Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Arithmetic Aspects of Elliptic Curves

David Bodiu

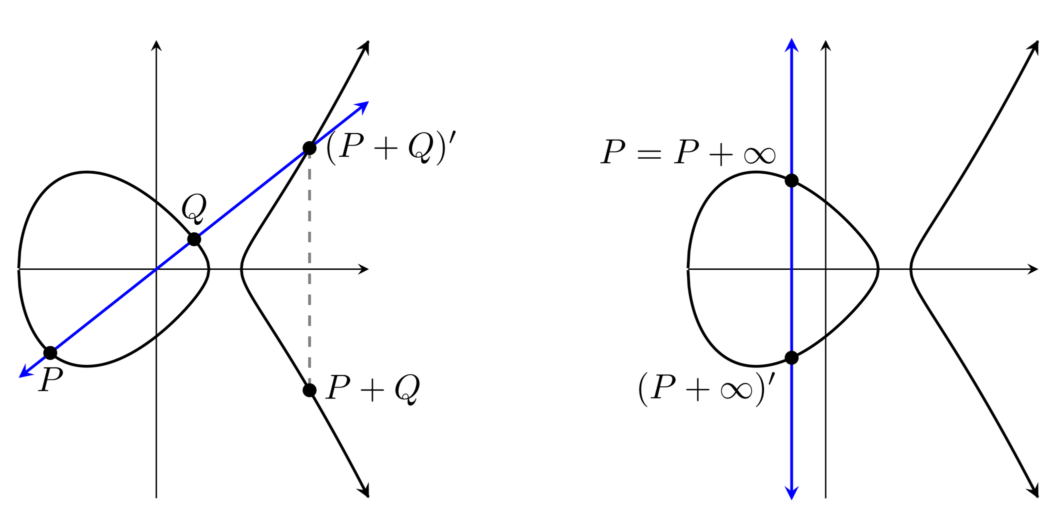
Supervised by Prof. Nicolas Mascot

Introduction

- An *elliptic curve* E over the field $\mathbb{Q}$ is defined by an equation of the form
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
with coefficients $a_i \in \mathbb{Q}$ such that the curve is non-singular.
- Using a suitable change of coordinates, the equation above can be simplified to
$$y^2 = x^3 + Ax + B$$
with $A, B \in \mathbb{Z}$. In this presentation we assume that all elliptic curves E are specified in this form.

The Group Law

- Finding points on E with coordinates in $\mathbb{C}$ or $\mathbb{R}$ is not hard. On the other hand, locating points with coordinates strictly in $\mathbb{Q}$ can be quite difficult.
- If we can locate two rational points P, Q on E, then in general we can draw a line through P, Q which is guaranteed to intersect the curve at another rational point R'.
- Since E is symmetric about the x-axis we can reflect R' to obtain another rational point R. We name this method of obtaining R *addition* and we write $P + Q = R$.



(a) $P + Q$ (b) $P + \infty$

Figure: Addition on elliptic curves

- If we define a point at ∞ so that every vertical line on the plane intersects this point, we see that $P + \infty = P$.
- It can then be demonstrated that $E(\mathbb{Q})$, the set of rational points on E, along with the operation of addition and ∞ as the identity form a group.
- It's not difficult to see that $E(\mathbb{Q})$ is also abelian.

Points of Finite Order

- Let $E_T(\mathbb{Q})$ denote the set of points in $E(\mathbb{Q})$ of finite order (or torsion points). One can show that this forms a subgroup of $E(\mathbb{Q})$.

Example

Consider the elliptic curve E given by $y^2 = x^3 + 4x$. We have the obvious torsion point $(0, 0)$. Performing a quick computer search we also find the torsion points $(2, \pm 4)$. There are in fact no other torsion points implying that
$$E_T(\mathbb{Q}) = \{\infty, (0, 0), (2, \pm 4)\} \simeq \mathbb{Z}_4$$
where the structure is obtained by examining how the points interact with each other.

Lutz-Nagell Theorem

- **Theorem** *(Lutz-Nagell) Let $P = (x, y)$ be a point on E. If $y \neq 0$ then $y^2 \mid 4A^3 + 27B^2$.*
- Using the above result one can demonstrate that $E_T(\mathbb{Q})$ is finite. As a result, $E_T(\mathbb{Q})$ is a finite abelian group so that
$$E_T(\mathbb{Q}) \simeq \mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{k_n}}.$$
- **Theorem** *(Mazur) $E_T(\mathbb{Q})$ is isomorphic to one of the below for all elliptic curves E:*
$$\mathbb{Z}_n \text{ with } 1 \leq n \leq 10 \text{ or } n = 12;$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_{2n} \text{ with } 1 \leq n \leq 4.$$

Points of non-Finite Order

- Write E in the form $y^2 = (x - e_1)(x - e_2)(x - e_3)$ with $e_1, e_2, e_3 \in \mathbb{Z}$. We define
$$\varphi : E(\mathbb{Q}) \to \left(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\right) \oplus \left(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\right) \oplus \left(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\right)$$
$$(x, y) \mapsto (x - e_1, \quad x - e_2, \quad x - e_3)$$
$$\infty \mapsto (1, \quad 1, \quad 1)$$
for points with $y \neq 0$.
- The map φ is a homomorphism with $\ker(\varphi) = 2E(\mathbb{Q})$. This allows us to prove the following:
- **Theorem** *(Weak Mordell-Weil) $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite for all elliptic curves E.*

Mordell-Weil Theorem

- To generalize the Weak Mordell-Weil Theorem we introduce a quadratic form called the *canonical height* of a point, denoted $\hat{h}(P)$.
- Given any constant c there exist only finitely many points P with $\hat{h}(P) \leq c$.
- **Theorem** *(Mordell-Weil) $E(\mathbb{Q})$ is finitely generated for all elliptic curves E.*
- Since $E(\mathbb{Q})$ is a finitely generated abelian group by the above, we must have that
$$E(\mathbb{Q}) \simeq E_T(\mathbb{Q}) \oplus \mathbb{Z}^r$$
where $r \in \mathbb{N}$ is called the *rank* of E.
- The results above are the basis for the descent procedure described to the right-hand side. Making use of a theorem due to Silverman and the height pairing allows us to obtain a generating set also.

Example

Consider the elliptic curve E given by $y^2 = x^3 + 1836x + 11961$. Using the Lutz-Nagell theorem enables us to search through a finite number of possibilities to obtain the torsion point $P = (12, 189)$. We have $2P = (12, -189)$ and $3P = \infty$. Our computer finds no more torsion points therefore
$$E_T(\mathbb{Q}) = \{\infty, (12, \pm 189)\} \simeq \mathbb{Z}_3.$$
Next, using the descent procedure described on the right-hand side we obtain a set of two independent points of non-finite order, namely $(-6, 27)$ and $(39, 378)$. We cannot make this set any larger therefore
$$E(\mathbb{Q}) \simeq \mathbb{Z}_3 \oplus \mathbb{Z}^2$$
with generating set $\{(12, 189), (-6, 27), (39, 378)\}$.

Descent Procedure

1. We have that
$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong E_T(\mathbb{Q})/2E_T(\mathbb{Q}) \oplus (\mathbb{Z}/2\mathbb{Z})^r$$
and
$$|E_T(\mathbb{Q})/2E_T(\mathbb{Q}) \oplus (\mathbb{Z}/2\mathbb{Z})^r| = 2^{t+r}$$
2. The integer t can be determined using the Lutz-Nagell Theorem and associated results by first calculating $E_T(\mathbb{Q})$ and then taking its quotient.
3. We can determine a finite set of possible triples
$$(a, b, c) \in \left(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\right) \oplus \left(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\right) \oplus \left(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\right)$$
which places an upper bound on r.
4. To reduce this bound as much as possible we eliminate triples which do not yield p-adic points for a certain finite set of primes p.
This is done by encoding everything in matrices, applying a few transformations and then solving a final system of linear equations.
5. In most cases the new bound is exact and gives r. To check this we run a computer search to find r independent points of non-finite order in $E(\mathbb{Q})$.
6. We then have that
$$E(\mathbb{Q}) \simeq E_T(\mathbb{Q}) \oplus \mathbb{Z}^r$$
where we have just determined $E_T(\mathbb{Q})$ and r.
7. Finally, to find a set of generators we perform a computer search through a finite (albeit large) set of possible points $P \in \mathbb{Q} \times \mathbb{Q}$ which satisfy
$$\hat{h}(P) < c$$
for a certain constant c, and use the height pairing to check for independence and reduce the set.

References

[1] Collaboration, The LMFDB. The L-Functions and Modular Forms Database. 2022, http://www.lmfdb.org.

[2] Washington, Lawrence C. Elliptic Curves: Number Theory and Cryptography. Chapman and Hall/CRC, 2008.