Formy kwadratowe

Definicja 107. *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*

$$q(\alpha) = h(\alpha, \alpha).$$

Fakt 170. *Niech V będzie skończenie wymiarową przestrzenią liniową nad K i niech $(\alpha_1, \ldots, \alpha_n)$ będzie bazą przestrzeni V. Następujące warunki są równoważne.*

- *funkcja $q : V \to K$ jest formą kwadratową na przestrzeni V,*
- *istnieją elementy $a_{ij} \in K$, dla $i, j = 1, \ldots, n$ takie, że dla każdych skalarów $x_1, \ldots, x_n$ z ciała K zachodzi równość:*

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

Dowód. Niech $q(\alpha) = h(\alpha, \alpha)$, dla pewnej formy dwuliniowej h na V. Niech $a_{ij} = h(\alpha_i, \alpha_j)$, dla $i, j = 1, \ldots, n$. Dla $x_1, \ldots, x_n$, $y_1, \ldots, y_n \in K$ 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 $q(x_1\alpha_1 + \ldots + x_n\alpha_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j$.

Na odwrót: 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 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 $h(\alpha, \alpha) = q(\alpha)$. □

Przyjmując $b_{ii} = a_{ii}$ dla $i = 1, \ldots, n$ oraz $b_{ij} = a_{ij} + a_{ji}$ dla $1 \leq i, j \leq n$ w powyższej uwadze możemy ją przeformułować następująco.

Fakt 171. *Niech V będzie skończenie wymiarową przestrzenią liniową nad K i niech $(\alpha_1, \ldots, \alpha_n)$ będzie bazą przestrzeni V. Wówczas funkcja $q : V \to K$ jest formą kwadratową na przestrzeni V wtedy i tylko wtedy, gdy istnieją elementy $b_{ij} \in K$, dla $i, j = 1, \ldots, n$ takie, że dla każdych $x_1, \ldots, x_n \in K$:*

$$q(x_1\alpha_1 + \ldots + x_n\alpha_n) = \sum_{1 \leq i \leq j \leq n} b_{ij} x_i x_j.$$

Rozważmy kilka przykładów.

- Każda forma kwadratowa na przestrzeni K^n jest postaci:

$$q((x_1, \ldots, x_n)) = \sum_{1 \leq i \leq j \leq n} b_{ij} x_i x_j,$$

na przykład

$$q_1((x_1, x_2)) = 2x_1^2 + 3x_1x_2 - 5x_3^2$$
$$q_2((x_1, x_2, x_3)) = x_1^2 + 4x_1x_2 + 7x_2^2 - 6x_2x_3 + 3x_3^2.$$

- Jeśli $q : V \to K$ jest formą kwadratową na przestrzeni V, to dla każdej podprzestrzeni liniowej $W \subseteq V$ funkcja $q|_W : W \to K$, zadana jako $q|_W(\alpha) = q(w)$ dla każdego $\alpha \in W$, jest formą kwadratową na przestrzeni W.

Definicja 108. *Niech $q : V \to K$ będzie formą kwadratową.* Postacią diagonalną formy kwadratowej *q nazwiemy przedstawienie jej w formie:*

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

gdzie $(\alpha_1, \ldots, \alpha_n)$ jest pewną bazą przestrzeni V oraz $a_1, \ldots, a_n \in K$.

Przykład. Niech

$$q((x_1, x_2, x_3, x_4)) = x_1^2 + 8x_1x_2 + 7x_2^2 + 2x_3x_4.$$

Forma q określona jest na $\mathbb{R}^4$, a zapisany wzór oparty jest o współrzędne wektora w bazie standardowej. Rozważmy bazę $\alpha_1 = (1, 0, 0, 0)$, $\alpha_2 = (4, -1, 0, 0)$, $\alpha_3 = (0, 0, 1, 1)$, $\alpha_4 = (0, 0, 1, -1)$. Jest to baza ortogonalna w $(\mathbb{R}^4, h)$, gdzie h jest symetryczna i $h(\alpha, \alpha) = q(\alpha)$, dla każdego α (to wyjaśnię niżej). Wówczas forma q zapisywać się będzie wzorem:

$$q((y_1\alpha_1 + y_2\alpha_2 + y_3\alpha_3 + y_4\alpha_4)) = y_1^2 - 9y_2^2 + 2y_3^2 - 2y_4^2.$$

Chcemy mieć narzędzia do rozróżniania określoności (zawsze diagonalizowalnych) form rzeczywistych, a dla dowolnego ciała – do diagonalizacji form kwadratowych i do stwierdzania kiedy ta ostatnia jest możliwa. Dla ciał charakterystyki różnej od 2 istnieje bardzo bliski związek pomiędzy formami kwadratowymi i symetrycznymi formami dwuliniowymi. Mówi o tym następujące stwierdzenie.

Fakt 172. *Niech V będzie przestrzenią liniową nad ciałem K charakterystyki różnej od 2. Jeśli $q : V \to K$ jest formą kwadratową, to istnieje dokładnie jedna forma dwuliniowa symetryczna $h : V \to K$ taka, że dla każdego $\alpha \in V$ zachodzi $q(\alpha) = h(\alpha, \alpha)$. Dokładniej, dla ciała 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.

Zanim zobaczymy dowód zobaczmy krótki przykład. Weźmy formę kwadratową $q : \mathbb{R}^2 \to \mathbb{R}$ daną wzorem

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

Istnieje naturalnie wiele form dwuliniowych $h : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ takich, że $q(\alpha) = h(\alpha, \alpha)$, dla każdego $\alpha \in V$, na przykład

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

lub

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

ale istnieje wśród nich tylko jedna forma dwuliniowa symetryczna, mianowicie

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

Dowód. Niech $h' : V \times V \to K$ będzie dowolną formą dwuliniową taką, że dla każdego $\alpha \in V$ zachodzi $q(\alpha) = h'(\alpha, \alpha)$. Wówczas funkcja $h : V \times V \to K$ zadana warunkami $h(\alpha, \beta) = \frac{1}{2}(h'(\alpha, \beta) + h'(\beta, \alpha))$ jest formą dwuliniową symetryczną na przestrzeni V i mamy równość $q(\alpha) = h'(\alpha, \alpha) = h(\alpha, \alpha)$, dla każdego $\alpha \in V$. To dowodzi istnienia żądanej formy dwuliniowej symetrycznej h. Aby wykazać jej jednoznaczność zauważmy, że jeśli h jest formą dwuliniową symetryczną spełniającą $q(\alpha) = h(\alpha, \alpha)$ dla każdego $\alpha \in V$, to dla każdych $\alpha, \beta \in V$ mamy

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

czyli h jest wyznaczona jednoznacznie przez q. □

Odtąd, aż do końca wykładu zakładamy, że ciało K jest charakterystyki różnej od 2.

Definicja 109. *Niech $q : V \to K$ będzie formą kwadratową na skończenie wymiarowej przestrzeni liniowej.* MACIERZĄ FORMY KWADRATOWEJ *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 formy $q : K^n \to K$ zadanej wzorem $q((x_1,\ldots,x_n)) = x_1^2 + \ldots + x_n^2$ mamy $G(q;st) = I$. Dla formy $q : \mathbb{R}^2 \to \mathbb{R}$ zadanej wzorem

$$q((x_1,x_2)) = x_1^2 + 3x_1x_2 + 7x_2^2$$

mamy

$$G(q;st) = \begin{bmatrix} 1 & \frac{3}{2} \\ \frac{3}{2} & 7 \end{bmatrix},$$

a w bazie $\mathcal{A} = ((1,1),(1,-1))$ mamy $G(q;\mathcal{A}) = \begin{bmatrix} 11 & -6 \\ -6 & 5 \end{bmatrix}$.

Opis form kwadratowych w języku form dwuliniowych symetrycznych uruchamia całą maszynerię i rezultaty uzyskane wcześniej. W szczególności mamy następujące własności macierzy form kwadratowych.

Fakt 173. *Jeśli $A = [a_{ij}]$ jest macierzą formy kwadratowej q w bazie $\mathcal{A} = (\alpha_1,\ldots,\alpha_n)$, to dla dowolnych elementów $x_1,\ldots,x_n \in K$ zachodzi równość $q(x_1\alpha_1 + \ldots + x_n\alpha_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j$.*

Fakt 174. *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 175. *Dla każdej formy kwadratowej q na skończenie wymiarowej przestrzeni V (gdzie* $\operatorname{char} K \neq 2$*) 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 $q(x_1\alpha_1 + \ldots + x_n\alpha_n) = a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2$.*

Na ćwiczeniach będziecie Państwo stosować różne sposoby na diagonalizację formy q. Trzy podstawowe metody to:

- szukanie bazy prostopadłej przestrzeni dwuliniowej (V,h), gdzie h jest formą symetryczną odpowiadającą formie kwadratowej q,
- szukanie bazy ortonormalnej złożonej z wektorów własnych rzeczywistej macierzy symetrycznej $A = G(h;st)$ w przestrzeni euklidesowej ze standardowym iloczynem skalarnym (tutaj $K = \mathbb{R}$),
- intuicyjna metoda uzupełniania do kwadratów (jest ona opisana w skrypcie i na pewno będzie wspomniana na ćwiczeniach, choć powyższe dwie w zupełności wystarczają do diagonalizacji).

Definicja 110. *Mówimy, że forma kwadratowa kwadratowej) $q : V \to \mathbb{R}$ jest*

- DODATNIO OKREŚLONA, *jeśli $q(\alpha) > 0$, dla każdego niezerowego $\alpha \in V$,*
- UJEMNIE OKREŚLONA, *jeśli $q(\alpha) < 0$, dla każdego niezerowego $\alpha \in V$,*
- 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 $\alpha, \beta \in V$ takie, że $q(\alpha) > 0$ oraz $q(\beta) < 0$.*

Definicje te mają ogromne znaczenie w zastosowaniach, zwłaszcza w analizie. Powyższym pojęciom odpowiadają analogiczne dotyczące macierzy form.

Definicja 111. *Mówimy, że macierz kwadratowa $A \in M_n(\mathbb{R})$ jest*

- DODATNIO OKREŚLONA, *jeśli $v^T Av > 0$, dla każdego $v \in \mathbb{R}^n \setminus \{0\}$,*
- UJEMNIE OKREŚLONA, *jeśli $v^T Av < 0$, dla każdego $v \in \mathbb{R}^n \setminus \{0\}$,*
- DODATNIO PÓŁOKREŚLONA, *jeśli $v^T Av \geq 0$, dla każdego $v \in \mathbb{R}^n$,*
- UJEMNIE PÓŁOKREŚLONA, *jeśli $v^T Av \leq 0$, dla każdego $v \in \mathbb{R}^n$,*
- NIEOKREŚLONA, *jeśli istnieją $v, w \in \mathbb{R}^n$, takie, że $v^T Av > 0$ oraz $w^T Aw < 0$.*

Określoność formy ma duży związek z jej postacią diagonalną.

Fakt 176. *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 $a_j < 0$.*

Badanie określoności rzeczywistej formy kwadratowej opiera się na kryterium Sylvestera.

Fakt 177. *Niech $q : V \to \mathbb{R}$ będzie rzeczywistą formą kwadratową mającą 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 $\iff (-1)^i \det A^{(i)} > 0$, *dla $i = 1, \ldots, n$.*

Na koniec odnotujmy jak twierdzenia klasyfikacyjne dla form dwuliniowych i macierzy symetrycznych przenoszą się na formy kwadratowe.

Definicja 112. RZĘDEM FORMY KWADRATOWEJ *(odpowiednio:* SYGNATURĄ*, w przypadku ciała* $\mathbb{R}$*)* *nazywamy rząd (sygnaturę) odpowiadającej jej formy dwuliniowej symetrycznej. Mówimy, że formy kwadratowe* $q_1 : V_1 \to K, q_2 : V_2 \to K$ *są* równoważne*, jeśli istnieją bazy* $\mathcal{A}_1$ *przestrzeni* V_1 *oraz* $\mathcal{A}_2$ *przestrzeni* V_2 *takie, że* $G(q_1; \mathcal{A}_1) = G(q_2; \mathcal{A}_2)$*.*

Fakt 178. *Formy kwadratowe* $q_1 : V_1 \to K$ *oraz* $q_2 : V_2 \to K$ *są równoważne wtedy i tylko wtedy, gdy dla każdej bazy* $\mathcal{A}_1$ *przestrzeni* V_1 *oraz każdej bazy* $\mathcal{A}_2$ *przestrzeni* V_2 *macierze* $G(q_1; \mathcal{A}_1)$*,* $G(q_2; \mathcal{A}_2)$ *są kongruentne nad* K*.*

Fakt 179. *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.*

Fakt 180. *Każda forma kwadratowa na* n *wymiarowej przestrzeni liniowej nad* $\mathbb{R}$ *jest równoważna formie* $q : \mathbb{R}^n \to \mathbb{R}$ *postaci*

$$q((x_1, \ldots, x_n)) = x_1^2 + \ldots + x_r^2 - x_{r+1}^2 - \ldots - x_{r+s}^2,$$

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.*

Na tym kończy się część wykładu dotycząca wprowadzania dodatkowej struktury na przestrzeni liniowej, pozwalającej przede wszystkim na rozważanie pojęcia ortogonalności wektorów, a w przypadku rzeczywistym także na mówienie o kątach, miarach, orientacji itd.

Teoria ta pozwoliła nam na wyrobienie wstępnych intuicji geometrycznych niezbędnych do pracy w przestrzeniach afinicznych. Dała nam też posmak zjawiska, które będziecie Państwo często obserwować – zamiast rozważać czysto algebraiczne struktury typu przestrzenie liniowe czy przekształcenia między nimi uczyć się Państwo będziecie o ich szczególnych typach, wyposażonych w dodatkowe struktury algebraiczne (jak iloczyn skalarny), metryczne (jak choćby izometrie), i wiele innych.

Konkluzją wykładu będzie badanie zbiorów opisanych (niekoniecznie liniowymi) równaniami algebraicznymi w przestrzeni afinicznej.

Uzupełnienie. Minima i maksima

Możliwość diagonalizacji formy kwadratowej ma olbrzymie znaczenie w teorii liczb i geometrii, a także w wielu innych działach matematyki. Przyjrzymy się teraz prostemu zastosowaniu, mającemu dalej istotne zastosowania analityczne.

Zainteresowanych odsyłam do wykładu z Analizy II, np. do notatek dr. M. Krycha: Lokalne ekstrema, formy kwadratowe: https://www.mimuw.edu.pl/~krych/matematyka/AM2skrypt/am2cz06L.pdf.

Formy kwadratowe służą w analizie np. do określania kryteriów osiągania lub nie ekstremów lokalnych. Są to wyniki analogiczne jak dla funkcji różniczkowalnej jednej zmiennej, gdzie np. minimum lokalne osiągane jest w punkcie zerowania się pochodnej, pod warunkiem, że druga pochodna jest dodatnia. Dla funkcji wielu zmiennych zamiast pochodnych odpowiednich stopni mamy różniczki, przy czym pierwsza różniczka jest przekształceniem liniowym, a druga – symetryczną formą dwuliniową. Jeśli np. różniczkowalna w pewnym punkcie funkcja dwóch zmiennych ma zerową różniczkę oraz jej druga różniczka jest dodatnio określona to w punkcie tym jest minimum lokalne. Patrz też: http://smurf.mimuw.edu.pl/node/244.

Fakt 181. *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 $q(\alpha_n/\|\alpha_n\|) = a_n$.

Co to twierdzenie oznacza? Mówi ono, że przedstawienie formy kwadratowej w postaci diagonalnej, a więc w „nowym układzie prostopadłym" pozwala odczytać kierunki „najszybszego" jej wzrostu i „najszybszego" jej spadku.

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.

Otóż w bazie $(\alpha_1, \alpha_2) = ((1,1),(1,-1))$ (ortogonalnej w $(\mathbb{R}^2, \langle\,,\rangle_{st})$) funkcja f „traktowana jako" forma kwadratowa może być zapisana w postaci $f(y_1\alpha_1 + y_2\alpha_2) = 3y_1^2 - y_2^2$. Twierdzenie mówi, że po wzięciu kierunków powyższych wektorów o normie 1, czyli

$$\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right) \quad \text{oraz} \quad \left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right)$$

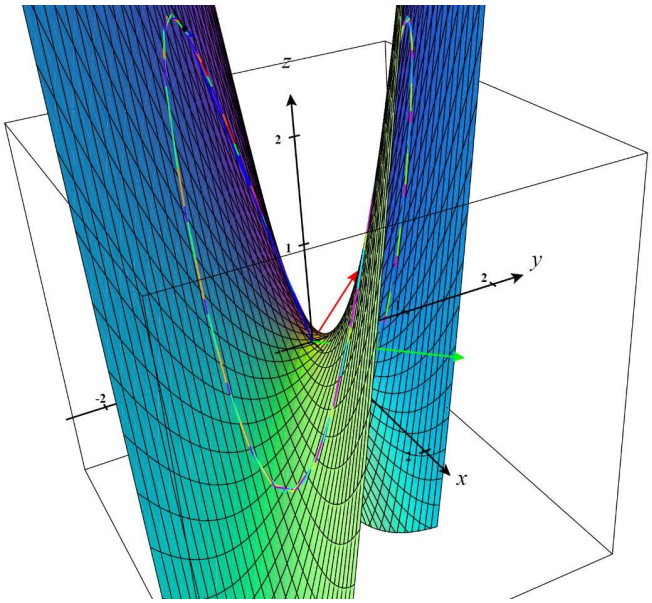
uzyskamy, że największa i najmniejsza wartość naszej funkcji na zbiorze I wynoszą odpowiednio

$$f\left(\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)\right) = 3 \quad \text{oraz} \quad f\left(\left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right)\right) = -1.$$

Co ciekawe, moglibyśmy też wziąć wektory

$$\left(-\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right) \quad \text{oraz} \quad \left(-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)$$

i również dla nich dostaniemy odpowiednio największą w zbiorze I wartość f czyli 3 oraz najmniejszą wartość równą -1. Poniżej poglądowy obrazek.



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

Pozostał nam dowód wyjściowego faktu. Niech h będzie formą dwuliniową symetryczną na $\mathbb{R}^n$ odpowiadającą formie kwadratowej q. Na mocy twierdzenia o diagonalizowalności macierzy symetrycznych rzeczywistych wiemy, że istnieje baza ortonormalna w $(\mathbb{R}^n, \langle\,,\rangle_{st})$ złożona z wektorów własnych macierzy $A = G(h; st)$. Niech $(\alpha_1, \ldots, \alpha_n)$ będzie tą bazą przy czym $A\alpha_i = \lambda_i$, dla $i - 1, \ldots, n$. Załóżmy też, że $\lambda_1 \geq \ldots \geq \lambda_n$. Dla każdego $\alpha \in \mathbb{R}^n$ mamy rozkłady wektorów α oraz $A\alpha$ w bazie ortonormalnej postaci:

$$\alpha = \langle \alpha, \alpha_1\rangle\alpha_1 + \ldots + \langle \alpha, \alpha_n\rangle\alpha_n, \quad A\alpha = \lambda_1\langle \alpha, \alpha_1\rangle\alpha_1 + \ldots + \lambda_n\langle \alpha, \alpha_n\rangle\alpha_n.$$

Jeśli założymy, że $\|\alpha\| = 1$, to mamy też $\langle \alpha, \alpha_1\rangle^2 + \ldots + \langle \alpha, \alpha_n\rangle^2 = 1$, a także

$$\langle \alpha, A\alpha\rangle = \lambda_1\langle \alpha, \alpha_1\rangle^2 + \ldots + \lambda_n\langle \alpha, \alpha_n\rangle^2.$$

A zatem dla α o normie 1 mamy (proszę dokładnie przemyśleć zwłaszcza trzecią równość):

$$\begin{aligned} q(\alpha) = h(\alpha, \alpha) = \alpha^T A\alpha = \langle \alpha, A\alpha\rangle &= \lambda_1\langle \alpha, \alpha_1\rangle^2 + \ldots + \lambda_n\langle \alpha, \alpha_n\rangle^2 \\ &\leq \lambda_1\langle \alpha, \alpha_1\rangle^2 + \ldots + \lambda_1\langle \alpha, \alpha_n\rangle^2 = \lambda_1. \end{aligned}$$

Analogicznie pokazujemy, że $q(\alpha) \geq \lambda_n$, dla $\|\alpha\| = 1$. Jeśli teraz α jest wektorem własnym A odpowiadającym λ_1 oraz $\|\alpha\| = 1$, to

$$q(\alpha) = h(\alpha, \alpha) = \langle \alpha, A\alpha\rangle = \langle \alpha, \lambda_1\alpha\rangle = \lambda_1\|\alpha\|^2 = \lambda_1.$$

Podobnie $q(\alpha) = \lambda_n$, jeśli $\|\alpha\| = 1$ oraz α jest wektorem własnym A odpowiadającym wartości własnej λ_n. Dowód jest zatem zakończony.

Dodatek. Twierdzenie Hasse-Minkowskiego

Załóżmy, że chcecie Państwo rozwiązać w liczbach całkowitych równanie $x^3 - 2x + 17 = 0$. Oczywiście znamy rezultat szkolny, który mówi jak to robić, ale on ukrywa meritum sprawy. To równanie nie ma rozwiązań w $\mathbb{Z}$ (ani w $\mathbb{Q}$), bo jeśli „zajrzymy z nim" do małego świata ciała pięcioelementowego $\mathbb{Z}_5$, to ma ono postać $x^3 + 3x + 2 = 0$ i nie ma w tym ciele rozwiązań. Stąd i wyjściowe równanie nad $\mathbb{Z}$ ich nie ma. Pytanie: czy z każdym równaniem wielomianowym o współczynnikach całkowitych wystarczy „zajrzeć" do pewnych ciał skończonych, aby dowiedzieć się czy rozwiązanie w $\mathbb{Z}$ istnieje? O tym mówi i owo twierdzenie szkolne, i wynik Hasse-Minkowskiego, o którym chcemy powiedzieć tu kilka zdań. Aby zrozumieć wysłowienie tego faktu odsyłam do jednego z wcześniejszych dodatków dotyczących ciał p-adycznych, a także do notatek z wykładu gwiazdkowego/

Wykłady https://mimuw.edu.pl/~amecel/2021l/gal21/GAL2+_AM_w16.pdf, https://mimuw.edu.pl/~amecel/2021l/gal21/GAL2+_AM_w17.pdf.

Na czym polega problem z rozwiązaniem równania wyżej? Niestety, gdybyśmy znaleźli rozwiązanie powyższego równania w $\mathbb{Z}_5$, to nie mielibyśmy pewności, że istnieje ono nad $\mathbb{Z}$ czy też $\mathbb{Q}$. Zacznijmy od zacytowania następującego rezultatu.

Fakt 182 (https://arxiv.org/pdf/2102.08379.pdf)**.** *Dana jest liczba całkowita $n \neq 1$ spełniająca warunki:*

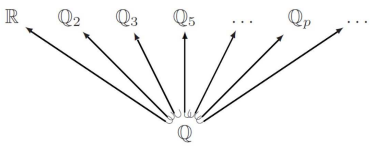
- *n jest niepodzielna przez sześcian liczby pierwszej,*
- *$n \equiv 1$ (mod 9),*
- *jeśli liczba pierwsza q dzieli n, to $q \equiv 1$ (mod 3).*

Wówczas wielomian:

$$(x^3 - n)(x^2 + 3) = 0$$

nie ma pierwiastków wymiernych, choć ma rozwiązania w ciele $\mathbb{Z}_p$.

Istnienie wielomianów o współczynnikach w $\mathbb{Z}$ takich jak powyższe przeczy prawdziwości *zasady lokalno-globalnej* dla dowolnego równania $f = 0$, $f \in \mathbb{Q}[x]$. Pytanie: czy po ograniczeniu do pewnych klas równań zasada ta może działać (i jak ją dokładnie sformułować)? To jedno z centralnych zagadnień teorii liczb. Poniższy rezultat to jedno z ważniejszych twierdzeń teorii form kwadratowych początku XX stulecia, otwierające nowy rozdział jej rozwoju.



Oczywiście $\mathbb{Q}_p \subseteq Q_p$, więc rozważanie formy q_p ma sens. Więcej o tym twierdzeniu można przeczytać w tekście http://www.math.union.edu/hatleyj/Capstone.pdf.

Fakt 183 (Zasada lokalno-globalna (Hasse-Minkowski), 1921)**.** *Niech q będzie formą kwadratową na skończenie wymiarowej przestrzeni nad ciałem $\mathbb{Q}$ oraz niech q_p oznacza formę q rozważaną nad ciałem liczb p-adycznych $\mathbb{Q}_p$, gdzie $p \in \mathbb{P}$ lub $p = \infty$ (konwencja: $\mathbb{Q}_\infty = \mathbb{R}$). Wówczas równanie $q(x) = 0$ ma rozwiązanie wtedy i tylko wtedy, gdy równania $q_p = 0$ mają rozwiązania dla każdego $p \in \mathbb{P} \cup \{\infty\}$.*

Notka historyczna. Sumy kwadratów

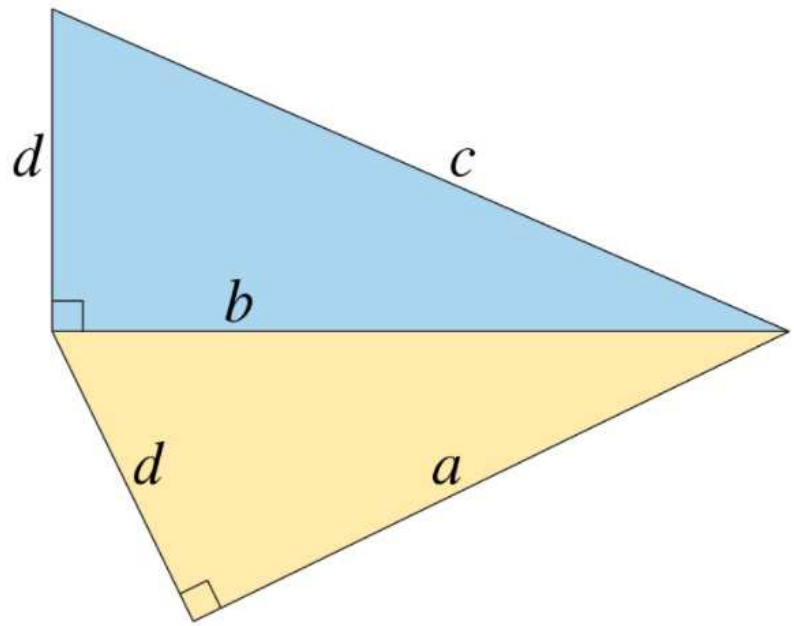
Wyrażeniami i równaniami typu kwadratowego zajmowano się już w starożytnym Babilonie. W starożytnej Grecji, a później w Afryce Północnej i Europie badano je także w kontekście geometrycznym (twierdzenie Pitagorasa, układ współrzędnych, stożkowe...) Najważniejszym czysto matematycznym źródłem była jednak teoria liczb. Punktem wyjścia był Problem 8 z Księgi II starożytnego traktatu *Arithmetica* Diofantosa z III wieku: daną liczbę wymierną przedstawić jako sumę kwadratów liczb wymiernych. Liczne przeformułowania były źródłami wielu słynnych problemów matematycznych stawianych najpierw przez uczonych arabskich w IX wieku, później przez czerpiącego z dorobku arabskiego Fibonacciego walczącego w XIII wieku z problemem CONGRUUM.

Fibonacci (1170-1250), a właściwie Leonardo (z Pizy) zasłynął przez upowszechnienie w początkach XIII wieku notacji arabskiej opartej na cyfrach $0-9$ pochodzącej z tekstu al-Khwārizmiego z 825 roku (od którego nazwę bierze algebra). Nikogo by to nie interesowało gdyby nie fakt, że *Liber Abbaci* (Księga Liczydła), obok wprowadzenia słynnego dziś ciągu jako rozwiązania problemu rozmnażania się królików, zawierała istotne praktyczne wskazówki dotyczące używania ułamków i rozwiązywania rachunkowych problemów powstających przy... wymianie dóbr, zwłaszcza różnych walut. To było wtedy ważne.

W 1225 roku Pizę odwiedził cesarz Fryderyk II (syn Barbarossy). Znając reputację Leonardo cesarz uznał, że warto poddać ją próbie przez... zorganizowanie turnieju (typowe w tamtych czasach). Zawodnicy zadawali sobie nawzajem pytania. Drużynę cesarza stanowili Jan z Palermo i Mistrz Teodor, zaś drużynę Leonarda stanowił on sam. Pytanie mu postawione brzmiało: znaleźć kwadrat liczby wymiernej, który pozostaje kwadratem liczby wymiernej zarówno gdy dodamy do niego 5, jak i gdy odejmiemy od niego 5. Innymi (naszymi) słowy oczekiwano przykładu, że 5 stanowi *congruum*, czyli różnicę w ciągu arytmetycznym trzech kwadratów liczb wymiernych. Najmniejszy przykład rozwiązania problemu turniejowego to $1681/144$ – co Leonardo wykrył (choć przed nim inni). W swoim ważnym dziele *Liber quadratorum* Fibonacci atakował ogólny problem congruum próbując zastąpić liczbę 5 innymi, w tym kwadratami liczb całkowitych (np. 1), dla których nie umiał go rozwiązać. Zrobił to dopiero Fermat, co wymagało prostego pomysłu zakładającego, że z istnienia „najmniejszej realizacji kwadratowego congruum" wywieść można istnienie jeszcze mniejszej realizacji (i dostać sprzeczność). Jest to *technika nieskończonego schodzenia*.

Do 1915 roku znano wszystkie congrua mniejsze niż 100. W 1986 roku – mniejsze niż 2000 (komputer). Ogólne rozwiązanie problemu congruum nie jest znane.

Fermat w 1670 roku rozwiązał problem Fibonacciego pokazując, ze jeśli różnice pewnych dwóch par kwadratów liczb całkowitych (lub ogólniej: liczb wymiernych) są identyczne, to nie mogą być one kwadratami. Innymi słowy, w poniższej konfiguracji trójkątów prostokątnych jedna z długości a, b, c, d musi być liczbą niewymierną.



Jeśli $d^2 = b^2 - a^2 = c^2 - b^2$, to jedna z liczb a, b, c, d jest niewymierna. Źródło: Wikipedia. Fermat's right triangle theorem.

Fermat zajmował się między innymi badaniem możliwości rozkładania liczb na sumy kwadratów. Aby opowiedzieć nieco o historii tego znanego zagadnienia przejdźmy do języka form kwadratowych. W notce tej zajmiemy się niezwykle ważnym i ciekawym problemem reprezentowalności formy kwadratowej o współczynnikach całkowitych. Interesuje nas jakie wartości całkowite przyjmować może ta forma. Zaczniemy od ogólnej definicji.

Definicja 113. *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 $D_K(q) = K \setminus \{0\}$.*

Interesuje nas odpowiedź na pytanie **jakie liczby całkowite mogą być reprezentowane przez formy kwadratowe o wyrazach całkowitych**?

Kiedy formy te mają zbiór wartości $\mathbb{Z}_+$, co określamy mianem **całkowitej formy uniwersalnej**?

Zobaczmy kilka przykładów.

- Równanie $x^2 - xy + y^2 = 2$ nie ma całkowitych rozwiązań.

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 $x \in \{-1, 0, 1\}$.

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

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

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

Więc jeśli $\begin{bmatrix} x \\ y \end{bmatrix}$ jest rozwiązaniem, to jest nim także

$$\begin{bmatrix} -3 & 8 \\ -1 & 3 \end{bmatrix}^n \cdot \begin{bmatrix} x \\ y \end{bmatrix}, \quad \text{dla} \quad n \geq 1,$$

czyli rozważane równanie ma nieskończenie wiele rozwiązań.

Problem reprezentowalności form kwadratowych znany jest (pod różnymi nazwami) od wieków. Oto kilka przykładów znanych rezultatów.

- **Euklides, -300.** Opis trójek liczb całkowitych, na których zeruje się forma całkowita (tzw. trójki pitagorejskie)

$$q(x_1, x_2, x_3) = x_1^2 + x_2^2 - x_3^2.$$

- **Fermat, 1640.** Forma kwadratowa 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 kwadratowa 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 kwadratowa 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 $a, k \in \mathbb{Z}$.

- **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 $q(x_1, x_2, x_3, x_4) = ax_1^2 + bx_2^2 + cx_3^2 + dx_4^2$.

- **Dickson, 1926.** Ramanujan nie ma racji, są tylko 54 uniwersalne formy całkowite o czterech zmiennych. Jest nieskończenie wiele całkowitych form uniwersalnych, dla każdej liczby zmiennych większej niż 4 (co wynika z twierdzenia o czterech kwadratach Lagrange'a), 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: $\{1, 2, 3, 5, 6, 7, 10, 14, 15\}$).

- **Conway, Schneeberger, 1993 (15-theorem).** Wynik Halmosa jest prawdziwy dla dowolnej formy

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

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 problemu otwartego: forma ternarna Ramanujana.

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.

• **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!

Ważny 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 wnieśli do teorii zagadnienia takie, jak równoważność form, początki teorii genusu, użycie wyróżnika, teoria kompozycji form, wyższe prawa wzajemności.
- Dedekind, Kronecker, Minkowski, Dirichlet, Hilbert rozważali całkowite formy kwadratowe w kontekście algebraicznej teorii liczb i prapoczątków geometrii algebraicznej.

Na koniec przytoczmy **bardzo trudne pytanie**. Czy istnieje nieskończenie wiele liczb pierwszych postaci

$$x^2 + 1,$$

dla $x \in \mathbb{Z}$? To jeden z czterech problemów zestawionych w 1912 roku przez E. Landau na Międzynarodowym Kongresie Matematycznym.

Pozostałe *problemy Landau* to: hipoteza Goldbacha, hipoteza liczb bliźniaczych i hipoteza Legendre'a o istnieniu liczby pierwszej pomiędzy $n^2 > 1$ a $(n+1)^2$.

Fundamentalny wkład w badanie wspomnianego problemu ma Profesor Henryk Iwaniec, Absolwent Wydziału MIM UW (żyje i pracuje w USA), pochodzący z Elbląga. W 1978 roku Profesor Iwaniec uzyskał wybitny rezultat: istnieje nieskończenie wiele liczb postaci $x^2 + 1$, które są iloczynami co najwyżej dwóch liczb pierwszych. Natomiast w 1997 Profesor udowodnił wraz z Friendlanderem, że istnieje nieskończenie wiele liczb pierwszych postaci $x^2 + y^4$.

Za wkład w rozwiązanie tej hipotezy prof. Iwaniec otrzymał (wraz z Peterem Sarnakiem i Richardem Taylorem) w 2001 roku nagrodę Ostrowskiego (w 1995 otrzymał ją A. Wiles za dowód Wielkiego Twierdzenia Fermata, a w 2005 r. – Ben Green i Terrence Tao za twierdzenie o ciągach arytmetycznych w zbiorze liczb pierwszych). W 2015 roku. Profesor otrzymał Nagrodę Shawa (razem z Gerdem Faltingsem). Osoby zainteresowane sylwetką najbardziej utytułowanego obecnie matematyka z Polski zachęcam między innymi do lektury wywiadu „Matematyka to moja miłość" (https://www.cultureave.com/matematyka-to-moja-milosc/), gdzie można dowiedzieć się więcej o życiu Profesora i Jego matematycznych osiągnięciach.

Literatura dotycząca zacytowanych wyżej zagadnień jest bardzo szeroka. Na elementarnym poziomie można o niektórych z nich poczytać w znakomitych tekstach Keitha Conrada (https://kconrad.math.uconn.edu/blurbs/), np. Pythagorean triples, Sums of two squares and lattices, Fermat's method of descent, Congruent number problem, Quadratic residue patterns modulo a prime, i wielu innych. Zainteresowanych – gorąco zachęcam.