ELLIPTISCHE KURVEN ([1], S. 223–224, [2], S. 6–7, 9–12)

In Ihrem Vortrag sollen Sie einen Zusammenhang zwischen kongruenten Zahlen und Punkten auf gewissen elliptischen Kurven herstellen.

Führen Sie zunächst den Begriff eines rationalen Punktes auf einer Kurve ein. Betrachten Sie zunächst als Beispiel die rationalen Punkte auf der Kurve, die durch die Gleichung

$$x^2 + y^2 = 1$$

definiert ist, oder äquivalent die ganzzahligen Lösungen von

$$X^2 + Y^2 = Z^2. \tag{1}$$

Eine Lösung $(X, Y, Z) \in \mathbb{Z}^3$ von (1) nennen wir *primitiv*, wenn X, Y, Z positiv sind und keinen echten gemeinsamen Teiler haben. Zeigen Sie:

Satz 1. *Es seien $a > b$ zwei ganze, teilerfremde, positive Zahlen mit $2|ab$. Dann ist (X, Y, Z) mit $X = a^2 - b^2$, $Y = 2ab$, $Z = a^2 + b^2$ eine primitive Lösung von (1). Jede primitive Lösung von (1) ist von dieser Gestalt.*

Wiederholen Sie die Definition einer kongruenten Zahl aus dem vorangegangenen Vortrag. Beweisen Sie:

Satz 2. *Es gibt genau dann ein rechtwinkliges Dreieck mit rationalen Seitenlängen und Flächeninhalt $n \in \mathbb{N}$, wenn die Gleichung*

$$y^2 = x^3 - n^2 x, \tag{2}$$

eine rationale Lösung $(x, y) \in \mathbb{Q}^2$ der Gestalt $x = \frac{r^2}{4s^2}$ mit $r, s \in \mathbb{Z}$, $\mathrm{ggT}(r, 2sn) = 1$ hat.

Die Gleichung (2) liefert ein Beispiel einer „elliptischen Kurve“. Es sei nun K ein Körper. Erinneren Sie daran, dass die *Charakteristik* $\mathrm{char}(K)$ von K die kleinste Zahl $n \in \mathbb{N}$ ist, so dass für jedes $x \in K$ die Gleichung $nx = 0$ gilt. Es sei nun $\mathrm{char}(K) \neq 2$ und $f(x) \in K[x]$ ein kubisches Polynom mit voneinander verschiedenen Nullstellen (ggf. in einer endlichen *Erweiterung* $K' \supseteq K$ von K). Dann nennen wir

$$y^2 = f(x) \tag{3}$$

eine *elliptische Kurve über K*. Es sei K' eine Körpererweiterung von K. Die Lösungen $(x, y) \in K'^2$ der Gleichung (3) nennen wir die *über K' definierten Punkte* auf der elliptischen Kurve (3), oder einfach die *K'-Punkte* von (3).

Theorem 2 liefert also eine Charakterisierung der kongruenten Zahlen durch rationale Punkte auf gewissen elliptischen Kurven. Definieren Sie auch, was ein glatter Punkt auf einer Kurve ist. Gehen Sie schließlich auf projektive Koordinaten ein und erklären Sie was unter dem „Punkt im Unendlichen“ verstanden wird.

Literatur

[1] G. Jones, J. Jones, Elementary number theory, Springer, Berlin, 1999.

[2] N. Koblitz, Introduction to Elliptic Curves and Modular Forms, Springer, Berlin, 1993.