REVIEW: A HEUISTIC FOR BOUNDEDNESS OF RANKS OF ELLIPTIC CURVES

SOOBIN CHO

1. Introduction and History

It is well known that the set $E(\mathbb{Q})$ of rational points of an elliptic curve E over $\mathbb{Q}$ has the structure of an abelian group. In 1922, Mordell proved that $\mathrm{rk}\ E(\mathbb{Q}) < \infty$. Then, it is natural to ask the question of boundedness:

Conjecture 1.1. Does there exists a constant $B > 0$ such that for every elliptic curve E over $\mathbb{Q}$, one has $\mathrm{rk}\ E(\mathbb{Q}) \leq B$?

In the article, the authors presented a probabilistic model providing a heuristic for the arithmetic of elliptic curves and proved theorems about the model that suggest $\mathrm{rk}\ E(\mathbb{Q}) \leq 21$ for all but finitely many elliptic curves E. This model can be summarized as follows. Fix an increasing function $X(H)$. Then, also fix an increasing function $\eta(H)$ which grow sufficiently slowly and satisfies $X(H)^{\eta(H)} = H^{1/12+o(1)}$ as $H \to \infty$. Then, model an elliptic curve E of height H as follows.

(Step 1) Choose n from the pair $\{\lceil \eta(H) \rceil, \lceil \eta(H) \rceil + 1\}$ uniformly at random.
(Step 2) Choose $A_E \in M_n(\mathbb{Z})_{\mathrm{alt}}$ with entries bounded by $X(H)$ in absolute value, uniformly at random.
Then $(\mathrm{coker}\ A_E)_{\mathrm{tors}}$ models $Ш(E)$, the Shafarevich-Tate group of E, and $\mathrm{rk}\ (\ker A_E)$ models $\mathrm{rk}\ E(\mathbb{Q})$.

Thus, heuristically, for an elliptic curve E of height H, we have that by Theorem 7.2.1,

$$\mathbb{P}(\mathrm{rk}\ E(\mathbb{Q}) \geq r) = \mathbb{P}(\mathrm{rk}\ (\ker A_E) \geq r) = H^{-(r-1)/24+o(1)} \qquad \text{as } H \to \infty.$$

Since the number of elliptic curves of height H is known as $O(H^{5/6})$, this heuristic suggests that there are only finitely many E over $\mathbb{Q}$ with $\mathrm{rk}\ E(\mathbb{Q}) > 21$ which gives a big clue for the answer of Conjecture **1**. Moreover, it also lead to the prediction that for each fixed $1 \leq r \leq 20$, the number of E of height up to H satisfying $\mathrm{rk}\ E(\mathbb{Q}) \geq r$ is approximately $H^{(21-r)/24+o(1)}$ as $H \to \infty$.

1.1. Brief history of boundedness guesses.

Many authors have proposed guesses as to whether Conjecture 1 is true, and their thoughts have shifted from positive to negative over time. In 1960, Honda conjectured that even for any abelian variety A over $\mathbb{Q}$, there is a constant c_A such that $\mathrm{rk}\ A(K) \leq c_A[K : \mathbb{Q}]$ for every number field K not only when $K = \mathbb{Q}$. However, from the mid-1960s to the present, it seems that the common belief is that ranks are unbounded. Here are two possible reasons for this opinion shift towards unboundedness:

1. Tate and Shafarevich (1967) and Ulmer (2002) constructed families of elliptic curves over $\mathbb{F}_p(t)$ (not a number field) in which the rank is unbounded.

2. The lower bound for the maximum rank of an elliptic curve over $\mathbb{Q}$ has been increasing. The current record is held by Elkies (2006), who found an elliptic curve E over $\mathbb{Q}$ of rank ≥ 28, and an infinite family of elliptic curves over $\mathbb{Q}$ of rank ≥ 19.

Some authors have even proposed a rate at which rank grow relative to the conductor N:

- Ulmer (2002),

$$\limsup_{N\to\infty} \frac{\text{rk } E(\mathbb{Q})}{\log N/\log\log N} > 0?$$

- Farmer, Gonek and Hughes (2007),

$$\limsup_{N\to\infty} \frac{\text{rk } E(\mathbb{Q})}{\sqrt{\log N \log\log N}} = 1?$$

1.2. **Conjectures for rank 2 asymptotics.**

We first recall some basic notions in the theory of elliptic curves.

Definition 1.1. (1) (Quadratic twist) First assume that $char(K) \neq 2$. Let E be an alliptic curve over K of the form:

$$y^2 = x^3 + a_2x^2 + a_4x + a_6.$$

Given $d \in K \setminus K^2$, the quadratic twist of E is the curve E_d, defined by the equation:

$$dy^2 = x^3 + a_2x^2 + a_4x + a_6.$$

Observe that $E_d(x, y) = 0$ if and only if $E(x, y\sqrt{d}) = 0$. Hence, the two elliptic curves E and E_d are isomorphic over the field extension $K(\sqrt{d}) \cong K[X]/(X^2 - d)$.

Now assume that $char(K) = 2$. Let E be an elliptic curve over K of the form:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Given $d \in K \setminus \{0\}$, the quadratic twist of E is the curve E_d, defined by the equation:

$$y^2 + a_1xy + a_3y = x^3 + (a_2 + da_1^2)x^2 + a_4x + a_6 + da_3^2.$$

In this case, we can check that $E_d(x, y) = 0$ if and only if $E(x, y + (a_1x + a_3)\zeta) = 0$ where ζ is any of the solutions of the equation $X^2 + X + d = 0$ in fixed algebraic closure of K. Hence, the two elliptic curves E and E_d are isomorphic over the field extention $K[X]/(X^2 + X + d)$.

(2) (Fundamental discriminant) $D \in \mathbb{Z}$ is a fundamental discriminant if and only if one of the following statements holds:

- $D \equiv 1 \pmod 4$ and is square-free;
- $D = 4m$, where $m \equiv 2$ or $3 \pmod 4$ and m is square-free.

There exists a one-to-one correspondence between the set of fundamental discriminants with the union of set of quadratic fields and $\mathbb{Q}$, that is, each nontrivial fundamental discriminant is the discriminant of a unique (up to isomorphism) quadratic number field.

(3) ((naive) Height) An elliptic curve E over $\mathbb{Q}$ is isomorphic to the projective closure of a curve $y^2 = x^3 + Ax + B$ for a unique pair of integers (A, B) such that there is no prime p such that $p^4|A$ and $p^6|B$. Define the (naive) height of E by

$$\text{ht } E := \max\{|4A^3|, |27B^2|\}.$$

(4) (Conductor for the simplified form) Let an elliptic curve E over $\mathbb{Q}$ has a Weierstrass equation in the simplified form $y^2 = x^3 + Ax + B$. Let p be a prime in $\mathbb{Z}$. By reducing each of the coefficients A and B modulo p, we obtain the equation of a cubic curve $\widehat{E}$ over the finite field $\mathbb{F}_p$. If $\widehat{E}$ is a non-singular curve, then we say that E has good reduction at p. Else if $\widehat{E}$ has a cusp (i.e. the discriminant of $\widehat{E}$ equals to 0 and $A = 0 \pmod p$), then we say that E has additive reduction at p. Otherwise, if $\widehat{E}$ has a node, (i.e. the discriminant of $\widehat{E}$ equals to 0 and $A \neq 0 \pmod p$), then we say that E has multiplicative reduction at p.

For each prime $p \in \mathbb{Z}$, define the quantity f_p as follows:

$$f_p = \begin{cases} 0, & \text{if } E \text{ has good reduction at } p, \\ 1, & \text{if } E \text{ has multiplicative reduction at } p, \\ 2, & \text{if } E \text{ has additive reduction at } p, \text{ and } p \neq 2, 3, \\ 2 + \delta_p, & \text{if } E \text{ has additive reduction at } p, \text{ and } p \in \{2, 3\}. \end{cases}$$

Then, the conductor $N_{E/\mathbb{Q}}$ of an elliptic curve E over $\mathbb{Q}$ is defined as

$$N_{E/\mathbb{Q}} := \prod_{p\text{: prime}} p^{f_p}.$$

Example 1.2. Let E be an alliptic curve over $\mathbb{Q}$ of the form $y^2 = x^3 + Ax + B$ for some constants A and B such that $4A^3 + 27B^2 \neq 0$. Then, for each $d \in \mathbb{Q} \setminus \mathbb{Q}^2$, the quadratic twist of E_d is defined by the equation $dy^2 = x^3 + Ax + B$. We can check that this is equivalent to the equation $y^2 = x^3 + d^2Ax + d^3B$. Hence, we obtain ht $E_d = \max\{|4d^6A^3|, |27d^6B^2|\} \asymp d^6$ for general elliptic curve E over $\mathbb{Q}$.

Fix an elliptic curve E over $\mathbb{Q}$. Let d range over fundamental discriminants in $\mathbb{Z}$. Given $r \in Z_{\geq 0}$ and $D > 0$, define

$$\begin{aligned} N_{\geq r}(D) &:= \#\{d : |d| \leq D,\ \text{rk } E_d(\mathbb{Q}) \geq r\}, \\ N_{\geq r,\text{ even}}(D) &:= \#\{d : |d| \leq D,\ \text{rk } E_d(\mathbb{Q}) \geq r,\ \text{and } w(E_d) = +1\}, \\ N_{\geq r,\text{ odd}}(D) &:= \#\{d : |d| \leq D,\ \text{rk } E_d(\mathbb{Q}) \geq r,\ \text{and } w(E_d) = -1\}, \end{aligned}$$

where $w(E_d) \in \{-1, +1\}$ is the global root number of E_d.

Conjecture 1.2. Does it hold that

$$N_{\geq 2,\text{ even}}(D) = D^{3/4+o(1)}\ ?$$

In other words, the prediction is that for d such that $w(E_d) = +1$, the probability that rk $E_d(\mathbb{Q}) \geq 2$ should be about $d^{3/4+o(1)}/d \simeq d^{-1/4}$. Since ht $E_d \asymp d^6$ by Example 1.2, this prediction corresponds to a probability of $h^{-1/24}$ for an elliptic curve of height h.

Remark 1.3. (a) The Birch and Swinnerton-Dyer conjecture would imply the parity conjecture,

Conjecture 1.3. Does it hold that

$$w(E) = (-1)^{\mathrm{rk}\, E(\mathbb{Q})} \ ?$$

Let E be an elliptic curve over $\mathbb{Q}$ with $w(E) = +1$. Then, it is known that for a weight $3/2$ cusp form $f = \sum a_n q^n$ such that for all odd fundamental discriminants $d < 0$ coprime to the conductor of E, we have $a_{|d|} = 0$ if and only if $L(E_d, 1) = 0$. If the BSD conjecture is true, then the condition $L(E_d, 1) = 0$ is equivalent to $\mathrm{ord}_{s=1} L(E_d, s) \geq 2$, which is equivalent to rk $E_d(\mathbb{Q}) \geq 2$. The Ramanujan conjecture predicts that $a_|d|$ is an integer satisfying $|a_|d|| \leq |d|^{1/4+o(1)}$. Hence, heuristically, we can expect that $a_|d| = 0$ occurs with "probability" $|d|^{-1/4+o(1)}$ and hence $N_{\geq 2,\, \mathrm{even}}(D) \simeq \sum_{|d| \leq D} |d|^{-1/4+o(1)} \simeq |D|^{3/4+o(1)}$.

(b) Conrey, Keating, Rubinstein and Snaith used random matrix theory to get a developed conjecture, that is, there exist constants $c_E, e_E \in \mathbb{R}$ such that

Conjecture 1.4.

$$N_{\geq 2,\, \mathrm{even}}(D) = (c_E + o(1)) D^{3/4} (\log D)^{e_E} \ ?$$

On the other hand, Watkins developed a variant for the family of all elliptic curves over $\mathbb{Q}$, that is, there exists a constant $c_0 > 0$ such that

Conjecture 1.5.

$$\#\{E : \mathrm{ht}\ E \leq H,\ \mathrm{rk}\ E_d(\mathbb{Q}) \geq 2,\ \text{and}\ w(E_d) = +1\} = (c_0 + o(1)) H^{19/24} (\log H)^{3/8} \ ?$$

An elementary seive argument shows that

$$\#\{E : \mathrm{ht}\ E \leq H\} = (\kappa + o(1)) H^{5/6},$$

where $\kappa := 2^{4/3} 3^{-3/2} \zeta(10)^{-1}$. Hence, the Conjecture 5 is related to Conjecture 4 through the equation that $19/24 = 5/6 - 1/24$.

1.3. **Conjectures for rank 3 asymptotics.** Recall that the conjectures for $N_{\geq 2,\, \mathrm{even}}(D)$ are in agreement. However, the conjectures for $N_{\geq 3,\, \mathrm{odd}}(D)$ are very different in literature. For instance, Rubin and Silveberg conjectured a lower bound $N_{\geq 3,\, \mathrm{odd}}(D) >> D^{1/3}$ for many E while the Birch and Swinnerton-Dyer conjecture implies $N_{\geq 3,\, \mathrm{odd}}(D) \asymp D^{1/4}$. In the model used in this paper suggests that $N_{\geq 3}(D) \asymp D^{1/2+o(1)}$ and $N_{\geq 3,\, \mathrm{odd}}(D) \asymp D^{1/2+o(1)}$.

Notation. For $x = (x_1, ..., x_m)$ and $a = (a_1, ..., a_n)$, the notation $f(x, a) \ll_a g(x, a)$ means that for every fixed a, there exists a positive constant $C(a)$ such that $f(x, a) \leq C(a) g(x, a)$ for all x. Then, $f(x, a) \asymp_a g(x, a)$ means that $f(x, a) \ll_a g(x, a)$ and $g(x, a) \ll_a f(x, a)$.

For an abelian group G and $n \in \mathbb{N}$, denote by $G[n] := \{x \in G : nx = 0\}$. For p prime, define $G[p^\infty] := \cup_{m \in \mathbb{N}} G[p^m]$ and define the p-rank of G to be $\dim_{\mathbb{F}_\mathrm{p}} G[p]$.

For a commutative ring R, denote by $M_n(R)$ be the set of $n \times n$ matrices with entries in R. For $X > 0$, let $M_n(\mathbb{Z})_{\leq X} \subset M_n(\mathbb{Z})$ be the subset of matrices whose entries have absolute value less than or equal to X. We also let $M_n(R)_{\mathrm{alt}}$ be the set of alternating matrices, i.e. $A^T = -A$ and all the diagonal entries are 0.

For a subset $S \subset M_n(\mathbb{Z}_p)$, define $\mathrm{Prob}(S) = \mathrm{Prob}(S|A \in M_n(\mathbb{Z}_p))$ as the probability of S with respect to the normalized Haar measure on the compact group $M_n(\mathbb{Z}_p)$.

2. Cohen-Lenstra Heuristics for Class Groups

2.1. **Class groups as cokernels of integer matrices.** Let K be a number field and I be the group of nonzero fractional ideals of K. Let P be the subgroup of I consisting of principal fractional ideals. Then, the class group is defined as $\mathrm{Cl}\ K := I/P$. It is well-known that $\mathrm{Cl}\ K$ is a finite abelian group.

Let $\mathcal{O}_K$ be the ring of integers of K. Let S_∞ be the set of all archimedean places of K and S be a finite set of places of K containing S_∞. Let $n := \#(S \setminus S_\infty)$. Then, the Dirichlet unit theorem states that the unit group $\mathcal{O}_K^\times$ is a finitely generated abelian group of rank $u := \#S_\infty - 1$ and the unit group $\mathcal{O}_{K,S}^\times$, where $\mathcal{O}_{K,S}$ is the ring of S-integers of K, is also a finitely generated abelian group of rank $\#S - 1 = n + u$.

Let I_S be the group of fractional ideals generated by the nonarchimedean primes in S and let P_S be the subgroup of I_S consisting of principal fractional ideals. Assume that primes of S generate the whole finite group $\mathrm{Cl}\ K$ so that we obtain $I_S/P_S \simeq I/P = \mathrm{Cl}\ K$.

Note that the group I_S is a free abelian group of rank n and P_S is the image of the homomorphism $\mathcal{O}_{K,S}^\times \to I_S$, whose kernel is the torsion subgroup of $\mathcal{O}_{K,S}^\times$ so that P_S is a free abelian group of rank $n + u$. It follows that we can represent $\mathrm{Cl}\ K$ as the cokernel of a homomorphism $P_S \simeq \mathbb{Z}^{n+u} \to \mathbb{Z}^n \simeq I_S$. Write this cokernel as coker A for some $n \times (n + u)$ matrix A over $\mathbb{Z}$. By viewing this matrix A as a matrix over $\mathbb{Z}_p$, we get coker $(A : \mathbb{Z}_p^{n+u} \to \mathbb{Z}_p^n) = (\mathrm{Cl}\ K)[p^\infty]$.

2.2. **Distribution of class groups.** Let $\mathscr{K}$ be the family of all imaginary quadratic fields up to isomorphism. In this section, we discuss about the distribution of $\mathrm{Cl}\ K$ as K varies over $\mathscr{K}$. To deal with this problem, we define the density of a subset $S \subset \mathscr{K}$. For $X > 0$, let $\mathscr{K}_{\leq X}$ be the set of elements in $\mathscr{K}$ whose absolute value of the discriminant is less than or equal to X. Then, the density μ is defined by

$$\mu(S) = \mu(S|K \in \mathscr{K}) := \lim_{X\to\infty} \frac{\#(S \cap \mathscr{K}_{\leq X})}{\#\mathscr{K}_{\leq X}},$$

whenever this limit make sense.

It is known that $\#\mathrm{Cl}\ K$ diverges as the discriminant of K goes to infinity. More precisely, Siegel proved that $\#\mathrm{Cl}\ K = |D|^{1/2+o(1)}$, where D is the discriminant of K. It follows that for any finite abelian group G, we have that $\mu(\mathrm{Cl}\ K \simeq G\} = 0$ since the set $\{K \in \mathscr{K} : \mathrm{Cl}\ K \simeq G\}$ is finite.

Hence, to get a meaningful density, we consider the p-Sylow subgroup $(\mathrm{Cl}\ K)[p^\infty]$ for a fixed prime $p \neq 2$ instead of whole group $\mathrm{Cl}\ K$. (There is a different phenomenon in case $p = 2$.) For each finite abelian p-group G, the density $\mu((\mathrm{Cl}\ K)[p^\infty] \simeq G)$ is expected to positive. Here, we give two conjectures for its value.

Conjecture 2.1. The density is inversely proportional to $\#\mathrm{Aut}\ G$:

$$\mu((\mathrm{Cl}\ K)[p^\infty] \simeq G) = \frac{1}{\eta(p)} \frac{1}{\#\mathrm{Aut}\ G}\ ?$$

The normalization constant $\eta(p)$ is needed to make μ a probability measure and is given by

$$\eta(p) := \sum_{G\text{:fintie abelian } p\text{-group}} \frac{1}{\#\text{Aut } G} = \prod_{i=1}^{\infty}(1-p^{-i})^{-1}.$$

Conjecture 2.2. Recall that $\mathscr{K}$ is the family of all *imaginary* quadratic fields. Applying the discussion in Section 2.1 with unit rank $u = \#S_\infty - 1 = 0$, one models $(\text{Cl } K)[p^\infty]$ as $(\text{coker } A)[p^\infty]$ for a "random" $n \times n$ matrix A over $\mathbb{Z}$ or $\mathbb{Z}_p$. That is,

$$\begin{aligned}\mu((\text{Cl } K)[p^\infty] \simeq G) &= \lim_{n\to\infty}\lim_{X\to\infty} \frac{\#\{A \in M_n(\mathbb{Z})_{\le X} : (\text{coker } A)[p^\infty] \simeq G\}}{\#M_n(\mathbb{Z})_{\le X}} \ ? \\ &= \lim_{n\to\infty} \mathbb{P}\big(\text{coker } A \simeq G | A \in M_n(\mathbb{Z}_p)\big).\end{aligned}$$

(The equality of the probabilities in the last two expressions follows from the fact that $\mathbb{Z}$ is uniformly distributed in $\mathbb{Z}_p$ asymptotically .)

In fact, the above two Conjectures are equivalent.

Theorem 2.1. (Friedman and Washington.) *For every finite abelian p-group G,*

$$\lim_{n\to\infty} \mathbb{P}\big(\mathit{coker}\ A \simeq G | A \in M_n(\mathbb{Z}_p)\big) = \frac{1}{\eta(p)}(\#\mathit{Aut}\ G)^{-1}.$$

We remark that if we consider the family of *real* quadratic fields instead of $\mathscr{K}$, then the unit rank u becomes 1 so that Section 2.1 suggests that Cl K should be modeled by the cokernel of a "random" $n \times (n+1)$ matrix.

3. Heuristics for Shafarevich-Tate Groups

In this section, we study conjectures for the Sharfarevich-Tate group $Ш(E)$ of an elliptic curve E over $\mathbb{Q}$, analogous to the conjectures for class groups.

Let $\mathscr{E}$ be the set of elliptic curves, one in each $\mathbb{Q}$-isomorphism class. Then, for $H > 0$, define $\mathscr{E}_{\le H} := \{E \in \mathscr{E} : \text{ht } E \le H\}$. Similar to the previous section, for a subset $S \subset \mathscr{E}$, we define densities

$$\begin{aligned}\mu(S) &:= \lim_{H\to\infty} \frac{\#(S \cap \mathscr{E}_{\le H})}{\#\mathscr{E}_{\le H}}, \\ \mu(S \mid \text{rk } E(\mathbb{Q}) = r) &:= \lim_{H\to\infty} \frac{\#\{E \in S \cap \mathscr{E}_{\le H} \mid \text{rk } E(\mathbb{Q}) = r\}}{\#\{E \in \mathscr{E}_{\le H} \mid \text{rk } E(\mathbb{Q}) = r\}},\end{aligned}$$

whenever the limits make sense. We mention that if there is no $E \in \mathscr{E}$ such that rk $E(\mathbb{Q}) = r$, then the density $\mu(S \mid \text{rk } E(\mathbb{Q}) = r)$ does not exist.

The n-Selmer group $\text{Sel}_n\ E$ and the Shafarevich-Tate group $Ш(E)$ associated to an elliptic curve $E \in \mathscr{E}$ are related by the exact sequence

$$0 \to E(\mathbb{Q}) \otimes \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \to \text{Sel}_{p^\infty} \to Ш(E)[p^\infty] \to 0. \tag{3.1}$$

The idea of this paper is that instead of predicting a distribution of rk $E(\mathbb{Q})$ in isolation, model all three invariants at once. This allows us check the model against other theorems and conjectures in the literature.

Definition 3.1. (1) A pairing $[,]$ is called alternating if $[m,m]=0$ for all m.
(2) A pairing $[,]$ is called nondegenrate if $[m,n]=0$ for all m implies that $n=0$.
(3) A symplectic finite abelian group is a pair $(G,[,])$, where G is a finite abelian group and $[,]: G\times G\to\mathbb{Q}/\mathbb{Z}$ is a nondegenerate alternating pairing.

Let $\mathfrak{G}$ be a set of symplectic finite abelian groups containing exactly one from each isomorphism class. If J is a finite abelian group, then $J\times J^\vee$ equipped with a natural pairing, that is, $[(x,f),(y,g)]=f(y)-g(x)$, is a symplectic finite abelian group. Moreover, it is known that every symplectic finite abelian group is isomorphic to one of this form. It follows that symplectic finite abelian groups have square order. Let $\mathfrak{G}_p$ be the set of $G\in\mathfrak{G}$ such that $\#G=p^n$ for some $n\in 2\mathbb{Z}$.

Most experts conjectured that $\text{Ш}(E)$ is finite. In 1962, Cassels constructed a alternating pairing $\langle\ ,\ \rangle:\text{Ш}(E)\times\text{Ш}(E)\to\mathbb{Q}/\mathbb{Z}$. He also proved that $\langle\ ,\ \rangle$ is a nondegenerate pairing provided that $\text{Ш}(E)$ is finite. Hence, if $\text{Ш}(E)$ is finite, $(\text{Ш}(E),\langle\ ,\ \rangle)$ is a symplectic finite abelian group, and in particular $\#\text{Ш}(E)$ is a square.

It follows that the distribution of $\text{Ш}(E)$ will be different from the conjectural distribution of class gorups given in Conjecture 2.1. and Conjecture 2.2. It is natural to ask the following question for the distribution of $\text{Ш}(E)$.

Question 3.1. Let p be a prime. Given $r\geq 0$ and $G\in\mathfrak{G}_p$, what is the density

$$\mu\big(\text{Ш}(E)[p^\infty]\simeq G\mid \text{rk } E(\mathbb{Q})=r\big)?$$

There are three conjectural answers to this question in the literature.

($\mathscr{D}_r$) Delaunay, in analogy with the Cohen-Lenstra heuristics for class groups, made conjectures on the answer to Question 3.1. That is, the answer is given by the probability measure $\mathscr{D}_r=\mathscr{D}_{r,p}$ on $\mathfrak{G}_p$ defined by

$$\mathscr{D}_r(G):=\frac{1}{\eta(r,p)}\frac{\#G^{1-r}}{\#\text{Aut } G}=\frac{\#G^{1-r}}{\#\text{Aut } G}\prod_{i\geq r+1}(1-p^{1-2i}),\quad\text{(cf. Conjecture 2.1.,)}$$

where Aut G denotes the group of automorphisms of G that respects the pairings.

($\mathscr{T}_r$) Work of Poonen and Rains [PR12], and Bhargava, Kane, Lenstra, Poonen and Rains [BKLPR15] predicted the isomorphism type of the Selmer group $\text{Sel}_p E$ and the short exact sequence (3.1), respectively. One can extract a probability measure $\mathscr{T}_r$ on $\mathfrak{G}_p$ which model $\text{Ш}(E)[p^\infty]$ from these works.

($\mathscr{A}_r$) In [BKLPR15], the authors also showed that $\text{coker}(A:\mathbb{Z}_p^n\to\mathbb{Z}_p^n)_{\text{tors}}$ is a symplectic fintie ablian p-group for each $A\in M_n(\mathbb{Z}_p)_{\text{alt}}$. Inspired by this result, let

$$\mathscr{A}_{n,r}:=\mathbb{P}\big((\text{coker } A)_{\text{tors}}\simeq G|A\in M_n(\mathbb{Z}_p)_{\text{alt}},\ \text{rk}_{\mathbb{Z}_p}(\text{ker } A)=r\big).$$

Then, we define a probability measure $\mathscr{A}_r$ on $\mathfrak{G}_p$ by

$$\mathscr{A}_r(G):=\lim_{n\equiv r\ (\text{mod } 2),\ n\to\infty}\mathscr{A}_{n,r}(G).$$

In fact, these three answers are equivalent.

Theorem 3.2 (BKLPR15, Theorem 1.6(c) and 1.10(b))**.** *The probability measures $\mathscr{D}_r$, $\mathscr{T}_r$ and $\mathscr{A}_r$ coincide.*

Remark 3.3. Note that class groups of quadratic fields are large if the field is imaginary ($u = 0$) and conjecturally small if the field is real ($u = 1$). (Recall that $(\mathrm{Cl}\ K)[p^\infty]$ is modeled by $\mathrm{coker}(A : \mathbb{Z}_p^{n+u} \to \mathbb{Z}_p^n)$.) Just as this observation, conjecturally, $\text{Ш}(E)$ is large on average when $r = 0$ and small when $r \geq 1$. Indeed, from the conjecture ($\mathscr{D}_r$), we see that $\mu(\#\text{Ш}(E) \leq B \mid \mathrm{rk}\ E(\mathbb{Q}) = 0) = 0$ for every fixed $B > 0$ while for each $r \geq 1$, $\mu(\#\text{Ш}(E) \leq B \mid \mathrm{rk}\ E(\mathbb{Q}) = r) \to 1$ as $B \to \infty$. This phenomenon comes from the numerator $\#G^{1-r}$.

4. Average Size of the Shafarevich-Tate Group

In construction of a model for ranks and $\text{Ш}(E)$, we will need to know the typical size of $\#\text{Ш}(E)$ for a rank 0 elliptic curve of height about H.

4.1. **Size of the real period.** Let $A, B \in \mathbb{R}$ satisfy $4A^3 + 27B^2 \neq 0$, so that the equation $y^2 = x^3 + Ax + B$ defines an elliptic curve E over $\mathbb{R}$. Recall that the discriminant of E is defined as $\Delta := -16(4A^3 + 27B^2)$ and height is defined as $\mathrm{ht}\ E := \max\{|4A^3|, |27B^2|\}$. Let

$$\Omega := \int_{E(\mathbb{R})} \left| \frac{dx}{2y} \right|.$$

Lemma 4.1. *Let $A, B \in \mathbb{R}$ satisfy $4A^3 + 27B^2 \neq 0$, so that the equation $y^2 = x^3 + Ax + B$ defines an elliptic curve E over $\mathbb{R}$. Let $H := ht\, E$. Then,*

$$H^{-1/12} \ll \Omega \ll H^{-1/12} \log(64H/|\Delta|).$$

Corollary 4.2. *Under the hypotheses of Lemma 4.1, we have $\Omega \ll |\Delta|^{-1/12}$.*

Corollary 4.3. *Under the hypotheses of Lemma 4.1, we have $H^{-1/12} \ll \Omega \ll H^{-1/12} \log H$.*

Remark 4.4. (1) Although more precise results are know, the above estimates are sufficient for our model.

(2) Observe that for $\lambda \in \mathbb{R}^\times$, changing (A, B) to $(\lambda^4 A, \lambda^6 B)$ preserves the elliptic curve. Since this operation changes (H, Δ, Ω) to $(\lambda^{12} H, \lambda^{12}\Delta, \lambda^{-1}\Omega)$, the number $-1/12$ in the exponent terms are natural.

(3) The bounds in Corollary 4.3 are best possible, up to constants. Indeed, by the above remark(2), we see that the lower bound is sharp. Moreover, for large $a \in \mathbb{Z}_{>0}$, let E be the curve determined by the equation $y^2 = (x - a)(x - a - 1)(x + 2a + 1)$. Then, it is easy to

check that $H \asymp a^6$ and

$$\begin{aligned}\Omega &\asymp \int_{-2a-1}^{0} \frac{dx}{\sqrt{(a-x)(a+1-x)(x+2a+1)}} + \int_{0}^{a} \frac{dx}{\sqrt{(a-x)(a+1-x)(x+2a+1)}} \\ &\quad + \int_{a+1}^{\infty} \frac{dx}{\sqrt{(x-a)(x-a-1)(x+2a+1)}} \\ &\asymp a^{-1} \int_{-2a-1}^{0} \frac{dx}{\sqrt{x+2a+1}} + a^{-1/2} \int_{0}^{a} \frac{dx}{\sqrt{(a-x)(a+1-x)}} \\ &\quad + a^{-1/2} \int_{a+1}^{3a} \frac{dx}{\sqrt{(x-a)(x-a-1)}} + \int_{3a}^{\infty} \frac{dx}{x^{3/2}} \\ &\asymp a^{-1/2} + a^{-1/2}\log a + a^{-1/2}\log a + a^{-1/2} \asymp a^{-1/2}\log a.\end{aligned}$$

It shows that the upper bound is sharp.

4.2. **Average size of the Shafarevich-Tate group.** Let $E \in \mathscr{E}$. Define

$$Ш_0(E) := \begin{cases} \#Ш(E), & \text{if } \operatorname{rk} E(\mathbb{Q}) = 0; \\ 0, & \text{if } \operatorname{rk} E(\mathbb{Q}) > 0. \end{cases}$$

Then, the Birch and Swinnerton-Dyer conjecture implies that

$$Ш_0(E) = \frac{\#E(\mathbb{Q})_{\mathrm{tors}}^2 L(E,1)}{\Omega \prod_p c_p},$$

where the constant c_p is the Tamagawa factor.

We conjecture the following (related to the Tiemann hypthesis for the L-functions).

Conjecture 4.1. It holds that

$$\mathrm{Average}_{E \in \mathscr{E}_{\leq H}} L(E,1) = H^{o(1)} \quad \text{as} \quad H \to \infty.$$

It is well known that $\prod_p c_p = H^{o(1)}$ and $\#E(\mathbb{Q})_{\mathrm{tors}} \leq 16$. By combining all results, we get the following estimates for $Ш_0(E)$.

Theorem 4.5. *Assume that the Birch and Swinnerton-Dyer conjecture and Conjecture 4.1 are true. Then,*

$$\mathit{Average}_{E \in \mathscr{E}_{\leq H}} Ш_0(E) = H^{1/12+o(1)} \quad \mathit{as} \quad H \to \infty.$$

5. The Basic Model for Ranks and Shafarevich-Tate Groups

In view of Theorem 3.2, we propose the following model for the arithmetic of an elliptic curve E over $\mathbb{Q}$ of height H. Informally, to each elliptic curve E, we will associate a random matrix $A \in M_n(\mathbb{Z})_{\mathrm{alt},\leq X}$ such that rk(ker A) models rk $E(\mathbb{Q})$ and (coker A)$_{\mathrm{tors}}$ models $Ш(E)$.

5.1. **The random model.** We now construct a collection of independent random variables $(\mathrm{rk}'_E, Ш'_E)_{E\in\mathscr{E}}$ taking values in $\mathbb{Z}_{\geq 0} \times \mathfrak{G}$.

(1) Choose an elliptic curve E and let $H := \mathrm{ht}\ E$. Choose two unbounded increasing functions $\eta(H)$ and $X(H)$.

(2) Choose n uniformly at random from $\mathbb{Z} \cap [\eta(H), \eta(H) + 2)$.

(3) Choose $A \in M_n(\mathbb{Z})_{\mathrm{alt},\leq X(H)}$ uniformly at random.

(4) Define $\mathrm{rk}'_E := \mathrm{rk}(\ker\ A)$, and $Ш'_E := (\mathrm{coker}\ A)_{\mathrm{tors}}$ equipped with its canonically defined nondegenerate alternating pairing.

Remark 5.1. The second step is needed since the probability measure $\mathscr{A}_r$ on $\mathfrak{G}_p$ is defined by some limit with the relation $n \equiv r \pmod 2$. (Recall that $\mathscr{A}_r(G) := \lim_{n\equiv r \pmod 2,\, n\to\infty} \mathscr{A}_{n,r}(G)$.) Indeed, replacing $[\eta(H), \eta(H)+2)$ with any other interval of length $o(\eta(H))$ containing $\eta(H)$ would not affect main results as long as the parity of n becomes equidistributed as $H \to \infty$.

Now, we state the estimates for $(\mathrm{rk}'_E, Ш'_E)_{E\in\mathscr{E}}$. Define the random variable

$$Ш'_{0,E} := \begin{cases} \#Ш'_E, & \text{if } \mathrm{rk}'_E = 0; \\ 0, & \text{if } \mathrm{rk}'_E > 0. \end{cases}$$

Theorem 5.2. *If the function $X(H)$ grows sufficiently quickly relative to $\eta(H)$, then the following hold for $E \in \mathscr{E}$ as $H := ht\ E \to \infty$.*

(a) (0) The probability that $rk'_E = 0$ is $1/2 - o(1)$.
(1) The probability that $rk'_E = 1$ is $1/2 - o(1)$.
(2) The probability that $rk'_E \geq 2$ is $o(1)$.

(b) (1) We have $Ш'_{0,E} \leq (X(H)^{\eta(H)})^{1+o(1)}$.
(2) The probability that $Ш'_{0,E} \geq (X(H)^{\eta(H)})^{1-o(1)}$ is at least $1/3$.

(c) For fixed $r \geq 1$, we have $Prob(rk'_E \geq r) = (X(H)^{\eta(H)})^{-(r-1)/2+o(1)}$.

Corollary 5.3. *If the function $X(H)$ grows sufficiently quickly relative to $\eta(H)$, then the following hold with probability 1.*

(a) We have

$$\mu(\{E : rk'_E = 0\}) = \mu(\{E : rk'_E = 1\}) = 1/2 \qquad and \qquad \mu(\{E : rk'_E \geq 2\}) = 0.$$

(b) We have

$$Average_{E\in\mathscr{E}_{\leq H}}\ Ш'_{0,E} = (X(H)^{\eta(H)})^{1+o(1)} \quad as \quad H \to \infty,$$

assuming that the function $f(H) := X(H)^{\eta(H)}$ satisfies $f(2H) \leq f(H)^{1+o(1)}$.

Ideas of proof for Theorem 5.2. (a) Informally, from the random matrix theory, if we choose $A \in M_n(\mathbb{Z})_{\leq X}$ uniformly at random, then with probability almost one, we have $\det A \neq 0$ which means that $\mathrm{rk}(\ker\ A) = 0$. Combining this with the fact that size of any invertible alternating matrix is even, we can deduce that if we choose $A \in M_n(\mathbb{Z})_{\mathrm{alt},\leq X}$ uniformly at random, then with probability almost one, we have $\mathrm{rk}(\ker\ A) = 0$ if n is even and $\mathrm{rk}(\ker\ A) = 1$ if n is odd. Since the parity of n becomes equidistributed as $H \to \infty$, we obtain the results.

(b) If $\mathrm{rk}'_E = 0$, then $Ш'_{0,E}$ is the absolute value of the determinant of a random matrix $A \in M_n(\mathbb{Z})_{\mathrm{alt},\le X}$. Hence, with probability $p \in (1/3, 1/2)$, we obtain

$$Ш'_{0,E} \asymp |X|^{n+o(1)} \asymp (X^\eta)^{1+o(1)}.$$

(c) We have the following fact:

If $1 \le r \le n$ and $n - r$ is even, then

$$\#\{A \in M_n(\mathbb{Z})_{\mathrm{alt},\le X} : \mathrm{rk}(\ker A) \ge r\} \asymp_n X^{n(n-r)/2}. \tag{5.1}$$

Using (5.1), we have

$$\begin{aligned}\mathrm{Prob}\big(\mathrm{rk}(\ker A) \ge r | n \equiv r \pmod 2\big) &= \frac{X^{n(n-r)/2+o(1)}}{X^{n(n-1)/2+o(1)}} \\ &= (X^n)^{-(r-1)/2+o(1)} \\ &= (X^\eta)^{-(r-1)/2+o(1)},\end{aligned}$$

and

$$\begin{aligned}\mathrm{Prob}\big(\mathrm{rk}(\ker A) \ge r | n \not\equiv r \pmod 2\big) &= \mathrm{Prob}\big(\mathrm{rk}(\ker A) \ge r+1 | n \not\equiv r \pmod 2\big) \\ &= (X^\eta)^{-r/2+o(1)}.\end{aligned}$$

Combining these yields the result. □

5.2. **Consequences for coranks of random matrices.** Comparing Theorem 4.5 and Theorem 5.2(b) suggests choosing $X(H)$ and $\eta(H)$ satisfying

$$X(H)^{\eta(H)} = H^{1/12+o(1)} \quad \text{as} \quad H \to \infty.$$

Now, we are ready to state the main result in this paper.

Theorem 5.4. *If $\eta(H)$ grow sufficiently slowly relative to H, and $X(H)^{\eta(H)} = H^{1/12+o(1)}$, then the following hold with probability* 1*:*
(a) All but finitely many $E \in \mathscr{E}$ satisfy $rk'_E \le 21$.
(b) For $1 \le r \le 20$, we have $\#\{E \in \mathscr{E}_{\le H} : rk'_E \ge r\} = H^{(21-r)/24+o(1)}$.
(c) We have $\#\{E \in \mathscr{E}_{\le H} : rk'_E \ge 21\} \le H^{o(1)}$.

Proof. Fix $r \ge 1$. For $E \in \mathscr{E}$, we let $H = H_E := \mathrm{ht}\, E$ and $p_{E,r} := \mathbb{P}(\mathrm{rk}'_E \ge r)$. By Theorem 5.2(c), we have that

$$p_{E,r} = (X(H)^{\eta(H)})^{-(r-1)/2+o(1)} = H^{-(r-1)/24+o(1)}.$$

It follows that since $\#\mathscr{E}_{\le H} \asymp H^{5/6}$,

$$\sum_{E \in \mathscr{E}_{\le H}} p_{E,r} \asymp \int_1^H h^{-(r-1)/24+o(1)} h^{5/6-1} dh = \begin{cases} H^{(21-r)/24+o(1)}, & \text{if } 1 \le r \le 21; \\ O(1), & \text{if } r > 21. \end{cases}$$

Then, the Borel-Cantelli lemma yields the result. □