On the Torsion Subgroup of an Elliptic Curve

Zachary DeStefano

S.U.R.E. Presentation

October 15, 2010

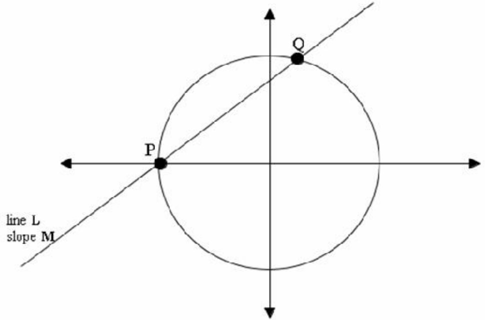
Linear Equations

Consider line $ax + by = c$ with $a, b, c \in \mathbb{Z}$

- Integer points exist iff $gcd(a, b)|c$
- If two points are rational, line connecting them has rational slope.

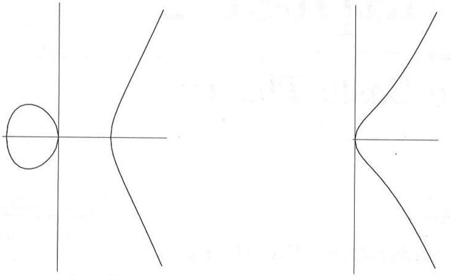
Rational Points on Conics

1. Find a rational point P
2. Draw a line L through P with slope $M \in \mathbb{Q}$



Rational Points on Cubic Curves

Let $E : f(x, y) = 0$ be the zero set of a cubic polynomial in 2 variables with coefficients in $\mathbb{Q}$. What can be said about the rational points $E(\mathbb{Q})$? Can be finite!



(a) $y^2 = x^3 - x$ (b) $y^2 = x^3 + x$

Figure: Elliptic curves drawn in $\mathbb{R}^2$

Weierstrass Normal Form

Any cubic with a rational point can be transformed into a special form called the Weierstrass Normal Form, which is as follows

$$E : y^2 = f(x) = x^3 + Ax + B$$

Any non-singular cubic curve expressable in this form is called an **elliptic curve**. E is nonsingular iff its **discriminant** $D = 4A^3 + 27B^2 \neq 0$.

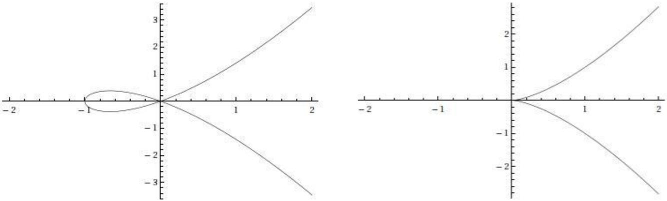


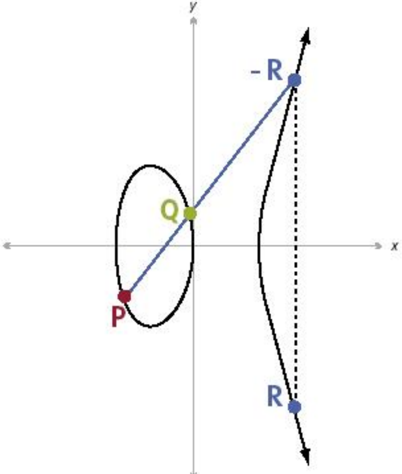
Figure: $y^2 = x^3 + x^2$ (left) and $y^2 = x^3$ (right)

Can try to find new points from old ones on elliptic curves:

- Given two rational points P_1, P_2, draw the line through them
- Third point of intersection, P_3, will be rational

Group Law on Cubic Curves

Define a composition law by: $P_1 + P_2 + P_3 = O$



Composition law gives $E(\mathbb{Q})$ structure of an abelian group, with identity element "point at infinity". In fact:

Theorem

(Mordell-Weil) The group of rational points on en elliptic curve is a finitely generated abelian group: $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$.

Formulas for the group law

Explicit formulas exist for the group law

- If $P = (x, y)$ then $-P = (x, -y)$.
- $P_1 + P_2 = -P_3$
- Line through P_1 and P_2 is $y = \lambda x + \upsilon$
- x-coord. of P_1, P_2, P_3 are roots of $(\lambda x + \upsilon)^2 = f(x)$
- If $P_1 = P_2$ then λ is slope of tangeant
- If $P_1 \neq P_2$ then λ is slope of line through them

Points of Order Two

The order $m \in \mathbb{Z}^+$ of point P is lowest number for which $mP = O$.
Points where $m = 2$:

- If $2P = O$ then $P = -P$ so $y = 0$
- Roots of $f(x)$ gives those points.
- Either 0, 1, or 3 of these points in curve

The Discriminant

The discriminant of $f(x)$ is

$$D = 4A^3 + 27B^2.$$

If $\alpha_1, \alpha_2, \alpha_3$ are roots of $f(x)$, then

$$D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2.$$

Fact

If $P, 2P$ have integer coordinates, then $y = 0$ or $y|D$.

Points of Finite Order Have Integer Coordinates

In general, for $P = (x, y)$, $x, y \in \mathbb{Z}$ if P has finite order.

Theorem

(Nagell-Lutz strong form) If $P = (x, y)$ has finite order, then $x, y \in \mathbb{Z}$ and $y^2 | D$.

This helps us compute $E(\mathbb{Q})_{\text{tors}}$.

Theorem

(Mazur) If P has order N then $1 \leq N \leq 10$ or $N = 12$.

Proof is very difficult.

Allows us to, combined with Nagel-Lutz, compute $E(\mathbb{Q})_{\text{tors}}$.

Algorithm Summary

There is a simple algorithm for computing $E(\mathbb{Q})_{\text{tors}}$.

1. Find integers y where $y^2|D$
2. For every y found above, find roots of $f(x) - y^2$ to obtain x-coordinates.
3. For every $(x, y) = P$, compute nP where $n = 2, \ldots, 10, 12$
   - If $nP = 0$ then $P \in E(\mathbb{Q})_{\text{tors}}$.
   - If nP has non-integer coordinates, $P \notin E(\mathbb{Q})_{\text{tors}}$

Examples of $E(\mathbb{Q})_{\text{tors}}$

$E : y^2 = x^3 + 5$

- No non-trivial points

$E : y^2 = x^3 + x$

- Only $(0, 0)$ and 0

$E : y^2 = x^3 + 4$

- 3 points
- $O, (0, \pm 2)$

$E : y^2 = x^3 - 43x + 166$

- 7 points
- $O, (3, \pm 8), (5, \pm 16), (11, \pm 32)$

$E : y^2 = x^3 + 4x$

- $(0, 0)$ has order 2
- $(2, \pm 4)$ have order 4

$E : y^2 = x^3 + 1$

- 6 points
- $(-1, 0)$ has order 2
- $(0, \pm 1)$ have order 3
- $(2, \pm 3)$ have order 6