Seminar on Elliptic Curves

Markus Schwagenscheidt
ETH Zürich
mschwagen@ethz.ch
www.markus-schwagenscheidt.de

September 2023

Organisation

Organisation

- The seminar takes place **Tuesdays 14:15 - 16:00 in CHN D 42**
- The first talk will be on **Oct. 3rd**.
- 12 talks in total (last talk on Dec. 19)
- Talks should be between **80 and 90 minutes**.
- Two students share one talk.
- Lecture notes of the talks (written in LaTex) are required (10-15 pages).
- The talks and notes should be in english.
- Board or beamer talks are possible.
- We'll meet one week before the talk to discuss the topic.

General remarks for the talks

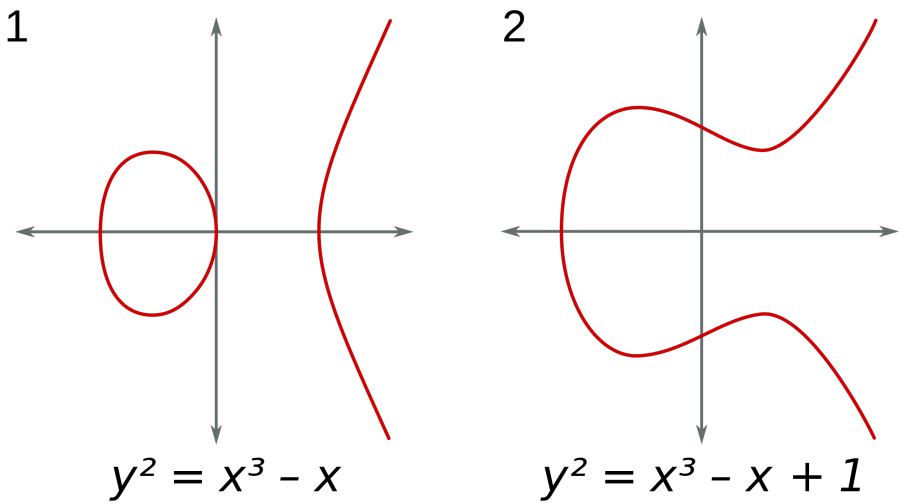
- The references contain a lot of material, so try to emphasize the important things and leave out details and long computations.
- Give examples and draw pictures!
- Do a test talk before the actual talk.
- Try to finish the lecture notes before the talk.
- Try to give a talk that you would like to listen to yourself.

Elliptic curves

- An elliptic curve C is a non-singular cubic plane curve.
- It given by the set of all $(x, y) \in \mathbb{C}^2$ satisfying an equation of the form

$$C : ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

with $a, b, c, d, e, f, g, h, i, j \in \mathbb{C}$.



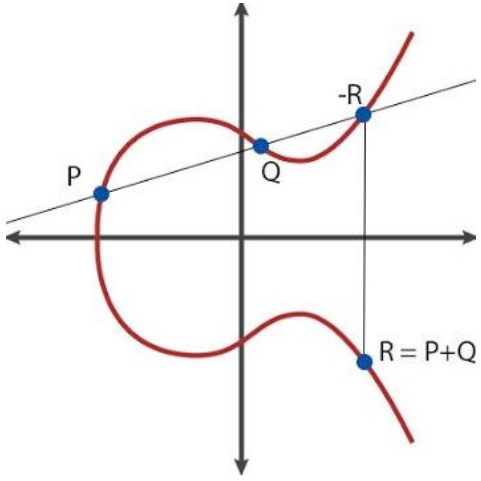
- By a change of variables one can transform the above equation into *Weierstrass normal form*

$$C : y^2 = x^3 + ax^2 + bx + c$$

with $a, b, c \in \mathbb{C}$.

The addition law

- One can define an addition law on an elliptic curve C, which turns it into an abelian group.



- The group law can also be described by explicit formulas.

Rational elliptic curves

- Let C be a *rational* elliptic curve, i.e.

$$C : y^2 = x^3 + ax^2 + bx + c, \qquad a, b, c \in \mathbb{Q}\,.$$

- We can ask for *rational* or even *integral* points on C (whose coordinates are rational or integral).
- **Example** Integral solutions of $x^2 + y^2 = n$ for $n \in \mathbb{Z}$?
- **Theorem** (Mordell) The set $C(\mathbb{Q})$ of rational points is a finitely generated abelian group. In particular, it is of the form

$$C(\mathbb{Q}) = C(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$$

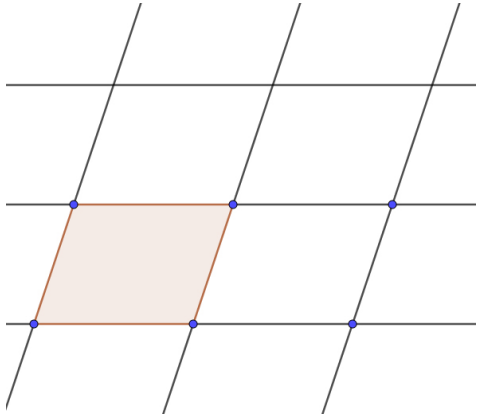
  for some $r \in \mathbb{N}_0$, which is called the rank of $C(\mathbb{Q})$.
- The group $C(\mathbb{Q})_{\text{tors}}$ of points of finite order can be determined using the Nagell-Lutz Theorem.
- **Theorem** (Siegel) A rational elliptic curve has only finitely many integral points. (Note that the integral points do not form a subgroup).
- If a, b, c are integers, we can reduce them modulo a prime p and ask for the points on C in $\mathbb{Z}/p\mathbb{Z}$.

Complex elliptic curves

- A complex elliptic curve C corresponds to a lattice

$$\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$$

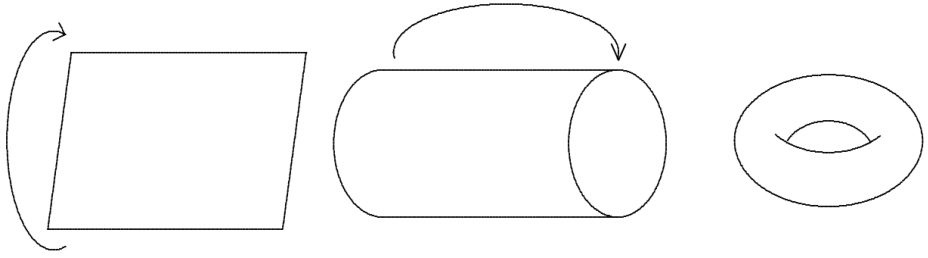
in $\mathbb{C}$ for some $\tau \in \mathbb{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$.



- More precisely, there is an isomorphism of abelian groups

$$C \cong \mathbb{C}/\Lambda_\tau.$$

- This isomorphism is constructed using the theory of elliptic functions, in particular the Weierstrass $\wp$-function.
- Hence, one can identify a complex elliptic curve with a torus.



Fermat's Last Theorem

- In 1995, Andrew Wiles proved Fermat's Last Theorem:
- For $n \geq 3$ the equation

$$x^n + y^n = z^n$$

  does not have any positive integral solutions (x, y, z).
- A major step in the proof is the Modularity Theorem, which states that

every rational elliptic curve is modular

- This essentially means that one can construct a very nice analytic function (a modular form) from every rational elliptic curve.
- In particular, the proof of Fermat's Last Theorem crucially involves elliptic curves.
- Explaining the statement of the Modularity Theorem and its role in the proof of Fermat's Last Theorem will be the topic of one of the last talks.

All talks

1. Cubic curves
2. Points of finite order
3. Heights
4. Mordell's Theorem
5. Cubic curves over finite fields
6. Integral points on elliptic curves
7. Elliptic functions
8. Complex elliptic curves
9. Complex multiplication
10. Modular forms
11. Fermat's Last Theorem
12. The Birch and Swinnerton-Dyer Conjecture

More detailed descriptions can be found on the website

www.markus-schwagenscheidt.de $\rightarrow$ Teaching $\rightarrow$ Elliptic Curves