Elliptische Kurven & Kryptologie Serie 3

Anwendungen projektiver Transformationen algebraischer Kurven Abgabe: 17. März

---

1. Bestimme, mit Hilfe einer projektiven Transformation, alle rationalen Punkte auf dem Einheitskreis (verwandle zum Beispiel den Einheitskreis in eine geeignete Parabel oder Hyperbel). Leite damit ein Verfahren her, mit dem sich alle pythagoräischen Tripel bestimmen lassen.

2. (a) Zeige, mit Hilfe von Modulorechnen (oder sonstwie), dass es auf dem Kreis

$$K: \; x^2 + y^2 = 3$$

keine rationalen Punkte gibt.

(b) Zeige, dass die Gleichung $48q^2 - 1 = p^2$ keine rationalen Lösungen hat.
Hinweis: Betrachte die rationale projektive Transformation mit den neuen Achsen

$$\tilde{X} = 0: \; X - 2Z = 0\,, \quad \tilde{Y} = 0: \; X + 2Z = 0\,, \quad \tilde{Z} = 0: \; Y = 0\,.$$

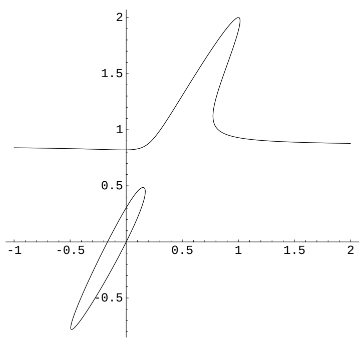
(c) Zeige, dass K nicht rational äquivalent zu einer rationalen Parabel $y = ax^2 + bx + c$ ist.

3. Gegeben sei ein rationaler Kegelschnitt $K_f: \; f(x,y) = 0$ sowie ein rationaler Punkt P_0 auf K_f.

Wie lassen sich die rationalen Punkte auf K_f bestimmen?

4. Gegeben sei die rationale cubische Kurve

$$C_f \; : \quad f(x,y) \; = \; 48x^2 \; - \; 56x^2y \; + \; 59xy^2 \; + \; 8x \; - \; 58xy \; - \; 16y^3 \; + \; 18y^2 \; - \; 4y \; = \; 0\,,$$



sowie der rationale Punkt $P_0 = (0,0)$ auf C_f.

Transformiere C_f in die Weierstrass'sche Normalform $y^2 = x^3 + bx + c$ mit $b, c \in \mathbb{Q}$.

Hinweis: Die projektive Transformation liefert

$$4\tilde{x}\tilde{y}^2 + (-4\tilde{x} - 64)\tilde{y} = p\tilde{x}^2 - 48\tilde{x}\,.$$