G, J}(X), \mathcal{E}_{G, J}(X), S_{G, J}(X) \), and so on. Let

\[
W_{G, J} = \prod_k W_{G, J_k} \text{ for } J_k \equiv (A_k, B_k) \pmod{p_k}.
\]

Then,
Proposition 3.14. For $P = \{ p_k \}$ and $J = \{ (A_k, B_k) \}$, pairs of $\mathbb{Z}/p_k\mathbb{Z}$ such that $(A_k, B_k) \neq (0, 0)$ for all $k$, and a group $G$ in $G_{\leq 4}$, we have
\[ |\mathcal{E}_{G,J}(X)| = c(G)|W_{G,J}| \prod_k \left( \frac{1}{P_k^2} \frac{15}{P_k^{12}} \right)^{\frac{1}{d(G)}} X^{\frac{1}{d(G)}} + O\left( \prod_k p_k^{-1} X^{\frac{1}{d(G)}} + X^{\frac{1}{12}} \right). \]

We will denote $S = (\mathcal{L}C_{p_i})$ as a finite set of local conditions $\mathcal{L}C_{p_i}$. When an elliptic curve has the local property corresponding to $\mathcal{L}C_{p_i}$ at $p_i$ for all local conditions in $S$, we say that $E$ satisfies $S$. Let
\[ \mathcal{E}_G^S(X) = \{ (A, B) \in \mathcal{E}_G(X) : E_{A,B} \text{ satisfies } S \}, \]
and
\[ |\mathcal{L}C_{p_i}|_G := \lim_{X \to \infty} \frac{|\mathcal{E}_{G,P}^{\mathcal{L}C_p}(X)|}{|\mathcal{E}_G(X)|}, \quad |S|_G = \prod |\mathcal{L}C_{p_i}|_G. \]

Now we address that the local conditions under the torsion restriction are independent.

Theorem 3.15. Let $P = \{ p_k \}$ and $S$ be a set of local conditions at primes $p_k \geq 5$. Then, we have
\[ |\mathcal{E}_G^S(X)| = c(G)|S|_G X^{\frac{1}{d(G)}} + O\left( \prod_k p_k \right) X^{\frac{1}{d(G)}} + \left( \prod_k p_k^2 \right) X^{\frac{1}{12}}. \]

We replace the exponents 1 and 2 of $p_k$ in the error term by 0 and 1, respectively, when $\mathcal{L}C$ is multi, split, or non-split. When $\mathcal{L}C$ is a in the Weil bound, $p_k$ and $p_k^2$ are replaced by $H_G(a, p_k)/p_k$ and $H_G(a, p_k)$, respectively.

4 | PROOFS OF THE MAIN THEOREMS

4.1 | Boundedness of average analytic rank of elliptic curves with prescribed torsion

In this section, we show that the average analytic rank of elliptic curves with prescribed torsion $G$ is bounded under the GRH for elliptic curve $L$-functions. Let $\phi$ be an even non-negative Schwartz class function with its Fourier transform $\hat{\phi}$ compactly supported. Let $\gamma_E$ 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 [18, Proposition 2.1] and Ogg’s formula [6, §4] we have
\[ \frac{1}{|\mathcal{E}_G(X)|} \sum_{E \in \mathcal{E}_G(X)} \sum_{\gamma_E} \phi\left( \frac{\log X}{2\pi} \right) \gamma_E \log N_E \log X \left( \frac{\log X \cdot r}{2\pi} \right) \Re \frac{\Gamma'_{E}}{\Gamma_{E}} \left( \frac{1}{2} + ir \right) dr \]
\[ = \frac{\hat{\phi}(0)}{|\mathcal{E}_G(X)|} \sum_{E \in \mathcal{E}_G(X)} \frac{\log N_E}{\log X} + \frac{2}{\pi} \int_{-\infty}^{\infty} \phi\left( \frac{\log X}{2\pi} \right) \Re \frac{\Gamma'_{E}}{\Gamma_{E}} \left( \frac{1}{2} + ir \right) dr. \]
\[- \frac{2}{\log X} \sum_{n=1}^{\infty} \frac{\Lambda(n)}{\sqrt{n}} \hat{\phi} \left( \frac{\log n}{\log X} \right) \sum_{E \in E_G(X)} \hat{a}_E(n) \]
\[\leq \hat{\phi}(0) - \frac{2}{\log X} \sum_{n=1}^{\infty} \frac{\Lambda(n)}{\sqrt{n}} \hat{\phi} \left( \frac{\log n}{\log X} \right) \sum_{E \in E_G(X)} \hat{a}_E(n) + O \left( \frac{1}{\log X} \right) \]
\[\leq \hat{\phi}(0) - S_1 - S_2 + O \left( \frac{1}{\log X} \right), \]

where

\[S_1 = \frac{2}{\log X} \sum_p \frac{\log p}{\sqrt{p}} \hat{\phi} \left( \frac{\log p}{\log X} \right) \sum_{E \in E_G(X)} \hat{a}_E(p), \]
\[S_2 = \frac{2}{\log X} \sum_p \frac{\log p}{p} \hat{\phi} \left( \frac{2\log p}{\log X} \right) \sum_{E \in E_G(X)} \hat{a}_E(p^2), \]

the coefficients \(\hat{a}_E(n)\) come from the logarithmic derivative of \(L(s, E)\)
\[- \frac{L'(s, E)}{L(s, E)} = \sum_{n=1}^{\infty} \frac{\hat{a}_E(n)\Lambda(n)}{n^s}. \]

From now on, for a positive constant \(\sigma\), we specify the test function \(\phi\) and \(\hat{\phi}\):
\[\hat{\phi}(u) = \frac{1}{2} \left( \frac{1}{2} \sigma - \frac{1}{2} |u| \right) \text{ for } |u| \leq \sigma, \quad \text{and} \quad \phi(x) = \frac{\sin^2(2\pi \frac{1}{2} \sigma x)}{(2\pi x)^2}. \]

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

If we show
\[-S_1 - S_2 = \frac{1}{2} \phi(0) + o(1), \quad (15)\]

by the positivity of \(\phi\), we have
\[\frac{1}{|E_G(X)|} \sum_{E \in E_G(X)} r_E \leq \frac{1}{2} + \frac{\hat{\phi}(0)}{\phi(0)} + o(1) \leq \frac{1}{2} + \frac{1}{\sigma} + o(1). \quad (16)\]

Hence, it is left to show that (15) holds for each torsion group \(G\) with some explicit \(\sigma\). For this purpose, we need the following lemmas.

**Lemma 4.1.** Assume the moment condition (9) when \(G = \mathbb{Z}/n\mathbb{Z}\) for \(n = 7, \ldots, 10\), and 12 or \(G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}\). For a torsion group \(G\) in \(G_{\geq 5}\),
\[\sum_{E \in E_G(X)} \hat{a}_E(p) \ll \left( p^{-1}X^\frac{1}{d(G)} + p^2X^\frac{1}{d(G)} + pX^\frac{1}{d(G)} \log X \right). \]
For $G = \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$,
\[
\sum_{E \in \mathcal{E}_G(X)} \hat{a}_E(p) \ll p^{-1} X^{\frac{1}{\#(G)}} + pX^{\frac{1}{\#(G)}} + p^2 X^{\frac{1}{12}}.
\]

**Proof.** We know that
\[
\sum_{E \in \mathcal{E}_G(X)} \hat{a}_E(p) = \sum_{\|a\| < 2 \sqrt{p}} \sum_{E \in \mathcal{E}_G(X)} \hat{a}_E(p) + \sum_{E \in \mathcal{E}_G(X)} \hat{a}_E(p).
\]

When $G$ is in $G_{\geq 5}$, by Corollary 3.10,
\[
\left| \sum_{E \in \mathcal{E}_G(X)} \hat{a}_E(p) \right| \ll p^{-\frac{1}{2}} X^{\frac{1}{\#(G)}} + p^{\frac{1}{2}} X^{\frac{1}{\#(G)}} + p^{-\frac{1}{2}} X^{\frac{1}{\#(G)}} \log X.
\]

By Corollary 3.10, (8), and (9),
\[
\sum_{\|a\| < 2 \sqrt{p}} \sum_{E \in \mathcal{E}_G(X), \ a_E(p) = a} \hat{a}_E(p)
\]
\[
= \sum_{\|a\| < 2 \sqrt{p}} \frac{a}{\sqrt{p}} \left( c(G) \frac{H_G(a, p)}{p^2} X^{\frac{1}{\#(G)}} + O \left( \frac{H_G(a, p)}{p} X^{\frac{1}{\#(G)}} \log X \right) \right)
\]
\[
\ll p^{-1} X^{\frac{1}{\#(G)}} + p^2 X^{\frac{1}{\#(G)}} + pX^{\frac{1}{\#(G)}} \log X.
\]

For $G = \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$, by Theorem 3.7,
\[
\left| \sum_{E \in \mathcal{E}_G(X)} \hat{a}_E(p) \right| \ll \frac{1}{\sqrt{p}} \left( \frac{1}{p} X^{\frac{1}{\#(G)}} + X^{\frac{1}{\#(G)}} + pX^{\frac{1}{12}} \right) \ll p^{-\frac{1}{2}} X^{\frac{1}{\#(G)}} + p^{\frac{1}{2}} X^{\frac{1}{\#(G)}} + p^{\frac{1}{2}} X^{\frac{1}{12}}.
\]

By Theorem 3.7, (8), and (9),
\[
\sum_{\|a\| < 2 \sqrt{p}} \sum_{E \in \mathcal{E}_G(X), \ a_E(p) = a} \hat{a}_E(p)
\]
\[
= \sum_{\|a\| < 2 \sqrt{p}} \frac{a}{\sqrt{p}} \left( c(G) \frac{H_G(a, p)}{p^2} X^{\frac{1}{\#(G)}} + O \left( \frac{H_G(a, p)}{p} X^{\frac{1}{\#(G)}} \right) \right)
\]
\[
\ll p^{-1} X^{\frac{1}{\#(G)}} + pX^{\frac{1}{\#(G)}} + p^2 X^{\frac{1}{12}}.
\]

\qed
Lemma 4.2. Assume the moment condition (10) when $G = \mathbb{Z}/n\mathbb{Z}$ for $n = 7, \ldots , 10$ or $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. For a torsion group $G$ in $G_{>5}$,

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

For $G = \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$,

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

Proof. We know that

$$
\sum_{E \in \mathcal{E}_G(X)} \hat{a}_E(p^2) = \sum_{|a| < 2\sqrt{p}} \sum_{E \in \mathcal{E}_G(X)} \hat{a}_E(p^2) + \sum_{E \in \mathcal{E}_G(X)} \frac{1}{p}.
$$

By Corollary 3.10,

$$
\sum_{E \in \mathcal{E}_G(X)} \frac{1}{p} \ll p^{-\frac{1}{2}}X^{\frac{1}{\sigma(\hat{G})}} + p^{-1}X^{\frac{1}{\sigma(\hat{G})}} \log X.
$$

For the first sum, we have

$$
\sum_{|a| < 2\sqrt{p}} \sum_{E \in \mathcal{E}_G(X)} \hat{a}_E(p^2) = \sum_{|a| < 2\sqrt{p}} \sum_{E \in \mathcal{E}_G(X)} (\hat{a}_E(p^2) - 2)
$$

$$
= \sum_{|a| < 2\sqrt{p}} \left(\frac{a^2}{p} - 2\right) \left(c(G)\frac{H_G(a, p)}{p^2 - 1}X^{\frac{1}{\sigma(\hat{G})}} + O\left(H_G(a, p)X^{\frac{1}{\sigma(\hat{G})}} + \frac{H_G(a, p)}{p}X^{\frac{1}{\sigma(\hat{G})}} \log X\right)\right)
$$

$$
= c(G)\sum_{|a| < 2\sqrt{p}} a^2H_G(a, p)X^{\frac{1}{\sigma(\hat{G})}} - 2c(G)\sum_{|a| < 2\sqrt{p}} H_G(a, p)X^{\frac{1}{\sigma(\hat{G})}} + O(p^2X^{\frac{1}{\sigma(\hat{G})}} + pX^{\frac{1}{\sigma(\hat{G})}} \log X)
$$

$$
= -c(G)X^{\frac{1}{\sigma(\hat{G})}} + O\left(p^{-\frac{1}{2}}X^{\frac{1}{\sigma(\hat{G})}} + p^2X^{\frac{1}{\sigma(\hat{G})}} + pX^{\frac{1}{\sigma(\hat{G})}} \log X\right)
$$

by Corollary 3.10, (8), and (10).

For $G = \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$, by Theorem 3.7, (8), and (10), similarly we can show that

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

By Lemma 4.1, for a group $G$ in $G_{>5}$,

$$
S_1 \ll \frac{1}{\log X} \sum_{p} \frac{\log p}{\sqrt{p}} \phi\left(\frac{\log p}{\log X}\right)\left(\frac{1}{p} + p^2X^{-\frac{1}{\sigma(\hat{G})}} + pX^{-\frac{1}{\sigma(\hat{G})}} \log X\right)
$$

$$
\ll X^{-\frac{1}{\sigma(\hat{G})}} \sum_{p \leq X^\sigma} p^{3} \log p \ll X^{-\frac{1}{\sigma(\hat{G})}} + \frac{\sigma}{2}
$$
and for $G = \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$,

$$S_1 \ll \frac{1}{\log X} \sum_p \frac{\log p}{\sqrt{p}} \frac{\Phi}{\log p} \left( \frac{1}{p} + pX \frac{1}{\phi(G)} - \frac{1}{\phi(G)} + p^2 X \frac{1}{\phi(G)} \right) \quad (18)$$

$$\ll X^{-\frac{1}{\phi(G)}} \sum_{p \leq X^\sigma} \left( p^{\frac{1}{2}} \log pX \frac{1}{\phi(G)} + p^{\frac{3}{2}} \log pX \frac{1}{\phi(G)} \right) \ll X^{-\frac{1}{\phi(G)}} \left( X \frac{1}{\phi(G)} + X^{\frac{1}{12}} + \frac{5}{2} \right).$$

By Lemma 4.2, for a group $G$ in $G_{\geq 5}$,

$$S_2 = \frac{2}{\log X} \sum_p \frac{\log p}{p} \frac{\Phi}{\log p} \left( \frac{2 \log p}{\log X} \right) \left( -1 + O \left( p^{-\frac{1}{2}} + pX \frac{1}{\phi(G)} + pX \frac{1}{\phi(G)} \log X \right) \right)$$

$$= -\frac{2}{\log X} \sum_p \frac{\log p}{p} \frac{\Phi}{\log p} \left( \frac{2 \log p}{\log X} \right) + O \left( \frac{1}{\log X} + \sum_{p \leq X^\sigma} p \log p X^{-\frac{1}{\phi(G)}} \right)$$

$$= -\frac{1}{2} \phi(0) + O \left( \frac{1}{\log X} + X^{-\frac{1}{\phi(G)} + \sigma} \right)$$

and for $G = \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$,

$$S_2 = \frac{2}{\log X} \sum_p \frac{\log p}{p} \frac{\Phi}{\log p} \left( \frac{2 \log p}{\log X} \right) \left( -1 + O \left( p^{-\frac{1}{2}} + pX \frac{1}{\phi(G)} + p^2 X \frac{1}{\phi(G)} \right) \right)$$

$$= -\frac{2}{\log X} \sum_p \frac{\log p}{p} \frac{\Phi}{\log p} \left( \frac{2 \log p}{\log X} \right) + O \left( \sum_{p \leq X^\sigma} p \log p X^{-\frac{1}{\phi(G)}} + p \log p X \frac{1}{\phi(G)} \right)$$

$$= -\frac{1}{2} \phi(0) + O \left( X \frac{1}{\phi(G)} - \frac{1}{\phi(G)} + \frac{5}{2} \right).$$

From our computation, if we take $\sigma = \frac{1}{18}$, and $\frac{1}{5d(G)}$ for $G = \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ and $G$ in $G_{\geq 5}$, respectively, then (15) and (16) hold. Therefore, the average analytic rank is bounded by

$$18 + \frac{1}{2}, \quad 18 + \frac{1}{2}, \quad \text{and} \quad 5d(G) + \frac{1}{2}$$

for $G = \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ and $G$ in $G_{\geq 5}$, respectively, and we have shown Theorem 1 except for $G = \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which will be treated in the next section.

### 4.2 Trace formula for elliptic curves with torsion points

In this section we assume that $G = \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

**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 $i = 1, \ldots, k$. 


Then,
\[
\sum_{E \in \mathcal{E}_G(X)} \hat{a}_E(p_1^{e_1} r_1) \hat{a}_E(p_2^{e_2} r_2) \cdots \hat{a}_E(p_k^{e_k} r_k) = c \frac{c(G)}{\zeta(12/d(G))} X^{\frac{1}{d(G)}} + O_k \left( \sum_{i=1}^k \frac{1}{p_i} X^{\frac{1}{d(G)}} \right) + O_k \left( \prod_{i=1}^k p_i X^{\frac{1}{\ell(G)}} + \prod_{i=1}^k p_i^2 X^{\frac{1}{12}} \right),
\]

where
\[
c = \begin{cases} 
0 & \text{if } e_j = 1 \text{ and } r_j \text{ is odd for some } j, \\
-1 & \text{if } r_j = 2 \text{ for all } j \text{ with } e_j = 1, \text{ and the number of indexes } j \text{ with } e_j = 2 \text{ is odd,} \\
1 & \text{otherwise},
\end{cases}
\]

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

**Proof.** First, we consider the case \( e_j = 1 \) and \( r_j \) is odd for some \( j \). Without loss of generality, we can assume that \( e_1 = 1 \) and \( r_1 \) is odd. We fix the local conditions at primes \( p_j \), \( j = 2, 3, \ldots, k \) and the local condition at \( p_1 \) is \( a_E(p_1) = a \). By Theorem 3.15, there are
\[
c(G) \frac{H_G(a, p_1)}{p_1^2} \left| S' \right| G(X^{\frac{1}{d(G)}}) + O \left( \frac{H_G(a, p_1)}{p_1} \left( \prod_{i=2}^k c_1(p_i) X^{\frac{1}{\ell(G)}} \right) + H_G(a, p_1) \left( \prod_{i=2}^k c_2(p_i) X^{\frac{1}{12}} \right) \right)
\]
such elliptic curves in \( \mathcal{E}_G(X) \), and \( S' \) is the set of the fixed local conditions at \( p_i, i = 2, 3, \ldots, k \). For the values of \( c_1(p_i) \) and \( c_2(p_i) \), we refer to Theorem 3.15. Since \( \hat{a}_E(p_2^{e_2} r_2) \cdots \hat{a}_E(p_k^{e_k} r_k) \) is a constant and \( \sum_a q^{r_1} H_G(a, p_1) = 0 \) for odd \( r_1 \), only the error term above contributes to the sum. Due to \( \sum_a H_G(a, p) = p^2 + O_G(p) \), we can see that the total contribution from the error term is at most
\[
O \left( \prod_{i=1}^k p_i X^{\frac{1}{\ell(G)}} + \prod_{i=1}^k p_i^2 X^{\frac{1}{12}} \right).
\]
Next, we need to deal with the case of bad prime \( p_1 \). Since \( a_E(p) = 0 \) when \( E \) has additive reduction at \( p \), it is enough to consider the left two local conditions, which are split and nonsplit. The number of elliptic curves with split reduction at \( p_1 \) and that of elliptic curves with nonsplit reduction at \( p_1 \) is the same up to an error term. Hence, by the similar argument above, the contribution comes from the error term and is at most
\[
O_k \left( \frac{1}{p_1^2} \left( \prod_{i=2}^k p_i X^{\frac{1}{\ell(G)}} \right) + \frac{p_1}{p_1^2} \left( \prod_{i=2}^k p_i^2 X^{\frac{1}{12}} \right) \right)
\]
and the case \( e_j = 1 \) and \( r_j \) is odd for some \( j \) is done.

The next case we treat is \( e_i = 1 \) and \( r_i = 2 \) for all \( i \). First, we compute the contribution from good primes by imposing the local conditions \( \mathcal{L}C_{p_i} = a_i \) for all \( i = 1, \ldots, k \) and varying the \( a_i \) within the Weil bound \( |a_i| < 2 \sqrt{p_i} \). The corresponding contribution is, by Theorem 3.15,
\[
\left( \prod_{i=1}^{k} \frac{p_i^{12/d(G)}}{p_i^3} \right) \frac{c(G)}{\zeta(12/d(G))} X^{1/2} \left( \sum_{|a_i|<\sqrt{p_i}} a_i^2 H_G(a_1, p_1) a_2^2 H_G(a_2, p_2) \cdots a_k^2 H_G(a_k, p_k) \right) \]

which is, by the identity \( \sum_{|a|<\sqrt{p}} a^2 H_G(a, p) = p^3 + O_G(p^2) \),

\[
\frac{c(G)}{\zeta(12/d(G))} X^{1/2} + O_k \left( \left( \sum_{i=1}^{k} \frac{1}{p_i^2} \right) X^{1/4} + \left( \prod_{i=1}^{k} \frac{1}{p_i} \right) X^{1/12} + \left( \prod_{i=1}^{k} \frac{1}{p_i} \right)^2 X^{1/12} \right).
\]

When \( \mathcal{L}C_{p_i} \) is multi, \( \hat{\alpha}_E(p_i)^2 = \frac{1}{p_i} \). Then using the trivial bound \( \hat{\alpha}_E(p_i)^2 \leq 4 \) for the other primes \( p_j \), the contribution for this case is

\[
\ll k \left( \sum_{i=1}^{k} \frac{1}{p_i^2} \right) X^{1/4} + \sum_{i=1}^{k} \frac{1}{p_i} X^{1/12} + X^{1/12}.
\]

The last case is when \( e_1 = e_2 = \cdots = e_l = 2 \) and \( e_j = 1 \) and \( r_j = 2 \) for \( l < j \leq k \). Note that \( \hat{\alpha}_E(p^2) = \hat{\alpha}_E(p)^2 - 2 \) for \( E \) with good reduction at \( p \) and \( \hat{\alpha}_E(p^2) = \hat{\alpha}_E(p)^2 \) for \( E \) with bad reduction at \( p \). Hence, it is enough to consider elliptic curves with good reduction at all the primes \( p_i \). This amounts to

\[
\sum_{E \text{ has good reduction at functions of } p_i} (\hat{\alpha}_E(p_1)^2 - 2) \cdots (\hat{\alpha}_E(p_l)^2 - 2) \hat{\alpha}_E(p_{l+1})^2 \cdots \hat{\alpha}_E(p_k)^2,
\]

which is equal to

\[
(-1)^l \frac{c(G)}{\zeta(12/d(G))} X^{1/4} + O_k \left( \left( \sum_{i=1}^{k} \frac{1}{p_i^2} \right) X^{1/4} + \left( \prod_{i=1}^{k} \frac{1}{p_i} \right) X^{1/12} + \left( \prod_{i=1}^{k} \frac{1}{p_i} \right)^2 X^{1/12} \right)
\]

by the result of the previous case and the identity \( (1-2)^l = (-1)^l \).

\[
\boxempty
\]

### 4.3 The distribution of analytic ranks of elliptic curves

From now on, assume that every elliptic curve \( L \)-function satisfies the generalized Riemann hypothesis. Let \( \gamma_E \) denote the imaginary part of a non-trivial zero of \( L(s, E) \). We index them using the natural order in real numbers:

\[
\cdots \gamma_{E,-3} \leq \gamma_{E,-2} \leq \gamma_{E,-1} \leq \gamma_{E,0} \leq \gamma_{E,1} \leq \gamma_{E,2} \leq \gamma_{E,3} \cdots
\]

if analytic rank \( r_E \) is odd,
\[ \gamma_{E,-3} \leq \gamma_{E,-2} \leq \gamma_{E,-1} \leq 0 \leq \gamma_{E,1} \leq \gamma_{E,2} \leq \gamma_{E,3} \]

otherwise.

In this section, we also assume that \( G = \mathbb{Z}/2\mathbb{Z} \) or \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \). For elliptic curves in \( E_G \), we obtain an upper bound on every \( n \)th moment of analytic ranks, and as a corollary, we show that there are not so many elliptic curves with large ranks. For this purpose, we compute an \( n \)-level density with multiplicity. The primary reference is [16, Part VI].

For the \( n \)-level density, we choose the same test function for some \( \sigma_n \) in the previous section:

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

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

\[
\int_{\mathbb{R}} |u| \hat{\phi}_n(u)^2 du = \frac{1}{6} \phi_n(0)^2. \tag{19}
\]

We show that the \( n \)-level density holds by taking \( \sigma_n = \frac{1}{9n} \) and \( \frac{1}{10n} \) for \( G = \mathbb{Z}/2\mathbb{Z} \) and \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \), respectively.

The \( n \)-level density with multiplicity is

\[
D^*_n(E_G, \Phi) = \frac{1}{|E_G(X)|} \sum_{E \in E_G(X)} \sum_{j_1, j_2, \ldots, j_n} \phi_n(\gamma_{E,j_1} \log X \frac{1}{2\pi}) \phi_n(\gamma_{E,j_2} \log X \frac{1}{2\pi}) \cdots \phi_n(\gamma_{E,j_n} \log X \frac{1}{2\pi}),
\]

where \( \gamma_{E,j_k} \) is an imaginary part of \( j_k \)th zero of \( L(s, E) \). Then, trivially we have

\[
\frac{1}{|E_G(X)|} \sum_{E \in E_G(X)} r_E^n \leq \frac{1}{\phi_n(0)^n} D^*_n(E_G, \Phi). \tag{20}
\]

By the same argument in [6, §4], we have

\[
D^*_n(E_G, \Phi) \leq \frac{1}{|E_G(X)|} \sum_S |\hat{\phi}_n(0)|^{|S|} \left( -\frac{2}{\log X} \right)^{|S|} \times \sum_{m_{i_1}, m_{i_2}, \ldots, m_{i_k}} \frac{\Lambda(m_{i_1}) \Lambda(m_{i_2}) \cdots \Lambda(m_{i_k})}{\sqrt{m_{i_1} m_{i_2} \cdots m_{i_k}}} \hat{\phi}_n(\log m_{i_1} \log X) \cdots \hat{\phi}_n(\log m_{i_k} \log X) \times \sum_{E \in E_G(X)} \hat{a}_E(m_{i_1}) \hat{a}_E(m_{i_2}) \cdots \hat{a}_E(m_{i_k}) + O\left( \frac{1}{\log X} \right),
\]

where each of the integers \( m_i \) is a prime or a square of a prime with \( m_i \leq X^{\sigma_n} \) and \( S = \{i_1, i_2, \ldots, i_k\} \) runs over every subset of \( \{1, 2, 3, \ldots, n\} \). Using the Frobenius trace formula (Theorem 4.3), we can prove the following propositions as we did in [6, Proposition 4.1, 4.2].
**Proposition 4.4.** Let $\hat\phi$ 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

$$
\sum_{E \in \mathcal{E}_G(X)} \sum_{m_1 m_2 \ldots m_k \neq \square} \frac{\Lambda(m_1) \cdots \Lambda(m_k)\hat{\alpha}_E(m_1) \cdots \hat{\alpha}_E(m_k)}{\sqrt{m_1 m_2 \ldots m_k}} \hat{\phi}_n \left( \frac{\log m_1}{\log X} \right) \cdots \hat{\phi}_n \left( \frac{\log m_k}{\log X} \right) \ll |\mathcal{E}_G(X)|.
$$

**Proof.** Note that $\hat{\alpha}_E(m_1) \hat{\alpha}_E(m_2) \cdots \hat{\alpha}_E(m_k)$ is of the form

$$
\hat{\alpha}_E(p_1)^{e_1} \hat{\alpha}_E(p_2)^{e_2} \cdots \hat{\alpha}_E(p_t)^{e_t} \hat{\alpha}_E(q_2^{l_1}) \hat{\alpha}_E(q_2^{l_2}) \cdots \hat{\alpha}_E(q_2^{l_s}),
$$

with $e_1 + \cdots + e_t + l_1 + \cdots + l_s = k$. Here $p_1, p_2, \ldots, p_t$ are distinct primes and $q_1, q_2, \ldots, q_s$ are distinct primes, but some $q_j$ might be equal to some $p_i$. For a while we assume that the primes $p_1, \ldots, p_t, q_1, \ldots, q_s$ are all distinct.

By our assumption, one of the exponents $e_i$ is odd. In this case, the proof of Theorem 4.3 also works, and we have

$$
\sum_{E \in \mathcal{E}(X)} \hat{\alpha}_E(p_1)^{e_1} \hat{\alpha}_E(p_2)^{e_2} \cdots \hat{\alpha}_E(p_t)^{e_t} \hat{\alpha}_E(q_2^{l_1}) \hat{\alpha}_E(q_2^{l_2}) \cdots \hat{\alpha}_E(q_2^{l_s}) = O \left( \prod_{p < X} \log p \right)^k\left( \sum_{p < X^{3n}} p^{\delta} \log p \right)^k.
$$

The contribution of this case in the worst situation is at most

$$
\ll X^{\frac{1}{\delta(G)}} \left( \sum_{p < X^{3n}} p^{\delta} \log p \right)^k + X^{\frac{1}{12}} \left( \sum_{p < X^{3n}} p^{\delta} \log p \right)^k
$$

$$
\ll X^{\frac{1}{\delta(G)}} (X^{\frac{2}{3}})^n + X^{\frac{1}{12}} (X^{\frac{2}{3}})^n \ll X^{\frac{1}{\delta(G)}},
$$

where the last inequality holds by taking $\sigma_n = \min\left( \frac{2}{3n} \left( \frac{1}{d(G)} - \frac{1}{\delta(G)} \right), \frac{2}{5n} \left( \frac{1}{d(G)} - \frac{1}{12} \right) \right)$, which are $\frac{1}{9n}$ and $\frac{1}{10n}$, respectively.

We assume that some $p_i$ is equal to some $q_j$. Since $\hat{\alpha}_E(q_2^j) \hat{\alpha}_E(q_2^j) = (\hat{\alpha}_E(q_2^j)^2 - 2)^j$ if $E$ has good reduction at $q$, and $\hat{\alpha}_E(q_2^j) = \hat{\alpha}_E(q_2^j)$ otherwise, still we can use the Frobenius trace formula. □

**Proposition 4.5.** Let $\hat{\phi}$ 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 $\{1, 2, \ldots, n\}$,

$$
\frac{1}{|\mathcal{E}_G(X)|} \left( \sum_{E \in \mathcal{E}_G(X)} \sum_{m_1 m_2 \ldots m_k \neq \square} \frac{\Lambda(m_1) \cdots \Lambda(m_k)\hat{\alpha}_E(m_1) \cdots \hat{\alpha}_E(m_k)}{\sqrt{m_1 m_2 \ldots m_k}} \hat{\phi}_n \left( \frac{\log m_1}{\log X} \right) \cdot \hat{\phi}_n \left( \frac{\log m_2}{\log X} \right) \cdots \hat{\phi}_n \left( \frac{\log m_k}{\log X} \right) \right)
$$

$$
= \sum_{S_2 \subseteq S \subseteq \{1, 2, \ldots, n\}} \left( \frac{1}{2} \hat{\phi}_n(0) \right)^{|S_2|} |S_2|! \left( \int_{\mathbb{R}} |u| \hat{\phi}_n(u)^2 \ du \right)^{|S_2|} + O \left( \frac{1}{\log X} \right).
$$
Proof. In this proof, we compute the double sum not considering the term \( \frac{1}{|E(X)|} \left( \frac{-2}{\log X} \right)^k \). We show that every contribution except one is \( \ll X^{\frac{1}{\log(\log X)}} (\log X)^{k-1} \); hence, they become the error term \( O(1/\log X) \) in the end.

Note that \( \hat{a}_E(m_{i_1}) \hat{a}_E(m_{i_2}) \cdots \hat{a}_E(m_{i_k}) \) is of the form
\[
\hat{a}_E(p_{i_1})^{e_1} \hat{a}_E(p_{i_2})^{e_2} \cdots \hat{a}_E(p_{i_t})^{e_t} \hat{a}_E(q_{j_1})^{l_1} \hat{a}_E(q_{j_2})^{l_2} \cdots \hat{a}_E(q_{j_s})^{l_s},
\]
with \( e_1 + \cdots + e_t + l_1 + \cdots + l_s = k \) and the exponents \( e_i \) are even. If \( e_i \geq 4 \) for some \( i \) or \( l_j \geq 2 \) for some \( j \), then by the trivial bound, this term is majorized by \( X^{\frac{1}{\log(\log X)}} (\log X)^{k-1} \). Let \( S_2 \) be a subset of \( S \) with even cardinality \( 2t \):
\[
S_2 = \{ i_{a_1}, i_{a_2}, \ldots, i_{a_{2t-1}}, i_{a_{2t}} \}, \quad S^c_2 = \{ i_{b_1}, i_{b_2}, \ldots, i_{b_s} \}.
\]
There are \((2t)!/2^t\) ways to pair up two elements in \( S_2 \). For example, we consider the following pairings:
\[
(i_{a_1}, i_{a_2}), (i_{a_3}, i_{a_4}), (i_{a_5}, i_{a_6}), \ldots, (i_{a_{2t-1}}, i_{a_{2t}}).
\]
This set of pairings corresponds the following sum:
\[
\sum_{E \in \mathcal{E}_G(X)} \hat{a}_E(p_{i_{a_1}})^2 \hat{a}_E(p_{i_{a_3}})^2 \cdots \hat{a}_E(p_{i_{a_{2t-1}}})^2 \hat{a}_E(q_{j_{b_1}})^2 \hat{a}_E(q_{j_{b_2}})^2 \cdots \hat{a}_E(q_{j_{b_s}})^2,
\]
where \( 2t + s = k \). By the Frobenius trace formula (Theorem 4.3), the above sum is
\[
|\mathcal{E}_G(X)| \cdot \left\{ \begin{array}{ll}
1 & \text{if } s \text{ is even}, \\
-1 & \text{if } s \text{ is odd}
\end{array} \right. + O \left( \left( \frac{1}{p_1} + \cdots + \frac{1}{p_t} + \frac{1}{q_1} + \cdots + \frac{1}{q_s} \right) X^{\frac{1}{\log(\log X)}} \right) + O \left( p_1 \cdots p_t q_1 \cdots q_s X^{\frac{1}{\log(\log X)}} + (p_1 \cdots p_t q_1 \cdots q_s)^2 X^{\frac{1}{\log X}} \right).
\]
The contribution from the second big O-term is dominated by
\[
(X^{2\sigma_n} \log X)^t (X^{2\sigma_n} \log X)^{s} X^{\frac{1}{\log(\log X)}} + (X^{2\sigma_n} \log X)^t (X^{2\sigma_n} \log X)^{s} X^{\frac{1}{\log(\log X)}} \ll X^{\frac{1}{\log(\log X)}} (\log X)^t.
\]
The contribution from the error term \( O \left( \left( \frac{1}{p_1} + \cdots + \frac{1}{p_t} + \frac{1}{q_1} + \cdots + \frac{1}{q_s} \right) X^{\frac{1}{\log(\log X)}} \right) \) is dominated by \( X^{\frac{1}{\log(\log X)}} (\log X)^{k-1} \). The main term of the sum, after being divided by \( |\mathcal{E}_G(X)| (\log X)^k \), is equal to
\[
\prod_{i=1}^{t} \left( \frac{-2}{\log X} \right)^2 \sum_{p} \frac{\log^2 p}{p} \hat{\phi}_n \left( \frac{\log p}{\log X} \right)^2 \times \prod_{j=1}^{s} \left( \frac{2}{\log X} \sum_{q} \frac{\log q}{q} \hat{\phi}_n \left( \frac{2 \log q}{\log X} \right) \right),
\]
which equals, by the prime number theorem,
\[
\left( 2^t \prod_{i=1}^{t} \int_{\mathbb{R}} |u| \hat{\phi}_n(u)^2 du \right) \left( \left( \frac{1}{2} \right)^s \prod_{j=1}^{s} \int_{\mathbb{R}} \hat{\phi}_n(u) du \right).
\]
Since there are \((2t)!/2^t\) ways to pair up two elements in \( S_2 \), the claim follows. \( \square \)
By Proposition 4.4, Proposition 4.5, and (19) we have the following inequality

\[ D^*_n(E_G, \Phi) \leq \phi_n(0)^n \sum_{S} \left( \frac{1}{\sigma_n} \right)^{|S|} \sum_{S \subseteq S \subseteq |S| \text{even}} \left( \frac{1}{2} \right)^{|S|} |S_2|! \left( \frac{1}{6} \right)^{|S_2|} + O \left( \frac{1}{\log X} \right), \]

and, by (20), we have

**Theorem 4.6.** Assume GRH for elliptic curve $L$-functions. Let $r_E$ be the analytic rank of an elliptic curve $E$. For every positive integer $n$, we have

\[ \limsup_{X \to \infty} \frac{1}{|E_G(X)|} \sum_{E \in E_G(X)} r_E^n \leq \sum_{S} \left( \frac{1}{\sigma_n} \right)^{|S|} \sum_{S \subseteq S \subseteq |S| \text{even}} \left( \frac{1}{2} \right)^{|S|} |S_2|! \left( \frac{1}{6} \right)^{|S_2|} \left( 1 \right) \left( \frac{1}{2} \right)^{|S_2|}, \]

where $S$ runs over subsets of $\{1, 2, 3, \ldots, n\}$, and $S_2$ runs over subsets of even cardinality of the set $S$. In particular, the average analytic rank for $E_{\mathbb{Z}/2\mathbb{Z}}$ is bounded by 9.5 and the average analytic rank for $E_{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}}$ is bounded by 10.5.

Now, we show the sparsity of elliptic curves in $E_G$ with large analytic ranks. We choose the test function $\phi_{2n}(\alpha)$. Then $\hat{\phi}_{2n}(0) = \frac{1}{4} \sigma_{2n}$, and $\phi_{2n}(0) = \frac{1}{4} \sigma_{2n}^2$.

By Weil’s explicit formula, we have

\[ r_E \phi_{2n}(0) \leq \hat{\phi}_{2n}(0) - \frac{2}{\log X} \sum_{m_i} \hat{a}_E(m_i) \Lambda(m_i) \frac{\log m_i}{\log X} \left( \frac{\log m_i}{\log X} \right) + O \left( \frac{1}{\log X} \right), \]

hence

\[ r_E \leq \frac{1}{\sigma_{2n}} + \frac{4}{\sigma_{2n}^2} \left( - \frac{2}{\log X} \sum_{m_i} \hat{a}_E(m_i) \Lambda(m_i) \frac{\log m_i}{\log X} \left( \frac{\log m_i}{\log X} \right) \right) + O \left( \frac{1}{\sigma_{2n}^2 \log X} \right). \]

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

\[ - \frac{2}{\log X} \sum_{m_i} \hat{a}_E(m_i) \Lambda(m_i) \frac{\log m_i}{\log X} \left( \frac{\log m_i}{\log X} \right) \geq \frac{C \sigma_{2n}}{4}. \]

Therefore,

\[ \left| \left\{ E \in E_G(X) \mid r_E \geq \frac{1 + C}{\sigma_{2n}} \right\} \right| \left( \frac{C \sigma_{2n}}{4} \right)^{2n} \leq \sum_{E \in E_G(X)} \left( - \frac{2}{\log X} \sum_{m_i} \hat{a}_E(m_i) \Lambda(m_i) \frac{\log m_i}{\log X} \left( \frac{\log m_i}{\log X} \right) \right)^{2n} \leq \left( \frac{\sigma_{2n}^2}{4} \right)^{2n} \sum_{S \subseteq \{1, 2, 3, \ldots, n\}} \left( \frac{1}{2} \right)^{|S_2|} \left( \frac{1}{6} \right)^{|S_2|} |E_G(X)| + O \left( \frac{X^{\frac{1}{4} \log X}}{\log X} \right), \]

where the second inequality is justified by Proposition 4.4 and Proposition 4.5, and finally, we obtain
Theorem 4.7. Assume GRH for elliptic curve $L$-functions. Let $C$ be a positive constant and $n$ be a positive integer. We have

$$P\left(r_E \geq \frac{(1 + C)}{\sigma_{2n}}\right) \leq \sum_{k=0}^{n} \binom{2n}{2k} \left(\frac{1}{2}\right)^{2n-2k}(2k)!\left(\frac{1}{6}\right)^{k} \left(\frac{C}{\sigma_{2n}}\right)^{2n},$$

where $\sigma_{2n} = \frac{1}{18n}$ and $\frac{1}{20n}$ for $G = \mathbb{Z}/2\mathbb{Z}$ and $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, respectively.

APPENDIX A

Here we summarize $f_G(a, b)$ and $g_G(a, b)$ for all torsion subgroup.

\[
\begin{align*}
f_5 &= -27a^4 + 324a^3b - 378a^2b^2 - 324ab^3 - 27b^4, \\
g_5 &= 54a^6 - 972a^5b + 4050a^4b^2 + 4050a^2b^4 + 972ab^5 + 54b^6, \\
f_6 &= -243a^4 - 324a^3b - 810a^2b^2 - 324ab^3 - 27b^4, \\
g_6 &= -1458a^6 - 2916a^5b + 7290a^4b^2 + 9720a^3b^3 + 5346a^2b^4 + 972ab^5 + 54b^6, \\
f_7 &= -324a^4 + 336a^3b + 1512a^2b^2 + 378a^2b^3 + 945ab^4 + 378b^5 - 108ab^7 - 27b^8, \\
g_7 &= 54a^{12} - 972a^{11}b + 6318a^{10}b^2 - 19116a^9b^3 + 30780a^8b^4 - 26244a^7b^5 + 14742a^6b^6 - 11988a^5b^7 + 9396a^4b^8 - 810a^2b^9 + 324ab^{11} + 54b^{12}. \\
f_8 &= -432a^8 + 1728a^7b - 6048a^6b^2 + 12096a^5b^3 - 12960a^4b^4 + 7776a^3b^5 - 2592a^2b^6 + 432ab^7 - 27b^8, \\
g_8 &= -3456a^{12} + 20736a^{11}b - 190080a^{10}b^2 + 555984a^9b^3 - 855360a^8b^4 + 840672a^7b^5 + 54b^{12}, \\
f_9 &= -27a^{12} + 324a^{11}b - 1458a^{10}b^2 + 3456a^9b^3 - 5103a^8b^4 + 4860a^7b^5 - 3078a^6b^6 + 972a^5b^7 + 486a^4b^8 - 756a^3b^9 + 324a^2b^{10} - 27b^{12}, \\
g_9 &= 54a^{18} - 972a^{17}b + 7290a^{16}b^2 - 30780a^{15}b^3 + 84078a^{14}b^4 - 160380a^{13}b^5 + 222912a^{12}b^6 - 228420a^{11}b^7 + 174960a^{10}b^8 - 109728a^9b^9 + 73386a^8b^{10} - 58320a^7b^{11} + 39690a^6b^{12} - 16524a^5b^{13} + 1458a^4b^{14} + 2268a^3b^{15} - 972a^2b^{16} + 54b^{18}, \\
f_{10} &= -432a^{12} + 3456a^{11}b - 11232a^{10}b^2 + 19440a^9b^3 - 19440a^8b^4 + 7776a^7b^5 + 6912a^6b^6 - 11664a^5b^7 + 6480a^4b^8 - 1080a^3b^9 - 432a^2b^{10} + 216ab^{11} - 27b^{12}, \\
g_{10} &= 3456a^{18} - 41472a^{17}b + 217728a^{16}b^2 - 661824a^{15}b^3 + 129600a^{14}b^4 - 1767744a^{13}b^5 + 139288a^{12}b^6 - 2037312a^{11}b^7 + 2133216a^{10}b^8 - 1803600a^9b^9 + 981072a^8b^{10} - 199584a^7b^{11} - 128304a^6b^{12} + 112752a^5b^{13} - 32400a^4b^{14} - 216a^3b^{15} + 2592a^2b^{16} - 648ab^{17} + 54b^{18}. 
\end{align*}
\]
\[ f_{12} = -3888a^{16} + 31104a^{15}b - 194400a^{14}b^2 + 816480a^{13}b^3 - 2269296a^{12}b^4 + 4416768a^{11}b^5 \\
- 6318000a^{10}b^6 + 6855840a^9b^7 - 5747760a^8b^8 + 3753216a^7b^9 - 1907712a^6b^{10} \\
+ 747792a^5b^{11} - 221616a^4b^{12} + 47952a^3b^{13} - 7128a^2b^{14} + 648ab^{15} - 27b^{16} \]

\[ g_{12} = -93312a^{24} + 1119744a^{23}b - 2519424a^{22}b^2 - 19502208a^{21}b^3 + 175146624a^{20}b^4 \\
- 738377856a^{19}b^5 + 2114216640a^{18}b^6 - 4566176064a^{17}b^7 + 7806726864a^{16}b^8 \\
- 10854158400a^{15}b^9 + 12478123872a^{14}b^{10} - 11984223456a^{13}b^{11} \\
+ 9676823760a^{12}b^{12} - 659002032a^{11}b^{13} + 3786612624a^{10}b^{14} \\
- 1831706784a^9b^{15} + 742184208a^8b^{16} - 249811776a^7b^{17} + 68988672a^6b^{18} \\
- 15353712a^5b^{19} + 2682720a^4b^{20} - 353808a^3b^{21} + 33048a^2b^{22} - 1944ab^{23} + 54b^{24} \]

\[ f_{2 \times 4} = -27a^4 - 378a^2b^2 - 27b^4 \]

\[ g_{2 \times 4} = -54a^6 + 1782a^4b^2 + 1782a^2b^4 - 54b^6 \]

\[ f_{2 \times 6} = -27a^8 + 1296a^6b^2 - 12960a^4b^4 - 393984a^2b^6 - 62208b^8 \]

\[ g_{2 \times 6} = 54a^{12} - 3888a^{10}b^2 + 85356a^8b^4 - 2363904a^6b^6 + 43670016a^4b^8 + 86593536a^2b^{10} \\
- 5971968b^{12} \]

\[ f_{2 \times 8} = -452984832a^{16} - 1811939328a^{15}b - 3170893824a^{14}b^2 - 3170893824a^{13}b^3 \\
- 1953497088a^{12}b^4 - 707788800a^{11}b^5 - 88473600a^{10}b^6 + 51314688a^9b^7 \\
+ 31961088a^8b^8 + 6414336a^7b^9 - 1382400a^6b^{10} - 1382400a^5b^{11} - 476928a^4b^{12} \\
- 96768a^3b^{13} - 12096a^2b^{14} - 864ab^{15} - 27b^{16} \]

\[ g_{2 \times 8} = 3710851743744a^{24} + 22265110462464a^{23}b + 61229053771776a^{22}b^2 \\
+ 10248422952960a^{21}b^3 + 114456583471104a^{20}b^4 + 90104118902784a^{19}b^5 \\
+ 49618146557952a^{18}b^6 + 17546820452352a^{17}b^7 + 219471151040a^{16}b^8 \\
- 1694163271680a^{15}b^9 - 1411953721344a^{14}b^{10} - 656375021568a^{13}b^{11} \\
- 246536994816a^{12}b^{12} - 82046877696a^{11}b^{13} - 22061776896a^{10}b^{14} \\
- 3308912640a^9b^{15} + 535818240a^8b^{16} + 535486464a^7b^{17} + 189278208a^6b^{18} \\
+ 42964992a^5b^{19} + 6822144a^4b^{20} + 760320a^3b^{21} + 57024a^2b^{22} + 2592ab^{23} + 54b^{24} \]

**ACKNOWLEDGEMENT**

We would like to thank Dohyeong Kim, John Voight, John Cullinan, and Junyeong Park for the valuable discussion, Chan-Ho Kim for introducing the work of Harron and Snowden [12], and Daniel Fiorilli for his comments.

Peter J. Cho and Keunyoung Jeong acknowledge the support by the NRF grant funded by the Korea government(MSIT) (No. 2019R1F1A1062599, 2019R1C1C1004264), respectively, and both of them are also supported by the Basic Science Research Program (2020R1A4A1016649).

**JOURNAL INFORMATION**

The *Journal of the London Mathematical Society* is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission.
All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

REFERENCES

1. M. Bhargava and W. Ho, *On average sizes of Selmer groups and ranks in families of elliptic curves having marked points*, Preprint.
2. M. Bhargava and A. Shankar, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, Ann. of Math. (2) **181** (2015), no. 2, 587–621.
3. M. Bhargava and A. Shankar, *The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1*, Preprint, https://arxiv.org/abs/1312.7859.
4. A. Brumer, *The average rank of elliptic curves I*, Invent. Math. **109** (1992), no. 3, 445–472.
5. S. Chan, J. Hanselman, and W. Li, *Ranks, 2-Selmer groups, and tamagawa numbers of elliptic curves with \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \)-torsion*, Proceedings of the 13th Algorithmic Number Theory Symposium, Open Book Ser. 2, Math. Sci. Publ., Berkeley, CA, 2019, pp. 173–189.
6. P. J. Cho and K. Jeong, *On the distribution of analytic ranks of elliptic curves*, Preprint.
7. J. Cullinan, M. Kenney, and J. Voight, *On a probabilistic local-global principle for torsion on elliptic curves*, Preprint, https://arxiv.org/abs/2005.06669.
8. L. E. Dickson, *Criteria for the irreducibility of functions in a finite field*, Bull. Amer. Math. Soc. **13** (1906), no. 1, 1–8.
9. F. Diamond and J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer, New York, 2005, xvi+436 pp. ISBN: 0-387-23229-X
10. D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illnois Univ., Carbondale, Ill., 1979), Lecture Notes in Mathematics, vol. 751, Springer, Berlin, 1979, pp. 108–118.
11. I. Gracia-Selfa and J. M. Tornero, *A complete Diophantine characterization of the rational torsion of an elliptic curve*, Acta Math. Sin. (Engl. Ser.) **28** (2012), no. 1, 83–96.
12. R. Harron and A. Snowden, *Counting elliptic curves with prescribed torsion*, J. Reine Angew. Math. **729** (2017), 151–170.
13. D. R. Heath-Brown, *The average analytic rank of elliptic curves*, Duke Math. J. **122** (2004), no. 3, 591–623.
14. D. S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) **33** (1976), no. 2, 193–237.
15. N. Kaplan and I. Petrow, *Elliptic curves over a finite field and the trace formula*, Proc. Lond. Math. Soc. (3) **115** (2017), no. 6, 1317–1372.
16. S. J. Miller, *1- and 2-level densities for families of elliptic curves: Evidence for the underlying group symmetries*, Ph.D. thesis, Princeton University, 2002, 225 pp. ISBN: 978-0493-55316-0.
17. J. Park, B. Poonen, J. Voight, and M. M. Wood, *A heuristic for boundness of ranks of elliptic curves*, J. Eur. Math. Soc. **21** (2019), no. 9, 2859–2903.
18. Z. Rudnick and P. Sarnak, *Zeros of principal L-functions and random matrix theory*, Duke Math. J. **81** (1996), no. 2, 269–322.
19. SageMath, *The Sage Mathematics Software System (Version 9.2)*, The Sage Developers, https://www.sagemath.org.
20. R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. **A 46** (1987), no. 2, 183–211.
21. M. Watkins, *A dis cursus on 21 as a bound for ranks of elliptic curves over \( \mathbb{Q} \), and sundry related topics*, https://magma.maths.usyd.edu.au/~watkins/papers/DISCURSUS.pdf.
22. M. Watkins, S. Donnelly, N. D. Elkies, T. Fisher, A. Granville, and N. F. Rogers, *Ranks of quadratic twists of elliptic curves*, Numéro consacré au trimestre "Méthodes arithmétiques et applications"; automne 2013, Publ. Math. Basançon Algèbre Théorie Nr., 2014/2, Presses Univ. Franche-Comté, Besançon, 2015, pp. 63–98.
23. M. P. Young, *Low-lying zeros of families of elliptic curves*, J. Amer. Math. Soc. **19** (2006), no. 1, 205–250.