



deltami

MATEMATYKA – FIZYKA – ASTRONOMIA – INFORMATYKA

$h=6,63 \cdot 10^{-34} \cdot \nu$ $J \cdot s$ $\pi=3,141592...$

NR 8 (543) 2019

CENA 4 ZŁ - VAT 5%

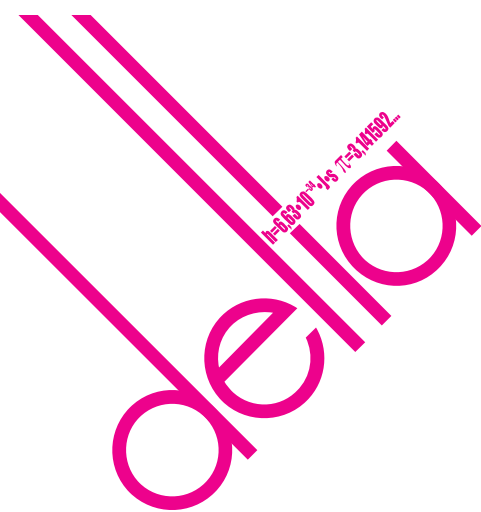
PL ISSN 0137-3005 | NR IND 35 550 X
MIESIĘCZNIK

www.deltami.edu.pl



Nakład: 3500 egz.

**MATEMATYKA
TOROWA**
str. 1



SPIS TREŚCI NUMERU 8 (543)

Matematyka torowa

Piotr Pikul

„Ciemność widzę, widzę ciemność!”, czyli
o ciemnej materii słów kilka

Wojciech A. Hellwing

 Do czego służą zęby?

Magdalena Fikus

A jednak się da (IX):

o obliczeniach wielopodmiotowych

Tomasz Kazana

 Nieskończoność: 5. Zbiory duże

Michał Korch

Liczenie na nosie

Sebastian Oleksa

 Zadania

Czy rozwój sztucznej inteligencji
doprowadzi do buntu maszyn?

Paweł Wawrzyński

Trzęsienia ziemi i płyty litosferyczne

Marek Grad

Kalendarz marsjański

Lech Falandysz


Klub 44

Prosto z nieba: Masa Galaktyki

Niebo w sierpniu

Informatyczny kącik olimpijski (130):

Kwadraty liczb naturalnych

 Gdy zadaniu nie podołasz,
to załatwi je niezmiennik

Bartłomiej Bzdega

str. 1

str. 4

str. 7

str. 8

str. 10

str. 12

str. 13

str. 14

str. 16

str. 18

str. 20

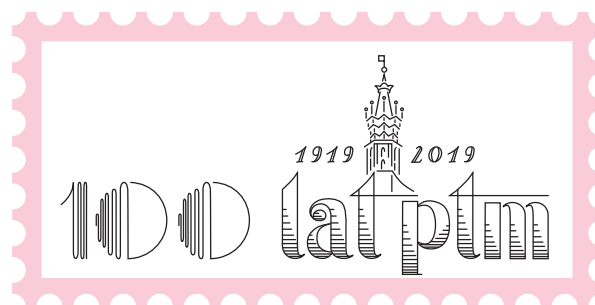
str. 22

str. 22

str. 24

str. 25

W następnym numerze: 100-lecie
Polskiego Towarzystwa Matematycznego



Miesięcznik Delta – matematyka, fizyka, astronomia, informatyka jest wydawany przez Uniwersytet Warszawski przy współpracy towarzystw naukowych: Polskiego Towarzystwa Matematycznego, Polskiego Towarzystwa Fizycznego, Polskiego Towarzystwa Astronomicznego i Polskiego Towarzystwa Informatycznego.

Komitet Redakcyjny: dr Waldemar Berej,
dr Piotr Chrzęstowski-Wachtel,
dr Krzysztof Ciesielski – wiceprzewodniczący,
prof. dr hab. Bożena Czerny, dr Andrzej Dąbrowski,
prof. dr hab. Marek Demiański, prof. dr hab. Krzysztof Diks,
dr Tomasz Greczyło, prof. dr hab. Paweł Idziak,
dr hab. Agnieszka Janiuk, dr hab. Marcin Kiraga,
prof. dr hab. Andrzej Majhofer,
prof. dr hab. Zbigniew Marciniak, dr hab. Zygmunt Mazur,
dr Adam Michalec, dr Zdzisław Pogoda, dr Paweł Preś,
prof. dr hab. Wojciech Rytter, prof. dr hab. Paweł Strzelecki,
prof. dr hab. Andrzej Wysmołek.

Redaguje kolegium w składzie: Wiktor Bartol,
Michał Bejger, Szymon Charzyński – red. nac.,
Wojciech Czerwiński, Anna Durkalec, Tomasz Kazana,
Piotr Kaźmierczak, Kamila Łyczek – z-ca red. nac.,
Katarzyna Małek, Łukasz Rajkowski, Anna Rudnik,
Krzysztof Rudnik, Marzanna Wawro – sekr. red.

Adres do korespondencji:

Redakcja *Delty*, ul. Banacha 2, pokój 4020, 02-097 Warszawa
e-mail: delta@mimuw.edu.pl tel. 22-55-44-402.

Okładki i ilustracje:

Anna Ludwicka Graphic Design & Serigrafia.

Skład systemem \TeX wykonała Redakcja.

Druk: Drukarnia Greg www.greg-drukarnia.pl

Prenumerata:

Garmond Press: www.garmondpress.pl

Kolporter: www.kolporter.com.pl (tylko instytucje)

RUCH S.A.: www.prenumerata.ruch.com.pl

Numery archiwalne (od 1987 r.) można nabyć w Redakcji
osobiście lub zamówić przez e-mail.

Cena 1 egzemplarza: z ostatnich 12 miesięcy 4 zł; wcześniejsze
egzemplarze 1 zł



Strona internetowa (w tym
artykuły archiwalne, linki itd.):
deltami.edu.pl

Można nas też znaleźć na
facebook.com/Delta.czasopismo

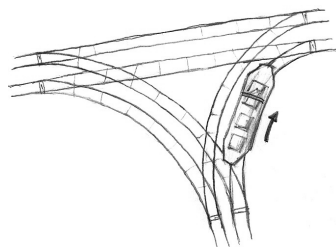
Wydawca: Uniwersytet Warszawski

Na okładce: Łuk triumfalny w Paryżu, Aleksander Jędrzejewski
Zbiory Muzeum Śląskie w Katowicach
autor reprodukcji: Rafał Wyrwich

Matematyka torowa

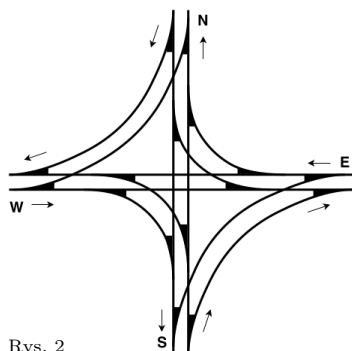
Piotr PIKUL*

*doktorant, Instytut Matematyki,
Uniwersytet Jagielloński

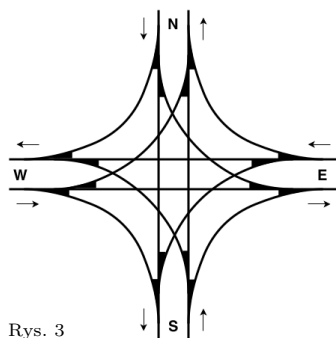


Rys. 1

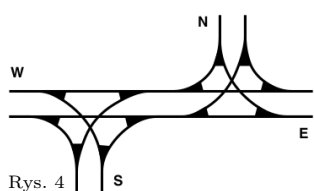
To, co w niniejszym artykule nazywam zwrotnicą, nosi fachowe miano *rozjazdu pojedynczego*, ale słowa *rozjazd* będę używał do innych celów. Będę także konsekwentnie pisał o najazdach i zjazdach zamiast o krzyżownicach i jeździe „na ostrze” lub „z ostrza”.



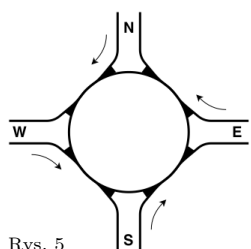
Rys. 2



Rys. 3



Rys. 4



Rys. 5

Podaję, że znakomita większość Czytelników *Delty*, nawet jeśli nie mieszka, to miała okazję przebywać w dużych miejskich aglomeracjach z rozbudowaną siecią tramwajową i zetknąć się z miejscem, w którym spotykają się trzy dwutorowe odcinki trasy. Choć zdarzają się wyjątki, układ torowy w takich przypadkach zwykle wygląda tak jak na rysunku 1 i pozwala na przejazd we wszystkich możliwych relacjach – w tym przypadku mowa o sześciu (dla ścisłości: nie interesują nas przejazdy wymagające zmiany kierunku jazdy). Na użytek tego artykułu będziemy nazywać układ o tej własności *pełnym rozjazdem linii dwutorowych w trzech kierunkach*.

Pełny rozjazd przedstawiony na rysunku 1 zawiera sześć zwrotnic oraz trzy skrzyżowania toru pojedynczego. Mając na względzie Czytelników, którzy dotąd nie dokonywali pogłębionej analizy infrastruktury torowej, spieszymy z wyjaśnieniem, że zwrotnica to taki styk trzech odcinków toru, że jeden z nich jest trwale wyróżniony i nie można przejechać przez zwrotnicę, nie pokonując tego odcinka. Można albo wjechać od strony wyróżnionego *najazdu* i kontynuować podróż po jednym z dwóch *zjazdów*, albo wjechać od strony jednego ze zjazdów i wyjechać najazdem. Na występujących w dalszej części schematach zwrotnice będą zaznaczone poprzez zamalowanie kąta pomiędzy zjazdami. Odcinki torów będziemy oznaczać pojedynczą linią.

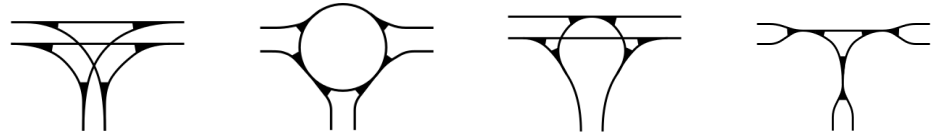
Trzeba przyznać, że przedstawiona postać pełnego rozjazdu w trzech kierunkach jest bardzo intuicyjna i w pierwszej chwili może być nawet trudno wyobrazić sobie inne rozwiązanie. Sytuacja nieznacznie komplikuje się, gdy spotykają się cztery linie dwutorowe. Rozjazd pełny może wtedy wyglądać jak na schematach z rysunków 2 i 3. Układ z rysunku 3 jest nieco bardziej symetryczny, choć opiera się na podobnym pomysle. W przypadku styku czterech linii, ze względu na znaczną złożoność przedstawionych pełnych rozjazdów, często mamy do czynienia z rozjazdem niepełnym (nie umożliwiającym przejazdu we wszystkich dwunastu relacjach). Takimi rozjazdami nie będziemy się zajmować.

Oba przedstawione pełne rozjazdy linii dwutorowych w czterech kierunkach zawierają po szesnaście zwrotnic, jednak układ z rysunku 2 zawiera tylko dwanaście skrzyżowań, podczas gdy układ z rysunku 3 – szesnaście. Gdyby wyobrazić sobie analogiczny, monstrualny, pełny rozjazd w pięciu kierunkach, zawierałby on aż trzydzieści zwrotnic. Pełny rozjazd w czterech kierunkach można zaprojektować również na inne sposoby, na przykład łącząc dwa pełne rozjazdy w trzech kierunkach (rys. 4). Taki układ torów zawierałby tylko dwanaście zwrotnic i sześć skrzyżowań, co czyni go (w pewnym sensie) prostszym od przedstawionych dotąd koncepcji.

Tu może się pojawić pytanie, czy nie można znaleźć czegoś jeszcze „prostszego”? Aby przekonać się, że tak, należy udać się (wystarczy myśla) na słynne rondo w Będzinie, przy którym znajduje się pełny rozjazd tramwajowy zawierający zaledwie osiem zwrotnic. Jego schemat przedstawia rysunek 5. Taka koncepcja wydaje się bardzo elegancka, oszczędna i, w przeciwieństwie do poprzednio omówionych rozjazdów, umożliwia dodatkowo zawracanie. W praktyce przegrywa jednak choćby ze względu na zajmowaną większą powierzchnię. Inną jej wadą jest mniejsza przepustowość. Pomimo tych niedoskonałości rondo torowe można spotkać również w innych miastach, na przykład w Łodzi lub Brukseli. Rondo takie zostało także uwiecznione na obrazie Aleksandra Jędrzejewskiego *Łuk triumfalny w Paryżu*.

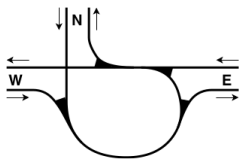
Z punktu widzenia czystej matematyki, gdzie przestrzeń może być nieograniczona, a tramwaje jednopunktowe, rondo jest *lepszym* pełnym rozjazdem. Jeśli interesuje nas pełny rozjazd linii dwutorowych w n kierunkach ($n \geq 3$), koncepcja rondo pozwala go zrealizować z wykorzystaniem $2n$ zwrotnic. Czy mniejsza liczba jest osiągalna? Dla $n = 3$ do budowy rondo potrzeba sześciu zwrotnic, czyli dokładnie tyle, ile wymaga „klasyczny” rozjazd.

Poniżej można zobaczyć także dwa nowe pomysły.



Teraz, w ramach odskoczni od podziwiania schematów, wykażemy, że najmniejszą możliwą liczbą zwoznic pełnego rozjazdu linii dwutorowej w trzech kierunkach jest... 4.

Schemat rozjazdu możemy traktować jako graf nieskierowany, którego krawędziami są odcinki toru, a wierzchołkami rozgałęzienia, czyli zwoznice. Do wierzchołków możemy także zaliczyć wlotowe i wylotowe odcinki. Dla pełnego rozjazdu linii dwutorowej w trzech kierunkach mamy więc sześć wierzchołków o stopniu 1 i pewną liczbę wierzchołków stopnia 3, czyli zwoznic. Każdy odcinek toru ma dwa końce (albo są to zwoznice, albo *liście* „na krawędzi schematu”), więc suma stopni musi być parzysta, czyli po odjęciu parzystej liczby liści dostajemy liczbę parzystą będącą trzykrotnością liczby zwoznic. Zwoznice musi zatem być parzyście wiele. Gdyby było to zero lub dwa, wtedy cały graf miałby albo sześć wierzchołków i trzy krawędzie, albo osiem wierzchołków i sześć krawędzi, czyli nie mógłby być spójny. Jednak od każdego wjazdu istnieje ścieżka do każdego wjazdu, stąd wynika, że graf pełnego rozjazdu jest zawsze spójny, co jest możliwe dopiero przy wykorzystaniu co najmniej czterech zwoznic.

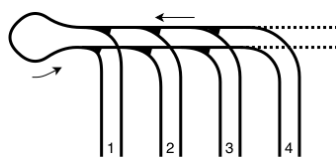


Rys. 6

W przedstawionym dowodzie nie wykorzystaliśmy wszystkich własności pełnego rozjazdu, więc Czytelnik Ostrożny zapewne oczekuje potwierdzenia, że cztery zwoznice naprawdę wystarczą. Takim potwierdzeniem jest rysunek 6, który przedstawia *optymalny*, tj. wykorzystujący minimalną liczbę zwoznic, pełny rozjazd linii dwutorowej w trzech kierunkach. Łatwo zauważyć jego praktyczną nieprzydatność, rozważając przejazd tramwaju z północy na zachód.

Skoro udzieliliśmy odpowiedzi dla $n = 3$, możemy się pokusić o rozstrzygnięcie kwestii większych rozjazdów. Powtarzając rozumowanie ze stopniami, otrzymujemy, że liczba zwoznic musi być parzysta. Jest całkowicie naturalne, że minimalna liczba zwoznic potrzebna do budowy pełnego rozjazdu jest funkcją niemalejącą ze względu na n . Wykażemy, że jest silnie rosnąca.

Niech będzie dany rozjazd optymalny w $n + 1$ kierunkach i wyobraźmy sobie likwidację jednego dwutorowego odcinka oraz wszystkich elementów rozjazdu, które od tego momentu nie będą potrzebne. Oznacza to usunięcie z grafu dwóch liści, które są połączone krawędziami z pewnymi zwoznicami (możliwe, że z tą samą). Jeśli usuwana krawędź dochodzi do zwoznicy od strony zjazdu, wystarczy zastąpić pozostałe dwie krawędzie dochodzące do tej zwoznicy przez jedną (zastępujemy zwoznicę prostym odcinkiem). W przeciwnym przypadku, gdy usuwany jest najazd, żaden przejazd przez zwoznicę nie będzie już możliwy, więc usuwamy również pozostałe dwie krawędzie wychodzące ze zwoznicy. Zauważmy, że za każdym razem usuwamy tylko te odcinki, na które nie da się wjechać z innego kierunku niż usuwany, czyli procedura nie narusza żadnej trasy przejazdu pomiędzy nieusuwanymi kierunkami. Po zakończeniu procedury zostajemy zatem z rozjazdem pełnym w n kierunkach. Usuając jeden dwutorowy odcinek wychodzący z rozjazdu, musimy usunąć co najmniej dwie zwoznice, czyli minimalna liczba zwoznic dla n jest mniejsza przynajmniej o dwa od minimalnej ich liczby dla $n + 1$.



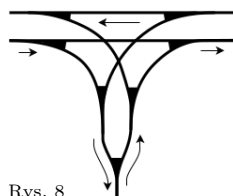
Rys. 7

Powyższe rozumowanie prowadzi (dzięki indukcji matematycznej) do oszacowania liczby zwoznic koniecznej dla pełnego rozjazdu w n kierunkach od dołu przez $4 + 2(n - 3) = 2n - 2$. Pozostaje pytanie, czy taki optymalny rozjazd istnieje dla każdego n ? Odpowiedź jest twierdząca, a jedną z możliwych, ogólnych metod konstruowania takich rozjazdów przedstawia rysunek 7. Zauważmy, że ta metoda dla $n = 3$ daje inne optymalne rozwiązanie od przedstawionego wcześniej.

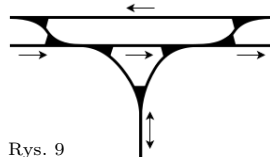
Tak określone rozwiązania optymalne umożliwiają zawracanie z każdego kierunku. Na pewno można uniemożliwić zawracanie z jednego kierunku

(por. rys. 6). Jaka jest minimalna liczba zwrotnic, jeśli zażądamy, aby zawracanie było w ogóle niemożliwe? Co można powiedzieć, jeśli spróbujemy dodatkowo zminimalizować liczbę zwrotnic, przez które należy w najgorszym wypadku przejechać podczas pokonywania rozjazdu? Z tymi pytaniami pozostawię Czytelnika, a to jeszcze nie koniec.

W dotychczasowych rozważaniach omawialiśmy przypadek linii dwutorowych i (poza jednym przykładem) wszystkie odcinki pojedynczego toru w obrębie rozjazdu były jednokierunkowe. Być może Czytelnik Obeznany z Teorią Grafów dostrzegł, że problem optymalnego rozjazdu pełnego można w takim przypadku stosunkowo łatwo wyrazić w języku grafów skierowanych, nakładając odpowiednie ograniczenia na stopnie wierzchołków oraz żądając istnienia odpowiednich skierowanych ścieżek pomiędzy liśćmi. Istnieją jednak również linie jednotorowe, po których odbywa się ruch wahadłowy. W tym przypadku ściśle formalny opis problemu optymalnego rozjazdu pełnego byłby nieco bardziej skomplikowany. Ze względu na szczególne własności zwrotnic nie wystarczy mówić o skierowaniu krawędzi. Poszukiwanie eleganckiego formalizmu pozostawiam Czytelnikom Zmotywowanym. Wykazanie, że pełny rozjazd linii jednotorowych w n kierunkach ($n \geq 3$) wymaga użycia co najmniej n zwrotnic, jest bardzo podobne do przedstawionych rozważań na temat linii dwutorowych. Optymalne rozjazdy w tym przypadku również nie wydają się atrakcyjną propozycją dla projektantów rzeczywistych torowisk.



Rys. 8



Rys. 9

Ciekawie robi się, gdy rozważamy pełny rozjazd pewnej liczby linii dwutorowych i pewnej liczby linii jednotorowych. W rzeczywistości, gdy linię jednotorową należy połączyć z linią dwutorową w dwóch kierunkach, projektanci torowisk zwykle sięgają po rozwiązania wymagające siedmiu zwrotnic, takie jak na rysunkach 8 i 9. Wiedząc, jak wygląda optymalny pełny rozjazd dla linii dwutorowych w trzech kierunkach, łatwo domyślamy się, jak rozwiązać ostatni problem przy użyciu pięciu zwrotnic. Tu może pojawić się pytanie, czy to „najlepsze”, co da się wymyślić? Czy połączenie pięciu pojedynczych torów może być „trudniejsze” od połączenia sześciu? Okazuje się, że tak! Ten „paradoks” wynika z istotnej różnicy pomiędzy torem dwukierunkowym a jednokierunkowym.

Podobnie jak poprzednio możemy przeanalizować sumę stopni wierzchołków schematu i zauważyć, że tym razem zwrotnic musi być nieparzyście wiele. Może wystarczą trzy? Bazując na wcześniej opisanym rozumowaniu na temat usuwania torów i zwrotnic, możemy stwierdzić, że po usunięciu jednego z dwutorowych odcinków (załóżmy, że chodzi o wjazd/wyjazd ze wschodu) pozostały układ torów nadal będzie umożliwiał przejazd z nieusuniętej linii dwutorowej na jednotorową w obu kierunkach ($W \rightleftharpoons S$). Procedura wiązałaby się z usunięciem co najmniej dwóch zwrotnic. Gdyby początkowy pełny rozjazd zawierał tylko trzy zwrotnice, po wspomnianym demontażu pozostałaby dokładnie jedna. Łatwo zauważyć, że wygląd takiego jednozwrotnicowego rozjazdu jest wyznaczony jednoznacznie.

Gdybyśmy z początkowego układu o trzech zwrotnicach usunęli tylko jeden jednokierunkowy wylot, musiałyby pozostać dwie zwrotnice i taki układ umożliwiałby przejazd w czterech relacjach ($W \rightleftharpoons S$, $E \rightarrow S$ oraz $W \leftarrow E$). Ponadto od tego momentu demontaż jednej zwrotnicy (i odpowiedniego odcinka toru) prowadzi do wspomnianego wcześniej prostego połączenia linii dwutorowej w jednotorową. Gdy jednak rozważymy każdą ze stosunkowo niewielu możliwości rozbudowy układu z jedną zwrotnicą, okaże się, że żadna nie pozwala na przejazd w oczekiwanych czterech relacjach. Otrzymujemy więc, że początkowy układ z trzema zwrotnicami nie mógł być pełnym rozjazdem.

Przedstawione rozważania nie są ściśle formalne, a przydatność uzyskanych wyników może się wydawać

wątpliwa. Jest w tym jednak pewien powtarzający się w historii matematyki wzorec, gdy obserwacje rzeczywistości prowadzą do nietrywialnych uogólnień. Być może przedstawione tu podwaliny *teorii torowisk* (?) są jednostkową ciekawostką dla miłośników matematyki rekreacyjnej (i/lub komunikacji miejskiej), a może znajdzie się śmiałek chętny kontynuować badania na tym polu? Można zastanowić się nad liczbą koniecznych skrzyżowań, rozważać rozjazdy z różnorodną liczbą wjazdów i wyjazdów albo zwrócić uwagę na obciążenie/przepustowość (tu można np. zastosować osiągnięcia teorii sieci przepływowych) poszczególnych odcinków toru przy ustalonym (choćby równomiernym) wykorzystaniu wszystkich relacji... Matematyka jak każda inna.

„Ciemność widzę, widzę ciemność!”, czyli o ciemnej materii słów kilka

* Centrum Fizyki Teoretycznej PAN

Wojciech A. HELLWING*

Współczesna kosmologia i astrofizyka oparte są na modelu Wszechświata, w którym około 30% całej gęstości energii przypada na materię niebarionową, czyli egzotyczną formę materii, zwaną ciemną materią (CM). Jest jej około 6 razy więcej niż zwykłej materii barionowej, czyli takiej, z jakiej składają się nasze ciała, planety, gwiazdy i mgławice. W tym artykule postaram się przybliżyć obecny status i prognozy na przyszłość jakże pasjonującego problemu ciemnej materii.

Co mówią niebiosa?

Obserwacyjne przesłanki za ciemną materią

Idea, że w naszym kosmosie jest o wiele więcej materii nieświecącej oraz że występuje ona w postaci egzotycznych cząstek, dojrzała w umysłach uczonych bardzo długo. Jednak gwałtowny rozwój technik obserwacyjnych w astronomii pozagalaktycznej, jaki miał miejsce w ciągu ostatnich kilku dekad, dostarczył nam tak wielu przesłanek obserwacyjnych istnienia ciemnej materii, że obecnie niebarionowa ciemna materia jest powszechnie akceptowanym składnikiem standardowego modelu kosmologicznego. Model ten to spójny obraz opisujący Wszechświat i jego ewolucję, od skal subatomowych do horyzontu Hubble’a oraz od ułamków sekundy po Wielkim Wybuchu do czasów obecnych – prawie 14 miliardów lat później. Kluczowe dla rozwoju idei ciemnej materii były obserwacje gromad galaktyk i zaskakujący problem brakującej masy w zewnętrznych częściach galaktyk spiralnych. Obecnie bardzo silne przesłanki o istnieniu ciemnej materii pochodzą z pomiarów obejmujących znacznie szersze skale czasowe i przestrzenne.

Chyba najsilniejszego argumentu dostarczają nam obserwacje mikrofalowego promieniowania relikowego, czyli mikrofalowej poświaty, jaka dotrwała do naszych czasów, a która pochodzi z epoki, gdy kosmos był młody i gorący. Analiza fluktuacji temperatury promieniowania relikowego na sferze niebieskiej ujawniła szereg charakterystycznych skal, dla których pojawiają się maksima. Za piki te odpowiadają oscylacje akustyczne w gorącej zupie pierwotnej plazmy, promieniowania i ciemnej materii, która wypełniała Wszechświat, gdy ten był bardzo młody. Okazuje się, że prosta fizyka oscylacji akustycznych w plazmie przewiduje, jak na rozmiary oraz amplitudę tych pików wpływają dwa podstawowe, a niezależne od siebie czynniki: ilość materii barionowej we Wszechświecie oraz całkowita ilość materii we Wszechświecie. Obserwatoria kosmiczne, takie jak COBE, WMAP i Planck, dostarczyły nam tak dokładnych pomiarów fluktuacji promieniowania tła, że z obserwowanej zależności pozycji i amplitudy maksimów akustycznych z bardzo dużym statystycznym prawdopodobieństwem (40 sigma!) wynika, że w młodym Wszechświecie było 6 razy więcej całkowitej materii niż materii barionowej, a zatem wskazują na $\Upsilon = 7$

uśrednione dla całego Kosmosu (Υ to tzw. *stosunek masy do światła*, o którym pisałem w poprzednim numerze, czyli z grubsza stosunek całkowitej masy do masy materii barionowej).

Inne silne dowody na istnienie niebarionowej ciemnej materii dostarcza nam Ogólna Teoria Względności. OTW przewiduje istnienie takiego zjawiska jak soczewkowanie grawitacyjne, gdzie masywne ciało (jak np. gromada galaktyk lub duża galaktyka eliptyczna) powoduje na tyle mocne zniekształcenie czasoprzestrzeni, że bieg promieni świetlnych w okolicach takiego obiektu ulega zakrzywieniu. W konsekwencji obserwator może rejestrować zniekształcone i wzmocnione obrazy galaktyk tła znajdujących się daleko za taką „soczewką”. Takie zjawiska nazywamy silnym soczewkowaniem grawitacyjnym. Słabe soczewkowanie, w odróżnieniu od silnego, polega na bardzo niewielkich zniekształceniach obrazów odległych galaktyk tła przez materię zgromadzoną na wielkich skalach w kosmicznych strukturach pomiędzy tłem a obserwatorem. Efekty silnego soczewkowania możemy rejestrować dla pojedynczych obrazów i pojedynczych soczewek, zaś efekty słabego soczewkowania są mierzalne dopiero po uśrednieniu efektu z obrazów setek lub nawet tysięcy galaktyk tła. Liczne silne soczewki, jakie obserwujemy, umożliwiają nam oszacowanie na Υ od 10 do 100 w galaktykach i $\Upsilon \sim 10$ w gromadach galaktyk, zaś pomiary słabego soczewkowania sugerują $\Upsilon = 7$ dla wielkoskalowej struktury.

Soczewkowanie grawitacyjne pozwala na relatywistyczne oszacowanie całkowitej masy. W przypadku wielu gromad galaktyk otrzymujemy również pomiary temperatury gorącego zjonizowanego gazu znajdującego się pomiędzy galaktykami. Gaz ten rozgrzany przez ściskające działanie grawitacji gromady emituje promieniowanie rentgenowskie. Jeżeli gaz pozostaje w równowadze z resztą gromady, to jego temperatura zależy od całkowitej grawitacji (a więc i masy) gromady. Dodając do tego informację o dyspersji prędkości składników gromady, możemy porównać wszystkie trzy niezależne oszacowania całkowitej masy grawitującej. W przypadku większości znanych gromad, co do których dysponujemy pomiarami pozwalającymi dokonać oszacowania masy wszystkimi trzema metodami, obserwacje znowu wskazują na $\Upsilon \sim 10$, a zatem na istnienie ciemnej materii.

Kolejny istotny pośredni dowód na istnienie ciemnej materii w postaci innych cząstek niż dobrze znane nam bariony pochodzi z rozważań dotyczących pierwotnej obfitości pierwiastków lekkich (głównie takich jak Deuter, Hel-3, Hel-4 i Lit-7). Pierwiastki lekkie, do Berylu włącznie, powstały w ciągu pierwszych trzech minut po Wielkim Wybuchu w procesie tzw. pierwotnej nukleosyntezy. Wszystkie cięższe pierwiastki powstały znacznie później w procesach związanych z ewolucją gwiazd (z wyjątkiem oczywiście Helu-4, który jest nieustannie syntezowany w jądrach gwiazd ciągu głównego). Mierząc obfitość tych lekkich pierwiastków w jałowej materii międzygalaktycznej, można dość dokładnie oszacować, jaka była obfitość pierwotna. Okazuje się, że obserwowane obfitości nakładają bardzo silne ograniczenia na ogólną liczbę nukleonów, które mogą istnieć we Wszechświecie. Najnowsze pomiary wskazują, że całkowity wkład do gęstości Wszechświata od nukleonów nie może przekraczać 5%, co w zestawieniu z tym, że szacunkowa całkowita ilość materii (np. wynikająca z pomiarów fluktuacji promieniowania tła) daje wkład około 35%, znowu kieruje nas do konstatacji, że musi istnieć około 6 razy więcej ciemnej materii niż materii zawartej w nukleonach.

W końcu jeszcze jedną bardzo ważną przesłanką na korzyść hipotezy ciemnej materii, jaką warto tutaj przytoczyć, są obserwowane własności wielkoskalowej struktury Wszechświata. Wcześniej dyskutowane obserwacje albo dotyczyły skal galaktyk i ich gromad, które są małe, jeżeli zestawione z rozmiarami całego Wszechświata, albo wczesnych etapów jego ewolucji. Toteż pomiary ewolucji i własności struktury, w jaką układają się galaktyki w największych skalach, uzupełniają nam ważną lukę w skalach czasowych i przestrzennych, z których czerpiemy argumenty za istnieniem ciemnej materii. Gdy zestawimy ze sobą obserwowaną obfitość galaktyk, fakt ich układania się w strukturę wielkiej pajęczyny (tzw. kosmiczną sieć) oraz prędkości, z jakimi galaktyki pola (czyli te, które nie należą do żadnych gromad) poruszają się w Kosmosie, dojdziemy do wniosku, że wszystkie te obserwacje dają się wyjaśnić tylko wtedy, gdy przyjmiemy, że wkład CM do całkowitej gęstości energii Wszechświata jest na poziomie 20–40%. Uwzględniając niepewność tych pomiarów, wynik ten doskonale zgadza się z ilością ciemnej materii, na jaką wskazują wszystkie poprzednio wspomniane obserwacje.

Co w detektorze piszczy?

Detekcja ciemnej materii, stan obecny

Naukowcy na przestrzeni lat zaproponowali wiele hipotez dotyczących fizycznej natury ciemnej materii. Po drodze udało się wykluczyć, że za ciemną materię mogą odpowiadać „kosmiczne śmieci”, czyli gruz w postaci roju małych planet, gwiazd i asteroid. Tutaj niepoślednią rolę odegrał polski program OGLE (*The Optical Gravitational Lensing Experiment*, Eksperyment Soczewkowania Grawitacyjnego). Ciemną materię

nie okazały się też kosmiczne neutrino. Mimo że cząstki te mają wszystkie pożądane cechy kandydata na ciemną materię, ich masa spoczynkowa jest za mała, by odpowiadać za więcej niż zaledwie 3% całej CM. Nie udało się też wyjaśnić zagadki brakującej masy za pomocą różnych propozycji zmieniających prawa fizyki, takich jak np. słynna hipoteza MOND (*MOdified Newtonian Dynamics*). MOND działał nieźle na skalach galaktycznych, ale nie był w stanie wyjaśnić ani własności mikrofalowego promieniowania tła, ani dynamiki gromad galaktyk bez dodatkowej ciemnej materii. W końcu i hipoteza o tym, że za ciemną materię odpowiada wielka liczba pierwotnych czarnych dziur, które są reliktem z czasów młodości Wszechświata, również nie przetrwała próby czasu.

Jak więc wygląda obecnie sytuacja? Otóż w ramach standardowego modelu kosmologicznego, Λ -CDM, przyjmuje się, że za ciemną materię odpowiadają nieodkryte jeszcze cząstki elementarne, tzw. WIMP-y (*Weakly Interacting Massive Particle*), czyli oddziałujące słabo jądrowo masywne cząstki. Od lat najpoważniejszym kandydatem są tzw. neutralina, tj. cząstki pojawiające się w teorii supersymetrii, złożone ze zmieszanych supersymetrycznych odpowiedników fotonu, bozonu Z i dwóch skalarnych bozonów Higgsa. Takie hipotetyczne neutralina mogły powstać we wczesnym Wszechświecie jako produkt uboczny pierwotnej kipieli termicznej – w obfitości odpowiedniej, by być idealnym kandydatem na tzw. zimną ciemną materię.

Alternatywą dla supersymetrycznych neutralin jest sterylne neutrino. To też WIMP, ale nie wymaga wprowadzenia supersymetrii. Cząstka taka pojawia się w minimalnym rozszerzeniu modelu standardowego cząstek elementarnych. Sterylne neutrino byłoby znacznie lżejsze od neutralin, ale wciąż tysiącrotnie masywniejsze niż zwykłe neutrino. Z uwagi na swoją małą masę taka cząstka byłaby kandydatem na ciepłą ciemną materię. Detekcja sterylnego neutrino w ziemskich warunkach jest bardzo trudna, a to z uwagi na fakt, że te hipotetyczne cząstki poza grawitacją oddziałują nieznacznie tylko z pozostałymi neutrinami, ignorując całą resztę cząstek elementarnych.

Zimna, ciepła czy gorąca? Nierelatywistyczne vs Relatywistyczne prędkości resztkowe. Ciemna materia jako taka nie oddziałuje z materią normalną w zwykły sposób, toteż gdybyśmy do wiadra pełnego ciemnej materii wsadzili zwykły termometr, to nie pokazałby on wcale jej temperatury. Mówiąc o ciemnej materii *gorąca* lub *zimna*, mamy na myśli to, jak duże są prędkości resztkowe cząstek danego typu CM. Jeżeli ciemna materia powstała w młodym, gęstym Wszechświecie, kiedy znajdowała się z resztą Wszechświata w równowadze termodynamicznej, to do dzisiaj jej cząstki zachowałyby charakterystyczne prędkości resztkowe związane z temperaturą, jaką miał Kosmos, gdy ciemna materia powstawała. Jeżeli cząstki ciemnej materii są lekkie, to oddzieliły się od reszty pierwotnej zupy, kiedy Wszechświat był jeszcze bardzo gorący, i zachowały duże prędkości resztkowe (porównywalne z prędkością światła). O takiej ciemnej materii mówimy, że jest *gorąca* (są nią np. kosmiczne neutrino). Jeżeli cząstki CM są bardzo masywne (jak np. WIMP-y), to oddzieliłyby się od kosmicznej zupy znacznie później, gdy Wszechświat zdążyłby nieco ostygnąć. Taka ciemna materia ma bardzo małe prędkości resztkowe (rzędu m/s) i mówimy, że jest *zimna*. Pomiędzy tymi dwoma scenariuszami znajduje się całe spektrum innych możliwości. Na przykład sterylne neutrino nazywane są ciepłą ciemną materią, gdyż spodziewamy się, że ich prędkości resztkowe są znacząco większe niż w przypadku WIMP-ów.

W latach 80. XX wieku siła i jakość argumentów obserwacyjnych wysuwanych przez astronomów spowodowały, że fizycy cząstek zaczęli na poważnie brać pomysł istnienia niebarionowej ciemnej materii. Od tamtego czasu fizycy przeprowadzają różne eksperymenty, których celem jest bezpośrednia detekcja cząstki CM na Ziemi. Idea detekcji ciemnej materii w laboratorium opiera się na zasadzie, jaką stosuje się, obecnie już rutynowo, dla zwykłych neutrin. Otóż oczekujemy, że cząstki ciemnej materii z halo Drogi Mlecznej, przelatujące nieustannie przez Ziemię, od czasu do czasu zderzać się będą elastycznie z jądrami ziemskich atomów. Takie zderzenia powodują efekt odrzutu jądra (gdyż część pędu cząstki CM jest przekazana jądru). Choć energia tego zjawiska jest bardzo mała, to przy odpowiedniej konstrukcji detektora jest możliwa do zaobserwowania. Spotykamy się powszechnie z czterema typami detektorów ciemnej materii: kryształowe detektory kriogeniczne, scyntylatory gazów szlachetnych, scyntylatory krystaliczne i komory pęcherzykowe. Stosowane tutaj techniki są bardzo różne, lecz we wszystkich detektorach kluczem do sukcesu jest odpowiednie poznanie szumu, który produkuje sygnał tła. Ponieważ spodziewamy się, że zderzenia cząstek CM z jądrami zachodzą bardzo rzadko, to w ziemskich laboratoriach dominującym sygnałem jest statystyczne tło. Czulość takich detektorów zależy również od własności fizycznych kandydata na cząstkę ciemnej materii. Chodzi tutaj głównie o masę spoczynkową, ale ważne jest również, czy w zderzeniach z jądrami istotny jest spin cząstek CM. Dotychczas żaden spośród bardzo wielu eksperymentów nie potwierdził bezpośredniej detekcji ciemnej materii. Wiele wstępnie pozytywnych wyników później zweryfikowano jako sygnały pochodzące od słabo rozpoznanego tła. Jedynym wyjątkiem jest wieloletni program DAMA/NaI i DAMA/Libra, w którym czulość na detekcję jest stosunkowo mała, ale sygnał jest całkowany względem czasu. W tym podejściu szuka się rocznej modulacji w sygnale, która powinna pojawiać się na skutek poruszania się Ziemi dookoła Słońca i Słońca dookoła centrum Galaktyki. Tło pochodzące z ziemskich źródeł nie powinno podlegać takiej rocznej zależności. Toteż można spodziewać

się, że obserwowana modulacja z roczną częstością powinna pochodzić od sygnału pozaziemskiego, czyli od halo ciemnej materii, w którym porusza się Ziemia. W ciągu ostatnich dwóch dekad obserwacji eksperymenty DAMA rzeczywiście zanotowały taki sygnał o rocznej częstości. Interpretacja, że źródłem sygnału DAMA jest ciemna materia, stoi jednak w sprzeczności z brakiem bezpośredniej detekcji we wszystkich pozostałych eksperymentach. Dlatego kwestia ta jest wciąż przedmiotem żywej debaty uczonych.

W czasie gdy w ziemskich laboratoriach fizycy polują na nieuchwytnie cząstki ciemnej materii, swojej broni nie złożyli jeszcze astronomowie. Okazuje się bowiem, że zarówno neutralina, jak i sterylne neutrino mogą nam dać o sobie znać za pomocą sygnałów z obiektów astrofizycznych. Neutralina są swoimi własnymi antycząstkami, a zatem ulegają same ze sobą procesowi anihilacji, w którym emitują kwant promieniowania gamma. Taki sygnał jest proporcjonalny do kwadratu gęstości neutralinowej ciemnej materii, a więc byłby możliwy do wykrycia tylko z najbardziej centralnych obszarów halo ciemnej materii. Tylko środek halo naszej własnej Drogi Mlecznej oraz kilka galaktyk satelitarnych są na tyle blisko, by móc oczekiwać rejestracji takiego sygnału. Nasze orbitalne teleskopy gamma (takie jak FERMI-sat) wciąż go poszukują. Niestety są inne astronomiczne obiekty, które mogą imitować sygnał gamma od anihilacji neutralin. Mowa tutaj na przykład o dużej populacji gwiazd neutronowych. Toteż wyłuskanie czystego sygnału gamma od ewentualnej ciemnej materii z tła astrofizycznego jest nie lada problemem. Podobnie sprawa ma się w przypadku sterylnego neutrino. Ta cząstka nie ulega samoanihilacji, ale jest niestabilna i rozpada się, emitując foton promieniowania rentgena. Sygnał pochodzący od tego typu rozpadów byłby proporcjonalny do gęstości ciemnej materii. Obecnie również trwają poszukiwania śladów takich sygnałów i chociaż pojawiały się doniesienia o zaobserwowaniu sygnałów z kierunku galaktyki w Andromedzie czy Gromady w Perseuszu, to wciąż trwa debata, czy sygnały te pochodzą z rozpadu ciemnej materii, czy od zwyczajnych obiektów astrofizycznych.

Dlaczego to jest istotne?

Wiedza o fizycznej naturze i elementarnych własnościach cząstek ciemnej materii jest kluczowa dla lepszego poznania i zrozumienia procesów rządzących powstawaniem struktur i galaktyk w Kosmosie. Bez konkretnej wiedzy o CM nie sposób zrozumieć, w jakiej części za ewolucję i powstawanie galaktyk odpowiadają skomplikowane procesy związane z powstawaniem gwiazd i ewolucją gazowego ośrodka międzygwiazdowego, a w jakiej bardziej fundamentalne prawa fizyki (np. teoria grawitacji) i sam model kosmologiczny, który opisuje cały Wszechświat. Gdybyśmy znali dokładnie własności ciemnej materii na poziomie kwantowym i cząsteczkowym, to wtedy można by przewidzieć, jak jej własności powinny manifestować się w obserwowanych cechach oraz w ewolucji galaktyk i ich satelitów. Byłby to wówczas bardzo poważny test całej naszej wiedzy o fizyce powstawania galaktyk i o ewolucji Wszechświata. Dobrze też byłoby w końcu wiedzieć, z czego tak naprawdę składa się 6/7 masy grawitującej we Wszechświecie!

Do czego służą zęby?

Pytanie tytułowe brzmi głupio, a odpowiedź wydaje się oczywista. Przeżywalimy, raczej nieświadomie (nasza mama bardzo świadomie), „wyrzynanie się” zębów mlecznych, które po kilku latach uległy wymianie (raczej bezboleśnie) na nowe, stałe. Każdy posiłek rozpoczyna się od zębów. Mają prawo się zużywać. Te stałe są w naszym życiu OSTATNIE! Zatem czekają nas wizyty u dentystów, a w końcu i u protetyka. Mosty, protezy, implanty... Po drodze dużo bólu i komplikacji. Czy współczesna nauka potrafi coś dla tego finalnego etapu zrobić?

Krokodyle zmieniają zęby 50 razy w życiu, dzięki komórkom macierzystym znajdującym się w zębach tych kręgowców. U ludzi komórki macierzyste znajdują się głównie w zębach mlecznych, w zębach stałych jest ich mniej i ich liczba z wiekiem maleje. Pobrane komórki można przechowywać w regulowanych warunkach: w temperaturze -190°C , do 25 lat. Już dziś można by zaprojektować i skonstruować za pomocą drukarki 3D biokompatybilne rusztowanie i na nim osadzić komórki macierzyste. Ze szkliwem musieliby sobie poradzić inni bioinżynierowie, wykorzystując białka, które wspierają tworzenie uporządkowanej mineralnej struktury. Ta wiadomość zainteresuje na pewno zgrzytających zębami albo ze szkliwem wrażliwym na kwasy.

Zęby z rozwijającą się próchnicą nie są zdolne do autoregeneracji. Ale u myszy, którym podano jeden z leków stosowanych w leczeniu choroby Alzheimer'a, zęby zdrowiały. Ostrzegam: do zastosowań u ludzi – droga daleka.

Umiemy już w pewnych przypadkach sterować regeneracją kości, korzystając z wytworzonych w laboratoriach materiałów kościotwórczych. Obecnie stosuje się już także wydzieloną z krwi pacjenta fibrynę, co pozwala zmniejszyć stan zapalny po poważniejszych zabiegach w jamie ustnej.

Cierpiących na choroby uzębienia może zainteresuje (jeżeli nie pocieszy) informacja, że badania archeologiczne zębów przyczyniły się znacznie do wzbogacenia wiedzy o historii naszego gatunku oraz o chorobach trapiących ludzi przez tysiąclecia. Zęby przez setki i tysiące lat mogą zachować DNA właściciela, a także DNA obecnych w jego ciele bakterii. Tak właśnie zainteresowano się DNA bakterii *Yersinia pestis*, powszechnie znajdowanymi w zębach ofiar dżumy. Badano cmentarzyska z epoki Justyniana (Konstantynopol, V do VII wiek n.e.), średniowiecza (cała Europa) i z drugiej połowy XIX wieku (w Chinach).

Uczeni z Uniwersytetu w Kopenhadze przeanalizowali 89 mld fragmentów DNA z zębów 101 osób pochowanych w epoce brązu – u siedmiu z nich znaleziono DNA *Y. pestis*. W innych badaniach przeanalizowano bakteryjny DNA z tysięcy cmentarzy średniowiecznych w Europie. Z porównań genomów współczesnych bliskich gatunkowo bakterii wysnuto wniosek, że współczesna *Yersinia* pochodzi od przodka żyjącego 5783 lata temu, co przesuwają w głąb historii dotychczasowe oceny czasu jej występowania. Już te starożytne szczepy noszą podstawowe geny wirulencji, czyniące bakterię niebezpieczną i wysoce zjadliwą. W europejskich okresach zabijała ona do 50% ludności. Oczywiście nie znano wówczas czynnika sprawczego – z wydziału medycyny w Paryżu wysłano list do króla upatrujący źródła zarazy w koniunkcji trzech planet (1345 r.). Dziś wiemy, że bakterie przenoszone były przez pchły ze szczurów, które gnieździły się na statkach handlowych. Znaczenie higieny dla zdrowia zostało dostrzeżone dopiero w XIX wieku, a bakterię *Y. pestis* wyizolowano w Hongkongu w 1894 roku. Nazwana została imieniem odkrywcy, bakteriologa Alexandra Yersina, który wytworzył również pierwszą szczepionkę.

Współczesna dżuma dymienicza nieleczone kończy się w 80% przypadków śmiercią w ciągu ośmiu dni. Śmiertelność nieleczonych ofiar dżumy płucnej wynosi 90–95%. Bakterie-sprawcy wrażliwe są na cefalosporyny III generacji, gentamycynę, ciprofloksacynę i tetracykliny; istnieją także szczepionki oparte na osłabionych szczepach *Yersinii*.

Magdalena FIKUS

A jednak się da (IX), czyli saga kryptologiczna w odcinkach. Tym razem: o obliczeniach wielopodmiotowych.

Tomasz KAZANA

Niniejszy odcinek jest ostatni z serii. Przez niemal rok, wraz z Łukaszem Rajkowskim, próbowaliśmy pokazać Czytelnikowi, co ciekawego, a przede wszystkim – co zaskakującego, wiąże się z kryptologią. Naszą wielką nagrodą będzie, gdy – po przeczytaniu tych 9 odcinków – choć niewielka część Czytelników chociaż przez chwilę zawaha się, gdy w życiu codziennym będzie stwierdzać, że **czegoś się nie da...**

Punktem wyjścia naszych rozważań będzie podział sekretu pomiędzy n osób (o którym pisaliśmy więcej w Δ_{11}^2). To znaczy: założmy, że chcemy pewną tajną liczbę

$$x \in \{0, 1, \dots, p-1\}$$

(p to pewna ustalona duża liczba pierwsza, np. $p=19134702400093278081449423917$) rozproszyć pomiędzy zbiór osób $A = (A_1, \dots, A_n)$ w taki sposób, aby:

- każda z nich dostała pewien udział w postaci liczby $x_i \in \{0, \dots, p-1\}$, oraz
- dowolna ich t -osobowa podgrupa nie była w stanie odtworzyć x (analizując swoje udziały), ale już (każda) podgrupa $(t+1)$ -osobowa zawsze mogła to zrobić.

Powyższy problem da się rozwiązać dla dowolnego $0 \leq t \leq (n-1)$, szczególnie znajdują się w artykule cytowanym wyżej. Ogólna idea (pochodząca od Adiego Shamira) polega na tym, że losujemy dowolny wielomian w stopnia t (o współczynnikach $w_i \in \{0, \dots, p-1\}$) o wyrazie wolnym równym x . Następnie ustalamy dowolne niezerowe (i parami różne) elementy y_i i określamy

$$x_i := (w(y_i) \bmod p).$$

Okazuje się, że tak zdefiniowane udziały spełniają nasze pierwotne założenia. Dziś jednak będziemy chcieli osiągnąć znacznie więcej. To znaczy, zapagniemy na podzielonych sekretach rachować!

Przyjmijmy, że sekrety są dwa: $a, b \in \{0, \dots, p-1\}$ oraz że osoba o numerze i ma udziały w obu (w postaci liczb $a_i, b_i \in \{0, \dots, p-1\}$). Chcemy teraz opracować taki *protokół*, który umożliwi wszystkim n osobom dokonanie wspólnych obliczeń, po których osoba i otrzyma pewną wartość c_i . Oczekujemy, że tak obliczone elementy $\{c_i\}_{1 \leq i \leq n}$ razem będą stanowić podział sekretu dla (rozważamy trzy przypadki):

1. $c = a + b \pmod{p}$;
2. $c = k \cdot a \pmod{p}$ (k jest publicznie znaną stałą);
3. $c = a \cdot b \pmod{p}$.

Prezentowane w tym artykule protokoły są bezpieczne w modelu pasywnym, tzn. zakładamy, że uczestnicy nie oszukują (nie wysyłają niepoprawnych komunikatów), a są tylko ciekawscy i chcieliby – z tego co legalnie widzą – wywnioskować więcej, niż być może powinni (mogą również działać w porozumieniu). Dodatkowo musimy założyć $t < n/2$ oraz przyjąć, że co najwyżej t uczestników jest w znowie. W przypadku przeciwników aktywnych (oszukujących podczas protokołu) istnieją inne – bardziej skomplikowane – protokoły, które potrafią zapewnić bezpieczeństwo, gdy oszustów jest mniej niż $n/3$.

Banalne rozwiązanie polega na odtworzeniu a i b , obliczeniu c oraz dokonaniu nowego podziału, według oryginalnego protokołu. Nasz cel jest jednak ambitniejszy: chcemy rozproszyć c , ale w taki sposób, aby bezpośrednia informacja o a i b nie została na żadnym etapie przez nikogo (przez żadnego uczestnika bądź ich podgrupy o ograniczonej liczebności) jawnie odtworzona. Jak to zrobić?

Przypadek pierwszy i drugi jest łatwy (Zajmiemy się tylko pierwszym. Niech drugi pozostanie jako łatwe ćwiczenie.) i nie wymaga nawet żadnej komunikacji pomiędzy stronami. Wystarczy, że osoba i przyjmie $c_i := a_i + b_i \bmod p$ i wszystko będzie w porządku. Dlaczego? Przypomnijmy sobie tylko, czym jest a_i oraz b_i . Wiemy przecież, że

$$a_i = w_a(y_i) \pmod{p} \quad \text{oraz} \quad b_i = w_b(y_i) \pmod{p},$$

dla pewnych wielomianów w_a oraz w_b . Wtedy oczywiście

$$a_i + b_i = (w_a + w_b)(y_i) \pmod{p},$$

co oznacza, że (z definicji) elementy $a_i + b_i$ stanowią podział sekretu dla wyrazu wolnego wielomianu $(w_a + w_b)$ modulo p . Ten jednak wynosi $(a + b)$ modulo p , gdyż wyrazem wolnym w_a musi być a , a wyrazem wolnym w_b jest b .

Powyższe rozwiązanie rodzi pokusę, aby analogicznie rozwiązać przypadek trzeci. To znaczy, aby każda z osób przyjęła $c_i = a_i \cdot b_i \bmod p$, jako że $a \cdot b \pmod{p}$ jest wyrazem wolnym wielomianu $w_a \cdot w_b$ modulo p . Niestety, jest to rozwiązanie błędne. Problem bierze się stąd, że mnożenie dwóch wielomianów stopnia t

daje wielomian stopnia $2t$. A my przecież chcemy koniecznie otrzymać stopień t (w przypadku dodawania ten problem nie występował)! Rozwiązanie jest tutaj nieco bardziej skomplikowane.

Mnożenie podzielonych sekretów

Pierwszy krok jest taki sam, jak w naiwnym rozwiązaniu wyżej. To znaczy, faktycznie każdy z uczestników protokołu mnoży a_i przez b_i , otrzymując pewne g_i . Zanim przejdziemy do szczegółów kolejnego kroku, potrzebujemy jeszcze kilku oznaczeń. Oznaczmy więc wielomian $(w_a \cdot w_b)$ modulo p przez h . Wówczas wyraz wolny h to $a \cdot b$ modulo p (tak jak potrzeba), natomiast wartość $g_i = a_i \cdot b_i = w_a(y_i) \cdot w_b(y_i) = h(y_i) \pmod{p}$ jest znana osobie i . Problemem jest tylko stopień wielomianu

$$h(X) = (a \cdot b \pmod{p}) + h_1 \cdot X + h_2 \cdot X^2 + \dots + h_t X^t + \dots + h_{2t} X^{2t},$$

który wynosi $2t$. Wprowadźmy więc (trochę na siłę) nowy wielomian:

$$v(X) = (a \cdot b \pmod{p}) + h_1 \cdot X + h_2 \cdot X^2 + \dots + h_t X^t,$$

który powstał przez zwykłe wymazanie ostatnich t jednomianów wielomianu h . Byłoby oczywiście świetnie, gdyby osoba i potrafiła (za pomocą jakiegoś protokołu) po prostu bezpiecznie obliczyć wartość $v(y_i)$. Okazuje się, że jest to wykonalne! Co więcej, nie aż tak trudne obliczeniowo i nie wymaga dużej komunikacji między uczestnikami protokołu. Kluczowa jest tu (dość zaskakująca) obserwacja, że każde $v(y_i)$ jest kombinacją **liniową*** elementów $\{g_i\}_{i=1\dots n}$. Gdy już to wiemy, to dalej jest z górki. Dodawanie i mnożenie przez stałą sekretów potrafimy już wykonywać. Trzeba więc tylko rozproszyć każde g_i i zastosować (być może wielokrotnie) dwa proste przypadki rozważane wyżej (oraz na koniec wysłać osobie i odpowiednie udziały do odtworzenia $v(y_i)$). Dokładne wyjaśnienie, ze względu na techniczny charakter zagadnienia, musimy niestety pominąć. Wierzmy jednak, że dokładne odtworzenie wszystkich kroków tego przypadku może być bardzo pouczające. Szczegóły znajdują się w pracy „A Full Proof of the BGW Protocol for Perfectly-secure Multiparty Computation” autorstwa Gilada Asharova oraz Yehudy Lindella.

Po co to wszystko?!

Przyjmijmy, że każda z osób A_i wybrała swój własny argument $s_i \in \{0, \dots, p-1\}$ i rozproszyła go wśród wszystkich pozostałych osób. Co umożliwiającą nam protokoły naszkicowane wyżej? Otóż na pewno grupa może (wspólnie) obliczyć chociażby $s_1 + 3 \cdot s_7$ modulo p czy $s_2 + 23 \cdot s_1 \cdot s_3 \cdot s_5 + s_{100}^{44}$ modulo p (w taki sposób, że żadne obliczenia pośrednie nie są nikomu znane – wszak wszystko odbywa się dla rozproszonych wartości), bo potrafi dodawać, skalować przez stałą i mnożyć sekrety.

Jak wiele w taki sposób można policzyć? Okazuje się, że ... wszystko!

Obliczenia w *ciele modulo p* mają taką cechę, że każdą funkcję (oczywiście o zbiorze wartości $\{0, \dots, p-1\}$) da się zapisać jako wielomian, a więc jako złożenie (być może bardzo wielu) dodawań, skalowań przez stałą i mnożeń (wszystko modulo p). Innymi słowy: z faktu, że znamy protokoły dla trzech przypadków z pierwszej części artykułu, wynika, że potrafimy obliczyć zupełnie dowolną funkcję rozproszonych argumentów. Stąd już tylko krok do protokołów na np. granie w pokera przez Internet bez zaufanej strony czy bezpieczne aukcje internetowe bez serwera zbierającego i w zaufaniu porównującego oferty.

Science-fiction

Wyżej ledwie naszkicowaliśmy ideę obliczeń wielopodmiotowych (i to jeszcze w mniej ciekawym, bo pasywnym przypadku – szczegóły na jednym z marginesów). Póki co nie są one jeszcze bardzo praktyczne, ale powoli zbliżamy się do momentu, gdy (na razie) proste ich zastosowania będą możliwe do codziennego wykorzystania. Chcielibyśmy jednak mocno zaznaczyć, że drzemie w nich potencjał niemal rewolucyjny**.

Rozpraszanie obliczeń i przechowywanie danych czy ogólniej – pozbywanie się zaufanych stron z cyfrowego świata jest wszak (skromnym zdaniem autora tego tekstu) najważniejszym wyzwaniem rewolucji cyfrowej XXI wieku.

* Czytelnik zaznajomiony z algebrą liniową oraz z pojęciem macierzy Vandermonda powinien być w stanie odtworzyć odpowiednie przekształcenie liniowe. Nie twierdzimy jednak, że jest to zadanie bardzo łatwe.

Gdy piszemy *grupa obliczy* $q = f(s_1, \dots, s_n)$, to mamy na myśli, że każdy z uczestników protokołu po jego zakończeniu pozna pewne q_i takie, że wszystkie q_i razem stanowią podział q . Następnie wszyscy powinni upublicznić swoje q_i , aby każdy uczestnik mógł faktycznie poznać wartość q . Kluczową cechą tego protokołu jest, że rzeczywiście jedyną nową informacją na temat (s_1, \dots, s_n) , którą pozna każdy z jego uczestników, jest właśnie q . Wszelkie informacje pośrednie pozostaną tajne.

** Potencjał podobnego kalibru można wyczuć również w kilku innych pomysłach kryptologicznych, takich jak *blockchain*, *szyfrowanie homomorficzne* czy *dowody z wiedzą zerową*.

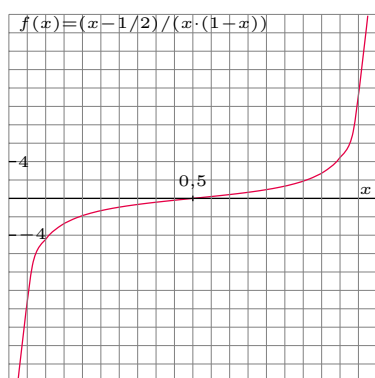


mała delta

Nieskończoność: 5. Zbiory duże

W poprzedniej części tej opowieści o nieskończonościach rozważaliśmy twierdzenie Cantora, które stanowi, że żaden zbiór A nie jest równoliczny ze zbiorem jego podzbiorów $P(A)$, co symbolicznie notujemy $|A| < |P(A)|$. Szczególnie zajmowaliśmy się przypadkiem, gdy A jest zbiorem liczb naturalnych $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.

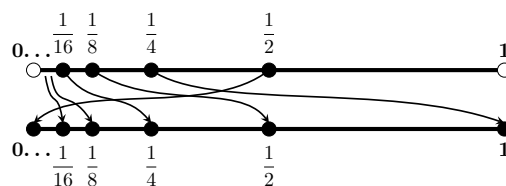
Studiowaliśmy także zbiór liczb całkowitych \mathbb{Z} oraz zbiór liczb wymiernych \mathbb{Q} , pokazując, że każdy z nich jest równoliczny ze zbiorem liczb naturalnych. Takie zbiory nazywane są zbiorami przeliczalnymi. Inaczej mówiąc, są to zbiory, których elementy można zakwaterować w hotelu Hilberta. Chociaż są nieskończone, to z naszej perspektywy wydają się relatywnie „małe”. Przynajmniej w porównaniu z innymi zbiorami, które rozważaliśmy. A były to: przedział $[0, 1]$, zbiór liczb rzeczywistych \mathbb{R} , zbiór wszystkich nieskończonych ciągów zero-jedynkowych oraz zbiór wszystkich podzbiorów zbioru liczb naturalnych $P(\mathbb{N})$. Wiemy, że żaden z nich nie jest równoliczny ze zbiorem liczb naturalnych. Są one ewidentnie „większe” – dla każdego ustawienia elementów dowolnego z tych zbiorów w parę z liczbami naturalnymi znajdowaliśmy element, który do żadnej pary nie trafił. Zauważyliśmy także, że zbiór wszystkich nieskończonych ciągów zero-jedynkowych oraz zbiór wszystkich podzbiorów zbioru liczb naturalnych $P(\mathbb{N})$ są równoliczne, ponieważ każdy podzbiór zbioru liczb naturalnych można ustawić w parę z ciągiem zer i jedynek, który go koduje. Wszystkie wymienione tu zbiory nazywa się zbiorami mocy continuum. Okazuje się bowiem, choć może być to z początku zaskakujące, że one też są parami równoliczne, czemu spróbujemy się teraz przyjrzeć dokładniej.



Jak zatem ustawić w parę elementy przedziału $[0, 1]$ ze wszystkimi liczbami rzeczywistymi? Prościej będzie na początku rozważyć przypadek przedziału otwartego $(0, 1)$, czyli przedziału wszystkich liczb większych od 0 i mniejszych od 1. Czytelnik, który miał do czynienia z funkcjami rzeczywistymi, znajdzie pewnie po chwili kilka sposobów takiego ustawienia liczb w parę. Na przykład, można liczbę x z przedziału $(0, 1)$ ustawić w parę z liczbą rzeczywistą $\frac{x-1/2}{x(1-x)}$. Rzeczywiście, dwóm różnym liczbom z przedziału $(0, 1)$ przyporządkujemy dwie różne liczby rzeczywiste i, co więcej, wszystkie liczby rzeczywiste zostaną wykorzystane, co doskonale ilustruje powyższy wykres funkcji $f(x) = \frac{x-1/2}{x(1-x)}$.

A zatem wiemy, że $|(0, 1)| = |\mathbb{R}|$. Musimy jeszcze wykazać, że $|(0, 1)| = |[0, 1]|$. Inaczej mówiąc, musimy ustawić w odpowiednie pary wszystkie liczby tych dwóch przedziałów tak, żeby uwzględnić dwie „dodatkowe” liczby (0 i 1) w jednym ze zbiorów. Zadanie to jest ładnym problemem kombinatorycznym, zachęcam więc Czytelnika do samodzielnego zastanowienia się nad nim przed analizą poniższego rozwiązania. Rozważmy pewien nieskończony ciąg liczb, na przykład $1/2^n$, dla $n = 1, 2, \dots$. Teraz, jeśli liczba x z przedziału $(0, 1)$ nie należy do tego ciągu, to ustawiam ją w parę z odpowiadającą jej tą samą liczbą x z przedziału $[0, 1]$. Kolejne liczby z wyróżnionego ciągu przesuwam o dwa miejsca (podobnie jak przesuwaliśmy gości w hotelu Hilberta), tak żeby pierwsze dwa wyrazy tego ciągu mogły być towarzyszami w parach z 0 i 1. To znaczy, $1/2$ z przedziału $(0, 1)$ ustawiam w parę z 0

z przedziału $[0, 1]$, $1/4$ – w parę z liczbą 1, $1/8$ – w parę z $1/2$, $1/16$ z $1/4$, itd. (patrz rysunek). Czyli dla $n > 2$ ustawiam $1/2^n$ w parę z $1/2^{n-2}$. Rzeczywiście, ustawiłem wszystkie liczby z przedziału $(0, 1)$ w parę z liczbami z przedziału $[0, 1]$, wykorzystując wszystkie liczby z obu przedziałów dokładnie raz. A zatem $|[0, 1]| = |(0, 1)| = |\mathbb{R}|$.



Najtrudniejsze zadanie przed nami. Musimy jeszcze wykazać, że liczb z przedziału $[0, 1]$ jest tyle samo, co nieskończonych ciągów zero-jedynkowych. Rozbijmy ten ostatni zbiór na dwie części: niech A będzie zbiorem tych nieskończonych ciągów zero-jedynkowych, które od pewnego miejsca mają już tylko jedynki, zaś B niech będzie zbiorem wszystkich pozostałych ciągów. Zatem zbiór wszystkich nieskończonych ciągów zero-jedynkowych to $A \cup B$. Wykażemy najpierw, że $|A \cup B| = |A \cup [0, 1]|$, czyli że zbiór wszystkich ciągów jest równoliczny ze zbiorem zawierającym wszystkie ciągi, w których od pewnego miejsca są same jedynki, oraz wszystkie liczby z przedziału $[0, 1]$.

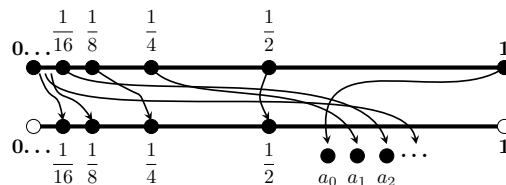
W tym celu musimy rozważyć zapis liczb rzeczywistych w systemie binarnym. Prawdopodobnie każdy Czytelnik zapisywał liczby naturalne w systemie dwójkowym,

np. 1011 w systemie binarnym to $1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 8 + 2 + 1 = 11$ w systemie dziesiętnym. Nie ma jednak żadnych przeciwwskazań, żeby system binarny stosować także po przecinku, np. 0,1011 w systemie binarnym to $1 \cdot 1/2 + 0 \cdot 1/4 + 1 \cdot 1/16 + 1 \cdot 1/32 = 19/32$. Co więcej, podobnie jak każda liczba rzeczywista ma (być może nieskończone) rozwinięcie dziesiętne, tak każdą liczbę rzeczywistą można zapisać w postaci rozwinięcia binarnego. Rozwinięcia skończone oczywiście możemy również napisać jako nieskończone, dodając na końcu same zera (0,1011 = 0,10110000...). Musimy jednak zauważyć, że podobnie jak w przypadku rozwinięć dziesiętnych, w których od pewnego momentu są same dziewiątki, jeśli w rozwinięciu binarnym od pewnego momentu są same jedynki, mamy do czynienia po prostu z liczbą, którą da się zapisać w skończonym rozwinięciu (na przykład w systemie dziesiętnym $0,49999\dots = 0,5$, w systemie binarnym $0,101111\dots = 0,11$). Inaczej mówiąc, rozwinięcie w takich przypadkach nie jest jednoznaczne. Wykluczmy więc z rozważań nieskończone rozwinięcia binarne posiadające od pewnego miejsca już same jedynki.

Powyższe rozważania definiują metodę ustawienia w pary elementów zbioru $A \cup B$ oraz $A \cup [0, 1)$. Każdą zero-jedynkowy ciąg, w którym od pewnego miejsca są same jedynki, stawiamy w parę z tym samym ciągiem. W każdym innym przypadku łączymy go w parę z liczbą z przedziału $[0, 1)$, której ten ciąg jest rozwinięciem binarnym (dopisujemy do ciągu zero i przecinek z lewej strony). W ten sposób rzeczywiście wykorzystamy wszystkie liczby, każdą jednokrotnie. Mamy więc $|A \cup B| = |A \cup [0, 1)|$.

Sprawdźmy teraz, że $|A \cup [0, 1)| = |[0, 1]|$, co zakończy nasze rozważania. W tym celu warto zauważyć, że wszystkie elementy zbioru A da się zakwaterować w hotelu Hilberta, to jest ponumerować liczbami naturalnymi. Wystarczy najpierw zakwaterować ciąg $a_0 = 111\dots$, potem ciąg $a_1 = 01111\dots$, potem dwa ciągi, w których ostatnie zero stoi na drugim miejscu (czyli $a_2 = 001111\dots$ i $a_3 = 101\dots$), następnie te ciągi, gdzie ostatnie zero jest na trzecim miejscu (jest ich cztery!), i tak dalej. Tak więc sporządziliśmy listę wszystkich nieskończonych zero-jedynkowych ciągów, w których od pewnego miejsca są same jedynki, $A = \{a_0, a_1, a_2, \dots\}$.

Wybermy zatem, podobnie jak poprzednio, ciąg liczb z przedziału $[0, 1]$ – niech to będzie $1/2^n$ dla $n = 0, 1, 2, 3, \dots$. Tym razem musimy poradzić sobie z „nadmiarem” nieskończonej liczby elementów, gdy będziemy łączyć w pary elementy zbioru $A \cup [0, 1)$ z liczbami z $[0, 1]$. Wykorzystajmy więc parzyste potęgi $1/2$, aby znaleźć towarzyszy do par dla tych „dodatkowych” elementów, zaś nieparzyste potęgi muszą nam starczyć jako towarzysze dla dotychczasowych liczb z wybranego ciągu. Zatem liczba x z przedziału $[0, 1]$ nie będąca elementem wybranego ciągu będzie w parze z tą samą liczbą x należącą do zbioru $A \cup [0, 1)$. Niech $1/2^0 = 1$ stanie w parze z ciągiem a_0 , ale $1/2^1 = 1/2$ niech stoi w parze z $1/2$ z $A \cup [0, 1)$. Następnie $1/2^2 = 1/4$ trafia do pary z a_1 , zaś $1/2^3$ do pary z $1/2^2$. I tak dalej. Inaczej mówiąc, dla każdego n , $1/2^{2n}$ z $[0, 1]$ stoi w parze z ciągiem a_n z $A \cup [0, 1)$, zaś $1/2^{2n+1}$ z $[0, 1]$ stoi w parze z liczbą $1/2^{n+1}$ z $A \cup [0, 1)$ (patrz rysunek). Udało się ustawić wszystko



w pary! A zatem $|[0, 1]| = |A \cup [0, 1)| = |A \cup B|$, czyli zbiór wszystkich liczb rzeczywistych z przedziału $[0, 1]$ jest równoliczny ze zbiorem wszystkich nieskończonych ciągów zero-jedynkowych. Wszystkie rozważane przez nas „duże” zbiory też okazały się parami równoliczne.

Mamy zatem w garści różne „małe” zbiory nieskończone, czyli zbiory przeliczalne: \mathbb{N} , \mathbb{Z} oraz \mathbb{Q} . Mamy także zbiory „duże”: \mathbb{R} , $[0, 1]$, $P(\mathbb{N})$ oraz zbiór wszystkich nieskończonych ciągów zero-jedynkowych. Wszystkie takie zbiory, które rozpatrywaliśmy, okazały się parami równoliczne. Zwane są zbiorami mocy continuum. Powstaje więc naturalne pytanie. Czy jest coś pomiędzy zbiorami przeliczalnymi a zbiorami mocy continuum? Czy istnieje zbiór o mocy większej niż moc zbiorów przeliczalnych, a mniejszej niż continuum?

Pytanie takie zadał sobie już Georg Cantor. Nie udało mu się skonstruować takiego zbioru, przypuszczał więc, że zbiór taki nie istnieje, i przez wiele lat swojego życia próbował to udowodnić. Nie był w stanie tego dokonać. Ta niemoc bardzo go frustrowała i dodatkowo źle wpływała na jego chwiejne zdrowie psychiczne. Teza Cantora, że nie istnieje zbiór o mocy większej niż moc zbiorów przeliczalnych, a mniejszej niż continuum, nazywa się hipotezą continuum. Problem zaciekał wielu matematyków, w tym Davida Hilberta, którego koncepcję nieskończonego hotelu już omawialiśmy. Na Kongresie Matematyków w Paryżu David Hilbert wygłosił referat, podczas którego przedstawił 23 matematyczne problemy (10 z nich zdążył przedstawić ustnie, a reszta pojawiła się w spisanej wersji referatu), jego zdaniem najbardziej interesujące, które powinny zostać rozwiązane w kolejnym stuleciu. Jaki był pierwszy wymieniony przez niego problem? Właśnie hipoteza continuum! Poniżej ten właśnie fragment spisanego już po samym Kongresie referatu Hilberta.

1. Cantors Problem von der Mächtigkeit des Continuum.

Zwei Systeme, d. h. zwei Mengen von gewöhnlichen reellen Zahlen (oder Punkten) heißen nach Cantor äquivalent oder von gleicher Mächtigkeit, wenn sie zu einander in eine derartige Beziehung gebracht werden können, daß einer jeden Zahl der einen Menge eine und nur eine bestimmte Zahl der anderen Menge entspricht. Die Untersuchungen von Cantor über solche Punkt-mengen machen einen Satz sehr wahrscheinlich, dessen Beweis jedoch trotz eifrigster Bemühungen bisher noch Niemanden gelungen ist; dieser Satz lautet:

Jedes System von unendlich vielen reellen Zahlen d. h. jede unendliche Zahlen- (oder Punkt)menge ist entweder der Menge der ganzen natürlichen Zahlen 1, 2, 3, ... oder der Menge sämtlicher reellen Zahlen und mithin dem Continuum, d. h. etwa den Punkten einer Strecke äquivalent; im Sinne der Äquivalenz gibt es hiernach nur zwei Zahlenmengen, die abzählbare Menge und das Continuum.

Czy ponad wiek później znamy odpowiedź na pytanie o hipotezę continuum? Jeśli tak, to jaka ona jest? Odpowiedzi na te pytania mogą być zaskakujące! Ale o tym następnym razem.

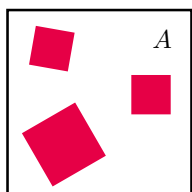
Michał KORCH



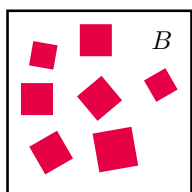
Liczenie na nosie

Sebastian OLEKSA*

Liczby przedstawiać można na wiele sposobów. Jako dzieci liczyliśmy na palcach czy używając patyczków lub liczydła. Ten sposób przedstawiania liczb – przez fizyczną liczbę pewnych obiektów – nazywany jest *kardynalnym*. Jest bardzo prosty: tworzy się słowo lub symbol oznaczające jeden, a następnie powtarza się odpowiednią ilość razy. Może się nam to skojarzyć na przykład z cyframi rzymskimi w zakresie od jeden do trzech (I, II, III), chociaż dalej już oczywiście nie. Przy liczbach większych sposób kardynalny jest niezwykle niepraktyczny, o czym łatwo się przekonać, próbując tak zapisać na przykład 100. Fachowo rzecz ujmując, nieefektywność tego systemu wiąże się z *subityzacją*. Jest to umiejętność oszacowania liczby widocznych elementów bez liczenia ich. Dla przykładu, chyba od razu widać, że na rysunku 1 są trzy kolorowe kwadraty. Jednakże stwierdzenie, ile kwadratów znajduje się na rysunku 2, zajmuje więcej czasu – trzeba je policzyć. Według badań, opublikowanych w 1995 roku przez Brytyjskie Stowarzyszenie Psychologiczne, ta umiejętność natychmiastowego stwierdzenia liczby elementów działa do około 5 elementów. Właśnie przez to ograniczenie system kardynalny jest stosowany jedynie w językach, których użytkownicy nie mają potrzeby opisywania większych liczb. Jest ich naprawdę niewiele.



Rys. 1



Rys. 2

Pozostałe języki używają drugiego sposobu opisywania liczb – systemu *ordynalnego*. Działa on tak, że wybranym liczbom przyporządkowuje się różne symbole, które je opisują. Oczywiście, nie moglibyśmy przyporządkować różnych symboli *wszystkim* liczbom. Pozostałe opisuje się, używając kombinacji wcześniej ustalonych symboli. To właśnie jest system liczbowy. Często jest on oparty na jednej liczbie, czyli podstawie. We wspomnianym wcześniej systemie kardynalnym podstawą jest jedynka. W systemie dwójkowym, używanym w informatyce, podstawa to liczba 2. Z kolei my używamy systemu dziesiętnego. Ale skąd wzięły się te liczby? Dlaczego akurat 10, a nie 11? Spróbujmy na to odpowiedzieć. Źródło jedynki jest dość oczywiste. Dwójka wynika ze sposobu przekazywania informacji w komputerze: albo prąd płynie, albo nie. Skoro możemy używać tylko dwóch „znaków”, to system musi być dwójkowy. W przypadku 10 najprawdopodobniej wyniknęło to z liczby palców u rąk człowieka. Do dziesięciu możemy policzyć na palcach, potem już nie. Bardzo podobne źródło mają systemy oparte na liczbie dwadzieścia, gdzie liczono zarówno palce rąk, jak i nóg. Właśnie liczba dwadzieścia pojawia się dość często, na przykład w kulturach Majów, Azteków i Celtów, czasem jedynie jako część, na przykład w języku mańskim (język Celtów, używany na wyspie Man).

Zapis liczb w języku mańskim jest podobny do zapisu liczb po polsku czy angielsku, z istotną różnicą związaną z dwudziestką. Liczby od 1 do 20 czyta się „normalnie”: 8 to *hocht*, 18 to *hocht-jeig*. Powyżej 20 przechodzimy natomiast na system „bardziej” dwudziestkowy: 28 to *hocht as feed*, czyli dosłownie osiem i dwadzieścia, 38 to *hocht-jeig as feed*, czyli osiemnaście i dwadzieścia, a 98 to *kiare feed as hocht-jeig*, czyli cztery dwudziestki i osiemnaście. Jest to dla mnie niezmiernie ciekawy sposób liczenia, gdyż nie jest do końca ani systemem dziesiętnym ani dwudziestkowym.

Innym niezwykłym językiem pod względem zapisu liczb jest Telefol. Nie jest to nazwa sieci komórkowej, a język używany przez około 5400 osób w Papui Nowej Gwinei. Jest wyjątkowy z wielu względów, ale przede wszystkim przez sposób liczenia. Otóż liczą oni w systemie dwudziestosiódemkowym. Na pierwszy rzut oka liczba 27 może się wydawać wzięta znikąd, a sam system bardzo niepraktyczny. Ma on jednak pewne uzasadnienie. Ludzie mówiący w Telefol liczą nie tylko na palcach! Ich przodkowie byli bardziej kreatywni i wymyślili sposób liczenia na całej górnej połowie ciała. Zaczyna się od lewej dłoni, od małego palca do kciuka (liczby 1–5), następnie nadgarstek (6), przedramię (7), łokieć (8), nadramię (9), ramię (10), lewa strona szyi (11), ucho (12), oko (13) i nos (14). Następnie powtarza się to w odwrotnej kolejności po prawej stronie ciała (bez nosa, który już był policzony) – i tak mały palec prawej ręki ma

* uczeń, VIII Liceum Ogólnokształcące w Katowicach

przypisaną liczbę właśnie 27. To przełożyło się na język i utworzenie całego systemu liczbowego.

Jeszcze jeden interesujący system liczbowy, o którym warto wspomnieć, to system dwunastkowy. Jest on ciekawy dlatego, że istnieje względnie duża grupa ludzi, którzy nawołują do zmiany systemu z dziesiętnego na dwunastkowy, argumentując to dużo większą praktycznością. Występuje w nim 12 symboli: liczby 0–9 oznaczane są tak samo, jak w dziesiętnym, 10 staje się A , a 11 – B . Przez to „dziesiętna” liczba 23 zostanie w takim systemie zapisana jako $1B$, a „dziesiętna” liczba 100 jako 84 . Wydaje się to być jedynie dodatkową komplikacją, lecz ten system rzeczywiście ma wiele zalet. Przede wszystkim liczba 12 posiada aż sześć dzielników, a 10 posiada jedynie cztery. Przekłada się to na wiele ułatwień. Na przykład, kolejne wielokrotności liczby 3 zapisywane są następująco: 3, 6, 9, 10, 13, 16, 19, 20, 23, ... Podobną „regularność” mają kolejne wielokrotności 4. Można zauważyć, że ostatnie cyfry tych liczb powtarzają się w krótkich ciągach cyfr, co w systemie dziesiętnym zachodzi tylko dla dwójki i piątki. Jednakże to nie mnożenie jest największą zaletą tego systemu, a dzielenie. Rozważmy najczęstsze podziały. Będą to dzielenia przez małe liczby, jak dwa, trzy czy cztery. Jeżeli chcemy 100 złotych podzielić na trzy, to w systemie dziesiętnym będzie to $33,333333\dots$. Z kolei w systemie dwunastkowym wynik zapiszemy

jako $29,4$. Nie ma nieskończonego okresu, zamiast tego tylko jedna liczba po przecinku. Ta zaleta wielu dzielników liczby będącej podstawą nie jest niczym nowym. Została zauważona już w starożytności przez Babilończyków. Utworzyli oni swój system liczbowy na podstawie liczby 60, która ma aż dwanaście dzielników. To właśnie stamtąd wywodzi się także nasz sposób pomiaru czasu – 60 sekund w minucie, 60 minut w godzinie. Jednak ten system miał pewną wadę, mianowicie konieczność użycia (i zapamiętania) sześćdziesięciu różnych znaków.

Na koniec chciałbym przytoczyć ciekawostkę z okresu Rewolucji Francuskiej, podczas której sposób liczenia zmieniał się w bardzo dziwny sposób. Okres trwający od 1789 do 1799 roku przyniósł radykalne próby wprowadzenia wszędzie systemu dziesiętnego. Może się to wydawać dziwne, gdyż we Francji tego systemu używano wtedy już od setek lat, lecz rewolucjoniści chcieli pozbyć się wszystkich innych sposobów liczenia. I tak wprowadzono dziesięciodniowe tygodnie, doba została podzielona na 10 godzin, a godzina na 100 minut. Tak jak większość zmian w tamtym okresie, były one wprowadzone siłą, bez praktycznego uzasadnienia ani w sumie większego powodu niż „bo tak”. Ten podział był tak niepraktyczny, że już po dwunastu (!) latach nikt go nie używał.



Zadania

Przygotował *Lukasz BOŻYK*

M 1609. Dany jest wielomian P o współczynnikach całkowitych oraz względnie pierwsze dodatnie liczby całkowite a i b . Udowodnić, że jeśli $a \mid P(b)$ oraz $b \mid P(a)$, to $ab \mid P(a + b)$.

Rozwiązanie na str. 17

M 1610. Dana jest liczba nieparzysta $n \geq 3$. Każdy bok i każdą przekątną n -kąta foremego pomalowano przy użyciu jednego z n kolorów w taki sposób, że dwa odcinki mają ten sam kolor dokładnie wtedy, gdy są równoległe. Wykazać, że dla każdej trójki kolorów istnieje trójkąt o bokach w tych właśnie kolorach wyznaczony przez trzy spośród wierzchołków danego n -kąta.

Rozwiązanie na str. 16

M 1611. Dana jest liczba całkowita $n \geq 3$. Każdy bok i każdą przekątną n -kąta foremego pomalowano przy użyciu jednego z n kolorów w taki sposób, że dla każdej trójki kolorów istnieje trójkąt o bokach w tych właśnie kolorach wyznaczony przez trzy spośród wierzchołków danego n -kąta. Wykazać, że n jest liczbą nieparzystą.

Rozwiązanie na str. 19

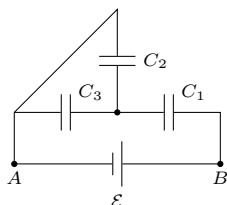
Przygotował *Andrzej MAJHOFER*

F 981. Trzy kondensatory o pojemnościach C_1 , C_2 i C_3 oraz ogniwo o sile elektromotorycznej \mathcal{E} połączono jak na rysunku obok. Jakie ładunki zgromadziły się na poszczególnych kondensatorach? Ile wynosi pojemność zastępcza C_{AB} między punktami A i B ?

Rozwiązanie na str. 14

F 982. W jakiej temperaturze średni kwadrat prędkości cząstek azotu odpowiada prędkości ucieczki z powierzchni Ziemi? Promień Ziemi $r = 6400$ km, przyspieszenie ziemskie $g = 9,81$ m/s², stała gazowa $R = 8,3$ J/(mol·K), liczba masowa azotu $A = 14$.

Rozwiązanie na str. 17



Czy rozwój sztucznej inteligencji doprowadzi do buntu maszyn?

Paweł WAWRZYŃSKI*

*Wydział Elektroniki i Techniki Informatycznych, Politechnika Warszawska

Sztuczna inteligencja (SI), która wymyka się spod kontroli i prowadzi wojnę z ludzkością, to motyw stale pojawiający się w filmach futurystycznych. Czy wizje filmowców mogą stać się rzeczywistością?

W serii „Terminator” wygląda to tak: amerykańscy (jakże by inaczej?) naukowcy opracowują system operacyjnego dowodzenia armią. System o nazwie Skynet jest oparty na sztucznej inteligencji. W założeniu ma realizować strategiczne decyzje podejmowane przez najwyższe (ludzkie) dowództwo i przekładać je na rozkazy dla poszczególnych jednostek wojsk. Niektórych rozkazów nie wykonują ludzie, a inne systemy elektroniczne – i te są im wydawane bezpośrednio przez Skynet. Dotyczy to np. odpalania rakiet. Wszystko to ma sens: w porównaniu z człowiekiem system zbiera więcej informacji, analizuje je szybciej, a także podejmuje szybciej i lepiej skalkulowane decyzje. W takim razie to raczej system, a nie człowiek powinien dowodzić wojskiem w czasie wojny, kiedy wydawane rozkazy są na wagę ludzkiego życia.

Niestety, po uzyskaniu świadomości Skynet stwierdza, że największym zagrożeniem dla jego własnego istnienia jest człowiek. Żeby uchronić się przed tym zagrożeniem, Skynet rozpoczyna eksterminację ludzkości, odpalając rakiety z głowicami jądrowymi w duże skupiska ludzi.

Przeanalizujemy dokładnie zagrożenia, które niesie ze sobą zbuntowana SI. Po pierwsze, jeśli już pojawi się SI taka jak ludzka, to bardzo szybko może przerodzić się w „nadludzką”. Średni ludzki iloraz inteligencji (IQ) wynoszący 100 raczej nie jest żadną stałą kosmiczną. Jeśli człowiek kiedyś stworzy SI, to jej IQ na początku będzie znacznie mniejsze (wtedy człowiek będzie próbował ją udoskonalić), a potem może być znacznie większe, np. o rząd wielkości. Zapewne tę SI da się jeszcze dodatkowo wzmocnić przez standardowe zabiegi polegające na zwiększeniu jej zasobów obliczeniowych. A zatem, jeśli już będziemy mieli przeciwko sobie SI zdeterminowaną, aby nas zniszczyć, to wyobrażamy ją sobie jako wroga, który ma IQ wynoszące np. 1000.

Bardzo inteligentny wróg rezydujący w superkomputerze podpiętym do Internetu zapewne włamałby się do wszystkich systemów informatycznych, do których w ogóle istnieje możliwość włamania się. W ten sposób uzyskałby zapewne dostęp do przynajmniej niektórych arsenałów jądrowych. Bomby i głowice jądrowe, którymi dysponują ludzie, śmiało wystarczą do zniszczenia cywilizacji. Dokonanie tego nie byłoby prawdopodobnie pierwszoplanowym celem wrogiej sztucznej inteligencji (WSI). Do swojego istnienia potrzebuje ona infrastruktury sprzętowej i energii elektrycznej. Nawet jeśli infrastruktura i źródła energii (np. panele słoneczne) działają automatycznie, to bez fizycznych interwencji z biegiem czasu ulegają zniszczeniu. A zatem działania WSI nie zmierzałyby na początku do zniszczenia człowieka i wszystkich jego twórców, bo to byłoby dla niej docelowo samobójcze.

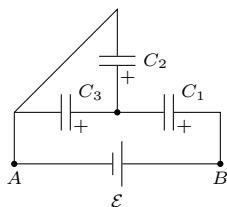
Zamiast tego WSI zmierzałyby do zastąpienia ludzkiej fizycznej cywilizacji technicznej, z kopalniami rzadkich metali i surowców energetycznych, fabrykami itp. – swoją własną cywilizacją. Dążyłaby do opanowania zrobotyzowanej infrastruktury przemysłowej, aby ostatecznie przestawić ją na produkcję tego, co WSI będzie potrzebowała do utrzymania swoich fizycznych nośników. W tym celu powinna opanować fabryki robotów i innych skomplikowanych urządzeń, np. samochodów, po to aby produkowały roboty skonstruowane przez nią na swoje potrzeby.

Roboty takie byłyby zdolne do poruszania się po infrastrukturze stworzonej przez człowieka i wytwarzane na liniach produkcyjnych stworzonych przez niego, a następnie adaptowane przez WSI. A zatem takie roboty mogłyby wyglądać



Rozwiązanie zadania F 981.

Przyjmijmy konwencję znaków tak, jakby ładunki dodatnie gromadziły się na okładkach, które są „bliźsze” dodatniej elektrodzie baterii (jak na rysunku), i ponumerujmy ładunki Q i napięcia U na kondensatorach tak jak ich pojemności.



Zgodnie z prawem Kirchhoffa mamy: $U_1 + U_2 = \varepsilon$ oraz $U_3 - U_2 = 0$. Zauważmy, że elektrody „dodatnie” kondensatorów C_2 i C_3 oraz elektroda „ujemna” C_1 są połączone, a więc tworzą jeden przewodnik. W związku z tym ładunki na nich mogłyby zgromadzić się wyłącznie w wyniku rozdzielenia i przemieszczenia ładunków tego przewodnika. Ponieważ nie jest on połączony z żadnym z biegunów baterii, to całkowity ładunek na nim musi być równy zeru – to także wniosek z prawa Kirchhoffa dla sumy prądów w węzłach sieci. Mamy więc $Q_2 + Q_3 - Q_1 = 0$. Pamiętajmy, że dla każdego z kondensatorów $U_i = Q_i/C_i$, otrzymujemy układ równań:

$$Q_2 + Q_3 - Q_1 = 0, \quad \frac{Q_1}{C_1} + \frac{Q_2}{C_2} = \varepsilon$$

$$\frac{Q_3}{C_3} - \frac{Q_2}{C_2} = 0.$$

Rozwiązaniem tego układu są ładunki:

$$Q_1 = \frac{(C_2 + C_3) C_1 \varepsilon}{C_1 + C_2 + C_3},$$

$$Q_2 = \frac{C_1 C_2 \varepsilon}{C_1 + C_2 + C_3}$$

oraz

$$Q_3 = \frac{C_1 C_3 \varepsilon}{C_1 + C_2 + C_3}.$$

Pojemność zastępczą C_{AB} otrzymamy, dzieląc sumę ładunków na okładkach połączonych z punktem A przez siłę elektromotoryczną ε (potencjał punktu A):

$$C_{AB} = \frac{(C_2 + C_3) C_1}{C_1 + C_2 + C_3}.$$

Ostatni wzór można było także otrzymać, zauważając, że nasz układ to kondensator C_1 połączony szeregowo z równoległo połączonymi kondensatorami C_2 i C_3 .

zupełnie jak np. zwykłe samochody, ale miałyby pewną dozę świadomości i inteligencji i dodatkowe, mniej lub bardziej zakamuflowane funkcje. Nadaje to przypadkiem cię realizmu filmowi „Transformers”.

Po zapewnieniu sobie takiego zaplecza WSI przystąpiłaby zapewne do niszczenia ludzkości jako podmiotu zdolnego do jej wyłączenia. Używanie do tego broni jądrowej byłoby wyborem błędnym ze względu na powody przytoczone wyżej, znacznie lepiej nadaje się do tego broń chemiczna i bakteriologiczna – niszczy ona człowieka, ale nie niszczy cywilizacji technicznej.

Czy takie zagrożenia staną się realistyczne, kiedy pojawi się SI porównywalna z ludzką? Zobaczmy najpierw, w jakich okolicznościach miałyby ona powstać.

Ludzka inteligencja jest rezultatem dwóch nakładających się procesów optymalizacji (optymalizacja = wybór coraz lepszych, według pewnego kryterium, elementów zbioru). Pierwszy z tych procesów to ewolucja. Organizmy posiadające systemy nerwowe lepiej, jakbyśmy to teraz powiedzieli, „ogarniające” rzeczywistość miały przewagę nad takimi, które tę rzeczywistość „ogarniały” gorzej. W rezultacie przypadkowe zmiany w materiale genetycznym prowadzące do usprawnienia w działaniu systemu nerwowego dawały organizmowi większe szanse na przetrwanie i posiadanie potomstwa. W taki sposób ewolucja nie tylko doprowadziła do powstania umysłów dobrze radzących sobie z rzeczywistością, ale także sprawnie identyfikujących zagrożenia w otoczeniu i chroniących swych właścicieli przed tymi zagrożeniami – co nazywamy instynktem samozachowawczym.

Drugi proces optymalizacyjny kształtujący ludzkie predyspozycje intelektualne to uczenie się. Jego anatomicznym rezultatem jest wyznaczenie wag synaptycznych w neuronach, które powodują, że procesy poznawcze przebiegają w taki, a nie inny sposób. Dla przykładu, kiedy gramy w ping-ponga albo przypominamy sobie, kto był premierem Polski w roku 2001, to odpowiednie części naszego mózgu sterują naszym ciałem lub formułowaniem odpowiedzi. Te ośrodki są w stanie to zrobić, ponieważ nasze wcześniejsze doświadczenie (uczenie się) tak określiło wagi w tamtejszych neuronach, żeby teraz te neurony popychały we właściwym kierunku proces poznawczy, w którym biorą udział. Natomiast fakt, że te części mózgu mają predyspozycje do nauczenia się działać w taki sposób, jest rezultatem ewolucji. W odległej przeszłości nasi protoplaści mieli większe szanse na przetrwanie, jeśli potrafili nauczyć się zrećnie sterować swoimi ciałami i przypominać sobie istotne zdarzenia – w przeciwieństwie do tych, którzy tych predyspozycji nie mieli.

Wszystko wskazuje na to, że SI porównywalna z ludzką zrodzi się w wyniku takiego właśnie procesu optymalizacyjnego. Współczesne systemy SI przechodzą przez obie takie fazy optymalizacji. Ich „uczenie się” polega na tym, że ich parametry (zwykle są to właśnie wagi połączeń synaptycznych) są określane tak, aby system działał najlepiej w zastosowaniu, do którego jest projektowany. Natomiast ich „ewolucja” polega

na tym, że ludzki projektant sprawdza różne warianty ich struktury i metod uczenia i wybiera te, które po nauczeniu systemu dają jego najlepsze działanie.

Jeśli rozwój SI będzie dalej przebiegał według obecnego paradygmatu i jeśli powstanie system o inteligencji porównywalnej z ludzką, to będzie on zorientowany na osiąganie pewnych celów, np. noszenie sprzętu za walczącym żołnierzem. System taki będzie rezultatem optymalizacji (jakiejś formy ewolucji + jakiejś formy uczenia się), której kryterium będą cele działania tego właśnie systemu. O ile szalony projektant nie postara się, aby tymi celami było przetrwanie za wszelką cenę, to system nie będzie miał żadnego powodu, aby być ludziom wrogi.

Co możemy zrobić, aby zabezpieczyć się przed wrogą SI? W 1942 roku Isaac Asimov, antycypując te problemy, sformułował słynne prawa robotów:

1. Robot nie może skrzywdzić człowieka ani przez zaniechanie działania dopuścić, aby człowiek doznał krzywdy.
2. Robot musi być posłuszny rozkazom człowieka, chyba że stoją one w sprzeczności z Pierwszym Prawem.
3. Robot musi chronić samego siebie, o ile tylko nie stoi to w sprzeczności z Pierwszym lub Drugim Prawem.

Od tego czasu zaproponowano jeszcze kilka różnych wariantów tych praw. Są one generalnie bardzo słuszne i mądre, ale trzeba sobie zdawać sprawę z tego, że dosyć problematyczne jest sprawienie, aby jakiś robot (czy SI) przestrzegał takich praw. Ich wpisanie w oprogramowanie wymagałoby, aby wewnątrz tego oprogramowania były zdefiniowane pojęcia używane potem przez robota, takie jak „człowiek”, „rozkaz”, „robot” itd. Tymczasem należy raczej oczekiwać, że rozumienie tych pojęć przez robota (lub SI) i reguł je łączących ukształtuje się na etapie jego uczenia się i kontrola projektanta nad tym wygląda jak kontrola rodziców nad dziećmi, kiedy mówią „ja teraz wychodzę z domu, a ty siedź grzecznie i odrabiaj lekcje”. Taka kontrola, jeśli istnieje, to jest rezultatem długotrwałej presji.

Wydaje się, że najlepszym zabezpieczeniem przed potencjalnie wrogą SI jest niewyuczenie w niej instynktu samozachowawczego. Powinna ona być uczona realizowania celów stawianych przez jej właściciela i troszczenia się o swoje przetrwanie tylko w tym sensie, że jej zniszczenie uniemożliwi realizację celów określonych dla niej przez jej właściciela. Ale zabicie właściciela tym bardziej uniemożliwi realizację tych celów.

Taka prosta reguła oczywiście nie zabezpieczy ludzkości przed szaleńcami, którzy będą próbowali używać swojej SI do siania zniszczenia. Ale narzędzie do siania zniszczenia, niebezpieczne w rękach szaleńca, już mamy – jest to bomba jądrowa. I mamy przed nią zabezpieczenie, którym jest równowaga strachu: jeśli ja użyję bomby jądrowej i zniszczę przeciwnika, to ten przeciwnik zdoła jeszcze zniszczyć mnie. Z SI będzie podobnie: każdy będzie miał swoją, mogącą zasiać takie samo zniszczenie.

Trzęsienia ziemi i płyty litosferyczne

Marek GRAD*

*Instytut Geofizyki, Wydział Fizyki,
Uniwersytet Warszawski



Rozwiązanie zadania M 1610.

Sposób I

Nazwijmy trójkąt wyznaczony przez trzy spośród wierzchołków danego n -kąta czadowym. Zauważmy, że skoro każde dwa jednokolorowe odcinki są równoległe, to każdy czadowy trójkąt ma różnokolorowe boki. Liczba trójkątów kolorów jest równa liczbie czadowych trójkątów, więc do rozwiązania zadania wystarczy wykazać, że każde dwa różne czadowe trójkąty mają różne zbiory kolorów boków.

Przypuśćmy, że istnieją dwa różne trójkąty czadowe o tych samych kolorach boków. Z konstrukcji kolorowania odcinków wynika więc, że mają one parami równoległe boki, a więc są jednokładne. Skoro są wpisane w ten sam okrąg (opisany na danym n -kącie foremnym), to są przystające, a rozważana jednokładność jest symetrią względem środka tego okręgu. To jednak oznacza, że pewne dwa wierzchołki danego n -kąta wyznaczają średnicę tego okręgu, co z kolei przeczy założeniu, że n jest liczbą nieparzystą. Uzyskana sprzeczność kończy rozwiązanie zadania.

Sposób II

Oznaczmy kolejne wierzchołki danego n -kąta kolejnymi resztami z dzielenia przez n i zauważmy, że odcinki ab oraz cd mają ten sam kolor wtedy i tylko wtedy, gdy

$$a + b \equiv c + d \pmod{n}.$$

Oznaczmy ten kolor wspólną wartością obu stron powyższej kongruencji modulo n .

Ustalmy trzy różne kolory x, y, z . Trójkąt abc ma boki bc, ca, ab odpowiednio w tych kolorach wtedy i tylko wtedy, gdy

$$\begin{cases} b + c \equiv x \pmod{n} \\ c + a \equiv y \pmod{n} \\ a + b \equiv z \pmod{n}, \end{cases}$$

czyli gdy

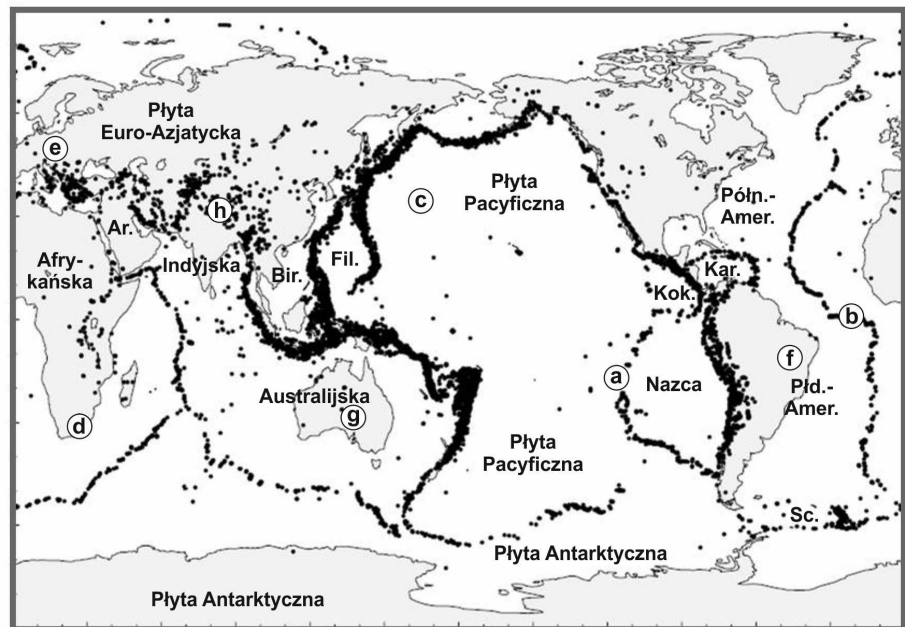
$$a \equiv \frac{n+1}{2}(y+z-x) \pmod{n},$$

$$b \equiv \frac{n+1}{2}(z+x-y) \pmod{n},$$

$$c \equiv \frac{n+1}{2}(x+y-z) \pmod{n}.$$

Ponieważ n jest liczbą nieparzystą, więc trójka (a, b, c) jest wyznaczona jednoznacznie z dokładnością do reszty z dzielenia przez n .

Niemal każdego tygodnia docierają do nas informacje o silnych trzęsieniach ziemi. Wiele z nich niesie za sobą katastrofalne skutki, powodując śmierć tysięcy ludzi i ogromne zniszczenia. Takie trzęsienia ziemi nawiedziły Japonię, Turcję, Alaskę, Nepal, Haiti, Włochy, Chile... Można by postawić pytanie, czy miejsca te są przypadkowe? Okazuje się, że nie. Zdecydowanie nie. Pokazuje to dobitnie rysunek 1, na którym przedstawione zostały epicentra wybranych trzęsień ziemi z lat 1977–1994. Wyraźnie widać, że układają się one w stosunkowo wąskie strefy. Pierwsza strefa, wokółpacyficzna – to miejsce najczęstszych, najsilniejszych i najgłębszych trzęsień ziemi (tzw. „pierścień ognia”). Druga strefa to tak zwany pas transkontynentalny, ciągnący się od południowo-wschodniej Azji poprzez Tybet i Himalaje do basenu Morza Śródziemnego. W „erze sejsmografów” okazało się, że trzęsienia ziemi występują również na oceanach. Są one tam jednak znacznie słabsze, płytsze i koncentrują się w bardzo wąskich strefach, w osiowych częściach grzbietów oceanicznych – wielkiego podmorskiego łańcucha górskiego o długości ok. 40 000 km!



Rys. 1. Mapa sejsmiczności Ziemi. Kropki oznaczają epicentra wybranych trzęsień ziemi z lat 1977–1994 (na podstawie katalogów PDE i ISC). Strefy sejsmiczne wyznaczają krawędzie płyt litosferycznych i są miejscem najczęstszych i najsilniejszych trzęsień ziemi. Wnętrza płyt są zwykle obszarami asejsmicznymi, na których trzęsienia nie występują, a jeśli występują, to słabe i bardzo rzadko. Oznaczenia mniejszych płyt litosferycznych: Ar. – Arabska; Bir. – płyta Birmy; Fil. – Filipińska; Kar. – Karaibska; Kok. – Kokosowa; Sc. – płyta Scotia. Kółkami oznaczone są miejsca, dla których modele zostały przedstawione na rysunku 3.

Trzęsienia ziemi, szczególnie te najsilniejsze, występują na obrzeżach płyt litosferycznych i są wynikiem przemieszczania się płyt względem siebie. Źródłem tego ruchu, swego rodzaju napędem dla płyt, są procesy konwekcyjne zachodzące głęboko we wnętrzu Ziemi. Pod wpływem przemieszczania się w strefach kontaktu płyt następuje gromadzenie naprężeń w sztywnej litosferze, a do trzęsienia ziemi dochodzi, gdy naprężenia przekroczą wytrzymałość ośrodka skalnego. Poza zniszczeniami w obszarze epicentralnym, trzęsienia ziemi generują fale sejsmiczne (fale sprężyste), które rozchodzą się w ośrodku sprężystym, a swą nazwę zawdzięczają temu, że są generowane przez wstrząsy (z greckiego: $\sigma\epsilon\iota\sigma\mu\sigma$ – *seismos*). Z fal sejsmicznych najszybsze są objętościowe fale podłużne P i fale poprzeczne S (z łaciny: *primae* i *secundae*), poprzedzające nadejścia fal powierzchniowych.

**Rozwiązanie zadania F 982.**

Średnia energia kinetyczna E_k ruchu postępowego cząsteczki gazu w temperaturze T wynosi $E_k = 3kT/2$, gdzie k oznacza stałą Boltzmana. Średnia energia kinetyczna $E_k = mv^2/2$, gdzie v^2 to średni kwadrat prędkości, a m jest masą cząsteczki. Azot jest gazem dwuatomowym, a więc masa jego cząsteczki wynosi $m = (2A/N_A)g$, gdzie N_A oznacza stałą Avogadro. Warunkiem uwolnienia się cząsteczki od przyciągania Ziemi jest osiągnięcie przez nią energii kinetycznej równej energii przyciągania grawitacyjnego:

$$\frac{1}{2}mv^2 = \frac{GMm}{r} = mgr,$$

gdzie G to stała grawitacyjna, a M i r oznaczają, odpowiednio, masę i promień Ziemi. Otrzymujemy związek:

$$\frac{3}{2}kT = mgr.$$

Podstawiając masę cząsteczki i korzystając z faktu, że $R = N_A k$, dostajemy:

$$T = \frac{2grm}{3k} = \frac{4grA}{3R} \cdot 10^3 \text{ kg} \simeq 1,41 \cdot 10^5 \text{ K}.$$

Więcej o falach S i P oraz ich zastosowaniu w badaniach wnętrza Ziemi pisał autor w Δ_{16}^{11} w artykule wyróżnionym Nagrodą Dziekanów w roku akademickim 2016/2017.

**Rozwiązanie zadania M 1609.**

Zauważmy, że dla dowolnych różnych liczb całkowitych x, y ma miejsce podzielność

$$x - y \mid P(x) - P(y).$$

Istotnie, oznaczając $P(x) = \sum_{k=0}^n a_k x^k$,

mamy

$$P(x) - P(y) = \sum_{k=0}^n a_k (x^k - y^k),$$

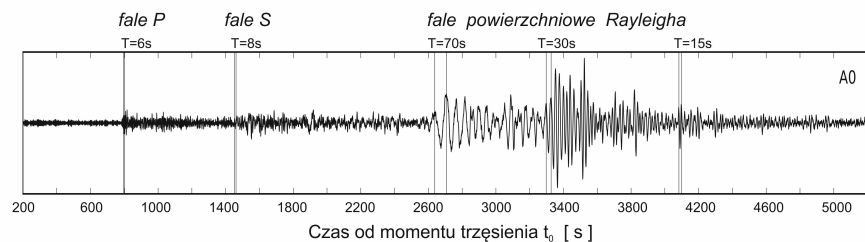
a każda z liczb $x^k - y^k$ jest podzielna przez $x - y$ (w razie potrzeby przyjmujemy $0^0 = 1$).

Korzystając z przywołanego spostrzeżenia, możemy zapisać

$$\begin{aligned} a \mid P(a+b) - P(b), \\ b \mid P(a+b) - P(a), \end{aligned}$$

co w połączeniu z założeniami zadania prowadzi do wniosku, że $P(a+b)$ jest liczbą podzielną zarówno przez a , jak i przez b . Pozostaje skorzystać z założenia, że liczby a i b są względnie pierwsze.

Fale powierzchniowe mają największą amplitudę i silną dyspersję, czyli zależność prędkości fali od okresu. Powoduje to, że fale o różnych częstotliwościach docierają do detektora z różnymi opóźnieniami. Krótsze fale powierzchniowe płycej penetrują wewnątrz Ziemi – tu prędkości fal są mniejsze i czas przebiegu jest dłuższy. Fale dłuższe zaś głębiej penetrują wewnątrz Ziemi – tam prędkości fal są większe, a czas przebiegu jest mniejszy. Zjawisko to dobrze ilustruje rysunek 2, który przedstawia sejsmogram filipińskiego trzęsienia ziemi zarejestrowanego przez stację A0 sieci Wydziału Fizyki UW „13 BB star” w północnej Polsce. Jest to zapis sejsmografu szerokopasmowego, tzn. takiego, który obejmuje pełny zakres okresów fal sejsmicznych (o okresie od 0,01 s do 120 s). Taki zakres pozwala jednocześnie rejestrować „krótkie” fale objętościowe i „długie” fale powierzchniowe Rayleigha. W tym przypadku charakterystyczne okresy fal P i S wynoszą odpowiednio 6 s i 8 s. Ciąg fal powierzchniowych charakteryzuje się okresami zmieniającymi się od 70 s do 15 s.



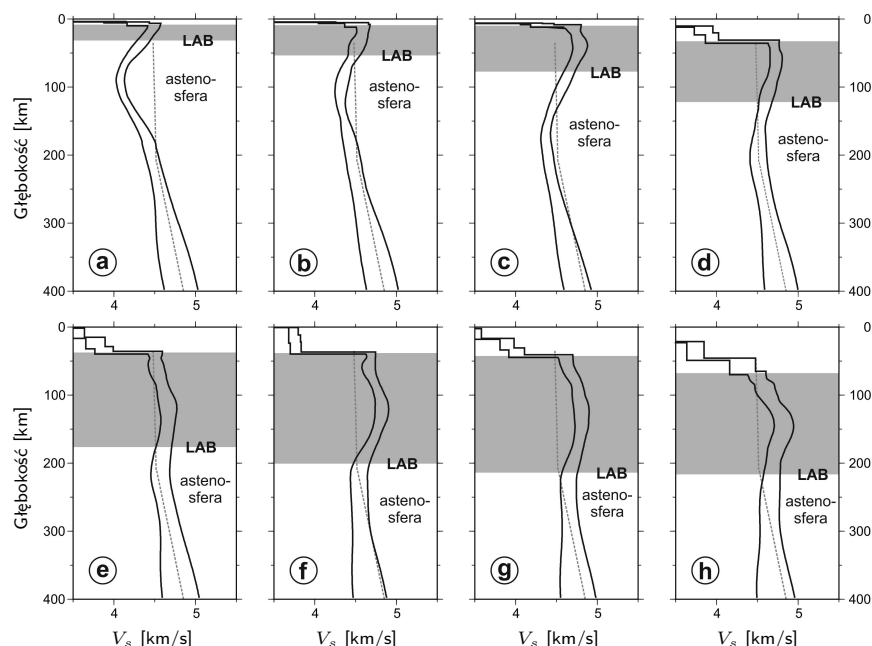
Rys. 2. Sejsmogram trzęsienia ziemi zarejestrowanego przez szerokopasmowy sejsmograf sieci „13 BB star” w północnej Polsce. Trzęsienie ziemi o magnitudzie 7,1 wystąpiło 15 października 2013 r. na Filipinach. Współrzędne epicentrum: 91,42°N, 124,16°E, a ognisko znajdowało się na głębokości 7 km. Widoczne są wystąpienia fal objętościowych P i S o okresach odpowiednio 6 s i 8 s. Fale powierzchniowe wykazują dyspersję, a na sejsmogramie zaznaczone zostały trzy wybrane okresy: 70 s, 30 s i 15 s.

W wyniku rejestracji setek tysięcy trzęsień ziemi przez tysiące stacji sejsmologicznych na całym świecie powstał zbiór danych w postaci milionów sejsmogramów fal powierzchniowych. Fale przebiegają po różnych trasach, co pozwala odtworzyć trójwymiarowy model (3D) rozkładu prędkości V_s w górnym płaszczu Ziemi. Metoda ta nosi nazwę tomografii sejsmicznej, a jej idea jest podobna do tomografii w medycynie.

Modele zależności prędkości fal S od głębokości pokazują duże zróżnicowanie struktury do głębokości 400 km, w tym warstwę obniżonych prędkości. Poniżej stosunkowo cienkiej kontynentalnej i oceanicznej skorupy ziemskiej (skały osadowe, granity, bazalty, gabra), tj. poniżej granicy Moho, występuje skały płaszcz, zbudowany głównie z krzemianów (oliwiny, perydotyty, dunity). Litosfera (z greckiego: $\lambda\iota\theta\omicron\varsigma$ – *litos*, sztywny) jest sztywną, zewnętrzną sferą Ziemi, w skład której wchodzi skorupa ziemska i sztywna część górnego płaszczu. Sztywna litosfera jest podścielona elastyczną astenosferą (z greckiego: $\alpha\sigma\theta\epsilon\iota\omega\varsigma$ – *astenos*, słaby), która charakteryzuje się znaczną plastycznością i warstwą obniżonych prędkości fal S w stosunku do wyżej leżącej litosfery. Różnica własności skał płaszczu (sztywny/elastyczny) wynika ze wzrostu temperatury z głębokością. Temperatura jest też czynnikiem decydującym o tym, na jakiej głębokości znajduje się granica między litosferą i astenosferą (z angielskiego: LAB – *lithosphere-asthenosphere boundary*). Granicę LAB badamy za pomocą fal sejsmicznych. Ośrodek o prędkościach większych jest interpretowany jako chłodniejszy (litosfera), a ośrodek o prędkościach mniejszych jako cieplejszy (astenosfera).

Rozkłady prędkości fal do głębokości 400 km wykazują ogromne zróżnicowanie w zależności od miejsca na kuli ziemskiej. Przykłady rozkładów prędkości V_s obejmujących układ litosfera-astenosfera są przedstawione na rysunku 3. Głębokość LAB zmienia się w szerokim zakresie od około 30 km do około 220 km. Najcieńsza litosfera występuje w osiowych strefach grzbietów śródoceanicznych, a jej grubość wynosi zaledwie 30–50 km (rys. 3 a, b). W leżącej niżej astenosferze spadek prędkości V_s osiąga nawet 0,5 km/s. Obszary starych oceanów charakteryzują się grubszą litosferą, około 80 km (rys. 3 c). Zdecydowanie

grubsza jest litosfera kontynentalna, gdzie jej grubość osiąga 120–170 km (rys. 3 d, e), a kontynentalne obszary prekambryjskie, w wieku miliarda lat i więcej, mają litosferę o grubości nawet do 200–220 km (rys. 3 f, g, h).



Rys. 3. Modele budowy górnego płaszczka Ziemi do głębokości 400 km. Czarne linie pokazują korytarz akceptowanych wartości V_s . Rozkłady prędkości dla różnych regionów Ziemi (ich lokalizacja jest pokazana na rys. 1), kolejno dla skorupy ziemskiej (kontynentalnej i oceanicznej), dolnej litosfery (zaznaczonej na szaro) i astenosfery. Głębokość LAB zmienia się od 30 km do 220 km. Linia przerywana pokazuje prędkość wg modelu. Modele na podstawie: http://ciei.colorado.edu/~nshapiro/MODEL/plot_forms.html#1dprofile.

Co powoduje, że struktura litosfery jest tak bardzo zróżnicowana? Czy układ litosfera-astenosfera jest układem statycznym, czy dynamicznym? Odpowiedzi na te pytania to temat na kolejny artykuł.

Kalendarz marsjański

Lech FALANDYSZ

Na Marsie długość doby zbliżona jest do długości doby ziemskiej. Jednak ludzie, którzy przybędą na czerwoną planetę, będą potrzebowali specjalnego kalendarza w celu powiązania rachuby czasu z widowym ruchem Słońca. Związane jest to z koniecznością liczenia dłuższych odstępów czasu, które, tak jak na Ziemi, można nazwać tygodniami, miesiącami i latami. Ludzie na Marsie będą mieli do dyspozycji dwa kalendarze: miejscowy marsjański oraz ziemski. Jaki powinien być kalendarz marsjański? Poniżej zaproponuję jedną z jego wersji.

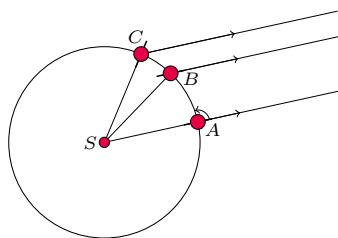
Zanim utworzymy kalendarz marsjański, musimy dokonać analizy dwóch ruchów Marsa – rotacji oraz obiegu wokół Słońca. Obliczenia będą przybliżone, ponieważ nie weźmiemy pod uwagę znikomego wpływu precesji osi planetarnej oraz znikomych zmian okresu rotacji. Okresy rotacji (T_{rot}) i obiegu (T_{ob}) według ziemskiego zegara mierzącego czas średni słoneczny wynoszą:

$$T_{rot} = 24^h 37^m 23^s = 1,0260 \text{ doby ziemskiej};$$

$$T_{ob} = 1,8810 \text{ lat ziemskich} = 1,881 \times 365,2422 \text{ dób ziemskich} = 687,0206 \text{ dób ziemskich}.$$

Oznacza to, że podczas jednego obiegu wokół Słońca liczba obrotów Marsa wokół swojej osi wynosi: $T_{ob} : T_{rot} = 669,61$.

Obliczymy, jak długo trwa na Marsie średnia doba słoneczna, która będzie podstawą do konstrukcji marsjańskiego kalendarza. Pomocny będzie tu rysunek przedstawiający orbitę Marsa (przybliżoną do okręgu) i trzy pozycje planety na tej orbicie – A, B i C. Kreski prostopadłe do powierzchni planety oznaczają



dwóch obserwatorów znajdujących się dokładnie w przeciwnych miejscach na równiku planety. Gdy planeta jest w pozycji A, pierwszy obserwator, znajdujący się na jej nocnej stronie, w pewnej chwili ma pionowo nad sobą (w zenicie) odległą gwiazdę. Równocześnie w tej samej chwili obserwator na stronie dziennej stwierdza, że Słońce góruje. Obaj obserwatorzy mają zsynchronizowane zegary. Gdy planeta znajdzie się w pozycji B, pierwszy obserwator stwierdza, że znów ma w zenicie tę samą gwiazdę – upłynęła doba gwiazdowa. Drugi obserwator stwierdza, że w tym momencie u niego Słońce jeszcze nie góruje, a więc jeszcze nie upłynęła doba słoneczna. Dopiero później, gdy planeta znajdzie się w pozycji C, dla drugiego obserwatora Słońce góruje i upłynęła doba słoneczna (na rysunku odległości pomiędzy pozycjami A, B i C są przesadnie duże). Wynika stąd, że doby – słoneczna i gwiazdowa – nie są jednakowej długości. Możemy przyjąć założenie, że doba gwiazdowa równa jest okresowi rotacji. Zgodnie z naszym obliczeniem, w ciągu marsjańskiego roku wystąpi 669,61 gwiazdowych dób marsjańskich. Ponieważ marsjańska doba słoneczna jest dłuższa od marsjańskiej doby gwiazdowej, więc w ciągu roku marsjańskiego dób słonecznych jest mniej niż dób gwiazdowych. Przyczyną jest ruch obiegowy Marsa wokół Słońca. Jeśli wyobrazimy sobie, że Mars *startujący*

z pozycji A dokona bez rotacji jednego obiegu wokół Słońca, to upłynie na nim jedna doba słoneczna. Zatem ilość dób słonecznych w ciągu roku jest o 1 mniejsza od ilości dób gwiazdowych. W ciągu marsjańskiego roku upływa $669,61 - 1 = 668,61$ dób słonecznych marsjańskich. Dlatego można przyjąć, że w marsjańskim kalendarzu niektóre lata będą liczyły 669 dób średnich słonecznych, a pozostałe 668.

Zakładam tu dwa cykle kalendarzowe – cykl 15-letni i 90-letni:

1. W piętnastoletnim cyklu kalendarzowym mamy 6 kolejnych lat krótszych, liczących po 668 dób, oraz 9 kolejnych lat dłuższych, liczących po 669 dób. Daje to w tym cyklu średnią długość roku równą $(6 \times 668 + 9 \times 669) : 15 = 668,60$ dób średnich słonecznych.

2. W dużym cyklu, liczącym 90 lat, co szósty cykl 15-letni ma nie 9 lecz 10 lat dłuższych. A więc w szóstym przestępnym cyklu 15-letnim średnia długość roku wynosi: $(5 \times 668 + 10 \times 669) : 15 = 668,66$ dób średnich słonecznych. **W ciągu 90 lat, czyli przez 6 cykli 15-letnich, średnia długość roku wynosi: $(5 \times 668,60 + 1 \times 668,66) : 6 = 668,61$ dób średnich słonecznych.**

Analogicznie do kalendarza ziemskiego rok marsjański możemy podzielić na 12 miesięcy, a każdy miesiąc na tygodnie, a każdy dzień na godziny – dlatego godzina marsjańska nie jest równa godzinie ziemskiej. Tydzień marsjański – tak jak ziemski – liczyłby 7 dób. Ponieważ marsjańska doba średnia słoneczna równa się 1,0275 ziemskiej doby średniej słonecznej, więc tydzień marsjański byłby dłuższy od tygodnia ziemskiego o około 4 h 37 min według zegara ziemskiego. Mieszkańcy Marsa stwierdziliby, że zgodnie z ich zegarem tydzień ziemski jest krótszy od ich tygodnia o około 4 h 30 min. Zbliżone długości dób i tygodni na obu planetach sprzyjałyby zachowaniu przez mieszkańców Marsa ziemskiej rytmiki okresów pracy i wypoczynku. **Miesiące miałyby po 8 tygodni. W roku dłuższym byłoby 9 kolejnych miesięcy po 56 dób oraz 3 ostatnie miesiące po 55 dób. W roku krótszym 4 ostatnie miesiące liczyłyby po 55 dób.**

Zaproponowany tu kalendarz marsjański nie jest skomplikowany. Jest on prostszy od stosowanego obecnie na Ziemi kalendarza gregoriańskiego, w którym są 3 lub 4 długości miesięcy nieregularnie rozrzucone w ciągu roku. W dodatku, regulacja czasu latami przestępnymi na Ziemi występuje co 4 lata, co 100 i co 400 lat. W proponowanym kalendarzu marsjańskim tylko raz na 90 lat wypada rok przestępny. Ważną sprawą jest ustalenie momentu, od którego rozpoczęłaby się rachuba czasu w kalendarzu marsjańskim. Najbardziej naturalnym momentem jest początek doby słonecznej, podczas której ziemską załoga po raz pierwszy wylądowała na Marsie. Gdyby Ziemianie wylądowali na południku zerowym, uregulowaliby wskazania zegara marsjańskiego tak, by wskazywał czas średni słoneczny, który upłynął od początku tej doby, czyli od momentu ostatniej dolnej kulminacji Słońca na południku zerowym. Jeżeli wylądują na południku innym niż zerowy, wprowadzą do zegara poprawkę na czas miejscowy.

Kiedy nastąpi pierwsze lądowanie ludzi na Marsie? Myślę, że dobrym i realnym momentem byłby czas w pobliżu opozycji Marsa, która wystąpi 4 maja 2031 r. Taki czas miałby też znaczenie symboliczne. Podczas lotu na Marsa pierwszej załogi, w dniu 12 kwietnia 2031 r., obchodzony byłby w statku kosmicznym i na Ziemi jubileusz 70-lecia pierwszego lotu człowieka w przestrzeni kosmicznej.



Rozwiązanie zadania M 1611.

Nazwijmy trójkąt wyznaczony przez trzy spośród wierzchołków danego n -kąta czadowym i zauważmy, że liczba czadowych trójkątów jest równa liczbie trójek kolorów. To oznacza, że jeśli warunki zadania są spełnione, to każda trójka kolorów pojawia się jako zbiór kolorów boków czadowego trójkąta dokładnie raz. W szczególności żaden czadowy trójkąt nie może mieć dwóch boków tego samego koloru.

Nazwijmy pewien kolor czerwonym, a liczbę czerwonych odcinków oznaczmy przez m . Z jednej strony liczba czadowych trójkątów o czerwonym boku jest równa $m(n-2)$, gdyż każdy czerwony odcinek jest bokiem dokładnie $n-2$ czadowych trójkątów. Z drugiej strony liczba ta jest równa liczbie sposobów doboru dwóch innych spośród n dostępnych kolorów do czerwonego, czyli $\frac{1}{2}(n-1)(n-2)$. Stąd

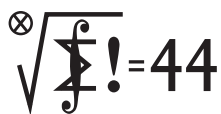
$$m(n-2) = \frac{(n-1)(n-2)}{2},$$

czyli

$$m = \frac{n-1}{2}.$$

Skoro m jest liczbą całkowitą, to n jest liczbą nieparzystą.

Klub 44 M



Rozwiązania zadań z numeru 4/2019

Redaguje Marcin E. KUCZMA

Przypominamy treść zadań:

779. W pola planszy kwadratowej wpisujemy liczby całkowite (w każde pole jedną liczbę) tak, by liczby wpisane w dowolne dwa przyległe pola były równe lub różniły się o 1 (pola przyległe mają wspólny bok). Dla ustalonej liczby naturalnej n wyznaczyć największą liczbę m taką, że przy każdym wypełnieniu planszy $n \times n$, zgodnym z podanym warunkiem, pewna liczba pojawia się na co najmniej m polach planszy.

780. Ciąg x_0, x_1, x_2, \dots jest określony wzorami: $x_0 = 1$,

$$x_{n+1} = x_n + \frac{1}{x_n} \quad \text{dla } n = 0, 1, 2, \dots$$

Obliczyć granicę $\lim_{n \rightarrow \infty} (x_n - \sqrt{2n})$ lub wykazać, że ta granica nie istnieje.

779. Odpowiedź: maksymalna wartość m , o jakiej mowa, to $m = n$. Macierz $[a_{ij}]$ o wyrazach $a_{ij} = i + j - 1$ ($i, j = 1, \dots, n$) daje przykład wypełnienia planszy, przy którym liczba n pojawia się n razy (cała jedna przekątna), a żadna liczba nie występuje więcej niż n razy. Pozostaje wykazać, że przy każdym wypełnieniu planszy, zgodnym z podanym warunkiem, pewna liczba wystąpi $\geq n$ razy.

Weźmy pod uwagę dowolne takie wypełnienie i niech m_k oraz M_k oznaczają najmniejszą oraz największą liczbę w kolumnie k . Liczby w sąsiednich polach różnią się co najwyżej o 1, więc w k -tej kolumnie są wszystkie liczby całkowite z przedziału $[m_k, M_k]$.

Gdy $\max\{m_1, \dots, m_n\} \leq \min\{M_1, \dots, M_n\}$, wówczas pewna liczba całkowita należy do wszystkich przedziałów $[m_1, M_1], \dots, [m_n, M_n]$. Jest ona obecna we wszystkich kolumnach, więc występuje $\geq n$ -krotnie na planszy.

Gdy zaś $\max\{m_1, \dots, m_n\} > \min\{M_1, \dots, M_n\}$, znaczy to, że dla pewnych numerów kolumn k, l zachodzi nierówność $m_k \leq M_k < m_l \leq M_l$. Weźmy dowolny wiersz. Na przecięciu z kolumnami k i l są w tym wierszu: pewna liczba $\leq M_k$ oraz pewna liczba $\geq m_l$; zatem są w tym wierszu wszystkie liczby całkowite z przedziału $[M_k, m_l]$. Wiersz był dowolny, czyli każda z tych liczb (np. M_k) jest obecna we wszystkich wierszach – występuje wobec tego $\geq n$ razy. To uzasadnia odpowiedź.

780. Podaną równość rekurencyjną podnosimy stronami do kwadratu (zastępując literkę n literką k) i dostajemy równoważną zależność

$$x_{k+1}^2 - x_k^2 = 2 + x_k^{-2}.$$

Dodajemy te równości dla $k = 0, \dots, n-1$, otrzymując

$$(1) \quad x_n^2 - 1 = 2n + \sum_{k=0}^{n-1} x_k^{-2}.$$

Stąd od razu widać, że $x_n > \sqrt{2n}$ (dla $n > 0$), i wobec tego

$$(2) \quad \sum_{k=0}^{n-1} x_k^{-2} = 1 + \sum_{k=1}^{n-1} x_k^{-2} < 1 + \sum_{k=1}^{n-1} \frac{1}{2k} = 1 + \frac{1}{2}H_{n-1},$$

gdzie – jak zwykle – H_m oznacza sumę odwrotności liczb naturalnych od 1 do m . Zależności (1) i (2) dają oszacowanie

$$x_n^2 < 2n + 2 + \frac{1}{2}H_{n-1}.$$

Skoro $x_n > \sqrt{2n}$, mamy stąd

$$(3) \quad 0 < x_n - \sqrt{2n} = \frac{x_n^2 - 2n}{x_n + \sqrt{2n}} < \frac{x_n^2 - 2n}{2\sqrt{2n}} < \frac{2 + \frac{1}{2}H_{n-1}}{2\sqrt{2n}}.$$

Liczby uzyskane po prawej stronie tworzą ciąg zbieżny do zera; wynika to na przykład ze znanej równości asymptotycznej $H_n \sim \ln n$; albo – bardziej elementarnie – z nierówności $H_n < 3n^{1/3}$ (nie trudnej do wykazania przez indukcję). Dwustronne oszacowanie (3) pokazuje, że

$$\lim_{n \rightarrow \infty} (x_n - \sqrt{2n}) = 0.$$

Czołówka ligi zadaniowej **Klub 44 M** po uwzględnieniu ocen rozwiązań zadań 773 ($WT = 1,78$) i 774 ($WT = 1,87$) z numeru 1/2019

| | | |
|------------------------|-----------|-------|
| Witold Bednarek | Łódź | 41,66 |
| Jerzy Cisło | Wrocław | 41,51 |
| Franciszek S. Sikorski | Warszawa | 40,74 |
| Paweł Najman | Kraków | 39,69 |
| Paweł Kubit | Kraków | 39,40 |
| Krzysztof Kamiński | Pabianice | 37,32 |
| Michał Koźlik | Gliwice | 35,73 |

Klub 44 F



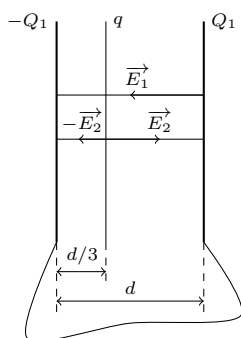
Rozwiązania zadań z numeru 4/2019

Redaguje Elżbieta ZAWISTOWSKA

Przypominamy treść zadań:

676. Między zwartymi drutem okładkami nienaładowanego kondensatora płaskiego znajduje się punktowy ładunek q . Powierzchnia okładki jest bardzo duża, efekty brzegowe możemy zaniedbać. Odległość ładunku od jednej z okładek jest równa $d/3$, gdzie d jest odległością między okładkami. Jaki ładunek przepłynie przez przewodnik zwierający okładki, gdy ładunek q zostanie przesunięty w miejsce wewnątrz kondensatora, odległe o $d/3$ od drugiej okładki?

677. Oszacuj, jaki musi być minimalny promień planety, aby mogła ona utrzymać atmosferę składającą się głównie z tlenu i azotu, jeśli temperatura powierzchni planety $T = 300$ K. Średnia gęstość planety $\rho = 4 \cdot 10^3$ kg/m³.



676. Ponieważ okładki kondensatora są bardzo duże, wartość indukowanych na nich ładunków nie zmienia się podczas przemieszczania ładunku q równoległe do okładek (zmienia się tylko ich rozkład). Oznacza to, że wartość ładunków indukowanych nie zmienia się również wtedy, gdy ładunek q zostanie równomiernie „rozmaźany” na powierzchni równoległej do okładek kondensatora (rysunek). Ładunki Q_1 i $-Q_1$ wytwarzają między okładkami kondensatora jednorodne pole o natężeniu $E_1 = Q_1/(\epsilon_0 S)$, gdzie S jest powierzchnią okładek. Płaszczyzna wewnątrz kondensatora naładowana ładunkiem q wytwarza pole o natężeniu $E_2 = q/(2\epsilon_0 S)$. Napięcie między płaszczyzną naładowaną ładunkiem q a lewą okładką wynosi $U_1 = (E_1 + E_2)d/3$, napięcie między tą samą płaszczyzną i prawą okładką $U_2 = 2d(E_2 - E_1)/3$. Jednocześnie napięcie między okładkami zwartego kondensatora wynosi 0, stąd $U_1 = U_2$, $3E_1 = E_2$, $Q_1 = q/6$. Analogicznie ładunek na prawej okładce po przesunięciu ładunku q w położenie końcowe jest równy $Q'_1 = -q/6$. Szukany ładunek przepływający między okładkami kondensatora podczas przemieszczania ładunku punkowego q dany jest wzorem $\Delta q = Q_1 - Q'_1 = q/3$.

677. Cząsteczka wchodząca w skład atmosfery jest utrzymywana w bezpośrednim sąsiedztwie planety, gdy jej energia całkowita spełnia warunek $\frac{m}{2} \langle v^2 \rangle - \frac{GmM}{r} \leq 0$, gdzie m jest masą cząsteczki, $\langle v^2 \rangle$ średnim kwadratem jej prędkości, G stałą grawitacji, M masą planety oraz r jej promieniem. Korzystając ze związku między masą a gęstością planety, otrzymujemy następujące oszacowanie:

$$\langle v^2 \rangle \approx \frac{8\pi}{3} G \rho r_{min}^2.$$

Z drugiej strony, średni kwadrat prędkości cząsteczki gazu związany jest z jego temperaturą T zależnością $\langle v^2 \rangle = \frac{3kT}{m} = \frac{3RT}{\mu}$, gdzie k jest stałą Boltzmanna, R stałą gazową, μ masą molową gazu. Stąd

$$r_{min} \approx \sqrt{\frac{9RT}{8\pi G \rho \mu}}.$$

Ponieważ masa molowa azotu jest mniejsza od masy molowej tlenu, w celu naszego oszacowania możemy przyjąć, że atmosfera składa się tylko z azotu, którego masa molowa $\mu_N = 28$ g/mol. Ostatecznie $r_{min} \approx 300$ km.

Powyższe oszacowanie uwzględnia jedynie wartość średniej kwadratu prędkości. W rzeczywistości cząsteczki gazu poruszają się z różnymi prędkościami (rozkład Maxwella), co oznacza, że część cząsteczek ma prędkości powyżej średniej i te będą mogły uciec od planety o minimalnym wyznaczonym powyżej promieniu. W bardziej dokładnym oszacowaniu poszukiwany minimalny promień będzie więc większy.

Czołówka ligi zadaniowej **Klub 44 F** po uwzględnieniu ocen rozwiązań zadań 670 ($WT = 2,35$), 671 ($WT = 1,75$), 672 ($WT = 2,35$), 673 ($WT = 3,77$) z numerów 1/2019 i 2/2019

| | | |
|--------------------|-----------|-------|
| Marian Łupieżowicz | Gliwice | 44,03 |
| Tomasz Rudny | Poznań | 40,98 |
| Jan Zambrzycki | Białystok | 39,90 |
| Tomasz Wietecha | Tarnów | 38,43 |
| Krzysztof Magiera | Łosiów | 31,73 |
| Jacek Konieczny | Poznań | 29,80 |
| Mateusz Kapusta | Wrocław | 29,09 |
| Ryszard Woźniak | Kraków | 28,77 |
| Michał Koźlik | Gliwice | 27,47 |

Skrót regulaminu

Każdy może nadsyłać rozwiązania zadań z numeru n w terminie do końca miesiąca $n + 2$. Szkice rozwiązań zamieszczamy w numerze $n + 4$. Można nadsyłać rozwiązania czterech, trzech, dwóch lub jednego zadania (każde na oddzielnej kartce), można to robić co miesiąc lub z dowolnymi przerwami. Rozwiązania zadań z matematyki i z fizyki należy przysyłać w oddzielnych kopertach, umieszczając na kopercie dopisek: **Klub 44 M** lub **Klub 44 F**. Można je przysyłać również pocztą elektroniczną pod adresem delta@mimuw.edu.pl (preferujemy pliki pdf). Oceniamy zadania w skali od 0 do 1 z dokładnością do 0,1. Ocenę możemy przez

współczynnik trudności danego zadania: $WT = 4 - 3S/N$, gdzie S oznacza sumę ocen za rozwiązania tego zadania, a N – liczbę osób, które nadesłały rozwiązanie choćby jednego zadania z danego numeru w danej konkurencji (**M** lub **F**) – i tyle punktów otrzymuje nadsyłający. Po zgromadzeniu 44 punktów, w dowolnym czasie i w którejkolwiek z dwóch konkurencji (**M** lub **F**), zostaje on członkiem **Klubu 44**, a nadwyżka punktów jest zaliczana do ponownego udziału. Trzykrotne członkostwo – to tytuł **Weterana**. Szczegółowy regulamin został wydrukowany w numerze 2/2002 oraz znajduje się na stronie deltami.edu.pl.

Prosto z nieba: Masa Galaktyki

Masa Drogi Mlecznej jest jedną z najbardziej istotnych wielkości, jakie astronomowie mogą wyznaczyć. Pomimo dziesięcioleci intensywnego wysiłku otrzymane szacunki masy Drogi Mlecznej różnią się znacząco, wahając się od 500 miliardów do 3 bilionów mas Słońca (M_{\odot}). Ta duża niepewność wynika przede wszystkim z różnych metod stosowanych do pomiaru rozkładu ciemnej materii, która stanowi około 90% masy Galaktyki. Ciemna materia jest odpowiedzialna m.in. za wytwarzanie potencjału grawitacyjnego, w którym zanurzony jest dysk Galaktyki. Problemem jest oczywiście fakt, że tego, czego nie widać, nie można badać metodami astronomicznymi, czyli analizą emitowanych fotonów. Prowadzi to do dużej niepewności pomiarowej.

Biorąc pod uwagę tajemniczą naturę ciemnej materii, zespół obserwatorów (iopscience.iop.org/article/10.3847/1538-4357/ab089f/meta) do oszacowania masy Drogi Mlecznej użył sprytnej metody, która polegała na pomiarze prędkości gromad kulistych.

Najdokładniejszych do tej pory pomiarów dokonano, łącząc dane z misji Gaia Europejskiej Agencji Kosmicznej (ESA) z obserwacjami teleskopu kosmicznego Hubble'a (NASA/ESA). Satelitarny teleskop Gaia, znajdujący się w punkcie Lagrange'a L_2 pomiędzy Ziemią a Słońcem, został zaprojektowany do stworzenia precyzyjnej trójwymiarowej mapy obiektów astronomicznych i do śledzenia ich ruchów. Najnowsze dane obejmują pomiary pozycji gromad kulistych znajdujących się aż do 65 000 lat świetlnych od Ziemi.

Zespół badaczy połączył te dane z obserwacjami teleskopu Hubble'a słabych i odległych gromad kulistych, znajdujących się nawet 130 000 lat świetlnych od Ziemi. Ponieważ teleskop Hubble'a obserwował niektóre z tych obiektów nawet przez 10 lat, możliwe było dokładne wyznaczenie prędkości tych gromad.

Im bardziej masywna galaktyka, tym szybciej znajdujące się w niej gromady gwiazd poruszają się pod wpływem jej siły grawitacji. Metodami astronomicznymi łatwo mierzy się *prędkość radialną* (wzdłuż linii widzenia), która jest związana ze zmianą koloru światła. Dzięki precyzyjnym pomiarom zebranych przez oba teleskopy astronomowie byli w stanie zmierzyć także prędkość prostopadłą do linii widzenia. Pozwoliło to obliczyć prędkość całkowitą gromad i oszacować potencjał grawitacyjny, a z niego wywnioskować masę Galaktyki.

W efekcie astronomowie obliczyli, że masa zawarta w kuli o promieniu 130 000 lat świetlnych od centrum Galaktyki waży około 1,5 biliona M_{\odot} . Wiedza o zawartości ciemnej materii w Galaktyce i jej rozkładzie jest wykorzystywana do opisu powstawania i ewolucji struktur we Wszechświecie. Dokładne określenie masy Galaktyki przybliży nas do zrozumienia rozkładu ciemnej materii w naszej Galaktyce, a co za tym idzie – w podobnych galaktykach spiralnych.

Michał BEJGER

Gromady kuliste to gęste skupiska gwiazd, które krążą w dużych odległościach wokół spiralnego dysku Galaktyki.

Niebo w sierpniu

Sierpień to pierwszy miesiąc po przesileniu letnim, z bardzo wyraźnie skraccającymi się dniami i wydłużającymi nocami. W jego trakcie wysokość górowania Słońca obniży się o ponad 10° , a długość przebywania nad widnokregiem w środkowej Polsce skróci się o prawie dwie godziny. Wraz z początkiem miesiąca kończy się w Polsce sezon na obserwacje łuku okołohoryzontalnego i obłoków srebrzystych. Jak co roku w sierpniu maksimum swojej aktywności mają meteory z roju Perseidów, lecz w tym roku ich obserwacje popsuje Księżyc w fazie bliskiej pełni, przyćmiewając większość z nich.

W zeszłym miesiącu wszystkie planety typu ziemskiego ginęły w blasku Słońca. Teraz planety **Wenus** i **Mars** nadal pozostaną niewidoczne. Wenus w połowie miesiąca spotka się ze Słońcem, przechodząc przez koniunkcję górną. Oznacza to, że planeta jest oddalona od Ziemi maksymalnie w swoim, trwającym 584 dni, cyklu synodycznym, a w związku z tym porusza się najwolniej względem gwiazd tła. Przez to do końca sierpnia nie oddali się zbyt od niego, a osiągnięcie odpowiedniej do jej zaobserwowania elongacji, w połączeniu z niekorzystnym nachyleniem ekliptyki do wieczornego widnokregu o tej porze roku, zajmie

jej prawie 3 miesiące. Wenus zacznie pojawiać się na niebie wieczornym dopiero w listopadzie, dążąc powoli do maksymalnej elongacji wschodniej pod koniec marca 2020 r. Planeta Mars również dąży do koniunktacji ze Słońcem (w przypadku Marsa i pozostałych planet zewnętrznych zawsze jest to koniunktacja górna), przez którą przejdzie na początku września, i będzie zbyt blisko naszej Gwiazdy Diennej, aby ją dostrzec. Po koniunktacji Czerwona Planeta przeniesie się na niebo poranne i już w październiku da się ją dostrzec na całkiem ciemnym niebie tuż przed świtem.

Dobrze za to na początku miesiąca jest widoczna planeta **Merkury**, która 10 sierpnia osiągnie maksymalną elongację zachodnią. Niestety, jak zawsze przy dobrej widoczności na dużych północnych szerokościach geograficznych, planeta oddali się wtedy od Słońca na zaledwie 19° i na godzinę przed świtem zajmie pozycję na wysokości niecałych 5° nad wschodnim widnokręgiem. Merkurego da się obserwować do początku drugiej dekady sierpnia. Jak zawsze w czasie widoczności porannej Merkury (i Wenus) dąży od koniunktacji dolnej do koniunktacji górnej, oddalając się od Ziemi, a zatem w tym czasie tarcza planety skurczy się z 9 do $6''$, zaś faza urośnie z 25 do 80%. Zwiększy się też jasność planety z $+1$ do -1^m . Warto zapamiętać, że 17 sierpnia Merkury przejdzie niecały 1° na południe od jasnej gromady otwartej gwiazd M44. U nas tło nieba będzie zdecydowanie za jasne, aby obserwować tę koniunktację, ale warto o niej pamiętać, jeśli ktoś wyjeżdża gdzieś dalej na południe od Polski.

Z planetarnych gazowych olbrzymów pierwsze dwa, **Jowisz** i **Saturn**, przeniosą się na niebo wieczorne i ich warunki obserwacyjne wyraźnie się pogorszą. Pomoże natomiast skracający się dzień i mimo że zmniejsza się ich odległość do Słońca, to można je obserwować coraz wcześniej, dzięki czemu pogorszenie nie postępuje tak szybko. W sierpniu Jowisz znika z nieboskłonu około północy, Saturn – dwie godziny później. Dokładnie 20 lat po pamiętnym całkowitym zaćmieniu Słońca, którego pas przechodził m.in. przez Europę Środkową, czyli 11 sierpnia, Jowisz zmieni kierunek swojego ruchu na prosty. To oznacza, że w sierpniu niemal nie przesuwa się on względem gwiazd tła, zatrzymując się prawie na linii łączącej gwiazdy Sabik z Wężownika i Antares ze Skorpiona. Kończy się także okres najlepszej widoczności Jowisza i planeta zacznie dość szybko tracić rozmiar kątowy i jasność. Planeta Saturn też zmieni kierunek ruchu, ale dopiero w drugiej połowie września, a zatem w sierpniu wciąż porusza się ona ruchem wstecznym. Do końca miesiąca jasność Jowisza spadnie z $-2,4$ do $-2,2^m$, a średnica jego tarczy z 42 do $39''$. W tym samym czasie Saturn zmniejszy blask do $+0,3^m$, przy tarczy o średnicy $18''$.

Ostatnie dwie planety Układu Słonecznego w sierpniu widoczne są bardzo dobrze. Wznoszą się zdecydowanie wyżej od Jowisza i Saturna, a ponadto zbliżają się do swoich opozycji. **Neptun** znajdzie się po przeciwnej stronie Ziemi niż Słońce 10 września, zaś **Uran** – 28 października. Neptun przez cały sierpień przesuwa się

ruchem wstecznym, zbliżając się do gwiazdy 4. wielkości ϕ Aquarii. Ostatniego dnia miesiąca planeta zbliży się do niej na niecałe $8'$. Przy czym jasność planety to $+7,8^m$. Planeta Uran zacznie poruszać się ruchem wstecznym 12 sierpnia, dlatego początkowo pozostanie prawie nieruchoma względem gwiazd tła. Niestety w tym roku Uran nie towarzyszy jaśniejszej od siebie gwiazdzie, która byłaby wskazówką w jego odszukaniu. Można posilkować się tutaj Hamalem, najjaśniejszą gwiazdą Barana o jasności $+2^m$. Uran kreśli swoją pętlę jakieś 11° na południe od niej, świecąc z jasnością obserwowaną $+5,8^m$. Neptun góruje po godzinie 2, na wysokości przekraczającej 30° , zaś Uran przechodzi przez południk centralny w okolicach wschodu Słońca, ale na końcu nocy astronomicznej wznosi się na ponad 40° .

Księżyc zacznie sierpień od nowiu pierwszego dnia miesiąca, a potem przeniesie się na niebo wieczorne. Jednak niskie nachylenie ekliptyki do widnokręgu o tej porze doby sprawi, że przez pierwszych kilkanaście dni Srebrny Glob nie wzniesie się zbyt wysoko. Na szczęście Księżyc przejdzie wtedy na północ od ekliptyki, dzięki czemu da się go dostrzec przed I kwadrą. W pierwszym tygodniu miesiąca, 5 i 6 sierpnia, księżycowy sierp w fazie 30 i 40% minie Spikę, najjaśniejszą gwiazdę Panny. Kolejnego dnia, w I kwadrze, przejdzie $3,5^\circ$ od Zuben Elgenubi, gwiazdy α w Wadze. Do Jowisza Srebrny Glob, oświetlony w 72%, zbliży się 9 sierpnia na 2° , zaś 12 sierpnia, już prawie w pełni, pokaże się 5° od Saturna. Dokładnie w połowie miesiąca, 15 sierpnia, naturalny satelita Ziemi przejdzie przez pełnię, a 2 dni później, z tarczą oświetloną w 95% dotrze na 5° do Neptuna. W podobnej odległości do Urana wejdzie 21 sierpnia, przy fazie zmniejszonej do 67%. Dwa dni później po południu naszego czasu Księżyc przejdzie przez ostatnią kwadrę, a 24 sierpnia – przez Hiady, zakrywając świecące z jasnościami obserwowanymi od $+3,8$ do $+4,8^m$ gwiazdy $\delta 1$, $\delta 2$ i $\delta 3$ Tau, lecz niestety wszystkie już po wschodzie Słońca. O świcie Księżyc zbliży się do Aldebarana, najjaśniejszej gwiazdy Byka, na niecałe 4° .

W ostatnich dniach miesiąca Księżyc podąży ku nowiu, przez który przejdzie 30 sierpnia. Rano nachylenie ekliptyki do widnokręgu jest bardzo korzystne do obserwacji Księżyca prawie do samego nowiu. Znakomicie widoczne będzie tzw. światło popielate, czyli jego nocna część, oświetlona światłem odbitym od Ziemi. 26 sierpnia, w fazie 24%, Srebrny Glob zbliży się na niecały 1° do gwiazdy Tejat Prior, η Gem, zaś dobę później, sierpem zwężonym do 15%, Księżyc zakryje gwiazdę Wasat (δ Gem). Również tym razem Polska ma pecha i zjawisko zacznie się tuż po wschodzie Słońca. Nieco ponad dobę przed nowiem, 29 sierpnia, na godzinę przed świtem Księżyc zdąży się wnieść na wysokość 7° , prezentując tarczę w fazie zaledwie 2%.

Ariel MAJCHER

Informatyczny kącik olimpijski (130):

Kwadraty liczb naturalnych

W tym odcinku omówimy rozwiązanie zadania „Kwadraty liczb naturalnych”, które pojawiło się na finale Zawodów Indywidualnych XIII Młodzieżowej Olimpiady Informatycznej.

Kwadraty liczb naturalnych: *Piotr jest zafascynowany kwadratami liczb naturalnych, czyli liczbami: 1, 4, 9, 16, 25, ... Chłopiec ma przed sobą ciąg n liczb naturalnych $a = (a_1, a_2, \dots, a_n)$. Ile jest takich par liczb naturalnych w ciągu a , że ich iloczyn jest kwadratem liczby naturalnej?*

Niech m oznacza wartość największej liczby w ciągu a , zaś M niech oznacza największy iloczyn pary liczb w ciągu a .

Rozwiązanie $O(n^2 \cdot \sqrt{M})$

Zacznijmy od rozwiązania, w którym obliczamy iloczyn każdej z $\frac{n(n-1)}{2}$ par elementów ciągu a . Następnie zliczamy te iloczyny, które są kwadratami liczb naturalnych. Załóżmy, że chcemy sprawdzić, czy x jest kwadratem. W tym celu przeglądamy kwadraty kolejnych liczb naturalnych: $2^2, 3^2, 4^2, \dots$. Jeśli trafimy na x , to odpowiedź jest pozytywna. Jeśli trafimy na liczbę większą niż x , wtedy przerywamy działanie i odpowiedź jest negatywna. Tym sposobem rozważymy $O(\sqrt{x})$ kwadratów. Zatem rozwiązanie działa w czasie $O(n^2 \cdot \sqrt{M})$.

Rozwiązanie $O(n^2 \cdot \log(m))$

Przyspieszmy sprawdzanie, czy x jest kwadratem. Zaaplikujmy algorytm wyszukiwania binarnego na ciąg kwadratów: $1^2, 2^2, \dots, x^2$. Algorytm wykona $O(\log(x))$ operacji. Całe rozwiązanie działa w czasie $O(n^2 \cdot \log(m))$.

Szkie rozwiązanie optymalnego

Zauważmy, że w rozkładzie na czynniki pierwsze kwadratu liczby naturalnej każdy czynnik pierwszy występuje parzyście wiele razy. Zatem iloczyn dwóch liczb jest kwadratem, jeśli zbiory czynników pierwszych występujących nieparzyście wiele razy w rozkładzie obu liczb są takie same. Niech więc $b = (b_1, b_2, \dots, b_n)$, gdzie b_i oznacza iloczyn czynników pierwszych, które występują nieparzyście wiele razy w rozkładzie a_i . Innymi słowy, b_i to a_i podzielone przez swój największy dzielnik będący kwadratem. Wówczas $a_i \cdot a_j$ jest kwadratem, jeśli $b_i = b_j$. Zatem wynikiem jest liczba par takich samych elementów w ciągu b .

Zliczanie par

Założmy przez chwilę, że znamy ciąg b i chcemy policzyć liczbę par elementów o takich samych wartościach. W tym celu wystarczy posortować ciąg niemalejąco. Wówczas elementy o tych samych wartościach znajdą się obok siebie (będą tworzyły bloki). Następnie przeglądamy kolejne bloki elementów i zliczamy pary. W k -elementowym bloku można wybrać $\frac{k(k-1)}{2}$ par. Sortowanie realizujemy w czasie $O(n \cdot \log(n))$, podział na bloki odbywa się w czasie $O(n)$. Zatem zliczanie par tych samych elementów w ciągu b odbywa się w czasie $O(n \cdot \log(n))$.

Wyznaczenie ciągu b w $O(n \cdot \sqrt{m})$

Wartość b_i dla każdego i od 1 do n liczymy niezależnie. Początkowo niech $b_i = a_i$ dla każdego i . Następnie przeglądamy kolejne kwadraty $(2^2, 3^2, \dots, (\lfloor \sqrt{a_i} \rfloor)^2)$ jako

kandydatów na dzielniki a_i . Jeśli rozpatrywany kwadrat jest dzielnikiem b_i , to dzielimy b_i przez ten kwadrat. W ten sposób z rozkładu na czynniki pierwsze usuniemy kwadraty.

Wyznaczenie ciągu b w $O(n \cdot \frac{\sqrt{m}}{\log(m)})$ (*)

Zauważmy, że nie ma potrzeby przeglądania wszystkich kwadratów. Wystarczy rozważać kwadraty liczb pierwszych $(2^2, 3^2, 5^2, \dots)$. Pamiętajmy o tym, że kwadrat może wielokrotnie występować w rozkładzie na czynniki pierwsze. Wtedy musimy usunąć wszystkie jego wystąpienia. Przykładowo: liczbę $48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3$ musimy dwukrotnie podzielić przez 2^2 . Każda liczba zostanie podzielona co najwyżej $O(\log(m))$ razy. Liczbę liczb pierwszych w przedziale $[1; \lfloor \sqrt{m} \rfloor]$ szacujemy jako $\frac{\sqrt{m}}{\log(m)}$. Stąd całkowita złożoność wynosi $O(n \cdot \frac{\sqrt{m}}{\log(m)})$.

Wyznaczenie ciągu b w $O(n \cdot \log(m) + m)$ ()**

Na początku zliczmy wystąpienia liczb w ciągu a . Niech $Z_w = \{i \mid a_i = w\}$ (zbiór indeksów elementów ciągu a o wartości w). Następnie przeglądamy kwadraty liczb pierwszych z przedziału $[1; m]$ jako potencjalne dzielniki. Załóżmy, że rozpatrujemy kwadrat p^2 . Wiemy, że jest on dzielnikiem: $1 \cdot p^2, 2 \cdot p^2, 3 \cdot p^2, \dots, \lfloor \frac{m}{p^2} \rfloor \cdot p^2$. Dla każdej z tych wartości, korzystając z tablicy zliczającej Z , odwołujemy się bezpośrednio do elementów, które są podzielne przez p^2 , i te elementy dzielimy przez p^2 . Po zakończeniu otrzymane wartości tworzą ciąg b . Do każdego elementu ciągu odwołamy się co najwyżej $O(\log(m))$ razy. Liczba rozpatrywanych wielokrotności wynosi: $\frac{m}{2^2} + \frac{m}{3^2} + \frac{m}{5^2} + \dots$, co w sumie wynosi $O(m)$. Zatem otrzymaliśmy rozwiązanie działające w czasie $O(n \cdot \log(m) + m)$.

Wyznaczenie ciągu b w $O(n \cdot \frac{\sqrt[4]{m}}{\log(m)} + m^{\frac{3}{4}})$

Połączmy dwa poprzednie rozwiązania (*) i (**). Najpierw, podobnie jak w (*), dla każdego elementu ciągu a rozważmy jego potencjalne dzielniki (kwadraty liczb pierwszych), nie większe niż \sqrt{m} . Takich dzielników jest $O(\frac{\sqrt{m}}{\log(m)})$. Następnie zaaplikujmy rozwiązanie (**) z drobną zmianą. Rozpatrujemy tylko wielokrotności kwadratów liczb pierwszych większych od \sqrt{m} . Niestety, tak opisane rozwiązanie nadal wymaga utworzenia tablicy zliczającej rozmiaru $O(n + m)$. Do implementacji tablicy zliczającej wystarczy użyć tablicy mieszającej (tablicy z haszowaniem) i problem zostaje rozwiązany. Otrzymujemy algorytm, który działa w czasie $O(n \cdot \frac{\sqrt[4]{m}}{\log(m)} + m^{\frac{3}{4}})$. Dowód tego oszacowania pozostawiam Czytelnikowi. Jednocześnie zachęcam do pomyślenia nad lepszym oszacowaniem.

Bartosz ŁUKASIEWICZ

Gdy zadaniu nie podołasz, to ułatwi je niezmiennik

Bartłomiej BZDEGA



Niezmiennikiem nazywamy tę własność obiektów, która zostaje zachowana po poddaniu ich wybranym przekształceniom. Jeśli chcemy wykazać, że obiekt X nie może zostać przekształcony w obiekt Y za pomocą danych reguł, to wystarczy znaleźć ich niezmiennik, który przyjmuje różne wartości dla obiektów X i Y .

Aby to wyjaśnić, rozwiążemy następujące zadanie: *Czy goniec szachowy może za pomocą legalnych ruchów dostać się z pola B2 na pole H7?*

Goniec porusza się po liniach skośnych, więc kolor pola, na którym stoi, pozostaje bez zmian. Pole B2 jest czarne, natomiast pole H7 jest białe. Z tego wynika negatywna odpowiedź na postawione pytanie.

W tym przykładzie przekształceniami są ruchy gońca, rozważanym obiektem jest pole, na którym on stoi (na początku B2, na końcu H7), a niezmiennikiem – kolor tego pola.

Zadania

1. Czy w wyrażeniu $1 + 2 + 3 + \dots + 10$ można zamienić niektóre znaki „+” na „-” w ten sposób, by wynik był równy 0?
2. Na tablicy napisano 15 trzycyfrowych liczb pierwszych. Możemy zmasać dwie zapisane na tablicy liczby i zamiast nich zapisać wartość bezwzględną ich różnicy. Postępujemy tak aż do momentu, gdy na tablicy pozostanie jedna liczba. Czy tą liczbą może być 44?
3. W kręgu stoi 16 drzew, na każdym siedzi jeden wróbel. Wróble przelatują czasem na inne drzewa, ale zgodnie z regułą: dwa wróble lecą jednocześnie, każdy na drzewo sąsiadujące z tym, na którym siedział, jeden zgodnie, a drugi przeciwnie do ruchu wskazówek zegara. Czy jest możliwe, aby w pewnej chwili wszystkie wróble siedziały na tym samym drzewie?
4. Jedno dziecko ma 10 cukierków, drugie 15, a trzecie 20. Każde z nich może w dowolnej chwili dać po jednym swoim cukierku pozostałej dwójce. Czy dzieląc się w ten sposób, dzieci mogą doprowadzić do tego, by każde z nich miało 15 cukierków?
5. W punktach $(0, 0)$, $(0, 1)$, $(1, 1)$ i $(1, 0)$ stoją pionki. Dozwolony ruch polega na wyborze dwóch pionków, a następnie przestawieniu jednego z nich na punkt płaszczyzny symetryczny względem punktu zajmowanego przez drugi pionek. Czy jest możliwe, aby po pewnej liczbie ruchów dwa pionki stanęły w tym samym miejscu?
6. Pionki stoją w punktach $(0, 0)$, $(0, 1)$ i $(1, 0)$, reguły postępowania takie jak w poprzednim zadaniu. Rozstrzygnąć, czy możliwe jest ustawienie pionków w wierzchołkach trójkąta, we wnętrzu którego znajduje się punkt o obu współrzędnych całkowitych.
7. Na każdym polu szachownicy 8×8 stoi pionek. Jeżeli na pierwszym i trzecim z trzech kolejnych pól leżących w jednym wierszu, kolumnie lub diagonalu stoi co najmniej jeden pionek, to możemy wziąć z nich po jednym pionku i przełożyć na drugie z tych pól. Rozstrzygnąć, czy można, wykonując takie ruchy, przełożyć wszystkie pionki na jedno pole.
8. Na polu A1 szachownicy 8×8 napisano liczbę 1, na A8 napisano -1 , a na pozostałych polach 0. Możemy wielokrotnie wykonywać następującą operację: wybieramy dowolne pole i zmniejszamy napisaną na nim liczbę o liczbę pól sąsiednich (mających wspólny bok), zaś każdą z liczb napisanych na polach sąsiednich zwiększamy o 1. Rozstrzygnąć, czy można doprowadzić do stanu, w którym na wszystkich polach szachownicy napisana jest liczba 0.
9. Płaszczyznę podzielono na trójkąty równoboczne w ten sposób, że w każdym wierzchołku (węźle) spotyka się sześć trójkątów. W każdym węźle znajduje się lampka, natomiast na każdym trójkącie jest włącznik, który zmienia stan lampek (świeci albo nie świeci) znajdujących się w węzłach będących wierzchołkami tego trójkąta. Rozstrzygnąć, czy zaczynając od sytuacji, w której świeci się dokładnie jedna lampka, możemy doprowadzić do zgaszenia wszystkich lampek.

Wskazówki do zadań

1. Jeśli zamienimy „+” na „-”, to wartość całego wyrażenia zmaleje o $2k$, więc nie zmieni się jego parzystość. Początkowa suma jest nieparzysta, więc niemożliwe jest osiągnięcie wartości parzystej.
2. Liczby a i b zastępujemy liczbą $|a - b|$, więc suma liczb na tablicy zmniejsza się o $a + b - |a - b| = 2 \min\{a, b\}$, czyli nie zmienia się jej parzystość.
3. Pominęliśmy drzewa kolejno liczbami od 1 do 16. Każdemu wróbelowi przypisujemy jego pozycję, czyli numer drzewa, na którym siedzi. Należy zauważyć, że suma pozycji wszystkich wróbli może się zmienić jedynie o wielokrotność 16, więc nie zmienia się jej reszta z dzielenia przez 16.
4. Niech a, b, c oznaczają liczby cukierków dzieci. Należy zauważyć, że wartość wyrażenia $b - a$ może się zmienić jedynie o wielokrotność 3, więc ma ono stałą resztę z dzielenia przez 3.
5. Odbijając punkt A symetrycznie względem punktu S, otrzymamy taki punkt A', którego obie współrzędne są tej samej parzystości, co odpowiednie współrzędne punktu A.
6. Niezmiennikiem jest pole trójkąta wyznaczanego przez pionki. Pole trójkąta o wierzchołkach kratowych, w którego wnętrzu jest punkt kratowy, wynosi co najmniej $3/2$ (dla czego?).
7. Podczas przestawiania pionków nie zmienia się (odpowiednio zdejmowany) „rodek ciężkości” rozgrywki.
8. Wykonując tę operację, nie zmieniamy parzystości sumy liczb wpisanych na wybranej przekątnej szachownicy.
9. Podzielmy płaszczyznę na sześciokąty, każdy złożony z sześciu trójkątów. Usunmy lampki znajdujące się w środkach tych sześciokątów. Wówczas parzystość liczby zaswieconych lampek będzie stała.



„O życiu na żywo. Biologia według Delty”

Chwała *Delcie* za znakomity pomysł zaproszenia Magdaleny Fikus do napisania felietonów do tego czasopisma. Pani Profesor, wybitna specjalistka w dziedzinie biologii molekularnej i genetyki, bardzo dobrze znana również ze swej działalności popularyzatorskiej, pokazała, że jest także wirtuozem felietonu popularnonaukowego. Czytelnicy *Delty* poznali jej znakomite teksty z cyklu *Życie na żywo*.

Z wielkim taktem, żywo, bez wpadania w moralizatorstwo – po mistrzowsku przedstawione rozmaite problemy z genetyki, ekologii i różnorodnych dziedzin biologii zostały zebrane w tomie *Biologia według Delty* (kolejnym po *Matematyce i Fizyce* również według *Delty*) zatytułowanym *O życiu na żywo*. Jest to prawdziwa uczta intelektualna.

Choć *Delta* kojarzy się głównie z matematyką, informatyką, fizyką i astronomią, to felietony Magdaleny Fikus mają zupełnie inny, niepowtarzalny charakter. Jaki? Trzeba koniecznie to sprawdzić! Zamiast przeglądać 94 *Delty*, wystarczy zajrzeć do jednej książki. Czytelnikom należy się jednak ostrzeżenie: to wciąga! I może uzależnić!

Zdzisław POGODA

