Elliptische Kurven und Kryptographie

Serie 1

rationale Punkte auf Kegelschnitten — Musterlösungen

---

3. Eine Gerade

$$G\colon aX + bY + cZ = 0$$

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

Ein Kegelschnitt

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

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.

Beweis:

(a) Sind $G_0\colon aX+bY+cZ=0$ und $G_1\colon a'X+b'Y+c'Z=0$ zwei verschiedene rationale Geraden, so gibt es kein λ in $\mathbb{R}$ so, dass $(a,b,c) = \lambda(a',b',c')$ und die Lösungen des Gleichungssystems

$$\begin{aligned} aX + bY + cZ &= 0 \\ a'X + b'Y + c'Z &= 0 \end{aligned}$$

sind die Vielfachen von $(a,b,c) \times (a',b',c')$. Dies entspricht einem rationalen Punkt, da sich alle Koordinaten simultan rational schreiben lassen.

(b) Sei K wie oben, $Q = (x,y,z)$. Der Gradient von K im Punkt Q liefert die rationale Geradengleichung

$$(2a_{11}x + a_{12}y + a_{13}z)X + (2a_{22}y + a_{12}x + a_{23}z)Y + (2a_{33}z + a_{13}x + a_{23}y)Z = 0$$

für die Tangente.

(c) Seien G und K wie oben. Da a, b und c nicht simultan 0 sein können, gilt ohne Einschränkung $c = 1$. Also folgt aus der Geradengleichung von G, dass $Z = -aX - bY$.
Eingesetzt in die Gleichung für K ergibt sich eine quadratische Gleichung mit rationalen Koeffizienten:

$$\beta_{11}X^2 + \beta_{12}XY + \beta_{22}Y^2 = 0,$$

und aufgelöst nach X:

$$X_{0,1} = \frac{-\beta_{12}Y \pm \sqrt{\beta_{12}^2 Y^2 - 4\beta_{11}\beta_{22}Y^2}}{2\beta_{11}}.$$

Nun ist $\frac{-\beta_{12}Y}{2\beta_{11}}$ genau dann rational, wenn Y rational ist.

i. Entweder ist für jedes rationale $Y \neq 0$ die Wurzel (und somit $X_{0,1}$) irrational. Dann ist keiner der Schnittpunkte rational.

ii. Oder es gibt $Y \neq 0$ rational und so, dass die Wurzel (und somit $X_{0,1}$) rational ist. Dann sind auch $Z_{0,1}$ und entsprechend beide Schnittpunkte rational.

4. Welche der Kreise

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

besitzen rationale Punkte?

Lösung:

Wir homogenisieren und erhalten

$$X^2 + Y^2 - pZ^2 = 0 \qquad \text{für} \quad p \in \{17, 23, 29\}\,, \tag{1}$$

was bereits in der gewünschten Form ist. Gesucht ist nun $(x_0, y_0, z_0) \in \mathbb{Z}^3 \setminus \{\vec{0}\}$ so, dass

$$x_0^2 + y_0^2 + pz_0^2 < 4p \tag{2}$$

und (1) erfüllt sind.

$p = 17$: Die Gleichung $17 = 4^2 + 1^2$ liefert unter anderem den Punkt $(4, 1, 1)$.

$p = 29$: Die Gleichung $29 = 5^2 + 2^2$ liefert unter anderem den Punkt $(5, 2, 1)$.

$p = 23$: Auf dem Kreis liegen nur "endliche" Punkte, also gilt $z_0 \neq 0$. Aus (2) erhalten wir $z_0^2 < 4$, also $z_0^2 = 1$. Somit muss wegen (1) gelten, dass $x_0^2 + y_0^2 = 23$. Jedoch ist für alle $x_0 \in \{0, \ldots, 4\}$ der Wert $y_0^2 = 23 - x_0^2 \in \{7, 14, 19, 22, 23\}$ kein Quadrat. Entsprechend gibt es keinen rationalen Punkt auf diesem Kreis.

5. Finde einen rationalen Punkt auf dem Kegelschnitt

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

Lösung:

Wir transformieren $x = \tilde{x} - \frac{11}{2}y$ und erhalten:

$$\tilde{x}^2 - \frac{53}{4}y^2 - 13 = \left(\tilde{x} - \frac{11}{2}y\right)^2 + 17y^2 - 13 + 11\left(\tilde{x} - \frac{11}{2}y\right)y = 0\,.$$

Eine weitere Tranformation $y = 2\tilde{y}$ liefert:

$$\tilde{x}^2 - 53\tilde{y}^2 - 13 = 0\,.$$

Nun sind $1, 53$ und 13 quadratfrei und paarweise teilerfremd, also können wir mit Computersuche zum Beispiel den ganzzahligen Punkt $(15, 2, 1)$ finden, der (zurücktransformiert) der Lösung $(-7, 4, 1)$ entspricht.