



Geometria w teorii liczb

Antoni Łuczak

17.12.2024

Teoria

Twierdzenie 1 (Przekształcenia liniowe skalują objętości)

Niech $X \in \mathbb{R}^n$ będzie figurą o objętości V oraz A odwracalną macierzą $n \times n$ o współczynnikach rzeczywistych. Wtedy figura

$$AX = \{Ax \mid x \in X\}$$

ma objętość $|\det A| \cdot V$.

Nie będziemy dokładnie definiowali czym jest objętość, natomiast w rozpatrywanych przykładach powinno być to w miarę jasne. Możemy o tym myśleć w następujący sposób: podobnie jak podczas całkowania przybliżamy pole za pomocą prostokątów, możemy przybliżać objętość rozpatrywanej figury za pomocą prostopadłościanów.

Definicja 1 (Kraty)

Kratę rozpinaną przez wektory $v_1, \dots, v_m \in \mathbb{R}^n$ nazwiemy zbiór wszystkich kombinacji całkowitych tych wektorów. Inaczej

$$\Lambda = \{a_1 v_1 + \dots + a_m v_m \mid a_1, \dots, a_m \in \mathbb{Z}\}.$$

Dodatkowo jeśli $m = n$ oraz rozpatrywane wektory są liniowo niezależne, to *równoległościannem fundamentalnym kraty Λ nazwiemy zbiór*

$$\{x_1 v_1 + \dots + x_n v_n \mid x_1, \dots, x_n \in [0, 1]\},$$

a jego objętość oznaczmy przez $Vol(\Lambda)$.

Twierdzenie 2 (Minkowskiego o figurze wypukłej)

Niech A będzie wypukłą oraz symetryczną względem 0 figurą w $\mathbb{R}^n$. Niech dodatkowo Λ będzie kratą rozpinaną przez n liniowo niezależnych wektorów. Wtedy jeżeli

$$Vol(A) > 2^n Vol(\Lambda),$$

to wewnątrz A znajduje się pewien niezerowy element kraty Λ .

Przykład: Każda liczba pierwsza postaci $4k + 1$ jest sumą dwóch kwadratów liczb całkowitych.

Dowód. Pomysł jest następujący: będziemy chcieli znaleźć taki niezerowy punkt (x, y) o współrzędnych całkowitych wewnątrz dysku $D = \{(x, y) \mid x^2 + y^2 < 2p\}$, że $p \mid x^2 + y^2$. W tym celu skonstruujemy taką kratę Λ , że każdy jej element (x, y) będzie spełniał $p \mid x^2 + y^2$ oraz $\text{Vol}(\Lambda) = p$. Wiemy, że istnieje taka liczba całkowita c , że $p \mid c^2 + 1$ (przykładowo $c = (\frac{p-1}{2})!$). W takim razie dowolny wektor będący wielokrotnością $(c, 1)$ spełnia $p \mid x^2 + y^2$. Dodatkowo zwiększając współrzędną x o wielokrotność p , nie wpływamy na sumę kwadratów współrzędnych mod p . W takim razie dowolny element kraty generowanej przez $(c, 1)$ oraz $(p, 0)$ ma sumę kwadratów współrzędnych podzieloną przez p . Dodatkowo

$$\text{Vol}(\Lambda) = \left| \det \begin{bmatrix} c & p \\ 1 & 0 \end{bmatrix} \right| = p.$$

Mamy

$$\text{Vol}(D) = 2p\pi > 4p = 4\text{Vol}(\Lambda),$$

zatem na mocy twierdzenia Minkowskiego, istnieje taka niezerowa para (x, y) liczb całkowitych, że $p \mid x^2 + y^2$ oraz $0 < x^2 + y^2 < 2p$. W takim razie $x^2 + y^2 = p$. $\square$

Ćwiczenie 1. Udowodnij, że objętość kraty nie zależy od wyboru wektorów generujących ją (zaczniemy od przypadku 2 wymiarowego).

Ćwiczenie 2. Rozpatrzmy zbiór postaci

$$\{(x, y) \mid ax^2 + bxy + cy^2 < d\},$$

gdzie a, b, c, d są liczbami rzeczywistymi oraz $d > 0$. Udowodnij, że obszar ten jest ograniczony wtedy i tylko wtedy, gdy $4ac > b^2$. Pokaż, że w tym wypadku jest on wypukły oraz że jego objętość wynosi

$$\frac{2\pi d}{\sqrt{4ac - b^2}}.$$

Generowanie punktów na krzywych

Lemat 1 (Generowanie punktów na stożkowej)

Załóżmy, że punkt X o współrzędnych wymiernych leży na krzywej stożkowej Γ , której współczynniki również są wymierne. Niech dodatkowo Y będzie pewnym punktem rzeczywistym na Γ . Wtedy Y ma współrzędne wymierne $\iff$ nachylenie prostej XY jest wymierne.

Przykład: Wyznacz wszystkie punkty wymierne na okręgu jednostkowym.

Dowód. Zauważmy, że na okręgu jednostkowym leży punkt $(0, 1)$. Możemy teraz rozpatrzyć prostą o równaniu $y = tx + 1$ o nachyleniu t , przechodzącą przez $(0, 1)$. Obliczmy jej drugie przecięcie z okręgiem jednostkowym:

$$1 = (tx + 1)^2 + x^2 = x^2(t^2 + 1) + 2tx + 1 \iff x(x(t^2 + 1) + 2t) = 0.$$

W takim razie $x = \frac{-2t}{t^2 + 1}$ oraz $y = \frac{1 - t^2}{t^2 + 1}$. Skoro każdemu punktowi na okręgu odpowiada pewne wymierne nachylenie oraz każdemu nachyleniu odpowiada punkt wymierny, to za pomocą takiej parametryzacji otrzymamy wszystkie punkty wymierne na okręgu. Dodatkowo podstawiając $t = \frac{m}{n}$ otrzymujemy charakteryzację wszystkich trójkątów pitagorejskich. $\square$

Ćwiczenie 3. Rozwiąż równanie $x^2 + xy + y^2 = 1$ w liczbach wymiernych.

Definicja 2 (Krzywa sześcienna)

Krzywą sześcienną będziemy nazywali zbiór punktów spełniających równanie postaci

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

Lemat 2 (Generowanie punktów na krzywych sześciennych)

Dana jest krzywa sześcienna Γ oraz dwa punkty wymierne X, Y na niej leżące. Prosta XY przecina Γ po raz trzeci w punkcie Z . Wtedy Z również ma współrzędne wymierne.

Przykład: Udowodnij, że istnieją takie liczby wymierne a, b , że $a^3 + b^3 = 9$ oraz $\{a, b\} \neq \{1, 2\}$. Podaj przykład takich liczb.

Dowód. Popatrzmy na krzywą $\Gamma : x^3 + y^3 = 9$. Leżą na niej 2 oczywiste punkty wymierne $(1, 2)$ oraz $(2, 1)$. Niestety prosta przechodząca przez te punkty nie przecina ponownie Γ (jak możemy to interpretować geometrycznie?). Zamiast prowadzić prostą przez $(1, 2)$ oraz $(2, 1)$, poprowadźmy prostą przez $(1, 2)$ oraz $(1, 2)$. Czym jest ta prosta? Jest to styczna do Γ w $(1, 2)$. Ma ona równanie $y = 2 + f'(1)(x - 1)$, gdzie

$$f'(x) = \left(\sqrt[3]{9 - x^3} \right)' = -3x^2 \cdot \frac{1}{3}(9 - x^3)^{-\frac{2}{3}}.$$

W takim razie $f'(1) = -\frac{1}{4}$. Popatrzmy na "trzecie" przecięcie tej prostej z Γ :

$$9 = \left(\frac{9}{4} - \frac{x}{4} \right)^3 + x^3 = \frac{63}{64}x^3 + \frac{27}{64}x^2 + \dots$$

Dostaliśmy wielomian sześcienny, który ma podwójny pierwiastek $x = 1$ (Można to zweryfikować ręcznie), zatem jego trzeci pierwiastek to z wzorów Viete'a $x = -\frac{27}{63} - 2 = -\frac{3}{7} - 2 = -\frac{17}{7}$. Wstawiając to do równania prostej dostajemy parę $(-\frac{17}{7}, \frac{20}{7})$. $\square$

Zadania

Zadanie 1. Dodatnie liczby a, b, c spełniają $ac = b^2 + b + 1$. Udowodnij, że równanie

$$ax^2 - (2b + 1)xy + cy^2 = 1$$

ma rozwiązanie całkowite.

Zadanie 2 (59OM-3-6). Niech S będzie zbiorem wszystkich dodatnich liczb całkowitych, które można przedstawić w postaci $a^2 + 5b^2$ dla pewnych względnie pierwszych liczb całkowitych a i b . Niech ponadto p będzie liczbą pierwszą dającą resztę 3 z dzielenia przez 4. Wykazać, że jeżeli pewna dodatnia wielokrotność liczby p należy do zbioru S , to również liczba $2p$ należy do zbioru S .

Zadanie 3 (Lemat Thuego). Dana jest liczba pierwsza p oraz pewna liczba całkowita c . Wtedy istnieje taka para liczb całkowitych $(x, y) \neq (0, 0)$, że $p \mid x + cy$ oraz $|x|, |y| < \sqrt{p}$.

Zadanie 4 (Twierdzenie Minkowskiego o formach liniowych). Niech $A = (a_{ij})$ będzie n wymiarową odwracalną macierzą o współczynnikach rzeczywistych oraz niech $c_1, \dots, c_n$ będą takimi dodatnimi liczbami rzeczywistymi, że $c_1 \cdots c_n > |\det A|$. Wykaż, że istnieją takie liczby całkowite $x_1, \dots, x_n$, że

$$\left| \sum_{j=1}^n a_{ij} x_j \right| < c_i$$

dla każdego i .

Zadanie 5. Dane są liczby rzeczywiste $a_1, \dots, a_n$, dodatnia liczba całkowita M oraz dodatnia liczba rzeczywista ϵ . Udowodnij, że istnieją takie liczby całkowite $m_1, \dots, m_n$ oraz p , że $|p| \leq M^n(1 + \epsilon)$ oraz $|m_i - pa_i| < \frac{1}{M}$ dla każdego i . Czy dla $\epsilon = 0$ teza dalej będzie prawdziwa?

Zadanie 6. Dana jest liczba naturalna n . Udowodnij, że równanie $x^2 + xy + y^2 = n$ ma rozwiązanie wymierne wtedy i tylko wtedy, gdy ma rozwiązanie całkowite.

Zadanie 7. Udowodnij, że każda liczba naturalna jest sumą czterech kwadratów liczb całkowitych. *Uwaga:* Objętość czterowymiarowej kuli jednostkowej wynosi $\pi^2/2$.

Zadanie 8 (68OM-3-5). Dane są dodatnie liczby całkowite $a < b$. Dowieść, że istnieją takie liczby całkowite p, q, r, s , że $a < \frac{p}{q} < \frac{r}{s} < b$ oraz $p^2 + q^2 = r^2 + s^2$.

Zadanie 9 (RMM 2016-3). *Ciągiem sześciennym* nazwiemy ciąg postaci $a_n = n^3 + bn^2 + cn + d$, gdzie b, c, d są liczbami całkowitymi, a n przebiega przez wszystkie liczby całkowite.

(a) Udowodnij, że istnieje taki ciąg sześcienny, że jedyne wyrazy, które są kwadratami liczb całkowitych to a_{2015} oraz a_{2016} .

(b) Wyznacz wszystkie możliwe wartości liczby $a_{2015} \cdot a_{2016}$ dla ciągu spełniającego (a).

Zadanie 10. Niech a będzie ustaloną dodatnią liczbą całkowitą. Udowodnij, że równanie

$$x^3 + x + a^2 = y^2$$

ma rozwiązanie w dodatnich liczbach całkowitych.

Zadanie 11. Udowodnij, że jeśli pewna liczba całkowita jest sumą trzech kwadratów liczb wymiernych, to również jest sumą kwadratów trzech liczb całkowitych.