ROCZNIKI POLSKIEGO TOWARZYSTWA MATEMATYCZNEGO
Seria II: WIADOMOŚCI MATEMATYCZNE XIX (1975)

wmptm 1897

Ministerstwo Nauki i Szkolnictwa Wyższego

J. WÓJCIK (Warszawa)

O zastosowaniu geometrii liczb do przedstawień liczb naturalnych przez sumy kwadratów

Celem niniejszego artykułu jest podanie pewnych wiadomości z geometrii liczb oraz jej zastosowań do przedstawień liczb naturalnych przez sumy kwadratów. Niech R^n oznacza n-wymiarową przestrzeń euklidesową. Punkty przestrzeni R^n będziemy oznaczali tłustymi literami i interpretowali jako macierze jednokolumnowe; np. $\boldsymbol{x} = [x_1,\ldots,x_n]^T$, x_i rzeczywiste, $i = 1,\ldots,n$, gdzie dla danej macierzy A przez A^T oznaczamy jej macierz transponowaną. Przez $\mathbf{0}$ będziemy rozumieć punkt $[0,\ldots,0]^T$ (n współrzędnych) nazywany dalej początkiem układu współrzędnych.

Przez $(\boldsymbol{x},\boldsymbol{y})$ będziemy oznaczali iloczyn skalarny punktów $\boldsymbol{x}$, $\boldsymbol{y}$. $[\boldsymbol{a}_1,\ldots,\boldsymbol{a}_k]$ oznacza macierz, której i-tą kolumną jest punkt $\boldsymbol{a}_i$. $R^{n,k}$ oznacza zbiór wszystkich punktów $[x_1,\ldots,x_n]^T$ takich, że: $x_i = 0$ dla $i \leqslant k$.

Jeżeli $A \subset R^{n,1}$, to przez $A^{(1)}$ będziemy oznaczać podzbiór przestrzeni R^{n-1} taki, że $[x_1,\ldots,x_{n-1}]^T \in A^{(1)}$ wtedy i tylko wtedy, gdy $[0,x_1,\ldots,x_{n-1}]^T \in A$.

Niech $\mathcal{S} \subset R^n$, $\boldsymbol{y} \in R^n$, t oznacza liczbę rzeczywistą, A macierz rzeczywistą o n kolumnach, φ przekształcenie przestrzeni R^n w siebie. Przez $t\mathcal{S}$, $A\mathcal{S}$, $\varphi\mathcal{S}$, $\mathcal{S}+\boldsymbol{y}$ będziemy oznaczać zbiór punktów postaci odpowiednio $t\boldsymbol{x}$, $A\boldsymbol{x}$, $\varphi\boldsymbol{x}$, $\boldsymbol{x}+\boldsymbol{y}$, gdzie $\boldsymbol{x} \in \mathcal{S}$.

Jednym z ważnych pojęć geometrii liczb jest pojęcie kraty.

DEFINICJA KRATY. *Kratą* K nazywamy podzbiór przestrzeni R^n spełniający warunki: (i) Jeżeli $\boldsymbol{x}, \boldsymbol{y} \in K$, to $\boldsymbol{x}+\boldsymbol{y} \in K$ i $\boldsymbol{x}-\boldsymbol{y} \in K$. (ii) Dla każdej liczby rzeczywistej M istnieje co najwyżej skończona ilość punktów należących do K takich, że $0 \leqslant x_i \leqslant M$ $(i = 1,\ldots,n)$.

Warunek (i) oznacza, że zbiór K jest grupą ze względu na dodawanie punktów. Zbiór spełniający warunek (ii) nazywamy *dyskretnym*. Krótko mówiąc, *kratą* nazywamy podzbiór przestrzeni R^n, który jest grupą ze względu na dodawanie punktów i jest dyskretny.

Układ punktów $\boldsymbol{x}_1,\ldots,\boldsymbol{x}_k$ przestrzeni R^n nazywamy *liniowo niezależnym*, jeżeli równość $\alpha_1\boldsymbol{x}_1+\ldots+\alpha_k\boldsymbol{x}_k = 0$, gdzie α_i oznaczają liczby rzeczywiste, zachodzi tylko w przypadku gdy $\alpha_1 = \ldots = \alpha_k = 0$.

Punkty $\boldsymbol{a}_1,\ldots,\boldsymbol{a}_r$ kraty L nazywamy *bazą całkowitą* kraty L, jeżeli

1° $\boldsymbol{a}_1,\ldots,\boldsymbol{a}_r$ są liniowo niezależne;

2° każdy punkt $\boldsymbol{a}\in L$ jest postaci: $\boldsymbol{a}=x_1\boldsymbol{a}_1+\ldots+x_r\boldsymbol{a}_r$, gdzie $x_1,\ldots,x_r$ są liczbami całkowitymi.

Zachodzi ważne

TWIERDZENIE 1. *Każda krata ma bazę całkowitą.*

Dowód tego twierdzenia znajduje się w [6], str. 29–31. Należy tylko zastąpić tam słowo „rational" słowem „real".

Liczba elementów bazy kraty jest równa maksymalnej liczbie liniowo niezależnych punktów kraty i oczywiście nie przekracza n. W przypadku, gdy ilość ta wynosi n, kratę nazywamy *pełną*. Oczywiście by stwierdzić, że krata jest pełna wystarczy znaleźć n punktów liniowo niezależnych należących do kraty.

Punkt przestrzeni R^n nazywamy *wymiernym* lub *całkowitym*, jeżeli jego współrzędne są odpowiednio wymierne lub całkowite. *Kratę* nazywamy *wymierną*, jeżeli wszystkie jej punkty są wymierne. Niech Λ_0 oznacza kratę wszystkich punktów całkowitych,

$$\boldsymbol{e}_i \overset{\text{def}}{=} [0,\ldots,\underbrace{1}_{i\text{-ta współrzędna}},\ldots,0]^T, \qquad i=1,\ldots,n.$$

Oczywiście punkty $\boldsymbol{e}_i$ $(i=1,\ldots,n)$ tworzą bazę całkowitą kraty Λ_0.

Z twierdzenia 1 wynika, że dla każdej kraty wymiernej K istnieje liczba naturalna d taka, że $dK\subset\Lambda_0$. Najmniejszą taką liczbę naturalną nazywamy *mianownikiem kraty* K. Analogicznie określamy *mianownik macierzy wymiernej*. Łatwo widzieć, że mianownik kraty wymiernej K jest równy mianownikowi macierzy utworzonej ze współrzędnych punktów bazy całkowitej kraty K.

Bazę całkowitą $\boldsymbol{a}_1,\ldots,\boldsymbol{a}_k$ $(k\leqslant n)$ kraty K nazywamy *trójkątną*, jeżeli jest postaci:

$$\boldsymbol{a}_1=[a_{11},a_{21},\ldots,a_{n1}], \quad \boldsymbol{a}_2=[0,a_{22},\ldots,a_{n2}], \quad \ldots,$$

$$\boldsymbol{a}_k=[0,\ldots,0,a_{kk},\ldots,a_{nk}], \quad a_{ii}=0,\ i=1,\ldots,k.$$

Zachodzi następujące

TWIERDZENIE 2. *Każda krata wymierna ma bazę trójkątną.*

Twierdzenie to jest natychmiastowym wnioskiem z twierdzenia 2, podanego w [7], str. 118. Jeżeli krata nie jest wymierna, to może nie mieć bazy trójkątnej. Jest oczywiste, że np. krata o bazie całkowitej: $[1,\ 1]^T$, $[\sqrt{2},\ -\sqrt{2}]^T$ nie ma bazy trójkątnej. Niech Λ będzie kratą pełną i niech punkty $\boldsymbol{a}_i=[a_{1i},\ldots,a_{ni}]^T$ $(1\leqslant i\leqslant n)$ tworzą jej bazę.

Wiadomo, że $|\det(a_{ij})|$ nie zależy od wyboru bazy (niekoniecznie trójkątnej) kraty Λ. Wielkość tę nazywamy *wyróżnikiem kraty* Λ i oznaczamy przez $d(\Lambda)$. *Równoległościanem podstawowym* P kraty Λ nazywamy zbiór punktów postaci:

$$x_1\boldsymbol{a}_1+\ldots+x_n\boldsymbol{a}_n \qquad (0\leqslant x_j<1,\ j=1,\ldots,n).$$

Równoległościan podstawowy P jest więc identyczny ze zbiorem punktów $[y_1,\ldots, y_n]^T$, gdzie $y_i = \sum_{j=1}^{n} a_{ij}x_j$ $(0 \leqslant x_j < 1,\ 1 \leqslant i \leqslant n)$.

Objętość jego jest równa:

$$(1)\qquad V(P) = \int\ldots\int_{(0\leqslant x_j<1,\ 1\leqslant j\leqslant n)} dy_1 \ldots dy_n =$$

$$= |\det (a_{ij})| \int\ldots\int_{(0\leqslant x_j<1,\ 1\leqslant j\leqslant n)} dx_1 \ldots dx_n = |\det (a_{ij})| = d(\Lambda).$$

Oznacza to, że *wyróżnik kraty jest równy objętości jej równoległościanu podstawowego.* Jest oczywiste, że każdy punkt $\boldsymbol{x}$ przestrzeni R^n można przedstawić jednoznacznie w postaci

$$(2)\qquad \boldsymbol{x} = \boldsymbol{u}+\boldsymbol{v}, \quad \text{gdzie } \boldsymbol{u}\in\Lambda,\ \boldsymbol{v}\in P.$$

Przypominamy: P to równoległościan podstawowy, Λ — krata. Podzbiór przestrzeni R^n otwarty i spójny nazywamy *obszarem.* Jednym z ważnych zagadnień geometrii liczb jest badanie istnienia punktów kraty Λ w jakimś danym obszarze $\mathscr{S}$. Badanie istnienia takiego punktu dla odpowiednio dobranych Λ i $\mathscr{S}$ pozwala w niektórych przypadkach dowieść rozwiązalności pewnych równań diofantycznych w liczbach całkowitych. Dowody następujących twierdzeń 3, 4 i 5 podane są w [3], str. 68–72 oraz str. 246–250. Zachodzi następujące

TWIERDZENIE 3 (Blichfeldt). *Niech Λ będzie kratą pełną o wyróżniku $d(\Lambda)$, zaś $\mathscr{S}$ obszarem o objętości $V(\mathscr{S})$. Załóżmy, że $V(\mathscr{S}) > d(\Lambda)$. Wtedy istnieją 2 różne punkty $\boldsymbol{x}_1, \boldsymbol{x}_2$ należące do $\mathscr{S}$, takie że: $\boldsymbol{x}_1-\boldsymbol{x}_2 \in \Lambda$.*

Dowód. Niech P będzie równoległościanem podstawowym kraty Λ. Niech $\boldsymbol{u}\in\Lambda$. Przez $R(\boldsymbol{u})$ będziemy oznaczać zbiór punktów $\boldsymbol{v}$ spełniających warunek: $\boldsymbol{v}\in P$, $\boldsymbol{v}+\boldsymbol{u}\in\mathscr{S}$. Niech $\boldsymbol{x}\in\mathscr{S}$. Wtedy $\boldsymbol{x} = \boldsymbol{u}+\boldsymbol{v}$, $\boldsymbol{u}\in\Lambda$, $\boldsymbol{v}\in P$ na mocy (2). Oznacza to, że $\boldsymbol{x}\in R(\boldsymbol{u})+\boldsymbol{u}$. Stąd

$$(3)\qquad \mathscr{S} = \bigcup_{\boldsymbol{u}\in\Lambda} \{R(\boldsymbol{u})+\boldsymbol{u}\}.$$

Ponieważ przedstawienie (2) jest jednoznaczne, zbiory $R(\boldsymbol{u})+\boldsymbol{u}$ są rozłączne. Na mocy (3)

$$V(\mathscr{S}) = \sum_{\boldsymbol{u}\in\Lambda} V\{R(\boldsymbol{u})+\boldsymbol{u}\} = \sum_{\boldsymbol{u}\in\Lambda} V\{R(\boldsymbol{u})\},$$

i zgodnie z założeniem twierdzenia, wobec (1)

$$\sum_{\boldsymbol{u}\in\Lambda} V\{R(\boldsymbol{u})\} > d(\Lambda) = V(P).$$

Ponieważ zbiory $R(\boldsymbol{u})$ są zawarte w P, istnieje co najmniej jeden punkt $\boldsymbol{v}_0\in P$ należący do dwóch zbiorów $R(\boldsymbol{u})$, powiedzmy $\boldsymbol{v}_0\in R(\boldsymbol{u}_j)$ $(j=1, 2)$, gdzie $\boldsymbol{u}_1 \neq \boldsymbol{u}_2$.

Zgodnie z określeniem $R(\boldsymbol{u})$ punkty $\boldsymbol{x}_j = \boldsymbol{v}_0 + \boldsymbol{u}_j$ należą do $\mathscr{S}$ $(j = 1, 2)$, przy czym

$$\boldsymbol{x}_1 - \boldsymbol{x}_2 = \boldsymbol{u}_1 - \boldsymbol{u}_2 \begin{cases} \in \Lambda, \\ \neq 0. \end{cases}$$

Twierdzenie 3 jest więc udowodnione.

Z twierdzenia Blichfeldta wynika łatwo podstawowe dla geometrii liczb twierdzenie Minkowskiego o obszarze wypukłym.

TWIERDZENIE 4 (Minkowski). *Niech $\mathscr{S}$ będzie obszarem wypukłym, symetrycznym względem początku układu współrzędnych o objętości $V(\mathscr{S})$ i niech Λ będzie kratą pełną o wyróżniku $d(\Lambda)$. Jeżeli*

$$V(\mathscr{S}) > 2^n d(\Lambda),$$

to obszar $\mathscr{S}$ zawiera punkt kraty Λ różny od początku układu.

Dowód. Zastosujemy twierdzenie 3 do obszaru $\frac{1}{2}\mathscr{S}$, którego objętość wynosi $2^{-n} V(\mathscr{S})$. Istnieją zatem punkty $\frac{1}{2}\boldsymbol{x}_j \in \frac{1}{2}\mathscr{S}$ $(j = 1, 2)$ takie, że

$$\tfrac{1}{2}\boldsymbol{x}_1 - \tfrac{1}{2}\boldsymbol{x}_2 \begin{cases} \in \Lambda, \\ \neq 0. \end{cases}$$

Ponieważ obszar $\mathscr{S}$ jest symetryczny, więc $-\boldsymbol{x}_2 \in \mathscr{S}$

$$\tfrac{1}{2}\boldsymbol{x}_1 - \tfrac{1}{2}\boldsymbol{x}_2 = \tfrac{1}{2}\boldsymbol{x}_1 + \tfrac{1}{2}(-\boldsymbol{x}_2) \in \mathscr{S}$$

ponieważ $\mathscr{S}$ jest wypukły. Twierdzenie 4 jest udowodnione.

Podamy kilka dalszych określeń związanych z obszarami i kratami. Niech $\mathscr{S}$ będzie obszarem. Jeżeli krata Λ nie ma w $\mathscr{S}$ punktów różnych od $\mathbf{0}$ i $\mathbf{0} \in \mathscr{S}$, to mówimy, że krata Λ jest *dopuszczalna dla $\mathscr{S}$* lub *$\mathscr{S}$-dopuszczalna*. Kres dolny

$$\Delta(\mathscr{S}) = \inf d(\Lambda)$$

wyróżników $d(\Lambda)$ wszystkich krat $\mathscr{S}$-dopuszczalnych Λ nazywamy *wyróżnikiem krytycznym* obszaru $\mathscr{S}$. Jeżeli nie ma krat $\mathscr{S}$-dopuszczalnych, to mówimy, że $\mathscr{S}$ jest *typu nieskończonego* i piszemy $\Delta(\mathscr{S}) = \infty$. W przeciwnym razie mówimy, że $\mathscr{S}$ jest *obszarem typu skończonego* i $0 \leqslant \Delta(\mathscr{S}) < \infty$. Jeżeli krata jest $\mathscr{S}$-dopuszczalna oraz $d(\Lambda) = \Delta(\mathscr{S})$, to Λ nazywamy *kratą krytyczną* dla $\mathscr{S}$. Ogólnie mówiąc, nie ma żadnych podstaw twierdzić, że dowolny obszar ma kratę krytyczną. Określenie $\Delta(\mathscr{S})$ można „odwrócić": $\Delta(\mathscr{S})$ jest to największa z takich liczb Δ, że każda krata Λ, dla której $d(\Lambda) < \Delta$, ma w $\mathscr{S}$ punkt różny od $\mathbf{0}$.

Przez *upakowanie zbioru $\mathscr{S}$* w pewnym zbiorze $\mathscr{T}$ będziemy rozumieć dowolną rodzinę zbiorów rozłącznych postaci $\mathscr{S}_r = \mathscr{S} + \boldsymbol{y}_r$ zawartych w $\mathscr{T}$, gdzie $\boldsymbol{y}_r$ przebiega punkty jakiegoś zbioru. Jeżeli punkty $\boldsymbol{y}_r$ przebiegają zbiór punktów $\mathscr{T} \cap \Lambda$, gdzie Λ jest kratą, to mówimy, że *upakowanie* jest *kratowe*.

Zajmiemy się teraz oszacowaniem wyróżnika krytycznego kuli jednostkowej z dołu.

Niech $\mathscr{S}$ będzie obszarem o objętości $V(\mathscr{S})$, Λ oznacza kratę pełną o wyróżniku $d(\Lambda)$, niech wreszcie $N(t)$ oznacza liczbę punktów kraty Λ w obszarze $t\mathscr{S}$. Zachodzi następujący wzór (patrz [5], str. 133):

$$\lim_{t\to\infty} N(t)/t^n = V(\mathscr{S})/d(\Lambda). \tag{4}$$

Wiadomo, że objętość kuli jednostkowej $D_n = \{x, |x| < 1\}$ wynosi

$$V_n = V(D_n) = \frac{\pi^{n/2}}{\Gamma(1+n/2)},$$

gdzie Γ jest funkcją gamma Eulera.

Niech

$$\Gamma_n = \Delta(D_n)$$

oznacza wyróżnik krytyczny kuli D_n i niech $\mathscr{S}$ będzie dowolnym ograniczonym zbiorem o objętości $V(\mathscr{S})$. Niech zbiory

$$\mathscr{S}_r = \mathscr{S} + x_r \quad (1 \leqslant r \leqslant R) \tag{5}$$

będą upakowaniem $\mathscr{S}$ w pewnym zbiorze $\mathscr{T}$ o objętości $V(\mathscr{T})$. Wtedy oczywiście

$$V(\mathscr{T}) \geqslant RV(\mathscr{S}). \tag{6}$$

Załóżmy teraz, że istnieje funkcja $\varphi(x)$ punktu x taka, że

(i) $\varphi(x) = 0$, jeżeli $|x| \geqslant \varrho$ dla pewnego ϱ,

(ii) $\sum_r \varphi(x-x_r) = \psi(x) \leqslant 1$ dla wszystkich x,

jeżeli (5) jest upakowaniem zbioru $\mathscr{S}$.

Niech $\mathscr{T}(\varrho)$ będzie ϱ-otoczeniem zbioru $\mathscr{T}$, to jest zbiorem punktów odległych nie więcej niż ϱ od zbioru $\mathscr{T}$ (włączając również punkty zbioru $\mathscr{T}$).

Na podstawie (ii)

$$\int_{\mathscr{T}(\varrho)} \psi(x)\,dx \leqslant V(\mathscr{T}(\varrho)). \tag{7}$$

Z drugiej strony, na mocy (i),

$$\int_{\mathscr{T}(\varrho)} \psi(x)\,dx = \sum_r \int \varphi(x-x_r)\,dx = R\int \varphi(x)\,dx = RV(\varphi), \tag{8}$$

ponieważ punkty x, dla których $\varphi(x-x_r) \neq 0$ należą do $\mathscr{T}(\varrho)$. Porównując (7) i (8) otrzymujemy nierówność

$$R \leqslant V\{\mathscr{T}(\varrho)\}/V(\varphi). \tag{9}$$

Oczywiście, funkcja charakterystyczna zbioru $\mathscr{S}$ równa 1 na $\mathscr{S}$, a 0 poza $\mathscr{S}$, spełnia (i) i (ii). Jeżeli jako funkcję φ wziąć funkcję charakterystyczną, to $V(\varphi) = V(\mathscr{S})$ ($V(\varphi) = \int \varphi(x)\,dx$) i nierówność (9) jest słabsza niż nierówność (6), ponieważ $V(\mathscr{T})$ zamieniamy na $V\{\mathscr{T}(\varrho)\}$. Blichfeldt zauważył, że w pewnych przypadkach istnieją

funkcje prowadzące do lepszych oszacowań niż funkcja charakterystyczna. Tak jest na przykład, jeżeli $\mathscr{S} = D_n$ jest kulą jednostkową. Warunkiem koniecznym i wystarczającym na to, by otwarte kule o promieniu 1 i o środkach x_1, x_2 były rozłączne, jest warunek $|x_1-x_2| \geqslant 2$.

LEMAT 1. *Oznaczmy*

$$\varphi(x) = \max\{0, 1-\tfrac{1}{2}|x|^2\}.$$

Niech x_r $(1 \leqslant r \leqslant R)$ *będą punktami spełniającymi warunek*

$$|x_r-x_s| \geqslant 2 \quad (1 \leqslant r < s \leqslant R). \tag{10}$$

Wtedy dla każdego punktu x

$$\sum_{1\leqslant r\leqslant R} \varphi(x-x_r) \leqslant 1. \tag{11}$$

Dowód. Nie zmniejszając ogólności możemy założyć, że

$$0 < \varphi(x-x_r) = 1-\tfrac{1}{2}|x-x_r|^2 \quad (1 \leqslant r \leqslant R).$$

Jeżeli $y, y_1, \ldots, y_R$ są dowolnymi liczbami rzeczywistymi, to

$$R\sum_r (y-y_r)^2 = \sum_{r<s}(y_r-y_s)^2 + \Big(Ry-\sum_r y_r\Big)^2 \geqslant \sum_{r<s}(y_r-y_s)^2.$$

Stosując tę nierówność dla kolejnych współrzędnych wektorów x, x_i $(i = 1,\ldots, R)$ i korzystając z faktu, że $|x|^2 = x_1^2+x_2^2+\ldots+x_n^2$, na mocy (10) otrzymujemy

$$R\sum_{1\leqslant r\leqslant R} |x-x_r|^2 \geqslant \sum_{r<s} |x_r-x_s|^2 \geqslant 2R(R-1).$$

Zatem zachodzi nierówność (11). Lemat 1 jest udowodniony.

TWIERDZENIE 5. *Niech* x_r $(1 \leqslant r \leqslant R)$ *będą punktami leżącymi w* n*-wymiarowej kuli* $|x| \leqslant X$ *i niech* $|x_r-x_s| \geqslant 2$ $(1 \leqslant r < s \leqslant R)$.

Wtedy

$$R \leqslant 2^{-n/2}\,(1+n/2)\,(X+2^{1/2})^n.$$

Dowód. Niech $\varphi(x)$ będzie funkcją daną w lemacie 1. Otrzymujemy

$$V(\varphi) = \int \varphi(x)\,dx = \int_{|x|^2<2} (1-\tfrac{1}{2}|x|^2)\,dx = 2^{n/2}(1+n/2)^{-1}V_n,$$

gdzie V_n oznacza objętość kuli jednostkowej.

Ostatnia równość wynika z następującego wzoru:

$$I_n = \int_{|x|^2<2} |x|^2\,dx = 2^{1+n/2}\,\frac{n}{n+2}\,V_n, \tag{12}$$

który wyprowadzimy. Dokonując podstawienia $x = 2^{1/2}y$ i zastępując następnie $\boldsymbol{y}$ przez $\boldsymbol{x}$, mamy

$$I_n = 2^{1+n/2} \int\limits_{|\boldsymbol{x}|^2<1} |\boldsymbol{x}|^2 d\boldsymbol{x} = 2^{1+n/2} K_n. \tag{13}$$

W celu obliczenia K_n wprowadzimy uogólnione współrzędne sferyczne:

$$\begin{aligned} x_1 &= r \sin \varphi_1, \\ x_k &= r \cos \varphi_1 \dots \cos \varphi_{k-1} \sin \varphi_k, \quad k = 2, \dots, n-1, \\ x_n &= r \cos \varphi_1 \dots \cos \varphi_{n-1}. \end{aligned} \tag{14}$$

Wartość bezwzględna jakobianu J przekształcenia (14) wynosi

$$|J| = \left| \frac{\partial(x)}{\partial(r, \varphi)} \right| = r^{n-1} J(\varphi), \quad \text{gdzie } \varphi = [\varphi_1, \dots, \varphi_{n-1}]^T.$$

Stąd mamy

$$V_n = \int\limits_{|\boldsymbol{x}|^2<1} d\boldsymbol{x} = \iint\limits_{r,\varphi} r^{n-1} J(\varphi)\, dr d\varphi = T \int\limits_0^1 r^{n-1} dr = \frac{1}{n} T, \tag{15}$$

gdzie $T = \int\limits_{\varphi} J(\varphi)\, d\varphi$;

$$K_n = \int\limits_{|\boldsymbol{x}|^2<1} |\boldsymbol{x}|^2 d\boldsymbol{x} = \iint\limits_{r,\varphi} r^{n+1} J(\varphi) dr d\varphi = T \int\limits_0^1 r^{n+1} dr = \frac{1}{n+2} T = \frac{n}{n+2} V_n$$

na mocy (15). Stąd i z (13) otrzymujemy (12).

Teza twierdzenia 5 wynika z nierówności (9), ponieważ $\mathscr{T}(\varrho)$ jest w naszym przypadku kulą $|\boldsymbol{x}| < X + 2^{1/2}$ o objętości $(X+2^{1/2})^n V_n$. Twierdzenie 5 jest więc udowodnione.

Wniosek 1. *Wyróżnik krytyczny Γ_n i objętość V_n kuli jednostkowej $|\boldsymbol{x}| < 1$ spełniają nierówność*

$$\Gamma_n \geqslant 2^{-n/2}(1+n/2)^{-1} V_n.$$

Dowód. Niech Λ będzie kratą dopuszczalną dla kuli $|\boldsymbol{x}| < 1$. Punkty $\boldsymbol{x}_r$ kraty 2Λ spełniają założenia twierdzenia 5. Rzeczywiście:

$$\boldsymbol{x}_r - \boldsymbol{x}_s = 2\boldsymbol{y}, \quad \boldsymbol{y} \in \Lambda, \quad |\boldsymbol{x}_r - \boldsymbol{x}_s| = 2|\boldsymbol{y}| \geqslant 2 \quad (1 \leqslant r < s \leqslant R).$$

Niech $N(X)$ oznacza ilość punktów kraty 2Λ w kuli

$$D_n(X) = \{\boldsymbol{x};\ |\boldsymbol{x}| < X\}.$$

Na mocy wzoru (4)

$$\lim_{x \to \infty} N(X)/(X^n) = V_n/(2^n d(\Lambda)). \tag{16}$$

Z drugiej strony na mocy twierdzenia 5

$$\lim N(X)/(X^n) \leqslant 2^{-n/2}(1+n/2).$$

Stąd i z (16)

$$d(\Lambda) \geqslant 2^{-n/2}(1+n/2)^{-1}V_n.$$

Teza wniosku wynika łatwo z określenia wyróżnika krytycznego. Połóżmy $V_n(X) = V(D_n(X))$.

TWIERDZENIE 6. *Niech Λ będzie kratą pełną o wyróżniku $d(\Lambda)$. Jeżeli*

$$V_n(X) > 2^{n/2}(1+n/2)\, d(\Lambda),$$

to kula $D_n(X)$ zawiera punkt kraty Λ różny od początku układu współrzędnych.

Dowód. Oczywiście objętość i wyróżnik krytyczny kuli $D_n(X)$ są równe odpowiednio:

$$V_n(X) = X^n V_n, \qquad \Delta(D_n(X)) = X^n \Gamma_n.$$

Stąd z założenia twierdzenia oraz wniosku 1 otrzymujemy

$$\Delta(D_n(X)) \geqslant 2^{-n/2}(1+n/2)^{-1} \cdot V_n(X) > d(\Lambda).$$

Teza twierdzenia 6 wynika łatwo z określenia wyróżnika krytycznego.

Uwaga 1. Twierdzenie 6 jest silniejsze niż twierdzenie 4 (Minkowskiego) w przypadku $\mathscr{S} = D_n(X)$.

Przejdziemy teraz do zastosowań geometrii liczb dotyczących istnienia baz ortonormalnych dla pewnych krat. Zachodzi następujący

LEMAT 2. *Niech $1 \leqslant n \leqslant 7$. Jeżeli wyróżnik kraty pełnej Λ jest równy jedności, a iloczyn skalarny dwóch dowolnych jej punktów jest całkowity, to istnieje punkt $x \in \Lambda$ taki, że $|x| = 1$.*

Dowód. W twierdzeniu 6 połóżmy $d(\Lambda) = 1$, $X = \sqrt{2}$. Jeżeli $1 \leqslant n \leqslant 7$, to

$$V_n(X) = 2^{n/2}\pi^{n/2}/\Gamma(1+n/2) > 2^{n/2}(1+n/2)\, d(\Lambda).$$

Na mocy twierdzenia 6 istnieje punkt $x \in \Lambda$ taki, że $0 < |x|^2 < 2$. Ponieważ $|x|^2 = (x, x)$ jest liczbą całkowitą, to ostatnia nierówność oznacza, że $|x| = 1$, c.b.d.o.

Uwaga 2. Jeżeli $n \leqslant 4$, to lemat 2 wynika również z twierdzenia Minkowskiego o obszarze wypukłym, ponieważ kula $D_n(\sqrt{2})$ ma objętość większą niż 2^n.

Mówimy, że układ punktów $a_1, \ldots, a_k$ jest *ortonormalny*, jeżeli zachodzi warunek

$$(a_i, a_j) = \begin{cases} 0 & \text{dla } i \neq j, \\ 1 & \text{dla } i = j. \end{cases}$$

Wiadomo dobrze, że układ ortonormalny jest liniowo niezależny.

Niech φ będzie przekształceniem liniowym nieosobliwym przestrzeni R^n na siebie. Niech Λ będzie kratą o bazie $a_1, \ldots, a_k$ ($k \leqslant n$). Zbiór $\varphi\Lambda$ jest kratą o bazie $\varphi a_1, \ldots, \varphi a_k$. Wiadomo, że przekształcenie liniowe φ przestrzeni R^n w siebie nazywamy *ortogonalnym*, jeżeli nie zmienia iloczynu skalarnego punktów. Przekształ-

cenie ortogonalne jest nieosobliwe. Wyróżnik kraty pełnej jest niezmiennikiem przekształceń ortogonalnych, to znaczy

$$d(\varphi\Lambda) = d(\Lambda). \tag{17}$$

Rzeczywiście, na mocy twierdzenia Cauchy'ego o mnożeniu wyznaczników mamy

$$d(\varphi\Lambda) = |\det[\varphi\boldsymbol{a}_1,\ldots,\varphi\boldsymbol{a}_n]| = |\det(\varphi\boldsymbol{a}_i,\ \varphi\boldsymbol{a}_j)|^{1/2} = |\det(\boldsymbol{a}_i,\boldsymbol{a}_j)|^{1/2} =$$
$$= |\det[\boldsymbol{a}_1,\ldots,\boldsymbol{a}_n]| = d(\Lambda).$$

LEMAT 3. *Niech* $1 \leqslant n \leqslant 7$. *Jeżeli wyróżnik kraty pełnej* K *jest równy jedności, a iloczyn skalarny dwóch dowolnych jej punktów jest całkowity, to krata* K *ma bazę ortonormalną.*

Dowód. Dowód przeprowadzimy przez indukcję względem n. Dla $n = 1$ lemat jest oczywisty. Załóżmy słuszność lematu dla $n-1$, gdzie $2 \leqslant n \leqslant 7$. Wystarczy dowieść, że istnieje przekształcenie ortogonalne φ takie, że krata φK ma bazę ortonormalną. Na mocy lematu 2 istnieje punkt $\boldsymbol{x} \in K$, dla którego $|\boldsymbol{x}| = 1$. Istnieje przekształcenie ortogonalne φ przestrzeni R^n takie, że $\varphi\boldsymbol{x} = \boldsymbol{e}_1$ (patrz [2], str. 33–34), ponieważ $|\varphi\boldsymbol{x}| = 1$. Połóżmy $L = \varphi K \cap R^{n,1}$. Niech $\boldsymbol{y}$ będzie dowolnym punktem należącym do φK. Mamy

$$\boldsymbol{y} = y_1\boldsymbol{e}_1 + \boldsymbol{z}, \tag{18}$$

gdzie $y_1 = (\boldsymbol{y}, \boldsymbol{e}_1)$ oznacza pierwszą współrzędną punktu $\boldsymbol{y}$, a $\boldsymbol{z} \in R^{n,1}$.

Ponieważ $\boldsymbol{y}, \boldsymbol{e}_1 \in \varphi K$, więc y_1 jest liczbą całkowitą. Stąd $\boldsymbol{z} \in L$. Na mocy twierdzenia 1 krata L ma bazę całkowitą $\boldsymbol{a}_1,\ldots,\boldsymbol{a}_k$. Stąd i z (18)

$$\boldsymbol{y} = y_1\boldsymbol{e}_1 + z_1\boldsymbol{a}_1 + \ldots + z_k\boldsymbol{a}_k,$$

gdzie $y_1, z_1,\ldots,z_k$ są liczbami całkowitymi.

Ponieważ $\boldsymbol{a}_i \in R^{n,1}$, więc punkty $\boldsymbol{e}_1, \boldsymbol{a}_1,\ldots,\boldsymbol{a}_k$ są liniowo niezależne. Oznacza to, że punkty $\boldsymbol{e}_1, \boldsymbol{a}_1,\ldots,\boldsymbol{a}_k$ tworzą bazę kraty φK, a stąd $k = n-1$. Punkty $\boldsymbol{a}_1^{(1)},\ldots,\boldsymbol{a}_{n-1}^{(1)}$ tworzą oczywiście bazę kraty $L^{(1)}$. Dalej mamy $L^{(1)} \subset R^{n-1}$. Oznacza to, że krata $L^{(1)}$ jest pełna. Oczywiście iloczyn skalarny dwóch dowolnych punktów kraty $L^{(1)}$ jest całkowity. Dalej mamy

$$d(L^{(1)}) = |\det[\boldsymbol{a}_1^{(1)},\ldots,\boldsymbol{a}_{n-1}^{(1)}]| = |\det[\boldsymbol{e}_1,\boldsymbol{a}_1,\ldots,\boldsymbol{a}_{n-1}]| = d(\varphi K) = d(K) = 1$$

na mocy (17).

Na mocy założenia indukcyjnego krata $L^{(1)}$ ma bazę ortonormalną $\boldsymbol{b}_1^{(1)},\ldots,\boldsymbol{b}_{n-1}^{(1)}$, $\boldsymbol{b}_j \in L$, $j = 1,\ldots,n-1$. Ponieważ $\boldsymbol{z} \in L$, mamy:

$$\boldsymbol{y} = y_1\boldsymbol{e}_1 + \alpha_1\boldsymbol{b}_1 + \ldots + \alpha_{n-1}\boldsymbol{b}_{n-1},$$

gdzie y_1, α_1, $\ldots$, α_{n-1} są liczbami całkowitymi.

Ponieważ $\boldsymbol{b}_j \in R^{n,1}$, to punkty $\boldsymbol{e}_1, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{n-1}$, są liniowo niezależne i tworzą bazę ortonormalną kraty φK, c.b.d.o.

Przez *formę kwadratową symetryczną n zmiennych* będziemy rozumieć wyrażenie postaci: $f(\boldsymbol{x}) = \sum_{i,j=1}^{n} a_{ij} x_i x_j$, gdzie a_{ij} są rzeczywiste, a $a_{ij} = a_{ji}$.

Macierz kwadratową A o elementach całkowitych i o wyznaczniku równym ± 1 nazywamy *unimodularną*.

Mówimy, że dwie takie formy f i g są *równoważne*, jeżeli istnieje macierz unimodularna A taka, że $f(A\boldsymbol{x}) = g(\boldsymbol{x})$.

Uwaga 3. Lemat 3 jest równoważny następującemu dobrze znanemu twierdzeniu Hermite'a:

TWIERDZENIE 7. *Niech* $1 \leqslant n \leqslant 7$. *Każda forma kwadratowa n zmiennych, symetryczna, o współczynnikach całkowitych, dodatnio określona i o wyróżniku* 1 *jest równoważna formie* $x_1^2 + \ldots + x_n^2$.

Dowód. Z lematu 3 wynika twierdzenie 7. Niech $f(\boldsymbol{x})$ będzie formą kwadratową symetryczną n zmiennych ($1 \leqslant n \leqslant 7$) o współczynnikach całkowitych, dodatnio określoną, o wyróżniku 1; $f(\boldsymbol{x}, \boldsymbol{y})$ niech oznacza odpowiadającą jej formę dwuliniową, tzn. $f(\boldsymbol{x}, \boldsymbol{x}) = f(\boldsymbol{x})$. Istnieje macierz rzeczywista A taka, że

$$f(\boldsymbol{x}) = |A\boldsymbol{x}|^2, \quad \det A = 1. \tag{19}$$

Stąd mamy

$$(A\boldsymbol{x}_0, A\boldsymbol{y}_0) = \tfrac{1}{4}(|A\boldsymbol{x}_0 + A\boldsymbol{y}_0|^2 - |A\boldsymbol{x}_0 - A\boldsymbol{y}_0|^2) = \tfrac{1}{4}\big(|A(\boldsymbol{x}_0 + \boldsymbol{y}_0)|^2 - |A(\boldsymbol{x}_0 - \boldsymbol{y}_0)|^2\big) =$$
$$= \tfrac{1}{4}[f(\boldsymbol{x}_0 + \boldsymbol{y}_0) - f(\boldsymbol{x}_0 - \boldsymbol{y}_0)] = f(\boldsymbol{x}_0, \boldsymbol{y}_0),$$

a więc $(A\boldsymbol{x}_0, A\boldsymbol{y}_0)$ jest całkowite dla $\boldsymbol{x}_0, \boldsymbol{y}_0 \in \Lambda_0$. Oznacza to, że iloczyn skalarny dowolnych dwóch punktów kraty $A\Lambda_0$ jest całkowity. Wyróżnik jej wynosi 1 na mocy (19). Na mocy lematu 3 istnieje macierz ortogonalna B taka, że $A\Lambda_0 = B\Lambda_0$, czyli $\Lambda_0 = A^{-1}B\Lambda_0$. A więc macierz $A^{-1}B$ jest unimodularna. Dalej na mocy (19) mamy

$$f(A^{-1}B\boldsymbol{x}) = |B\boldsymbol{x}|^2 = |\boldsymbol{x}|^2.$$

Z twierdzenia 7 wynika lemat 3. Niech K będzie kratą, o której mowa w lemacie 3. Istnieje więc macierz rzeczywista B taka, że

$$K = B\Lambda_0, \quad \det B = 1. \tag{20}$$

Forma kwadratowa $|Bx|^2$ ma współczynniki całkowite, gdyż liczby $(B\boldsymbol{x}_0, B\boldsymbol{y}_0)$ są całkowite dla $\boldsymbol{x}_0, \boldsymbol{y}_0 \in \Lambda_0$ na mocy (20). Wspomniana forma jest dodatnio określona, symetryczna, jej wyróżnik jest równy jedności, gdyż otrzymujemy ją z formy kwadratowej $|\boldsymbol{y}|^2$ przez podstawienie $\boldsymbol{y} = B\boldsymbol{x}$, $\det B = 1$.

Na mocy twierdzenia 7 istnieje macierz unimodularna A taka, że $|BA\boldsymbol{x}|^2 = |\boldsymbol{x}|^2$. Oznacza to, że macierz BA jest ortogonalna. Dalej na mocy (20) mamy $\Lambda_0 = A\Lambda_0$, $K = B\Lambda_0 = BA\Lambda_0$.

Niech K_1, K_2 będą podkratami kraty K. Wprowadzamy definicje:

$$K_1+K_2=\{\boldsymbol{a}_1+\boldsymbol{a}_2 |\ \boldsymbol{a}_1\in K_1,\ \boldsymbol{a}_2\in K_2\}.$$

Niech $\boldsymbol{Z}$ oznacza zbiór liczb całkowitych. Przez kratę $\boldsymbol{Zx}$ będziemy rozumieć zbiór punktów postaci $z\boldsymbol{x}$, gdzie $z\in\boldsymbol{Z}$.

TWIERDZENIE 8. *Niech* $1\leqslant n\leqslant 7$, *zaś* $\boldsymbol{x}$ *niech będzie punktem wymiernym, dla którego* $(\boldsymbol{x},\boldsymbol{x})\in\boldsymbol{Z}$ *i* $M=\{\boldsymbol{u}\in\Lambda_0 |\ (\boldsymbol{u},\boldsymbol{x})\in\boldsymbol{Z}\}$. *Krata* $M+\boldsymbol{Zx}$ *jest pełna i ma bazę ortonormalną.*

LEMAT 4. *Załóżmy, że krata K ma bazę trójkątną:*

$$[a_{11},\ldots,a_{n1}]^T,\ [0,a_{22},\ldots,a_{n2}]^T,\ \ldots,\ [0,\ldots,0,a_{kk},\ldots,a_{nk}]^T$$
$$(k\leqslant n),\ a_{ii}\neq 0\ (1\leqslant i\leqslant k).$$

Jeżeli punkt $[0,\ldots,0,b_i,\ldots,b_n]^T$ *należy do K, to* b_i/a_{ii} *jest liczbą całkowitą.*

Dowód lematu jest natychmiastowy.

LEMAT 5. *Niech* $\boldsymbol{x}$ *będzie punktem wymiernym takim, że* $(\boldsymbol{x},\boldsymbol{x})\in\boldsymbol{Z}$ *i niech* $M=\{\boldsymbol{u}\in\Lambda_0 |\ (\boldsymbol{u},\boldsymbol{x})\in\boldsymbol{Z}\}$. *Krata* $M+\boldsymbol{Zx}$ *jest pełna, jej wyróżnik jest równy jedności, zaś iloczyn skalarny dwóch dowolnych jej punktów jest całkowity.*

Dowód. Połóżmy $K=M+\boldsymbol{Zx}$:

$$\boldsymbol{x}=[x_1/d,\ldots,x_n/d]^T,\quad x_1,\ldots,x_n,d\in\boldsymbol{Z},\ (x_1,\ldots,x_n,d)=1. \tag{21}$$

Do kraty K należą punkty:

$$\boldsymbol{d}_1=[d,\ldots,0]^T,\ \boldsymbol{d}_2=[0,d,\ldots,0]^T,\ldots,\boldsymbol{d}_n=[0,\ldots,0,d]^T.$$

Oznacza to, że krata K jest pełna.

Jeżeli $\boldsymbol{u}+t\boldsymbol{x},\ \boldsymbol{v}+s\boldsymbol{x}\in K$, to

$$(\boldsymbol{u}+t\boldsymbol{x},\ \boldsymbol{v}+s\boldsymbol{x})=(\boldsymbol{u},\boldsymbol{v})+t(\boldsymbol{x},\boldsymbol{v})+s(\boldsymbol{u},\boldsymbol{x})+ts(\boldsymbol{x},\boldsymbol{x})\in\boldsymbol{Z}$$

na mocy definicji M, czyli iloczyn skalarny dwóch dowolnych punktów kraty K jest całkowity. Należy dowieść, że $d(K)=1$. Dla $n=1$ lemat jest oczywisty. Możemy więc założyć, że $n>1$.

Na mocy twierdzenia 2 krata pełna K ma bazę trójkątną:

$$\boldsymbol{a}_1=[a_{11}/d,\ldots,a_{n1}/d]^T,\ \boldsymbol{a}_2=[0,a_{22}/d,\ldots,a_{2n}/d]^T,\ \ldots,\ \boldsymbol{a}_n=[0,\ldots,0,a_{nn}/d],$$
$$a_{ii}\neq 0,\ a_{ij}\in\boldsymbol{Z}.$$

Stąd $d(K)=a_{11}a_{22}\ldots a_{nn}/d^n=D/d^n$.

Niech p będzie dowolną liczbą pierwszą. Nie zmniejszając ogólności na mocy (21) oraz $(\boldsymbol{x},\boldsymbol{x})\in\boldsymbol{Z}$ możemy założyć, że

$$\text{Jeżeli } p\mid d,\ \text{to } p\nmid x_1\ \ldots p\nmid x_n. \tag{22}$$

Połóżmy

$$D=p^{\mu}D_1,\quad d=p^{\nu}d_1,\quad p\nmid D_1d_1,\quad \mu,\nu\geqslant 0.$$

Dla zakończenia dowodu wystarczy dowieść, że $\mu = nv$, wówczas bowiem $d(K) = 1$. Połóżmy $a_{ii} = p^{v_i} b_i$, $p \nmid b_i$ $(i = 1,\ldots, n)$. Ponieważ $\boldsymbol{x}, \boldsymbol{d}_i \in K$, na mocy lematu 4 mamy

$$a_{11} | x_1, \quad a_{ii} | d^2 \quad (i = 1,\ldots, n). \tag{23}$$

Stąd i z (22)

$$v_1 = 0. \tag{24}$$

Mamy dalej $p \nmid (x_{k+1},\ldots, x_n, d)$ $(k = 2,\ldots, n-1)$, a stąd

$$(x_{k+1},\ldots, x_n, d) | d_1 x_k.$$

Oznacza to, że równanie

$$d_1 x_k + u_{k+1} x_{k+1} + \ldots + u_n x_n = td$$

ma rozwiązanie w liczbach całkowitych $u_{k+1},\ldots, u_n, t$. Stąd punkt $[0,\ldots, 0, d_1, u_{k+1},\ldots, u_n]^T$ należy do K.

Na mocy lematu 4 $a_{kk} | d d_1$, stąd

$$v_k \leqslant v \quad (k = 1,\ldots, n-1). \tag{25}$$

Na mocy (23)

$$v_n \leqslant 2v. \tag{26}$$

Ponieważ $a_k \in K$ $(k = 2,\ldots, n-1)$, więc istnieją liczby całkowite v_{1k}, v_{kk}, t_k takie, że

$$0 = v_{1k} d + t_k x_1, \quad a_{kk} = v_{kk} d + t_k x_k.$$

Stąd $t_k x_1 \equiv 0 \bmod p^v$, $t_k \equiv 0 \bmod p^v$ na mocy (22), $a_{kk} \equiv 0 \bmod p^v$, czyli

$$v \leqslant v_k \quad (k = 2,\ldots, n-1). \tag{27}$$

Ponieważ $\boldsymbol{x}, \boldsymbol{a}_n \in K$, na mocy udowodnionej już ostatniej części tezy lematu 5 mamy $(\boldsymbol{a}_n, \boldsymbol{x}) \in \boldsymbol{Z}$. Stąd $a_{nn} x_n \equiv 0 \bmod d^2$, $a_{nn} \equiv 0 \bmod p^{2v}$ na mocy (22). Zatem

$$2v \leqslant v_n. \tag{28}$$

Wobec (24), (25), (26), (27) i (28)

$$v_1 = 0, \quad v_k = v \quad (k = 2,\ldots, n-1), \quad v_n = 2v,$$

$$D = a_{11} \ldots a_{nn} = p^{nv} b_1 \ldots b_n, \quad p \nmid b_1 \ldots b_n,$$

a więc $\mu = nv$, c.b.d.o.

Dowód twierdzenia 8. Teza twierdzenia wynika natychmiast z lematów 5 i 3. Korzystając z twierdzenia 8 możemy również wyprowadzić następujące twierdzenia:

TWIERDZENIE 9. *Niech* $3 \leqslant n \leqslant 7$. *Dla każdej liczby naturalnej* m *istnieją liczby naturalne* $x_1,\ldots, x_n$ *względnie pierwsze takie, że*

$$m^2 = x_1^2 + \ldots + x_n^2$$

z wyjątkiem przypadków

$$\begin{aligned} &n = 3, \quad m \equiv 0 \bmod 2, \quad m = 1, 5, \\ &n = 4, \quad m \equiv 0 \bmod 4, \quad m = 1, 3, \\ &n = 5, \quad m = 1, 2, 3, \\ &n = 6, \quad m = 1, 2, 4, \\ &n = 7, \quad m = 1, 2, 3. \end{aligned}$$

TWIERDZENIE 10. *Niech* $n \geqslant 5$. *Dla każdej liczby naturalnej* m *istnieją liczby naturalne* $x_1, \ldots, x_n$ *względnie pierwsze takie, że*

$$m^2 = x_1^2 + \ldots + x_n^2$$

z wyjątkiem przypadków, gdy m^2 *należy do ciągu*

$$1, 2, 3, \ldots, n-1, n+1, n+2, n+4, n+5, n+7, n+10, n+13.$$

Dowody tych twierdzeń stanowią treść § 3 pracy [8]. Twierdzenie 8 niniejszego artykułu jest identyczne z lematem 2 podanym w pracy [8].

Pewne zastosowania geometrii liczb do przedstawień liczb całkowitych przez formy kwadratowe można znaleźć w [3], str. 98–102, w [4], str. 206–210, oraz [1], str. 316–319.

Prace cytowane

[1] N. C. Ankeny, *Sums of three squares*, Proc. Amer. Math. Soc. 8 (1957), str. 316–319.
[2] K. Borsuk, *Geometria analityczna wielowymiarowa*, Warszawa 1964.
[3] J. W. S. Cassels, *An introduction to the geometry of numbers*, Berlin–Göttingen–Heidelberg 1959.
[4] H. Davenport, *The geometry of numbers*, Mathematical Gazette 31 (1947), str. 206–210.
[5] C. G. Lekkerkerker, *Geometry of numbers*, Wolters-Nordhoff Publ., Groningen 1969.
[6] H. Mann, *Introduction to algebraic number theory*, The Ohio State University Press, Columbus 1955.
[7] З. И. Боревич, И. Р. Шафаревич, *Теория чисел*, Москва 1964.
[8] J. Wójcik, *On rational automorphs of quadratic forms*, Colloq. Math. 30 (1974), str. 69–88.