Study Group on Mazur's Torsion Theorem

Lucie Gatzmaga Haoran Liang Jenny Roberts

May 11, 2026

Introduction

An important problem in number theory is to understand the set of rational points of an algebraic curve C. Much progress has been made on this problem over the last century, beginning with the trichotomy of algebraic curves depending on the genus of the curve, g. Assuming $C(\mathbb{Q}) \neq \emptyset$, we have the following:

- if $g = 0$: C is isomorphic to $\mathbb{P}^1$ and therefore has infinitely many rational points;
- if $g = 1$: $C(\mathbb{Q})$ is a finitely generated abelian group (due to Mordell [Mor22]);
- if $g \geq 2$: $C(\mathbb{Q})$ is finite (proven by Faltings [Fal83]).

Let $E/\mathbb{Q}$ be an elliptic curve, then Mordell's theorem tells us that $E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$. In order to understand $E(\mathbb{Q})$, we can break this down into understanding the rank r and the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$. Very little is known about the possible values of the rank. The current largest known rank was found in 2020 by Elkies and Klagsbrun [EK20], where they gave an example of an elliptic curve with rank $r \geq 29$. On the other hand, we have a very good understanding of the torsion subgroup thanks to the following result of Mazur in his seminal work *Modular curves and the Eisenstein ideal* [Maz77]:

Theorem 1 (Mazur's torsion theorem)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following 15 groups:*

- $\mathbb{Z}/n\mathbb{Z}$ *for* $1 \leq n \leq 10$ *or* $n = 12$,
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ *for* $n = 2, 4, 6, 8$.

The goal of this study group will be to understand the proof of Mazur's theorem and then, if time permits, to see how Mazur's Eisenstein ideal paper has influenced various areas in current number theory research.

Mainly, our focus will be on proving the following problem, which is the hardest part of the proof of Mazur's theorem:

Theorem 2. *Let $N > 7$ be a prime, then no elliptic curve $E/\mathbb{Q}$ has a rational point of order N.*

The proof of Theorem 2 can be broken down into three main steps.

Step 1. A criterion relating the non-existence of order-N point of an elliptic curve to the existence a certain rank zero abelian variety.

Consider the algebraic curve $Y_1(N)/\mathbb{Q}$, whose complex points are parametrised by pairs (E, P), where $E/\mathbb{C}$ is an elliptic curve and $P \in E$ is a point of order N. Furthermore, $Y_1(N)(\mathbb{Q})$ is given by the set of pairs (E, P) for which E is defined over $\mathbb{Q}$ and $P \in E(\mathbb{Q})$. So, the proof of Theorem 2 boils down to showing $Y_1(N)(\mathbb{Q})$ is empty for $N > 7$ prime.

We study $Y_1(N)$ by considering the slightly easier algebraic curve $Y_0(N)/\mathbb{Q}$. $Y_0(N)$ parametrises pairs of points (E, G) where $E/\mathbb{C}$ is an elliptic curve and $G \subset E$ is a cyclic subgroup of order N. We have a natural map $Y_1(N) \to Y_0(N)$ by taking G to be the subgroup generated by the point P. We can compactify $Y_0(N)$ by adding two points 0 and ∞ which we call the cusps. The compactified curve is denoted by $X_0(N)$. We then have the following result.

Theorem A. *Suppose $N > 7$ is a prime and there exists an abelian variety $A/\mathbb{Q}$ together with a morphism $f : X_0(N) \to A$ with the following properties:*

- *A has good reduction away from N,*
- *$f(\infty) \neq f(0)$,*
- *$A(\mathbb{Q})$ has rank 0.*

Then no elliptic curve over $\mathbb{Q}$ has a rational N-torsion point.

Step 2. A criterion ensuring that an abelian variety has rank 0.

To apply Theorem A, we must construct such an abelian variety and verify it satisfies the conditions of the theorem. The most difficult of these is to verify the rank zero condition. For this, we will prove the following criterion.

Theorem B. *Let $A/\mathbb{Q}$ be an abelian variety and let N and p be distinct primes with N odd. If we have the following conditions:*

- *A has good reduction away from N,*
- *A has completely toric reduction at N,*
- *The Jordan–Hölder constituents of $A[p](\overline{\mathbb{Q}})$ are one dimensional and either trivial or cyclotomic.*

Then $A(\mathbb{Q})$ has rank 0.

Step 3. Constructing the abelian variety using the Eisenstein ideal.

The abelian variety A will be a quotient of the Jacobian $J_0(N)$ of $X_0(N)$. Viewing $X_0(N)$ as a modular curve, we obtain a family of Hecke operators on $J_0(N)$, which generate a commutative ring of operators called the Hecke algebra. One then constructs A by taking a specific ideal in the Hecke algebra, called the Eisenstein ideal, and the corresponding quotient on $J_0(N)$. We can then verify that the abelian variety A satisfies all the conditions of Theorem A and B.

This only works if $N > 13$ so the cases $N = 11$ and $N = 13$ are shown separately using results of Billing–Mahler [BM40] and Mazur–Tate [MT73] respectively, this then completes the proof of Theorem 2. The remaining part of the proof of Theorem 1 involves a case by case verification of all remaining possible torsion subgroups.

The study group is organised as follows:

- In talks 2-3 we will cover most of the necessary background in order to prove theorems A and B. This will include studying elliptic curves over DVRs, groups schemes and Néron models.
- In talks 4-5 we will cover some background on modular curves and Jacobians as well as the proofs of Theorem A (talk 4) and Theorem B (talk 5).
- In talks 6-7 we will introduce the Hecke algebra and define and study some properties of the Eisenstein ideal.
- In talks 8-9 we will finish off the proof of Mazur's torsion theorem.
- In talk 10 we will see how Mazur's results have influenced recent developements in number theory (i.e. rational points on modular curves, $R = T$ theorems and Eisenstein congruences).

Schedule

Talk 1. Overview (29/04) – Netan

Talk 2. (Admissible) group schemes (06/05) – Shin Thant

Review the basic theory of group schemes, with a focus on étale and finite flat group schemes. State Raynaud's theorem ([Sno13], Lecture 7) on uniqueness of prolongations for finite group schemes over $K/\mathbb{Q}_p$ with ramification degree $< p-1$. Introduce admissible group schemes, explain why we need fppf cohomology, and sketch a proof of the key inequality

$$h^1(G) - h^0(G) \leq \delta(G) - \alpha(G),$$

in Lecture 11 of [Sno13]. You may find Tate's article [Tat97] and Conrad's notes [Con04] helpful.

Talk 3. Abelian varieties, Jacobians, and their Néron models (13/05) – Naina

Recall some basics of abelian varieties (Lectures 3-4 of [Sno13]) as well as Weil's construction of the Jacobian (Lecture 10 of [Sno13] or Chapter III of [Mil08]). Introduce the theory of Néron models for elliptic curves and explain how this theory extends to abelian varieties (Lecture 9 of [Sno13] or Chapter IV of [Sil94]). State the Ogg–Néron–Shafarevich criterion and Grothendieck's generalization. If time permits, define toric reduction and prove that it is preserved under taking quotients, using for instance [PR16].

Talk 4. Modular curves and the proof of Theorem A (20/05)

For the first part of the talk, very briefly review some basics of complex analytic and algebraic modular curves, for instance consulting Lecture 12, 14-15 of [Sno13]. In particular, discuss moduli interpretation of modular curves and their representability for $\Gamma(N)$, $\Gamma_1(N)$, as well as $\Gamma_0(N)$ level structures. Explain how to compactify modular curves using generalised elliptic curves. Consult Diamond and Im's survey article [DI95] or the classic book by Katz and Mazur [KM85] if necessary.

For the second part, state and prove Theorem A, following Lecture 18 of [Sno13].

Talk 5. The proof of Theorem B and Toric Reduction (27/05)

Prove Theorem B following Lecture 11 of [Sno13]. In particular, explain Mazur's descent argument. For this, you may want to consult Parson's notes [Par04]. Prove that the Jacobian $J_0(N)$ has completely toric reduction at N, following Lecture 19 of [Sno13].

Talk 6. Hecke algebras and the Eichler–Shimura relation (03/06)

Recall geometric construction of Hecke operators as correspondences. Discuss the structure of Hecke algebras, for instance, as endomorphism algebras of the Jacobian of modular curves. Introduce the Atkin–Lehner involution and explain its interaction with the Hecke action. Prove the Eichler–Shimura relation.

If time permits, sketch the construction of ℓ-adic Galois representations attached to modular forms of weight 2, and briefly hint at their extensions to arbitrary weights.

References: Lectures 16-17 of [Sno13], Sections 7, 8, and 10 of Diamond and Im's survey article [DI95].

Talk 7. The Eisenstein ideal (10/06)

Introduce the Eisenstein ideal (Lecture 20 of [Sno13]). State and prove some of its local properties. You may want to consult Section 4 of Mazur's expository article [Maz06] for a summary of the relevant properties, where precise references to their proofs in the original paper [Maz77] are also provided.

Talk 8. Finishing up I (17/06)

Following Lecture 20-21 of [Sno13], sketch a proof of Mazur's theorem: if $p > 7$ is a prime other than 13, then no elliptic curve over $\mathbb{Q}$ has a rational point of order p.

Talk 9. Finishing up II (24/06)

Complete Mazur's classification theorem of torsion points on elliptic curves over $\mathbb{Q}$, which is now reduced to a lengthy case-by-case analysis of the remaining torsion orders. The speaker is encouraged to either

A) provide a more thorough study of the relevant cases, including Mazur–Tate's theorem on 13-torsion [MT73], as in Lecture 22-23 [Sno13]; or

B) focus on one or several particularly interesting cases, and then move on to other applications of the theory of the Eisenstein ideal, such as the ones in Section 3 of [Maz77] or Ribet's converse to Herbrand's theorem.

Talk 10. Further developments (01/07)*

Survey some aspects of recent developments in the theory of the Eisenstein ideal and its applications. Alternatively, this talk could be kept flexible depending on how fast we progress, or simply canceled if needed.

References

[BM40] G Billing and Kurt Mahler. On exceptional points on cubic curves. *Journal of the London Mathematical Society*, 1(1):32–43, 1940.

[Con04] Brian Conrad. Classification of quasi-finite étale separated group schemes. Available at: `https://math.stanford.edu/~conrad/vigregroup/vigre03/zmt.pdf`, 2004.

[DI95] Fred Diamond and John Im. Modular forms and modular curves. In V. Kumer Murty, editor, *Seminar on Fermat's Last Theorem*, volume 17 of *CMS Conference Proceedings*, pages 39–133. American Mathematical Soc., 1995.

[EK20] Noam D Elkies and Zev Klagsbrun. New rank records for elliptic curves having rational torsion. In *Proceedings of the Fourteenth Algorithmic Number Theory Symposium, Mathematical Sciences Publishers, Berkeley*, pages 233–250, 2020.

[Fal83] Gerd Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Inventiones mathematicae*, 73(3):349–366, 1983.

[KM85] Nicholas M. Katz and Barry Mazur. *Arithmetic Moduli of Elliptic Curves*. Princeton University Press, 1985.

[Maz77] Barry Mazur. Modular curves and the Eisenstein ideal. *Publ. Math. Inst. Hautes Études Sci.*, 47(1):33–186, 1977.

[Maz06] Barry Mazur. Rational points on modular curves. In J. W. S. Cassels and A. Fröhlich, editors, *Modular Functions of One Variable V*, volume 601 of *Lecture Notes in Mathematics*, pages 107–148. Springer, 2006.

[Mil08] James S. Milne. Abelian Varieties, 2008. Available at: `https://www.jmilne.org/math/CourseNotes/AV.pdf`.

[Mor22] Louis Joel Mordell. On the rational resolutions of the indeterminate equations of the third and fourth degree. In *Proc. Cambridge Phil. Soc.*, volume 21, pages 179–192, 1922.

[MT73] Barry Mazur and John Tate. Points of order 13 on elliptic curves. *Invent. Math.*, 22(1):41–49, 1973.

[Par04] James Parson. Mazur's Eisenstein Descent. Available at: `https://virtualmath1.stanford.edu/~conrad/vigregroup/vigre03/eisendescent.pdf`, 2004.

[PR16] Mihran Papikian and Joseph Rabinoff. Optimal Quotients of Jacobians With Toric Reduction and Component Groups. *Canadian Journal of Mathematics*, 68(6):1362–1381, 2016.

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer New York, 1994.

[Sno13] Andrew Snowden. Course on Mazur's torsion theorem. Available at: `https://websites.umich.edu/~asnowden/teaching/2013/679/index.html`, 2013.

[Tat97] John Tate. Finite Flat Group Schemes. In *Modular Forms and Fermat's Last Theorem*, pages 121–154. Springer New York, 1997.