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 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 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 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 $A_E \in M_n(\mathbb{Z})_{\text{alt}}$ with entries bounded by $X(H)$ in absolute value, uniformly at random.
Then $(\text{coker } A_E)_{\text{tors}}$ models $\text{Ш}(E)$, the Shafarevich-Tate group of E, and rk $(\ker A_E)$ models rk $E(\mathbb{Q})$.

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

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

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 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 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 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 $\dim_{\mathbb{F}_p} G[p]$.

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 $\#\mathrm{Aut}\ G$:

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

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

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

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,

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

(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,*

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

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.