Rational points on elliptic curves

part I – introduction

Miška Kuk. & Jakub Bulín

Spring school of the Department of algebra 2010

Outline

Diophantine equations

- Fermat's Last Theorem: For every $n \geq 3$, the equation

$$X^n + Y^n = Z^n$$

has no solutions in non-zero integers X, Y, Z.
(Equivalently, the only rational solutions of $x^n + y^n = 1$ are such that $x = 0$ or $y = 0$.)

- Bachet's equation: let $c \in \mathbb{Z}$ be fixed

$$y^2 - x^3 = c$$

duplication formula – from one rational solution we can obtain "geometrically" infinitely many ones

Diophantine equations

- A *diophantine equation* in n variables is an equation of the form

$$f(x_1, \ldots, x_n) = 0,$$

  where f is a polynomial with integer coefficients.
- Questions:
  - Are there any integer solutions?
  - Are there any rational solutions?
  - Are there infinitely many integer solutions?
  - Are there infinitely many rational solutions?

Algebraic curves

- a *rational algebraic curve* is the set of real solutions to the equation $f(x, y) = 0$, where $f \in \mathbb{Q}[x, y]$
- solutions to a diophantine equation = rational points on an algebraic curve

Rational points

- a point $(x, y) \in \mathbb{R}^2$ is *rational*, if $x, y \in \mathbb{Q}$
- a line $ax + by = c$ is *rational*, if $a, b, c \in \mathbb{Q}$

Observation

- *a line connecting two rational points is a rational line*
- *the intersection of two rational lines is a rational point*

Some easy cases

- $n = 1$: polynomials in one variable
- $deg(f) = 1$: linear equations
- $deg(f) = 2$: quadrics (conics, ...)
- But: in general, even for $n = 2$ the problem whether a given diophantine equation has an integer solution is undecidable.

Rational points on conics

- rational algebraic curves of degree two = rational conics
- Given a rational conic, we can describe all of its rational points:
  - there is a procedure to determine if there exists at least one rational point O (Legendre's theorem)
  - take any rational line L and project the conic onto L from O
  - rational points on the conic correspond to rational points on the line
  - we get a parametrized description of rational points on the conic

Outline

Elliptic curves

The first interesting case: $n = 2$, $deg(f) = 3$:

- rational curves of degree three = *elliptic* (or *cubic*) curves
- an elliptic curve C is *non-singular*, if each point of C has a well-defined tangent
- if C is singular, we can do similar trick as with the conics

The singular case

Let C be an elliptic curve with a singular point S.

- take any rational line L such that $S \notin L$
- project C onto L from $S \longrightarrow$ we get a parametrized description of the rational points on C

In the following, we will consider non-singular elliptic curves with at least one rational point.

Projective plane

The real projective plane:

$$\mathbb{P}^2 = \{\langle(x, y, z)\rangle : (0, 0, 0) \neq (x, y, z) \in \mathbb{R}^3\}$$

Affine part of $\mathbb{P}_2$ = the plane given by $z = 1$ In the projective plane every two distinct lines intersect at precisely one point. Moreover:

Theorem (Bezout)

Let C_1, C_2 be two projective curves with no common components. Then

$$\sum_{P \in C_1 \cap C_2} \textit{multiplicity of } P = \textit{deg}(C_1) \cdot \textit{deg}(C_2).$$

A point $X \in \mathbb{P}^2$ is *rational*, if X is a rational line in $\mathbb{R}^3$, i.e., $X = \langle(p_1, p_2, p_3)\rangle$ for some $p_1, p_2, p_3 \in \mathbb{Q}$.

The group operation

Let C be a non-singular elliptic curve with a rational point O.

- every line meets C at three points
- for $P, Q \in C$ rational, let L be the line connecting P and Q (the tangent at P if $P = Q$)

$$P \star Q := \text{ the third point of the intersection of } L \text{ with } C$$

- $P + Q := O \star (P \star Q)$ is a group operation on the set of rational points of C
- to prove associativity, we need the following

Lemma

Let C, C_1, C_2 be elliptic curves. If C goes through eight points of $C_1 \cap C_2$, then it also goes through the ninth intersection point.

- if we start with different rational point O', we get isomorphic groups

Mordell's theorem

In the future talks...

Theorem

If a non-singular elliptic curve has a rational point, then the group of its rational points is finitely generated.

Outline

Weierstrass normal form

- idea: change the coordinate system so that the polynomial for C in the new coordinates is simpler
- Weierstrass normal form: $y^2 = x^3 + ax^2 + bx + c$
  classical WNF: $y^2 = 4x^3 - g_2x - g_3$

Proposition

Each elliptic curve C with a rational point O is birationally equivalent to a curve in WNF.

- birationally equiv. $=$ the new coordinates are rational functions of the old ones; thus the "rationality" of points is preserved
- the point O becomes a point at infinity, namely the vertical direction
- the transformation is not linear, but the groups of C and C' are isomorphic

Explicit formulas for the group operations

If C is in Weierstrass normal form,

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

then

- $O = \langle(0, 1, 0)\rangle =$ "vertical direction" is rational, we use it as the neutral element
- C is symmetric along the x axis
- we can express the group operations by simple formulas

Let $P = (x, y), Q = (x', y') \in C$ be rational. Then $-P = (x, -y)$, and if the line connecting P and Q is given by $y = \lambda x + \nu$, then $P + Q = (x'', y'')$, where

$$x'' = \lambda^2 - a - x - x',$$
$$y'' = \lambda x'' + \nu$$

Excercises & thanks

$$P + Q = (\left(\frac{y' - y}{x' - x}\right)^2 - a - x - x',$$
$$\frac{y' - y}{x' - x}\left[\frac{y' - y}{x' - x}^2 - a - x - x'\right] + y - \frac{y' - y}{x' - x}x)$$

Thank you for your attention!