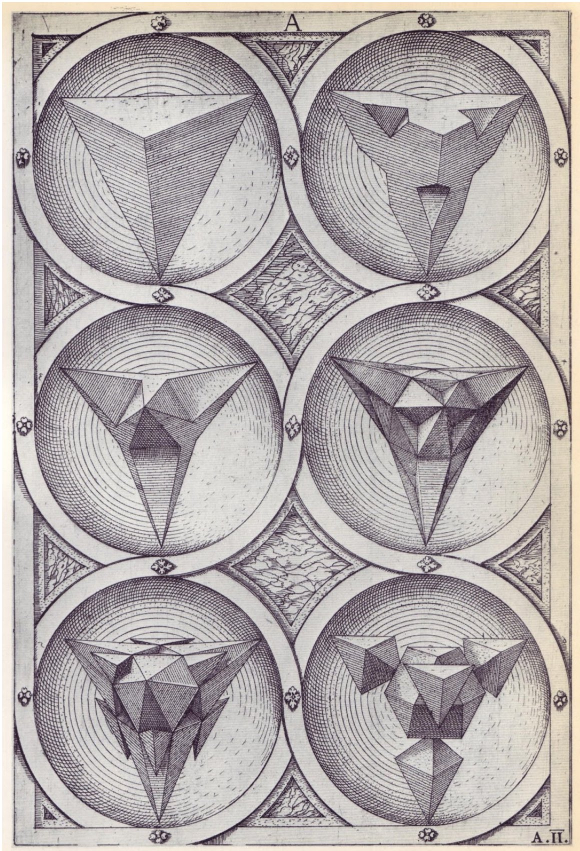
[MACIERZATOR56]

Gazetka redagowana przez Koło Naukowe Matematyków Uniwersytetu Śląskiego



Witamy w listopadowym numerze [MACIERZATORA]!

[Od Redakcji]

Miło nam przedstawić pierwszy od dłuższego czasu numer [MACIERZATORA]. Otwiera go recenzja *Bezmiaru matematycznej wyobraźni* – jednej z najlepszych polskich książek popularyzujących matematykę wyższą. W tym numerze można też przeczytać pierwszą część artykułu Marcina Jenczmyka *O metodach mnożenia wielomianów* oraz pierwszy z cyklu artykuł Mateusza Szymańskiego o zawiłości matematycznych rozumowań.

Początek roku akademickiego jest jednocześnie dla redakcji [MACIERZATORA] czasem zmian. Kiedy kilka lat temu rozpoczęliśmy pracę, dopiero kształtowała się jego postać. W ciągu pięciu lat z niszowej, nieregularnej gazetki udało nam się – dzięki pomocy i wsparciu wielu Życzliwych Osób – przekształcić go w bardziej profesjonalny, regularnie ukazujący się studencki miesięcznik matematyczny, posiadający własny numer ISSN. [MACIERZATOR] stał się grubszy i ładniejszy (LaTeX!). Wprowadziliśmy cykle artykułów (impresje olimpijskie, recenzje, Kącik TeXowy, biografie...), opowiadaliśmy o rezultatach nowych, a czasem nawet i pierwszych własnych wynikach naukowych członków Koła Naukowego Matematyków UŚ.

To dobry moment, by przekazać kierowanie [MACIERZATOREM] w ręce młodszych redaktorów, będących jeszcze studentami Uniwersytetu Śląskiego – bowiem ci, którzy mieli największy wkład w zmiany w naszym miesięczniku, zakończyli już studia. Miło nam ogłosić, że obowiązki redaktora naczelnego [MACIERZATORA] od tego numeru obejmuje wiceprzewodniczący ds. naukowych KNM UŚ, student III roku I stopnia, Mateusz Szymański. Mateuszowi życzymy tyle radości i satysfakcji w tworzeniu [MACIERZATORA], ile przez te lata było naszym udziałem.

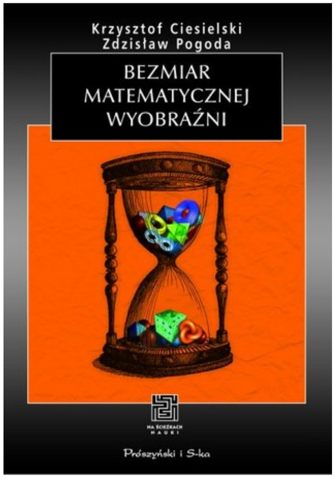
Redakcja

[Opowiedzieć matematykę]

Bezmiar matematycznej wyobraźni

Dotychczas w cyklu *Opowiedzieć matematykę* prezentowałam książki najnowsze, wydane w Polsce jeśli nie w kilku ostatnich miesiącach, to w kilku ostatnich latach. Tym razem jednak „wracam do moich źródeł" – chciałabym opowiedzieć o książce, wydanej po raz pierwszy w grudniu roku 1990.

Trudno jest wyważyć poziom trudności książki, mającej popularyzować matematykę; większość z nich jest prosta, czy wręcz upraszczana (niestety! wielu autorów nie wychodzi poza proste działania arytmetyczne i algebraiczne), albo odwrotnie: zbyt trudna dla czytelnika, który nie miał wcześniej kontaktu z matematyką wyższą. Tym bardziej cenię dar ciekawego i zrozumiałego dzielenia się wiedzą u Krzysztofa Ciesielskiego i Zdzisława Pogody – autorów pierwszej „poważniejszej” książki o matematyce, jaka trafiła w moje ręce. *Bezmiar matematycznej wyobraźni*, bo o nim mowa, to w mojej opinii jedna z najciekawszych i najlepszych pozycji popularyzujących naukę, z jaką kiedykolwiek się spotkałam.



Ale najpierw o książce. Podzielona jest na rozdziały, które tworzą samodzielne całości; lepiej czyta się ją w kolejności, ale można wybrać także losowo wybrany fragment i dalej czerpać radość z lektury. Autorzy z lekkością, znawstwem i dowcipem próbują odpowiedzieć na pytanie, czym jest matematyka, opowiadają o słynnych matematykach (i matematyczkach), a także o Medalu Fieldsa, najbardziej prestiżowej nagrodzie matematycznej. Pierwsze cztery rozdziały mówią bardziej o historii matematyki, a nie o niej samej – i dobrze; jest to lektura ciekawa dla tych, którzy mieli już kontakt z tą dziedziną nauki, ale i „oswajająca” dla osób, które nie wykraczają wiedzą matematyczną poza zakres wiedzy z poziomu szkoły średniej, a może nawet i gimnazjalnej. Rozdział piąty traktuje o dowodzie, a szósty to już matematyka w swej najczystszej postaci: *To i owo o topologii*, przy współudziale płaszczaków i plasteliny. Stąd łatwo autorzy przeszli do rozmaitości (sic!), geometrii, rozważań dotyczących wymiaru oraz fraktali. Dalej mówią też o abstrakcyjnej algebrze, topologii algebraicznej, hipotezie Poincarego i innych słynnych nierozwiązanych lub dopiero-co-rozwiązanych problemach matematycznych, elementach logiki i podstaw matematyki. Oczywiście, na próżno by szukać twierdzeń czy wręcz dowodów, ale nie o to przecież chodzi, a o intuicję; to też udało się autorom nadzwyczajnie.

Wielką zaletą książki jest ukazywanie matematyki przez pryzmat jej twórców. Podczas lektury spotykamy całą plejadę barwnych postaci. Są tu więc Riemann, Cauchy, Galois, Bourbaki, Abel, Goldbach, jest Brouwer i Fields... Autorzy sypią anegdotami z życia matematyków, umilają – i ułatwiają – lekturę całą rzeszą dowcipnych, arcytrafnych rysunków. Cieszy połączenie ogromnej wiedzy matematycznej autorów (obaj są pracownikami naukowo-dydaktycznymi Instytutu Matematyki UJ), ich erudycji i lekkości pisania. Są to zresztą cechy charakterystyczne i dla pozostałych ich książek:

Diamentów matematyki czy niedawno wydanej *Królowej bez Nobla*. Miłą jest dla mnie świadomość, że jedne z najlepszych książek popularyzujących matematykę piszą Polacy.

Bezmiar matematycznej wyobraźni dostałam w prezencie w gimnazjum. Do dziś pamiętam swoje wrażenie: *magia*. Książkę tę przeczytałam jednak z o wiele większą przyjemnością ponownie podczas studiów, gdy pojawiające się postaci i pojęcia były mi już znajome. O ile można polecić tę lekturę każdemu zainteresowanemu matematyką, o tyle wydaje mi się, że najtrafniejszymi jej odbiorcami będą wyróżniający się uczniowie szkół średnich, studenci czy absolwenci studiów matematycznych. To jednak żaden zarzut.

Autorzy podjęli się trudnego zadania i opowiadają niemal wyłącznie o matematyce współczesnej. To chyba najbardziej wyróżnia tę książkę spośród innych w tej tematyce, i to jest w niej szczególnie wartościowe. *Bezmiar...* cenię bardzo wysoko. Być może to i kwestia sentymentu, ale gdybym miała polecić jedną jedyną książkę traktującą o matematyce – chyba wybrałabym właśnie tę.

Joanna Zwierzyńska

[Niektóre sofizmaty matematyczne]

Część pierwsza

Tematem dzisiejszych rozważań są sofizmaty oraz inne błędy w rozumowaniach. Artykuł podzielony został na dwie części: w pierwszej zajmiemy się rzeczami elementarnymi, do których niewymagana jest głębsza znajomość aparatu matematycznego, w drugiej przeskoczymy na nieco wyższy poziom rozważań.

Warto byłoby przypomnieć w tym momencie, czym właściwe są sofizmaty – przytoczmy zatem definicję tego słowa[1]:

Definicja. **Sofizmat** – rozumowanie pozornie poprawne, ale w istocie zawierające rozmyślnie utajone błędy logiczne.

Część problemów jest ogólnie znana, część została zaczerpnięta z *Matematyki dla Ciekawych Świata* [1].

[1] Za `sjp.pwn.pl`.

1. Błędne intuicje

1.1. Piłeczka i ziemia

Pierwszy przykład nie będzie co prawda sofizmatem, ale skieruje nas po części na dzisiejszą problematykę.

Wyobraźmy sobie, iż obwiązujemy sznurkiem piłeczkę o średnicy 10 cm o takiej długości, by w całości opasała tę piłkę. Teraz wydłużamy sznurek dokładnie o jeden metr, lecz w taki sposób, by dalej tworzył okrąg. Wówczas łatwo obliczyć, że sznurek teraz „odstaje” od piłki o około 16 cm. Teraz zamiast piłki użyjmy całego globu ziemskiego: przyjmijmy, iż jest to kula o średnicy 6400 km. Jeżeli sznurek wydłużymy o 1 m, jak wysoko będzie on „odstawać” od Ziemi?

Odpowiedź brzmi: również około 16 cm. Wiele osób spodziewa się w tym momencie innej, znacznie mniejszej wartości. Tymczasem rachunki są nieubłagane, przeliczmy przypadek pierwszy:

$$
\begin{gathered}
r = 5 \text{ cm}, \;\; 2\pi r = 10\pi \text{ cm}, \\
2\pi r' = 10\pi \text{ cm} + 1 \text{ m} = 10\pi \text{ cm} + 100 \text{ cm}, \\
r' = \frac{10\pi \text{ cm} + 100 \text{ cm}}{2\pi} = 5 \text{ cm} + \frac{50}{\pi} \text{ cm}, \\
\Delta r = r' - r = 5 \text{ cm} + \frac{50}{\pi} \text{ cm} - 5 \text{ cm} = \frac{50}{\pi} \text{ cm} \approx 16 \text{ cm}.
\end{gathered}
$$

Natomiast dla $R = 6400$ km:

$$
\begin{gathered}
R = 6400 \text{ km}, \;\; 2\pi R = 12800\pi \text{ km}, \\
2\pi R' = 12800\pi \text{ km} + 1 \text{ m} = 12800\pi \text{ km} + 100 \text{ cm}, \\
R' = \frac{12800\pi \text{ km} + 100 \text{ cm}}{2\pi} = 6400 \text{ km} + \frac{50}{\pi} \text{ cm}, \\
\Delta R = R' - R = 6400 \text{ km} + \frac{50}{\pi} \text{ cm} - 6400 \text{ km} = \frac{50}{\pi} \text{ cm} \approx 16 \text{ cm},
\end{gathered}
$$

co potwierdza odpowiedź.

Dalsze problemy będą opierały się głównie na subtelnym wpajaniu błędnych przekonań.

1.2. Paradoks Zenona

Biegacz ma do pokonania pewien dystans. Zanim pokona całość, musi pokonać połowę drogi. Jednakże jeżeli nawet pokona połowę, to pozostaje mu ćwierć dystansu. Pokonując ćwierć, ma do przebycia $\frac{1}{8}$ całej trasy. I tak dalej w nieskończoność – biegacz musi przebiec nieskończoną liczbę odcinków o skończonej długości. Jednakże nie da się pokonać nieskończonej liczby odcinków w skończonym czasie. Stąd też biegacz nigdy nie ukończy biegu.

Wyjaśnienie. W wypowiedzi paradoksu ukryte jest założenie, że suma o nieskończonej liczbie elementów musi być nieskończona. Nic bardziej mylnego: w matematyce (zauważmy, że paradoks ma ujęcie, które da się przeformułować w języku matematyki) istnieją nieskończone sumy (szeregi), których sumy są skończone. W szczególności, ze wzoru na sumę szeregu geometrycznego:

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots = \sum_{n=1}^{\infty} \frac{1}{2^n} = 1.$$

1.3. Fałszywe monety

Bierzemy dwie jednakowe monety. Jedną kładziemy nieruchomo, drugą toczymy po jej brzegu. Skoro moneta wykonuje drogę równą swojemu obwodowi, wykona jeden pełny obrót. Niestety, doświadczenie życiowe pokazuje, że obroty są dwa.

Wyjaśnienie. Ponieważ problem jest na tyle ciekawy, rozwiązanie pozostawiam do znalezienia Czytelnikowi.

2. Problematyczny język

2.1. Żargon a język potoczny

Podstawą cechą matematycznego języka jest ścisłość i jednoznaczność zadanych stwierdzeń. (Nie)stety, człowiek nie myśli w sposób formalny i, przykładowo, stosuje pewne uproszczenia, **których sens zależy od rzeczywistego[2] kontekstu**. Ta cecha nie może dotyczyć matematyki – ta, jako pewien system formalny, nie jest zależna od kontekstów. Język mówiony i pisany nie odzwierciedla w całości matematycznej abstrakcji. Jedną z emanacji tej właściwości jest obecność (w mniejszym lub większym stopniu) języka potocznego, który wielokrotnie pomaga objaśniać „matematyczne fakty”.

Naturalną „odpowiedzią” na powyższy problem jest pewien specyficzny sposób konstrukcji zdań zwany **matematycznym żargonem**, który „stara się” możliwie wyrugować niejednoznaczności oraz nadać wypowiedzi precyzję.

[2] Tu: odnoszącego się do rzeczywistości.

Przykład 2.1. Naturalnie brzmiące zdanie:

> *Liczba jest parzysta, gdy dzieli się przez* 2.

w matematycznym żargonie brzmi:

> *Liczba jest parzysta* **wtedy i tylko wtedy, gdy** *dzieli się przez* 2.

dla podkreślenia występujacej równoważności i jednocześnie uniknięcia niejednoznaczności – w końcu zdanie: p, gdy q dla niektórych mogłoby oznaczać jedynie przeciwną implikację „$\Leftarrow$".

Dalej unaocznimy sobie, iż potoczne konstrukcje zdaniowe użyte w matematycznych definicjach mogą zaburzać przekazywany sens.

Przykład 2.2. Potocznie moglibyśmy powiedzieć:

> *Suma zbiorów* $A \cup B$ *to zbiór złożony z elementów* A *i* B.

Zdanie to zapewne nie budzi(łoby?) większych nieporozumień. Tymczasem spójnik „i" zarezerwowany jest dla koniunkcji, a przez to części wspólnej: wszak x należy do $A \cap B$ (wtedy i tylko wtedy), gdy należy do A i należy do B. W celu zachowania precyzji wypowiedzi warto wystrzegać się używania spójników językowych w sytuacjach, gdy nie odpowiadają one spójnikom logicznym.

Opisaliśmy pewne cechy żargonu matematycznego, jednakże by lepiej zrozumieć istotę i potrzebę wdrażania pewnych stałych szablonów językowych, których nie sposób znaleźć w literackiej polszczyźnie, przytoczmy parę stałych zwrotów:

- *bez straty ogólności* – nakładając dodatkowy warunek, z którego po odpowiednim prostym przeformułowaniu uzyskuje się wszystkie możliwe badane przypadki; na przykład: „Niech x i y będą różnymi liczbami rzeczywistymi. Bez straty ogólności załóżmy, że $x < y$". Istotnie, zamieniając rolę y z x, czyli dokonując prostego przeformułowania, wyczerpuje się wszystkie możliwości,
- *trywialny* – oczywisty; wynikający bezpośrednio z założeń lub znanych twierdzeń; czasami – zerowy,
- *dla dostatecznie dużego* – dla liczby większej od pewnej innej liczby, o której wiadomo, że musi zaistnieć; na przykład „Dla dostatecznie dużego x funkcja $\log_2 x$ jest większa od 10^{15}",

- *istnieje* – daje się zdefiniować bez popadania w sprzeczność,
- *dokładnie jeden* – istniejący i jednoznacznie określony obiekt o opisywanej własności.

W każdym z powyższych zwrotów sens jest jednoznaczny i jest kwestią ogólnie przyjętej umowy. Zauważmy, iż zwrot *dokładnie jeden* jest pleonazmem[3], natomiast słowo *trywialny* wbrew żądaniom zależy od kontekstu wypowiedzi, jednakże i w tej sytuacji pozostawiona jest jednoznaczność – termin „oczywisty" nie może odnosić się do obiektów zerowych i vice versa, stąd wieloznaczność tego słowa nie prowadzi do nieporozumień[4].

2.2. Metajęzyk

Przykład 2.3. Ania i Beata dostały zadanie: miały ocenić prawdziwość zdań z pewnej listy. Lista ta miała tylko jedno zdanie i brzmiało ono:

Dokładnie jedno ze zdań tej listy jest prawdziwe.

Ania bez wahania stwierdziła, że zdanie jest prawdziwe, natomiast Beata temu zaprzeczyła. Kto ma rację?

Załóżmy najpierw, że Ania ma rację – zdanie z listy jest prawdziwe. Istotnie, jako że jest jedyne (i jest z tej listy), to nie występuje tu żadna sprzeczność. Przyjmijmy teraz wersję Beaty – zdanie jest nieprawdziwe. Skoro jest nieprawdziwe, to znaczy, iż, ponieważ lista jest tylko jednoelementowa, w tej liście nie ma zdań prawdziwych, co pokrywa się z oczekiwaniami. Po raz kolejny nie występuje tu żadna sprzeczność. Ponieważ zadane założenia nie prowadziły do żadnych sprzeczności, to są prawdziwe. Zatem przedstawione zdanie jest jednocześnie prawdziwe i fałszywe, co jest niemożliwe na gruncie logiki dwuwartościowej.

Wyjaśnienie. Mamy do czynienia ze zdaniem, które orzekaja o sobie samym. Paradoks ten wynika z połączenia języka oraz tak zwanego **metajęzyka**, który zostanie przedstawiony niżej. Podobnym zagadnieniem jest tak zwany **paradoks kłamcy** (paradoksem Eubulidesa), który „zauważa" wewnętrzną sprzeczność zdań typu „ja teraz kłamię".

Nieco upraszczając, **metajęzykiem** nazywamy język (podmiotowy) służący do opisu innego języka (nazwijmy go przedmiotowym). W ramach metajęzyka oceniamy prawdziwość zdań języka podmiotowego, natomiast

[3] Potocznie masło maślane.
[4] Wyrażenie *gdy nie prowadzi do nieporozumień* również należy do żargonu!

w języku podmiotowym wyrażone są pewne zdania i konstrukcje językowe (niekoniecznie w sensie języka mówionego/pisanego, możemy myśleć o języku jak o pewnym systemie formalnym, struktury o pewnych ściśle określonych regułach). Jeżeli pewien język opisuje inny, to w stosunku do drugiego jest **językiem wyższego rzędu**. Pytania o prawdziwość zdań języka niższego rzędu nie należą do badanego języka – innymi słowy prawdziwość pewnego języka F jest nierozstrzygalna w jego obrębie – gdyby była, mielibyśmy język, który stanowi sam o sobie – czyli dokładnie tego, czego chcemy uniknąć – kopię problemu zdań samoorzekających.

Zauważmy ponadto, że metajęzyki mogą tworzyć pewną hierarchię – niech F_1, F_2, F_3 będą pewnymi językami skonstruowanymi w taki sposób, iż F_2 opisuje język F_1, natomiast F_3 opisuje F_2. Szczegółowy opis zagadnienia definiowania prawdy jako takiej znajduje się w jednej z prac polskiego logika XX wieku Alfreda Tarskiego [3]. Informacje o problemach związanych z samym obiektem metajęzyka można znaleźć tu: [4].

3. Algebraiczne wpadki

Wykonując pewne obustronne operacje, zawsze powinniśmy sprawdzać, czy kroki, które wykonujemy są równoważne (jeżeli nie, to mówimy, że są nieodwracalne). Skrzętnie ukryte dzielenie przez zero jest podstawą wielu sofizmatów – rozważmy poniższy przykład.

Przykład 3.1. Niech dana będzie równość:

$$\frac{2-x}{1-2x} = \frac{1-3x}{x-3}.$$

Wówczas:

$$\begin{aligned} (2-x)(3-x) &= (1-2x)(1-3x), \\ 6-2x-3x+x^2 &= 1-3x-2x+6x^2, \\ x^2 &= 1+6x^2-6, \\ x^2-1 &= 6(x^2-1), \\ 1 &= 6. \end{aligned}$$

Wyjaśnienie. Jak w większości tego typu przypadkach, w którymś momencie dzielimy przez 0. Ostatni krok można wykonać pod warunkiem, iż $x^2 \neq 1$. Niestety, rozwiązaniem zadanego równania są właśnie liczby $x = 1$ oraz $x = -1$, co sprawia, iż dzielimy przez 0.

Otrzymana "równość" $1 = 6$ sugeruje rozpatrzenie kongruencji $\mod 5$, w której przystawanie $1 \equiv 6 \pmod 5$ jest prawdziwe. Rozważmy zatem $\mathbb{Z}_5$. Wówczas:

$$\begin{aligned} 6 - 2x - 3x + x^2 &\equiv 1 - 3x - 2x + 6x^2 \pmod 5, \\ 1 - 0 \cdot x + x^2 &\equiv 1 - 0 \cdot x + x^2 \pmod 5, \\ 1 + x^2 &\equiv 1 + x^2 \pmod 5, \\ 0 &\equiv 0 \pmod 5. \end{aligned}$$

Tożsamość ta mówi nam, iż każda liczba ciała $\mathbb{Z}_5$, dla której mianowniki się nie zerują (tj. poza 3), spełnia zadane równanie.

Spora część błędów związana jest z faktem, iż wykonuje się kroki nieodwracalne, zwiększając tym samym liczbę rozwiązań. Rozważmy kolejny przykład.

Przykład 3.2. Należy rozwiązać równanie $2x - x\sqrt{5} = -1$.

$$\begin{aligned} 2x - x\sqrt{5} &= -1, \\ 2x + 1 &= x\sqrt{5}, \\ 4x^2 + 4x + 1 &= 5x^2, \\ 0 &= x^2 - 4x - 1. \end{aligned}$$

Zatem $x = 2 - \sqrt{5}$ lub $x = 2 + \sqrt{5}$. Ale $2 \cdot (2 - \sqrt{5}) - (2 - \sqrt{5})\sqrt{5} = 4 - 2\sqrt{5} - 2\sqrt{5} + 5 = 9 - 4\sqrt{5} \neq 1$!

Wyjaśnienie. Jak nietrudno się domyślić, przejścia nie są równoważne – krok polegający na obustronnym podniesieniu do kwadratu nie jest odwracalny. Rozwiązując równania w powyższy sposób, to jest z użyciem kroków nieodwracalnych, musimy zawsze na końcu sprawdzić, które z otrzymanych rozwiązań są właściwymi – najłatwiej poprzez wstawienie wyników do pierwotnego równania.

Dodatkowo zauważmy, że zadane równanie było równaniem **pierwszego stopnia**, a więc nie mogło mieć więcej niż jednego rozwiązania.

Istnieje bardziej wysublimowany sofizmat łączący poznane fakty.

Przykład 3.3. Rozwiążmy równanie $x^2 + x + 1 = 0$. Nietrudno się przekonać, iż 1 nie jest pierwiastkiem tego równania, zatem możemy podzielić stronami równość przez x:

$$x + 1 + \frac{1}{x} = 0,$$

co można doprowadzić do postaci:

$$\frac{1}{x} = -(x+1).$$

Ale wyjściowe równanie jest równoważne $x^2 = -(x+1)$, zatem możemy wywnioskować równość:

$$\frac{1}{x} = x^2,$$

skąd mamy $x^3 = 1$, którego jednym z pierwiastków jest 1. Sprzeczność: $1^2 + 1 + 1 = 3 \neq 0$.

Wyjaśnienie. Pozostawię to Czytelnikowi. Do wyjaśnienia tego problemu wystarczy wiedzieć, iż $x^3 = (x-1)(x^2+x+1)$.

Wejdźmy teraz na nieco wyższy poziom abstrakcji.

Przykład 3.4. Wprowadźmy taką liczbę i, dla której $i^2 = -1$. Jest to tak zwana jednostka urojona, czasami zapisywana jako $\sqrt{-1}$. Zauważmy, że:

$$1 = \sqrt{1} = \sqrt{(-1)^2} = \sqrt{-1}\sqrt{-1} = i \cdot i = i^2 = -1.$$

Wyjaśnienie. O ile dla liczb dodatnich zachodziła tożsamość: $\sqrt{a \cdot b} = \sqrt{a}\sqrt{b}$, o tyle dla **liczb zespolonych**, tj. liczb postaci $x + i \cdot y$ dla $x, y \in \mathbb{R}$ ta równość w ogólności nie jest prawdziwa.

Oczywiście, przykłady można mnożyć. To jednak wszystko, co zostało przygotowane na dzisiaj.

Mateusz Szymański

Literatura

[1] *Matematyka dla Ciekawych Świata*, 2011/2012 `http://licealisci.icm.edu.pl/drupal/?q=node/12`.

[2] *Słownik języka polskiego.*

[3] **Alfred Tarski** Pojęcie prawdy w językach nauk dedukcyjnych. Warszawa 1933.

[4] **Zbigniew Tworak** *Współczesne teorie prawdy.* Wydawnictwo Naukowe UAM, Poznań 2009.

[5] **Jan Kraszewski** *Wstęp do matematyki.* Wydawnictwa Naukowo-Techniczne.

[O metodach mnożenia wielomianów]

Część pierwsza

Załóżmy, że mamy dane dwa wielomiany $f, g : \mathbb{C} \longmapsto \mathbb{C}$, $f_i, g_i \in \mathbb{C}$, $i = 0, \dots, n$ zadane wzorami

$$f(x) = f_0 + f_1 x + \ldots + f_n x^n,$$
$$g(x) = g_0 + g_1 x + \ldots + g_n x^n.$$

Ich iloczyn jest wielomianem stopnia $2n$:

$$f(x) \cdot g(x) = c_0 + c_1 x + \ldots + c_{n-1} x^{n-1} + \ldots + c_{2n} x^{2n}, \qquad (1.1)$$

gdzie i-ty, $i = 0, \dots, 2n$, współczynnik c_i wyraża się wzorem

$$c_i = \sum_{\substack{0 \leqslant k,l \leqslant n \\ k+l=i}} f_k b_l.$$

Jak wyznaczyć iloczyn dwóch wielomianów? Chcemy skorzystać z algorytmu, który wyznaczy iloczyn dwóch wielomianów w możliwie najszybszy sposób – tzn. wykonując przy tym jak najmniejszą ilość operacji arytmetycznych. Najoczywistszym rozwiązaniem jest oczywiście...

"Brute-force"

Najbardziej oczywistą metodą uzyskania iloczynu h wielomianów

$$f = f_0 + f_1 x + \ldots + f_n x^n \text{ oraz } g = g_0 + g_1 x + \ldots + g_n x^n$$

jest skorzystanie z wzoru 1.1 – bezpośrednie mnożenie kolejnych współczynników f_i, g_j, $i, j = 0, \ldots n$ przez siebie i dodawanie otrzymanych wartości do odpowiednich współczynników liczonego przez nas iloczynu (tzn. iloczyn współczynników f_i, g_j leżących przy potęgach odpowiednio x^i, x^j wielomianów f i g dodawany jest do współczynnika h_{i+j} leżącego przy potędze x^{i+j}). Opisany algorytm zapisany został w poniższym pseudokodzie.

Algorytm 1 Mnożenie wielomianów "brute-force"-em

Input: Tablice $f = [f_0, \ldots, f_n]$, $g = [g_0, \ldots, g_n]$ w których przechowywane są współczynniki mnożonych wielomianów.
Output: Tablica $h = [h_0, \ldots, h_{2n}]$ przechowująca współczynniki iloczynu wielomianów f i h.

```
def Brute-Force-Mul(f, g)
    h := [0, ..., 0]
    for i := 0 : n do
        for j := 0 : n do
            h[i + j] = h[i + j] + f[i] · g[j]
        end for
    end for
    return h
```

Pętla przebiegająca po zmiennej i wykonuje się $n + 1$ razy, wewnątrz niej pętla przebiegająca po j wykonuje się $n + 1$ razy; wewnątrz tych pętli wykonywane jest jedno mnożenie i jedno dodawanie – w sumie wykonywanych jest $2(n+1)^2$ operacji – daje to złożoność rzędu $\Theta(n^2)$. Może da się lepiej, szybciej? Da się!

Divide et imperia

W informatyce istnieje cała klasa algorytmów opartych na łacińskiej sentencji *divide et imperia* („dziel i zwyciężaj"), których idea polega na zastąpieniu problemu rekurencyjnym rozwiązywaniem problemów podobnych, ale o mniejszym rozmiarze tak długo, aż problem będzie rozwiązywalny bezpośrednio. Klasycznymi przykładami takich algorytmów jest *quicksort*, *mergesort*, czy przeszukiwanie binarne.

Takim algorytmem jest również algorytm Karatsuby, polegający na stosunkowo prostej obserwacji: wielomian stopnia n można zapisać w postaci

$$f(x) = f^0(x) + x^{\lfloor \frac{n}{2} \rfloor} f^1(x),$$

gdzie f_0 jest wielomianem stopnia mniejszego lub równego $\lfloor \frac{n}{2} \rfloor$. Zapisując w ten sposób wielomiany f i g stopnia n

$$f(x) = f^0(x) + x^{\lfloor \frac{n}{2} \rfloor} f^1(x),$$
$$g(x) = g^0(x) + x^{\lfloor \frac{n}{2} \rfloor} g^1(x),$$

możemy przedstawić ich iloczyn w postaci

$$f(x) \cdot g(x) = \big(f^0(x) + x^{\lfloor \frac{n}{2} \rfloor} f^1(x)\big) \cdot \big(g^0(x) + x^{\lfloor \frac{n}{2} \rfloor} g^1(x)\big) =$$
$$(f^0 \cdot g^0)(x) + \big(f^0 \cdot g^1 + f^1 \cdot g^0\big)(x) \cdot x^{\lfloor \frac{n}{2} \rfloor} + (f^1 \cdot g^1)(x) \cdot x^{2\lfloor \frac{n}{2} \rfloor}.$$

Zastępujemy więc mnożenie dwóch wielomianów stopnia n czterema mnożeniami wielomianów stopnia $\sim \frac{n}{2}$. Ponieważ dodawanie wielomianów ma złożoność liniową, to zależność opisująca złożoność takiego algorytmu może być opisana równaniem

$$T(n) = 4T\left(\frac{n}{2}\right) + \Theta(n).$$

Niestety, nie daje to znaczącej poprawy – rozwiązując powyższe równanie (np. przy wykorzystaniu tw. o rekurencji uniwersalnej) dostajemy złożoność $T(n) = \Theta(n^2)$. Jeśli jednak zapiszemy sumę $f^0 \cdot g^1 + f^1 \cdot g^0$ jako

$$f^0 \cdot g^1 + f^1 \cdot g^0 = (f^1 + f^0) \cdot (g^1 + g^0) - (f^1 \cdot g^1) - (f^0 \cdot g^0),$$

to iloczyn przyjmie postać

$$\begin{aligned} f(x) \cdot g(x) = (f^0 \cdot g^0)(x) \\ +\big((f^1 + f^0) \cdot (g^1 + g^0) - (f^1 \cdot g^1) - (f^0 \cdot g^0)\big)(x) \cdot x^{\lfloor \frac{n}{2} \rfloor} \\ + (f^1 \cdot g^1)(x) \cdot x^{2\lfloor \frac{n}{2} \rfloor}, \end{aligned}$$

a obliczenie iloczynu wielomianów stopnia n zastąpimy obliczeniami trzech wielomianów stopnia $\sim \frac{n}{2}$. Złożnoność takiej rekurencji można opisać wzorem

$$T(n) = 3T\left(\frac{n}{2}\right) + \Theta(n),$$

a po rozwiązaniu powyższej rekurencji uzyskujemy $T(n) = \Theta(n^{\log_2 3})$, więc $T(n) \sim O(n^{1.59})$, co daje dużo lepszy wynik niż bezpośrednie podejście do problemu.

Algorytm 2 Algorytm Karatsuby

Input: Tablice $f = [f_0, \ldots, f_n]$, $g = [g_0, \ldots, g_n]$ w których przechowywane są współczynniki mnożonych wielomianów.

Output: Tablica $h = [h_0, \ldots, h_m]$ przechowująca współczynniki iloczynu wielomianów f i g.

def KARATSUBA-MUL(f, g)
    if n==0 **then**
        return $[f_0 g_0]$
    else if n%2==0 **then** ▷ Upewniamy się że f i g
        $f := [f_0, \ldots, f_n, 0]$ ▷ są parzystej długości.
        $g := [g_0, \ldots, g_n, 0]$
        $n := n + 1$
    end if

    $f^0 := [f_0, \ldots, f_{\frac{n}{2}}]$ ▷ Dzielimy problem na podproblemy.
    $f^1 := [f_{\frac{n}{2}+1}, \ldots, f_n]$
    $g^0 := [g_0, \ldots, g_{\frac{n}{2}}]$
    $g^1 := [g_{\frac{n}{2}+1}, \ldots, g_n]$

    $a :=$ KARATSUBA-MUL(f^0, g^0) ▷ Rozwiązujemy podproblemy.
    $b :=$ KARATSUBA-MUL($f^0 + f^1, g^0 + g^1$)
    $c :=$ KARATSUBA-MUL(f^1, g^1)

    $b := [\underbrace{0, \ldots, 0}_{\frac{n}{2}}, b_0 - a_0 - c_0, \ldots, b_n - a_n - c_n]$
    $c := [\underbrace{0, \ldots, 0}_{n}, c_0, \ldots, c_n]$
    $h := a + b + c$ ▷ Odtwarzamy rozwiązanie wyjściowego problemu
    return h

Istnieje szybszy sposób mnożenia wielomianów – o tym sposobie będzie można przeczytać w kolejnym numerze [MACI$_E$RZATORA].

Marcin Jenczmyk

[Koło Naukowe Matematyków UŚ zaprasza!]

Koło Naukowe Matematyków UŚ to grupa studentów, których interesuje matematyka i którzy lubią spędzać razem czas. Organizujemy spotkania, wykłady, wyjazdowe konferencje naukowe w Szczyrku, angażujemy się w organizację Święta Liczby Pi, redagujemy [MACIERZATOR,] ale po pierwsze: spotykamy się niemal codziennie w pokoju 524 Instytutu Matematyki UŚ, gdzie rozmawiamy (nie tylko o matematyce!), gramy w szachy, pijemy herbatę i po prostu spędzamy razem czas.

Zapraszamy wszystkich – nie będziemy Cię pytać o oceny ani egzaminować z wiedzy matematycznej. Ważne jest dla nas, żeby każdy czuł się w Kole dobrze. Możesz przyjść po prostu na spotkanie (nie ma żadnych zapisów), pojechać na sesję wyjazdową do Szczyrku, wpaść pograć w szachy, opowiedzieć o czymś ciekawym podczas oficjalnego spotkania, albo po prostu z nami posiedzieć. Każdy jest mile widziany. Do KNM nie ma żadnych zapisów – można tak po prostu przyjść.

Informacje o planowanych formalnych spotkaniach, wieczorach gier, konferencjach itp. umieszczamy na stronie `www.knm.katowice.pl` i kołowym profilu na facebooku: `fb.com/knm.katowice`. Zapraszamy!

[Stopka redakcyjna]

Redaktor naczelny: Mateusz Szymański
Autorzy artykułów: Marcin Jenczmyk, Mateusz Szymański,
Joanna Zwierzyńska
Skład i łamanie w LaTeX: Marcin Jenczmyk
Kontakt z redakcją bezpośrednio w pokoju KNM (p.524) lub
elektronicznie:
macierzator@knm.katowice.pl

Wszystkie archiwalne numery [MACIERZATORA] dostępne są również w wydaniu elektronicznym na stronie internetowej KNM UŚ: `www.knm.katowice.pl`. Wydanie elektroniczne [MACIERZATORA] posiada numer ISSN: 2083-9774.

listopad 2014