Seminar Elliptic Curves

Dr. Markus Schwagenscheidt
ETH Zürich
Fall 2023

General informations

The talks should take between 90-100 minutes. Two students share a talk. A script in latex is required. The seminar takes place Tuesdays from 14:15-16:00 in CHN D 42, starting on 03.10. until 19.12. (12 talks).

You can find handouts from the talks of the Elliptic Curves Seminar 2020 on the website

`https://people.math.ethz.ch/~mschwagen/ellipticcurves`

Topics

1. Cubic curves (L. Marconi, M. Mittelholzer)

Introduce cubic curves; explain addition on cubic curves and sketch the proof of associativity; show that every cubic curve can be put into Weierstrass normal form; give explicit formulas for the addition of two points on elliptic curves, and in particular give the duplication formula.

References: [7], Chapter I, Sections 2–4.

2. Points of finite order (M. Imris, N. Navea de Grahl)

Determine the points of order two and three; define the discriminant; state the Nagell-Lutz Theorem and sketch the proof; give examples of the use of the theorem; state Mazur's Theorem.

References: [7], Chapter II, without Section 2.

3. Heights (J. Roshardt, M. Schlatter)

Define the height; state Lemmas 1–3 and give their proofs (see [7], III.1–3); omit the Descent Theorem (this will be covered in the next talk).

References: [7], Chapter III, Sections 1–3.

4. Mordell's Theorem (A. Weidmann, C. Wolter)

State Mordell's Theorem; give the homomorphism in the Proposition in [7], III.4, but omit the proof; state Lemma 4 and the main ingredients for its proof (see [7], III.5; you will have to omit many details); state and prove the Descent Theorem (see [7], III.1) and thereby finish the proof of Mordell's Theorem.

References: [7], Chapter III, Sections 1 and Sections 4–5.

5. Cubic curves over finite fields (P. Edera, F. Hoffmann)

Introduce cubic curves over finite fields $\mathbb{F}_p$; explain how to find all rational points; state the Hasse-Weil Theorem; discuss the Theorem of Gauss on the number of integral points of $x^3 + y^3 = 0$ and sketch the proof (but omit many computations); state and prove the 'Reduction Mod p Theorem' and give some examples; briefly explain good and bad reduction, and the different types of possible bad reduction (nodal, split and non-split multiplicative).

References: [7], Chapter IV, Sections 1–3; [5], Chapter II, Section 3

6. Integral points on elliptic curves (I. Sofronova, L. Zegg)

Give examples that elliptic curves may have integral points of infinite order, and that multiples of integral points need not be integral; state Siegel's Theorem; state Thue's Theorem ([7], V.3, on p. 152) and explain how its proof can be reduced to Thue's Diophantine Approximation Theorem. Give the outline of the proof of the Diophantine Approximation Theorem.

References: [7], Chapter V

7. Elliptic functions (R. Ziegler, M. Gong)

Introduce lattices in $\mathbb{C}$ and some of its most important properties (but omit many details, in particular [2], I.§1.7); define elliptic functions, mention that they form a field, and give Liouville's Theorems; introduce the Weierstrass $\wp$-function and some of its properties, in particular its analytic properties from from [2], I.§2.3; omit discussions of convergence and the Laurent expansion, but explain the differential equations, in particular **Korollar F** in [2], I.§3.

References: [2], Chapter I, §1-§3

8. Complex elliptic curves (N. Goldhirsch, P. Golliard)

Introduce Eisenstein series; explain how they behave under scaling of the lattice and why it suffices to consider lattices of the form $\mathbb{Z}\tau + \mathbb{Z}$ with $\tau \in \mathbb{H}$; state the transformation of $\wp$ and Eisenstein series under $\mathrm{SL}_2(\mathbb{Z})$; introduce the discriminant and the j-invariant; give the addition law for the $\wp$-function and sketch the proof; explain how an elliptic curve over $\mathbb{C}$ can be identified with $\mathbb{C}/\Omega$ for a suitable lattice Ω; explain why the set of all elliptic curves over $\mathbb{C}$ can be parametrized by $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$.

References: [2], Chapter I, §1.7 and §3-§5

9. Complex multiplication (M. Jauch, G. Wolff)

Define isogenies between complex elliptic curves; explain that the isomorphism class of complex elliptic curves are determined by their j-invariants; define elliptic curves with complex multiplication, and show that their endomorphism rings are orders in imaginary quadratic fields (you might want to recall some basic facts about imaginary quadratic fields); omit the part about automorphisms in [8]; state the Main Theorem of Complex Multiplication (Theorem 4.1 in [8]) and compare it to the Kronecker-Weber Theorem about the abelian extension of $\mathbb{Q}$.

References: [8]

10. Modular forms (A. Guadagnini, S. Bhat)

Define modular forms of weight k for $\mathrm{SL}_2(\mathbb{Z})$; define Eisenstein series, the Delta function, and the j-function, and compare them to the earlier definition as functions on lattices; give the Fourier expansion of the Eisenstein series as an example; explain briefly why spaces of modular forms are finite dimensional; introduce the L-function of a modular form and state its meromorphic continuation and functional equation; sketch the proof if time permits.

References: [2], Chapter II, §1-§4

11. Fermat's Last Theorem (C. Graf, J. Guillan)

Explain Fermat's Last Theorem and give a historical overview on proofs of special cases; explain the outline of Wiles' proof and its connection to elliptic curves and modular forms; in particular, explain what the sentence 'every rational elliptic curve is modular' means in terms of L-series.

References: [3]

12. The Birch and Swinnerton-Dyer Conjecture (L. Mombelli, C. Tschopp)

Recall Mordell's Theorem, the definition of the rank of a rational elliptic curve, and its meaning for the number of rational points; explain the content of the Birch and Swinnerton-Dyer Conjecture; give some historical overview and some remarks on the state of the Conjecture; explain the application to the Congruent Number Problem via Tunnell's Theorem.

References: [4]

Contact

Dr. Markus Schwagenscheidt, mschwagen@ethz.ch
`https://people.math.ethz.ch/~mschwagen/ellipticcurves23`

Literatur

[1] Knapp, *Elliptic Curves*

[2] Koecher, Krieg, *Elliptische Funktionen und Modulformen*

[3] Kramer, *Der große Satz von Fermat – die Lösung eines 300 Jahre alten Problems*, available online

[4] Kramer, *Die Vermutung von Birch und Swinnerton-Dyer*, available online

[5] Milne, *Elliptic Curves*, available online

[6] Silverman, *The Arithmetic of Elliptic Curves*

[7] Silverman and Tate, *Rational Points on Elliptic Curves*

[8] Waldschmidt, *Elliptic Curves and Complex Multiplication*, available online