On the distribution of analytic ranks of elliptic curves

Peter J. Cho$^1$ · Keunyoung Jeong$^2$

Received: 22 July 2020 / Accepted: 12 September 2023 / Published online: 5 October 2023
© The Author(s), under exclusive licence to Springer-Verlag GmbH Germany, part of Springer Nature 2023

Abstract
In this paper, under GRH for elliptic curve $L$-functions, we give an upper bound for the probability for an elliptic curve with analytic rank $\leq a$ for $a \geq 11$, and also provide an upper bound of $n$-th moments of analytic ranks of elliptic curves. These are applications of counting elliptic curves with local conditions.

Keywords Elliptic curve · Rank · Trace formula · GRH · BSD conjecture

Mathematics Subject Classification Primary 11G05; Secondary 11G40 · 11M26

1 Introduction

In this article, we study the distribution of analytic ranks of elliptic curves over rational numbers. First, we explain the model of elliptic curves in our consideration. We treat elliptic curves of the form:

$$E_{A,B} : y^2 = x^3 + Ax + B, \ A, B \in \mathbb{Z} \quad \text{if a prime } q \text{ satisfies } q^4 \mid A, \text{ then } q^6 \nmid B.$$

We denote the prime condition by (M), and define a naive height of $E_{A,B}$ by

$$H(E_{A,B}) := \max(|A|^3, |B|^2).$$

Peter J. Cho was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (2022R1A2C1009297).

Keunyoung Jeong was supported by the National Research Foundation of Korea (NRF) funded by the Ministry of Education, under the Basic Science Research Program (2019R1C1C1004264).

$^1$ Department of Mathematical Sciences, Ulsan National Institute of Science and Technology, UNIST-gil 50, Ulsan 44919, Republic of Korea

$^2$ Department of Mathematics Education, Chonnam National University, 77, Yongbong-ro, Buk-gu, Gwangju 61186, Republic of Korea
The family of our interest is
\[ E(X) := \{(A, B) \in \mathbb{Z}^2 : 4A^3 + 27B^2 \neq 0, H(E_{A,B}) \leq X, \text{ and } (A, B) \text{ satisfies (M)}\}. \]

Note that \(|E(X)| = \frac{4}{\zeta(10)}X^{\frac{5}{6}} + O(X^{\frac{1}{2}})\) [5, Lemma 4.3]. Let \(a\) be a positive integer. Then, we define the proportion \(P(r_E \geq a)\) of elliptic curves with analytic rank \(r_E \geq a\) as
\[
\limsup_{X \to \infty} \frac{1}{|E(X)|} \sum_{(A, B) \in E(X)} \frac{1}{r_E A, B \geq a}.
\]

We give a numerical bound for \(P(r_E \geq a)\).

**Theorem 1.1** Assume GRH for elliptic curve L-functions. Let \(C\) be a positive constant, and let \(n\) be a positive integer. We have
\[
P(r_E \geq (1 + C)9n) \leq \sum_{k=0}^{n} \frac{\binom{2n}{2k} \left(\frac{1}{2}\right)^{2n-2k} (2k)! \left(\frac{1}{5}\right)^k}{(C \cdot 9n)^{2n}}.
\]

Next, we show that there are, at most, a small proportion of elliptic curves with large analytic ranks. Let \(P(r_E \leq a) := 1 - P(r_E \geq a + 1)\).

**Corollary 1.2** Assume GRH for elliptic curve L-functions. Let \(f(t) = \sum_{k=0}^{t} \binom{2t}{2k} \left(\frac{1}{2}\right)^{2t-2k} (2k)! \left(\frac{1}{5}\right)^k\). Then,

1. \(P(r_E \leq a) \geq 1 - \frac{f(t)}{(a-8)^2}\) for \(11 \leq a \leq 17\).
2. \(P(r_E \leq a) \geq 1 - \min_{1 \leq l \leq n} \left\{ \frac{f(l)}{(a+1-9)^2} \right\}\) for \(9n \leq a \leq 9n + 8, n \geq 2\).

Let \(LB(r_E \leq a)\) be the lower bound of \(P(r_E \leq a)\). For some small \(a\)’s, \(LB(r_E \leq a)\) is recorded in the following table and graph.

| \(a\) | \(LB(r_E \leq a)\) | \(a\) | \(LB(r_E \leq a)\) | \(a\) | \(LB(r_E \leq a)\) | \(a\) | \(LB(r_E \leq a)\) |
|------|-------------------|------|-------------------|------|-------------------|------|-------------------|
| 11   | 0.935185          | 16   | 0.990885          | 21   | 0.996548          | 26   | 0.999812          |

![Graph showing LB(r_E ≤ a)](image)
Remark (1) The model of [11] conjectures that there are only finitely many elliptic curves with rank $> 21$. Our result shows that the proportion of elliptic curves with analytic rank $> 21$ is less than 0.0035 under the GRH for elliptic curve $L$-functions.

(2) Our upper bound for $P(r_E \geq (1 + C)9n)$ decays exponentially for a suitable constant $C$. We can see this easily as follows:

$$
\sum_{k=0}^{n} \frac{(2k)!}{(C \cdot 9n)^{2n}} \frac{1}{n^2 (2k)!^2} \geq \frac{(2n)!}{(C \cdot 9n)^{2n}} \frac{1}{(\sqrt{6e} \cdot C \cdot 9n)^{2n}} = \frac{n^{\frac{1}{2}} 2^{2n}}{(\sqrt{6e} \cdot C \cdot 9)^{2n}}.
$$

Therefore, Heath–Brown’s result [9, Theorem 2]

$$
P(r_E \geq a) \ll \left( \frac{3}{2} a \right)^{-\frac{a}{12}}
$$

is stronger than ours for a very large rank $a$. However, our emphasis is on a small rank $a$, not a large rank $a$. Theorem 1.1 is not an explicitation of the implicit constant in [9, Theorem 2], and our method of the proof is different. For the proof, we establish the Frobenius trace formula for elliptic curves (Theorem 3.1). Our approach is in the same spirit as Katz and Sarnak’s $n$-level density conjecture. For the introduction to the $n$-level density conjecture and some partial results, we refer to [6, 10, 12].

(3) In the proof of the Frobenius trace formula, Theorem 3.1, we use similar arguments in [6]. The new feature here is the Eichler–Selberg trace formula which replaces the role of orthogonality of characters in [6].

(4) For algebraic ranks, we remark that the recent development of [2, 3] gives better bounds than ours. Since the average of the order of $\text{Sel}_5(E/\mathbb{Q})$ is 6 by [3], we have

$$
P(r_E \geq a) 5^a \leq 6
$$

by the exact sequence

$$
0 \to E(\mathbb{Q}) \to 5E(\mathbb{Q}) \to \text{Sel}_5(E/\mathbb{Q}) \to III(E/\mathbb{Q})[5] \to 0.
$$

Hence for example, $P(r_E < 20)$ is bounded below by $1 - 6/5^{20} = 0.99999999999993708544$. However, for the average of analytic ranks, Young’s bound $\frac{25}{14}$ [15] under GRH is the best record. It gives a bound for $P(r_E \geq a)$, which is $\frac{25}{14a}$.

The second one concerns the moments of the analytic ranks of elliptic curves. One can show that the limsup of $n$-th moments of analytic ranks of elliptic curves exists by applying the result of Heath-Brown [9, Theorem 2]. Using an approach of Miller [10], we propose an explicit upper bound on the $n$-th moment of analytic ranks for every positive integer $n$.

**Theorem 1.3** Assume GRH for elliptic curve $L$-functions. Let $r_E$ be the analytic rank of an elliptic curve $E$. For every positive integer $n$, we have

$$
\limsup_{X \to \infty} \frac{1}{|E(X)|} \sum_{E \in E(X)} r_E^n \leq \sum_S \left( \frac{9n}{2} \right)^{|S'|} \sum_{S_2 \subset S} \left( \frac{1}{2} \right)^{|S_2'|} |S_2|! \left( \frac{1}{6} \right)^{|S_2|}.
$$

where $S$ runs over subsets of $\{1, 2, 3, \ldots, n\}$, and $S_2$ runs over subsets of even cardinality of the set $S$. In particular, the limsup of the 2nd moment of analytic ranks is bounded by 90.584, and the limsup of the 3rd moment of analytic ranks is bounded by 2758.
After the proof of Theorem 1.3, we also show that the upper bound is asymptotically
\[
\frac{243}{241} \left( \frac{9n + 1}{2} \right)^n \left( 1 + O(n^{-\frac{1}{2}}) \right).
\]

These results are obtained by an accurate count of elliptic curves with local conditions, which is of its own interest. A local condition at prime \( p \) is a condition that is satisfied when an elliptic curve is reduced modulo \( p \). In this paper, a local condition is one of good reduction, bad reduction, multiplicative reduction, additive reduction, \( a \) in the Weil bound,\(^1\) split reduction, non-split reduction, or Kodaira–Néron types.

We can count elliptic curves with a local condition. Let
\[
\mathcal{E}^\mathcal{LC}_p(X) = \{(A, B) \in \mathcal{E}(X) : E_{A,B} satisfies \mathcal{LC} at the prime \ p\},
\]
where \( \mathcal{LC} \) is one of the local conditions. Then, we have

**Theorem 1.4** For \( 5 \leq p \leq X^{\frac{1}{3m_{\mathcal{LC}}}} \),
\[
\left| \mathcal{E}^\mathcal{LC}_p(X) \right| = c_{\mathcal{LC}}(p) \frac{4}{\xi(10)} X^\frac{5}{2} + O(h_{\mathcal{LC},p}(X)),
\]
where \( m_{\mathcal{LC}}, c_{\mathcal{LC}}(p), h_{\mathcal{LC},p}(X) \) are given by the following table.

| Local conditions       | \( c_{\mathcal{LC}}(p) \)            | \( h_{\mathcal{LC},p}(X) \) | \( m_{\mathcal{LC}} \) |
|-----------------------|--------------------------------------|-------------------------------|-------------------------|
| good                  | \( \frac{p^2 - p}{p^2 - p} \frac{p^{10}}{p^{10} - 1} \) | \( pX^\frac{1}{2} \) 1         | 1                       |
| bad                   | \( \frac{p^2 - p}{p^2 - p} \frac{p^{10}}{p^{10} - 1} \) | \( pX^\frac{1}{2} \) 1         | 1                       |
| mult                  | \( \frac{p^2 - p}{p^2 - p} \frac{p^{10}}{p^{10} - 1} \) | \( pX^\frac{1}{2} \) 1         | 1                       |
| split, non-split      | \( \frac{p^2 - p}{p^2 - p} \frac{p^{10}}{p^{10} - 1} \) | \( pX^\frac{1}{2} \) 1         | 1                       |
| addi                  | \( \frac{p^2 - p}{p^2 - p} \frac{p^{10}}{p^{10} - 1} \) | \( pX^\frac{1}{2} \) 1         | 1                       |
| \( a \frac{p-1}{2p^2}(a^2-4p) \) | \( \frac{p^{10}}{p^{10} - 1} \) | \( H(a^2 - 4p) X^\frac{1}{2} \) | 1                       |
| \( I_m \)             | \( \frac{1}{p} \left( 1 - \frac{1}{p} \right)^2 \frac{p^{10}}{p^{10} - 1} \) | \( pX^\frac{1}{2} \) \( m + 1 \) | 1                       |
| \( II \)              | \( \frac{1}{p^2} \left( 1 - \frac{1}{p} \right)^2 \frac{p^{10}}{p^{10} - 1} \) | \( X^\frac{1}{2} \) 2         | 1                       |
| \( III \)             | \( \frac{1}{p^2} \left( 1 - \frac{1}{p} \right)^2 \frac{p^{10}}{p^{10} - 1} \) | \( X^\frac{1}{2} \) 3         | 1                       |
| \( IV \)              | \( \frac{1}{p^2} \left( 1 - \frac{1}{p} \right)^2 \frac{p^{10}}{p^{10} - 1} \) | \( X^\frac{1}{2} \) 4         | 1                       |
| \( IV^* \)            | \( \frac{1}{p^2} \left( 1 - \frac{1}{p} \right)^2 \frac{p^{10}}{p^{10} - 1} \) | \( p^{-1} X^\frac{1}{2} \) 6    | 1                       |
| \( III^* \)           | \( \frac{1}{p^2} \left( 1 - \frac{1}{p} \right)^2 \frac{p^{10}}{p^{10} - 1} \) | \( p^{-2} X^\frac{1}{2} \) 5    | 1                       |
| \( II^* \)            | \( \frac{1}{p^2} \left( 1 - \frac{1}{p} \right)^2 \frac{p^{10}}{p^{10} - 1} \) | \( p^{-2} X^\frac{1}{2} \) 7    | 1                       |
| \( I_m^* \)           | \( \frac{1}{p^m+\frac{5}{2}} \left( 1 - \frac{1}{p} \right)^2 \frac{p^{10}}{p^{10} - 1} \) | \( pX^\frac{1}{2} \) \( m + 6 \) | 1                       |
| \( I_0^* \)           | \( \frac{1}{p^x} \left( 1 - \frac{1}{p} \right)^2 \frac{p^{10}}{p^{10} - 1} \) | \( pX^\frac{1}{2} \) 5         | 1                       |

\(^1\) We say that an elliptic curve \( E \) satisfies a local condition \( a \) in the Weil bound if \( E \) has good reduction at \( p \) and \( a = a_E(p) := p + 1 - \#E(\mathbb{F}_p) \).
Here \( H(\cdot) \) is the Hurwitz class number.

We can count elliptic curves not only with a single local condition but also with finitely many local conditions. Let \( S = \{ \mathcal{LC}_{p_i} \} \) be a finite set of local conditions, where \( \mathcal{LC}_p \) can be good, bad, split, non-split, additive, \( a \) in the Weil bound, or \( T \) one of Kodaira–Néron types.

Let \( |\mathcal{LC}_p| \) be the probability given in Theorems 1.4 and let us define \(|S| = \prod_i |\mathcal{LC}_{p_i}|. \) We simply denote \( m_{\mathcal{LC}_{p_i}} \) by \( m_i \). Let

\[
\mathcal{E}^S(X) = \{(A, B) \in \mathcal{E}(X) : E_{A,B} \text{ satisfies } S\},
\]

and let

\[
c_{p_i} := \begin{cases} 
p_i & \text{if } \mathcal{LC}_{p_i} \text{ is bad,} \\
p_i + 1 & \text{if } \mathcal{LC}_{p_i} \text{ is additive,} \\
|\mathcal{LC}_{p_i}| \left(\frac{p_i^{10} - 1}{p_i^{10}}\right) p_i^{m_i} & \text{otherwise.}
\end{cases}
\]

In the following theorem, we show that these local conditions are independent.

**Theorem 1.5** Let \( S = \{ \mathcal{LC}_{p_i} : i = 1, 2, \ldots, n \} \) be a set of local conditions at primes \( p_i \)'s \( \geq 5 \) such that \( \prod_{i=1}^{n} p_i^{m_i} \leq X^{\frac{1}{2}} \) for some \( \epsilon > 0 \). Then, we have

\[
\mathcal{E}^S(X) = |S| \frac{4}{\zeta(10)} X^5 + O\left(\left(\prod_{i=1}^{n} c_{p_i}\right) X^{\frac{1}{2}}\right).
\]

In [14, §3.4], Watkins predicted probabilities for Kodaira–Néron types at a prime \( p \geq 5 \) with a heuristic approach. Our results agree with those in [14]. Also, we found a result [1] of counting elliptic curves with the local condition \( a \) in the Weil bound. In [1], they consider the family of elliptic curves \( y^2 = x^3 + Ax + B \) without the minimality condition \((M)\). Hence it contains many isomorphic elliptic curves. Their dominant error term is \( O(X^{\frac{1}{2}}/p) \), which is much weaker than \( O(H(a^2 - 4p)X^{\frac{1}{2}}) \) in Theorem 1.4 for a small prime \( p \).

In Cremona and Sadek’s recent work [8], the authors consider similar problems. They use the general Weierstrass model, so their approach also gives a natural probability for each local condition at \( p = 2 \) or 3. Their model gives the probability for semi-stability, which is 60.85%. This result seems more natural than Wong’s probability for semi-stability 17.9% [17]. We can only count elliptic curves with finitely many local conditions, but we have an explicit error term. There will be potential applications in elliptic curve \( L \)-functions.

In Sect. 2, we give proof for Theorems 1.4 and 1.5. In Sect. 3, we state and provide proof for the Frobenius trace formula for elliptic curves. Section 4 is devoted to the proof for Theorems 1.1 and 1.3.

## 2 Counting elliptic curves

### 2.1 With a single local condition

In this section, we give proof of Theorem 1.4. First, we must define the mod \( p^m \) analogue of the sets in [5, §4], where \( p \) is prime and \( m \) is a positive integer. Let

\[
\mathcal{D}(X) := \{(A, B) \in \mathbb{Z}^2 : \max(|A|^3, |B|^2) \leq X\}
\]
and
\[ D_{p^m,\alpha,\beta}(X) := \{(A, B) \in D(X) : (A, B) \equiv (\alpha, \beta) \pmod{p^m}\} \]
for \( \alpha, \beta \in (\mathbb{Z}/p^m\mathbb{Z})^2 \). For example, \( D_{p,0,0}(X) \) is a pair of integers with a height condition which is equivalent to (0, 0) modulo \( p \). We also define
\[ M_{p^m,\alpha,\beta}(X) := \{(A, B) \in D_{p^m,\alpha,\beta}(X) : (A, B) \text{ satisfies (M)}\} \]
and
\[ E_{p^m,\alpha,\beta}(X) := \{(A, B) \in M_{p^m,\alpha,\beta}(X) : 4A^3 + 27B^2 \neq 0\}, \tag{2.1} \]
and \( S_{p^m,\alpha,\beta}(X) \) as the unique set satisfying \( M_{p^m,\alpha,\beta}(X) = E_{p^m,\alpha,\beta}(X) \bigcup S_{p^m,\alpha,\beta}(X) \).

The next lemma will be used to estimate the size of \( D_{p^m,\alpha,\beta}(X) \).

**Lemma 2.1** Let \( m \leq C, n \leq D \) and \( \alpha, \beta \in \mathbb{Z}/m\mathbb{Z}, \beta \in \mathbb{Z}/n\mathbb{Z} \). The cardinality of the set
\[ \{(c, d) \in \mathbb{Z}^2 : |c| \leq C, |d| \leq D, (c, d) \equiv (\alpha, \beta) \pmod{\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}}\}, \]
is
\[ 4 \cdot \left\lfloor \frac{C + 1}{m} \right\rfloor \cdot \left\lfloor \frac{D + 1}{n} \right\rfloor + O \left( \left\lfloor \frac{C + 1}{m} \right\rfloor + \left\lfloor \frac{D + 1}{n} \right\rfloor + 1 \right). \]

In the next lemma, we want to consider three types of \((\alpha, \beta)\):

1. \((\alpha, \beta) \in (\mathbb{Z}/p\mathbb{Z})^2\) which is not equal to (0, 0) modulo \( p \),
2. \((\alpha, \beta) \in ((\mathbb{Z}/p^m\mathbb{Z})^\times)^2\),
3. \((\alpha, \beta) \in (\mathbb{Z}/p^m\mathbb{Z})^2\) with \( p^4 \nmid \alpha \) or \( p^6 \nmid \beta \).

Those three types are related to the elliptic curves with good, multiplicative, and additive reduction, respectively (cf. (2.3), Lemmas 2.4 and 2.5).

To precisely define the third case, let us define the divisibility of elements in \( \mathbb{Z}/p^m\mathbb{Z} \). We say that \( \alpha \in \mathbb{Z}/p^m\mathbb{Z} \) is divisible by \( p^n \) when \( \alpha = ap^n \) for some \( a \in \mathbb{Z}/p^m\mathbb{Z} \). Especially if \( a \in \mathbb{Z}/p^m\mathbb{Z} \) is divisible by \( p^n \) for \( n > m \), then \( a \) should be zero. We also say that \( \alpha \) is exactly divisible by \( p^n \) when there exists \( u \in (\mathbb{Z}/p^m\mathbb{Z})^\times \) such that \( \alpha = up^n \). So \( \alpha \in \mathbb{Z}/p^m\mathbb{Z} \) cannot be exactly divisible by \( p^n \) for \( n > m \). Note that the third case now includes the first two cases.

We define \(*\)-operator on a pair by \( d * (a, b) := (d^4a, d^6b) \), and \( d * \{(a_i, b_i)\}_{i \in I} := \{d * (a_i, b_i)\}_{i \in I} \) for a set of pairs \( \{(a_i, b_i)\}_{i \in I} \). The latter operator will be used in §2.2.

**Lemma 2.2** For a nonzero \((\alpha, \beta) \in (\mathbb{Z}/p^m\mathbb{Z})^2\) such that \( p^4 \nmid \alpha \) or \( p^6 \nmid \beta \),
\[ D_{p^m,\alpha,\beta}(X) = \bigsqcup_{d \leq X^{\frac{1}{m}}} d * M_{p^m,d^{-4}\alpha,d^{-6}\beta}(d^{-12}X). \]

**Proof** This is an analogue of [5, (4.2)], but note that the condition \( p^4 \nmid \alpha \) or \( p^6 \nmid \beta \) gives a restriction on \( d \).

We note that when \( p^4 \nmid \alpha \) or \( p^6 \nmid \beta \), Lemma 2.2 gives
\[ |M_{p^m,\alpha,\beta}(X)| = \sum_{d \leq X^{\frac{1}{m}}} \mu(d) |D_{p^m,d^{-4}\alpha,d^{-6}\beta}(d^{-12}X)|. \tag{2.2} \]
We also note that the size of $S_{p^m,\alpha,\beta}(X)$ is bounded by the number of $A$ satisfying $|A| \leq X^{\frac{1}{2}}$ and $A \equiv \alpha \pmod{p^m}$. Hence $|S_{p^m,\alpha,\beta}(X)| = O(X^{\frac{1}{2}}/p^m + 1)$. We have a better estimate of the size of $S_{p^m,\alpha,\beta}(X)$ when $p \nmid \alpha$ and $p \nmid \beta$, or $m = 1$. However, we use the trivial bound only.

**Proposition 2.3** For a prime $5 \leq p^m \leq X^{\frac{1}{2}}$ and nonzero $(\alpha, \beta) \in (\mathbb{Z}/p^m\mathbb{Z})^2$ such that $p^4 \nmid \alpha$ or $p^6 \nmid \beta$,

$$|\mathcal{E}_{p^m,\alpha,\beta}(X)| = \frac{1}{p^{2m}} \frac{p^{10}}{p^{10} - 1} \frac{4}{\xi(10)} X^{\frac{5}{6}} + O\left(\frac{X^{\frac{1}{2}}}{p^m}\right).$$

Furthermore,

$$|\mathcal{E}_{p,0,0}(X)| = \frac{p^8 - 1}{p^{10} - 1} \frac{4}{\xi(10)} X^{\frac{5}{6}} + O\left(pX^{\frac{1}{2}}\right).$$

**Proof** We have $|\mathcal{E}_{p^m,\alpha,\beta}(X)| = |\mathcal{M}_{p^m,\alpha,\beta}(X)| O(|S_{p^m,\alpha,\beta}(X)|)$. We use the trivial bound $|S_{p^m,\alpha,\beta}(X)| \ll X^{\frac{3}{2}}/p^m + 1$. On the other hand

$$|\mathcal{E}_{p^m,\alpha,\beta}(X)| = |\mathcal{M}_{p^m,\alpha,\beta}(X)| + O(|S_{p^m,\alpha,\beta}(X)|)$$

by Lemma 2.1. By (2.2), we have

$$|\mathcal{E}_{p^m,\alpha,\beta}(X)| = \sum_{d \leq X^{\frac{1}{12}} \atop p^m|d} \mu(d) \left|\mathcal{D}_{p^m,d^{-4} \alpha, d^{-6} \beta}\left(\frac{X}{d^{12}}\right)\right| + O\left(\frac{X^{\frac{1}{2}}}{p^m} + 1\right),$$

which is equal to

$$= \sum_{d \leq X^{\frac{1}{12}} \atop p^m|d} \mu(d) \left(\frac{4X^{\frac{5}{6}}}{p^{2m}d^{10}} + O\left(\frac{X^{\frac{1}{2}}}{p^m d^6} + \frac{X^{\frac{1}{2}}}{p^m d^4} + 1\right)\right) + O\left(\frac{X^{\frac{3}{2}}}{p^m} + 1\right)$$

$$= \sum_{\substack{d \geq 1 \atop p^m|d}} \mu(d) \left(\frac{4X^{\frac{5}{6}}}{p^{2m}d^{10}} + O\left(\frac{X^{\frac{1}{2}}}{p^m} + X^{\frac{1}{12}} + \frac{X^{\frac{1}{2}}}{p^m} + 1\right)\right)$$

$$= \sum_{\substack{d \geq X^{\frac{1}{12}} \atop p^m|d}} \mu(d) \left(\frac{4X^{\frac{5}{6}}}{p^{2m}d^{10}} + O\left(\frac{X^{\frac{1}{2}}}{p^m} + \frac{X^{\frac{1}{2}}}{p^m} + 1\right)\right)$$

$$= \frac{4X^{\frac{5}{6}}}{p^{2m}} \sum_{d = 1 \atop p^m|d} \mu(d) \left(\frac{X^{\frac{1}{2}}}{p^m} + X^{\frac{1}{12}} + \frac{X^{\frac{1}{2}}}{p^m} + 1\right) = \frac{1}{p^{2m}} \frac{p^{10}}{p^{10} - 1} \frac{4}{\xi(10)} X^{\frac{5}{6}} + O\left(\frac{X^{\frac{1}{2}}}{p^m}\right)$$

for $p^m \leq X^{\frac{5}{6}}$. However, we restrict the range of $p$ to $p^m \leq X^{\frac{1}{3}}$ because we wish the main term to be larger than the error term.
Hence we have the first one. On the other hand, \(|E(X)| = \frac{4}{\xi(10)} X^{\frac{5}{6}} + O(X^{\frac{1}{2}})\) from \([5, \text{Lemma 4.3}]\) and

\[
|E(X)| = |E_{p,0,0}(X)| + \sum_{(0,0) \neq (\alpha, \beta) \in (\mathbb{Z}/p\mathbb{Z})^2} |E_{p,\alpha,\beta}(X)|,
\]
give the result for \(|E_{p,0,0}(X)|\).

We collect auxiliary lemmas on the number of elliptic curves corresponding to each local condition. For the good and bad reduction conditions, we use the cardinality of

\[
[(\alpha, \beta) \in (\mathbb{Z}/p\mathbb{Z})^2 : 4\alpha^3 + 27\beta^2 \equiv 0 \pmod{p}] = p,
\]

which follows from that half of the cubes in \(\mathbb{F}^2_p\) are quadratic residues. Let \(K\) be an imaginary quadratic field and \(\mathcal{O}\) be an order of \(K\). We define the Hurwitz class number \(H(\mathcal{O})\) by

\[
H(\mathcal{O}) := \sum_{\mathcal{O} \subset \mathcal{O}' \subset \mathcal{O}_K} \frac{2}{|\mathcal{O}'\times|} h(\mathcal{O}'),
\]

where \(h(\mathcal{O}')\) is the class number of an order \(\mathcal{O}'\). We also write \(H(\mathcal{O})\) as \(H(D)\), when \(D\) is the discriminant of \(\mathcal{O}\). By \([7, \text{Theorem 14.18}]\), we have

\[
[(\alpha, \beta) \in (\mathbb{Z}/p\mathbb{Z})^2 : 4\alpha^3 + 27\beta^2 \equiv 0 \pmod{p} \setminus a_{E,\alpha,\beta}(p) = a] \equiv \frac{p-1}{2} H(a^2 - 4p) \quad (2.4)
\]

where \(E_{\alpha,\beta} : y^2 = x^3 + \alpha x + \beta\) is an elliptic curve over \(\mathbb{F}_p\) and \(a_{E,\alpha,\beta}(p)\) is the trace of the Frobenius automorphism.

For multiplicative reduction, we need

**Lemma 2.4** Let \(p \geq 5\) be a prime, and let \(m \geq 1\) be an integer. Then,

\[
[(\alpha, \beta) \in (\mathbb{Z}/p^m\mathbb{Z})^2 : 4\alpha^3 + 27\beta^2 \equiv 0 \pmod{p^m}] = p^m \left(1 - \frac{1}{p}\right),
\]

and

\[
[(\alpha, \beta) \in (\mathbb{Z}/p\mathbb{Z})^2 : 4\alpha^3 + 27\beta^2 \equiv 0 \pmod{p}, \beta = -\beta^2] = \frac{p-1}{2}.
\]

The following results from Tate’s algorithm for \(E_{A,B}\).

**Lemma 2.5** Let \(p \geq 5\), and let \(E_{A,B} : y^2 = x^3 + Ax + B\) be a minimal model over \(\mathbb{Q}_p\). Then, \(E\) has

\[
\begin{cases}
\text{Type II if and only if } p \mid A, p \parallel B \\
\text{Type III if and only if } p \parallel A, p^2 \parallel B \\
\text{Type IV if and only if } p^2 \mid A, p^3 \parallel B
\end{cases}
\]

Furthermore, for the fixed positive integer \(m\), an elliptic curve \(E\) has reduction type \(I_m^x\) at \(p\) if and only if \(\sqrt{p} \parallel A\) or \(p^3 \parallel B\), and \(v_p(4(A/p^{3})^3 + 27(B/p^{3})^2) = m\).

Finally for the local conditions \(I_m^x\), we need

**Lemma 2.6** For \(m > 0\), we have

\[
[(\alpha, \beta) \in (\mathbb{Z}/p^{m+6}\mathbb{Z})^2 : p^2 \parallel \alpha, p^3 \parallel \beta, p^{m+6} \mid (4\alpha^3 + 27\beta^2)] = p^{m+5}(p-1)^2.
\]

For \(m = 0\), we have

\[
[(\alpha, \beta) \in (\mathbb{Z}/p^{6}\mathbb{Z})^2 : p^2 \parallel \alpha, p^3 \parallel \beta, p^6 \mid (4\alpha^3 + 27\beta^2)] = p^6(p-1).
\]
Proof of Theorem 1.4. We give a proof for $CC = \text{good}$, $\alpha$ in the Weil bound, $II^*$, and $II_{m}^*$. Let $S^\text{good} := \{(\alpha, \beta) \in (\mathbb{Z}/p\mathbb{Z})^2 : 4\alpha^3 + 27\beta^2 \not\equiv 0 \pmod{p}\}$. Now, the number of elliptic curves which have good reduction at $p \geq 5$ with height bounded by $X$ is

$$|\mathcal{E}_p^\text{good}(X)| = \sum_{(\alpha, \beta) \in S^\text{good}} |\mathcal{E}_{p,\alpha,\beta}(X)|.$$  

By Proposition 2.3, we have

$$|\mathcal{E}_p^\text{good}(X)| = \frac{(p^2 - p)}{p^2} \frac{p^{10}}{p^{10} - 1} \frac{4}{\zeta(10)} X^5 + O((p - 1)X^{\frac{1}{2}}).$$

For $a$ in the Weil bound,

$$\frac{(p - 1)\zeta(a^2 - 4p) H(a^2 - 4p)}{2p^2} \frac{p^{10}}{p^{10} - 1} \frac{4}{\zeta(10)} X^5 + O\left((p - 1) \frac{H(a^2 - 4p)}{2p} X^{\frac{1}{2}}\right),$$

by (2.4). Similarly, by Lemma 2.5, an elliptic curve $E_{A,B}$ has type $II^*$ at $p$ if and only if $(A, B)$ satisfies $p^4 | A$ and $p^5 | B$ modulo $p^7$. Since there are $p^3(p^2 - p)$ such pairs, we have

$$|\mathcal{E}^{II^*}_p(X)| = \frac{3(p^2 - p)}{p^{14}} \frac{p^{10}}{p^{10} - 1} \frac{4}{\zeta(10)} X^5 + O\left(p^3 (p^2 - p) X^{\frac{1}{2}}\right).$$

Now, $II_{m}^*$ case directly follows from Lemma 2.6. More concretely,

$$|\mathcal{E}^{II_{m}^*}_p(X)| = \sum_{\alpha, \beta} |\mathcal{E}_{p^{m+6},\alpha,\beta}(X)| = \frac{m+5(p - 1)}{p^{12}} \frac{p^{10}}{p^{10} - 1} \frac{4}{\zeta(10)} X^5 + O\left(p^m(p - 1)^2 X^{\frac{1}{2}}\right).$$

The other cases can be shown similarly.

\[\square\]

2.2 With finitely many local conditions

In this section, we give proof of Theorem 1.5. Let $P = \{p_i^{m_i}\}$ be a finite set of powers of primes such that $p_i \geq 5$, and let $I = I_P$ be a set of nonzero $(\alpha_i, \beta_i) \in (\mathbb{Z}/p_i^{m_i} \mathbb{Z})^2$. We recall that $d \ast I := \{(d^4 \alpha_i, d^6 \beta_i) : (\alpha_i, \beta_i) \in I\}$. Let

$$\mathcal{D}_{P,I}(X) := \{(A, B) \in \mathcal{D}(X) : (A, B) \equiv (\alpha_i, \beta_i) \pmod{p_i^{m_i}} \text{ for all } p_i^{m_i} \in P\},$$

and

$$\mathcal{M}_{P,I}(X) := \{(A, B) \in \mathcal{D}_{P,I}(X) : (A, B) \text{ satisfies (M)}\}. $$

Then, the analogue of Lemma 2.2 is as follows.

Lemma 2.7 Assume that all pairs in $I$ satisfy $p_i^4 \nmid \alpha_i$ or $p_i^6 \nmid \beta_i$. Then,

$$\mathcal{D}_{P,I}(X) = \bigsqcup_{d \leq X^{\frac{12}{12}}} d \ast \mathcal{M}_{P,d^{-1}}(d^{-12}X).$$

We also define

$$\mathcal{E}_{P,I}(X) := \{(A, B) \in \mathcal{M}_{P,I}(X) : 4A^3 + 27B^2 \not\equiv 0\},$$

and $S_{P,I}(X)$ as the unique set satisfying $\mathcal{M}_{P,I}(X) = \mathcal{E}_{P,I}(X) \bigcup S_{P,I}(X)$. The bound for the error term $S_{P,I}(X)$ is as follows.
Lemma 2.8 For $P$, $I$ as above, we have

$$|S_{P,I}(X)| \ll \frac{X^{\frac{1}{3}}}{\prod_i p_i^{m_i}} + 1.$$  

Proposition 2.9 Assume that all pairs in $I$ satisfy $p_i^4 \nmid \alpha_i$ or $p_i^6 \nmid \beta_i$, and $\prod p_i^{m_i} \leq X^{\frac{1}{3}}$. Then,

$$|E_{P,I}(X)| = \prod_i \left( \frac{1}{p_i^{2m_i}} \frac{p_i^{10}}{p_i^{10} - 1} \right) \frac{4}{\zeta(10)} X^{\frac{5}{12}} + O \left( \frac{X^{\frac{1}{2}}}{\prod p_i^{m_i}} + 1 \right).$$

Proof A modification of Lemmas 2.7 and 2.8 gives

$$|E_{P,I}(X)| = |M_{P,I}(X)| + O(S_{P,I}(X)) = \sum_{d \leq X^{\frac{1}{12}}} \mu(d) \left| D_{P,d^{-1} \ast I} \left( \frac{X}{d^{12}} \right) \right| + O \left( \frac{X^{\frac{1}{2}}}{\prod p_i^{m_i}} + 1 \right).$$

By Lemma 2.1, we have

$$D_{P,d^{-1} \ast I}(d^{-12}X) = \frac{4X^{\frac{5}{12}}}{\prod p_i^{2m_i} d^{10}} + O \left( \frac{X^{\frac{1}{2}}}{\prod p_i^{m_i} d^6} + \frac{X^{\frac{1}{3}}}{\prod p_i^{m_i} d^4} + 1 \right)$$

and the claim follows. $\square$

We recall some notations in Sect. 1. Let $LC_p$ be one of good, bad, split, non-split, an integer $a$ in the Weil’s bound, or Kodaira–Néron types $T$. We define

$$|LC_p| = \lim_{X \to \infty} \frac{|P^{LC_p}(X)|}{|E(X)|},$$

which is $c_{LC_p}(p)$ in Theorem 1.4. For the finite set of local conditions $S = \{LC_p_i\}$, we define $|S| = \prod_i |LC_p_i|$.

Now we are ready to prove Theorem 1.5. We first assume that any $LC_p$ is neither bad nor additive. Let $P = \{p_i^{m_i}\}$, then in the proof of Theorem 1.4, there are

$$|LC_{p_i}| \left( \frac{p_i^{10} - 1}{p_i^{10}} \right) p_i^{2m_i}$$

pairs $(\alpha_{i,j}, \beta_{i,j})$ in $(\mathbb{Z}/p_i^{m_i}\mathbb{Z})^2$ such that $E_{A,B}$ satisfies $LC_{p_i}$ if and only if $(A, B) \equiv (\alpha_{i,j}, \beta_{i,j}) \pmod{p_i^{m_i}}$ for some $(\alpha_{i,j}, \beta_{i,j})$. Let $I_{p_i} = \{ (\alpha_{i,j}, \beta_{i,j}) \}$ be the set of all the aforementioned pairs.

Let $I = \prod_i I_{p_i}$. We denote an element of $I$ by $(\alpha, \beta)$ whose $I_{p_i}$ component is $(\alpha_{i,j}, \beta_{i,j})$, and define $(A, B) \equiv (\alpha, \beta) \pmod{P}$ if and only if $(A, B) \equiv (\alpha_{i,j}, \beta_{i,j}) \pmod{p_i^{m_i}}$. By the Chinese remainder theorem, there are

$$\prod_i |LC_{p_i}| \left( \frac{p_i^{10} - 1}{p_i^{10}} \right) p_i^{2m_i}$$

Springer
elements \((\alpha, \beta)\) in \(I\) such that \(E_{A, B}\) satisfies all \(LC_p\) if and only if \((A, B) \equiv (\alpha, \beta) \pmod{P}\) for some \((\alpha, \beta)\) in \(I\). Together with Proposition 2.9, we have

\[
|E^S(X)| = \sum_i |E_{P, I}(X)| = \sum_i \left( \prod p_{i}^{m_{i}} \cdot \left( \frac{1}{p_{i}^{2m_{i}} - p_{i}^{10} - 1} \right) \cdot \frac{4}{\xi(10)} X^{5} + O \left( \frac{X^{4}}{\prod_{i} p_{i}^{m_{i}}} \right) \right)
\]

\[
= \left( \prod_{i} \left| LC_{p_{i}} \right| \right) X^{5} + O \left( \prod_{i} \left| LC_{p_{i}} \right| \left( \frac{p_{i}^{10} - 1}{p_{i}^{10}} \right) p_{i}^{m_{i}} X^{\frac{1}{2}} \right)
\]

\[
= |S| \cdot \frac{4}{\xi(10)} X^{5} + O \left( \prod_{i} \left| LC_{p_{i}} \right| \left( \frac{p_{i}^{10} - 1}{p_{i}^{10}} \right) p_{i}^{m_{i}} X^{\frac{1}{2}} \right).
\]

Hence we proved this theorem except when there is a local condition \(LC_p\) which is either bad or additive.

We use induction on the number of \(LC_p\)’s that are bad. Let \(S = \{LC_{p_{i}}\}\) be a finite set of local conditions such that there is an \(LC_{p_{n}}\) which is bad, and \(S' = S - \{LC_{p_{n}}\}\). By induction hypothesis for \(S' \cup \{LC'_{p_{n}}\}\) where \(LC'_{p_{n}}\) is good, we have

\[
|E^{S\cup\{LC'_{p_{n}}\}}(X)| = |S'| \cdot \frac{p_{n}^{2} - p_{n}^{10}}{p_{n}^{2}} \cdot \frac{4}{\xi(10)} X^{5} + O \left( \prod_{i=1}^{n-1} c_{p_{i}} (p_{n} - 1) X^{\frac{1}{2}} \right).
\]

Again by induction hypothesis for \(S'\), we have

\[
|E^{S'}(X)| = |S'| \cdot \frac{4}{\xi(10)} X^{5} + O \left( \prod_{i=1}^{n-1} c_{p_{i}} X^{\frac{1}{2}} \right).
\]

Since \(|E^{S'}(X)| = |E^{S\cup\{LC'_{p_{n}}\}}(X)| + |E^{S}(X)|\), we can count elliptic curves with bad reduction conditions.

We can do the same thing for the additive condition because the additive condition is the complement of the union of the conditions good, split, and non-split.

### 3 The Frobenius trace formula for elliptic curves

Let \(L(s, E)\) be the normalized elliptic curve \(L\)-function and for which we have

\[
L(s, E) = \sum_{n=1}^{\infty} \frac{\lambda_{E}(n)}{n^s} = \prod_{p} \left( 1 - \frac{\alpha_{E}(p)}{p^s} \right)^{-1} \left( 1 - \frac{\beta_{E}(p)}{p^s} \right)^{-1},
\]

\[
-\frac{L'}{L}(s, E) = \sum_{n=1}^{\infty} \frac{\tilde{\alpha}_{E}(n) \Delta(n)}{n^s}.
\]

Recall that

\[
\alpha_{E}(p) = \begin{cases} 
    p + 1 - \#E(\mathbb{F}_p) & \text{if } E \text{ has good reduction at } p, \\
    1, -1, 0 & \text{if } E \text{ has split, non-split, or additive reduction at } p.
\end{cases}
\]
For $\lambda_E(p) = \alpha_E(p) + \beta_E(p)$,\(^2\) we have
\[
\hat{\alpha}_E(p) = \frac{\alpha_E(p)}{\sqrt{p}}, \quad \hat{\alpha}_E(p^k) = \alpha_E(p)^k + \beta_E(p)^k.
\]

Here is the Frobenius trace formula for elliptic curves.

**Theorem 3.1** (Frobenius trace formula for elliptic curves) Let $k$ be a fixed positive integer. Let $p_i$ be distinct primes $\geq 5$ such that $\prod_{i=1}^{k} p_i = O(X^{\frac{1}{2} - \epsilon})$ for a fixed $\epsilon > 0$. 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,
\[
\sum_{E \in \mathcal{E}(X)} \hat{\alpha}_E(p_1^{e_1})^{r_1} \hat{\alpha}_E(p_2^{e_2})^{r_2} \cdots \hat{\alpha}_E(p_k^{e_k})^{r_k} = c|\mathcal{E}(X)| + O_k \left( 2^r \left( \prod_{i=1}^{k} p_i \right) X^{\frac{1}{2}} \right) + O_k \left( \left( \sum_{i=1}^{k} \frac{1}{p_i} \right) X^{\frac{5}{6}} \right)
\]
where
\[
c = \begin{cases} 
0 & \text{if } e_j = 1 \text{ and } r_j \text{ is odd for some } j, \\
-1 & \text{if } r_j = 2 \text{ for all } j \text{ with } e_j = 1, \text{ and the sum of } r_j \text{'s with } e_j = 2 \text{ is odd}, \\
1 & \text{otherwise},
\end{cases}
\]
and $r$ is either the smallest odd integer $r_i$ or 0 if there is no odd $r_i$, and the last error term exists only if $e_i = 1$ and $r_i = 2$ or $e_i = 2$ for all $i$.

Also, we have
\[
\sum_{E \in \mathcal{E}(X)} \lambda_E(p_1^{e_1})^{r_1} \lambda_E(p_2^{e_2})^{r_2} \cdots \lambda_E(p_k^{e_k})^{r_k} = d|\mathcal{E}(X)| + O_k \left( 2^r \left( \prod_{i=1}^{k} p_i \right) X^{\frac{1}{2}} \right) + O_k \left( \left( \sum_{i=1}^{k} \frac{1}{p_i} \right) X^{\frac{5}{6}} \right)
\]
where
\[
d = \begin{cases} 
0 & \text{if } e_j = 2 \text{ or } e_j = 1 \text{ and } r_j \text{ is odd for some } j, \\
1 & \text{if } e_i = 1 \text{ and } r_i = 2 \text{ for all } i.
\end{cases}
\]
and the last error term exists only if $e_i = 1$ and $r_i = 2$ or $e_i = 2$ for all $i$.

Before its proof, we compare this theorem with the results of [16]. The author computes
\[
\lim_{X \to \infty} \frac{1}{|\mathcal{E}_{6q,r,t}(X)|} \sum_{E \in \mathcal{E}_{6q,r,t}(X)} \lambda_E(n_1) \cdots \lambda_E(n_k)
\]
where $\mathcal{E}_{6q,r,t}(X)$ is defined in (2.1) and $r, t \in \mathbb{Z}/6q\mathbb{Z}$ for a square-free $q$, in [16, Lemma 3.2, Proposition 4.1, 4.2]. His proof is elegant. [16, Lemma 3.2] turns (3.1) into computing a certain finite sum over tuples of $\mathbb{Z}/p\mathbb{Z}$. However, for this reason, his proof does not give an error term as we have in Theorem 3.1, which is essential for our applications.

We give proof of Theorem 3.1 for one prime and two primes. First, we consider
\[
\sum_{E \in \mathcal{E}(X)} \hat{\alpha}_E(p)^r = \sum_{|a| \leq \sqrt{p}} \sum_{E \in \mathcal{E}(X)} \hat{\alpha}_E(p)^r + \sum_{E \in \mathcal{E}(X)} \hat{\alpha}_E(p)^r + \sum_{E \in \mathcal{E}(X)} \hat{\alpha}_E(p)^r
\]
\(^{2}\) If $E$ has bad reduction at $p$, then $\beta_E(p) = 0 \)
for an odd \( r \). By Theorem 1.4 for \(|a| \leq \lfloor 2\sqrt{p} \rfloor\), there are
\[
\frac{(p - 1)H(a^2 - 4p)}{2p^2} \cdot \frac{p^{10}}{p^{10} - 1} \cdot \frac{4}{\xi(10)} \cdot X^{\frac{5}{2}} + O \left( \frac{(p - 1)H(a^2 - 4p)}{2p} \cdot X^{\frac{1}{2}} \right)
\]
elastic curves in \( \mathcal{E}(X) \) with \( \hat{a}_E(p) = a/\sqrt{p} \). Since \( \sum_{|a| \leq \lfloor 2\sqrt{p} \rfloor} a^r H(a^2 - 4p) = 0 \), only the contribution from the error term survives, and it is at most \( O(2^r p X^{\frac{1}{2}}) \) because
\[
\frac{p - 1}{2p} \sum_{|a| \leq \lfloor 2\sqrt{p} \rfloor} \left( \frac{|a|}{\sqrt{p}} \right)^r H(a^2 - 4p) \leq 2^{r-1} \frac{p - 1}{p} \sum_{|a| \leq \lfloor 2\sqrt{p} \rfloor} H(a^2 - 4p) = 2^r (p - 1).
\]

If an elliptic curve \( E \) has additive reduction at prime \( p \), then \( \hat{a}_E(p) = 0 \). So there is no contribution from the additive reduction case. If \( E \) has split (resp. non-split) multiplicative reduction, then \( \hat{a}_E(p) = 1/\sqrt{p} \) (resp. \( \hat{a}_E(p) = -1/\sqrt{p} \)). There are
\[
\frac{p - 1}{2p^2} \cdot \frac{p^{10}}{p^{10} - 1} \cdot \frac{4}{\xi(10)} \cdot X^{\frac{5}{2}} + O(X^{\frac{1}{2}})
\]
elastic curves in \( \mathcal{E}(X) \) with split multiplicative reduction at \( p \), and also there are the same number of elastic curves with non-split multiplicative reduction at \( p \) up to error term \( O(X^{\frac{1}{2}}) \), by Theorem 1.4. The contribution from multiplicative reduction is \( O(X^{\frac{1}{2}}/p^{\frac{5}{2}}) \), hence we have
\[
\sum_{E \in \mathcal{E}(X)} \hat{a}_E(p)^r = O(2^r p X^{\frac{1}{2}}).
\]
The next case is
\[
\sum_{E \in \mathcal{E}(X)} \hat{a}_E(p)^2.
\]
From the identity \( \sum_{|a| \leq \lfloor 2\sqrt{p} \rfloor} a^2 H(a^2 - 4p) = 2p^2 - 2 \) which is an application of the Eichler–Selberg trace formula [4],\(^3\) the contribution from good reduction at \( p \) is
\[
\sum_{|a| \leq \lfloor 2\sqrt{p} \rfloor} \sum_{E \in \mathcal{E}(X) \atop a_E(p) = a} \hat{a}_E(p)^2 = \left( 1 + O \left( \frac{1}{p} \right) \right) \sum_{|a| \leq \lfloor 2\sqrt{p} \rfloor} \frac{4}{\xi(10)} \cdot X^{\frac{5}{2}} + O(p X^{\frac{1}{2}}),
\]
and the contribution from the multiplicative reduction is
\[
\sum_{E \in \mathcal{E}(X) \atop E \text{ mult red at } p} \hat{a}_E(p)^2 = \frac{p - 1}{p^3} \cdot \frac{p^{10}}{p^{10} - 1} \cdot \frac{4}{\xi(10)} \cdot X^{\frac{5}{2}} + O \left( \frac{X^{\frac{1}{2}}}{p} \right).
\]
Hence we have
\[
\sum_{E \in \mathcal{E}(X)} \hat{a}_E(p)^2 = \frac{4}{\xi(10)} X^{\frac{5}{2}} + O \left( \frac{X^{\frac{5}{2}}}{p} + p X^{\frac{1}{2}} \right).
\]
The last case for a single prime \( p \) is
\[
\sum_{E \in \mathcal{E}(X)} \hat{a}_E(p^2).
\]
\(^3\) There is a typo in [4, Theorem 2].
Note that $\widehat{a}_E(p^2) = \widehat{a}_E(p)^2 - 2$ when $E$ has good reduction at $p$, and $\widehat{a}_E(p^2) = \widehat{a}_E(p)^2$ when $E$ has bad reduction at $p$. Then, from the computation for the previous case, we can easily see that

$$\sum_{E \in E(X)} \widehat{a}_E(p^2) = -\frac{4}{\zeta(10)} X^\frac{5}{6} + O \left( \frac{X^\frac{5}{6}}{p} + pX^{\frac{1}{2}} \right),$$

which is exactly the trace formula for one prime in Theorem 3.1.

Now, we consider the trace formula for two primes

$$\sum_{E \in E(X)} \widehat{a}_E(p_1^{e_1})^{r_1} \widehat{a}_E(p_2^{e_2})^{r_2}.$$

Assume that $e_1 = 1$ and $r_1$ are odd. Fix a local condition for the second prime $p_2$. We vary the local conditions for the first prime $p_1$, and this gives $O(2^{r_1} p_1c_{p_2}^{-1} X^{\frac{1}{2}})$. Then we sum up this term over all the local conditions for $p_2$, and the error term $O(2^{r_1} p_1p_2^{-1} X^{\frac{1}{2}})$ follows.

We must deal with the cases $e_i = 1$ and $r_i = 2$ or $e_i = 2$ and $r_i = 1$ for $i = 1, 2$. First, we consider the cases $\mathcal{LC}_{p_1} = \mathcal{A}_1$, and $\mathcal{LC}_{p_2} = \mathcal{A}_2$ for $|a_1| \leq \lfloor \sqrt[4]{p_1} \rfloor$, $|a_2| \leq \lfloor \sqrt[4]{p_2} \rfloor$. Their contribution is, for example, when $r_1 = r_2 = 2$,

$$\left( \prod_{i=1}^{2} \frac{(p_i - 1)p_i^{10}}{2p_i^3(p_i^{10} - 1)} \right) \frac{4}{\zeta(10)} X^\frac{5}{6} \sum_{|a_1| \leq \lfloor \sqrt[4]{p_1} \rfloor, |a_2| \leq \lfloor \sqrt[4]{p_2} \rfloor} a_1^2 H(a_1^2 - 4p_1)a_2^2 H(a_2^2 - 4p_2)$$

$$+ O \left( \sum_{|a_1| \leq \lfloor \sqrt[4]{p_1} \rfloor, |a_2| \leq \lfloor \sqrt[4]{p_2} \rfloor} a_1^2 H(a_1^2 - 4p_1)a_2^2 H(a_2^2 - 4p_2) \frac{X^{\frac{1}{2}}}{(2p_1)(2p_2)} \right),$$

which is, by the identity $\sum_{|a| \leq \sqrt[4]{p}} a^2 H(a^2 - 4p) = 2p^2 - 2$,

$$\frac{4}{\zeta(10)} X^\frac{5}{6} + O \left( \left( \frac{1}{p_1} + \frac{1}{p_2} \right) X^\frac{5}{6} + p_1p_2 X^{\frac{1}{2}} \right).$$

Since the case that $p_1$ or $p_2$ has multiplicative reduction, using the trivial bound for $\widehat{a}_E(p_1^{e_1})^{r_1} \widehat{a}_E(p_2^{e_2})^{r_2}$, gives $O \left( \left( \frac{1}{p_1} + \frac{1}{p_2} \right) X^\frac{5}{6} \right)$, we verify the trace formula for $r_1 = r_2 = 2$ case. The other three cases can be handled similarly, and we have

$$\sum_{E \in E(X)} \widehat{a}_E(p_1^{e_1})^{r_1} \widehat{a}_E(p_2^{e_2})^{r_2} = (-1)^{r_1+r_2} \frac{4}{\zeta(10)} X^\frac{5}{6} + O \left( \left( \frac{1}{p_1} + \frac{1}{p_2} \right) X^\frac{5}{6} + p_1p_2 X^{\frac{1}{2}} \right).$$

For general $k$ primes, we can prove the trace formula similarly.

For $\lambda_E(p^s)$, we note that $\lambda_E(p) = \widehat{a}_E(p)$ and $\lambda_E(p^2) = \widehat{a}_E(p)^2 - 1$ if $E$ has good reduction at $p$ and $\lambda_E(p^2) = \widehat{a}_E(p)^2$ otherwise. Hence, we can similarly prove the trace formula for $\lambda_E(n)$.

**4 The distribution of analytic ranks of elliptic curves**

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

\[ \sum_{\gamma \in \mathbb{C}} \ \text{where} \ \gamma \]

if analytic rank $r_E$ is odd,

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

otherwise.

In this section, first, we obtain an upper bound on every $n$-th moment of analytic ranks of elliptic curves and get a bound on the proportion of elliptic curves with analytic rank $r_E \geq (1 + C)9n$ for a positive constant $C$ and a positive integer $n$. For this purpose, we compute an $n$-level density with multiplicity. See [10, Part VI].

We choose the following test function for $\sigma_n = \frac{2}{9n}$:

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

Note that $\phi_n(0) = \frac{\sigma_n^2}{4}$ and $\hat{\phi}_n(0) = \frac{\sigma_n}{4}$. We can understand the constant $\frac{2}{9}$ as the limit of our trace formula. Then, easily we can check

\[ \int_{\mathbb{R}} |u\hat{\phi}_n(u)|^2 = \frac{1}{6} \phi_n(0)^2. \quad (4.1) \]

The $n$-level density with multiplicity is

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

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

\[ \frac{1}{|E(X)|} \sum_{E \in E(X)} r^*_n \leq \frac{1}{\phi_n(0)^n} D^*_n(E, \Phi). \quad (4.2) \]

We show that for any $n$, $D^*_n(E, \Phi)$ has a closed expression. By Weil’s explicit formula,

\[ \sum_j \phi_n \left( \gamma_{E,j} \log X \frac{2\pi}{2\pi} \right) = \hat{\phi}_n(0) \log N_E \log X \left( \log X \frac{2\pi}{2\pi} \right) - 2 \sum_{k=1}^{2} \sum_p \hat{a}_E(p^k) \log p \hat{\phi}_n \left( \log p \log X \frac{2\pi}{2\pi} \right) + O \left( \frac{1}{\log X} \right) \]

\[ \leq \hat{\phi}_n(0) - 2 \sum_{k=1}^{2} \sum_p \hat{a}_E(p^k) \log p \hat{\phi}_n \left( \log p \log X \frac{2\pi}{2\pi} \right) + O \left( \frac{1}{\log X} \right), \quad (4.3) \]

where $N_E$ is the conductor of the elliptic curve. By Ogg’s formula (cf. [13, IV §11.1]), the conductor is less than the discriminant. By the height condition, we have

\[ N_E \leq 16(4A^3 + 27B^2) \leq cX \]

for a fixed $c$, which implies that $\log N_E \leq \log X + O(1)$. This justifies the inequality (4.3).

Hence, we have

\[ \frac{1}{|E(X)|} \sum_{E \in E(X)} \sum_{j_1, j_2, \ldots, j_n} \phi_n \left( \gamma_{E,j_1} \log X \frac{2\pi}{2\pi} \right) \phi_n \left( \gamma_{E,j_2} \log X \frac{2\pi}{2\pi} \right) \cdots \phi_n \left( \gamma_{E,j_n} \log X \frac{2\pi}{2\pi} \right) \]

\[ \leq \frac{1}{|E(X)|} \sum_{E \in E(X)} \left( \hat{\phi}_n(0) - \frac{2}{\log X} \sum_{m < X} \frac{\hat{a}_E(m) \log m \hat{\phi}_n \left( \log m \log X \frac{2\pi}{2\pi} \right) + O \left( \frac{1}{\log X} \right)}{\sqrt{m}} \right)^n. \]

Springer
where m’s are primes or squares of primes. By the standard argument such as [12, Lemma 2] or [6, Lemma 4.4], we can take the term $O(1/\log X)$ out of the bracket, and we have

$$D_n^*(E, \Phi) \leq \frac{1}{|E(X)|} \sum_S \hat{\phi}_n(0)^{|S^c|} \left( - \frac{2}{\log X} \right)^{|S|}$$

$$\times \sum_{m_1, m_2, \ldots, m_k} \frac{\Lambda(m_1) \Lambda(m_2) \cdots \Lambda(m_k)}{\sqrt{m_1 m_2 \cdots m_k}} \phi_n \left( \frac{\log m_1}{\log X} \right) \phi_n \left( \frac{\log m_2}{\log X} \right) \cdots \phi_n \left( \frac{\log m_k}{\log X} \right)$$

$$\times \sum_{E \in E(X)} \hat{a}_E(m_1) \hat{a}_E(m_2) \cdots \hat{a}_E(m_k) + O \left( \frac{1}{\log X} \right),$$

where $m_i$’s are primes or squares of primes with $m_i \leq X^{\frac{2}{n}}$ and $S = \{i_1, i_2, \ldots, i_k\}$ runs over every subset of $\{1, 2, 3, \ldots, n\}$. In the next two propositions, we show that only the terms $m_1 m_2 \cdots m_k = \Box$ give the main term, and the contribution of the other terms is $O(1/\log X)$.

**Proposition 4.1**

$$\sum_{E \in E(X)} \sum_{m_1, m_2, \ldots, m_k \neq \Box} \frac{\Lambda(m_1) \cdots \Lambda(m_k) \hat{a}_E(m_1) \cdots \hat{a}_E(m_k)}{\sqrt{m_1 m_2 \cdots m_k}} \phi_n \left( \frac{\log m_1}{\log X} \right) \phi_n \left( \frac{\log m_2}{\log X} \right) \cdots \phi_n \left( \frac{\log m_k}{\log X} \right) \ll |E(X)|.$$

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

$$\hat{a}_E(p_1)^{e_1} \hat{a}_E(p_2)^{e_2} \cdots \hat{a}_E(p_t)^{e_t} \hat{a}_E(q_1^{l_1}) \hat{a}_E(q_2^{l_2}) \cdots \hat{a}_E(q_s^{l_s}),$$

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

Since one of $e_i$’s is odd by our assumption, then by the Frobenius trace formula 3.1,

$$\sum_{E \in E(X)} \hat{a}_E(p_1)^{e_1} \hat{a}_E(p_2)^{e_2} \cdots \hat{a}_E(p_t)^{e_t} \hat{a}_E(q_1^{l_1}) \hat{a}_E(q_2^{l_2}) \cdots \hat{a}_E(q_s^{l_s}) = O(p_1 p_2 \cdots p_t q_1 q_2 \cdots q_s X^{\frac{1}{2}}).$$

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

$$\ll X^{\frac{1}{2}} \left( \sum_{p < X^{\frac{2}{n}}} p^{\frac{1}{2} \log p} \right)^k \ll X^{\frac{1}{2}} (X^{\frac{1}{n}})^n \ll X^5.$$

Now, we assume that some $p_t$ equals some $q_j$. Since $\hat{a}_E(q_j^{l_j}) = (\hat{a}_E(q^l) - 2)$ if $E$ has good reduction at $q$ and $\hat{a}_E(q_j^{l_j}) = \hat{a}_E(q^{l_j})$ otherwise, still we can use the Frobenius trace formula. □
Proposition 4.2 For a subset $S = \{i_1, i_2, \ldots, i_k\}$ of $\{1, 2, \ldots, n\}$,
\[
\frac{1}{|\mathcal{E}(X)|} \left(\frac{-2}{\log X}\right)^{|S|} \sum_{E \in \mathcal{E}(X)} \sum_{m_{i_1}m_{i_2} \ldots m_{i_k} = \square} \left(\prod_{j=1}^{|S|} \frac{\Lambda(m_{i_j})\hat{a}_E(m_{i_j})}{\sqrt{m_{i_j}}} \hat{\phi}_n \left(\frac{\log m_{i_j}}{\log X}\right)\right)
= \sum_{S_2 \subset S, |S_2| \text{ even}} \left(\frac{1}{2} \phi_n(0)\right)^{|S_2|} |S_2|! \left(\int_{\mathbb{R}} |u|\hat{\phi}_n(u)^2 du\right)^{\frac{|S_2|}{2}} + O\left(\frac{1}{\log X}\right).
\]

Proof In this proof, we compute the double sum not considering the term $\frac{1}{|\mathcal{E}(X)|} \left(\frac{-2}{\log X}\right)^k$. We show that every contribution except one is $\ll X^\frac{5}{8} (\log X)^{k-1}$, hence they become the error term $O(1/\log X)$ in the end.

Note that $\hat{a}_E(m_{i_1})\hat{a}_E(m_{i_2}) \cdots \hat{a}_E(m_{i_k})$ is of the form
\[
\hat{a}_E(p_1)^{e_1}\hat{a}_E(p_2)^{e_2} \cdots \hat{a}_E(q_1)^{e_1}\hat{a}_E(q_2)^{e_2} \cdots \hat{a}_E(q_s)^{e_s},
\]
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 $X^\frac{5}{8} (\log X)^{k-1}$. Let $S_2$ be a subset of $S$ with even cardinality $2t$:
\[
S_2 = \{i_{a_1}, i_{a_2}, \ldots, i_{a_{2t-1}}, i_{a_{2t}}\}, \quad |S_2| = \{b_1, b_2, \ldots, b_s\}.
\]
There are $(2t)!/2^t$ ways to pair up two elements in $S_2$. For example, we consider the following pairings.
\[
(i_{a_1}, i_{a_2}), (i_{a_3}, i_{a_4}), (i_{a_5}, i_{a_6}), \ldots, (i_{a_{2t-1}}, i_{a_{2t}}).
\]

This set of pairings corresponds to the following sum
\[
\sum_{E \in \mathcal{E}(X)} \hat{a}_E(p_{i_{a_1}})^{2\hat{a}_E(p_{i_{a_2}})^2} \cdots \hat{a}_E(p_{i_{a_{2t-1}}})^2 \hat{a}_E(q_{i_{b_1}})^2 \hat{a}_E(q_{i_{b_2}})^2 \cdots \hat{a}_E(q_{i_{b_s}})^2
\]
where $2t + s = k$. By the Frobenius trace formula, the above sum is
\[
|\mathcal{E}(X)| \left\{\begin{array}{ll} 1 & \text{if } s \text{ is even}, \\
-1 & \text{if } s \text{ is odd} \end{array}\right.\right. + O\left(\frac{1}{p_1} + \cdots + \frac{1}{p_t} + \frac{1}{q_1} + \cdots + \frac{1}{q_s}\right) X^\frac{5}{8}.
\]

The contribution from the error term $O(p_1 \cdots p_t q_1 \cdots q_s X^\frac{1}{2})$ is dominated by
\[
(X^\frac{5}{8} \log X)^t (X^\frac{1}{2} X^\frac{1}{2}) \ll X^\frac{5}{8} (\log X)^{k-1}.
\]

The contribution from the error term $O\left(\left(\frac{1}{p_1} + \cdots + \frac{1}{p_t} + \frac{1}{q_1} + \cdots + \frac{1}{q_s}\right) X^\frac{5}{8}\right)$ is dominated by $X^\frac{5}{8} (\log X)^{k-1}$. The main term of the sum, after being divided by $|\mathcal{E}(X)|\left(\frac{\log X}{-2}\right)^k$, gives rise to
\[
\prod_{i=1}^t \left(\frac{-2}{\log X}\right)^2 \sum_p \frac{\log^2 p}{p} \hat{\phi}_n \left(\frac{\log p}{\log X}\right)^2 \times \prod_{j=1}^s \left(\frac{2}{\log X} \sum_q \frac{\log q}{q} \hat{\phi}_n \left(\frac{2 \log q}{\log X}\right)\right)
= \left(\frac{1}{2}\right)^s \left(\int_{\mathbb{R}} |u|\hat{\phi}_n(u)^2 du\right)^s \left(\int_{\mathbb{R}} \hat{\phi}_n(u) du\right)^s.
\]
Since there are $(2t)!/2^t$ ways to pair up two elements in $S_2$, the claim follows. □

**Proof of Theorem 1.3** By Propositions 4.1, 4.2, and (4.1) we have the following inequality

$$D_n^* (\mathcal{E}, \Phi) \leq \phi_n (0)^n \sum \left( \frac{1}{\sigma_n} \right)^{|S|} \sum_{S_2 \subset S} \left( \frac{1}{2} \right)^{|S_2|/2 |S_2|!} \left( \frac{1}{6} \right)^{|S_2|/2} + O \left( \frac{1}{\log X} \right).$$

and, by (4.2), Theorem 1.3 follows. □

**Remark** Here is an asymptotic of the upper bound of $n$-th moment. Let $[n] := \{1, \cdots, n\}$, $S_1 := S - S_2$, and $S_3 := [n] - S$. Then $S_3 = S^c$, $S_1 = S^c_3$ in the above notation and the our upper bound is

$$\sum_{S \subset [n]} \left( \frac{9n}{2} \right)^{|S_1|} \sum_{S_2 \subset S} \left( \frac{1}{2} \right)^{|S_2|} |S_2|! \left( \frac{1}{6} \right)^{|S_2|/2} = \sum_{S_1 \cup S_2 \cup S_3 = [n]} \left( \frac{9n}{2} \right)^{|S_1|} \left( \frac{1}{2} \right)^{|S_2|} |S_2|! \left( \frac{1}{6} \right)^{|S_2|}.$$

Hence by taking $|S_2| = 2l$, it is

$$\sum_{l=0}^{[n/2]} \left( \frac{9n}{2} \right)^{2l} \left( \frac{n}{2l} \right) (2l)! \left( \frac{9n + 1}{2} \right)^{n-2l} = \left( \frac{9n + 1}{2} \right)^{n} \sum_{l=0}^{[n/2]} \left( \frac{2}{3(9n+1)^2} \right)^l \times n(n-1) \cdots (n-l+1).$$

It has an upper bound

$$\left( \frac{9n + 1}{2} \right)^{n} \sum_{l=0}^{\infty} \left( \frac{2}{3(9n+1)^2} \right)^l n^l = \left( \frac{9n + 1}{2} \right)^{n} \frac{3(9n+1)^2}{3(9n+1)^2 - 2n^2}.$$

and a lower bound

$$\left( \frac{9n + 1}{2} \right)^{n} \sum_{l=0}^{\infty} \left( \frac{2}{3(9n+1)^2} \right)^l (n - \sqrt{n})^l = \left( \frac{9n + 1}{2} \right)^{n} \frac{3(9n+1)^2}{3(9n+1)^2 - 2(n - \sqrt{n})^2}.$$

Hence, we have an asymptotic bound

$$\frac{243}{241} \left( \frac{9n + 1}{2} \right)^{n} (1 + O(n^{-1/2})).$$

**Proof of Theorem 1.1** We choose the test function $\phi_{2n}(x)$. Then $\hat{\phi}_{2n}(0) = \frac{1}{4} \sigma_{2n}$, and $\phi_{2n}(0) = \frac{1}{4} \sigma_{2n}^2$. By Weil’s explicit formula, we have

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

© Springer
hence
\[ r_E \leq \frac{1}{\sigma_{2n}} + \frac{4}{\sigma_{2n}^2} \left( -\frac{2}{\log X} \sum_{m_i} \frac{\hat{E}(m_i) \Lambda(m_i)}{\sqrt{m_i}} \phi_{2n} \left( \frac{\log m_i}{\log X} \right) \right) + O \left( \frac{1}{\sigma_{2n}^2 \log X} \right). \]

Now assume that \( r_E \geq \frac{1+C}{\sigma_{2n}} \) with some positive constant \( C \). Then, for sufficiently large \( X \),
\[ -\frac{2}{\log X} \sum_{m_i} \frac{\hat{E}(m_i) \Lambda(m_i)}{\sqrt{m_i}} \phi_{2n} \left( \frac{\log m_i}{\log X} \right) \geq \frac{C \sigma_{2n}}{4}. \]

Therefore,
\[ \left| \{ E \in \mathcal{E}(X) \mid r_E \geq \frac{1+C}{\sigma_{2n}} \} \right| \left( \frac{C \sigma_{2n}}{4} \right)^{2n} \leq \sum_{E \in \mathcal{E}(X)} \left( -\frac{2}{\log X} \sum_{m_i} \frac{\hat{E}(m_i) \Lambda(m_i)}{\sqrt{m_i}} \phi_{2n} \left( \frac{\log m_i}{\log X} \right) \right)^{2n} \]
\[ \leq \left( \frac{\sigma_{2n}}{4} \right)^{2n} \sum \left| S_2 \right|^2 \left( \frac{1}{2} \right) \left| S_2 \right|! \left( \frac{1}{6} \right) \left| S_2 \right|^{1/2} \left| \mathcal{E}(X) \right| + O \left( \frac{X^{5/6}}{\log X} \right), \]
where the second inequality is justified by Propositions 4.1, 4.2, and finally we obtain
\[ P \left( r_E \geq (1+C) \cdot 9n \right) \leq \frac{\sum_{k=0}^{n} \left( \frac{2n}{2k} \right) \left( \frac{1}{2} \right)^{2n-2k} (2k)! \left( \frac{1}{6} \right)^k}{(C \cdot 9n)^{2n}}. \]

\[ \Box \]

Acknowledgements We thank to Seok Hyeong Lee for providing the asymptotic of Theorem 1.3.

References
1. Balog, A., Cojocaru, A.-C., David, C.: Average twin prime conjecture for elliptic curves. Am. J. Math. 133(5), 1179–1229 (2011)
2. Bhargava, M., Shankar, A.: Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. Ann. Math. (2) 181(2), 587–621 (2015)
3. Bhargava, M., Shankar, A.: The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1, preprint. arxiv:1312.7859
4. Birch, B.J.: How the number of points of an elliptic curve over a fixed prime field varies. J. Lond. Math. Soc. 43, 57–60 (1968)
5. Brumer, A.: The average rank of elliptic curves I. Invent. Math. 109(3), 445–472 (1992)
6. Cho, P.J., Kim, H.H.: \( n \)-Level densities of Artin \( L \)-functions. Int. Math. Res. Not. IMRN 2015(17), 7861–7883 (2015)
7. Cox, D.A.: Primes of the Form \( x^2 + ny^2 \), Fermat, Class Field Theory, and Complex Multiplication, Pure and Applied Mathematics, 2nd edn. Wiley, Hoboken (2013)
8. Cremona, J.E., Sadek, M.: Local and global densities for Weierstrass models of elliptic curves. Math. Res. Lett. 30(2), 413–461 (2023)
9. Heath-Brown, D.R.: The average analytic rank of elliptic curves. Duke Math. J. 122(3), 591–623 (2004)
10. Miller, S.J.: 1- and 2-level densities for families of elliptic curves: Evidence for the underlying group symmetries. Thesis (Ph.D.)—Princeton University. (2002). 225. ISBN:978-0493-55316-0
11. Park, J., Poonen, B., Voight, J., Wood, M.M.: A heuristic for boundness of ranks of elliptic curves. J. Eur. Math. Soc. 21(9), 2859–2903 (2019)
12. Rubinstein, M.O.: Low-lying zeros of \( L \)-functions and random matrix theory. Duke Math. J. 109(1), 147–181 (2001)
13. Silverman, J.H.: Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, 151. Springer, New York (1994)
14. Watkins, M.: Some heuristics about elliptic curves. Exp. Math. 17(1), 105–125 (2008)
15. Young, M.P.: Low-lying zeros of families of elliptic curves. J. Am. Math. Soc. 19(1), 205–250 (2006)
16. Young, M.P.: Moments of the critical values of families of elliptic curves, with applications. Can. J. Math. 62(5), 1155–1181 (2010)
17. Wong, W.: On the density of elliptic curves. Compos. Math. 127(1), 23–54 (2001)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.