Teil II. Quadratische Körper und ihre Zetafunktionen

§8 Binäre quadratische Formen

Neben dem Beweis des Satzes, daß arithmetische Folgen unendlich viele Primzahlen enthalten, war der Wunsch, Klassenzahlen binärer quadratischer Formen ausrechnen zu können, einer der Hauptgründe Dirichlets, Charaktere und L-Reihen einzuführen. Was diese Klassenzahlen sind und wie sie mit L-Reihen zusammenhängen, wollen wir in diesem Paragraphen erläutern, wobei wir im wesentlichen Dirichlets Argument folgen werden.

Als erstes müssen wir etwas über die Theorie der quadratischen Formen erzählen, die fast ganz von Gauß in den *Disquisitiones Arithmeticae* entwickelt wurde. Der Ausgangspunkt dieser Theorie ist die Frage nach der *Lösbarkeit* von quadratischen Diophantischen Gleichungen, z.B. der Nachweis, daß die *Pellsche Gleichung*

$$(1) \qquad t^2 - Du^2 = 4$$

für jede Nichtquadratzahl $D > 0$ eine Lösung mit $u \neq 0$ hat oder der Fermatsche Satz, daß jede Primzahl $p \equiv 1 \pmod 4$ eine Darstellung

$$(2) \qquad p = x^2 + y^2$$

zuläßt. Außerdem interessiert man sich für die *Anzahl* der Lösungen, z.B für die Tatsache, daß die Darstellung (2) bis auf die Reihenfolge von x und y eindeutig ist. Allgemein ist eine *binäre quadratische Form* ein Ausdruck der Gestalt

$$(3) \qquad f(x,y) = ax^2 + bxy + cy^2 \; ,$$

wobei a, b, c (die *Koeffizienten* der Form) als fest und x, y als veränderlich anzusehen sind. Wir werden stets annehmen, daß die Koeffizienten a, b, c in $\mathbb{Z}$ liegen und auch, da wir nur binäre Formen (d.h. Formen in zwei Variablen) betrachten, das Wort "binär" häufig weglassen. Die Hauptfrage ist dann, für eine gegebene quadratische Form f und ganze Zahl n die Lösungen der Gleichung $f(x,y) = n$ $(x,y \in \mathbb{Z})$ zu beschreiben.

Sei $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ eine 2×2 Matrix mit ganzzahligen Koeffizienten und Determinante 1. Ersetzen wir x und y in (3) durch

$$\begin{aligned} x' &= \alpha x + \beta y\ , \\ y' &= \gamma x + \delta y\ , \end{aligned} \tag{4}$$

so geht (3) in die Form $a'x^2 + b'xy + c'y^2$ mit

$$a'x^2 + b'xy + c'y^2 = a(\alpha x+\beta y)^2 + b(\alpha x+\beta y)(\gamma x+\delta y) + c(\gamma x+\delta y)^2, \tag{5}$$

d.h. mit

$$\begin{aligned} a' &= a\alpha^2 + b\alpha\gamma + c\gamma^2 \\ b' &= 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta \\ c' &= a\beta^2 + b\beta\delta + c\delta^2\ , \end{aligned} \tag{6}$$

über. Die Frage, ob für eine Zahl n die Gleichung

$$ax^2 + bxy + cy^2 = n \tag{7}$$

lösbar ist, ist jetzt offensichtlich mit der Frage äquivalent, ob

$$a'x^2 + b'xy + c'y^2 = n \qquad (x,\ y \in \mathbb{Z}) \tag{8}$$

lösbar ist, denn jede Lösung von (8) liefert wegen (5) eine Lösung $(\alpha x + \beta y,\ \gamma x + \delta y)$ von (7), und umgekehrt führt jede Lösung von (7) vermöge der zu (4) inversen Transformation

$$\begin{aligned} x &= \delta x' - \beta y' \\ y &= -\gamma x' + \alpha y' \end{aligned}$$

zu einer Lösung von (8). Es gibt also eine natürliche bijektive Korrespondenz zwischen den Lösungsmengen der Gleichungen (7) und (8), und da wir uns ja gerade für diese Lösungen interessieren, ist es natürlich, die entsprechenden quadratischen Formen als äquivalent zu betrachten. Dies führt zu folgender

<u>Definition</u>: Zwei quadratische Formen $f(x,y) = ax^2 + bxy + cy^2$ und $f'(x,y) = a'x^2 + b'xy + c'y^2$ heißen *äquivalent*, falls sie unter einer Substitution $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$, $\alpha,\ \beta,\ \gamma,\ \delta \in \mathbb{Z}$, $\alpha\delta - \beta\gamma = 1$ wie in (5) inein-

ander übergehen, d.h. falls die Koeffizienten von f und f' durch (6) verknüpft sind.

Da die Menge $SL_2(\mathbb{Z})$ der Matrizen $\begin{pmatrix}\alpha & \beta \\ \gamma & \delta\end{pmatrix}$ mit $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$, $\alpha\delta - \beta\gamma = 1$, eine Gruppe bildet, also unter Inversenbildung und Zusammensetzung abgeschlossen ist, ist es klar, daß diese Relation symmetrisch und transitiv, also wirklich eine Äquivalenzrelation ist.

Wieviele Äquivalenzklassen gibt es? Sicherlich unendlich viele, denn - wie man leicht nachprüft - die *Diskriminante*

$$D = b^2 - 4ac \tag{9}$$

einer Form (3) ist eine Invariante der Äquivalenzklasse (d.h., sie bleibt unverändert unter der Transformation (6)), und es gibt umgekehrt zu jeder Zahl D mit

$$D \equiv 0 \quad \text{oder} \quad 1 \pmod 4 \tag{10}$$

mindestens eine Form der Diskriminante D, nämlich die *Grundform*

$$f_1(x,y) = \begin{cases} x^2 - \frac{D}{4}y^2, & \text{falls } D \equiv 0 \pmod 4 \\ x^2 + xy + \frac{1-D}{4}y^2, & \text{falls } D \equiv 1 \pmod 4 . \end{cases} \tag{11}$$

Eine vernünftigere Frage wäre also: wieviele Äquivalenzklassen von Formen gibt es mit gegebener Diskriminante? Das erste Hauptergebnis besagt, daß es nur endlich viele gibt:

<u>SATZ 1</u>: *Sei* $D \in \mathbb{Z}$, D *kein Quadrat. Dann gibt es nur endlich viele Äquivalenzklassen von quadratischen Formen mit der Diskriminante* D.

<u>Bemerkung</u>: Die Behauptung des Satzes bleibt richtig für D ein Quadrat, $D \neq 0$ (s. Aufgabe 1). Formen mit quadratischer Diskriminante werden wir im folgenden aber nicht betrachten, da diese in lineare Faktoren zerfallen.

<u>Beweis</u>: Wir zeigen, daß jede Form $f = ax^2 + bxy + cy^2$ zu einer Form $a'x^2 + b'xy + c'y^2$ äquivalent ist, deren Koeffizienten den Ungleichungen

$$|b'| \leq |a'| \leq |c'| \tag{12}$$

genügen. Die Behauptung folgt dann, da es nur endlich viele Zahlentripel (a', b', c') gibt, die (12) erfüllen und einen gegebenen Wert $b'^2 - 4a'c' = D$ haben: es ist nämlich

$$|D| = |b'^2-4a'c'| \geq |4a'c'| - |b'|^2$$
$$\geq 4|a'|^2 - |a'|^2 = 3a'^2 ,$$

also

$$|a'| \leq \sqrt{\frac{|D|}{3}} , \quad |b'| \leq |a'| , \quad c' = \frac{b'^2-D}{4a'} ,$$

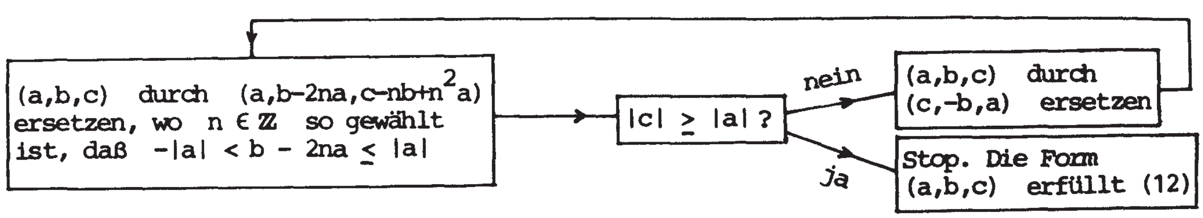
so daß nur endlich viele Werte für a', b', c' in Frage kommen. Um (12) zu erreichen, wählen wir a' als die dem Absolutbetrag nach kleinste Zahl, die durch f darstellbar ist. Dann gibt es Zahlen α und γ mit

$$a' = a\alpha^2 + b\alpha\gamma + c\gamma^2 ,$$

und der größte gemeinsame Teiler r von α und γ muß gleich 1 sein, weil a'/r^2 durch f darstellbar ist. Wir können also Zahlen β und δ so wählen, daß $\alpha\delta - \beta\gamma = 1$ ist; dann transformiert $\left(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}\right)$ die Form f in eine Form $a'x^2 + b''xy + c''y^2$ mit a' als erstem Koeffizienten (vgl. (6)). Wir wählen dann eine ganze Zahl n so, daß $b' := b'' - 2a'n$ dem Absolutbetrag nach kleiner gleich a' ist. Wegen

$$a'(x - ny)^2 + b''(x - ny)y + c''y^2$$
$$= a'x^2 + (b'' - 2a'n)xy + (a'n^2 - b''n + c'')y^2$$

ist dann $a'x^2 + b''xy + c''y^2$ (und somit auch f) zu einer Form $a'x^2 + b'xy + c'y^2$ äquivalent mit $|b'| \leq |a'|$ (oder sogar $-|a'| < b' \leq |a'|$). Schließlich ist nach Wahl von a' automatisch $|c'| \geq |a'|$, also (12) erfüllt. Damit ist der Satz bewiesen. Dieser Beweis, der ineffektiv ist (wie findet man a'?), kann durch einen effektiven Algorithmus ersetzt werden; dieser Algorithmus wird durch das Flußdiagramm



verdeutlicht und bricht deswegen nach endlich vielen Schritten ab, weil $|a|$ bei jedem Umlauf um mindestens 1 heruntergeht.

Die Aussage des Satzes folgt auch aus den später in diesem Paragraphen ausgeführten Überlegungen über Darstellungsanzahlen.

Wir wollen die Klassenzahl von D, also die Anzahl der Äquivalenzklassen von quadratischen Formen der Diskriminante D, einführen und studieren. Neben der Diskriminante gibt es aber zwei weitere elementare Invarianten von quadratischen Formen, und wir wollen die Einteilung von Formen in Äquivalenzklassen verfeinern, indem wir auch diese festlegen. Die Invarianten sind:

1) der g.g.T. der Koeffizienten von f,
2) das Vorzeichen des ersten Koeffizienten, falls $D < 0$.

In der Tat, wenn a, b und c durch r teilbar sind, ist r nach (6) auch ein Teiler von a', b' und c'; es gilt also $(a,b,c) \mid (a',b',c')$ und wegen der Symmetrie dann $(a,b,c) = (a',b',c')$. Sind $ax^2 + bxy + cy^2$ und $a'x^2 + b'xy + c'y^2$ äquivalent und $D < 0$, so ist nach (6)

$$(13) \qquad aa' = a^2\alpha^2 + ab\alpha\gamma + ac\gamma^2 = (a\alpha + \tfrac{1}{2}b\gamma)^2 + \tfrac{1}{4}|D|\gamma^2 > 0 ,$$

also haben a und a' dasselbe Vorzeichen. Ist dieses Vorzeichen positiv, so ist $f(\alpha,\gamma)$ wegen (13) für alle $(\alpha,\gamma) \neq (0,0)$ positiv; die Form heißt dann *positiv-definit*. Ist $a < 0$, so stellt f nur negative Zahlen dar und heißt *negativ-definit*. Die Äquivalenzklassen von quadratischen Formen zerfallen also für $D < 0$ in zwei Typen, je nachdem, ob sie positiv- oder negativ-definite Formen enthalten; wir brauchen nur die positiv-definiten zu betrachten, da die negativ-definiten Formen durch Multiplikation mit -1 aus ihnen entstehen. Wir können uns auch auf Formen beschränken, für die der g.g.T. der Koeffizienten gleich 1 ist - solche Formen heißen *primitiv* - weil eine Form der Diskriminante D mit $(a,b,c) = r$ einfach r mal eine primitive Form der Diskriminante D/r^2 ist. Wir definieren also die *Klassenzahl* von D als

$$h(D) = \begin{cases} \text{Anzahl der Äquivalenzklassen von primitiven} \\ \text{quadratischen Formen der Diskriminante } D, \\ \text{falls } D > 0, \\[1ex] \text{Anzahl der Äquivalenzklassen von positiv-} \\ \text{definiten primitiven Formen der Diskriminante} \\ D, \text{ falls } D < 0. \end{cases}$$

Diese Anzahl ist nach Satz 1 endlich. Sie ist Null, falls (10) nicht erfüllt ist, da dann (9) keine Lösung hat, ist dagegen ≥ 1, falls (10) erfüllt ist, da es dann immer mindestens die Grundform (11) gibt. Wir fügen eine kleine Tabelle von Klassenzahlen bei. (Wie man diese Werte berechnet, werden wir später sehen.)

D	-24	-23	-20	-19	-16	-15	-12	-11	-8	-7	-4	-3
h(D)	2	3	2	1	1	2	1	1	1	1	1	1

D	1	4	5	8	9	12	13	16	17	20	21	24	25	28	29
h(D)	1	1	1	1	2	2	1	2	1	3	2	2	4	2	1

Warnung: Es gibt zwei Begriffe von Äquivalenz (und damit auch zwei Klassenzahlen), die in der Literatur gebraucht werden. Die oben eingeführte Äquivalenz bezüglich $SL_2(\mathbb{Z})$ heißt *Äquivalenz im engeren Sinne*. Die *Äquivalenz im weiteren Sinne* ist definiert durch die Formel: $f' \sim f$, falls

$$f'(x,y) = \mu f(\alpha x+\beta y, \gamma x+\delta y) \quad , \tag{14}$$

wobei $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ eine 2×2 Matrix mit ganzzahligen Koeffizienten und Determinante $\alpha\delta - \beta\gamma = \mu = \pm 1$ ist. Dieser letzte Begriff (allerdings häufig fehlerhaft definiert, indem der Faktor μ in (14) fehlt) wird in vielen Lehrbüchern zugrundegelegt und die Klassenzahl $h(D)$ entsprechend definiert als die Anzahl der Äquivalenzklassen von primitiven quadratischen Formen der Diskriminante D (nicht notwendig positiv-definit, falls $D < 0$) im weiteren Sinne. Diese andere Klassenzahl, die wir mit $h_0(D)$ bezeichnen werden, stimmt für D negativ mit unserer Klassenzahl überein, da die Transformationen (14) mit $\mu = -1$ einfach die positiv- und negativ-definiten Formen vertauschen. Für $D > 0$ gilt $h_0(D) = h(D)$ oder $h_0(D) = \frac{1}{2}\, h(D)$ (s. Aufgabe 5).

Sei jetzt f eine quadratische Form. Wir wollen wissen, welche Zahlen f darstellt und wie oft, d.h. die Lösungen der Diophantischen Gleichung

$$f(x,y) = n \qquad (x,\ y \in \mathbb{Z}) \tag{15}$$

untersuchen. Auf der Menge dieser Lösungen gibt es eine natürliche Äquivalenzrelation. Ist nämlich $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in SL_2(\mathbb{Z})$ eine Matrix mit der Eigenschaft, daß die durch (6) definierte quadratische Form $a'x^2 + b'xy + c'y^2$ mit f übereinstimmt, dann führt die Transformation (4) offenbar eine Lösung von (15) in eine andere über. In diesem Falle nennen wir $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ einen *Automorphismus* von f. Es ist klar, daß die Automorphismen von f eine Untergruppe U_f von $SL_2(\mathbb{Z})$ bilden; nach (6) ist

$$U_f = \left\{ \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; ① \;\; a\alpha^2 + b\alpha\gamma + c\gamma^2 = a, \right.$$
$$\left. ② \;\; 2a\alpha\beta + b\beta\gamma + b\alpha\delta + 2c\gamma\delta = b,\;\; ③ \;\; a\beta^2 + b\beta\delta + c\delta^2 = c \right\} . \tag{16}$$

Wir definieren die *Darstellungsanzahl* $R(n,f)$ *von* n *durch die Form* f als die Anzahl der unter der Operation von U_f inäquivalenten Lösungen der Gleichung (15). Es wird sich herausstellen, daß $R(n,f)$ endlich ist. Offenbar hängt sie nur von der Äquivalenzklasse von f ab. Wir definieren die *Gesamtdarstellungsanzahl* $R(n)$ *von* n *durch Formen der Diskriminante* D als

$$(17)\qquad R(n) = \sum_{i=1}^{h(D)} R(n,f_i)\ ,$$

wobei $f_1, \ldots, f_{h(D)}$ Repräsentanten der Äquivalenzklassen von primitiven binären quadratischen Formen der Diskriminante D sind (positiv- bzw. negativ-definit, falls $D < 0$ und n positiv bzw. negativ ist).

Für die einzelnen Darstellungsanzahlen $R(n,f_i)$ ist kein geschlossener Ausdruck bekannt; man kann i.a. nur den Mittelwert $\lim\limits_{N\to\infty} \frac{1}{N} \sum\limits_{n=1}^{N} R(n,f_i)$ berechnen. Dagegen läßt sich die Gesamtdarstellungsanzahl $R(n)$ in geschlossener Form angeben. Die Schritte zur Berechnung der Klassenzahl nach Gauß und Dirichlet werden also die folgenden sein:

i) Bestimmung der Struktur der Automorphismengruppe U_f;
ii) Berechnung von $R(n)$ (also auch von deren mittlerem Wert);
iii) Berechnung der mittleren Werte der $R(n,f_i)$, $1 \le i \le h(D)$;
iv) Bestimmung von $h(D)$ durch Vergleich von ii) und iii).

Diese vier Schritte werden in den nächsten vier Sätzen durchgeführt.

<u>SATZ 2</u>: *Sei* $f(x,y) = ax^2 + bxy + cy^2$ *eine primitive quadratische Form der Diskriminante* D, D *keine Quadratzahl. Dann liefert die Abbildung*

$$(18)\qquad (t,u) \mapsto \begin{pmatrix} \frac{t-bu}{2} & -cu \\ au & \frac{t+bu}{2} \end{pmatrix}$$

eine Bijektion zwischen der Menge der Lösungen (t,u) *der Pellschen Gleichung (1) und der Automorphismengruppe von* f. *Diese Bijektion ist ein Gruppenisomorphismus bezüglich der Kompositionsregel*

$$(19)\qquad (t_1,u_1) \circ (t_2,u_2) = \left(\frac{t_1t_2 + Du_1u_2}{2}\ ,\ \frac{t_1u_2 + u_1t_2}{2}\right)$$

für Lösungen von (1). Die Gruppe U_f *ist für* $D < 0$ *endlich, und zwar zyklisch von der Ordnung*

$$(20)\qquad w = \begin{cases} 6 & \text{für } D = -3\ , \\ 4 & \text{für } D = -4\ , \\ 2 & \text{für } D < -4\ . \end{cases}$$

Für $D > 0$ *ist* $U_f \cong \mathbb{Z} \times \mathbb{Z}/2$.

<u>Beweis</u>: Aus (16) finden wir für $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in U_f$

$$\begin{aligned} a\beta &= \beta(a\alpha^2 + b\alpha\gamma + c\gamma^2) \qquad \text{(wegen (1))} \\ &= \alpha(a\alpha\beta + b\beta\gamma) + c\beta\gamma^2 \\ &= \alpha(-c\gamma\delta) + c\beta\gamma^2 \end{aligned}$$

(da wegen (2) $2(a\alpha\beta + b\beta\gamma + c\gamma\delta) = b(1 - \alpha\delta + \beta\gamma) = 0$)

$$= -c\gamma \qquad (\text{wegen } \alpha\delta - \beta\gamma = 1)$$

und analog

$$\begin{aligned} c(\alpha-\delta) &= \alpha(a\beta^2 + b\beta\delta + c\delta^2) - c\delta \qquad \text{(wegen (3))} \\ &= \beta(a\alpha\beta + c\gamma\delta) + b\alpha\beta\delta \qquad (\text{wegen } \alpha\delta - \beta\gamma = 1) \\ &= -\beta(b\beta\gamma) + b\alpha\beta\delta \quad (\text{wieder wegen } a\alpha\beta + b\beta\gamma + c\gamma\delta = 0) \\ &= \beta b\ , \end{aligned}$$

also $\frac{\gamma}{a} = \frac{\delta-\alpha}{b} = \frac{-\beta}{c}$. Da $(a,b,c) = 1$ ist, ist dieser gemeinsame Wert eine ganze Zahl u; mit $t = \alpha + \delta$ haben wir dann

$$\alpha = \frac{t-bu}{2}\ ,\ \delta = \frac{t+bu}{2}\ ,\ \beta = -cu\ ,\ \gamma = au\ ,$$

und aus $\alpha\delta - \beta\gamma = 1$ folgt dann $t^2 - Du^2 = 4$. Umgekehrt findet man durch Einsetzen, daß die Matrix in (18) ein Automorphismus von f ist. Daß die Matrizenmultiplikation der Regel (19) entspricht, ergibt sich ebenfalls durch direktes Rechnen.

Ist jetzt $D < 0$, so ist $t^2 - Du^2 \geq t^2$ und $t^2 - Du^2 \geq |D|u^2$; also hat (1) nur Lösungen für $|t| \leq 2$, $|u| \leq 2$, und zwar

$$\begin{aligned} &(t,u) = (\pm 2,0) \quad \text{oder} \quad (\pm 1,\pm 1) \quad \text{für} \quad D = -3\ , \\ (21) \qquad &(t,u) = (\pm 2,0) \quad \text{oder} \quad (0,\pm 1) \quad \text{für} \quad D = -4\ , \\ &\text{nur} \quad (t,u) = (\pm 2,0)\ , \qquad \text{falls} \quad D < -4\ . \end{aligned}$$

Damit ist gezeigt, daß die Anzahl der Lösungen von (1) gleich der in (20) angegebenen Zahl w ist. Wenn wir für jede Lösung (t,u) von (1)

$$(22) \qquad \varepsilon = \frac{t + u\sqrt{D}}{2}\ ,\ \varepsilon' = \frac{t - u\sqrt{D}}{2} \qquad (\varepsilon\varepsilon' = 1)$$

setzen (bei fester Wahl von $\sqrt{D}$), dann entspricht (19) einfach der Multiplikation der entsprechenden Zahlen ε; wir erhalten also durch

$$(23) \qquad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mapsto \varepsilon = \frac{\alpha+\delta}{2} + \frac{\gamma}{2a}\sqrt{D}$$

einen injektiven Homomorphismus von U_f in $\mathbb{C}^*$. Für $D < 0$ haben wir nach (21)

$$(24) \qquad \begin{aligned} \varepsilon &= \pm 1 \quad \text{oder} \quad \frac{\pm 1 \pm i\sqrt{3}}{2} && \text{für} \quad D = -3 \\ \varepsilon &= \pm 1 \quad \text{oder} \quad \pm i && \text{für} \quad D = -4 \\ \varepsilon &= \pm 1 && \text{für} \quad D < -4 \; , \end{aligned}$$

also genau die w-ten Einheitswurzeln; das zeigt, daß U_f zyklisch ist. (Man kann natürlich auch direkt nachrechnen, daß alle Lösungen (21) unter dem Gruppengesetz (19) Potenzen von $(1,1)$ bzw. $(0,1)$ bzw. $(-2,0)$ sind.)

Für $D > 0$ liefert (23) eine Injektion $U_f \to \mathbb{R}^*$. Das Bild ist eine Untergruppe von $\mathbb{R}^*$, die -1 enthält. Da (mit der positiven Wahl von $\sqrt{D}$) die Zahl ε in (22) für $t, u > 0$ mindestens gleich $\frac{1+\sqrt{D}}{2} > 1$ ist, ist das Bild nicht dicht in $\mathbb{R}^*$. Es gibt also nur zwei Möglichkeiten: entweder ist die Pellsche Gleichung nur trivial (d.h. mit $u = 0$, $t = \pm 2$) lösbar und $U_f = \{\pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\}$, oder es gibt eine kleinste Lösung (t_0,u_0) von (1) mit $t_0, u_0 > 0$ und die Menge der ε in (22) ist gleich $\{\pm\varepsilon_0^n | n \in \mathbb{Z}\}$ mit $\varepsilon_0 = \frac{t_0 + u_0\sqrt{D}}{2}$, also $U_f \cong \mathbb{Z} \times \mathbb{Z}/2$. Wir werden später sehen, daß stets der zweite Fall zutrifft, womit auch die letzte Behauptung des Satzes bewiesen sein wird. Die Zahl ε_0 heißt die *Grundeinheit* der Form f. Sie hängt nur von D ab.

Der Einfachheit halber formulieren wir den nächsten Satz und sein Korollar nur für Fundamentaldiskriminanten. Für den allgemeinen Fall s. Aufgabe 8.

<u>SATZ 3</u>: *Sei* D *eine Fundamentaldiskriminante,* $n \neq 0$ *eine ganze Zahl. Dann wird die Gesamtanzahl* $R(n)$ *der Darstellungen von* n *durch (primitive) Formen der Diskriminante* D *durch*

$$(25) \qquad R(n) = \sum_{m|n} \chi_D(m)$$

gegeben, wobei m *über alle positiven Teiler von* n *läuft und* $\chi_D(m)$ *der in §5 eingeführte Charakter ist. Insbesondere sind* $R(n)$ *und somit alle* $R(n,f)$ *endlich.*

<u>Bemerkung</u>: Die rechte Seite von (25) ist identisch mit der in (6.10) eingeführten Summte $\rho(n)$. Somit erhalten die in §6 für den Nachweis