INTERNATIONAL CENTRE
OF EXCELLENCE FOR
EDUCATION IN
MATHEMATICS

Rational points on elliptic curves

Gareth White, School of Mathematics and Statistics, University of Sydney

Over the Summer holidays I had the opportunity of undertaking a vacation scholarship in the area of number theory and elliptic curves, under the guidance of Martine Girard at Sydney University.

My main reference during this scholarship was the book by Silverman and Tate, ``Rational Points on Elliptic Curves''. With much help from this book, I studied the relationships between elliptic curves, algebra, number theory, and geometry. Some of the areas that I focused on were:

- Weierstrass normal form, and how projective transformations can be used to obtain elliptic curves of this form from any degree 3 curve.
- Addition of points on elliptic curves, and how it is a group action.
- Rational points on elliptic curves, and how they form a group under addition. In particular, I studied Mordell's Theorem, which states that the group of rational points is finitely generated.
- Integer points, and methods of finding them.
- Integer points of finite order, and properties of the group that they form.
- The height of points on an elliptic curve, and its properties.
- The behaviour of elliptic curves over finite fields.
- Complex multiplication.

As part of my studies, I learnt the school's mathematical programming language MAGMA, which enabled me to quickly calculate certain properties of elliptic curves such as height, order, and rational point solutions.

Elliptic curves have an increasing importance in modern mathematics. They were used to prove Fermat's Last Theorem, and are being used extensively in important fields such as cryptography.

Gareth received an ICE-EM Vacation Scholarship in January 2005.
See www.ice-em.org.au/students.html#scholarship.