KAZAKH MATHEMATICAL JOURNAL ISSN 1682–0525

25:3 (2025) 13–22

On Selmer Ranks of Elliptic Curves with a Rational 2-Torsion

Mohammad Mahdi Jafari

Al-Farabi Kazakh National University, Almaty, Kazakhstan

dzhafari_mokhammad_m@live.kaznu.kz

Communicated by: Viktor V. Verbovskiy

Received: 05.05.2025 ⋆ Accepted/Published Online: 03.07.2025 ⋆ Final Version: 30.05.2025

Abstract. This study investigates the asymptotic behavior of the ranks of Selmer groups associated with elliptic curves possessing a rational 2-torsion point defined over the integers. The Selmer group plays a central role in understanding the Mordell–Weil group and the Birch and Swinnerton-Dyer conjecture. The arithmetic of elliptic curves with torsion points has long attracted significant interest, with foundational results tracing back to the work of Mordell, Selmer, and later refinements by Cassels and others. In particular, the behavior of 2-Selmer groups provides insights into the distribution of ranks and the structure of rational points. Building upon previous methods developed for quadratic twists and leveraging tools from Galois cohomology, we demonstrate that the upper bounds on the size of these Selmer groups are unbounded within certain infinite families of elliptic curves. Our approach highlights the interplay between local conditions at primes and global properties of the curve, offering new perspectives on how torsion influences Selmer ranks.

Keywords: Elliptic Curves, Selmer groups, Galois Cohomology.

1 Introduction

Considering an elliptic surface

$$E_{A,B} : y^2 = x^3 + A(t)x + B(t) \text{ for } A, B \in \mathbb{Q}[t], deg(A, B) \leq 2$$

we investigate the rank of its fibers at particular values of t. Generally, it is known that for a rational elliptic surface with generic rank r_E, the subset of fibers with ranks $r_E + \{1, 2, 3\}$ is not thin. One might ask further questions about the average ranks of fibers and the method of computing the generators of the weak Mordell-Weil group. This task is carried out by computing the Selmer group.

2020 Mathematics Subject Classification: 11G05; 14H52; 14G05.

DOI: https://doi.org/10.70474/sqw8ys05

We begin by marking the families of elliptic curves by a 2-torsion point $(\frac{r}{h^2}, 0)$ and their isogeneus family of curves. We consider the families

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

With $h = 1$, e.g, integral torsion points, and translating the torsion to $(0, 0)$ we get the family

$$E : Y^2 = X^3 + 2rX^2 + (t^2 + r^2)X$$

and the natural isogeny at the point $(r, 0)$.

The main objective of this work is to demonstrate the following:

Theorem 1. *The upper bound of the Selmer rank for a family of elliptic curves with a rational 2-Torsion up to naive height X is* $\log \log X$

In recent years, several authors, most notably Klagsbrun et. al. [6], [8], have studied the average behavior and distribution of Selmer ranks in families of elliptic curves, often using Tamagawa ratios by the matrix construction described by Monsky in appendix of [5]. In this work, we propose a direct and elementary argument showing that the upper bound of the Selmer ranks in a family of elliptic curves with rational 2-torsion grows like $\log \log X$, relying on local Galois cohomology and the probabilistic distribution of twists and local images, as laid out in [4]. Another approach to the construction of Selmer groups is the graph theoretical method described in [2], [3] in which methods of graph theory are used to describe the Selmer groups. The same method is used in [9] over $\mathbb{Q}(i)$. A notable similarity in most of these works is the focus on an special case of this problem for the curves

$$E : y^2 = x^3 - nx$$

either focusing on the case where n is an square, or general case as in [9]. Our aim is for higher generality in this case, but we note that setting $r = 0$ gives the same curve here.

2 Selmer Groups

For a variety A and a number field k with a set of places ν, we denote by $A(k_\nu)$ the set of points on A in the ν-completion of k. Let

$$H^i(k, A) := H^i(Gal(\bar{k}/k), A/k)$$

denote the Galois cohomology classes of A, in particular,

$$A(k) = H^0(k, A)$$

is the set of k-rational points on A.

The Tate-Shafarevich group is defined as

$$\underset{A/k}{Ш} = ker(H^1(k, A) \to \prod_{\nu} H^1(k_\nu, A))$$

such that the non-trivial elements correspond to homogeneous spaces (also called k-torsors) measuring the failure of Hasse principal. Conjecturally, this value is finite. This is only known to hold for the class of elliptic curves with a zero of order at most one at $L(E/\mathbb{Q}, 1)$, or curves of rank ≤ 1 given that the BSD conjecture is proven for all such curves.

For an isogeny of elliptic curves, we have the following sequence

$$0 \longrightarrow E(k)[\varphi] \longrightarrow E(\bar{k}) \longrightarrow E'(\bar{k}) \longrightarrow 0$$

where $E(k)[\varphi]$ is the kernel of isogeny. Applying Galois cohomology gives us

$$0 \longrightarrow E(k)[\varphi] \longrightarrow E(k) \longrightarrow E'(k) \longrightarrow$$

$$H^1(k, E[\varphi]) \longrightarrow H^1(k, E) \longrightarrow H^1(k, E') \longrightarrow \dots$$

Now, setting $\varphi = m$, the multiplication by m map and rewriting the sequence we get

$$0 \longrightarrow E(k)/mE(k) \xrightarrow{\delta} H^1(k, E[m]) \longrightarrow H^1(k, E)[m] \longrightarrow 0$$

which we can restrict at each place ν to get

$$0 \longrightarrow E(k_\nu)/mE(k_\nu) \xrightarrow{\delta_\nu} H^1(k_\nu, E[m]) \longrightarrow H^1(k_\nu, E)[m] \longrightarrow 0.$$

The Selmer group is defined as the kernel

$$Sel^m(E/k) = ker(H^1(k, E[m]) \to \prod_{\nu} H^1(k_\nu, E)/\delta_\nu(E'(K)/mE(K)))$$

of the mapping of m-torsion of the first Galois cohomology group to its restriction in all places. In this way, we get the exact sequence

$$0 \longrightarrow E(k)/mE(k) \longrightarrow Sel^m(E/k) \longrightarrow \underset{E/k}{Ш}[m] \longrightarrow 0.$$

In [4], an algorithm is given for computing the connecting homomorphisms δ_p and δ_2. These images are used coupled with the definition

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

to describe the full Selmer groups for each elliptic curve. A full description of the Selmer group gives an upper bound on the rank of the elliptic curves as we have

$$rank(E) = dim_{F_2} Sel^{\varphi}(E/\mathbb{Q}) + dim_{F_2} Sel^{\varphi'}(E'/\mathbb{Q}) - dim_{F_2}\, Ш(E/\mathbb{Q})[\varphi] - dim_{F_2}\, Ш(E'/\mathbb{Q})[\varphi'] - 2 \quad (1)$$

from which it follows that

$$rank(E) \leq dim_{F_2} Sel^2(E/\mathbb{Q}) + dim_{F_2} Sel^2(E'/\mathbb{Q}) - 2 \quad (2)$$

relating the rank of elliptic curve to the dimension of the 2-Selmer group spanned as an $\mathbb{F}_2$ vector space. In particular, if the Tate-Shafarevich group is trivial, the two sides will be equal. We refer to the right side of (2) as the *Selmer rank* of the curve E. In the next section. The algorithm given in [4] is reproduced, which we will use as the basis for our argument.

2.1. Prior Results

The problem of understanding the distribution of Selmer ranks in large families of elliptic curves has attracted significant attention in recent years. Bhargava and Shankar have shown in a series of foundational works that, in large enough families of elliptic curves ordered by height, the average size of 2-Selmer groups is bounded. Specifically, in [12], they establish that the average size of the 2-Selmer group across all elliptic curves over $\mathbb{Q}$ is exactly 3, and in [11], for families with a marked 2-torsion point, the average rises to 6. These results suggest that, for a majority of curves, the Mordell–Weil rank is either 0 or 1, though they do not resolve the Birch and Swinnerton-Dyer conjecture in individual cases.

The behavior in more constrained families, particularly those with prescribed torsion structures, is subtler. In [13], Xiong investigates a specific one-parameter family

$$E_n : y^2 = x^3 - n^3,$$

showing that the average size of the 2-Selmer group grows slowly, approximately as

$$\sqrt{\frac{1}{2}\log\log X}$$

as $n \leq X$. A more general result appears in [6], where Klagsbrun and Lemke-Oliver demonstrate that the 2-Selmer rank in families of quadratic twists of curves with a marked 2-torsion point can grow arbitrarily large. Their proof relies on studying the Tamagawa ratio between a curve E and its 2-isogenous partner E',

$$T(E/E') = \frac{|\mathrm{Sel}_{\varphi}(E)|}{|\mathrm{Sel}_{\varphi'}(E')|},$$

and evaluating its 2-adic valuation across quadratic twists E^χ. The growth is controlled by local cohomological invariants at primes dividing 2, the discriminants Δ, Δ', and infinity:

$$\operatorname{ord}_2 T(E^\chi/E'^\chi) = g(\chi) + \sum_{\nu|2,\Delta,\infty} \left(\dim_{\mathbb{F}_2} H^1_\varphi(K_\nu, E[\varphi]) - 1\right),$$

where $g(\chi)$ involves average Legendre symbols over ramified primes.

In a follow-up work [7], they show that the distribution of Selmer ranks across such families of twists has mean 0 and variance $\log\log X$, and they deduce that arbitrarily high Selmer ranks occur infinitely often. However, these results apply specifically to twist families and depend crucially on analyzing the variation of the Tamagawa ratio.

The present work differs in both setting and method. We consider a static family of elliptic curves over $\mathbb{Q}$ with a rational point of order 2 at the origin, not twists. We demonstrate that even without extension to quadratic fields, the Selmer rank can exhibit unbounded growth, and that the average rank exhibits logarithmic fluctuation. While our local analysis uses similar cohomological terms, such as the local image under the Kummer map δ_ν, our method is based on direct reduction and descent calculations adapted from Goto [4], rather than Tamagawa ratios or isogeny-based arguments.

Moreover, while [6] suggests a $\sqrt{\log X}$ average size of individual Selmer groups in such families, no published proof of this claim appears in their later work [8], which instead focuses on Cohen–Lenstra-type distributions for Selmer group structures given fixed rank. As such, the present work contributes a distinct perspective on the problem by re-analyzing the growth of 2-Selmer ranks directly over $\mathbb{Q}$, using concrete local-global computations without relying on isogeny decompositions or twist families.

3 Algorithm for Computation of the Selmer Group

We now reproduce the algorithm given in [4] to compute the Selmer groups. We note here that the images of the connecting homomorphisms δ_p and δ'_p are orthogonal with the $(,)_p$ Hillbert symbol, such that for all $x \in \delta_p, y \in \delta'_p$ we have $(x,y)_p = 1$.

In the following section, we have the curve

$$E : y^2 = x^3 + Ax^2 + Bx$$

with values

$$a = Ord_p(A), b = Ord_p(B), d = Ord_p(A^2 - 4B)$$

and $\left(\frac{a}{p}\right)$ denoting the Legendre symbol, and u is a non-square modulo p. We have the following cases

1. $b = 0$:

(a) $2|d$ and $\left(\frac{-2A}{p}\right) = -1 \to Im(\delta_p) = \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2}$

(b) otherwise $Im(\delta_p) = \{1\}$

2. $b \neq 0$:

(a) $a = 0$:

i. $2|b$ and $\left(\frac{A}{p}\right) = -1 \to Im(\delta_p) = \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2}$.

ii. otherwise $Im(\delta_p) = \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$.

(b) $a \neq 0$:

i. $b = 1 \to Im(\delta_p) = \langle B \rangle$.

ii. $b = 2, a = 1$: let $A = pA', B = p^2B'$, and $\alpha = \left(\frac{A'^2 - 4B'}{p}\right), \beta = \left(\frac{A' + 2\sqrt{B'}}{p}\right)$ with $\sqrt{B'}$ denoting the p adic square root:

A. $\alpha = 0 \to Im(\delta_p') = \langle 2A, A'2 - 4B \rangle$.

B. $\alpha = -1 \to Im(\delta_p) = \langle B \rangle$.

C. B' is not a square in $\mathbb{Q}_p \to Im(\delta_p) = \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$.

D. $\beta = 1 \to Im(\delta_p') = \langle p \rangle$.

E. $\beta = 1 \to Im(\delta_p') = \langle pu \rangle$.

(c) $b = 2, a \geq 2$:

i. $-B$ is not a square in $\mathbb{Q}_p \to Im(\delta_p) = \langle B \rangle$.

ii. $p \equiv 3 \bmod 4 \to Im(\delta_p) = \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$.

iii. $p \equiv 1 \bmod 4 \to Im(\delta_p) = \langle p \rangle, \langle pu \rangle$ depending on whether the quartic character of $-B$ in p is 1 or -1.

(d) $b \geq 3, a = 1 \to Im(\delta_p) = \langle B \rangle$.

(e) $b = 3, a \geq 2 \to Im(\delta_p) = \langle -A, B \rangle$.

The algorithm concludes here. For δ_2, the algorithm is similar, but produces, on average, larger groups. The algorithm can be simplified by making use of quartic characters, as in [9].

4 Main Theorem

Let $F(X)$ denote the family of elliptic curves of bounded height:

$$F(X) = \{E_{A,B} : h(E_{A,B}) < X\}$$

where the height function is defined by

$$h(E) = \max(3A^3, 27B^2).$$

We are concerned with the behavior of the 2-Selmer rank $S(E)$ for $E \in F(X)$. Recall that the algorithms described in the previous section define local connecting homomorphisms δ_p and their duals δ'_p, which are orthogonal. These maps capture the image of $E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)$ in $H^1(\mathbb{Q}_p, E[2])$, and their interaction across all primes controls the dimension of the 2-Selmer group.

Now consider a curve of the form:

$$E : y^2 = x^3 + pA'x^2 + p^2B'x,$$

which is a quadratic twist of the curve

$$E_p : y^2 = x^3 + A'x^2 + B'x.$$

This twist relation implies that the local images at p can be heuristically related, and in particular, the twisting by p modifies the Selmer rank by introducing or removing local obstructions.

We model the expected size of the image of each local connecting homomorphism δ_p by:

$$\mathbb{E}[|\delta_p|] \approx \sum_{n=1}^{\log X} \frac{n}{p^n} \approx \frac{p}{(p-1)^2} \sim \frac{1}{p},$$

where the last approximation holds in the limit as $X \to \infty$. That is, the expected contribution to the Selmer rank from each prime p behaves like $1/p$.

Summing over all primes $p \leq X$, the total expected Selmer rank satisfies:

$$\mathbb{E}[S(F(X))] \approx \sum_{p \leq X} \frac{1}{p} \sim \log\log X.$$

Possible overlaps (i.e., dependencies between local conditions at different primes) contribute correction terms of order $\sum_{p \neq q} \frac{1}{pq}$, which is convergent and thus does not affect the asymptotic growth. Therefore, we obtain:

$$\mathbb{E}[S(F(X))] \sim \log\log X,$$

which completes the proof of Theorem 1.

This heuristic matches the behavior observed in the works of Klagsbrun–Lemke Oliver [6], [7] and Klagsbrun–Kane [8], who study the distribution of 2-Selmer ranks via Tamagawa ratios and show that the average and variance of Selmer ranks grow like $\log\log X$.

5 Conclusion

Firstly, we point out the relevance of this to Birch and Swinnerton-Dyer (BSD) conjecture. Recall that the BSD claims:

Claim 2. The order of zero of the L-function $L(E, s)$ associated to an elliptic curve E at $s = 1$ is equal to its rank; further, the first nonzero coefficient of the Taylor series associated to this point is

$$L_1 = \frac{|Ш(E)|\Omega_E R_E c_E}{|E_{Tors}|^2},$$

where Ω_E, R_E and c_E are constants related to the curve.

This result shows the growth of Selmer ranks for this family of elliptic curves. From the equation (1) we see that this result, together with a study of the growth of Tate-Shafarevich group could lead to the exact calculation of the above value for the L-functions, for further testing the validity of the claim in the case of this family. Moreover, this result can help to solve the following open problem by providing counterexamples.

Problem 3. Does there exist $B \in \mathbb{Z}$ such that for all elliptic curves E over $\mathbb{Q}$, one has $rank(\mathbb{Q}) \leq B$?

We note that, in light of results such as [12] and [11], the vast majority of elliptic curve families exhibit bounded average Selmer ranks, making them unlikely sources of counterexamples to bounded rank conjectures. In contrast, families with unbounded Selmer rank, such as the one examined here, become natural candidates for detecting potential violations. In this context, one of two conclusions must hold: either the Mordell–Weil rank becomes unbounded in such families, or the Tate–Shafarevich group $Ш(E)$ absorbs the excess growth. The latter scenario raises a distinct and unresolved problem of its own, as no general algorithm exists for computing $Ш(E)$, and its behavior in large families over $\mathbb{Q}$ remains poorly understood.

The general consensus is in favor of this, for example, as in [10]. We see that in this case the boundedness of the rank would imply that the Tate-Shafarevich group also grows without bounds. There are methods for studying this problem, as in [1], but it remains for future undertakings to apply these to this particular family strictly over $\mathbb{Q}$.

6 Acknowledgment

I express my sincere gratitude to Professor Simon Serovajsky for his constant support.

References

[1] Shiga, A. *Behaviors of the Tate-Shafarevich group of elliptic curves under quadratic field extensions*, Arxiv (unpublished) 2411.12316, 2024.

[2] Feng, K. *on-congruent numbers, odd graphs and the Birch-Swinnerton-Dyer conjecture*, Acta Arith. 80, 71–83, 1996.

[3] Feng, K., Xiong, M. *On Selmer groups and Tate-Shafarevich groups for elliptic curves* $y^2 = x^3 - n^3$, Mathematika 58, no. 2, 236–274, 2012.

[4] Goto, T. *A study on the Selmer groups of elliptic curves with a rational 2-torsion*, Kyushu University Doctoral Thesis, 2002.

[5] Heath-Brown, D. R. *The size of Selmer groups for the congruent number problem. II*, Invent. Math., 118, 331–370, 1994.

[6] Klagsburn, Z., Lemke-Oliver, R. *The distribution of 2-Selmer ranks of quadratic twists of elliptic curves with partial two-torsion*, Mathematika, 2013.

[7] Klagsburn, Z., Lemke-Oliver, R. *The distribution of the Tamagawa ratio in the family of elliptic curves with a two-torsion point*, Res. Math. Sci., 1:15.

[8] Kane, D., Klagsburn, Z. *On the Joint Distribution Of* $Sel_\phi(E/Q)$ *and* $Sel_\phi(E'/Q)$ *in Quadratic Twist Families*, Arxiv (unpublished) 1702.02687, 2017.

[9] Kling, A., Savoie, B. *Computing Selmer group for elliptic curves* $y^2 = x^3 + bx$ *over* $Q(i)$, Arxiv (unpublished) 2410.22714, 2024.

[10] Park, J., Poonen, B., Voight, J., Matchett Wood, M. *A heuristic for boundedness of ranks of elliptic curves*, J. Eur. Math. Soc. 21:9, pp. 2859–2903, 2019.

[11] Bhargava, M., Ho, W. *Coregular spaces and genus one curves*, Cambridge J. Math., 4:1, pp. 1-119, 2016.

[12] Bhargava, M., Shankar, A. *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Annals of Math., 181:1, pp. 191-242, 2015.

[13] Xiong, M. *On Selmer groups of quadratic twists of elliptic curve a two-torsion over* $\mathbb{Q}$, Mathematika, 2013.

Джафари М. М. РАЦИОНАЛ 2-ТӘРТІПТІ НҮКТЕСІ БАР ЭЛЛИПТИКАЛЫҚ ҚИСЫҚТАРДЫҢ СЕЛЬМЕР РАНГЫ ТУРАЛЫ

Бұл зерттеуде бүтін сандар үстінде анықталған рационал 2-ретті кручениесі бар эллиптикалық қисықтарға сәйкес келетін Сельмер топтарының рангісінің асимптотикалық қасиеттері қарастырылады. Сельмер тобы Морделль–Вейль тобы мен Бёрч — Свиннертон-Дайер болжамын зерттеуде маңызды рөл атқарады. Кручение нүктелері бар эллиптикалық қисықтардың арифметикасы ұзақ уақыт бойы ғалымдардың назарында болып келді. Бұл салада алғашқы нәтижелер Морделль мен Сельмердің еңбектерінен басталып, кейін Касселс және басқа зерттеушілер тарапынан дамытылды. Әсіресе, 2-Сельмер топтары рационал нүктелердің құрылымын және рангісінің таралуын тереңірек түсінуге мүмкіндік береді. Квадраттық твисттер үшін жасалған әдістерге сүйене отырып және Галуа когомологиясының құралдарын пайдалана отырып, біз осындай топтардың өлшемінің жоғарғы бағасы кейбір шексіз эллиптикалық қисықтар отбасында шектел-

мейтінін көрсетеміз. Жұмыста жай сандардағы локал шарттар мен қисықтың глобал қасиеттерінің байланысы айқындалып, крученинің Сельмер тобына әсері талданады.

Түйін сөздер: эллиптикалық қисықтар, Сельмер топтары, Галуа когомологиясы.

Джафари М. М. О РАНГАХ СЕЛЬМЕРА ЭЛЛИПТИЧЕСКИХ КРИВЫХ С РАЦИОНАЛЬНОЙ ТОЧКОЙ ПОРЯДКА 2

В данной работе исследуется асимптотическое поведение рангов групп Сельмера, ассоциированных с эллиптическими кривыми, обладающими рациональной 2-кручением, определённой над целыми числами. Группа Сельмера играет ключевую роль в изучении группы Морделля–Вейля и гипотезы Бёрча — Свиннертона-Дайера. Арифметика эллиптических кривых с точками кручения давно привлекает внимание, начиная с классических результатов Морделля и Сельмера и последующих усовершенствований Касселсом и другими исследователями. В частности, 2-группы Сельмера позволяют глубже понять распределение рангов и структуру рациональных точек. Опираясь на ранее разработанные методы, применимые к квадратичным твистам, и используя аппараты когомологии Галуа, мы показываем, что верхние оценки размеров таких групп не ограничены в определённых бесконечных семействах эллиптических кривых. Подход подчёркивает взаимосвязь локальных условий в простых числах и глобальных свойств кривой, раскрывая влияние кручения на структуру групп Сельмера.

Ключевые слова: эллиптические кривые, группы Сельмера, когомология Галуа.