Elliptische Kurven & Kryptologie Serie 7

Das elliptische an elliptischen Kurven Abgabe: 21. April

---

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

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

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

2. Seien a und b reelle Zahlen mit $0 < b \leq a$ und sei E die Ellipse

$$E : \frac{x^2}{a^2} + \frac{y^2}{b^2} = 1\,.$$

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

$$4a \int_0^{\pi/2} \sqrt{1 - k^2\cos^2(\theta)}\, d\theta$$

ist, für ein geeignetes k (abhängig von a und b).

(b) Zeige, dass gilt:

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

Um Bogenlängen von Ellipsen zu bestimmen, müssen also Integrale der Form $\int \frac{1-k^2t^2}{u} dt$ berechnet werden, wobei $C_g : u^2 = g(t)$ eine quartische Kurve ist, welche für $0 < b \leq a$ in eine "elliptische" Kurve $C_f : y^2 = f(x)$ transformiert werden kann.