Geometria z Algebrą Liniową II*

Arkadiusz Męcel

WYKŁAD 14, 27.04.2021 r.

Definicja

Niech V będzie przestrzenią liniową nad ciałem K. Funkcję $q : V \to K$ nazywamy **formą kwadratową na przestrzeni** V, jeśli istnieje forma dwuliniowa $h : V \times V \to K$ taka, że dla każdego $\alpha \in V$ zachodzi $q(\alpha) = h(\alpha, \alpha)$.

Definicja

Niech V będzie przestrzenią liniową nad ciałem K. Funkcję $q : V \to K$ nazywamy **formą kwadratową na przestrzeni** V, jeśli istnieje forma dwuliniowa $h : V \times V \to K$ taka, że dla każdego $\alpha \in V$ zachodzi $q(\alpha) = h(\alpha, \alpha)$.

- **Przykład 1.** Na przestrzeni $\mathbb{R}^2$ mamy formę kwadratową q zadaną wzorem

$$q((x_1, x_2)) = 3x_1^2 + 6x_1x_2 - 4x_2^2,$$

bo $q(\alpha) = h(\alpha, \alpha)$, gdzie h jest formą dwuliniową na $\mathbb{R}^2$ postaci:

$$h((x_1, x_2), (y_1, y_2)) = 3x_1y_1 + 6x_1y_2 - 4x_2y_2,$$

Definicja

Niech V będzie przestrzenią liniową nad ciałem K. Funkcję $q : V \to K$ nazywamy **formą kwadratową na przestrzeni** V, jeśli istnieje forma dwuliniowa $h : V \times V \to K$ taka, że dla każdego $\alpha \in V$ zachodzi $q(\alpha) = h(\alpha, \alpha)$.

- **Przykład 1.** Na przestrzeni $\mathbb{R}^2$ mamy formę kwadratową q zadaną wzorem
$$q((x_1, x_2)) = 3x_1^2 + 6x_1x_2 - 4x_2^2,$$
bo $q(\alpha) = h(\alpha, \alpha)$, gdzie h jest formą dwuliniową na $\mathbb{R}^2$ postaci:
$$h((x_1, x_2), (y_1, y_2)) = 3x_1y_1 + 6x_1y_2 - 4x_2y_2,$$
- **Przykład 2.** Na przestrzeni $\mathbb{Q}^4$ mamy formę kwadratową q zadaną wzorem
$$q((x_1, x_2, x_3, x_4)) = x_1^2 + 8x_1x_2 + 7x_2^2 + 2x_3x_4,$$
bo $q(\alpha) = h(\alpha, \alpha)$, gdzie h jest formą dwuliniową na $\mathbb{Q}^4$ postaci:
$$h((x_1, x_2, x_3, x_4), (y_1, y_2, y_3, y_4)) = x_1y_1 + 4x_1y_2 + 4x_2y_1 + 7x_2y_2 + x_3y_4 + x_4y_3.$$

Uwaga

Niech V – sk. wymiarowa nad K i niech $(\alpha_1, \ldots, \alpha_n)$ będzie bazą przestrzeni V. Wówczas $q : V \to K$ jest formą kwadratową na V wtedy i tylko wtedy, gdy istnieją $a_{ij} \in K$, dla $i, j = 1, \ldots, n$ takie, że dla każdych $x_1, \ldots, x_n \in K$ zachodzi równość:

$$q(x_1\alpha_1 + \ldots + x_n\alpha_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j.$$

Uwaga

Niech V – sk. wymiarowa nad K i niech $(\alpha_1, \ldots, \alpha_n)$ będzie bazą przestrzeni V. Wówczas $q : V \to K$ jest formą kwadratową na V wtedy i tylko wtedy, gdy istnieją $a_{ij} \in K$, dla $i, j = 1, \ldots, n$ takie, że dla każdych $x_1, \ldots, x_n \in K$ zachodzi równość:

$$q(x_1\alpha_1 + \ldots + x_n\alpha_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j.$$

Dowód w jedną stronę. Niech $q(\alpha) = h(\alpha, \alpha)$, dla pewnej formy dwuliniowej h na V. Niech $a_{ij} = h(\alpha_i, \alpha_j)$. Dla każdych $x_1, \ldots, x_n$, $y_1, \ldots, y_n \in K$ mamy:

$$h(x_1\alpha_1 + \ldots + x_n\alpha_n, y_1\alpha_1 + \ldots + y_n\alpha_n) = \sum_{i,j=1}^{n} a_{ij}x_iy_j,$$

a więc w szczególności $q(x_1\alpha_1 + \ldots + x_n\alpha_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j$.

Uwaga

Niech V – sk. wymiarowa nad K i niech $(\alpha_1, \ldots, \alpha_n)$ będzie bazą przestrzeni V. Wówczas $q : V \to K$ jest formą kwadratową na V wtedy i tylko wtedy, gdy istnieją $a_{ij} \in K$, dla $i, j = 1, \ldots, n$ takie, że dla każdych $x_1, \ldots, x_n \in K$ zachodzi równość:

$$q(x_1\alpha_1 + \ldots + x_n\alpha_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j.$$

Dowód w drugą stronę. Mając $q(x_1\alpha_1 + \ldots + x_n\alpha_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j$. dla każdych $x_1, \ldots, x_n \in K$ zadajemy formę dwuliniową $h : V \times V \to K$ wzorem

$$h(x_1\alpha_1 + \ldots + x_n\alpha_n, y_1\alpha_1 + \ldots + y_n\alpha_n) = \sum_{i,j=1}^{n} a_{ij}x_iy_j.$$

Wówczas dla każdego $\alpha = x_1\alpha_1 + \ldots + x_n\alpha_n$ mamy $h(\alpha, \alpha) = q(\alpha)$.

Stwierdzenie

Niech V będzie przestrzenią liniową nad ciałem K charakterystyki różnej od 2. Przyporządkowania:

- $h \mapsto q$, gdzie $q(\alpha) = h(\alpha, \alpha)$, dla każdego $\alpha \in V$
- $q \mapsto h$, gdzie $h(\alpha, \beta) = \frac{1}{2}\left(q(\alpha + \beta) - q(\alpha) - q(\beta)\right)$

zadają bijekcje pomiędzy formami dwuliniowymi symetrycznymi na przestrzeni V a formami kwadratowymi na przestrzeni V.

Stwierdzenie

Niech V będzie przestrzenią liniową nad ciałem K charakterystyki różnej od 2. Przyporządkowania:

- $h \mapsto q$, gdzie $q(\alpha) = h(\alpha, \alpha)$, dla każdego $\alpha \in V$
- $q \mapsto h$, gdzie $h(\alpha, \beta) = \frac{1}{2}(q(\alpha + \beta) - q(\alpha) - q(\beta))$

zadają bijekcje pomiędzy formami dwuliniowymi symetrycznymi na przestrzeni V a formami kwadratowymi na przestrzeni V.

Przykład. Dla formy kwadratowej na $\mathbb{R}^2$ danej wzorem

$$q((x_1, x_2)) = 3x_1^2 + 6x_1x_2 - 4x_2^2$$

mamy $q((x_1, x_2)) = h((x_1, x_2), (y_1, y_2)$ np. dla

- $h((x_1, x_2), (y_1, y_2)) = 3x_1y_1 + 2x_1y_2 + 4x_2y_1 - 4x_2y_2$,
- $h((x_1, x_2), (y_1, y_2)) = 3x_1y_1 + 6x_1y_2 \quad\quad - 4x_2y_2$,
- $h((x_1, x_2), (y_1, y_2)) = 3x_1y_1 + 3x_1y_2 + 3x_2y_1 - 4x_2y_2$.

Stwierdzenie

Niech V będzie przestrzenią liniową nad ciałem K charakterystyki różnej od 2. Przyporządkowania:

- $h \mapsto q$, gdzie $q(\alpha) = h(\alpha, \alpha)$, dla każdego $\alpha \in V$
- $q \mapsto h$, gdzie $h(\alpha, \beta) = \frac{1}{2}(q(\alpha + \beta) - q(\alpha) - q(\beta))$

zadają bijekcje pomiędzy formami dwuliniowymi symetrycznymi na przestrzeni V a formami kwadratowymi na przestrzeni V.

Dowód. Niech $h' : V \times V \to K$ będzie formą dwuliniową taką, że dla każdego $\alpha \in V$ zachodzi $q(\alpha) = h'(\alpha, \alpha)$. Wówczas funkcja $h(\alpha, \beta) = \frac{1}{2}(h'(\alpha, \beta) + h'(\beta, \alpha))$ jest formą dwuliniową symetryczną na V i $q(\alpha) = h'(\alpha, \alpha) = h(\alpha, \alpha)$, dla $\alpha \in V$.

Stwierdzenie

Niech V będzie przestrzenią liniową nad ciałem K charakterystyki różnej od 2. Przyporządkowania:

- $h \mapsto q$, gdzie $q(\alpha) = h(\alpha, \alpha)$, dla każdego $\alpha \in V$
- $q \mapsto h$, gdzie $h(\alpha, \beta) = \frac{1}{2}(q(\alpha + \beta) - q(\alpha) - q(\beta))$

zadają bijekcje pomiędzy formami dwuliniowymi symetrycznymi na przestrzeni V a formami kwadratowymi na przestrzeni V.

Dowód. Niech $h' : V \times V \to K$ będzie formą dwuliniową taką, że dla każdego $\alpha \in V$ zachodzi $q(\alpha) = h'(\alpha, \alpha)$. Wówczas funkcja $h(\alpha, \beta) = \frac{1}{2}(h'(\alpha, \beta) + h'(\beta, \alpha))$ jest formą dwuliniową symetryczną na V i $q(\alpha) = h'(\alpha, \alpha) = h(\alpha, \alpha)$, dla $\alpha \in V$.

Jeśli zaś h jest formą dwuliniową symetryczną spełniającą $q(\alpha) = h(\alpha, \alpha)$ dla $\alpha \in V$, to h jest wyznaczona jednoznacznie przez q, bo mamy

$$\frac{1}{2}(q(\alpha + \beta) - q(\alpha) - q(\beta)) = \frac{1}{2}(h(\alpha + \beta, \alpha + \beta) - h(\alpha, \alpha) - h(\beta, \beta)) = h(\alpha, \beta).$$

Uwaga. Od tej pory zakładamy, że wszystkie ciała są charakterystyki różne od 2.

Definicja

Niech $q : V \to K$ będzie formą kwadratową na skończenie wymiarowej przestrzeni liniowej. **Macierzą formy kwadratowe**j q w bazie $\mathcal{A}$ przestrzeni V nazywamy macierz formy dwuliniowej symetrycznej odpowiadającej formie q. Macierz formy kwadratowej q w bazie $\mathcal{A}$ oznaczamy $G(q; \mathcal{A})$. Zatem $G(q; \mathcal{A}) = G(h; \mathcal{A})$ gdzie $h : V \times V \to K$ jest formą dwuliniową symetryczną spełniającą $q(\alpha) = h(\alpha, \alpha)$, dla każdego $\alpha \in V$.

Przykład. Dla $q : \mathbb{R}^2 \to \mathbb{R}$ zadanej wzorem $q((x_1, x_2)) = x_1^2 + 3x_1x_2 + 7x_2^2$ mamy

- $G(q; st) = \begin{bmatrix} 1 & \frac{3}{2} \\ \frac{3}{2} & 7 \end{bmatrix}$,
- $G(q; \mathcal{A}) = \begin{bmatrix} 11 & -6 \\ -6 & 5 \end{bmatrix}$, w bazie $\mathcal{A} = ((1, 1), (1, -1))$.

Fakt

Jesli $A = [a_{ij}]$ jest macierzą formy kwadratowej q w bazie $\mathcal{A} = (\alpha_1, \ldots, \alpha_n)$, to dla każdych $x_1, \ldots, x_n \in K$ zachodzi równość $q(x_1\alpha_1 + \ldots + x_n\alpha_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j$.

Fakt

Jeśli A, B są macierzami formy kwadratowej q w bazach $\mathcal{A}$, $\mathcal{B}$ odpowiednio, to $B = C^TAC$, gdzie $C = M(\mathrm{id})_{\mathcal{B}}^{\mathcal{A}}$.

Fakt

Dla każdej formy kwadratowej q na skończenie wymiarowej przestrzeni V (gdzie $\mathrm{char}\, K \neq 2$) istnieje taka baza, w której macierz q ma macierz diagonalną, czyli taka baza $\mathcal{A} = (\alpha_1, \ldots, \alpha_n)$ przestrzeni V, że zachodzi równość

$$q(x_1\alpha_1 + \ldots + x_n\alpha_n) = a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2.$$

Definicja

Niech $f = f(x_1, \ldots, x_n)$ oraz $g = g(y_1, \ldots, y_n)$ będą formami kwadratowymi na skończenie wymiarowej przestrzeni V nad K. Powiemy, że formy f, g są **równoważne**, ozn. $f \cong g$, jeśli istnieje macierz odwracalna $P \in M_n(K)$ taka, że

$$\begin{aligned} x_1 &= p_{11}y_1 + p_{12}y_2 + \ldots + p_{1n}y_n \\ \vdots \quad &\vdots \qquad\quad \vdots \qquad \ddots \qquad \vdots \\ x_n &= p_{n1}y_1 + p_{n2}y_2 + \ldots + p_{nn}y_n, \end{aligned}$$

że $f(x_1, \ldots x_n) = g(y_1, \ldots, y_n)$, dla dowolnych $y_j \in K$.

Definicja

Niech $f = f(x_1, \ldots, x_n)$ oraz $g = g(y_1, \ldots, y_n)$ będą formami kwadratowymi na skończenie wymiarowej przestrzeni V nad K. Powiemy, że formy f, g są **równoważne**, ozn. $f \cong g$, jeśli istnieje macierz odwracalna $P \in M_n(K)$ taka, że

$$\begin{aligned} x_1 &= p_{11}y_1 + p_{12}y_2 + \ldots + p_{1n}y_n \\ &\vdots \quad \vdots \qquad \vdots \qquad \ddots \qquad \vdots \\ x_n &= p_{n1}y_1 + p_{n2}y_2 + \ldots + p_{nn}y_n, \end{aligned}$$

że $f(x_1, \ldots x_n) = g(y_1, \ldots, y_n)$, dla dowolnych $y_j \in K$.

Przykład. Następujące formy są równoważne nad $\mathbb{R}^4$:

$q_1((x_1, x_2, x_3, x_4)) = x_1^2 + 8x_1x_2 + 7x_2^2 + 2x_3x_4, \quad q_2((y_1, y_2, y_3, y_4)) = y_1^2 - 9y_2^2 + 2y_3^2 - 2y_4^2.$

bo $q_1(y_1 - 4y_2, y_2, y_3 + y_4, y_3 - y_4)$ równe jest

$(y_1 - 4y_2)^2 + 8(y_1 - 4y_2)y_2 + 7(y_2)^2 + 2(y_3 + y_4)(y_3 - y_4) = y_1^2 - 9y_2^2 + 2y_3^2 - 2y_4^2.$

Definicja

Niech $f = f(x_1, \ldots, x_n)$ oraz $g = g(y_1, \ldots, y_n)$ będą formami kwadratowymi na skończenie wymiarowej przestrzeni V nad K. Powiemy, że formy f, g są **równoważne**, ozn. $f \cong g$, jeśli istnieje macierz odwracalna $P \in M_n(K)$ taka, że

$$\begin{aligned} x_1 &= p_{11}y_1 + p_{12}y_2 + \ldots + p_{1n}y_n \\ &\vdots \quad \vdots \qquad \vdots \qquad \ddots \qquad \vdots \\ x_n &= p_{n1}y_1 + p_{n2}y_2 + \ldots + p_{nn}y_n, \end{aligned}$$

że $f(x_1, \ldots x_n) = g(y_1, \ldots, y_n)$, dla dowolnych $y_j \in K$.

Uwaga. Jeśli przyjąć $X = \begin{bmatrix} x_1 & \ldots & x_n \end{bmatrix}^T$, $Y = \begin{bmatrix} y_1 & \ldots & y_n \end{bmatrix}^T$, to układ wyżej ma postać $X = PY$. W szczególności jeśli $f(X) = X^T G(f, \mathcal{B})X$, dla pewnej bazy $\mathcal{B}$ przestrzeni K^n, to biorąc bazę $\mathcal{A}$ przestrzeni K^n taką, że $M(\mathrm{id})_{\mathcal{A}}^{\mathcal{B}} = P$ mamy:

$$g(Y) = f(X) = f(PY) = (PY)^T \cdot G(f; \mathcal{B}) \cdot PY = Y^T \cdot P^T G(f; \mathcal{B}) P \cdot Y = Y^T \cdot G(f, \mathcal{A}) \cdot Y.$$

Twierdzenie (Lagrange)

Niech V będzie przestrzenią nad ciałem K charakterystyki różnej od 2 o bazie $\mathcal{B} = (\beta_1, \ldots, \beta_n)$ oraz niech forma kwadratowa q zapisuje się w bazie $\mathcal{B}$ macierzą $G(q, \mathcal{B}) = [b_{ij}]$, czyli

$$q(x_1\beta_1 + \ldots + x_n\beta_n) = \sum_{i,j=1}^{n} b_{ij}x_iy_j.$$

Wówczas można wskazać taką zamianę zmiennych $X = PY$, że dla bazy $\mathcal{A} = (\alpha_1, \ldots, \alpha_n)$ przestrzeni V spełniającej $P = M(\mathrm{id})_{\mathcal{A}}^{\mathcal{B}}$ mamy

$$q(y_1\alpha_1 + \ldots + y_n\alpha_n) = a_1y_1^2 + \ldots + a_ny_n^2.$$

Twierdzenie (Lagrange)

Niech V będzie przestrzenią nad ciałem K charakterystyki różnej od 2 o bazie $\mathcal{B} = (\beta_1, \ldots, \beta_n)$ oraz niech forma kwadratowa q zapisuje się w bazie $\mathcal{B}$ macierzą $G(q, \mathcal{B}) = [b_{ij}]$, czyli

$$q(x_1\beta_1 + \ldots + x_n\beta_n) = \sum_{i,j=1}^{n} b_{ij}x_iy_j.$$

Wówczas można wskazać taką zamianę zmiennych $X = PY$, że dla bazy $\mathcal{A} = (\alpha_1, \ldots, \alpha_n)$ przestrzeni V spełniającej $P = M(\mathrm{id})_{\mathcal{A}}^{\mathcal{B}}$ mamy

$$q(y_1\alpha_1 + \ldots + y_n\alpha_n) = a_1y_1^2 + \ldots + a_ny_n^2.$$

Dowód. Indukcja po wymiarze V. Dla $n = 1$ jest jasne. Załóżmy, że opisaliśmy metodę dla $\dim V \leq n - 1$. Niech $\dim V = n$. Rozważamy dwa przypadki:

- Przypadek 1. Istnieje i takie, że $b_{ii} \neq 0$.
- Przypadek 2. Dla każdego i mamy $b_{ii} = 0$.

Dowód. Przypadek 1. Istnieje i takie, że $b_{ii} \neq 0$.

Bsog można założyć, że $b_{11} \neq 0$. Mamy $b_{ij} = b_{ji}$, czyli:

$$q(\sum_{i=1}^{n} x_i\beta_i) = \sum_{i,j=1}^{n} b_{ij}x_ix_j = b_{11}x_1^2 + 2b_{12}x_1x_2 + \ldots + 2b_{1n} + \sum_{i,j=2}^{n} b_{ij}x_ix_j =$$

$$= \frac{1}{b_{11}}(b_{11}x_1 + b_{12}x_2 + \ldots + b_{1n}x_n)^2 + \sum_{i,j=2}^{n} b'_{ij}x_ix_j$$

$$= \frac{1}{b_{11}}y_1^2 + \sum_{i,j=2}^{n} b'_{ij}y_iy_j$$

dla pewnych $b'_{ij} \in K$ oraz $y_1 = b_{11}x_1 + \ldots + b_{1n}x_n$, $y_j = x_j$, dla $j > 1$
(czyli zmieniliśmy bazę $\beta_1, \ldots, \beta_n$ na bazę $\gamma_1, \ldots, \gamma_n$ zadaną warunkiem
$\beta_1 = b_{11}\gamma_1, \beta_2 = b_{12}\gamma_1 + \gamma_2, \ldots, \beta_n = b_{1n}\gamma_1 + \gamma_n$, co daje $\sum_{i=1}^{n} x_i\beta_i = \sum_{i=1}^{n} y_i\gamma_i$).
Dalszy ciąg wynika z założenia indukcyjnego.

Dowód. Przypadek 2. Dla każdego i mamy $b_{ii} = 0$.

Jeśli $b_{ij} = 0$ to q jest zerowa i teza jest oczywista. Załóżmy (bsog), że $b_{12} \neq 0$. Wtedy podstawiając:

$$x_1 = y_1 + y_2, x_2 = y_1 - y_2, x_3 = y_3, \ldots, x_n = y_n,$$

(czyli zmieniając bazę $\beta_1, \ldots, \beta_n$ na bazę $\gamma_1, \ldots, \gamma_n$ zadaną warunkiem $\gamma_1 = \beta_1 + \beta_2, \gamma_2 = \beta_1 - \beta_3, \gamma_i = \beta_i, i > 2$), dostajemy $c_{ij} \in K$ takie, że:

$$q\left(\sum_{i=1}^{n} y_i \gamma_i\right) = \sum_{i,j=1}^{n} c_{ij} y_i y_j,$$

przy czym $c_{11} = b_{12} \neq 0$, co sprowadza tezę do Przypadku 1.

Dowód. Przypadek 2. Dla każdego i mamy $b_{ii} = 0$.

Jeśli $b_{ij} = 0$ to q jest zerowa i teza jest oczywista. Załóżmy (bsog), że $b_{12} \neq 0$. Wtedy podstawiając:

$$x_1 = y_1 + y_2, x_2 = y_1 - y_2, x_3 = y_3, \ldots, x_n = y_n,$$

(czyli zmieniając bazę $\beta_1, \ldots, \beta_n$ na bazę $\gamma_1, \ldots, \gamma_n$ zadaną warunkiem $\gamma_1 = \beta_1 + \beta_2, \gamma_2 = \beta_1 - \beta_3, \gamma_i = \beta_i, i > 2$), dostajemy $c_{ij} \in K$ takie, że:

$$q\left(\sum_{i=1}^{n} y_i \gamma_i\right) = \sum_{i,j=1}^{n} c_{ij} y_i y_j,$$

przy czym $c_{11} = b_{12} \neq 0$, co sprowadza tezę do Przypadku 1.

* * *

Inne metody diagonalizacji form kwadratowych:

- diagonalizacja odpowiadającej symetrycznej formy dwuliniowej,
- (nad $K = \mathbb{R}$) za pomocą wektorów własnych symetrycznej macierzy.

Dowód. Przypadek 2. Dla każdego i mamy $b_{ii} = 0$.

Jeśli $b_{ij} = 0$ to q jest zerowa i teza jest oczywista. Załóżmy (bsog), że $b_{12} \neq 0$. Wtedy podstawiając:

$$x_1 = y_1 + y_2, x_2 = y_1 - y_2, x_3 = y_3, \ldots, x_n = y_n,$$

(czyli zmieniając bazę $\beta_1, \ldots, \beta_n$ na bazę $\gamma_1, \ldots, \gamma_n$ zadaną warunkiem $\gamma_1 = \beta_1 + \beta_2, \gamma_2 = \beta_1 - \beta_3, \gamma_i = \beta_i, i > 2$), dostajemy $c_{ij} \in K$ takie, że:

$$q\left(\sum_{i=1}^{n} y_i \gamma_i\right) = \sum_{i,j=1}^{n} c_{ij} y_i y_j,$$

przy czym $c_{11} = b_{12} \neq 0$, co sprowadza tezę do Przypadku 1.

Wniosek

Niech $\operatorname{char} K \neq 2$. Formy kwadratowe $q_1 : V_1 \to K$ oraz $q_2 : V_2 \to K$ są równoważne nad K wtedy i tylko wtedy, gdy dla każdej bazy $\mathcal{A}_1$ p-ni V_1 oraz każdej bazy $\mathcal{A}_2$ p-ni V_2 macierze $G(q_1; \mathcal{A}_1)$, $G(q_2; \mathcal{A}_2)$ są kongruentne nad K.

Twierdzenie (przypomnienie)

Niech $(\mathbb{R}^n, \langle\ ,\ \rangle)$ będzie przestrzenią euklidesową ze standardowym iloczynem skalarnym oraz niech $q : V \to \mathbb{R}$ będzie formą kwadratową, którą w pewnej bazie $(\alpha_1, \ldots, \alpha_n)$ można przedstawić w postaci diagonalnej

$$q(x_1\alpha_1 + \ldots + x_n\alpha_n) = a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2,$$

przy czym $a_1 \geq a_2 \geq \ldots \geq a_n$. Niech $I \subseteq (\mathbb{R}^n, \langle\ ,\ \rangle)$ oznacza zbiór wektorów o normie 1. Wówczas na zbiorze I forma q ma największą wartość równą $q(\alpha_1/\|\alpha_1\|) = a_1$, a najmniejszą wartość równą $q(\alpha_n/\|\alpha_n\|) = a_n$.

Twierdzenie (przypomnienie)

Niech $(\mathbb{R}^n, \langle\ ,\ \rangle)$ będzie przestrzenią euklidesową ze standardowym iloczynem skalarnym oraz niech $q : V \to \mathbb{R}$ będzie formą kwadratową, którą w pewnej bazie $(\alpha_1, \ldots, \alpha_n)$ można przedstawić w postaci diagonalnej

$$q(x_1\alpha_1 + \ldots + x_n\alpha_n) = a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2,$$

przy czym $a_1 \geq a_2 \geq \ldots \geq a_n$. Niech $I \subseteq (\mathbb{R}^n, \langle\ ,\ \rangle)$ oznacza zbiór wektorów o normie 1. Wówczas na zbiorze I forma q ma największą wartość równą $q(\alpha_1/\|\alpha_1\|) = a_1$, a najmniejszą wartość równą $q(\alpha_n/\|\alpha_n\|) = a_n$.

Przykład. Wyznaczymy największą i najmniejszą wartość funkcji dwóch zmiennych $f : \mathbb{R}^2 \to \mathbb{R}$ postaci $f((x_1, x_2)) = x_1^2 + x_2^2 + 4x_1x_2$ na okręgu zadanym równaniem $x_1^2 + x_2^2 = 1$. Wykresem naszej funkcji jest pewna powierzchnia w $\mathbb{R}^3$. Wkrótce dowiemy się więcej na temat tego jak ona w zasadzie wygląda.

Przykład. Wyznaczymy największą i najmniejszą wartość funkcji dwóch zmiennych $f : \mathbb{R}^2 \to \mathbb{R}$ postaci $f((x_1, x_2)) = x_1^2 + x_2^2 + 4x_1x_2$ na okręgu zadanym równaniem $x_1^2 + x_2^2 = 1$. Wykresem naszej funkcji jest pewna powierzchnia w $\mathbb{R}^3$. Wkrótce dowiemy się więcej na temat tego jak ona w zasadzie wygląda.

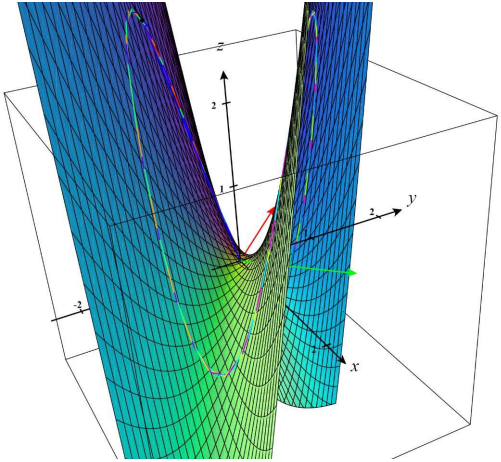
W bazie $(\alpha_1, \alpha_2) = ((1,1),(1,-1))$ (ortogonalnej w $(\mathbb{R}^2, \langle\ ,\ \rangle_{st})$) funkcja f *traktowana jako* forma kwadratowa ma postać

$$f(y_1\alpha_1 + y_2\alpha_2) = 3y_1^2 - y_2^2.$$

Twierdzenie mówi, że po wzięciu kierunków powyższych wektorów o normie 1, czyli $\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)$ oraz $\left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right)$ uzyskamy, że:

- największa wartość naszej funkcji na zbiorze I wynosi $f\left(\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)\right) = 3$,
- zaś najmniejsza wartość wynosi $f\left(\left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right)\right) = -1$.

Przykład. Wyznaczymy największą i najmniejszą wartość funkcji dwóch zmiennych $f : \mathbb{R}^2 \to \mathbb{R}$ postaci $f((x_1, x_2)) = x_1^2 + x_2^2 + 4x_1x_2$ na okręgu zadanym równaniem $x_1^2 + x_2^2 = 1$.



Obrazek wygenerowany online: https://www.monroecc.edu/faculty/paulseeburger/calcnsf/CalcPlot3D/

Definicja

Niech q będzie formą kwadratową na przestrzeni V nad[a] $\mathbb{R}$ lub $\mathbb{Q}$. Mówimy, że forma q (oraz jej macierz w dowolnej bazie)

- **dodatnio określona**, jeśli $q(\alpha) > 0$, dla każdego niezerowego wektora $\alpha \in V$,
- **ujemnie określona**, jeśli $q(\alpha) < 0$, dla każdego niezerowego wektora $\alpha \in V$,
- **dodatnio półokreślona**, jeśli $q(\alpha) \geq 0$, dla każdego wektora $\alpha \in V$,
- **ujemnie półokreślona**, jeśli $q(\alpha) \leq 0$, dla każdego wektora $\alpha \in V$,
- **nieokreślona**, jeśli istnieją wektory $\alpha, \beta \in V$ takie, że $q(\alpha) > 0$ oraz $q(\beta) < 0$.

[a] A także nad $\mathbb{Z}$, o czym dalej, choć bez formalności...

Już mieliśmy okazję zobaczyć przydatność pojęcia określoności macierzy omawiając np. twierdzenie o rozkładzie biegunowym. Pojęcia te mają ogromne znaczenie w wielu działach matematyki.

Uwaga - wnioski z tw. spektralnego i tw. Jacobiego

Jeśli rzeczywista forma kwadratowa q ma w bazie $\mathcal{A} = (\alpha_1, \ldots, \alpha_n)$ postać diagonalną daną wzorem $q(x_1\alpha_1 + \ldots + x_n\alpha_n) = a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2$, dla pewnych $a_1, \ldots, a_n \in \mathbb{R}$, to forma q jest:

- **dodatnio określona** $\iff a_i > 0,$ dla $i = 1, \ldots, n.$
- **ujemnie określona** $\iff a_i < 0,$ dla $i = 1, \ldots, n.$
- **dodatnio półokreślona** $\iff a_i \geq 0,$ dla $i = 1, \ldots, n.$
- **ujemnie półokreślona** $\iff a_i \leq 0,$ dla $i = 1, \ldots, n.$
- **nieokreślona** $\iff$ istnieją $1 \leq i, j \leq n$ takie, że $a_i > 0$ oraz $a_j < 0.$

Jeśli q ma w bazie $\mathcal{A}$ przestrzeni V macierz $G(q; \mathcal{A}) = A \in M_{n\times n}(\mathbb{R})$.
Wówczas forma q jest:

- **dodatnio określona** $\iff \det A^{(i)} > 0,$ dla $i = 1, \ldots, n.$
- **ujemnie określona** $\iff (-1)^i i \det A^{(i)} > 0,$ dla $i = 1, \ldots, n.$

Definicja

Rzędem formy kwadratowej (odpowiednio: **sygnaturą**, w przypadku ciała $\mathbb{R}$) nazywamy rząd (sygnaturę) odpowiadającej jej formy dwuliniowej symetrycznej.

Wniosek

Każda forma kwadratowa na n wymiarowej przestrzeni liniowej nad $\mathbb{C}$ jest równoważna formie $q : \mathbb{C}^n \to \mathbb{C}$ postaci $q((x_1, \ldots, x_n)) = x_1^2 + \ldots + x_r^2$, dla pewnego $0 \leq r \leq n$. Formy kwadratowe $q_1 : \mathbb{C}^n \to \mathbb{C}$, $q_2 : \mathbb{C}^n \to \mathbb{C}$ są równoważne wtedy i tylko wtedy, gdy mają równe rzędy.

Wniosek

Każda forma kwadratowa na n wymiarowej przestrzeni liniowej nad $\mathbb{R}$ jest równoważna formie $q((x_1, \ldots, x_n)) = x_1^2 + \ldots + x_r^2 - x_{r+1}^2 - \ldots - x_{r+s}^2$, dla pewnych $r, s \geq 0$, $r + s \leq n$. Formy kwadratowe $q_1 : \mathbb{R}^n \to \mathbb{R}$, $q_2 : \mathbb{R}^n \to \mathbb{R}$ są równoważne wtedy i tylko wtedy, gdy mają równe rzędy i sygnatury.

Problem reprezentowalności formy kwadratowej

Niech q będzie formą kwadratową na przestrzeni n wymiarowej V nad ciałem K. Element niezerowy $a \in K$ **jest reprezentowany przez** q nad ciałem K, jeśli istnieją $x_1, \ldots, x_n$ takie, że $f(x_1, \ldots, x_n) = a$.

- Zbiór niezerowych elementów ciała K reprezentowanych przez formę q nazywamy **zbiorem wartości** tej formy, ozn. $D_K(q)$.
- Formę q nazywamy **izotropową**, jeśli istnieje $x \neq 0$ należący do V, że $q(x) = 0$. Formę q nazywamy **anizotropową**, jeśli $q(x) = 0 \Rightarrow x = 0$.
- Formę q nazywamy **uniwersalną**, jeśli $D_K(q) = K \setminus \{0\}$.

Problem reprezentowalności formy kwadratowej

Niech q będzie formą kwadratową na przestrzeni n wymiarowej V nad ciałem K. Element niezerowy $a \in K$ **jest reprezentowany przez** q nad ciałem K, jeśli istnieją $x_1, \ldots, x_n$ takie, że $f(x_1, \ldots, x_n) = a$.

- Zbiór niezerowych elementów ciała K reprezentowanych przez formę q nazywamy **zbiorem wartości** tej formy, ozn. $D_K(q)$.
- Formę q nazywamy **izotropową**, jeśli istnieje $x \neq 0$ należący do V, że $q(x) = 0$. Formę q nazywamy **anizotropową**, jeśli $q(x) = 0 \Rightarrow x = 0$.
- Formę q nazywamy **uniwersalną**, jeśli $D_K(q) = K \setminus \{0\}$.

Historycznie, i dla rozważań na kolejnych wykładach kluczowy jest problem form o współczynnikach całkowitych, czyli tzw. **całkowitych form kwadratowych**. Formalnie są to formy nad tzw. $\mathbb{Z}$-modułami. Interesuje nas **jakie liczby całkowite mogą być reprezentowane przez formy całkowite**? Kiedy formy te mają zbiór wartości $\mathbb{Z}_+$, co określamy również mianem **całkowitej formy uniwersalnej**?

Motywujące (choć raczej przypadkowe) przykłady

- Czy można rozwiązać równanie $x^2 - xy + y^2 = 2$ w liczbach całkowitych?

Motywujące (choć raczej przypadkowe) przykłady

- Czy można rozwiązać równanie $x^2 - xy + y^2 = 2$ w liczbach całkowitych?

  Oczywiście można argumentować modulo 3, ale można też zauważyć, że:

  $$x^2 - xy + y^2 = (x - \frac{1}{2}y)^2 + \frac{3}{4}y^2 = 2 \Rightarrow \frac{3}{4}y^2 \leq 3 \Rightarrow |y| < 2,$$

  czyli $y \in \{-1, 0, 1\}$, a przez symetrię $x \in \{-1, 0, 1\}$. Sprawdzenie, że dla tych wartości nie ma rozwiązania to w zasadzie to samo, co rozumowanie mod 3.

Motywujące (choć raczej przypadkowe) przykłady

- Czy można rozwiązać równanie $x^2 - xy + y^2 = 2$ w liczbach całkowitych?

  Oczywiście można argumentować modulo 3, ale można też zauważyć, że:

  $$x^2 - xy + y^2 = (x - \frac{1}{2}y)^2 + \frac{3}{4}y^2 = 2 \Rightarrow \frac{3}{4}y^2 \leq 3 \Rightarrow |y| < 2,$$

  czyli $y \in \{-1, 0, 1\}$, a przez symetrię $x \in \{-1, 0, 1\}$. Sprawdzenie, że dla tych wartości nie ma rozwiązania to w zasadzie to samo, co rozumowanie mod 3.

- Zadanie z koreańskiej Olimpiady Matematycznej Juniorów 2005 (sic!)
  Liczby rzeczywiste a, b, c, x, y spełniają $a^2 + b^2 + c^2 = x^2 + y^2 = 1$ Znajdź maksymalną wartość wyrażenia $(ax + by)^2 + (bx + cy)^2$.

  Wskazówka: zwijaj do kwadratu, a jeśli nie wychodzi, to policz wielomian charakterystyczny macierzy formy powyżej... Więcej takich zabaw:
  `https://artofproblemsolving.com/community/c6h1158074p5501289`.

Motywujące (choć raczej przypadkowe) przykłady

- Ile jest całkowitoliczbowych rozwiązań równania $x^2 - 3xy + y^2 = 1$?

Motywujące (choć raczej przypadkowe) przykłady

- Ile jest całkowitoliczbowych rozwiązań równania $x^2 - 3xy + y^2 = 1$?

  Oczywiście rozwiązaniami są $(x, y) = \pm(1, 0), \pm(0, 1)$, ale też $(x, y) = (8, 3)$. Pomnóżmy jednak strony wyjściowego równania przez 2 i zapiszmy:

$$2x^2 - 6xy + 2y^2 = \begin{bmatrix} x & y \end{bmatrix} \cdot \begin{bmatrix} 2 & -3 \\ -3 & 2 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = 2.$$

Motywujące (choć raczej przypadkowe) przykłady

- Ile jest całkowitoliczbowych rozwiązań równania $x^2 - 3xy + y^2 = 1$?

  Oczywiście rozwiązaniami są $(x, y) = \pm(1, 0), \pm(0, 1)$, ale też $(x, y) = (8, 3)$. Pomnóżmy jednak strony wyjściowego równania przez 2 i zapiszmy:

$$2x^2 - 6xy + 2y^2 = \begin{bmatrix} x & y \end{bmatrix} \cdot \begin{bmatrix} 2 & -3 \\ -3 & 2 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = 2.$$

  Ale mamy też:

$$2x^2 - 6xy + 2y^2 = \begin{bmatrix} x & y \end{bmatrix} \cdot \overbrace{\begin{bmatrix} -3 & -1 \\ 8 & 3 \end{bmatrix} \cdot \begin{bmatrix} 2 & -3 \\ -3 & 2 \end{bmatrix} \cdot \begin{bmatrix} -3 & 8 \\ -1 & 3 \end{bmatrix}} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = 2.$$

  Więc jeśli $\begin{bmatrix} x \\ y \end{bmatrix}$ jest rozwiązaniem, to jest nim także $\begin{bmatrix} -3 & 8 \\ -1 & 3 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix}$, dla $n \geq 1$, czyli są to $\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 8 \\ 3 \end{bmatrix}, \begin{bmatrix} 55 \\ 21 \end{bmatrix}, \begin{bmatrix} 377 \\ 144 \end{bmatrix}, \ldots$ – nieskończenie wiele rozwiązań.

Problem reprezentowalności całkowitych form kwadratowych

- **Euklides, -300.** Opis trójek liczb całkowitych, na których zeruje się forma całkowita $q(x_1, x_2, x_3) = x_1^2 + x_2^2 - x_3^2$.

Problem reprezentowalności całkowitych form kwadratowych

- **Euklides, -300.** Opis trójek liczb całkowitych, na których zeruje się forma całkowita $q(x_1, x_2, x_3) = x_1^2 + x_2^2 - x_3^2$.
- **Fermat, 1640.** Forma na $\mathbb{Z}^2$ postaci $q(x_1, x_2) = x_1^2 + x_2^2$ reprezentuje liczbę pierwszą p wtedy i tylko wtedy, gdy $p = 1 \bmod 4$.

Problem reprezentowalności całkowitych form kwadratowych

- **Euklides, -300.** Opis trójek liczb całkowitych, na których zeruje się forma całkowita $q(x_1, x_2, x_3) = x_1^2 + x_2^2 - x_3^2$.
- **Fermat, 1640.** Forma na $\mathbb{Z}^2$ postaci $q(x_1, x_2) = x_1^2 + x_2^2$ reprezentuje liczbę pierwszą p wtedy i tylko wtedy, gdy $p = 1 \bmod 4$.
- **Lagrange, 1772.** Forma na $\mathbb{Z}^4$ postaci $q(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 + x_4^2$ reprezentuje każdą liczbę całkowitą nieujemną.

Problem reprezentowalności całkowitych form kwadratowych

- **Euklides, -300.** Opis trójek liczb całkowitych, na których zeruje się forma całkowita $q(x_1, x_2, x_3) = x_1^2 + x_2^2 - x_3^2$.
- **Fermat, 1640.** Forma na $\mathbb{Z}^2$ postaci $q(x_1, x_2) = x_1^2 + x_2^2$ reprezentuje liczbę pierwszą p wtedy i tylko wtedy, gdy $p = 1 \bmod 4$.
- **Lagrange, 1772.** Forma na $\mathbb{Z}^4$ postaci $q(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 + x_4^2$ reprezentuje każdą liczbę całkowitą nieujemną.
- **Legendre, 1798.** Forma na $\mathbb{Z}^3$ postaci $q(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$ reprezentuje wszystkie liczby całkowite nieujemne, które nie mają postaci $4^a(8k + 7)$, dla pewnych $a, k \in \mathbb{Z}$.

Problem reprezentowalności całkowitych form kwadratowych

- **Euklides, -300.** Opis trójek liczb całkowitych, na których zeruje się forma całkowita $q(x_1, x_2, x_3) = x_1^2 + x_2^2 - x_3^2$.
- **Fermat, 1640.** Forma na $\mathbb{Z}^2$ postaci $q(x_1, x_2) = x_1^2 + x_2^2$ reprezentuje liczbę pierwszą p wtedy i tylko wtedy, gdy $p = 1 \bmod 4$.
- **Lagrange, 1772.** Forma na $\mathbb{Z}^4$ postaci $q(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 + x_4^2$ reprezentuje każdą liczbę całkowitą nieujemną.
- **Legendre, 1798.** Forma na $\mathbb{Z}^3$ postaci $q(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$ reprezentuje wszystkie liczby całkowite nieujemne, które nie mają postaci $4^a(8k + 7)$, dla pewnych $a, k \in \mathbb{Z}$.
- **Jacobi, 1828.** Forma na $\mathbb{Z}^4$ postaci $q(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 + x_4^2$ reprezentuje liczbę całkowitą m na dokładnie $8 \sum_{0<d|m,\ d\neq 4k} d$ sposobów.

Problem reprezentowalności całkowitych form kwadratowych

- **Liouville 1859-60.** Forma całkowita $x_1^2 + x_2^2 + 2x_3^2 + 2x_4^2$ jest uniwersalna, zaś forma całkowita $x_1^2 + x_2^2 + 5x_3^2 + 5x_4^2$ nie reprezentuje jedynie 3. Natomiast $x_1^2 + x_2^2 + 4x_3^2 + 4x_4^2$ nie reprezentuje tylko liczb dających resztę 3 modulo 4.

Problem reprezentowalności całkowitych form kwadratowych

- **Liouville 1859-60.** Forma całkowita $x_1^2 + x_2^2 + 2x_3^2 + 2x_4^2$ jest uniwersalna, zaś forma całkowita $x_1^2 + x_2^2 + 5x_3^2 + 5x_4^2$ nie reprezentuje jedynie 3. Natomiast $x_1^2 + x_2^2 + 4x_3^2 + 4x_4^2$ nie reprezentuje tylko liczb dających resztę 3 modulo 4.
- **Ramanujan, 1917.** Jest dokładnie 55 uniwersalnych form całkowitych postaci $q(x_1, x_2, x_3, x_4) = ax_1^2 + bx_2^2 + cx_3^2 + dx_4^2$ (zostały wypisane...).

Problem reprezentowalności całkowitych form kwadratowych

- **Liouville 1859-60.** Forma całkowita $x_1^2 + x_2^2 + 2x_3^2 + 2x_4^2$ jest uniwersalna, zaś forma całkowita $x_1^2 + x_2^2 + 5x_3^2 + 5x_4^2$ nie reprezentuje jedynie 3. Natomiast $x_1^2 + x_2^2 + 4x_3^2 + 4x_4^2$ nie reprezentuje tylko liczb dających resztę 3 modulo 4.
- **Ramanujan, 1917.** Jest dokładnie 55 uniwersalnych form całkowitych postaci $q(x_1, x_2, x_3, x_4) = ax_1^2 + bx_2^2 + cx_3^2 + dx_4^2$ (zostały wypisane...).
- **Dickson, 1926.** Ramanujan nie ma racji, są tylko 54 uniwersalne formy całkowite o czterech zmiennych. Oczywiście jest nieskończenie wiele całkowitych form uniwersalnych, dla każdej liczby zmiennych większej niż 4 (co wynika z twierdzenia o czterech kwadratach), ale też żadna forma postaci $ax_1^2 + bx_2^2 + cx_3^2$ nie jest uniwersalna (fajne ćwiczenie dla $a \leq b \leq c$).

Problem reprezentowalności całkowitych form kwadratowych

- **Liouville 1859-60.** Forma całkowita $x_1^2 + x_2^2 + 2x_3^2 + 2x_4^2$ jest uniwersalna, zaś forma całkowita $x_1^2 + x_2^2 + 5x_3^2 + 5x_4^2$ nie reprezentuje jedynie 3. Natomiast $x_1^2 + x_2^2 + 4x_3^2 + 4x_4^2$ nie reprezentuje tylko liczb dających resztę 3 modulo 4.
- **Ramanujan, 1917.** Jest dokładnie 55 uniwersalnych form całkowitych postaci $q(x_1, x_2, x_3, x_4) = ax_1^2 + bx_2^2 + cx_3^2 + dx_4^2$ (zostały wypisane...).
- **Dickson, 1926.** Ramanujan nie ma racji, są tylko 54 uniwersalne formy całkowite o czterech zmiennych. Oczywiście jest nieskończenie wiele całkowitych form uniwersalnych, dla każdej liczby zmiennych większej niż 4 (co wynika z twierdzenia o czterech kwadratach), ale też żadna forma postaci $ax_1^2 + bx_2^2 + cx_3^2$ nie jest uniwersalna (fajne ćwiczenie dla $a \leq b \leq c$).
- **Halmos, 1938.** Jeśli $a, b, c, d \in \mathbb{Z}_+$, to forma $ax_1^2 + bx_2^2 + cx_3^2 + dx_4^2$ jest uniwersalna wtedy i tylko wtedy, gdy reprezentuje pierwsze 15 dodatnich liczb całkowitych (tak naprawdę wystarczy 9 liczb: $\{1, 2, 3, 5, 6, 7, 10, 14, 15\}$).

Problem reprezentowalności całkowitych form kwadratowych

- **Conway, Schneeberger, 1993 (15-theorem).** Wynik Halmosa jest prawdziwy dla dowolnej formy $q(x_1, \ldots, x_n) = a_1 x_1^2 + \ldots + a_n x_n^2$ na $\mathbb{Z}^n$, gdzie $a_i \in \mathbb{Z}_+$. Hipoteza: jeśli nie założymy, że a_i są dodatnie, ale tylko, że q jest dodatnio określona (czyli $q(x) > 0$, dla $x \neq 0$, $x \in \mathbb{Z}^n$), to uniwersalność q zapewnia *już* reprezentowalność pierwszych 290 liczb całkowitych dodatnich.

Problem reprezentowalności całkowitych form kwadratowych

- **Conway, Schneeberger, 1993 (15-theorem).** Wynik Halmosa jest prawdziwy dla dowolnej formy $q(x_1, \ldots, x_n) = a_1 x_1^2 + \ldots + a_n x_n^2$ na $\mathbb{Z}^n$, gdzie $a_i \in \mathbb{Z}_+$. Hipoteza: jeśli nie założymy, że a_i są dodatnie, ale tylko, że q jest dodatnio określona (czyli $q(x) > 0$, dla $x \neq 0$, $x \in \mathbb{Z}^n$), to uniwersalność q zapewnia *już* reprezentowalność pierwszych 290 liczb całkowitych dodatnich.
- **Bhargava, 2000.** Wynik Halmosa działa dla dowolnej liczby zmiennych w mocniejszej wersji (9 liczb). Dowód jest elementarny, warto przeczytać pracę ze znakomitym wstępem Conwaya (który wywołał całe to *zamieszanie*): `http://www.fen.bilkent.edu.tr/~franz/mat/15.pdf`.

Problem reprezentowalności całkowitych form kwadratowych

- **Conway, Schneeberger, 1993 (15-theorem).** Wynik Halmosa jest prawdziwy dla dowolnej formy $q(x_1, \ldots, x_n) = a_1 x_1^2 + \ldots + a_n x_n^2$ na $\mathbb{Z}^n$, gdzie $a_i \in \mathbb{Z}_+$. Hipoteza: jeśli nie założymy, że a_i są dodatnie, ale tylko, że q jest dodatnio określona (czyli $q(x) > 0$, dla $x \neq 0$, $x \in \mathbb{Z}^n$), to uniwersalność q zapewnia *już* reprezentowalność pierwszych 290 liczb całkowitych dodatnich.

- **Bhargava, 2000.** Wynik Halmosa działa dla dowolnej liczby zmiennych w mocniejszej wersji (9 liczb). Dowód jest elementarny, warto przeczytać pracę ze znakomitym wstępem Conwaya (który wywołał całe to *zamieszanie*): `http://www.fen.bilkent.edu.tr/~franz/mat/15.pdf`.

- **Bhargava, Hanke 2011.** Hipoteza Conwaya z 1993 roku jest prawdziwa. Do uniwersalności dodatnio określonej całkowitej formy kwadratowej potrzeba i wystarcza sprawdzenie reprezentowalności 27 liczb: $1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 203, 290$. Takich form jest 6436 (to już policzono komputerowo).

Przykład *specyficznego* problemu otwartego: forma ternarna Ramanujana

- **Ramanujan 1916.** Forma $x^2 + y^2 + 10z^2$ nie reprezentuje liczb parzystych postaci $4^a(16b + 6)$, dla $a, b \in \mathbb{Z}_+$ oraz liczb nieparzystych:

$$3, 7, 31, 33, 33, 43, 67, 79, 87, 133, 217, 219, 223, 253, 307, 391.$$

Przykład *specyficznego* problemu otwartego: forma ternarna Ramanujana

- **Ramanujan 1916.** Forma $x^2 + y^2 + 10z^2$ nie reprezentuje liczb parzystych postaci $4^a(16b + 6)$, dla $a, b \in \mathbb{Z}_+$ oraz liczb nieparzystych:

$$3, 7, 31, 33, 33, 43, 67, 79, 87, 133, 217, 219, 223, 253, 307, 391.$$

- **Gupta, 1941** Forma $x^2 + y^2 + 10z^2$ nie reprezentuje też 2719.

Przykład *specyficznego* problemu otwartego: forma ternarna Ramanujana

- **Ramanujan 1916.** Forma $x^2 + y^2 + 10z^2$ nie reprezentuje liczb parzystych postaci $4^a(16b + 6)$, dla $a, b \in \mathbb{Z}_+$ oraz liczb nieparzystych:

$$3, 7, 31, 33, 33, 43, 67, 79, 87, 133, 217, 219, 223, 253, 307, 391.$$

- **Gupta, 1941** Forma $x^2 + y^2 + 10z^2$ nie reprezentuje też 2719.
- **Ono, Sonudararajan 2011.** Hipoteza. Forma $x^2 + y^2 + 10z^2$ nie reprezentuje innych liczb nieparzystych, niż wypisane wyżej. Jeśli jednak zachodzi uogólniona Hipoteza Riemanna, to hipoteza jest prawdziwa (sic!).

Przykład *specyficznego* problemu otwartego: forma ternarna Ramanujana

- **Ramanujan 1916.** Forma $x^2 + y^2 + 10z^2$ nie reprezentuje liczb parzystych postaci $4^a(16b + 6)$, dla $a, b \in \mathbb{Z}_+$ oraz liczb nieparzystych:

$$3, 7, 31, 33, 33, 43, 67, 79, 87, 133, 217, 219, 223, 253, 307, 391.$$

- **Gupta, 1941** Forma $x^2 + y^2 + 10z^2$ nie reprezentuje też 2719.
- **Ono, Sonudararajan 2011.** Hipoteza. Forma $x^2 + y^2 + 10z^2$ nie reprezentuje innych liczb nieparzystych, niż wypisane wyżej. Jeśli jednak zachodzi uogólniona Hipoteza Riemanna, to hipoteza jest prawdziwa (sic!).

* * *

Więcej: K. Williams: *A "Four Integers" Theorem and a "Five Integers" Theorem*, The American Mathematical Monthly , Vol. 122, No. 6 (June–July 2015), pp. 528-536, pod adresem (wymagane zalogowanie przez BUW):
`https://www.jstor.org/stable/10.4169/amer.math.monthly.122.6.528`.

Arcyważny problem: jakie liczby pierwsze reprezentowane są przez formy $x^2 + ay^2$? Zagadnienie to było motywem przewodnim rozwoju teorii liczb.

- Fermat (dowody dał Euler, dając początki prawu wzajemności)
  - forma $x^2 + y^2$ reprezentuje liczby pierwsze $p = 1 \bmod 4$,
  - forma $x^2 + 2y^2$ reprezentuje liczby pierwsze $p = 1, 3 \bmod 8$,
  - forma $x^2 + 3y^2$ reprezentuje $p = 3$ oraz $p = 1 \bmod 3$.

Arcyważny problem: jakie liczby pierwsze reprezentowane są przez formy $x^2 + ay^2$? Zagadnienie to było motywem przewodnim rozwoju teorii liczb.

- Fermat (dowody dał Euler, dając początki prawu wzajemności)
  - forma $x^2 + y^2$ reprezentuje liczby pierwsze $p = 1 \bmod 4$,
  - forma $x^2 + 2y^2$ reprezentuje liczby pierwsze $p = 1, 3 \bmod 8$,
  - forma $x^2 + 3y^2$ reprezentuje $p = 3$ oraz $p = 1 \bmod 3$.
- Hipotezy Eulera (nie umiał ich udowodnić, zrobił to Gauss)
  - forma $x^2 + 5y^2$ repr. liczby pierwsze $p = 3, 7 \bmod 20$,
  - forma $x^2 + 14y^2$ repr. liczby pierwsze $p = 1, 9, 15, 23, 25, 39 \bmod 56$,
  - forma $x^2 + 27y^2$ repr. $p = 1 \bmod 3$ gdzie 2 jest resztą sześcienną mod p,
  - forma $x^2 + 64y^2$ repr. $p = 1 \bmod 4$ gdzie 2 jest resztą dwukwadratową mod p.

Arcyważny problem: jakie liczby pierwsze reprezentowane są przez formy $x^2 + ay^2$? Zagadnienie to było motywem przewodnim rozwoju teorii liczb.

- Fermat (dowody dał Euler, dając początki prawu wzajemności)
  - forma $x^2 + y^2$ reprezentuje liczby pierwsze $p = 1 \bmod 4$,
  - forma $x^2 + 2y^2$ reprezentuje liczby pierwsze $p = 1, 3 \bmod 8$,
  - forma $x^2 + 3y^2$ reprezentuje $p = 3$ oraz $p = 1 \bmod 3$.
- Hipotezy Eulera (nie umiał ich udowodnić, zrobił to Gauss)
  - forma $x^2 + 5y^2$ repr. liczby pierwsze $p = 3, 7 \bmod 20$,
  - forma $x^2 + 14y^2$ repr. liczby pierwsze $p = 1, 9, 15, 23, 25, 39 \bmod 56$,
  - forma $x^2 + 27y^2$ repr. $p = 1 \bmod 3$ gdzie 2 jest resztą sześcienną mod p,
  - forma $x^2 + 64y^2$ repr. $p = 1 \bmod 4$ gdzie 2 jest resztą dwukwadratową mod p.
- Lagrange, Legendre, Gauss, równoważność form, początki teorii genusu, użycie wyrożnika, teoria kompozycji form, wyższe prawa wzajemności.

Arcyważny problem: jakie liczby pierwsze reprezentowane są przez formy $x^2 + ay^2$? Zagadnienie to było motywem przewodnim rozwoju teorii liczb.

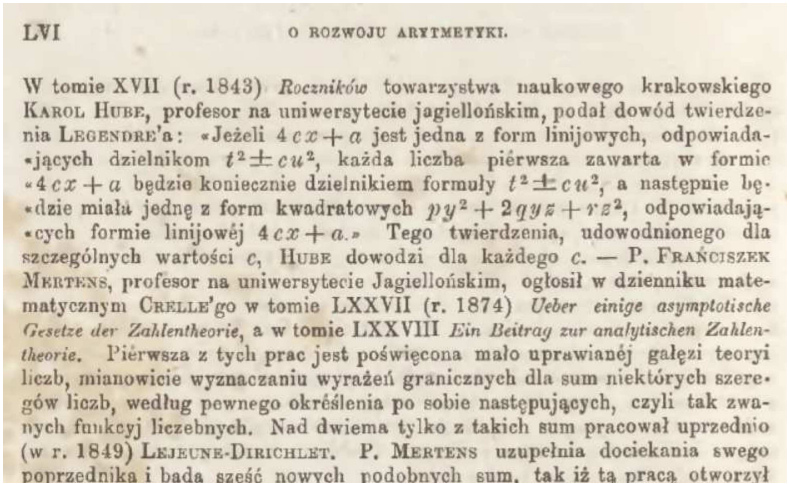
- Fermat (dowody dał Euler, dając początki prawu wzajemności)
  - forma $x^2 + y^2$ reprezentuje liczby pierwsze $p = 1 \bmod 4$,
  - forma $x^2 + 2y^2$ reprezentuje liczby pierwsze $p = 1, 3 \bmod 8$,
  - forma $x^2 + 3y^2$ reprezentuje $p = 3$ oraz $p = 1 \bmod 3$.
- Hipotezy Eulera (nie umiał ich udowodnić, zrobił to Gauss)
  - forma $x^2 + 5y^2$ repr. liczby pierwsze $p = 3, 7 \bmod 20$,
  - forma $x^2 + 14y^2$ repr. liczby pierwsze $p = 1, 9, 15, 23, 25, 39 \bmod 56$,
  - forma $x^2 + 27y^2$ repr. $p = 1 \bmod 3$ gdzie 2 jest resztą sześcienną mod p,
  - forma $x^2 + 64y^2$ repr. $p = 1 \bmod 4$ gdzie 2 jest resztą dwukwadratową mod p.
- Lagrange, Legendre, Gauss, równoważność form, początki teorii genusu, użycie wyrożnika, teoria kompozycji form, wyższe prawa wzajemności.
- Dedekind, Kronecker, Minkowski, Dirichlet, Hilbert, czyli początki algebraicznej teorii liczb i prapoczątki geometrii algebraicznej.

Arcyważny problem: jakie liczby pierwsze reprezentowane są przez formy $x^2 + ay^2$? Zagadnienie to było motywem przewodnim rozwoju teorii liczb.

- **Bardzo trudne pytanie**. Czy istnieje nieskończenie wiele liczb pierwszych postaci $x^2 + 1$, dla $x \in \mathbb{Z}$? To jeden z czterech problemów postawionych w 1912 roku przez E. Landau na Międzynarodowym Kongresie Matematycznym (pozostałe to hipoteza Goldbacha, hipoteza liczb bliźniaczych i hipoteza Legendre'a o istnieniu liczby pierwszej pomiędzy n^2 a $(n+1)^2$, dla $n > 1$).

Arcyważny problem: jakie liczby pierwsze reprezentowane są przez formy $x^2 + ay^2$? Zagadnienie to było motywem przewodnim rozwoju teorii liczb.

- **Bardzo trudne pytanie**. Czy istnieje nieskończenie wiele liczb pierwszych postaci $x^2 + 1$, dla $x \in \mathbb{Z}$? To jeden z czterech problemów postawionych w 1912 roku przez E. Landau na Międzynarodowym Kongresie Matematycznym (pozostałe to hipoteza Goldbacha, hipoteza liczb bliźniaczych i hipoteza Legendre'a o istnieniu liczby pierwszej pomiędzy n^2 a $(n+1)^2$, dla $n > 1$).
- **Fundamentalny wkład.** Profesor Henryk Iwaniec, Absolwent naszego Wydziału (żyje w USA), w 1978 roku uzyskał wybitny rezultat: istnieje nieskończenie wiele liczb postaci $x^2 + 1$, które są iloczynami co najwyżej dwóch liczb pierwszych. Natomiast w 1997 udowodnił wraz z Friendlanderem, że istnieje nieskończenie wiele liczb pierwszych postaci $x^2 + y^4$. Za wkład w ten wynik otrzymał (wraz z P. Sarnakiem i R. Taylorem) w 2001 roku nagrodę Ostrowskiego (w 1995 otrzymał ją A. Wiles za WTF, a w 2005 r. – B. Green i T. Tao). W 2015 roku otrzymał Nagrodę Shawa (razem z G. Faltingsem).



LVI O ROZWOJU ARYTMETYKI.

W tomie XVII (r. 1843) *Roczników* towarzystwa naukowego krakowskiego KAROL HUBE, profesor na uniwersytecie jagiellońskim, podał dowód twierdzenia LEGENDRE'a: «Jeżeli $4cx+a$ jest jedna z form linijowych, odpowiadających dzielnikom $t^2 \pm cu^2$, każda liczba piérwsza zawarta w formie «$4cx+a$ będzie koniecznie dzielnikiem formuły $t^2 \pm cu^2$, a następnie będzie miała jednę z form kwadratowych $py^2+2qyz+rz^2$, odpowiadających formie linijowéj $4cx+a$.» Tego twierdzenia, udowodnionego dla szczególnych wartości c, HUBE dowodzi dla każdego c. — P. FRAŃCISZEK MERTENS, profesor na uniwersytecie Jagiellońskim, ogłosił w dzienniku matematycznym CRELLE'go w tomie LXXVII (r. 1874) *Ueber einige asymptotische Gesetze der Zahlentheorie*, a w tomie LXXVIII *Ein Beitrag zur analytischen Zahlentheorie*. Piérwsza z tych prac jest poświęcona mało uprawianéj gałęzi teoryi liczb, mianowicie wyznaczaniu wyrażeń granicznych dla sum niektórych szeregów liczb, według pewnego określenia po sobie następujących, czyli tak zwanych funkcyj liczebnych. Nad dwiema tylko z takich sum pracował uprzednio (w r. 1849) LEJEUNE-DIRICHLET. P. MERTENS uzupełnia dociekania swego poprzednika i bada sześć nowych podobnych sum, tak iż ta praca otworzył

Arytmetyka, kurs teoretyczny. Mariana Baranieckiego (1884) to **podręcznik dla szkół średnich** przygotowujący do studiów „na kierunkach specjalistycznych". Długie i bardzo detaliczne wprowadzenie dotyczące historii arytmetyki od czasów najdawniejszych autor podsumowuje „choćby pobieżnym zaznaczeniem poważnych prac w stuleciu bieżącym, odnoszących się do teoryi liczb". Wyraźnie widać czego dotyczą te prace. Swoją drogą w XIX wieku (bardzo nieliczni) uczniowie szkół średnich raczej nie czytali podręczników (polecano nie pokazywać im ich do czasu zakończenia nauki). Podręczniki pisano dla nauczycieli. Źródło: https://www.wbc.poznan.pl/dlibra/publication/534971/edition/466234.