Elliptische Kurven und Kryptographie

Serie 5

zur Hesse'schen Normalform | Musterlösungen

Eine cubische Kurve C in der reellen projektiven Ebene ist in ***Hesse'scher Normalform*** (HNF) falls

$$C\colon\; X^3 + Y^3 + Z^3 + c\,XYZ = 0 \quad \text{für } c \in \mathbb{R}.$$

16. Zeige: Die Hesse'sche Kurve einer Kurve in HNF mit $c \neq 0$ ist, nach Division durch $-6c^2$, in HNF.

Beweis:

Die Hesse'sche Kurve einer Kurve von C ist

$$H_C\colon\; -6c^2(X^3 + Y^3 + Z^3) + (216 + 2c^3)XYZ\,.$$

17. Zeige, dass eine Kurve in HNF nur für $c = -3$ singulär ist.

Beweis:

Für $c = -3$ ist der Gradient im Punkt $(1, 1, 1) \in C$ gleich $(0, 0, 0)$.

Setzen wir nun den Gradienten gleich $(0, 0, 0)$:

$$3X^2 + cYZ = 3Y^2 + cXZ = 3Z^2 + cXY = 0\,.$$

Insbesondere ist $3X^3+cXYZ = 0 = 3Y^3+cXYZ$, also $X = Y$ und aus Symmetriegründen $X = Y = Z$. Da nicht möglich ist, dass $X = Y = Z = 0$, muss $c = -3$ gelten.

18. Zeige, dass jede nicht-singuläre Kurve in HNF die drei Wendepunkte

$$(-1, 1, 0),\; (0, -1, 1),\; (-1, 0, 1)$$

besitzt.

Beweis:

Die drei Punkte liegen auf jeder Kurve C in HNF, also auch auf H_C für $c \neq 0$. Für $c = 0$ geht $H_C\colon XYZ = 0$ ebenfalls durch die drei Punkte. Als Schnittpunkte von einem nicht-singulären C mit seiner Hesse'schen Kurve H_C muss es sich dabei also um Wendepunkte von C handeln.

19. Zeige: Ist (X_0, Y_0, Z_0) ein Punkt auf einer Kurve in HNF, so gilt:

$$(X_0, Y_0, Z_0) \# (X_0, Y_0, Z_0) = \big(X_0(Y_0^3 - Z_0^3)\,, Y_0(Z_0^3 - X_0^3)\,, Z_0(X_0^3 - Y_0^3)\big)$$

Beweis:

Es genügt, zu zeigen, dass der Punkt $\big(X_0(Y_0^3 - Z_0^3)\,, Y_0(Z_0^3 - X_0^3)\,, Z_0(X_0^3 - Y_0^3)\big)$ sowohl auf der Kurve C in HNF, als auch auf der Tangente an C durch $P_0 := (X_0, Y_0, Z_0)$ liegt – vorausgesetzt, dass P_0 selbst auf C liegt.

Nun erfüllen die Koordination von P_0 in die Tangentengleichung

$$(3X_0^2 + cY_0Z_0)X + (3Y_0^2 + cX_0Z_0)Y + (3Z_0^2 + cX_0Y_0)Z = 0\,,$$

wenn wir sie für (X, Y, Z) einsetzen.

Dass P_0 die Kurvengleichung von C erfüllt, folgt daraus, dass wir nach Einsetzen und Umformen (mit Computer-Unterstützung) ein Vielfaches von $X_0^3 + Y_0^3 + Z_0^3 + c\,X_0\,Y_0\,Z_0$ erhalten, was nach Voraussetzung 0 ist.

20. Sei C eine Kurve in HNF mit $c = -\frac{2q^3+1}{q^2}$ für $q \in \mathbb{Q} \setminus \{-\frac{1}{2}, 0, 1\}$ und sei $\mathscr{O} := (-1, 1, 0)$ das Neutralelement der elliptischen Kurve $C(\mathbb{Q})$.

Zeige: $(\frac{1}{q}, 1, 1)$ ist ein Element von $C(\mathbb{Q})$ der Ordnung 6.

Beweis:

Der Punkt liegt auf der Kurve und nach (19) gilt

$$\big(q^{-1}, 1, 1\big) \;\#\; \big(q^{-1}, 1, 1\big) = \big(0, 1 - q^{-3}, q^{-3} - 1\big) = (0, -1, 1).$$

Da nun $(0, -1, 1)$ als von $\mathscr{O}$ verschiedener Wendepunkt von der Ordnung 3 ist, ist $(q^{-1}, 1, 1)$ von der Ordnung 6.