Final Project: The group law on elliptic curves, and finding rational and integral points

Written by Jonathan Hanke

February 14, 2005

Abstract

In class we will briefly study the integer and rational solutions of the Diophantine equations $y^2 = f(x)$ where $f(x)$ is some cubic polynomial. This solutions of such equations are called elliptic curves, and understanding them is a very rich area of number theory. (For example, they were used to prove Fermat's Last Theorem!) It is an amazing fact that you can use lines to define an addition operation on the rational points on an elliptic curve, which helps us to answer questions like: "How many rational points are there on an elliptic curve?" and "What do they look like?". For a given elliptic curve, one can use this (and other) ideas to try to find all of of its rational (and integral) points. Your project should describe the addition law for elliptic curves, and some techniques for finding and understanding their integral and rational points. Using these methods, you should compute the rational an integral points for a few different examples. Along the way, you will also be able to use a simple version of this idea to find all rational points on any conic (circle, ellipse, or hyperbola). **[4-5]**

The following is a rough outline which may be useful in thinking about/organizing your project. Good references for the general theory are [2] and [1,], while elliptic curves are mentioned much more briefly in [,] and [,]. If you have any questions about your project and/or readings, feel free to let me know, and we can setup a time to talk about it. Have Fun! =)

1. **Projective space and Weierstrass form**
2. **Defining the group law**
3. **The structure of the rational points**
4. **Computing the torsion and the rank**
5. **Finding integral points**
6. **Examples**

References

[1] Anthony W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.

[2] Joseph H. Silverman and John Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

