Równania diofantyczne kwadratowe jednorodne

Andrzej SCHINZEL *

Od Redakcji: Autor artykułu używa pojęć, które nie wszystkim Czytelnikom są znane. Dlatego na tym i sąsiednim marginesie zamieszczamy nieco objaśnień.

Zbiór punktów przestrzeni kartezjańskiej $\mathbb{R}^n$ spełniających równanie k-tego stopnia nazywamy tworem algebraicznym stopnia k. W artykule obok rozważane równania diofantyczne mogą być interpretowane jako poszukiwanie punktów kratowych (czyli mających wszystkie współrzędne całkowite) leżących na tworach algebraicznych stopnia 2.

Tworami algebraicznymi stopnia 2 są np. na płaszczyźnie $x_1^2 + 2x_2 = 0$ czy w przestrzeni trójwymiarowej $x_1^2 - x_2^2 + 2x_3 = 0$ – w pierwszym przypadku jest to parabola, a w drugim paraboloida hiperboliczna, czyli kształt dachu nad warszawskim przystankiem kolejowym Ochota.

Twory stopnia 1 w dowolnym wymiarze są tzw. hiperpłaszczyznami, czyli przestrzeniami o jeden wymiar mniejszymi od przestrzeni, w której są rozpatrywane – na płaszczyźnie są to proste, a w przestrzeni trójwymiarowej płaszczyzny.

Proste w przestrzeni dowolnego wymiaru można przedstawić jako zbiory punktów postaci $(a_1 + b_1 t, a_2 + b_2 t, \dots, a_n + b_n t)$, gdzie t przebiega wszystkie liczby rzeczywiste. Punkty tworu algebraicznego, dla których każda przechodząca przez nie prosta albo cała leży na tworze, albo nie ma z nim już więcej punktów wspólnych, nazywamy osobliwymi (np. wierzchołek stożka).

Przy bardziej zaawansowanych badaniach dogodnie jest przenieść twory algebraiczne do (obszerniejszej) przestrzeni rzutowej, która powstaje z $\mathbb{R}^n$ przez dołączenie do każdej prostej jej kierunku (jako dodatkowego punktu). Przyjmuje się przy tym umowę, że te nowe punkty leżą na jednej hiperpłaszczyźnie. Technicznie sprowadza się to do dopisania w równaniach tworów do każdego z jednomianów dodatkowej współrzędnej x_0 w takiej potędze, by, po pierwsze, stopień równania nie zwiększył się, i, po drugie, by każdy jednomian był tego samego stopnia (czyli by wielomian był jednorodny) – w podanych przykładach będzie to $x_1^2 + 2x_0x_2 = 0$ i $x_1^2 - x_2^2 + 2x_0x_3 = 0$. Punkty też otrzymują nową współrzędną – „stare" punkty dostają zerową współrzędną 1, współrzędne „nowych" punktów zaczynają się od 0. Jednorodność równań powoduje, że teraz punkt ma wiele układów współrzędnych – układy proporcjonalne oznaczają ten sam punkt.

Rozwiązywać będziemy diofantyczne równania kwadratowe jednorodne postaci

$$Q(x_0, \dots, x_n) = \sum_{i,j=0}^{n} A_{ij} x_i x_j = 0, \quad \text{gdzie } A_{ij} = A_{ji}, \tag{1}$$

dlatego zakładamy, iż wszystkie A_{ij} są liczbami całkowitymi, oraz że poszukujemy tylko całkowitych wartości x_i $(i = 0, 1, \dots, n)$.

Należy zwrócić uwagę, że rozróżniamy rozwiązanie $[x_0, \dots, x_n]$ w przestrzeni kartezjańskiej $\mathbb{R}^{n+1}$ od punktu $(x_0, \dots, x_n)$ w przestrzeni rzutowej P^n. Udowodnimy następujące twierdzenia i wnioski.

Twierdzenie 1. *Jeżeli $(b_0, \dots, b_n)$ jest punktem nieosobliwym tworu* (1)*, b_i są całkowite i $b_0 \neq 0$, to wszystkie rozwiązania całkowite równania* (1) *poza hiperpłaszczyzną*

$$\sum_{i,j=0}^{n} A_{ij} b_i x_j = 0 \tag{2}$$

dane są wzorami

$$\begin{aligned} \rho x_0 &= -b_0 \sum_{i,j=1}^{n} A_{ij} r_i r_j \\ \rho x_k &= -b_k \sum_{i,j=1}^{n} A_{ij} r_i r_j + 2 r_k \sum_{i=0}^{n} \sum_{j=1}^{n} A_{ij} b_i r_j \quad (0 < k \leqslant n), \end{aligned} \tag{3}$$

gdzie r_i $(1 \leqslant i \leqslant n)$ oraz $\rho \neq 0$ przebiegają liczby całkowite, przy czym ρ jest wspólnym dzielnikiem prawych stron.

Twierdzenie 2. *Przy założeniach Twierdzenia* 1 *jeżeli pierwszy i drugi wskaźnik rzutowy tworu* (1) *wynoszą odpowiednio $n+1$ i $n-1$, to dla $n > 1$ wzory* (3) *dają wszystkie rozwiązania całkowite równania* (1).

Stosując to twierdzenie do równania

$$\Big(\sum_{i=0}^{n} x_i \Big)^2 - n \sum_{i=0}^{n} x_i^2 = 0, \tag{4}$$

wygodnie jest położyć

$$\sum_{i=1}^{n} r_i = r, \quad \sum_{i=1}^{n} r_i^2 = R; \quad \sum_{i=1}^{n} s_i = s, \quad \sum_{i=1}^{n} s_i^2 = S$$

i zauważyć, że dla $n = 1$ równanie (4) daje $x_0 x_1 = 0$, zatem ten przypadek można pominąć jako banalny. Mamy

Wniosek 1. *Dla $n > 1$ wszystkie rozwiązania równania* (4) *w liczbach całkowitych x_i $(0 \leqslant i \leqslant n)$ dane są wzorami*

$$\rho x_0 = nR - r^2, \quad \rho x_i = nR - r^2 + 2n r_i r_n \quad (1 \leqslant i < n), \quad \rho x_n = 2n r_n^2, \tag{5}$$

gdzie r_i $(1 \leqslant i \leqslant n)$ oraz $\rho \neq 0$ przebiegają liczby całkowite, przy czym ρ jest wspólnym dzielnikiem prawych stron równań (5).

Tomasz Ordowski zauważył jeszcze inne wzory dające rozwiązania równania (4) i w liście do autora wysunął przypuszczenie, że z wzorów tych można otrzymać wszystkie rozwiązania równania (4) w liczbach całkowitych nieujemnych. Tak rzeczywiście jest dla $n > 1$, zachodzi bowiem

Wniosek 2. *Dla $n > 1$ wszystkie rozwiązania równania* (4) *w liczbach całkowitych x_i $(0 \leqslant i \leqslant n)$ dane są wzorami*

$$\sigma x_i = \frac{S + s^2}{2} - s s_{i+1} \quad (0 \leqslant i < n), \quad \sigma x_n = s^2, \tag{6}$$

gdzie s_i $(1 \leqslant i \leqslant n)$ oraz $\sigma \neq 0$ przebiegają liczby całkowite, przy czym σ jest wspólnym dzielnikiem prawych stron równań (6).

*Instytut Matematyczny PAN, Warszawa

Od Redakcji cd.:

Standardy geometrii analitycznej z każdym tworem stopnia 2 wiążą macierz symetryczną, mającą tę własność, że gdy pomnoży się ją przez punkt, otrzymuje się równanie tego tworu – w podanych przykładach będzie to odpowiednio

$$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

i

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

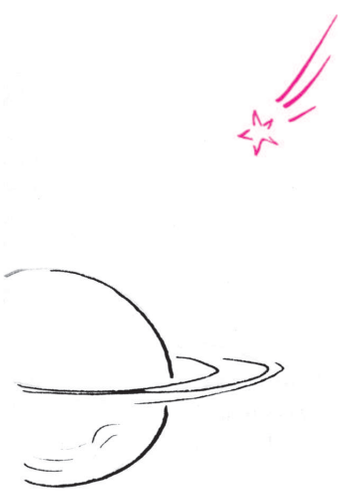
Jeśli macierz tę oznaczymy $[A_{ij}]$, to równanie tworu będzie postaci

$$\sum_{i,j=0}^{n} A_{ij}x_ix_j = 0.$$

Zerowanie się wyznacznika tej macierzy oznacza, że opisany przez nią twór ma punkty osobliwe.

Jeśli od każdego z wyrazów na głównej przekątnej macierzy tworu odejmiemy zmienną λ, to jej wyznacznik będzie względem λ wielomianem stopnia $n+1$. Liczba jego pierwiastków nazywana jest pierwszym wskaźnikiem rzutowym tworu, a wartość bezwzględna różnicy między liczbą pierwiastków dodatnich i ujemnych – drugim wskaźnikiem rzutowym.

[Tego rodzaju formalizm można znaleźć w książce: Karol Borsuk, *Geometria analityczna wielowymiarowa*, Warszawa, 1976.]



Dowód twierdzenia 1. Przypuśćmy, że liczby x_i są całkowite, i niech $r_i = b_0x_i - b_ix_0$ $(0 \leqslant i \leqslant n)$. Zatem r_i są całkowite, $r_0 = 0$ i mamy

$$\begin{aligned} 0 &= b_0^2Q(x_0,\dots,x_n) = \\ &= Q(b_0x_0 + r_0,\dots,b_nx_0 + r_n) = \\ &= \sum_{i,j=0}^{n} A_{ij}(b_ix_0 + r_i)(b_jx_0 + r_j) = \\ &= x_0^2Q(b_0,\dots,b_n) + 2x_0\sum_{i,j=0}^{n} A_{ij}b_ir_j + \sum_{i,j=1}^{n} A_{ij}r_ir_j. \end{aligned} \tag{7}$$

Otóż $Q(b_0,\dots,b_n) = 0$,

$$\begin{aligned} \sum_{i,j=0}^{n} A_{ij}b_ir_j &= \sum_{i,j=0}^{n} A_{ij}b_i(b_0x_j - b_jx_0) = \\ &= b_0\sum_{i,j=0}^{n} A_{ij}b_ix_j - x_0\sum_{i,j=0}^{n} A_{ij}b_ib_j = \\ &= b_0\sum_{i,j=0}^{n} A_{ij}b_ix_j, \end{aligned} \tag{8}$$

zatem, jeżeli punkt $(x_0,\dots,x_n)$ leży na (1) poza hiperpłaszczyzną (2), z równania (7) otrzymujemy

$$x_0 = \frac{-\sum_{i,j=1}^{n} A_{ij}r_ir_j}{2\sum_{i=0}^{n}\sum_{j=1}^{n} A_{ij}b_ir_j}, \qquad x_k = \frac{r_k + b_kx_0}{b_0}.$$

Zatem wzory (3) zachodzą dla $\rho = 2b_0\sum_{i=0}^{n}\sum_{j=1}^{n} A_{ij}b_ir_j$.

Odwrotnie, przypuśćmy, że liczby x_k dane są wzorami (3), gdzie liczby r_i oraz $\rho \neq 0$ są całkowite i ρ jest wspólnym dzielnikiem prawych stron. Zatem liczby x_k są całkowite i wobec jednorodności równania (1) wystarcza dowieść, że przy pewnym $\rho \neq 0$ liczby x_k spełniają (1). Jeżeli $\sum_{i=0}^{n}\sum_{j=1}^{n} A_{ij}b_ir_j = 0$, to przy $\rho = 1$

$$Q(x_0,\dots,x_n) = \Big(\sum_{i,j=1}^{n} A_{i,j}r_ir_j\Big)^2 Q(b_0,\dots,b_n) = 0.$$

Jeżeli $\sum_{i=0}^{n}\sum_{j=1}^{n} A_{ij}b_ir_j \neq 0$, to kładąc

$$\rho = 2b_0\sum_{i=0}^{n}\sum_{j=1}^{n} A_{ij}b_ir_j,$$

z (3) otrzymujemy (7), zatem na mocy (7) zachodzi (1).

Do dowodu Twierdzenia 2 potrzebny będzie następujący techniczny

Lemat. *Przy założeniach Twierdzenia* 2 *hiperpłaszczyzna* (2) *ma z tworem* (1) *tylko jeden punkt wspólny, mianowicie* $(b_0,\dots,b_n)$.

Przyjmiemy go tutaj bez dowodu.

Dowód twierdzenia 2. Rozwiązanie $[0,\dots,0]$ otrzymuje się ze wzorów (3), przyjmując $r_i = 0$ $(1 \leqslant i \leqslant n)$, $\rho = 1$. Dlatego na mocy Lematu wystarczy wykazać, że jeśli przy pewnym $t \neq 0$ wymiernym wszystkie liczby tb_i $(0 \leqslant i \leqslant n)$ są całkowite, to rozwiązanie $t[b_0,\dots,b_n]$ otrzymuje się ze wzorów (3) przy całkowitych r_i oraz $\rho \neq 0$. Niech więc $t = l/m$, gdzie liczby l, m są całkowite względnie pierwsze; $l \neq 0$ i $m \mid b_i$ $(0 \leqslant i \leqslant n)$. Na mocy Lematu dla $n > 1$ istnieją liczby całkowite p_i $(0 \leqslant i \leqslant n)$, takie że $\sum_{i,j=0}^{n} A_{ij}b_ip_j = 0$, $Q(p_0,\dots,p_n) \neq 0$. Kładąc $r_i = b_0lp_i - b_ilp_0$ i stosując wzory (7) i (8) dla $x_i = lp_i$, otrzymujemy, że

$$\sum_{i=0}^{n}\sum_{j=1}^{n} A_{ij}b_ir_j = 0, \qquad \sum_{i,j=1}^{n} A_{ij}r_ir_j \neq 0,$$

zatem rozwiązanie $\frac{l}{m}[b_0,\dots,b_n]$ otrzymuje się ze wzorów (3) dla

$$\rho = -\frac{m}{l}\sum_{i,j=1}^{n} A_{ij}r_ir_j.$$

Uwaga 1. Założeń o wskaźnikach rzutowych nie można w Twierdzeniu 2 pominąć, jak wskazuje przykład równania $x_0^2 + x_1^2 - x_2^2 - x_3^2 = 0$ i rozwiązania $[b_0, b_1, b_2, b_3] = [1, 0, 1, 0]$. Rozwiązań $[x_0, x_1, x_0, x_1]$ przy $x_1 \neq 0$ nie da się otrzymać ze wzoru (3).

Symbol $(k_1, \ldots, k_n)$ oznacza największy wspólny dzielnik liczb $k_1, \ldots, k_n$.

Uwaga 2. Jeżeli $n = 2$ i $\sqrt{A_{12}^2 - A_{11}A_{22}}$ nie jest liczbą wymierną, to istnieje taka liczba całkowita $A \neq 0$ niezależna od r_1, r_2, że $\rho \mid A(r_1, r_2)^2$.

Dowód wniosku 1. Aby zastosować Twierdzenie 2, oznaczmy lewą stronę równania (4) przez $F_n(x_0, \ldots, x_n)$. Z tożsamości

$$F_1(x_0, x_1) = \frac{1}{2}(x_0 + x_1)^2 - \frac{1}{2}(x_0 - x_1)^2,$$
$$F_n(x_0, \ldots, x_n) = \frac{n}{n-1} F_{n-1}(x_0, \ldots, x_{n-1}) + \\ + (1-n)\left(\frac{x_0}{n-1} + \ldots + \frac{x_{n-1}}{n-1} - x_n\right)^2 \qquad (n > 1)$$

wynika przez indukcję, że pierwszy i drugi wskaźnik rzutowy tworu $F_n(x_0, \ldots, x_n)$ wynosi odpowiednio $n+1$ i $n-1$. Ponieważ $F_n(1, \ldots, 1, 0) = 0$, Twierdzenie 2 stosuje się przy $b_i = 1$ $(0 \leqslant i < n)$, $b_n = 0$.

Uwaga 3. Wniosek można też wyprowadzić bezpośrednio z Twierdzenia 1, dowód byłby krótszy, ale jego skuteczność niewyjaśniona.

Dowód wniosku 2. Załóżmy, że liczby całkowite x_i spełniają (4). Na mocy Wniosku 1 istnieją liczby całkowite r_i oraz $\rho \neq 0$ spełniające (5), przy czym $\rho \mid (nR - r^2, 2nr_ir_n, \ldots, 2nr_n^2)$. Połóżmy

$$s_1 = 2r, \qquad s_{i+1} = 2r - 2nr_i \quad (1 \leqslant i < n), \qquad \sigma = 2n\rho.$$

Mamy więc

$$r_i = \frac{s_1 - s_{i+1}}{2n}, \qquad r_n = \frac{s}{2n}, \qquad r = \frac{s_1}{2}, \qquad R = \frac{ns_1^2 - 2ss_1 + S}{4n^2},$$

zatem

$$\sigma x_0 = 2n\rho x_0 = 2n(nR - r^2) = \frac{S + s^2}{2} - ss_1,$$
$$\sigma x_i = 2n\rho x_i = 2n(nR - r^2 + 2nr_nr_i) =$$
$$= \frac{S + s^2}{2} - ss_1 + s(s_1 - s_{i+1}) = \frac{S + s^2}{2} - ss_{i+1} \qquad (1 \leqslant i < n),$$
$$\sigma x_n = 2n\rho x_n = 2n \cdot 2nr_n^2 = s^2,$$

czyli zachodzą wzory (6). Załóżmy teraz, że dla całkowitych s_i oraz $\sigma \neq 0$ zachodzą wzory (6), przy czym σ jest wspólnym dzielnikiem prawych stron. Ponieważ $S \equiv s^2 \bmod 2$, liczby x_i są całkowite. Połóżmy $r_i = s_1 - s_{i+1}$ $(1 \leqslant i < n)$, $r_n = s$, $\rho = 2n\sigma$. Mamy więc $s_1 = \frac{r}{n}$, $s_{i+1} = \frac{r}{n} - r_i$ $(1 \leqslant i < n)$, $s = r_n$ oraz

$$S = -\frac{r^2}{n} + 2\frac{r \cdot r_n}{n} + R - r_n^2,$$

zatem

$$\rho x_0 = 2n\sigma x_0 = 2n\left(\frac{S + s^2}{2} - ss_1\right) = nR - r^2,$$
$$\rho x_i = 2n\sigma x_i = 2n\left(\frac{S + s^2}{2} - ss_{i+1}\right) = nR - r^2 + 2nr_1r_n \qquad (1 \leqslant i < n),$$
$$\rho x_n = 2n\sigma x_n = 2ns^2 = 2nr_n^2,$$

dlatego na mocy Wniosku 1 liczby x_i spełniają (4).

Uwaga 4. Dowód Wniosku 2 można również przeprowadzić bezpośrednio, wychodząc z wzorów T. Ordowskiego $s_i = x_0 + \ldots + x_n - nx_{i-1}$ $(1 \leqslant i \leqslant n)$. Trzeba wówczas przyjąć $\sigma = n^2x_n$.

Przykład. Dla $n = 3$ otrzymujemy wzory

$$\sigma x_0 = s_2^2 + s_2s_3 + s_3^2, \qquad \sigma x_1 = s_1^2 + s_1s_3 + s_3^2,$$
$$\sigma x_2 = s_1^2 + s_1s_2 + s_2^2, \qquad \sigma x_3 = (s_1 + s_2 + s_3)^2.$$

Literatura

[1] L. E. Dickson, *Introduction to the Theory of Numbers*, reprint Dover 1957, §§29–31 i 57–59;

[2] L. E. Dickson, *Modern Elementary Theory of Numbers*, reprint The Chicago University Press 1950, Chapter ix.

[3] C. Hooley, *On the Diophantine equation* $ax^2 + by^2 + cz^2 + 2fyz + 2gzx + 2hxy = 0$, Arch. Math. (Basel) 19 (1968), 472–478.

[4] C. L. Siegel, *Zur Theorie der quadratischen Formen*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II 1972, No. 3, 21–46.