

Finding Rational Points on Elliptic Curves
(Over \mathbb{Q})

Alan Silverster

February 28, 2005

1 History

One substantial part of number theory is Diophantine equations. These are polynomial equations that we wish to solve in terms of integer or rational solutions. They are named after Diophantus of Alexandria, one of the greatest Greek mathematicians who posed many problems of this form. The questions usually asked are

1. Are there any solutions in integers?
2. Are there any solutions in rational numbers?
3. How many integer solutions are there?
4. How many rational solutions are there?

For linear and quadratic equations, we already know the answers to these questions. For a linear equation $ax + by = c$, there are always infinitely many rational solutions. If $\gcd(a, b) \nmid c$, there are infinitely many integer solutions. Otherwise if $\gcd(a, b) \mid c$, then there are no integer solutions. For a quadratic equation, if one can find a rational solution then there are infinitely many rational solutions. But what about elliptic curves

$$y^2 = x^3 + ax^2 + bx + c?$$

The integer and rational number solutions to equations of this form are not completely understood. The description of these solutions usually involve an interesting mix of algebra, number theory, and geometry.

2 Integer and Rational Points

In the 1920's, Siegel showed that an elliptic curve has only finitely many integer solutions. Much later, in 1970, Baker and Coates gave an explicit upper bound on the largest solution, based on the coefficients of the elliptic curve polynomial. Unfortunately, this bound is quite large and generally impractical.

For rational points on elliptic curves, Poincaré conjectured in 1901 that there exists a finite set of points that would generate all of the (possibly infinite) rational points. This was later proved by Mordell in 1923. So far, Mordell's method *often* allows one to find such a finite generating set, but it had not been proven to always work – this is still just a conjecture.

3 This Paper

Let E be an elliptic curve over \mathbb{Q} and let $E(\mathbb{Q}) = \{(x, y) \in E \mid x, y \in \mathbb{Q}\} \cup \{\infty\}$ denote the additive group of rational points on E . What can we say about this group, about its size and structure?

In this paper, we will begin with a brief introduction to the history of Diophantine equations and rational solutions to elliptic curves. We will then proceed to find rational points of order 2 and 3, discuss the group of rational points $E(\mathbb{Q})$ on E , and subgroups of $E(\mathbb{Q})$. Next, we will follow this by introducing the Nagell-Lutz Theorem

Theorem (Nagell-Lutz): Let $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ be an elliptic curve and let D be the discriminant of $f(x)$. If $P = (x, y)$ is a rational point of finite order then x, y are integers and either $y = 0$ or $y \mid D$.

We will quickly develop this theorem and a couple key observations into Mazur's Theorem

Theorem (Mazur): Let E be an elliptic curve and suppose that $E(\mathbb{Q})$ contains a point of finite order m . Then either $1 \leq m \leq 10$ or $m = 12$.

This theorem will give a restriction on the possible subgroups of $E(\mathbb{Q})$.

From here, we will proceed by introducing the concept of the height of a rational number and the method of descents. We will discuss the method of a 2-descent and, time and space permitting, the more general method of p -descents. This will allow us to consider the Mordell-Weil Theorem

Theorem (Mordell-Weil): Let E be an elliptic curve. Then $E(\mathbb{Q})$ is a finitely generated abelian group.

Once we have the Mordell-Weil Theorem, we will consider a few explicit elliptic curves and show how to compute both the torsion subgroup of E and the rank of E . In general, computing the rank of $E(\mathbb{Q})$ is hard, and these examples will demonstrate some of the problems encountered in attempting these calculations.

At this point, again time and space permitting, we may briefly discuss 2-Selmer and Shafarevich-Tate groups by redefining descent in terms of Galois cohomology. Finally, we will state the Birch and Swinnerton-Dyer Conjecture and explain how it relates to the problem of finding rational points on an elliptic curve.

References

- [1] I. Kiming. “Theorem of Nagell-Lutz: The Decisive Lemma”. <http://www.math.ku.dk/~kiming/courses/2003/intro.ell/nagell_lutz2.pdf>
- [2] F. Lemmermeyer. “General 2-Descent”. <<http://www.fen.bilkent.edu.tr/~franz/ta/ta-2d.pdf>>
- [3] J. S. Milne. *Elliptic Curves*. “Chapter 8: Torsion Points”. <<http://www.jmilne.org/math/CourseNotes/math679.pdf>>
- [4] B. Poonen. “Computing Rational Points on Curves”. <<http://math.berkeley.edu/~poonen/papers/millennial.pdf>>
- [5] Á. L. Robledo. “Finding Points on Elliptic Curves: Very Explicit Methods”. <<http://math.bu.edu/people/alozano/finding%20points.pdf>>
- [6] E. F. Schaefer and M. Stoll. “How to do a p -Descent on an Elliptic Curve”. *Trans. Amer. Math. Soc.* Vol. 356, No. 3. pp. 1209-1231.
- [7] J. Silverman and J. Tate. *Rational Points on Elliptic Curves*. Springer: New York. 1992.
- [8] L. Washington. *Elliptic Curves: Number Theory and Cryptography*. Chapman & Hall/CRC: New York. 2003.
- [9] A. Wiles. “The Birch and Swinnerton-Dyer Conjecture”. <http://www.claymath.org/millennium/Birch_and_Swinnerton-Dyer_Conjecture/>