# AVERAGE ANALYTIC RANK OF ELLIPTIC CURVES WITH PRESCRIBED TORSION 

PETER J. CHO AND KEUNYOUNG JEONG


#### Abstract

We show that average analytic rank of elliptic curves with prescribed torsion $G$ is bounded for every torsion group $G$ under GRH for elliptic curve $L$-functions.


## 1. Introduction

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

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

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 and $\mathcal{E}$ has a bijection with 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 [Gol79] would be true.

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

Recently, Park, Poonen, Voight, and Wood [PPVW19] has brought out a more refined conjecture ${ }^{1}$ which not only claims Conjecture 1 but also proposes the number of elliptic curves with algebraic rank $\geq r$ for $1 \leq r \leq 20$.

Conjecture 2. [PPVW19, Corollary 7.2.6, Theorem 7.3.3]
(1) The proportion of elliptic curves with algebraic rank 0 and the proportion of 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 proportion of elliptic curves over $\mathbb{Q}$ with algebraic rank $\geq r$ and height $\leq X$ is $X^{\frac{21-r}{24}+o(1)}$.

A major breakthrough for Conjecture 1 was made by Bhargava and Shankar [BS15, BS]. 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

Peter J. Cho and Keunyoung Jeong acknowledge the support by the NRF grant funded by the Korea government(MSIT) (No. 2019R1F1A1062599, 2019R1C1C1004264) respectively and they are also supported by the Basic Science Research Program(2020R1A4A1016649) together.
${ }^{1}$ We note that Conjecture 2 is also suggested by [Wat ${ }^{+} 14$, Wat] with a different heuristic method.

Table 1.

| $G$ | $d(G)$ | $G$ | $d(G)$ |  | $G$ |
| ---: | ---: | ---: | ---: | ---: | ---: |
| 0 | $6 / 5$ | $\mathbb{Z} / 6 \mathbb{Z}$ | 6 |  | $\mathbb{Z} / 12 \mathbb{Z}$ |
| $\mathbb{Z} / 2 \mathbb{Z}$ | 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 |

0.2062. For the average analytic rank, Brumer [Bru92] showed that it is bounded by 2.3 under GRH for elliptic curve $L$-functions. This bound was lowered to 2 and $\frac{25}{14}$ by Heath-Brown [Hea04] and Young [You06] respectively.

On the other hand, Harron and Snowden [HS14] counted elliptic curves with prescribed torsion $G$. From now on, 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

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

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

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

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

Let

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

Harron and Snowden showed that

$$
\lim _{X \rightarrow \infty} \frac{\log \left|\mathcal{E}_{G}(X)\right|}{\log X}=\frac{1}{d(G)},
$$

where $d(G)$ 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.

Not much is known about the distribution of (algebraic or analytic) ranks of elliptic curves with prescribed torsion group $G$. In [PPVW19, §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 [BH, Theorem 1.1] obtained bounds for the average algebraic rank of the families of elliptic curves with marked torsion point $(0,0)$ of order 2 and 3 respectively, which are $7 / 6$ and $3 / 2$. We show that for any torsion group $G$ average analytic rank over the family $\mathcal{E}_{G}$ is bounded.

Theorem 1. Let $G$ be a torsion group. For $G=\mathbb{Z} / n \mathbb{Z}, n=7,9,8,9,10$, and 12 and $G=\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 2 m \mathbb{Z}$, $m=3,4$, we assume the moment conditions (8), (9). 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 $\frac{1}{2}+5 d(G)$.

For $G=\mathbb{Z} / 2 \mathbb{Z}$ and $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 2 \mathbb{Z}$, we have additional information on the distribution of analytic ranks. First, we can show that there are not many elliptic curves with torsion $G$ with a high rank. Let $P_{G}\left(r_{E} \geq a\right)$ denote the probability of elliptic curves with torsion $G$ such that analytic rank $r_{E} \geq a$.

Theorem 2 (Theorem 4.7). Assume GRH for elliptic curve $L$-functions. Let $C$ be a positive constant, let $n$ a positive integer. We have, for $G=\mathbb{Z} / 2 \mathbb{Z}$ and $G=\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 2 \mathbb{Z}$,

$$
P_{G}\left(r_{E} \geq \frac{(1+C)}{\sigma_{2 n}}\right) \leq \frac{\sum_{k=0}^{n}\binom{2 n}{2 k}\left(\frac{1}{2}\right)^{2 n-2 k}(2 k)!\left(\frac{1}{6}\right)^{k}}{\left(\frac{C}{\sigma_{2 n}}\right)^{2 n}}
$$

where $\sigma_{2 n}=\frac{1}{18 n}$ and $\frac{1}{20 n}$ for $G=\mathbb{Z} / 2 \mathbb{Z}$ and $G=\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 2 \mathbb{Z}$ respectively. In particular, the probabilities $P_{\mathbb{Z} / 2 \mathbb{Z}}\left(r_{E} \geq 23\right)$ and $P_{\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 2 \mathbb{Z}}\left(r_{E} \geq 25\right)$ are both at most 0.0234.

We note that there is an analogue [Hea04, Theorem 2] of Theorem 2 without torsion restriction, which says

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

We can also give an explicit bound on the $n$-th moment of analytic ranks of elliptic curves with torsion $G$.
Theorem 3 (Theorem 4.6). Assume GRH for elliptic curve $L$-functions. Let $\sigma_{n}=\frac{1}{9 n}$ and $\frac{1}{10 n}$ for $G=\mathbb{Z} / 2 \mathbb{Z}$ and $G=\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 2 \mathbb{Z}$ respectively. For every positive integer $n$, we have

$$
\limsup _{X \rightarrow \infty} \frac{1}{\left|\mathcal{E}_{G}(X)\right|} \sum_{E \in \mathcal{E}_{G}(X)} r_{E}^{n} \leq \sum_{S}(9 n)^{\left|S^{c}\right|} \sum_{\substack{S_{2} \subset S \\\left|S_{2}\right| \text { even }}}\left(\frac{1}{2}\right)^{\left|S_{2}^{c}\right|}\left|S_{2}\right|!\left(\frac{1}{6}\right)^{\left|S_{2}\right| / 2}
$$

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 of $\mathcal{E}_{\mathbb{Z} / 2 \mathbb{Z}}$ and that of $\mathcal{E}_{\mathbb{Z}} / 2 \mathbb{Z} \times \mathbb{Z} / 2 \mathbb{Z}$ are at most 9.5 and 10.5 respectively.

Our rank results are obtained from 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 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 toward 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 a result of Chan, Hanselman and Li [CHL19]. Young [You06, §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 EichlerSelberg trace formula by Kaplan and Petrow [KP17]. This version of Eichler-Selberg trace formula is indispensable to deal with every torsion group $G$. However, to bound up the average rank, we need to count elliptic curves satisfying a local condition. 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 $a_{E}(p)=p+1-\left|E\left(\mathbb{F}_{p}\right)\right|=a$ respectively. For torsion groups $G \in \mathcal{G}_{\leq 4}$, we have

Theorem 4 (Theorem 3.7). For a prime $p \geq 5$, a local condition $\mathcal{L C}$, and a group $G$ in $\mathcal{G}_{\leq 4}$,

$$
\left|\mathcal{E}_{G, p}^{\mathcal{L C}}(X)\right|=c(G) \cdot c_{G, \mathcal{L C}}(p) \cdot \frac{p^{\frac{12}{d(G)}}}{p^{\frac{12}{d(G)}}-1} X^{\frac{1}{d(G)}}+O\left(h_{G, \mathcal{L C}}(p, X)\right)
$$

where $c_{G, \mathcal{L C}}(p)$ is a constant depending on $G, p, \mathcal{L C}$ and $h_{G, \mathcal{L C}}(p, X)$ is a function whose order of magnitude is less than $p X^{\frac{1}{e(G)}}+p^{2} X^{\frac{1}{12}}$.

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

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

$$
\lim _{X \rightarrow \infty} \frac{\left|\mathcal{E}_{p}^{\mathcal{L}}(X)\right|}{|\mathcal{E}(X)|} \neq \lim _{X \rightarrow \infty} \frac{\left|\mathcal{E}_{G, p}^{\mathcal{L}}(X)\right|}{\left|\mathcal{E}_{G}(X)\right|} .
$$

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 $\mathcal{L C}=$ 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 $G \in \mathcal{G}_{\leq 4}$. 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 $G \in \mathcal{G}_{\geq 5}$, there is a set of primes $p$ of positive density such that $c_{G, \operatorname{mult}}(p)$ is proportional to the number of cusps of corresponding modular curves.

We note that $c_{G, \text { mult }}(p)$ can be interpreted as the probability that an elliptic curve with prescribed torsion $G$ has multiplicative reduction at $p$. For details and other examples, we recommend to see Corollaries 3.11 to 3.13.

## 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

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

and $\mathcal{G}_{\geq 5}$ be the set of torsion groups of order $\geq 5$. We often use $n$ and $2 \times 2 m$ in place of $G=\mathbb{Z} / n \mathbb{Z}$ and $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 2 m \mathbb{Z}$ to ease the notation.

For each torsion subgroup, we should clarify the model we use. When $G$ in $\mathcal{G}_{\leq 4}$, we recall the result of [GT12, Theorem 1.1] shows that $E_{A, B}: y^{2}=x^{3}+A x+B$ 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 $\Phi_{G}=\left(f_{G}, g_{G}\right)$ for

$$
\begin{array}{ll}
f_{2}(a, b)=a, & g_{2}(a, b)=b^{3}+a b, \\
f_{3}(a, b)=6 a b+27 a^{4}, & g_{3}(a, b)=b^{2}-27 a^{6},  \tag{1}\\
f_{4}(a, b)=-3 a^{2}+6 a b^{2}-2 b^{4}, & g_{4}(a, b)=\left(2 a-b^{2}\right)\left(a^{2}+2 a b^{2}-b^{4}\right), \\
f_{2 \times 2}(a, b)=-\left(a^{2}+3 b^{2}\right) / 4, & g_{2 \times 2}(a, b)=\left(b^{3}-a^{2} b\right) / 4 .
\end{array}
$$

We recall that the set

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

which parametrizes all elliptic curves $E_{A, B}$ whose height is less than $X$ and each isomorphism class appears only at once, by the minimality condition. When $G$ is in $\mathcal{G}_{\leq 4}$, the set

$$
\mathcal{E}_{G}(X)=\left\{(A, B) \in \mathcal{E}(X):(A, B)=\Phi_{G}(a, b) \text { for some } a, b \in \mathbb{Z}\right\}
$$

parametrizes all elliptic curves with prescribed torsion subgroup $G$.
For $G$ in $\mathcal{G}_{\geq 5}$, we use Tate's normal form

$$
\begin{equation*}
E(u, v): y^{2}+(1-v) x y-u y=x^{3}-u x^{2}, \tag{2}
\end{equation*}
$$

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 follow: (for example, [Kub76, Table 3])

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

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 $f_{G}(a, b)=b^{\operatorname{deg} f} f_{G}(a / b)$ and $g_{G}(a, b)=b^{\operatorname{deg} g} g_{G}(a / b)$ of $f_{G}$ and $g_{G}$ and change of coordinate give

$$
\begin{equation*}
y^{2}=x^{3}+f_{G}(a, b) x+g_{G}(a, b) . \tag{3}
\end{equation*}
$$

For simplicity, we use $f_{2 \times 4}(a, 4 b) / 8^{4}, g_{2 \times 4}(a, 4 b) / 8^{6}$ and $f_{2 \times 6}(a+3 b, b), g_{2 \times 6}(a+3 b, b)$ for $f_{2 \times 4}, g_{2 \times 4}, f_{2 \times 6}$ and $g_{2 \times 6}$. One can check that $f_{2 \times 4}, g_{2 \times 4}$ and $f_{2 \times 6}, g_{2 \times 6}$ represent all isomorphism classes of elliptic curves with the corresponding torsion. In Appendix 5, the table for $f_{G}$ and $g_{G}$ is provided. For any torsion subgroup $G$ in $\mathcal{G}_{\geq 5}$ we have $3 \operatorname{deg} f_{G}=2 \operatorname{deg} g_{G}$, and we define $d(G)$ as

$$
3 \operatorname{deg} f_{G}=2 \operatorname{deg} g_{G}=2 d(G)
$$

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

$$
\left\{(A, B) \in \mathcal{E}(X):(A, B)=\left(f_{G}, g_{G}\right)(a, b) \text { for some } a, b \in \mathbb{Z}\right\}
$$

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 $e^{4} \mid f_{G}(a, b)$ and $e^{6} \mid g_{G}(a, b)$, 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.

Here the problem is that the map $\left(f_{G}, g_{G}\right)$ does not care the minimality condition. Following [CKV, Theorem 3.3.1], we define a defect of $(a, b)$ to be

$$
e(a, b)=e=\max _{\substack{e^{\prime \prime}\left|f_{G}(a, b) \\ e^{\prime 6}\right| g_{G}(a, b)}} e^{\prime} .
$$

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 a defect of $(a, b)$. We remark that the image of $\Phi_{G}$ satisfies the minimality condition, so

$$
\begin{equation*}
\mathcal{E}_{G}(X)=\left\{(A, B) \in \mathcal{E}(X):(A, B)=\Phi_{G}(a, b) \text { for relatively prime integers } a, b\right\} \tag{4}
\end{equation*}
$$

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

$$
M_{G}(X)=\left\{(a, b) \in \mathbb{Z}^{2}:(a, b)=1, h\left(\Phi_{G}(a, b)\right) \leq X\right\}
$$

Hence $\Phi_{G}$ is a map from $\mathbb{Z}^{2}$ to $\mathbb{Z}^{2}$ when $G$ is in $\mathcal{G}_{\leq 4}$ and from $M_{G}(X)$ to $\mathbb{Z}^{2}$ when $G$ is in $\mathcal{G}_{\geq 5}$. Also, we define $M_{G}^{e}(X)$ as a set of elements of $M_{G}(X)$ 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 $\mathcal{G}_{\geq 5} \backslash\{\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 6 \mathbb{Z}, \mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 8 \mathbb{Z}\}$, 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 $(a, b) \equiv(1,1)(\bmod 2)$ or,
- $G=\mathbb{Z} / 8 \mathbb{Z}$ and $(a, b) \equiv(1,0)(\bmod 2)$ or,
- $G=\mathbb{Z} / 10 \mathbb{Z}$ and $(a, b) \equiv(1,0)(\bmod 2)$ or,
- $G=\mathbb{Z} / 12 \mathbb{Z}$ and $(a, b) \equiv(1,0)(\bmod 2)$ or,
- $G=\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 4 \mathbb{Z}$ and $(a, b) \equiv(1,1)(\bmod 2)$.
(ii) e has a prime divisor 3 if and only if
- $G=\mathbb{Z} / 7 \mathbb{Z}$ and $(a, b) \equiv(1,2)$ or $(2,1)(\bmod 3)$ or,
- $G=\mathbb{Z} / 9 \mathbb{Z}$ and $(a, b) \equiv(1,2)$ or $(2,1)(\bmod 3)$ or,
- $G=\mathbb{Z} / 12 \mathbb{Z}, a \not \equiv 0$, and $b \equiv 0(\bmod 3)$.

Proof. By the argument [CKV, p.17], the defect $e$ is a divisor of the least common multiplier of the two resultants $\operatorname{Res}\left(f_{G}(a, 1), g_{G}(a, 1)\right)$ and $\operatorname{Res}\left(f_{G}(1, b), g_{G}(1, b)\right)$. Sagemath [Sag] gives

| $G$ | l.c.m of resultants | $G$ | l.c.m of resultants |
| :---: | :---: | :---: | :---: |
| $\mathbb{Z} / 5 \mathbb{Z}$ | $2^{16} 3^{36} 5$ | $\mathbb{Z} / 10 \mathbb{Z}$ | $2^{72} 3^{108} 5^{3}$ |
| $\mathbb{Z} / 6 \mathbb{Z}$ | $-2^{24} 3^{39}$ | $\mathbb{Z} / 12 \mathbb{Z}$ | $2^{96} 3^{156}$ |
| $\mathbb{Z} / 7 \mathbb{Z}$ | $-2^{32} 3^{72} 7$ | $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 4 \mathbb{Z}$ | $2^{24} 3^{36}$ |
| $\mathbb{Z} / 8 \mathbb{Z}$ | $2^{48} 3^{72}$ | $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 6 \mathbb{Z}$ | $2^{192} 3^{78}$ |
| $\mathbb{Z} / 9 \mathbb{Z}$ | $-2^{48} 3^{117}$ | $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 8 \mathbb{Z}$ | $2^{576} 3^{144}$ |

Hence any prime divisor of $e$ should divide $6|G|$.
First, we find all the pairs pairs $(a, b) \in\left(\mathbb{Z} / p^{6} \mathbb{Z}\right)^{2}$ such that $a, b$ are relatively prime to $p$ and $p^{4} \mid f_{G}(a, b)$ and $p^{6} \mid g_{G}(a, b)$ for each prime divisor $p$ of $6|G|$. Then, there is no such pair $(a, b)$ except for the following 4 cases:

- when $G=\mathbb{Z} / 6 \mathbb{Z}$ and $(a, b) \equiv(1,1)(\bmod 2), 2$ exactly divides $e$
- when $G=\mathbb{Z} / 7 \mathbb{Z}$ and $(a, b) \equiv(1,2)$ or $(2,1)(\bmod 3), 3$ exactly divides $e$.
- when $G=\mathbb{Z} / 9 \mathbb{Z}$ and $(a, b) \equiv(1,2)$ or $(2,1)(\bmod 3), 3$ exactly divides $e$.
- when $G=\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 4 \mathbb{Z}$ and $(a, b) \equiv(1,1)(\bmod 2), 2$ exactly divides $e$.

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 5), 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 $(a, b) \equiv(1,0)(\bmod 2), 2$ divides $e$.
- when $G=\mathbb{Z} / 10 \mathbb{Z}$ and $(a, b) \equiv(1,0)(\bmod 2), 2$ divides $e$.
- when $G=\mathbb{Z} / 12 \mathbb{Z}$ and $(a, b) \equiv(1,0)(\bmod 2), 2$ divides $e$.
- when $G=\mathbb{Z} / 12 \mathbb{Z}, a \not \equiv 0$, and $b \equiv 0(\bmod 3), 3$ divides $e$.

For the first three cases we can check that there is no $(a, b) \in\left(\mathbb{Z} / 2^{6} \mathbb{Z}\right)^{2}$ such that $2^{5} \mid f_{G}(a, b)$ and $2^{6} \mid g_{G}(a, b)$, which implies that $2^{2} \nmid e$. Similarly for the fourth case, we can check that there is no $(a, b) \in\left(\mathbb{Z} / 3^{6} \mathbb{Z}\right)^{2}$ such that $3^{6} \mid f_{G}(a, b)$ and $3^{6} \mid g_{G}(a, b)$. For cross-check, we refer Appendix 5 for our $f_{G}$ and $g_{G}$.

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 $a \equiv 0(\bmod 4)$ and $b \not \equiv 0(\bmod 2), 2^{2}$ exactly divides $e(a, b)$ and when $a \equiv 2(\bmod 4)$ and $b \equiv 1(\bmod 2), 2^{3}$ divides $e(a, b)$. It seems that the defect is $2^{4}$ but to check it we need more computing power. Instead, 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 $\left(f_{G}, g_{G}\right)$ 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 $\left(f_{G}, g_{G}\right)(I) \equiv J$ modulo $p$.

For a given $J,\left|W_{G, J}\right|$ 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

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

follows directly.

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

| $G$ | $p$ | $\sum\left\|W_{G, J}\right\|$ | $G$ | $p$ | $\sum\left\|W_{G, J}\right\|$ |
| :--- | :--- | :--- | :--- | :--- | :--- |
| $\mathbb{Z} / 2 \mathbb{Z}$ | $\cdot$ | $2 p-1$ | $\mathbb{Z} / 9 \mathbb{Z}$ | $1(\bmod 3), \gamma_{9} \in\left(\mathbb{F}_{p}^{\times}\right)^{3}$ | $8 p-7$ |
| $\mathbb{Z} / 3 \mathbb{Z}$ | $\cdot$ | $2 p-1$ | $\mathbb{Z} / 9 \mathbb{Z}$ | $1(\bmod 3), \gamma_{9} \notin\left(\mathbb{F}_{p}^{\times}\right)^{3}$ | $5 p-4$ |
| $\mathbb{Z} / 4 \mathbb{Z}$ | $\cdot$ | $3 p-2$ | $\mathbb{Z} / 9 \mathbb{Z}$ | $2(\bmod 3), \gamma_{9} \in\left(\mathbb{F}_{p}[\sqrt{-3}]^{\times}\right)^{3}$ | $6 p-5$ |
| $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 2 \mathbb{Z}$ | $\cdot$ | $3 p-2$ | $\mathbb{Z} / 9 \mathbb{Z}$ | $2(\bmod 3), \gamma_{9} \notin\left(\mathbb{F}_{p}[\sqrt{-3}]^{\times}\right)^{3}$ | $3 p-2$ |
| $\mathbb{Z} / 5 \mathbb{Z}$ | $\pm 1 \quad(\bmod 5)$ | $4 p-3$ | $\mathbb{Z} / 10 \mathbb{Z}$ | $\pm 1(\bmod 5)$ | $8 p-7$ |
| $\mathbb{Z} / 5 \mathbb{Z}$ | $\pm 2(\bmod 5)$ | $2 p-1$ | $\mathbb{Z} / 10 \mathbb{Z}$ | $\pm 2(\bmod 5)$ | $4 p-3$ |
| $\mathbb{Z} / 6 \mathbb{Z}$ | $\cdot$ | $4 p-3$ | $\mathbb{Z} / 12 \mathbb{Z}$ | $1(\bmod 12)$ | $10 p-9$ |
| $\mathbb{Z} / 7 \mathbb{Z}$ | $\gamma_{7} \in\left(\mathbb{F}_{p}[\sqrt{-3}]^{\times}\right)^{3}$ | $6 p-5$ | $\mathbb{Z} / 12 \mathbb{Z}$ | $5,7,11 \quad(\bmod 12)$ | $6 p-5$ |
| $\mathbb{Z} / 7 \mathbb{Z}$ | $\gamma_{7} \notin\left(\mathbb{F}_{p}[\sqrt{-3}]^{\times}\right)^{3}$ | $3 p-2$ | $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 4 \mathbb{Z}$ | $\cdot$ | $4 p-3$ |
| $\mathbb{Z} / 8 \mathbb{Z}$ | $\pm 1(\bmod 8)$ | $6 p-5$ | $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 6 \mathbb{Z}$ | $\cdot$ | $6 p-5$ |
| $\mathbb{Z} / 8 \mathbb{Z}$ | $\pm 3(\bmod 8)$ | $4 p-3$ | $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 8 \mathbb{Z}$ | $1(\bmod 8), \geq 11$ | $10 p-9$ |
|  |  |  | $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 8 \mathbb{Z}$ | $7(\bmod 8), \geq 11$ | $8 p-7$ |
|  |  |  | $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 8 \mathbb{Z}$ | $5(\bmod 8), \geq 11$ | $6 p-5$ |
|  |  | $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 8 \mathbb{Z}$ | $3(\bmod 8), \geq 11$ | $4 p-3$ |  |

where $\gamma_{7}=4(637+147 \sqrt{-3})$ and $\gamma_{9}=4(-9 \pm 3 \sqrt{-3})$. Here . means that there is no condition on $p$. Furthermore, we have

$$
\sum_{\alpha=a^{2} \in(\mathbb{Z} / p \mathbb{Z})^{\times}}\left|W_{3,\left(-3 \alpha^{2}, 2 \alpha^{3}\right)}\right|= \begin{cases}2(p-1) & \text { for } p \equiv 1 \bmod 12,  \tag{5}\\ (p-1) & \text { for } p \equiv 5 \operatorname{or} 11 \bmod 12, \\ 0 & \text { for } p \equiv 7 \bmod 12 .\end{cases}
$$

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 $\left(f_{G}, g_{G}\right)(I) \equiv(0,0)$ $(\bmod p)$. For the groups $G$ with order $\leq 4$, one can directly check it. We show the case of $G=\mathbb{Z} / 3 \mathbb{Z}$. We parametrize $(A, B)$ satisfying $4 A^{3}+27 B^{2} \equiv 0$ by $\left(-3 \alpha^{2}, 2 \alpha^{3}\right)$ for $\alpha \in \mathbb{Z} / p \mathbb{Z}$. Directly solving the equations $\Phi_{G}(a, b)=(A, B)$, we know that $\left|W_{3,(A, B)}\right|$ 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 $A \not \equiv 0$. Since $h_{-3 \alpha^{2}, 2 \alpha^{3}}(x)$ is factored into

$$
3^{5}\left(x^{2}-\frac{\alpha}{3}\right)^{3}\left(x^{2}+\alpha\right),
$$

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 $2(p-1)+1=2 p-1$. Furthermore, if -1 and 3 are quadratic residue which is equivalent to $p \equiv 1(\bmod 12)$, then the sum of $\left|W_{3,\left(-3 \alpha^{2}, 2 \alpha^{3}\right)}\right|$ over quadratic residues $\alpha$ in $\mathbb{Z} / p \mathbb{Z}$ is equal to the sum of $\left|W_{3,\left(-3 \alpha^{2}, 2 \alpha^{3}\right)}\right|$ over all non-zero residues $\alpha$ in $\mathbb{Z} / p \mathbb{Z}$. Hence, we obtain the $G=\mathbb{Z} / 3 \mathbb{Z}$ row and the equation (5).

Let $(a, b)$ be a pair such that $4 f_{G}(a, b)^{3}+27 g_{G}(a, b)^{2} \equiv 0(\bmod p)$. Then, this $(a, b)$ determines $\alpha$ in $\mathbb{Z} / p \mathbb{Z}$ satisfying $\left(f_{G}, g_{G}\right)(a, b) \equiv\left(-3 \alpha^{2}, 2 \alpha^{3}\right)$. Hence, if we find such all 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 $E_{\left(f_{G}(a, b), g_{G}(a, b)\right)}$, instead of $\left(f_{G}, g_{G}\right)(a, b)$.

Let $\Delta_{G}(a, b)$ be the discriminant of $E_{\left(f_{G}, g_{G}\right)(a, b)}$. Then, we have

| $G$ | $\Delta_{G}(a, b)$ |
| :--- | :--- |
| $\mathbb{Z} / 5 \mathbb{Z}$ | $2^{12} 3^{12} a^{5} b^{5}\left(a^{2}-11 a b-b^{2}\right)$ |
| $\mathbb{Z} / 6 \mathbb{Z}$ | $-2^{8} 3^{12} a^{6} b^{2}(9 a+b)(a+b)^{3}$ |
| $\mathbb{Z} / 7 \mathbb{Z}$ | $2^{12} 3^{12} a^{7} b^{7}(a-b)^{7}\left(a^{3}-8 a^{2} b+5 a b^{2}+b^{3}\right)$ |
| $\mathbb{Z} / 8 \mathbb{Z}$ | $2^{12} 3^{12} a^{8} b^{2}(-2 a+b)^{4}(-a+b)^{8}\left(8 a^{2}-8 a b+b^{2}\right)$ |
| $\mathbb{Z} / 9 \mathbb{Z}$ | $2^{12} 3^{12} a^{9} b^{9}(a-b)^{9}\left(a^{2}-a b+b^{2}\right)^{3}\left(a^{3}-6 a^{2} b+3 a b^{2}+b^{3}\right)$ |
| $\mathbb{Z} / 10 \mathbb{Z}$ | $2^{12} 3^{12} b^{5}(-2 a+b)^{5}(-a+b)^{10} a^{10}\left(-4 a^{2}+2 a b+b^{2}\right)\left(a^{2}-3 a b+b^{2}\right)^{2}$ |
| $\mathbb{Z} / 12 \mathbb{Z}$ | $2^{12} 3^{12} b^{2}(-2 a+b)^{6}(-a+b)^{12} a^{12}\left(6 a^{2}-6 a b+b^{2}\right)\left(2 a^{2}-2 a b+b^{2}\right)^{3}\left(3 a^{2}-3 a b+b^{2}\right)^{4}$ |
| $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 4 \mathbb{Z}$ | $2^{8} 3^{12} b^{2} a^{2}(a-b)^{4}(a+b)^{4}$ |
| $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 6 \mathbb{Z}$ | $2^{18} 3^{12} a^{2}(a-6 b)^{2}(a+6 b)^{2} b^{6}(a-2 b)^{6}(a+2 b)^{6}$ |
| $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 8 \mathbb{Z}$ | $2^{20} 3^{12} b^{8} a^{8}(2 a+b)^{8}(4 a+b)^{8}\left(8 a^{2}-b^{2}\right)^{2}\left(8 a^{2}+8 a b+b^{2}\right)^{2}\left(8 a^{2}+4 a b+b^{2}\right)^{4}$ |

First, let's treat the cases where $\Delta_{G}(a, b)$ is a product of linear polynomials and quadratic polynomials. For example, consider

$$
\Delta_{8}(a, b)=2^{12} 3^{12} a^{8} b^{2}(-2 a+b)^{4}(-a+b)^{8}\left(8 a^{2}-8 a b+b^{2}\right)
$$

So in this case we have four types of $(a, b)$ satisfies the condition which are $a=0, b=0,2 a / b=1, a / b=1$, and $a / b$ is a zero of the quadratic polynomial $8 t^{2}-8 t+1$. The first four cases give $(p-1)$-pairs, and the quadratic polynomial has a zero in $\mathbb{F}_{p}$ when $p \equiv 1,7(\bmod 8)$. Since the value of $8 t^{2}-8 t+1$ at $t=1,1 / 2$ is $\pm 1$, 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.

Now, let's verify the cases where $\Delta_{G}(a, b)$ contains a cubic polynomial. For this purpose, we need the following lemma.

Lemma 2.3. Let $f(t)=t^{3}+a t+b$ be a polynomial over $\mathbb{F}_{p}$ with the discriminant $\Delta=\left(-4 a^{3}-27 b^{2}\right)$. The number of zeros (without multiplicity) of $f(t)$ is
(1) zero if and only if $\Delta=81 \mu^{2}$ is square and $(-b+\mu \sqrt{-3}) / 2$ is not cube in the field $\mathbb{F}_{p}[\sqrt{-3}]$.
(2) one if and only if $\Delta$ is non-square.
(3) two if and only if $\Delta$ is zero.
(4) three for other cases.

Proof. The first, second and fourth statements are shown in [Dic06] and the third one follows from the fact that a monic cubic which has two zeros and has no degree two term is parametrized by $(t-2 a)(t+a)^{2}$.

When $G=\mathbb{Z} / 7 \mathbb{Z}$, there is a polynomial $\left(a^{3}-8 a^{2} b+5 a b^{2}+b^{3}\right)$ in $\Delta_{G}(a, b)$. We obtain $\left(t^{3}-\frac{49}{3} t-\frac{637}{27}\right)$ by change of coordinate. In this case the discriminant of this polynomial is $2401=7^{4}$, so when $p>7$ then the number of zeros is one of 0 or 3. Also, $\mu=49 / 9$ and the number of zeros is determined by $\frac{1}{2}\left(-\frac{637}{27}+\frac{49}{9} \sqrt{-3}\right)$ which is equal to $4(-637+147 \sqrt{-3})$ up to a cube. We note that the 0 or 1 is not a solution of the given polynomial which means that there is no overlap, so we obtain the row for $G=\mathbb{Z} / 7 \mathbb{Z}$. When $G=\mathbb{Z} / 9 \mathbb{Z}$, we can prove it similarly.

We need to 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 $\mathcal{G}_{\geq 5}$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $e(G)$ | 2 | 3 | 4 | 6 | 6 | $2 d(G)$ |

Lemma 2.4. For $G \in \mathcal{G}_{\leq 4}$, there is a positive integer $r(G)$ such that the number of the preimages of $\Phi_{G}$ is $r(G)$ except $O\left(X^{\frac{1}{e(G)}}\right)$-points.

Proof. The cases $G=\mathbb{Z} / 2 \mathbb{Z}, \mathbb{Z} / 3 \mathbb{Z}$ are essentially in [HS14, 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 are $\left(a^{\prime}, b^{\prime}\right) \neq(a, \pm b)$ such that

$$
\left(-3 a^{2}+6 a b^{2}-2 b^{4},\left(2 a-b^{2}\right)\left(a^{2}+2 a b^{2}-b^{4}\right)\right)=\left(-3 a^{\prime 2}+6 a^{\prime} b^{\prime 2}-2 b^{\prime 4},\left(2 a^{\prime}-b^{\prime 2}\right)\left(a^{\prime 2}+2 a^{\prime} b^{\prime 2}-b^{\prime 4}\right)\right) .
$$

The elliptic curve $E_{\Phi_{4}(a, b)}$ has a 4-torsion point $\left(a, b\left(-b^{2}+3 a\right)\right)$. 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 $\left(a^{\prime}, b^{\prime}\right)$ also satisfy

$$
\left(a, b\left(-b^{2}+3 a\right)\right)=\left(a^{\prime}, \pm b^{\prime}\left(-b^{\prime 2}+3 a^{\prime}\right)\right)
$$

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

Let $G=\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 2 \mathbb{Z}$. By a similar argument, we need to count $(A, B)$ such that

$$
(A, B)=\left(-\frac{a^{2}+3 b^{2}}{4}, \frac{b^{3}-b a^{2}}{4}\right)=\left(-\frac{a^{\prime 2}+3 b^{\prime 2}}{4}, \frac{b^{\prime 3}-b^{\prime} a^{\prime 2}}{4}\right),
$$

and

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

We note that since $A$ and $B$ are integers, $a$ and $b$ should have the same parity. The set equality allows the identity of $y$-coordinates on the first equation, and it holds if and only if one of the following six linear systems

$$
\binom{a^{\prime}}{b^{\prime}}=A_{i}\binom{a}{b},
$$

for $A_{0}=I$, and

$$
A_{1}=\left(\begin{array}{cc}
-1 & 0 \\
0 & 1
\end{array}\right), A_{2}=\left(\begin{array}{rr}
\frac{1}{2} & -\frac{3}{2} \\
-\frac{1}{2} & -\frac{1}{2}
\end{array}\right), A_{3}=\left(\begin{array}{cc}
-\frac{1}{2} & \frac{3}{2} \\
-\frac{1}{2} & -\frac{1}{2}
\end{array}\right), A_{4}=\left(\begin{array}{cc}
\frac{1}{2} & \frac{3}{2} \\
\frac{1}{2} & -\frac{1}{2}
\end{array}\right), A_{5}=\left(\begin{array}{rr}
-\frac{1}{2} & -\frac{3}{2} \\
\frac{1}{2} & -\frac{1}{2}
\end{array}\right)
$$

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

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

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

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

is the collection of all the representatives of the above (not necessarily distinct) six points. On the other hand, the number of points such that the number of their preimages is strictly less than six is $O\left(X^{\frac{1}{6}}\right)$. Hence, we obtain the result with $r(\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 2 \mathbb{Z})=6$.

For $G \in \mathcal{G}_{\geq 5}$, we can prove analogous statement by using the argument of [CKV].
Lemma 2.5. For $G \in \mathcal{G}_{\geq 5}$, there is an integer $r(G)$ such that the preimages of $\Phi_{G}$ is $r(G)$ except $O\left(X^{\frac{1}{e(G)}}\right)$ points.

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

$$
\left\{(a, b) \in \mathbb{Z}^{2}:\left|f_{G}(a, b)\right| \leq X^{\frac{1}{3}},\left|g_{G}(a, b)\right| \leq X^{\frac{1}{2}},(a, b)=1\right\}
$$

Now, the natural map from the elliptic curve with $\Gamma$-structure to the set of elliptic curves which has $\Gamma$-structure is $r(G)$-to-one map by [CKV, Lemma 3.1.8] except negligible set comes from the curves with $\Gamma^{\prime}$-structure for $\Gamma^{\prime} \subset \Gamma$ and curves whose $j$-invariants is 0 or 1728 .

Let $J$ be an element in $(\mathbb{Z} / p \mathbb{Z})^{2}$ 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 $E(u, v)$ whose equation is (2) to $E_{J}: y^{2}=x^{3}+f_{G}(a, b) x+g_{G}(a, b)$ which is defined earlier. 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 $\Psi_{G, J}: W_{G, J} \rightarrow E_{J}\left(\mathbb{F}_{p}\right)$ whose image is in the set of points of maximal order in $G$.

Lemma 2.6. Let $G \in \mathcal{G}_{\leq 4}, G=\mathbb{Z} / 5 \mathbb{Z}, \mathbb{Z} / 6 \mathbb{Z}$, or $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 4 \mathbb{Z}$, and $J \in(\mathbb{Z} / p \mathbb{Z})^{2}$ for $p \geq 5$ such that $E_{J}$ is an elliptic curve. Then,

$$
E_{J}\left(\mathbb{F}_{p}\right) \geq G \quad \text { if and only if } \quad J=\Phi_{G}(a, b)
$$

for some $(a, b)$. Furthermore, $\left|W_{G, J}\right|$ is the number of embedding of $G$ into $E_{J}\left(\mathbb{F}_{p}\right)$.
Proof. When $G \in \mathcal{G}_{\leq 4}$, for the if and only if part we will use the computation of [GT12]. For example when $G=\mathbb{Z} / 4 \mathbb{Z}$, assume that $\left(x_{1}, w_{1}\right)$ is a point of order 4 of an elliptic curve $E_{A, B} / \mathbb{F}_{p}$. From the computation of the first coordinate of $[3]\left(x_{1}, w_{1}\right)=\left(x_{1},-w_{1}\right)$ for $w_{1} \neq 0$, we have

$$
B=\frac{1}{4}\left(5 x_{1}^{3}-A x_{1} \pm \sqrt{\left(3 x_{1}^{2}-2 A\right)\left(A+3 x_{1}^{2}\right)^{2}}\right) .
$$

Hence, $B$ is in $\mathbb{F}_{p}$ if and only if there exists $x_{2} \in \mathbb{F}_{p}$ such that $3 x_{1}^{2}-2 A=x_{2}^{2}$. The computation of the second coordinate gives that $w_{1}^{2}=\left(3 x_{1}-x_{2}\right)\left(x_{2}+3 x_{1}\right)^{2} / 8$, so we have $x_{2} \neq 3 x_{1}$ and there exists $x_{3} \in \mathbb{F}_{p}^{\times}$such that $x_{3}^{2}=\left(3 x_{1}-x_{2}\right) / 2$. By the change of variables $a=x_{1}$ and $b=x_{3}$, we have $(A, B)=\Phi_{4}(a, b)$ with points of order $4,\left(x_{1}, w_{1}\right)=\left(a, \pm b\left(-b^{2}+3 a\right)\right)$. For the converse, we know that $\left(a, \pm b\left(-b^{2}+3 a\right)\right)$ 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 [GT12, p. 92] should be

$$
\left(-z_{2}, 0\right), \quad\left(\frac{1}{2}\left(z_{2} \pm \sqrt{z_{2}^{2}-4 z_{1}}\right), 0\right) ;
$$

Now we prove the second statement when $G \in G_{\leq 4}$. When $G$ is cyclic, it suffices to prove that $\Psi_{G, J}$ is bijective. For example $G=\mathbb{Z} / 4 \mathbb{Z}$, we note that for $J=\Phi_{4}(a, b)$, the 2-tuple ( $a,-b$ ) also corresponds to the same $J$ but they induce the two points of order $4,\left(a, \pm b\left(-b^{2}+3 a\right)\right)$. Therefore, for each points of order 4 in $E_{A, B}\left(\mathbb{F}_{p}\right)$ there is an $(a, b) \in W_{4,(A, B)}$. For the converse, let $\Phi_{4}\left(a^{\prime}, b^{\prime}\right)=(A, B)$ and $\left(a^{\prime}, b^{\prime}\left(-b^{\prime 2}+3 a^{\prime}\right)\right)=\left(a, b\left(-b^{2}+3 a\right)\right)$. If $b \neq b^{\prime}$ then we have $a=a^{\prime}$ and $b b^{\prime}=0$ which implies that the one of the points $\left(a^{\prime}, b^{\prime}\left(-b^{\prime 2}+3 a^{\prime}\right)\right)$ and $\left(a, b\left(-b^{2}+3 a\right)\right)$ is of order 2. The cases $G=\mathbb{Z} / 2 \mathbb{Z}$ and $\mathbb{Z} / 3 \mathbb{Z}$ can be dealt similarly.

We treat the case $G=\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 2 \mathbb{Z}$ separately. We recall that $E_{J}$ has a $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 2 \mathbb{Z}$ if and only if $J=\left(f_{2 \times 2}(a, b), g_{2 \times 2}(a, b)\right)$. Hence if $E_{J}$ does not have full 2-torsion, then $\left|W_{2 \times 2, J}\right|$ should be zero. It is easily deduced that if $E_{J}$ does not have full 2-torsion, then $W_{2 \times 2, J}$ should be empty. If $E_{J}$ has the full 2-torsions, then $b^{3}+A b+B \equiv 0(\bmod p)$ has three zeros and $A=f_{2 \times 2}(a, b)=-\left(a^{2}+3 b^{2}\right) / 4$ for some $a$. This $a$ is not zero,
since if so then $f_{2 \times 2}(0, b)=-3 b^{2} / 4$ and $g_{2 \times 2}(0, b)=b^{3} / 4$ so $4 f_{2 \times 2}(0, b)^{3}+27 g_{2 \times 2}(0, b)^{2} \equiv 0(\bmod p)$. Hence, there are exactly six $(a, b)$ such that

$$
b^{3}+A b+B \equiv 0, \quad 4 A \equiv-\left(a^{2}+3 b^{2}\right) \quad(\bmod p)
$$

Since this equation is equivalent to a system of equation $J=\left(f_{2 \times 2}(a, b), g_{2 \times 2}(a, b)\right)$, we can conclude that if $E_{J}\left(\mathbb{F}_{p}\right) \geq \mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 2 \mathbb{Z}$ then $\left|W_{2 \times 2, J}\right|=6$.

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

$$
\left(3 a^{2}-18 a b+3 b^{2}, \pm 108 a b^{2}\right), \quad\left(3 a^{2}+18 a b+3 b^{2}, \pm 108 a^{2} b\right)
$$

are points with order 5 of $E_{J}$ where $J=\Phi_{G}(a, b)$. When $(a, b)$ gives one of above four points, then other three come from $(-b, a),(b,-a)$ and $(-a,-b)$.

We claim that the four pairs are all the pairs $(c, d)$ such that $\Phi_{5}(c, d)=J$ and

$$
3 a^{2}-18 a b+3 b^{2}=3 c^{2}-18 c d+3 d^{2}, \quad 3 a^{2}+18 a b+3 b^{2}=3 c^{2}+18 c d+3 d^{2}
$$

or

$$
3 a^{2}-18 a b+3 b^{2}=3 c^{2}+18 c d+3 d^{2}, \quad 3 a^{2}+18 a b+3 b^{2}=3 c^{2}-18 c d+3 d^{2}
$$

Both systems do not generate new pairs. Therefore, $\Psi_{5}$ is injective and $\left|W_{G, J}\right|$ 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 $E_{J}\left(\mathbb{F}_{p}\right)$ and $E_{J}: y^{2}=x^{3}+A x+B$. Let $x_{1}$ and $x_{2}$ be the $x$-coordinates of $P$ and $2 P$. Then by the duplication formula, we have

$$
\frac{x_{1}^{4}-2 A x_{1}^{2}-8 B x_{1}+A^{2}}{4\left(x_{1}^{3}+A x_{1}+B\right)}=x_{2}, \quad \frac{x_{2}^{4}-2 A x_{2}^{2}-8 B x_{2}+A^{2}}{4\left(x_{2}^{3}+A x_{2}+B\right)}=x_{1} .
$$

From the identity above, we can see that $2 x_{1}+x_{2}$ and $x_{1}+2 x_{2}$ are squares in $\mathbb{F}_{p}$. Let $\sqrt{2 x_{1}+x_{2}}$ and $\sqrt{x_{1}+2 x_{2}}$ be one of the square roots of $2 x_{1}+x_{2}$ and $x_{1}+2 x_{2}$ respectively. Then, by putting

$$
a=\frac{\sqrt{2 x_{1}+x_{2}}+\sqrt{x_{1}+2 x_{2}}}{6}, \quad b=\frac{\sqrt{2 x_{1}+x_{2}}-\sqrt{x_{1}+2 x_{2}}}{6},
$$

we have

$$
x_{1}=3 a^{2}+18 a b+3 b^{2}, \quad x_{2}=3 a^{2}-18 a b+3 b^{2},
$$

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 $P=\left(3 a^{2}-18 a b+3 b^{2}, 108 a b^{2}\right)$ which shows the surjectivity of $\Psi_{5}$.

As we did in the $\mathbb{Z} / 5 \mathbb{Z}$-case, we can show that

$$
\left(-9 a^{2}-18 a b+3 b^{2}, \pm\left(108 a^{2} b+108 a b^{2}\right)\right)
$$

are points of order 6 of elliptic curve $E_{J}$ where $J=\Phi_{6}(a, b)$ for some $a, b \in \mathbb{F}_{p}$. Since $(-a,-b)$ also gives a same points, we have a map $\Psi_{6}$ from $W_{6, J}$ to the points of order 6 of $E_{J}\left(\mathbb{F}_{p}\right)$.

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

$$
\begin{aligned}
-9 a^{2}-18 a b+3 b^{2} & =-9 c^{2}-18 c d+3 d^{2} \\
27 a^{2}+18 a b+3 b^{2} & =27 c^{2}+18 c d+3 d^{2} \\
-9 a^{2}+18 a b+3 b^{2} & =-9 c^{2}+18 c d+3 d^{2}
\end{aligned}
$$

since the $x$-coordinate of $2 P$ and $3 P$ is $27 a^{2}+18 a b+3 b^{2},-9 a^{2}+18 a b+3 b^{2}$, respectively. This system does not generate a new pair. Therefore $\Psi_{6}$ is injective.

Let $P:=\left(x_{1}, y_{1}\right)$ be a point of order 6 of $E_{J}\left(\mathbb{F}_{p}\right)$ and let $\left(x_{2}, y_{2}\right):=2 P$, and $\left(x_{3}, 0\right):=3 P$. By the duplication formula, we know that $2 x_{1}+x_{2}$ is square. Since $2 P$ is a point of order 3 , then $J=\Phi_{3}\left(a_{3}, b_{3}\right)$ for some $a_{3}, b_{3} \in \mathbb{F}_{p}$ and $\left(3 a_{3}^{2}, \pm\left(9 a_{3}^{3}+b_{3}\right)\right)$ are 3 -torsion point of $E_{J}$. Especially, we note that $x_{2} / 3$ is square in $\mathbb{F}_{p}$. Now, we define

$$
a:=\frac{3 \sqrt{x_{2} / 3}+\sqrt{2 x_{1}+x_{2}}}{12}, \quad b:=\frac{\sqrt{x_{2} / 3}-\sqrt{2 x_{1}+x_{2}}}{4} .
$$

Both are in $\mathbb{F}_{p}$ and we have $x_{2}=27 a^{2}+18 a b+3 b^{2}, x_{1}=-9 a^{2}-18 a b+3 b^{2}$. Using the result on 3 -torsion case, one can easily check that $\left(f_{6}(a, b), g_{6}(a, b)\right)=(A, B)$.

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 $a, b$. The claim is

$$
\left|W_{2 \times 4, J}\right|=\left\{\begin{array}{cl}
24 & \text { if } E_{J}\left(\mathbb{F}_{p}\right)[4] \cong \mathbb{Z} / 4 \mathbb{Z} \times \mathbb{Z} / 4 \mathbb{Z} \\
8 & \text { if } E_{J}\left(\mathbb{F}_{p}\right)[4] \cong \mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 4 \mathbb{Z}
\end{array}\right.
$$

Considering 6 systems deduced by $\Phi_{2 \times 4}(a, b)=\Phi_{2 \times 4}(c, d)$, we can see that $\left|W_{2 \times 4, J}\right|$ is at least 8 and it should be exactly 8 if either $p \equiv 3(\bmod 4)$ or $p \equiv 1(\bmod 4)$ and $a b$ is non-square in $\mathbb{F}_{p}$. If $p \equiv 1(\bmod 4)$ and $a b$ is a square in $\mathbb{F}_{p}$, the 6 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,

$$
\left|W_{2 \times 4, J}\right|=\left\{\begin{array}{cl}
24 & \text { if } \sqrt{a b} \in \mathbb{F}_{p} \text { and } p \equiv 1 \quad(\bmod 4) \\
8 & \text { otherwise }
\end{array}\right.
$$

We recall that $E_{J}$ has three non-trivial 2-torsion points whose $x$-coordinates are $-\left(3 a^{2}-18 a b+3 b^{2}\right),-\left(3 a^{2}+\right.$ $\left.18 a b+3 b^{2}\right),\left(6 a^{2}+6 b^{2}\right)$ respectively. The points $P$ with $2 P=\left(6 a^{2}+6 b^{2}, 0\right)$ are already included in the $E_{J}\left(\mathbb{F}_{p}\right)$, and one can check that the two points

$$
\left(3 a^{2}+18 a b+3 b^{2} \pm 18 \sqrt{a b}(a+b), \sqrt{-1} \cdot 2 \cdot 3^{3} \sqrt{a b}(\sqrt{a} \pm \sqrt{b})^{2}(a+b)\right)
$$

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

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

$$
(A, B)=\left(-\left(u^{2}+3 v^{2}\right) / 4,\left(v^{3}-u^{2} v\right) / 4\right)=\left(-3 s^{2}+6 s t^{2}-2 t^{4},\left(2 s-t^{2}\right)\left(s^{2}+2 s t^{2}-t^{4}\right)\right)
$$

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

$$
\left|W_{6, J}\right|=\left\{\begin{array}{cl}
24 & \text { if } E_{J}\left(\mathbb{F}_{p}\right)[6] \cong \mathbb{Z} / 6 \mathbb{Z} \times \mathbb{Z} / 6 \mathbb{Z}, \\
8 & \text { if } E_{J}\left(\mathbb{F}_{p}\right)[6] \cong \mathbb{Z} / 6 \mathbb{Z} \times \mathbb{Z} / 3 \mathbb{Z}, \\
6 & \text { if } E_{J}\left(\mathbb{F}_{p}\right)[6] \cong \mathbb{Z} / 6 \mathbb{Z} \times \mathbb{Z} / 2 \mathbb{Z}, \\
2 & \text { if } E_{J}\left(\mathbb{F}_{p}\right)[6] \cong \mathbb{Z} / 6 \mathbb{Z}, \\
0 & \text { if } E_{J}\left(\mathbb{F}_{p}\right)[6] \nsupseteq \mathbb{Z} / 6 \mathbb{Z} .
\end{array}\right.
$$

Comparing to Lemma 2.5, we should remark that the analogues result does not hold for all torsion groups.
Example 2. Let $E_{1}: y^{2}=x^{3}+2 x+1$ and $E_{2}: y^{2}=x^{3}+2 x+4$ be elliptic curves over $\mathbb{F}_{5}$. Then, $E_{1}$ and $E_{2}$ are isomorphic, and $E_{1}\left(\mathbb{F}_{5}\right) \cong E_{2}\left(\mathbb{F}_{5}\right) \cong \mathbb{Z} / 7 \mathbb{Z}$. However, one can compute that $\left|W_{7,(2,1)}\right|=0$ and $\left|W_{7,(2,4)}\right|=12$.
2.3. Moments of traces of the Frobenious. Now, we define a class number weighted by $\left|W_{G, J}\right|$.

Definition. We define

$$
\begin{equation*}
H_{G}(a, p):=\sum_{\substack{J=(A, B) \in(\mathbb{Z} / p \mathbb{Z})^{2} \\ a_{p}\left(E_{J}\right)=a \\ 4 A^{3}+27 B^{2} \neq 0(\bmod p)}}\left|W_{G, J}\right|, \tag{6}
\end{equation*}
$$

where $a_{p}(E)$ is a trace of the Frobenius of an elliptic curve $E$ at $p$.
The goal of this section is to show

$$
\begin{align*}
\sum_{|a|<2 \sqrt{p}} H_{G}(a, p) & =p^{2}+O_{G}(p),  \tag{7}\\
\sum_{|a|<2 \sqrt{p}} a H_{G}(a, p) & =O_{G}\left(p^{\frac{3}{2}}\right),  \tag{8}\\
\sum_{|a|<2 \sqrt{p}} a^{2} H_{G}(a, p) & =p^{3}+O_{G}\left(p^{\frac{5}{2}}\right) . \tag{9}
\end{align*}
$$

The main tool is the Eichler-Selberg trace formula [KP17]. We recall some notations first. The Chebyshev polynomials of the second kind are defined as

$$
U_{0}(t)=1, \quad U_{1}(t)=2 t, \quad U_{j+1}(t)=2 t U_{j}(t)-U_{j-1}(t)
$$

We define normalized Chebyshev polynomials to be

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

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

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

be the Chebyshev coefficients. We have

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

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

$$
\begin{equation*}
t^{0}=U_{0}(t, q), \quad t=U_{1}(t, q), \quad t^{2}=U_{2}(t, q)+q U_{0}(t, q) \tag{10}
\end{equation*}
$$

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

$$
\Phi_{A}(E)= \begin{cases}1 & \text { if there exists an injective homomorphism } A \hookrightarrow E\left(\mathbb{F}_{p}\right) \\ 0 & \text { otherwise }\end{cases}
$$

We define

$$
\mathbb{E}_{q}\left(a^{R} \Phi_{A}\right):=\frac{1}{q} \sum_{\substack{E \in \mathcal{C} \\ A \hookrightarrow E\left(\mathbb{F}_{q}\right)}} \frac{a_{q}(E)^{R}}{\left|\operatorname{Aut}_{\mathbb{F}_{q}}(E)\right|}
$$

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. Also, we denote $\psi(n)=n \prod_{p \mid n}(1+1 / p), \varphi(n)=n \prod_{p \mid n}(1-1 / p)$ and $\phi(n)=n \prod_{p \mid n}(-\varphi(p))$.

For $\lambda \mid\left(p-1, n_{1}\right)$, let

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

with

$$
\begin{aligned}
T_{\text {trace }} & :=\frac{1}{\varphi\left(n_{1}\right)} \operatorname{Tr}\left(T_{p} \mid S_{k}\left(\Gamma\left(n_{1}, \lambda\right)\right)\right) \\
T_{\text {hyp }} & :=\frac{1}{4} \sum_{\substack{i=0 \\
\tau\left|n_{1} \lambda \\
g\right| p-1}} \frac{\varphi(g) \varphi\left(n_{1}\left(n_{1}(\lambda, g) / g\right)\right.}{\varphi\left(n_{1}\right)}\left(\delta_{n_{1}(\lambda, g) / g}\left(y_{i}, 1\right)+(-1)^{k} \delta_{n_{1}(\lambda, g) / g}\left(y_{i},-1\right)\right), \\
T_{\text {dual }} & :=\frac{p+1}{\varphi\left(n_{1}\right)} \delta(k, 2),
\end{aligned}
$$

where $g=\left(\tau, n_{1} \lambda / \tau\right), y_{i}$ is the unique element of $\left(\mathbb{Z} /\left(n_{1} \lambda / g\right) \mathbb{Z}\right)^{\times}$such that $y_{i} \equiv p^{i}(\bmod \tau)$ and $y_{i} \equiv p^{1-i}(\bmod$ $\left.n_{1} \lambda / \tau\right), \delta(a, b)$ is the indicator function of $a=b$, and $\delta_{c}(a, b)$ is the indicator function of the congruence $a \equiv b$ $(\bmod c)$.

Theorem 2.7. [KP17, Theorem 3, when $q=p]$ Let $A$ be a finite abelian group of rank at most 2. Suppose $(p,|A|)=1$ and $k \geq 2$. If $p \equiv 1\left(\bmod n_{2}(A)\right)$ we have

$$
\begin{equation*}
\mathbb{E}_{p}\left(U_{k-2}(t, p) \Phi_{A}\right)=\frac{1}{\varphi\left(n_{1} / n_{2}\right)} \sum_{\nu \left\lvert\, \frac{\left(p-1, n_{1}\right)}{n_{2}}\right.} \phi(\nu) T_{n_{1}, n_{2} \nu}(p, 1) \tag{11}
\end{equation*}
$$

and if $p \not \equiv 1\left(\bmod n_{2}(A)\right)$, then $\mathbb{E}_{p}\left(U_{k-2}(t, p) \Phi_{A}\right)=0$.
Proposition 2.8. Let $G$ be one of the groups $\mathbb{Z} / n \mathbb{Z}$ for $2 \leq n \leq 6$ or $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 2 \mathbb{Z}$. Then, (7), (8) and (9) hold.

Proof. For each group $G$, we denote $n_{1}$ be its first invariant factor. We define $A_{G, i}$ be abelian groups satisfying $G \leq A_{G, i} \leq \mathbb{Z} / n_{1} \mathbb{Z} \times \mathbb{Z} / n_{1} \mathbb{Z}$, and $j<i$ if and only if $A_{G, j}<A_{G, i}$. We define $\widetilde{\omega}_{G, i}$ to be $\left|W_{G, I}\right|$ if $E_{I}\left[n_{1}\right]\left(\mathbb{F}_{p}\right) \cong$ $A_{G, i}$. This is well defined by Lemma 2.6. Let

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

Then, one can obtain that

$$
\sum_{|a|<2 \sqrt{p}} a^{R} H_{G}(a, p)=p(p-1) \sum_{i} \omega_{G, i} \mathbb{E}_{p}\left(a^{R} \Phi_{A_{G, i}}\right)
$$

For arbitrary $G$, we can show that

$$
\sum_{|a|<2 \sqrt{p}} H_{G}(a, p)=p^{2}+O(p)
$$

by Proposition 2.2. Hence,

$$
\begin{equation*}
\sum_{i} \omega_{G, i} \mathbb{E}_{p}\left(\Phi_{A_{G, i}}\right)=1+O\left(\frac{1}{p}\right) \tag{12}
\end{equation*}
$$

Since $t^{2}=U_{2}(t, p)+p U_{0}(t, p)$, we have the identity

$$
\mathbb{E}_{p}\left(t^{2} \Phi_{A}\right)=\mathbb{E}_{p}\left(U_{2}(t, p) \Phi_{A}\right)+p \mathbb{E}_{p}\left(U_{0}(t, p) \Phi_{A}\right)
$$

and this together with (12) implies

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

because $\mathbb{E}_{p}\left(U_{2}(t, p) \Phi_{A}\right) \ll_{G} \frac{p^{1.5}}{p}<_{G} p^{0.5}$ by Theorem 2.7 and Deligne bound.
Using the identity $t=U_{1}(t, p)$ and $\mathbb{E}_{p}\left(U_{1}(t, p) \Phi_{A}\right) \ll_{G} p^{-0.5}$, it is easy to see that

$$
\sum_{|a|<2 \sqrt{p}} a H_{G}(a, p)=O_{G}\left(p^{1.5}\right)
$$

by Theorem 2.7 and Deligne bound.
When $G=\mathbb{Z} / 2 \mathbb{Z}$ or $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 2 \mathbb{Z}$, we can obtain the $2 R+1$-th moments.
Proposition 2.9. When $G=\mathbb{Z} / 2 \mathbb{Z}$ or $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 2 \mathbb{Z}$, we have

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

for $R \geq 0$.
Proof. Let $N_{n}(a)$ (resp. $\left.N_{n \times n}(a)\right)$ be the number of isomorphism classes of elliptic curves over $\mathbb{F}_{p}$ such that $E\left(\mathbb{F}_{p}\right)[n] \geq \mathbb{Z} / n \mathbb{Z}\left(\right.$ resp. $\left.E\left(\mathbb{F}_{p}\right)[n]=\mathbb{Z} / n \mathbb{Z} \times \mathbb{Z} / n \mathbb{Z}\right)$ with weights $2 / \mid$ Aut $_{\mathbb{F}_{p}}(E) \mid$. Then, [Sch87, Theorem 4.6, 4.9] shows that for a prime $p \geq 5$, an $a$ in the Weil bound, and a positive integer $n \geq 2$,

$$
N_{n}(a)=\left\{\begin{array}{cc}
H\left(a^{2}-4 p\right) & \text { if } a \equiv p+1 \quad(\bmod n) \\
0 & \text { otherwise }
\end{array}\right.
$$

and

$$
N_{n \times n}(a)=\left\{\begin{array}{ccc}
H\left(\frac{a^{2}-4 p}{n^{2}}\right) & \text { if } p \equiv 1 & (\bmod n) \text { and } a \equiv p+1 \\
0 & \left(\bmod n^{2}\right), \\
\text { otherwise } .
\end{array}\right.
$$

By Lemma 2.6,

$$
H_{2}(a, p)=\frac{p-1}{2}\left(N_{2}(a)+2 N_{2 \times 2}(a)\right), \quad H_{2 \times 2}(a, p)=6 \cdot \frac{p-1}{2} N_{2 \times 2}(a) .
$$

Since $N_{2}(a)=N_{2}(-a)$ and $N_{2 \times 2}(a)=N_{2 \times 2}(-a)$, the result follows.
This will be used for the Frobenius trace formula for elliptic curves.

## 3. Counting elliptic curves with torsion points and local conditions

We introduce some notations first. Let

$$
R_{G}(X)=\left\{(a, b) \in \mathbb{R}^{2}:\left|f_{G}(a, b)\right| \leq X^{\frac{1}{3}},\left|g_{G}(a, b)\right| \leq X^{\frac{1}{2}}\right\}
$$

For $G$ in $\mathcal{G}_{\leq 4}$ we define

$$
\begin{aligned}
\mathcal{D}_{G}(X) & =\left\{(A, B) \in \mathbb{Z}^{2}:(A, B)=\Phi_{G}(a, b) \text { for some }(a, b) \in R_{G}(X) \cap \mathbb{Z}^{2}\right\}, \\
\mathcal{M}_{G}(X) & =\left\{(A, B) \in \mathcal{D}_{G}(X): \text { if } p^{4} \mid A, \text { then } p^{6} \nmid B\right\},
\end{aligned}
$$

and

$$
\mathcal{E}_{G}(X)=\left\{(A, B) \in \mathcal{M}_{G}(X): 4 A^{3}+27 B^{2} \neq 0\right\}, \quad \mathcal{S}_{G}(X)=\left\{(A, B) \in \mathcal{M}_{G}(X): 4 A^{3}+27 B^{2}=0\right\},
$$

where $\mathcal{E}_{G}(X)$ represents elliptic curves with $G$ torsion and $\mathcal{S}_{G}(X)$ takes up singular curves. We note that $\mathcal{E}_{G}(X)$ coincide with the previous definition.

For $G \in \mathcal{G}_{\geq 5}$, we recall that $M_{G}(X)$ is the set of relatively prime pairs $(a, b)$ with $h\left(\Phi_{G}(a, b)\right) \leq X$. We define

$$
\widetilde{M}_{G}^{e}(X)=\left\{(a, b) \in \mathbb{Z}^{2}:(a, b)=1, e=e(a, b),\left|f_{G}(a, b)\right| \leq X^{\frac{1}{3}},\left|g_{G}(a, b)\right| \leq X^{\frac{1}{2}}\right\}
$$

and $\widetilde{M}_{G}(X)$ as the union of $\widetilde{M}_{G}^{e}(X)$ for all $e \geq 1$. We define $\mathcal{E}_{G}(X)$ as (4) and

$$
\mathcal{S}_{G}(X)=\left\{(A, B) \in \mathcal{S}(X): \Phi_{G}(a, b) \text { for relatively prime }(a, b)\right\}
$$

where

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

For the reader's convenience we remark that $(a, b)$ denotes an element in the domain of $\Phi_{G}$ and $R_{G}$ (resp. $M_{G}$ for $G$ in $\left.\mathcal{G}_{\geq 5}\right)$ and $(A, B)$ does in the range of $\Phi_{G}$. Also, $\mathcal{D}_{G}, \mathcal{M}_{G}, \mathcal{E}_{G}$, and $\mathcal{S}_{G}$ are sets on the range side. For pairs $I, J \in(\mathbb{Z} / p \mathbb{Z})^{2}$, the subscripts $-_{G, I}(X)$ or $-_{G, J}(X)$ means that this is the subset of the original set consisting of elements $(a, b) \equiv I(\bmod p)$ or $(A, B) \equiv J(\bmod p)$ 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

$$
\operatorname{Area}\left(R_{G}(1)\right) X^{\frac{1}{d(G)}}+O\left(X^{\frac{1}{e(G)}}\right)
$$

Proof. We note that [HS14, Lemma 5.2] proves this lemma for $G=\mathbb{Z} / 2 \mathbb{Z}, \mathbb{Z} / 3 \mathbb{Z}$. Since $f_{4}(a, b)=X^{\frac{1}{3}}, g_{4}(a, b)=$ $X^{\frac{1}{2}}$ are equivalent to $f_{4}\left(a / X^{\frac{1}{6}}, b / X^{\frac{1}{12}}\right)=1, g_{4}\left(a / X^{\frac{1}{6}}, b / X^{\frac{1}{12}}\right)=1$, by change of variables we have

$$
\operatorname{Area}\left(R_{4}(X)\right)=X^{\frac{1}{4}} \operatorname{Area}\left(R_{4}(1)\right)
$$

Then, the claim follows from the Principle of Lipschitz, $[H S 14,(5.3)]$. We can do the same thing 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 $3 \operatorname{deg} f_{G}(a, b)=2 \operatorname{deg} g_{G}(a, b)=2 d(G)$.

By the Principle of Lipschitz, we have
Corollary 3.2. For a prime $p \geq 5, I$ an element in $(\mathbb{Z} / p \mathbb{Z})^{2}$, and a torsion subgroup $G$, we have

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

For $G=\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 2 \mathbb{Z}$, we consider only the pairs $(a, b)$ with $a \equiv b(\bmod 2)$. By Lemma 3.1 and Möbious inversion argument gives the following corollary, which is a complement of [HS14, Theorem 5.6]. For details, we refer to the proof of Proposition 3.6.

Corollary 3.3. For $G$ in $\mathcal{G}_{\leq 4}$, let

$$
c(G):=\frac{\operatorname{Area}\left(R_{G}(1)\right)}{2^{\delta_{G}=2 \times 2} r(G) \zeta\left(\frac{12}{d(G)}\right)} .
$$

Then,

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

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

$$
\left|\mathcal{D}_{G, J}(X)\right|=\frac{\left|W_{G, J}\right|}{2^{\delta_{G=2 \times 2} r} r(G)}\left|R_{G, I}(X)\right|+O\left(1+p^{-1} X^{\frac{1}{e(G)}}\right)
$$

where $I \in W_{G, J}$. For $G \in \mathcal{G}_{\geq 5}$, we have

$$
\left|\mathcal{E}_{G, J}(X)\right|=\frac{\left|W_{G, J}\right|}{r(G)} \sum_{I \in W_{G, J}} \sum_{e}\left|M_{I}^{e}(X)\right|+O\left(1+p^{-1} X^{\frac{1}{e(G)}}\right) .
$$

Proof. We fix a group $G$ and omit it from subscription. For $G \in \mathcal{G}_{\leq 4}, \Phi$ induces a surjective map

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

Let $h_{J}(X)$ be the number of the 2-tuples $(A, B)$ for which its pre-image is not equal to $r(G)$. Then, $h_{J}(X)$ is bounded by $O\left(p^{-1} X^{\frac{1}{e(G)}}\right)$ by the proof of Lemma 2.4. We note that the number of solutions of a system of equations

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

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

$$
\left|\mathcal{D}_{J}(X)\right|=\frac{\left|W_{J}\right|}{2^{\delta_{G}=2 \times 2} r(G)}\left|R_{I}(X)\right|+O\left(h_{J}(X)\right) .
$$

For $G \in \mathcal{G}_{\geq 5}, \Phi$ induces a surjective map

$$
\bigcup_{I \in W_{J}} \bigcup_{e} M_{I}^{e}(X) \rightarrow \mathcal{E}_{J}(X) \bigcup \mathcal{S}_{J}(X)
$$

Hence, the above argument and an estimate of $\mathcal{S}_{J}(X)$ 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 $*$ by $d *(A, B)=$ ( $d^{4} A, d^{6} B$ ).

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

$$
\left|\mathcal{M}_{G, J}(X)\right|=\sum_{\substack{d \leq X^{\frac{1}{12}} \\ p \nmid d}} \mu(d)\left|\mathcal{D}_{G, d^{-1} * J}\left(d^{-12} X\right)\right|,
$$

and $\left|\mathcal{S}_{G, J}(X)\right|=O\left(X^{\frac{1}{6}} / p\right)$.
Proof. Let $(A, B) \in \mathcal{D}_{G, J}(X)$ and let $d$ be the maximum of $d^{\prime}$ satisfying $d^{\prime 4} \mid A$ and $d^{\prime 6} \mid B$. 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

$$
\frac{1}{d^{4}} f_{G}(a, b)=f_{G}\left(\frac{a}{d^{m}}, \frac{b}{d^{n}}\right), \quad \frac{1}{d^{6}} g_{G}(a, b)=g_{G}\left(\frac{a}{d^{m}}, \frac{b}{d^{n}}\right),
$$

for given $G$. Also, we can check that $a / d^{m}$ and $b / d^{n}$ are integers. Hence if $(A, B)=\left(f_{G}(a, b), g_{G}(a, b)\right)$ for some $a, b \in \mathbb{Z}$, then

$$
d^{-1} *(A, B)=\left(f_{G}\left(\frac{a}{d^{m}}, \frac{b}{d^{n}}\right), g_{G}\left(\frac{a}{d^{m}}, \frac{b}{d^{n}}\right)\right)
$$

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

$$
(A, B) \rightarrow d^{-1} *(A, B), \quad \mathcal{D}_{G, J}(X) \rightarrow \bigsqcup_{\substack{d \leq X \frac{1}{12} \\ p \nmid d}} \mathcal{M}_{G, d^{-1}{ }^{*} * J}\left(d^{-12} X\right)
$$

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

Proposition 3.6. For a non-zero 2 -tuple $J \in(\mathbb{Z} / p \mathbb{Z})^{2}$ where $p \geq 5, G$ in $\mathcal{G}_{\leq 4}$ we have

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

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

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

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

$$
\begin{aligned}
\left|\mathcal{E}_{G, J}(X)\right| & =\left|\mathcal{M}_{G, J}(X)\right|+O\left(\mathcal{S}_{G, J}(X)\right)=\sum_{\substack{d \leq X^{\frac{1}{12}}}} \mu(d)\left|\mathcal{D}_{G, d^{-1} * J}\left(\frac{X}{d^{12}}\right)\right|+O\left(\frac{X^{\frac{1}{6}}}{p}\right) \\
& =\sum_{\substack{d \leq X^{\frac{1}{12}} \\
p \nmid d}} \mu(d)\left(\frac{\left|W_{G, d^{-1} * J}\right|}{\left.2^{\delta_{G=2 \times 2} r(G)}\left|R_{G, I}\left(\frac{X}{d^{12}}\right)\right|+O\left(1+p^{-1} \frac{X^{\frac{1}{e(G)}}}{d^{\frac{12}{e(G)}}}\right)\right)+O\left(\frac{X^{\frac{1}{6}}}{p}\right)}\right. \\
& =\frac{\left|W_{G, J}\right|}{2^{\delta_{G=2 \times 2}} r(G)} \sum_{d \leq X^{\frac{1}{12}}} \mu(d)\left|R_{G, I}\left(\frac{X}{d^{12}}\right)\right|+O\left(X^{\frac{1}{12}}+\frac{X^{\frac{1}{e(G)}}}{p}\right),
\end{aligned}
$$

by Lemma 3.4. Here we also used that $\left|R_{G, I}(X)\right|$ does not depend on $I \in W_{J}$. Using Corollary 3.2, the sum is

$$
\begin{aligned}
& =\frac{\left|W_{G, J}\right| \operatorname{Area}\left(R_{G}(1)\right)}{2^{\delta_{G=2 \times 2}} r(G) p^{2}} \sum_{d \leq X^{\frac{1}{12}}} \mu(d)\left(\frac{X^{\frac{1}{d(G)}}}{d^{\frac{12}{d(G)}}}+O\left(\frac{p X^{\frac{1}{e(G)}}}{d^{\frac{12}{e(G)}}}+p^{2}\right)\right)+O\left(X^{\frac{1}{12}}+\frac{X^{\frac{1}{e(G)}}}{p}\right) \\
& =c(G) \frac{\left|W_{G, J}\right|}{p^{2}} \frac{p^{\frac{12}{d(G)}}}{p^{\frac{12}{d(G)}}-1} X^{\frac{1}{d(G)}}+O\left(\frac{X^{\frac{1}{e(G)}}}{p}+X^{\frac{1}{12}}\right) .
\end{aligned}
$$

By [HS14, Theorem 5.6] and Corollary 3.3, the main term of

$$
\left|\mathcal{E}_{G,(0,0)}(X)\right|=\left|\mathcal{E}_{G}(X)\right|-\sum_{J \neq(0,0)}\left|\mathcal{E}_{G, J}(X)\right|
$$

is

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

This gives the main term, and the error term is easily checked.
For torsion $G$, we define

$$
c_{G, \mathcal{L C}}(p)=\sum_{E_{I} \text { satisfies } \mathcal{L C}} \frac{\left|W_{G, I}\right|}{p^{2}} .
$$

Theorem 3.7. For a prime $p \geq 5$, a local condition $\mathcal{L C}$, and a group $G$ in $\mathcal{G}_{\leq 4}$,

$$
\left|\mathcal{E}_{G, p}^{\mathcal{C}}(X)\right|=c(G) \cdot c_{G, \mathcal{L C}}(p) \cdot \frac{p^{\frac{12}{d(G)}}}{p^{\frac{12}{d(G)}}-1} X^{\frac{1}{d(G)}}+O\left(h_{G, \mathcal{L C}}(p, X)\right)
$$

where $c_{G, \mathcal{L C}}(p)$ is

|  | 2 | 3 | 4 | $2 \times 2$ |
| :---: | :---: | :---: | :---: | :---: |
| good | $(p-1)^{2} / p^{2}$ | $(p-1)^{2} / p^{2}$ | $(p-1)(p-2) / p^{2}$ | $(p-1)(p-2) / p^{2}$ |
| mult | $(2 p-2) / p^{2}$ | $(2 p-2) / p^{2}$ | $(3 p-3) / p^{2}$ | $(3 p-3) / p^{2}$ |
| 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

$$
c_{3, \text { split }}(p)= \begin{cases}2(p-1) / p^{2} & \text { for } p \equiv 1 \bmod 12 \\ (p-1) / p^{2} & \text { for } p \equiv 5 \operatorname{or} 11 \bmod 12 \\ 0 & \text { for } p \equiv 7 \bmod 12\end{cases}
$$

Finally for $\epsilon>0$, the function $h_{G, \mathcal{L C}}(p, X)$ is

|  | $h_{G, \mathcal{L C}}(p, X)$ |
| :---: | :---: |
| good/bad | $p X^{\frac{1}{e(G)}}+p^{2} X^{\frac{1}{12}}$ |
| mult | $X^{\frac{1}{e(G)}}+p X^{\frac{1}{12}}$ |
| split | $X^{\frac{( }{e(G)}}+p X^{\frac{1}{12}}$ |
| addi | $p X^{\frac{1}{e(G)}}+p^{2} X^{\frac{1}{12}}$ |
| $a$ | $H_{G}(a, p)\left(p^{-1} X^{\frac{1}{e(G)}}+X^{\frac{1}{12}}\right)$ |

Proof. By Proposition 3.6,

$$
\begin{aligned}
\left|\mathcal{E}_{G, p}^{\mathrm{good}}(X)\right| & =\sum_{\substack{J=(A, B) \in \mathbb{F}_{p}^{2} \\
4 A^{3}+27 B^{2} \neq 0}}\left|\mathcal{E}_{G, J}(X)\right| \\
& =\sum_{\substack{J=(A, B) \in \mathbb{F}_{p}^{2} \\
4 A^{3}+27 B^{2} \neq 0}} c(G) \frac{\left|W_{G, J}\right|}{p^{2}} \frac{p^{\frac{12}{d(G)}}}{p^{\frac{12}{d(G)}}-1} X^{\frac{1}{d(G)}}+O\left(p(p-1)\left(\frac{X^{\frac{1}{e(G)}}}{p}+X^{\frac{1}{12}}\right)\right) .
\end{aligned}
$$

By Propositions 2.2, we have

$$
\sum_{\substack{J=(A, B) \in \mathbb{F}_{p}^{2} \\
4 A^{3}+27 B^{2} \neq 0}}\left|W_{2, J}\right|=\sum_{\substack{J=(A, B) \in \mathbb{F}_{p}^{2} \\
\\
\sum_{\begin{subarray}{c}{J=(A, B) \in \mathbb{F}_{p}^{2} \\
4 A^{3}+27 B^{2} \neq 0} }}\left|W_{4, J}\right|=}\end{subarray}}\left|W_{3, J}\right|=(p-1)^{2},
$$

This proves good reduction cases. The other cases can be shown similarly.
For $G \in \mathcal{G}_{\geq 5}$, we note that

$$
\left|\widetilde{M}_{G}(X)\right|=\frac{\operatorname{Area}(R(1))}{\zeta(2)} X^{\frac{1}{d(G)}}+O\left(X^{\frac{1}{2 d(G)}} \log X\right)
$$

by the Möbius inversion and the Principle of Lipschitz. For details, we refer to the proof of the following lemma.

Lemma 3.8. For arbitrary prime power $p^{m}$ and a pair $I \in\left(\mathbb{Z} / p^{m} \mathbb{Z}\right)^{2}$ whose coordinates are not divided by $p$ simultaneously,

$$
\left|\widetilde{M}_{G, I}(X)\right|=\frac{1}{p^{2 m}} \frac{p^{2}}{p^{2}-1} \frac{\operatorname{Area}(R(1))}{\zeta(2)} X^{\frac{1}{d(G)}}+O\left(X^{\frac{1}{2 d(G)}}+p^{-m} X^{\frac{1}{2 d(G)}} \log X\right)
$$

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

$$
R_{G, I}(X) \cong \bigsqcup_{\substack{d \leq X^{\frac{1}{2(G)}} \\ p \nmid d}} d * \widetilde{M}_{G, d^{-1} * I}\left(d^{-2 d(G)} X\right), \quad(a, b) \rightarrow d *\left(\frac{a}{d}, \frac{b}{d}\right)
$$

where $d$ is the gcd of $a$ and $b$. By Möbius inversion argument and Corollary 3.2, we have

$$
\begin{aligned}
\left|\widetilde{M}_{G, I}(X)\right| & =\sum_{\substack{d \leq X^{\frac{1}{2 d(G)}} \\
p \nmid d}} \mu(d)\left|R_{G, d^{-1} * I}\left(d^{-2 d(G)} X\right)\right| \\
& =\sum_{\substack{d \leq X^{\frac{1}{2 d(G)}} \\
p \nmid d}} \mu(d)\left(\frac{1}{p^{2 m}} \operatorname{Area}(R(1)) \frac{X^{\frac{1}{d(G)}}}{d^{2}}+O\left(p^{-m} d^{-1} X^{\frac{1}{2 d(G)}}\right)\right) \\
& =\frac{1}{p^{2 m}} \frac{p^{2}}{p^{2}-1} \frac{\operatorname{Area}(R(1))}{\zeta(2)} X^{\frac{1}{d(G)}}+O\left(X^{\frac{1}{2 d(G)}}+p^{-m} X^{\frac{1}{2 d(G)}} \log X\right) .
\end{aligned}
$$

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

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

Proof. We use the strategy of [CKV, §3]. Let $\epsilon=\epsilon(G)$ be a positive integer which is the least common multiplier of the possible defects of $\left(f_{G}, g_{G}\right)$ which is well-defined by Lemma 2.1. Since $M_{G}^{e}(X)=\widetilde{M}_{G}^{e}\left(e^{12} X\right)$,
$\left|\mathcal{E}_{G, J}(X)\right|=\frac{1}{r(G)} \sum_{I \in W_{J}} \sum_{e \mid \epsilon}\left|M_{G, I}^{e}(X)\right|+O\left(1+p^{-1} X^{\left.\frac{1}{e(G)}\right)}\right)=\frac{1}{r(G)} \sum_{I \in W_{G, J}} \sum_{e \mid \epsilon}\left|\widetilde{M}_{G, I}^{e}\left(e^{12} X\right)\right|+O\left(1+p^{-1} X^{\frac{1}{2 d(G)}}\right)$,
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 $G \in \mathcal{G} \geq 5$ except $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 6 \mathbb{Z}$ 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 $I_{e}$ be the set of pairs $(\mathbb{Z} / \epsilon \mathbb{Z})^{2}$ which has a defect $e$. Then,

$$
\widetilde{M}_{G, I}^{e}(X)=\bigsqcup_{I^{\prime} \in I_{e}} \widetilde{M}_{G, I, I^{\prime}}(X),
$$

where $\widetilde{M}_{G, I, I^{\prime}}(X)$ is a subset of $\widetilde{M}_{G, I}(X)$ where the additional condition $(a, b) \equiv I^{\prime} \quad(\bmod \epsilon)$ is imposed. Since $\epsilon$ is a prime, $e=1$ or $\epsilon$. By Lemma 3.8 and CRT,

$$
\left|\widetilde{M}_{G, I}^{\epsilon}(X)\right|=\frac{\left|I_{\epsilon}\right|}{\left(\epsilon^{2}-1\right)} \frac{1}{\left(p^{2}-1\right)} \frac{\operatorname{Area}(R(1))}{\zeta(2)} X^{\frac{1}{d(G)}}+O\left(X^{\frac{1}{2 d(G)}}+p^{-1} X^{\frac{1}{2 d(G)}} \log X\right)
$$

and

$$
\left|\widetilde{M}_{G, I}^{1}(X)\right|=\frac{\left(\epsilon^{2}-1-\left|I_{\epsilon}\right|\right)}{\left(\epsilon^{2}-1\right)} \frac{1}{\left(p^{2}-1\right)} \frac{\operatorname{Area}(R(1))}{\zeta(2)} X^{\frac{1}{d(G)}}+O\left(X^{\frac{1}{2 d(G)}}+p^{-1} X^{\frac{1}{2 d(G)}} \log X\right) .
$$

Therefore,

$$
\left|\mathcal{E}_{G, J}(X)\right|=\frac{\left|W_{G, J}\right|}{p^{2}-1} \frac{\left(\left(\epsilon^{\frac{12}{d(G)}}-1\right)\left|I_{\epsilon}\right|+\epsilon^{2}-1\right)}{\left(\epsilon^{2}-1\right)} \frac{1}{r(G)} \frac{\operatorname{Area}(R(1))}{\zeta(2)} X^{\frac{1}{d(G)}}+O\left(X^{\frac{1}{2 d(G)}}+p^{-1} X^{\frac{1}{2 d(G)}} \log X\right) .
$$

Similarly, for the groups with no defect, we have

$$
\left|\mathcal{E}_{G, J}(X)\right|=\frac{\left|W_{G, J}\right|}{p^{2}-1} \frac{1}{r(G)} \frac{\operatorname{Area}(R(1))}{\zeta(2)} X^{\frac{1}{d(G)}}+O\left(X^{\frac{1}{2 d(G)}}+p^{-1} X^{\frac{1}{2 d(G)}} \log X\right) .
$$

By taking $c(G)=\frac{\left(\left(\epsilon^{\frac{12}{d(G)}}-1\right)\left|I_{\epsilon}\right|+\epsilon^{2}-1\right)}{\left(\epsilon^{2}-1\right)} \frac{1}{r(G)} \frac{\operatorname{Area}(R(1))}{\zeta(2)}$ 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 when $G=\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 6 \mathbb{Z}$ and $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 8 \mathbb{Z}$. Even for such $G$, if one know the defects (see Remark 1) then can calculate $c(G)$ precisely.

Proposition 2.2 and Theorem 3.9 analogously give results like Theorem 3.7. Instead of listing them all, we record the results which will be used in the applications.

Corollary 3.10. For $G \in \mathcal{G}_{\geq 5}$ and a prime $p \geq 5$,

$$
\begin{align*}
\left|\mathcal{E}_{G}(X)\right| & =c(G) X^{\frac{1}{d(G)}}+O\left(X^{\frac{1}{e(G)}}\right) \\
\left|\mathcal{E}_{G, p}^{a}(X)\right| & =c(G) \frac{H_{G}(a, p)}{p^{2}-1} X^{\frac{1}{d(G)}}+O\left(H_{G}(a, p) X^{\frac{1}{e(G)}}+\frac{H_{G}(a, p)}{p} X^{\frac{1}{e(G)}} \log X\right),  \tag{13}\\
\left|\mathcal{E}_{G, p}^{\mathrm{mult}}(X)\right| & =O\left(\frac{1}{p} X^{\frac{1}{d(G)}}+p X^{\frac{1}{e(G)}}+X^{\frac{1}{e(G)}} \log X\right) .
\end{align*}
$$

Theorems 3.7 and 3.9 gives some results on the probability for elliptic curves with local condition. In particular, for $\mathcal{L C}=$ mult, we observe an interesting phenomenon.

Corollary 3.11. The ratios of $c_{G, \text { mult }}(p)$ 's for $G \in \mathcal{G}_{\leq 4}$ 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 positive density such that the ratios of $c_{G, \text { mult }}(p)$ 's for $G \in \mathcal{G}_{\geq 5}$ are proportional to the number of cusps of the corresponding modular curves when $p \in S$.

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 $1,2,2,3,3$, respectively (For example, see [DS05, §3.9]). So we have the result for $G$ in $\mathcal{G}_{\leq 4}$ by 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 $M=4,6,8$ are $4,4,6,6,8,8,10$ and $4,6,10$. For primes $p$ which satisfy the conditions that make $\sum_{4 A^{3}+27 B^{2} \equiv 0} W_{G,(A, B)}$ largest among the possible values in Proposition 2.2, the proportion of $c_{G, \text { mult }}(p)$ for $G$ in $\mathcal{G}_{\geq 5}$ is coincide with above values. Now Theorem 3.9 and Chebotarev density theorem give $G$ in $\mathcal{G}_{\geq 5}$ part.

It is well-known that every elliptic curve with torsion $G \in \mathcal{G}_{\geq 5}$ has semistable reduction at $p \nmid|G|$. We can confirm this phenomenon with probability 1. Also, we have the analogous result for $G$ in $\mathcal{G}_{\leq 4}$.
Corollary 3.12. For $G$ in $\mathcal{G}_{\geq 5}$ and a prime $p \nmid 6|G|$, we have

$$
\lim _{X \rightarrow \infty} \frac{\left|\mathcal{E}_{G, p}^{\mathrm{ss}}(X)\right|}{\left|\mathcal{E}_{G}(X)\right|}=1
$$

For a torsion subgroup $G$ in $\mathcal{G}_{\leq 4}$ and a prime $p \geq 5$,

$$
c_{G, \mathrm{ss}}(p)=1-\frac{1}{p^{2}} .
$$

As we can see in the [CJ, Theorem 1.1], the number of elliptic curves with split and non-split reduction at $p$ are the same for all primes $p$. When we consider elliptic curves with torsion $G$, this property no more holds.

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

$$
\lim _{X \rightarrow \infty} \frac{\left|\mathcal{E}_{\mathbb{Z} / 3 \mathbb{Z}, p}^{\text {split }}(X)\right|}{\left|\mathcal{E}_{\mathbb{Z} / 3 \mathbb{Z}, p}^{\text {mult }}(X)\right|}= \begin{cases}\frac{1}{2} & \text { when } p \equiv 5,11 \quad(\bmod 12) \\ 1 & \text { when } p \equiv 1 \quad(\bmod 12) \\ 0 & \text { when } p \equiv 7 \quad(\bmod 12)\end{cases}
$$

We note that Corollaries 3.12 and 3.13 follow from Proposition 2.2, Theorem 3.7 and 3.9.

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 with that of [CJ, Theorem 8], we just introduce the notations and state the results.

Let $P=\left\{p_{k}\right\}_{k}$ be a finite set of primes such that $p_{k} \geq 5$, and $\mathcal{J}=\mathcal{J}_{P}$ be a finite set of 2-tuples $\left\{\left(A_{k}, B_{k}\right)\right\}$ for $A_{k}, B_{k} \in \mathbb{Z} / p_{k} \mathbb{Z}$ such that $\left(A_{k}, B_{k}\right) \not \equiv(0,0)\left(\bmod p_{k}\right)$. We define analogously $\mathcal{M}_{G, \mathcal{J}}(X), \mathcal{E}_{G, \mathcal{J}}(X), \mathcal{S}_{G, \mathcal{J}}(X)$, and so on. Let

$$
W_{G, \mathcal{J}}=\prod_{k} W_{G, J_{k}} \text { for } J_{k} \equiv\left(A_{k}, B_{k}\right) \quad\left(\bmod p_{k}\right)
$$

Then,
Proposition 3.14. For $P=\left\{p_{k}\right\}$ and $\mathcal{J}=\left\{\left(A_{k}, B_{k}\right)\right\}$, 2-tuples of $\mathbb{Z} / p_{k} \mathbb{Z}$ such that $\left(A_{k}, B_{k}\right) \not \equiv(0,0)$ for all $k$, and $G$ in $\mathcal{G}_{\leq 4}$, we have

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

We will denote $\mathcal{S}=\left(\mathcal{L C}_{p_{i}}\right)$ as a finite set of local conditions $\mathcal{L C}_{p_{i}}$. When an elliptic curve has the local property corresponding to $\mathcal{L} \mathcal{C}_{p_{i}}$ at $p_{i}$ for all local conditions in $\mathcal{S}$, we say that $E$ satisfies $\mathcal{S}$. Let

$$
\mathcal{E}_{G}^{\mathcal{S}}(X)=\left\{(A, B) \in \mathcal{E}_{G}(X): E_{A, B} \text { satisfies } \mathcal{S}\right\}
$$

and

$$
\left|\mathcal{L}_{p}\right|_{G}:=\lim _{X \rightarrow \infty} \frac{\left|\mathcal{E}_{G, p}^{\mathcal{L}_{p}}(X)\right|}{\left|\mathcal{E}_{G}(X)\right|}, \quad|\mathcal{S}|_{G}=\prod_{i}\left|\mathcal{L}_{p_{i}}\right|_{G}
$$

Now we address that the local conditions under the torsion restriction are also independent.
Theorem 3.15. Let $P=\left\{p_{k}\right\}$ and $\mathcal{S}$ be a set of local conditions at $p_{k}$. Then, we have

$$
\left|\mathcal{E}_{G}^{\mathcal{S}}(X)\right|=c(G)|\mathcal{S}|_{G} X^{\frac{1}{d(G)}}+O\left(\left(\prod_{k} p_{k}\right) X^{\frac{1}{e(G)}}+\left(\prod_{k} p_{k}\right)^{2} X^{\frac{1}{12}}\right)
$$

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 $H_{G}\left(a, p_{k}\right) / p_{k}$ and $H_{G}\left(a, p_{k}\right)$ respectively.

## 4. Proofs of the Main Theorems

4.1. Boundedness of average analytic rank of elliptic curves with prescribed torsion group. In this section, we show that 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 function with its Fourier transform $\widehat{\phi}$ 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, we have

$$
\begin{aligned}
\frac{1}{\left|\mathcal{E}_{G}(X)\right|} \sum_{E \in \mathcal{E}_{G}(X)} \sum_{\gamma_{E}} \phi\left(\gamma_{E} \frac{\log X}{2 \pi}\right) & =\frac{\widehat{\phi}(0)}{\left|\mathcal{E}_{G}(X)\right|} \sum_{E \in \mathcal{E}_{G}(X)} \frac{\log N_{E}}{\log X}+\frac{2}{\pi} \int_{-\infty}^{\infty} \phi\left(\frac{\log X \cdot r}{2 \pi}\right) \operatorname{Re} \frac{\Gamma_{E}^{\prime}}{\Gamma_{E}}\left(\frac{1}{2}+i r\right) d r \\
& -\frac{2}{\log X\left|\mathcal{E}_{G}(X)\right|} \sum_{n=1}^{\infty} \frac{\Lambda(n)}{\sqrt{n}} \widehat{\phi}\left(\frac{\log n}{\log X}\right) \sum_{E \in \mathcal{E}_{G}(X)} \hat{a}_{E}(n) \\
& \leq \widehat{\phi}(0)-\frac{2}{\log X\left|\mathcal{E}_{G}(X)\right|} \sum_{n=1}^{\infty} \frac{\Lambda(n)}{\sqrt{n}} \widehat{\phi}\left(\frac{\log n}{\log X}\right) \sum_{E \in \mathcal{E}_{G}(X)} \hat{a}_{E}(n)+O\left(\frac{1}{\log X}\right) \\
& \leq \widehat{\phi}(0)-S_{1}-S_{2}+O\left(\frac{1}{\log X}\right),
\end{aligned}
$$

where

$$
S_{1}=\frac{2}{\log X\left|\mathcal{E}_{G}(X)\right|} \sum_{p} \frac{\log p}{\sqrt{p}} \widehat{\phi}\left(\frac{\log p}{\log X}\right) \sum_{E \in \mathcal{E}_{G}(X)} \hat{a}_{E}(p)
$$

and

$$
S_{2}=\frac{2}{\log X\left|\mathcal{E}_{G}(X)\right|} \sum_{p} \frac{\log p}{p} \widehat{\phi}\left(\frac{2 \log p}{\log X}\right) \sum_{E \in \mathcal{E}_{G}(X)} \hat{a}_{E}\left(p^{2}\right) .
$$

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

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

Note that $\phi(0)=\frac{\sigma^{2}}{4}$ and $\widehat{\phi}_{n}(0)=\frac{\sigma}{4}$.
If we show

$$
\begin{equation*}
-S_{1}-S_{2}=\frac{1}{2} \phi(0)+o(1) \tag{14}
\end{equation*}
$$

by the positivity of $\phi$, we have

$$
\begin{equation*}
\frac{1}{\left|\mathcal{E}_{G}(X)\right|} \sum_{E \in \mathcal{E}_{G}(X)} r_{E} \leq \frac{1}{2}+\frac{\widehat{\phi}(0)}{\phi(0)}+o(1) \leq \frac{1}{2}+\frac{1}{\sigma}+o(1) . \tag{15}
\end{equation*}
$$

Hence, it is left to show (14) holds for each torsion group $G$ with some explicit $\sigma$. For this purpose, we need the following lemmas.

Lemma 4.1. For a torsion group $G$ in $\mathcal{G}_{\geq 5}$,

$$
\sum_{E \in \mathcal{E}_{G}(X)} \hat{a}_{E}(p) \ll\left(\frac{X^{\frac{1}{d(G)}}}{p}+p^{2} X^{\frac{1}{e(G)}}+p X^{\frac{1}{e(G)}} \log X\right) .
$$

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

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

Proof. We know that

$$
\sum_{E \in \mathcal{E}_{G}(X)} \hat{a}_{E}(p)=\sum_{\substack{|a|<2 \sqrt{p}}} \sum_{\substack{E \in \mathcal{G}_{G}(X) \\ a_{E}(p)=a}} \hat{a}_{E}(p)+\sum_{\substack{E \in \mathcal{E}_{G}(X) \\ E \operatorname{mult} \text { at } p}} \hat{a}_{E}(p) .
$$

When $G \in \mathcal{G}_{\geq 5}$ by Corollary 3.10,

$$
\left|\sum_{\substack{E \in \mathcal{E}_{G}(X) \\ E \text { mult red at } p}} \hat{a}_{E}(p)\right| \ll \frac{1}{p^{\frac{3}{2}}} X^{\frac{1}{d(G)}}+p^{\frac{1}{2}} X^{\frac{1}{e(G)}}+\frac{1}{p^{\frac{1}{2}}} X^{\frac{1}{e(G)}} \log X .
$$

By Corollary 3.10, (7) and (8),

$$
\begin{aligned}
\sum_{\substack{|a|<2 \sqrt{p}}} \sum_{\substack{E \in \mathcal{E}_{G}(X) \\
a_{E}(p)=a}} \hat{a}_{E}(p) & =\sum_{|a|<2 \sqrt{p}} \frac{a}{\sqrt{p}}\left(c(G) \frac{H_{G}(a, p)}{p^{2}-1} X^{\frac{1}{d(G)}}+O\left(H_{G}(a, p) X^{\frac{1}{e(G)}}+\frac{H_{G}(a, p)}{p} X^{\frac{1}{e(G)}} \log X\right)\right) \\
& \ll \frac{X^{\frac{1}{d(G)}}}{p}+p^{2} X^{\frac{1}{e(G)}}+p X^{\frac{1}{e(G)}} \log X .
\end{aligned}
$$

For $G=\mathbb{Z} / 3 \mathbb{Z}$ or $\mathbb{Z} / 4 \mathbb{Z}$, by Theorem 3.7,

$$
\left|\sum_{\substack{E \in \mathcal{E}_{G}(X) \\ E \text { mult red at } p}} \hat{a}_{E}(p)\right| \ll \frac{1}{\sqrt{p}}\left(\frac{1}{p} X^{\frac{1}{d(G)}}+X^{\frac{1}{e(G)}}+p X^{\frac{1}{12}}\right) \ll \frac{1}{p^{\frac{3}{2}}} X^{\frac{1}{d(G)}}+\frac{1}{p^{\frac{1}{2}}} X^{\frac{1}{e(G)}}+p^{\frac{1}{2}} X^{\frac{1}{12}} .
$$

By Theorem 3.7, (7) and (8),

$$
\begin{aligned}
\sum_{|a|<2 \sqrt{p}} \sum_{\substack{E \in \mathcal{Z}_{G}(X) \\
a_{E}(p)=a}} \hat{a}_{E}(p) & =\sum_{|a|<2 \sqrt{p}} \frac{a}{\sqrt{p}}\left(c(G) \frac{H_{G}(a, p)}{p^{2}} \frac{p^{\frac{12}{d(G)}}}{p^{\frac{12}{d(G)}}-1} X^{\frac{1}{d(G)}}+O\left(H_{G}(a, p)\left(p^{-1} X^{\frac{1}{e(G)}}+X^{\frac{1}{12}}\right)\right)\right) \\
& \ll \frac{X^{\frac{1}{d(G)}}}{p}+p X^{\frac{1}{e(G)}}+p^{2} X^{\frac{1}{12}} .
\end{aligned}
$$

Lemma 4.2. For a torsion group $G$ in $\mathcal{G}_{\geq 5}$,

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

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

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

Proof. We know that

$$
\sum_{E \in \mathcal{E}_{G}(X)} \hat{a}_{E}\left(p^{2}\right)=\sum_{\substack{|a|<2 \sqrt{p} \\ \mid}} \sum_{\substack{E \in \mathcal{E}_{G}(X) \\ a_{E}(p)=a}} \hat{a}_{E}\left(p^{2}\right)+\sum_{\substack{E \in \mathcal{E}_{G}(X) \\ E \text { mult at } p}} \frac{1}{p} .
$$

By Corollary 3.10,

$$
\sum_{\substack{E \in \mathcal{E}_{G}(X) \\ E \text { mult at } p}} \frac{1}{p} \ll \frac{X^{\frac{1}{d(G)}}}{p^{2}}+X^{\frac{1}{e(G)}}+\frac{X^{\frac{1}{e(G)}} \log X}{p}
$$

and

$$
\begin{aligned}
& \sum_{|a|<2 \sqrt{p}} \sum_{\substack{E \in \mathcal{E}_{G}(X) \\
a_{E}(p)=a}} \hat{a}_{E}\left(p^{2}\right)=\sum_{|a|<2 \sqrt{p}} \sum_{\substack{E \in \mathcal{E}_{G}(X) \\
a_{E}(p)=a}}\left(\hat{a}_{E}(p)^{2}-2\right) \\
& =\sum_{|a|<2 \sqrt{p}}\left(\frac{a^{2}}{p}-2\right)\left(c(G) \frac{H_{G}(a, p)}{p^{2}-1} X^{\frac{1}{d(G)}}+O\left(H_{G}(a, p) X^{\frac{1}{e(G)}}+\frac{H_{G}(a, p)}{p} X^{\frac{1}{e(G)}} \log X\right)\right) \\
& =c(G) \frac{\sum_{|a|<2 \sqrt{p}} a^{2} H_{G}(a, p)}{p\left(p^{2}-1\right)} X^{\frac{1}{d(G)}}-2 c(G) \frac{\sum_{|a|<2 \sqrt{p}} H_{G}(a, p)}{\left(p^{2}-1\right)} X^{\frac{1}{d(G)}}+O\left(p^{2} X^{\frac{1}{e(G)}}+p X^{\frac{1}{e(G)}} \log X\right) \\
& =-c(G) X^{\frac{1}{d(G)}}+O\left(\frac{1}{p^{\frac{1}{2}}} X^{\frac{1}{d(G)}}+p^{2} X^{\frac{1}{e(G)}}+p X^{\frac{1}{e(G)}} \log X\right),
\end{aligned}
$$

by Corollary 3.10 and (7) and (9).
For $G=\mathbb{Z} / 3 \mathbb{Z}$ or $\mathbb{Z} / 4 \mathbb{Z}$, by Theorem 3.7, (7) and (9), similarly we can show that

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

By Lemma 4.1, for $G$ in $\mathcal{G}_{\geq 5}$,

$$
\begin{align*}
S_{1} & \ll \frac{1}{\log X} \sum_{p} \frac{\log p}{\sqrt{p}} \widehat{\phi}\left(\frac{\log p}{\log X}\right)\left(\frac{1}{p}+p^{2} X^{-\frac{1}{e(G)}}+p X^{-\frac{1}{e(G)}} \log X\right)  \tag{16}\\
& \ll X^{-\frac{1}{e(G)}} \sum_{p \leq X^{\sigma}} p^{\frac{3}{2}} \log p \ll X^{-\frac{1}{e(G)}+\frac{5 \sigma}{2}}
\end{align*}
$$

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

$$
\begin{align*}
S_{1} & \ll \frac{1}{\log X} \sum_{p} \frac{\log p}{\sqrt{p}} \widehat{\phi}\left(\frac{\log p}{\log X}\right)\left(\frac{1}{p}+p X^{\frac{1}{e(G)}-\frac{1}{d(G)}}+p^{2} X^{\frac{1}{12}-\frac{1}{d(G)}}\right)  \tag{17}\\
& \ll X^{-\frac{1}{d(G)}} \sum_{p \leq X^{\sigma}}\left(p^{\frac{1}{2}} \log p X^{\frac{1}{e(G)}}+p^{\frac{3}{2}} \log p X^{\frac{1}{12}}\right) \ll X^{-\frac{1}{d(G)}}\left(X^{\frac{1}{e(G)}+\frac{3 \sigma}{2}}+X^{\frac{1}{12}+\frac{5 \sigma}{2}}\right) .
\end{align*}
$$

By Lemma 4.2, for $G$ in $\mathcal{G}_{\geq 5}$,

$$
\begin{aligned}
S_{2} & =\frac{2}{\log X} \sum_{p} \frac{\log p}{p} \widehat{\phi}\left(\frac{2 \log p}{\log X}\right)\left(-1+O\left(\frac{1}{p^{\frac{1}{2}}}+p^{2} X^{-\frac{1}{e(G)}}+p X^{-\frac{1}{e(G)}} \log X\right)\right) \\
& =-\frac{2}{\log X} \sum_{p} \frac{\log p}{p} \widehat{\phi}\left(\frac{2 \log p}{\log X}\right)+O\left(\frac{1}{\log X}+\sum_{p \leq X^{\frac{\sigma}{2}}} p \log p X^{-\frac{1}{e(G)}}\right) \\
& =-\frac{1}{2} \phi(0)+O\left(\frac{1}{\log X}+X^{-\frac{1}{e(G)}+\sigma}\right)
\end{aligned}
$$

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

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

From our computation, if we take $\sigma=\frac{1}{18}, \frac{1}{18}$, and $\frac{1}{5 d(G)}$ for $G=\mathbb{Z} / 3 \mathbb{Z}, \mathbb{Z} / 4 \mathbb{Z}$ and $G$ in $\mathcal{G}_{\geq 5}$ respectively then (14) and (15) hold. Therefore, the average of ranks is bounded by

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

for $G=\mathbb{Z} / 3 \mathbb{Z}, \mathbb{Z} / 4 \mathbb{Z}$ and $G$ in $\mathcal{G}_{\geq 5}$ respectively and we obtain Theorem 1 except for the cases of $G=\mathbb{Z} / 2 \mathbb{Z}$ 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 , and $r_{i}$ is odd or 2 if $e_{i}=1, r_{i}=1$ if $e_{i}=2$ for $i=1, \ldots, k$. Then,

$$
\begin{aligned}
\sum_{E \in \mathcal{\mathcal { E } _ { G }}(X)} \widehat{a_{E}}\left(p_{1}^{e_{1}}\right)^{r_{1}} \widehat{a_{E}}\left(p_{2}^{e_{2}}\right)^{r_{2}} \ldots \widehat{a_{E}}\left(p_{k}^{e_{k}}\right)^{r_{k}} & =c \frac{c(G)}{\zeta(12 / d(G))} X^{\frac{1}{d(G)}}+O_{k}\left(\left(\sum_{i=1}^{k} \frac{1}{p_{i}}\right) X^{\frac{1}{d(G)}}\right) \\
& +O_{k}\left(\left(\prod_{i=1}^{k} p_{i}\right) X^{\frac{1}{e(G)}}+\left(\prod_{i=1}^{k} p_{i}\right)^{2} X^{\frac{1}{12}}\right)
\end{aligned}
$$

where

$$
c=\left\{\begin{aligned}
0 & \text { if } e_{j}=1 \text { and } r_{j} \text { is odd for some } j, \\
-1 & \text { if } r_{j}=2 \text { for all } j \text { with } e_{j}=1 \text {, and the number of } j \text { 's with } e_{j}=2 \text { is odd, } \\
1 & \text { otherwise. }
\end{aligned}\right.
$$

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 $j$. WLOG, we can assume that $e_{1}=1$ and $r_{1}$ is odd. We fix local conditions at primes $p_{j}, j=2,3, \ldots, k$ and the local condition at $p_{1}$ is $a_{E}\left(p_{1}\right)=a$. By Theorem 3.15, there are

$$
c(G) \frac{H_{G}\left(a, p_{1}\right)}{p_{1}^{2}}\left|S^{\prime}\right|_{G} X^{\frac{1}{d(G)}}+O\left(\frac{H_{G}\left(a, p_{1}\right)}{p_{1}}\left(\prod_{i=2}^{k} c_{1}\left(p_{i}\right)\right) X^{\frac{1}{e(G)}}+H_{G}\left(a, p_{1}\right)\left(\prod_{i=2}^{k} c_{2}\left(p_{i}\right)\right) X^{\frac{1}{12}}\right)
$$

such elliptic curves in $\mathcal{E}_{G}(X)$, and $S^{\prime}$ is the set of the fixed local conditions at $p_{i}, i=2,3, \ldots, k$. For the values of $c_{1}\left(p_{i}\right)$ and $c_{2}\left(p_{i}\right)$, we refer to Theorem 3.15. Since $\widehat{a_{E}}\left(p_{2}^{e_{2}}\right)^{r_{2}} \cdots \widehat{a_{E}}\left(p_{k}^{e_{k}}\right)^{r_{k}}$ is a constant and $\sum_{a} a^{r_{1}} H_{G}\left(a, p_{1}\right)=0$ for odd $r_{1}$, only the error term above generates a contribution 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 $O\left(\left(\prod_{i=1}^{k} p_{i}\right) X^{\frac{1}{e(G)}}+\left(\prod_{i=1}^{k} p_{i}\right)^{2} X^{\frac{1}{12}}\right)$.

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 is split and non-split. Since the number of elliptic
curves with split reduction at $p_{1}$ and that of elliptic curves with non-split reduction at $p_{1}$ is the same up to an error term, by the similar argument above, the contribution comes from the error term and is at most

$$
O_{k}\left(\frac{1}{p_{1}^{\frac{r_{1}}{2}}}\left(\prod_{i=2}^{k} p_{i}\right) X^{\frac{1}{e(G)}}+\frac{p_{1}}{p_{1}^{\frac{r_{1}}{2}}}\left(\prod_{i=2}^{k} p_{i}\right)^{2} X^{\frac{1}{12}}\right)
$$

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 $\left|a_{i}\right|<2 \sqrt{p_{i}}$. The corresponding contribution is by Theorem 3.15

$$
\begin{array}{r}
\left(\prod_{i=1}^{k} \frac{p_{i}^{\frac{12}{d(G)}}}{p_{i}^{3}\left(p_{i}^{\frac{12}{d(G)}}-1\right)}\right) \frac{c(G)}{\zeta(12 / d(G))} X^{\frac{1}{d(G)}} \cdot \sum_{\left|a_{i}\right|<2 \sqrt{p_{i}}} a_{1}^{2} H_{G}\left(a_{1}, p_{1}\right) a_{2}^{2} H_{G}\left(a_{2}, p_{2}\right) \cdots a_{k}^{2} H_{G}\left(a_{k}, p_{k}\right) \\
+O\left(\sum_{\left|a_{i}\right|<2 \sqrt{p_{i}}}\left[\prod_{i=1}^{k} \frac{a_{i}^{2} H_{G}\left(a_{i}, p_{i}\right)}{p_{i}^{2}} X^{\frac{1}{e(G)}}+\prod_{i=1}^{k} \frac{a_{i}^{2} H_{G}\left(a_{i}, p_{i}\right)}{p_{i}} X^{\frac{1}{12}}\right]\right),
\end{array}
$$

which is, by the identity $\sum_{|a|<2 \sqrt{p}} a^{2} H_{G}(a, p)=p^{3}+O_{G}\left(p^{2}\right)$,

$$
\frac{c(G)}{\zeta(12 / d(G))} X^{\frac{1}{d(G)}}+O_{k}\left(\left(\sum_{i=1}^{k} \frac{1}{p_{i}}\right) X^{\frac{1}{d(G)}}+\left(\prod_{i=1}^{k} p_{i}\right) X^{\frac{1}{e(G)}}+\left(\prod_{i=1}^{k} p_{i}\right)^{2} X^{\frac{1}{12}}\right) .
$$

When $\mathcal{L C}_{p_{i}}$ is multi, $\widehat{a_{E}}\left(p_{i}\right)^{2}=\frac{1}{p_{i}}$. Then using the trivial bound $\widehat{a_{E}}\left(p_{i}\right)^{2} \leq 4$ for the other primes $p_{j}$, the contribution for this case is

$$
<_{k}\left(\sum_{i=1}^{k} \frac{1}{p_{i}^{2}}\right) X^{\frac{1}{d(G)}}+\left(\sum_{i=1}^{k} \frac{1}{p_{i}}\right) X^{\frac{1}{e(G)}}+X^{\frac{1}{12}} .
$$

The last case is when $e_{1}=e_{2}=\cdots=e_{l}=2$ and $e_{j}=1$ and $r_{j}=2$ for $j>l$ for some $i \leq l \leq k$. Note that $\widehat{a_{E}}\left(p^{2}\right)=\widehat{a_{E}}(p)^{2}-2$ for $E$ with good reduction at $p$ and $\widehat{a_{E}}\left(p^{2}\right)=\widehat{a_{E}}(p)^{2}$ for $E$ with bad reduction at $p$. Hence, it is enough to consider elliptic curves with good reduction at all the primes $p_{i}$ 's. This amounts to

$$
\sum_{E \text { has good reduction at } p_{i}^{\prime} \text { 's }}\left(\widehat{a_{E}}\left(p_{1}\right)^{2}-2\right) \cdots\left(\widehat{a_{E}}\left(p_{l}\right)^{2}-2\right) \widehat{a_{E}}\left(p_{l+1}\right)^{2} \cdots \widehat{a_{E}}\left(p_{k}\right)^{2},
$$

which is equal to

$$
(-1)^{l} \frac{c(G)}{\zeta(12 / d(G))} X^{\frac{1}{d(G)}}+O_{k}\left(\left(\sum_{i=1}^{k} \frac{1}{p_{i}}\right) X^{\frac{1}{d(G)}}+\left(\prod_{i=1}^{k} p_{i}\right) X^{\frac{1}{e(G)}}+\left(\prod_{i=1}^{k} p_{i}\right)^{2} X^{\frac{1}{12}}\right)
$$

by the result of the previous case and the identity $(1-2)^{l}=(-1)^{l}$.
4.3. The distribution of analytic ranks of elliptic curves. From now on, assume that every elliptic curve $L$-function satisfies 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,

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

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 $\mathcal{E}_{G}$, 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 a high rank. For this purpose, we compute an $n$-level density with multiplicity. The main reference is [Mil, Part VI].

For the $n$-level denisty, we choose the same test function for some $\sigma_{n}$ in the previous section:

$$
\widehat{\phi}_{n}(u)=\frac{1}{2}\left(\frac{1}{2} \sigma_{n}-\frac{1}{2}|u|\right) \text { for }|u| \leq \sigma_{n}, \quad \text { and } \quad \phi_{n}(x)=\frac{\sin ^{2}\left(2 \pi \frac{1}{2} \sigma_{n} x\right)}{(2 \pi x)^{2}} .
$$

Note that $\phi_{n}(0)=\frac{\sigma_{n}^{2}}{4}, \widehat{\phi}_{n}(0)=\frac{\sigma_{n}}{4}$ and

$$
\begin{equation*}
\int_{\mathbb{R}}|u| \widehat{\phi}_{n}(u)^{2} d u=\frac{1}{6} \phi_{n}(0)^{2} . \tag{18}
\end{equation*}
$$

We show that the $n$-level density holds by taking $\sigma_{n}=\frac{1}{9 n}$ and $\frac{1}{10 n}$ 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

$$
D_{n}^{*}\left(\mathcal{E}_{G}, \Phi\right)=\frac{1}{\left|\mathcal{E}_{G}(X)\right|} \sum_{E \in \mathcal{E}_{G}(X)} \sum_{j_{1}, j_{2}, \ldots, j_{n}} \phi_{n}\left(\gamma_{E, j_{1}} \frac{\log X}{2 \pi}\right) \phi_{n}\left(\gamma_{E, j_{2}} \frac{\log X}{2 \pi}\right) \cdots \phi_{n}\left(\gamma_{E, j_{n}} \frac{\log X}{2 \pi}\right),
$$

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

$$
\begin{equation*}
\frac{1}{\left|\mathcal{E}_{G}(X)\right|} \sum_{E \in \mathcal{E}_{G}(X)} r_{E}^{n} \leq \frac{1}{\phi_{n}(0)^{n}} D_{n}^{*}\left(\mathcal{E}_{G}, \Phi\right) . \tag{19}
\end{equation*}
$$

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

$$
\begin{aligned}
D_{n}^{*}\left(\mathcal{E}_{G}, \Phi\right) & \leq \frac{1}{\left|\mathcal{E}_{G}(X)\right|} \sum_{S} \widehat{\phi}_{n}(0)^{\left|S^{c}\right|}\left(-\frac{2}{\log X}\right)^{|S|} \\
& \times \sum_{m_{i_{1}}, m_{i_{2}}, \ldots, m_{i_{k}}} \frac{\Lambda\left(m_{i_{1}}\right) \Lambda\left(m_{i_{2}}\right) \cdots \Lambda\left(m_{i_{k}}\right)}{\sqrt{m_{i_{1}} m_{i_{2}} \cdots m_{i_{k}}}} \widehat{\phi}_{n}\left(\frac{\log m_{i_{1}}}{\log X}\right) \cdots \widehat{\phi}_{n}\left(\frac{\log m_{i_{k}}}{\log X}\right) \\
& \times \sum_{E \in \mathcal{E}_{G}(X)} \widehat{a}_{E}\left(m_{i_{1}}\right) \widehat{a}_{E}\left(m_{i_{2}}\right) \cdots \widehat{a}_{E}\left(m_{i_{k}}\right)+O\left(\frac{1}{\log X}\right),
\end{aligned}
$$

where $m_{i}$ 's are primes or squares of a prime with $m_{i} \leq X^{\sigma_{n}}$ and $S=\left\{i_{i}, i_{2}, \ldots, i_{k}\right\}$ runs over every subset of $\{1,2,3, \cdots, n\}$. Using the Frobenius trace formula (Theorem 4.3), we can prove the following propositions as we did in [CJ, Proposition 4.1, 4.2].

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

$$
\sum_{E \in \mathcal{E}_{G}(X)} \sum_{m_{i_{1}} m_{i_{2} \cdots m_{i_{k}} \neq \square} \frac{\Lambda\left(m_{i_{1}}\right) \cdots \Lambda\left(m_{i_{k}}\right) \widehat{a}_{E}\left(m_{i_{1}}\right) \cdots \widehat{a}_{E}\left(m_{i_{k}}\right)}{\sqrt{m_{i_{1}} m_{i_{2}} \cdots m_{i_{k}}}} \widehat{\phi}_{n}\left(\frac{\log m_{i_{1}}}{\log X}\right) \cdots \widehat{\phi}_{n}\left(\frac{\log m_{i_{k}}}{\log X}\right)}^{\ll\left|\mathcal{E}_{G}(X)\right| .} \begin{aligned}
&
\end{aligned}
$$

Proof. Note that $\widehat{a}_{E}\left(m_{i_{1}}\right) \widehat{a}_{E}\left(m_{i_{2}}\right) \cdots \widehat{a}_{E}\left(m_{i_{k}}\right)$ is of the form

$$
\widehat{a}_{E}\left(p_{1}\right)^{e_{1}} \widehat{a}_{E}\left(p_{2}\right)^{e_{2}} \cdots \widehat{a}_{E}\left(p_{t}\right)^{e_{t}} \widehat{a}_{E}\left(q_{1}^{2}\right)^{l_{1}} \widehat{a}_{E}\left(q_{2}^{2}\right)^{l_{2}} \cdots \widehat{a}_{E}\left(q_{s}^{2}\right)^{l_{s}},
$$

with 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 $e_{i}$ 's is odd. In this case, the proof of Theorem 4.3 also works and we have,

$$
\begin{aligned}
& \sum_{E \in \mathcal{E}(X)} \widehat{a}_{E}\left(p_{1}\right)^{e_{1}} \widehat{a}_{E}\left(p_{2}\right)^{e_{2}} \cdots \widehat{a}_{E}\left(p_{t}\right)^{e_{t}} \widehat{a}_{E}\left(q_{1}^{2}\right)^{l_{1}} \widehat{a}_{E}\left(q_{2}^{2}\right)^{l_{2}} \cdots \widehat{a}_{E}\left(q_{s}^{2}\right)^{l_{s}} \\
& \quad=O\left(p_{1} p_{2} \cdots p_{t} q_{1} q_{2} \cdots q_{s} X^{\frac{1}{e(G)}}+\left(p_{1} p_{2} \cdots p_{t} q_{1} q_{2} \cdots q_{s}\right)^{2} X^{\frac{1}{12}}\right) .
\end{aligned}
$$

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

$$
\begin{aligned}
& \ll X^{\frac{1}{e(G)}}\left(\sum_{p<X^{\sigma_{n}}} p^{\frac{1}{2}} \log p\right)^{k}+X^{\frac{1}{12}}\left(\sum_{p<X^{\sigma_{n}}} p^{\frac{3}{2}} \log p\right)^{k} \\
& \ll X^{\frac{1}{e(G)}}\left(X^{\frac{3}{2} \sigma_{n}}\right)^{n}+X^{\frac{1}{12}}\left(X^{\frac{5}{2} \sigma_{n}}\right)^{n} \ll X^{\frac{1}{d(G)}}
\end{aligned}
$$

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

Now, we assume that some $p_{i}$ is equal to some $q_{j}$. Since $\widehat{a}_{E}\left(q^{2}\right)^{l}=\left(\widehat{a}_{E}(q)^{2}-2\right)^{l}$ if $E$ has good reduction at $q$ and $\widehat{a}_{E}\left(q^{2}\right)^{l}=\widehat{a}_{E}(q)^{2 l}$ otherwise, still we can use the Frobenius trace formula.

Proposition 4.5. Let $\widehat{\phi}$ be as above with $\sigma_{n}=\frac{1}{9 n}$ and $\frac{1}{10 n}$ for $G=\mathbb{Z} / 2 \mathbb{Z}$ and $\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 2 \mathbb{Z}$ respectively. For a subset $S=\left\{i_{1}, i_{2}, \ldots, i_{k}\right\}$ of $\{1,2, \ldots, n\}$,

$$
\begin{array}{r}
\frac{1}{\left|\mathcal{E}_{G}(X)\right|}\left(\frac{-2}{\log X}\right)^{|S|} \sum_{E \in \mathcal{E}_{G}(X)} \sum_{m_{i_{1}} m_{i_{2}} \ldots m_{i_{k}}=\square}\left(\prod_{j=1}^{|S|} \frac{\Lambda\left(m_{i_{j}}\right) \widehat{a}_{E}\left(m_{i_{j}}\right)}{\sqrt{m_{i_{j}}}} \widehat{\phi}_{n}\left(\frac{\log m_{i_{j}}}{\log X}\right)\right) \\
=\sum_{\substack{S_{2} \subset S \\
\left|S_{2}\right| \text { even }}}\left(\frac{1}{2} \phi_{n}(0)\right)^{\left|S_{2}^{c}\right|}\left|S_{2}\right|!\left(\int_{\mathbb{R}}|u| \widehat{\phi}_{n}(u)^{2} d u\right)^{\frac{\left|S_{2}\right|}{2}}+O\left(\frac{1}{\log X}\right) .
\end{array}
$$

Proof. In this proof, we compute the double sum not considering the term $\frac{1}{\mathcal{E}(X) \mid}\left(\frac{-2}{\log X}\right)^{k}$. We show that every contribution except one is $\ll X^{\frac{1}{d(G)}}(\log X)^{k-1}$, hence they become the error term $O(1 / \log X)$ in the end.

Note that $\widehat{a}_{E}\left(m_{i_{1}}\right) \widehat{a}_{E}\left(m_{i_{2}}\right) \cdots \widehat{a}_{E}\left(m_{i_{k}}\right)$ is of the form

$$
\widehat{a}_{E}\left(p_{1}\right)^{e_{1}} \widehat{a}_{E}\left(p_{2}\right)^{e_{2}} \cdots \widehat{a}_{E}\left(p_{t}\right)^{e_{t}} \widehat{a}_{E}\left(q_{1}^{2}\right)^{l_{1}} \widehat{a}_{E}\left(q_{2}^{2}\right)^{l_{2}} \cdots \widehat{a}_{E}\left(q_{s}^{2}\right)^{l_{s}},
$$

with with $e_{1}+\cdots+e_{t}+l_{1}+\cdots+l_{s}=k$ and $e_{i}$ 's are all 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 $X^{\frac{1}{d(G)}}(\log X)^{k-1}$. Let $S_{2}$ be a subset of $S$ with even cardinality $2 t$ :

$$
S_{2}=\left\{i_{a_{1}}, i_{a_{2}}, \cdots, i_{a_{2 t-1}}, i_{a_{2 t}}\right\}, \quad S_{2}^{c}=\left\{i_{b_{1}}, i_{b_{2}}, \cdots, i_{b_{s}}\right\} .
$$

There are $(2 t)!/ 2^{t}$ ways to pair up two elements in $S_{2}$. For example, we consider the following pairings.

$$
\left(i_{a_{1}}, i_{a_{2}}\right),\left(i_{a_{3}}, i_{a_{4}}\right),\left(i_{a_{5}}, i_{a_{6}}\right), \cdots,\left(i_{a_{2 t-1}}, i_{a_{2 t}}\right) .
$$

This set of pairings corresponds the following sum

$$
\sum_{E \in \mathcal{E}_{G}(X)} \widehat{a}_{E}\left(p_{i_{a_{1}}}\right)^{2} \widehat{a}_{E}\left(p_{i_{a_{3}}}\right)^{2} \cdots \widehat{a}_{E}\left(p_{i_{a_{2 t-1}}}\right)^{2} \widehat{a}_{E}\left(q_{i_{b_{1}}}^{2}\right) \widehat{a}_{E}\left(q_{i_{b_{2}}}^{2}\right) \cdots \widehat{a}_{E}\left(q_{i_{b_{s}}}^{2}\right)
$$

where $2 t+s=k$. By the Frobenius trace formula, the above sum is

$$
\begin{array}{r}
\left|\mathcal{E}_{G}(X)\right| \cdot\left\{\begin{array}{rl}
1 & \text { if } s \text { is even, } \\
-1 & \text { if } s \text { is odd }
\end{array}+O\left(\left(\frac{1}{p_{1}}+\cdots+\frac{1}{p_{t}}+\frac{1}{q_{1}}+\cdots \frac{1}{q_{s}}\right) X^{\frac{1}{d(G)}}\right)\right. \\
+O\left(p_{1} \cdots p_{t} q_{1} \cdots q_{s} X^{\frac{1}{e(G)}}+\left(p_{1} \cdots p_{t} q_{1} \cdots q_{s}\right)^{2} X^{\frac{1}{12}}\right)
\end{array}
$$

The contribution from the 2nd big O-term is dominated by

$$
\left(X^{\sigma_{n}} \log X\right)^{t}\left(X^{\frac{\sigma_{n}}{2}}\right)^{s} X^{\frac{1}{e(G)}}+\left(X^{2 \sigma_{n}} \log X\right)^{t}\left(X^{\sigma_{n}}\right)^{s} X^{\frac{1}{12}} \ll X^{\frac{1}{d(G)}}(\log X)^{t}
$$

The contribution from the error term $O\left(\left(\frac{1}{p_{1}}+\cdots+\frac{1}{p_{t}}+\frac{1}{q_{1}}+\cdots \frac{1}{q_{s}}\right) X^{\frac{1}{d(G)}}\right)$ is dominated by $X^{\frac{1}{d(G)}}(\log X)^{k-1}$. The main term of the sum, after being divided by $\left|\mathcal{E}_{G}(X)\right|\left(\frac{\log X}{-2}\right)^{k}$, gives rise to

$$
\prod_{i=1}^{t}\left(\left(\frac{-2}{\log X}\right)^{2} \sum_{p} \frac{\log ^{2} p}{p} \widehat{\phi}_{n}\left(\frac{\log p}{\log X}\right)^{2}\right) \times \prod_{j=1}^{s}\left(\frac{2}{\log X} \sum_{q} \frac{\log q}{q} \widehat{\phi}_{n}\left(\frac{2 \log q}{\log X}\right)\right)
$$

which equals, by the prime number theorem,

$$
\left(2^{t} \prod_{i=1}^{t} \int_{\mathbb{R}}|u| \widehat{\phi}_{n}(u)^{2} d u\right)\left(\left(\frac{1}{2}\right)^{s} \prod_{j=1}^{s} \int_{\mathbb{R}} \widehat{\phi}_{n}(u) d u\right) .
$$

Since there are $(2 t)!/ 2^{t}$ ways to pair up two elements in $S_{2}$, the claim follows.
By Propositions 4.4 and 4.5 , and (18) we have the following inequality

$$
D_{n}^{*}\left(\mathcal{E}_{G}, \Phi\right) \leq \phi_{n}(0)^{n} \sum_{S}\left(\frac{1}{\sigma_{n}}\right)^{\left|S^{c}\right|} \sum_{\substack{S_{2} \subset S \\\left|S_{2}\right| \text { even }}}\left(\frac{1}{2}\right)^{\left|S_{2}^{c}\right|}\left|S_{2}\right|!\left(\frac{1}{6}\right)^{\frac{\left|S_{2}\right|}{2}}+O\left(\frac{1}{\log X}\right)
$$

and, by (19), 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

$$
\limsup _{X \rightarrow \infty} \frac{1}{\left|\mathcal{E}_{G}(X)\right|} \sum_{E \in \mathcal{E}_{G}(X)} r_{E}^{n} \leq \sum_{S}\left(\frac{1}{\sigma_{n}}\right)^{\left|S^{c}\right|} \sum_{\substack{S_{2} \subset S \\\left|S_{2}\right| \text { even }}}\left(\frac{1}{2}\right)^{\left|S_{2}^{c}\right|}\left|S_{2}\right|!\left(\frac{1}{6}\right)^{\frac{\left|S_{2}\right|}{2}}
$$

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 ranks of $\mathcal{E}_{\mathbb{Z} / 2 \mathbb{Z}}$ is bounded by 9.5 and the average analytic ranks of $\mathcal{E}_{\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 2 \mathbb{Z}}$ is bounded by 10.5.

Now, we show the sparsity of elliptic curves in $\mathcal{E}_{G}$ with high analytic ranks. We choose the test function $\phi_{2 n}(x)$. Then $\widehat{\phi}_{2 n}(0)=\frac{1}{4} \sigma_{2 n}$, and $\phi_{2 n}(0)=\frac{1}{4} \sigma_{2 n}^{2}$.

By Weil's explicit formula, we have

$$
r_{E} \phi_{2 n}(0) \leq \widehat{\phi}_{2 n}(0)-\frac{2}{\log X} \sum_{m_{i}} \frac{\widehat{a}_{E}\left(m_{i}\right) \Lambda\left(m_{i}\right)}{\sqrt{m_{i}}} \widehat{\phi}_{2 n}\left(\frac{\log m_{i}}{\log X}\right)+O\left(\frac{1}{\log X}\right)
$$

hence

$$
r_{E} \leq \frac{1}{\sigma_{2 n}}+\frac{4}{\sigma_{2 n}^{2}}\left(-\frac{2}{\log X} \sum_{m_{i}} \frac{\widehat{a}_{E}\left(m_{i}\right) \Lambda\left(m_{i}\right)}{\sqrt{m_{i}}} \widehat{\phi}_{2 n}\left(\frac{\log m_{i}}{\log X}\right)\right)+O\left(\frac{1}{\sigma_{2 n}^{2} \log X}\right)
$$

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

$$
-\frac{2}{\log X} \sum_{m_{i}} \frac{\widehat{a}_{E}\left(m_{i}\right) \Lambda\left(m_{i}\right)}{\sqrt{m_{i}}} \widehat{\phi}_{2 n}\left(\frac{\log m_{i}}{\log X}\right) \geq \frac{C \sigma_{2 n}}{4}
$$

Therefore,

$$
\begin{aligned}
\left|\left\{E \in \mathcal{E}_{G}(X) \left\lvert\, r_{E} \geq \frac{1+C}{\sigma_{2 n}}\right.\right\}\right| & \left(\frac{C \sigma_{2 n}}{4}\right)^{2 n} \leq \sum_{E \in \mathcal{E}_{G}(X)}\left(-\frac{2}{\log X} \sum_{m_{i}} \frac{\widehat{a}_{E}\left(m_{i}\right) \Lambda\left(m_{i}\right)}{\sqrt{m_{i}}} \widehat{\phi}_{2 n}\left(\frac{\log m_{i}}{\log X}\right)\right)^{2 n} \\
& \leq\left(\frac{\sigma_{2 n}^{2}}{4}\right)^{2 n} \sum_{S_{2} \subset\{1,2,3, \ldots, 2 n\}}\left(\frac{1}{2}\right)^{\left|S_{S}^{c}\right|}\left|S_{2}\right|!\left(\frac{1}{6}\right)^{\frac{\left|S_{2}\right|}{2}}\left|\mathcal{E}_{G}(X)\right|+O\left(\frac{X^{\frac{1}{d(G)}}}{\log X}\right),
\end{aligned}
$$

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

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

where $\sigma_{2 n}=\frac{1}{18 n}$ and $\frac{1}{20 n}$ for $G=\mathbb{Z} / 2 \mathbb{Z}$ and $G=\mathbb{Z} / 2 \mathbb{Z} \times \mathbb{Z} / 2 \mathbb{Z}$ respectively.
Acknowledgement We would like to thank Dohyeong Kim, John Voight, John Cullinan, and Junyeong Park for the useful discussion, Chan-Ho Kim for introducing the work of Harron and Snowden [HS14], Daniel Fiorilli for his comments.

## 5. Appendix

Here we summarize $f_{G}(a, b)$ and $g_{G}(a, b)$ for all torsion subgroup.

$$
\begin{aligned}
& \hline f_{5}=-27 a^{4}+324 a^{3} b-378 a^{2} b^{2}-324 a b^{3}-27 b^{4}, \\
& g_{5}=54 a^{6}-972 a^{5} b+4050 a^{4} b^{2}+4050 a^{2} b^{4}+972 a b^{5}+54 b^{6}, \\
& \hline f_{6}=-243 a^{4}-324 a^{3} b-810 a^{2} b^{2}-324 a b^{3}-27 b^{4}, \\
& g_{6}=-1458 a^{6}-2916 a^{5} b+7290 a^{4} b^{2}+9720 a^{3} b^{3}+5346 a^{2} b^{4}+972 a b^{5}+54 b^{6}, \\
& \hline f_{7}=-27 a^{8}+324 a^{7} b-1134 a^{6} b^{2}+1512 a^{5} b^{3}-945 a^{4} b^{4}+378 a^{2} b^{6}-108 a b^{7}-27 b^{8} \\
& g_{7}=54 a^{12}-972 a^{11} b+6318 a^{10} b^{2}-19116 a^{9} b^{3}+30780 a^{8} b^{4}-26244 a^{7} b^{5}+14742 a^{6} b^{6} \\
&-11988 a^{5} b^{7}+9396 a^{4} b^{8}-2484 a^{3} b^{9}-810 a^{2} b^{10}+324 a b^{11}+54 b^{12} \\
& \hline
\end{aligned}
$$

$$
\begin{aligned}
& \hline f_{8}=-432 a^{8}+1728 a^{7} b-6048 a^{6} b^{2}+12096 a^{5} b^{3}-12960 a^{4} b^{4}+7776 a^{3} b^{5}-2592 a^{2} b^{6}+432 a b^{7}-27 b^{8} \\
& g_{8}=-3456 a^{12}+20736 a^{11} b-190080 a^{9} b^{3}+555984 a^{8} b^{4}-855360 a^{7} b^{5}+840672 a^{6} b^{6} \\
&-554688 a^{5} b^{7}+246240 a^{4} b^{8}-71712 a^{3} b^{9}+12960 a^{2} b^{10}-1296 a b^{11}+54 b^{12} \\
& \hline f_{9}=-27 a^{12}+324 a^{11} b-1458 a^{10} b^{2}+3456 a^{9} b^{3}-5103 a^{8} b^{4}+4860 a^{7} b^{5}-3078 a^{6} b^{6} \\
&+972 a^{5} b^{7}+486 a^{4} b^{8}-756 a^{3} b^{9}+324 a^{2} b^{10}-27 b^{12} \\
& g_{9}= 54 a^{18}-972 a^{17} b+7290 a^{16} b^{2}-30780 a^{15} b^{3}+84078 a^{14} b^{4}-160380 a^{13} b^{5}+222912 a^{12} b^{6} \\
&-228420 a^{11} b^{7}+174960 a^{10} b^{8}-109728 a^{9} b^{9}+73386 a^{8} b^{10}-58320 a^{7} b^{11}+39690 a^{6} b^{12} \\
&-16524 a^{5} b^{13}+1458 a^{4} b^{14}+2268 a^{3} b^{15}-972 a^{2} b^{16}+54 b^{18} \\
& \hline
\end{aligned}
$$



## References

[BH] M. Bhargava, W. Ho, On average sizes of Selmer groups and ranks in families of elliptic curves having marked points, preprint. 2
[BS15] M. Bhargava, 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) $\mathbf{1 8 1}$ (2015), no. 2, pp.587-621. 1
[BS] M. Bhargava, 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. 1
[Bru92] A. Brumer, The average rank of elliptic curves I, Invent. Math. 109 (1992), no. 3, pp.445-472. 2
[CHL19] S. Chan, J. Hanselman, 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 Thirteenth Algorithmic Number Theory Symposium, pp.173-189, Open Book Ser., 2, Math. Sci. Publ., Berkeley, CA, 2019. 3
[CJ] P. J. Cho, K. Jeong, On the distribution of analytic ranks of elliptic curves, preprint. 23, 29
[CKV] J. Cullinan, M. Kenney, J. Voight, On a probabilistic local-global principle for torsion on elliptic curves, preprint, https://arxiv.org/abs/2005.06669 4, 5, 6, 10, 11, 21
[Dic06] L. E. Dickson, Criteria for the irreducibility of functions in a finite field, Bull. Amer. Math. Soc. 13 (1906), no. 1, pp.1-8. 9 [DS05] F. Diamond, J. Shurman, A first course in modular forms. Graduate Texts in Mathematics, 228. Springer-Verlag, New York, 2005. xvi+436 pp. ISBN: 0-387-23229-X 22
[Gol79] D. Goldfeld, Conjectures on elliptic curves over quadratic fields, Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979) , Lecture Notes in Math. 751 (Springer, Berlin, 1979) pp.108-118. 1
[GT12] I. Gracía-Selfa, J. M. Tornero, A complete Diophantine characterization of the rational torsion of an elliptic curve. Acta Math. Sin. (Engl. Ser.) 28 (2012), no. 1, pp.83-96. 4, 11
[HS14] R. Harron, A. Snowden, Counting elliptic curves with prescribed torsion, J. Reine Angew. Math. 729 (2017), pp.151-170. $2,10,17,19,32$
[Hea04] D. R. Heath-Brown, The average analytic rank of elliptic curves, Duke Math. J. 122 (2004), no. 3, pp.591-623. 2, 3
[Kub76] D. S. Kubert, Universal bounds on the torsion of elliptic curves. Proc. London Math. Soc. (3) 33 (1976), no. 2, pp.193-237. 5
[KP17] N. Kaplan, I. Petrow, Elliptic curves over a finite field and the trace formula, Proc. Lond. Math. Soc. (3) 115 (2017), no. 6, pp.1317-1372. 3, 14, 15
[Mil] S. J. Miller, 1- and 2-level densities for families of elliptic curves: Evidence for the underlying group symmetries, Thesis (Ph.D.) - Princeton University. 2002. 225 pp. ISBN: 978-0493-55316-0 29
[PPVW19] J. Park, B, Poonen, J. Voight, M. M. Wood, A heuristic for boundness of ranks of elliptic curves, J. Eur. Math. Soc. 21 (2019), no. 9, pp.2859-2903. 1, 2
[Sag] SageMath, the Sage Mathematics Software System (Version 9.2), The Sage Developers, https://www. sagemath.org. 6
[Sch87] R. Schoof, Nonsingular plane cubic curves over finite fields. J. Combin. Theory Ser. A 46 (1987), no. 2, pp.183-211. 16
[Wat] M. Watkins, A discursus 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. 1
[Wat $\left.{ }^{+} 14\right]$ M. Watkins, S. Donnelly, N. D. Elkies, T. Fisher, A. Granville, N. F. Rogers, Ranks of quadratic twists of elliptic curves, Numéro consacré au trimestre "Méthodes arithmétiques et applications", automne 2013, pp. 63-98, Publ. Math. Basançon Algébre Théorie Nr., 2014/2, Presses Univ. Franche-Comté, Besançon, 2015. 1
[You06] M. P. Young, Low-lying zeros of families of elliptic curves, J. Amer. Math. Soc. 19 (2006), no. 1, pp.205-250. 2, 3
Department of Mathematical Sciences, Ulsan National Institute of Science and Technology, UniSt-gil 50, Ulsan 44919, Korea

Email address: petercho@unist.ac.kr
Department of Mathematical Sciences, Ulsan National Institute of Science and Technology, UniSt-gil 50, Ulsan 44919, Korea

Email address: kyjeong@unist.ac.kr

