Elliptische Kurven und Kryptographie

Serie 5

zur Hesse'schen Normalform — Besprechung am 31. Oktober

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

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

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

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

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

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

besitzt.

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

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

20. Sei C eine Kurve in HNF mit $c = -\frac{2q^3+1}{q^2}$ für $q \in \mathbb{Q} \setminus \{-\frac{1}{2}, 1\}$ 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.