ACTA ARITHMETICA
XXXIV (1977)

# Darstellungen durch definite ternäre quadratische Formen

von

MEINHARD PETERS (Münster)

**0. Einleitung und Bezeichnungen.** Diese Arbeit ist ein Beitrag zut Lösung der folgenden Frage: Welche ganzen rationalen Zahlen stellr eine ganzzahlige quadratische Form $f$ in $n \geqslant 3$ Variablen dar? Offenbar notwendig für die Darstellbarkeit einer ganzen Zahl $a$ über dem Ring $\boldsymbol{Z}$ der ganzen rationalen Zahlen ist die Darstellbarkeit von $a$ über den Ringen $\boldsymbol{Z}_p$ der ganzen $p$-adischen Zahlen, was auf Kongruenzbedingungen hinausläuft; diese finden sich z. B. in [11], [23]. Andererseits gibt es zu jeder Zahl $a \in \boldsymbol{Z}$, die über $\boldsymbol{Z}_p$ für alle Primstellen $p$ (einschließlich $\infty$) dargestellt wird, eine quadratische Form $f'$ im Geschlecht von $f$, welche $a$ über $\boldsymbol{Z}$ darstellt (s. z. B. [24], 102 : 5). Ist $a$ darstellbar über $\boldsymbol{Z}_p$ für alle Primstellen $p$, so sagen wir im folgenden, daß $a$ lokal überall darstellbar ist; Darstellbarkeit über $\boldsymbol{Z}$ wird auch globale Darstellbarkeit genannt.

Bei indefiniten quadratischen Formen in $n \geqslant 4$ Variablen sind die lokal überall darstellbaren Zahlen auch global darstellbar; schärfer gilt sogar, daß die Darstellungsmaße von $a$ ($\neq 0$) für alle quadratischen Formen im Geschlecht von $f$ dieselben sind ([32], [5], [17]). Dasselbe gilt für indefinite quadratische Formen in 3 Variablen, wenn man endlich viele genau angebbare Quadratklassen für $a$ ausnimmt ([13], [17]).

Für definite quadratische Formen gilt ein solches Lokal-Global-Prinzip nur mit gewissen Einschränkungen: Für $n \geqslant 5$ sind die lokal überall darstellbaren Zahlen bis auf endlich viele Ausnahmen auch global darstellbar, und für $n = 4$ sind die lokal überall *primitiv* darstellbaren Zahlen bis auf endlich viele Ausnahmen auch global darstellbar ([34], [14], [26], [6], [18] § 26), sogar global primitiv darstellbar bis auf endlich viele Ausnahmen (s. [20], p. 104, Theorem 4, vgl. auch [36], Theorem 76).

Im folgenden wird als Hauptsatz gezeigt, daß bei definitem $f$ für $n = 3$ die lokal überall durch $f$ primitiv darstellbaren ganzen Zahlen $a$ global durch $f$ primitiv darstellbar sind, wenn man folgende $a$ ausnimmt: Es werden

1) endlich viele Zahlen ausgenommen, und

2) im Fall, daß das Geschlecht von $f$ mehrere Spinorgeschlechter enthält, werden zusätzlich endlich viele Quadratklassen für $a$ ausgenommen. (Diese Quadratklassen gehören zu Teilern der Determinante von $f$.)

(Die Zahlen aus 1) sind i.a. effektiv nicht angebbar, die Quadratklassen aus 2) hingegen werden in (1.3) (§ 1) charakterisiert.) Der Hauptsatz wird jedoch nur bewiesen unter der Annahme der sog. verallgemeinerten Riemannschen Vermutung, welche besagt, daß alle Nullstellen im Streifen $0<\sigma<1$ von Dirichletschen $L$-Reihen auf der Geraden $\sigma=\frac{1}{2}$ liegen; tatsächlich wird nur eine schwächere Hypothese verwendet, die in § 1 genau formuliert ist ("Riemann-Hypothese").

Der Beweis des Hauptsatzes benutzt einerseits den starken Approximationssatz von M. Kneser (s. z.B. [15], § 2, [16], § 2, [18], Kap. VIII), andererseits die Methoden von Linnik und Malyshev zur Behandlung von ternären quadratischen Formen (s. z.B. [19], [20], [21]).

Linnik und Malyshev beweisen auch den Hauptsatz im Spezialfall von quadratischen Formen mit ungeraden und zueinander primen Elementarteilern (Ordnungsinvarianten) — in diesem Fall enthält das Geschlecht der Form nur ein Spinorgeschlecht.

Der Hauptsatz bestätigt — unter Annahme der verallgemeinerten Riemannschen Vermutung — eine Vermutung von Pall und Ross ([26], p. 60) und eine Vermutung von Watson ([35], p. 110); beide Vermutungen besagen im wesentlichen, daß eine ternäre quadratische Form nur endlich viele quadratfreie "Ausnahmen" besitzt, wobei mit "Ausnahme" eine lokal überall, aber nicht global darstellbare Zahl bezeichnet wird.

Daß, wie oben gesagt, eine effektive Bestimmung der Ausnahmen einer ternären Form mit den hier verwendeten Methoden nicht möglich ist, liegt u.a. daran, daß der Satz von Siegel über die Klassenzahl quadratischer Zahlkörper ([31]) bei Abschätzungen benutzt wird. So folgt z. B. aus dem Hauptsatz, daß die quadratische Form $f=x_1^2+x_2^2+10x_3^2$ nur endlich viele Ausnahmen hat (unter Annahme der Riemann-Hypothese für $f$), aber ob die bekannten 18 Ausnahmen dieser Form ([10]), die bis auf zwei schon von Ramanujan angegeben wurden ([28], p. 172), sämtliche sind, bleibt unentschieden. Bei quadratischen Formen in 4 oder mehr Variablen lassen sich die Ausnahmen dagegen effektiv bestimmen (s. [8], [2], [37]).

Die Arbeit ist folgendermaßen aufgebaut: In § 1 werden die Resultate genau formuliert. In § 2 wird die Frage der Darstellbarkeit einer Zahl durch das Geschlecht der zugrundeliegenden quadratischen Form im wesentlichen auf die Darstellbarkeit durch das Spinorgeschlecht reduziert. In § 3 wird weiter reduziert auf Darstellungen mit festem Primzahlpotenznenner. In § 4 werden die für die weiteren Beweise grundlegenden Zusammenhänge zwischen ternären quadratischen Formen und Quaternionenordnungen angegeben. In § 5 werden die Resultate dieser Arbeit bewiesen bis auf ein Lemma, das die in diesem Rahmen relevanten Ergebnisse der Methode von Linnik–Malyshev zur Untersuchung ternärer quadratischer Formen zusammenfaßt. Der Beweis dieses Lemmas wird in § 6 nachgetragen. In § 7 wird ein Ausblick auf weitere Probleme in diesem Bereich gemacht.



Ich bedanke mich sehr bei Herrn M. Kneser und Herrn W. Scharlau für anregende Gespräche und die Förderung dieser Arbeit, und bei der Deutschen Forschungsgemeinschaft für die Gewährung eines Habilitandenstipendiums. Herrn A. V. Malyshev danke ich sehr für kritische Bemerkungen.

**Bezeichnungen.** Es bezeichnet

$\boldsymbol{N}$ die natürlichen Zahlen,

$\boldsymbol{Z}$ den Ring der ganzen rationalen Zahlen,

$\boldsymbol{Q}$ den Körper der rationalen Zahlen,

$\boldsymbol{R}$ den Körper der reellen Zahlen,

$V$ einen 3-dimensionalen $\boldsymbol{Q}$-Vektorraum mit einer nicht-ausgearteten positiv-definiten quadratischen Form $f$ und zugehöriger Bilinearform $b$, wobei
$$2f(x)=b(x,x) \quad \text{für} \quad x\in V,$$

$E$ ein $\boldsymbol{Z}$-Gitter in $V$ mit $f(E)\subseteq \boldsymbol{Z}$,

$e_1, e_2, e_3$ eine Basis von $E$,

$d:=d(E):=|b(e_i,e_j)|_{i,j=1,2,3}$ die Determinante von $E$,

$d':=d'(E):=\frac{1}{2}d(E)$,

$n(E)$ die Norm von $E$ (den größten gemeinsamen Teiler der $f(x)$ mit $x\in E$)

$d_2:=d_2(E)$ den größten gemeinsamen Teiler der Unterdeterminanten 2. Ordnung der Matrix $(b(e_i,e_j))_{i,j=1,2,3}$,

$D':=D'(E):=\dfrac{d(E)}{d_2(E)}$,

$D:=D(E):=\dfrac{2d(E)}{d_2(E)^2}$,

} für ein Gitter $E$ mit $n(E)=1$

$p$ eine Primstelle von $\boldsymbol{Q}$ (eine endliche Primstelle oder $\infty$).

Durch den Index $p$ werden jeweils die Komplettierungen an der Stelle $p$ bezeichnet, z.B. ist

$\boldsymbol{Q}_p$ der Körper der $p$-adischen Zahlen,

$\boldsymbol{Z}_p$ der Ring der ganzen $p$-adischen Zahlen,

$V_p := V \otimes_{\mathbf{Q}} \mathbf{Q}_p$
$E_p := E \otimes_{\mathbf{Z}} \mathbf{Z}_p$ } für eine endliche Primstelle $p$,

$V_\infty := E_\infty := E \otimes \mathbf{R}$.

Es bezeichnet

$f(E)$ die von $E$ dargestellten Zahlen,

$f^*(E)$ die von $E$ primitiv dargestellten Zahlen (genauer s. § 1),

$\bar{f}(E) := \{a \in \mathbf{Z} \mid a \in f(E_p)$ für alle Primstellen $p\}$,

$\bar{f}^*(E) := \{a \in \mathbf{Z} \mid a \in f^*(E_p)$ für alle Primstellen $p\}$,

$\mathrm{gen}(E)$ das Geschlecht von $E$,
$\mathrm{spn}(E)$ das Spinorgeschlecht von $E$, } (Definition s. § 1)

$O(V)$ die orthogonale Gruppe von $V$ bezüglich $f$,

$O(E)$ die Untergruppe der Einheiten von $E$,

$O^+(V)$ die spezielle orthogonale Gruppe von $V$,

$O(V, x)$ für ein $x \in V$ die Fixgruppe von $x$ in $O(V)$,

$O(E, x) := O(V, x) \cap O(E)$,

$O_A(V, x)$ das eingeschränkte direkte Produkt der Gruppen $O(V$ bezüglich der Untergruppen $O(E_p, x)$,

$\theta$ die Spinornorm,

$O'(E)$ diejenige Untergruppe von $O^+(E)$, deren Elemente Spinornorm 1 haben,

$\mathrm{ind}\, V$ den Wittindex von $V$,

$\mathfrak{P}$ eine Fortsetzung von $p$ in einem algebraischen Zahlkörper $K$,

$N_{K_\mathfrak{P} \mathbf{Q}_p}$ die Norm der Erweiterung $K_\mathfrak{P}/\mathbf{Q}_p$

$K_\mathfrak{P}^\times$ die multiplikative Gruppe der von Null verschiedenen Elemente von $K_\mathfrak{P}$,

$\bar{A}(a, E)$ für ein $a \in \mathbf{Z}$ das Darstellungsmaß von $a$ durch das Geschlecht von $E$ (Definition s. § 2),

$\bar{A}^*(a, E)$ das entsprechende primitive Darstellungsmaß,

$h(n)$ für ein $n \in \mathbf{N}$ die Anzahl der eigentlichen Klassen positivdefiniter primitiver binärer quadratischer Formen der Determinante $n$,

$C_0(V)$ die 2. Cliffordalgebra von $V$,

$C_0(E)$ die 2. Cliffordalgebra von $E$ (in der Terminologie von Eichler ([7], § 14)),

Sp die Spur
$N$ die Norm
$-$ die Konjugation } in einer Quaternionenalgebra.

Zur Definition von $\mathfrak{O}$, $\mathfrak{B}$ s. § 4.



**1. Resultate.** Die Terminologie lehnt sich an [7], [18] an: Sei $V$ ein dreidimensionaler $\mathbf{Q}$-Vektorraum mit einer nicht-ausgearteten quadratischen Form $f$ und zugehöriger Bilinearform $b$, wobei $2f(x) = b(x, x)$ für $x \in V$; $E$ sei ein $\mathbf{Z}$-Gitter in $V$, d.h. ein $\mathbf{Z}$-Modul vom Rang 3, mit $f(E) \subseteq \mathbf{Z}$; wenn $e_1, e_2, e_3$ eine Basis von $E$ ist, so heißt $d = d(E) = |b(e_i, e_j)|$ die Determinante von $E$. Ist $a = f(x_1, x_2, x_3)$ mit $(x_1, x_2, x_3) \in E$, so sagt man, $a$ wird dargestellt von $E$ oder durch $f$. Sind bei einer derartigen Darstellung $x_1, x_2, x_3$ teilerfremd, so heißt die Darstellung primitiv; besitzt $a$ eine primitive Darstellung, so heißt $a$ primitiv darstellbar. Es bezeichnen $f(E)$ bzw. $f^*(E)$ die Menge aller von $E$ darstellbaren bzw. primitiv darstellbaren Zahlen. Analog wird $f(E_p)$ und $f^*(E_p)$ für endliche $p$ definiert, und es wird gesetzt: $f^*(E_\infty) = f(E_\infty)$. Die Mengen $\bar{f}(E)$ und $\bar{f}^*(E)$ der lokal überall darstellbaren bzw. lokal überall primitiv darstellbaren Zahlen sind folgende:

$$\bar{f}(E) := \{a \in \mathbf{Z} \mid a \in f(E_p) \text{ für alle Primstellen } p\},$$

$$\bar{f}^*(E) := \{a \in \mathbf{Z} \mid a \in f^*(E_p) \text{ für alle Primstellen } p\}.$$

Die Menge $\bar{f}(E) - f(E)$ soll die Menge der *Ausnahmen* von $E$, die Menge $\bar{f}^*(E) - f^*(E)$ soll die Menge der *Primitivausnahmen* von $E$ genannt werden.

Bemerkung. Man beachte, daß die Menge der Primitivausnahmen i.a. nicht in der Menge der Ausnahmen enthalten ist, z.B.: $E$ sei gegeben durch $f(x_1, x_2, x_3) = x_1^2 + 12x_2^2 + 36x_3^2$, dann ist $25 \in f(E)$, aber $25 \in \bar{f}^*(E) - f^*(E)$, wie aus ([12], Table II) ersichtlich.

Zwei $\mathbf{Z}$-Gitter $E, E'$ in den Räumen $V, V'$ liegen im gleichen Geschlecht ($\mathrm{gen}(E)$), wenn es für jede Primstelle $p$ eine Isometrie $u_p: V_p \to V'_p$ gibt mit $u_p E_p = E'_p$, im gleichen Spinorgeschlecht ($\mathrm{spn}(E)$), wenn es eine Isometrie $u: V \to V'$ und Automorphismen $v_p \in O'(E_p)$ mit $E'_p = u v_p E_p$ für alle Primstellen $p$ gibt. Hierbei ist $O'(E_p)$ diejenige Untergruppe der speziellen orthogonalen Gruppe $O^+(E_p)$, deren Elemente Spinornorm 1 haben. Der Wittindex von $V$ ist die Dimension des maximalen totalisotropen Teilraums von $V$ (Bezeichnung: $\mathrm{ind}\, V$). Bekanntlich ist (s. z.B. [24], 102 : 5, [36], Theorem 51):

$$\bar{f}(E) = \bigcup_{E' \in \mathrm{gen}(E)} f(E'), \quad \bar{f}^*(E) = \bigcup_{E' \in \mathrm{gen}(E)} f^*(E'),$$

somit sind die (Primitiv-)Ausnahmen einer Form $f$ diejenigen Zahlen, die zwar von $f$ nicht (primitiv) dargestellt werden, jedoch von einer Form aus dem Geschlecht von $f$ (primitiv) dargestellt werden.

Folgende schwache Form der verallgemeinerten Riemannschen Vermutung für Dirichletsche $L$-Reihen wird verwendet:

RIEMANN-HYPOTHESE. *Für alle hinreichend großen $a \in \bar{f}^*(E)$ besitzen die Dirichletschen L-Reihen*

$$L(s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad \chi(n) = \left(\frac{-2da}{n}\right) \quad (\mathrm{Re}\, s > 1)$$

*und ihre analytischen Fortsetzungen keine Nullstellen im Kreis*

$$|s-1| < \frac{(\ln\ln a)^2 \ln\ln\ln a}{\sqrt{\ln a}}.$$

Mit diesen Bezeichnungen lautet das Hauptresultat:

(1.1) HAUPTSATZ. *Sei $E$ ein positiv-definites ternäres Gitter der Determinante $d$ und es gelte die soeben formulierte Riemann-Hypothese für $E$. Dann gilt:*

(a) (i) *Falls das Geschlecht von $E$ nur ein Spinorgeschlecht enthält, ist die Menge der Primitivausnahmen von $E$ endlich.*

(ii) *Falls das Geschlecht von $E$ mehrere Spinorgeschlechter enthält, liegen die Primitivausnahmen von $E$ in endlich vielen Quadratklassen.*

(b) *Die Ausnahmen von $E$ liegen in endlich vielen Quadratklassen.*

Bemerkungen und Ergänzungen:

(1.2) Die endliche Menge der Primitivausnahmen aus (a) (i) ist (mit den hier verwendeten Methoden) nicht effektiv bestimmbar.

(1.3) Im Fall (a) (ii) tritt ebenfalls eine effektiv nicht bestimmbare endliche Menge von Primitivausnahmen auf. Zusätzlich können noch unendlich viele Primitivausnahmen auftreten, die in den durch die Teiler von $d$ bestimmten Quadratklassen liegen. Genauer ergibt sich beim Beweis (s. § 2), daß letztere Primitivausnahmen $a$ folgende Bedingung erfüllen müssen: Ist $d' = d/2$, $K = \boldsymbol{Q}(\sqrt{-d'a})$, so muß für alle endlichen Primstellen $p$ gelten:

$$(*) \qquad \theta\big(O^+(E_p)\big) \subseteq N_{K_{\mathfrak{P}}/\boldsymbol{Q}_p}(K_{\mathfrak{P}}^{\times}),$$

wobei $\mathfrak{P}$ eine Fortsetzung von $p$ in $K$ ist. Daß aus dieser Bedingung folgt, daß $a$ bis auf Quadrate ein Determinantenteiler ist, sieht man folgendermaßen: Für die nicht in der Determinante aufgehenden Primzahlen $p$ enthält $\theta\big(O^+(E_p)\big)$ bekanntlich alle Einheiten von $\boldsymbol{Q}_p$ (s. z.B. [24], 91 : 8). Damit die obige Inklusion für derartige $p$ erfüllt ist, müssen diese $p$ in $\boldsymbol{Q}(\sqrt{-d'a})$ unverzweigt sein, dürfen also $a$ nicht teilen.

(1.4) Um die Menge der Ausnahmen in (b) genauer zu beschreiben, definiert man zu jeder natürlichen Zahl $k$ die Menge

$$A_k := \{a \text{ Ausnahme} \mid p^{2k} \nmid a, \text{ falls ind } V_p = 0\}.$$



(Man beachte, daß ind $V_p = 0$ nur für $p \mid d$ gelten kann.) Es gilt dann: Falls das Geschlecht von $E$ nur ein Spinorgeschlecht enthält, sind alle $A_k$ endlich. Falls das Geschlecht von $E$ mehrere Spinorgeschlechter enthält, gehören zu den $A_k$ zusätzlich evtl. noch unendlich viele Zahlen, die wieder in den durch Bedingung (*) in (1.3) beschriebenen Quadratklassen liegen.

(1.5) Hat $E$ eine Ausnahme $a$, ist ind $V_p = 0$ und ist $E_p$ maximal, so sind auch alle $ap^{2k}$, $k = 0, 1, 2, \ldots$, Ausnahmen. Man erhält also mit einer Ausnahme eine unendliche „$p$-Serie" von Ausnahmen. Ist $E_p$ nicht maximal, ind $V_p = 0$ und $E'_p$ das $E_p$ umfassende maximale Gitter, so sei $E'$ definiert durch

$$(E')_q := E_q \text{ für } q \neq p, \quad (E')_p := E'_p.$$

Mit einer Ausnahme $a$ hat $E$ genau dann die $p$-Serie $ap^{2k}$, $k = 0, 1, 2, \ldots$, als Ausnahmen, wenn $E'$ ebenfalls die Ausnahme $a$ hat; andernfalls hat $E$ nur endlich viele Ausnahmen der Gestalt $ap^{2k}$.

(1.6) Eine Teilaussage des Hauptsatzes kann auch ohne Annahme der Riemann-Hypothese bewiesen werden: Sei ohne Einschränkung der Allgemeinheit $n(E) = 1$, und sei $D = D(E)$ wie in § 0 definiert. Sei $p$ fest gewählt mit $(p, 2D) = 1$ und ind $V_p > 0$. Beim Beweis des Hauptsatzes in § 5 ergibt sich dann: Die Riemann-Hypothese wird nicht benötigt, wenn man sich beschränkt auf die Betrachtung von Zahlen $a$ mit $\left(\frac{-Da}{p}\right) = 1$. Dies bedeutet fast keine Einschränkung in folgendem Fall: Es gibt ein $p \mid d$ mit $(p, 2D) = 1$ und für ein von $E$ dargestelltes $a$ ist die Bedingung $\left(\frac{-Da}{p}\right) = 1$ erfüllt; diese Bedingung ist dann nämlich auch bereits für alle von $E$ dargestellten $a$ mit $(a, p) = 1$ erfüllt, wie in der Terminologie der Geschlechtscharaktere von Eisenstein und Smith begründet worden ist (s. [33], vgl. auch [3], § 32). Insgesamt ergeben sich also für gewisse Geschlechter die Aussagen des Hauptsatzes auch ohne Annahme einer Riemann-Hypothese, wenn man sich auf Zahlen beschränkt, die prim zur Determinante sind.

(1.7) Linnik und Malyshev untersuchen ternäre quadratische Formen mit ungeraden, zueinander primen Ordnungsinvarianten (s. [20], Kap. V, [21], pp. 565–567). In diesem Fall enthält das Geschlecht der Form nur ein Spinorgeschlecht (z.B. nach dem Kriterium [18], (24.4)). Aus den Ergebnissen von Linnik und Malyshev läßt sich der Hauptsatz und (1.6) im genannten Spezialfall ablesen.

**2. Reduktion vom Geschlecht auf das Spinorgeschlecht.** Die Untersuchung indefiniter ternärer quadratischer Formen in [17] läßt sich auf definite Formen übertragen. Zunächst werden Darstellungsmaße mit der

in § 3 verwendeten Normierung definiert: Sei $E_i$ $(i = 1, \dots, g)$ ein Vertretersystem der Klassen des Geschlechts von $E$, sei $O(E_i)$ die Einheitengruppe von $E_i$, $|O(E_i)|$ deren Ordnung. Sei $A(a, E_i)$ die Anzahl der Vektoren der Länge $a$ im Gitter $E_i$, d.h. die Anzahl der Darstellungen von $a$ durch eine zu $E_i$ gehörige quadratische Form $f_i$. Sei

$$w_i := |O(E_i)|^{-1} / \sum_{j=1}^{g} |O(E_j)|^{-1}.$$

Dann ist

$$\bar{A}(a, E) := \sum_{i=1}^{g} w_i A(a, E_i)$$

die gemittelte Darstellungsanzahl von $a$ durch die Klassen des Geschlechts von $E$ oder das Darstellungsmaß von $a$ durch das Geschlecht von $E$. Die entsprechenden Anzahlen primitiver Darstellungen werden mit $A^*(a, E)$, $\bar{A}^*(a, E)$ bezeichnet, letztere werde auch das primitive Darstellungsmaß von $a$ durch das Geschlecht von $E$ genannt. Man lege nun ein Vertretersystem $E_i$ $(i = 1, \dots, s)$ der Klassen des Spinorgeschlechts von $E$ zugrunde. Dann definiert man analog zu oben das Darstellungsmaß bzw. primitive Darstellungsmaß von $a$ durch das Spinorgeschlecht von $E$. Für diese Darstellungsmaße gilt nun folgendes:

(2.1) Satz. *Sei $E$ ein positiv-definites ternäres $\mathbf{Z}$-Gitter mit quadratischer Form $f$ und der Determinante $d$.*

*Es sei $a \in \mathbf{Z}$ $(a \neq 0)$, $d' = d/2$, $K = \mathbf{Q}(\sqrt{-d'a})$ und $\mathfrak{P}$ eine Fortsetzung der endlichen Primstelle $p$ in $K$. Das Geschlecht von $E$ enthalte mindestens zwei Spinorgeschlechter, etwa $2^k$ $(k \geqslant 1)$. Dann gilt:*

(a) *Das Darstellungsmaß von $a$ durch die Spinorgeschlechter im Geschlecht von $E$ ist entweder für alle Spinorgeschlechter das gleiche, oder aber die $2^k$ Spinorgeschlechter lassen sich auf zwei "Halbgeschlechter" von je $2^{k-1}$ Spinorgeschlechtern verteilen derart, daß zwei Spinorgeschlechter aus demselben Halbgeschlecht das gleiche Darstellungsmaß liefern. Der letztere Fall kann nur dann eintreten, wenn für alle endlichen Primstellen $p$ gilt:*

$$\theta\big(O^+(E_p)\big) \subseteq N_{K_{\mathfrak{P}}/\mathbf{Q}_p}(K_{\mathfrak{P}}^{\times}). \tag{2.2}$$

(b) *Eine analoge Aussage gilt, wenn statt der Darstellungsmaße die primitiven Darstellungsmaße betrachtet werden.*

Der Beweis lehnt sich so genau an den Beweis von [17], Satz 2 an, daß auf eine Darstellung verzichtet werden kann.

Durch diesen Satz ist die Frage der Darstellbarkeit und der primitiven Darstellbarkeit einer Zahl $a$ vom Geschlecht der Form auf das Spinorgeschlecht zurückgeführt, abgesehen von gewissen $a$, die in der durch Bedingung (2.2) beschriebenen Menge liegen; diese $a$ liegen in endlich vielen Quadratklassen, wie in (1.3) bewiesen.



(2.3) Bemerkung. Wenn man die vom Geschlecht von $E$, aber nicht vom Spinorgeschlecht von $E$ dargestellten Zahlen die *Spinorausnahmen* von $E$ nennt, und analog für primitive Darstellbarkeit *Spinorprimitivausnahmen* definiert, so kann man durch Übertragung von [13], Satz 2, vom indefiniten auf den definiten Fall zeigen: Die Spinorausnahmen liegen in der Menge, die durch Bedingung (2.2) beschrieben wird mit der zusätzlichen Einschränkung:

Wenn $d'a = n_1 n_2^2$, $n_1$ quadratfrei, gesetzt wird, so folgt aus $(p, d) = 1$, $\left(\frac{-n_1}{p}\right) = -1$, daß $p \nmid n_2$.

Diese Einschränkung ist nicht richtig bei Spinorprimitivausnahmen, wie aus [36], Chap. 7, § 6 hervorgeht: Die Vereinigung der Mengen der Spinorprimitivausnahmen über alle Spinorgeschlechter eines Geschlechts wird dort als Menge der „exceptional integers" des Geschlechts bezeichnet; sie besteht nach [36], Theorem 75, im wesentlichen aus vollen Quadratklassen.

**3. Darstellungen mit festem Primzahlpotenznenner.** Zur Vorbereitung der Untersuchung der Anzahl von Darstellungen mit festem Primzahlpotenznenner wird das in § 2 definierte primitive Darstellungsmaß $\bar{A}^*(a, E)$ von $a$ durch das Geschlecht von $E$ folgendermaßen abgeschätzt:

(3.1) Satz. *Sei $E$ ein positiv-definites ternäres Gitter der Determinante $d$, und bezeichne $h(n)$ für ein natürliches $n$ die Anzahl der eigentlichen Klassen positiv-definiter primitiver binärer quadratischer Formen der Determinante $n$. Dann existieren (nur vom Geschlecht von $E$ abhängige) positive Konstanten $g_1, g_2$ derart, daß für alle $a \in \bar{f}^*(E)$ gilt:*

$$g_1 h(2da) < \bar{A}^*(a, E) < g_2 h(2da).$$

Beweis. Nach [36], Theorem 51, gibt es wegen $a \in \bar{f}^*(E)$ eine primitive Darstellung von $a$ durch ein $E' \in \mathrm{gen}(E)$; für die Aussage des Satzes ist die Annahme $E' = E$ keine Einschränkung. Es werden jetzt einige Begriffe aus [17] verwendet, allerdings eingeschränkt auf primitive Darstellungen: eine primitive Darstellung von $a$ durch $E$: $f(x) = a$, wird bezeichnet mit $(x, E)$. Primitive Darstellungen $(x, E)$, $(x', E')$ heißen äquivalent, wenn es ein $u \in O(V)$ gibt mit $ux = x'$, $uE = E'$, verwandt, wenn es zu jeder Primstelle $p$ ein $u_p \in O(V_p)$ gibt mit $u_p x = x'$, $u_p E_p = E'_p$. Äquivalente primitive Darstellungen bilden eine Klasse, verwandte primitive Darstellungen bilden ein Geschlecht von primitiven Darstellungen. Es bezeichne $O(V, x)$ die Fixgruppe von $x$ in $O(V)$, $O(E, x) := O(V, x) \cap O(E)$, $O_A(V, x)$ sei das eingeschränkte direkte Produkt der Gruppen $O(V_p, x)$ bezüglich der Untergruppen $O(E_p, x)$,

$$O_A(E) := \{u \in O_A(V) \mid uE = E\} \quad \text{und} \quad O_A(E, x) := O_A(E) \cap O_A(V, x).$$

Man sieht genau wie in [17], § 3: die Klassen primitiver Darstellungen des Geschlechts der primitiven Darstellung $(x, E)$ entsprechen umkehrbar eindeutig den zweiseitigen Restklassen $O(V,x)uO_A(E,x)$ mit $u \in O_A(V,x)$. Wenn statt der orthogonalen Gruppen $O$ überall die speziellen orthogonalen Gruppen $O^+$ zugrundegelegt werden, so übertragen sich die Aussagen auf die u.U. engere Einteilung; für die Anzahlen des Satzes ergibt das höchstens Änderungen um Faktoren 2, die keine Rolle spielen. Nun ist bekanntlich die Drehgruppe $O^+(V,x)$ im dreidimensionalen Raum $V$ um die von $x$ erzeugte Gerade $G$ isomorph zur Drehgruppe $O^+(G^\perp)$ des orthogonalen Komplements $G^\perp$ von $G$ in $V$, ebenso für die $p$-adischen Komplettierungen. Somit ist $O_A^+(V,x) \cong O_A^+(G^\perp)$. Man identifiziere $G$ mit der zu $x$ orthogonalen Hyperebene in $V$. Da $x$ primitiv ist, läßt es sich zu einer Basis von $E$ ergänzen, und $\hat{E} := E \cap G^\perp$ ist ein binäres Gitter im Raum $G^\perp$. Die Determinante von $E$ ist $2da/e^2$, wobei $e \mid (d, 2a)$. Die Formel von Dirichlet für das Verhältnis der Klassenzahl von Ordnungen in quadratischen Zahlkörpern zur Klassenzahl der zugehörigen Hauptordnung (s. z.B. [1], p. 270, Aufg. 20) zeigt, daß das Auftreten imprimitiver (mit gewissen Determinantenteilern) binärer Gitter nur für die Aussage des Satzes irrelevante Korrekturen hervorruft. Man kann also ohne Einschränkung der Allgemeinheit statt $\hat{E}$ auch $e\hat{E}$ betrachten. Ebenso wie $O_A^+(V,x)$ auf den Darstellungen $(x, E)$ operiert, so operiert $O_A^+(G^\perp)$ auf den binären Gittern $e\hat{E}$; hierbei wird das Geschlecht dieser binären quadratischen Formen durchlaufen. Wenn man die Anzahl der Klassen primitiver Darstellungen im Geschlecht einer Darstellung über alle Geschlechter von primitiven Darstellungen von $a$ durch ein Gitter im Geschlecht von $E$ summiert, summiert man entsprechend die Anzahlen der Klassen obiger binärer Gitter über gewisse Geschlechter binärer Gitter der Determinante $2da$. Der Quotient $q$ aus der Anzahl der Geschlechter primitiver binärer Formen der Determinante $2da$ und der Anzahl der betrachteten Darstellungsgeschlechter hängt nur von $E$ ab $-$ $q$ besteht aus gewissen Faktoren, die herrühren von den Primstellen $p$ mit $p \mid d$. Derartige nur von $E$ abhängige Faktoren interessieren aber für die Aussage des Satz (3.1) nicht. Aus diesen Überlegungen ergibt sich die Behauptung des Satzes.

(3.2) Bemerkung. Ähnliche Überlegungen finden sich in [7], p. 175, für die ternäre Einheitsform, für ternäre Formen mit gewissen Einschränkungen bei [11], Chap. 8. Man kann Satz (3.1) auch direkt unter Anwendung des Satzes von Siegel [30] durch Ausrechnung der $p$-adischen Darstellungsdichten beweisen.

(3.3) Korollar. *Es existiert ein* $g_3 = g_3(E) > 0$, *das nur von* $\mathrm{gen}(E)$ *abhängt, so daß gilt:*



(a) *Für jedes* $a \in \bar{f}^*(E)$ *gibt es ein* $E_i \in \mathrm{gen}(E)$ *mit*

$$A^*(a, E_i) > g_3 h(2da). \tag{3.4}$$

(b) *Für jedes* $a \in \bar{f}^*(E)$, *das nicht Bedingung* (2.2) *erfüllt, gibt es ein* $E_i \in \mathrm{spn}(E)$ *mit* (3.4).

Beweis. (a) folgt unmittelbar aus Satz (3.1), (b) gilt, da die primitiven Darstellungsmaße von $a$ durch die Spinorgeschlechter im Geschlecht von $E$ nach Satz (2.1) (b) alle gleich sind.

Sei jetzt eine Primzahl $p$ mit $\mathrm{ind}\, V_p > 0$ fest gewählt. Wenn das Geschlecht des Gitters $E$ nur ein Spinorgeschlecht enthält, also $\mathrm{gen}(E) = \mathrm{spn}(E)$, so existiert ein $t_0 \in \mathbf{N}$ mit $\bar{f}(p^{t_0}E) \subseteq f(E)$ nach dem starken Approximationssatz, angewandt auf arithmetisch indefinite Formen ([16], § 2, [18], (26.5)). Aus dem Beweis von [18], (26.5) erkennt man genauer:

(3.5) Lemma. *Zu einer Primzahl* $p$ *mit* $\mathrm{ind}\, V_p > 0$ *existiert ein* $t_0 \in \mathbf{N}$ *mit* $p^{t_0}E' \subseteq E$ *für alle* $E' \in \mathrm{spn}(E)$.

Im folgenden werden nur noch Zahlen $a$ betrachtet, die nicht Bedingung (2.2) erfüllen. Aus Korollar (3.3) (b) und Lemma (3.5) folgt dann:

$$A\left(a(p^{t_0})^2, E\right) > g_3 h(2da).$$

Wir betrachten jetzt weiterhin nur noch Zahlen $a$ mit $(a, p) = 1$. Da jede hier auftretende Darstellung von $a(p^{t_0})^2$ von einer primitiven Darstellung von $a(p^t)^2$ mit geeignetem $t$ ($0 \leqslant t \leqslant t_0$ und $t = t(a)$ von $a$ abhängig) herkommt, ergibt sich

$$A^*\left(a(p^t)^2, E\right) > g_4 h(2da) \tag{3.6}$$

mit einem von $E$ und $p$ abhängigen positiven $g_4$ (z.B. $g_4 = g_3/(t_0+1)$). Man teilt nun die Gesamtheit $K$ der betrachteten Zahlen $a$ in $t_0+1$ Mengen

$$K_t := \{a \in K \mid (3.6) \text{ gilt für } a \text{ mit } p^t\}, \quad (t = 0, 1, \ldots, t_0),$$

ein. Die $K_t$ sind nicht notwendig disjunkt und evtl. z.T. leer. Zusammengefaßt gilt somit:

(3.7) Lemma. *Sei* $p$ *gegeben mit* $\mathrm{ind}\, V_p > 0$. *Sei* $a \in \bar{f}^*(E)$, $(a, p) = 1$, *und* $a$ *sei keine der durch Bedingung* (2.2) *beschriebenen Zahlen. Dann existiert zu* $p$ *ein natürliches* $t_0$ *derart, daß die betrachteten* $a$ *in* $t_0+1$ (*nicht notwendig disjunkten*) *Mengen* $K_t$ $(t = 0, 1, \ldots, t_0)$ *liegen mit*

$$A^*\left(a(p^t)^2, E\right) > g_4 h(2da)$$

*für alle* $a \in K_t$ *mit einem positiven nur von* $E$ *und* $p$ *abhängigen* $g_4$.

**4. Ternäre Gitter und Quaternionenordnungen.** Die Zusammenhänge zwischen ternären quadratischen Formen und Quaternionen sind von Venkov, Brandt, Linnik, Pall u.a. dargelegt worden. Sie werden hier beschrieben in der Terminologie von Eichler ([7], § 14, vgl. auch [18], Kap. II), und zwar im Anschluß an [27].

$E$ sei ein ternäres $\mathbf{Z}$-Gitter im Raum $V$ mit $f(E) \subseteq \mathbf{Z}$. Der Einfachheit halber werde $E$ primitiv angenommen, d.h. $n(E) = 1$, wobei die Norm den g.g.T. der $f(x)$ mit $x \in E$ bezeichnet. Es bezeichne $C_0(E)$ die 2. Cliffordalgebra von $E$ in der Terminologie von Eichler ([7], § 14); $C_0(E)$ ist eine Ordnung in der Quaternionenalgebra $C_0(V)$. Es bezeichne Sp die Spur, $N$ die Norm und $^-$ die Konjugation in einer Quaternionenalgebra. Durch die Definition $B(y, z) := \mathrm{Sp}(y\bar{z})$ erhält $C_0(V)$ eine Metrik durch die symmetrische Bilinearform $B$. Dann ist $C_0(E)$ ein 4-dimensionales $\mathbf{Z}$-Gitter in $C_0(V)$. Es bezeichne $C_0(E)^\#$ das (bzgl. $B$) duale Gitter von $C_0(E)$, und $\mathfrak{E}$ bezeichne die Elemente von $C_0(E)$ mit Spur 0. Es ist $\mathfrak{E}$ als orthogonales Komplement von 1 (bzgl. der durch $B$ gegebenen Metrik) in $C_0(E)^\#$ ein ternäres Gitter. Es ist $C_0(\mathfrak{E}) \cong C_0(E)$ (s. z.B. [27], Satz 8), also gibt es (nach [27], Lemma, p. 334) ein $q \in \boldsymbol{Q}$ mit $\mathfrak{E} \cong qE$. Durch Normbildung bei den Gittern ergibt sich wegen $n(E) = 1$ hieraus: $n(\mathfrak{E}) = \left(\frac{1}{2}d(E)\right)^{-1}$ (vgl. [27], p. 344), also ist $E$ isomorph zu $\mathfrak{E}$ versehen mit der Normform $d'N$, wobei $d' = d/2$ und $N$ die Norm in $C_0(V)$ ist.

Wir betrachten jetzt den von 1 und $g\mathfrak{E}$ für ein $g \in \mathbf{Z}$ erzeugten $\mathbf{Z}$-Modul $M := \mathbf{Z}\cdot 1 + g\mathfrak{E}$ in $C_0(V)$ und fragen, wann dieser Modul eine Ordnung ist. Nach [27], Korollar, p. 345, ist mit den dortigen Bezeichnungen $M$ sicher dann eine Ordnung, wenn $\mathfrak{q}(M) = \mathfrak{d}(M)$ ist und wenn $M$ nur aus ganzzahligen Elementen der Quaternionenalgebra $C_0(V)$ besteht. Unter Verwendung der expliziten Formeln für das Dualgitter einer Quaternionenordnung in [4], § 3 (dort Komplement genannt), berechnet man: dies ist der Fall für $g = D'(E)$, wobei $D' = D'(E) = \dfrac{d(E)}{d_2(E)}$ in § 0 definiert ist. Also ist $\mathbf{Z}\cdot 1 + D'\mathfrak{E}$ eine Ordnung. Dies kann man auch zeigen durch direktes Nachrechnen der Ringeigenschaften, wiederum unter Verwendung der expliziten Formeln für das Dualgitter einer Quaternionenordnung.

Es bezeichne $\mathfrak{O} := \mathbf{Z}\cdot 1 + D'\mathfrak{E}$, $\mathfrak{P} = D'\mathfrak{E}$. Die Elemente von $\mathfrak{P}$ werden auch die „Vektoren" in $\mathfrak{O}$ genannt. Es bezeichne $D := D(E) := \dfrac{2d(E)}{d_2(E)^2}$, dann ist wegen $D = \dfrac{D'^2}{d'}$ das Gitter $E$ isomorph zu $\mathfrak{P}$ versehen mit der Normform $\dfrac{1}{D}N$. Man kann also sagen:

(4.1) *Die Vektoren der Länge $a$ im Gitter $E$ entsprechen umkehrbar eindeutig den Vektoren der Länge $Da$ in der Quaternionenordnung $\mathfrak{O}$.*

Es heißt $R \in \mathfrak{O}$ primitiv, wenn aus $R = rR'$ mit $R' \in \mathfrak{O}$, $r \in \mathbf{Z}$ folgt: $r = \pm 1$; primitiv mod $k$, wenn $(r, k) = 1$ folgt. Analog zu (4.1) ergibt sich:

(4.2) *Die primitiven Vektoren der Länge $a$ im Gitter $E$ entsprechen umkehrbar eindeutig den primitiven Vektoren der Länge $Da$ in der Quaternionenordnung $\mathfrak{O}$.*



**5. Beweis der Resultate.** Die Methoden von Linnik–Malyshev zur Untersuchung ternärer quadratischer Formen gestatten es, unter gewissen Voraussetzungen von primitiver Darstellbarkeit einer Zahl $a(p^t)^2$ auf primitive Darstellbarkeit der Zahl $a$ durch eine ternäre quadratische Form zu schließen. Entscheidend in unserem Zusammenhang ist das folgende Lemma (5.1), das im wesentlichen auf Linnik–Malyshev zurückgeht. Es werden die Bezeichnungen aus § 4 verwendet. Wiederum sei $n(E) = 1$ vorausgesetzt; dies schränkt die Allgemeinheit beim Beweis des Hauptsatzes nicht ein. Sei $p$ eine Primzahl mit $(p, d) = 1$, also $\mathrm{ind} V_p > 0$. Dann gibt es ein primitives $R \in \mathfrak{O}$, dessen Norm eine $p$-Potenz ist; dies sieht man, wenn man den schon in der Einleitung aufgeführten Satz verwendet, daß die durch die (4-dimensionale) Normform von $\mathfrak{O}$ lokal überall primitiv darstellbaren Zahlen auch global primitiv darstellbar sind bis auf endlich viele Ausnahmen.

(5.1) Lemma. *Sei $p$ eine fest gewählte Primzahl mit $(p, d) = 1$. Sei $R \in \mathfrak{O}$ primitiv mit $N(R) = p^h$ für ein geeignetes $h \in \boldsymbol{N}$. Sei $a \in \tilde{f}^*(E)$ und sei $a$ keine der durch Bedingung (2.2) gekennzeichneten Zahlen. Ferner sei $\left(\dfrac{-Da}{p}\right) = 1$. Es werde gesetzt $c := p^t$ für ein $t$ mit $1 \leqslant t \leqslant t_0$, $t_0$ gemäß Lemma (3.7). Weiter sei $a \in K_t$ (s. Lemma (3.7)).*

*Dann gibt es für hinreichend großes $a$ eine Gleichung*

$$cl + L = WB \quad \text{mit} \quad B = ARC,$$

*wobei $l \in \mathbf{Z}$, $L \in \mathfrak{P}$ primitiv, $N(L) = Dac^2$, $W, B, A, C \in \mathfrak{O}$ mit $N(B) = p^s$, $N(C) = p^r$ für gewisse $r, s \in \boldsymbol{N}$ mit $s - t \geqslant r \geqslant t$.*

Der Beweis ist der Inhalt von § 6.

Bei der Anwendung dieses Lemmas wird folgender einfache Hilfssatz benutzt ([20], p. 116, s. auch [21], p. 562, Prop. 3):

(5.2) Lemma. *Seien $A_1, A_2 \in \mathfrak{O}$, $m \in \boldsymbol{N}$ mit $(m, d) = 1$, $A_2A_1$ primitiv mod $m$, $L \in \mathfrak{P}$ mit $LA_1 \equiv A_2L \equiv 0 \bmod m$, dann ist $L \equiv 0 \bmod m$.*

Aus Lemma (5.1) ergibt sich nun folgendes: Die Gleichung in (5.1) ist äquivalent zu

$$cl + L' = CWAR \quad \text{mit} \quad L' = CLC^{-1};$$

dabei ist $L' \in \mathfrak{P}$ mit $N(L') = Dac^2$, ferner ist $\bar{C}L' \equiv L'(\overline{AR}) \equiv 0 \bmod c$ (denn $N(C) = p^r$, $r \geqslant t$ und $N(AR) = p^{s-r}$, $s - r \geqslant t$). Außerdem ist $\bar{C}(\overline{AR}) = \bar{B}$ primitiv mod $c$ (andernfalls wäre auch $L$ nicht primitiv mod $c$). Somit ist nach Lemma (5.2) $L' \equiv 0 \bmod c$, also ist $\dfrac{1}{c}L' \in \mathfrak{P}$ mit $N\left(\dfrac{1}{c}L'\right) = Da$. Weiter folgt aus der Primitivität von $L$ die Primitivität von $\dfrac{1}{c}L'$.

Hieraus folgt nach (4.2): Wenn man die durch Bedingung (2.2) gekennzeichneten Zahlen $a$ ausnimmt, ferner nur $a$ mit $\left(\frac{-Da}{p}\right)=1$ und $a\in K_t$ betrachtet, so impliziert $a\in\bar{f}^*(E)$ für hinreichend großes $a$, daß $a\in f^*(E)$. Dabei gilt für $t$: $1\leqslant t\leqslant t_0$. Für $t=0$ gilt die Aussage trivialerweise. Weil $t_0$ nur von $E$ und $p$ abhängt, kann bei festem $p$ die Voraussetzung $a\in K_t$ weggelassen werden. Zusammengefaßt gilt also:

Wenn man $p$ vorgibt mit $(p,d)=1$, wenn man nur Zahlen $a$ mit $\left(\frac{-Da}{p}\right)=1$ betrachtet und ferner die durch Bedingung (2.2) gekennzeichneten Zahlen ausnimmt, so impliziert $a\in\bar{f}^*(E)$ für hinreichend großes $a$, daß $a\in f^*(E)$.

Malyshev zeigt in [20], p. 179 ff., daß unter Annahme der in § 1 formulierten Riemann-Hypothese gilt: Es gibt zu $a$ eine Primzahl $q$, $(q,d)=1$ mit $\left(\frac{-Da}{q}\right)=1$ derart, daß

$$q<g_5\exp\left(g_6\frac{\sqrt{\ln a}}{\ln\ln a}\right)$$

mit nur von $E$ abhängigen positiven Konstanten $g_5, g_6$. Daraus wird gefolgert ([20], p. 184 ff.), daß unter dieser Annahme die Einschränkung $\left(\frac{-Da}{p}\right)=1$ weggelassen werden kann. Diese Überlegungen übertragen sich auf die Situation in Lemma (5.1) und somit auf unsere Situation hier.

Wenn wir alles dies zusammentragen und Satz (2.1) (b) verwenden, haben wir damit Teil (a) des Hauptsatzes (1.1) und den Zusatz (1.3) bewiesen.

Zum Beweis von Teil (b) des Hauptsatzes betrachten wir zunächst ein maximales Gitter $E$. Wenn $a$ Ausnahme für $E$ ist, so auch $ap^{2k}$, $k=1,2,\ldots$ für jedes $p$ mit $\operatorname{ind}V_p=0$, denn bekanntlich ([7], § 9,3) ist dann

$$E_p\cong\{x\in V_p\mid f(x)\in\mathbf{Z}_p\};$$

wäre also $f(x)=ap^{2k}$ mit $x\in E$, so wäre $f\left(\frac{x}{p^k}\right)=a$ mit $\frac{x}{p^k}\in E$, also $a$ keine Ausnahme. (Ähnliche Überlegungen finden sich bei Ross ([29], p. 41) und Pall ([25], p. 48).) Aus der Struktur der maximalen Gitter im Lokalen ([7], § 9,3) liest man ab:

$$\bar{f}^*(E)=\{a\in\bar{f}(E)\mid p^2\nmid a \text{ für alle } p \text{ mit } \operatorname{ind}V_p=0\}.$$

Somit folgt für maximale Gitter aus dem Teil (a) des Hauptsatzes sofort Teil (b), wenn man Satz (2.1) (a) verwendet.



Ist für ein $p$ das Gitter $E_p$ nicht maximal, so sei $E'_p$ ein maximales $E_p$ umfassendes Gitter und $E'$ definiert durch

$$(E')_q:=E_q \quad \text{für} \quad q\neq p, \qquad (E')_p:=E'_p.$$

Der Index $[E':E]$ ist eine $p$-Potenz, es ist also für ein $n\in\mathbf{N}$: $p^nE'\subseteq E$. Daraus folgt: Wenn $E$ eine Ausnahme $a$ hat, so hat $E$ genau dann eine unendliche $p$-Serie $ap^{2k}$ $(k=0,1,2,\ldots)$ von Ausnahmen, wenn dies für $E'$ zutrifft. Letzteres tritt höchstens für $p$ mit $\operatorname{ind}V_p=0$ auf, und zwar genau dann, wenn $a$ Ausnahme für $E'$ ist; wegen $\operatorname{ind}V_p=0$ und der oben angeführten Struktur maximaler lokaler anisotroper Gitter ist $E'$ eindeutig bestimmt.

Damit sind Teil (b) des Hauptsatzes und die genaueren Aussagen (1.4) und (1.5) bewiesen. Die Aussagen in (1.6) sind ebenfalls bewiesen bis auf den Fall, daß $(p,2D)=1$, aber $p\mid d$; dieser Fall läßt sich genauso wie in [20], p. 176, 177 (Abschnitt 3°) behandeln.

**6. Zur Methode von Linnik–Malyshev.** Es ist der Beweis von Lemma (5.1) nachzutragen, das, wie schon erwähnt, aus den Ergebnissen von Linnik und Malyshev folgt. Wir führen die von Linnik und Malyshev verwendeten Methoden für unsere Situation auf und stellen den Beweis des Lemmas (5.1) dar bis auf zwei Hilfssätze ((6.23), (6.25)), für deren Beweis hinreichende Literatur vorliegt.

Sei durchweg $n(E)=1$, $a\in\bar{f}^*(E)$ und sei $a$ keine der durch Bedingung (2.2) gekennzeichneten Zahlen. Sei $p$ eine fest gewählte Primzahl mit $(p,d)=1$, also $\operatorname{ind}V_p>0$, und sei $\left(\frac{-Da}{p}\right)=1$, also $(a,p)=1$. Weiter sei $a\in K_t$, $1\leqslant t\leqslant t_0$ (s. Lemma (3.7)). Setze $c:=p^t$, dann gilt nach Lemma (3.7):

$$A^*(ac^2,E)>g_4h(2da), \tag{6.1}$$

wobei die positive Konstante $g_4$ nur von $E$ und $p$ abhängt. Die im folgenden auftretenden $g_i$ (bzw. $g_{i,\varepsilon}$) sind positive Konstanten, die nur von $E$ und $p$ (bzw. $E, p$ und $\varepsilon$) abhängen.

Für die Quaternionenordnung $\mathfrak{O}$ besagt (6.1) nach (4.2): es gibt mehr als $g_4h(2da)$ primitive Vektoren aus $\mathfrak{B}$ mit Norm $Dac^2$. Wegen

$$4Dac^2=2da\,\frac{4c^2}{d_2^2} \quad \text{mit} \quad \sqrt{\frac{4c^2}{d_2^2}}\in Q$$

ist nach dem schon beim Beweis von Satz (3.1) benutzten Satz von Dirichlet über das Verhältnis der Klassenzahl von Ordnungen in quadratischen Zahlkörpern zur Klassenzahl der zugehörigen Hauptordnung:

$$g_7h(4Dac^2)<h(2da)<g_8h(4Dac^2).$$

Somit gilt:

(6.2) Es gibt mehr als $g_9 h(4Dac^2)$ primitive Vektoren aus $\mathfrak{V}$ mit Norm $Dac^2$.

Wir referieren jetzt die im folgenden benutzten Sätze von Venkov–Linnik über „Rotationen" von Vektoren (s. [20], Kap. IV, 5, s. auch [21], p. 562, 563): primitive Vektoren $L, L' \in \mathfrak{V}$ der Norm $Dac^2$ heißen äquivalent, wenn es zu jedem $g \in \mathbf{Z}$ ein $W_g \in \mathfrak{O}$ gibt mit $(N(W_g), g) = 1$ und $W_g^{-1} L W_g = L'$. Es gilt: wenn $L \equiv L' \bmod d$, dann sind $L$, $L'$ äquivalent; wenn $L$ und $L'$ äquivalent sind und für $g = dac^2$ gesetzt wird $W_g =: W$, dann existiert ein $B \in \mathfrak{O}$ und ein $l \in \mathbf{Z}$ mit

$$l + L = WB. \tag{6.3}$$

Ferner ist folgende Abbildung $\alpha$: $(L, L') \to \mathfrak{R}$ wohldefiniert: dem Paar $(L, L')$ („Rotation") wird zugeordnet die eigentliche Äquivalenzklasse $\mathfrak{R}$ der positiv-definiten binären quadratischen Form $(w, l, b) := wx^2 + 2lxy + by^2$ (wobei $w := N(W)$, $b := N(B)$) mit $wb - l^2 = Dac^2$, $(w, 2l, b) = 1$, also einer primitiven Form der Determinante $4Dac^2$ (man beachte unsere Terminologie: $x^2 + y^2$ hat z.B. die Determinante 4). Es gilt weiter: wenn $\alpha(L, L') = \mathfrak{R}$, $\alpha(L', L'') = \mathfrak{R}'$, so ist $\alpha(L, L'') = \mathfrak{R} \cdot \mathfrak{R}'$, wobei $\cdot$ die Gaußsche Komposition bezeichnet.

Da die Anzahl der Äquivalenzklassen von Vektoren in $\mathfrak{V}$ durch eine nur von $E$ abhängige Konstante begrenzt ist, folgt aus (6.2), daß es mehr als $g_{10} h(4Dac^2)$ primitive äquivalente Vektoren $L_i \in \mathfrak{V}$ mit $N(L_i) = Dac^2$ gibt. Mit diesen Vektoren $L_i$ lassen sich Gleichungen (6.3) bilden und nach Venkov–Linnik ist $\alpha(L_1, L_i) = \mathfrak{S}_i$ mit einer eigentlichen Äquivalenzklasse $\mathfrak{S}_i$ primitiver positiv-definiter binärer quadratischer Formen der Determinante $4Dac^2$. Nach einem weiteren Satz von Venkov–Linnik liefert nur Transformation mit den (endlich vielen) Einheiten der Quaternionenordnung $\mathfrak{O}$ dieselbe Klasse, somit sind

$$h' > g_{11} h(4Dac^2) \tag{6.4}$$

der Klassen $\mathfrak{S}_i$ verschieden.

Um Lemma (5.1) zu beweisen, macht man einen Umweg und zeigt das allgemeinere

(6.5) Lemma. *Sei $p$ eine fest gewählte Primzahl mit $(p, d) = 1$. Sei $R \in \mathfrak{O}$ primitiv mit $N(R) = p^h$ für ein geeignetes $h \in \mathbf{N}$. Sei $a \in \bar{f}^*(E)$ und sei $a$ keine der durch Bedingung (2.2) gekennzeichneten Zahlen. Ferner sei $\left(\frac{-Da}{p}\right) = 1$. Es werde gesetzt $c := p^t$ für ein $t$ mit $1 \leqslant t \leqslant t_0$ (hierbei $t_0$ gemäß Lemma (3.7)). Weiter sei $a \in K_t$ (s. Lemma (3.7)).*

*Dann gibt es ein $\varrho$ mit $0 < \varrho \leqslant \frac{1}{2}$ derart, daß für hinreichend großes $a$ mehr als $g_{12} h(4Dac^2)$ Gleichungen*

$$cl + L = WB \tag{6.6}$$



*mit*

$$B = ARC \tag{6.7}$$

*existieren, wobei $l \in \mathbf{Z}$, $L \in \mathfrak{V}$ primitiv mit $N(L) = Dac^2$, $W, B, A, C \in \mathfrak{O}$ mit $N(W) = w$, $(w, p) = 1$, $N(B) = p^s$,*

$$N(C) = p^r, \tag{6.8}$$

$$\frac{1}{p} a^\varrho < p^s < a^\varrho,$$

$$s - t \geqslant r \geqslant t. \tag{6.9}$$

*Dabei hängen $\varrho$ und die positive Konstante $g_{12}$ nur vom zugrundeliegenden Gitter $E$ und der Primzahl $p$ ab.*

Der Beweis folgt dem Vorgehen in [20], Kap. V, 4. Falls $t$ derart, daß $K_t$ eine endliche Menge ist, ist das Lemma für $a \in K_t$ trivialerweise richtig. Dieser Fall sei forthin ausgeschlossen.

1. Schritt. Beweis der Aussagen des Lemmas ohne Bedingung (6.7) (dann sind (6.8) und (6.9) leer): Sei $z := \left[\frac{1}{g_{11}}\right] + 1$, so daß nach (6.4):

$$h' z > h(4Dac^2). \tag{6.10}$$

Sei $e \in \mathbf{Z}$ definiert durch

$$\frac{1}{p} a^{z'} < p^e < a^{z'} \quad \text{mit} \quad z' := \frac{1}{8z}, \tag{6.11}$$

und sei

$$v_i := p^{(2z+i)e}, \quad i = 0, 1, \ldots, z. \tag{6.12}$$

Es sei $a$ so groß, daß $v_0 > c^2$. Wegen $\left(\frac{-Da}{p}\right) = 1$ gibt es ein $l \in \mathbf{Z}$ mit

$$l^2 + Da \equiv 0 \bmod p. \tag{6.13}$$

Zu $v_i$ sucht man $l_i$ mit

$$\begin{cases} l_i \equiv l \bmod p, \\ (cl_i)^2 + Dac^2 \equiv 0 \bmod v_i, \\ 2|cl_i| \leqslant v_i, \end{cases} \tag{6.14}$$

$$\left(\frac{1}{v_i}\left((cl_i)^2 + Dac^2\right), p\right) = 1. \tag{6.15}$$

Wegen (6.13) gibt es $l_i'$ mit

$$l_i' \equiv l \bmod p,$$

$$l_i'^2 + Da \equiv 0 \bmod p^{(2z+i)e-2t},$$

$$|l_i'| \leqslant \tfrac{1}{2} p^{(2z+i)e-2t}.$$

Die $l_i'$ erfüllen also (6.14); falls auch (6.15) erfüllt wird, setzt man $l_i := l_i'$, andernfalls setzt man

$$l_i := l_i' + \frac{v_i}{c^2},$$

dann erfüllen $l_i$ die Bedingungen (6.14) und (6.15) (hierzu beachte man, daß $c \geqslant 3$). Mit der Abkürzung

$$u_i := \frac{1}{v_i}\left((cl_i)^2 + Dac^2\right)$$

ist wegen (6.11):

$$v_i \leqslant v_z = p^{3ze} < a^{3/8}, \qquad u_i > \frac{a}{v_z} > a^{5/8},$$

somit $v_i \leqslant u_i$, also ist $(v_i, cl_i, u_i) := v_i x^2 + 2cl_i xy + u_i y^2$ eine primitive reduzierte positiv-definite binäre quadratische Form der Determinante $4(u_i v_i - (cl_i)^2) = 4Dac^2$, deren eigentliche Äquivalenzklasse mit $\mathfrak{R}_i$ bezeichnet werde $(i = 0, 1, \ldots, z)$. Diese $z+1$ Klassen sind verschieden, da die Formen reduziert sind. Man betrachtet nun die komponierten Klassen

$$\mathfrak{S}_j \cdot \mathfrak{R}_k \qquad (j = 1, \ldots, h';\ k = 0, 1, \ldots, z).$$

Da $h(4Dac^2)$ die Gesamtanzahl der primitiven eigentlichen Klassen der Determinante $4Dac^2$ ist, gibt es somit mehr als $h'(z+1) - h(4Dac^2)$ Gleichungen

$$\mathfrak{S}_j \cdot \mathfrak{R}_k = \mathfrak{S}_l \cdot \mathfrak{R}_m \qquad (1 \leqslant j, l \leqslant h',\ j \neq l,\ 0 \leqslant m < k \leqslant z).$$

Nach (6.10) und (6.4) ist die letztere Anzahl größer als $g_{11} h(4Dac^2)$. Daher gibt es ein festes Indexpaar $(k_0, m_0)$, für welches es mehr als $\frac{g_{11}}{(z+1)^2} h(4Dac^2)$ Indizes $j$ $(1 \leqslant j \leqslant h')$ mit $\mathfrak{S}_j^{-1} \cdot \mathfrak{S}_l = \mathfrak{R}_{k_0} \cdot \mathfrak{R}_{m_0}^{-1}$ gibt. Die Klasse $\mathfrak{R}_{k_0} \cdot \mathfrak{R}_{m_0}^{-1}$ wird repräsentiert (nach der obigen Konstruktion und nach expliziter Ausrechnung der Gaußschen Komposition ([9], Art. 243)) durch $(w, cl', p^s)$ mit $(w, p) = 1$, $l' \equiv l \bmod p$, $s = e(k_0 - m_0)$. Andererseits gilt nach Venkov–Linnik für die primitiven äquivalenten $L_i \in \mathfrak{B}$, mit denen die $\mathfrak{S}_i$ definiert wurden (s. den Absatz vor (6.4)): $a(L_j, L_l) = \mathfrak{S}_j^{-1} \cdot \mathfrak{S}_l$. Somit entspricht jedem $j$ eine Gleichung $cl' + L_j = W_j B_j$ mit $W_j, B_j \in \mathfrak{O}$, $N(W_j) = w$, $(w, p) = 1$, $N(B_j) = p^s$. Wenn man für $l'$ wieder $l$ schreibt und $\varrho := (k_0 - m_0)/8z$, $g_{12} := g_{11}/(z+1)^2$ setzt, so folgt die Behauptung des 1. Schrittes. Man beachte, daß — über die Behauptung von Lemma (6.5) hinausgehend — das $l$ dasselbe ist für alle Gleichungen (6.6).



2. Schritt. Indirekter Beweis des Lemmas (6.5): Angenommen, es gäbe unter den im 1. Schritt konstruierten $h''$ Gleichungen

$$cl + L_i = W_i B_i \qquad (i = 1, \ldots, h'') \tag{6.16}$$

mit

$$h'' > g_{12} h(4Dac^2) \tag{6.17}$$

nicht auch schon für ein $g_{13}$ mehr als $g_{13} h(4Dac^2)$ Gleichungen, die alle Bedingungen des Lemmas (6.5) erfüllen, wobei $r$ aus Bedingung (6.8) für alle diese Gleichungen dasselbe sein soll, dann existierte zu jedem $\eta > 0$ eine unendliche stark monotone Folge $F$ (abhängig von $E, p, \eta$) von Zahlen $a \in K_t$ derart, daß für jedes $r$ mit $r \geqslant t$, $r \leqslant s - t$ für die Anzahl $I$ der Indizes $i \in \{1, \ldots, h''\}$ mit

$$B_i = A_i R C_i \quad \text{für} \quad A_i, C_i \in \mathfrak{O}, \quad N(C_i) = p^r \tag{6.18}$$

gälte:

$$I < \eta h''. \tag{6.19}$$

Insbesondere gälte dies für die folgendermaßen definierten $r_1, \ldots, r_{s_1}$: Es werde $r_0$ fest gewählt gemäß Lemma (6.25) (s.u.), und $s_1$ sei derart, daß $r_1 := t$, $r_2 := r_1 + r_0$, $r_3 := r_2 + r_0$, $\ldots$, $r_{s_1} := r_{s_1 - 1} + r_0 \leqslant s - t$, $r_{s_1} + r_0 > s - t$ (dabei sei $a$ so groß, daß $s_1 \geqslant 1$).

Im folgenden sei $a$ aus der Folge $F$. Von den $h''$ Gleichungen (6.16) betrachten wir diejenigen $h'''$ (unter eventueller Umnumerierung):

$$cl + L_i = W_i B_i \qquad (i = 1, \ldots, h''') \tag{6.20}$$

mit der Eigenschaft: für jedes $i = 1, \ldots, h'''$ ist die Anzahl der Indizes $r \in \{r_1, \ldots, r_{s_1}\}$ mit Bedingung (6.18) kleiner als $2\eta s_1$. Dann wäre

$$h''' > \tfrac{1}{2} h'', \tag{6.21}$$

denn es gibt $h'' - h'''$ Gleichungen (6.16), in welchen $\geqslant 2\eta s_1$ Indizes $r \in \{r_1, \ldots, r_{s_1}\}$ mit (6.18) liegen; andererseits wäre die Anzahl solcher Indizes $r$ in den Gleichungen (6.16) gemäß (6.19) kleiner als $\eta h'' s_1$, somit $(h'' - h''') 2\eta s_1 < \eta h'' s_1$, also (6.21).

Nach dem Satz von Siegel über die Klassenzahl quadratischer Zahlkörper ([31]) ist für $\varepsilon > 0$:

$$h(a) > g_{14,\varepsilon} a^{1/2 - \varepsilon}.$$

Somit folgte aus (6.21) und (6.17):

$$h''' > g_{15,\varepsilon} a^{1/2 - \varepsilon}. \tag{6.22}$$

In dieser Situation ist das folgende Lemma anwendbar:

(6.23) LEMMA. *Es liegen vor die Gleichungen*

$$l+L_i = W_i B_i \quad (i = 1, \ldots, n)$$

*mit* $l \in \mathbf{Z}$, $L_i \in \mathfrak{B}$ *primitiv und alle verschieden mit* $N(L_i) = m$, $W_i, B_i \in \mathfrak{O}$ *mit* $N(W_i) = w$, $(w, p) = 1$, $N(B_i) = p^s$, $n > g_{16,\varepsilon} m^{1/2-\varepsilon}$,

$$g_{17,\varepsilon} m^{\varrho-\varepsilon} \leqslant p^s \leqslant g_{18,\varepsilon} m^{\varrho-\varepsilon}, \quad (m, p) < g_{19,\varepsilon} m^{\varepsilon}, \quad 0 < \varrho \leqslant 1/2.$$

*Dann gilt für die Anzahl* $b$ *der verschiedenen* $B_i$:

$$b > g_{20,\varepsilon} m^{\varrho-3\varepsilon}.$$

Das Lemma findet sich in [20], p. 156 (Lemma 1), im Spezialfall einer ungeraden halben Determinante $d'$. Der Beweis ohne diese Einschränkung geht analog. Ein einfacherer Zugang zu diesem Lemma ist kürzlich in einem Spezialfall von Malyshev in [21], § 5, und [22] angegeben worden.

Für die Anzahl $b'$ der verschiedenen $B_i \in \mathfrak{O}$ in (6.20) folgt nun aus (6.22) und Lemma (6.23) mit $m = Dac^2$:

$$b' > g_{21,\varepsilon} a^{\varrho-3\varepsilon}. \tag{6.24}$$

Andererseits gilt folgendes

(6.25) LEMMA. *Sei* $\varrho$ *gegeben mit* $0 < \varrho \leqslant 1/2$ *und* $\frac{1}{p} a^{\varrho} < p^s < a^{\varrho}$.

*Sei* $b''$ *die Anzahl der primitiven* $b \in \mathfrak{O}$ *mit* $N(B) = p^s$ *und der Eigenschaft: die Anzahl der Indizes* $r \in \{r_1, \ldots, r_{s_1}\}$ *mit* $B = ARC$, $A, C \in \mathfrak{O}$, $N(C) = p^r$, *ist kleiner als* $2\eta s_1$.

*Dann existieren* $r_0 \in \mathbf{N}$, $\eta > 0$, $\mu > 0$ *mit*

$$b'' < g_{22} a^{\varrho-\mu}. \tag{6.26}$$

Das Lemma findet sich in [20], p. 170, wiederum im Spezialfall eines ungeraden $d'$. Der Beweis ohne diese Einschränkung geht analog. Das entscheidende Hilfsmittel beim Beweis sind Sätze über das asymptotische Verhältnis der Anzahlen der Hauptideale einer festen Norm in einer Quaternionenordnung zur Anzahl der Ideale dieser Norm, unter zusätzlicher Forderung der (Rechts-) Teilbarkeit sämtlicher Ideale durch das Quaternion $B$ und der (Links-) Teilbarkeit durch ein Ideal einer vorgegebenen Norm. Diese Sätze werden zurückgeführt auf Sätze über asymptotische Gleichverteilung von Gitterpunkten auf 4-dimensionalen Ellipsoiden.

Seien jetzt $r_0, \eta, \mu$ gemäß Lemma (6.25) gewählt. Die in (6.20) auftretenden $B_i$ sind primitiv, weil die $L_i$ primitiv sind. Wenn man nun $3\varepsilon < \mu$ wählt, ergäben (6.24) und (6.26) bei hinreichend großem $a$ einen Widerspruch, der den Beweis von Lemma (6.5) abschließt.



**7. Ausblick auf weitere Probleme.** Die durch Bedingung (2.2) gekennzeichneten Zahlen umfassen die Spinorprimitivausnahmen (s. Bemerkung (2.3)); die ersteren sind bei den meisten Betrachtungen ausgeschlossen worden, es ist jedoch offen, ob es (z. B. bei Lemma (3.7) und somit Lemma (5.1)) genügt, letztere auszuschließen.

Wie schon in der Einleitung gesagt, ist die effektive Bestimmung der Ausnahmen mit den hier verwendeten Methoden nicht möglich. Offen ist auch die Frage nach der Bestimmung hinreichend großer Ausnahmen, welche Determinantenteiler nur in beschränkter Potenz enthalten. Die in der mir bekanntgewordenen Literatur aufgeführten Beispiele weisen nur solche hinreichend großen Ausnahmen auf, die Quadrate sind ([12], Table II, [36], p. 115). Daß dies nicht notwendig der Fall ist, zeigt folgendes Beispiel:

$$f_1(x_1, x_2, x_3) = x_1^2 + 2x_2^2 + 64 \cdot 17 x_3^2$$

*und*

$$f_2(x_1, x_2, x_3) = (2x_1 + x_3)^2 + 2x_2^2 + 16 \cdot 17 x_3^2$$

*liegen im selben Geschlecht;* $f_1$ *stellt* $17u^2$, *für Primzahlen* $u$ *mit* $u \equiv 1 \bmod 8$ *dar,* $f_2$ *jedoch nicht.*

(Beweis. Die binären Formen $x_1^2 + 64 \cdot 17 x_3^2, (2x_1 + x_3)^2 + 16 \cdot 17 x_3^2$ gehören demselben Geschlecht an, denn sie haben beide die Determinante $4 \cdot 64 \cdot 17$ und die Äquivalenz in $\mathbf{Z}_2$ und $\mathbf{Z}_{17}$ folgt aus

$$(2x_1 + x_3)^2 + 16 \cdot 17 x_3^2 = (16 \cdot 17 + 1)\left(x_3 + \frac{2}{16 \cdot 17 + 1} x_1\right)^2 + \frac{64 \cdot 17}{16 \cdot 17 + 1} x_1^2$$

und $16 \cdot 17 + 1 \equiv 1^2 \bmod 16$ und $16 \cdot 17 + 1 \equiv 1^2 \bmod 17$.

Daher liegen auch $f_1$ und $f_2$ im selben Geschlecht. Die Behauptung über $f_1$ ist offensichtlich, die über $f_2$ folgt indirekt so: Wäre

$$(2x_1 + x_3)^2 + 2x_2^2 + 16 \cdot 17 x_3^2 = 17u^2$$

ganzzahlig lösbar, so wäre der g.g.T. $(x_1, x_2, x_3) = 1$, da $u$ Primzahl ist und $f_2$ offenbar 17 nicht darstellt. Setzt man $v := 2x_1 + x_3$, so wäre $v^2 + 2x_2^2 \equiv 1 \bmod 8$, somit $v$ und $x_3$ ungerade. Setzt man $r := u + 4x_3$, $s := u - 4x_3$, so wäre $r \equiv s \equiv 5 \bmod 8$ und

$$17rs = 17u^2 - 17 \cdot 16 x_3^2 = v^2 + 2x_2^2 \quad \text{und} \quad (x_2, r, s) = 1,$$

letzteres weil $t \mid (x_2, r, s)$ impliziert $t \mid r - s = 8x_3$, also $t \mid x_3$, ferner $t \mid v$, somit $t \mid (x_1, x_2, x_3) = 1$. Weil $r \equiv 5 \bmod 8$, gäbe es eine Primzahl $p \equiv -1$ oder $5 \bmod 8$, die in $r$ in ungerader Potenz steckte. Dann wäre $-2$ quadratischer Nichtrest mod $p$ und aus $v^2 \equiv -2x_2^2 \bmod p$ folgte $p \mid x_2$ und $p \mid v$, somit $p \nmid s$ (da $p \mid r$, $p \mid x_2$ und $(x_2, r, s) = 1$). Daher wäre $v^2 + 2x_2^2 = 17rs$ genau durch eine ungerade Potenz von $p$ teilbar, was einen Widerspruch ergäbe.)

Die in dieser Arbeit behandelte Frage nach der Darstellbarkeit von Zahlen $a$ durch ternäre quadratische Formen $f$ besagt: wann gibt es einen Gitterpunkt auf dem Ellipsoid $f = a$? Genauer kann man fragen nach der Anzahl dieser Gitterpunkte. Die in Lemma (6.5) aufgeführten Abschätzungen liefern in Verbindung mit den §§ 2–5 folgende Schranken (in Verallgemeinerung von Ergebnissen von Linnik und Malyshev):

$$g' h(Da) < A^*(a, E) < g'' h(Da), \tag{7.1}$$

wenn $a \epsilon \bar{f}^*(E)$ und wenn $a$ keine der durch Bedingung (2.2) gekennzeichneten Zahlen ist, und wenn die verallgemeinerte Riemannsche Vermutung als richtig vorausgesetzt wird. Dabei bezeichnen $g', g''$ positive Konstanten, die nur von $f$ abhängen.

Mit Methoden von Linnik und Malyshev lassen sich die Ungleichungen (7.1) (wieder mit den dortigen Ausnahmen und Annahmen) sogar zeigen für die Anzahl der Gitterpunkte in einem vorgegebenen Winkelraum; die Konstanten $g', g''$ hängen dabei von $f$ und diesem Winkelraum ab. Insbesondere heißt dies: in jedem Winkelraum werden — unter Annahme der verallgemeinerten Riemannschen Vermutung — alle vom Geschlecht darstellbaren Zahlen dargestellt, abgesehen von gewissen Ausnahmen, die in endlich vielen Quadratklassen liegen.

Ich vermute, daß der Hauptsatz (1.1) sich auf den Fall freier Gitter in algebraischen Zahlkörpern verallgemeinern läßt. Der Inhalt der §§ 2–4 läßt sich im wesentlichen übertragen, die Methode von Linnik–Malyshev jedoch nicht ohne weiteres — z.B. werden ja explizit reduzierte binäre quadratische Formen über $\boldsymbol{Z}$ konstruiert (s. § 6, Beweis von Lemma (6.5), 1. Schritt).

**Zusatz bei der Korrektur** (10.9.77): Die Ergebnisse von §2 sind inzwischen von Herrn R. Schulze-Pillot in seiner Diplomarbeit *Darstellung von Zahlen durch Spinorgeschlechter ternärer quadratischer Gitter* (Göttingen 1977) verschärft worden.

## Literaturverzeichnis


[1] S. I. Borewicz und I. R. Šafarevič, *Zahlentheorie*, Basel 1966.

[2] G. Bottorf, *On quaternary quadratic forms*, Thesis, Pennsylvania State University 1970.

[3] L. E. Dickson, *Studies in the theory of numbers*, Chicago 1930, Chelsea Reprint 1957.

[4] M. Eichler, *Untersuchungen in der Zahlentheorie der rationalen Quaternionenalgebren*, J. Reine Angew. Math. 174 (1935), S. 129–156.

[5] — *Die Ähnlichkeitsklassen indefiniter Gitter*, Math. Z. 55 (1952), S. 216–252.

[6] — *Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion*, Arch. Math. 5 (1954), S. 355–366.

[7] — *Quadratische Formen und orthogonale Gruppen*, 2. Aufl., Springer 1974.

[8] O. M. Fomenko, *Estimates of the Petersson inner product with application to the theory of quaternary quadratic forms*, Soviet Math. Doklady 4 (1963), S. S. 1372–1375.





[9] C. F. Gauß, *Disquisitiones arithmeticae*, Neudruck der deutschen Übersetzung, Chelsea 1965.

[10] H. Gupta, *Some idiosyncratic numbers of Ramanujan*, Proc. Indian Acad. Sci. A 13 (1941), S. 519–520.

[11] B. W. Jones, *The arithmetic theory of quadratic forms*, AMS Monograph, 1950.

[12] — und G. Pall, *Regular and semiregular positive ternary quadratic forms*, Acta Math. 70 (1939), S. 165–191.

[13] — und G. L. Watson, *On indefinite ternary quadratic forms*, Canad. J. Math. 8 (1956), S. 592–608.

[14] H. D. Kloosterman, *On the representation of numbers in the form* $ax^2 + by^2 + cz^2 + dt^2$, Acta Math. 49 (1926), S. 407–464.

[15] M. Kneser, *Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veränderlichen*, Arch. Math. 7 (1956), S. 323–332.

[16] — *Klassenzahlen definiter quadratischer Formen*, Arch. Math. 8 (1957), S. 241–250.

[17] — *Darstellungsmaße indefiniter quadratischer Formen*, Math. Z. 77 (1961), S. 188–194.

[18] — *Quadratische Formen*, Vorlesungsausarbeitung, Göttingen 1974.

[19] Yu. V. Linnik, *Ergodic properties of algebraic fields*, Springer 1968.

[20] A. V. Malyshev, *Über die Darstellung ganzer Zahlen durch positiv definite quadratische Formen* (russ.), Trudy Mat. Inst. Stekl. 65, Moskau–Leningrad 1962.

[21] — *Yu. V. Linnik's ergodic method in number theory*, Acta Arith. 27 (1975), S. 555–598.

[22] — *Eine neue Variante der ergodischen Methode Yu. V. Linnik's in der Zahlentheorie* (russ.), Zapiski nauč. sem. LOMI, t. 50, Leningrad 1975, S. 179–186.

[23] O. T. O'Meara, *The integral representation of quadratic forms over local fields*, Amer. J. Math. 80 (1958), S. 843–878.

[24] — *Introduction to quadratic forms*, 3rd ed., Springer 1973.

[25] G. Pall, *The completion of a problem of Kloosterman*, Amer. J. Math. 68 (1946), S. 47–58.

[26] G. Pall und A. E. Ross, *An extension of a problem of Kloosterman*, Amer. J. Math. 68 (1946), S. 59–65.

[27] M. Peters, *Ternäre und quaternäre quadratische Formen und Quaternionenalgebren*, Acta Arith. 15 (1969), S. 329–365.

[28] S. Ramanujan, *Collected papers*, Cambridge 1927.

[29] A. E. Ross, *On a problem of Ramanujan*, Amer. J. Math. 68 (1946), S. 29–46.

[30] C. L. Siegel, *Über die analytische Theorie der quadratischen Formen*, Ann. Math. 36 (1935), S. 527–606.

[31] — *Über die Klassenzahl quadratischer Zahlkörper*, Acta Arith. 1 (1936), S. 83–86.

[32] — *Indefinite quadratische Formen und Funktionentheorie I, II*, Math. Ann. 124 (1951), S. 17–54; 366–387.

[33] H. J. S. Smith, *On the orders and genera of the ternary quadratic forms*, Coll. Math. Papers, vol. I, S. 455–508, Oxford 1894.

[34] V. A. Tartakowsky, *Die Gesamtheit der Zahlen, die durch eine positive quadratische Form* $F(x_1, \ldots, x_s)$ $(s \geqslant 4)$ *darstellbar sind*, Izv. Akad. Nauk SSSR 7 (1929), S. 111–122, 165–195.

[35] G. L. Watson, *The representation of integers by positive ternary quadratic forms*, Mathematika 1 (1954), S. 104–110.

[36] G. L. Watson, *Integral quadratic forms*, Cambridge 1960.
[37] — *Quadratic Diophantine equations*, Phil. Trans. Roy. Soc. London, Ser. A, 1026, 253 (1960), S. 227–254.

MATHEMATISCHES INSTI UT DER UNIVERSITÄT
Münster

*Eingegangen am 22. 4. 1976*

ACTA ARITHMETICA
XXXIV (1977)

# On permutations containing no long arithmetic progressions

by

J. A. Davis, R. C. Entringer (Albuquerque, N. Mex.), R. L. Graham (Murray Hill, N. J.) and G. J. Simmons (Albuquerque, N. Mex.)

**Introduction.** It has often been noted (e.g., see [1], [4], [5]) that it is possible to arrange $n$ consecutive integers into a sequence $a_1 a_2 \dots a_n$ which contains no subsequence forming an increasing or decreasing 3-term arithmetic progression (A.P.). In other words, if $a_i = c$, $a_j = c+d$, $a_k = c+2d$ for some positive $d$, then either $j = \max\{i, j, k\}$ or $j = \min\{i, j, k\}$. In this note we investigate several questions related to this idea. For example, we show that any doubly-infinite permutation $\dots a_{-2} a_{-1} a_0 a_1 a_2 \dots$ of *all* the positive integers must contain an increasing or decreasing (i.e., monotone) 3-term A.P. as a subsequence. On the other hand, we construct a doubly-infinite permutation of the positive integers which contains no monotone 4-term A.P.

**Permutations of finite intervals.** Let us denote by $M(n)$ the number of permutations $a_1 a_2 \dots a_n$ of $\{1, 2, \dots, n\} \equiv [1, n]$ containing no monotone 3-term A.P. To see that $M(n) > 0$ for all $n$ simply note if $A = a_1 a_2 \dots a_m$ has no monotone 3-term A.P. then

$$A' = (2A)(2A-1) \equiv (2a_1)(2a_2) \dots (2a_m)(2a_1-1) \dots (2a_m-1)$$

also has no monotone 3-term A.P. (since the first and last terms of a 3-term A. P. must have the same parity!) Of course, if $A$ is a permutation of $[1, m]$ then $A'$ is a permutation of $[1, 2m]$. Finally, since no monotone A.P.'s are created by *deleting* entries of $A$, the assertion $M(n) > 0$ for all $n$ follows immediately. In fact, much more is true.

Fact 1.

$$M(n) \geqslant 2^{n-1} \quad \textit{for} \quad n \geqslant 1. \tag{1}$$

Proof. As we have already noted, if $A$ has no monotone 3-term A.P., then neither do $2A$ and $2A-1$. Thus, if $A$ and $A'$ are 3-term A.P.-