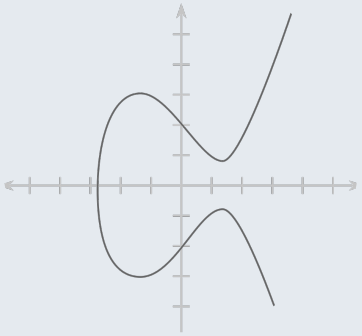

An elliptic curve

Elliptic Curves

MATH 317

Course info

Tuesday & Thursday

9:55-11:15a

Park Science 159

Instructor

Professor John Bergdall

Park Science 334

jbergdall@brynmawr.edu

x5356

Office Hrs:
M 2:30-3:30p
Tu 11:30a-12:30p
Th 1:30-2:30p

Overview

This is a special topics course on the theory of *elliptic curves*. The mathematics we will study lies at the intersection of algebra and geometry, with significant motivation coming from number theory and analysis.

The pre-history of our subject is the theory of quadratic equations, which geometrically arise as conics (the intersection of a plane with a cone). Given a conic, there was a historic emphasis on describing special points, those points with rational coordinates. We call them rational points. What was known since antiquity is that one could use geometric constructions, intersecting chords, to generate many rational points from just one. This leads to, among other things, the classification of Pythageorean triples, like $(3,4,5)$, $(5,12,13)$, and $(8,15,17)$, which are the integer side lengths of right triangles.

After conics, the next step is cubic equations. This is the realm of elliptic curves. To construct a point on the conic requires two things: a point and a line. Similarly, constructing a point on a cubic also requires two things: two points. While it may seem in going from degree 2 to degree 3, you've traded two for two, the shift results in remarkable complexity! In fact, the structure of points on a cubic curve is remarkably complex: it is actually an abelian group! Here we have the first deep connection with algebra. The rest of the development of the theory will require even more algebra, so we omit it from this overview.

Our first goal in this course is to study elliptic curves and their group law. The main theorem of the course will be that rational points form a *finitely generated* group. Following that we will turn toward more refined questions about cubic curves and their applications to computational questions in number theory and cryptography. Along the way we will make detailed detours in the connection between algebra and geometry.

Learning goals

- Develop an understanding for how geometry can be studied using algebra.
- Learn the connections between algebra, geometry, and number theory through the example of elliptic curves.
- Gain experience searching for and studying advanced mathematics outside the classroom.
- Practice explaining mathematics concepts to peers.
- Prepare mathematical exposition for consumption by experts and peers alike.
- Learn to develop and use computer software to make calculations in abstract mathematics.

Grade breakdown

15%	Course contribution
30%	Problem sets portfolios
15%	Mini project
40%	Research project

The default grade lines will be: >93% earns a 4.0, >90% earns a 3.7, >87% earns a 3.3, >83% earns a 3.0, and so on. We reserve the right to make the gradelines *more* generous.

Course contribution

The course contribution portion of your score will be determined by your presence in the course and the way you interact with the material. You may be active in class discussions, or you may prefer to take careful notes and raise questions or doubts in private. Both are valid ways of contributing to the class. Helping your peers navigate the material is yet another way. *We expect you to earn full marks*. Issues such as extraordinary absences (more than 3) or other disruptive behavior may result in the lowering of the marks. We will dialogue about your contributions throughout the course, so that we are both clear.

FAQs

Why “elliptic”?

You’re right to be skeptical, since when you draw an elliptic curve it does not look like an ellipse. We will discuss in the class, however, that elliptic curves arise naturally when you try to calculate the *arc length* of an ellipse. The corresponding integrals were classically “elliptical integrals” and so the name stuck.

Can I suggest my own project?

Yes, of course! We ask only two things. First, you run your suggestion by us. Second, you are not re-using a project from a previous experience.

Do I need to know algebraic geometry?

No! We will go over any of the algebra and geometry we really need.

Do I need to know how to code?

Not really. You’ll learn what you need to. We are going to be using a computer algebra system called SAGE to do our computations. Sometimes you will write programs by hand and sometimes you will use in-built commands to do your work. Understanding the math and logic will be far more difficult than the rudiments of python you will need to pick up.

Material

Required texts

Silverman, J. H. and Tate, J. T. *Rational Points on Elliptic Curves*. 2nd Edition, 2015. Springer.

Available from the BMC bookstore. Also available on moodle in electronic form (thanks to TriCo library access).

Recommended texts

Ash, A. and Gross, R. *Elliptic tales*. Princeton University Press.
Washington, L. *Elliptic curves*. Discrete mathematics and its applications. Chapman & Hall.
Lozano-Robledo, A. *Elliptic curves, modular forms, and their L-functions*. Vol. 58 of *Student mathematical library*. AMS.
Cassels, J. W. S. *Lectures on elliptic curves*. Vol. 24 of *LMS student texts*. Cambridge University Press.
Cox, D. A. *Primes of the form $x^2 + ny^2$*. Wiley & Sons.

Further recommended texts (graduate level)

Husemöller, D. *Elliptic curves*. Vol. 11 of *Graduate texts in mathematics*. Springer.
Koblitz, N. *Introduction to elliptic curves and modular forms*. Vol. 97 of *Graduate texts in mathematics*. Springer.
Silverman, J. H. *The arithmetic of elliptic curves*. Vol. 106 of *Graduate texts in mathematics*. Springer.
Silverman, J. H. *Advanced topics in the arithmetic of elliptic curves*. Vol. 151 of *Graduate texts in mathematics*. Springer.

Computers

We will try to learn some python and do some computer coding in this course. An early class period will be dedicated to this, but you may want to think about where you will want to access computing resources.

Accessibility

Bryn Mawr College is committed to providing equal access to students with a documented disability. Students needing academic accommodations for a disability must first register with Access Services. Students can call 610-526-7516 to make an appointment with the Access Services Director, Deb Alder, or email her the address dalder@brynmawr.edu to begin this confidential process. Once registered, students should schedule an appointment with the professor as early in the semester as possible to share the verification form and make appropriate arrangements. Please note that accommodations are not retroactive and require advance notice to implement. More information can be obtained at the Access Services website whose URL is http://www.brynmawr.edu/access-services/

Any student who has a disability-related need to tape record this class first must speak with the Access Services Director and to me, the instructor. Class members need to be aware that this class may be recorded.

Academic Integrity

The Bryn Mawr College Honor Code is in effect for all students enrolled in this course. We also provide some specific guidelines for *this* course.

We expect you to consult multiple sources (other textbooks, peers, office hours, etc.) in the process of the learning the material. However, any written work you submit should be *in your own words* and *reflect your own understanding*. The easiest way to achieve this, and an excellent way to make sure you understand what you are writing, is to write up each piece of your final work alone and away from any notes you’ve gathered. Remember, whether you are typing or handwriting an assignment, there is no need to create the “final product” all at once — you can write up a final version of a problem before moving onto solving the next one.

Late work and make-up policy

The "deliverables" for the course (problem sets, project pieces, etc.) will have assigned due dates and we expect you to meet those dates except in remarkable circumstances. In case an issue arises:

- We ask for at least *24 hours notice* for extension requests.
- You should also include, when you request an extension, a new due date you will meet. (You are automatically given a 24 hour extension, but the precise time beyond that is subject to approval.)

There are exceptions to the extension policy:

- You will not receive an extension on your mini project mathematical conversation.
- You will not receive an extension on your research project presentation, since they will take place *during class*.

Problem set portfolios

Rather than having a problem set each week, we will have "portfolios" of problems due at somewhat irregular intervals. Problems will be regularly assigned in lecture (a few each class period). They will include:

- Problems assigned from the textbook (or written by me).
- Computer programs/code *you write* in order to perform calculations.
- Calculations performed in SAGE using pre-built computer programs.

Each problem will come with a number of $\star$'s in the range 1-4. A detailed list will be maintained on the course moodle page.

Every few weeks, I will ask you to choose problems to turn in for grading. Our only constraint will be the number of $\star$'s you must turn in. It will never be more than *half* the possible number, but I could ask for less than half.

All problems with at least 3 stars are mandatory for students taking the course for graduate credit.

Research projects

In this course we will have a major research project due at the end of the course. It will include a written paper and an in-class presentation. The goal of the research project is to determine a topic adjacent to elliptic curves, study it, and then present your findings to your peers.

Many of the projects, however, have prerequisites that we do not have time to cover in class. So, the project will be split into two pieces: a "mini project" and the "research project." The mini project will be due partway through the semester.

Mini project

For your mini project you will:

- Choose a topic which technically does not appear in the course but will be helpful for doing a larger research project.
- Write and submit a plan of study (at most 1 page). Your plan should identify the topic you have chosen, why you chose it, and at least 2 sources you will learn from. (Be specific.)
- Update me, in writing, on benchmarks for how you will determine when you have learned your topic. (1-3 pages.)
- (Optional) Prepare written solutions to exercises you solved in learning the topic.
- Prepare an written summary (4-6 pages in length) of your topic *in a narrative style*. You should explain the relevant definitions and key results you learned, but you should not write 4-6 pages of a textbook. Consider this a briefing document a peer could read to catch up, if they needed to know what's what.
- Engage in a mathematical conversation with myself and, if applicable, a selection of your peers about your topic.

Research project

For the research project, you are encouraged to work with a partner. You could even choose this early and design your mini projects to cover two separate minor topics! For the research project, you will:

- Choose an advanced topic in the theory of elliptic curves (from a list).
- Write and submit a research proposal on your chosen topic.
- Prepare a research paper (no more than 15 pages in length). A skeleton draft of your paper will be submitted before the final product is due.
- Prepare a presentation (20-25 minutes) on your topic using slides, a poster, or the chalkboard.

Schedule

We will regularly update you on readings and topics in the course, but part of the nature of a topics course is to allow the course to evolve in a natural fashion. Let's go!