[4] Serge Lang, *Algebra*, Addison-Wesley, Reading 1965.
[5] Henry B. Mann and William Yslas Vélez, *On normal radical extensions of the rationals*, J. Lin. Multilin. Alg. 3 (1975), pp. 73–80.
[6] Michael J. Norris and William Yslas Vélez, *Structure theorems for radical extensions of fields*, Acta Arith., to appear.
[7] A. Schinzel, *Abelian binomials, power residues and exponential congruences*, Acta Arith. 32 (1976), pp. 245–274.
[8] N. G. Tschebotarów and H. Schwerdtfeger, *Grundzüge der Galois'schen Theorie*, Groningen–Djakarta 1950.

Received on 8. 9. 1976
and in revised form on 25. 1. 1977 (892)

ACTA ARITHMETICA
XXXV (1979)

Über die simultane Darstellung zweier ganzer Zahlen durch quadratische und lineare Formen

von

A. A. Walfisz (Tbilissi)

1. Einleitung. In der vorliegenden Arbeit wird eine asymptotische Formel für die Anzahl der ganzzahligen Lösungen $r(q, n; l, m)$ des diophantischen Gleichungssystems

$$\begin{aligned} q(x_1, \ldots, x_s) &= n, \\ l(x_1, \ldots, x_s) &= m, \end{aligned} \tag{1.1}$$

bei $s \geqslant 5$ aufgestellt und untersucht. Hier ist

$$q = q(X) = q(x_1, \ldots, x_s) = \sum_{i,k=1}^{s} q_{ik} x_i x_k = X^T Q X$$

eine positiv definite ganzzahlige quadratische Form mit der symmetrischen Matrix $Q = (q_{ik})$ und der Determinate $D = \det q$; $X^T = (x_1, \ldots, x_s)$, und

$$l = l(X) = l(x_1, \ldots, x_s) = \sum_{i=1}^{s} c_i x_i = C^T X \tag{1.2}$$

ist eine ganzzahlige lineare Form; $C^T = (c_1, \ldots, c_s)$.

Ohne Beschränkung der Allgemeinheit kann man annehmen, daß die Elemente der Matrix $Q = (q_{ik})$ ganze Zahlen (1) und q, l primitive Formen sind, d.h. $\mathrm{ggT}(q_{ik}) = 1$, $\mathrm{ggT}(c_1, \ldots, c_s) = 1$.

Die Hauptergebnisse dieser Arbeit sind in dem Bericht [10] mitgeteilt.

I. M. Winogradow [13] war der erste, der die Kreismethode auf Probleme diophantischer Gleichungssysteme (sogar allgemeinere als (1.1)) angewendet hat. Er hat eine Methode für die Aufstellung und Untersuchung der asymptotischen Formeln für die Lösungszahl solcher Systeme ausge-

(1) Es ist nicht schwer unsere Ergebnisse auch auf beliebige ganze Formen q zu übertragen, d.h. auf homogene Polynome des zweiten Grades mit ganzen Koeffizienten.

arbeitet. Diese Forschungen haben K. K. Mardshanischwili [18], [19], G. W. Jemeljanow [15] und andere Autoren fortgesetzt. Die Untersuchungen über diophantische Gleichungssysteme findet man im Übersichtsartikel [21] zusammengestellt. Diese allgemeinen Untersuchungen kann man auch auf unser System (1.1) anwenden, aber die erhaltenen Abschätzungen werden weniger scharf sein, als bei der speziellen Behandlung des Systems (1.1). Diesem System ist eine ganze Reihe von Arbeiten gewidmet. Die meisten Autoren: G. Pall [7], [8], H. D. Kloosterman [6], N. G. de Bruijn [4], P. Bronkhorst [3], F. van der Blij [1], G. A. Lomadse [16] haben exakte (nicht asymptotische) Formeln für die Funktion $r(q, n; l, m)$ in verschiedenen speziellen Fällen bezüglich q und l aufgestellt. Insbesondere werden in diesen Artikeln mit verschiedenen Methoden ziemlich einfache exakte Formeln für die Lösungszahl $r_s(n, m)$ des diophantischen Gleichungssystems

$$\begin{aligned} x_1^2 + \ldots + x_s^2 &= n, \\ x_1 + \ldots + x_s &= m \end{aligned} \tag{1.3}$$

im Falle $3 \leqslant s \leqslant 8$ erhalten. In der Arbeit [14] ist es dagegen bewiesen, daß es für $s \geqslant 9$ unmöglich ist, solche Formeln herzuleiten. Die asymptotische Formel für $r_s(n, m)$ ist bei $s \geqslant 8$ in der Arbeit von A. Z. Walfisz [11] (siehe auch den Übersichtsartikel [12]) hergeleitet worden.

Wir formulieren jetzt die erhaltenen Ergebnisse, deren Beweise in 2.–4. durchgeführt werden.

Satz 1.1. *Es sei* $\operatorname{ggT}(c_1, \ldots, c_s) = 1$. *Dann läßt sich eine unimodulare ganzzahlige Transformation* V *der Veränderlichen* $X^T = (x_1, \ldots, x_s)$

$$X = VY, \quad \det V = 1, \quad Y^T = (y_1, \ldots, y_s) \tag{1.4}$$

angeben, die das System (1.1) *in ein äquivalentes System*

$$\begin{aligned} q'(y_1, \ldots, y_s) &= n, \\ l'(y_1, \ldots, y_s) &= y_s = m \end{aligned} \tag{1.5}$$

überführt, wobei $q' = q'(Y) = q(VY)$ *die zu* q *äquivalente quadratische Form ist mit der Matrix* $Q' = V^T Q V$, $\det q' = \det q = D$. *Außerdem sind* $l' = l'(Y) = c_1' y_1 + \ldots + c_s' y_s$, $c_1' = \ldots = c_{s-1}' = 0$, $c_s' = 1$.

2. *Es seien*

$$\bar{q}' = \sum_{i,k=1}^{s} \bar{q}_{ik}' y_i y_k \tag{1.6}$$

die zu q' *adjungierte Form, d.h.* $\bar{q}_{ik}'$ *ist die Adjunkte von* q_{ik}', *und*

$$\Delta_k = \bar{q}_{sk}' \ (k = 1, \ldots, s), \quad \Delta = \Delta_s, \quad N = \Delta n - D m^2. \tag{1.7}$$

Weiter möge

$$\varphi(y_1, \ldots, y_{s-1}) = q'(y_1, \ldots, y_{s-1}, 0) \tag{1.8}$$

eine positiv definite quadratische Form mit der Determinante Δ *sein. Dann kann man jeder ganzzahligen Lösung* $X^T = (x_1, \ldots, x_s)$ *des Systems* (1.1) *eineindeutig eine ganzzahlige Lösung* $Z^T = (z_1, \ldots, z_{s-1})$ *des diophantischen Problems*

$$\begin{aligned} \varphi(Z) &= \Delta N, \\ Z^T &\equiv -m\,\theta^T \pmod{\Delta} \end{aligned} \tag{1.9}$$

zuordnen, $\theta^T = (\Delta_1, \ldots, \Delta_{s-1})$. *Insbesondere haben wir*

$$r(q, n; l, m) = r(\varphi, \Delta N; \Delta; -m\Delta_1, \ldots, -m\Delta_{s-1}). \tag{1.10}$$

Hier bezeichnet $r(\varphi, \Delta N; \Delta; -m\Delta_1, \ldots, -m\Delta_{s-1})$ *die Lösungszahl des Systems* (1.9), *und es gilt*

$$\Delta = \bar{q}(c_1, \ldots, c_s) = \bar{q}(C), \tag{1.11}$$

wobei $\bar{q}$ *die zu* q *adjungierte Form und* c_i *die Koeffizienten der Form* (1.2) *sind.*

Wir haben damit unser Problem auf das Problem der Darstellungen (aus gegebener Restklasse) der Zahlen durch eine spezielle quadratische Form von $(s-1)$ Veränderlichen zurückgeführt. Das wird uns die Möglichkeit geben, für die Herleitung der gewünschten asymptotischen Formel für $r(q, n; l, m)$ die Ergebnisse von A. W. Malyschew [20], Kap. III zu verwenden. Der Beweis des Satzes 1 wird in 2. durchgeführt, wo auch die Gestalt von V, φ, $\Delta_1, \ldots, \Delta_{s-1}$ in dem Falle angegeben wird, daß einer der Koeffizienten c_i der Form l gleich 1 ist. Zu Satz 1 ähnliche Ergebnisse kann man in den Arbeiten [1], [2], [7] finden.

Wie für exakte, so spielt auch für asymptotische Formeln die Berechnung und Abschätzung der dem Problem (1.1) entsprechenden singulären Reihe $H(q, n; l, m)$ eine wichtige Rolle. Man kann sie folgendermassen definieren:

$$H(q, n; l, m) = \prod_p \chi_p(q, n; l, m), \tag{1.12}$$

wobei das unendliche Produkt über alle Primzahlen p erstreckt wird. Hier ist

$$\chi_p(q, n; l, m) = \lim_{t \to \infty} p^{-(s-2)t} \varrho(p^t; q, n; l, m), \tag{1.13}$$

und $\varrho(p^t; q, n; l, m)$ bezeichnet die Lösungszahl des Kongruenzsystems

$$\left.\begin{aligned} q(x_1, \ldots, x_s) &\equiv n \\ l(x_1, \ldots, x_s) &\equiv m \end{aligned}\right\} \pmod{p^t}. \tag{1.14}$$

Die Folge (1.13) stabilisiert sich für große t, und der Limes existiert.

Für $s \geqslant 5$ man kann auch eine andere äquivalente Definition der singulären Reihe $H(q, n; l, m)$ angeben, und zwar

$$H(q, n; l, m) = \sum_{a=1}^{\infty}\sum_{b=1}^{\infty}(ab)^{-s}\sum_{h \bmod a}'\sum_{d \bmod b}' S(hq, a; dl, b)e\left(-\frac{nh}{a}-\frac{md}{b}\right),$$

wobei in den inneren Summen h ein reduziertes Restsystem modulo a und d ein solches modulo b durchlaufen, $e(y) = e^{2\pi i y}$, hierbei ist $S(hq, a; dl, b)$ die bekannte Gauss'sche Summe:

$$S(hq, a; dl, b) = \sum_{x_1,\dots,x_s=1}^{ab} e\left(\frac{h}{a}q(x_1, \dots, x_s)+\frac{d}{b}l(x_1, \dots, x_s)\right).$$

Den speziellen Fall der Funktion $H(q, n; l, m)$, nämlich die dem Problem (1.3) entsprechende singuläre Reihe $H_s(n, m)$, haben H. D. Kloosterman [6], P. Bronkhorst [3], A. Z. Walfisz [11], [12] und G. A. Lomadse [17] behandelt. In dem letzteren Artikel ist die Reihe $H_s(n, m)$ für alle $s \geqslant 3$ berechnet.

Die singuläre Reihe $H(\varphi, \Delta N; \Delta; -m\Delta_1, \dots, -m\Delta_{s-1})$ des Problems (1.9) definieren wir ähnlich, und zwar durch

$$H(\varphi, \Delta N; \Delta; -m\Delta_1, \dots, -m\Delta_{s-1}) = \prod_p \chi_p(\varphi, \Delta N; \Delta; -m\Delta_1, \dots, -m\Delta_{s-1}), \tag{1.15}$$

wobei

$$\chi_p(\varphi, \Delta N; \Delta; -m\Delta_1, \dots, -m\Delta_{s-1}) = \lim_{t\to\infty} p^{-(s-2)t}\varrho\left(p^t \mid \varphi(Z) \equiv \Delta N \pmod{p^t},\ Z^T \equiv -m\theta^T \pmod{p^{u_p}}\right). \tag{1.16}$$

Hier bedeuten $\varrho(p^t|\dots)$ — die Anzahl der verschiedenen $(\bmod p^t)$ ganzzahligen Vektoren $Z^T = (z_1, \dots, z_{s-1})$, die den vorgeschriebenen Bedingungen genügen, und p^{u_p} — die höchste in Δ aufgehende Potenz von p, $p^{u_p}\|\Delta$; $\theta^T = (\Delta_1, \dots, \Delta_{s-1})$.

Der folgende Satz gibt eine Abschätzung von unten für die Funktion $H(q, n; l, m)$.

Satz 2. 1. *Es gilt die Identität*

$$H(q, n; l, m) = \Delta^{s-3}H(\varphi, \Delta N; \Delta; -m\Delta_1, \dots, -m\Delta_{s-1}). \tag{1.17}$$

2. $\mathfrak{P}_\varphi$ *bezeichne die Menge der herabsetzender* (2) *Primzahlen* p *der Form* φ. *Es sei weiter*

$$L = \Delta(n - q'_{ss}m^2), \quad p^{\delta_p}\|8\Delta^2 L. \tag{1.18}$$

(2) Die Definition siehe in [20], S. 72. Wenn $s-1 > 5$ ist, so gibt es solche Zahlen nicht; wenn $s-1 = 4$ und $p \in \mathfrak{P}_\varphi$, so muß $p|2\Delta$.

Ist dann $s \geqslant 5$ *und das Kongruenzsystem*

$$q(x_1, \dots, x_s) \equiv n \pmod{8L}, \quad l(x_1, \dots, x_s) \equiv m \pmod{\Delta} \tag{1.19}$$

lösbar, so folgt

$$H(q, n; l, m) \gg N^{-\varepsilon}\prod_{\mathfrak{P}_\varphi} p^{-\delta_p(s-3)/2}, \tag{1.20}$$

wobei die im Symbol $\gg$ *auftretenden Konstanten nur von* q, l *und einer beliebigen reellen Zahl* $\varepsilon > 0$ *abhängen.*

Der Satz 2 wird in 3. bewiesen. Wir bemerken, daß die Formel (1.17) (und die entsprechende Formel (3.2) in 3. für die $\chi_p(q, n; l, m)$) es uns erlauben, unter Benutzung der Ergebnisse des § 2, Kap. III von [20] die singuläre Reihe des Problems (1.1) auszurechnen. Insbesondere kann man die Formeln von G. A. Lomadse [17] auf diesem Wege bekommen. Wir möchten auch darauf hinweisen, daß sich die singuläre Reihe mit Hilfe der allgemeinen Abschätzungen von E. W. Podsypanin [22] untersuchen läßt.

Schließlich enthält der Satz 3 die von uns aufgestellte asymptotische Formel.

Satz 3. *Es seien* $r(q, n; l, m)$ — *die Anzahl der ganzzahligen Lösungen des diophantischen Gleichungssystems* (1.1), $H(q, n; l, m)$ *die singuläre Reihe* (1.12) *desselben Problems und* $D = \det q$, $\Delta = \bar{q}(c_1, \dots, c_s)$, $N = \Delta n - Dm^2$. *Sei* $s \geqslant 5$. *Dann gilt bei* $N \to \infty$

$$r(q, n; l, m) = \frac{\pi^{(s-1)/2}N^{(s-3)/2}}{\Delta^{s/2-1}\Gamma\left((s-1)/2\right)}H(q, n; l, m)+O(N^{s/4-1/2+\varepsilon}), \tag{1.21}$$

wobei die im Symbol O *auftretenden Konstanten nur von* q, l *und einer beliebigen reellen Zahl* $\varepsilon > 0$ *abhängen.*

Der Satz 3 wird in 4. bewiesen. Die Formel (1.21) ist für $s \geqslant 5$ gültig. Für $s \leqslant 3$ sind kaum irgendwelche gute asymptotischen Formeln möglich. Im Grenzfall $s = 4$ kann man die auf Grund der ergodischen Methode von Linnik durchgeführten Untersuchungen der Kap. V und VI von [20] anwenden. In diesem Falle, wenn φ (siehe Satz 1) eine primitive Form der ungeraden eineindeutig Priminvarianten ist, dann kann man für $r(q, n; l, m)$ eine Abschätzung von unten angeben (siehe [20], Kap. V). Wenn φ dabei als Summe von drei Quadraten ganzzahliger linearen Formen darstellbar ist, so läßt sich für $r(q, n; l, m)$ auch eine asymptotische Formel erhalten (ibid. Kap. VI).

Aus den Sätzen 2 und 3 erhält man sofort die Lösbarkeitsbedingungen des Systems (1.1) bei hinreichend großen $N = \Delta n - Dm^2$. Insbesondere gilt die

FOLGERUNG. *Es sei $s \geqslant 6$ oder $s = 5$, aber alle Primteiler p von 2Δ gehen in $L = \Delta(n - q'_{ss}m^2)$ in begrenzten Potenzen auf. Ist dann das Kongruenzsystem* (1.19) *lösbar, so ist für hinreichend große $N = \Delta n - Dm^2$ auch das diophantische Gleichungssystem* (1.1) *lösbar. Ist dagegen das System* (1.19) *nicht lösbar, so ist das System* (1.1) *auch nicht lösbar.*

Schließlich bemerken wir, daß es ebenfalls möglich wäre, unser Problem (1.1), statt auf das Problem (1.9), auf das Problem der Lösungszahlen der inhomogenen quadratischen Gleichung

$$\varphi(x_1, \ldots, x_{s-1}) + b_1 x_1 + \ldots + b_{s-1}x_{s-1} = M \tag{1.22}$$

zurückzuführen, wobei φ — eine geeignete positiv definite quadratische Form ist. Im Falle $s-1 \geqslant 5$ hat G. L. Watson [9] eine asymptotische Formel für die Lösungszahl der Gleichung (1.22) aufgestellt. Die in [20] entwickelten Methoden erlauben auch den Fall $s-1 = 4$ der Gleichung (1.22) zu untersuchen.

2. Die Zurückführung des Problems der simultanen Darstellung auf das Problem der Darstellungen der Zahlen durch eine geeignete quadratische Form. Beweis des Satzes 1

HILFSSATZ 1. *Es seien $c_1 = \ldots = c_{s-1} = 0$, $c_s = 1$, so daß das System* (1.1) *die Gestalt*

$$\begin{aligned} q(x_1, \ldots, x_s) &= n, \\ x_s &= m \end{aligned} \tag{2.1}$$

hat, wobei q eine positiv definite ganzzahlige quadratische Form mit der Matrix $Q = (q_{ik})$ und der Determinante $D = \det q$ ist.

Es seien

$$\Delta_k = \bar{q}_{sk} \quad (k = 1, \ldots, s) \tag{2.2}$$

die Adjunkte von q_{sk} und

$$N = \Delta n - Dm^2. \tag{2.3}$$

Weiter möge

$$\varphi(x_1, \ldots, x_{s-1}) = q(x_1, \ldots, x_{s-1}, 0) \tag{2.4}$$

eine positiv definite quadratische Form mit der Determinante $\Delta = \Delta_s$ sein. Die Beziehungen

$$z_k = \Delta x_k - m\Delta_k \quad (k = 1, \ldots, s-1) \tag{2.5}$$

ordnen jeder ganzzahligen Lösung $X^T = (x_1, \ldots, x_s)$ des Systems (2.1) *eineindeutig eine ganzzahlige Lösung $Z^T = (z_1, \ldots, z_{s-1})$ des diophantischen Problems*

$$\varphi(Z) = \Delta N, \qquad Z^T \equiv -m\theta^T (\mathrm{mod}\,\Delta) \tag{2.6}$$

zu; $\theta^T = (\Delta_1, \ldots, \Delta_{s-1})$.

Beweis. Das System (2.1) ist äquivalent der inhomogenen quadratischen Gleichung

$$q(x_1, \ldots, x_{s-1}, m) = n. \tag{2.7}$$

Im Raum $\boldsymbol{R}^{s-1} = \{(x_1, \ldots, x_{s-1})\}$ ist die Menge der reellen Punkte $(x_1, \ldots, x_{s-1})$, die der Gleichung (2.7) genügen, entweder leer oder stellt ein Ellipsoid mit Zentrum $(x_1^0, \ldots, x_{s-1}^0)$ dar. Die Zahlen $x_1^0, \ldots, x_{s-1}^0$ müssen dann dem System

$$\sum_{k=1}^{s-1} q_{ik}x_k^0 + q_{is}m = 0 \quad (i = 1, \ldots, s-1) \tag{2.8}$$

mit der Determinante $\Delta > 0$ genügen, woraus sich nach der Kramerschen Formel die Werte

$$x_k = m\Delta_k/\Delta \quad (k = 1, \ldots, s-1)$$

ergeben. Berücksichtigt man weiter, daß

$$q(\Delta_1, \ldots, \Delta_{s-1}, \Delta) = \sum_{i=1}^{s} \Delta_i \sum_{k=1}^{s} q_{ik}\Delta_k = \Delta_s \sum_{k=1}^{s} q_{sk}\Delta_k = \Delta D$$

ist, so erhält man nach der Substitution

$$x_k = x'_k + x_k^0 \quad (k = 1, \ldots, s-1)$$

folgenden Ausdruck

$$\begin{aligned} &q(x_1, \ldots, x_{s-1}, m) \\ &= q(x'_1, \ldots, x'_{s-1}, 0) + q(x_1^0, \ldots, x_{s-1}^0, m) + 2q(x'_1, \ldots, x'_{s-1}, 0; x_1^0, \ldots, x_{s-1}^0, m) \\ &= q(x_1 - m\Delta_1/\Delta, \ldots, x_{s-1} - m\Delta_{s-1}/\Delta, 0) + q(m\Delta_1/\Delta, \ldots, m\Delta_{s-1}/\Delta, m) \\ &= \varphi(x_1 - m\Delta_1/\Delta, \ldots, x_{s-1} - m\Delta_{s-1}/\Delta) + m^2 D/\Delta, \end{aligned} \tag{2.9}$$

da die bilineare Form $q(x'_1, \ldots, x'_{s-1}, 0; x_1^0, \ldots, x_{s-1}^0, m)$ nach (2.8) verschwindet. Die Gleichung (2.7) nimmt wegen (2.9) und (2.3) folgende Gestalt an

$$\varphi(\Delta x_1 - m\Delta_1, \ldots, \Delta x_{s-1} - m\Delta_{s-1}) = \Delta N. \tag{2.10}$$

Die Gleichung (2.10) ist aber dem Problem (2.6) äquivalent, und die Beziehungen (2.5) liefern die eineindeutige Zuordnung zwischen den Lösungen von (2.1) und (2.6). Damit ist der Hilfssatz 1 bewiesen.

HILFSSATZ 2. *Es sei* $\mathrm{ggT}(c_1, \dots, c_s) = 1$. *Wir wählen* [3] *eine unimodulare ganzzahlige Matrix*

$$U = (u_{ik}) \quad (i, k = 1, \dots, s) \tag{2.11}$$

mit

$$u_{sk} = c_k \quad (k = 1, \dots, s), \tag{2.12}$$

und es sei $V = (v_{ik}) = U^{-1}$. *Es sei weiter* $q' = q'(Y) = q(VY)$ *die zu* q *äquivalente quadratische Form mit der Matrix* $Q' = V^T Q V$.

Das System (1.1) *ist dann dem diophantischen Gleichungssystem*

$$\begin{aligned} q'(y_1, \dots, y_s) &= n, \\ y_s &= m \end{aligned} \tag{2.13}$$

äquivalent, und die eineindeutige Zuordnung zwischen den Lösungen von (1.1 *und* (2.13) *ergibt sich mittels der Beziehung*

$$X = VY. \tag{2.14}$$

Dabei hängt die Adjunkte $\Delta'_k = \bar{q}'_{sk}$ $(k = 1, \dots, s)$ *des Elementes* q'_{sk} $(k = 1, \dots, s)$ *der Matrix* Q' *nur von* q *und* l *(und nicht von* n *und* m *ab); und insbesondere gilt*

$$\Delta' = \Delta'_s = \bar{q}(c_1, \dots, c_s) = \bar{q}(C), \tag{2.15}$$

wobei $\bar{q}$ *die zu* q *adjungierte Form ist.*

Beweis. Alle Behauptungen des Hilfssatzes 2, außer (2.15), lassen sich unmittelbar nachprüfen. Daher werden wir nur (2.15) beweisen. Nach Definition gilt

$$\Delta' = \bar{q}'(C') = \bar{q}'(0, \dots, 0, 1). \tag{2.16}$$

Weiter ist die Größe $\bar{q}(c_1, \dots, c_s)$ eine Invariante des Systems (1.1) bezüglich der linearen Transformation der Veränderlichen $X^T = (x_1, \dots, x_s)$. Denn wenn $X = WX_0$ ist, so haben wir

$$\begin{aligned} q'(X_0) = X_0^T Q' X_0 = q(WX_0), \quad Q' &= W^T Q W, \\ l'(X_0) = C'^T X_0 = l(WX_0), \quad C'^T &= C^T W, \end{aligned}$$

woraus

$$\bar{q}(C) = DC^T Q^{-1} C = DC'^T (Q')^{-1} C' = \bar{q}'(C')$$

folgt. Hieraus erhalten wir insbesondere für $W = V$ nach (2.16) die Beziehung (2.15). Der Hilfssatz 2 ist damit bewiesen.

Der Satz 1 folgt jetzt unmittelbar aus den Hilfssätzen 1 und 2.

---

[3] Daß ist immer möglich, siehe z.B. bei B. W. Jones [5], S. 62.

Wenn die Koeffizienten $c_1, \dots, c_s$ der Form l vorgegeben sind, ist es nicht schwer, die unimodulare ganzzahlige Matrix V herzuleiten, die das System (1.1) in das System (2.13) überführt. In dem Falle, daß einer der Koeffizienten c_k gleich ± 1 ist, sind die Matrix V, die Form φ und die Größen Δ_k $(k = 1, \dots, s-1)$ besonders leicht darstellbar.

Bemerkung. Sei $c_s = 1$ und

$$V = \begin{pmatrix} E & 0 \\ -B^T & 1 \end{pmatrix}, \tag{2.17}$$

wobei hier E die $(s-1)\times(s-1)$ — Einheitsmatrix, 0 — die Nullmatrix der Dimension $(s-1)\times 1$ und $B^T = (c_1, \dots, c_{s-1})$ sind. Wenn dann

$$q'(Y) = q(VY) = \sum_{i,k=1}^{s} q'_{ik} y_i y_k \tag{2.18}$$

ist, so haben wir

$$\begin{aligned} q'_{ik} &= q_{ik} - c_s c_k q_{is} - c_s c_i q_{ks} + c_i c_k q_{ss} \quad (i, k = 1, \dots, s-1), \\ q'_{is} &= c_s q_{is} - c_i q_{ss} \quad (i = 1, \dots, s-1), \\ q'_{ss} &= q_{ss}; \end{aligned} \tag{2.19}$$

$$\Delta_k = \sum_{i=1}^{s} c_i \bar{q}_{ik} = \bar{q}(c_1, \dots, c_{s-1}; 0, \dots, 0, \underset{(k)}{1}, 0, \dots, 0) \quad (k = 1, \dots, s-1). \tag{2.20}$$

Beweis. Die den Formen q und q' entsprechenden Matrizen Q und Q' schreiben wir in der folgenden Gestalt

$$Q = \begin{pmatrix} \Phi & F \\ F^T & q_{ss} \end{pmatrix}, \quad Q' = \begin{pmatrix} \Phi' & F' \\ F'^T & q'_{ss} \end{pmatrix},$$

wobei Φ' die Matrix der Form φ ist, $F'^T = (q'_{s1}, \dots, q'_{s,s-1})$. Dann kann man die Matrizengleichung

$$Q' = V^T Q V \tag{2.21}$$

wegen (2.17) in der Form

$$\begin{pmatrix} \Phi' & F' \\ F'^T & q'_{ss} \end{pmatrix} = \begin{pmatrix} \Phi - FB^T - BF^T + q_{ss} BB^T & F - q_{ss} B \\ F^T - q_{ss} B^T & q_{ss} \end{pmatrix} \tag{2.22}$$

schreiben. (2.22) ist äquivalent den Beziehungen (2.19).

Wir beweisen jetzt (2.20). Aus (2.17) und (2.21) schließen wir

$$U = V^{-1} = \begin{pmatrix} E & 0 \\ B^T & 1 \end{pmatrix}, \quad \bar{Q}' = V^{-1} \bar{Q} (V^{-1})^T = U \bar{Q} U^T,$$

$$\bar{Q}' = \begin{pmatrix} E & 0 \\ B^T & 1 \end{pmatrix} \begin{pmatrix} A & G \\ G^T & \bar{q}_{ss} \end{pmatrix} \begin{pmatrix} E & B \\ 0^T & 1 \end{pmatrix} = \begin{pmatrix} A & AB + G \\ B^T A + G^T & \bar{q}(c_1, \dots, c_s) \end{pmatrix}, \tag{2.23}$$

wobei

$$G^T = (\bar{q}_{s1}, \dots, \bar{q}_{s,s-1}), \qquad A = \begin{pmatrix} \bar{q}_{11} & \cdots & \bar{q}_{1,s-1} \\ \cdots & \cdots & \cdots \\ \bar{q}_{s-1,1} & \cdots & \bar{q}_{s-1,s-1} \end{pmatrix}.$$

(2.23) führt zu den Formeln (2.20), womit die Bemerkung bewiesen ist.

3. Die Untersuchung der singulären Reihe. Beweis des Satzes 2

HILFSSATZ 3. *Es gilt die Identität*

$$H(q, n; l, m) = \Delta^{s-3} H(\varphi, \Delta N; \Delta; -m\Delta_1, \dots, -m\Delta_{s-1}). \tag{3.1}$$

Beweis. Es sei $p^{u_p} \| \Delta$. Man hat (siehe [20], S. 70 und auch die Beweise unserer Hilfssätze 1 und 2) für $t \geqslant 2u_p$, $t - 2u_p = t'$

$$\begin{aligned} &p^{-(s-2)t} \varrho\left(p^t | \varphi(Z) \equiv \Delta N (\mathrm{mod}\, p^t),\ Z^T \equiv -m\theta^T (\mathrm{mod}\, p^{u_p})\right) \\ &= p^{-(s-2)t-(s-1)u_p} \varrho\left(p^t | \varphi(p^{u_p} y_1 - m\Delta_1, \dots, p^{u_p} y_{s-1} - m\Delta_{s-1}) \equiv \Delta N (\mathrm{mod}\, p^t)\right) \\ &= p^{-(s-2)t-(s-1)u_p} \varrho\left(p^t | \Delta^2 q'(y_1, \dots, y_{s-1}, m) \equiv \Delta^2 n (\mathrm{mod}\, p^t)\right) \\ &= p^{(s-1)u_p-(s-2)t} \varrho\left(p^{t-2u_p} | q'(y_1, \dots, y_{s-1}, m) \equiv n (\mathrm{mod}\, p^{t-2u_p})\right) \\ &= p^{-(s-3)u_p-(s-2)t'} \varrho(p^{t'}; q', n; l', m) = p^{-(s-3)u_p} p^{-(s-2)t'} \varrho(p^{t'}; q, n; l, m). \end{aligned}$$

Strebt hier t (und damit auch $t' = t - 2u_p$) gegen Unendlich, so bekommt man wegen (1.13) und (1.16)

$$\chi_p(q, n; l, m) = p^{(s-3)u_p} \chi_p(\varphi, \Delta N; \Delta; -m\Delta_1, \dots, -m\Delta_{s-1}). \tag{3.2}$$

Der Hilfssatz 3 folgt jetzt aus (3.2), (1.12) und (1.15).

Nach Definition der Funktion $\varphi(x_1, \dots, x_{s-1})$ gilt

$$\begin{aligned} \varphi(\Delta_1, \dots, \Delta_{s-1}) &= \sum_{i,k=1}^{s-1} q'_{ik} \Delta_i \Delta_k = \sum_{i=1}^{s} \Delta_i \sum_{k=1}^{s} q'_{ik} \Delta_k + q'_{ss} \Delta^2 - 2\Delta \sum_{i=1}^{s} q'_{si} \Delta_i \\ &= q'_{ss} \Delta^2 - \Delta D = \Delta (q'_{ss} \Delta - D), \end{aligned}$$

und deshalb

$$\begin{aligned} \Delta N - \varphi(-m\Delta_1, \dots, -m\Delta_{s-1}) &= \Delta (\Delta n - D m^2) - m^2 \Delta (q'_{ss} \Delta - D) \\ &= \Delta L, \end{aligned} \tag{3.3}$$

wobei L durch die Formel (1.18) definiert ist.

HILFSSATZ 4. *Es seien $p^{u_p} \| \Delta$, $p^{w_p} \| \Delta L$, $t_p = w_p + 2 + (-1)^p$, $S_p = \mathrm{Max}(t_p, u_p)$ und $H(\varphi, \Delta N; \Delta; -m\Delta_1, \dots, -m\Delta_{s-1})$ die singuläre Reihe (1.15) des Problems (1.9). Weiter bezeichne $\mathfrak{P}_\varphi$ die Menge der herabsetzenden Primzahlen p der Form φ. Ist dann $s \geqslant 5$ und für jeden Primteiler p von 2Δ das Kongruenzsystem*

$$\begin{aligned} \varphi(Z) &\equiv \Delta N (\mathrm{mod}\, p^{S_p}), \\ Z^T &\equiv -m\theta^T (\mathrm{mod}\, p^{u_p}) \end{aligned} \tag{3.4}$$

lösbar, so gilt

$$H(\varphi, \Delta N; \Delta; -m\Delta_1, \dots, -m\Delta_{s-1}) \gg N^{-\varepsilon} \prod_{p \in \mathfrak{P}_\varphi} p^{-t_p(s-3)/2}, \tag{3.5}$$

wobei die im Symbol $\gg$ auftretenden Konstanten nur von Δ und einer beliebigen reellen Zahl $\varepsilon > 0$ abhängen.

Beweis. Siehe [20], Kap. III, Bemerkung 7. Um diese Bemerkung anzuwenden, bemerken wir, daß $t_p \geqslant T_p$ ist.

Es sei weiter die notwendige Bedingung

$$\varphi(-m\Delta_1, \dots, -m\Delta_{s-1}) \equiv \Delta N (\mathrm{mod}\, \Delta)$$

der Lösbarkeit des Systems (1.9) erfüllt. Dann hat man nach (3.3) $u_p \leqslant w_p$, und daher

$$S_p = t_p = \begin{cases} w_p + 1, & p > 2, \\ w_p + 3, & p = 2. \end{cases} \tag{3.6}$$

Hieraus folgt, daß das Kongruenzsystem (3.4) für jedes $p | 2\Delta$ lösbar ist, wenn das Kongruenzsystem

$$\begin{aligned} \varphi(Z) &\equiv \Delta N (\mathrm{mod}\, 8\Delta^2 L), \\ Z^T &\equiv -m\theta^T (\mathrm{mod}\, \Delta) \end{aligned} \tag{3.7}$$

lösbar ist.

HILFSSATZ 5. *Es seien $L = \Delta(n - q'_{ss} m^2)$, $p^{\delta_p} \| 8\Delta^2 L$, $H(q, n; l, m)$ die singuläre Reihe (1.12) des Problems (1.1) und $\mathfrak{P}_\varphi$ die Menge der herabsetzenden Primzahlen p der Form φ. Ist dann $s \geqslant 5$ und das Kongruenzsystem*

$$\begin{aligned} q(x_1, \dots, x_s) &\equiv n (\mathrm{mod}\, 8L), \\ l(x_1, \dots, x_s) &\equiv m (\mathrm{mod}\, \Delta) \end{aligned} \tag{3.8}$$

lösbar, so ist die Abschätzung

$$H(q, n; l, m) \gg N^{-\varepsilon} \prod_{p \in \mathfrak{P}_\varphi} p^{-\delta_p(s-3)/2} \tag{3.9}$$

gültig, wobei die im Symbol $\gg$ auftretenden Konstanten nur von q, l und einer beliebigen reellen Zahl $\varepsilon > 0$ abhängen.

Beweis. Wegen $\Delta | L$ ist das System (3.8) dem (3.7) äquivalent. Da weiter das System (3.8) lösbar ist, so gilt das auch für (3.7), und daher ist (3.4) für jedes $p | 2\Delta$ lösbar. Nach Hilfssatz 4 gilt dann die Abschätzung (3.5). Wegen (3.6), (1.18) und der Definition von w_p bekommt man $t_p \leqslant \delta_p$. Der Hilfssatz 5 folgt jetzt aus der Abschätzung (3.5), wenn man die Beziehungen (1.17) und (1.11) berücksichtigt.

Der Satz 2 ist eine unmittelbare Folgerung der Hilfssätze 3 und 5.

4. Asymptotische Formel. Beweis des Satzes 3

HILFSSATZ 6. *Es seien* $r(\varphi, \Delta N; \Delta; -m\Delta_1, \dots, -m\Delta_{s-1})$ *die Anzahl der ganzzahligen Lösungen des diophantischen Gleichungssystems* (1.9) *und* $H(\varphi, \Delta N; \Delta; -m\Delta_1, \dots, -m\Delta_{s-1})$ *die singuläre Reihe* (1.15) *desselben Problems. Sei* $s \geqslant 5$. *Dann gilt für* $N \to \infty$

$$(4.1)\quad r(\varphi, \Delta N; \Delta; -m\Delta_1, \dots, -m\Delta_{s-1}) = \frac{\pi^{(s-1)/2} N^{(s-3)/2}}{\Delta^{-s/2+2}\Gamma((s-1)/2)} H(\varphi, \Delta N; \Delta; -m\Delta_1, \dots, -m\Delta_{s-1}) + O(N^{s/4-1/2+\varepsilon}).$$

Hierbei hängen die im Symbol O auftretenden Konstanten nur von Δ *und einer beliebigen reellen Zahl* $\varepsilon > 0$ *ab.*

Beweis. Siehe [20], Kap. III, Satz 2.

Der Satz 3 folgt aus dem Hilfssatz 6, wenn man die Beziehungen (1.10), (1.17) und (1.11) berücksichtiht.

Literaturverzeichnis

[1] F. van der Blij, *On the theory of simultaneous linear and quadratic representation, I–V*, Proc. Kon. Ned. Akad. Wet. 50 (1947), S. 31–40, 41–48, 166–172, 298–306, 390–396 = Indag. math. 9 (1947), S. 16–25, 26–33, 129–135, 188–196, 248–254,

[2] — *Simultaneous representation of integers by a quadratic and a linear form*. Nieuw Arch. Wisk. (3) 7 (1959), S. 109–114.

[3] P. Bronkhorst, *Over het aantal oplossingen van het stelsel Diophantische vergelijkingen* $x_1^2+x_2^2+\dots+x_s^2=n$, $x_1+x_2+\dots+x_s=m$ *voor* $s=6$ *en* $s=8$, Diss., Groningen 1943.

[4] N. G. de Bruijn, *Over het aantal oplossingen van het stelsel* $x_1^2+x_2^2+x_3^2=n$, $x_1+x_2+x_3=m$, Nieuw Arch. Wisk. (2) 22 (1943), S. 53–56.

[5] B. W. Jones, *The arithmetic theory of quadratic forms*, Baltimore 1950.

[6] H. D. Kloosterman, *Simultane Darstellung zweier ganzen Zahlen als einer Summe von ganzen Zahlen und deren Quadratsumme*, Math. Ann. 118 (1942), S. 319–364.

[7] G. Pall, *Simultaneous quadratic and linear representations*, Quart. J. Math. 2 (1931), S. 136–143.

[8] — *Simultaneous representation in a quadratic and linear form*, Duke **Math.** J. 8 (1941), S. 173–180.

[9] G. L. Watson, *Quadratic Diophantine equations*, Phil. Trans. Roy. Soc. **London** A 253 (1960), S. 227–254.

[10] А. А. Вальфиш, *Об одновременном представлении двух целых чисел линейной и квадратичной формами*, Сообщ. Акад. Наук ГССР 82 (1976), S. 305–308.

[11] А. З. Вальфиш, *Аддитивная теория чисел, XI*, Труды Тбилисского матем. ин-та 19 (1952), S. 33–59.

[12] — *О представлении чисел суммами квадратов. Асимптотические формулы*, Успехи матем. наук 7 (1952), № 6 (52), S. 97–178. Engl. Übers.: *On the representation of numbers by sums of squares. Asymptotic formulas*, Transl. Amer. Math. Soc. ser. 2, 3 (1956), S. 163–248.

[13] И. М. Виноградов, *Об одном классе совокупных диофантовых уравнений*, Изв. АН СССР, отд. физ.- мат. наук (1929), S. 355–376 = Избранные труды, Москва 1952, S. 151–168.

[14] А. Б. Воронецкий, А. В. Малышев, *Об одновременном представлении пары чисел суммами целых чисел и их квадратов*, Труды МИАН 142 (1976), S. 122–134.

[15] Г. В. Емельянов, *Об одной системе диофантовых уравнений*, Ученые записки Ленинград. ун-та, сер. матем. 19 (1950), S. 3–39.

[16] Г. А. Ломадзе, *Об одновременном представлении двух целых чисел суммами целых чисел и их квадратов*, Труды Тбилисского матем. ин-та 18 (1950), S. 153–181.

[17] — *О суммировании одного сингулярного ряда, I-II*, ibid.19 (1953), S. 61–77; 20(1954), S. 21–45.

[18] К. К. Марджанишвили, *Об одновременном представлении n чисел суммами полных первых, вторых, ..., n-ых степеней*, Изв. АН СССР, сер. матем. 1 (1937), S. 609–631.

[19] — *О некоторых нелинейных системах уравнений в целых числах*, Матем. сб. 33 (75) (1953), S. 639–675.

[20] А. В. Малышев, *О представлении целых чисел положительными квадратичными формами*, Труды МИАН 65, Москва–Ленинград 1962.

[21] А. В. Малышев, Е. В. Подсыпанин, *Аналитические методы в теории систем диофантовых уравнений и неравенств с большим числом неизвестных*, ИНТ Алгебра, топология, геометрия 12 (1974), S. 5–50.

[22] Е. В. Подсыпанин, *О сингулярном ряде в задаче представления системы чисел системами форм*, Записки научн. семин. ЛОМИ 50 (1975), S. 130–136.

MATHEMATISCHES INSTITUT DER AKADEMIE DER WISSENSCHAFTEN
Tbilissi, UdSSR

Eingegangen am 29. 12. 1976 (907)