Nieskończoność: 8. Nieskończoność nieskończoności

Michał KORCH

W poprzednim odcinku zastanawialiśmy się, czy istnieje „nieskończoność” pomiędzy licznością zbioru liczb naturalnych i licznością zbioru liczb rzeczywistych. Pora na ostatni etap naszej podróży. Będzie to etap jeszcze dalej prowadzący w nieskończoność – będziemy rozważać i konstruować coraz większe „nieskończoności”. Okaże się, że jest ich bardzo nieskończenie wiele. Może aż za bardzo.

Piszemy tutaj „nieskończoności”, mając oczywiście na myśli możliwe liczności, czyli moce, nieskończonych zbiorów. Matematycy nazywają je też liczbami kardynalnymi. Będziemy mówić, że jedna „nieskończoność” (liczność lub moc zbioru A) jest mniejsza od drugiej „nieskończoności” (liczności lub mocy zbioru B), jeśli wszystkich elementów zbioru A nie da się ustawić w pary ze wszystkimi elementami zbioru B, ale można je ustawić z pewną częścią zbioru B.

W poprzednich odcinkach rozmawialiśmy o twierdzeniu Cantora. Mówi ono, że każdy zbiór A ma tę cechę, że zbiór $\mathcal{P}(A)$ wszystkich podzbiorów zbioru A nie jest równoliczny ze zbiorem A. Skoro jednak dla każdego elementu a zbioru A do zbioru $\mathcal{P}(A)$ należy $\{a\}$, czyli jednoelementowy podzbiór z tym elementem, to część zbioru $\mathcal{P}(A)$ złożona z jednoelementowych zbiorów jest równoliczna ze zbiorem A. Możemy zatem powiedzieć, że moc zbioru $\mathcal{P}(A)$ jest większa od mocy zbioru A, co oznaczamy $|\mathcal{P}(A)| > |A|$.

Znając to twierdzenie, bez trudu możemy tworzyć coraz większe nieskończoności. Rzeczywiście, niech $A_0 = \mathbb{N}$ to zbiór liczb naturalnych. Wtedy niech $A_1 = \mathcal{P}(A_0)$. Oczywiście, $|A_0| < |A_1|$. Niech zatem $A_2 = \mathcal{P}(A_1)$ i w takim razie $|A_0| < |A_1| < |A_2|$. I tak dalej, niech $A_{i+1} = \mathcal{P}(A_i)$. Otrzymujemy w ten sposób

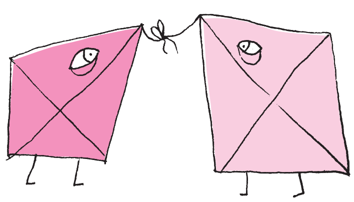
$$|A_0| < |A_1| < |A_2| < \ldots < |A_i| < \ldots$$

nieskończony ciąg coraz większych nieskończoności!

Ale i ten nieskończony ciąg nieskończoności to jeszcze nie koniec. Niech bowiem

$$X = A_0 \cup A_1 \cup A_2 \cup \ldots$$

będzie sumą wszystkich tych nieskończenie wielu zbiorów. Zauważmy, że X jest jeszcze większy niż którykolwiek z nich. Rzeczywiście, dla dowolnego i mamy $|A_i| < |X|$, bowiem zbiór X zawiera zbiór A_{i+1}, a przecież $|A_{i+1}| > |A_i|$.



I to także oczywiście nie koniec, bo przecież możemy wziąć zbiór wszystkich podzbiorów tak zdefiniowanego zbioru X, aby otrzymać zbiór o jeszcze większej liczności. I tak dalej. W pewnym sensie w nieskończoność i za nieskończonością w nieskończoność.

Ale i na tym nie kończy się nasza przygoda. Przyjrzyjmy się temu procesowi tworzenia coraz większych „nieskończoności” bardziej metodycznie. Metodę tworzenia z liczności $|A|$ większej liczności $|\mathcal{P}(A)|$ będziemy tu nazywać metodą podzbiorów. Metodą sumy będziemy nazywać stworzenie z nieskończonej rodziny zbiorów, w której dla każdego zbioru A z tej rodziny jest w tej rodzinie zbiór B taki, że $|A| < |B|$, zbioru jeszcze większego od dowolnego jej elementu, mianowicie jej sumy.

Zauważmy jednak, że metodą podzbiorów niekoniecznie z danej liczności otrzymamy najmniejszą liczność większą od niej. Być może istnieją liczby kardynalne pomiędzy $|A|$ oraz $|\mathcal{P}(A)|$. Zresztą właśnie hipoteza continuum odnosi się do tego typu rozważań.

Okazuje się, na szczęście (choć aby podać dowód tego faktu, potrzebne są definicje, które wykraczają poza tę serię artykułów), że dla każdej rodziny „nieskończoności” istnieje w niej „nieskończoność” najmniejsza. W szczególności, wynika z tego, że dla danego zbioru A można znaleźć pewien zbiór B, o liczności najmniejszej z tych, które są większe od liczności zbioru A. To przejście będziemy nazywać metodą następnikową.

Z reguły kolejne możliwe nieskończone liczby kardynalne oznacza się za pomocą pierwszej litery z języka hebrajskiego $\aleph$ (*alef*) z odpowiednim indeksem. Tak więc $\aleph_0$ to liczność zbioru liczb naturalnych, a $\aleph_1$ to najmniejsza liczba kardynalna większa od $\aleph_0$, zaś $\aleph_2$ to najmniejsza liczba kardynalna większa od $\aleph_1$. Hipotezę continuum możemy więc sformułować jako stwierdzenie, że $|\mathcal{P}(\mathbb{N})| = \aleph_1$.

Warto w tym momencie odnotować wprost dwa mniej lub bardziej zaskakujące wnioski. Po pierwsze, nie istnieje największa „nieskończoność". Rzeczywiście, dla każdego zbioru A istnieje zbiór o większej mocy, mianowicie zbiór $\mathcal{P}(A)$.

Drugi wniosek jest następujący: nie istnieje zbiór wszystkich „nieskończoności". Znów, załóżmy przeciwnie, że taki zbiór istnieje. Ale zgodnie z poprzednim wnioskiem, skoro nie ma największej liczby kardynalnej, to dla każdej liczby kardynalnej w tym zbiorze jest w nim też większa liczba kardynalna. Ale w takim razie możemy metodą sumowania (biorąc sumę wszystkich elementów tego zbioru) wyprodukować jeszcze większą liczbę kardynalną, która jest większa od każdej z tego zbioru, więc nie jest elementem tego zbioru. Ale zbiór miał zawierać wszystkie liczby kardynalne, co stanowi sprzeczność.

Niemniej znaleźliśmy trzy metody konstruowania coraz większych liczb kardynalnych: metodę następnikową, metodę podzbiorów i metodę sumowania. Nasuwa się od razu nurtujące pytanie. Czy poczynając od liczności zbioru liczb naturalnych, można „dojść" do dowolnej „nieskończoności" (liczby kardynalnej), stosując te trzy metody?

Potrzebne będą nam jeszcze dwie definicje. Powiemy, że pewna liczba kardynalna jest graniczna, jeśli wśród mniejszych od niej nie ma największej. Zauważmy, że $\aleph_0$ jest graniczną liczbą kardynalną, bowiem każdy zbiór o liczności mniejszej niż jego moc to zbiór skończony. A zatem liczności mniejsze od $\aleph_0$ to po prostu skończone liczby i nie ma wśród nich największej.

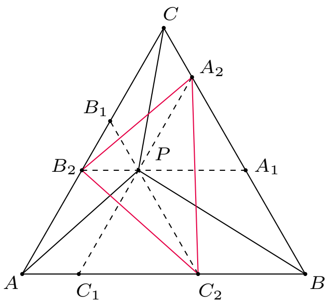
Druga definicja to regularność „nieskończoności". Powiemy, że pewna liczba kardynalna jest regularna, jeśli nie da się jej otrzymać metodą sumy ze zbioru liczności mniejszych od niej, który sam ma od niej mniejszą liczność. Ponownie zauważmy, że $\aleph_0$ jest liczbą regularną, bowiem skończona suma skończonych zbiorów jest tylko skończona. Niemniej nie każda „nieskończoność" jest regularna. Na przykład zastosujmy metodę sumy do zbioru liczb kardynalnych $\aleph_0, \aleph_1, \aleph_2, \ldots$ Skoro elementy tego zbioru w oczywisty sposób są ponumerowane liczbami naturalnymi, to jest ich tyle samo co liczb naturalnych, czyli $\aleph_0$. Jednak liczba, którą dostaniemy, jest większa od każdej z nich, i w szczególności od $\aleph_0$. Nie jest więc regularna.

Inaczej mówiąc, liczb kardynalnych granicznych nie można skonstruować metodą następnikową z mniejszych liczności. Za to liczb kardynalnych regularnych nie da się skonstruować metodą sumowania, używając tylko zbiorów o mniejszej mocy. Matematycy nazywają liczbę kardynalną większą od liczności zbioru liczb naturalnych słabo nieosiągalną, jeśli łączy w sobie te dwie cechy, czyli jeśli jest regularna i graniczna. Takiej liczby nie da się więc skonstruować z mniejszych „nieskończoności", stosując tylko metody następnikową i sumy!

No dobrze, w takim razie zastanówmy się nad „nieskończonościami", których nie da się skonstruować z mniejszych liczb kardynalnych, używając dowolnych z tych trzech metod. Takie hipotetyczne liczby kardynalne (większe od liczności zbioru liczb naturalnych), których nie można osiągnąć z mniejszych liczb, używając metod następnikowej, podzbiorów i sumy, nazywamy silnie nieosiągalnymi.

Czy jednak takie liczby istnieją? Odpowiedź na to pytanie jest podobna, ale może jeszcze bardziej subtelna niż w przypadku hipotezy continuum. Zakładając nawet, że taka liczba istnieje, możemy rozpatrzeć najmniejszą z nich – i zauważmy, że z powodzeniem możemy uprawiać teorię zbiorów

Rozwiązanie zadania M 1626.



Przez punkt P poprowadźmy proste równoległe do boków trójkąta ABC, przecinające te boki w punktach A_i, B_i, C_i $(i = 1, 2)$, jak na rysunku. Wówczas $PA = B_2C_2$, podobnie z długościami PB i PC, stąd należy zmaksymalizować pole trójkąta $A_2B_2C_2$. Oznaczając przez $[\mathcal{F}]$ pole figury $\mathcal{F}$, dostajemy

(*)
$$[A_2B_2C_2] = \frac{1}{2}([AC_1PB_2] + [BA_1PC_2] + [CB_1PA_2]) = \frac{1}{2}([ABC] - [PA_1A_2] - [PB_1B_2] - [PC_1C_2]).$$

Trójkąty PA_1A_2, PB_1B_2 i PC_1C_2 są podobne do ABC w skalach odpowiednio A_1A_2, B_1B_2 i C_1C_2. W związku z tym

(**)
$$[PA_1A_2] + [PB_1B_2] + [PC_1C_2] = [ABC](A_1A_2^2 + B_1B_2^2 + C_1C_2^2) \leqslant \leqslant \frac{1}{3}[ABC](A_1A_2 + B_1B_2 + C_1C_2)^2 = \frac{1}{3}[ABC]$$

Łącząc (*) i (**), dostajemy $[A_2B_2C_2] \leqslant \frac{1}{3}[ABC] = \frac{\sqrt{3}}{12}$. Równość otrzymamy, biorąc za punkt P środek ciężkości trójkąta ABC, co kończy rozwiązanie.

Rozwiązanie zadania F 992.

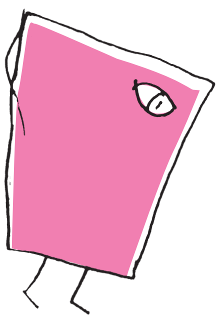
Zgodnie z kryterium Rayleigha granica rozdzielczości obrazu uzyskanego za pomocą przyrządu o średnicy D i fali o długości λ wynosi $\alpha = 1{,}22\lambda/D \approx \lambda/D$, gdzie α oznacza najmniejszy kąt tworzony przez kierunki, pod jakimi widzimy dwa punkty jako rozdzielone. Będzie to więc kąt, pod jakim widzimy najmniejsze rozróżnialne szczegóły o wielkości d z odległości L. Światło widzialne odpowiada długościom fal świetlnych z przedziału od 380 do 770 nm. Do oszacowania przyjmijmy $\lambda = 500\,\mathrm{nm}$. Jak się wydaje, do odczytania tablicy rejestracyjnej wystarczy rozróżnianie szczegółów o wielkości $d = 5\,\mathrm{mm}$. Mamy więc:

$$\alpha \approx \lambda/D = d/L,$$

a stąd $L = dD/\lambda = 24\,\mathrm{km}$.

Rozwiązanie zadania F 991.
Jako model serca możemy rozważyć cylinder z tłokiem. Moc takiego urządzenia otrzymamy, mnożąc siłę, z jaką działamy na tłok przez jego prędkość. Siła jest równa iloczynowi ciśnienia p i powierzchni tłoka, a iloczyn powierzchni tłoka przez jego prędkość jest równy objętości krwi pompowanej w jednostce czasu. Otrzymujemy więc:

$$L = nVp \approx 1{,}3\,\mathrm{W}.$$

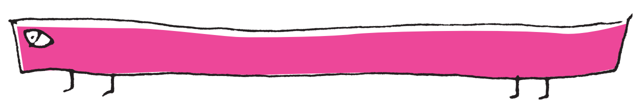


i matematykę tylko w ramach zbiorów mniej licznych niż ona. Nigdy wtedy jej nie napotkamy! To, czy ona istnieje, nie będzie miało dla nas wtedy żadnego znaczenia. Doprecyzowanie tego rozumowania prowadzi do dowodu, że z aksjomatów nie da się wykazać, że taka liczba istnieje.

W drugą stronę jest jeszcze trudniej. Da się bowiem udowodnić, że w ramach aksjomatów nie da się udowodnić, że nie da się udowodnić, że taka „nieskończoność” nie istnieje! Gdyby bowiem było to możliwe, dawałoby to dowód niesprzeczności aksjomatów, co przeczyłoby twierdzeniu Gödla o niezupełności (patrz odcinek „Rozmyślania o myślakach”). Istnienie takich „nieskończoności” jest więc jeszcze bardziej ulotne niż istnienie nieskończoności pomiędzy licznością liczb naturalnych a licznością liczb rzeczywistych.

W takim razie wszechświat zbiorów wygląda następująco: najmniejszym zbiorem jest zbiór pusty, potem są coraz większe zbiory skończone, aż w końcu najmniejsza nieskończona liczba kardynalna $\aleph_0$, czyli liczność zbioru liczb naturalnych. Potem spotkamy zbiory, których liczności to coraz większe „nieskończoności”, które możemy skonstruować, poczynając od $\aleph_0$ i korzystając z metod następnikowej, podzbiorów i sumy. I dalej jest horyzont, za którym być może nic nie ma, a być może jest pierwsza silnie nieosiągalna liczba kardynalna. Z tej „nieskończoności” znów moglibyśmy konstruować coraz większe liczby kardynalne, ale mniejsze niż kolejny hipotetyczny horyzont, którego przekroczyć nie możemy, a który stanowi kolejna silnie nieosiągalna liczba kardynalna. I tak dalej. To jest podróż w nieskończoność i za nieskończoność.

Przygodę tę wypada zakończyć, cytując jednego z bohaterów, od których zaczęliśmy nasze rozważania, czyli Davida Hilberta. „Nieskończoność! Żadne inne pytanie nie poruszyło tak głęboko duszy człowieka”.



Złożoność algorytmów teorioliczbowych

Rozważmy następujący algorytm:

```
function czynnik(int n)
{
   int i = 2;
   while (i < n)
   {
      if (n % i) == 0 return i;
      i = i + 1;
   }
   return 0;
}
```

Jak łatwo sprawdzić, podany kod zwraca najmniejszy nietrywialny czynnik podanej na wejściu liczby n, bądź 0 – gdy takiego czynnika nie ma (bo np. n jest liczbą pierwszą).

Zastanówmy się, jaka jest złożoność podanego programu. Pętla `while` wykona co najwyżej $O(n)$ obrotów.
W pojedynczym jej wykonaniu niemal wszystkie operacje mają koszt stały, poza operacją `%` (reszta z dzielenia), której koszt możemy bardzo zgrubnie oszacować z góry przez $O(n)$ (w rzeczywistości można łatwo osiągnąć $O(\log(n))$). Oznacza to, że cały algorytm działa w czasie nie większym niż $O(n^2)$.

Czy oznacza to, że właśnie pokazaliśmy wielomianowy algorytm na szukanie nietrywialnych czynników? Rozkład nawet dużych liczb na czynniki pierwsze już nie jest dla nas kłopotem?

Oczywiście, nic z tych rzeczy.

Nieporozumienie bierze się z problemu z ustaleniem, co jest parametrem, względem którego liczymy złożoność programów komputerowych. Otóż parametrem jest dla nas zawsze *rozmiar danych*, ale rozumiany jako długość *napisu* reprezentującego wejście. Konkretniej: `1 000 000 000` ma dla nas rozmiar „dziesięć”, a nie „miliard”...

Wracając do naszego algorytmu: jeśli rozmiar danych to k, to wówczas liczba n, którą reprezentują te dane jest rzędu 10^k. Skoro więc oszacowaliśmy czas działania algorytmu przez $O(n^2)$, to w języku rozmiaru danych przekłada się to na $O((10^k)^2) = O(100^k)$, czyli jest jednak wykładniczy od k.

Potencjalny algorytm wielomianowy na rozkład na czynniki musiałby więc być pewnie nieco bardziej wyrafinowany...

Tomasz KAZANA