WARTO BYĆ MŁODYM ...

ANDRZEJ ORLICKI, ANNA SZCZEPKOWSKA

Wydział Matematyki i Informatyki UWM w Olsztynie

Mamy nadzieję drogi Czytelniku, że posiadasz elementarne pojęcie o wielomianach (dowolnej ilości zmiennych i dowolnego stopnia). Interesować nas będą tylko wielomiany o współczynnikach całkowitych. Zapis $w(x_1, \ldots, x_n)$ będzie oznaczał wielomian o współczynnikach całkowitych od n zmiennych, oznaczanych przez $x_1, \ldots, x_n$. Tak więc

$$w(x_1, x_2, x_3) = x_1 x_3 + 4x_2 - 1$$

jest wielomianem od trzech zmiennych x_1, x_2, x_3, a jego stopień jest równy 2. Rozważmy wielomian $w(x_1, \ldots, x_n)$ i niech będą dane liczby całkowite $c_1, \ldots, c_n$. Przez $w(c_1, \ldots, c_n)$ będziemy oznaczać wartość tego wielomianu, gdy za zmienną x_1 podstawimy c_1, za zmienną x_2 liczbę c_2 itd. Dla podanego wyżej wielomianu w mamy np.

$$w(1, -1, 3) = 1 \cdot 3 + 4 \cdot (-1) - 1 = -2.$$

Definicja 1. *Powiemy, że wielomian $w(x_1, \ldots, x_n)$ posiada zero całkowite, jeżeli istnieją liczby całkowite $c_1, \ldots, c_n$ takie, że*

$$w(c_1, \ldots, c_n) = 0.$$

Zauważmy, że w przypadku wielomianów jednej zmiennej zamiast pojęcia "zero całkowite" używamy raczej sformułowania "pierwiastek całkowity". Rozważmy wielomian jednej zmiennej

$$w(x_1) = a_0 + a_1 x_1 + \ldots + a_n x_1^n,$$

gdzie stopień wielomianu $n \geq 1$ oraz $a_n \neq 0$. W szkole dowodzimy następujące twierdzenie:

Twierdzenie 1. *Jeśli liczba całkowita c jest zerem całkowitym (pierwiastkiem całkowitym) wielomianu w, to liczba c jest dzielnikiem wyrazu wolnego a_0.*

Tak więc potencjalne pierwiastki wielomianu

$$x_1^3 - x_1^2 + 7x_1 + 6$$

znajdują się wśród liczb całkowitych

$$1, -1, 2, -2, 3, -3, 6, -6.$$

Wystarczy teraz liczby te podstawić za zmienną x_1 i przekonać się, czy przy którymś z tych podstawień otrzymamy wartość zero. Z twierdzenia 1 otrzymujemy natychmiast następujący

Wniosek 1. *Istnieje algorytm, który dla dowolnego wielomianu jednej zmiennej o współczynnikach całkowitych rozstrzyga, czy wielomian ten posiada zero całkowite.*

Przejdźmy teraz do wielomianów innej postaci. Niech

$$w(x_1, \ldots, x_n) = a_1x_1 + \ldots + a_nx_n + b$$

(gdzie $n \geq 1$) będzie wielomianem n zmiennych o współczynnikach całkowitych stopnia 1. Załóżmy ponadto, że przynajmniej jeden spośród współczynników $a_1, \ldots, a_n$ jest różny od zera. Można udowodnić następujące

Twierdzenie 2. *Wielomian w posiada zera całkowite wtedy i tylko wtedy, gdy największy wspólny dzielnik współczynników $a_1, \ldots, a_n$ jest dzielnikiem liczby b.*

Rozważmy następujące dwa przykłady:

Przykład 1. *Niech $w(x_1, x_2, x_3, x_4) = 8x_1 - 6x_3 - 10x_4 + 16$. Największym wspólnym dzielnikiem liczb $8, 0, -6, -10$ jest 2, a ponieważ liczba 2 jest także dzielnikiem liczby 16, to możemy wnioskować, na mocy podanego wyżej twierdzenia, że wielomian w zera całkowite rzeczywiście posiada.*

Przykład 2. *Niech teraz $v(x_1, x_2, x_3) = -3x_1 + 12x_2 - 9x_3 + 4$. Największym wspólnym dzielnikiem liczb $-3, 12, -9$ jest liczba 3, ale nie jest ona dzielnikiem liczby 4. Stąd orzec już możemy, że podany wielomian zer całowitych po prostu nie posiada.*

Z twierdzenia 2 otrzymujemy natychmiast następujący wniosek

Wniosek 2. *Istnieje algorytm, który dla dowolnego wielomianu dowolnej ilości zmiennych stopnia 1 (o współczynnikach całkowitych) rozstrzyga, czy wielomian ten posiada zero całkowite.*

Sytuacje opisane we wnioskach 1 i 2 są dość szczególne. We wniosku 1 nie ograniczamy stopnia wielomianu, ale ograniczamy ilość jego zmiennych (do jednej). Z kolei we wniosku 2 ilość zmiennych jest zupełnie dowolna, ale restrykcja dotyczy stopnia wielomianu - musi to być wielomian stopnia 1. Matematycy bardzo lubią sytuacje ogólne. Dlatego też w 1900 roku sławny matematyk David Hilbert postawił następujący problem:

Czy istnieje algorytm, który dla dowolnego wielomianu dowolnej ilości zmiennych i dowolnego stopnia o współczynnikach całkowitych rozstrzyga, czy wielomian posiada zero całkowite?

Problem ten, zwany 10 - tym problemem Hilberta, okazał się bardzo trudnym. Dopiero w 1970 roku rosyjski matematyk Jurij Matiasewicz udowodnił, że stosownego algorytmu nie ma.

Metoda zastosowana przy rozwiązaniu 10 - tego problemu Hilberta dała pewien bardzo interesujący "efekt uboczny". Zanim przejdziemy do dalszych rozważań, przypomnijmy jeszcze tylko, że liczba naturalna p jest liczbą pierwszą, jeśli $p \geq 2$ oraz jedynymi naturalnymi dzielnikami p są 1 i p. Wypiszmy kilka początkowych liczb pierwszych: $2, 3, 5, 7, 11, 13$. Wiadomo, że wszystkich liczb pierwszych jest nieskończenie wiele (uważa się, że dowód tego faktu po raz pierwszy podał starożytny grecki matematyk Euklides). Liczby pierwsze od dawna fascynowały matematyków. W szczególności poszukiwano "wzorów", które dawałyby pewne liczby pierwsze. Znakomity matematyk Fermat (XVII wiek) rozważał liczby postaci

$$F_n = 2^{2^n} + 1,$$

gdzie $n = 0, 1, \ldots$. Dla liczb $n = 0, 1, 2, 3, 4$ liczby F_0, F_1, F_2, F_3 i F_4 są liczbami pierwszymi. Fermat miał nadzieję, że również liczby F_n dla $n \geq 5$ są pierwsze, ale tego nie sprawdził. Dopiero w 1772 roku Euler pokazał, że liczba F_5 jest podzielna przez 641, a więc nie jest liczbą pierwszą. Nadzieje na łatwy "wzorek" na liczby pierwsze upadły. A co z tym wszystkim ma wspólnego twierdzenie Matiasewicza? Otóż opierając się na tym twierdzeniu można udowodnić następujące

Twierdzenie 3. *Istnieje liczba naturalna $n \geq 1$ oraz wielomian $w(x_1, \ldots, x_n)$ o współczynnikach całkowitych o następującej własności: dla dowolnej liczby naturalnej p równoważne są następujące warunki:*
(1) p jest liczbą pierwszą;
(2) $p = w(m_1, \ldots, m_n)$ dla pewnych liczb naturalnych $m_1, \ldots, m_n$.

Tak więc wszystkie liczby pierwsze możemy otrzymać obliczając wartość wielomianu w na wszystkich możliwych naborach liczb naturalnych $m_1, \ldots, m_n$, dla których wartość ta jest liczbą naturalną. Twierdzenie 3 było dużym zaskoczeniem dla matematyków zajmujących się liczbami pierwszymi. Innym zaskoczeniem był fakt, że w 1970 roku Jurij Matiasewicz miał 22 lata i był studentem matematyki. Warto więc być młodym i studiować matematykę!