Douglas Ulmer
School of Mathematics
Georgia Institute of Technology
Undergraduate Research Project, Spring 2010

Overview: The project involves making some computer calculations to gather evidence about a question in the theory of elliptic curves. At a minimum, this will require identifying a suitable software package, writing and testing some code, teaching me how it works, and collecting data on the question. It is possible that the data and algorithms used to generate it may lead to enough insight to prove a theorem. The project can be done for pay (roughly ten hours per week, $10 per hour) or for credit (3 units).

Prerequisites: Solid command of linear algebra and basic abstract algebra, including finite fields. Ability to write efficient and understandable computer code. Good communication skills.

Mathematical background: Let K be a field. Roughly speaking, an elliptic curve E over K is given by a cubic equation in two variables with coefficients in K. For example, when $K = \mathbf{Q}$, we can consider $y^2 = x^3 + 2x - 7$. The set of solutions to the equation can be made into an abelian group via a geometrically defined law of addition.

We are most interested in the case when K is a so-called global field, namely a finite extension of $\mathbf{Q}$ or a finite extension of $\mathbf{F}_p(t)$, the field of rational functions with coefficients in the field of p elements, p a prime number. A big theorem in the theory of elliptic curves says that when K is a global field, then the group of points on any elliptic curve over K is *finitely generated*. That means starting from a finite set of solutions, we can get all solutions by repeated additions and subtractions in the group law. We write $E(K)$ for the group of points with coordinates in K.

For the project, we fix an odd prime number p and we have a specific elliptic curve E over the field $\mathbf{F}_p(t)$. For each power $q = p^{2f}$ of p^2, we have a collection of explicit points with coordinates in $K = \mathbf{F}_q(t)$. I want to know whether these points generate the entire group of points with coordinates in K. General theory tells me that the index of the group generated by the points I have in the full group is a power of p. General theory also gives me an injective group homomorphism

$$E(K)/pE(K) \to H$$

where H is some vector space over $\mathbf{F}_p$. Let's call our explicit points $P_1, \dots, P_n$ and let's write V for the vector space over $\mathbf{F}_p$ with basis $P_1, \dots, P_n$. There is an obvious homomorphism $V \to E(K)/pE(K)$ and our points $P_1, \dots, P_n$ generate $E(K)$ if and only if this map is an isomorphism; for dimension reasons it is equivalent to show that it is injective, and this in turn is equivalent to the injectivity of the composed map

$$V \to E(K)/pE(K) \to H.$$

Now the vector space H and the map $E(K)/pE(K) \to H$ have rather fancy definitions, but ultimately everything can be boiled down to explicit formulas involving operations in the polynomial ring $\mathbf{F}_q[t]$ and taking derivatives. The formulas are compact, but too complicated to evaluate by hand in any but the simplest cases. They should, however, be quite doable by machine computation. So the project is to compute explicitly the images of the points P_i in H for several small values of p and $q = p^{2f}$ and check whether $V \to H$ is 1-1. If it is not 1-1, there is the further interesting question of finding more points on $E(K)$.

Software: Part of the project is to choose a suitable package. It should be capable of making calculations in finite fields $\mathbf{F}_q$ where q is a prime power (not just a prime number) and to handle compound objects like polynomials or rational functions over $\mathbf{F}_q$. My guess is that the open-source platform SAGE is likely to be the best choice.

Timeframe: I would like to get started in January and I expect that the project could extend over most of the Spring semester.

Contact info: Doug Ulmer, Professor of Mathematics, `ulmer@math.gatech.edu`, 404-894-2747, Skiles 118B.