# Elliptic Tales: Curves, Counting and Number Theory



26 April 2012

In mathematics, numbers such as 0, ±1, ±2, ±3 are called integers, and ratios of two integers such as 1/3 and -2012/2011 are called rational numbers. Number theory is a branch of mathematics, and determining solutions of an equation within the rational numbers is one of the main subjects in number theory. For example, $3x^2-2y^2=1$ is an equation, and it is fairly easy to find a pair of rational solutions: $x=1$ and $y=1$. However, it may not be so easy to find pairs such as $x=163/197$ and $y=143/197$, and $x=683/725$ and $y=661/725$. In fact, there are infinitely many pairs of solutions to this equation, and Avner Ash and Robert Gross' book begins with the algorithm that reaches all of them.

The algorithm is enlightening and requires only basic algebra to understand. If all of this sounds interesting to you, and if you have done first-year calculus, you may thoroughly enjoy reading this book, which offers "tales" of the mathematical ideas surrounding an equation called an elliptic curve.

The equation $3x^3-2y^2=1$ is an example of an elliptic curve. It is very similar to the earlier example, but simply has a one-higher exponent. One of the stranger things about elliptic curves is that the solutions are much harder to find than in the case of exponent 2 shown above, and no one has yet managed to figure out an algorithm that can solve all of them. The difficulties of computing the complete set of solutions to an elliptic curve have been beautifully formulated into a mathematical object called the Tate-Shafarevich group, and this elegant and sophisticated theory surrounding elliptic curves has been one of the key attractions for many modern mathematicians who study them. Imagine yourself using a telescope to measure the size of the complete set of solutions to an elliptic curve that is located in a galaxy far, far away. Then, this Tate-Shafarevich group gets stuck to the elliptic curve and blurs the image on your telescope, preventing you from correctly measuring the size.

As in science, some developments in number theory are driven by experimental results, and this book introduces a beautiful example of this approach, the Birch and Swinnerton-Dyer conjecture, or BSD. In essence, this conjecture introduces a different lens for our telescope that filters out the Tate-Shafarevich group. This problem is the first of the seven Millennium Prize Problems announced by the Clay Mathematics Institute in 2000 and it has not been solved yet: when it is, it will bring the successful mathematician a $1 million (£630,000) prize. Number theory is a source of many beautiful mathematical ideas, including complex numbers, modular forms, commutative algebra and algebraic geometry, and this book's main goal is to introduce a general audience to some of the ideas in number theory that surround elliptic curves and that build up to the statement of BSD.

The authors of *Elliptic Tales* do a superb job in demonstrating the approach that mathematicians take when they confront unsolved problems involving elliptic curves. Establishing the validity and completeness of a method in mathematics sometimes requires a serious development that can be abstract and philosophical. On the one hand, mathematics goes hand in hand with other scientific fields where it is put to practical use, but on the other, the discipline also pursues its own interests, such as abstract construction and the classification of *all* possibilities.

Since the dawn of Einstein's general theory of relativity, which uses quite an abstract mathematical construction, in many fields today where mathematics is deployed, the art of mathematical thinking has become a practical way of intelligently pursuing one's imagination and vision. No one knew until



Printable version
Comment on this story
View comments on all stories

recently that we would be using number theory on an everyday basis for internet security. Indeed, one of the safest systems available today uses - guess what - elliptic curves!

## Elliptic Tales: Curves, Counting and Number Theory

By Avner Ash and Robert Gross. Princeton University Press. 280pp, £19.95. ISBN 9780691151199 and 9781400841714 (e-book). Published 12 March 2012

**Reviewer :**

Sungkon Chang is assistant professor of mathematics at Armstrong Atlantic State University in Savannah, Georgia. His 2005 doctoral thesis concerned "The arithmetic of twists of the jacobians of superelliptic curves".

### Comment on this story

You must fill in all fields marked *

**Story date** 26 April, 2012

**Your Name***

**Your Email***

**Comment***

Post

**Please note:** By adding a comment you confirm that you have read and agreed with the code of conduct under our Terms & Conditions. Comments posted on timeshighereducation.co.uk may be moderated.

Back Print Top