Elliptische Kurven und Kryptographie

Serie 4

Weierstrass'sche Kurven & kongruente Zahlen — Besprechung am 24. Oktober

---

13. Die cubische Kurve

$$C : 4x^2y - 4xy^2 - 8y^3 + 24y^2z - 24yz^2 + 8z^3 = 0$$

hat im Punkt $P_0 = (1, 1, 1)$ einen Wendepunkt mit Wendetangente $x = y$.

Finde eine rationale projektive Transformation, welche C auf eine Weierstrass'sche Kurve $C[a, b, c]$ mit $a, b, c \in \mathbb{Q}$ abbildet.

Hinweis: Wähle für $\tilde{x} = 0$ die Gerade $y = 1$.

Eine positive natürliche Zahl n heisst ***kongruente Zahl***, falls es positive rationale Zahlen a, b, c gibt, für die gilt:

$$a^2 + b^2 = c^2 \quad \text{und} \quad \tfrac{1}{2}ab = n.$$

Mit anderen Worten ist n eine kongruente Zahl, falls n der Flächeninhalt eines rechtwinkligen Dreiecks mit rationalen Seiten ist.
Sei nun n eine positive natürliche Zahl. Dann definieren wir

$$K_n := \left\{(a, b, c) \in \mathbb{Q}^3 \mid a, b, c > 0,\ a^2 + b^2 = c^2,\ \tfrac{1}{2}ab = n\right\}.$$

Weiter sei die Weierstrass'sche Kurve C_n wie folgt definiert:

$$C_n : y^2 = x^3 - n^2x$$

Es sei V_n die Menge aller rationalen Punkte auf C_n im ersten Quadranten von $\mathbb{Q}^2$:

$$V_n := C_n(\mathbb{Q}) \cap \left\{(x, y) \in \mathbb{Q}^2 \mid x, y > 0\right\}.$$

14. Zeige, dass für eine kongruente, quadratfreie Zahl n ein Punkt $(x, y) \in V_n$ existiert, welcher

$$x = \left(\frac{p}{2q}\right)^2$$

erfüllt, das heisst, x ist das Quadrat einer rationalen Zahl mit geradem Nenner.

Hinweis: Finde eine Bijektion

$$\left\{x \in \mathbb{Q} : x - n, x, x + n \text{ Quadrate in } \mathbb{Q}\right\} \to \left\{(a, b, c) \in K_n : a < b < c\right\}.$$

15. (a) Finde eine Bijektion $V_n \to K_n$.

(b) Zeige, dass n genau dann eine kongruente Zahl ist, wenn $V_n \neq \emptyset$.