Summary on the average size of p-Selmer groups

Jiahe Shen, (✉) js6157@columbia.edu[1]

[1]Department of Mathematics, Columbia University

December 12, 2023

1 Introduction

Any elliptic curve E over the rational field $\mathbb{Q}$ is isomorphic to a unique curve of the form $E_{A,B} : y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Z}$ and for all primes p, $p^6 \nmid B$ whenever $p^4 \mid A$. Let $H_{A,B}$ denote the (naive) height of $E_{A,B}$, defined by $H(E_{A,B}) = \max\{4|A|^3, 27B^2\}$. Let $\triangle(E_{A,B}) = -4A^3 - 27B^2$ be the discriminant, and

$$C(E_{A,B}) = \prod_p p^{f_p(E)}$$

denote the conductor. Here $f_p(E) = 0, 1, 2$, depending on whether E has good, multiplicative, or additive reduction at p.

The document aims to prove the following statement:

Let $p \leq 5$ be a prime. When elliptic curves in any large family are ordered by height, the average size of the p-Selmer group is $p + 1$.

Here, we need to recall the definition of "large family." For each prime l, let Σ_l be a closed subset of $\{(A, B) \in \mathbb{Z}_l^2 : \triangle(A, B) = -4A^3 - 27B^2 \neq 0\}$ with boundary of measure zero. To such a collection $\Sigma = (\Sigma_l)_l$, we associate the set F_Σ of elliptic curves over $\mathbb{Q}$, where $E_{A,B} \in F_\Sigma$ if and only if $(A, B) \in \Sigma_l$ for all l. We then say that F_Σ is a family of elliptic curves over $\mathbb{Q}$ that is defined by congruence conditions. Furthermore, we can also impose "congruence conditions at infinity", where Σ_∞ consists of all (A, B) with $\triangle(A, B)$ positive, negative, or either.

A family $F = F_\Sigma$ of elliptic curves defined by congruence conditions is said to be large if, for all sufficiently large primes l, the set Σ_l contains all $E_{A,B}$ with $(A, B) \in \mathbb{Z}_l^2$ such that $l^2 \nmid \triangle(A, B)$. In particular, any family of elliptic curves $E_{A,B}$ defined by finitely many congruence conditions over A and B is large, and the set of all elliptic curves over $\mathbb{Q}$ is large (no congruence conditions).

Finally, by the statement above, we can prove a majority (66.48%) of all elliptic curves over $\mathbb{Q}$, when ordered by height, satisfies the BSD rank conjecture.

2 The case $p = 2$

This section is divided into two parts. For the first part, we study the distribution of $GL_2(\mathbb{Z})$-equivalence classes of binary quartic forms $f(x, y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ with respect to their fundamental invariants $I(f) = 12ae - 3bd + c^2$ and $J(f) = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3$; In particular, we prove the following theorem:

①Let $h^{(i)}(I, J)$ denote the number of $GL_2(\mathbb{Z})$-equivalence classes of irreducible binary quadratic forms having $4 - 2i$ real roots in $\mathbb{P}^1$ and invariants equal to I and J. Then:
(a)$\sum_{H(I,J)<X} h^{(0)}(I, J) = \frac{4}{135}\zeta(2)X^{5/6} + O(X^{3/4+\epsilon})$
(b)$\sum_{H(I,J)<X} h^{(1)}(I, J) = \frac{32}{135}\zeta(2)X^{5/6} + O(X^{3/4+\epsilon})$
(c)$\sum_{H(I,J)<X} h^{(2)}(I, J) = \frac{8}{135}\zeta(2)X^{5/6} + O(X^{3/4+\epsilon})$
Here $H(f) = \max\{|I|^3, \frac{J^2}{4}\}$ is the height.

②A pair $(I, J) \times \mathbb{Z} \times \mathbb{Z}$ occurs as the invariants of an integral binary quartic form if and only if it satisfies one of the following congruence conditions:
(a)$I \equiv 0 (\mathrm{mod}\ 3)$ and $J \equiv 0 (\mathrm{mod}\ 27)$
(b)$I \equiv 1 (\mathrm{mod}\ 9)$ and $J \equiv \pm 2 (\mathrm{mod}\ 27)$
(c)$I \equiv 4 (\mathrm{mod}\ 9)$ and $J \equiv \pm 16 (\mathrm{mod}\ 27)$
(d)$I \equiv 7 (\mathrm{mod}\ 9)$ and $J \equiv \pm 7 (\mathrm{mod}\ 27)$
We say the pair (I, J) is eligible if it satisfies the above condition.

③Let $h^{(i)}(I, J)$ denote the number of $GL_2(\mathbb{Z})$-equivalence classes of irreducible binary quadratic forms having $4 - 2i$ real roots in $\mathbb{P}^1$ and invariants equal to I and J. Let $n_0 = 4, n_1 = 2, n_2 = 2$. Then for $i = 0, 1, 2$, we have

$$\lim_{X \to \infty} \frac{\sum_{H(I,J)<X} h^{(i)})(I, J)}{|\{(I, J)\text{eligible} \mid (-1)^i \triangle(I, J) > 0, H(I, J) < X\}|} = \frac{2\zeta(2)}{n_i}$$

Here $\triangle(f) = \frac{4I(f)^3 - J(f)^2}{27}$ is the discriminant.

The second part describes the precise connection between binary quartic forms and elements in the 2-Selmer groups of elliptic curves. This connection allows us, through the use of certain mass formulae for elliptic curves over $\mathbb{Q}_p$, to compute the average size of the 2-Selmer groups of elliptic curves (or of appropriate families of elliptic curves) via a count of binary quartic forms satisfying a certain weighted infinite set of congruence conditions. We then apply the uniformity results of the first part to count these binary quartic forms, thus completing the proof.

2.1 Part I: The number of classes of integral binary quartic forms having bounded invariants

Let $V_{\mathbb{R}}$ denote the vector space of binary quartic forms over the real numbers, $f(x, y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$. We say $f \in V_{\mathbb{Z}}$, or f is integral if $a, b, c, d, e \in \mathbb{Z}$. The group $GL_2(\mathbb{R})$ acts on $V_{\mathbb{R}}$ naturally by

$$\gamma \cdot f(x,y) = f((x,y)\cdot\gamma), \quad \gamma \in GL_2(\mathbb{R}), x, y \in \mathbb{R}, f \in V_{\mathbb{R}}$$

For $i = 0, 1, 2$, let $V_{\mathbb{Z}}^{(i)}$ denote the set of elements in $V_{\mathbb{Z}}$ having nonzero discriminant and i pairs of complex conjugate roots and $4-2i$ real roots. For any $GL_2(\mathbb{Z})$-invariant set $S \subset V_{\mathbb{Z}}$, let $N(S;X)$ denote the number of $GL_2(\mathbb{Z})$-equivalence classes of irreducible elements $f \in S$ satisfying $H(f) < X$. Then, the main theorem of this section is the following restatement:

(a)$N(V_{\mathbb{Z}}^{(0)}; X) = \frac{4}{135}\zeta(2)X^{5/6} + O(X^{3/4+\epsilon})$;
(b)$N(V_{\mathbb{Z}}^{(1)}; X) = \frac{32}{135}\zeta(2)X^{5/6} + O(X^{3/4+\epsilon})$;
(c)$N(V_{\mathbb{Z}}^{(2)}; X) = \frac{8}{135}\zeta(2)X^{5/6} + O(X^{3/4+\epsilon})$.

For $i = 0, 1, 2$, let $V_{\mathbb{R}}^{(i)}$ denote the set of points in $V_{\mathbb{R}}$ having nonzero discriminant and i pairs of complex roots and $4-2i$ real roots. Then $V_{\mathbb{R}}^{(2)}$ is the set of definite forms in $V_{\mathbb{R}}^{(i)}$. Let $V_{\mathbb{R}}^{(2+)}$ and $V_{\mathbb{R}}^{(2-)}$ denote the subset of $V_{\mathbb{R}}^{(2)}$ consisting of the positive and negative definite forms. Let $V_{\mathbb{Z}}^{(i)} = V_{\mathbb{R}}^{(i)} \cap V_{\mathbb{Z}}$ for $i = 0, 1, 2+, 2-$. Then we have the following facts:

(a)The set of binary quartic forms in $V_{\mathbb{R}}$ having fixed invariants I and J consists of just one $SL_2^{\pm}(\mathbb{R})$-orbit if $4I^3 - J^2 < 0$; this orbit lies in $V_{\mathbb{R}}^{(1)}$.

(b)The set of binary quartic forms in $V_{\mathbb{R}}$ having fixed invariants I and J consists of three $SL_2^{\pm}(\mathbb{R})$-orbit if $4I^3 - J^2 > 0$; In this case, there is one orbit from each of $V_{\mathbb{R}}^{(0)}$, $V_{\mathbb{R}}^{(2+)}$, and $V_{\mathbb{R}}^{(2-)}$.

Then we have the following lemma: Let f be an element in $V_{\mathbb{R}}^{(i)}$ having nonzero discriminant. Then the order of the stabilizer of f in $GL_2(\mathbb{R})$, denoted as $2n_i$ (note that we have changed the meaning of symbol n_i here), is 8 if $i = 0, 2$, and 4 if $i = 1$.

Let $\mathcal{F}$ denote a fundamental domain for the action of $GL_2(\mathbb{Z})$ on $GL_2(\mathbb{R})$ by left multiplication. We also assume that $\mathcal{F} \subset GL_2(\mathbb{R})$ is semi-algebraic and connected and that it is contained in a standard Siegel set, i.e., $\mathcal{F} \subset N'A'K\Lambda$. (See the paper for the definition of the sets K, A', N', Λ.) In the same way as before in the proof of density of discriminates of quartic/quintic field, we may write

$$N(V_{\mathbb{Z}}^{(i)}; X) = \frac{\int_{h \in G_0} \#\{x \in \mathcal{F}h \cdot L \cap V_{\mathbb{Z}}^{\text{irr.}} : H(x) < X\} dh}{n_i \cdot \int_{h \in G_0} dh}$$

Where $V_{\mathbb{Z}}^{\text{irr.}}$ denotes the set of irreducible elements in $V_{\mathbb{Z}}$, $L = L^{(i)}$ is the fundamental set for the action of $GL_2(\mathbb{R})$ over $V_{\mathbb{R}}^{(i)}$, dh denotes the Haar measure. And G_0 is a compact, semialgebraic, left K-invariant set in $GL_2(\mathbb{R})$ that is the closure of a nonempty open set and in which every element has determinant greater than or equal to 1.

Now, let us consider the integral elements in the multiset $\mathcal{R}_X(h \cdot L^{(i)}) = \{w \in \mathcal{F}h \cdot L^{(i)} : |H(w)| < X\}$. Then, we could show that the number of integral binary quartic forms in $\mathcal{R}_X(h \cdot L^{(i)})$ that are reducible over $\mathbb{Q}$ with $a \neq 0$ is $O(X^{2/3+\epsilon})$, and the number of $GL_2(\mathbb{Z})$-orbits of integral binary quartic forms $f \in V_{\mathbb{Z}}$ such that $\triangle(f) \neq 0$ and $H(f) < X$ whose stabilizer in $GL_2(\mathbb{Q})$ has size greater than 2 is $O(X^{3/4+\epsilon})$. To sum up, we have

$$N(V_{\mathbb{Z}}^{(i)}; X) = \text{Vol}(\mathcal{R}_X(L)/n_i + O(X^{3/4+\epsilon})$$

Finally, by calculus computation, we could show

$$\mathrm{Vol}(\mathcal{R}_X(L^{(i)})) = \begin{cases} \frac{16}{135}\zeta(2)X^{5/6} & i = 0, 2+, 2- \\ \frac{64}{135}\zeta(2)X^{5/6} & i = 1 \end{cases}$$

Which ends our proof.

Finally, at the end of this subsection, we prove a stronger version of the conclusion that involves congruence conditions. First, suppose S is a subset of $V_{\mathbb{Z}}$ defined by congruence conditions modulo finitely many prime powers. Then we have

$$N(S \cap V_{\mathbb{Z}}^{(i)}; X) = N(S \cap V_{\mathbb{Z}}^{(i)}; X) \prod_p \mu_p(S) + O(X^{3/4+\epsilon})$$

where $\mu_p(S)$ denotes the p-adic density of S in $V_{\mathbb{Z}}$ and where the implied constant depends only on S and ϵ. Here $N(S; X)$ denote the number of irreducible $GL_2(\mathbb{Z})$-orbits in S having height less than X.

There is a generalized version of the above theorem. Let $p_1, ..., p_k$ be distinct prime numbers. For $j = 1, ..., k$, let $\phi_{p_j} : V_{\mathbb{Z}} \to \mathbb{R}$ be a $GL_2(\mathbb{Z})$-invariant function on $V_{\mathbb{Z}}$ such that $\phi_{p_j}(f)$ depends only on the congruence class of f modulo some power of p_j. Let $N_\phi(V_{\mathbb{Z}}^{(i)}; X)$ denote the number of the irreducible $GL_2(\mathbb{Z})$-orbits in $V_{\mathbb{Z}}^{(i)}$ having invariants bounded by X, where each orbit $GL_2(\mathbb{Z}) \cdot f$ is counted with weight $\phi(f) = \prod_{j=1}^k \phi_{p_j}(f)$. Then we have

$$N_\phi(V_{\mathbb{Z}}^{(i)}; X) = N(V_{\mathbb{Z}}^{(i)}; X) \prod_{j=1}^{k} \int_{f \in V_{\mathbb{Z}_{p_j}}} \tilde{\phi}_{p_j}(f) df + O(X^{3/4+\epsilon})$$

where $\tilde{\phi}_{p_j}$ is the natural extension of ϕ_{p_j} to $V_{\mathbb{Z}_{p_j}}$, df denotes the additive measure on $V_{\mathbb{Z}_{p_j}}$ normalized so that $\int_{f \in V_{\mathbb{Z}_{p_j}}} df = 1$, and where the implied constant in the error term depends only on the local weight functions ϕ_{p_j} and ϵ.

2.2 Part II: The average size of the 2-Selmer groups of elliptic curves

Recall that every elliptic form over $\mathbb{Q}$ can be written in the form

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

where $A, B \in \mathbb{Z}$ and $p^4 \nmid A$ if $p^6 \mid B$. Let $I(E) = -3A$ and $J(E) = -27B$, and also denote the curve $E = E_{A,B}$ by $E^{I,J}$. The height of this curve is defined by

$$H(E_{A,B}) = \max\{4|A|^3, 27B^2\} = \frac{4}{27} \max\{I(E)^3, J(E)^2/4\}$$

A slightly different height $H'(E)$ is defined by

$$H'(E) = H(I(E), J(E)) = \max\{|I(E)|^3, |J(E)|^2/4\}$$

We say that a binary quartic form over a field K is K-soluble if the equation $z^2 = f(x, y)$ has a nonzero solution with $x, y, z \in K$. Next, a binary quartic form $f \in V_{\mathbb{Q}}$ is called locally soluble if it is $\mathbb{R}$-soluble and $\mathbb{Q}_p$ for all primes p. Then we have the following theorem, which turns the 2-Selmer group into a form that is more convenient for us to handle:

Let $E = E^{I,J}$ be an elliptic curve over $\mathbb{Q}$. Then the elements of the 2-Selmer group of E are in one-to-one correspondence with $PGL_2(\mathbb{Q})$-equivalence classes of locally soluble integral binary quartic form having invariants equal to $2^4 I$ and $2^6 J$.

Furthermore, the set of integral binary quartic forms that have rational linear functions and invariants equal to $2^4 I$ and $2^6 J$ lie in one $PGL_2(\mathbb{Q})$-equivalence class and this class corresponds to the identity element in the 2-Selmer group of E.

Therefore, to compute the number of $PGL_2(\mathbb{Q})$-equivalence classes of locally soluble integral binary quartic forms with bounded height and no rational linear factor, we need to count each $PGL_2(\mathbb{Z})$-orbit, $PGL_2(\mathbb{Z}) \cdot f$, weighted by $1/n(f)$, where $n(f)$ is equal to the number of $PGL_2(\mathbb{Z})$-orbits inside the number of $PGL_2(\mathbb{Q})$-equivalence class of f in $V_{\mathbb{Z}}$. Since only negligible many cases make a difference, there is no loss for us to change the weight from $1/n(f)$ to $1/m(f)$, where

$$m(f) = \sum_{f' \in B(f)} \frac{\#\mathrm{Aut}_{\mathbb{Q}}(f')}{\#\mathrm{Aut}_{\mathbb{Z}}(f')} = \sum_{f' \in B(f)} \frac{\#\mathrm{Aut}_{\mathbb{Q}}(f)}{\#\mathrm{Aut}_{\mathbb{Z}}(f')}$$

Here $B(f)$ denotes a set of representatives for the action of $PGL_2(\mathbb{Z})$ on the $PGL_2(\mathbb{Q})$-equivalence class of f in $V_{\mathbb{Z}}$, and $\mathrm{Aut}_{\mathbb{Q}}(f)$ (resp.$\mathrm{Aut}_{\mathbb{Z}}(f)$) denotes the stabilizer of f in $PGL_2(\mathbb{Q})$ (resp.$PGL_2(\mathbb{Z})$).

And there is also the local version:

$$m_p(f) = \sum_{f' \in B_p(f)} \frac{\#\mathrm{Aut}_{\mathbb{Q}_p}(f')}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f')} = \sum_{f' \in B_p(f)} \frac{\#\mathrm{Aut}_{\mathbb{Q}_p}(f)}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f')}$$

with the following proposition: Suppose $f \in V_{\mathbb{Z}}$ has nonzero discriminant. Then $m(f) = \prod_p m_p(f)$.

Now, let F be a large family of elliptic curves. By the theorem at the end of the last subsection, we have

$$\sum_{E \in F, H'(E) < X} (\#S_2(E) - 1) = N(V_{\mathbb{Z}} \cap S_\infty(F); 2^{12}X) \prod_p \int_{S_p(F)} \frac{1}{m_p(f)} df + o(X^{5/6})$$

Where $N(V_{\mathbb{Z}} \cap S_\infty(F); 2^{12}X)$ is equal to $\frac{2^{10}}{27}\mathrm{Vol}(PGL_2(\mathbb{Z})\backslash PGL_2(\mathbb{R}))M_\infty(V, F; X)$, and $\int_{S_p(F)} \frac{1}{m_p(f)} df$ is equal to $\left|\frac{2^{10}}{27}\right|_p \mathrm{Vol}(PGL_2(\mathbb{Z}_p))M_p(V; F) + o(X^{5/6})$.(Here, M_p and M_∞ denote the "local mass"; see the paper.) This implies that $\sum_{E \in F, H'(E) < X}(\#S_2(E) - 1) = \mathrm{Vol}(PGL_2(\mathbb{Z})\backslash PGL_2(\mathbb{R}))M_\infty(V, F; X) \times \prod_p \mathrm{Vol}(PGL_2(\mathbb{Z}_p))M_p(V; F) + o(X^{5/6})$. On the other hand, we have

$$\sum_{E \in F, H'(E) < X} 1 = M_\infty(F; X) \prod_p M_p(F) + o(X^{5/6})$$

Which indicates that

$$\lim_{X\to\infty}\frac{\Sigma_{E\in F,H'(E)<X}(\#S_2(E)-1)}{\Sigma_{E\in F,H'(E)<X}1}=\mathrm{Vol}(PGL_2(\mathbb{Z})\backslash PGL_2(\mathbb{R}))\frac{M_\infty(V,F;X)}{M_\infty(F;X)}\prod_p(\mathrm{Vol}(PGL_2(\mathbb{Z}_p))\frac{M_p(V,F)}{M_p(F)})$$

Notice that $\frac{M_\infty(V,F;X)}{M_\infty(F;X)}=\frac{1}{2}$, and $\frac{M_p(V,F)}{M_p(F)}=1$ except for $p=2$, where the fraction equals 2. Therefore,

$$\lim_{X\to\infty}\frac{\Sigma_{E\in F,H'(E)<X}(\#S_2(E)-1)}{\Sigma_{E\in F,H'(E)<X}1}=\mathrm{Vol}(PGL_2(\mathbb{Z})\backslash PGL_2(\mathbb{R}))\prod_p\mathrm{Vol}(PGL_2(\mathbb{Z}_p))$$

$$=2\zeta(2)\prod_p(1-p^{-2})=2$$

Which ends our proof.

3 The case $p = 3$

The techniques for the case $p = 3$ are similar to the case $p = 2$. Due to the time limit, I only list some crucial steps here.

The proof could also be divided into two parts. For the first part, we study the distribution of $SL_3(\mathbb{Z})$-equivalence classes of strongly irreducible integral ternary cubic forms $f = f(x, y, z)$ with respect to their fundamental invariants $I(f)$ and $J(f)$, which comes from the Hessian matrix

$$\mathcal{H}(f(x,y,z)) = \begin{vmatrix} f_{xx} & f_{xy} & f_{xz} \\ f_{yx} & f_{yy} & f_{yz} \\ f_{zx} & f_{zy} & f_{zz} \end{vmatrix}$$

with the relation $\mathcal{H}(\mathcal{H}(f)) = 12288I(f)^2 \cdot f + 512J(f) \cdot \mathcal{H}(f)$. Here $I(f)$ has degree 4, and $J(f)$ has degree 6. (We say an integral ternary cubic form f is strongly irreducible if f is irreducible, and the common zero set of f and its Hessian $\mathcal{H}(f)$ in $\mathcal{P}^2$ contains no rational points.) In particular, we prove the following theorem:

①Let $h(I, J)$ denote the number of $SL_3(\mathbb{Z})$-equivalence classes of strongly irreducible integral ternary cubic forms having invariants equal to I and J. Then:

(a)$\sum_{\triangle(I,J)>0, H(I,J)<X} h(I, J) = \frac{32}{45}\zeta(2)\zeta(3)X^{5/6} + o(X^{5/6})$

(b)$\sum_{\triangle(I,J)<0, H(I,J)<X} h(I, J) = \frac{128}{45}\zeta(2)\zeta(3)X^{5/6} + o(X^{5/6})$

Here $H(f) = \max\{|I|^3, \frac{J^2}{4}\}$ is the height, and $\triangle(f) = (4I(f)^3 - J(f)^2)/27$ is the discriminant.

②A pair (I, J) occurs as the pair of invariants of an integral ternary cubic form if and only if $(I, J) \in \frac{1}{16}\mathbb{Z} \times \frac{1}{32}\mathbb{Z}$, and the pair $(16I, 32J)$ satisfies congruence conditions modulo 64 (see the paper.)

③Let $h(I, J)$ denote the number of $SL_3(\mathbb{Z})$-equivalence classes of strongly irreducible integral ternary cubic forms having invariants equal to I and J. Then

$$\lim_{X\to\infty} \frac{\sum_{\triangle(I,J)>0, H(I,J)<X} h(I, J)}{\sum_{\triangle(I,J)>0, H(I,J)<X} 1} = \frac{\sum_{\triangle(I,J)<0, H(I,J)<X} h(I, J)}{\sum_{\triangle(I,J)<0, H(I,J)<X} 1} = 3\zeta(2)\zeta(3)$$

In the second part, we describe the precise correspondence between ternary cubic forms and elements of the 3-Selmer groups of elliptic curves. In particular, let $E/\mathbb{Q}$ be an elliptic curve. Then, the elements in the 3-Selmer group of E are in bijective correspondence with $PGL_3(\mathbb{Q})$-orbits on the set of locally soluble ternary cubic forms in $V_\mathbb{Z}$ having invariants equal to $I(E)$ and $J(E)$. Furthermore, the set of all ternary cubic forms in $V_\mathbb{Z}$ having invariants equal to $I(E)$ and $J(E)$ that are not strongly irreducible lie in a single $PGL_3(\mathbb{Q})$-orbit and this orbit corresponds to the identity element in the 3-Selmer group of E. We then apply this correspondence, together with the counting results of the first part and the local mass formulae, which ends our proof:

$$\lim_{X\to\infty} \frac{\Sigma_{E\in F, H'(E)<X}(\#S_3(E) - 1)}{\Sigma_{E\in F, H'(E)<X} 1} = \mathrm{Vol}(PGL_3(\mathbb{Z})\backslash PGL_3(\mathbb{R})) \prod_p \mathrm{Vol}(PGL_3(\mathbb{Z}_p))$$

$$= 3\zeta(2)\zeta(3) \prod_p ((1 - p^{-2})(1 - p^{-3})) = 3$$

4 The case $p = 5$

The techniques for the case $p = 5$ are similar to the case $p = 2$. Due to the time limit, I only list some crucial steps here.

The proof could also be divided into two parts. For the first part, consider the space $V_{\mathbb{R}} = \mathbb{R}^5 \otimes \wedge^2 \mathbb{R}^5$ consisting of quintuples (A, B, C, D, E) of skew-symmetric 5×5 real matrices. For any ring R, we also define V_R such that the entries are elements in R. The ring $GL_5(R) \times GL_5(R)$ acts on V_R as

$$(g_1, g_2) \cdot (A, B, C, D, E) = (g_1 A g_1^t, g_1 B g_1^t, g_1 C g_1^t, g_1 D g_1^t, g_1 E g_1^t) \cdot g_2^t$$

Define the determinant of (g_1, g_2) as $\det(g_1, g_2) = \det(g_1^2 g_2)$. Now let us consider the group

$$G_R = \{(g_1, g_2) \in GL_5(R) \times GL_5(R) : \det(g_1, g_2) = 1 \mid \det(g_1, g_2) = 1\}/\{(\lambda I_5, \lambda^{-2} I_5)\}$$

It is clear that the action of $GL_5(R) \times GL_5(R)$ over v_R descends to an action of G_R.

The ring of invariants for the action of $G_{\mathbb{C}}$ over $v_{\mathbb{C}}$ is freely generated by two elements I and J having degree 20 and 30, respectively. Define the discriminant of an element $v \in V_{\mathbb{R}}$ as $\triangle(v) = \triangle(I, J) = (4I^3 - J^2)/27$, which has degree 60; Define the height as $H(v) = H(I, J) = \max\{|I|^3, \frac{J^2}{4}\}$.

Define $V_{\mathbb{Z}}^+$ and $V_{\mathbb{Z}}^-$ having positive and negative discriminant. For any $G_{\mathbb{Z}}$ invariant set $S \subset V_{\mathbb{Z}}$, let $N(S; X)$ denote the number of $G_{\mathbb{Z}}$-orbits on strongly irreducible elements in S having height less than X. Then we have the following theorem:

There exists a nonzero rational constant $\mathcal{J}$ such that

$$N(V_{\mathbb{Z}}^{\pm}; X) = |\mathcal{J}| \cdot \mathrm{Vol}(G_{\mathbb{Z}}/G_{\mathbb{R}}) \cdot N^{\pm}(X) + o(X^{5/6})$$

Here $N^{\pm}(X)$ is the number of pairs $(I, J) \in \mathbb{Z} \times \mathbb{Z}$ having height less than X and positive/negative discriminant. In fact, we have $N^+(X) = \frac{8}{5} X^{5/6} + O(X^{1/2})$ and $N^-(X) = \frac{32}{5} X^{5/6} + O(X^{1/2})$.

In the second part, we describe the precise correspondence between ternary cubic forms and elements of the 5-Selmer groups of elliptic curves. In particular, let $E/\mathbb{Q}$ be an elliptic curve. Then, the elements in the 5-Selmer group of E are in bijective correspondence with $G_{\mathbb{Q}}$-orbits on the set of locally soluble ternary cubic forms in $V_{\mathbb{Z}}$ having invariants equal to $I(E)$ and $J(E)$. Furthermore, the elements in $V_{\mathbb{Z}}$ having invariants equal to $I(E)$ and $J(E)$ that are not strongly irreducible lie in a single $PGL_3(\mathbb{Q})$-orbit and this orbit corresponds to the identity element in the 5-Selmer group of E. We then apply this correspondence, together with the counting results of the first part and the local mass formulae:

$$\lim_{X \to \infty} \frac{\Sigma_{E \in F, H'(E) < X} (\# S_5(E) - 1)}{\Sigma_{E \in F, H'(E) < X} 1} = \mathrm{Vol}(G_{\mathbb{Z}} \backslash G_{\mathbb{R}}) \prod_p \mathrm{Vol}(G_{\mathbb{Z}_p})$$

This equals the Tamagawa number $\tau(G) = 5$ and ends our proof.

5 Applications in the BSD rank conjecture

In this section, we will prove that a majority (66.48%) of all elliptic curves over $\mathbb{Q}$, when ordered by height, satisfies the BSD conjecture, as stated before in Section 1. As a corollary, a majority of all elliptic curves over $\mathbb{Q}$ have finite Tate-Shafarevich group.

First, we list two criteria that could determine that a given elliptic curve satisfies the BSD rank conjecture:

①Let p be an odd prime. Let E be an elliptic curve over $\mathbb{Q}$ with conductor N such that:
(a)E has good or multiplicative reduction at p;
(b)$E[p]$ is an irreducible $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-module;
(c)there is at least one prime $l \neq p$ such that $l \mid\mid N$ and $E[p]$ is ramified at l;
(d)The p-Selmer group $S_p(E)$ of E is trivial.
Then, the algebraic and analytic ranks of E are both equal to 0.

②Let $p \geq 5$ be a prime. Let E be an elliptic curve with conductor N such that
(a)E has good or multiplicative reduction at p;
(b)$E[p]$ is an irreducible $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-module;
(c)For all primes $l \mid\mid N$ such that $l \equiv \pm 1 (\mathrm{mod}\ p)$, $E[p]$ is ramified at l;
(d)If N is not squarefree, then there exists at least two prime factors $l \mid\mid N$ with $l \neq p$ and where $E[p]$ is ramified;
(e)If f has multiplicative reduction at p then $E[p]$ is not finite at p, and if E has split multiplication reduction at p then p-adic Mazur-Tate-Teitelbaum $\mathfrak{L}$-invariant $\mathfrak{L}(E)$ of E satisfies $\mathrm{ord}_p(\mathfrak{L}(E)) = 1$;
(f)the p-Selmer group $S_p(E)$ has order p.
Then, the algebraic and analytic ranks of E are both equal to 1.

It is worth mentioning that, when ordered by height, 100% of the elliptic curves over $\mathbb{Q}$ satisfies (b)(c) of Theorem 5 and (b)(d) of Theorem 9.

For any prime $p \geq 5$, let $S_0(p)$ be the set of elliptic curve $E_{A,B} : y^2 = x^3 + Ax + B$ over $\mathbb{Q}$ such that:

•$E_{A,B}$ has good ordinary or multiplicative reduction at p;

Let $S_1'(p)$ be the subset of curves $E_{A,B} \in S_0(p)$ also satisfying:

•If $E_{A,B}$ has multiplicative reduction at p, then $p \nmid$, then $p \nmid \mathrm{ord}_p(\triangle(A, B))$,
•If $E_{A,B}$ has split multiplicative reduction at p, then $\mathrm{ord}_p(\mathfrak{L}(E_{A,B})) = 1$;

and Let $S_1(p)$ be the subset of curves $E_{A,B} \in S_1'(p)$ also satisfying:

•$p \nmid \mathrm{ord}_l(\triangle(A, B))$ for all primes $l \equiv \pm 1$ (mod p) such that $\mathrm{ord}_l(\triangle(A, B)) > 0$.

$S_0(p) \supset S_1'(p) \supset S_1(p)$ are all large families. We could compute the densities of $S_0(5), S_1'(5), S_1(5)$ as

$$\mu(S_0(5)) = \frac{4 \cdot 5^{10}}{5(5^{10}-1)} > 0.8, \mu(S_1'(5)) = 0.7918054..., \mu(S_1(5)) > 0.7917957$$

In particular, we have $\mu(S_1'(5)) - \mu(S_1(5)) < 0.00001$.

Now let us state a theorem by Dokchitser–Dokchitser: Let E be an elliptic curve and let p be a prime. Let $s_p(E)$ and $t_p(E)$ denote the rank of the p-Selmer group of E and the rank of $E(\mathbb{Q})[p]$, respectively. Then $s_p(E) - t_p(E)$ is even if and only if the root number of E is ± 1. Also, another theorem says that: Let F be any large family of elliptic curves over $\mathbb{Q}$ defined by congruence conditions modulo powers of primes p such that $p \equiv 1 \pmod 4$. Then, there exists a finite union F' of large subfamilies of F such that when ordered by height, all elliptic curves in F and F' are equidistributed, and F' contains a density of greater than 55.01% of the elliptic curves in F.

Now, we could begin to prove the theorem that when ordered by height, at least 66.48% of elliptic curves over $\mathbb{Q}$ have algebraic and analytic rank 0 and 1. By the theorem above, we can find a finite union F' of large subfamilies in $S_1(5)$ of density $\kappa\mu(S_1'(5))$ with $\kappa \geq 0.5501$ such that for all $E \in F'$, the root number of E and its -1-twist have opposite signs. Let $F = F' \cap S_1(5)$. We could show that at least $7/8$ of the curves in F have an algebraic and analytic rank equal to 0 or 1, which consists of a proportion

$$\frac{7}{8}\mu(F) \geq \frac{7}{8}(\kappa\mu(S_1'(5)) - 0.00001)$$

Next, we consider the set F'' of curves in $S_1(5)$ which the above arguments have not been applied. We could show that this part at least consists of a proportion

$$\frac{19}{24}(\mu(S_1(5)) - \mu(F)) \geq \frac{19}{24}((1-\kappa)\mu(S_1'(5)) - 0.00001)$$

of elliptic curves having algebraic and analytic rank 0 or 1. Finally, for the set of elliptic curves in $S_0(5)$ on which the above arguments have not been applied, which has density at least $0.8 - 0.79179 = 0.00820...$, we could find an additional set of curves of density at least $3/8 \times \kappa \times 0.00820 = 0.00169...$ that have algebraic and analytic rank 0. To sum up all the three cases we list above, a proportion of at least

$$(\frac{7}{8}\kappa + \frac{19}{24}(1-\kappa)) \times \mu(S_1'(5)) - (\frac{7}{8} + \frac{19}{24}) \times 0.00001 + 0.00169...$$

of elliptic curves have algebraic and analytic rank 0 or 1. Since $\kappa \geq 0.5501$, this proportion is at least 0.6648..., and therefore we are done.

See the illustration below. We neglect the difference between $S_1'(5)$ and $S_1(5)$ since $\mu(S_1'(5)) - \mu(S_1(5)) < 0.00001$ is quite small amount.