Zera funkcji kwadratowych

Arkadiusz MĘCEL[*]

Niejeden maturzysta marzy zapewne, żeby na egzaminie dojrzałości rozwiązywać następujące, z pozoru błahe, zadanie:

Zadanie 1. *Wyznacz liczbę miejsc zerowych funkcji* $f(x) = x^2 + 1$.

Abiturienta nie zraziłaby prawdopodobnie nawet drobna przeszkoda, jaką jest wyraźny brak informacji o dziedzinie funkcji f. Z uwagi na wszechobecność zbioru liczb rzeczywistych w obecnym programie nauczania wydaje się, że o żadnych zerach mowy być nie może. Nawet słynna „delta" nie jest tu potrzebna.

Tym, którzy z powodzeniem przejdą przez egzamin maturalny, przyjdzie, być może, zetknąć się z liczbami zespolonymi. Mają one tę własność, że wśród nich znajdują się pierwiastki nawet tak opornych funkcji, jak $f(z) = z^2 + 1$. Co więcej, każdy wielomian jednej zmiennej zespolonej o dowolnych współczynnikach (nie tylko całkowitych) ma pierwiastek zespolony. Dowód tego ważnego faktu, znanego powszechnie jako Zasadnicze Twierdzenie Algebry, młodzi adepci matematyki poznają w przynajmniej kilku odsłonach, nierzadko bardzo nieoczekiwanych.

Dowód Zasadniczego Twierdzenia Algebry przypisywany jest powszechnie Gaussowi. Rozumowanie Księcia Matematyków zawierało jednak subtelną lukę, wyeliminowaną dopiero na początku XX wieku. Autor pierwszego pełnego dowodu, paryski księgarz Jean-Robert Argand, zajmował się matematyką jedynie hobbystycznie...

Równanie $z^2 + 1 = 0$ ma dwa pierwiastki zespolone: i oraz $-i$. Liczba pierwiastków pokrywa się zatem ze stopniem wielomianu i nie jest to żaden przypadek. Zamieniając $x^2 + 1$ na dowolną inną funkcję kwadratową, nigdy nie dostaniemy więcej niż dwóch różnych miejsc zerowych. Co więcej, nie jest to fenomen dotyczący wyłącznie liczb zespolonych. Okazuje się, że ograniczenie nie powiększy się, o ile założymy przynajmniej tyle, że zarówno współczynniki, jak i dziedzina funkcji $f(x) = ax^2 + bx + c$ wyposażone są w dowolną strukturę określaną w algebrze mianem *ciała*. Jak się jednak okaże, „przynajmniej" nie zawsze znaczy „mało".

„Wolno dodawać" i „wolno mnożyć" oznacza, że jeśli a, b są elementami ciała, to są nimi także $a + b$ oraz $a \cdot b$.

Niepusty zbiór K nazwiemy ciałem, jeśli wolno w nim odpowiednio dodawać i mnożyć pary elementów. Działania te oznaczamy zwykle przez „+" oraz „$\cdot$". Co znaczy „odpowiednio"? Muszą być łączne i związane znanymi prawami rozdzielności. Każde ciało musi mieć zero, oznaczane przez „0", oraz jedynkę, oznaczaną przez „1". Są one elementami neutralnymi odpowiednio dodawania i mnożenia, a więc dodawanie zera i mnożenie przez jedynkę nie zmieniają elementu, który poddajemy tym operacjom. Każdy element musi mieć element przeciwny, a każdy poza zerem – element odwrotny. I rzecz dla nas kluczowa: działania „+" i „$\cdot$" mają być przemienne.

Działanie dwuargumentowe $\oplus$ jest przemienne, jeśli dla każdych $a, b \in X$ zachodzi równość

$$a \oplus b = b \oplus a.$$

Wspomnieliśmy już o liczbach rzeczywistych i zespolonych. Są to przykłady ciał nieskończonych. Tymczasem już na zbiorze dwuelementowym można wprowadzić strukturę ciała. Rozważmy zbiór $\{0, 1\}$. Przyjmijmy, że działania dodawania i mnożenia określone są zgodnie z następującymi tabelkami:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Nietrudno zidentyfikować powyższe reguły z działaniami na resztach z dzielenia przez 2. Czytelnik bez trudu sprawdzi, że powyższe warunki zadają na zbiorze $\{0, 1\}$ strukturę ciała dwuelementowego, oznaczanego zwykle przez $\mathbb{F}_2$. Skoro mamy ciało, możemy rozważać funkcje kwadratowe i wyznaczać miejsca zerowe. Spójrzmy na funkcję $f : \mathbb{F}_2 \to \mathbb{F}_2$ zadaną wzorem $f(x) = x^2 + 1$, której współczynniki należą przecież do $\mathbb{F}_2$. Podstawiając elementy dziedziny, dostajemy:

$$f(0) = 0^2 + 1 = 1, \qquad f(1) = 1^2 + 1 = 0.$$

Ogólnie, dla każdej liczby pierwszej p zbiór $\{0, 1, \ldots, p-1\}$ reszt z dzielenia przez p, wyposażony w działanie dodawania i mnożenia reszt, jest ciałem.

[*]doktorant, Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

Analogiczna struktura zadana na zbiorze reszt z dzielenia przez liczbę złożoną ciałem być nie może – zachęcamy Czytelnika do poszukiwania powodu.

A co z liczbami złożonymi? Czy umiemy wskazać takie n, że x^2+1 ma więcej niż dwa pierwiastki modulo n? Czy dla różnych n może ich być dowolnie (skończenie) wiele?

Co oznacza bycie pierwiastkiem wielomianu x^2+1 w ciele $\mathbb{F}_p$? Jest to, oczywiście, związane z podzielnością przez p. Jeśli rozważymy zbiór X liczb całkowitych, takich, które podniesione do kwadratu i powiększone o 1 są podzielne przez p, to elementy tego zbioru dają co najwyżej dwie różne reszty z dzielenia przez p. Które dwie? To już inna historia...

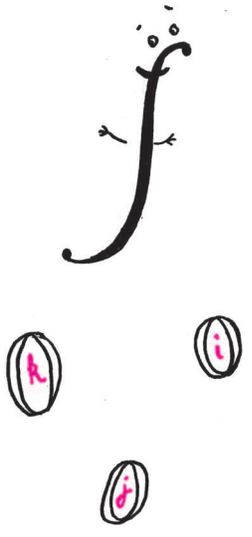
Postawmy jeszcze jedno pytanie. Czy funkcja $f(x)=x^2+1$ może mieć nieskończenie wiele miejsc zerowych? Odpowiedź brzmi: tak! Przykład dziedziny mającej tę własność jest tym bardziej zaskakujący, że znajduje się bardzo blisko ciał. Mowa tu bowiem o kwaternionach, uogólnieniu liczb zespolonych, których odkrycie, datowane na rok 1843, przypisuje się Hamiltonowi. Czym one są?

Historia odkrycia kwaternionów jest dobrze znana głównie z uwagi na dubliński most Brougham i formuły mnożenia, które w twórczym zachwycie wyrył tam sam Hamilton. Jakiż to wielki kontrast w porównaniu do wspomnianego już Gaussa, który, odkrywszy kwaterniony niemal ćwierć wieku wcześniej niż Hamilton, uznał je za obiekt niegodny publikacji...

Konstruując ciało liczb zespolonych, do zbioru liczb rzeczywistych dokładaliśmy tajemniczy element i, którego kwadrat był równy -1. Kwaterniony powstają na podobnej zasadzie, ale zamiast jednego elementu obcego rozważa się aż trzy. Nazwijmy je i, j, k. Każdy z nich, podobnie jak jednostka urojona, ma tę własność, że jego kwadrat to -1. Co więcej, iloczyn dowolnych dwóch równy jest trzeciemu (z dokładnością do znaku). Dokładniej,

$$ij=k, \quad jk=i, \quad ki=j, \quad ji=-k, \quad ik=-j, \quad kj=-i.$$

O ile dowolny element w ciele liczb zespolonych wyraża się jako $a+bi$, gdzie $a,b\in\mathbb{R}$, w przypadku kwaternionów dowolny element przedstawia się jako $a+bi+cj+dk$, gdzie a,b,c,d to dowolne liczby rzeczywiste. Kwaterniony można dodawać i mnożyć (stosując analogiczną metodę jak dla liczb zespolonych). Działania są łączne, zachowane są prawa rozdzielności. Znajdą się, rzecz jasna, zero i jedynka. Niemniej jednak kwaterniony nie są ciałem, a powód podaliśmy już na starcie. Pogwałcona została przemienność mnożenia. Istotnie, $ij=k$, ale $ji=-k$. Ta drobna (i jedyna!) różnica – brak przemienności mnożenia, który wyklucza kwaterniony z klasy ciał – ma poważne konsekwencje dla zliczania pierwiastków wielomianów.



Przyjrzyjmy się sprawie dokładniej. Funkcja $f(x)=x^2+1$ ma na pewno przynajmniej trzy kwaternionowe zera. Są to elementy i, j, k. Za dużo jak na ciało, ale wciąż za mało jak na „nieskończenie wiele". Podstawiajmy więc dalej:

$$f\left(\frac{i}{\sqrt{3}}+\frac{j}{\sqrt{3}}+\frac{k}{\sqrt{3}}\right)=\frac{i^2}{3}+\frac{j^2}{3}+\frac{k^2}{3}+\frac{ij}{3}+\frac{ik}{3}+\frac{jk}{3}+\frac{ji}{3}+\frac{ki}{3}+\frac{kj}{3}+1=$$
$$=\frac{-1-1-1+k-j+i-k+j-i}{3}+1=0.$$

Nie tylko otrzymaliśmy kolejne miejsce zerowe, lecz także złapaliśmy nieprzemienność kwaternionów na gorącym uczynku. Otrzymane zero to skutek reguły mnożenia elementów i, j, k. W podobny sposób możemy otrzymać coraz więcej pierwiastków. Dokładny rachunek pokazuje, że wśród kwaternionów postaci $a+bi+cj+dk$ funkcja x^2+1 zeruje się dokładnie na tych, w których współczynnik a równy jest 0 (tzw. kwaterniony czyste), a które leżą na sferze opisanej równaniem $b^2+c^2+d^2=1$.

Kwaterniony zaprowadziły nas zatem daleko od początkowych rozważań. Ale czy aby na pewno? Czy nie ma w tym żadnego podstępu? Pierwiastki przez nas wskazane, choć jest ich dużo, są bardzo podobne. Wiele z nich różni jedynie tzw. sprzężenie. Oznacza to, że jeśli utożsamilibyśmy wszystkie pary pierwiastków x, y, dla których istnieje kwaternion odwracalny u, taki, że spełniony jest warunek $x=u^{-1}yu$, to zostałyby nam dokładnie... dwa pierwiastki! I nie jest to przypadek, ale całkiem poważne twierdzenie i właściwość mająca analogię wśród wielomianów wyższych stopni. Ale o tym to już przy innej okazji...