Elliptic curves

Daniel Linssen, Department of Mathematics, Macquarie University

For my project I studied elliptic curves and how they can be used in factorizing numbers. My project focused primarily on Lenstra's elliptic curve algorithm as well as some related topics. This algorithm is difficult to summarize but deals with some nice properties of groups of points which lie on a particular elliptic curve and have coefficients in the modular integers. As such my project interwove many areas of mathematics such as algebra (using groups and fields), geometry (working with elliptic curves and calculating the group operation) and number theory (Lenstra's algorithm itself).

I familiarized myself with the programming language PARI, which has been designed to optimize the computations often used in number theory. For my own understanding, I spent a lot of my time writing a program in PARI which tries to determine the prime factors of any given number using Lenstra's elliptic curve algorithm. The program was usually able to factorize numbers with up to 35 digits in a matter of seconds, but it slowed down exponentially when trying to factorize numbers with more digits. Still, it was rewarding to be able to write a program which could factorize enormous numbers (for example, numbers such as 23090867707670165315648830903132 1599).

I spent the remainder of my time investigating the success rate and speed of my algorithm, and both theoretically and experimentally how this could be improved. I found that, when working with numbers of a very large magnitude, seemingly trivial improvements (such as how a product was calculated) could often increase my program's running time by more than ten-fold.

The Big Day In itself was a great opportunity to meet mathematics honours students from other universities. It also gave me the chance to attend a wide range of interesting presentations, both from mathematics as well as other science divisions. While I found the material in my project difficult at times, it was interesting and satisfying, and I was introduced to areas of mathematics I wouldn't have otherwise covered in my undergraduate course.

Daniel was an AMSI/MASCOS vacation scholar for 2007-8.