STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1959 - 015

Voordracht in de serie "Actualiteiten"

Dr. C.G. Lekkerkerker

31 oktober 1959

Indefiniete binaire kwadratische vormen

MC
1959

Voordracht in de serie "Actualiteiten"

door

Dr C.G. Lekkerkerker

31 oktober 1959

Indefiniete binaire kwadratische vormen

1. In het volgende zijn $a, b, x, y, z, x^n, \ldots$ punten van R_2 en $u, v, \ldots$ punten met gehele coördinaten. Zij Y het rooster der punten u. We gebruiken vectoriële schrijfwijze. We beschouwen indefiniete vormen

$$Q(x) = \alpha x_1^2 + \beta x_1 x_2 + \gamma x_2^2 \quad (\alpha, \beta, \gamma \text{ reëel});$$

ze zijn (niet eenduidig) te schrijven als een product van lineaire vormen

(1) $$Q(x) = L_1(x)\, L_2(x) = (a_{11}x_1 + a_{12}x_2)(a_{21}x_1 + a_{22}x_2)$$

en hebben discriminant

$$\delta = \delta(Q) = \beta^2 - 4\alpha\gamma = \{\det(a_{ij})\}^2 \geqq 0.$$

We onderstellen steeds dat $\delta > 0$.

In deze voordracht houden we ons uitsluitend bezig met het z.g. inhomogene minimum $\mu(Q)$, gedefinieerd door

(2) $$\mu(Q) = \sup_z \mu(Q;z), \text{ waarin } \mu(Q;z) = \inf_u |Q(u-z)| .$$

Ruw gezegd is $\sqrt{\mu(Q)}$ de "maximale" afstand van een punt van het vlak tot het "dichtstbijzijnde" roosterpunt, alles gemeten in de afstandsfunctie $\sqrt{|Q(x)|}$. Een andere meetkundige beschrijving krijgen we als volgt.

Ga uit van een splitsing (1), zet $(a_{ij}) = A$ en beschouw het rooster $\Lambda = AY$ der punten

(3) $$Au = (a_{11}u_1 + a_{12}u_2,\ a_{21}u_1 + a_{22}u_2).$$

Zet verder $-Az = y$ en beschouw het "inhomogene" rooster (grid)

(4) $$\Gamma = \Lambda + y = \{Au + y\}, \text{ met determinant } d(\Gamma) = d(\Lambda) = |\det A| .$$

Zij tenslotte S het sterlichaam $|x_1x_2| \leq 1$; dan is $\sqrt{\tau}.S$ ($\tau > 0$) het sterlichaam $|x_1x_2| \leq \tau$, in het volgende gemakshalve aangegeven met

(5) $$\sqrt{\tau}.S = S_\tau .$$

Een relatie $\mu(Q;z)=\mu$ betekent nu dat het rooster $\Gamma = \Lambda - Az$ een punt heeft binnen $\sqrt{\tau}.S$, als $\tau > \mu$, maar niet meer voor $\tau = \mu$. In het laatste geval zeggen we dat Γ toegelaten is voor S_μ. De grootheid $\mu(Q)$ is dan de onderste grens van de getallen $\mu > 0$ met de eigenschap:

(a) voor elke y is $\Gamma = \Lambda + y$ niet toegelaten voor S_μ.

De eigenschap (a) kan ook aldus uitgedrukt worden: bij elk punt y bestaat een punt $x \in \Lambda$ met $x+y \in S_\mu$, ofwel $y \in S_\mu - x$. Dus (a) is aequivalent met: de lichamen $S_\mu + x$, $x \in \Lambda$ overdekken R_2. We zeggen dan dat Λ een overdekkingsrooster is van S_μ. Dus $\mu(Q)$ is de onderste grens der getallen $\mu > 0$, waarvoor het rooster Λ der punten (3) een overdekkingsrooster van S_μ is.

In het volgende zullen we de vraag bespreken hoe we boven- en ondergrenzen voor de grootheid $\mu(Q)$ kunnen afleiden, zowel in het algemeen als voor speciale vormen Q. Onder meer zullen we te maken krijgen met de kwestie van het al of niet bestaan van de algorithme van Euclides in een reëel kwadratisch getallenlichaam. Ook zullen we spreken over het voorkomen van oneindig veel roosterpunten u waarvoor voldaan is aan een ongelijkheid van de vorm

$$|Q(u-z)| \leq \mu .$$

2. Een resultaat van Minkowski [1] wordt uitgedrukt door

Stelling 1. We hebben steeds $\mu(Q) \leq \frac{1}{4}\sqrt{\delta(Q)}$ ($\delta(Q) > 0$). Het gelijkteken geldt alleen als Q(x) aequivalent is met $\beta\, x_1x_2$ ($\beta \neq 0$).

Van deze stelling zijn vele bewijzen bekend. We schetsen er enige.

1^e bewijs. Zij Λ een rooster met determinant 1. Men kan een parallelogram P vinden met middelpunt in O en oppervlakte 1, zó dat geldt:

1°. P is bevat in $\frac{1}{2}S$: $|x_1x_2| \leq \frac{1}{4}$

2°. Λ is overdekkingsrooster van P (en dus van $\frac{1}{2}S$).

En wel kan men, als Λ een primitief punt a bevat met lengte 1, voor P een vierkant met een zijde $\parallel$ a nemen; het algemene geval is tot dit geval terug te brengen.

2^e bewijs. (Macbeath [2], arithmetisch bij Mordell [3] en Cassels [4]). Zij weer Λ een rooster met determinant 1. Zij $y \in R_2$ willekeurig en $\{a,b\}$ een basis van Λ met $a \in S$. Kies m geheel, zó dat $|\det(a,y+mb)|$ minimaal is. Op de rechte door y+mb, evenwijdig met a, ligt nu een punt $y+mb+ka \in \frac{1}{2}S$ (k geheel).

3^e bewijs (arithmetisch). Perron [5] neemt $\delta(Q)=1$ en voert Q door een gehele, unimodulaire transformatie over in $Q_1(x)=x_1(\rho x_1+x_2)$, dan wel $Q_2(x) = \alpha(x_1+\rho x_2)^2 - \frac{1}{4\alpha}x_2^2$. Vervolgens bepaalt hij $x_1 \equiv z_1$, $x_2 \equiv z_2$, zó dat $|Q_1(x)| \leq \frac{1}{4}$, resp. $|Q_2(x)| \leq \frac{1}{4}$.

4^e bewijs (zie [6], p.34-35): het geval n=2 van de stelling van Tsjebotarew (voor het product van n inhomogene lineaire vormen).

5^e bewijs. Sawyer [7] leidt stelling 1 af uit de beide volgende beweringen:

A) Zij $\Gamma = \Lambda + y$ een inhomogeen rooster, zonder punten op de assen. Dan zijn er vier punten a,b,c,d van Γ, één in elk kwadrant, zodanig dat de gesloten vierhoek R met hoekpunten a,b,c,d geen andere punten van Γ bevat.

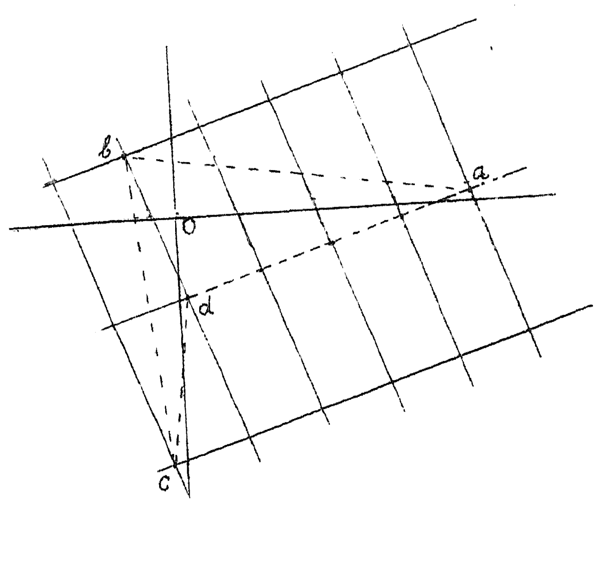
B) Is R zo'n vierhoek en Γ toegelaten voor S, dan geldt:

$$\text{opp } R = d(\Gamma) \quad \text{en} \quad \text{opp } R \geq 4.$$

Het bewijs van B) is als volgt:

$$\begin{aligned} \text{opp } R &= \tfrac{1}{2}\,|\det(a,b)+\det(b,c)+\det(c,d)+\det(d,a)| \\ &= \tfrac{1}{2}\{|a_1b_2| + |a_2b_1| + \ldots + |d_1a_2| + |d_2a_1| \\ &\geq \tfrac{1}{2}\{\left|\frac{a_1}{b_1}\right| + \left|\frac{b_1}{a_1}\right| + \ldots + \left|\frac{d_1}{a_1}\right| + \left|\frac{a_1}{d_1}\right| \geq 4. \end{aligned}$$

Sawyer's bewijs van A) is fout. Het is met name niet voldoende een roostervierhoek te nemen, die niet meer een roostervierhoek echt bevat (steeds zijn vierhoeken met één hoekpunt in elk kwadrant bedoeld). Een dergelijke redenering betreffende het al of niet voorkomen van primitieve roosterpunten binnen het gebied $|(x_1-1)x_2| < 1$ leidde tot een fout resultaat (zie Chalk [8,9]). Toch is A) juist. We hebben zelfs de volgende



Stelling van Delone [10]. Heeft Γ geen punten op de assen, dan is er in Γ een roosterparallelogram, met één hoekpunt in elk kwadrant (o.a. ook bewezen door Rédei [11]).
Deze stelling is op zichzelf van belang. Delone stelt een algorithme van zulke "gedeelde" parallelogrammen op, als inhomogeen analogon van de kettingbreukalgorithme (zie ook [11]).

3. Voor speciale vormen Q kunnen we verscherpingen van stelling 1 afleiden. Een meetkundige methode van Heinhold [12] kan het best uitgedrukt worden door de volgende
Stelling 2. Een rooster Λ, met basis $\{a,b\}$, is een overdekkingsrooster van S_μ, als S_μ de punten $\frac{1}{2}a, \frac{1}{2}b$ en één van de punten $\frac{1}{2}(a \pm b)$ bevat.

Arithmetisch geformuleerd geeft dit (zie bijv. Barnes [13]):

(6) Gevolg. $$\mu(Q) \leq \frac{1}{4} \max \{ |Q(1,0)|, |Q(0,1)|, \min(|Q(1,1)|, |Q(1,-1)|) \}.$$

Bewijs van stelling 2. Het is voldoende om aan te tonen dat het parallelogram Π op a,b overdekt wordt door enige gebieden $S_\mu + x$, $x \in \Lambda$. Laat $\frac{1}{2}a, \frac{1}{2}b, \frac{1}{2}(a+b)$ tot S_μ behoren en zij algemeen $T(x,y)$ de gerichte rechthoek met een hoekpunt in x en een hoekpunt in y. Dan wordt Π overdekt door

$$T(o,a),\ T(o,b),\ T(o,a+b),\ T(a,a+b),\ T(b,a+b)$$

(zoals gemakkelijk uit een figuur volgt). Voor ieder van deze vijf rechthoeken volgt verder uit de onderstelling dat hij overdekt wordt door twee van de vier gebieden S_μ, $S_\mu+a$, $S_\mu+b$, $S_\mu+a+b$.
Opmerking 1. Uit het gegeven bewijs volgt nog dat $\mu(Q;z)$ gelijk μ kan zijn aan het rechterlid van (6) hoogstens in de gevallen $z \equiv (\frac{1}{2},0), (0,\frac{1}{2}), (\frac{1}{2},\frac{1}{2}) \pmod 1$.

Een methode van Cassels [14] sluit nauw aan bij het eerste bewijs van stelling 1 en berust op het volgende triviale
Lemma 1. Zij a primitief punt van een rooster Λ en zij M een gebogen parallelogram, begrensd door twee lijnsegmenten L_1, L_2 en twee enkelvoudige, elkaar niet snijdende bogen C_1, C_2, zodanig dat

1°. $C_2 = C_1 - a$ (en L_1, L_2 zijn evenwijdig met en in lengte gelijk aan a)

2°. opp $M \geq d(\Lambda)$.

Dan is Λ overdekkingsrooster van M.

Cassels kiest nu μ zo, dat S_μ zo'n gebied M bevat, ofook twee gebieden M_1, M_2 waarvoor $M = M_1 \cup (M_2+a)$ van dat type is. Uitvoering van dit idee leidt na enige berekening tot het resultaat dat $\mu(Q) \leq \mu$, mits (we stellen $Q(a)=\alpha$)

$$4\mu \geq |\alpha| \text{ en } \begin{cases} 16\mu|\alpha| + 4([2\mu/|\alpha|]\cdot|\alpha|)^2 \geq \delta(Q) & \text{als } \alpha \neq 0 \\ 16\mu^2 \geq \delta(Q) & \text{als } \alpha = 0. \end{cases}$$

Vervangen we hierin $[2\mu/|\alpha|]$ door $\max\{0, 2\mu/|\alpha| - 1\}$, dan krijgen we in geval $\alpha \neq 0$ een door Davenport [15] arithmetisch verkregen resultaat.

Als voorbeeld beschouwen we $Q(x) = x_1^2 + kx_1x_2 - x_2^2$. Voor $k > 0$ en even leiden de genoemde methoden alle tot de juiste waarde

$$(7) \qquad \mu(Q) = \frac{1}{4}k = \frac{1}{4}\sqrt{\delta(Q)} \cdot \sqrt{k^2/(k^2+4)}.$$

Hieronder behandelen we de toepassing op normvormen van reële kwadratische getallenlichamen.

4. Zij m een <u>kwadraatvrij, positief geheel getal</u>. De algebraische gehelen uit het getallenlichaam $K(\sqrt{m})$ worden gegeven door

$$\xi = u_1 + u_2\omega, \text{ waarin } \omega = \begin{cases} \sqrt{m} & \text{als } m \equiv 2 \text{ of } 3 \pmod 4 \\ \frac{1}{2}(1+\sqrt{m}) & \text{als } m \equiv 1 \pmod 4). \end{cases}$$

De norm van zo'n getal is gelijk aan $N_m(u)$, als we stellen

$$(8) \qquad N_m(x) = \begin{cases} x_1^2 - mx_2^2 & \text{als } m \equiv 2 \text{ of } 3 \pmod 4) \\ x_1^2 + x_1x_2 - \frac{1}{4}(m-1)x_2^2 & \text{als } m \equiv 1 \pmod 4). \end{cases}$$

In $K(\sqrt{m})$ geldt de algorithme van Euclides (afgekort E.A.), als bij elk tweetal gehelen $\xi_0, \xi_1 \in K(\sqrt{m})$, met $\xi_1 \neq 0$, een geheel getal $\omega \in K(\sqrt{m})$ bestaat met

$$\xi_0 = \omega\xi_1 + \xi_2, \qquad |\text{norm } \xi_2| < |\text{norm } \xi_1|.$$

Delen we door ξ_1, dan zien we dat de eis is: bij elk getal $\rho = z_1 + z_2\omega$ in $K(\sqrt{m})$ bestaat een geheel getal $\xi = u_1 + u_2\omega$ met

$$|\text{norm}(\rho - \xi)| = |\text{norm}\{(z_1-u_1) + (z_2-u_2)\omega\}| = |N_m(u-z)| < 1.$$

Anders gezegd: E.A. geldt als de vorm N_m voldoet aan

$$(9) \qquad \mu(N_m; z) < 1 \text{ voor alle rationale punten } z.$$

In het bijzonder geldt E.A., als $\mu(N_m) < 1$.

Thans is bekend dat E.A. geldt slechts in de 16 gevallen

$$m = 2,3,5,6,7,11,13,17,19,21,29,33,37,41,57,73.$$

Behalve het "slechts" was dit zelfs vrij lang bekend (zie Rédei [16] voor literatuuropgaven; hij geeft ook m=97, maar deze m is 10 jaar later onttroond door Barnes en Swinnerton-Dyer [17]). Voor m=2,3,5, 6,7,13,17,21,33,37,41 kan Heinhold [12] het uit stelling 2 halen. In sterk vereenvoudigde vorm ziet zijn afleiding er als volgt uit.

Stel in de twee gevallen $m \not\equiv 1$ en $m \equiv 1 \pmod 4$:

$$m=q^2+p \quad (1 \leq p \leq 2q), \text{ resp. } m=(2q+1)^2+4p \quad (1 \leq p \leq 2q+1)$$

en pas stelling 2, gevolg toe op de met N_m aequivalente vorm

$$N_m(x_1+qx_2,x_2) = x_1^2+2qx_1x_2-px_2^2, \text{ resp. } x_1^2+(2q+1)x_1x_2-px_2^2.$$

Dan krijgt men

$$\mu(N_m) \leq \frac{1}{4}\max(p,2q+1-p), \text{ resp.} \leq \frac{1}{4}\max(p,2q+2-p).$$

Daaruit volgt het resultaat, mits men nog gebruik maakt van opmerking 1.

Met de in 3. geschetste methoden behandelt Cassels [14] de gevallen m=11,29 en Barnes [13] de gevallen m=57,73. Het resterende geval m=19, recentelijk behandeld door Varnavides [18] , laat zich niet zo vangen.

We vermelden nog een meetkundige methode om scherpe schattingen voor $\mu(N_m)$ en zelfs de punten z, waarvoor $\mu(N_m;z)$ boven een geschikte waarde μ ligt, te vinden, voor niet te grote m. Zij μ zo'n waarde, T_μ het sterlichaam $|N_m(x)|<\mu$ en W het vierkant $-\frac{1}{2} \leq x_i < \frac{1}{2}$ (i=1,2). Kies een aantal roosterpunten u^i, zodanig dat een voldoende groot deel R^* van W overdekt wordt door de gebieden $T_\mu+u^i$. Zij R het complement van R^* in W - het kan bestaan uit enige punten of één of meer kleine gebiedjes - en zij C de gezochte deelverzameling van punten $z \in R$ met $\mu(N_m;z) \geq \mu$. Een willekeurige gehele automorfie U van N_m voert een willekeurig punt z over in een punt $\bar{z}$ met $\mu(N_m;\bar{z}) = \mu(N_m;z)$. Dus is $UC \subset C \pmod Y$. Het is nu duidelijk dat we vaak ons doel kunnen bereiken door toepassing van het volgende

Lemma 2 (Cassels) Zij U een gehele, unimodulaire transformatie, met reële eigenwaarden $\neq \pm 1$, en zij a de eigenvector, behorende bij de absoluut kleinste eigenvector. Laat $C \subset W$ voldoen aan

$$UC \subset C + u^0 \qquad (u^0 \text{ een roosterpunt})$$

en zij z^0 het dekpunt van $Ux=x+u^0$. Dan is C gelegen op de rechte door z^0 evenwijdig met a. Als bovendien geldt $U^{-1}C \subset C$ (mod Y), dan bestaat C alleen uit het punt z^0.

Het lemma volgt uit het feit dat de transformatie

$$U_1 : x \to U_1x = Ux-z^0$$

een hyperbolische rotatie om z^0 is die C in zichzelf afbeeldt. Er is een generalisatie voor het geval van een aantal verzamelingen C_i met $UC_i \subset C_{i+1}+u^{i+1}$ (cyclisch; $u^i \in Y$). Zie bijv. Bambah [19] en Barnes en Swinnerton-Dyer [17] . Met de geschetste methode is onder meer weerlegd dat E.A. zou gelden in $K(\sqrt{97})$.

5. We behandelen enige algemene eigenschappen van de grootheden $\mu(Q)$ en $\mu(Q;z)$ (voor I en II vgl. [17]).

I. De functie $\mu(Q;z)$ is semicontinu naar boven in z.

Bewijs. Kies $z^0 \in R_2$ en $\varepsilon > 0$. Neem een u^0 met

$$|Q(u^0-z^0)| < \mu(Q;z^0) + \varepsilon$$

(zie (2)). Voor $|z-z^0|$ voldoende klein is dan

$$|Q(u^0-z)| < \mu(Q;z^0) + 2\varepsilon \text{ , dus } \mu(Q;z) < \mu(Q;z^0) + 2\varepsilon \text{ .}$$

We zeggen dat het minimum $\mu(Q)$ wordt bereikt als bij elke z een punt $u \in Y$ bestaat met $|Q(u-z)| \leq \mu(Q)$. Er geldt

II. Als $\mu(Q)$ bereikt wordt, dan zijn er punten z,u met

$$|Q(u-z)| = \mu(Q;z) = \mu(Q).$$

Bewijs. De functie $\mu(Q;z)$ van z is periodiek modulo Y. Wegens I wordt dus de bovenste grens $\mu(Q)$ aangenomen. Zij $\mu(Q;z)=\mu(Q)$ en onderstel dat $\mu(Q)$ bereikt wordt. Voor een u uit de definitie is $|Q(u-z)| \leq \mu(Q)$, en wegens (2) ook $|Q(u-z)| \geq \mu(Q;z)=\mu(Q)$.

Er is een voorbeeld, waarbij $\mu(Q)$ niet bereikt wordt, nl. de normvorm N_{13}. Inkeri [20] bewees dat $\mu(N_{13}) = \frac{1}{3}$ en toonde tevens aan dat voor $\rho = \frac{1}{3}\omega$, $\sigma = -\frac{1}{3}\omega$, waarbij $\omega = \frac{1}{2}(1+\sqrt{13})$, geldt:

$$|(\xi-\rho)(\xi'-\sigma)| > \tfrac{1}{3}, \text{ i.e. } |(3\xi-\omega)(3\xi'+\omega)| > 3$$

voor alle gehelen ξ in $K(\sqrt{13})$. Anders gezegd: er is een (irrationaal punt z, zodanig dat

$$| N_{13}(u-z) | > \mu(N_{13}) = \frac{1}{3} \text{ voor alle } \mu \in Y.$$

III. Als $Q^n \rightarrow Q^o$ en $z^n \rightarrow z^o$, dan is $\mu(Q^o;z^o) \geq \lim\sup \mu(Q^n;z^n)$.

Bewijs. Meetkundig betekent het: zij gegeven een rij inhomogene roosters $\Gamma_n = \Lambda_n + y^n$, met $y^n \rightarrow y^o$ en $\Lambda_n \rightarrow \Lambda_o$, zij Γ_n toegelaten voor $\tau_n S$ $(\tau_n > 0)$, waarbij $\lim\sup \tau_n = 1$; dan is $\Gamma_o = \Lambda_o + y^o$ toegelaten voor S. Dit wordt gemakkelijk uit het ongerijmde bewezen.

6. We snijden vervolgens het probleem aan om ondergrenzen voor $\mu(Q)$ af te leiden. Met een methode van Morimoto (zie ook hieronder) bewees Davenport [21] de diepliggende eigenschap: er is een universele constante κ, bijv. $\kappa = \frac{1}{128}$, zodanig dat

$$\mu(Q) \geq \kappa \sqrt{\delta(Q)} \tag{10}$$

voor alle vormen Q die geen rationaal nulpunt hebben (we merken op dat wegens 5, III de eigenschap dan ook algemeen geldt). Een bijkomende eigenschap is dat ingeval van rationale vormen Q er ook een rationaal punt z is met $\mu(Q;z) \geq \kappa \sqrt{\delta(Q)}$. In verband met (9) heeft dit de onmiddellijke implicatie dat in getallenlichamen $K(\sqrt{m})$ E.A. niet geldt als $\delta(N_m) > \kappa^{-2}$. Dit houdt in dat E.A. slechts geldt in eindig veel lichamen $K(\sqrt{m})$.

Een betrekkelijk eenvoudig bewijs van bovengenoemde eigenschappen, met $\kappa = \frac{1}{51}$ (later verbeterd tot $\kappa = \frac{1}{45}$), is gegeven door Cassels [22]. We komen hierop terug in [6].

Een poging om de tweede eigenschap direct uit (10) af te leiden leidt tot de volgende overweging. Zij z een punt met $\mu(Q;z) \geq \kappa\sqrt{\delta(Q)}$ en zij U een (niet-triviale) automorfie van Q. Dan is ook $\mu(Q;U^n z) \geq \kappa\sqrt{\delta(Q)}$ voor alle gehele n. Wegens 5,III zouden we nu klaar zijn als we het volgende probleem konden oplossen:

Probleem. Heeft de verzameling der punten $U^n z$ (mod Y) een rationaal verdichtingspunt?

Eéndimensionaal zou dit probleem luiden: heeft de verzameling der getallen αr^n (mod 1), waarbij α willekeurig en $r > 1$ rationaal is, een rationaal verdichtingspunt?

7. Onder zekere voorwaarden voor het punt z en de vorm $Q(x) = L_1(x)L_2(x)$ heeft de ongelijkheid $|Q(u-z)| \leqq \frac{1}{4}\sqrt{\delta(Q)}$ oneindig veel oplossingen. Met de notaties van 1 kunnen we schrijven $Q(u-z)=(L_1(u)-y_1)(L_2(u)-y_2)$. Er geldt

Stelling 3. Zij $Q(x)=L_1(x)L_2(x)$, $y \in R_2$ willekeurig en $L_1(x)$ geen veelvoud van een rationale vorm. Voor $\varepsilon > 0$ is dan oplosbaar

(11) $$|(L_1(u)-y_1)(L_2(u)-y_2)| < \frac{1}{4}\sqrt{\delta(Q)}, \qquad |L_1(u)-y_1| < \varepsilon.$$

De meeste bewijzen van stelling 1 zijn geschikt om ook de iets sterkere stelling af te leiden. Zo is het voldoende om in het 1^e bewijs van stelling 1 het punt a te kiezen in een voldoend smalle strook $|x_1| < \varepsilon'$; dit is juist mogelijk onder de voorwaarde voor $L_1(x)$.

De stelling is kennelijk niet meer juist als $L_1(x)$ een veelvoud van een rationale vorm is. Als er verder een punt u is met $L_1(u)-y_1=0$, dan volgt meteen dat er oneindig veel punten u zijn waarvoor (11) geldt. Neemt $L_1(u)-y_1$ wèl de waarde 0 aan, dan heeft, wegens de corresponderende resultaten in het geval $y_1=y_2=0$ (stelling van Hurwitz!), (11) oneindig veel oplossingen als we de factor $\frac{1}{4}$ vervangen door $1/\sqrt{5}+\varepsilon$. Zie hiervoor Mordell [23] .

Toepassing van stelling 3 op $Q(x) = (x_1-\theta x_2)x_2$ levert

Stelling 4. Zij θ irrationaal, α reëel en $\varepsilon > 0$. Dan is oplosbaar

(12) $$|(u_1-\theta u_2-\alpha)u_2| < \frac{1}{4}, \qquad |u_1-\theta u_2-\alpha| < \varepsilon.$$

Neemt $u_1-\theta u_2-\alpha$ niet de waarde 0 aan, dan zijn er oneindig veel oplossingen.

Een dergelijk resultaat (met een grotere constante) is het eerst afgeleid in 1866 door Tsjebysjew [24] . Zie Koksma [25] . Zoals ingeval van stelling 1 kunnen voor speciale θ verfijningen gegeven worden. Dit komt neer op een studie, voor verschillende θ, van de grootheid

(13) $$\mu_\infty(\theta;\alpha) = \liminf_{|u_2| \to \infty} |(u_1-\theta u_2-\alpha)u_2| \qquad (\theta \text{ irrationaal}).$$

We merken op dat wegens (10) de uitdrukking $\sup_\alpha \mu_\infty(\theta;\alpha)$ voor alle θ boven een vast positief bedrag ligt. Immers passen we (10) toe op de vorm $Q(x)=(x_1-\theta x_2)x_2$, dan vinden we dat er getallen α,α' zijn zodanig dat

$$|(u_1-\theta u_2-\alpha)(u_2-\alpha')| \geqq \kappa \qquad \text{voor alle } u_1,u_2.$$

Dan is zeker $\sup_{\alpha} \mu_{\infty}(\theta;\alpha) \geq \kappa$.

De laatste relatie kan gezien worden als een eigenschap die nauw samenhangt met het feit dat E.A. slechts geldt in eindig veel lichamen $K(\sqrt{m})$.

We besluiten met de opmerking, dat er ook onderzoekingen zijn verricht aangaande de grootheid

$$\mu^{*}_{\infty}(\theta;\alpha) = \liminf_{u_2\to\infty} |(u_1-\theta u_2-\alpha)u_2| .$$

-.-

Literatuur

[1] H. Minkowski, Ges. Abhandlungen I, p.336 vv.

[2] A.M. Macbeath, Non-homogeneous linear forms, Journal London Math.Soc.23, 141-147 (1948)

[3] L.J. Mordell, Minkowski's theorem on the product of two linear forms, Journal London Math.Soc.3, 19-22 (1928)

[4] J.W.C. Cassels, Yet another proof of Minkowski's theorem, etc., Proc. Cambridge Phil.Soc.49, 365-366 (1953)

[5] O. Perron, Neuer Beweis eines Satzes von Minkowski, Math. Annalen 115, 656-657 (1938)

[6] M.v.d. Meer e.a., Syllabus Colloquium "Meetkunde der Getallen", Mathematisch Centrum, 32-36 (1959)

[7] D.B. Sawyer, The product of two non-homogeneous linear forms, Journal London Math.Soc.23, 250-251 (1948)

[8] J.H.H. Chalk, The minimum of a non-homogeneous bilinear form, Quart. J.Math., Oxford (2)3, 119-129 (1952)

[9] ————————, On the primitive lattice points in the region $|(x+c)y| \leq 1$, ibidem 5, 203-211 (1954)

[10] B.H. Delone, Algorifm razdelennych parallelogrammow, Izwestija Akad.Nauk SSSR 11, 505-538 (1947)

[11] E.S. Barnes-H.P.F. Swinnerton-Dyer, The inhomogeneous minima of binary quadratic forms III, Acta Math.92, 199-234 (1954)

[12] J. Heinhold, Verallgemeinerung und Verschärfung eines Minkowskischen Satzes, Math.Zschr.44, 659-688 (1939)

[13] E.S. Barnes, Non-homogeneous binary quadratic forms, Quart.J.Math., Oxford (2) 1, 199-210 (1950)

[14] J.W.S. Cassels, The lattice properties of asymmetric hyperbolic regions. II On a theorem of Davenport, Proc. Cambridge Phil.Soc.44, 145-154 (1948)

[15] H. Davenport, Non-homogeneous binary quadratic forms, Indagationes 8, 518-524 (1946)

[16] L. Rédei, Zur Frage des Euklidischen Algorithmus in quadratischen Zahlkörpern, Math. Annalen 118, 588-608 (1942)

[17] E.S. Barnes- H.P.F. Swinnerton-Dyer, The inhomogeneous minima of binary quadratic forms. I, Acta Math. 87, 259-323 (1952)

[18] P. Varnavides, The Euclidean real quadratic fields, Indagationes 14, 111-122 (1952)

[19] R.P. Bambah, Non-homogeneous binary quadratic forms. II The second minimum of $(x+x_0)^2-7(y+y_0)^2$, Acta Math.86, 31-56 (1951)

[20] K. Inkeri, Non-homogeneous binary quadratic forms, Den 11te Skandinaviske Matematikerkongress, Trondheim, 1949, 216-224

[21] H. Davenport, Indefinite binary quadratic forms, and Euclid's algorithm in real quadratic fields, Proc.London Math.Soc.(2) 53, 65-82 (1951)

[22] J.W.S. Cassels, The inhomogeneous minimum of binary quadratic ternary cubic and quaternary quartic forms, Proc. Cambridge Phil.Soc.48, 72-86 (1952). Addendum, ibidem 48, 519-520 (1952)

[23] L.J. Mordell, The product of two non-homogeneous linear forms IV, Journal London Math.Soc.26, 93-95. (1951)

[24] P.L. Tchebychef, Oeuvres I, p.637-684

[25] J.F. Koksma, Diophantische Approximationen, Springer 1936, Kap VI, § 2.

[11] L. Rédei, Neuer Beweis eines Satzes von Delone über ebene Punktgitter, Journal London Math.Soc. 34, 205-207 (1959)