c) Für jede Primzahl p ist das *Legendresche Symbol*

$$(2) \qquad \left(\frac{n}{p}\right) = \begin{cases} 0, & \text{falls } p \mid n \\ 1, & \text{falls } p \nmid n,\ n \equiv x^2 \pmod p \text{ für ein } x \in \mathbb{Z} \\ -1, & \text{sonst} \end{cases}$$

ein Dirichletscher Charakter (mod p).

Wir haben zwei einfache, aber sehr nützliche Sätze:

SATZ 2: *Sei* χ *ein Dirichletscher Charakter modulo* N. *Dann ist*

$$(3) \qquad \sum_{n \pmod N} \chi(n) = \begin{cases} \phi(N), & \text{falls } \chi = \chi_0 \\ 0, & \text{falls } \chi \neq \chi_0 . \end{cases}$$

(Hier bezeichnet $\sum_{n \pmod N}$ eine Summe über ein beliebiges Vertretersystem von $\mathbb{Z}/N\mathbb{Z}$, z.B. $\sum_{n=1}^{N}$.)

KOROLLAR: *Seien* χ_1, χ_2 *zwei Dirichletsche Charaktere* (mod N). *Dann ist*

$$(4) \qquad \frac{1}{\phi(N)} \sum_{n \pmod N} \chi_1(n)\, \bar{\chi}_2(n) = \begin{cases} 1, & \text{falls } \chi_1 = \chi_2 \\ 0, & \text{falls } \chi_1 \neq \chi_2 . \end{cases}$$

Beweis: Für $\chi = \chi_0$ ist (3) trivial. Sei $\chi \neq \chi_0$ und $m \in \mathbb{Z}$ so gewählt, daß $(m,N) = 1$ und $\chi(m) \neq 1$ ist. Dann ist

$$(1 - \chi(m)) \sum_{n \pmod N} \chi(n) = \sum_{n \pmod N} [\chi(n) - \chi(mn)]$$

$$= \sum_{n \pmod N} \chi(n) - \sum_{n \pmod N} \chi(n) = 0$$

(da mit n auch mn ein Vertretersystem von $\mathbb{Z}$ (mod N) durchläuft), also, da $\chi(m) \neq 1$,

$$\sum_{n \pmod N} \chi(n) = 0 .$$

Das Korollar folgt, indem man $\chi_1 \bar{\chi}_2$ für χ wählt.

SATZ 3: *Sei* $n \in \mathbb{Z}$. *Dann ist*

$$(5) \qquad \sum_{\chi} \chi(n) = \begin{cases} \phi(N), & \text{falls } n \equiv 1 \pmod N \\ 0, & \text{falls } n \not\equiv 1 \pmod N , \end{cases}$$

wobei über alle Dirichletschen Charaktere (mod N) *summiert wird.*

Korollar: *Seien* $a,b \in \mathbb{Z}$, $(b,N) = 1$. *Dann ist*

$$(6) \qquad \frac{1}{\phi(N)} \sum_{\chi} \chi(a)\,\bar{\chi}(b) = \begin{cases} 1, & \textit{falls } a \equiv b \pmod N \\ 0, & \textit{falls } a \not\equiv b \pmod N \end{cases}.$$

Beweis: Für $n \equiv 1 \pmod N$ ist (5) trivial, da es $\phi(N)$ Charaktere gibt und für alle χ $\chi(n) = 1$ gilt. Für $(n,N) > 1$ gilt (5) auch, da dann $\chi(n)$ für alle χ verschwindet. Sei $n \not\equiv 1 \pmod N$, $(n,N) = 1$, und χ_1 ein Dirichletscher Charakter (mod N) mit $\chi_1(n) \neq 1$. Ein solcher existiert wegen Satz 1, denn die Charaktere χ mit $\chi(n) = 1$ sind Charaktere auf der Quotientengruppe $(\mathbb{Z}/N\mathbb{Z})^\times/\langle n\rangle$, und deren Anzahl ist demnach kleiner als $|(\mathbb{Z}/N\mathbb{Z})^\times|$. Dann ist

$$\begin{aligned}(1 - \chi_1(n)) \sum_{\chi} \chi(n) &= \sum_{\chi} [\chi(n) - \chi\chi_1(n)] \\ &= \sum_{\chi} \chi(n) - \sum_{\chi} \chi(n) = 0\,,\end{aligned}$$

da $\chi\chi_1$ mit χ über die Gruppe $(\mathbb{Z}/N\mathbb{Z})^\times$ läuft. Da $1 - \chi_1(n) \neq 0$, folgt hieraus, daß die Summe verschwindet. Das Korollar folgt, indem man n mit $nb \equiv a \pmod N$ wählt.

Sei N_1 ein von N verschiedener Teiler von N und χ_1 ein Charakter (mod N_1). Dann definiert die Zusammensetzung

$$(7) \qquad (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/N_1\mathbb{Z})^\times \xrightarrow{\chi_1} \mathbb{C}^*\,,$$

wobei der erste Pfeil die Reduktion (mod N_1) ist, einen Charakter χ (mod N). Wir sagen, daß χ von χ_1 *induziert* wird und nennen einen Charakter χ, der so entsteht, *imprimitiv*; ein Charakter, der nicht auf diese Weise erhalten werden kann, heißt *primitiv* (oder *eigentlich*). Z.B. ist der Hauptcharakter χ_0 (mod N) für $N > 1$ nie primitiv, weil er von dem trivialen Charakter (mod 1) induziert wird. Für jeden Dirichletschen Charakter χ (mod N) gibt es eine kleinste Zahl N_1, so daß χ dargestellt werden kann als die Zusammensetzung (7) mit geeignetem Charakter χ_1 (mod N_1), und dies ist die einzige Darstellung (7) von χ, für die χ_1 primitiv ist. Diese Zahl N_1 mit der Eigenschaft, daß χ von einem primitiven Charakter (mod N_1) induziert wird, nennt man den *Führer* von χ.

Wir werden uns vor allem für *reelle* Charaktere ($\chi = \bar{\chi}$) interessieren, d.h. solche, die nur die Werte 1, 0, -1 annehmen. Wir beweisen einen Satz, in dem alle primitiven reellen Charaktere angegeben

werden.

Definition: Eine *Grundzahl* ist eine ganze Zahl D mit

$$D \equiv 1 \pmod 4,\ D \text{ quadratfrei},$$

oder

$$D \equiv 0 \pmod 4,\ \frac{D}{4} \text{ quadratfrei},\ \frac{D}{4} \equiv 2 \text{ oder } 3 \pmod 4 .$$

(Solche Zahlen nennt man auch *Fundamentaldiskriminanten*). Für eine Grundzahl D definieren wir eine Funktion $\chi_D\colon \mathbb{N} \to \mathbb{Z}$ durch

$$\chi_D(p) = \left(\frac{D}{p}\right) \qquad (p \text{ ungerade Primzahl}) \tag{8a}$$

$$\chi_D(2) = \begin{cases} 0, & \text{falls } D \equiv 0 \pmod 4, \\ 1, & \text{falls } D \equiv 1 \pmod 8, \\ -1, & \text{falls } D \equiv 5 \pmod 8, \end{cases} \tag{8b}$$

$$\chi_D(p_1^{n_1}\cdots p_k^{n_k}) = \chi_D(p_1)^{n_1}\cdots\chi_D(p_k)^{n_k} . \tag{8c}$$

Insbesondere ist χ_1 der triviale Charakter.

SATZ 4: *Die Funktion* $n \mapsto \chi_D(n)$ *(D eine Grundzahl) ist periodisch* (mod $|D|$) *und definiert einen primitiven Dirichletschen Charakter modulo* $|D|$ (ebenfalls mit χ_D bezeichnet) *mit*

$$\chi_D(-1) = \begin{cases} 1, & \textit{falls } D > 0, \\ -1, & \textit{falls } D < 0. \end{cases} \tag{9}$$

Jeder primitive reelle Dirichletsche Charakter ist einer der Charaktere χ_D.

Beweis: Wegen Satz 1 ist jeder Dirichletsche Charakter χ (mod N), mit $N = p_1^{r_1}\cdots p_k^{r_k}$, gleich einem Produkt $\chi_1\cdots\chi_k$, wo χ_i von einem Charakter (mod $p_i^{r_i}$) induziert wird:

$$\begin{array}{ccc} (\mathbb{Z}/N\mathbb{Z})^\times & \xrightarrow{\ \cong\ } & (\mathbb{Z}/p_1^{r_1}\mathbb{Z})^\times \times\cdots\times (\mathbb{Z}/p_k^{r_k}\mathbb{Z})^\times \\ & {\scriptstyle\chi}\searrow \quad \swarrow{\scriptstyle\chi_1\times\cdots\times\chi_k} & \\ & \mathbb{C}^* & \end{array}$$

Aus dem Diagramm geht hervor, daß χ dann und nur dann primitiv ist, wenn jeder χ_i das ist. Für die Klassifizierung solcher Charaktere genügt es also, sich auf Primzahlpotenzführer $N = p^r$ zu be-

wegen der strengen Multiplikativität $\chi(p^r) = \chi(p)^r$ ist sogar

$$L(s,\chi) = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}} \qquad (\sigma > 1) \; . \tag{2}$$

Für den Hauptcharakter χ_0 ist nach (2)

$$\begin{aligned} L(s,\chi_0) &= \prod_p (1 - \chi_0(p)p^{-s})^{-1} \\ &= \prod_{p \nmid N} (1 - p^{-s})^{-1} \\ &= \prod_{p|N} (1 - p^{-s}) \cdot \prod_{\text{alle } p} (1 - p^{-s})^{-1} \\ &= \prod_{p|N} (1 - p^{-s}) \cdot \zeta(s) \; ; \end{aligned} \tag{3}$$

also ist die L-Reihe in diesem Fall bis auf einen einfachen multiplikativen Faktor mit der Riemannschen Zetafunktion identisch. Insbesondere läßt sie sich auf die ganze komplexe Ebene meromorph fortsetzen mit einem einfachen Pol mit Residuum $\prod_{p|N} (1 - p^{-1}) = \frac{\phi(N)}{N}$ an der Stelle $s = 1$ als einziger Singularität.

Für $\chi \neq \chi_0$ ist für $x \to \infty$

$$\begin{aligned} \Big| \sum_{n=1}^{x} \chi(n) \Big| &= \Big| \sum_{n=1}^{N[x/N]} \chi(n) + \sum_{n=N\cdot[\frac{x}{N}]+1}^{x} \chi(n) \Big| \\ &= \Big| [\tfrac{x}{N}] \sum_{n \,(\mathrm{mod}\, N)} \chi(n) + \sum_{n=N[\frac{x}{N}]+1}^{x} \chi(n) \Big| \\ &= \Big| \sum_{n=N[\frac{x}{N}]+1}^{x} \chi(n) \Big| \leq |x - N[\tfrac{x}{N}]| \leq N = O(1) \end{aligned}$$

wegen Satz 2, §5; deswegen ist nach Satz 2 von §1 die Konvergenzabszisse von $L(s,\chi)$ kleiner oder gleich 0 (offensichtlich sogar gleich 0); insbesondere definiert (1) eine in $\sigma > 0$ holomorphe Funktion. In der Tat läßt sich diese Funktion auf ganz $\mathbb{C}$ holomorph fortsetzen und genügt einer Funktionalgleichung analog zu der von $\zeta(s)$ (s. §7).

Der wichtigste Satz über L-Reihen ist die Tatsache, daß der Wert von $L(1,\chi)$ (der nach dem eben Gesagten definiert ist) stets von Null verschieden ist; hieraus kann man leicht die Existenz unendlich vieler Primzahlen in arithmetischen Folgen schließen. Wir beweisen jetzt diese beiden Ergebnisse.

SATZ: *Sei χ ein von χ_0 verschiedener Dirichletscher Charakter. Dann ist*

$$L(1,\chi) \neq 0 \; . \tag{4}$$

Beweis: Sei

$$F(s) = \prod_{\chi} L(s,\chi) \ , \tag{5}$$

wo χ über sämtliche Dirichletschen Charaktere (mod N) läuft. Dann ist für $\sigma > 1$ nach (2)

$$\begin{aligned} \log F(s) &= \sum_{\chi} \sum_{p} \log\,(1 - \chi(p)p^{-s})^{-1} \\ &= \sum_{\chi} \sum_{p} \sum_{r=1}^{\infty} \frac{1}{r} \frac{\chi(p)^r}{p^{rs}} \\ &= \phi(N) \sum_{\substack{p \\ p^r \equiv 1 \,(\mathrm{mod}\ N)}} \ \sum_{r \geq 1} \frac{1}{rp^{rs}} \end{aligned} \tag{6}$$

(die letzte Gleichung folgt aus Satz 3, §5); insbesondere ist $\log F(s) \geq 0$ für s reell und > 1, und somit

$$\lim_{\substack{s \to 1 \\ s \text{ reell}}} F(s) \geq 1 \ . \tag{7}$$

Das Produkt (5) enthält nur einen Faktor, der an der Stelle $s = 1$ einen Pol hat, nämlich $L(s,\chi_0)$, und dieser Pol ist nach (3) einfach. Wenn $L(1,\chi) = 0$ wäre für *zwei oder mehr* Charaktere $\chi \neq \chi_0$, müßte demnach $F(s)$ an der Stelle $s = 1$ holomorph sein und den Wert 0 haben, was offensichtlich (7) widerspricht. Es kann also *höchstens einen* Charakter $\chi \neq \chi_0$ mit $L(1,\chi) = 0$ geben. Da mit $L(1,\chi) = 0$ auch $L(1,\bar{\chi}) = \overline{L(1,\chi)} = 0$ wäre, ist dieser Charakter χ (falls er existiert) gleich $\bar{\chi}$, also *reell*. Wir können uns also für den Beweis des Satzes auf reelle Charaktere beschränken.

Sei also χ reell mit $L(1,\chi) = 0$, und sei

$$\Phi(s) = \frac{L(s,\chi)\ L(s,\chi_0)}{L(2s,\chi_0)} \ . \tag{8}$$

Diese Funktion ist für $\sigma > \frac{1}{2}$ holomorph, da der Pol von $L(s,\chi_0)$ bei $s = 1$ durch die Nullstelle von $L(s,\chi)$ dort aufgehoben wird, während der Nenner $L(2s,\chi_0)$ wegen (3) für $\sigma > \frac{1}{2}$ von Null verschieden ist. Für $\sigma > 1$ ist

$$\begin{aligned} \Phi(s) &= \prod_{p} \frac{1 - \chi_0(p)p^{-2s}}{(1 - \chi(p)p^{-s})(1 - \chi_0(p)p^{-s})} \\ &= \prod_{p \nmid N} \frac{1 - p^{-2s}}{(1 - \chi(p)p^{-s})(1 - p^{-s})} \end{aligned}$$

$$= \prod_{p \nmid N} \frac{1 + p^{-s}}{1 - \chi(p)p^{-s}}$$

$$= \prod_{\chi(p)=1} \frac{1 + p^{-s}}{1 - p^{-s}}$$

(da $\chi(p) = \pm 1$ für $p \nmid N$ ist), also

$$\Phi(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \qquad (\sigma > 1) \qquad \text{mit } a_n \geq 0 .$$

(Um dies zu erreichen, brauchten wir den Faktor $1 + p^{-s} = \frac{1 - p^{-2s}}{1 - p^{-s}}$ in dem Euler-Produkt von Φ; das ist der Grund für die Wahl der Funktion (8).) Da $\Phi(s)$ in $\sigma > \frac{1}{2}$ holomorph ist, ist für $|s-2| < \frac{3}{2}$

$$\Phi(s) = \sum_{k=0}^{\infty} \frac{(s-2)^k}{k!} \Phi^{(k)}(2) = \sum_{k=0}^{\infty} \frac{(2-s)^k}{k!} \sum_{n=1}^{\infty} \frac{a_n (\log n)^k}{n^2} ,$$

und wegen $a_n \geq 0$ stellt die rechts stehende Doppelsumme für s reell, $\frac{1}{2} < s < 2$, eine monoton fallende Funktion dar, also ist

$$\Phi(s) \geq \Phi(2) \geq 1 \qquad (s \text{ reell}, \frac{1}{2} < s < 2) .$$

Aber nach (8) ist

$$\lim_{s \to \frac{1}{2}} \Phi(s) = \frac{L(\frac{1}{2},\chi)\, L(\frac{1}{2},\chi_0)}{\lim\limits_{s \to \frac{1}{2}} L(2s,\chi_0)} = 0 ,$$

da $L(2s,\chi_0)$ nach (3) an der Stelle $s = \frac{1}{2}$ einen Pol hat. Dieser Widerspruch beweist den Satz.

Es ist dem Leser vielleicht aufgefallen, daß dieser Beweis zu dem Beweis des Landauschen Satzes (Satz 4, §1) sehr analog ist, und in der Tat kann man (4) auch durch direkte Anwendung jenes Satzes beweisen. Sei nämlich χ reell, und

$$\psi(s) = L(s,\chi)\, \zeta(s) = \sum_{n=1}^{\infty} \frac{\rho(n)}{n^s} , \tag{9}$$

$$\rho(n) = \sum_{d \mid n} \chi(d) . \tag{10}$$

Dann ist

$$\psi(s) = \prod_{p} \frac{1}{(1 - \chi(p)p^{-s})(1 - p^{-s})}$$

$$= \prod_{\chi(p)=1} \frac{1}{(1 - p^{-s})^2} \cdot \prod_{\chi(p)=0} \frac{1}{1 - p^{-s}} \cdot \prod_{\chi(p)=-1} \frac{1}{1 - p^{-2s}} \tag{11}$$

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

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 $\{\pm\varepsilon_0^n \mid n \in \mathbb{Z}\}$ 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.

SATZ 3: *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*

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

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.*

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

von $L(1,\chi) \neq 0$ benutzten Ungleichungen (6.12) eine anschauliche Bedeutung, da offensichtlich $R(n) \geq 0$ und $R(n^2) > 0$ ist (ein Quadrat hat immer eine Darstellung durch (11) mit $y = 0$).

Beweis: Da es keine imprimitiven Formen der Diskriminante D gibt, können wir den Zusatz "primitive" im Satz weglassen. Sei $R^*(n)$ die Anzahl der inäquivalenten *primitiven* Darstellungen von n durch Formen der Diskriminante D (eine Darstellung (15) heißt primitiv, falls x und y teilerfremd sind). Offensichtlich ist

$$R(n) = \sum_{\substack{g \geq 1 \\ g^2 | n}} R^*\left(\frac{n}{g^2}\right) , \tag{26}$$

da jede Darstellung Vielfaches einer primitiven ist. Der Hauptschritt im Beweis ist der Nachweis der Formel

$$R^*(n) = \#\{b \pmod{2n} \mid b^2 \equiv D \pmod{4n}\} . \tag{27}$$

Der Beweis von (27) stützt sich auf folgendes allgemeine Prinzip. Sei G eine Gruppe, X und Y zwei Mengen, auf denen G operiert, und $S \subseteq X \times Y$ eine unter der Diagonaloperation von G invariante Teilmenge. Wenn zwei Elemente $s = (x,y)$, $s' = (x',y') \in S$ unter G äquivalent sind, also $(x',y') = (gx,gy)$, so sind insbesondere ihre ersten Komponenten G-äquivalent. Wir können also die Bahnenmenge S/G analysieren, indem wir erst X/G beschreiben und dann fragen, wieviele Elemente von S/G ein gegebenes Element von X/G als erste Komponente haben. Als Vertreter für diese Bahnen können wir Paare (x,y) nehmen, deren erste Komponente ein fester Vertreter der gegebenen Bahn in X/G ist. Zwei solche Paare (x,y) und (x,y') sind genau dann äquivalent, wenn $y' = gy$ mit $g \in G$, $gx = x$; die besagten Bahnen stehen also in eineindeutiger Korrespondenz mit den Bahnen von $Y_x = \{y \in Y \mid (x,y) \in S\}$ unter der Operation des Stabilisators $G_x = \{g \in G \mid gx = x\}$ von x in G. Insbesondere gilt für die Anzahl der Bahnen die Formel

$$|S/G| = \sum_{x \in X/G} |Y_x/G_x| , \tag{28}$$

falls beide Seiten endlich sind, und durch Rollenvertauschung natürlich auch

$$|S/G| = \sum_{y \in Y/G} |X_y/G_y| . \tag{29}$$

Wir wenden diese Formel an mit

$$G = SL_2(\mathbb{Z}) = \{\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \mid \alpha, \beta, \gamma, \delta \in \mathbb{Z},\ \alpha\delta - \beta\gamma = 1\} ,$$

$$X = \{\text{quadratische Formen } f(x,y) = ax^2+bxy+cy^2,\ b^2-4ac = D\} ,$$

$$Y = \{\text{Zahlenpaare } z = (x,y) \text{ mit } x, y \in \mathbb{Z} \text{ teilerfremd}\} ,$$

$$S = \{(f,z) \in X \times Y \mid f(z) = n\} .$$

Dann sind die Elemente von X/G die Äquivalenzklassen von Formen der Diskriminante D, und für $f \in X$ ist Y_f/G_f die Menge der inäquivalenten primitiven Darstellungen von n durch f, also nach (28)

$$|S/G| = \sum_{\substack{\text{Äquivalenz-}\\ \text{klassen von } f}} R^*(n,f) = R^*(n) .$$

Andererseits können wir $|S/G|$ durch (29) berechnen. Jedes Element von Y ist zu $(1,0)$ äquivalent, da es für $(x,y) \in Y$ Zahlen $a, b \in \mathbb{Z}$ gibt mit $ax + by = 1$, also $\begin{pmatrix}x & -b\\ y & a\end{pmatrix} \in G$, $\begin{pmatrix}x & -b\\ y & a\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = \begin{pmatrix}x\\ y\end{pmatrix}$. Somit besteht Y/G aus einer Bahn mit dem Vertreter $z = (1,0)$. Für dieses Element ist $G_z = \{\begin{pmatrix}1 & r\\ 0 & 1\end{pmatrix},\ r \in \mathbb{Z}\}$ und X_z die Menge der Formen $f \in X$ mit erstem Koeffizienten $a = n$, also

$$X_z = \{nx^2 + bxy + \frac{b^2-D}{4n} y^2,\ b \in \mathbb{Z},\ b^2 \equiv D \pmod{4n}\} .$$

Da die Operation von $\begin{pmatrix}1 & r\\ 0 & 1\end{pmatrix} \in G_z$ durch $b \to b + 2nr$ gegeben wird, ist $|X_z/G_z|$ gleich der rechten Seite der Formel (27), womit diese Formel auch bewiesen ist.

Um den Satz zu beweisen, müssen wir noch den Ausdruck in (27) explizit berechnen und das Ergebnis in (26) substituieren. Für $n = 2^{r_0}p_1^{r_1}\dots p_s^{r_s}$ (p_i ungerade) sieht man aus (27) leicht, daß

$$R^*(n) = R^*(2^{r_0})R^*(p_1^{r_1})\dots R^*(p_s^{r_s})$$

mit

$$R^*(p^r) = \#\{b \bmod p^r \mid b^2 \equiv D \pmod{p^r}\} \qquad (p \neq 2) . \tag{30}$$

Da die rechte Seite von (25) auch multiplikativ ist, brauchen wir nur Primzahlpotenzen zu betrachten. Für $p \nmid D$ (und $r > 0$) ist die rechte Seite von (30) gleich 0 oder 2, je nachdem, ob D ein quadratischer Rest oder Nichtrest modulo p ist; für $p|D$ ist sie gleich 1 für $r = 1$ (es gibt nur die Lösung $b = 0$) und gleich 0 für $r > 1$ (da $p^2 \nmid D$). Wenn wir diese Werte in (26) substituieren, finden wir:

$$R(p^r) = \sum_{0 \le s < \frac{r}{2}} 2 + \sum_{s=\frac{r}{2}} 1$$

$$= r + 1 = \sum_{0 \le i \le r} \chi_D(p^i) ,$$

falls $(\frac{D}{p}) = +1$,

$$R(p^r) = \sum_{0\le s<\frac{r}{2}} 0 + \sum_{s=\frac{r}{2}} 1$$

$$= \begin{cases} 1 & (r \text{ gerade}) \\ 0 & (r \text{ ungerade}) \end{cases} = \sum_{0\le i\le r} \chi_D(p^i) ,$$

falls $(\frac{D}{p}) = -1$, und

$$R(p^r) = \sum_{0\le s<\frac{r-1}{2}} 0 + \sum_{\frac{r-1}{2}\le s\le\frac{r}{2}} 1$$

$$= 1 = \sum_{0\le i\le r} \chi_D(p^i) ,$$

falls $p|D$. Somit ist (25) für $n = p^r$, p ungerade, in allen Fällen bewiesen. Den Beweis für $n = 2^r$, der ähnlich ist, überlassen wir dem Leser.

KOROLLAR: *Seien* D *und* χ_D *wie im Satz. Dann ist der Mittelwert der Gesamtdarstellungsanzahlen* $R(n)$ *gleich dem Wert der L-Reihe* $L(s,\chi_D)$ *an der Stelle* $s = 1$:

$$\lim_{N\to\infty} \left(\frac{1}{N} \sum_{n=1}^{N} R(n)\right) = L(1,\chi_D) . \tag{31}$$

Beweis: Nach (25) ist

$$\sum_{n=1}^{N} R(n) = \sum_{n\le N} \sum_{m|n} \chi_D(m)$$

$$= \sum_{km\le N} \chi_D(m)$$

$$= \sum_{m<\sqrt{N}} \chi_D(m) \cdot \sum_{k\le N/m} 1 + \sum_{k\le\sqrt{N}} \sum_{\sqrt{N}\le m\le\frac{N}{k}} \chi_D(m) .$$

(In der zweiten Summe, nämlich über die $m \ge \sqrt{N}$, ist wegen $km \le N$ automatisch $k \le \sqrt{N}$.) Es ist aber

$$\sum_{k\le N/m} 1 = [\frac{N}{m}] = \frac{N}{m} + O(1)$$

und

$$\sum_{\sqrt{N}\le m\le\frac{N}{k}} \chi_D(m) = O(1)$$

(da in jedem Intervall $(r-1)|D| < m \le r|D|$ die Summe von $\chi_D(m)$ wegen Satz 2, §5, verschwindet und die beiden Endintervalle

$\sqrt{N} \le m \le \left[\frac{\sqrt{N}}{|D|} + 1\right]|D|$ und $\left[\frac{N}{k|D|}\right]|D| < m \le \frac{N}{k}$ beschränkte Länge haben). Somit ist

$$\sum_{n\le N} R(n) = \sum_{m<\sqrt{N}} \chi_D(m)\cdot\left(\frac{N}{m} + O(1)\right) + \sum_{k\le\sqrt{N}} O(1)$$

$$= N \cdot \sum_{m=1}^{[\sqrt{N}]} \frac{\chi_D(m)}{m} + O(\sqrt{N}) ,$$

woraus die Behauptung folgt.

SATZ 4: *Sei* f *eine primitive, für* D < 0 *auch positiv definite, binäre quadratische Form der Diskriminante* D. *Dann wird der Mittelwert der Darstellungszahlen* R(n,f) *gegeben durch*

$$\lim_{N\to\infty} \frac{1}{N}\left(\sum_{n=1}^{N} R(n,f)\right) = \begin{cases} \frac{2\pi}{w\sqrt{|D|}} , & \text{falls } D < 0 , \\ \frac{\log \varepsilon_0}{\sqrt{D}} , & \text{falls } D > 0 , \end{cases} \tag{32}$$

wo w *die durch (20) angegebene Ordnung von* U_f *und* ε_0 *die Grundeinheit von* f *bezeichnen.*

Beweis: Dieser Satz wird auf geometrische Weise bewiesen. Sei zunächst D < 0. Weil $|U_f| = w < \infty$ ist und U_f auf $\mathbb{Z}^2 - 0$ ohne Fixpunkte operiert, sind jeweils genau w Lösungen von (15) zueinander äquivalent, also die Anzahl R(n,f) der inäquivalenten Lösungen gleich $\frac{1}{w}$ mal die Anzahl sämtlicher Lösungen:

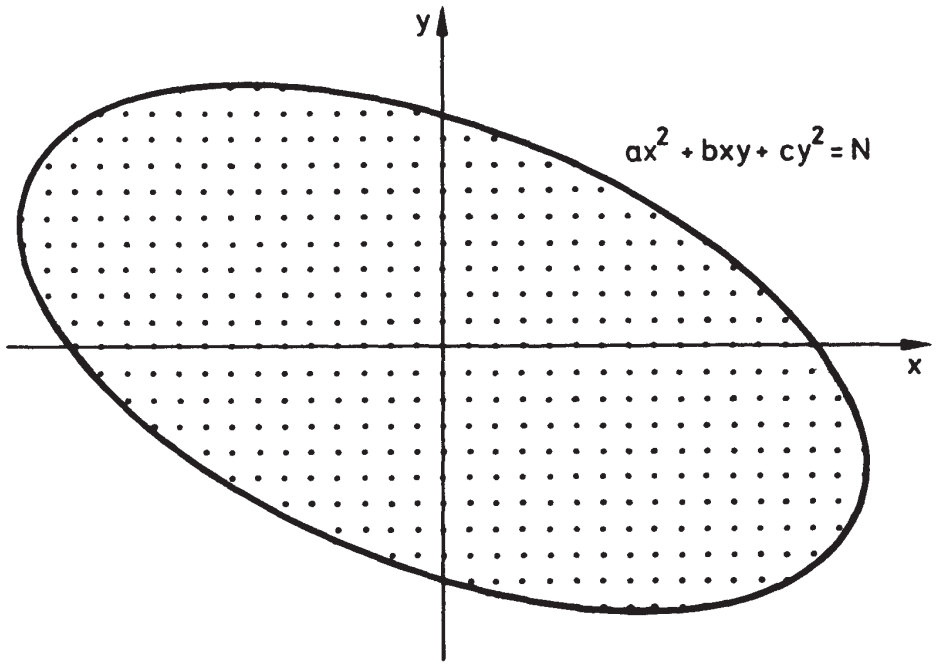
$$R(n,f) = \frac{1}{w}\#\{(x,y) \in \mathbb{Z}^2 \mid ax^2 + bxy + cy^2 = n\} . \tag{33}$$

Somit ist

$$\sum_{n=1}^{N} R(n,f) = \frac{1}{w}\#\{(x,y) \in \mathbb{Z}^2 \mid ax^2 + bxy + cy^2 \le N\} .$$

Die Ungleichung $ax^2 + bxy + cy^2 \le N$ beschreibt das Innere einer Ellipse (s. Bild). Dieses Gebiet hat den Flächeninhalt $\frac{2\pi N}{\sqrt{|D|}}$ (Aufgabe 6). Für N groß ist die Anzahl der Gitterpunkte in diesem Gebiet asymptotisch gleich dem Flächeninhalt (im Bild ist z.B. a = 2, b = 3, c = 5, N = 400, Anzahl der Gitterpunkte = 457, $\frac{2\pi N}{\sqrt{|D|}} = 451{,}4$), also

$$\lim_{N\to\infty} \frac{1}{N}\#\{(x,y) \in \mathbb{Z}^2 \mid ax^2 + bxy + cy^2 \le N\} = \frac{2\pi}{\sqrt{|D|}}.$$



Für $D > 0$ ist U_f unendlich, das Argument also anders. Falls (x',y') eine Lösung von (15) ist, die aus (x,y) durch Anwendung der Substitution (4) entsteht, wobei $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ ein Automorphismus von f ist, der unter (23) der Zahl ε entspricht, so ist

$$x' + \frac{b - \sqrt{D}}{2a} y' = \varepsilon(x + \frac{b - \sqrt{D}}{2a} y) ,$$

wie man leicht ausrechnet. Mit den Abkürzungen

$$\theta = \frac{-b + \sqrt{D}}{2a} , \quad \theta' = \frac{-b - \sqrt{D}}{2a}$$

(so daß $ax^2 + bxy + cy^2 = a(x - \theta y)(x - \theta' y)$ gilt) folgt also

$$x' - \theta y' = \varepsilon(x - \theta y) , \; x' - \theta' y' = \varepsilon'(x - \theta' y) ,$$

$$\frac{x'-\theta'y'}{x'-\theta y'} = \varepsilon^{-2} \frac{x-\theta' y}{x-\theta y} .$$

Da jedes ε die Gestalt $\pm\varepsilon_0^n$ hat, können wir genau eine zu (x,y) äquivalente Lösung (x',y') finden, die die Bedingungen

$$x' - \theta y' > 0 , \; 1 < \frac{x'-\theta'y'}{x'-\theta y'} \leq \varepsilon_0^2$$

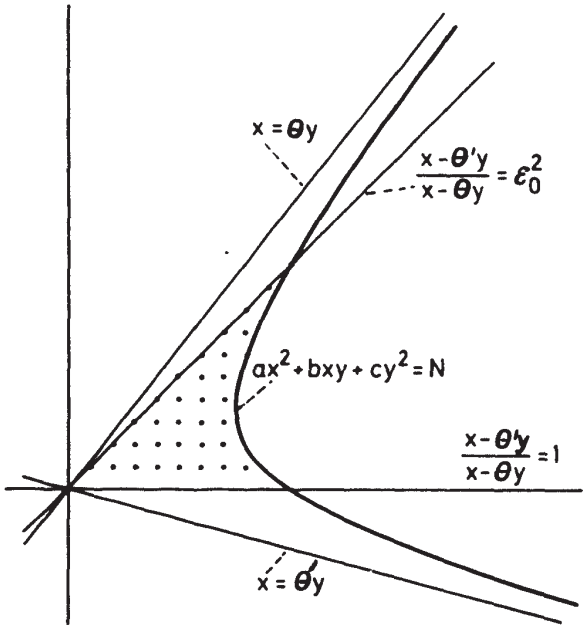
erfüllt. Das Analogon zu (33) für indefinite Formen ist also

$$R(n,f) = \#\{(x,y) \in \mathbb{Z}^2 \mid ax^2 + bxy + cy^2 = n,$$
$$x - \theta y > 0,\ 1 < \frac{x-\theta' y}{x-\theta y} \le \varepsilon_0^2\}\ .$$

Es folgt dann genau wie im Falle $D < 0$, daß der Limes in (32) gleich

$$\lim_{N\to\infty} \frac{1}{N} \cdot \text{Flächeninhalt von } \{(x,y) \in \mathbb{R}^2 \mid ax^2 + bxy + cy^2 \le N,$$
$$x - \theta y > 0,\ 1 < \frac{x-\theta' y}{x-\theta y} \le \varepsilon_0^2\}$$

ist. Die Ungleichungen beschreiben einen Sektor einer Hyperbel (s. Bild, wo $a = 1$, $b = 3$, $c = -3$, $N = 100$, $\varepsilon_0 = \frac{5+\sqrt{21}}{2}$), dessen Flächen-



inhalt gleich $\frac{\log \varepsilon_0}{\sqrt{D}} N$ ist (Aufgabe 7). Hieraus folgt die Behauptung des Satzes wie im Fall $D < 0$. Die Existenz der Grundeinheit folgt ebenfalls: wäre nämlich $U_f = \{\pm 1\}$, so wäre im Widerspruch zu der Existenz des Mittelwertes von $R(n)$ der Mittelwert von $R(n,f)$ unendlich, da das Gebiet zwischen der Hyperbel $ax^2 + bxy + cy^2 = N$ und ihren Asymptoten unendlichen Flächeninhalt hat.

Aus den Tatsachen, daß $R(n)$ den endlichen Mittelwert $L(1,\chi_D)$ hat und daß der Mittelwert von $R(n,f)$ positiv und nur von der Diskriminante abhängig ist, erhalten wir neue Beweise für die Endlichkeit der Klassenzahl und für das Nichtverschwinden von $L(1,\chi_D)$. Aus Satz 4 und dem Korollar zu Satz 3 erhalten wir (mindestens für Fundamentaldiskriminanten; für den allgemeinen Fall s. Aufgabe 8) das erste Haupt-

ergebnis Dirichlets, nämlich eine Beziehung zwischen $h(D)$ und $L(1,\chi_D)$:

SATZ 5: *Sei* D *eine Diskriminante. Dann ist*

$$h(D) = \begin{cases} \frac{w\sqrt{|D|}}{2\pi} L(1,\chi_D), & \textit{falls } D < 0 , \\ \frac{\sqrt{D}}{\log \varepsilon_0} L(1,\chi_D), & \textit{falls } D > 0 . \end{cases} \tag{34}$$

Im nächsten Paragraphen werden wir $L(1,\chi_D)$ berechnen und somit die endgültige Klassenzahlformel erhalten.

Aufgaben:

1. Man zeige, daß es genau m Äquivalenzklassen von quadratischen Formen (bzw. $\phi(m)$ Äquivalenzklassen von primitiven quadratischen Formen) der Diskriminante m^2, $m > 0$ gibt. Wie ist die Klassifikation der Formen der Diskriminante 0? Wie groß ist die Automorphismengruppe einer Form, deren Diskriminante eine Quadratzahl bzw. gleich Null ist?

2. Was sind die Automorphismen der Formen $x^2 + y^2$, $x^2 + xy + y^2$, $2x^2 + 3xy + y^2$, $x^2 - 5y^2$, $2x^2 + 6xy + 3y^2$?

3. Wieviele Darstellungen als Summe von zwei Quadraten hat eine ungerade Zahl n? (Zunächst Primzahlen betrachten; man braucht $h(-4) = 1$.) Vgl. das letzte Beispiel in §2. Wie lautet das Ergebnis für n gerade?

4. Unter Benutzung von $h(5) = 1$ zeige man, daß die einzigen Lösungen von

$$t^2 - 5u^2 = 4$$

durch $u = \pm F_{2n}$, $t = \pm(F_{2n-1} + F_{2n+1})$ gegeben sind, wo F_n die n-te Fibonacci-Zahl bezeichnet ($F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$).

5. Man zeige, daß für $D > 0$ die Klassenzahlen im engeren und im weiteren Sinne durch $h_0(D) = h(D)$ oder $h_0(D) = \frac{1}{2} h(D)$ verknüpft sind, je nachdem, ob die Gleichung $t^2 - Du^2 = -4$ eine ganzzahlige Lösung hat oder nicht.

6. Man verifiziere die im Beweis von Satz 4 benutzten Beziehungen

$$\iint\limits_{ax^2+bxy+cy^2\leq N} dx\,dy = \frac{2\pi N}{\sqrt{4ac-b^2}} \qquad (4ac > b^2,\ a > 0)\ ,$$

$$\iint\limits_{\substack{x,y\geq 0 \\ y\leq x(\varepsilon_0^2-1)/(\varepsilon_0^2\theta-\theta') \\ ax^2+bxy+cy^2\leq N}} dx\,dy = \frac{\log \varepsilon_0}{\sqrt{b^2-4ac}}\, N$$

$(b^2 - 4ac > 0,\ \varepsilon_0$ und θ, θ' wie im Text).

7. Man berechne $\sum\limits_{n=1}^{\infty} \frac{1}{9n^2-1}$, $\sum\limits_{n=1}^{\infty} \frac{1}{16n^2-1}$, $\sum\limits_{n=1}^{\infty} \frac{n}{(25n^2-1)(25n^2-4)}$.

8. Sei D ($\neq 0$ und $\equiv 0$ oder $1 \pmod 4$) eine allgemeine Diskriminante; D läßt sich dann eindeutig als $D_0 r^2$ schreiben mit $r \in \mathbb{N}$ und D_0 eine Fundamentaldiskriminante. Sei

$$\chi_D(m) = \begin{cases} \chi_{D_0}(m) & \text{, falls } (m,r) = 1 \\ 0 & \text{sonst} \end{cases}$$

der von χ_{D_0} induzierte Charakter. Man zeige:

a) Die Aussage von Satz 3 bleibt für zu r teilerfremde Zahlen richtig, d.h.

$$R_D(n) = \sum_{m\mid n} \chi_D(m)\, m \qquad \left(= \sum_{m\mid n} \chi_{D_0}(m)\, m\right) \quad \text{für } (n,r) = 1\ .$$

(Es ist hierbei gleichgültig, ob man die Darstellungen durch alle oder nur durch primitive Formen betrachtet, da eine zu r teilerfremde Zahl nicht durch eine imprimitive Form der Diskriminante D dargestellt werden kann.)

b) Das Korollar zu Satz 3 bleibt richtig, wenn man den Mittelwert nur über die n mit $(n,r) = 1$ bildet, d.h.

$$\lim_{N\to\infty} \left(\sum_{\substack{n=1 \\ (n,r)=1}}^{N} R_D(n) \Big/ \frac{\phi(r)}{r} N \right) = L(1,\chi_D)\ .$$

Hinweis: Im Beweis des Korollars muß man $(k,r) = 1$, aber nicht $(m,r) = 1$ zu den Summationsbedingungen hinzunehmen, da $\chi_D(m)$ für $(m,r) > 1$ sowieso verschwindet. Es gilt außerdem

$$\sum_{\substack{k\leq \frac{N}{m} \\ (k,r)=1}} 1 = \frac{\phi(r)}{r}\,\frac{N}{m} + O(1)\ .$$

c) Satz 4 bleibt ebenfalls richtig, wenn man den Mittelwert über die zu r teilerfremden Zahlen bildet, weil in jedem großen Gebiet der Ebene die Dichte der Zahlenpaare (x,y) mit $(f(x,y),r) = 1$ gleich $\frac{\phi(r)}{r}$ ist.

Hinweis: Für $p|r$ und $f(x,y) = ax^2 + bxy + cy^2$ eine primitive Form der Diskriminante D können a und c nicht beide durch p teilbar sein; ist etwa a zu p teilerfremd und $p \neq 2$, so folgt aus $4af(x,y) \equiv (2ax+by)^2 \pmod{p}$, daß

$$\#\{(x,y) \bmod p \,\big|\, p \nmid f(x,y)\} = p(p-1) .$$

d) Formel (34) (Satz 5) bleibt für Nichtfundamentaldiskriminanten richtig. Folglich sind die Klassenzahlen von $D = D_0 r^2$ und D_0 durch die Relation

$$h(D) = \frac{\gamma_{D_0}(r)}{\nu_r} h(D_0)$$

verknüpft. Hierbei ist

$$\gamma_{D_0}(r) = r \prod_{p|r} \left(1 - \frac{\chi_{D_0}(p)}{p}\right)$$

und ν_r der Index von U_D in U_{D_0} ($U_D = \{(t,u) \mid t^2 - Du^2 = 4\}$ mit dem Multiplikationsgesetz (19)), also $\nu_r = 1$ für $D < 0$ (außer im Falle $D_0 = -3$ bzw. -4 und $r > 1$, wo $\nu_r = 3$ bzw. 2) und

$$\nu_r = \min \{n \,|\, n > 0,\ u_n \equiv 0 \pmod{r}\}$$

für $D > 0$, wobei $\frac{t_n + u_n\sqrt{D_0}}{2} = \left(\frac{t_0 + u_0\sqrt{D_0}}{2}\right)^n$ mit (t_0,u_0) = kleinste positive Lösung der Pellschen Gleichung (1).

Bemerkung: Teil a) der Aufgabe gibt den Wert von $R_D(n)$ für $(n,r) = 1$ an. Das allgemeine Ergebnis, das sich ebenfalls aus (27) ableiten läßt, lautet wie folgt: Ist (r^2,n) kein Quadrat, so ist $R_D(n) = 0$. Ist $(r^2,n) = s^2$, also $n = n's^2$ und $D = D's^2$ mit $(n', \frac{D'}{D_0}) = 1$, so ist $R_D(n) = \gamma_{D'}(s) \cdot \sum_{m|n'} \chi_{D'}(m)$ (siehe etwa F. Hirzebruch, D. Zagier, *Invent. math. 36* (1976), S. 69-70, Proposition 2).

§9 Die Berechnung von $L(1,\chi)$ und die Klassenzahlformeln

Wir haben in §8 gesehen, wie man die Bestimmung der Klassenzahl binärer quadratischer Formen auf die Berechnung von $L(1,\chi)$ für reelle Charaktere $\chi = \chi_D$ zurückführen kann. In diesem Paragraphen werden wir $L(1,\chi)$ für beliebige Dirichletsche Charaktere $\chi \neq \chi_0$ berechnen. Wir haben schon bewiesen, daß dieser Wert endlich und von Null verschieden ist.

Sei also χ ein von dem Hauptcharakter verschiedener Dirichletscher Charakter. Wir setzen voraus, daß χ primitiv ist. (Wenn nämlich χ von einem Charakter χ_1 induziert wird, gibt es eine einfache Beziehung zwischen $L(1,\chi)$ und $L(1,\chi_1)$, da die L-Reihen $L(s,\chi)$ und $L(s,\chi_1)$ sich nur in endlich vielen Faktoren der Euler-Produkte unterscheiden.) Um $L(1,\chi)$ zu berechnen, machen wir Gebrauch von der *Gaußschen Summe*

$$(1) \qquad G = \sum_{n=1}^{N} \chi(n)\, e^{2\pi i n/N} .$$

Die Eigenschaften von G, die wir brauchen, sind in dem folgenden Hilfssatz zusammengestellt.

HILFSSATZ 1: *Sei* χ *ein primitiver Dirichletscher Charakter* (mod N) *und* G *durch (1) definiert. Dann gilt*

a) $$\sum_{n=1}^{N} \chi(n)\, e^{2\pi i k n/N} = \overline{\chi(k)}G \quad \textit{für alle} \quad k \in \mathbb{Z},$$

b) $$|G| = \sqrt{N} .$$

Beweis: a) ist leicht, falls $(k,N) = 1$, denn in diesem Fall ist

$$\sum_{n (\mathrm{mod}\ N)} \chi(n)\, e^{2\pi i n k/N} = \sum_{n (\mathrm{mod}\ N)} \chi(nk^{-1}) e^{2\pi i n/N}$$

$$= \sum_{n (\mathrm{mod}\ N)} \overline{\chi(k)}\, \chi(n)\, e^{2\pi i n/N}$$

$$= \overline{\chi(k)}G ,$$

wobei k^{-1} eine Zahl mit $k \cdot k^{-1} \equiv 1 \pmod N$ bezeichnet. Sei jetzt $(k,N) = d > 1$; dann ist $\chi(k) = 0$ und wir müssen zeigen, daß $\sum \chi(n)\, e^{2\pi i k n/N}$ auch 0 ist. Mit $k_1 = k/d$, $N_1 = N/d$ ist

$$\sum_{n (\mathrm{mod}\ N)} \chi(n)\, e^{2\pi i n k/N} = \sum_{n (\mathrm{mod}\ N)} \chi(n)\, e^{2\pi i n k_1/N_1}$$