ELLIPTISCHE KURVEN UND IHRE L-FUNKTIONEN ([1], S. 133-141)

In Ihrem Vortrag werden Sie die Beziehung zwischen elliptischen Kurven über $\mathbb{Q}$ und Modulformen untersuchen. Geben Sie hierzu zunächst eine kurze Einführung in die Theorie der elliptischen Kurven. Sei dazu K ein beliebiger Körper mit $\mathrm{char}(K) \nmid 6$. Dann ist eine elliptische Kurve E über K durch ihre *Weierstraß-Gleichung* (nach Karl Theodor Wilhelm Weierstraß, 1815-1897)

$$y^2 = x^3 + Ax + B$$

mit $A, B \in K$ definiert. Die *Diskriminante*

$$\Delta = -16\left(4A^3 + 27B^2\right)$$

von E bestimmt die Regularität von E als algebraische Kurve. Erläutern Sie anhand der Bilder auf S. 134 in [1] die verschiedenen Arten von Singularitäten, die bei elliptischen Kurven auftreten können.

Nehmen wir nun an, dass A und B ganze Zahlen sind, so dass $\Delta \neq 0$ gilt. Dann können wir die Kurve E modulo einer Primzahl p mit $p \nmid \Delta$ *reduzieren*, also als Kurve über dem endlichen Körper $\mathbb{F}_p$ auffassen, und die Anzahl $\nu(p)$ der *affinen Punkte* über $\mathbb{F}_p$, also die modulo p verschiedenen Lösungen der Kongruenz

$$y^2 \equiv x^3 + Ax + B \pmod{p},$$

bestimmen. Die für uns interessantere Größe $\lambda(p)$ ist durch

$$\lambda(p) = p - \nu(p)$$

definiert. Für $p \mid \Delta$ setzen wir $\lambda(p) = 0, 1, -1$, je nach dem, welche Singularität bei der reduzierten Kurve $E/\mathbb{F}_p$ auftritt (Sie brauchen die Details hier nicht zu geben).

Nach einem Resultat von Helmut Hasse (1898-1979) gilt die Abschätzung

$$\lambda(p) < 2\sqrt{p}, \tag{1}$$

woraus man folgern kann, dass die *Hasse-Weil L-Funktion* (nach Helmut Hasse und André Weil, 1906-1998) von E

$$L_E(s) = \prod_{p|\Delta} \left(1 - \lambda(p)p^{-s}\right)^{-1} \prod_{p\nmid\Delta} \left(1 - \lambda(p)p^{-s} + p^{1-2s}\right)^{-1}$$

für $\mathrm{Re}\,(s) > \frac{3}{2}$ absolut konvergiert. Dieses Euler-Produkt kann als Dirichlet-Reihe

$$L_E(s) = \sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s}$$

geschrieben werden. Geben Sie diese Resultate als Fakten an, beweisen brauchen Sie sie nicht.

Formulieren Sie als nächstes den Modularitätssatz. Dieser wurde von Yutaka Taniyama (1927-1958) und Goro Shimura (geb. 1930) in den 1950er Jahren vermutet und ab Mitte der 1990er Jahre in einer Reihe von z.T. gemeinsamen Arbeiten von Andrew Wiles (geb. 1953),

Richard Taylor (geb. 1962), Christophe Breuil (geb. 1968), Brian Conrad (geb. 1970) und Fred Diamond (geb. 1964) vollständig bewiesen.

Theorem 1. *Sei E eine elliptische Kurve über $\mathbb{Q}$ mit $\Delta \neq 0$ und* Führer *(das ist eine bestimmte natürliche Zahl mit den gleichen Primfaktoren wie Δ) N_E und sei L_E ihre Hasse-Weil L-Funktion. Dann existiert eine Spitzenform $f \in S_2(\Gamma_0(N_E))$ mit*

$$D_f(s) = L_E(s).$$

Diese Spitzenform f ist eine sogenannte Neuform*, was z.B. zur Folge hat, dass ihre Fourier-Koeffizienten $c(n)$* multiplikativ *sind, d.h. es gilt $c(mn) = c(m)c(n)$ für $\mathrm{ggT}(m, n) = 1$.*

Erinnern Sie kurz an die in der Formulierung des Satzes auftretenden Notationen und Begriffe aus vorherigen Vorträgen.

Der Modularitätssatz war der wichtigste Schritt in Wiles' Beweis des berühmten *Letzten Satzes von Fermat* (Pierre de Fermat, 1601-1667) und lieferte auch den ersten Beweis für die analytische Fortsetzbarkeit von Hasse-Weil L-Funktionen elliptischer Kurven, denn die Fortsetzbarkeit von modularen L-Funktionen haben wir z.B. auch in diesem Seminar bereits bewiesen.

Der Beweis des Modularitätssatzes in voller Allgemeinheit geht weit über das hinaus, was in einem Studentenseminar behandelt werden kann, aber für einen wichtigen Spezialfall kann man einen einfachen Beweis geben, was im Rest dieses sowie im nächsten Vortrag geschehen soll. Folgen Sie dazu der Darstellung in Kapitel 8 des Buches [1]. Wir beschränken uns im Folgenden auf eine unendliche Familie elliptischer Kurven, die so genannten *Heron-Zahlen-Kurven* (nach Heron von Alexandria, um 10 n.Chr. - um 70 n.Chr.), im Englischen *congruent number curves*. Diese Kurven werden mit E_r ($r \in \mathbb{N}$) bezeichnet und sind definiert durch die Weierstraß-Gleichung

$$y^2 = x^3 - r^2 x.$$

Zeigen Sie, dass es für einen Beweis des Modularitätssatzes für alle Kurven E_r ausreicht, ihn für die Kurve E_1 zu beweisen. Dies ist der Inhalt des folgenden Lemmas, dessen Beweis Sie in Ihrem Vortrag präsentieren sollen. Definieren Sie zuvor das *Jacobi-Symbol* $\left(\frac{r}{n}\right)$ (nach Carl Gustav Jacob Jacobi, 1804-1851).

Lemma 2. *Es bezeichne $\chi_r(n) = \left(\frac{r}{n}\right)$ das Jacobi-Symbol und $\lambda_r(p)$ die Größe aus* (1) *für die Kurve E_r. Dann gilt für $Re(s) > \frac{3}{2}$ die Gleichung*

$$L_{E_r}(s) = \sum_{2 \nmid n} \chi_r(n)\lambda_1(n)n^{-s}.$$

Bestimmen Sie als nächstes die Zahlen $\lambda_1(p)$.

Lemma 3. *Für eine Primzahl p gilt*

$$\lambda(p) = \begin{cases} 0 & \text{für } p = 2 \text{ oder } p \equiv -1 \pmod 4, \\ \pi + \overline{\pi} & \text{für } p \equiv 1 \pmod 4. \end{cases}$$

Hierbei ist $\pi \in \mathbb{Z}[i]$ mit $\pi\overline{\pi} = p$ und $\pi \equiv 1 \pmod{\mathfrak{a}}$, wobei $\mathfrak{a}$ das von $(1+i)^3$ erzeugte $\mathbb{Z}[i]$-Ideal sei (diese Bedingungen bestimmen π bis auf Konjugation eindeutig).

Literatur

[1] H. Iwaniec, *Topics in Classical Automorphic Forms*, Graduate Studies in Mathematics **17**, Amer. Math. Soc., Providence, RI, 1997.