Algebraic Number Theory (Math 2245)

Topic: Elliptic Curves

University of Pittsburgh, Spring Semester 2025

Welcome to Number Theory! Please read this syllabus carefully. Let me know if you have any questions at all!

The course webpage on Canvas is where the course will really happen, whether we are meeting online or in person.

`https://canvas.pitt.edu/courses/310418`

1 Course staff

Instructor

My name is Carl Wang-Erickson. You're welcome to call me "Carl," or "Dr. Carl," or "Professor Carl." Or "Dr. Wang-Erickson" or "Professor Wang-Erickson," but that is a mouthful. Let me know if you prefer me to call you by a name other than what I see in your official enrollment in the course (there will be a survey where you can tell me about that).

I am originally from Milwaukee, Wisconsin, USA. I finished my PhD studying number theory at Harvard University in 2013. Since then, I worked at Brandeis University and then Imperial College London, followed by Pitt starting in 2019.

While in high school, I became interested in number theory. That's a major reason that I wanted to study math more, and after trying it out in college, I decided to try to get a PhD and do research. The topics that we will discuss in this course are fundamental to my research today, and I really enjoy them.

How to contact me

Emailing me at `carl.wang-erickson@pitt.edu` is the best way to start. In particular, you are welcome to set up a meeting with me. Office hours are also an open time where you can come talk with me any time during the office hour period with no appointment needed. If you would like to find out more about me, you might be interested in my webpage at `https://sites.pitt.edu/~caw203/`.

2 Course coordinates

The course meeting time is Monday and Wednesday, 2:00pm-3:15pm. The meeting location is Thackeray Hall, room 703. In extenuating circumstances, such as severe winter weather, class may meet on Zoom as announced via Canvas.

The **Office hour time** is tentatively Monday and Wednesday, 3:30pm-4:30pm. The office hour location is my office in Thackeray Hall, Room 421. An updated schedule will be posted in Canvas.

3 What we are doing

The goal of this course is to introduce elliptic curves in the context of number theory. Another perspective on the course is that it aims to introduce the field of arithmetic geometry through the example of elliptic curves. An elliptic curve can be viewed as a cubic equation in two variables, and the overall goal is to understand the solutions of such equations in arithmetic fields such as the rational numbers $\mathbb{Q}$, finite fields $\mathbb{F}_p$, and p-adic fields $\mathbb{Q}_p$. Some algebraic number theory – that is, the arithmetic of rings like $\mathbb{Q}$, $\mathbb{F}_p$, and $\mathbb{Q}_p$ – will also be introduced along the way. A rough outline of the course content appears at the end of this syllabus.

I would like to recognize Tom Fisher's course, which I attended at the University of Cambridge in 2007, as an inspiration for the structure of this course.

4 How we will do it

Here are the major tools and resources that we will engage in order to accomplish this.

4.1 Class time and lecture notes

This course will rely on lecture content rather heavily because I plan to give a more accessible presentation of some topics than what is found in textbooks. I will be able to point to references in textbooks for the course content.

4.2 Textbook

The comprehensive textbook on the course content is *The Arithmetic of Elliptic Curves* by Joseph Silverman (Graduate Texts in Mathematics, volume 106). It is accessible via the Pitt library. I will refer to this textbook for reference, but I will aim for the class presentation to be more basic and demand less background than this textbook.

Other useful textbooks include

- *Rational Points on Elliptic Curves* by Silverman and Tate (Undergraduate Texts in Mathematics; accessible through Pitt library).
- *Lectures on Elliptic Curves* by J.W.S. Cassels (London Mathematical Society Student Texts, volume 24).

4.3 Problem sets

The point of the problem sets is to ensure that you spend enough time computing with the course material to get a feeling for what is really going on behind the theory and examples that are being presented in class. There will be bi-weekly written assignments that you can submit through Canvas. Use of LaTeXis strongly encouraged. There will probably be around 6 written assignments during the semester. You can use a free online version such as Overleaf to compile documents in LaTeX.[1] I have posted a template on Canvas.

If you need an extension on an assignment, please request one *in advance* and provide a reason. Otherwise, late assignments are generally not graded and receive a zero grade.

[1] To access a Pitt-sponsored Overleaf account, go to https://www.overleaf.com/edu/pitt.

The lowest single problem set score will be dropped.

Expression of mathematical ideals will be considered in the assessment of problem sets.

- use complete sentences to make arguments (not just symbols and equations)
- explain what is being claimed and proved.

4.3.1 Collaboration policy

You may collaborate with fellow students on any stage or your own written assignments, provided that you

- write up your explanations independently, and
- list the names of those that you collaborated with on your written assignment. It may be the case that you attribute the collaboration to "the whole class," but be specific as is reasonably possible.

Collaboration will not be allowed on the midterm exam.

4.3.2 Sourcing policy

You may use materials from the textbook and course sessions without limitation and without citing them, unless *upcoming content* from the course somehow obviates the assigned work – I expect you to use your own reasoning to avoid doing that.

You may also seek out and use inspiration from all sources, including the internet, provided that you follow standard professional and academic practice of citing your sources, and genuinely understand what you are writing down. You should think of the rule as "cite sources as much as reasonably possible." A good citation allows the reader to look up the source quickly, e.g. weblink and a precise reference within a source. I have included a LaTex template that includes a sample bibliography.

Naturally, these policies also apply to all of the work that you do for this course. They are particular instances of Pitt's academic integrity policies, which also apply in all cases to all kinds of work in this course.

4.4 Project

Each student will complete one project over the course of the semester. The timing and topics of projects will be the subject of discussion. As far as the classroom experience, you will find that your classmates will be giving presentations that are interspersed throughout the course of the semester.

Your project work will consist of

1. a 15-30 minute in-class presentation on a topic related to the course content
    - the length of the presentation will depend upon how many people are enrolled in the course
2. an expository writeup that complements the presentation
3. reading and providing feedback on one of your classmates' writeups
4. providing feedback on your classmates' in-class presentations.

The topic and timing of your project will be agreed upon through discussion between me and you, usually in office hours. Likewise, I will share a clear rubric for how the project will be assessed soon after the course begins.

Project topics are very flexible and could be of the following types: a topic that is used in the course but not dealt with in detail (for example, input from algebraic geometry that is used toward the beginning of the course); introducing an idea from elsewhere in math in which elliptic curves play a role; introducing an important idea we use in the course; discussing an idea in algebraic number theory that we will use in the course; applications of the course material, such as applications to further theoretical math or to cryptography.

This course will not have a final exam, but, as a graduate course, the course may possibly continue meeting during the undergradute exam period, especially if this allows for accommodating presentations.

The project portion of your grade will be calculated as 75% your own project (presentation plus writeup plus revision of the writeup after receiving feedback from a classmate), 15% your written feedback on a classmate's writeup, and 10% your written feedback on classmates' presentations.

4.5 Communication!

4.5.1 Between me and you

Communication between me and you is key for promoting your success in this course. The standard ways I communicate *to* you are

- the lecture components of course sessions
- feedback on your written assignments, final project, midterm exam, and Ts & Qs
- other interactions, such as office hours, appointments you request, email, etc.

The standard ways you communicate with me are reciprocal to the above: showing up to course sessions, looking over my grading, and showing up to office hours. I encourage you to drop by office hours!

In addition, I need to and want to hear from you if you are finding making the deadlines difficult. I know that it can be hard to reach out to me to ask for extensions, but I really encourage you to start that conversation in advance of falling behind.

4.5.2 Among you

Our peers can often be our best teachers. I started practicing this lesson only after graduating from college, which was my own loss. While it might possibly feel unusual to do as much peer discussion of math as is required in this course, it is, in fact, an important part of being a mathematician, and I want to treat you like mathematical adults. That is why there is some emphasis on peer feedback in this course.

5 Assessment

Your final numerical course grade, out of 100, will be calculated as

$$\text{Course grade } = \frac{1}{2}[\text{Problem Sets}] + \frac{1}{2}[\text{Project}].$$

Your final letter grade for the course will be calculated on an *absolute* basis to the maximum extent that I can achieve. In other words, a student will get an A for "superior" work, no matter the performance of other students; and so forth, according to the official grade scale.[2] While it is undeniable and natural that your peers' level of achievement may affect your grade in some sense, I use the overall class achievement level as only one calibration factor for letter grades. I welcome more discussion in person on this topic, and would be happy to occasionally provide an estimate of your letter grade based on your current grade status once the midterm exam has passed.

6 Other policies and procedures

- **Audit option.** Please contact me to set up a discussion of an audit option, if this interests you.
- **Expectations around class sessions:** I don't expect you to follow all the details of a math lecture in real time, but I do expect you to come to lecture and then fill in the gaps in your understanding between lectures. My goal is to distill a large amount of information into a concise presentation, and you should pay attention to my advice about what's important and what isn't.
- **Attendance.** Attendance is not "taken" nor graded, but the course is designed around the assumption that students attend course sessions. In particular, while I will aim to put all of the most important announcements for the course online, if you miss an announcement or explanation of how to do something that happens during a course session, it will be "on you" to find out about it.
- **Email and Canvas communication.** Students will be expected to be aware of updates about the course that are sent via email to their Pitt email account or posted on the course's Canvas page. To see how to make sure you get the right Canvas notifications, see the appropriate link under the Resources module on this course's Canvas page.
- **Disability resources.** If you have a disability for which you are or may be requesting an accommodation, you are encouraged to contact both your instructor and Disability Resources and Services (DRS), 140 William Pitt Union, (412) 648-7890, `drsrecep@pitt.edu`, (412) 228-5347 for P3 ASL users, as early as possible in the term. DRS will verify your disability and determine reasonable accommodations for this course. More information may be found at `https://www.studentaffairs.pitt.edu/drs/`.
- **Academic integrity.** Students in this course will be expected to comply with the University of Pittsburgh's Policy on Academic Integrity. (In particular, this includes following the problem set collaboration policy above.) Any student suspected of violating this obligation for any reason during the semester will be required to participate in the procedural process, initiated at the instructor level, as outlined in the University Guidelines on Academic Integrity. This may include, but is not limited to, the confiscation of the examination of any individual suspected of violating University Policy. Furthermore, no student may bring any unauthorized materials to an exam, including dictionaries and programmable calculators.

  To learn more about Academic Integrity, visit the Academic Integrity Guide for an overview of the topic. For hands-on practice, complete the Academic Integrity Modules.
- **Scheduling conflicts.** It your responsibility to take stock of schedule conflicts, for example, those resulting from athletic participation or religious observance. These should be discussed with the instructor in the first two weeks of the semester, and will be handled according to university guidelines.

[2] https://catalog.upp.pitt.edu/content.php?catoid=188& navoid=17780#grading-systems

7 Have a great semester!

Please get in touch with me to ask about any questions that arise from this syllabus! I am looking forward to working with you – all of us have a lot to learn this semester. In particular, just as I am expecting continuous improvement from you in your learning, I am expecting continuous improvement in my teaching.

8 Course outline

Here is a rough outline of the main topics of the course. It could be viewed as having the goal of outlining the proof of the Mordell-Weil theorem and understanding descent calculations, but the emphasis is on doing calculations with elliptic curves.

1. Motivating examples, introducing arithmetic geometry
2. Some basic algebraic geometry and how it applies to elliptic curves
3. The group law on elliptic curves; isogenies of elliptic curves and their degree
4. Differentials, the invariant differential, and Hasse's theorem
5. p-adic rings and fields, and points of elliptic curves valued in p-adic fields
6. Elliptic curves over number fields; rational torsion points on elliptic curves
7. Heights of rational points on elliptic curves
8. The weak Mordell-Weil theorem and the Mordell-Weil theorem
9. Final applications and applications depending on how the course goes and student interest, consisting of such possibilities as:
    - Selmer groups and Tate–Shafarevich groups
    - Weil pairing
    - Descent by cyclic isogeny
    - Applications to cryptography
    - L-functions of elliptic curves and the Birch and Swinnerton-Dyer conjecture