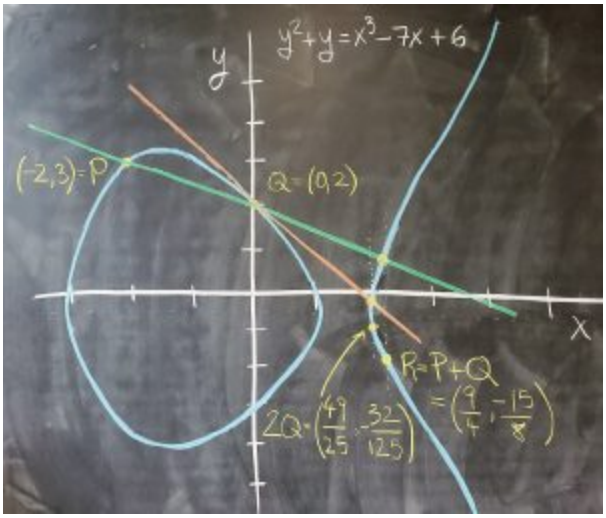
UCONN

DEPARTMENT OF MATHEMATICS
Álvaro Lozano-Robledo

MATH 5020 – The Arithmetic of Elliptic Curves

Course Description:



This course will be an introduction to elliptic curves which, roughly speaking, are smooth cubic curves in the projective plane with at least one rational point (turns out they have a simple model of the form y^2=x^3+ax+b). The surprising feature of elliptic curves is that their points can be made into an abelian group, and this group is finitely generated when we focus on points with coordinates in the rational numbers lying on an elliptic curve with rational coefficients. Elliptic curves are central in modern number theory, e.g., they were essential in the proof of Fermat's Last Theorem. The goal of the course will be to understand and calculate the group of all rational points on an elliptic curve (i.e., calculate its torsion and rank), and a number of more refined invariants (such as the order of the Shafarevich-Tate group).

The prerequisites for this course are the abstract algebra sequence (Math 5210 and 5211) and a basic understanding of algebraic number theory and algebraic geometry, although I will adjust the material to the audience background as much as I can. Our textbook will be "The Arithmetic of Elliptic Curves," by J. H. Silverman, which is the standard graduate-level textbook for the subject.

Prerequisites: MATH 5210 and MATH 5211 (i.e., a year of abstract algebra).
Recommended Preparation: A semester of Algebraic Number Theory, and a semester of Algebraic Geometry.
Credits: 3
Meets (Spring 2026): Mondays and Wednesdays, 3:30 – 4:45 at MONT 313.

About the Instructor: Álvaro Lozano-Robledo

I'm a Professor of mathematics at the University of Connecticut.

Office hours: TBA.



Alvaro Lozano-Robledo in action (Shawn Kornegay/UConn Photo), see this UConn Today's article.

About the Book and Other Resources

I will be following the main reference: **Joseph H. Silverman, "The Arithmetic of Elliptic Curves,"** Springer, 2nd Edition. However, there are other references that may be very useful.

1. H. Daniels and Á. Lozano-Robledo, "**What is... an elliptic curve?**", in the Notices of the American Mathematical Society, Vol 64, Issue 3, March 2017, pp. 241-243.

2. J. H. Silverman, J. Tate, "**Rational Points on Elliptic Curves,**" Springer – this book is an elementary version of the main reference.

3. Á. Lozano-Robledo, "**Elliptic Curves, Modular Forms, and their L-Functions**" is another elementary introduction to elliptic curves.

4. J. H. Silverman, "**Advanced Topics in the Arithmetic of Elliptic Curves,**" Springer.

5. J. S. Milne, "**Elliptic Curves,**" published by Kea Books – this book is freely available at Milne's website.

6. N. Koblitz, "**Introduction to Elliptic Curves and Modular Forms,**" Springer.

7. J. Tate, **"The arithmetic of elliptic curves,"** Invent. Math. 23 (1974), 179-206 – The main reference was heavily influenced by this key survey article.

8. D. Husemöller, "**Elliptic Curves,**" Second Edition, Springer.

9. L. Washington, "**Elliptic Curves: Number Theory and Cryptography,**" Second Edition (Discrete Mathematics and Its Applications) 2nd Edition, CRC Press.

10. E. Brown and A. Rice, "**Why Ellipses Are Not Elliptic Curves,**" Math. Mag. 85 (2012), *no. 3,* 163–176 – For those interested in the history of elliptic curves.

During the course we will discuss computability aspects of the theory, so it is helpful for students to familiarize themselves with computer packages that can handle computations on elliptic curves:

- A list of videos intros to the LMFDB, Magma, and Sage/CoCalc.
- LMFDB: The L-functions and Modular Forms DataBase.
- MAGMA. There is an online calculator here.
- SageMath and CoCalc.

Homework

Homework sets will be posted here periodically. The sets are a small selection of problems that should help students in understanding the theory, but of course there are many other problems available in Silverman's book that are also a great resource for the learner. This is a topics class, so the homework sets are not mandatory. I'll be happy to look at sets if you want to send me your solutions, but in general I expect that if you are interested in the material, you will be trying the problems on your own and reaching out to me when you need help or hints. For the sake of the grade, though, I do expect that you will submit some problems during the course (at least one per problem set). If you have difficulties, do not waste time — get help! Please come to office hours!

- **Lecture notes and Homework sets can be found at the GitHub repository for this course**

Tentative Schedule

The videos of the lectures can be found (as they become available) in this YouTube playlist. The course notes are in the GitHub repository.
Note: the PDF files below do not display correctly in some browsers. I recommend downloading the files and opening them locally in your machine.

Lecture	Topics (links to videos)	Notes
-1	What is... an elliptic curve? An introduction	Slides from the talk.
0	Class logistics and description of the course	Lecture 0

1	Introduction to diophantine equations	Lecture 1
2	Number Fields... VS ... Elliptic Curves	Lecture 2
3	Intro. to algebraic varieties and curves	Lecture 3
4	Varieties, function fields, dimension (part 1), and singularities, morphisms (part 2)	Lecture 4
5	Order of vanishing (part 1), an example (part 2), and ramification (part 3)	Lecture 5
6	More on ramification (part 1) and divisors, and differentials (part 2)	Lecture 6
7	Riemann-Roch, Hurwitz, Weierstrass models	Lecture 7
8	Models of elliptic curves, discriminant and j-invariant (part 1), and the group law (part 2)	Lecture 8
9	The (geometric) group law (part 1), and the (Picard) group law (part 2)	Lecture 9
10	Isogenies (part 1) and (part 2), and the dual isogeny (part 3)	Lecture 10
11	The Tate module.	Lecture 11
	(Optional lecture on adelic Galois representations)	Slides

12	The Weil pairing (construction) and (properties)	Lecture 12
13	Consequences of the Weil pairing (part 1), and elliptic curves over finite fields (Hasse's bound, part 2)	Lecture 13
14	An example of an elliptic curve over a finite field (part 1), and elliptic curves over C (part 2)	Lecture 14
15	An introduction to the formal group of an elliptic curve.	Lecture 15
16	Formal groups, homomorphisms (part 1), groups associated to formal groups, the formal logarithm, and formal exponential (part 2).	Lecture 16
	Happy Pi Day! (Extra lecture about pi and elliptic curves.)	Pi Day
17	Torsion points in the groups associated to formal groups over DVR's (part 1), and local fields, minimal models (part 2)	Lecture 17
18	Elliptic curves over local fields: the fundamental exact sequence (part 1), and points of finite order over local fields: an example (part 2).	Lecture 18
19	More on points of finite order (part 1), and the action of inertia (part 2)	Lecture 19

20	Criterion of Néron-Ogg-Shafarevich, and good and bad reduction (part 1), potential good reduction and the j-invariant (part 2), and the group E/E_0 (part 3).	Lecture 20 and a bit more
21	The weak Mordell–Weil theorem: the Kummer pairing	Lecture 21
22	Properties of the Kummer pairing (part 1) and the finiteness of the maximal abelian extension of exponent m unramified outside a finite set of primes (part 2)	Lecture 22
23	The proof of the weak Mordell-Weil theorem (part 1), the descent procedure and heights of elliptic curves (part 2)	Lecture 23
24	Torsion points (Nagell-Lutz) (part 1), and the canonical height (part 2)	Lecture 24
25	The canonical height pairing, and Z-linear independence of rational points (part 1); computing the Mordell-Weil group (part 2)	Lecture 25
	(Extra lectures) An introduction to group (and Galois) cohomology (part 1) and (part 2)	Cohomology notes
26	Complete 2-descent (part 1), and an example (part 2).	Lecture 26
27	Example of 2-descent (part 1), and definitions of Selmer and Sha (part 2)	Lecture 27

28	Selmer and Sha: the fundamental sequence (part 1), twists, homogeneous spaces, and descent (part 2), and an example of descent via 2-isogeny (part 3).	Lecture 28

University Policies

- Policy Against Discrimination, Harassment and Related Interpersonal Violence—*The University is committed to maintaining an environment free of discrimination or discriminatory harassment directed toward any person or group within its community – students, employees, or visitors. Academic and professional excellence can flourish only when each member of our community is assured an atmosphere of mutual respect. All members of the University community are responsible for the maintenance of an academic and work environment in which people are free to learn and work without fear of discrimination or discriminatory harassment. In addition, inappropriate amorous relationships can undermine the University's mission when those in positions of authority abuse or appear to abuse their authority. To that end, and in accordance with federal and state law, the University prohibits discrimination and discriminatory harassment, as well as inappropriate amorous relationships, and such behavior will be met with appropriate disciplinary action, up to and including dismissal from the University. Additionally, to protect the campus community, all non-confidential University employees (including faculty) are required to report sexual assaults, intimate partner violence, and/or stalking involving a student that they witness or are told about to the Office of Institutional Equity (OIE). Please be aware that while the information you provide will remain private, it will not be confidential and will be shared with University officials who can help.An exception to this reporting exists if students disclose information as a part of coursework submitted to an instructor in connection with a course assignment. Even in the absence of such obligation, all Employees are encouraged to contact OIE if they become aware of information that suggests a safety risk to the University community or any member thereof. The University takes all reports with the utmost seriousness.* More information, including resources and reporting options, is available at equity.uconn.edu and titleix.uconn.edu.
- **Student Conduct Code**—Students are expected to conduct themselves in accordance with UConn's Student Conduct Code.
- **Academic Integrity Statement**—*This course expects all students to act in accordance with the Guidelines for Academic Integrity at the University of Connecticut. Because questions of intellectual property are important to the field of this course, we will discuss academic honesty as a topic and not just a policy. If you have questions about academic integrity or intellectual*

property, you should consult with your instructor. Additionally, consult UConn's guidelines for academic integrity.

- **Copyright**—*My lectures, notes, handouts, and displays are protected by state common law and federal copyright law. They are my own original expression and I've recorded them prior or during my lecture in order to ensure that I obtain copyright protection. Students are authorized to take notes in my class; however, this authorization extends only to making one set of notes for your own personal use and no other use. I will inform you as to whether you are authorized to record my lectures at the beginning of each semester. If you are so authorized to record my lectures, you may not copy this recording or any other material, provide copies of either to anyone else, or make a commercial use of them without prior permission from me.*
- **Students with Disabilities—***The University of Connecticut is committed to protecting the rights of individuals with disabilities and assuring that the learning environment is accessible. If you anticipate or experience physical or academic barriers based on disability or pregnancy, please let me know immediately so that we can discuss options. Students who require accommodations should contact the Center for Students with Disabilities, Wilbur Cross Building Room 204, (860) 486-2020, or http://csd.uconn.edu/.*
- **Final Exam Policy**—*In accordance with UConn policy, students are required to be available for their final exam and/or complete any assessment during the time stated. If you have a conflict with this time you must obtain official permission to schedule a make-up exam with the Dean of Students. If permission is granted, the Dean of Students will notify the instructor. Please note that vacations, previously purchased tickets or reservations, graduations, social events, misreading the assessment schedule, and oversleeping are not viable reasons for rescheduling a final.*

Back to top

© University of Connecticut Disclaimers, Privacy & Copyright Accessibility Webmaster Login