BINÄRE QUADRATISCHE FORMEN ([1], S. 57–65)

Eine (ganzzahlige) *binäre quadratische Form* ist eine Funktion $f : \mathbb{Z}^2 \to \mathbb{Z}$ der Form

$$f(x, y) = ax^2 + bxy + cy^2$$

mit $a, b, c \in \mathbb{Z}$. In Ihrem Vortrag sollen sie die Grundlagen der Theorie der binären quadratischen Formen behandeln. Im nächsten Vortrag werden wir dann eine Verbindung zu L-Funktionen herstellen.

In der Theorie der quadratischen Formen wird unter anderem untersucht wieviele Lösungen $(x, y) \in \mathbb{Z}^2$ die Gleichung

$$f(x, y) = n \tag{1}$$

für eine gegebene Zahl $n \in \mathbb{N}$ hat. Es sei $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, d.h. $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ und $\alpha\delta - \beta\gamma = 1$. Wir setzen

$$f_M(x, y) = \left(a\alpha^2 + b\alpha\gamma + c\gamma^2\right) x^2 + \left(2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta\right) xy + \left(a\beta^2 + b\beta\delta + c\delta^2\right) y^2.$$

Zeigen Sie, dass für jedes $M \in \mathrm{SL}_2(\mathbb{Z})$ und jedes $n \in \mathbb{N}$ die Anzahl der Lösungen von $f(x, y) = n$ gleich der Anzahl der Lösungen von $f_M(x, y) = n$ ist. Wir nennen daher die Formen f und f_M *äquivalent*. Die Menge $\left\{f_M \middle| M \in \mathrm{SL}_2(\mathbb{Z})\right\}$ nennen wir *die Äquivalenzklasse von f*.

Wir nennen die Zahl $D = D_f = b^2 - 4ac$ die *Diskriminante* von $f(x, y) = ax^2 + bxy + cy^2$. Es gilt $D_f = D_{f_M}$. Genau jene Zahlen D sind Diskriminanten von binären quadratischen Formen, für die $D \equiv 0, 1 \pmod 4$ gilt. Wir sagen eine Diskriminante D ist eine *Fundamentaldiskriminante*, falls es keine ganze Zahl $r \neq \pm 1$ mit $r^2 \mid D$ und $\frac{D}{r^2} \equiv 0, 1 \pmod 4$ gibt. Zeigen Sie, dass es für jedes $D \neq 0$ nur endlich viele Äquivalenzklassen binärer quadratischer Formen mit Diskriminante D gibt.

Eine binäre quadratische Form nennen wir *primitiv*, falls $\mathrm{ggT}(a, b, c) = 1$ gilt. Eine binäre quadratische Form, die für $(x, y) \neq (0, 0)$ nur positive Werte $f(x, y) > 0$ annimmt, nennen wir *positiv definit*. Eine Form f ist genau dann primitiv (bzw. positiv definit), wenn f_M primitiv (bzw. positiv definit) ist. Wir nennen diese beiden Eigenschaften daher auch *Klasseninvarianten*. Es sei nun $D > 0$ (bzw. $D < 0$). Wir bezeichnen die Anzahl der Äquivalenzklassen primitiver (bzw. primitiver positiv definiter) binärer quadratischer Formen als die *Klassenzahl* $h(D)$ von D. Es sei $f_1, \ldots, f_{h(D)}$ ein Vertetersystem der entsprechenden Klassen. Wir schreiben $R(n, f_j)$ für die Anzahl der Lösungen von (1) mit $f = f_j$ und betrachten

$$R(n) = R_D(n) = \sum_{j=1}^{h(D)} R(n, f_j).$$

Um $R(n)$ zu berechnen, bestimmen wir die *Automorphismengruppe* $\left\{M \in \mathrm{SL}_2(\mathbb{Z}) \middle| f_M = f\right\}$ von $f = f_j$ $(1 \leq j \leq h(D)$. Hierzu betrachten wir Lösungen $(t, u) \in \mathbb{Z}$ der *Pellschen Gleichung*

$$t^2 - Du^2 = 4. \tag{2}$$

Beweisen Sie folgenden Zusammenhang zwischen der Automorphismengruppe von f_j $(1 \leq j \leq h(D))$ und den Lösungen der Pellschen Gleichung.

Satz 1. *Es sei* $f(x, y) = ax^2 + bxy + cy^2$ *eine primitive binäre quadratische Form, deren Diskriminante* D *kein Quadrat ist. Dann ist die Abbildung*

$$(t, u) \mapsto \begin{pmatrix} \frac{t-bu}{2} & -cu \\ au & \frac{t+bu}{2} \end{pmatrix}$$

eine Bijektion zwischen den Lösungen der Pellschen Gleichung (2) *und der Automorphismengruppe von* f.

Geben Sie auch den folgenden Satz ohne Beweis an.

Satz 2. *Falls* $D < 0$ *ist, so hat die Pellsche Gleichung genau* w *Lösungen, worin*

$$w = \begin{cases} 6 & \text{falls } D = -3, \\ 4 & \text{falls } D = -4, \\ 2 & \text{sonst.} \end{cases}$$

Falls $D > 0$ *ist, so ist die Automorphismengruppe von* f *zu* $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *isomorph.*

Im nächsten Vortrag werden wir die Berechnung von $R(n)$ fortsetzen sowie eine Verbindung zu L-Reihen herstellen.

Literatur

[1] D. Zagier, Zetafunktionen und quadratische Körper: eine Einführung in die höhere Zahlentheorie, Springer-Verlag, Berlin, 1981, 1–149.