PUNKTE UNENDLICHER ORDNUNG AUF E_n UND DAS PROBLEM DER KONGRUENTEN ZAHLEN ([1], S. 36–41, 43–49)

In Ihrem Vortrag sollen Sie die *Reduktion* der elliptischen Kurven E_n modulo gewisser Primzahlpotenzen betrachten, um schließlich zu zeigen, dass n genau dann eine kongruente Zahl ist, wenn die elliptische Kurve E_n über $\mathbb{Q}$ einen Punkt unendlicher Ordnung hat.

Bisher waren wir hauptsächlich an elliptischen Kurven E interessiert, die über $\mathbb{Q}$ definiert sind ($y^2 = f(x)$ mit $f(x) \in \mathbb{Q}[x]$), insbesondere an den Kurven $E_n : y^2 = x^3 - n^2x$ ($n \in \mathbb{N}$). Allgemeiner sagen wir, eine elliptische Kurve ist *über* dem Körper K definiert, wenn alle ihrer Koeffizienten in K enthalten sind. Die Punkte $(x, y, z) \in \mathbb{P}^2_K$ auf der elliptischen Kurve E_n nennen wir *über K definierte Punkte* oder einfach *K-Punkte* von E_n.

Erinnern Sie an die Definition der endlichen Körper $\mathbb{F}_q$ mit $q = p^f$ (p prim, $f \in \mathbb{N}$) Elementen. Indem wir die Koeffizienten von E_n modulo einer Primzahl $p \nmid 2n$ reduzieren, erhalten wir eine elliptische Kurve über dem Körper $\mathbb{F}_p$. Zeigen Sie:

Satz 1. *Es sei $p \nmid 2n$ eine Primzahl, $f \in \mathbb{N}$ und $q = p^f$ mit $q \equiv 3 \pmod 4$. Dann hat die elliptische Kurve $y^2 = x^3 - n^2x$ über $\mathbb{F}_q$ genau $q + 1$ Punkte.*

Definieren Sie die *Torsions-Untergruppe* A_{tors} einer abelischen Gruppe A. Folgenden Satz von Mordell können Sie ohne Beweis verwenden:

Satz 2 (Mordell)**.** *Die Gruppe $E(\mathbb{Q})$ der $\mathbb{Q}$-Punkte auf einer elliptischen Kurve E über $\mathbb{Q}$ ist eine endlich erzeugte abelsche Gruppe.*

Mordells Satz besagt, dass die Torsions-Untergruppe $E(\mathbb{Q})_{tors}$ endlich ist und dass es ein $r \in \mathbb{N}_0$ mit $E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r$ gibt. Die Zahl r nennen wir den *Rang* von $E(\mathbb{Q})$. Stellen Sie in Ihrem Vortrag folgenden Zusammenhang zwischen dem Rang der elliptischen Kurven E_n und dem Problem der kongruenten Zahlen her.

Satz 3. *Eine natürliche Zahl n ist genau dann eine kongruente Zahl, wenn der Rang von $E_n(\mathbb{Q})$ positiv ist.*

Bestimmen Sie zunächst die Anzahl der Elemente in den Torsions-Untergruppen von $E_n(\mathbb{Q})$:

Satz 4. *Für $n \in \mathbb{N}$ gilt $\#E_n(\mathbb{Q})_{tors} = 4$. Insbesondere gilt $E_n(\mathbb{Q})_{tors} = \{(0,0), (\pm n, 0), \infty\}$, worin ∞ der Punkt im Unendlichen ist.*

Wir bezeichnen das rechtwinklige Dreieck mit den Seitenlängen X, Y, Z mit $\blacktriangle(X, Y, Z)$. Formulieren Sie folgenden Satz ohne Beweis.

Satz 5. *Die Abbildung*

$$2E_n(\mathbb{Q}) \setminus \{0\} \to \{\blacktriangle\,(X, Y, Z) \ \textit{mit Flächeninhalt } n\},$$
$$(x, \pm y) \mapsto \blacktriangle\left(\sqrt{x+n} - \sqrt{x-n}, \sqrt{x+n} + \sqrt{x-n}, 2\sqrt{x}\right)$$

ist bijektiv mit Umkehrabbildung

$$\blacktriangle\,(X, Y, Z) \mapsto \left(Z^2/4, \pm(Y^2 - X^2)Z/8\right).$$

Literatur

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