Ordering elliptic curves by their conductors

Arul Shankar

Joint work with Ananth N. Shankar and Xiaoheng Wang

October 27

Why the conductor?

Let $\mathcal{E}$ be the family of all elliptic curves over $\mathbb{Q}$

$$\mathcal{E} = \left\{E_{A,B} : y^2 = x^3 + Ax + B \mid A, B \in \mathbb{Z}, p^4 \mid A \implies p^6 \nmid B\right\}.$$

Conjecture (Goldfeld,Katz–Sarnak)

50% *of curves in* $\mathcal{E}$ *have rank* 0*;* 50% *of curves in* $\mathcal{E}$ *have rank* 1*.*

Each curve $E \in \mathcal{E}$ has an attached L-function $L(E,s)$.
These conjectures were formulated by studying the associated family $\left\{L(E,s) : E \in \mathcal{E}\right\}$ of L-functions together with:

$$\mathrm{BSD}: \text{ rank of } E \;=\; \text{analytic rank of } E.$$

Most natural way to order L-functions is by their conductors.

What's the conductor? (away from 2 and 3)

Let $E : y^2 = f(x) = x^3 + Ax + B$ be an elliptic curve. Away from 2 and 3, the discriminant of E is

$$\Delta(E) = \Delta(f) = -4A^3 - 27B^2.$$

In particular, $p \mid \Delta(E)$ iff $f(x)$ has a multiple root r mod p.

$$\text{We define } C_p(E) := \begin{cases} p & \text{if r is a double root;} \\ p^2 & \text{if r is a triple root.} \end{cases}$$

Equivalently, $C_p(E) = p$ when E has multiplicative reduction at p, and $C_p(E) = p^2$ when E has additive reduction at p.
We then define the conductor of E to be

$$C(E) := \prod_{p \mid \Delta(E)} C_p(E).$$

Note in particular that $C(E) \mid \Delta(E)$.

What is expected?

Ordering curves by Δ, C: we are interested in the asymptotics of

$$\begin{aligned} N_\Delta(X,\mathcal{E}) &:= \#\{E\in\mathcal{E} : \Delta(E)<X\};\\ N_C(X,\mathcal{E}) &:= \#\{E\in\mathcal{E} : C(E)<X\}. \end{aligned}$$

When elliptic curves are ordered by discriminant, we have

Conjecture (Brumer–McGuinness)

$$\begin{aligned} N_\Delta(X,\mathcal{E}) &\sim \zeta(10)^{-1}\mathrm{Vol}(\{(A,B)\in\mathbb{R}^2 : \Delta(A,B)<X\})\\ &\sim \frac{(\sqrt{3}+3\sqrt{3})\sqrt{\pi}\Gamma(7/6)}{5\zeta(10)\Gamma(2/3)}\cdot X^{5/6}. \end{aligned}$$

Unlike when ordering by height, even finiteness of $N_\Delta(X,\mathcal{E})$ is not immediate. It requires some diophantine input. (For example: Siegel's theorem on finiteness of integral points on elliptic curves.)

What is expected?

To understand $N_C(X,\mathcal{E})$, partition $\mathcal{E}$ as $\mathcal{E} = \cup_{n\geq 1}\mathcal{E}_n$, where

$$\mathcal{E}_n := \{E \in \mathcal{E} : |\Delta(E)|/C(E) = n\}.$$

If $E \in \mathcal{E}_n$, then $C(E) < X \iff |\Delta(E)| < nX$.Thus, we expect

$$N_C(X,\mathcal{E}) \sim \sum_{n\geq 1} N_\Delta(nX,\mathcal{E}) \cdot \mathrm{Prob}(E \in \mathcal{E}_n) \asymp \sum_{n\geq 1} \frac{(nX)^{5/6}}{n^2} \asymp X^{5/6}.$$

Then the following conjecture is implicit in the work of Watkins.

Conjecture

We have

$$N_C(X,\mathcal{E}) \sim \alpha \cdot X^{5/6}$$

for some explicit constant α computed by Watkins.

The best known bounds

Lower bounds are easy to obtain:

1. Counting $(A, B) \in \mathbb{Z}^2$ of height $\ll X^{1+\epsilon}$ gives the correct lower bound for $N_\Delta(X, \mathcal{E})$.
2. Then summing $N_\Delta(nX)$ over $n \ll X^\epsilon$ gives the correct lower bound for $N_C(X, \mathcal{E})$.

Upper bounds are much more difficult:

1. $N_\Delta(X, \mathcal{E}) = O(X)$ follows from work of Davenport together with works of Delone–Nagell and Siegel.
2. $N_C(X, \mathcal{E}) = O(X^{1+\epsilon})$ is due to Duke–Kowalski, building on work of Brumer–Silverman.

Both upper bounds use ineffective results.The nature of those proofs make improvements very difficult.

The above two proofs motivate the following related questions:

Open Questions

How many binary cubic forms represent 1*? Equivalently, how many cubic rings are monogenic? How many cubic* fields *are monogenic? How does $\#E(\mathbb{Z})$ behave in families of elliptic curves?*

Here are some of the known results in these directions:

1. Alpoge–Ho: $\#E(\mathbb{Z})$ has bounded second moment.
2. Bhargava–S.: A positive proportion of elliptic curves have rank 0, and no integral points.
3. Akhtari–Bhargava: A positive proportion of cubic rings are not monogenic (despite no local obstructions).
4. Alpoge–Bhargava–Shnidman: A positive proportion of cubic fields are not monogenic (despite no local obstructions).

Getting to 0% seems difficult, needing different methods.

Seperating the Δ and C difficulties

There are two basic difficulties in estimating $N_C(X, \mathcal{E})$.

1. Hard to rule out elliptic curves with large height and small discriminant.
2. Hard to rule out elliptic curves with large discriminant and small conductor.

Issue 2 is a non-archemedian version of Issue 1.
Indeed, the first happens when $4A^3$ and $27B^2$ are unusually close.
While the second happens when $4A^3$ and $27B^2$ are unusually close p-adically. At one prime p, or many primes p.

We will rule out the first issue, and focus on the second.

$$\text{Define } \mathcal{E}' := \left\{E \in \mathcal{E} : j(E) < \log|\Delta(E)|\right\}$$

Curves E in $\mathcal{E}'$ satisfy $H(E) \ll_\epsilon |\Delta(E)|^{1+\epsilon}$. Only Issue 2 remains.

Asymptotics for $N_C(\mathcal{E}', X)$ would follow by bounding $N_C(\mathcal{E}'_n, X)$. More precisely, we need the bound

$$N_C(\mathcal{E}'_n, X) \ll X^{5/6}/n^{1+5/6+\delta} \tag{1}$$

for some $\delta > 0$, independent of n and X.

Bounds of this type are called uniformity or tail estimates.

They arise in many different contexts. For $F \in \mathbb{Z}[x_1, \ldots, x_n]$,

$$\#\{v \in \mathbb{Z}^n : \ |v| < X, \ p^2 \mid F(v)\} \ll X^n/p^{1+\delta} + o(X^n)$$

is enough to determine the odds that F takes a squarefree value.

S.–Tsimerman: *Precise* estimates on quantities analogous to $N_C(\mathcal{E}'_n, X)$, for degree-n polynomials, implies Malle's conjecture for degree-n S_n number fields.

In all these cases, we only need average bounds over $n \in [M, 2M]$.

Partial results (when n is squarefree)

We prove estimate (1), on average over *squarefree* n:

Theorem (Shankar, S., Wang)

We have

$$\sum_{\substack{n>M \\ n \text{ sq. free}}} N_C(\mathcal{E}'_n, X) \ll_\epsilon X^{5/6}/M^{1/6-\epsilon}. \tag{2}$$

This is enough to handle the following family. Define

$$\mathcal{E}_{\mathrm{sf}} := \left\{ E \in \mathcal{E}' : \frac{\Delta(E)}{C(E)} \text{ is squarefree} \right\}.$$

Theorem (Shankar, S., Wang)

(a) *The asymptotics of $N_C(\mathcal{E}_{\mathrm{sf}}, X)$ are as predicted by the heuristics.*

(b) *The average size of the 2-Selmer groups of curves in $\mathcal{E}_{\mathrm{sf}}$ is 3.*

For Part (b) we need an average tail estimate on $\widetilde{N}_C(\mathcal{E}'_n, X)$, where the tilde indicates that the elliptic curves $E \in \mathcal{E}'_n$ are weighted by the size of $\mathrm{Sel}_2(E)$.

Our proof yields the following uniformity estimate on the set W_p of integer binary quartic forms corresponding to rings that are non-maximal at p, when they are ordered by height

$$\sum_{p>M} |\{f(x,y) \in GL_2(\mathbb{Z})\backslash W_p : H(f)\}| \ll_\epsilon X^{5/6}/M^{1-\epsilon}.$$

This is the expected optimal bound (up to X^ϵ), and would be useful in (for example) obtaining a secondary main term in the $|\mathrm{Sel}_2(E)|$ average.
The idea of the proof is to map these sets into lattices equipped with a group action, using the group action to bring the points "closer together", and then using geometry-of-numbers techniques.

Thank you!