A positive proportion of plane cubics fail/satisfy the Hasse principle

Notes by Tony Feng
for a talk by Manjul Bhargava

June 16, 2016

1 Introduction

Selmer (1951) showed that the plane cubic $3x^3 + 4y^3 + 5z^3$ has a $\mathbb{Q}_v$-point for all v but no $\mathbb{Q}$-point. This is the non-trivial element of the Tate-Shafarevich group of its Jacobian.

We are interested more generally in plane cubics that fail the Hasse principle (thus representing non-trivial elements of Tate-Shafarevich groups.

Question. How frequent are such failures of the Hasse principle among plane cubics?

More precisely, for an integral ternary cubic form f, define its height $h(f)$ to be the maximum of the absolute values of its coefficients. Let $N_{fail}(X)$ be the set of integral tenary cubic forms f with $h(f) < X$ such that f fails the Hasse principle and $N_{sol}(X)$ be the set of integral ternary cubic forms f with $h(f) < X$ such that f has a $\mathbb{Q}$-point. Let $N_{tot}(X)$ be the set of all integral ternary cubic forms with $h(f) < X$.

A cubic ternary form has 10 coefficients, so $N_{tot}(X) \sim (2X+1)^{10}$.

Question. Does the limit

$$\lim_{X\to\infty} \frac{N_{fail}(X)}{N_{tot}(X)}$$

exist, and if so then what is its value? What about

$$\lim_{X\to\infty} \frac{N_{sol}(X)}{N_{tot}(X)}?$$

This question is first stated (in print) by Poonen-Voloch. It was also considered by Swinnerton-Dyer.

Many seemed to have believed that among cubics locally soluble everywhere, either 100% or 0% should have rational points. I believed this until I disproved it.

Theorem 1.1 (B-Cremona-Fisher)**.**

$$\lim_{X\to\infty} \frac{N_{locsol}(X)}{N_{tot}(X)} = 97.256...\%$$

This means that it's basically the same to consider $N_{tot}(X)$ versus $N_{locsol}(X)$. The punchline is that a positive proportion of locally soluble cubics have a rational point, and a positive proportion don't.

Theorem 1.2. *We have:*

$$\liminf_{X\to\infty} \frac{N_{fail}(X)}{N_{tot}(X)} > 0$$

and

$$\liminf_{X\to\infty} \frac{N_{sol}(X)}{N_{tot}(X)} > 0.$$

2 Peliminaries

2.1 Average size of Selmer groups

Any elliptic curve $E/\mathbb{Q}$ can be expressed uniquely as

$$y^2 = x^3 + Ax + B$$

with $A, B \in \mathbb{Z}$ and no p has $p^4 \mid A, p^6 \mid B$.

Calling this $E_{A,B}$, we can define the "naive height" $H(E_{A,B}) = \max\{4|A|^3, 27|B|^2\}$.

Theorem 2.1 (B-Shankar)**.** *When $E/\mathbb{Q}$ are listed by naive height,*

1. *The average size of the 2-Selmer group is* 3.

2. *The average size of the 3-Selmer group is* 4.

3. *The average size of the 4-Selmer groups is* 7.

4. *The average size of the 5-Selmer group is* 6.

Idea of proof. Apply geometry of numbers to spaces of integral

1. binary quartic forms (a 2-torsion element of Sha is represented by a hyperelliptic curve $z^2 = f(x, y)$)

2. ternary cubic forms (a 3-torsion element of Sha is a plane cubic)

3. pairs of quaternary quadratic forms (a 4-torsion element of Sha is an intersection of two quadrics in $\mathbb{P}^3$)

4. quintuples (A, B, C, D, E) of 5×5 skew-symmetric matrices.

The strategy is to count equivalence classes of such forms, and then sieve to the locally soluble ones (which are Selmer elements). □

These results certainly imply that the rank is bounded, and in fact they are successively better.

1. The average of $2r(E)$ is bounded by the average of $2^{\text{rank}(E)}$, which is at most 3. So the average rank is at most $\frac{3}{2}$.

2. The average of $20r(E) - 15$ is bounded by the average of $5^{\text{rank}(E)}$, which is 6. So the average rank is at most $21/20$.

For 3-Selmer averages, you get a bound of $1 + 1/6$. So many 3-Selmer elements have a non-trivial map to Ш!

2.2 Digression

Theorem 2.2 (B-Shankar)**.** *The average rank of E is* ≤ 0.885*. This implies that a positive proportion (at least* 20%*) of elliptic curves have rank* 0*.*

By playing off these averages for 3 and 5, and using results of Skinner and Urban, we obtain:

Theorem 2.3 (B-Skinner)**.** *The average rank of E is* ≥ 0.216*. This implies that a positive propotion (at least* 20%*) of elliptic curves have rank* 1*.*

By work of Wiles, Gross-Zagier, Kolyvagin, if an elliptic curve has analytic rank ≤ 1 then we know that its Ш is finite.

Theorem 2.4 (B-Skinner-Zhang)**.** *At least* 66% *of elliptic curves have analytic rank* ≤ 1*.*

Corollary 2.5. *Most E have finite* Ш*.*

3 Results

Theorem 3.1. *A positive proportion of 3-Selmer elements of elliptic curves E ordered by* $H(E)$ *do not have a rational point.*

Proof. Suppose otherwise that 100% of 3-Selmer elements had rational points. Then the average size of the Selmer group would be the average size of $3^{\text{rank}(E)}$.

Then we would be forced to accept that

$$2 \times 3 = 2 \cdot avg(3^{\text{rank}(E)} - 1) \leq avg(5^{\text{rank}(E)} - 1) \leq 5$$

which is false. □

Theorem 3.2. *A positive proportion of 3-Selmer elements of elliptic curves have a rational point.*

Proof. The average size of 3-Selmer groups is bounded, but the average rank of E is positive, so the must contribute to the 3-Selmer rank a positive proportion of the time. □

4 Proof of main result

The key observation is that the action of $GL_3(\mathbb{Z})$ on integral ternary cubic forms has two polynomial invariants (i.e. the ring of invariants is a polynomial algebra on two generators) S and T (of degrees 4 and 6), which are the A and B of the Jacobian.

Theorem 4.1 (Cremona-Fisher-Stoll)**.** *There is a map*

$$\mathrm{Sel}_3(E_{A,B}) \hookrightarrow \{\textit{integral ternary cubic forms with invariants } S = A, T = B\} / \mathrm{GL}_3 \mathbb{Z}$$

So in the image of this map, a positive proportion have rational points and a positive proportion don't. This is almost the theorem, but there is an issue.

1. We need to know that the image is of positive density.

   This turns out to be true if you order the right side by naive height. This basically follows from the fact that over 97% of elements are locally soluble everywhere. You still have to show that most 3-Selmer elements have only one representative on the right hand side. (It's true over $\mathbb{Q}$, but the surprise is over $\mathbb{Z}$. This is achieved by sieving to show that most discriminants of ternary cubic forms are squarefree.)

2. We need to compare the naive height and the original notion of height. The two heights are not always compatible, but one can show that they are compatible for most (100% in some sense) ternary cubic forms. The reason is reduction theory: you can do a $GL_3(\mathbb{Z})$ translation to get the coefficients to be pretty small. (The fundamental domain has cusps, with many points, but you show that most of them correspond to the identity element.)

5 The methods of proof

In all of the arguments, it is clear what the right answer should be at every step. For instance, the parity conjecture and that the average size of Selmer is $\sigma(n)$.

So the method suggests:

Conjecture 5.1.

$$\lim_{X\to\infty} \frac{N_{fail}(X)}{N_{locsol}(X)} = \frac{2}{3}.$$

so

$$\lim_{X\to\infty} \frac{N_{sol}(X)}{N_{locsol}(X)} = \frac{1}{3}.$$

The analogous expectation for genus 1 curves in $\mathbb{P}^n$ is $\frac{\phi(n)}{2n}$.