PUNKTE ÜBER ENDLICHEN KÖRPERN UND DIE KONGRUENZ-ZETA-FUNKTION. ([1], S. 51–54, 56–61, [2], S. 176–177)

In Ihrem Vortrag sollen Sie die Kongruenz-Zeta-Funktion einer elliptischen Kurve über einem endlichen Körper definieren und diese für die Reduktion der Kurven E_n modulo einer Primzahl p berechnen.

Zu einer Folge $\{N_r\}_{r=0}^{\infty}$ definieren wir die zugehörige *Zeta-Funktion* durch die formale Potenzreihe

$$Z(T) = \exp\left(\sum_{r=1}^{\infty} \frac{1}{r} N_r T^r\right),$$

worin

$$\exp(u) = \sum_{k=0}^{\infty} \frac{u^k}{k!}.$$

Es sei K ein Körper und

$$\mathbb{A}_K^m = \left\{(x_1, \ldots, x_m) \,\middle|\, x_j \in K\right\}$$

die Menge aller m-Tuppel mit Elementen aus K. Unter einer *affine algebraischen Varietät im m-dimensionalen Raum (definiert) über K* verstehen wir ein System polynomialer Gleichungen der Gestalt

$$f_i(x_1, \ldots, x_m) = 0, \quad \text{worin } f_i \in K[x_1, \ldots, x_m]. \tag{1}$$

Definieren Sie auch, was eine *projektive algebraische Varietät* ist.

Es sein nun V eine affine oder eine projektive algebraische Varietät über einem endlichen Körper $\mathbb{F}_q$. Zu jedem Körper $K \supset \mathbb{F}_q$ bezeichnen wir mit $V(K)$ die Menge der K-Punkte von V, d.h. die Lösungen von (1) mit $x_j \in K$ $(1 \leq j \leq m)$. Wenn K ein endlicher Körper ist, dann ist $V(K)$ endlich. Wir betrachten im Folgenden die Anzahl $\#V(K)$.

Die *Kongruenz-Zeta-Funktion von V über $\mathbb{F}_q$* ist die Zeta-Funktion zur Folge $N_r = \#V(\mathbb{F}_{q^r})$, d.h.

$$Z(V/\mathbb{F}_q; T) = \exp\left(\sum_{r=1}^{\infty} \frac{\#V(\mathbb{F}_{q^r})}{r} T^r\right).$$

Weil vermutete, dass $Z(V/\mathbb{F}_q; T)$ eine rationale Funktion in T der Gestalt

$$Z(V/\mathbb{F}_q; T) = \frac{P(T)}{(1-T)(1-qT)}$$

ist, worin P ein Polynom ist. Darüberhinaus formulierte er mehrere Eigenschaften des Polynoms P. Deligne bewies diese Vermutungen 1973 in einer bahnbrechenden Arbeit. Formulieren Sie in Ihrem Vortrag die Weil-Vermutungen, ohne auf ihren Beweis einzugehen.

Die Weil-Vermutungen waren zwar in voller Allgemeinheit sehr schwer zu beweisen, es gibt aber Spezialfälle in denen die Funktion $Z(V/\mathbb{F}_q; T)$ leichter verstanden werden kann. In Ihrem Vortrag sollen Sie insbesondere die Kongruenz-Zeta-Funktion der elliptischen Kurve E_n : $y^2 = x^3 - n^2 x$ berechnen. Führen Sie hierzu multiplikative Charaktere und Jacobi- sowie Gauss-Summen ein. Ein *multiplikativer Charakter von $\mathbb{F}_q$* ist ein Homomorphismus von der Einheitengruppe $\mathbb{F}_q \setminus \{0\}$ von $\mathbb{F}_q$ nach $\mathbb{C} \setminus \{0\}$. Es seien nun χ_1 und χ_2 zwei multiplikative Charaktere

von $\mathbb{F}_q$. Wir setzen $\chi_j(0) = 0$ und definieren die zugehörige *Jacobi-Summe*

$$J(\chi_1, \chi_2) = \sum_{x \in \mathbb{F}_q} \chi_1(x)\chi_2(1-x).$$

Desweiteren definieren wir zu einem multiplikativen Charakter χ auf $\mathbb{F}_q$ die *Gauss-Summe* ($q = p^f$ mit p eine Primzahl, $f \in \mathbb{N}$)

$$g(\chi) = \sum_{x \in \mathbb{F}_q} \chi(x) e^{\frac{2\pi i}{p} \operatorname{Sp}(x)},$$

worin

$$\operatorname{Sp}(x) = \sum_{j=0}^{f-1} x^{p^j}.$$

Es gelten folgende Eigenschaften der Jacobi- und Gauss-Summen, die Sie ohne Beweis verwenden können:

(1) Es sei χ ein multiplikativer Charakter von $\mathbb{F}_q$. Dann gilt

$$g(\chi) g(\overline{\chi}) = \chi(-1) q,$$
$$|g(\chi)| = \sqrt{q}.$$

(2) Es seien χ_1 und χ_2 multiplikative Charaktere von $\mathbb{F}_q$. Dann gilt

$$J(\chi_1, \chi_2) = \frac{g(\chi_1)\, g(\chi_2)}{g(\chi_1 \chi_2)} \qquad (\chi_1 \neq \overline{\chi_2}).$$

Es stellt sich heraus, dass die Anzahl der Punkte auf der elliptischen Kurve E_n über endlichen Körpern durch eine einfache Formel angegeben werden kann. Um diese Formel anzugeben, definieren wir zunächst, was wir unter Kongruenzen in dem Ring $\mathbb{Z}[i]$ verstehen. Wir schreiben ($\alpha, \beta, \gamma \in \mathbb{Z}[i]$)

$$\alpha \equiv \beta \pmod{\gamma},$$

wenn es ein $\delta \in \mathbb{Z}[i]$ gibt mit

$$\delta\gamma = \alpha - \beta.$$

Beweisen Sie nun folgenden Satz. Sie können hierzu benutzen, dass für einen Charakter $\chi_4 : \mathbb{F}_q^\star \to \mathbb{C}$ der Ordnung 4 mit $q \equiv 1 \pmod 4$ die Identiät $\chi_4(-4) = 1$ gilt.

Satz 1. *Es sei $p \nmid 2n$ eine Primzahl. Dann gilt*

$$\#E_n(\mathbb{F}_{p^r}) = p^r + 1 - \alpha^r - \overline{\alpha}^r,$$

worin $\alpha \equiv \left(\frac{n}{p}\right) \pmod{2+2i}$ ist, falls $p \equiv 1 \pmod 4$, und $\alpha = i\sqrt{p}$, falls $p \equiv 3 \pmod 4$.

Folgern Sie nun:

Satz 2. *Es sei $p \nmid 2n$ eine Primzahl. Dann gilt*

$$Z(E_n/\mathbb{F}_p; T) = \frac{(1-\alpha T)(1-\overline{\alpha} T)}{(1-T)(1-pT)},$$

worin α wie im vorangegangenen Satz definiert ist.

Literatur

[1] N. Koblitz, Introduction to Elliptic Curves and Modular Forms, Springer, Berlin, 1993.
[2] N. Robbins, Beginning number theory, Jones and Bartlett, Sudbury, MA, 2006.