AMS Short Course:

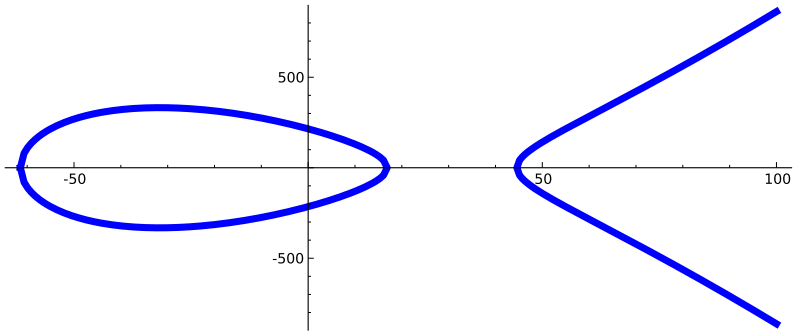
Computing with Elliptic Curves using Sage

Organized by **William Stein**, University of Washington

January 2012 in Boston

1 Introduction

This short course will explore computing with elliptic curves using the free open source mathematical software system Sage. Half of the lectures will be accessible to a general mathematical audience with little prior exposure to elliptic curves, and will provide a good way for mathematicians to learn about Sage in the context of strikingly beautiful mathematics.



An elliptic curve is a curve defined by a cubic equation of the form

$$y^2 = x^3 + Ax + B$$

in two variables x and y. The extent to which elliptic curves play a central role in both pure and applied modern number theory is astounding. Deep problems in number theory such as the *congruent number problem*—which integers are the area of a right triangle with rational side lengths?—translate naturally into questions about elliptic curves. Other questions, such as the famous unsolved *Birch and Swinnerton-Dyer conjecture*, propose startling relationships between algebra and analysis. Elliptic curves also play a starring role in Andrew Wiles's proof of *Fermat's Last Theorem* by arising naturally from any counterexample to the assertion. In a more applied direction, the abelian groups attached to elliptic curves over finite fields are extremely advantageous in the construction of public-key cryptosystems. In particular, elliptic curves are widely

believed to provide good security with small key sizes, which is useful in applications—if we are going to print an encryption key on a postage stamp, it is helpful if the key is short!

Sage (see `http://sagemath.org`) is a free open-source mathematics software system licensed under the GNU Public License. It has extensive capabilities for computing with elliptic curves. Sage is built out of around 100 open-source packages and features a unified interface. Sage can be used to study elementary and advanced, pure and applied mathematics. This includes a huge range of mathematics, including basic algebra, calculus, elementary to advanced number theory, cryptography, numerical computation, commutative algebra, group theory, combinatorics, graph theory, exact linear algebra and much more. It combines various software packages and seamlessly integrates their functionality into a common experience. It is well suited for education and research. The user interface is a notebook in a web browser or the command line. Using the notebook, Sage connects either locally to your own Sage installation or to a Sage server on the network. Inside the Sage notebook you can create embedded graphics, beautifully typeset mathematical expressions, add and delete input, and share your work across the network.

Topics covered in the course may include:

1. How to program Sage using Python.
2. How to use databases of elliptic curves with Sage.
3. How to construct and work with public-key cryptosystems using elliptic curves over finite fields. How to count points on elliptic curves over finite fields.
4. How to compute quantities appearing in the Birch and Swinnerton-Dyer conjecture: torsion points, Tamagawa numbers, Mordell-Weil groups, L-series, etc.
5. How to compute p-adic L-series and p-adic regulators, and use them to bound Shafarevich-Tate groups.

2 Lecture Series

2.1 Introduction to Python and Sage

Kiran Kedlaya, UC San Diego

Kedlaya will give an overview of how to use Sage using the Python programming language. No prior knowledge of Python or Sage will be assumed.

2.2 Computing with elliptic curves over finite fields using Sage

Ken Ribet, UC Berkeley

Ribet will explain how to use Sage to perform the sort of computations with elliptic curves over finite fields that are needed to follow along with a cryptography book and do exercises that involve long computations.

2.3 Computing with elliptic surfaces

Noam Elkies, Harvard University

Elkies's lectures will link some of the same arithmetical ideas that appear in the other lectures with other mathematical topics including algebraic geometry of surfaces, Euclidean and hyperbolic lattices, etc., that either are already or should be in Sage. This topic will also touch on elliptic curves of high rank, since every rank record is obtained by specialization from an elliptic surface (or possibly an elliptic curve over $\mathbf{P}^n$ for some $n > 1$).

2.4 Computing with Shafarevich-Tate Groups using Sage

Jared Weinstein, Boston University

The Shafarevich-Tate group is the most mysterious invariant attached to an elliptic curve. Weinstein will explain how to use Sage to compute information about Shafarevich-Tate groups. His talk may touch on work of Heegner, Kolvyagin, Kato, Schneider, Mazur and others.

2.5 Using Sage to explore the Birch and Swinnerton-Dyer conjecture

William Stein, University of Washington

Stein will introduce the Birch and Swinnerton-Dyer conjecture via the congruent number problem. He will then discuss how to use Sage to compute Mordell-Weil groups, values of L-functions, regulators, heights, and Tamagawa numbers. He will also talk about computing the Birch and Swinnerton-Dyer invariants for various tables of elliptic curves.