DIOPHANTISCHE GLEICHUNGEN UND ELLIPTISCHE KURVEN

1. *Rationale Parametrisierung von Koniken* (Martin Tscheschke, 17.10.).
   - Rationale Punkte auf der Kurve $x^2 + y^2 = 1$.
   - Weitere Beispiele: rationale Punkte auf den Kurven
     $$x^2 + y^2 + 5x - 7 = 0, y^2 - x^2(x-1) = 0.$$
   - Berechnung von Integralen des Typs
     $$\int g(x, \sqrt{ax^2 + bx + c})dx,$$
     wobei $g(x, y) \in \mathbb{R}(x, y)$.
   - Die Kurve $y^2 = x(x-1)(x-\lambda)$ ist nicht rational für $\lambda \neq 0, 1$ (mit einer Beweisskizze).

Literatur: zum ersten Punkt: zum Beispiel [2, Introduction, Theorem 3.1]; zur Nichtrationalität elliptischer Kurven: [6, Theorem 2.2]).

2. *Algebraische Grundlagen der elementaren Zahlentheorie* (Büsra Manap, 24.10.).
   - Sätze von Lagrange über die Ordnung einer Untergruppe bzw. Ordnung eines Gruppenelementes.
   - Der kleine Satz von Fermat: $a^{p-1} \equiv 1 \bmod p$, wobei $p \in \mathbb{P}$, $\mathsf{ggT}(a, p) = 1$.
   - Chinesischer Restsatz:
     $$\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r},$$
     wobei $m = m_1 \dots m_r$ mit $\mathsf{ggT}(m_i, m_j) = 1$
   - Einheiten im Ring $\mathbb{Z}_m$; der Satz von Euler:
     $$a^{\varphi(m)} \equiv 1 \bmod m, \quad \text{wobei} \quad \mathsf{ggT}(a, m) = 1.$$

Literatur: zum Beispiel: [1, 1], [4], [9].

3. *Quadratische Reste und Nichtreste modulo m* (2 Vorträge) (Lennard Pohler & Yannick Fuchs, 31.10. & 07.11.).
   - Legendre-Symbol $\left(\frac{a}{p}\right)$ und seine ersten elementaren Eigenschaften.
   - Das quadratische Reziprozitätsgesetz (ohne Beweis), Ergänzungsgesetze.
   - Beispiele von Berechnungen von Legendre-Symbolen.
   - Kriterium zur Lösbarkeit der Kongruenz $x^2 \equiv a \bmod m$ für $m = 2^e p_1^{t_1} \dots p_r^{t_r}$.
   - Jacobi-Symbol, seine elementaren Eigenschaften.
   - Satz von Lagrange über rationale Punkte auf der Kurve $ax^2 + by^2 = c$, wobei $a, b, c \in \mathbb{Z}$ (ohne Beweis).
   - Konkrete Beispiele: Lösbarkeit/Nichtlösbarkeit von $3x^2 + 5y^2 = 7$, $5x^2 + 7y^2 = 3$.

Literatur: Insbesondere [3, Proposition 5.1.2], [3, Proposition 17.3.1 und 17.3.2]

4. *Darstellbarkeit einer natürlichen Zahl als Summe von Quadraten* (Alina Rohde & Jan Christian Poll, 14.11.).

- Kriterium der Darstellbarkeit einer natürlichen Zahl als Summe zweier Quadrate (Satz von Euler).
- Jede natürliche Zahl ist als Summe von vier Quadraten darstellbar (Satz von Lagrange).

Literatur: Insbesondere [3, Section 17.7].

5. *Die Pellsche Gleichung* $x^2 - dy^2 = 1$ (Marius Dören, 21.11.).

- Die Struktur der Lösungen der Pellschen Gleichung, die Fundamentaleinheit.
- Beispiele: Lösungen von $x^2 - 2y^2 = 1$.

Literatur: Insbesondere [3, Section 17.5].

6. *Euklidische Ringe und Bachetsche Kurve* (Amelie Holtz, 28.11.).

- Euklidische Ringe, Eindeutigkeit der Primfaktorzerlegung.
- Der Ring $\mathbb{Z}[\sqrt{-2}]$ ist Euklidsch.
- Ganzzahlige Punkte auf der Bachetschen Kurve $y^2 = x^3 - 2$ (Fermatsche Herausforderung).

Literatur: zu Euklidschen Ringen: Insbesondere [3, Section 1.3], zur Fermatschen Herausforderung: [8, Introduction] (zur Geschichte), [3, Seite 289] oder [2, Introduction, Example 6.7] (Beweise).

7. *Einführung in die Theorie elliptischer Kurven* (Igor Burban, 05.12.).

- Der projektive Raum $\mathbb{P}^n(\Bbbk)$. Projektive und affine Varietäten.
- Gruppengesetz auf elliptischen Kurven.

8. *Resultante und Diskriminante. Gruppengesetz auf entarteten elliptischen Kurven* (Marcel Cedric Maasjost, 12.12.).

- Resultante zweier Polynome. Diskriminante eines Polynoms (mit Beweisen).
- Gruppengesetz auf $y^2 = x^3 + x^2$ und $y^2 = x^3$ (mit Details).
- Punkte der Ordnung zwei und drei auf einer elliptischen Kurve und ihre geometrische Bedeutung.

Literatur: [2, Appendix to Chapter II, Section 4], [2, Section III.4], [8, Section III.7 und II.1].

9. *Elliptische Kurven und die Fermatsche Gleichung I* (Enrico Armbrust, 19.12.).

- Fermat–Gleichung $u^4 + v^4 = w^2$.
- $E(\mathbb{Q}) \cong \mathbb{Z}/4$ für $E = V(y^2 - x^3 + 4x)$ (d.h. 2 ist keine kongruente Zahl).
- Rationale Punkte auf der Fibonacci–Kurve

$$\begin{cases} x^2 + y^2 &= u^2 \\ x^2 - y^2 &= v^2. \end{cases}$$

Literatur: zur Fermat [3, Section 17.2]; zur Fibonacci-Kurve: [6, Exercise 2.2.12]; zur elliptischen Kurve: [2, Example I.2.6].

10. *Elliptische Kurven und die Fermatsche Gleichung II* (Andre Simig, 09.01.).

- Fermat–Gleichung $u^3 + v^3 = 1$ (mit Beweis).
- $E(\mathbb{Q}) \cong \mathbb{Z}/3$ für $E = V(y^2 - x^3 + 432)$ (mit Beweis).

Literatur: zur Fermat: [3, Section 17.8], zur elliptischen Kurve: [2, Section I.2, Exercise 3].

11.**Die elliptische Kurve* $E = V(y^2 - x^3 + n^2x)$ *und kongruente Zahlen* (Johanna Jakob, 16.01.).

- Reduktion modulo p.
- Die Anzahl von Punkten von E über $\mathbb{F}_p$ (mit Beweis).
- $E_{\text{tors}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ (mit Beweis).

Literatur: [8, Appendix A, Section 5], [5, Chapter I, Propositions 16 und 17].

References

[1] S. Bosch, *Algebra*, Springer-Lehrbuch, Springer-Verlag, Berlin Heidelberg, 2013.
[2] D. Husemöller, *Elliptic curves*, Graduate Texts in Mathematics, 111. Springer-Verlag, New York, 1987.
[3] K. Ireland, M. Rosen, *A classical introduction to modern number theory*, Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990.
[4] J. C. Jantzen, J. Schwermer, *Algebra*, Springer-Lehrbuch, Springer-Verlag, Berlin Heidelberg, 2014.
[5] N. Koblitz, *Introduction to elliptic curves and modular forms*, Graduate Texts in Mathematics, 97. Springer-Verlag, New York, 1993.
[6] M. Reid, *Undergraduate algebraic geometry*, London Mathematical Society Student Texts, 12. Cambridge University Press, Cambridge, 1988.
[7] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1986.
[8] J. Silverman, J. Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.
[9] J. Wolfart, *Einführung in die Zahlentheorie und Algebra*, Vieweg+Teubner Verlag, Springer Fachmedien Wiesbaden GmbH, Wiesbaden, 2011.