Kleine AG Mazur's Torsion Theorem

Saverio Caleca

Bonn, 2nd of October 2025

Introduction

The purpose of this semester's Kleine AG is to prove the following theorem, which was conjectured[1] by Andrew Ogg in [8], before being proven by Mazur:

Theorem (Mazur's Torsion Theorem)**.** *Let E be an elliptic over $\mathbb{Q}$, then the only possibilities for the torsion subgroup of its rational Mordell-Weil group are:*

$$\mathbb{Z}/n\mathbb{Z} \quad for \quad n \leq 10 \quad or \quad n = 12$$

or

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} \quad for \quad 1 \leq m \leq 4$$

This is an interesting theorem for many reasons. Firstly, one might notice that, a priori, there is no clear reason why the torsion should be bounded at all, but indeed this was a breakthrough in a series of results on bounds on the torsion of abelian varieties defined over number fields. Secondly, its proof introduced many new techniques now popular in arithmetic geometry for the study of Galois representations and serves as a great motivation and example of why these are such central objects nowadays. Further, Mazur's Torsion Theorem is needed in order to prove Fermat's Last Theorem. An even longer and more precise motivation to read the Eisenstein ideal paper might be found in [1].
This Kleine AG is also planned to attract students with different backgrounds, increasing the difficulty throughout the day. Indeed, the first two talks will only assume as a prerequisite algebraic geometry on the level of Harthshorne and might provide students several classical examples which cannot be covered in basic courses. Master's students are therefore invited to come and see techniques they learned about during the first year, applied towards a result which might serve as an inspiration for their future studies. PhD students might find interesting to learn the details of this proof and might be led to delve deeper into the original papers of Mazur, who writes wonderfully. Others might just come to get together, meet students from other universities and have some fun while doing math.
The location will be Bonn and the date is the 2nd of October 2025. The talks will all last one hour and start at 10:00, bearing in mind that probably PhD students will show up directly for the second one. We will get lunch together after the second one, at around 12:30. The talks will resume in the afternoon at 14:00. The times are sharp, with no 15 minute delay. On the next pages, you will find the outline of the talks. If you are interested in giving a talk please contact us and tell us which ones you might like.

[1] Beppo Levi almost stated this conjecture already at the 1908 ICM, but not quite. See [9] for more details.

First talk: Crash course on elliptic curves. 10:00

Start with the definition of an elliptic curve over a field, Weierstrass form and define addition. Explain that its $\mathbb{C}$-points can be seen as the quotient of $\mathbb{C}$ by a lattice, and what this tells us about the torsion subgroup. State the Mordell-Weil Theorem, noting the difference from the situation over $\mathbb{C}$. Explain what a 2-torsion point is and how to compute them from the Weierstrass form. Recall Nagell-Lutz, briefly say what the gist of the elementary proof is. (If you have time, this would be a good moment to give an example of an elliptic curve over $\mathbb{Q}$ with a rational point of, say, 5-torsion.) Using duality, show that the torsion points defined over the rationals can only be a cyclic group or a cyclic group times $\mathbb{Z}/2\mathbb{Z}$. Reference: [11].

Second talk: Reminder on modular curves. 11:15

Explain the construction and the moduli interpretation of modular curves as compact Riemann surfaces by taking the quotient of the upper half plane by an arithmetic subgroup Γ; the only relevant cases for us are given by $\mathrm{SL}(2,\mathbb{Z}), \Gamma_1(p), \Gamma_0(p)$, where p is a prime number. Explain how we can compute their genus using Riemann-Hurwitz, without writing down all the explicit computations but by instead drawing a picture. Highlight the primes for which $g(X_1(p)) = 0$. Then explain that this has a model over $\mathbb{Q}$, mention that the cusps are defined over $\mathbb{Q}$, and explain why this gives us infinite families of examples for the cases in which the genus is 0. Now highlight the connection to the statement of our theorem and explain that our strategy from now on will be to study the rational points of the modular curves relevant to each moduli problem. Remind the audience what the Jacobian of a curve is and what Hecke correspondences are, including their action on q-expansions of modular forms. Please contact us and the speakers of the last two talks in order to keep notation steady and lighten the latters' work. Reference: [10].

Third talk: Eliminating small values. 14:00

This talk is meant to prove or at least mention the only cases outside Mazur's proof. Prove that there is no 13-torsion point, this is done in [6] and is an example of the general strategy. Then you will need to eliminate all possible cyclic groups whose order is divisible only by $p = 2, 3, 5, 7$ which do not appear. These are: $\mathbb{Z}/N\mathbb{Z}$ for $N = 14, 15, 20, 21, 24, 27, 49$ (treated in [3]), then $N = 18, 25, 35$ (Reference: [2]) and $N = 16$ was first done in [4]. The only remaining cases to be excluded are $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12$, which are again done in [2].
You have some freedom about which of these you want to talk. Our advice would be, if enough time is left, to talk about the work of [2], while just mentioning the results of [3] and [4].

Fourth talk: Mazur's second proof, part 1. 15:15

The goal is to explain the second proof Mazur gave of the theorem, following [7], assuming the finiteness of the Mordell-Weil group of the Eisenstein quotient. We suggest you work backwards, reducing Theorem 4.1 to Corollary 4.3, then Corollary 4.3 to Proposition 3.1 and the existence of an optimal quotient of the Jacobian of $X_0(N)$ with finite Mordell-Weil group over $\mathbb{Q}$. Explain the proof of Proposition 3.1 and then construct the Eisenstein quotient, whose main properties will be proved in the last talk. The reference for this last part is clearly [5], precisely Chapter I, §§6,10. Try to at least state Proposition 9.5, the definition of the Eisenstein ideal, 9.7 and 9.8.
You can assume a wider background from the audience than we did in the previous talks, but we would advise you to recall what a formal immersion is. Please keep in touch with us and the speaker of the last talk so as to keep notation steady and avoid overlaps.

Fifth talk: Mazur's second proof, part 2, the Mordell-Weil group of the Eisenstein quotient is finite. 16:30

The goal of this talk is to prove the main assumption left out in the last talk: for p a prime bigger than 7, there exists an optimal quotient of the Jacobian of $X_0(p)$ which has finite Mordell-Weil group. The plan is the following: pick up where the last talk finished; then explain in detail the proof of Prop. 14.1 in Chapter II of [5] and finally prove Theorem 3.1 loc.cit. This is comprehensibly a lot of material and you can surely blackbox any result on admissible groups, but it would be nice, if time allows it, to expand on the Galois representation associated to primes which are not Eisenstein, which is Proposition 14.2.

References

[1] Lycurgus cup (https://mathoverflow.net/users/140871/lycurgus-cup). *Why is the Eisenstein ideal paper so great?* MathOverflow. URL: https://mathoverflow.net/q/332050.

[2] Daniel Sion Kubert. "Universal Bounds on the Torsion of Elliptic Curves". In: *Proceedings of the London Mathematical Society* s3-33.2 (1976), pp. 193–237. URL: https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/plms/s3-33.2.193.

[3] Gerard Ligozat. "Courbes modulaires de genre 1". fre. In: *Mémoires de la Société Mathématique de France* 43 (1975), pp. 5–80. URL: http://eudml.org/doc/94716.

[4] C.E. Lind. *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom geschlecht Eins*. Appelberg, 1940. URL: https://books.google.it/books?id=KpUXOQEACAAJ.

[5] B. Mazur. "Modular curves and the Eisenstein ideal". en. In: *Publications Mathématiques de l'IHÉS* 47 (1977), pp. 33–186. URL: https://www.numdam.org/item/PMIHES_1977__47__33_0/.

[6] B. Mazur and J. Tate. "Points of order 13 on elliptic curves". In: *Inventiones mathematicae* 22 (Mar. 1973), pp. 41–49. ISSN: 1432-1297. URL: https://doi.org/10.1007/BF01425572.

[7] Barry Mazur and Dorian Goldfeld. "Rational isogenies of prime degree". In: *Inventiones mathematicae* 44 (1978), pp. 129–162. URL: https://api.semanticscholar.org/CorpusID:121987166.

[8] A. P. Ogg. ""Diophantine equations and modular forms"". In: *Bulletin of the American Mathematical Society, Bull. Amer. Math. Soc. 81(1), 14-27,* (January 1975).

[9] N. Schappacher and R. Schoof. "B. Levi and the Arithmetic of Elliptic Curves". In: *The Mathematical Intelligencer 18, 57–69* (1996). URL: https://irma.math.unistra.fr/~schappa/NSch/%20Publications_files/1996_RSchNSch.pdf.

[10] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Kanô memorial lectures. Princeton University Press, 1971. ISBN: 9780691080925. URL: https://books.google.it/books?id=-PFtGa9fZooC.

[11] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2009. ISBN: 9780387094946. URL: https://books.google.it/books?id=Z90CA_EUCCkC.