Elliptische Kurven & Kryptologie Serie 13

Aufgaben zur Repetition des Vorlesungsstoffes

---

1. Gegeben sei ein rationaler Kegelschnitt K mit einem rationalen Punkt P.

Wie lassen sich alle rationalen Punkte auf K bestimmen?

2. Gegeben sei eine rationale cubische Kurve C die keine Gerade enthält, sowie ein rationaler Wendepunkt P auf C.

Wie lässt sich die Kurve C in die Weierstrass'sche Normalform $y^2 = x^3 + bx + c$ transformieren?

3. Gegeben sei eine rationale cubische Kurve C die keine Gerade enthält, sowie zwei verschiedene rationale Geraden g_1 und g_2 welche die Kurve C im Punkt P schneiden.

(a) Welche Fälle sind bezüglich den weiteren Schnittpunkten von g_1 und g_2 mit C möglich und was lässt sich damit über die Kurve C sagen?

(b) Was bedeuten diese Fälle algebraisch?

4. Gegeben sie eine cubische Kurve $C : y^2 = f(x)$ mit $f(x) = x^3 + ax^2 + bx + c$.

Wann ist die Kurve singulär? (algebraisch/geometrisch)

5. Gegeben sei eine rationale cubische Kurve C welche keine Gerade enthält und sei P ein rationaler singulärer Punkt auf C.

Wie lassen sich alle rationalen Punkte auf C bestimmen?

6. *Sind C_1 und C_2 zwei cubische Kurven welche genau 9 verschiedene Punkte $P_1, \ldots, P_9$ gemeinsam haben, und ist C eine cubische Kurve welche durch $P_1, \ldots, P_8$ geht, so liegt auch P_9 auf C.*

Was hat dieser Satz zu tun mit der Assoziativität der Addition von Punkten auf cubischen Kurven?

7. Gegeben sei eine elliptische Kurve $E[a, b, c]$ über $\mathbb{Q}$ mit $a, b, c \in \mathbb{Z}$.

Wie lassen sich die Punkte der Ordnung ≥ 2 auf $E[a, b, c]$ bestimmen? (mögliche Existenz solcher Punkte sowie deren Berechnung)

8. Beschreibe geometrisch Punkte der Ordnung $2, 3, 4$ auf allgemeinen elliptischen Kurven sowie auf elliptischen Kurven $E[a, b, c]$.

9. Wann ist $n \in \mathbb{N}$ eine kongruente Zahl und welches sind die entsprechenden elliptischen Kurven?

10. Welches sind die entscheidenden Ideen im Beweis des Mordell Theorems für $E[a, b]$ mit $a, b \in \mathbb{Z}$?

11. Sei $E = E[a, b]$ eine elliptische Kurve mit $a, b \in \mathbb{Z}$.
Beschreibe die Gruppenstruktur von $E(\mathbb{Q})$.

12. Beschreibe das Massey-Omura Kryptosystem auf elliptischen Kurven.

13. Wann ist die Gleichung $Z^2 + Z + \alpha = 0$ in $\mathbb{F}_{2^m}$ lösbar, und was ist der Zusammenhang mit der Anzahl Elemente in $E(\mathbb{F}_{2^m})$ für $E = E[a_2, a_6]$?

14. Was ist die Voraussetzung, damit Pollards Algorithmus einen echten Teiler von n findet?

15. Was ist die Voraussetzung, damit Lenstras Algorithmus einen echten Teiler von n findet?

16. Warum mussten wir die Assoziativität der Addition von Punkten auf cubischen Kurven über endlichen Körpern $\mathbb{F}_q$ der Charakteristik ≥ 3 nicht beweisen?