Zasada lokalno-globalna

Doc. dr Kazimierz SZYMICZEK

Najpowszechniej znanym faktem matematycznym jest prawdopodobnie twierdzenie Pitagorasa o trójkącie prostokątnym. Z twierdzeniem tym związane jest stare zagadnienie poszukiwania trójkątów prostokątnych, których boki mają długości będące liczbami naturalnymi, a więc poszukiwanie rozwiązań równania

$$X^2+Y^2=Z^2 \tag{1}$$

w liczbach naturalnych X, Y, Z. Jak głosi legenda, jedno z takich rozwiązań, mianowicie $3^2+4^2=5^2$, służyło starożytnym Egipcjanom do praktycznego wyznaczania kąta prostego (używano do tego sznura z 13 węzłami w równych odległościach i ... trzech niewolników). Łatwo sprawdzić, że dla dowolnych liczb naturalnych m, n takich, że $m>n$, liczby naturalne $x=m^2-n^2$, $y=2mn$, $z=m^2+n^2$ spełniają równanie (1) (więc na przykład, dla $m=2$, $n=1$ otrzymujemy $x=3$, $y=4$, $z=5$). Mamy więc prosty sposób konstrukcji trójkątów pitagorejskich.

Równanie pitagorejskie (1) można także interpretować arytmetycznie: czy istnieją kwadraty liczb naturalnych, które można przedstawić w postaci sumy kwadratów dwóch liczb naturalnych? Przy takim sformułowaniu nasuwają się jednak od razu inne, podobne pytania. A więc, na przykład, podwojony kwadrat jest oczywiście sumą dwóch kwadratów $2Z^2=Z^2+Z^2$, ale czy prócz tego trywialnego rozkładu istnieją jeszcze inne, postaci

$$X^2+Y^2=2Z^2, \quad X\neq Y? \tag{2}$$

Tutaj także istnieje sposób skonstruowania całej serii rozwiązań. Jeśli mamy jedno rozwiązanie $x^2+y^2=2z^2$ oraz jakiekolwiek rozwiązanie równania pitagorejskiego $a^2+b^2=c^2$, to $(ax-by)^2+(ay+bx)^2=(a^2+b^2)(x^2+y^2)=2(cz)^2$, a więc dostajemy nowe rozwiązanie równania (2); na przykład, z trywialnego rozwiązania $x=y=z=1$ równania (2) oraz „egipskiego" rozwiązania równania (1) $a=4$, $b=3$, $c=5$ otrzymujemy $1^2+7^2=2\cdot 5^2$.

Jako następny przykład rozpatrzmy potrojony kwadrat liczby naturalnej Z i zapytajmy, czy taka liczba może być sumą dwóch kwadratów liczb naturalnych? Okazuje się, że nie! Mianowicie równanie

$$X^2+Y^2=3Z^2 \tag{3}$$

nie ma rozwiązań w liczbach naturalnych. Przypuśćmy bowiem, że równanie (3) ma rozwiązania w liczbach naturalnych i spośród wszystkich takich rozwiązań x, y, z wybierzmy to, w którym z jest najmniejsze.

Wtedy liczby x, y nie mogą być obie parzyste, gdyż jeśli $x=2u$, $y=2v$ to $3z^2=x^2+y^2=4(u^2+v^2)$, zatem także z jest parzyste, $z=2w$. Dzieląc teraz równość $x^2+y^2=3z^2$ stronami przez 4 otrzymujemy $u^2+v^2=3w^2$ a więc rozwiązanie równania (3), przy czym $w<z$ wbrew wyborowi rozwiązania x, y, z. A więc przynajmniej jedna z liczb x, y jest nieparzysta. Zauważmy teraz, że $(2a+1)^2=4(a^2+a)+1$, to zaś znaczy, że kwadrat liczby nieparzystej daje przy dzieleniu przez 4 resztę 1. Używając kongruencji zapisujemy ten fakt następująco: $(2a+1)^2\equiv 1 \pmod 4$. Podobnie $(2a)^2\equiv 0 \pmod 4$; kwadrat liczby parzystej dzieli się przez 4. Wracając do naszego rozwiązania równania (3), mamy $x^2+y^2\equiv 1 \pmod 4$, jeśli jedna z liczb x, y jest parzysta, oraz $x^2+y^2\equiv 2 \pmod 4$, jeśli obie liczby x, y są nieparzyste. Z drugiej strony, $z^2\equiv 0 \pmod 4$ lub $z^2\equiv 1 \pmod 4$, a więc $3z^2\equiv 0 \pmod 4$ lub $3z^2\equiv 3 \pmod 4$. Tak więc równość $x^2+y^2=3z^2$ jest wykluczona: reszty z dzielenia lewej i prawej strony przez 4 są różne! Udowodniliśmy więc, że równanie (3) nie ma rozwiązań w liczbach naturalnych.

Ten negatywny rezultat nie powinien nas zniechęcać do badania następnych równań tego typu; ostatecznie fakt, że równanie nie ma rozwiązań jest przecież faktem interesującym.

Równaniem $X^2+Y^2=4Z^2$ nie będziemy się zajmować, gdyż wobec $4Z^2=(2Z)^2$ równanie to sprowadza się właściwie do równania pitagorejskiego. Natomiast równanie $X^2+Y^2=5Z^2$ znowu ma całą serię rozwiązań w liczbach naturalnych, można tutaj bowiem użyć metody, którą wykorzystaliśmy do badania równania (2): jeśli $x^2+y^2=5z^2$ oraz $a^2+b^2=c^2$, to $(ax-by)^2+(ay+bx)^2=5(cz)^2$. A więc równość $1^2+2^2=5\cdot 1^2$ wraz z egipskim trójkątem $a=4$, $b=3$, $c=5$ daje $2^2+11^2=5\cdot 5^2$.

Dwa następne równania $X^2+Y^2=6Z^2$ oraz $X^2+Y^2=7Z^2$ znowu okazują się nierozwiązalne w liczbach naturalnych. Można to udowodnić podobnie jak w przypadku równania (3), z tym, że w przypadku równania $X^2+Y^2=6Z^2$ należy wziąć reszty z dzielenia przez 3 a nie przez 4.

Po rozpatrzeniu tych przykładów nasuwa się nieodparcie pytanie: jak stwierdzić, czy dla danej liczby naturalnej n równanie

$$X^2+Y^2=nZ^2 \tag{n}$$

ma rozwiązanie w liczbach naturalnych X, Y, Z?

Najpierw zauważmy, że równanie (n) wystarczy rozpatrywać dla liczb naturalnych n bezkwadratowych, to znaczy takich liczb n, które nie są podzielne przez kwadrat żadnej liczby naturalnej $k>1$. Rzeczywiście, niech $n=mk^2$. Jeśli x, y, z jest rozwiązaniem równania (n), to x, y, kz jest rozwiązaniem równania (m); na odwrót, jeśli x, y, z spełniają równanie (m), to kx, ky, z spełniają równanie (n).

Pełną odpowiedź na nasze pytanie dotyczące rozwiązalności równania (n) w liczbach naturalnych zawiera następujące twierdzenie, będące pewnym szczególnym przypadkiem zasady lokalno-globalnej.

Twierdzenie. *Niech n będzie bezkwadratową liczbą naturalną. Na to, aby równanie (n) miało rozwiązanie w liczbach naturalnych potrzeba i wystarcza, by istniały liczby naturalne x, y, z takie, że*

(W) $$x^2+y^2 \equiv nz^2 \pmod{n} \quad \text{i} \quad NWD(x,n)=1.$$

Dowód. Przypuśćmy najpierw, że równanie (n) ma rozwiązanie w liczbach naturalnych X, Y, Z. Niech $d = NWD(X, Y, Z)$; zatem liczby $x = X/d$, $y = Y/d$, $z = Z/d$ są względnie pierwsze, oraz $x^2+y^2 = nz^2$. Tutaj już $\mathrm{NWD}(x, n) = 1$. Rzeczywiście, jeśli liczba pierwsza p dzieli x i dzieli n, to p dzieli $x^2-nz^2 = y^2$, a więc p dzieli y. W takim razie p^2 dzieli $x^2+y^2 = nz^2$, a ponieważ n jest liczbą bezkwadratową, wnioskujemy stąd, że p dzieli z. A więc wspólny dzielnik pierwszy p liczb x, n jest wspólnym dzielnikiem liczb x, y, z, wbrew temu, że są one względnie pierwsze. A więc $\mathrm{NWD}(x, n) = 1$. Ponieważ liczby x^2+y^2 i nz^2 są równe, więc mają równe reszty z dzielenia przez n. Zatem $x^2+y^2 \equiv nz^2 \pmod{n}$ oraz $\mathrm{NWD}(x, n) = 1$. Warunek konieczny rozwiązalności równania (n) został więc udowodniony.

Dowód dostateczności warunku poprowadzimy niewprost. Przypuśćmy, że istnieją liczby naturalne n spełniające warunek (W) takie, że równanie (n) nie ma rozwiązań w liczbach naturalnych.
Wybierzmy najmniejszą liczbę naturalną n o tej własności i niech x, y, z będą liczbami spełniającymi warunek (W). Ponieważ x^2+y^2 jest równe nz^2, więc dzieli się przez n. Mamy zatem $x^2+y^2 = kn$. Obieramy przy tym liczby x, y tak, by k było możliwie najmniejsze.

Pokażemy najpierw, że wtedy $k \leqslant \frac{1}{2}n$. Rzeczywiście, można od razu zakładać, że $0 < x < n$, $0 < y < n$, gdyż wraz z liczbami x, y warunek (W) spełniają reszty z dzielenia x, y przez n.

Gdy $\frac{1}{2}n < x < n$, to zastępujemy x przez $n-x$; mamy wtedy $\mathrm{NWD}(n-x, n) =$
$= \mathrm{NWD}(x, n) = 1$ oraz $(n-x)^2+y^2 = x^2+y^2+n^2-2nx = kn+n^2-2nx = (k+n-2x)n$,
a więc $n-x$, y także spełniają (W) z tym, że teraz $0 < n-x < \frac{1}{2}n$. Podobnie można postąpić w przypadku, gdyby $\frac{1}{2}n < y < n$. A więc można zakładać, że $0 < x \leqslant \frac{1}{2}n$, $0 < y \leqslant \frac{1}{2}n$,
zatem $kn = x^2+y^2 \leqslant \frac{1}{4}n^2+\frac{1}{4}n^2 = \frac{1}{2}n^2$, skąd $k \leqslant \frac{1}{2}n$. Pokażemy teraz jeszcze, że $\mathrm{NWD}(x, k) = 1$. Rzeczywiście, gdy pewna liczba pierwsza p dzieliła x i k, to z równości $x^2+y^2 = kn$ wynikałoby, że p dzieli y, skąd z kolei wynika, że p^2 dzieli $x^2+y^2 = kn$. Ale p nie dzieli n, gdyż p dzieli x i $\mathrm{NWD}(x, n) = 1$; zatem p^2 dzieli k i w rezultacie $(x/p)^2+(y/p)^2 = (k/p^2)n$ oraz $k/p^2 < k$, wbrew wyborowi liczby k. A więc liczby x, k nie mają wspólnego dzielnika > 1. Teraz możemy stwierdzić, że liczba k spełnia warunek (W) — po zastąpieniu w nim n przez k. Istotnie, $x^2+y^2 = kn \equiv 0 \equiv k \cdot 1^2 \pmod{k}$ oraz $\mathrm{NWD}(x, k) = 1$. Ponadto wiemy, że $k < n$. Zatem zgodnie z wyborem liczby n jako najmniejszej liczby naturalnej, dla której spełnienie warunku (W) nie pociąga rozwiązalności równania (n), możemy stwierdzić, że równanie (k) jest rozwiązalne w liczbach naturalnych! Zatem istnieją liczby naturalne a, b, c takie, że $a^2+b^2 = kc^2$. Mamy więc $(ax-by)^2+(ay+bx)^2 = (a^2+b^2)(x^2+y^2) =$
$= kc^2 \cdot kn = n(kc)^2$, to znaczy, liczby $X = |ax-by|$, $Y = ay+bx$, $Z = kc$ są rozwiązaniem równania (n). Jest to rozwiązanie równania (n) w liczbach naturalnych: nie ma bowiem wątpliwości, że Y i Z są liczbami naturalnymi, zaś $X \neq 0$, gdyż w przeciwnym razie $Y^2 = nZ^2$, wbrew temu, że n jest liczbą bezkwadratową. A więc nasze przypuszczenie, że istnieją takie liczby bezkwadratowe n, które spełniają (W), ale dla których równanie (n) jest nierozwiązalne w liczbach naturalnych, prowadzi do sprzeczności. Twierdzenie jest zatem w zupełności udowodnione.

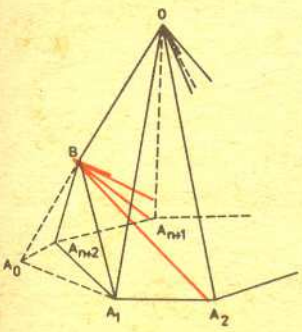
Praktyczne stosowanie naszego twierdzenia może być uciążliwe dla dużych n, dlatego warto zwrócić uwagę na następujące uproszczenia. Liczbę bezkwadratową n zapiszemy jako iloczyn (różnych!) liczb pierwszych: $n = p_1 \cdot \ldots \cdot p_s$. Okazuje się, że równanie (n) ma rozwiązanie w liczbach naturalnych wtedy i tylko wtedy, gdy każde z równań (p_i), $i = 1, \ldots, s$, ma rozwiązanie w liczbach naturalnych. Jeśli bowiem równanie (n) jest rozwiązalne, to spełniony jest warunek (W); biorąc reszty z dzielenia liczb x, y przez p_i otrzymamy liczby x_i, y_i takie, że $x_i^2+y_i^2 \equiv 0 \pmod{p_i}$ oraz $\mathrm{NWD}(x_i, p_i) = 1$. Zatem z naszego twierdzenia wynika, że równanie (p_i) jest rozwiązalne w liczbach naturalnych. Na odwrót, jeśli $x_i^2+y_i^2 = p_i z_i^2$, $i = 1, \ldots, s$, to wykorzystując tożsamość

$$(A^2+B^2)(X^2+Y^2) = (AX-BY)^2+(AY+BX)^2$$

stwierdzamy, że istnieją liczby naturalne x, y takie, że

$$x^2+y^2 = (x_1^2+y_1^2)\cdot \ldots \cdot (x_s^2+y_s^2) = n(z_1 \cdot \ldots \cdot z_s)^2,$$

Rozwiązanie zadania **M 219.** Na krawędzi OA_0 ostrosłupa o wierzchołku O i podstawie wypukłej $A_0A_1 \ldots A_{n+2}$ obierzmy punkt B. Szukanym wielościanem jest wielościan o ścianach A_1BA_{n+2}, A_1BO, $OA_1A_2, \ldots, \ldots, OA_nA_{n+1}$, $OA_{n+1}A_{n+2}$, $OA_{n+2}B$ i $A_1A_2 \ldots A_{n+2}$, a jego przekątnymi — odcinki $BA_2, \ldots, BA_{n+1}$.



to znaczy, równanie (n) ma rozwiązanie w liczbach naturalnych. A więc nasze twierdzenie można także sformułować następująco: Jeśli n jest bezkwadratową liczbą naturalną, to równanie (n) ma rozwiązanie w liczbach naturalnych wtedy i tylko wtedy, gdy dla każdej liczby pierwszej p dzielącej n kongruencja $X^2+Y^2 = nZ^2 \pmod p$ ma rozwiązanie w liczbach naturalnych x, y, z takie, że p nie dzieli x.

Na przykład równanie $X^2+Y^2 = 303Z^2$ nie jest rozwiązalne w liczbach naturalnych, bo $303 = 3 \cdot 101$ i równanie $X^2+Y^2 = 3Z^2$ nie ma rozwiązań w liczbach naturalnych. Natomiast równanie $X^2+Y^2 = 221Z^2$ ma rozwiązanie w liczbach naturalnych, gdyż $221 = 13 \cdot 17$ i równania (13), (17) są rozwiązalne w liczbach naturalnych.

Równanie (n) jest dość szczególnym równaniem stopnia drugiego o trzech niewiadomych. Czy nasze twierdzenie nie ma przypadkiem jakiegoś odpowiednika dla równań ogólniejszej postaci niż (n)? Na przykład, weźmy równanie

$$(*) \qquad a_1X_1^2+ \ldots +a_rX_r^2 = 0$$

gdzie $a_1, \ldots, a_r$ są liczbami całkowitymi, $r > 1$. Jak rozpoznać, czy równanie $(*)$ ma rozwiązanie w liczbach naturalnych? Jeden warunek konieczny jest dość oczywisty: jeśli równanie $(*)$ ma rozwiązanie w liczbach naturalnych, to liczby $a_1, \ldots, a_r$ nie mogą być wszystkie dodatnie (bo wtedy dla każdych liczb naturalnych $x_1, \ldots, x_r$ mamy $a_1x_1^2+ \ldots +a_rx_r^2 > 0$) ani też nie mogą być wszystkie ujemne. Ale przykład równania (3): $X_1^2+X_2^2-3X_3^2 = 0$ pokazuje, że ten oczywisty warunek konieczny rozwiązalności równania $(*)$ nie jest warunkiem wystarczającym. Szukajmy więc dalszych warunków koniecznych rozwiązalności równania $(*)$ w liczbach naturalnych.

Jeśli równanie $(*)$ ma rozwiązanie w liczbach naturalnych, to istnieje też rozwiązanie tego równania w liczbach naturalnych względnie pierwszych, to znaczy takich, że $\mathrm{NWD}(x_1, \ldots, x_r) = 1$. Rzeczywiście, jeśli liczby naturalne $y_1, \ldots, y_r$ spełniają równanie $(*)$ oraz $d = \mathrm{NWD}(y_1, \ldots, y_r)$, to liczby $x_1 = y_1/d, \ldots, x_r = y_r/d$ spełniają nasze równanie i są względnie pierwsze. Wtedy też dla dowolnej liczby naturalnej m mamy

$$a_1x_1^2+ \ldots +a_rx_r^2 \equiv 0 \pmod m \quad \text{i} \quad \mathrm{NWD}(x_1, \ldots, x_r, m) = 1.$$

Mamy więc następne warunki konieczne rozwiązalności $(*)$: Jeśli równanie $(*)$ ma rozwiązanie w liczbach naturalnych, to dla każdej liczby naturalnej m kongruencja $a_1X_1^2+ \ldots +a_rX_r^2 \equiv 0 \pmod m$ ma rozwiązanie w liczbach naturalnych $x_1, \ldots, x_r$ takich, że $\mathrm{NWD}(x_1, \ldots, x_r, m) = 1$.

Podobnie można było postąpić i dla równania (3): $x^2+y^2 = 3z^2$. Jeżeli liczby względnie pierwsze x, y, z spełniają to równanie, to widzimy, że prawa strona jest zawsze podzielna przez 3. Przez rozważenie różnych reszt z dzielenia x i y przez 3 dochodzimy do wniosku, że x i y też muszą dzielić się przez 3. Wtedy x^2+y^2 dzieli się przez 9, więc z musi dzielić się przez 3 — co sprzeczne jest z naszym założeniem, że x, y, z są względnie pierwsze.

Jakkolwiek trywialne wydawałyby się zauważone przez nas warunki konieczne rozwiązalności równania $(*)$, nie należy ich lekceważyć i to przynajmniej z dwóch powodów. Po pierwsze pozwalają one czasem stwierdzić, że równanie postaci $(*)$ nie ma rozwiązania w liczbach naturalnych. Na przykład, równanie $X_1^2+X_2^2+3X_3^2 = 0$ a także równanie $X_1^2+X_2^2-3X_3^2 = 0$ nie mają rozwiązań w liczbach naturalnych i stwierdzamy to na podstawie naszych warunków koniecznych rozwiązalności równania $(*)$. Po drugie, mamy interesującą wiadomość dla Czytelnika: nasze warunki konieczne rozwiązalności równania $(*)$ są równocześnie warunkami wystarczającymi! Jest to właśnie słynne stwierdzenie znane jako *zasada lokalno — globalna Minkowskiego — Hassego*:

Równanie $a_1X_1^2+ \ldots +a_rX_r^2 = 0$, *gdzie* $a_1, \ldots, a_r$ *są liczbami całkowitymi, ma rozwiązanie w liczbach naturalnych wtedy i tylko wtedy, gdy spełnione są dwa następujące warunki*:

(*a*) *Liczby* $a_1, \ldots, a_r$ *nie są wszystkie dodatnie ani nie są wszystkie ujemne.*

(*b*) *Dla każdej liczby naturalnej* m *kongruencja* $a_1X_1^2+ \ldots +a_rX_r^2 \equiv 0 \pmod m$ *ma rozwiązanie w liczbach naturalnych* $x_1, \ldots, x_r$ *takich, że* $\mathrm{NWD}(x_1, \ldots, x_r, m) = 1$.

Twierdzenie to jest dość trudne do udowodnienia i nie zrobimy tu żadnego kroku w kierunku jego dowodu. Zauważymy tylko, że dla równania (n) udowodniliśmy zasadę lokalno — globalną, a nawet twierdzenie znacznie lepsze. Mianowicie, zgodnie z naszym twierdzeniem, dla rozwiązalności równania (n) w liczbach naturalnych wystarcza istnienie odpowiedniego rozwiązania jednej tylko kongruencji $X^2+Y^2-nZ^2 \equiv 0 \pmod m$, podczas gdy ogólna zasada lokalno — globalna wymaga istnienia rozwiązań nieskończenie wielu kongruencji $X^2+Y^2-nZ^2 \equiv 0 \pmod m$, dla $m = 1, 2, 3, \ldots$. Przy tej okazji wychodzi na jaw pewna zasadnicza wątpliwość. Czy zasadę lokalno — globalną można naprawdę wykorzystać dla stwierdzenia istnienia rozwiązania równania $(*)$ w liczbach naturalnych? Jak sprawdzić mianowicie, czy spełniony jest warunek (*b*)? Jak sprawdzić rozwiązalność nieskończenie wielu kongruencji występujących w tym warunku?

Okazuje się, że jest to zawsze możliwe i że można to zrobić w skończonej liczbie kroków. Więc przede wszystkim można dowieść, że warunek (*b*) jest spełniony wtedy i tylko wtedy, gdy dla każdej liczby pierwszej p równanie $(*)$ ma niezerowe rozwiązanie w ciele Q_p liczb p-adycznych. Dalej dowodzi się, że dla każdej liczby pierwszej $p > 2$, która nie dzieli żadnego ze współczynników $a_1, \ldots, a_r$, równanie $(*)$ ma niezerowe rozwiązanie w ciele Q_p. Zatem pozostaje do sprawdzenia rozwiązalność równania $(*)$ w ciałach Q_p dla skończenie wielu liczb pierwszych, mianowicie dla $p = 2$ oraz tych liczb pierwszych, które dzielą przynajmniej jeden ze współczynników $a_1, \ldots, a_r$. Istnieją zaś sposoby pozwalające dokonać takiego sprawdzenia w skończonej liczbie kroków.

O liczbach p-adycznych pisaliśmy w Delcie 9/1978, 8/1979 i zamierzamy też napisać w następnym numerze.