Topics in Number Theory: Elliptic Curves

January 13, 2020

`http://math.colorado.edu/∼kstange/teaching.html`

1 Course Description

Arithmetic geometry is the study of rational and integer points on algebraic varieties. Elliptic curves are, perhaps, the best place to start: there's a great deal we know, and a great deal we don't. I'll follow Joseph H. Silverman's *The Arithmetic of Elliptic Curves.* We'll begin with a down-and-dirty practical approach to the basics of algebraic curves, with an emphasis on example and computation (and not proofs). Then we will cover the group law (the points on an elliptic curve form a group), isogenies between curves, the structure of the group of rational points over various fields, including $\mathbb{C}$, number fields, and finite fields. We will prove the Mordell-Weil Theorem describing this structure over $\mathbb{Q}$, and discuss further topics TBD. I will also discuss cryptographic aspects of elliptic curves, including now-standard elliptic curve cryptography and pairing-based cryptography, as well as post-quantum isogeny-based cryptography.

2 Pre-requisites

I will assume knowledge of the algebra pillar sequence, but a motivated student in the second half of this sequence could play catch-up. In particular, I will assume Galois theory. I will state and use results from algebraic number theory as needed, so that course is a benefit, but not required. I will not assume algebraic geometry, but that will also enhance the enjoyment of the student.

3 Resources

The primary resource will be *The Arithmetic of Elliptic Curves* by Joseph H. Silverman, preferably the 2nd edition (homework problems may be from here). Try Springerlink for online version.

4 Credit

Students seeking credit will be required to complete and present homework. Homework will be on the order of approximately one problem per lecture. This is not to be handed in. Instead, students will participate in homework presentation sessions. Approximately once every three weeks, students will present homework solutions in class (for a total of approximately 5 sessions). The presenter will be chosen by a roll of dice. Students are also expected to be part of a productive classroom atmosphere, and provide feedback on each others' solutions.

To pass the course, students must present solutions at least half the time they are called to do so. To earn an A, students must present solutions at least 3/4 of the time they are called to do so.