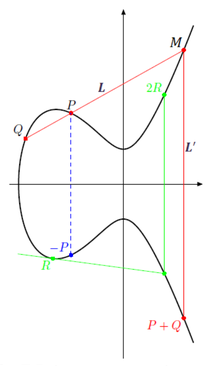
A Study on a Family of Elliptic Curves of Rank at Least Two

Pankaj Patel
Advisor: Prof. Debopam Chakraborty
Birla Institute of Technology & Science, Pilani-Hyderabad Campus, India

1. Introduction



Elliptic Curves: An **elliptic curve** over a field K is a nonsingular projective curve of genus one together with a distinguished point $\mathcal{O}$. It can be represented by a Weierstrass equation

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_i \in K$, whose discriminant is nonzero. Over a field of characteristic different from 2 and 3, every elliptic curve is isomorphic to one in the short Weierstrass form

$$y^2 = x^3 + ax + b, \qquad 4a^3 + 27b^2 \neq 0.$$

The set of K-rational points $E(K)$ forms an abelian group with identity element $\mathcal{O}$.

Rank of an Elliptic curve: The set of rational points on E is denoted by $E(\mathbb{Q})$. By the Mordell–Weil theorem,

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r.$$

for some integer $r \geq 0$. Here $E(\mathbb{Q})_{\text{tors}}$ is called the torsion group of E and the integer r, also referred to as $r(E)$, is called the Mordell-Weil rank of E.

2. Family of Elliptic Curves

We study the family of Elliptic curves

$$E_{m,t} : y^2 = x^3 + m^2x^2 - t^2x,$$

where

$$m^2 = 3t^2 + 1.$$

Key observations:

- $E_{m,t}(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$.
- Two explicit rational points are
$$P_1 = (t, mt), \qquad P_2 = (-1, 2t).$$
- For every Pell solution (m, t),
$$\text{rank}(E_{m,t}(\mathbb{Q})) \geq 2.$$
- The Pell equation
$$m^2 - 3t^2 = 1$$
has infinitely many integer solutions, producing infinitely many curves in the family.

3. Doubling Formula and Degree Growth

Using the duplication formula

$$x([2]P) = \frac{(x^2 + t^2)^2}{4y^2},$$

one finds

$$x([2]P_1) = \frac{t^2}{m^2} = \frac{m^2 - 1}{3m^2},$$
$$x([4]P_1) = \frac{m^8 + 2m^4t^2 + t^4}{4m^2t^2},$$
$$x([8]P_1) = \frac{m^{32} + 8m^{28}t^2 + \cdots}{16(m^{26}t^2 + \cdots)}.$$

Thus the growth of degrees for P_1 is

$$a_N = 2 \cdot 4^{N-1} = \frac{4^N}{2}.$$

For P_2, one similarly computes

$$b_N = 4^N.$$

For the sum $P_1 + P_2$, the degrees grow as

$$c_N = 5 \cdot 4^N.$$

4. Canonical Height

The canonical heights are computed from the degree growth of the x-coordinates of the multiples $[2^N]P$.
The canonical height is defined by

$$\hat{h}(P) = \frac{1}{2} \lim_{N\to\infty} \frac{H([2^N]P)}{4^N}.$$

where

$$H([2^N]P) = \log(m^{4^N \cdot k} + g(m, t))$$

For the constructed points,

$$\hat{h}(P_1) = \frac{1}{4}, \qquad \hat{h}(P_2) = \frac{1}{2}, \qquad \hat{h}(P_1 + P_2) = \frac{5}{2}.$$

5. Néron–Tate Height Pairing

The bilinear height pairing satisfies

$$\langle P, Q\rangle = \hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q).$$

Thus,

$$\langle P_1, P_1\rangle = 2\hat{h}(P_1) = \frac{1}{2},$$
$$\langle P_2, P_2\rangle = 2\hat{h}(P_2) = 1,$$
$$\langle P_1, P_2\rangle = \frac{5}{2} - \frac{1}{4} - \frac{1}{2} = \frac{7}{4}.$$

The height matrix is

$$H = \begin{pmatrix} \frac{1}{2} & \frac{7}{4} \\ \frac{7}{4} & 1 \end{pmatrix},$$

with determinant

$$\det(H) = -\frac{41}{16} \neq 0.$$

Hence P_1 and P_2 are linearly independent and so

$$\text{rank}(E_{m,t}(\mathbb{Q})) \geq 2.$$

6. Conclusion

- Two explicit rational points on each curve were identified.
- Canonical height computations and the Néron–Tate height pairing establish that these points are linearly independent.
- Consequently, every curve in the family satisfies
$$\text{rank}(E_{m,t}(\mathbb{Q})) \geq 2.$$
- This family provides infinitely many elliptic curves over $\mathbb{Q}$ with Mordell–Weil rank at least two.

7. Future Work

- Determine the exact Mordell–Weil rank of the family.
- Construct additional independent rational points of infinite order.
- Study the 2-Selmer and Shafarevich - Tate groups.

8. Acknowledgement

I gratefully acknowledge the support of the **Department of Mathematics, BITS Pilani Hyderabad Campus**. I sincerely thank my Advisor, **Prof. Debopam Chakraborty**, for his guidance and encouragement. I also thank the organizers of **CAVARET 2: "Curves, Abelian VArieties and RElated Topics"** for the opportunity to present this work and for their generous support. Computations were carried out using **SageMath**.

9. References

[1] Patel, P., Chakraborty, D., and Chattopadhyay, J., *On the Mordell–Weil Rank and 2-Selmer Group of a Family of Elliptic Curves*, The Ramanujan Journal, 69(2), 2026.
[2] Silverman, J. H., *The Arithmetic of Elliptic Curves*, 2nd ed., Springer, 2009.
[3] Silverman, J. H., *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, 1994.
[4] Washington, L. C., *Elliptic Curves: Number Theory and Cryptography*, 2nd ed., Chapman & Hall/CRC, 2008.