Dies ist eine Inhaltsverzeichnis mit Referenzen der Vorlesung *Elliptische Kurven* im Somersemester 2014.

1. Motivation: Diophantische Gleichungen, Pythagoräische Tripel, Beispiele von Gleichungen von Grad 3 [5, Intro, § I.1].

2. Ebene projektive Kurven: Der projektive Raum $\mathbb{P}^n_K$, Definition von ebene projektive Kurven und Eigenschaften (irredizibel, rediziert, glatt, rational), homogenisieren[5, Appendix § A.1+2].

3. Elliptische Kurven und das Gruppengesetz: Definition, Diskriminante, Gruppengesetz, Duplikationsformel, [5, § I.2+4], [4, § I.3] und Skript.

4. Schnittmultiplizitäten und der Satz von Bézout: Definition des Schnittmultiplizität einer Gerade mit einer beliebigen Kurven und Beweis des Satzes von Bézout in diesem Fall. Beweis der Assoziativität des Gruppengesetzes, [5, § A.3+4], [4, § I.1].

5. Intermezzo: Elliptische Kurven und Kryptographie: Das ECDLP ([6], [2, § 5.3-4]), Lenstras Faktorisierungsalgorithmus, [5, § IV.4], [2, § 5.6].

6. Reguläre Funktionen und der Satz von Riemann-Roch: Koordinatenring, Funktionenkörper, Lokalisierung, allgemeine Definition des Schnittmultiplizitäts, diskrete Bewertung und uniformisierendes Element, Satz: rationale Abbildung zwischen Kurven sind Morphismen. Satz: Elliptische Kurven sind nicht rational, [4, § I.4].

7. Divisoren und der Satz von Riemann–Roch. Divisoren, Hauptdivisoren, Picard-Gruppe, Satz: Hauptdivisoren haben Grad 0, Satz: $E \simeq \mathrm{Pic}^0(E)$. Satz von Riemann–Roch (ohne Beweis)[4, § I.4].

8. Die j-Invariante: Isomorphismen elliptischer Kurven, die j-Invariante, Automorphismengruppe, Isogenien, der Endomorphismusring, Satz: Isogenien sind Gruppenhomomorphismen [4, § II.1].

9. Elliptische Kurven über $\mathbb{C}$. Gitter $\Lambda = \mathbb{Z} \cdot 1 + \mathbb{Z}\tau \subset \mathbb{C}$ mit $\Im(\tau) > 0$, komplexe Tori $T := \mathbb{C}/\Lambda_\tau$, Isogenien komplexer Tori und Klassifikation den Endomorphismenring. ([4, § III].)

   Elliptische Funktionen, die Liouvillle'sche Sätze, die Weierstraße $\wp$-Funktion, Satz: $T := \mathbb{C}/\Lambda_\tau$ definiert ein elliptischer Kurve. ([1, § Kap. V].)

10. Der Endomorphismenring. Beschreibung der m-Torsionspunkte, die duale Isogenie, Grad einer Isogenie.

11. Elliptische Kurven über endlichen Körper. Der Frobenius-Morphismus. Die Hasse-Schranke, der Tate-Modul, die Zeta-Funktion. ([3, Chapter 13].)

12. Die Weil-Paarung und Anwendungen in der Kryptographie. Definition der Weil-Paarung, tripartite Diffie–Hellman, das MOV-Verfahren. ([2, Kap. 5]). Für die Definition und Eigenschafte der Weil–Paarung siehe [7, Abschnitt III.8].

References

[1] E. Freitag, R. Busam, *Funktionentheorie* I.

[2] J. Hoffstein, J. Pipher, J. Silverman, *An introduction to mathematical cryptography*.

[3] D. Husemoeller, *Elliptic curves*, second edition. http://www.math.rochester.edu/people/faculty/doug/otherpapers/Husemoller.pdf

[4] J.S. Milne, *Elliptic curves*.http://www.jmilne.org/math/Books/ectext5.pdf

[5] J. Silverman und J. Tate, *Rational points on elliptic curves*.

[6] J. Silverman, An introduction to the theory of elliptic curves, Summer school on computational number theory and cryptography, Wyoming, 2006. http://www.math.brown.edu/∼jhs/Presentations/WyomingEllipticCurve.pdf

[7] J. Silverman, *The arithmetic of elliptic curves*.