Combinatorial Nullstellensatz w teorii liczb

*Jacek DYMEL**

*nauczyciel, V Liceum Ogólnokształcące im. Augusta Witkowskiego w Krakowie

W *Delcie* 7/2017 przedstawiliśmy kilka „olimpijskich” zastosowań twierdzenia *Combinatorial Nullstellensatz*, które sformułowaliśmy następująco.

Twierdzenie (Combinatorial Nullstellensatz). *Niech $P(x_1, x_2, \ldots, x_n)$ będzie niezerowym wielomianem n zmiennych stopnia $\sum_{i=1}^{n} m_i$, w którym współczynnik przy $x_1^{m_1} \ldots x_n^{m_n}$ jest różny od zera. Wówczas dla dowolnych zbiorów $S_1, \ldots, S_n \subset \mathbb{R}$ spełniających warunki $|S_i| > m_i$ dla $1 \leqslant i \leqslant n$, istnieją takie $c_i \in S_i$, że $P(c_1, \ldots, c_n) \neq 0$.*

Okazuje się, że zamiast „zwykłych” wielomianów wielu zmiennych możemy rozważać wielomiany o współczynnikach będących resztami z dzielenia przez pewną liczbę pierwszą p, z dodawaniem i mnożeniem modulo p. Zbiór tych reszt wraz z tak określonymi operacjami oznaczać będziemy jako $\mathbb{Z}_p$. Dla $p = 5$ będziemy zatem mieli, na przykład,

$$3 \cdot 4 = 2, \ (3xy + 4x^2) + 2xy = -x^2, \ \text{ czy } (3x + y)(3x - y) = -x^2 - y^2.$$

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

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

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

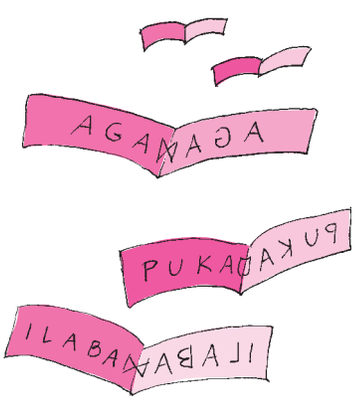
gdzie $A + B = \{a + b : a \in A, b \in B\}$.

Dowód. Przyjmijmy najpierw, 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 dowolności wyboru c otrzymujemy, że $A + B = \mathbb{Z}_p$.

Załóżmy teraz, że $|A| + |B| \leqslant p$. Dla dowodu nie wprost przypuśćmy, że $|A + B| \leqslant |A| + |B| - 2$. Wówczas w $\mathbb{Z}_p$ istnieje zbiór $C \supset A + B$ spełniający warunek $|C| = |A| + |B| - 2$. Rozważmy wielomian

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

o współczynnikach z $\mathbb{Z}_p$. 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 podzielne przez p, ponieważ $|A| + |B| \leqslant p$, jest zatem (modulo p) różne od 0. 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 $|A + B| \geqslant |A| + |B| - 1$. □



Twierdzenie (Erdősa–Heilbronna). *Dla dowolnej liczby pierwszej p i dla dowolnego zbioru $A \subset \mathbb{Z}_p$ zachodzi nierówność:*

$$|A \oplus A| \geqslant \min\{p, 2|A| - 3\},$$

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

Dowód. Dla $p = 2$ twierdzenie jest oczywiste. Załóżmy więc, że $p \geqslant 2$. Niech $2|A| - 3 \geqslant p$. Wykażemy, że $A \oplus A = \mathbb{Z}_p$. 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 $|A| \geqslant \frac{p+3}{2}$, na podstawie zasady Dirichleta, do zbioru A należą dwa różne elementy jednej z par, a więc $m \in A \oplus A$, co należało dowieść.

Niech teraz $2|A| - 3 < p$. Wybierzmy dowolny element $a \in A$ i zdefiniujmy $B = A \setminus \{a\}$. Łatwo zauważyć, że $A \oplus B \subset A \oplus A$. Potrzeba jeszcze pokazać, że $|A \oplus B| \geqslant \min\{p, 2|A| - 3\}$. Wykażemy, że w tym przypadku $|A \oplus B| \geqslant 2|A| - 3$. Dla dowodu nie wprost przyjmiemy, że istnieje taki podzbiór $C \subset \mathbb{Z}_p$, że

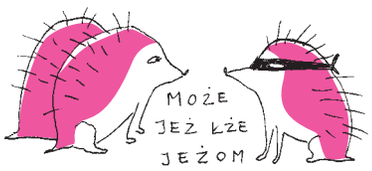
$|C| = 2|A| - 4$ oraz $A \oplus B \ \subset C$. Rozważmy wielomian

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

o współczynnikach z $\mathbb{Z}_p$. Jest to wielomian stopnia $2|A|-3$, a współczynnik przy $x^{|A|-1}y^{|A|-2}$ jest równy

$$\binom{2|A|-4}{|A|-2} - \binom{2|A|-4}{|A|-1} = \frac{(2|A|-4)!}{(|A|-2)!(|A|-1)!}$$

i jest różny od 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 (Erdősa–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. Najpierw wykażemy, że twierdzenie jest prawdziwe, jeśli n jest liczbą pierwszą; zgodnie z notacyjną tradycją przyjmijmy oznaczenie $p = n$. Niech $a_1, \ldots, a_{2p-1}$ będą danymi liczbami całkowitymi. Bez straty ogólności można założyć, że $0 \leqslant a_1 \leqslant \cdots \leqslant a_{2p-1} \leqslant p-1$, gdyż możemy rozważyć tylko reszty z dzielenia liczb $a_1, \ldots, a_{2p-1}$ 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

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

Wielomian P jest stopnia $p-1$ i współczynnik przy jednomianie $x_1 \cdot \ldots \cdot x_{p-1}$ 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 $(s_1, s_2, \ldots, s_p) \in S_1 \times S_2 \times \cdots \times S_p$, że $P(s_1, \ldots, s_p) \neq 0$. Gdyby suma $s = s_1 + \ldots + s_p$ 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 $s = s_1 + s_2 + \ldots + s_p$ jest podzielna przez p.

Teraz wykażemy, że twierdzenie jest prawdziwe dla dowolnej dodatniej liczby naturalnej n. Każda liczba naturalna n ma 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. Otrzymujemy w ten sposób $2b-1$ zbiorów, z których każdy zawiera a elementów, a suma tych elementów w każdym z tych zbiorów jest podzielna przez a. Potraktujmy sumę wybranych elementów 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 twierdzenia, jak również cały artykuł; Czytelnikom, którzy nawet teraz odczuwają niedosyt *Combinatorial Nullstellensatz*, polecam lekturę pozycji wymienionych na marginesie.

Literatura

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

[2] T. Bartnicki, *Combinatorial nullstellensatz, czyli o algebrze w kombinatoryce*, Matematyka Społeczeństwo Nauczanie, nr 38 (2007), str. 14–18. www.smp.uph.edu.pl/czasopismo/msn