Prace Koła Mat. Uniw. Ped. w Krak. 3 (2016), 13–23

Prace Koła Matematyków
Uniwersytetu Pedagogicznego w Krakowie (2016)

Jacek Dymel[1]

O zastosowaniach Combinatorial Nullstellensatz w pracy z olimpijczykami[2]

Streszczenie. Pretekstem do napisania artykułu jest zadanie z 48. Międzynarodowej Olimpiady Matematycznej z 2007 roku. Rozwiązanie tego zadania oparte jest na twierdzeniu *Combinatorial Nullstellensatz*, które udowodnił Noga Alon. W artykule zaprezentowano także inne problemy olimpijskie oraz znane twierdzenia, które można udowodnić z wykorzystaniem *Combinatorial Nullstellensatz*. Przedstawiono także rozważania nad zagadnieniem prezentowania uczniom współczesnych osiągnięć matematycznych.

Abstract. The inspiration for writing this article is one problem from the 48th International Mathematical Olympiad 2007. The solution is based on the theorem *Combinatorial Nullstellensatz* proved by Noga Alon. The article also presents other olympic problems and well-known theorems that can be proved applying *Combinatorial Nullstellensatz*. It also features the issue of familiarizing students with contemporary mathematical achievements.

Artykuł niniejszy jest adresowany zarówno do uczniów przygotowujących się do udziału w Olimpiadzie Matematycznej, jak i nauczycieli pracujących z uczniami uzdolnionymi matematycznie oraz studentów - przyszłych nauczycieli. Stąd wynika forma artykułu, a w szczególności dokładny opis dowodów twierdzeń i rozwiązań zadań.

Wśród sporej części uczestników Olimpiady Matematycznej matematyka jawi się jako zbiór zadań, do których trzeba dopasować odpowiednie algorytmy, twierdzenia, metody. Oczywiście, pojawiają się zadania, których nie można rozwiązać za pomocą typowych i mniej typowych metod, ale przeciętny olimpijczyk traktuje je jako błąd w systemie.

Wydaje się konieczne, aby pokazywać uczniom matematykę przez pryzmat twórczej pracy, jako żywą strukturę, która wyrasta z wiedzy, ale rozwija się poprzez

AMS (2010) Subject Classification: 97D50, 05E99.
Słowa kluczowe: Combinatorial Nullstellensatz, olimpiada matematyczna.

[2]Applications of Combinatorial Nullstellensatz while training Mathematical Olympiad competitors

tworzenie nowych problemów, podejmowanie prób ich rozwiązania, tworzenie nowych idei i metod.

Rzecz jasna, nie ma możliwości powrotu do sytuacji z początków istnienia olimpiad matematycznych, gdy o sukcesie decydował przede wszystkim talent. Ambitni uczestnicy współczesnych edycji olimpiad matematycznych mają świadomość istnienia obszernej wiedzy *olimpijskiej*, którą trzeba posiąść, jeżeli pragnie się odnieść sukces.

Międzynarodowa Olimpiada Matematyczna (International Mathematical Olympiad) jest najstarszą, przedmiotową olimpiadą międzynarodową. Po raz pierwszy odbyła się w 1959 roku w Braszowie w Rumunii. Brało w niej udział siedem państw: Bułgaria, Czechosłowacja, Niemiecka Republika Demokratyczna, Polska, Rumunia, Węgry, Związek Socjalistycznych Republik Radzieckich. Jak widać, początkowo były to zawody, w których uczestniczyli uczniowie z państw tzw. obozu socjalistycznego. W roku 2016 IMO odbędzie się w Hong Kongu, a udział wezmą reprezentacje 117 krajów.

Od swojego powstania zmieniła się nie tylko Olimpiada Matematyczna, ale także Międzynarodowa Olimpiada Matematyczna. Współcześnie na IMO szanse na najwyższe miejsca mają przede wszystkim uczniowie poddani gruntownemu treningowi. Bardzo dobrze pokazuje to przykład zadania z 48. Międzynarodowej Olimpiady Matematycznej z 2007 roku. Było to zadanie 6, które okazało się jednym z najtrudniejszych w historii IMO. Oto jego treść:

Zadanie 1 (zad 6 z 48. IMO)
Niech n będzie dodatnią liczbą naturalną. Przyjmijmy, że

$$S = \{(x, y, z) : x, y, z \in \{0, \dots, n\}, x + y + z > 0\}$$

jest zbiorem $(n+1)^3 - 1$ punktów w przestrzeni trójwymiarowej. Wyznacz najmniejszą możliwą liczbę płaszczyzn, których suma mnogościowa zawiera S, ale do której nie należy $(0, 0, 0)$.

Zadanie rozwiązało tylko pięciu zawodników: Konstantin Matwiejew z Rosji, Peter Scholze z Niemiec, Danylo Radczenko z Ukrainy, Iurie Boreico z Mołdawii i Pietro Verteci z Włoch. W zasadzie tylko znajomość twierdzenia *Combinatorial Nullstellensatz*, któremu poświęcony jest ten artykuł, umożliwiała szybkie rozwiązanie zadania. Noga Alon opublikował swój artykuł *Combinatorial Nullstellensatz* ([1]) w 1999 roku, a w 2007 roku kilku uczestników IMO już stosowało metodę w nim opisaną.

W numerze 145(1/1986) miesięcznika *Delta* pojawiła się krótka notka od redakcji:

W ubiegłorocznej (XXVI) Olimpiadzie Międzynarodowej miażdżący sukces odnieśli zespołowo Rumuni. Indywidualnie komplet punktów zdobyli Rumun i Węgier. Dopiero po pewnym odstępie pozostałe zespoły (w tym na „nastym" miejscu Polacy). Taki układ sił nikogo jednak nie zdziwił. Raz, że od kilku lat układ sił jest podobny. Dwa, że wiadomo dlaczego.

W Rumunii i na Węgrzech reprezentację olimpijską trenuje się długo i intensywnie. Nasi zaś zawodnicy to właściwie kompletni amatorzy. Całe przygotowanie reprezentacji to kilkunastodniowe zgrupowanie.

Na czym polega jednak trening? Chyba nie tylko na rozwiązywaniu zadań? Oczywiście rozwiązuje się zadania. Głównym jednak tematem treningu jest wyposażenie zawodników w zestaw „wytrychów" - elementarnych (mniej lub bardziej - ale tzw. szkolnych) twierdzeń „załatwiających" wiele technicznych kłopotów przy rozwiązywaniu zadań. I oczywiście wyćwiczenie rozpoznawania sytuacji, w których ten czy inny „wytrych" daje się zastosować.

Obecnie pogląd ten nie stracił na aktualności. W wielu krajach, oprócz specjalnych programów treningowych, opracowywane są pozycje książkowe i strony internetowe specjalnie dla uczestników IMO.

Przez ostatnie 40 lat sytuacja na IMO znacząco się zmieniła: już nie wystarczą "elementarne twierdzenia"; w obecnych czasach trzeba znać już nie tylko wiele mniej elementarnych twierdzeń, ale także współczesne wyniki nawiązujące charakterem do problemów olimpijskich.

Wniosek musi być taki: zawodnicy na najwyższym poziomie muszą być poddani specjalnemu treningowi, o ile chcą uzyskiwać wyniki na światowym poziomie. I nieodparte wrażenie jest takie, że właśnie przez pryzmat tego specyficznego treningu, opartego często na osiągnięciach współczesnych matematyków, pokazujemy wybitnym uczniom (a może powinniśmy pokazywać) obraz matematyki.

Przedstawmy zatem twierdzenie *Combinatorial Nullstellensatz*, które było kluczowe dla rozwiązania zadania 6 z 48. IMO.

Twierdzenie 2 (Combinatorial Nullstellensatz)
Niech $\mathbb{F}$ będzie ciałem oraz $P \in \mathbb{F}[x_1, \ldots, x_n]$ będzie niezerowym wielomianem stopnia $\sum_{i=1}^{n} m_i$, w którym współczynnik przy $x_1^{m_1} \cdots x_n^{m_n}$ jest różny od zera. Wówczas dla dowolnych zbiorów $S_1, \ldots, S_n \subset \mathbb{F}$ spełniających warunki $|S_i| > m_i$ dla $1 \leq i \leq n$, istnieją takie $c_i \in S_i$, że $P(c_1, \ldots, c_n) \neq 0$.

Uwaga 3
Combinatorial Nullstellensatz jest naturalnym uogólnieniem dobrze znanego uczniom twierdzenia, że wielomian jednej zmiennej stopnia n o współczynnikach rzeczywistych ma co najwyżej n pierwiastków rzeczywistych.

Dowód Combinatorial Nullstellensatz

Przeprowadzimy dowód indukcyjny, który można znaleźć w pracy [5]. Autorem pracy jest Mateusz Michałek, zdobywca srebrnego medalu na IMO w 2004 roku.

Przeprowadzimy dowód indukcyjny ze względu na stopień wielomianu $\deg P = k$.

Niech $\deg P = 1$. Bez straty ogólności można przyjąć, że $m_1 = 1$. Wielomian ma wówczas postać: $P(x_1, \ldots, x_n) = a_1x_1 + \cdots + a_nx_n + a_{n+1}$, gdzie $a_1, \ldots, a_{n+1} \in \mathbb{F}$ oraz $a_1 \neq 0$. Ponadto $|S_1| > 1, |S_2| \geq 1, \ldots, |S_n| \geq 1$.

Ponieważ $|S_1| > 1$, więc istnieją dwa elementy $(c_1, ..., c_n), (c_1', \ldots, c_n) \in S_1 \times \cdots \times S_n$, gdzie $c_1 \neq c_1'$.

Gdyby $P(c_1, \ldots, c_n) = 0$ oraz $P(c_1', c_2, \ldots, c_n) = 0$, to $a_1c_1 + \cdots + a_nc_n + a_{n+1} = 0$ oraz $a_1c_1' + a_2c_2 + \cdots + a_nc_n + a_{n+1} = 0$. A to oznacza, że $c_1 = c_1'$. Sprzeczność.

Załóżmy teraz, że $k > 1$ oraz, że teza zachodzi dla wszystkich wielomianów stopnia niższego niż k.

Niech wielomian P ma stopień k. Bez straty ogólności można przyjąć, że $m_1 > 0$. Jeżeli wielomian P potraktujemy jak wielomian zmiennej x_1 o współczynnikach z pierścienia $\mathbb{F}[x_2, \ldots, x_n]$, to w wyniku dzielenia wielomianu P przez wielomian $(x_1 - a)$, gdzie $a \in S_1$, otrzymamy

$$P = (x_1 - a)Q(x_1, \ldots, x_n) + R(x_2, \ldots, x_n),$$

gdzie $R(x_2, \ldots, x_n) = P(a, x_2, \ldots, x_n)$, Q musi zawierać nieznikający jednomian postaci $x_1^{m_1-1}x_2^{m_2}\cdots x_n^{m_n}$ oraz

$$\deg Q = \sum_{i=1}^{n} m_i - 1 = \deg(P) - 1.$$

Dla dowodu nie wprost załóżmy, że wielomian P nie spełnia tezy, to znaczy dla każdego elementu $(a_1, \ldots, a_n) \in S_1 \times \cdots \times S_n$: $P(a_1, \ldots, a_n) = 0$.

Dla dowolnego elementu $(a, a_2, \ldots, a_n) \in \{a\} \times S_2 \times \cdots \times S_n$ zachodzi równość $P(a, a_2, \ldots, a_n) = 0$, co oznacza, że także $R(a_2, \ldots, a_n) = 0$.

Weźmy zatem dowolny element $(a_1, \ldots, a_n) \in (S_1 \setminus \{a\}) \times S_2 \times \cdots \times S_n$. Otrzymujemy równości:

$$0 = P(a_1, \ldots, a_n) = (a_1 - a)Q(a_1, \ldots, a_n) + R(a_2, \ldots, a_n).$$

Ponieważ $(a_1 - a) \neq 0$ oraz $R(a_2, \ldots, a_n) = 0$, więc $Q(a_1, \ldots, a_n) = 0$. Wielomian Q ma stopień $k - 1$ i niezerowy współczynnik przy $x_1^{m_1-1}x_2^{m_2}\cdots x_n^{m_n}$ oraz przyjmuje wartość zero dla każdego elementu ze zbioru $(S_1 \setminus \{a\}) \times S_2 \times \cdots \times S_n$, co jest sprzeczne z założeniem indukcyjnym. Zatem istnieje taki element $(a_1, \ldots, a_n) \in S_1 \times \cdots \times S_n$, że $P(a_1, \ldots, a_n) \neq 0$. ∎

Twierdzenie *Combinatorial Nullstellensatz* należy do twierdzeń raczej rzadko spotykanych w zastosowaniach olimpijskich, a znajomość metody jego wykorzystania wynika z głębokiej wiedzy zawodników najwyższej klasy na temat zagadnień współczesnej matematyki.

Nieczęsto zdarza się, aby na olimpiadzie pojawiało się zadanie powiązane ze współczesnymi wynikami matematycznymi. W nauczaniu matematyki w ogóle rzadko pojawia sposobność do pokazania "żywej matematyki". W zasadzie tylko w przypadku kształcenia uczniów wybitnie uzdolnionych taka okazja może się pojawić.

Jak szybko przenika "żywa matematyka" do edukacji matematycznej najzdolniejszych? Wydaje się, że może to trwać od kilku do kilkunastu lat. Czy warto, aby takie treści pojawiały się w kształceniu najzdolniejszych? To pytanie jest silnie związane z pytaniem o cele konkursów takich jak olimpiady matematyczne. W mojej opinii zawody olimpiad matematycznych powinny być nastawione na wyławianie utalentowanych matematycznie uczniów, a zadania przedstawiane do rozwiązywania powinny wskazywać interesujące i warte poznania zagadnienia matematyczne, także te odkryte współcześnie. Zadania olimpijskie powinny raczej inspirować do poznania nowych, ciekawych obszarów matematyki. Zawody olimpijskie nie powinny być zwykłymi zawodami sportowymi, w których liczy się tylko doskonałość techniczna i to, kto zna więcej twierdzeń i tricków olimpijskich. W końcu przygotowujemy uczniów uzdolnionych do bycia twórczymi matematykami.

Należy pokazywać trudną, współczesną matematykę, ale nie jako wytrych do rozwiązywania zadań, ale jako pretekst do interesujących rozważań pokazujących szerszy kontekst matematyczny. Sam fakt, że takie wyniki jak *Combinatorial Nullstellensatz* są przydatne w rozwiązywaniu zadań, nie przemawia za tym, aby je pokazywać uczniom. Należy raczej wskazać na to, że metoda ta nie wymaga potężnego aparatu pojęciowego i pozostaje blisko intuicji oraz nauczania szkolnego. Bo *Combinatorial Nullstellensatz* w istocie jest twierdzeniem bardzo poglądowym i intuicyjnym, choć już jego stosowanie wymaga dużej wprawy.

Inną kwestią pozostaje problem dotarcia do współczesnych wyników, mających zastosowania w zadaniach olimpijskich. Zwiększył się (w stosunku do XX wieku) dostęp uczniów do wiedzy poprzez internet czy publikacje książkowe, ale tej wiedzy jest zbyt dużo, aby nawet świetny uczeń mógł dokonać selekcji. Skazany jest raczej na przypadkowe poszukiwania lub na przewodników. Od nas, nauczycieli (tych szkolnych i akademickich) zależy, jakimi będziemy przewodnikami i jaki obraz matematyki przedstawimy uczniom w czasie ich edukacji i poszukiwań. Bo warto pamiętać, że nie musimy uczyć tylko matematyki użytecznej, powinniśmy także pokazywać matematykę ładną.

Poniżej przedstawię kilka zastosowań *Combinatorial Nullstellensatz* do zadań olimpijskich, aby w końcu pokazać rozwiązanie zadania z IMO z 2007, które było pretekstem do opowiedzenia o tej metodzie.

Zadanie 4 (Rosja 2007)
W każdym wierzchołku wypukłego 100-kąta wpisano dwie liczby rzeczywiste. Udowodnić, że można z każdego wierzchołka usunąć po jednej liczbie w taki sposób, aby liczby w każdych dwóch sąsiednich wierzchołkach były różne.

Rozwiązanie (autor: Fedor Petrov)

Rozwiążemy zadanie ogólne:

W każdym wierzchołku wypukłego $2n$–kąta wpisano dwie liczby rzeczywiste. Udowodnić, że można z każdego wierzchołka usunąć po jednej liczbie w taki sposób, aby liczby w każdych dwóch sąsiednich wierzchołkach były różne.

Niech S_i $(i = 1, \ldots, 2n)$ oznacza dwuelementowy zbiór liczb umieszczonych w i–tym wierzchołku.

Określmy wielomian $P(x_1, \ldots, x_{2n}) = (x_1 - x_2)(x_2 - x_3)\cdots(x_{2n} - x_1)$. Wielomian P jest stopnia $2n$, współczynnik przy wyrażeniu $x_1 \cdots x_{2n}$, które jest stopnia $2n$, jest równy 2.

Na podstawie *Combinatorial Nullstellensatz* istnieje $(a_1, \ldots, a_{2n}) \in S_1 \times \cdots \times S_{2n}$, że $P(a_1, \ldots, a_{2n}) \neq 0$.

To oznacza, że każda z różnic: $(a_1 - a_2), (a_2 - a_3), \ldots, (a_{2n} - a_1)$ jest różna od 0, czyli istnieje taki wybór liczb ze zbiorów $S_1, \ldots, S_{2n}$, że

$$a_1 \neq a_2, a_2 \neq a_3, \ldots, a_{2n} \neq a_1. \qquad \blacksquare$$

Zadanie 5 (5th NIMO Winter Contest 2014)
Zdefiniujmy taką funkcję $\xi\colon \mathbb{Z}^2 \to \mathbb{Z}$, że $\xi(n,k) = 1$, gdy $n \leq k$ oraz $\xi(n,k) = -1$, gdy $n > k$ i zdefiniujmy wielomian

$$P(x_1, \ldots, x_{1000}) = \prod_{n=1}^{1000} \left(\sum_{k=1}^{1000} \xi(n,k) x_k \right).$$

(a) Wyznaczyć współczynnik przy $x_1 \cdots x_{1000}$ w wielomianie P.

(b) Wykazać, że jeżeli $a_1, \ldots, a_{1000} \in \{-1, 1\}$, to $P(a_1, \ldots, a_{1000}) = 0$.

Rozwiązanie. Najpierw wykażemy tezę z podpunktu (b).
Rozważmy 1000 różnych sum, które występują w $P(a_1, \ldots, a_{1000})$.
Zdefiniujmy je następująco:

$$T_n = -\sum_{k=1}^{n} a_k + \sum_{k=n+1}^{1000} a_k \text{ dla } n \in \{1, \ldots, 999\}$$

oraz

$$T_0 = a_1 + \cdots + a_{1000}.$$

Zauważmy, że $|T_n - T_{n+1}| = |2 \cdot a_{n+1}|$ i $a_{n+1} \in \{-1, 1\}$, więc $|2 \cdot a_{n+1}| = 2$.
Zatem dla każdej liczby $n \in \{0, \ldots, 998\}$ zachodzi równość $|T_n - T_{n+1}| = 2$. Zatem każda z sum $T_0, \ldots, T_{999}$ jest parzysta oraz $T_{999} = -T_0 + 2a_{1000}$.
Jeżeli $T_0 = 0$, to dowód został zakończony.
Załóżmy, że $T_0 \neq 0$. Bez straty ogólności przyjmijmy $T_0 > 0$, a zatem $T_0 \geq 2$. Zauważmy, że

$$T_{999} = -T_0 + 2a_{1000} \leq -2 + 2a_{1000}.$$

Ponieważ $a_{1000} \in \{-1, 1\}$, więc $T_{999} \leq 0$.
Gdyby $T_{999} = 0$, to kończyłoby to dowód.
Przyjmijmy więc, że $T_{999} < 0$. Ponieważ różnica pomiędzy dwoma kolejnymi sumami zawsze jest równa ± 2 oraz $T_0 > 0$, to co najmniej jedna z sum $T_1, \ldots, T_{998}$ jest równa 0.
(a) Zauważmy, że wielomian P jest stopnia 1000.
Załóżmy, że współczynnik przy $x_1 \cdots x_{1000}$ jest różny od 0.
Zdefiniujmy zbiory $S_1 = \cdots = S_{1000} = \{-1, 1\}$. Wówczas korzystając z *Combinatorial Nullstellensatz* otrzymujemy $c_i \in S_i$, gdzie $i \in \{1, \ldots, 1000\}$, że $P(c_1, \ldots, c_n) \neq 0$, co jest sprzeczne z tezą podpunktu (b).
Zatem współczynnik przy $x_1 \cdots x_{1000}$ jest równy 0. ■

Rozwiązania powyższych dwóch zadań pokazały zastosowania *Combinatorial Nullstellensatz* w prostych sytuacjach, ale głównie po to, by zaprezentować sposób stosowania metody.

Przejdziemy teraz do rozwiązania zadania 6 z IMO 2007, które jest problemem trudniejszym niż poprzednie zadania.

Zadanie 6 (zad. 6 z 48. IMO)
Niech n będzie dodatnią liczbą naturalną. Przyjmijmy, że

$$S = \{(x, y, z) : x, y, z \in \{0, \ldots, n\}, x + y + z > 0\}$$

jest zbiorem $(n+1)^3 - 1$ punktów w przestrzeni trójwymiarowej. Wyznacz najmniejszą możliwą liczbę płaszczyzn, których suma mnogościową zawiera S, ale do której nie należy $(0, 0, 0)$.

Rozwiązanie. Przedstawimy rozwiązanie zaproponowane przez Danylo Radchenko.

Niech $k \in \mathbb{N}_+$ i $k < 3n$. Weźmy k parami różnych płaszczyzn, których suma mnogościowa zawiera zbiór S i żadna z tych płaszczyzn nie przechodzi przez punkt $(0, 0, 0)$:

$$a_1x + b_1y + c_1z = d_1$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_kx + b_ky + c_kz = d_k,$$

gdzie $a_i^2 + b_i^2 + c_i^2 \neq 0$ oraz $d_i \neq 0$ dla $i \in \{1, \ldots, k\}$.

Niech wielomian P ma postać:

$$P(x, y, z) = \prod_{i=1}^{k} (a_ix + b_iy + c_iz - d_i) - \alpha \prod_{j=1}^{n} (x - j)(y - j)(z - j),$$

gdzie α jest tak dobrane, że $P(0, 0, 0) = 0$, czyli

$$\alpha = \frac{(-1)^{n-k} \prod_{i=1}^{k} d_i}{\prod_{j=1}^{n} j^3}.$$

Wielomian $P(x, y, z)$ przyjmuje wartość 0 dla każdego elementu należącego do zbioru S. Dla $k < 3n$ współczynnik przy $x^ny^nz^n$ nie jest równy 0, gdyż jest równy $\alpha \neq 0$.

Dla zbiorów $S_1 = S_2 = S_3 = \{0, \ldots, n\}$ zachodzą warunki: $|S_1| > n$, $|S_2| > n$, $|S_3| > n$, więc na podstawie *Combinatorial Nullstellensatz* istnieje taki punkt $(a, b, c) \in \{0, \ldots, n\}^3$, że $P(a, b, c) \neq 0$. Zatem istnieje punkt $(a, b, c) \in S$, dla którego $P(a, b, c) \neq 0$. Otrzymaliśmy sprzeczność. Wobec tego $k \geq 3n$.

Wystarczy jeszcze wskazać przykład $3n$ płaszczyzn, które spełniają warunki zadania. Są nimi na przykład:

$$x = 1, \ldots, x = n, y = 1, \ldots, y = n, z = 1, \ldots, z = n$$

■

Uwaga 7
Zadanie 6 z 48. IMO jest pewną wariacją na temat problemu, jaki postawił Peter Komjáth: ile potrzeba hiperpłaszczyzn, aby pokryć wszystkie, z wyjątkiem jednego, wierzchołki kostki jednostkowej w przestrzeni n–wymiarowej. Dowód tego problemu pojawił się przed 1993 rokiem, ale dopiero Noga Alon i Zoltan Füredi w 1993 roku w pracy [2] pokazali krótki dowód. Poniższy dowód pochodzi z pracy [1].

Twierdzenie 8
Niech $H_1, \ldots, H_m$ będzie rodziną hiperpłaszczyzn w $\mathbb{R}^n$, których suma zawiera wszystkie, z wyjątkiem jednego, wierzchołki kostki jednostkowej, czyli zbiór $\{0,1\}^n$. Wówczas $m \geq n$.

Dowód. Bez straty ogólności możemy przyjąć, że usuniętym wierzchołkiem jest punkt $(0, \ldots, 0)$.

Niech hiperpłaszczyzna H_i dana będzie równaniem $\langle a_i, x\rangle = b_i$, gdzie $x = (x_1, \ldots, x_n)$ oraz $\langle a, b\rangle$ jest iloczynem skalarnym a i b. Dla każdego $i \in \{1, \ldots, m\}$ zachodzi warunek $b_i \neq 0$, gdyż żadna z hiperpłaszczyzn nie przechodzi przez punkt $(0, \ldots, 0)$.

Załóżmy dla dowodu nie wprost, że $m < n$ i zdefiniujmy wielomian

$$P(x) = (-1)^{n+m+1} \prod_{j=1}^{m} b_j \prod_{i=1}^{n} (x_i - 1) + \prod_{i=1}^{m} [\langle a_i, x\rangle - b_i]$$

Wielomian P ma stopień n i współczynnik przy $x_1 \cdots x_n$, równy

$$(-1)^{n+m+1} \prod_{j=1}^{m} b_j,$$

jest różny od 0. Zatem na podstawie *Combinatorial Nullstellensatz* dla $m_1 = \cdots = m_n = 1$ oraz $S_1 = \cdots = S_n = \{0,1\}$, istnieje taki punkt $c \in \{0,1\}^n$, że $P(c) \neq 0$. Punkt c jest różny od $(0, \ldots, 0)$, gdyż wielomian P przyjmuje wartość 0 dla $x = (0, \ldots, 0)$, a zatem punkt c należy do zadanego zbioru i nie należy do żadnej z hiperpłaszczyzn. Otrzymaliśmy sprzeczność. Wobec tego $m \geq n$.

Teraz wystarczy wskazać hiperpłaszczyny spełniające warunki zadania: $x_1 = 1, \ldots, x_n = 1$. ■

Poniżej przedstawimy trzy klasyczne twierdzenia, których proste dowody są oparte na *Combinatorial Nullstellensatz.* Twierdzenia te są szczególnie bliskie zastosowaniom olimpijskim.

Twierdzenie 9 (Cauchy'ego–Davenporta)
Dla dowolnej liczby pierwszej p i dowolnych $A, B \subset \mathbb{Z}_p$ zachodzi nierówność:

$$|A + B| \geq \min\{p, |A| + |B| - 1\},$$

gdzie $A + B = \{a + b : a \in A, b \in B\}$.

Dowód. (Pochodzi z pracy [1])

Przypadek 1. Przyjmijmy, że $|A|+|B| > p$. Niech c będzie dowolnym elementem zbioru $\mathbb{Z}_p$. Zdefiniujmy dla elementu c zbiór $C = \{c - b : b \in B\}$. Zbiór C jest równoliczny ze zbiorem B, zatem $|A| + |C| > p$. To oznacza, że istnieje element wspólny zbiorów A i C. Niech elementem wspólnym będzie $a_0 \in A$ oraz $c - b_0 \in C$. Wówczas $a_0 = c - b_0$, czyli $a_0 + b_0 = c$. Wobec tego, że element c jest dowolnym elementem $\mathbb{Z}_p$, $A + B = \mathbb{Z}_p$.

Przypadek 2. Niech $|A|+|B| \leq p$. Dla dowodu nie wprost załóżmy, że $|A+B| \leq |A| + |B| - 2$. Wówczas w $\mathbb{Z}_p$ istnieje zbiór $C \supset A + B$ spełniający warunek $|C| = |A| + |B| - 2$.

Rozważmy wielomian

$$f(x,y) = \prod_{c \in C} (x + y - c)$$

należący do $\mathbb{Z}_p[x,y]$. Jego stopień jest równy $|A| + |B| - 2$, a współczynnik przy $x^{|A|-1}y^{|B|-1}$ jest przystający do $\binom{|A|+|B|-2}{|A|-1}$ modulo p. To wyrażenie nie jest równe zero, ponieważ $|A| + |B| \leq p$. Na podstawie *Combinatorial Nullstellensatz* istnieją takie elementy $a \in A, b \in B$, że $f(a,b) \neq 0$. To jest niemożliwe, gdyż $A + B \subset C$. Zatem $|A + B| \geq |A| + |B| - 1$.

■

TWIERDZENIE 10 (Erdösa–Heilbronna)
Dla dowolnej liczby pierwszej p i dowolnego zbioru $A \subset \mathbb{Z}_p$ zachodzi nierówność

$$|A \widetilde{+} A| \geq \min\{p, 2|A| - 3\},$$

gdzie $A \widetilde{+} B = \{a + b : a \in A, b \in B\, a \neq b\}$ dla $A, B \subset \mathbb{Z}_p$.

Dowód.

Przypadek 1. Niech $2|A| - 3 \geq p$. Wykażemy, że $A \widetilde{+} A = \mathbb{Z}_p$.

Wybierzmy dowolny element $m \in \mathbb{Z}_p$. Rozbijmy zbiór $\mathbb{Z}_p$ na pary elementów, których suma w $\mathbb{Z}_p$ jest równa m. Otrzymujemy $\frac{p-1}{2}$ par oraz jeden element, który tworzy parę sam ze sobą. Wobec założenia $|A| \geq \frac{p+3}{2}$, na podstawie zasady Dirichleta, do zbioru A należą dwa różne elementy jednej z par, a więc $m \in A \widetilde{+} A$, co należało dowieść.

Przypadek 2. Niech $2|A| - 3 < p$.

Wybierzmy dowolny element $a \in A$ i zdefiniujmy $B = A \backslash \{a\}$. Łatwo zauważyć, że $A \widetilde{+} B \subset A \widetilde{+} A$. Potrzeba jeszcze pokazać, że $|A \widetilde{+} B| \geq \min\{p, 2|A| - 3\}$.

Wykażemy, że w tym przypadku $|A \widetilde{+} B| \geq 2|A| - 3$.

Dla dowodu nie wprost przyjmiemy, że istnieje taki podzbiór $C \subset \mathbb{Z}_p$, że $|C| = 2|A| - 4$ oraz $A \widetilde{+} B \subset C$.

Rozważmy wielomian

$$f(x,y) = (x - y) \prod_{c \in C} (x + y - c)$$

należący do $\mathbb{Z}_p[x,y]$. Jest to wielomian stopnia $2|A| - 3$, a współczynnik przy $x^{|A|-1}y^{|A|-2}$ jest równy $\binom{2|A|-4}{|A|-2} - \binom{2|A|-4}{|A|-1} \neq 0$ w $\mathbb{Z}_p$, gdyż $2|A| - 4 < p$. Ponieważ zbiór A ma moc większą niż wykładnik x oraz $|B| = |A| - 1$, to z *Combinatorial Nullstellensatz* wynika, że istnieją takie elementy $a \in A, b \in B$, że $f(a,b) \neq 0$. Otrzymaliśmy sprzeczność z własnością $f(a,b) = 0$ dla dowolnych $a \in A, b \in B$. ■

Twierdzenie 11 (Erdösa–Ginzburga–Ziva)
Niech $n \in \mathbb{N}_+$. Wówczas wśród dowolnych $2n-1$ liczb całkowitych można wybrać n liczb, których suma jest podzielna przez n.

Dowód. (Na podstawie dowodu z pracy [6]) Najpierw pokażemy, że twierdzenie jest prawdziwe dla liczby pierwszej n. Oznaczmy $n = p$.

Niech $a_1, \ldots, a_{2p-1}$ będą danymi liczbami całkowitymi. Bez straty ogólności można założyć, że $0 \leq a_1 \leq \cdots \leq a_{2p-1} \leq p-1$, gdyż możemy rozważyć tylko reszty z dzielenia liczby $a_1, \ldots, a_{2p-1}$ przez n.

Rozważmy dwa przypadki.

Przypadek 1. Jeżeli $a_{i+p-1} = a_i$ dla pewnego $i \in \{1, \ldots, p\}$, to twierdzenie jest oczywiste: wybieramy liczby $a_i = a_{i+1} = \cdots = a_{i+p-1}$, których suma jest podzielna przez p.

Przypadek 2. Niech $a_{i+p-1} > a_i$ dla dowolnej liczby $i \in \{1, \ldots, p\}$. W tym przypadku rozważmy dwuelementowe zbiory

$$S_1 = \{a_1, a_p\}, S_2 = \{a_2, a_{p+1}\}, \ldots, S_{p-1} = \{a_{p-1}, a_{2p-2}\}$$

oraz zbiór jednoelementowy $S_p = \{a_{2p-1}\}$.

Zdefiniujmy wielomian

$$P(x_1, \ldots, x_p) = (x_1 + \cdots + x_p)^{p-1} - 1.$$

Wielomian P jest stopnia $p-1$ i współczynnik przy jednomianie $x_1 \cdots x_{p-1}$ jest równy $(p-1)!$. Nie jest on równy 0, gdyż na podstawie twierdzenia Wilsona $(p-1)! \equiv -1 \pmod{p}$.

Na podstawie *Combinatorial Nullstellensatz* istnieje taki element $(s_1, \ldots, s_p) \in S_1 \times \cdots \times S_p$, że $P(s_1, \ldots, s_p) \neq 0$.

Gdyby suma $s = s_1 + \cdots + s_p$ nie była podzielna przez p, to na podstawie Małego Twierdzenia Fermata p byłoby dzielnikiem $s^{p-1} - 1$, co nie jest prawdą, gdyż $P(s_1, \ldots, s_p) \neq 0$. Wobec tego suma $s = s_1 + \cdots + s_p$ jest podzielna przez p.

Teraz wykażemy, że twierdzenie jest prawdziwe dla dowolnej dodatniej liczby naturalnej n.

Każda liczba naturalna n posiada jednoznaczny rozkład, z dokładnością do kolejności, na iloczyn liczb pierwszych. Udowodniliśmy twierdzenie dla każdej liczby pierwszej. Zatem wystarczy wykazać, że twierdzenie jest prawdziwe dla dowolnego iloczynu liczb pierwszych. Wobec tego wystarczy wykazać, że jeżeli twierdzenie jest prawdziwe dla dwóch liczb naturalnych a i b, to jest prawdziwe dla ich iloczynu ab.

Załóżmy, że twierdzenie jest prawdziwe dla dwóch dodatnich liczb naturalnych a i b. Wykażemy, że jest także prawdziwe dla ich iloczynu ab.

Spośród $2ab-1$ liczb wybierzmy $2a-1$ liczb. Spośród nich można wybrać a liczb, których suma jest podzielna przez a. Zatem pozostaje $2ab - 1 - a$ liczb. Ponownie wybierzmy $2a-1$ spośród nich. Wśród nich jest a liczb, których suma jest podzielna przez a. Pozostaje $2ab - 1 - 2a$ liczb. Postępujemy analogicznie $2b-1$ razy. Zatem otrzymujemy $2b-1$ zbiorów, z których każdy ma a elementów, a suma w każdym z tych zbiorów jest podzielna przez a. Zatem potraktujmy sumę każdego z tych zbiorów jako jedną liczbę i podzielmy ją przez a. Otrzymujemy

$2b-1$ liczb, spośród których możemy wybrać b liczb, których suma jest podzielna przez b. Zatem uzyskaliśmy ab liczb, których suma jest podzielna przez ab, co kończy dowód. ■

Literatura

[1] N. Alon, *Combinatorial Nullstellensatz*. Combinatorics Probability and Computing nr 8(1999), str. 7–29, MR 1684621, Zbl 0920.05026.

[2] N. Alon, Z. Füredi, *Covering the cube by affine hyperplanes*, European Journal of Combinatorics nr 14(1993), str. 79–83, MR 1206612, Zbl 0773.52011.

[3] T. Andreescu, G. Dospinescu, *Problems from the book*, XYZ Press, 2008.

[4] T. Bartnicki, *Combinatorial Nullstellensatz, czyli o algebrze w kombinatoryce*, Matematyka Społeczeństwo Nauczanie, nr 38 (2007), str. 14–18.

[5] M. Michałek, *A short proof of Combinatorial Nullstellensatz*, American Mathematical Monthly nr 117(2010), str. 821–823, MR 2760383, Zbl 1215.13006.

[6] A. Neugebauer, *Matematyka olimpijska. Algebra i teoria liczb*, volumina.pl, Szczecin, 2011.

[1] *V LO im. Augusta Witkowskiego w Krakowie*
ul. Studencka 12, 31-116 Kraków
E-mail: jacek.dymel@gmail.com

Przysłano: 25.06.2016; publikacja on-line: 11.10.2016.