Many Cheerful Facts

Organizer(s): Yael Degany and Jason Ferguson

Friday, 2:10–3:00pm, 939 Evans

April 2 **Andrew Niles**, UC Berkeley

A Basic Introduction to Elliptic Curves

An elliptic curve is a smooth projective curve of genus 1, with a specified basepoint. Concretely and conveniently, we can view an elliptic curve as a particular type of plane cubic curve. It turns out that there is a natural way of putting the structure of a group on the set of rational points of an elliptic curve, and this allows us to say some very interesting things about the possible solutions to its defining equation. In this talk I will start with the basic definitions, illustrate the group law, and discuss some of the remarkable results that have been proven. Time permitting, I will discuss some applications, particularly to cryptography.

The only background I will assume is some knowledge of abstract algebra (groups, rings and fields); a few things I say will make more sense if you know about projective space.