

Elliptische Kurven und Kryptographie

Serie 1

rationale Punkte auf Kegelschnitten

Besprechung am 3. Oktober

3. Eine Gerade

$$G : aX + bY + cZ = 0$$

heisst **rational**, falls $a, b, c \in \mathbb{Q}$.

Ein Kegelschnitt

$$K : a_{11}X^2 + a_{22}Y^2 + a_{33}Z^2 + a_{12}XY + a_{13}XZ + a_{23}YZ = 0$$

heisst **rational**, falls die Koeffizienten a_{ij} alle rational sind.

- (a) Zeige, dass der Schnittpunkt von zwei verschiedenen rationalen Geraden rational ist.
- (b) Sei Q ein rationaler Punkt auf einem rationalen Kegelschnitt K .
Zeige, dass die Tangente an K im Punkt Q eine rationale Gerade ist.
- (c) Sei G eine rationale Gerade, welche den rationalen Kegelschnitt K in den Punkten Q und Q' schneidet.
Zeige: Q ist genau dann rational, wenn Q' rational ist.

4. Welche der Kreise

$$x^2 + y^2 = p \quad \text{für } p \in \{17, 23, 29\}$$

besitzen rationale Punkte?

5. Finde einen rationalen Punkt auf dem Kegelschnitt

$$x^2 + 17y^2 - 13 + 11xy = 0.$$