Prof. E.-W. Zink
HUB

VL Ausgewählte Kapitel der Algebra und Zahlentheorie

Zusammenfassung unter besonderer Berücksichtigung von Kapitel 3

1. Vorlesung

Kapitel 1 Grundlagen und Beispiele

1.0 Einführung. Diverse Beispiele für natürliche Zahlen mit besonderen Eigenschaften und damit zusammenhängende Fragestellungen.

1.1 Pythagoräische Zahlentripel (PT). Klassifizierung der primitiven pythagoräischen Zahlentripel (PPT). Die geometrische Betrachtungsweise.

2. Vorlesung

1.2 Beweis der Unlösbarkeit von $x^4+y^4=z^4$ mit ganzen Zahlen x, y, z. Der Fermat'sche Widerspruchsbeweis durch descent infini.

1.3 Charakterisierung des Ringes $\mathbb{Z}$ der ganzen Zahlen. Trichotomie und Wohlordnung. Als Konsequenz hat man die Möglichkeit der Division mit Rest und den euklidischen Algorithmus zur Bestimmung des größten gemeinsamen Teilers (ggT).

3. Vorlesung

Zerlegung einer ganzen Zahl in zwei Faktoren; eine Methode, welche von der binomischen Formel $x^2-y^2=(x+y)(x-y)$ ausgeht.

4. Vorlesung

1.3.4 Zur Effektivität des euklidischen Algorithmus.

1.3.7 Algorithmus zur Bestimmung von $a = \mathrm{ggT}(a_1, \cdots a_n)$ und zur Berechnung einer Linearkombination $a = x_1a_1 + \cdots + x_na_n$.

5. Vorlesung

1.3.8 /1.3.9 Das Hauptlemma über Primzahlen und die Eindeutigkeit der Primfaktorzerlegung.

1.4 Eine Anwendung der eindeutigen Primfaktorzerlegung ist der Satz von Euler: Die Summe der Reziproken aller Primzahlen divergiert.

Kapitel 2 Kongruenzen

2.1 Grundlagen

2.1.1 - 4 Die Kongruenz nach einem fixierten Modul $m(\geq 1)$ ist eine Äquivalenzrelation auf $\mathbb{Z}$ und teilt die Menge aller ganzen Zahlen in m paarweise disjunkte Äquivalenzklassen, nämlich die Restklassen modulo m.

6. Vorlesung

2.1.5 Die Menge $\mathbb{Z}/m\mathbb{Z}$ der Restklassen modulo m bildet einen Ring mit m Elementen.

2.1.6 Die Fermat-Zahlen $F_m = 2^{2^m} + 1$ und die Zerlegbarkeit von F_5.

2.1.7 Der Ring $\mathbb{Z}/m\mathbb{Z}$ ist ein Körper genau dann, wenn $m = p$ eine Primzahl ist.

2.1.8 Algorithmus zur Berechnung des Inversen in $\mathbb{Z}/p\mathbb{Z}$.

2.1.9 -2.1.11 Die primen Restklassen sind die Einheiten im Ring $R = \mathbb{Z}/m\mathbb{Z}$. Die Eulersche Funktion $\varphi(m)$ und der Satz von Fermat, Euler.

7. Vorlesung

2.2 Anwendung des Rechnens mit Kongruenzen.

2.2.1 Der chinesische Restsatz.

Es seien $m_1, \cdots, m_r$ ganze Zahlen, welche paarweise zueinander prim sind und es sei $M = m_1 \cdots m_r$ ihr Produkt. Dann hat die simultane Kongruenz $x \equiv x_i \mod m_i$ für $i = 1, \cdots, r$ mit beliebig vorgegebenen $x_i \in \mathbb{Z}$ stets eine Lösung $x \in \mathbb{Z}$ und die Restklasse von $x \mod M$ ist eindeutig bestimmt. Ringtheoretisch ausgedrückt heißt das:

$$\mathbb{Z}/_{M\mathbb{Z}} \cong \mathbb{Z}/_{m_1\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{m_r\mathbb{Z}}$$

Beispiel:

Lösen Sie die simultanen Kongruenzen

$$\begin{array}{rcll} x & \equiv & 4 & \mod 7 \\ & & 3 & \mod 12 \\ & & 9 & \mod 13. \end{array}$$

Beginne mit dem

Ansatz (1) $x = 7y + 4$.

Die zweite Kongruenz lautet dann $7y \equiv -1 \mod 12$.

Das Inverse von $7 \mod 12$ ergibt sich durch elementare Spaltenoperationen aus:

$$\begin{pmatrix} 12 & 7 \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 5 & 7 \\ -1 & 1 \end{pmatrix} \sim \begin{pmatrix} 5 & 2 \\ -1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 \\ -5 & 2 \end{pmatrix}.$$

Ergebnis: $[7]_{12}^{-1} = [-5]_{12}$. Daher

$$y \equiv (-5)(-1) \mod 12.$$

Ansatz (2) $y = 12z + 5$.

Daraus folgt $x = 7y + 4 = 84z + 39$ und die dritte Kongruenz lautet

$$\begin{aligned} 84z &\equiv -30 \mod 13, \text{d.h} \\ 6z &\equiv 9 \mod 13. \qquad (3) \end{aligned}$$

Das Inverse von $6 \mod 13$ folgt aus:

$$\begin{pmatrix} 13 & 6 \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 6 \\ -2 & 1 \end{pmatrix},$$

also gleich -2. Somit folgt aus (3)

$$\begin{aligned} z &\equiv (-2) \cdot 9 \equiv -5 \mod 13 \\ y &= 12z + 5 = -55 \\ x &= 7y + 4 = -381. \end{aligned}$$

Die Lösung ist eindeutig modulo $7 \cdot 12 \cdot 13 = 1092$, d.h.

$$x = -381 + 1092 \cdot n$$

für beliebiges $n \in \mathbb{Z}$ ist die allgemeine Lösung.

2.2.2 Der Satz von Fermat und Euler.

2.2.3 Zyklische Gruppen und ihre Untergruppen.

8. Vorlesung

2.2.4 Kongruenzen nach Untergruppen und der Satz von Lagrange.

2.3 Quadratische Reste.

2.3.1 Lösen von quadratischen Gleichungen im Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

2.3.2 Das Legendre-Symbol.

2.2.3 - 4 Das Kriterium von Euler und die Existenz von Primitivwurzeln.

2.3.5 Folgerungen aus dem Kriterium von Euler.

2.3.6 Das quadratische Reziprozitätsgesetz (QRepG).

9. Vorlesung

2.3.7 Das Jacobi-Symbol als Hilfsmittel zur Berechnung von Legendre-Symbolen.

Beispiel:

Entscheiden Sie, ob 113 ein quadratischer Rest modulo 1987 ist.

Es ist wichtig für das Verfahren, dass $p = 1987$ eine Primzahl ist (denn keine der Primzahlen $2, 3, 5, \cdots 43 < \sqrt{1987}$ teilt diese Zahl). Modulo 1987 gibt es 1986 Restklassen ungleich der Nullklasse. Davon sind 993 quadratische Reste und 993 quadratische Nichtreste.
Man könnte die Quadrate aller Zahlen $1, 2, \cdots, 993$ hinschreiben und modulo 1987 reduzieren. Dann könnte man direkt sehen, ob die 113 in dieser Menge der quadratischen Restklassen liegt oder im Komplement.

Viel effektiver ist aber das Rechnen mit dem Legendre- (bzw. Jacobi-) Symbol unter Benutzung des quadratischen Reziprozitätsgesetzes:

Für $a, b > 0$, beide <u>ungerade</u> und $\mathrm{ggT}(a, b) = 1$ gilt:

$$\begin{aligned} \left(\frac{a}{b}\right) &= \left(\frac{b}{a}\right) && \text{falls} \quad a \equiv 1(4) \quad \text{oder} \quad b \equiv 1(4) \\ &= -\left(\frac{b}{a}\right) && \text{falls} \quad a \equiv 3(4) \quad \text{und} \quad b \equiv 3(4). \end{aligned}$$

Aus $113 \equiv 1(4)$ folgt also

$$\begin{aligned} \left(\frac{113}{1987}\right) &= \left(\frac{1987}{113}\right) = \left(\frac{66}{113}\right) = \left(\frac{-47}{113}\right) = \left(\frac{-1}{113}\right)\left(\frac{47}{113}\right) \\ \left(\frac{47}{113}\right) &= \left(\frac{113}{47}\right) = \left(\frac{19}{47}\right) = -\left(\frac{47}{19}\right) = -\left(\frac{9}{19}\right) = -1, \end{aligned}$$

weil 9 ein Quadrat ist.

Außerdem $\left(\frac{-1}{113}\right) = 1$, also:

$\left(\frac{113}{1987}\right) = -1$, d.h. 113 ist quadratischer Nichtrest.

$\square$

$$\begin{aligned} \left(\frac{101}{1987}\right) &= \left(\frac{1987}{101}\right) = \left(\frac{-33}{101}\right) = \left(\frac{-1}{101}\right)\left(\frac{33}{101}\right) \\ &= \left(\frac{101}{33}\right) = \left(\frac{2}{33}\right) = 1, \end{aligned}$$

weil $33 \equiv 1 \mod 8$. (Zusatz zum quadratischen Reziprozitätsgesetz, Jacobi-Symbol.)

Also $101 \equiv x^2 \mod 1987$ ist *lösbar*.

Wir haben den Fall, wo $p = 1987, p \equiv 3(4)$. In diesem Fall ist $x \equiv 101^{\frac{p+1}{4}} = 101^{497}$ *eine Lösung*. Es gilt $497 = 2^8 + 2^7 + 2^6 + 2^5 + 2^4 + 1$ und man kann 101^{497} mit der Methode des fortgesetzten Quadrierens ausrechnen.

Lemma: *Sei* $a \equiv x^2 \mod p$ *und* $p \equiv 3 \mod 4$. *Dann ist* $x = a^{\frac{p+1}{4}}$ *eine Lösung.*

Denn: $$\begin{aligned} x^2 &= a^{\frac{p+1}{2}} = a \cdot a^{\frac{p-1}{2}} = a \cdot x^{p-1} \\ &\equiv a \mod p, \end{aligned}$$

weil stets $x^{p-1} \equiv 1 \mod p$.

$\square$

2.3.8 Eigenschaften des Jacobi-Symbols.

Kapitel 3 Binäre quadratische Formen (BQF).

3.1 Grundprinzipien

3.1.1 Definition einer BQF mit ganzzahligen Koeffizienten. $f(x,y) = ax^2 + bxy + cy^2$ Kurzschreibweise: $f = (a,b,c)$.
Zu gegebenem $m \in \mathbb{Z}$ suchen wir *ganzzahlige Lösungen* (x,y) der Gleichung

$$f(x,y) = m. \tag{4}$$

(Mit Lösbarkeit ist im Folgenden immer ganzzahlige Lösbarkeit gemeint.)

3.1.2 Eine Lösung (x,y) heißt **eigentlich**, falls ggT $(x,y) = 1$.

3.1.3 Sei $m \neq 0$. Dann läßt sich jede Lösung von (1) realisieren in der Form $(x,y) = (dx_0, dy_0)$, wobei d^2 ein Teiler von m und (x_0, y_0) eine eigentliche Lösung der Gleichung $f(x,y) = m/d^2$ ist. Für quadratfreies m hat (1) nur eigentliche Lösungen.

3.1.4 Definition ganzzahliger unimodularer Transformationen des $\mathbb{R}^2$. Mit $GL(2,\mathbb{Z})$ wird die Gruppe aller dieser Transformationen bezeichnet und mit $SL(2,\mathbb{Z})$ die Untergruppe derjenigen mit Determinante gleich 1.

3.1.5 Sei $L = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL(2,\mathbb{Z})$ eine unimodulare Transformation und $f = (a,b,c)$ eine BQF. Dann wird eine Form $f \circ L$ definiert durch:

$$(f \circ L)(x,y) := f((x,y) \cdot L^t),$$

wobei L^t die transponierte Matrix ist. Explizit:

$$\begin{aligned} (f \circ L)(x,y) &= f\left((x,y)\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}\right) \\ &= f(x\alpha + y\beta,\ x\gamma + y\delta) \\ &= a'x^2 + b'xy + c'y^2 \\ \text{mit} \qquad a' &= (f \circ L)(1,0) = f(\alpha,\gamma) \\ c' &= (f \circ L)(0,1) = f(\beta,\delta) \\ b' &= (f \circ L)(1,1) - (f \circ L)(1,0) - (f \circ L)(0,1) \\ &= f(\alpha+\beta, \gamma+\delta) - a' - c'. \end{aligned}$$

Zwei BQF f, g heißen äquivalent, falls ein $L \in SL(2,\mathbb{Z})$ existiert, sodass $g = f \circ L$. In diesem Fall ist $f(x,y) = m$ lösbar genau dann, wenn $g(x,y) = m$ lösbar ist.

Zusatz: Sei $S(f,m)$ die Menge aller $(x,y) \in \mathbb{Z}^{1\times 2}$ sodass $f(x,y) = m$. Dann gilt $S(f,m) = S(f \circ L, m) \cdot L^t$. Also genügt es die Lösungen von $(f \circ L)(x,y) = m$ für geeignete Matrizen $L \in SL_2(\mathbb{Z})$ zu finden.

3.1.6 Die Matrizenschreibweise $f(x,y) = \frac{1}{2}(x,y)F_f\begin{pmatrix} x \\ y \end{pmatrix}$ mit symmetrischer 2×2 Matrix $F_f = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$. Es gilt $F_{f\circ L} = L^t \cdot F_f \cdot L$ für $L \in GL(2,\mathbb{Z})$.

10. Vorlesung:

3.1.7 Die Diskriminante der Form $f = (a, b, c)$ ist $D_f = b^2 - 4ac$. Äquivalente BQF haben dieselbe Diskriminante. Dies folgt aus 3.1.6, weil $D_f = -\det(F_f)$, also $D_{f\circ L} = -\det(L^t \cdot F_f \cdot L) = D_f$.

3.1.8 Definite und indefinite BQF.
Für $f = (a, b, c)$ mit $a \neq 0$ und $D_f \neq 0$ ist die Form (positiv) definit für $D_f < 0$ (und $a > 0$). Im Fall $D_f > 0$ ist die Form indefinit.

3.1.9 Eine Matrix $L \in SL(2, \mathbb{Z})$ heißt Automorphismus von $f = (a, b, c)$, falls

$$(f \circ L)(x, y) = f(x, y).$$

Für je zwei Automorphismen L, L' ist auch $L \cdot L'$ Automorphismus von f und ebenso L^{-1}. Deshalb bilden die Automorphismen von f eine Untergruppe $A_f \subset SL(2, \mathbb{Z})$. Diese Gruppe enthält immer mindestens 2 Elemente, nämlich $L = \pm\, I$ (wobei $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ die Einheitsmatrix bezeichnet). Im definiten Fall (d.h. $D_f < 0$) besteht die Automorphismengruppe A_f bis auf seltene Ausnahmen nur aus diesen beiden Elementen.
Im indefiniten Fall (d.h. $D_f > 0$, das wurde in der VL nicht mehr behandelt) hat A_f im allgemeinen unendlich viele Elemente.

3.1.10 Konstruktion der *eigentlichen* Lösungen von $f(x, y) = m$ im Fall $m \neq 0$.
Sei $f = (a, b, c)$. Grundidee ist das Auffinden von Formen $f_i = (m, b_i, c_i)$, welche offensichtlich m darstellen und zu f *äquivalent* sind. Im *ersten Schritt* sucht man Formen f_i, welche *dieselbe Diskriminante* wie f haben, d.h. $b_i^2 - 4mc_i = D_f$. Solche Formen existieren genau dann, wenn die Kongruenz $x^2 \equiv D_f \bmod 4\,|m|$ lösbar ist. Im *zweiten Schritt* muss man entscheiden, welche dieser Formen sogar zu f *äquivalent* sind. In dem angenehmen Sonderfall, wo die Klassenzahl $h(D_f) = 1$ ist (siehe unten), folgt aus der Gleichheit der Diskriminanten bereits die Äquivalenz. Wichtig für die Anzahl der eigentlichen Lösungen ist auch die Größe der Automorphismengruppe A_f. Hier gibt es wesentliche Unterschiede zwischen dem definiten und dem indefiniten Fall (vgl. 3.1.9).

Zusatz: $f_i(x, y) = m$ **hat offensichtlich die Lösung** $(x, y) = (1, 0)$. **Ist nun** $f_i = f \circ L_i$ **äquivalent zu** f **dann folgt aus dem Zusatz zu 3.1.5 dass** $(1, 0) \cdot L_i^t \in S(f, m)$.

3.2 Der positiv definite Fall (PDBQF).
In diesem Abschnitt betrachten wir immer $f = (a, b, c)$ mit $D_f < 0$ und $a > 0$ (woraus auch $c > 0$ folgt). Dann sind Gleichungen $f(x, y) = m$ höchstens für positives m lösbar.

3.2.1 Auswirkungen der Transformationen $S^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ und $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ auf f.
(Achtung: Ganz am Ende des Abschnittes sind die Bezeichnungen S, T für diese Matrizen vertauscht.)

3.2.2 Die PDBQF $f = (a, b, c)$ heißt *reduziert*, falls $|b| \leq a \leq c$ gilt.

3.2.3 **Satz:** *Zu* $f = (a, b, c)$ *existiert immer eine äquivalente Form* $f \circ L$, $L \in SL(2, \mathbb{Z})$, *welche reduziert ist.*

3.2.4 Geometrische Veranschaulichung.
Definiert werden Vektoren $v, w \in \mathbb{R}^2$, sodass $f(x, y) = \|xv + yw\|^2$. Die Lösungen von $f(x, y) = m$ entsprechen damit den Punkten des von v, w erzeugten Gitters, welche auf dem Kreis mit Radius $\sqrt{m}$ (um den Ursprung) liegen.

11. Vorlesung

3.2.5 Die Vektoren $v, w, v \pm w$ haben nach Konstruktion die Absolutbeträge $\sqrt{a}$, $\sqrt{c}$ bzw. $\sqrt{a \pm b + c}$. Dem entsprechen im Fall einer reduzierten Form f drei sogenannte Minimumkreise, welche zu Lösungen führen (vgl. 3.2.4).

3.2.6 **Satz:** $D < 0$ *eine fixierte Diskriminante. Dann gibt es nur endlich viele Äquivalenzklassen von PDBQF, deren Diskriminante gleich* D *ist (vgl. 3.1.7).*

Bemerkung: $f = (a, b, c)$ heißt **primitive Form**, falls ggT $(a, b, c) = 1$ ist.
Sei d gemeinsamer Teiler von (a, b, c) und sei $f \circ U = f' = (a', b', c')$ für $U \in SL(2, \mathbb{Z})$. Dann ist d auch gemeinsamer Teiler von (a', b', c'). Insbesondere ist mit f auch $f \circ U$ primitiv.

3.2.7 **Definition:** Als Klassenzahl $h(D)$ bezeichnet man die Anzahl verschiedener Äquivalenzklassen von *primitiven* PDBQF mit Diskriminante $D < 0$.

Tiefliegende Sätze:

A) Satz von Heilbronn und Siegel: Mit $D \to -\infty$ geht $h(D) \to +\infty$, d.h. die Klassenzahl wird beliebig groß.

B) Satz von Heegner, Stark und Baker: Es gibt genau 13 negative Werte D mit $h(D) = 1$, nämlich: $D = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163$.
Wir betrachten jetzt die Form $f(x, y) = x^2 + y^2$, d.h. $f = (1, 0, 1)$ mit der Diskriminante $D_f = -4$. In diesem Fall ist die Klassenzahl $h(-4) = 1$ und die Automorphismengruppe (vgl. 3.1.9) ist $\{I, T, T^2, T^3\} \subset SL(2, \mathbb{Z})$, also von der Ordnung 4. Durch Anwendung von 3.1.10 folgt:

3.2.8 **Satz:** *Es sei* $m \geq 1$ *und* $r'(m)$ *sei die Anzahl der eigentlichen Lösungen von* $x^2 + y^2 = m$*. Dann ist*

$$\begin{array}{rcl} r'(m) & = & 0 \quad \textit{falls} \quad 4|m \quad \textit{oder falls} \quad p|m \quad \textit{für eine Primzahl} \quad p \equiv 3 \mod 4 \\ r'(m) & = & 4 \cdot 2^r \quad \textit{anderenfalls, wobei} \quad r \quad \textit{die Anzahl der Primteiler} \quad p \neq 2 \\ & & \textit{von} \quad m \quad \textit{bezeichnet (die dann alle} \quad \equiv 1 \mod 4 \quad \textit{sind).} \end{array}$$

Zum Beweis genügt es, die Anzahl der verschiedenen Formen $f_i = (m, b_i, c_i)$ zu finden, deren Diskriminante $D_{f_i} = b_i^2 - 4mc_i = -4$ ist. Wegen $h(-4) = 1$ sind diese

Formen alle äquivalent zu $f = (1,0,1)$. Da f_i offensichtlich die Zahl m darstellt, gilt dasselbe für f (vgl. 3.1.10). Also sind die Lösungen der Kongruenz $x^2 \equiv -4 \mod 4m$ zu untersuchen, d.h. $x = 2y$ und $y^2 \equiv -1 \mod m$. Mit dem chinesischen Restsatz reduziert man dies auf den Fall, wenn m eine Primzahlpotenz ist.
Hilfssatz: Für $p \neq 2$ ist $(\mathbb{Z}/p^e)^\times$ für alle Potenzen $e \geq 1$ eine zyklische Gruppe der Ordnung $\varphi(p^e) = p^e - p^{e-1}$. Also kann man hier (ebenso wie für $e = 1$) eine Indexrechnung durchführen und es folgt:

$$x^2 \equiv -1 \mod p^e \quad \text{hat zwei bzw. keine Lösung(en)}$$

je nachdem, ob $p \equiv 1 \mod 4$ oder $p \equiv 3 \mod 4$ ist.

12. Vorlesung:
Es sei $r(m)$ die Anzahl *aller* Lösungen vom $x^2+y^2 = m$ (nicht nur die eigentlichen).

3.2.9 **Satz:** (i) $r(m) = \sum\limits_{d^2|m} r'\left(\dfrac{m}{d^2}\right)$.

(ii) $\dfrac{1}{4}r(m)$ *ist multiplikative Funktion (siehe unten).*

(iii) $\dfrac{1}{4}r(m) = \sharp\{d;\ d|m \ \ und \ \ d \equiv 1 \mod 4\} - \sharp\{d;\ d|m \ \ und \ \ d \equiv 3 \mod 4\}$.

Bemerkung: Da $\frac{1}{4}r(m)$ multiplikative Funktion ist, wird die Formel (iii) eigentlich nur in dem Fall gebraucht, wenn $m = p^e$ Primzahlpotenz ist.
Zu (ii): Eine zahlentheoretische Funktion $f : \mathbb{N} \to \mathbb{C}$ heißt multiplikativ, falls $f(mn) = f(m)f(n)$ immer dann, wenn ggT $(m,n) = 1$.

3.2.10 **Satz:** *Die Faltung* $(f * g)(m) := \sum\limits_{d|m} f(d)g\left(\dfrac{m}{d}\right)$ *von zwei multiplikativen Funktionen ist wieder multiplikativ. Dies gilt insbesondere dann, wenn* $g(d) \equiv 1$ *ist.*

Aus 3.2.9 (i), 3.2.10 und der Tatsache, dass $\frac{1}{4}r'(m)$ eine multiplikative Funktion ist, folgt dasselbe für $\frac{1}{4}r(m)$.

Thema: Veranschaulichung der PDBQF durch Punkte der oberen Halbebene.
Wir ordnen jeder PDBQF $f = (a,b,c)$ eine komplexe Zahl $z = \omega_1(f)$ mit *positivem* Imaginärteil zu, welche als Punkt der oberen Halbebene betrachtet wird. (Bemerkung: Nach Voraussetzung sind $D_f < 0$ und $a > 0$, insbesondere $a \neq 0$.)
Wegen $D_f = b^2 - 4ac < 0$ sind die Nullstellen von $ax^2 + bx + c$ *nicht reell*, sondern es ergeben sich zwei konjugiert komplexe Nullstellen:

$$\omega_{1/2}(f) = -\frac{b}{2a} \pm \frac{\sqrt{|D_f|}}{2a}i,$$

wobei $\omega_1(f)$ positiven Imaginärteil hat. Der Absolutbetrag ist $|\omega_{1/2}(f)|^2 = \frac{c}{a}$. Mit $z = \omega_1(f)$ gilt dann: $ax^2 + bx + c = a(x-z)(x-\bar{z})$, wobei $\bar{z} = \omega_2(f)$ die konjugiert komplexe Zahl ist. Daraus folgt:

$$f(x,y) = ax^2 + bxy + cy^2 = a(x - zy)(x - \bar{z}y).$$

Ist $g = (da, db, dc)$ eine zu $f = (a, b, c)$ proportionale Form, dann folgt offensichtlich:

$$\omega_i(f) = \omega_i(g) \quad \text{für} \quad i = 1, 2.$$

Deshalb beschränkt man sich auf *primitive* Formen $f = (a, b, c)$, dh. ggT $(a, b, c) = 1$. Es seien $\mathcal{F}$ die Menge der primitiven PDBQF, $\mathbb{H} = \{z = s + ti;\ t > 0\}$ die obere Halbebene der komplexen Zahlenebene $\mathbb{C}$ und:

$$\mathbb{H}_0 = \{z \in \mathbb{H}; s = Re(z) \in \mathbb{Q},\ t = Im(z) \text{ habe } t^2 \in \mathbb{Q}\}.$$

3.2.11 **Satz:**

$$f = (a, b, c) \in \mathcal{F} \longmapsto z = \omega_1(f) \in \mathbb{H}_0$$

ist eine Bijektion mit der Umkehrabbildung

$$z = s + ti \in \mathbb{H}_0 \longmapsto f_z = (a_z,\ -2a_z s,\ a_z(s^2 + t^2)),$$

wobei $a_z = kgV$ *(Nenner* $(-2s)$*, Nenner* $(s^2 + t^2)$*). Es gilt dann* $D_{f_z} = -4a_z^2 \cdot t^2 < 0$.

Weitere Eigenschaften: Unter $f = (a, b, c) \mapsto z = \omega_1(t)$ gilt $|z| = \sqrt{\frac{c}{a}}$ und:
f ist reduziert, d.h. $|b| \leq a \leq c$ gdw. $z = \omega_1(t)$ hat $|z| \geq 1$ (also z außerhalb des Einheitskreises) und $Re(z) = -\frac{b}{2a}$ liegt im Intervall $\left[-\frac{1}{2}, \frac{1}{2}\right]$.
Die reduzierten Formen aus $\mathcal{F}$ werden also in den Bereich $B = \left\{z \in \mathbb{C};\ |z| \geq 1, Re(z) \in \left[-\frac{1}{2}, \frac{1}{2}\right]\right\}$ abgebildet.

3.2.12 Aktion von $SL(2, \mathbb{Z})$ auf der oberen Halbebene $\mathbb{H}$.
Für $L = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL(2, \mathbb{Z})$ und $z \in \mathbb{H}$ setzen wir $L\begin{pmatrix} z \\ 1 \end{pmatrix} = \dfrac{\alpha z + \beta}{\gamma z + \delta}$.
Dies ist die normale Multiplikation Matrix mal Spaltenvektor, wobei zwischen die beiden Koordinaten ein Bruchstrich gesetzt wird. Zu L gehört damit die Transformation $z \mapsto T_L(z) = L\begin{pmatrix} z \\ 1 \end{pmatrix}$.
Man kann zeigen, dass es zu jedem $z \in \mathbb{H}$ genau ein $L \in SL(2, \mathbb{Z})$ gibt, sodass $T_L(z) \in B$ ist. Für fixiertes z befindet sich also in der Menge $\{T_L(z);\ L \in SL(2, \mathbb{Z})\}$ genau ein Element aus B. Man nennt B einen **Fundamentalbereich** für die Aktion von $SL(2, \mathbb{Z})$ auf $\mathbb{H}$.

Satz: *Unter der Abbildung*

$$f \in \mathcal{F} \longmapsto z = \omega_1(f) \in \mathbb{H}_0$$

gilt $\omega_1(f \circ L) = T_{L^{-1}}(\omega_1(f))$*, für alle* $L \in SL(2, \mathbb{Z})$.

Anwendung 1: Zu $f \in \mathcal{F}$ gehöre $z \in \mathbb{H}_0$. Dann besteht die Automorphismengruppe A_f (vgl. 3.1.9) aus allen $L \in SL(2, \mathbb{Z})$ mit der Eigenschaft:

(5) $$T_L(z) = \frac{\alpha z + \beta}{\gamma z + \delta} = z.$$

Z.B. gehört zu $f(1,0,1)$ die Zahl $z = i$ und $\dfrac{\alpha i + \beta}{\gamma i + \delta} = i$ ist genau für

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \{I, T, T^2, T^3\} \quad \text{mit} \quad T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

erfüllt.
Bis auf Ausnahmefälle ist (2) nur für $L = I, -I$ erfüllt, d.h. die Automorphismengruppe besteht normalerweise nur aus 2 Elementen.

Anwendung 2: Seien $f,\ g \in \mathcal{F}$ zwei PDBQF mit derselben Diskriminante $D_f = D_g$. Dazu betrachten wir $z_f = \omega_1(f),\ z_g = \omega_1(g) \in \mathbb{H}$. Da B ein Fundamentalbereich ist, finden wir $L,\ U \in SL(2,\mathbb{Z})$ sodass $T_L(z_f),\ T_U(z_g) \in B$, und es gilt dann:
Satz: Die Formen $f,\ g$ sind äquivalent, $f \sim g$ genau dann wenn $T_L(z_f) = T_U(z_g) \in B$, und weil $T_L(z_f) = z_{f \circ L^{-1}}$, bedeutet dies: $f \circ L^{-1} = g \circ U^{-1}$ und $g = f \circ (L^{-1}U)$. Auf diese Weise kann man also entscheiden ob die Formen äquivalent sind und die zugehörige Transformationsmatrix finden.

Zusatz: Indefinite BQF, d.h. $f = (a,b,c)$ mit $D_f = b^2 - 4ac > 0$ wurden nicht mehr behandelt. Hier bestehen die Automorphismengruppen A_f im allgemeinen aus unendlich vielen Elementen wie bereits in 3.1.9 erwähnt wurde. Einfachste Beispiele sind:

$$f = (1,0,-d), \quad \text{d.h.} \quad f(x,y) = x^2 - dy^2$$

mit $d > 0$, d.h. $D_f = 4d > 0$. In diesem Fall hat bereits die sogenannte Pellsche Gleichung $x^2 - dy^2 = 1$ unendlich viele Lösungen,die sich aber alle auf eine Minimallösung zurückführen lassen (vgl. Silverman, Kap. 28-31).

3.2.13 **Ein Beispiel:** Wir betrachten $f = (1,1,1)$, d.h. $f(x,y) = x^2 + xy + y^2$ und die Gleichung

$$(1) \qquad f(x,y) = p,$$

wobei p eine Primzahl $\neq 2,3$ ist.

Die Diskriminante ist $D_f = -3$ und der erste Koeffizient von f ist positiv. Also ist f positiv definit.

Wir suchen eine Form:

$$(2) \qquad g(x,y) = px^2 + bxy + cy^2,$$

welche dieselbe Diskriminante wie f hat. (Offensichtlich gilt $g(1,0) = p$.) Die Gleichung

$$(3) \qquad D_g = b^2 - 4pc = -3$$

ist lösbar genau dann, wenn

$$(4) \qquad b^2 \equiv -3 \mod 4p.$$

Wegen dem chinesischen Restsatz genügt dafür die Lösbarkeit von

$$b^2 \equiv -3 \mod p, \tag{5}$$

d.h. das Legendre-Symbol $\left(\frac{-3}{p}\right) = 1$.
Aus dem quadratischen Reziprozitätsgesetz folgt

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right),$$

d.h. (5) ist lösbar, unlösbar je nachdem, ob $p \equiv 1 \mod 3$, $p \equiv -1 \mod 3$.

Weil die Klassenzahl $h(-3) = 1$ ist, folgt aus der Gleichheit $D_g = D_f = -3$ bereits die Äquivalenz der Formen g, f.
Somit:
Die Gleichung (1) ist lösbar genau dann, wenn $p \equiv 1 \mod 3$ ist.

Für $p = 7$ hat $b^2 \equiv -3 \mod 7$ die Lösungen $b = 2, -2 (\equiv 5 \mod 7)$ und für die Lösung $b = 5$ gilt sogar:

$$b^2 \equiv -3 \mod 28.$$

Es folgt $c = \frac{b^2+3}{28} = 1$, d.h.

$$g(x,y) = 7x^2 + 5xy + y^2 \tag{6}$$

hat dieselbe Diskriminante wie f,nämlich $D = -3$.

Zu $f = (1,1,1)$ bzw. $g = (7,5,1)$ gehören die komplexen Zahlen

$$z_f = -\frac{1}{2} + \frac{\sqrt{3}}{2}i,\ z_g = -\frac{5}{14} + \frac{\sqrt{3}}{14}i$$

der oberen Halbebene. Nun ist z_f bereits Element des Fundamentalbereiches B. Außerdem errechnet man:

$$z_f = \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \circ z_g = \begin{pmatrix} -3, & -1 \\ 1, & 0 \end{pmatrix} \circ z_g.$$

Daraus ergibt sich $g = f \circ U$ mit $U = \begin{pmatrix} -3 & -1 \\ 1 & 0 \end{pmatrix}$. Demzufolge ist dann:

$$(1,0) \cdot U^t = (-3,1)$$

eine Lösung der Gleichung

$$x^2 + xy + y^2 = 7.$$

Literatur: (zur VL und SE):

[S]	J.H. Silverman	A friendly introduction to Number Theory, Prentice Hall 1997
[Sh]	I.R. Shafarevich	Discourses on Algebra, Springer Verlag 2003
[BS]	S.I. Borevicz, I.R. Săfarevič	Zahlentheorie, Birkhäuser Verlag 1966
[H]	E. Hlawka, J Schoißengeier	Zahlentheorie, eine Einführung, Wien 1990, Manz Verlag
[Sc]	H. Scheid	Zahlentheorie, Mannheim 1994

Seminar „Ausgewählte Kapitel der Algebra und Zahlentheorie“

Vortragstitel und Literaturhinweis

SE1, Mo 17-19 Uhr

- Binomische Formel und Binomialkoeffizienten, [Sh], (Kliche)
- Binomialkoeffizienten und Kombinatorik, [Sh], (Voigt)
- Tschebyscheff-Abschätzungen für die Primzahlfunktion, [Sc], (Teichert, Claus)
- Das Bertrandsche Postulat, [Sc], (Nar)
- Kettenbrüche, [Sc], (List, Gande, Mielke)
- Potenzen modulo m und Kryptographie, [S], (Meixner)
- Primitivwurzeln und Indizes modulo p, [S], (Theuerkauf)
- Der Lucas-Test für Mersenne-Zahlen, [Sc], (Herrys, Stobernack)
- Darstellung von Zahlen als Summe zweier Quadrate, [S], (Mülle)

SE2, Mo 15-15 Uhr

- Mersenne-Zahlen und perfekte Zahlen, [S], (Gertfelder)
- Abzählformel für die Vereinigung von Teilmengen, [Sh], (Stier)
- Summen von Potenzen und Bernoulli-Polynome, [Sh], (Ebrahimi)
- Polynome und Bernoulli-Zahlen,[Sh], (Krüger)
- Primitivwurzeln und Indizes modulo p, [S], (Widuch, Widuch, Breunig, Winter)
- Bernoullische Zahlen, [BS], (Dimler)
- Quadrat-Dreieckszahlen und die Pellsche Gleichung, [S], (Zink)