MATH 115: ELLIPTIC CURVES
SPRING 2016

JOHN VOIGHT

Course Info

- **Lectures**: Monday, Wednesday, Friday, block 10 (10:00–11:05 a.m.)
- **x-period**: Thursday, 12:00–12:50 p.m.
- **Dates**: 28 March 2016 – 31 May 2016
- **Room**: 004 Kemeny Hall
- **Instructor**: John Voight
- **Office**: 341 Kemeny Hall
- **E-mail**: `jvoight@gmail.com`
- **Instructor's Office Hours**: Monday 3:00–4:30 p.m. and Tuesday 10:00–11:30 a.m., or by appointment
- **Course Web Page**: `http://www.math.dartmouth.edu/~m115s16/`
- **Prerequisites**: Math 101 and 111
- **Required Texts**: Joseph H. Silverman, *The arithmetic of elliptic curves*, second edition, 2009.
- **Recommended Texts**:
  (1) Joseph H. Silverman and John Tate, *Rational points on elliptic curves*, 1994.
  (2) Lawrence C. Washington, *Elliptic curves: Number theory and cryptography*, second edition, 2010.
  (3) J.S. Milne, *Elliptic Curves*, 2006, available at:
  `http://www.jmilne.org/math/Books/ectext5.pdf`
- **Grading**: Grade will be based on weekly homework (65%) and a final project (35%).

Homework

The homework assignments will be posted on the course webpage. Late homework will be accepted with a penalty. Standard weekly homework assignments, counting for 65% of the grade, will be typically due on Wednesdays.

Cooperation on homework is permitted (and encouraged), but if you work together, do not take any paper away with you—in other words, you can share your thoughts (say on a blackboard), but you have to walk away with only your understanding. In particular, write the solution up on your own. Please write on your assignment the names of any other collaborators you worked with.

Certain problems will be computational in nature and can be solved using a computer algebra package; please print out and attach complete code and output.

Plagiarism, collusion, or other violations of the Academic Honor Principle, after consultation, will be referred to the The Committee on Standards.

Final project

A final research project will be assigned in place of a final exam. You may work individually or in groups. Choose a chapter or research article on the topic of elliptic curves, write an article summarizing (an interesting part of) its contents, pose a research question naturally arising in this work, and then try to answer it. The approximate length should be 3–20 pages per person, and the intended audience is your peers. Depending on your choice of topic, you may get quite far into this sequence or you may have to stop after the summary itself. Further details will be forthcoming and posted on the course webpage.

Class participation and preparedness

You are expected to read the section before we cover it in class. Come with good questions! Your participation and preparedness in class is essential for your success.

Religious observances and accommodation

Some students may wish to take part in religious observances that occur during this academic term. If you have a religious observance that conflicts with your participation in the course, please meet with me before the end of the second week of the term to discuss appropriate accommodations.

Students with disabilities, including "invisible" disabilities such as chronic diseases and learning disabilities, enrolled in this course and who may need disability-related classroom accommodations are encouraged to make an appointment to see me before the end of the second week of the term. All discussions will remain confidential, although the Student Accessibility Services office may be consulted to discuss appropriate implementation of any accommodation requested.

Library

A key to successful research is the use of reliable, high-quality information sources. While some information can be found on the open web, the best place to start your research is at the Librarys Mathematics Research Guide, `http://researchguides.dartmouth.edu/math/`. This research guide has the librarys key mathematics resources organized for easy use. The Kresge Physical Science Library website, `Dartmouth.edu/~library/Kresge/`, also has information on useful research tools and services. In addition to the online information, Katie Harding, the Mathematics Librarian, has been assigned to this class to answer research questions and to help you find appropriate resources. Katie can be reached at `katie.harding@dartmouth.edu`.

Syllabus

An elliptic curve is a cubic plane curve with the structure of a group; the group law is defined by geometric formulas.

Elliptic curves are ubiquitous in mathematics, with deep connections between number theory, algebra, geometry, and complex analysis. Their study is rich and they remain a topic of significant ongoing research. They first made an (implicit) appearance in the problem of giving the arc length of an ellipse, hence their name. In number theory, the set of solutions to a cubic equation in two variables with rational solutions is often understood as the set of

rational points of an elliptic curve. From the point of view of manifolds, elliptic curves as Riemann surfaces are (flat) complex tori. In algebraic geometry, elliptic curves are perhaps the simplest nontrivial algebraic varieties. Finally, there are important applications of elliptic curves to cryptography.

In this course, we will survey elliptic curves from an arithmetic point of view. Topics may include: plane curves, basic theory of elliptic curves (Weierstrass equations), elliptic curves over the complex numbers, arithmetic of elliptic curves, and some relationships to modular forms.

A full schedule is available on the course webpage.