Elliptische Kurven & Kryptologie Serie 4

Tangenten, Wendepunkte und Singularitäten Abgabe: 4. April 2k+8

Im Folgenden sei $f(x, y)$ ein, über den reellen Zahlen, irreduzibles Polynom vom Grad 3 mit rationalen Koeffizienten. Ferner sei $C_f: \; f(x, y) = 0$ die assoziierte cubische Kurve (welche keine Gerade enthält) und C_F die entsprechende Kurve in der projektiven Ebene.

1. Sei G eine Gerade in der projektiven Ebene.

(a) Zeige, dass G die Kurve C_F in mindestens einem Punkt, höchstens in drei Punkten, schneidet.

(b) Zeige, dass C_f mindestens einen Punkt, höchstens aber drei Punkte, im Unendlichen hat.

(c) Sei die Gerade G eine Tangente an die Kurve C_F im Punkt P_0.
Zeige: Entweder schneidet die Gerade G die Kurve C_F nur in P_0, dann heisst P_0 **Wendepunkt** der Kurve C_F, oder G schneidet C_F in genau einem weiteren Punkt.

2. Sei P_0 ein Punkt der Kurve C_F. P_0 heisst **singulärer Punkt** der Kurve C_F falls $\operatorname{grad}(F)(P_0) = (0, 0, 0)$.

(a) Zeige: (x_0, y_0) ist ein singulärer Punkt von C_f, genau dann wenn $[x_0, y_0, 1]$ ein singulärer Punkt von C_F ist.
Hinweis: Der Gradient zeigt immer in die Richtung der grössten Zunahme.

(b) Ist P_0 ein singulärer Punkt von C_F, dann existiert eine lineare Abbildung aus $\mathrm{SO}(3)$, so dass der Punkt $[0, 0, 1]$ ein singulärer Punkt der transformierten Kurve $C_{\tilde{F}}$ ist.

3. Sei P_0 ein singulärer Punkt der Kurve C_F. Aus Aufgabe 2.(b) folgt, dass ohne Einschränkung der Allgemeinheit $P_0 = [0, 0, 1]$ angenommen werden darf.

(a) Zeige: Ist G eine Gerade durch P_0, dann schneidet G die Kurve C_F in höchstens einem weiteren Punkt P_1.

(b) Die Kurve C_F hat keine weiteren singulären Punkte; oder allgemeiner, eine cubische Kurve C_F hat höchstens einen singulären Punkt.

(c) Es gibt höchstens zwei Geraden durch P_0 welche C_F in keinem weiteren Punkt schneiden.

4. Zeige, dass unter einer projektiven Transformation sowohl Tangenten wie auch singuläre Punkte und Wendepunkte erhalten bleiben.

5. Sei P_0 ein rationaler, singulärer Punkt der Kurve C_F und sei G eine rationale Gerade durch P_0.

(a) Schneidet G die Kurve C_F in einem weiteren Punkt P_1, dann ist P_1 rational.

(b) Wie lassen sich die rationalen Punkte auf C_f bestimmen? Genauer: Definiere eine injektive, stetige Abbildung $C_F(\mathbb{Q}) \setminus \{P_0\} \to \mathbb{P}^1(\mathbb{Q})$.