Elliptische Kurven und Kryptographie

Serie 4

Weierstrass'sche Kurven & kongruente Zahlen — Musterlösungen

---

13. Die cubische Kurve

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

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 $y = 1$.

Lösung:

Sei $C\colon\ f(x,y,z) = 0$. Der Polarkegelschnitt von C in $P_0 = (1,1,1)$ ist dann gerade von der Form

$$K\colon\ 4x^2 - 4y^2 = f_x + f_y + f_z = 0\,.$$

Da die Wendetangente T_0 die Gleichung $x - y = 0$ erfüllt, wird die zweite Gerade G_0 des PKS durch $x + y = 0$ beschrieben. Betrachten wir nun die Schnittpunkte der drei Geraden, erhalten wir, dass $(0,0,1)$ in neuen Koordinaten $(1,0,0)$ sein soll, $(1,1,1)$ auf $(0,1,0)$ abgebildet wird und $(-1,1,1)$ auf $(0,0,1)$, also

$$\tilde{x} = y - z, \quad \tilde{y} = y + z, \quad \tilde{z} = x + y + z\,.$$

Dies ergibt

$$\widetilde{C}\colon\ x^3 - y^2 + z \;=\; \frac{f(\tilde{x},\tilde{y},\tilde{z})}{8} \;=\; 0.$$

14. Zeige, dass für eine quadratfreie kongruente 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

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

Beweis:
Sei $x \in Q_n$. Es gilt

$$\left(\sqrt{x+n} - \sqrt{x-n}\right)^2 + \left(\sqrt{x+n} + \sqrt{x-n}\right)^2 = \left(2\sqrt{x}\right)^2 \,,$$
$$\tfrac{1}{2}\left(\sqrt{x+n} - \sqrt{x-n}\right) \cdot \left(\sqrt{x+n} + \sqrt{x-n}\right) = n \,.$$

Daraus sehen wir, dass

$$x \mapsto \left(\sqrt{x+n} - \sqrt{x-n}, \sqrt{x+n} + \sqrt{x-n}, 2\sqrt{x}\right)$$

eine Abbildung $Q_n \to K_n^+$ ist. Die Umkehrabbildung

$$(a, b, c) \mapsto \left(\frac{c}{2}\right)^2$$

ist wohldefiniert, denn auch $\frac{c}{2} \pm n$ sind Quadrate, wie wir im Folgenden sehen werden.
Ausserdem zeigen wir:

- Die Zahl $\left(\frac{c}{2}\right)^2$ ist eine mögliche x-Koordinate eines rationalen Punktes auf der Kurve $C_n \colon y^2 = x^3 - n^2 x$.
- Ist $c = \frac{p}{q}$ gekürzt, dann ist p ungerade.

Wir können die Gleichung $y^2 = x^3 - n^2 x$ umschrieben zu

$$\frac{y^2}{x} = x^2 - n^2 \,.$$

Weiter gilt für $(a, b, c) \in K_n^+$

$$(a+b)^2 = c^2 + 4n$$
$$(a-b)^2 = c^2 - 4n$$

woraus zum einen folgt, dass auch $\frac{c}{2} \pm n$ Quadrate sind, zum andern, dass

$$\left(\frac{a^2 - b^2}{4}\right)^2 = \frac{(a+b)^2(a-b)^2}{16} = \frac{(c^2+4n)(c^2-4n)}{16} = \left(\frac{c}{2}\right)^4 - n^2 \,.$$

Also ist

$$\left(\left(\frac{c}{2}\right)^2, \left(\frac{c(a^2-b^2)}{8}\right)\right)$$

ein rationaler Punkt auf C_n.
Für die zweite Aussage seien $a = \frac{p_1}{q_1}$ und $b = \frac{p_2}{q_2}$ gekürzt. Dann erhalten wir

$$c^2 = \frac{p_1^2 q_2^2 + p_2^2 q_1^2}{q_1^2 q_2^2} \tag{1}$$

und

$$\tfrac{1}{2}ab = \frac{p_1 p_2}{2 q_1 q_2} \in \mathbb{N} \Rightarrow q_1 \mid p_2 \wedge q_2 \mid p_1 \Rightarrow (q_1, q_2) = 1 \Rightarrow (q_1, p_1 q_2) = 1 = (q_1 p_2, q_2) \,,$$

woraus folgt, dass (1) gekürzt ist. Für $c = \frac{p}{q}$ gekürzt ist also $p_1^2 q_2^2 + p_2^2 q_1^2 = p^2$.

Da n quadratfrei ist, gilt $(p_1, p_2) \in \{1, 2\}$, aber $8 \nmid p_1 p_2$.

Angenommen, sowohl p_1 als auch p_2 seien gerade, dann wäre $p_1^2 q_2^2 + p_2^2 q_1^2 = p^2$ durch 8, aber nicht durch 16 teilbar, denn $\left(\frac{p_1}{2}\right)^2 q_2^2 + \left(\frac{p_2}{2}\right)^2 q_1^2 \equiv 2 \mod 4$, da es sich dabei um eine Summe ungerader Quadrate handelt. Nun kann aber p^2 als Quadrat einer ganzen Zahl nicht durch 8 teilbar sein, ohne auch durch 16 teilbar zu sein – ein Widerspruch.

Entsprechend gilt also $2 \mid p_i$ für genau ein $i \in \{1, 2\}$, also ist p ungerade – was zu zeigen war.

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

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

Lösung:

(a) Bezeichne die gesuchte Bijektion mit $\varphi = (\varphi_a, \varphi_b, \varphi_c)\colon V_n \to K_n$. Nun soll zum einen gelten

$$\varphi_a(x, y)\, \varphi_b(x, y) \;=\; 2\, n \;=\; \frac{2\, n\, x\, (x^2 - n^2)}{y^2}\,,$$

zum andern soll $\varphi_a(x, y)^2 + \varphi_b(x, y)^2 = \varphi_c(x, y)^2$ ein Quadrat in $\mathbb{Q}$ sein. Wählen wir

$$a = \frac{(x^2 - n^2)}{y}, \quad b = \frac{2\, n\, x}{y} \quad \text{und} \quad c = \frac{(x^2 + n^2)}{y}\,,$$

so gelten alle gewünschten Eigenschaften. Die Umkehrfunktion ist gegeben durch die Identitäten

$$x = \frac{n\, (a + c)}{b} \quad \text{und} \quad y = \frac{2\, n^2\, (a + c)}{b^2}\,.$$

(b) Aus der Bijektion in (15a) erhalten wir, dass V_n genau dann leer ist, wenn K_n leer ist. Dies wiederum ist per Definition genau dann der Fall, wenn n eine kongruente Zahl ist.