On Selmer Ranks of Elliptic Curves With Rational 2-Torsion

Jafari M.M.

July 4, 2025

Outline

Hillbert's 10th Problem

Question

Given a number field k, is there any algorithm to determine whether a polynomial $f \in \mathbb{Q}[x_1, \ldots, x_n]$ admits a solution in k?

Answer

$k = \mathbb{Z} \rightarrow$ No. [Davis-Putnam-Robinson + Matiyasevich]
$k = \mathbb{Q} \rightarrow$ Yes in one variable, unknown in general.

Mordell-Weil Theorem

Theorem (Mordell-Weil-Faltings)

Given a variety C of genus g, the set $C(\mathbb{Q})$ is determined as

$g = 0 \to 0, \infty$

$g = 1 \to G \times \mathbb{Z}^r$

$g \geq 2 \to$ *finite*

We now focus on the case $g = 1$.

Elliptic Curves

Definition

An *elliptic curve* E over a number field k is a smooth, projective algebraic variety which in $Char(k) \neq 2, 3$ can be expressed as

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

It follows from the theorem above that $E/\mathbb{Q} \simeq E_{tors} \times \mathbb{Z}^r$

Selmer groups

Given two elliptic curves E, E' and isogenies φ, φ' we have

$$0 \longrightarrow E[\varphi] \longrightarrow E \longrightarrow E' \longrightarrow 0$$

which produces the exact sequence of Galois cohomology

$$0 \longrightarrow E'(k)/\varphi(E(k)) \xrightarrow{\delta_k} H^1(k, E[\varphi]) \longrightarrow H^1(k, E)[\varphi] \longrightarrow 0$$

where δ_k is the connecting homomorphism.
For each ν-adic completion of k we define the following groups

$$Sel^{\varphi}(E/k) = Ker\{H^1(k, E[\varphi]) \to \prod_{\nu} H^1(k_\nu, E)[\varphi]\}$$

$$Ш(E/k) = Ker\{H^1(k, E) \to \prod_{\nu} H^1(k_\nu, E)\}$$

Selmer groups

These two groups form the short exact sequence

$$0 \longrightarrow E'(\mathbb{Q})/\varphi(E(\mathbb{Q})) \longrightarrow Sel^{\varphi}(E/\mathbb{Q}) \longrightarrow Ш(E/\mathbb{Q})[\varphi] \longrightarrow 0$$

It holds that

$$rank(E/\mathbb{Q}) \leq dim_{\mathbb{F}_2} Sel^{\varphi}(E/\mathbb{Q}) + dim_{\mathbb{F}_2} Sel^{\varphi'}(E'/Q) - 2$$

Tamagawa ratios

Definition (Tamagawa ratio)

The ratio

$$T(E/E') = \frac{|Sel^{\varphi}(E/K)|}{|Sel^{\varphi'}(E'/K)|}$$

is called the *Tamagawa ratio* associated to isogenues curves.

In [KLO13,KLO14] the distribution of these ratios in isogenous families and quadratic twists is used to study the Selmer ranks.

Elliptic Curves with a 2-Torsion

Consider a family of curves E_r with a given 2-torsion point $(r, 0)$. Such family can be parametrized as

$$E_r : y^2 = x^3 + tx - rt - r^3$$

which after a translation $(r, 0) \mapsto (0, 0)$ becomes

$$E : y^2 = x^3 + 2rx^2 + (r^2 + t)x$$

equipped with an isogenous curve

$$E' : y^2 = x^3 - 6rx^2 - (3r^2 + 4t)x$$

Elliptic Curves with a 2-Torsion

Certain results are known about the average ranks of such families; in particular, we have the following

Theorem (Klagsburn-Lemke Oliver)

Given a family of elliptic curves with a 2-torsion, the rank $Sel_2(E/\mathbb{Q})$ grows with respect to the height of the family (e. g, the average is not a constant).

We would like to examine further the properties of Selmer group given r, t.

Connecting Homomorphisms and Selmer Groups

in [G02], two alogorithms are given for calculation of connecting homomorphisms δ_p and δ_2. These images are used coupled with the definition

$$S^{\varphi}(E/\mathbb{Q}) = \{x \in H^1(\mathbb{Q}, E[\varphi]) \mid res_p(x) \in Im(\delta_p) \text{ for all places } p\} \\ = \bigcap Im(\delta_p)$$

to describe the full Selmer group.

Algorithms for δ_p

In an elliptic curve $y^2 = x^3 + Ax^2 + Bx$, let
$a = ord_p(A), b = ord_p(B), d = ord_p(A^2 - 4B)$.
The algorithms deal with $b = 0, 1, 2, 3$ for all p, fully reproducing the Selmer groups.
We observe that in case $b \geq 1$ and $a \geq 2$, we have
$E : y = x^3 + pA'x + p^2B'x$ is a quadratic twist E^p, thus the algorithm above can recursively construct the Selmer group for higher cases omitted in the description.

Statistical Arguements for the Selmer ranks

Since the algorithm roughly implies a direct relation between upper bound of Selmer ranks and the order b, we can deduce the following upper bound for the p part of the image

$$sup(\delta_p) \sim \sum_{n=1}^{\infty} \frac{n}{p^n} = \frac{p}{(p-1)^2}$$

Adding all the contributions of primes p up to the naive height X of the curve family we get

$$sup(r) \sim \sum_{p \text{ prime}}^{X} \frac{p}{(p-1)^2} \sim \sum_{p}^{X} \frac{1}{p} \sim \log(\log(x))$$

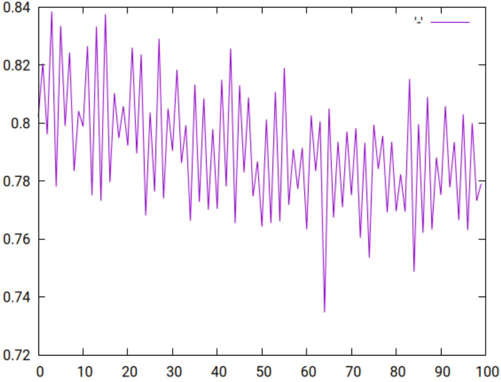
Statistical Arguments for the Selmer ranks

The observation above agrees with [KLO13] and [KK17], in which the distribution for Selmer ranks of quadratic twists is observed to fall in the normal distribution $N(0, \frac{1}{2}\log\log X)$, following different methods.

Other implications

Given the direct relation of orders, for the curve with 2-torsion at $(r, 0)$ we expect the highest relation with the order of 2 in r, as $ord_2(A) \geq 1$ is most likely to result in non-trivial Selmer group. We can observe this by taking the average rank for $0 < r \leq 100$ and $0 < t \leq 10,000$, plotted in the following figure

Plot for r



Citations

KLO13: THE DISTRIBUTION OF 2-SELMER RANKS OF QUADRATIC TWISTS OF ELLIPTIC CURVES WITH PARTIAL TWO-TORSION, Z. Klagsburn, R. Lemke Oliver
KLO14: THE DISTRIBUTION OF THE TAMAGAWA RATIO IN THE FAMILY OF ELLIPTIC CURVES WITH A TWO-TORSION POINT, Z. Klagsburn, R. Lemke Oliver
G02: A STUDY ON THE SELMER GROUPS OF ELLIPTIC CURVES WITH A RATIONAL 2-TORSION, T. Goto
KK17: ON THE JOINT DISTRIBUTION OF $Sel_{\varphi}(E/Q)$ AND $Sel_{\hat{\varphi}}(E/Q)$ IN QUADRATIC TWIST FAMILIES, D. Kane, Z. Klagsburn