Szyfry klasyczne

Wojciech GUZICKI

W tym artykule zajmiemy się najprostszymi sposobami szyfrowania, znanymi od wielu stuleci i nie mającymi już większego znaczenia praktycznego. Zostaną one pokazane po to, by wyjaśnić, co nazywamy „klasycznym systemem kryptograficznym". W kolejnym artykule (*Delta* 3/1997) opiszemy znacznie nowsze i lepsze sposoby szyfrowania, tzw. szyfry z publicznym kluczem.

Jeden z najstarszych sposobów szyfrowania pochodzi od Juliusza Cezara, który szyfrował swoją korespondencję z Cyceronem. Sposób ten polegał na tym, że zamiast każdej litery pisało się literę występującą w alfabecie trzy miejsca dalej. Tak więc, jeśli użyjemy dzisiejszego alfabetu łacińskiego:

ABCDEFGHIJKLMNOPQRSTUVWXYZ,

to zamiast litery A będziemy pisać D, zamiast K piszemy N, zamiast Y piszemy B. Widzimy więc, że alfabet traktujemy „cyklicznie", tzn. po ostatniej literze Z następuje znów pierwsza A itd.

Słynne słowa Cezara ALEA IACTA EST zaszyfrowalibyśmy więc jako DOHD LDFWD HVW. Na tym przykładzie objaśnimy dwa ważne pojęcia kryptografii (czyli nauki o szyfrowaniu): systemu kryptograficznego i klucza. System kryptograficzny to, mówiąc nieprecyzyjnie, ogólny sposób szyfrowania. W naszym przykładzie polega on na tym, że zamiast danej litery alfabetu piszemy literę występującą w tym samym alfabecie ileś miejsc dalej. Cezar zdecydował się akurat na trzy miejsca dalej, ale równie dobrze mógłby pisać literę występującą siedem miejsc dalej. Sposób szyfrowania (tzn. system kryptograficzny) byłby w zasadzie ten sam, różniłby się tylko wyborem *klucza*, czyli liczby wskazującej, o ile miejsc dalej w alfabecie stoi litera, którą mam napisać. Można powiedzieć, że system kryptograficzny polega tu na pisaniu litery stojącej k miejsc dalej, a liczba k jest kluczem. Podsumujmy: szyfrowanie polega na wyborze ogólnego sposobu, algorytmu szyfrowania, zwanego systemem kryptograficznym i pewnych parametrów, od których ten algorytm jest zależny, nazywanych kluczem szyfrowania.

Każdą zaszyfrowaną wiadomość trzeba kiedyś rozszyfrować. W szyfrze Cezara znajdujemy literę stojącą w alfabecie trzy miejsca bliżej, czyli w istocie stosujemy ten sam algorytm szyfrowania z innym kluczem. Do szyfrowania używamy klucza +3, a do rozszyfrowywania klucza −3. Gdy znamy klucz szyfrowania, to znamy też klucz rozszyfrowywania. Tak naprawdę jest to ten sam klucz, jeśli pominiemy jego znak.

Szyfr Cezara bardzo łatwo jest opisać w sposób matematyczny. Kolejnym literom alfabetu łacińskiego przyporządkujemy liczby od 0 do 25. Przyjmijmy oznaczenie: $a \bmod b$ oznacza (zawsze nieujemną!) resztę z dzielenia liczby całkowitej a przez dodatnią liczbę całkowitą b. System kryptograficzny Cezara może teraz być zdefiniowany wzorem

$$C = (P + k) \bmod 26,$$

gdzie k jest kluczem szyfrowania, P jest numerem litery, którą szyfrujemy, a C jest numerem litery po zaszyfrowaniu. Rozszyfrowywanie odbywa się według wzoru

$$P = (C - k) \bmod 26.$$

Jeśli ktoś zadaje sobie tyle trudu, by szyfrować wiadomości wysyłane do kogoś innego, to pewnie dlatego, że nie chce, by inne, niepowołane do tego osoby, mogły tę wiadomości odczytać. I pewnie znajdą się te inne osoby, które chcą koniecznie przeczytać to, co zostało zaszyfrowane. Jeśli nie znają one sposobu szyfrowania, to muszą ten szyfr „złamać". W jaki sposób można tego dokonać?

Kartezjański przewrót w filozofii?

Jan WASZKIEWICZ

Sen Kartezjusza

Nowoczesny świat, nasz świat triumfującej racjonalności, narodził się 10 listopada 1619 roku, wraz z objawieniem i koszmarem nocnym. Tak Philip J. Davis i Reuben Hersh rozpoczynają swą piękną książkę *Sen Kartezjusza* (z podtytułem *świat według matematyki*). To Kartezjusz bowiem, wówczas 23-letni oficer w służbie Maksymiliana Bawarskiego, owej nocy doznał olśnienia, które zmieniło nie tylko jego własne życie. Przez poprzedzające to przeżycie tygodnie zmagał się on z filozoficznym problemem zasadności naszego poznania. W czasie postoju w wiejskiej chacie, gdzieś koło niemieckiego miasta Ulm, w nagłym błysku intuicji dostrzega *podstawy zdumiewającej nauki*, po czym zapada w sen i śni trzy sny. Pierwsze dwa, wedle jego własnej interpretacji, zdają się kwestionować dotychczasowe życie Kartezjusza, trzeci – zdaje się dawać wskazówki co do przyszłego postępowania – unifikacji nauki dzięki systematycznemu i metodycznemu użyciu rozumu. Godzi się jeszcze dodać, że filozof w dowód wdzięczności za objawione prawdy zobowiązał się odbyć pieszą pielgrzymkę do sanktuarium Matki Boskiej w Loreto we Włoszech, którą istotnie odbył z czteroletnim opóźnieniem.

Radykalne zwątpienie

Jaka była natura objawionej prawdy? Najlepiej chyba syntetyzuje ją początek pierwszej z *Medytacji o pierwszej filozofii* napisanej w 1630 r.: *Przed kilkoma już laty spostrzegłem, jak wiele rzeczy fałszywych uważałem w mojej młodości za prawdziwe i jak wątpliwe jest to wszystko, co później na ich podstawie zbudowałem; doszedłem więc do przekonania, że jeśli chcę nareszcie coś pewnego i trwałego w naukach ustalić, to trzeba raz w życiu z gruntu wszystko obalić i na nowo rozpocząć od pierwszych podstaw.* Program, który Kartezjusz realizował od chwili swojego olśnienia, polegał więc na poddaniu całej wiedzy testowi radykalnego sceptycyzmu i sprawdzeniu, co z niej pozostanie. Dopiero od tego fundamentu można było zacząć budowę gmachu wiedzy wolnej od złudzeń i przesądów. Oczywiście, z czego

filozof zdaje sobie sprawę, analiza wszystkich poszczególnych stwierdzeń byłaby – jak to ujmuje – *nie kończącym się przedsięwzięciem*, proponuje więc drogę na skróty. Polega ona na kolejnym rozpatrzeniu całych kategorii twierdzeń i odrzucania ich, jeśli tylko znajdziemy powody do odrzucenia niektórych z nich. Poza tym, trzeba skupić się na fundamentalnych zasadach, gdyż *po zburzeniu fundamentów wszystko, co na nich zbudowane, samo upada.* Jako pierwsze ulegają zakwestionowaniu wszystkie stwierdzenia oparte na świadectwie zmysłów. Nietrudno bowiem podać przykłady, kiedy świadectwo owo zawodzi. Jasne jest, że tym bardziej kartezjuszowy test każe zakwestionować koncepcje wcześniejszych szkół filozoficznych. Każda z nich dostarcza zresztą argumentów za odrzuceniem konkurentów. Testu nie wytrzymują również twierdzenia teologiczne. Opierają się one bowiem na pewnych mniemaniach, dotyczących natury Boga, których zaprzeczenie również prowadzi do spójnych konsekwencji.

Myślę, więc jestem

Co ostatecznie zostaje na pobojowisku? Otóż jedynym, co wytrzymuje krytykę, jest fakt krytycznego myślenia i myślący podmiot. Mam wątpliwości, być może jestem zwodzony przez zmysły albo nawet przez samego Stwórcę (nawet tak radykalną hipotezę rozpatrywał Kartezjusz), ale to jednak *ja istnieję, a co więcej – to ja wątpię*. Tej prawdy nie mogą obalić żadne argumenty. Gdyby bowiem jakiś argument doprowadził do mojego zwątpienia we własne istnienie, to jednak musiałby on dotrzeć do mnie i to poprzez proces myślowy. Potwierdziłby tym samym i to, że istnieję, i to, że jestem bytem myślącym. *Myślę, więc jestem* – podsumowuje ten stan rzeczy najbardziej chyba znany aforyzm filozoficzny wszechczasów.

Od tego fundamentu Kartezjusz odbudowuje gmach swojej wiedzy, a ponieważ w różnych punktach wychodzi daleko poza ustalenia swoich poprzedników, ukazuje również potęgę swojego systemu, swej metody i jej głównego narzędzia – sceptycznie nastawionego ludzkiego rozumu.

Jak jednak wygląda rekonstrukcja? Co włącza Kartezjusz do obszaru niewątpliwej wiedzy? Wiedza ta, jeśli ma być doskonalsza od odrzuconych mniemań, musi być z góry odporna na test

Po pierwsze, będziemy zakładać, że osoba łamiąca szyfr zna system kryptograficzny i nie zna tylko klucza. Dlaczego przyjmujemy takie założenie? Wśród wielu powodów można wymienić ten, że system kryptograficzny na ogół trudniej zmienić niż klucz. Używa się więc tego samego systemu na tyle długo, że osoby niepowołane mogą wykraść informacje o samym systemie. Bezpieczeństwo szyfrowania będzie zapewnione dzięki częstym zmianom kluczy. Innym powodem jest ten, że często tego samego systemu używa bardzo wiele osób i sam system jest dobrze wszystkim znany.

A jak w takim razie zdobyć klucz, jeśli dysponuje się tylko tekstem zaszyfrowanym? Czasami nie jest to trudne. Np. szyfr Cezara można złamać bardzo łatwo. Przecież ma on tylko 26 kluczy. Wystarczy spróbować wszystkich, by przekonać się, że tylko jedna wiadomość brzmi sensownie, a pozostałe stanowią niezrozumiały bełkot. Klucz użyty w tym rozszyfrowywaniu jest właściwym kluczem. Widzimy więc, że system kryptograficzny dopuszczający niewiele kluczy nie jest bezpieczny i łatwo taki szyfr złamać. Kiedyś myślano, że bezpieczeństwo szyfru zależy po prostu od liczby kluczy. Girolamo Cardano, wybitny uczony XVI wieku, pisał, że niemożliwy do złamania jest nieco inny szyfr, polegający na tym, że zamiast każdej litery alfabetu piszemy ustaloną inną literę. Wyjaśni to najlepiej przykład. Przyjmijmy, że zamiast litery `A` piszemy `Q`, zamiast `B` piszemy `W` itd. według następującego schematu:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
QWERTYUIOPASDFGHJKLZXCVBNM
```

(zamiast litery stojącej w górnym wierszu piszemy literę znajdującą się pod nią w dolnym wierszu). Zdanie `ALEA IACTA EST` zostanie teraz zaszyfrowane jako `QSTQ OQEZQ TLZ`. System kryptograficzny polega tu na zastępowaniu każdej litery inną, a kluczem jest stojąca w dolnym wierszu permutacja liter alfabetu. Kluczem rozszyfrowywania jest oczywiście permutacja odwrotna, którą nietrudno wypisać:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
KXVMCNOPHQRSZYIJADLEGWBUFT
```

Liczba kluczy jest ogromna. Jest ich 26!, czyli 403291461126605635584000000. Oczywiście, przeszukanie wszystkich możliwych kluczy nie jest wykonalne, trwałoby zbyt długo. Jak więc można złamać ten szyfr? Sięgamy do metod statystycznych. Okazuje się, że w tekstach napisanych w danym języku poszczególne litery nie występują z tą samą częstotliwością. I tak, na przykład, w języku angielskim najczęściej występuje litera `E` (około 13% wszystkich liter odpowiednio długiego tekstu). Drugą z kolei jest litera `T` (około 9%), następnymi są `A`, `O`, `N`, `I`, `R`. W języku polskim nie ma litery tak bardzo wyróżniającej się od innych i dlatego łamanie zaszyfrowanego tekstu napisanego po polsku będzie nieco trudniejsze. Najczęściej występują litery `A` oraz `I` (po około 9%), a po nich `E` i `O` (po około 7,5%).

Taki sposób łamania szyfru opisał w opowiadaniu „Tańczące sylwetki" Artur Conan Doyle. Czytelnik-koneser może sprawdzić, czy Sherlock Holmes korzystał z odpowiednich rozkładów częstości.

Przypuśćmy teraz, że mamy dany tekst zaszyfrowany za pomocą opisanego wyżej systemu. Musimy, oczywiście, wiedzieć, w jakim języku napisano zaszyfrowaną wiadomość i znać rozkład częstości występowania liter alfabetu w tekstach napisanych w tym języku. Jeśli nasz tekst jest wystarczająco długi (wystarczy już kilkaset

liter), to rozkład częstości jego liter powinien być podobny. Najczęściej występujące litery w tekście zaszyfrowanym powinny odpowiadać najczęstszym literom danego języka (choć niekoniecznie w tej samej kolejności). Próbujemy przypisać te litery sobie; po kilku próbach okaże się, że dość łatwo możemy domyśleć się znaczenia następnych liter, potem jeszcze następnych, aż wreszcie domyślamy się znaczenia wszystkich liter klucza i odczytujemy cały tekst. Duża liczba kluczy nie jest więc warunkiem wystarczającym bezpieczeństwa szyfru.

Przyjrzymy się jeszcze jednemu systemowi kryptograficznemu. Od poprzedniego systemu będzie się on różnić tym, że ta sama litera może być zaszyfrowana w różny sposób, w zależności od tego, w którym miejscu tekstu występuje. Weźmy ciąg kilku liczb mniejszych od 26, na przykład $(3, 7, 1, 11, 2)$. Sposób szyfrowania polega teraz na tym, że zamiast pierwszej litery tekstu piszemy literę znajdującą się w alfabecie 3 miejsca dalej, zamiast drugiej litery tekstu piszemy literę znajdującą się w alfabecie 7 miejsc dalej, zamiast trzeciej literę znajdującą się 1 miejsce dalej, potem literę znajdującą się 11 miejsc dalej, potem 2 miejsca i zaczynamy od początku: 3 miejsca, 7 miejsc, 1 miejsce itd. A więc zdanie `ALEA IACTA EST` po zaszyfrowaniu będzie brzmiało `DSFL KDJUL GVA`. Zauważmy, że litery `A` w pierwszym słowie zostały zaszyfrowane inaczej. Natomiast pierwsza litera `A` i druga w drugim słowie zostały zaszyfrowane tak samo – dlatego, że druga z nich występuje w tekście pięć miejsc dalej i klucz ma pięć liczb. Ten system kryptograficzny, nazywany szyfrem Vigenère'a, jest więc jakby kombinacją wielu systemów Cezara, a kluczem szyfrowania jest odpowiedni ciąg liczb. Klucze, oczywiście, mogą być dowolnej długości. Często zapamiętujemy klucz w postaci słowa. Na przykład słowo `CEZAR` odpowiada ciągowi $(3, 5, 26, 1, 18)$: litera `C` jest trzecią literą alfabetu, litera `E` piątą itd. Liczba kluczy w tym systemie jest naprawdę olbrzymia. Kluczy długości 26, a więc takiej długości jak permutacje w poprzednim systemie, jest 26^{26}; ta liczba jest znacznie większa niż 26!. A jednak ten szyfr też można łatwo złamać.

Łamanie polega na tym, by najpierw odgadnąć długość klucza. Następnie łatwo już odgadnąć liczbę stojącą w kluczu na każdym miejscu. Na przykład, odgadliśmy, że klucz ma długość 5. Zliczamy litery stojące na co piątym miejscu: na pierwszym, szóstym, jedenastym itd. Rozkład częstości tych liter powinien być przesuniętym o kilka miejsc rozkładem częstości występowania liter danego alfabetu. Te dwa rozkłady można bardzo łatwo do siebie „dopasować" i w ten sposób odnajdujemy liczbę stojącą w kluczu na pierwszym miejscu. Potem tak samo odnajdujemy liczbę stojącą na drugim miejscu, na trzecim itd.

A jak odgadnąć długość klucza? Można po prostu próbować po kolei: najpierw przypuścić, że klucz ma długość 2 i spróbować dopasować odpowiednie rozkłady. Jeśli się nie uda, to próbujemy długości 3, potem 4 i tak dalej, dotąd, aż znajdziemy właściwą długość. Istnieją zresztą metody statystyczne, dzięki którym można tę długość wyznaczyć z dość dobrym przybliżeniem. Tak więc ten system kryptograficzny też nie jest bezpieczny.

Przyjrzyjmy się sposobom łamania tych dwóch szyfrów. W obu przypadkach próbowaliśmy znaleźć klucz szyfrowania. Wydaje się, że ten sposób postępowania jest najbardziej naturalny. Jeśli znajdziemy klucz szyfrowania, to łatwo odzyskamy z niego klucz rozszyfrowywania i odczytamy zaszyfrowaną wiadomość. Ale czy jest to jedyny sposób łamania szyfru? Czy odczytanie zaszyfrowanej

wątpliwości. Możemy więc akceptować jedynie te sądy, które stanowią *pewne, jasne i wyraźne ujęcie tego, co twierdzę.* Co więcej, owa *jasność i pewność* musi być cechą wszystkich elementów akceptowanego stwierdzenia. Możemy więc przy ich konstrukcji odwoływać się jedynie do tego, co przez radykalny test zostało dopuszczone. Konstrukcja przypomina więc budowanie gmachu matematyki od pojęć pierwotnych i dotyczących ich pewników (proszę zauważyć, że słowo to jest jakby zapożyczone ze słownika Kartezjusza!) do coraz mniej oczywistych stwierdzeń, mających wszakże za sobą sankcję ścisłego rozumowania, w którym odczucie oczywistości odgrywa istotną rolę.

Zgoda, że zarówno określenia *pewne, jasne, wyraźne*, jak też dyrektywa oparcia na nich poznania mogą budzić wątpliwości. Zauważmy jednak, że tę samą dyrektywę możemy sformułować w sposób mniej kontrowersyjny. Otóż Kartezjusz przeciwny był uznaniu *czegokolwiek, co do czego nie mamy pewności, co nie jest dla nas jasne, czego nie potrafimy wyraziście przedstawić* (chciałoby się użyć potocznego określenia: był przeciwny mętniactwu). I nie ulega wątpliwości, że taka dyrektywa przyświecała całemu nowożytnemu rozwojowi nauki.

Rekonstrukcja obrazu świata

Co więc Kartezjusz włączył w swój obraz świata? Pewne konsekwencje pociąga za sobą akceptacja istnienia mnie samego. Jeśli bowiem istnieję, to jako ktoś przeżywający pewne doświadczenia zmysłowe, z których niektóre są jasne i wyraźne (jak ból zęba). To samo dotyczy najbardziej oczywistych myśli – na przykład tych, które odnoszą się do idei matematycznych. Obszar pewności, a więc po kartezjuszowsku pojmowanej prawdy, poszerza się stopniowo. Pojawiają się w nim idee wrodzone (jako jasne i wyraźne), wśród których jest idea Boga. Kartezjusz idzie dalej i wykazuje, że istnieje nie tylko idea Boga, ale i Bóg, jako byt doskonały. Ułomny ludzki umysł nie może być twórcą tej idei, gdyż rzecz doskonała nie może powstać z niedoskonałych. Źródło więc idei bytu doskonałego musi być co najmniej tak doskonałe, jak owa idea. To kończy dowód.

Tak konstruowana rzeczywistość Kartezjusza rozpada się więc na dwa obszary: myślący umysł i świat materialny. Cechą pierwszego jest myślenie, cechą drugiego – rozciągłość w przestrzeni i ruch mający mechaniczny charakter. Jakie

wszakże związki łączą obie te dziedziny? Komentatorzy wskazują, że pojęcie Boga było Kartezjuszowi niezbędne do załatania istniejącej tu właśnie dziury w tworzonym systemie. Jak bowiem miał on uzasadnić związek między doświadczeniem a powstającą racjonalną rekonstrukcją rzeczywistości? Bóg, jako byt doskonały, stawał się poręczycielem prawdziwości konstrukcji rozumowych. Muszą one odpowiadać stworzonemu światu, gdyż w przeciwnym przypadku jego Stwórca, jako zwodziciel czy oszust, nie zasługiwałby na przypisywany mu atrybut doskonałości. Między zasadniczą strukturą rzeczywistości (w pewnej mierze potwierdzaną w doświadczeniu) a jej racjonalną rekonstrukcją zachodzi więc zasadnicza zgodność.

Z tą chwilą pojawia się możliwość pogodzenia się z obiektywną rzeczywistością, choć akceptowane z niej będzie tylko to, co przetrwa test radykalnego wątpienia bądź da się rozumowo – w sposób jasny i oczywisty! – wyprowadzić z zaakceptowanych już elementów. Na pewno zaś należy z gmachu wiedzy usuwać wszystko, co opiera się na ideach niejasnych i niewyraźnych i na sądach nie wytrzymujących krytyki.

Jeśli weźmiemy pod uwagę, jak zbudowany był obraz świata przed Kartezjuszem, w jakim stopniu zasiedlony był przez różne, pochodzące z niejasnych źródeł *byty widzialne i niewidzialne*, to zobaczymy, do jakiego stopnia świat kartezjański stał się prostszy, a w perspektywie mógł ulegać dalszym uproszczeniom. Jakim? To już zależało od tego, kto i w jakim celu puszczał w ruch wypracowane przez filozofa narzędzia. On sam zakwestionował, jako nie wytrzymujące racjonalnej krytyki, pojęcia próżni i oddziaływania na odległość. Dlatego jego racjonalna konstrukcja fizyki, która miała tłumaczyć fakty odkryte i analizowane przez Galileusza i innych wielkich badaczy owego okresu, opierała się na całym szeregu założeń, które raczej oddalały niż przybliżały newtonowską syntezę. Co ważniejsze, fizyka Kartezjusza była znacznie mniej zmatematyzowana od tego, co robił Galileusz i pod tym względem lepiej mieści się w tradycji arystotelesowskiej.

Tak więc, radykalny racjonalizm Kartezjusza nie we wszystkich obszarach był równie owocny. Zastosowany do matematyki przyniósł konstrukcję geometrii analitycznej, co dało dalszemu rozwojowi matematyki silny impuls.

wiadomości musi być równoważne znalezieniu klucza? Dla tych dwóch systemów kryptograficznych jest to równoważne. Przypuśćmy bowiem, że otrzymaliśmy jednocześnie tekst jawny (tzn. tekst oryginalny, przed zaszyfrowaniem) i tekst zaszyfrowany. Bez trudu w obu przypadkach wyznaczymy klucz, a właściwie oba klucze: szyfrowania i rozszyfrowywania. Wystarczy przyjrzeć się, jakie litery w tekście zaszyfrowanym odpowiadają kolejnym literom tekstu jawnego. Czy jednak tak będzie dla wszystkich innych systemów kryptograficznych? Spróbujmy sformułować wyraźnie pytania, które się narzucają.

Po pierwsze, jeśli poznamy klucz szyfrowania, to czy łatwo możemy odtworzyć z niego klucz rozszyfrowywania? We wszystkich powyższych przykładach było to oczywiste, ale nie zawsze musi tak być. Po drugie, jeśli mamy jednocześnie tekst jawny i tekst zaszyfrowany, to czy umiemy odtworzyć klucz szyfrowania (lub rozszyfrowywania)? Znów okaże się, że nie zawsze będziemy umieli to zrobić.

Klasyczne systemy kryptograficzne to właśnie takie systemy, których złamanie polega w istocie na znalezieniu klucza szyfrowania i tym samym klucza rozszyfrowywania. W następnym artykule poznamy tzw. szyfry z publicznym kluczem. Polegają one na tym, że klucz szyfrowania może być powszechnie znany i każdy będzie mógł go użyć do zaszyfrowania dowolnej wiadomości. Klucz rozszyfrowywania będzie jednak tajny i tylko jego „właściciel" będzie mógł z niego skorzystać. W tych systemach kryptograficznych znajomość klucza szyfrowania nie wystarczy do rozszyfrowania tekstu zaszyfrowanego. Potrzebna jest jeszcze pewna dodatkowa informacja, której nie udostępnia się publicznie i której w praktyce nie można uzyskać, jeśli zna się tylko klucz szyfrowania. Do skonstruowania takich szyfrów wykorzystano subtelne metody teorii liczb, algebry, geometrii algebraicznej i kombinatoryki.

Wycieczka w wirtualną przestrzeń

Jan BARANOWSKI

W *Delcie* 9/1996 Małgorzata Dworska opisywała *Najprostsze wypełnienie przestrzeni wielościanami*. Była tam mowa o pewnym wielościanie archimedesowym. Zamiast użytej tam nazwy *tetrakaidekahedron* wolałbym nazwę *ośmiościan ścięty*. Ta pierwsza nazwa to (po grecku) *czternastościan*, a różnych czternastościanów może być dużo (na przykład sześcian ścięty czy inny: sześcio-ośmiościan, znalazł się w *Małej Galerii Matematycznej* Zdzisława Pogody). Ośmiościan ścięty jest jeden – powstaje przez sprytne obcięcie naroży ośmiościanu foremnego, takie, że po narożach zostają kwadratowe ślady, ze ścian trójkątnych zaś – sześciokąty foremne. Cały wspomniany numer *Delty* jest pełen podobizn ośmiościanu ściętego.

W artykule Małgorzaty Dworskiej przedstawiona jest argumentacja przekonująca, że ośmiościan ścięty wypełnia przestrzeń. Rozumowanie odwołuje się do intuicji płaskiej. Proponuję przyjrzenie się temu w przestrzeni. Może się uda w wyobraźni, bez ani jednego rysunku?

„ – Co się tyczy rycin, to zaraz mogę ci wyrysować smoka z oczami z tysiąca słońc każde – jeśli rysunek masz za dowód prawdy – rzekł Klapaucjusz na to."
(Stanisław Lem, *Cyberiada, Wyprawa szósta*)

Widać, że zarówno Klapaucjusz, jak Lem podzielają opinię Autora o rysunkach. (Red.)

Wyobraź sobie, Drogi Czytelniku, sześcian i jego przekątną łączącą przeciwległe wierzchołki. Poprowadźmy taką płaszczyznę prostopadłą do tej przekątnej, żeby dzieliła sześcian na połowy. Taka płaszczyzna przecina 6 krawędzi, każdą w połowie. Uzyskaliśmy znany przekrój sześcianu – sześciokąt foremny. Czy widzisz go? Kiedyś Krzysztof Nowiński rysował w *Delcie* piękne przekroje brył foremnych w anaglifach... Mamy dwie połówki sześcianu.

Jak wygląda jedna taka połówka? Ma jedną ścianę sześciokątną, trzy ściany to kwadraty z odciętymi narożami i trzy małe ścianki – takie jak te naroża, trójkąty prostokątne równoramienne. Kiedy ustawimy taką bryłkę na ścianie sześciokątnej, może przypominać statek kosmiczny. Tam, gdzie spotykają się kwadraty bez naroży (pięciokąty), jest wierzchołek, zupełnie nienaruszony wierzchołek sześcianu.

Ustawmy teraz osiem „statków kosmicznych", żeby spotkały się w jednym punkcie tymi właśnie wierzchołkami. Jest to możliwe tak samo, jak jest to możliwe z sześcianami. Bryła, która powstała, ma osiem ścian sześciokątnych... Jeśli nie widzisz, że to ośmiościan ścięty, zamiast „statków kosmicznych" wstaw całe sześciany. Osiem sześcianów tworzy kostkę $2 \times 2 \times 2$. Trójkąciki – ściany „statków kosmicznych" – leżą na ścianach tej kostki i zbiegają się po cztery na środkach.

Wygodnie jest teraz operować całymi takimi kostkami, po osiem sześcianów, w każdej siedzi w środku ośmiościan ścięty. Jako sześciany – oczywiście wypełniają przestrzeń szczelnie. Weźmy pod uwagę wypełnienie *normalne*, co w tym przypadku znaczy, że w wierzchołkach spotyka się zawsze osiem kostek.

Jak w tych kostkach ustawione są nasze ośmiościany ścięte? Spotykają się ścianami kwadratowymi. Do każdej ściany sześciokątnej przylega połówka sześcianika. Tak jest w każdej sąsiedniej kostce. W wierzchołkach kostek (za każdym razem ośmiu) spotykają się połówki sześcianów będące na zewnątrz ośmiościanów ściętych. Za każdym razem jest ich osiem.

Jeżeli jeszcze chcesz wyobrażać sobie cokolwiek – widzimy dwie uzupełniające się, przystające struktury złożone z ośmiościanów ściętych stykających się ścianami kwadratowymi. Struktury te dotykają się ścianami sześciokątnymi.

Wydaje mi się, że taka argumentacja jest bardziej przekonująca, bowiem rozumowanie na rzucie może być złudne. Obracanie bryłami w wyobraźni może jest trudniejsze, ale w tym przypadku pewniejsze.

Ciekawe jest, że ośmiościany ścięte wypełniające przestrzeń możemy inaczej ustawić w dwie uzupełniające się, przystające struktury. Wybierzmy tak cztery ściany ośmiościanu ściętego, by żadna para nie miała wspólnej krawędzi (są fragmentami ścian czworościanu foremnego, który można by na nim opisać). Jeżeli będziemy teraz sklejać kolejne ośmiościany ścięte tylko tymi wybranymi ścianami (pilnując, by kwadratowe ściany były zawsze pionowe lub poziome), uzyskamy strukturę, która przypomina z grubsza strukturę diamentu. Wolna przestrzeń między sklejonymi bryłami ma dokładnie ten sam kształt, co one.

Zachęcam do takiego wyobrażania sobie przestrzennych faktów. Udane wycieczki po „wirtualnych" bryłach przynoszą dużo satysfakcji.

Odniesiony do funkcjonowania organizmu ludzkiego prowadził do wizji organizmu jako układu mechanicznego, dominującej co najmniej do XIX wieku. Można by wspomnieć też o przyczynkach Kartezjusza w innych obszarach nauki. Inna sprawa, że znaczna część spuścizny została dość późno opublikowana i jej wpływ na rozwój nauki był mniejszy niż powinien.

Trwały był ton nadany ludzkiemu dążeniu do poznania prawdy: zaufanie do ludzkiego rozumu, żądanie klarowności konstrukcji intelektualnych, poddawanie wszystkich elementów wiedzy testowi radykalnego wątpienia.

Jestem, więc muszę myśleć

Taki napis pojawił się kilka lat temu na wrocławskich murach. Dobrze oddaje on współczesną pozycję kartezjańskiego racjonalizmu. Nadaje się on do formułowania nostalgicznych żartów, ale nie przemawia do wyobraźni. Można nań spojrzeć jak na pewien program badawczy, który wyczerpał swoje możliwości. Polegał on na radykalnym kwestionowaniu wcześniej akceptowanych praw i prawidłowości, na zaczynaniu niejako wszystkiego ciągle od nowa, bez oglądania się na poprzedników i uznane autorytety. Ostatecznymi sędziami pozostawały rozum, myślenie i poczucie oczywistości.

Kartezjusz mógł jeszcze uważać, że te podstawy systemu są jednakowe dla wszystkich i dlatego jego analizy mają uniwersalną wartość. Z każdym kolejnym kartezjanistą sprawa stawała się coraz mniej oczywista. Na francuskiego filozofa powoływały się bowiem wszystkie bez mała późniejsze systemy filozoficzne. Każdy ich twórca zaczynał od radykalnego zakwestionowania dokonań poprzedników, każdy przeciwstawiał im własne rozumowania i własne odczucie oczywistości, a wnioski bywały diametralnie różne.

Dodatkowo, w ostatnich dekadach – i to przez nauki ścisłe – zmuszeni zostaliśmy do akceptacji sądów dalekich od oczywistości i zgodzić się na stosowanie pojęć niejasnych dla laików. Dla uratowania racjonalnego obrazu świata konieczne stało się odwołanie do autorytetów! Co gorsza, straciliśmy wiele z pewności siebie. Nie bardzo wiemy, co oznacza słowo *ja*, a i termin *myślenie* nie jest tak jednoznaczny, jak kiedyś. Przyczyniły się do tego nauki szczegółowe – psychologia (z psychoanalizą), lingwistyka, antropologia, logika...

Nie możemy więc wyjść z systematycznego stosowania kartezjuszowego zwątpienia w tym samym punkcie co on – na gruncie stwierdzenia oczywistości: *myślę, więc jestem*. Tym bardziej że i z poczuciem oczywistości nie jest najlepiej. Zwątpienie dokonało swojego dzieła – zakwestionowało niemal wszystko, co zakwestionować było można, a co gorsza – nie podsuwa żadnego punktu oparcia dla odbudowy obrazu świata.

Tu może leżeć jeden z powodów tego, że w 400 lat od chwili urodzenia się twórcy nowożytnego racjonalizmu widać regres racjonalizmu jako filozoficznej i życiowej postawy. Jeśli rację mieli cytowani na wstępie Davis i Hersh, to, być może, oznacza to i koniec nowoczesności – postmodernizm, jak zwie się modny obecnie prąd filozoficzny i kulturowy. Towarzyszy mu przypływ postaw irracjonalnych (tarot, kabała, astrologia, znachorstwo...).

Zresztą może nie warto zapominać, że wszystko zaczęło się od olśnienia, snu i pielgrzymki filozofa.

Patrz w niebo

Teoria ewolucji gwiazd głosi, że każda gwiazda po wyczerpaniu swoich zapasów wodoru zwiększa rozmiary stając się chłodnym czerwonym olbrzymem. Jeżeli masa gwiazdy jest zbliżona do słonecznej, to zewnętrzne warstwy gwiazdy oderwą się tworząc tzw. mgławicę planetarną. Odbywa się to łagodnie, tzn. nie w wyniku eksplozji, lecz raczej w wyniku silnego wiatru gwiazdowego. Niezbyt szczęśliwie sformułowana nazwa – mgławica planetarna – pochodzi, jak wiadomo, stąd, że pierwszym obserwatorom niektóre, bardziej regularne z tych mgławic przypominały tarcze planet.

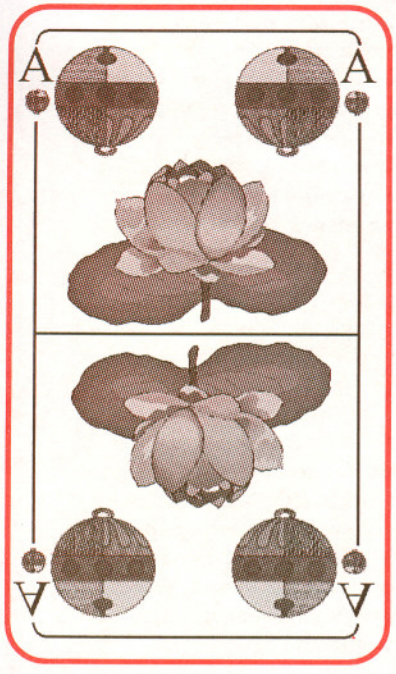
Gdy wziąć dosłownie przedstawiony tu w zarysie opis powstawania mgławicy planetarnej, można by się spodziewać, że oglądając ją z dowolnego kierunku powinno się widzieć pierścień – jako zbiór tych miejsc sferycznej rozszerzającej się otoczki, gdzie wzrok przenika przez najgrubszą warstwę materii, czyli w przybliżeniu na obrzeżu mgławicy. Przynajmniej tak powinna mgławica wyglądać w swojej młodości, gdyż napotykając różne przeszkody w ośrodku międzygwiazdowym powinna z biegiem czasu tracić symetrię i rozpływać się w przestrzeni.

Tymczasem skrupulatne obserwacje ruchów gazu w najsłynniejszej chyba mgławicy planetarnej M57, czyli Pierścienia w Lutni, przeprowadzone kilka lat temu w obserwatorium na Wyspach Kanaryjskich wykazały, że nie jest ona po prostu rozszerzającą się sferą. Wykryto w niej dwa wyraźne strumienie gazu, jeden ku obserwatorowi i drugi w przeciwną stronę, wypływające z centrum mgławicy. Mechanizm powstawania takiego obiektu może wyglądać następująco. Gwiazda pęcznieje do stadium czerwonego olbrzyma, ale wiatr gwiazdowy jest najsilniejszy w płaszczyźnie równika. Gwiazda otacza się więc rzeczywiście pierścieniem materii, który staje się przeszkodą dla dalszych fal wiatru gwiazdowego. W późniejszym więc okresie materia będzie łatwiej wypływać wzdłuż osi obrotu gwiazdy. W sumie powstanie obiekt o wyróżnionej osi symetrii, który oglądany właśnie z kierunku osi będzie wyglądał jak pierścień – np. mgławica M57. Gdyby oglądać ten sam obiekt w płaszczyźnie równika, to byłoby widać owe dwa płynące osiowo strumienie materii. I takie mgławice też się obserwuje.

Zdawałoby się, że nic w tym nadzwyczajnego: niesferyczny wypływ materii powoduje powstanie niesferycznego obiektu; ale godne uwagi chyba jest, że jeden mechanizm może wytłumaczyć wygląd całej klasy obiektów, przy czym to, co widać na niebie, zależy tylko od „punktu widzenia".

Tomasz KWAST

Zadania



Redaguje Krzysztof OLESZKIEWICZ

M 795. Funkcja $f : [0,1] \to [0,\infty)$ ma tę własność, iż dla dowolnych liczb nieujemnych x, y, których suma nie przekracza 1, spełniona jest nierówność $f(x+y) \geq f(x) + f(y)$. Ponadto $f(1) = 1$. Udowodnić, że dla każdej liczby $x \in [0,1]$ spełniona jest nierówność $f(x) \leq 2x$.
Rozwiązanie na str. 15

M 796. Czy przy założeniach poprzedniego zadania można udowodnić, że dla każdej liczby $x \in [0,1]$ spełniona jest także nierówność $f(x) \leq 1{,}99x$?
Rozwiązanie na str. 15

M 797. Dana jest liczba naturalna $n > 1$. Znaleźć wszystkie wielomiany P o współczynnikach rzeczywistych spełniające równość $P(x^n) = P(x)^n$ dla dowolnej liczby rzeczywistej x.
Rozwiązanie na str. 13

Redaguje Krzysztof REJMER

F 443. Znaleźć kształt orbity cząstki o masie m poruszającej się w polu centralnym o potencjale

$$V(r) = -\frac{\lambda}{r^4} \quad (\lambda > 0),$$

jeśli całkowita energia cząstki ma wartość równą zero.
Rozwiązanie na str. 16

F 444. Oszacować rozmiary kropli kapiących podczas deszczu z sufitu w domu, którego dach przecieka. Gęstość wody jest równa $\varrho = 10^3$ kg/m^3, napięcie powierzchniowe zaś $\sigma = 7{,}3 \cdot 10^{-2}$ N/m.
Rozwiązanie na str. 16