

# Elliptische Kurven und Kryptographie

## Serie 6

das "elliptische" an elliptischen Kurven

Musterlösungen

Gegeben sei ein reelles, quartisches Polynom  $g(t)$  mit paarweise verschiedenen (komplexen) Nullstellen und sei  $C_g : u^2 = g(t)$  die assoziierte quartische Kurve. Ferner sei  $\alpha$  eine reelle Nullstelle von  $g(t)$  und  $\beta \neq 0$  sei irgend eine reelle Zahl.

**21.** Zeige, dass die Substitutionen

$$x = \frac{\beta}{t - \alpha}, \quad y = x^2 u = \frac{\beta^2 u}{(t - \alpha)^2},$$

eine Transformation definieren welche die quartische Kurve  $C_g$  in die cubische Kurve

$$C_f : y^2 = f(x)$$

transformiert, wobei

$$f(x) = g'(\alpha)\beta x^3 + \frac{1}{2}g''(\alpha)\beta^2 x^2 + \frac{1}{6}g'''(\alpha)\beta^3 x + \frac{1}{24}g''''(\alpha)\beta^4.$$

*Bemerkung:* Es lässt sich zeigen, dass  $f(x)$  ebenfalls paarweise verschiedene (komplexe) Nullstellen hat, d.h.  $u^2 = g(t)$  definiert eine nicht-singuläre cubische Kurve in WNF.

**Beweis:**

Ersetzen wir  $\beta$  durch  $(t - \alpha)x$ , so erhalten wir

$$y^2 = f(x) = x^4 \sum_{i=1}^4 \frac{1}{i!} g^{(i)}(\alpha) (t - \alpha)^i = x^4 (g(t) - g(\alpha)) = x^4 g(t),$$

wie gewünscht.

**22.** Seien  $\alpha$  und  $\beta$  reelle Zahlen mit  $0 < \beta < \alpha$  und sei  $E$  die Ellipse

$$E : \frac{x^2}{\alpha^2} + \frac{y^2}{\beta^2} = 1.$$

(a) Zeige, dass der Umfang der Ellipse  $E$  gleich dem Integral

$$4\alpha \int_0^{\pi/2} \sqrt{1 - k^2 \sin^2(\theta)} d\theta$$

ist, für ein geeignetes  $k$  (abhängig von  $\alpha$  und  $\beta$ ).

(b) Zeige, dass gilt:

$$\int_0^{\pi/2} \sqrt{1 - k^2 \sin^2(\theta)} d\theta = \int_0^1 \sqrt{\frac{1 - k^2 t^2}{1 - t^2}} dt = \int_0^1 \frac{1 - k^2 t^2}{\sqrt{(1 - t^2)(1 - k^2 t^2)}} dt.$$

**Bemerkung:** Um Bogenlängen von Ellipsen (die keine Kreise sind) zu bestimmen, müssen also Integrale der Form  $\int \frac{1 - k^2 t^2}{u} dt$  berechnet werden, wobei  $C_g: u^2 = g(t)$  eine quartische Kurve ist, welche für  $0 < \beta < \alpha$  in eine cubische Kurve  $C_f: y^2 = f(x)$  in WNF transformiert werden kann.

**Beweis:**

1. Wir parametrisieren die Ellipse

$$x(\theta) = \alpha \sin \theta, \quad y(\theta) = \beta \cos \theta,$$

erhalten also  $\dot{x}(\theta) = \alpha \cos \theta$ ,  $\dot{y}(\theta) = -\beta \sin \theta$  und

$$\dot{x}(\theta)^2 + \dot{y}(\theta)^2 = \alpha^2 \cos^2 \theta + \beta^2 \sin^2 \theta = \alpha^2 - (\alpha^2 - \beta^2) \sin^2 \theta = \alpha^2(1 - k^2 \sin^2 \theta),$$

für  $k = \sqrt{1 - \beta^2/\alpha^2}$ . Das Integral für den Umfang ist also

$$\int_0^{2\pi} \sqrt{\dot{x}(\theta)^2 + \dot{y}(\theta)^2} d\theta = 4\alpha \int_0^{\pi/2} \sqrt{1 - k^2 \sin^2 \theta} d\theta,$$

da  $\sin^2$  zum einen  $\pi$ -periodisch ist und da zum andern  $\sin^2(\pi/2 - x) = \sin^2(x)$  für alle  $x$  im Definitionsbereich gilt.

2. Substituieren wir  $t = \sin \theta$  bzw.  $\theta = \arcsin t$ , so erhalten wir die erste Gleichheit, da  $\arcsin' t = \frac{1}{\sqrt{1-t^2}}$ . Für die zweite Gleichheit erweitern wir mit  $\sqrt{1 - k^2 t^2}$ . Da  $k \neq 1$  gilt, sind auch – wie gewünscht – alle Nullstellen des Nenners paarweise.