3-DESCENT: THE SELMER GROUP OF ELLIPTIC CURVES $y^2 = x^3 - n^2$

Dongchen Zou under the instruction of Ariel Weiss

Ohio State University

Introduction

Consider the family of curves with cubic twists $E_n : y^2 = x^3 - n^2$, where n varies over positive cubefree integers. There is a 3-isogeny ϕ from E_n to $E'_n : y^2 = x^3 + 27n^2$, with its dual being $\hat{\phi}$.

We want to study the distribution of $\operatorname{rank}\operatorname{Sel}_\phi(E_n) = \dim_{\mathbb{F}_3}\operatorname{Sel}_\phi(E_n)$ in this family of curves. Stephanie Chan carried out the computation for the curves $y^2 = x^3 + n^2$ and we aim to adapt her method.

Key Steps

1. Find a workable description of the 3-Selmer group. More specifically, $\operatorname{Sel}_\phi(E_n)$ can be described as the subgroup of $H^1(G_\mathbb{Q}, E_n[\phi])$ of classes that are in the image of the local Kummer map

$$\kappa_p : E'_n(\mathbb{Q}_p) \to H^1(G_{\mathbb{Q}_p}, E_n[\phi])$$

for **every** place p of $\mathbb{Q}$. A lemma by Cohen and Puzuki allows us to equate this condition with the "everywhere locally solvability" of a polynomial.

2. Investigate the local solvability of the polynomial from Step 1.

3. (to be done) Explicitly construct the matrix, with the terms being cubic residues and characteristic functions, such that its kernel is the 3-Selmer group.

4. (to be done) Analyze the random matrix to get some conclusion of the distribution of $\operatorname{rank}\operatorname{Sel}_\phi(E_n)$.

Step 1 (Investigate the Local Kummer Maps on E'_n

Fix our equation of our curves to be $E_n : y^2 = x^3 - n^2$ and $E'_n : y^2 = x^3 + 27n^2$. Let $K = \mathbb{Q}(\sqrt{3})$ and let τ be the nontrivial element in $\operatorname{Gal}(K/\mathbb{Q})$ such that $\tau(\sqrt{3}) = -\sqrt{3}$.

Now, we will investigate the Kummer map at p, which we denote by κ_p. It maps elements from $E'_n(\mathbb{Q}_p)$ to the subgroup G_3 of K^*/K^{*3} of classes $[u]$ of elements u such that $\operatorname{N}_{K/\mathbb{Q}}(u) \in \mathbb{Q}^{*3}$. A lemma proved by Cohen and Pazuki describes the image of κ_p as follow:

An element $[u] \in K^*/K^{*3}$ belongs to the image of κ_p if and only if for some representative $u \in K^*$, the homogeneous cubic equation

$$u\left(X + 3\sqrt{3}Y\right)^3 + \tau(u)\left(X - 3\sqrt{3}Y\right)^3 + 2nZ^3 \tag{1}$$

has a nontrvial solution in $\mathbb{Q}_p$. Therefore,

$$\operatorname{Sel}_\phi(E_n) = \{u \in G_3 \mid (1) \textbf{ is ELS}\}$$

Intuition

"(1) is soluble in $\mathbb{Q}$" means that u is in the image of the descent map while "(1) is everywhere locally soluble" means that u is in the Selmer group. These two conditions are equivalent if and only if the Tate-Shafarevich group is trivial. This is because the Tate-Shafarevich group is a measure of the failure of the local-global principle. In particular, it measures the existence of u's that are everywhere locally soluble but not soluble globally.

Step 2 (Investigate When (1) is ELS)

When p splits

Since 3 is a quadratic residue mod p, Equation (1) has a solution iff $u_1X^3 + u_2Y^3 + u_3Z^3 = 0$ does, where $u_1 = u$, $u_2 = \tau(u)$, and $u_3 = 2n$.

By dividing and multiplying, we can assume, WLOG, that $\gcd(u_1, u_2, u_3) = 1$, $\min(v_p(u_1), v_p(u_2), v_p(u_3)) = 0$, and $v_p(u_1u_2u_3) \leq 2$. Lemma 2.3 in Chan's paper gives us a nice criterion: solvable iff one of the following is satisfied:

- $v_p(u_1u_2u_3) = 0$;
- $v_p(u_i) > 0$, and u_j/u_k is a cube in $\mathbb{F}_p^\times$, where $\{i, j, k\} = \{1, 2, 3\}$;

When p doesn't split, things get a little more complicated. We can assume that the u we are testing for is a cube. This allows us to write u as $u = v \cdot \operatorname{Nm}(v)$ where $v = v_1 + v_2\sqrt{3}$.

When p is inert

Combining Lemma 6.4 and Lemma 6.6 in Cohen and Puzuki, (1) is solvable iff

- $\frac{\tau(v)}{v}$ modulo p is a cube in $\mathbb{F}_{p^2}^\times$

Note that when I say $\alpha \equiv \beta \pmod p$, I mean that the class of α and β in the residue field is the same.

When p is ramified ($p = 2$ or $p = 3$)

First of all, (1) is always solvable in $\mathbb{Q}_2$.

By Lemma 6.11, we have that (1) is solvable in $\mathbb{Q}_3$ iff one of the following holds: Let $w = \frac{2n}{\operatorname{Nm}(v)}$.

- $v_3(w) = 0$
- $v_3(w) > 0$ and $v_3(v_2) > 0$
- $w \equiv \pm 6v_1 \pmod{27}$ for an appropriate choice of $\pm$.

Contact

Dongchen Zou: dongchen-zou0711@outlook.com

Ariel Weiss: weiss.742@osu.edu

Acknowledgment

I would like to first thank my mentor, Ariel Weiss, who has supported me immensely. This project would not be possible without him. I would also like to thank OSU Cycle and the organizers who made this amazing opportunity possible. Finally, I would like to thank my friends, like Michael and Celine, for their support over the past year.

Major References

1. Cohen, H. and F. Pazuki. "Elementary 3-descent with a 3-isogeny." Acta Arith. 140, 4 (2009), 369–404

2. Chan, S. "The 3-isogeny Seller groups of the elliptic curves $y^2 = x^3 + n^2$, Int. Math. Res. Not. IMRN (2024), no. 9, 7571–7593.

3. Bhargava, M., N. Elkies, and A, Shnidman. "The average size of the 3-isogeny Selmer groups of elliptic curves $y^2 = x^3 + k$", Journal of the London Mathematical Society (2019), 299–327.