Twierdzenie Hilberta o nierozkładalności

Navid SAFAEI, Radosław ŻAK***

*Dyrektor oddziału Matematyka Olimpijska w Salam Schools Complex, Teheran, Iran
Instytut Matematyki i Informatyki, Bułgarska Akademia Nauk, Sofia
**Doktorant, Uniwersytet Oksfordzki

Teoria liczb jest jedną z dziedzin matematyki najchętniej pożyczających metody z innych obszarów. Jednym ze źródeł takich zapożyczeń jest analiza matematyczna. W ostatnich latach analityczna teoria liczb zyskała na popularności, nawet w kontekście olimpiad matematycznych: ciekawy wybór dostępnych metod przedstawił Tomasz Kobos w Δ^3_{16}. Jednak „obce" teorii liczb pojęcia granic, szeregów, zbieżności i pochodnych mogą nieco onieśmielać osoby rozpoczynające przygodę z tą dziedziną. Jedną z zalet twierdzenia Hilberta o nierozkładalności (w skrócie THN) jest to, że stanowi ono zrozumiałe, teorioliczbowe opakowanie dla głębokich rozważań z zakresu analizy czy też geometrii algebraicznej.

Przypomnijmy, że *wielomian dwóch zmiennych* $P(x,y)$ to skończona suma jednomianów, z których każdy ma postać $a_{ij}x^iy^j$. W dalszej części liczby a_{ij} będą całkowite; zbiór wszystkich takich wielomianów oznaczamy przez $\mathbb{Z}[x,y]$. Wśród przykładów mamy takie wielomiany, jak x^3-y^2, $x^2-2xy+2y^2$ czy $x^3-x^2y+y^4+1$. Innym przykładem jest y^3-2y+1, mimo że nie zawiera on zmiennej x, na co warto zwrócić uwagę. Mamy też odpowiednie pojęcie stopnia dla wielomianów dwóch zmiennych – z definicji, stopień jednomianu $a_{ij}x^iy^j$ to $i+j$, a *stopień wielomianu* to maksimum stopni jego jednomianów. Możemy też zdefiniować *stopień względem konkretnej zmiennej*: stopień $P(x,y)$ względem x to po prostu zwykły stopień, jeśli tylko zapomnimy, że y jest zmienną. Na przykład dla wielomianu $P(x,y)=x^3-x^2y^3+y^4+2$ mamy:

$$\deg P(x,y)=5,\quad \deg_x P(x,y)=3,\quad \deg_y P(x,y)=4.$$

Tak jak w przypadku jednej zmiennej, wielomian $P(x,y)$ nazywamy *rozkładalnym* – jeśli można go zapisać jako iloczyn $P_1(x,y)\cdot P_2(x,y)$ dwóch niestałych wielomianów, oraz *nierozkładalnym* – w przeciwnym przypadku. Znane narzędzie zwane lematem Gaussa implikuje, że jeśli $P(x,y)$ ma współczynniki całkowite i rozkłada się jako iloczyn $P_1(x,y)\cdot P_2(x,y)$ wielomianów o współczynnikach **wymiernych**, to możemy również znaleźć rozkład o współczynnikach **całkowitych**.

Podobnie jak dla liczb pierwszych i całkowitych, wielomiany nierozkładalne można traktować jako cegiełki, z których zbudowane są pozostałe wielomiany. Istotnie, każdy wielomian $P(x,y)$ można zapisać jako iloczyn $Q_1(x,y)^{\alpha_1}\cdot\ldots\cdot Q_k(x,y)^{\alpha_k}$, dla pewnych wielomianów nierozkładalnych $Q_1,\ldots,Q_k$ i pewnych dodatnich wykładników całkowitych α_i. Możemy teraz przedstawić tytułowe twierdzenie:

Zainteresowany Czytelnik może znaleźć dowód THN w artykule:
M. Villarino, W. Gasarch, K. Regan, *Hilbert's Proof of His Irreducibility Theorem*, Amer. Math. Monthly (2018), doi.org/10.1080/00029890.2018.1448181, arXiv:1611.06303.

Twierdzenie 1 (Hilbert)**.** *Niech $P(x,y)$ będzie wielomianem nierozkładalnym o współczynnikach całkowitych, zależnym od zmiennej x (tzn. $\deg_x P(x,y)>0$). Wtedy dla nieskończenie wielu liczb całkowitych t wielomian $f_t(y):=P(t,y)$ (jednej zmiennej) również jest nierozkładalny, a ponadto $\deg f_t=\deg_y P(t,y)$.*

Prosty przykład: $Q(x,y)=y^2-x$ jest nierozkładalny. Jeśli podstawimy $t=1$, to otrzymany wielomian $Q(1,y)=y^2-1$ rozłoży się jako $(y-1)(y+1)$. Jednak nietrudno zauważyć, że taki rozkład ma miejsce dokładnie wtedy, gdy t jest kwadratem – wystarczy więc wybrać dowolne t, które kwadratem nie jest, a otrzymamy wielomian nierozkładalny. Możemy pójść o krok dalej.

Stwierdzenie 2. *Załóżmy, że $R(x)$ jest takim wielomianem o współczynnikach całkowitych, że dla dowolnej liczby całkowitej t liczba $R(t)$ jest kwadratem. Wtedy istnieje wielomian $Q(x)$ o współczynnikach całkowitych spełniający tożsamość $R(x)=Q(x)^2$.*

Dowód. Rozważmy wielomian $P(x,y)=y^2-R(x)$ i przypuśćmy, że jest on nierozkładalny. Wtedy na mocy THN możemy znaleźć taką liczbę całkowitą t, że $P(t,y)$ jest nierozkładalny. Wiemy jednak, że $R(t)=a^2$ dla pewnego a, więc $P(t,y)=y^2-a^2=(y-a)(y+a)$ jest rozkładalny. Otrzymana sprzeczność oznacza, że $P(x,y)$ jest rozkładalny.

Możemy więc tak dobrać niestałe wielomiany P_1, P_2 o współczynnikach całkowitych, by $P(x,y) = P_1(x,y)P_2(x,y)$. Gdyby $\deg_y P_1 = 0$ (tzn. P_1 nie zawiera y), to P_1 zależałby tylko od x i musiałby dzielić współczynnik przy y^2 w $P(x,y)$. Ale ten współczynnik to 1, więc jest to niemożliwe. Jako jedyna możliwość pozostaje, że zarówno P_1, jak i P_2 są liniowe względem y (jako że $\deg_y P(x,y) = 2$). Wtedy jednak, analizując ponownie współczynnik wiodący, otrzymujemy postać $P_1(x,y) = y + Q_1(x)$, $P_2(x) = y + Q_2(x)$ dla pewnych wielomianów Q_1, Q_2 (współczynniki wiodące mnożą się do 1, a w razie potrzeby możemy oba nasze wielomiany domnożyć przez -1). Stąd

$$\begin{aligned} y^2 - R(x) = P(x,y) = P_1(x,y)P_2(x,y) &= (y + Q_1(x))(y + Q_2(x)) \\ &= y^2 + y(Q_1(x) + Q_2(x)) + Q_1(x)Q_2(x). \end{aligned}$$

Porównując współczynniki, dostajemy $Q_1(x) + Q_2(x) = 0$, a więc $R(x) = -Q_1(x)Q_2(x) = Q_1(x)^2$. □

Możemy udowodnić jeszcze mocniejsze sformułowanie. W tym celu jednak będziemy musieli się powołać na następujący niewinnie wyglądający fakt. Warto zaznaczyć, że nie jest wcale łatwy do wykazania; jeden z jego dowodów wykorzystuje twierdzenie Czebotariowa.

Twierdzenie 3. *Jeśli $f(x)$ jest wielomianem nierozkładalnym o współczynnikach całkowitych oraz $\deg f \geqslant 2$, to istnieje nieskończenie wiele liczb pierwszych p, które nie dzielą $f(t)$ dla dowolnej liczby całkowitej t.*

Pozostała część artykułu poświęcona jest dowodowi następującego twierdzenia:

Więcej o twierdzeniu 4 można przeczytać tutaj:
H. Davenport, D. Lewis, A. Schinzel, *Polynomials of certain special types*, Acta Arith. (1964), eudml.org/doc/207456.

Twierdzenie 4. *Niech $P(x,y) \in \mathbb{Z}[x,y]$ będzie wielomianem o następującej własności: dla dowolnego niestałego ciągu arytmetycznego $(a_n)_{n=-\infty}^{\infty}$ liczb całkowitych możemy znaleźć indeks $i \in \mathbb{Z}$ oraz liczbę całkowitą y, dla których $P(a_i, y) = 0$. Wówczas istnieje wielomian $R(x) \in \mathbb{Q}[x]$ spełniający tożsamość $P(x, R(x)) = 0$.*

Uogólnia to nasze stwierdzenie 2 na dwa sposoby. Po pierwsze, założenie nie musi już być spełnione dla wszystkich t, lecz jedynie dla wystarczająco wielu, by pokryć wszystkie możliwe ciągi arytmetyczne. Po drugie, w miejsce wielomianu y^2 możemy przyjąć jakikolwiek inny. Na końcu artykułu proponujemy Czytelnikowi zadanie, które ilustruje tę ostatnią obserwację.

Dowód twierdzenia 4. Zauważmy najpierw, że założenie o ciągach arytmetycznych tak naprawdę daje nam nieskończenie wiele indeksów i, dla których $P(a_i, y) = 0$ ma rozwiązanie y. Istotnie, na pewno możemy znaleźć jedno takie i, ale wtedy ciąg $a'_j := a_{i+1+2j}$ (zawierający nieparzyste wyrazy (a_n), gdy i jest parzyste, a parzyste wyrazy, gdy i jest nieparzyste) również jest arytmetyczny, a jednocześnie stanowi podciąg (a_n) niezawierający a_i. Korzystając z założenia, otrzymujemy w ten sposób nowy indeks, a następnie możemy tę procedurę powtarzać do woli.

Rozłóżmy $P(x,y)$ na iloczyn $Q_1(x,y) \cdot \ldots \cdot Q_k(x,y)$ nierozkładalnych wielomianów Q_j (niekoniecznie różnych). Jeśli któryś z czynników Q_j zależy wyłącznie od x, to możemy go pominąć, gdyż odpowiada jedynie za skończenie wiele wartości t, dla których $P(t,y) = 0$ ma rozwiązanie. Podobnie, gdy równanie $Q_j(x,y) = 0$ ma skończenie wiele rozwiązań (x,y) – w obu tych przypadkach wielomian $P' := P/Q_j$ spełnia zarówno założenia, jak i tezę twierdzenia dokładnie wtedy, gdy spełnia je wyjściowy wielomian P.

Możemy teraz użyć THN i znaleźć odpowiednie t_j $(j = 1, \ldots, k)$, dla których wielomiany $Q_j(t_j, y)$ są nierozkładalne, o tym samym stopniu względem y co $Q_j(x,y)$. Gdyby każdy z tych stopni wynosił 2 lub więcej, to z twierdzenia 3 otrzymalibyśmy liczby pierwsze spełniające $p_j \nmid Q_j(t_j, y)$ dla wszystkich j i y; możemy przy tym dobrać te liczby jako parami różne.

Chińskie twierdzenie o resztach pozwala nam teraz znaleźć rozwiązanie układu kongruencji $t \equiv t_j \pmod{p_j}$ dla $j = 1, \ldots, k$. Rozwiązanie to ma postać $t \equiv c \pmod{p_1 p_2 \ldots p_k}$ dla pewnego c; innymi słowy – zbiór rozwiązań tworzy

ciąg arytmetyczny $a_i = c + ip_1p_2 \dots p_k$. Wiemy, że dla pewnych i oraz y zachodzi $P(a_i, y) = 0$, a więc również $Q_j(a_i, y) = 0$ dla pewnego j. Z drugiej strony:

$$Q_j(a_i, y) \equiv Q_j(t_j, y) \not\equiv 0 \pmod{p_j},$$

więc otrzymujemy sprzeczność.

Stąd wniosek, że któryś czynnik Q_j jest liniowy względem y; bez straty ogólności niech będzie to Q_1. Możemy zapisać go w postaci $A(x)y + B(x)$ dla pewnych wielomianów A, B. Jak wspomnieliśmy, możemy przyjąć, że $Q_1(x, y) = 0$ ma nieskończenie wiele rozwiązań (x, y), zatem $A(x)$ dzieli $B(x)$ dla nieskończenie wielu wartości x. Ale to oznacza, że $A(x)$ dzieli $B(x)$ jako wielomian (żeby to zauważyć, można na przykład podzielić z resztą $B(x)$ przez $A(x)$). W konsekwencji $R(x) = -\frac{B(x)}{A(x)}$ jest wielomianem i ostatecznie $P(x, R(x)) = Q_1(x, R(x)) = 0$. □

Czytelnik Uważny spostrzeże, że w tezie twierdzenia 4 wielomian R ma jedynie współczynniki wymierne, a nie całkowite. Istotnie, na przykład dla $P(x, y) = x^2 + x - 2y$ dostaniemy $R(x) = \frac{x(x+1)}{2}$. Na koniec proponujemy więc zadanie ilustrujące, że w pewnych sytuacjach mimo wszystko R będzie miał współczynniki całkowite.

Zadanie. Załóżmy, że P, Q są dwoma wielomianami o współczynnikach całkowitych i o następującej własności: dla dowolnej liczby całkowitej n możemy znaleźć taką liczbę całkowitą m, że $P(n) = Q(m)$. Udowodnij, że wtedy istnieje wielomian $R(x)$ o współczynnikach wymiernych spełniający tożsamość $P(x) = Q(R(x))$. Jeśli ponadto wielomian $Q(\frac{x}{k})$ nie ma współczynników całkowitych dla żadnego $k \geqslant 2$, wykaż, że $R(x)$ ma współczynniki całkowite.

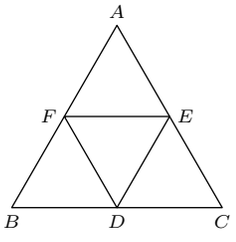
Policjanci i złodziej

*Alexandru BENESCU**

* Uczeń, Colegiul Național de Informatică Tudor Vianu, Rumunia

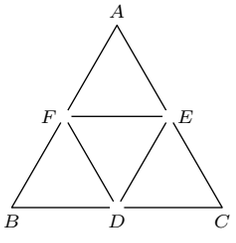
W tym artykule zajmiemy się następującym zagadnieniem.

Policjanci gonią złodzieja w pewnej wiosce, której uliczki tworzą trójkąt równoboczny wraz z jego środkowymi (rys. 1). Maksymalna prędkość złodzieja jest $\kappa > 0$ razy większa niż maksymalna prędkość policjantów. Zakładając, że wszyscy stale się widzą i ruch jest możliwy jedynie wzdłuż uliczek, należy określić, czy policjanci mogą schwytać złodzieja niezależnie od ich początkowego ustawienia.



Rys. 1

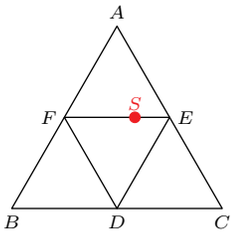
Rozpocznijmy rozwiązanie od analizy kilku prostych przypadków. Oznaczmy liczbę policjantów przez n. Załóżmy, że w wiosce znajduje się tylko jeden policjant, tj. $n = 1$. To banalny przypadek. Jeśli $\kappa < 1$ (tzn. złodziej jest wolniejszy od policjanta), policjant na pewno dościgne i schwyta złodzieja. Analogicznie, jeśli $\kappa \geqslant 1$, to złodziej może dowolnie długo uciekać przed policjantem, choćby biegając w cyklu $A \to B \to C \to A$ (rys. 1).



Rys. 2

Sytuacja zmienia się diametralnie (na korzyść wymiaru sprawiedliwości), gdy w pościgu bierze udział trzech (lub więcej) policjantów. Udowodnimy, że w tym przypadku schwytają oni złodzieja niezależnie od jego prędkości. Jedna ze strategii, które do tego doprowadzą, polega na jednoczesnym zajęciu punktów D, E i F (oznaczenia z rys. 1). W ten sposób policjanci podzielą całą wioskę na sześć spójnych części (składowych), jak pokazano na rysunku 2. W jednej z tych części znajduje się złodziej. Na jej krańcach (podobnie jak każdej innej części) znajdują się policjanci. Wystarczy, aby jeden z nich zaczął poruszać się (w ramach tej części) w stronę drugiego, a złodziej zostanie złapany.

Pozostaje rozważyć przypadek dwóch policjantów – ten jest bardziej wymagający. Udowodnimy najpierw, że dla $\kappa \leqslant 3$ policjanci zawsze złapią złodzieja. W tym celu jeden z policjantów będzie stale gonił rabusia – tego policjanta nazwiemy *gończym*. Jego jedynym zadaniem jest uniemożliwienie złodziejowi przyczajenia się na stałe w jednym miejscu. Dokładniej rzecz ujmując, musi on zadbać o to, by ostatnio odwiedzony przez złodzieja *punkt środkowy* zmieniał się w czasie (*punktami środkowymi* są punkty D, E lub F). Łatwo się przekonać, że aby to osiągnąć, wystarczy tylko jeden policjant.



Rys. 3

Drugi policjant, którego nazwiemy *stróżem*, ma bardziej subtelne zadanie. Najpierw musi udać się do „stróżówki” znajdującej się w punkcie S, który dzieli odcinek EF w stosunku $1:2$ (rys. 3). Kiedy już tam dotrze, musi uważnie obserwować poczynania złodzieja. Zadaniem tego policjanta jest odcinanie drogi ucieczki złodzieja, gdy tylko jest to możliwe. Na przykład, jeśli złodziej wejdzie do „górnego naroża” $E-A-F$ przez punkt E, stróż musi uniemożliwić mu ucieczkę przez punkt F. Ma taką możliwość, gdyż $\frac{|EA|+|AF|}{|SF|} = 3 \geqslant \kappa$. Jest też pewien mały haczyk – w tym samym momencie, w którym złodziej powróci do punktu E, stróż musi ponownie znaleźć się w punkcie S. Jest to jednak możliwe