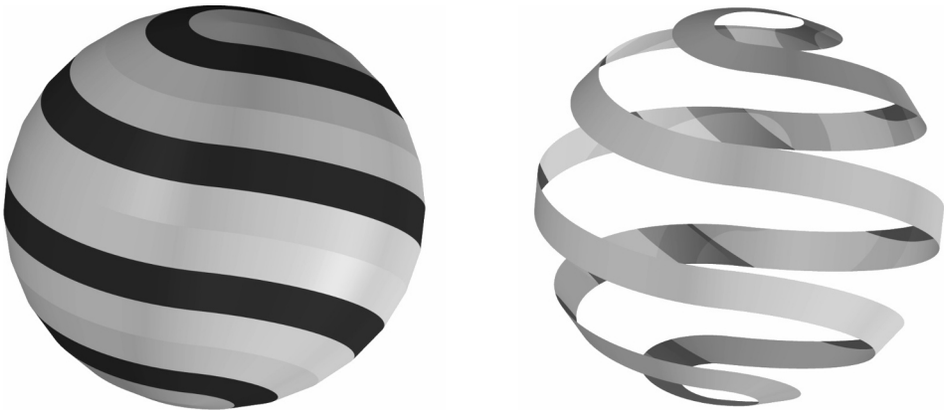
SPIS TREŚCI
NUMERU 1 (500)

W następnym numerze polecamy sferostożki



Czy coś takiego można poskładać z papieru?
Czy istnieje bryła, której każda ściana jest zapętlona?

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.

Adres do korespondencji:
Instytut Matematyki UW, Redakcja *Delty*, ul. Banacha 2, pokój 4020, 02-097 Warszawa, e-mail: `delta@mimuw.edu.pl` tel. 22-55-44-402.

Skład systemem TEX oraz rysunki techniczne wykonała Redakcja.

Wydrukowano w Drukarni Greg, ul. Górczewska 216 p. 101, 01-460 Warszawa.

PRENUMERATA
Garmond Press: `www.garmondpress.pl`

Kolporter: `www.kolporter.com.pl`

RUCH S.A.: `www.ruch.com.pl`, infolinia 804-200-600
Prenumerata realizowana przez RUCH S.A.:
Cena prenumeraty w 2016 roku wynosi 4 zł za egzemplarz.

Zamówienia na prenumeratę w wersji papierowej można składać bezpośrednio na stronie `www.prenumerata.ruch.com.pl`

Ewentualne pytania prosimy kierować na adres e-mail: `prenumerata@ruch.com.pl` lub kontaktując się z Centrum Obsługi Klienta RUCH pod numerem: 801 800 803 lub 22 693 70 00 – czynne w dni robocze w godzinach 7^{00}–17^{00}. Koszt połączenia wg taryfy operatora.

Numery archiwalne (od 1987 r.) można nabyć w Redakcji osobiście lub listownie.

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

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

Wydawca: Uniwersytet Warszawski **Cena 1 egzemplarza 4 zł**

Warsaw Center of Mathematics and Computer Science
`wcmcs.edu.pl`

Moja przygoda z najnowszą historią matematyki

*Paweł STRZELECKI**

Wybitny rosyjski geometra Michaił Gromow powiedział kiedyś w dokumentalnym programie telewizyjnym poświęconym Perelmanowi, że próba opowiadania zwykłemu odbiorcy o mocno zaawansowanej matematyce jest jak wspólna analiza chińskiego tekstu z kimś, kto chińskiego nie zna; po prostu nie należy tego robić. Skorzystam tym razem z tej rady (o Perelmanie i historii jego dokonań pisałem w *Delcie* 1/2004, a także w ostatnim rozdziale *Matematyki współczesnej dla myślących laików* i od merytorycznej strony nie mam nic istotnego do dodania). Z Czytelnikiem podzielę się kilkoma wrażeniami, które – za sprawą historii Perelmana i jego dowodu otwartej od 1904 roku hipotezy Poincarégo oraz późniejszej o 80 lat hipotezy geometryzacyjnej Thurstona, dowodu uznanego przez *Science* za naukowy przełom roku 2006 – są ze mną od lat i chyba mocniej kształtują moje poglądy niż czysto matematyczna treść tej historii.

O Thurstonie i hipotezie geometryzacyjnej można przeczytać w *Delcie* 1/2013.

1. W końcu sierpnia 2003 roku, wróciwszy do Bonn, gdzie wtedy przez chwilę był mój dom, z górskich wakacji przerwanych tygodniowym pobytem na konferencji w Oberwolfach, przeczytałem maila od Witka Sadowskiego, ówczesnego redaktora działu matematyki w *Delcie*, z pytaniem, czy nie miałbym pod ręką jakiegoś artykułu. Pomyślałem od razu, że muszę napisać o Perelmanie.

Odczuwałem wtedy bardzo intensywnie, że solidny kawał matematyki zmienia się na moich oczach. Podczas sierpniowego tygodnia w Oberwolfach, mimo koszmarnego upału i napiętego konferencyjnego programu, długo w noc słuchaliśmy dodatkowych wykładów; Gerd Huisken i Klaus Ecker, niemieccy specjaliści z pogranicza geometrii różniczkowej i analizy matematycznej, próbowali zawodowej, ale wcale nie tak wiele rozumiejącej publiczności wytłumaczyć, co (a raczej: jakim sposobem) zrobił właśnie Grigorij Jakowlewicz Perelman. Do dziś to żywo pamiętam. Chyba nigdy w życiu, z żadnej innej okazji nie miałem aż tak silnego wrażenia, że doświadczam czegoś historycznego. Różne odpryski i aspekty tamtej historii towarzyszą mi do dziś.

Wtedy, w 2003 roku, postąpiłem wbrew zaleceniu Gromowa i spróbowałem opowiedzieć także o matematyce. Dzięki *Delcie* i temu, co w jej nieco wcześniejszych numerach Czytelnicy mogli znaleźć, było to możliwe. Przypomnę:

– z tekstu Jarosława Górnickiego z *Delty* 6/1995 Czytelnik *Delty* dowiadywał się, jak wygląda pełna lista zwartych, orientowalnych rozmaitości dwuwymiarowych, tzn. takich powierzchni, które mają dwie strony, ale nie mają ani brzegu, ani żadnych nakłuć czy rozcięć, ani powyciąganych nieskończenie daleko odnóg;

– po informację, co to są rozmaitości trójwymiarowe (możliwe formy naszej przestrzeni, lokalnie, w małych fragmentach, przypominające do złudzenia zwykłą trójwymiarową przestrzeń), mogłem odesłać do artykułu Zbigniewa Marciniaka z *Delty* 5/1997;

– w *Delcie* 8/2000 sam napisałem o siedmiu problemach milenijnych Instytutu Claya, z nagrodami po milionie dolarów od sztuki;

– wreszcie, w *Delcie* 4/2003 (tzn. czystym przypadkiem akurat wtedy, gdy sam Perelman opowiadał o swoim dowodzie na kilku amerykańskich uniwersytetach – proszę jednak pamiętać, że cykl wydawniczy *Delty* jest dość długi) znajduje się artykuł o płynących krzywych i powierzchniach, z opowiastką o tym, co się dzieje, gdy wprawimy je w ruch ze zmienną, zależną od krzywizny prędkością (to akurat łatwo powiedzieć: krzywe zamknięte, choćby najbardziej fantazyjnie poskręcane, poruszając się z prędkością równą krzywiźnie, zaczynają stopniowo przypominać idealne okręgi; powierzchnie dwuwymiarowe wprawione w naturalny ruch podobnego typu mogą doznawać katastrof i rozpadać się na części, bo wąskie i długie rureczki kurczą się dużo szybciej niż kuliste, duże bąble).

2. Perelman ucieleśnia irytujące opinie o romantycznych, zdziwaczałych geniuszach zajmujących się matematyką. Jako szesnastolatek zdobył w 1982 roku złoty medal (i komplet punktów!) na Międzynarodowej Olimpiadzie Matematycznej. W wieku 24 lat obronił w Leningradzie doktorat. Przed trzydziestką pisał sążniste prace

*Instytut Matematyki, Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

Gdyby kilkanaście lat wcześniej, gdy sam kończyłem studia matematyczne, ktoś powiedział mi, że w przewidywalnej przyszłości owa hipoteza zostanie udowodniona, i to dzięki pomysłowi, żeby wyrównać kształt rozmaitości, poddając ją naturalnemu ruchowi opisanemu równaniami różniczkowymi cząstkowymi przypominającymi równanie ciepła i że w rozwiązaniu będzie więcej geometrii różniczkowej i twardej analizy niż topologii, z której problem pochodzi, uznałbym to za marne *science-fiction*. Życie jest jednak bogatsze niż pomysły marnych autorów oraz przekonania niedowiarków takich jak ja, a w matematyce chodzi o rozwiązywanie problemów i wszelkie metody, wszelkie chwyty, wszelkie wariackie i dalekosiężne pomysły są dozwolone – pod warunkiem, że ma się dość siły, żeby je realizować. Perelman miał.

John Ball, ówczesny przewodniczący Międzynarodowej Unii Matematycznej, wspominał o miłych, ale bezskutecznych rozmowach z Perelmanem, którego, pojechawszy do St. Petersburga, usiłował nakłonić do przyjęcia medalu i wizyty na kongresie.

z najlepszymi, grubo starszymi radzieckimi kolegami po fachu. Lata 1992–95 spędził w USA, w Nowym Jorku, Stony Brook i Berkeley. Tam poznał m.in. Richarda Hamiltona, autora pomysłu z pogranicza marzeń, aby trójwymiarowe rozmaitości wprawiać w ruch z prędkością zależną od tensora krzywizny (tak zwany potok Ricciego) i udowodnić hipotezę Poincarégo dzięki temu, że potok Ricciego lokalnie wygładza kształty i niweluje wszelkie fałdki sprawiające, że rozmaitość – może sfera, może torus, może inne fantazyjne dziwactwo – zaczyna wyglądać bardzo symetrycznie i równomiernie.

Problem w tym, że po drodze takie fantazyjne dziwactwo doznaje osobliwości, wpada samo na siebie, zwęża się i kurczy, więc trzeba o rozwiązaniach równań ruchu myśleć nieszablonowo, zapobiegać pojawianiu się osobliwości, umieć przewidzieć ich nadejście, umieć zrobić coś pozornie niemożliwego: przedłużyć ruch poza osobliwość, która jako taka do gładkiego świata geometrii różniczkowej nie należy. Hamilton nie potrafił tego projektu zrealizować w całości.

W 1995 roku Perelman wrócił do rodzinnego miasta (o zmienionej nazwie) i spędził kolejne 7 lat w Instytucie Stiekłowa, zmagając się z realizacją pomysłu Hamiltona. Między listopadem 2002 a lipcem 2003 roku udostępnił w Internecie trzy preprinty, w których anonsował dowód hipotezy geometryzacyjnej Thurstona. W ostatnim, napisanym już po pobycie z wykładami w Stanach, wskazywał, jak uprościć dowód w przypadku, który dotyczy jedynie hipotezy Poincarégo.

3. Między rokiem 2003 a 2006 kilka silnych zespołów matematyków przebrnęło przez zwięźle zapisane dowody Perelmana, i napisało ich swoje, znacznie dłuższe i bardziej szczegółowe wersje. Dlaczego dłuższe? Czy chodziło o łatanie luk? Otóż, wydaje się, że nie: z lektur i z rozmów z paroma kolegami ze świata, którzy byli blisko tego procesu, wyniosłem wrażenie, które mogę najprościej opisać za pomocą porównania: było tak, jakby sprawdzający wspinali się w górach drogą, skąpo przez zdobywcę opisaną i ponoć raz przebytą; czasem trzeba się namęczyć, napocić, cofnąć, żeby zrozumieć, co znaczy fraza „teraz 40 m trawersem w prawo w górę przez gładkie, nastromione płyty", potem jednak, gdzieś wyżej, widać stary hak zdobywcy, zostawione przez niego skórki pomarańczy i następny fragment ściany, wcześniej niewidoczny, lecz idealnie do opisu pasujący. Po serii takich zdarzeń nikt nie uważa, że ów opis drogi to produkt fantazji ambitnego grafomana, któremu się tylko wydaje, że jednak gdzieś był. Nie, naprawdę tam był.

W czerwcu 2006 roku dwaj chińscy matematycy, Xi Ping Zhu i Huai Dong Cao, opublikowali w *Asian Journal of Mathematics* ponad dwustustronicową pracę z takim streszczeniem: *Podajemy tu dowód hipotezy Poincarégo i hipotezy geometryzacyjnej. Niniejsza praca korzysta z sumy osiągnięć wielu matematyków, którzy w ostatnich 30 latach zajmowali się analizą geometryczną. Dowód należy uznać za ukoronowanie teorii Hamiltona i Perelmana, opisującej potok Ricciego.* Czyj dowód, niestety nie napisali. A w tekście różni ludzie znaleźli potem, prócz rzetelnej matematyki, także fragmenty, żywo nadające się na poglądowy przykład, co to jest plagiat.

W lipcu 2006 roku Instytut Claya udostępnił (za darmo, można skorzystać i dziś) w Internecie pełny tekst monografii Johna Morgana i Ganga Tiana *Ricci Flow and the Poincaré Conjecture*.

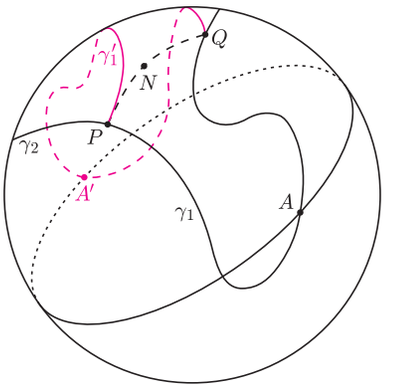
W tymże 2006 roku Perelmanowi przyznano medal Fieldsa. Odmówił jego przyjęcia; 22 sierpnia 2006 król Juan Carlos podczas ceremonii otwarcia Międzynarodowego Kongresu Matematyków w Madrycie zobaczył, zamiast czwartego z laureatów, puste krzesło w pierwszym rzędzie.

W tym samym czasie ukazał się w tygodniku *The New Yorker* kontrowersyjny artykuł Sylvii Nasar (m.in. autorki słynnej biografii Johna Nasha) oraz Davida Grubera, zatytułowany *Rozmaitość losów. Legendarny problem i bitwa o to, kto go rozwiązał*. Zamiast streszczać, odsyłam do oryginału:

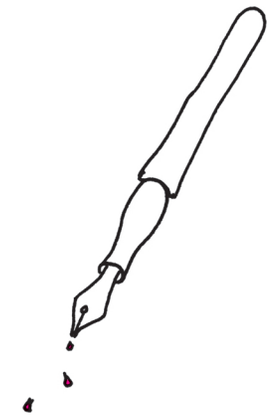
`http://www.newyorker.com/magazine/2006/08/28/manifold-destiny`.

W grudniu 2006 *Science*, potwierdzając dość powszechne wśród matematyków przekonanie, że Perelman nie tylko udowodnił jeden z problemów milenijnych Instytutu Claya, ale poważnie zmienił kawał matematyki, uznało dowód hipotezy

Rozwiązanie zadania M 1482.
Rozważmy dwa punkty P i Q na naszej krzywej, dzielące ją na dwie krzywe γ_1, γ_2 o równych długościach. Wtedy odległość między P i Q, liczona wzdłuż łuku okręgu wielkiego, wynosi mniej niż π. Niech N będzie środkiem tego łuku. Przyjmujemy, że jest to biegun północny naszej sfery. Pokażemy, że krzywa nie przecina równika sfery, czyli leży w całości na półkuli północnej.



Załóżmy przeciwnie, że krzywa γ_1 przecina równik w punkcie A. Niech γ_1' będzie obrazem γ_1 przy obrocie o 180° wokół osi wyznaczonej przez bieguny sfery. Punkty P i Q przy tym obrocie zamieniają się miejscami. Zauważmy, że krzywa $\gamma_1 \cup \gamma_1'$ ma taką samą długość jak $\gamma_1 \cup \gamma_2$, czyli mniejszą niż 2π. Z drugiej strony zawiera ona dwa punkty antypodyczne (punkt A i jego obraz przy obrocie), co oznacza, że jej długość wynosi co najmniej $\pi + \pi = 2\pi$.
Ta sprzeczność kończy dowód.



Jak działa, można zobaczyć na stronie `https://math.berkeley.edu/~sethian/2006/Applications/ImageProcessing/Movienoiseremoval-character.lbl.mpeg`.

Poincarégo za najważniejsze wydarzenie naukowe roku. Odkrycia spoza matematyki – pewnie znacznie bardziej przemawiające do szerokiej publiczności niż twierdzenie głoszące, że jedyną trójwymiarową rozmaitością zwartą, na której wszystkie pętle są ściągalne, jest sfera S^3 – znalazły się tym razem na dalszych miejscach listy.

4. W 2010 roku Perelman nie przyjechał na doroczną konferencję Instytutu Claya, zorganizowaną w Paryżu. Laudacje poświęcone jego pracy wygłosili Andrew Wiles z Princeton (autor dowodu Wielkiego Twierdzenia Fermata), Michael Atiyah z Oksfordu (medalista Fieldsa z 1966 roku), Simon Donaldson z Oksfordu (medalista Fieldsa z 1986 roku), Michaił Gromow (laureat nagrody Abela z 2009 roku) oraz William Thurston (medalista Fieldsa z 1982 roku).

W lipcu 2010 roku Perelman odmówił przyjęcia przyznanej mu nagrody Instytutu Claya. Milion dolarów oraz opinia publiczna były dlań mniej ważne niż własne przekonanie, że w matematyce – w nauce – najważniejsza jest uczciwość. Nie mam pojęcia, co dokładnie myślał, choć chyba potrafię to sobie wyobrazić. Kto chce wiedzieć, o co chodzi, niech, zachowując należny dystans, poczyta np. wspomniany tekst z tygodnika *The New Yorker*.

5. Czy wolno nam osądzać wybory Perelmana? Moim zdaniem, nie wolno. Zdarzało mi się wprawdzie słyszeć, że taką postawą mógł tylko zaszkodzić matematyce i temu, jak jest publicznie odbierana; kto chciał widzieć w matematykach przede wszystkim nieżyciowych dziwaków, którym wskutek zajmowania się abstrakcyjnymi problemami czasem szajba odbija, miał w 2006 i 2010 roku świeżą pożywkę. Niemniej, Perelman nie tylko rozwiązał słynny problem, wędrując śmiałą, wręcz fantastyczną drogą. Jak powiedział w swojej laudacji Thurston: *Uczyliśmy się od Perelmana matematyki. Może powinniśmy zatrzymać się na chwilę, zastanowić nad sobą i wynieść lekcję także ze stosunku Perelmana do życia.*

A że ta historia wpływa na obraz matematyki wśród innych? Cóż, to inna sprawa, trochę nasza (każdy może opowiadać o matematyce, jak potrafi najlepiej), a trochę nie.

6. Dla mnie historia Perelmana, czy może raczej najnowsza historia tych gałęzi matematyki, które dla jego przełomu były kluczowe, jest (również) jeszcze jednym świadectwem, że w gruncie rzeczy nie ma podziału na matematykę teoretyczną i matematykę stosowaną – to znaczy nie ma ostrej granicy między nimi.

W 2011 roku nagrodę ICIAM Pioneer Prize, ufundowaną przez amerykańskie Towarzystwo Matematyki Przemysłowej i Stosowanej (SIAM), otrzymał James Sethian z Berkeley. Za co? *Za swoje fundamentalne metody i algorytmy, które wywarły wielki wpływ na takie zastosowania jak rozpoznawanie kształtów i obrazów w medycynie, geofizyce, tomografii oraz opis dynamiki kropli w drukarkach atramentowych.* Co się za tymi słowami kryje? Między innymi pomysł Sethiana, jaką metodą szybko i sprawnie rozwiązywać numerycznie, z dobrym przybliżeniem, równania takie jak potok Ricciego albo ewolucja powierzchni z prędkością równą średniej krzywiźnie. Jeden z powszechnie wykorzystywanych, skutecznych algorytmów oczyszczania obrazów z szumu wykorzystuje pomysły, zaczerpnięte z geometrii różniczkowej i analizy matematycznej.

W pierwszej połowie lat 90. dwudziestego stulecia Perelman i Sethian mieli szansę spotykać się na korytarzach w Berkeley. Ciekaw jestem, czy kiedykolwiek rozmawiali o matematyce, o tym, gdzie – wbrew dzielącym wielki tort matematyki na drobne, rozłączne kawałki – topologia spotyka równania różniczkowe, analizę (także numeryczną) i algorytmy, które jednak mają wpływ na życie wielu śmiertelników.

Znana jest wypowiedź Newtona, że mógł zrobić to, co zrobił, gdyż stał na ramionach gigantów. Nie byłoby historii Perelmana, gdyby nie Poincaré, Thurston, Hamilton. Matematyka **jest** sztuką pokonywania własnych granic, rozwiązywania problemów i wyciągania wniosków ze znalezionych rozwiązań; wszelkie próby dzielenia tej działalności na odrębne, ściśle rozgraniczone tematyczne działki są koniec końców skazane na porażkę. Prawdziwi odkrywcy przekraczają sztucznie stawiane granice.

Reszta jest dziełem człowieka, czyli Fermat i inni

Mariusz SKAŁBA[*]

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

Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.

Leopold Kronecker

Nie ma słynniejszego twierdzenia niż Wielkie Twierdzenie Fermata (WTwF) i tego nie zamierzam tu dowodzić. Zacznę po prostu od sformułowania faktu, który od 1995 roku jest rzeczywiście twierdzeniem za sprawą Andrew Wilesa, a wcześniej przez około trzy i pół wieku był hipotezą zajmującą głowy największych matematyków i rzesze amatorów.

Twierdzenie 1. *Jeżeli n jest liczbą naturalną większą od* 2, *to równanie*

$$x^n + y^n = z^n \tag{1}$$

nie ma rozwiązań w liczbach naturalnych x, y, z.

Jak powszechnie wiadomo, wykładnik $n = 2$ jest zupełnie wyjątkowy, gdyż wtedy równanie (1), zwane równaniem Pitagorasa, ma nieskończenie wiele nieproporcjonalnych rozwiązań, a nawet dużo więcej – ma rozwiązanie w wielomianach o współczynnikach całkowitych:

$$x = k(m^2 - n^2), \qquad y = k \cdot 2mn, \qquad z = k(m^2 + n^2).$$

Pokażemy przede wszystkim, że dla ustalonego $n > 2$ równanie (1) nie ma rozwiązań w wielomianach $x(t), y(t), z(t)$ o współczynnikach zespolonych, chyba że wszystkie wymienione wielomiany są stałe! Załóżmy nie wprost, że trójka wielomianów $x(t), y(t), z(t)$ jest hipotetycznym rozwiązaniem równania (1), przy czym nie wszystkie wielomiany $x(t), y(t), z(t)$ są stałe oraz (co możemy założyć) $x(t), y(t), z(t)$ nie mają wspólnego dzielnika wielomianowego dodatniego stopnia. Jeśli $\omega_n = \exp(2\pi i/n)$, to mamy tożsamość algebraiczną

$$\alpha^n - 1 = (\alpha - 1)(\alpha - \omega_n)(\alpha - \omega_n^2) \cdot \ldots \cdot (\alpha - \omega_n^{n-1}),$$

z której po podstawieniu $\alpha = z/y$ i pomnożeniu obu stron przez y^n otrzymujemy

$$z^n - y^n = (z - y)(z - \omega_n y)(z - \omega_n^2 y) \cdot \ldots \cdot (z - \omega_n^{n-1} y).$$

Nasze hipotetyczne wielomiany spełniają więc równanie

$$x(t)^n = (z(t) - y(t))(z(t) - \omega_n y(t))(z(t) - \omega_n^2 y(t)) \cdot \ldots \cdot (z(t) - \omega_n^{n-1} y(t)).$$

Ponieważ czynniki po prawej stronie są parami względnie pierwsze, więc z jednoznaczności rozkładu wielomianów na czynniki wynika, że istnieją takie wielomiany $u(t), v(t), w(t)$, że

$$z(t) - y(t) = u(t)^n, \qquad z(t) - \omega_n y(t) = v(t)^n, \qquad z(t) - \omega_n^2 y(t) = w(t)^n.$$

Po rozwiązaniu pierwszych dwóch z powyższych równań względem $z(t)$ oraz $y(t)$ i podstawieniu tych wartości do trzeciego równania otrzymujemy po uproszczeniach

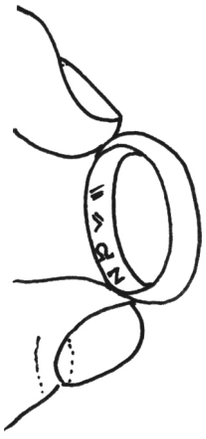
$$-\omega_n u(t)^n + (\omega_n + 1)v(t)^n = w(t)^n.$$

Ponieważ z liczb zespolonych można wyciągać pierwiastki dowolnych stopni, więc powyższą równość można zapisać jako

$$x_1(t)^n + y_1(t)^n = z_1(t)^n,$$

gdzie największy ze stopni wielomianów $x_1(t), y_1(t), z_1(t)$ jest n razy mniejszy niż największy ze stopni wielomianów $x(t), y(t), z(t)$. To postępowanie można kontynuować, ale to oczywista sprzeczność! Przeprowadzone rozumowanie ilustruje słynną *metodę regresji*: za pomocą hipotetycznego rozwiązania konstruujemy rozwiązanie w pewnym sensie mniejsze i to prowadzi do sprzeczności.
W rozważonym przykładzie mielibyśmy nieskończony ciąg wielomianów o ściśle malejących dodatnich stopniach! Metodę tę stosowano z pewnym powodzeniem również do przypadku liczbowego, chociaż pojawiają się tu już dość szybko fundamentalne trudności i, jak pokazała historia, nie udało się ich do końca przezwyciężyć.

Wielkie sukcesy uzyskał jednak Ernst Eduard Kummer w połowie XIX wieku. Rozważał on mianowicie pierścień $\mathbb{Z}[\omega_p]$, gdzie $n = p$ jest rozważanym wykładnikiem i zakłada się, że p jest liczbą pierwszą nieparzystą. Do pierścienia $\mathbb{Z}[\omega_p]$ należą liczby zespolone postaci $a_0 + a_1\omega_p + a_2\omega_p^2 + \cdots + a_{p-2}\omega_p^{p-2}$, gdzie $a_0, a_1, \ldots, a_{p-2}$ to zwykłe liczby całkowite. W przypadku, gdy w pierścieniu $\mathbb{Z}[\omega_p]$



Aby udowodnić WTwF, wystarczy rozważać wykładniki pierwsze nieparzyste i $n = 4$.

Rozwiązanie zadania M 1480.
Zauważmy, że dla całkowitych x mamy równość. Ponadto dodanie do dowolnego x liczby całkowitej k zmienia każdą ze stron nierówności o nk, możemy zatem zakładać, że x należy do przedziału $(0,1)$. Niech $t_{k,l} = k/l$ dla takich względnie pierwszych liczb całkowitych dodatnich k i l, że $k < l \leqslant n$. Zauważmy, że obie strony nierówności są w przedziale $(0,1)$ niemalejącymi funkcjami x, przy czym prawa strona zmienia wartość tylko w punktach $t_{k,l}$. Wystarczy więc sprawdzić nierówność tylko dla tych punktów. Niech od tej pory $x = t_{k,l}$.

Dla każdego $i = 1, 2, \ldots, n$ zachodzi równość $ik = q_i l + r_i$ dla pewnych jednoznacznie wyznaczonych liczb całkowitych $0 \leqslant r_i \leqslant l-1$ i $q_i \geqslant 0$ (dzielimy ik z resztą przez l). Zauważmy, że liczby $r_1, \ldots, r_{l-1}$ są dodatnie: $r_i \neq 0$ dla $i < l$, bo inaczej l dzieliłoby ik. Ponadto te liczby są parami różne – gdy $r_i = r_j$ dla $i \leqslant j < l$, to l dzieli $(i-j)k$, a stąd $i = j$. W takim razie ciąg $r_1, \ldots, r_{l-1}$ jest pewną permutacją liczb $1, 2, \ldots, l-1$. Stąd i z nierówności między średnimi dostajemy

$$\frac{r_1}{1} + \ldots + \frac{r_{l-1}}{l-1} \geqslant l - 1.$$

Zatem

$$r_n \leqslant l - 1 \leqslant \sum_{i=1}^{n} \frac{r_i}{i} = nk - l\sum_{i=1}^{n} \frac{q_i}{i} =$$
$$= q_n l + r_n - l\sum_{i=1}^{n} \frac{q_i}{i},$$

a stąd

$$\sum_{i=1}^{n} \frac{\lfloor ix \rfloor}{i} = \sum_{i=1}^{n} \frac{\lfloor ik/l \rfloor}{i} = \sum_{i=1}^{n} \frac{q_i}{i} \leqslant$$
$$\leqslant q_n = \lfloor nk/l \rfloor = \lfloor nx \rfloor.$$

rozkład na czynniki nierozkładalne jest jednoznaczny, nierozwiązalność równania (1) można uzyskać w podobny sposób jak wyżej dla wielomianów. Pewne komplikacje związane ze skutecznym przeprowadzeniem regresji związane są z istnieniem w pierścieniu $\mathbb{Z}[\omega_p]$ nietrywialnych elementów *odwracalnych*, tzn. takich elementów α, że $\alpha \cdot \beta = 1$ dla pewnego $\beta \in \mathbb{Z}[\omega_p]$. Za trywialne uznajemy elementy postaci $\pm\omega_p^k$; oczywiście są one odwracalne. Dla $p \geqslant 5$ istnieją również elementy odwracalne γ, które nie są pierwiastkami z jedności. Na przykład dla $p = 7$ przyjmijmy $\gamma = 1 + \omega_7$. Mamy wówczas

$$(1+\omega_7)^{-1} = \frac{1-\omega_7}{1-\omega_7^2} = \frac{1-\omega_7^8}{1-\omega_7^2} = 1 + \omega_7^2 + \omega_7^4 + \omega_7^6 \in \mathbb{Z}[\omega_7],$$

a więc γ jest odwracalny i, co łatwo wykazać, nietrywialny. Niestety, dla $p > 19$ w pierścieniu $\mathbb{Z}[\omega_p]$ nie ma jednoznaczności rozkładu na elementy nierozkładalne, a oto przykład dla $p = 23$. Niech $\omega = \omega_{23}$. Mamy

$$\alpha = (1+\omega^2+\omega^4+\omega^5+\omega^6+\omega^{10}+\omega^{11})(1+\omega+\omega^5+\omega^6+\omega^7+\omega^9+\omega^{11}) =$$
$$= 2(\omega^5+\omega^6+\omega^7+\omega^9+\omega^{10}+3\omega^{11}+\omega^{12}+\omega^{13}+\omega^{15}+\omega^{16}+\omega^{17}).$$

Zatem liczba α dzieli się przez 2 mimo tego, że 2 nie dzieli żadnego z czynników poprzedniego iloczynu. Ponadto można wykazać, że liczba 2 jest nierozkładalna w $\mathbb{Z}[\omega_{23}]$, a więc w $\mathbb{Z}[\omega_{23}]$ nie ma jednoznaczności rozkładu na czynniki nierozkładalne! Brak jednoznaczności rozkładu na czynniki to największa trudność, którą należy pokonać, adaptując metodę regresji. Genialny pomysł Kummera polegał na wprowadzeniu do rozważań nowych obiektów, tzw. *liczb idealnych* i wykazaniu, że każda liczba z $\mathbb{Z}[\omega_p]$ rozkłada się w jednoznaczny sposób na iloczyn liczb idealnych. Używając współczesnego języka (wprowadzonego przez Dedekinda), zbiory liczb z $\mathbb{Z}[\omega_p]$ podzielnych przez daną liczbę idealną Kummera to po prostu ideały pierwsze pierścienia $\mathbb{Z}[\omega_p]$ – stąd zresztą ich nazwa! Miarą niejednoznaczności rozkładu na poziomie liczb jest tzw. *grupa klas ideałów* pierścienia $\mathbb{Z}[\omega_p]$, której definicji tu nie podamy. Nadmienimy tylko, że Kummer udowodnił, między innymi, następujące twierdzenie.

Twierdzenie 2. *Jeżeli $p > 2$ jest liczbą pierwszą oraz rząd grupy klas ideałów nie dzieli się przez p, to równanie* (1) *nie ma rozwiązań dla wykładnika $n = p$.*

Metody wypracowane przez Kummera, Dedekinda i innych dały początek *algebraicznej teorii liczb*, ważnemu działowi matematyki współczesnej. Grupa klas ideałów i grupa elementów odwracalnych są bardzo blisko spokrewnione z funktorami K_0 oraz K_1 *algebraicznej K-teorii* – nowoczesnego działu współczesnej matematyki, który próbuje łączyć algebrę i geometrię na wysokim i abstrakcyjnym poziomie.

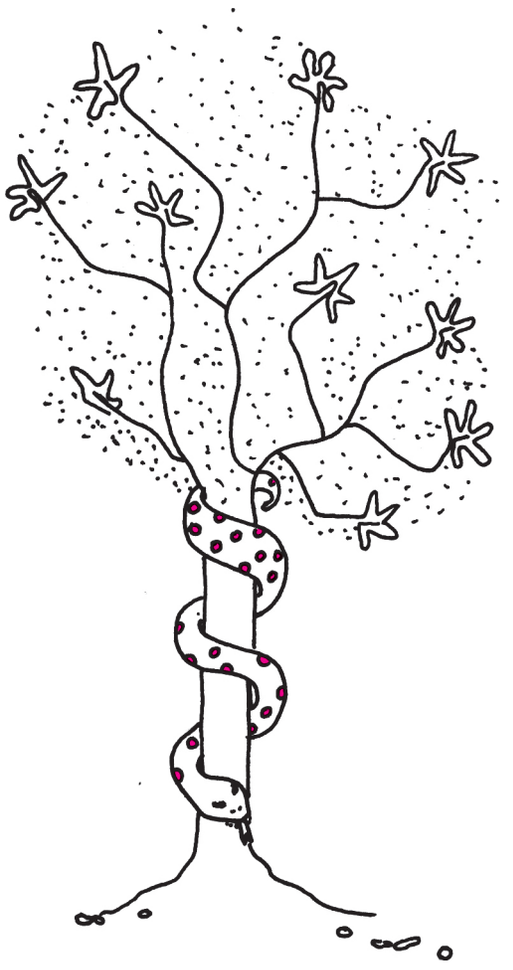
Trzeba zmierzać do końca tej historii i dlatego muszę przemilczeć wiele ciekawych częściowych rezultatów uzyskanych przed rokiem 1983. W tymże roku Gerd Faltings udowodnił hipotezę Mordella o tym, że na każdej krzywej rodzaju większego od 1 istnieje co najwyżej skończenie wiele punktów wymiernych. Wynika stąd, że dla $n \geqslant 4$ równanie (1) ma co najwyżej skończenie wiele *nieproporcjonalnych* rozwiązań.

To oczywiście wspaniały wynik, ale przecież nie tego oczekiwał Fermat. Na szczęście historia nabrała tempa, gdy w 1986 roku Gerhard Frey związał z hipotetycznym rozwiązaniem równania (1) $x = a$, $y = b$, $z = c$ następującą krzywą eliptyczną

$$y^2 = x(x + a^p)(x - b^p).$$

Wyróżnik tej krzywej wynosi $(abc)^{2p}$ i to nasunęło Freyowi przypuszczenie, że taka krzywa... w ogóle nie powinna istnieć – to oczywiście zakończyłoby dowód WTwF! Pomysł okazał się trafiony, ale szczegóły dopinało wielu wybitnych matematyków. I tak Jean-Pierre Serre sformułował precyzyjnie przypuszczenie Freya, a Ken Ribet wyprowadził je w tym samym roku ze słynnej hipotezy Taniyamy–Shimury–Weila o tym, że każda krzywa eliptyczna o współczynnikach wymiernych jest *modularna*. Tę właśnie hipotezę udowodnił Andrew Wiles w 1995 roku z pomocą swojego ucznia Richarda Taylora dla tzw. krzywych półstabilnych – klasa tych krzywych obejmuje krzywe typu Freya i to... kończy dowód WTwF. Artykuł zakończymy omówieniem pojęcia *krzywa eliptyczna modularna*. Jest wiele sformułowań tej własności – wybieramy wersję arytmetyczną. Z każdą krzywą eliptyczną

$$y^2 = x^3 + Ax^2 + Bx + C, \qquad \text{gdzie } A, B, C \in \mathbb{Z}$$



i liczbą pierwszą p można związać kongruencję

$$y^2 \equiv x^3 + Ax^2 + Bx + C \pmod{p}.$$

Niech N_p oznacza liczbę rozwiązań tej kongruencji modulo p.
Helmut Hasse udowodnił w 1933 roku hipotezę Artina głoszącą, że

$$|N_p - p| < 2\sqrt{p}.$$

Wynika z niej natychmiast, że rozwiązania kongruencji istnieją dla dostatecznie dużych p. Jest to satysfakcjonujący rezultat ilościowy, ale być może o liczbie $a_p := p - N_p$ można powiedzieć coś więcej, niż tylko to, że jest mniejsza od $2\sqrt{p}$? Okazuje się, że tak! Przyjrzyjmy się najpierw krzywej

$$y^2 = x^3 + x.$$

Bardzo łatwo wykazać, że jeśli $p \equiv 3 \pmod 4$, to $a_p = 0$. Dużo trudniej zauważyć, że dla $p \equiv 1 \pmod 4$ też istnieje dość zwarty i dość jednolity wzór na liczbę a_p. Mianowicie liczbę p przedstawiamy w postaci $p = a^2 + b^2$, gdzie a, b są dodatnie, przy czym a jest nieparzysta (b zaś parzysta). Jak wiadomo, takie przedstawienie liczby pierwszej $p \equiv 1 \pmod 4$ zawsze istnieje i jest dokładnie jedno – jest to twierdzenie Fermata (ani małe, ani wielkie, ale wspaniałe). Wówczas a_p dane jest następującym wzorem

$$a_p = \begin{cases} 2a & \text{gdy } a \equiv 1 \pmod 4 \\ -2a & \text{gdy } a \equiv 3 \pmod 4. \end{cases}$$

Krzywa eliptyczna $y^2 = x^3 + x$ należy do dość wąskiej klasy krzywych eliptycznych z *mnożeniem zespolonym* – odwzorowanie $(x, y) \mapsto (-x, yi)$ przeprowadza punkty krzywej na punkty krzywej. Niewiele krzywych ma tego typu algebraiczne „symetrie".

Rozpatrzmy teraz typową krzywą eliptyczną (bez mnożenia zespolonego)

$$y^2 = x^3 - 4x^2 + 16$$

oraz, jak wyżej, odpowiednie kongruencje modulo różne liczby pierwsze p. Okazuje się, że ciąg liczb a_p można uzyskać w następujący sposób. Rozważmy iloczyn funkcyjny

$$\Theta(T) = T \prod_{j=1}^{\infty} \left((1 - T^j)(1 - T^{11j})\right)^2$$

przy czym dla uproszczenia pomińmy kwestię zbieżności. Jeśli zapiszemy teraz powyższy iloczyn formalny jako szereg formalny

$$\Theta(T) = \sum_{k=1}^{\infty} c_k T^k,$$

to okazuje się, że dla każdej liczby pierwszej $p \geqslant 3$ zachodzi równość $a_p = c_p$, a więc znowu otrzymaliśmy „wzór" na a_p. Hipoteza Taniyamy–Shimury–Weila przewidywała właśnie, że tego typu „wzór" na a_p można podać dla każdej krzywej eliptycznej o współczynnikach wymiernych. Znaczenie twierdzenia o modularności znacznie wykracza poza zastosowanie do dowodu WTwF. Daje ono, na przykład, fundament do ścisłego sformułowania hipotezy Bircha–Swinnertona-Dyera, która nadal jest jednym z problemów milenijnych. Do tych zastosowań trzeba przywołać sformułowania bardziej geometryczno-analityczne od stosowanych w tym tekście.

Polecam w tej sprawie znakomity artykuł Zbigniewa Marciniaka *O Wielkim Twierdzeniu Fermata*, *Matematyka-Społeczeństwo-Nauczanie* 22, `www.msn.uph.edu.pl/smp/msn/22/10-15.pdf`.

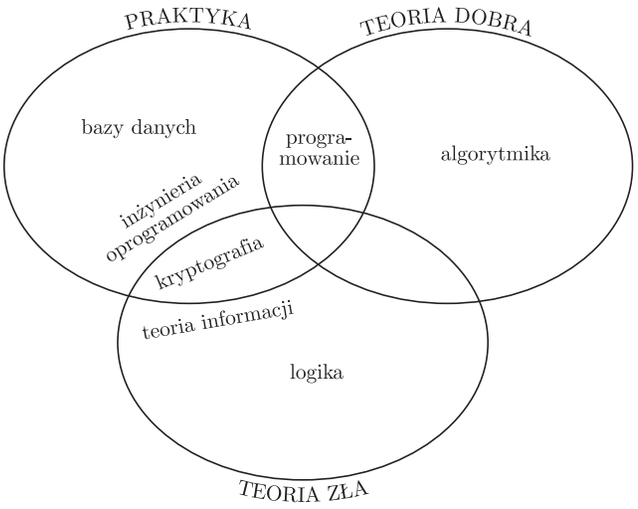
Na koniec odnieśmy się do słynnej myśli wypowiedzianej przez Leopolda Kroneckera, że liczby całkowite stworzył Bóg, a *reszta jest dziełem człowieka*. Historia WTwF doskonale ilustruje starą prawdę, że jeśli chcemy się czegoś dowiedzieć (pozornie prostego!) o bardzo prostych obiektach, musimy wyjść ze świata tychże obiektów i mieć nadzieję, że wzbogacona w ten sposób perspektywa pozwoli nam dostrzec te powiązania, które nie były widoczne z bliska. Do lat osiemdziesiątych XX wieku to wyjście z raju liczb naturalnych było bardzo ograniczone – cały czas obracano się w świecie liczb algebraicznych i ich rozkładów na czynniki. Pomysł Freya wyrwał badaczy WTwF z zaklętego kręgu liczb, a świat krzywych eliptycznych i form modularnych okazał się wystarczającym wzbogaceniem ubogiego i jakże błahego kontekstu WTwF.

A jednak się da!
czyli o współczesnej kryptologii

*Tomasz KAZANA**

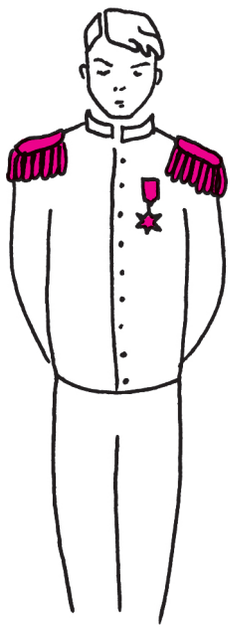
Lubię próżnie mówić o sobie, że jestem matematykiem. Bardziej precyzyjnie to jestem informatykiem, ale przecież informatyka to gałąź matematyki, więc w zasadzie nie oszukuję. Czasem, gdy ktoś mnie ciągnie za język, i pojawi się to, z niejasnych powodów nielubiane przeze mnie, słowo na „i", to i tak od razu uściślam: tak, jestem informatykiem, ale informatykiem teoretycznym. Zawsze miałem to dziwne przekonanie, że „teoretyczny" znaczy w jakimś sensie lepszy, ważniejszy, mądrzejszy, głębszy.

Podobne buńczuczne myślenie o sobie ma chyba spore grono matematyków. Chociażby Karol Gauss (już za życia zwany Księciem Matematyków), który choć badał bardzo różne dziedziny wiedzy, to ponoć najbardziej cenił sobie zgłębianie sekretów teorii liczb. To właśnie ona wydawała mu się zupełnie niepraktyczna, a zatem nieziemsko piękna. *L'art pour l'art!*



I tak to przez długi czas świat nauk ścisłych dzieliłem na teorię (bosko piękną) i praktykę (ludzko konieczną). Dziś widzę to trochę inaczej, w dużej mierze dzięki kryptologii – dziedzinie wiedzy, którą się zajmuję. Wizja ta ewoluowała, a aktualny stan mojego umysłu żartobliwie przedstawiam obok jako diagram Venna.

Jak widać, podzieliłem teorię na tę badającą zło (negatywne wyniki) i tę badającą dobro. Ta druga to wyniki pozytywne – dla mnie nuda, bo najfajniejsze są przecież wszelkie twierdzenia o niemożności lub szacowania z dołu, czyli pokazywanie ściśle, że czegoś się nie da. I, o ile dopuściłem, że teoretyczne wyniki pozytywne (np. algorytmy) mogą być praktyczne, to najgłębsza (czyli niepraktyczna) nauka musi się znajdować w części mrocznej. Kurt Gödel, Paul Cohen – to byli więc idole mojej młodości, a w głowie miałem tylko *saeculum obscurum* matematyki.



Wszystko to zburzyła współczesna kryptologia, dzięki której zrozumiałem, że wyniki negatywne (czegoś na pewno się nie da i nigdy to się nie zmieni) też mogą być praktyczne. No bo przecież, jeśli udowodnimy (formalnie!), że podsłuchiwacz, pomimo przechwycenia szyfrogramu, nigdy nie dowie się niczego na temat wysyłanej wiadomości, to jest to przecież ogromnie praktyczne.

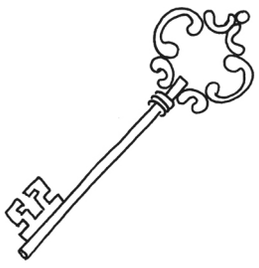
I ja tak właśnie patrzę na kryptologię: jako na część twardej matematyki ulokowanej gdzieś między klasycznymi twierdzeniami o niemożności a teorią obliczeń. Nic nie poradzę, że wolę myśleć o maszynie Turinga niż o maszynie Apple'a (choć na swój sposób cenię obie).

Kończę ten przydługi wstęp, licząc, że dostatecznie się zaasekurowałem i wytłumaczyłem, dlaczego w tym tekście tak mało będzie trzyliterowych skrótów, a tak dużo twierdzeń. Po prostu wszedłem na ten statek tylnymi drzwiami i, być może, patrzę przez inne okulary. Czytelnik sam oceni, czy takie spojrzenie mu odpowiada.

Dla mnie prawdziwa współczesna kryptologia zaczyna się w listopadzie 1976 roku, kiedy to w czasopiśmie *IEEE Transactions on Information Theory* ukazuje się artykuł *New directions in cryptography* autorstwa Whitfielda Diffiego i Martina Hellmana. W tym samym czasie w kioskach mamy *Deltę* numer 35, pierwszym sekretarzem jest Edward Gierek, a Polska jest potentatem w sportach zespołowych (złoto siatkarzy i srebro piłkarzy na letnich igrzyskach olimpijskich w Montrealu). A wspomniani wyżej autorzy publikują rewolucyjny pomysł kryptografii klucza publicznego.

Jest to dla mnie rewolucja, bo pojawia się pomysł, który jest zupełnie, ale to zupełnie nieoczywisty. Ba, podobno Oded Goldreich zawsze swój kurs kryptologii (w Instytucie Nauki Weizmanna w Izraelu) zaczyna od pracy domowej, w której

*Instytut Informatyki, Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski



prosi studentów o wykazanie, że kryptografia klucza publicznego jest niemożliwa. Dopiero na kolejnym wykładzie pokazuje, że jednak się da!

O co chodzi w tej idei?

Kryptografia klucza publicznego. Pomyślmy chwilę o zwykłym, klasycznym szyfrowaniu. Nieśmiertelna w tej branży Alicja chce wysłać wiadomość m do Boba. Nie chcą oni, by wiadomość wpadła w niepowołane ręce, a, niestety, kanał komunikacyjny jest podsłuchiwany przez Ewę. W ogólności problem rozwiązujemy następująco: Alicja i Bob zawczasu ustalają między sobą tajny klucz k. I teraz, gdy Alicja chce wysłać wiadomość, to wysyła do Boba wartość pewnej funkcji $E(m,k)$. Natomiast gdy Bob odbierze c, to oblicza $D(c,k)$. Wszystko jest poprawne, gdy:

- $D(E(m,k),k) = m$;
- znajomość $c = E(m,k)$ nie umożliwia obliczenia m (bądź umożliwia, ale konieczne obliczenia trwałyby niesłychanie długo).

Opisany wyżej model jest znany i (mniej lub bardziej skutecznie) stosowany od tysięcy lat. W ten schemat wpisuje się zarówno szyfr Cezara, szyfr Vigenère'a czy maszyna szyfrująca Enigma. Pewną niedogodnością jest tu jednak konieczność ustalenia klucza k przed komunikacją. Pomysł Diffiego i Hellmana ociera się o bezczelność. Zapytali oni, czy da się przeprowadzić powyższą procedurę, ale bez klucza k. Innymi słowy, chcemy, aby Alicja mogła szyfrować wiadomości do Boba bez uprzedniego spotkania i ustalania jakiegokolwiek sekretu. Innymi słowy, funkcja E ma być publicznie znana (także Ewie) i nie zależeć od k.

„Na oko" widać, że zrobić się tego nie da. Przecież wystarczy, że Ewa, podsłuchawszy $c = E(m)$, obliczy odwrotność $E^{-1}(c)$ i pozna wiadomość!

A jednak, czasem się da! Powodem jest fakt, że dla pewnych funkcji E obliczenie funkcji odwrotnej E^{-1} może być dla Ewy koszmarnie trudne. Z drugiej strony Bob da sobie radę, bo zna pewną tajemnicę na temat E, której nikomu (nawet Alicji) nie ujawnił. Szczegóły tej magii zostawiam Czytelnikowi Zaciekawionemu do własnych poszukiwań. Dodam tylko, że w jednym z rozwiązań (RSA) korzysta się (o ironio!) ze zdobyczy teorii liczb, tak wielbionej przez Gaussa za niepraktyczność!

Dziś w matematyce urzeka mnie chyba najbardziej właśnie to – dowody faktów nieoczywistych, sprzecznych z intuicją. Nazywam to efektem „A jednak się da!" i dostrzegam ogrom takich rozumowań w kryptologii. Ostatnie 500 miesięcy to wręcz wysyp takich cudownych perełek, o których spróbuję trochę opowiedzieć.

Dowody z wiedzą zerową. Wyobraź sobie Czytelniku Sekretny, że udowodniłeś, iż $P \neq NP$ albo pokazałeś prawdziwość hipotezy Riemanna. Chcesz teraz:

- przekonać świat, że rozważana hipoteza faktycznie jest prawdziwa;
- zachować szczegóły dowodu tylko dla siebie.

Sprzeczne? A jednak się da! Prace z lat 80. XX wieku takich kryptologów jak Oded Goldreich czy Shafrira Goldwasser opisują, jak to zrobić.

Szyfrowanie homomorficzne. Tym razem, Czytelniku Ciekawski, wyobraź sobie, że chcesz wyszukać w Internecie informację na jakiś temat T. Znasz wiele wyszukiwarek (choćby tę na literę G), które znajdą listę interesujących Cię stron w ułamku sekundy. Jednakże Ty chciałbyś więcej:

- poznać listę stron na temat T;
- mieć gwarancję, że dostawca usługi (wyszukiwarka G) zupełnie nic się nie dowie, czego szukałeś (czyli T pozostanie dla niego tajne).

Innymi słowy, usługodawca poprawnie odpowiada na Twoje pytanie, pomimo że nie zna pytania. Jak poprzednio: da się, choć, póki co, nie jest to bardzo efektywne. I żadna wyszukiwarka tego nie oferuje. Czytelnik Zainteresowany niech wpisze w G hasło *fully homomorphic encryption*. No, chyba że nie chce, żeby ktokolwiek dowiedział się, czego szuka. W takiej sytuacji pozostaje zwykła czytelnia.

E-gotówka. Czytelnik Kapitalista zapewne zna podstawową zaletę gotówki. Anonimowość! A teraz wyobraźmy sobie, że mamy cyfrowy odpowiednik monet i banknotów – specjalne pliki, które spełniają następujące, pozornie sprzeczne, warunki:

- posiadanie pojedynczej kopii takiego pliku nie zdradza (nawet bankowi!) tożsamości osoby, która posiadała ten plik wcześniej;
- jeśli (nielegalnie) przekażemy nasz plik dwóm różnym osobom, to w przyszłości bank to wykryje i odkryje naszą tożsamość.

W rzeczywistości podczas procesu przekazywania plik się lekko zmienia, za każdym razem trochę inaczej.

Że się da, proszę się przekonać, sięgając do pracy Stefana Brandsa *Electronic Cash* z roku 1996.

Poker przez Internet. Możliwość brania udziału w grach hazardowych przez Internet nie jest zaskakująca. Dobrze, ale co, jeśli chcemy grać bez zaufanej trzeciej strony (serwera)? Pomyślmy chociażby o znacznie łatwiejszym pytaniu: jak „rzucić monetą przez Internet" bez zaufanej trzeciej strony tak, aby żaden z graczy nie mógł złośliwie wpłynąć na wynik. Intuicja podpowiada, że z pewnością się nie da! A jednak: zachęcam do sięgnięcia do pracy Manuela Bluma *Coin Flipping by Telephone* z roku 1981 czy późniejszej pracy Moniego Naora *Bit Commitment Using Pseudo-Randomness* z roku 1991. Oczywiście, nikogo nie zaskoczę, gdy dodam, że poker przez Internet bez zaufanych trzecich stron też jest możliwy.

Wiele przykładów, które pokazałem w tym artykule, to, prawdę powiedziawszy, trochę rubieże (ale jakże piękne) klasycznej kryptologii. Spośród tego, co wydarzyło się w ciągu ostatnich 500 miesięcy, wybrałem to, co, moim zdaniem, najciekawsze, ale, być może, nie najważniejsze dla bezpieczeństwa cyfrowego świata. Należy dodać, że klasyczna kryptologia jako taka też znakomicie rozwijała się w tym czasie. Przede wszystkim omawiana dziedzina zaczęła być przedstawiana w rygorze formalizmów matematycznych. Definicje stały się ostre, często pomysłowe.

Oczywiście, motywacja do rozwoju jest zupełnie jasna: w XXI wieku informacja ma dużą wartość, a więc jej ochrona staje się niezwykle kluczowa. Ludzie chcą bezpiecznie trzymać, wysyłać, podpisywać czy odbierać wiadomości. Przy tym chcą również chronić swoją prywatność, nawet gdy wszystko dzieje się „w chmurze". A w epoce *digital natives* te problemy będą jeszcze ważniejsze.

Tym bardziej jest pocieszające, że przy tej okazji rozwija się ciekawa gałąź prawdziwej matematyki, z niebanalnymi modelami, twierdzeniami i hipotezami.

Zadania

Redaguje Tomasz TKOCZ

M 1480. Udowodnić, że dla dowolnej liczby nieujemnej x i dowolnej liczby całkowitej dodatniej n prawdziwa jest nierówność

$$\lfloor nx \rfloor \geqslant \frac{\lfloor x \rfloor}{1} + \frac{\lfloor 2x \rfloor}{2} + \ldots + \frac{\lfloor nx \rfloor}{n},$$

gdzie $\lfloor a \rfloor$ oznacza największą liczbę całkowitą nie większą od a.
Rozwiązanie na str. 5

M 1481. W tablicę $n \times n$ wpisano w pewnej kolejności liczby $1, 2, \ldots, n^2$. Powiemy, że para liczb *sąsiaduje*, jeśli znajdują się one obok siebie w pewnym wierszu lub w pewnej kolumnie. Wykazać, że istnieje para sąsiadujących liczb, które różnią się co najmniej o n.
Rozwiązanie na str. 18

M 1482. Na sferze o promieniu 1 dana jest krzywa zamknięta o długości mniejszej niż 2π. Wykazać, że ta krzywa jest zawarta w pewnej półsferze.

Uwaga. Można uważać za oczywiste następujące stwierdzenie: *najkrótsza krzywa łącząca dwa punkty na sferze to łuk okręgu wielkiego.*
Rozwiązanie na str. 3

Przygotował Andrzej MAJHOFER

F 895. (a) Ile elektronów zawiera średnio 1 g ciała człowieka?
(b) Ile elektronów zawiera średnio 1 g otaczającej nas materii?
Rozwiązanie na str. 15

F 896. Kondensator powietrzny o pojemności $C = 100$ pF wypełniono roztworem soli kuchennej o oporze właściwym $\rho = 0{,}15\ \Omega$m. Ile wynosi opór elektryczny R między elektrodami tak otrzymanego opornika? Przenikalność elektryczna próżni to $\varepsilon_0 \approx 8{,}85 \cdot 10^{-12}$ F/m.
Rozwiązanie na str. 17

Sieć

Marcin PECZARSKI Instytut Informatyki, Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

Otworzyłem mój pierwszy numer *Delty* z marca 1979 roku. Czytam adres Redakcji: nazwa ulicy, numer budynku, numer pokoju, kod pocztowy, nazwa miasta. Nie podano e-maila ani strony www. Nawet nie ma numeru telefonu. Wtedy telefon (stacjonarny, bo o komórkach nikt nie słyszał) był w naszym kraju trudno osiągalnym dobrem luksusowym. Programy komputerowe pisało się na papierze i oddawało do wyperforowania na kartach lub taśmie, by po kilku dniach otrzymać wydruk z wynikami. Komputer widzieli nieliczni. Sieć komputerowa – taki termin jeszcze nie istniał w języku polskim.

Jest rok 2015. Korzystając z podłączonego do sieci laptopa, piszę artykuł do numeru jubileuszowego. Gotowy tekst prześlę do Redakcji mejlem. Oprócz papierowej powstanie wersja elektroniczna, która zostanie opublikowana w sieci. Mogę zdalnie uruchamiać programy na komputerach sieci uniwersyteckiej i prawie natychmiast dostawać ich wyniki. W każdej chwili mogę wysłać w sieć zapytanie, gdy chcę się czegoś dowiedzieć, na przykład, ile komputerów jest w sieci. Tę i wiele innych informacji może Czytelnik wyszukać sam, jeśli tylko starczy mu cierpliwości w przeglądaniu wyników wyświetlanych przez wyszukiwarkę i umie w morzu danych wyłowić te prawdziwe. Zapytania w sieć wysyłają nie tylko ludzie. Duża część przesyłanych w sieci danych to pytania i odpowiedzi wymieniane automatycznie między komputerami. Aby szybko udzielać odpowiedzi, specjalnie do tego przeznaczone farmy komputerów bez przerwy, pracowicie przeszukują sieć i indeksują pojawiające się w niej nowe informacje. Oto zbudowana przez Ziemian ogólnoświatowa sieć. Bardzo często jej nazwę, jako własną, piszemy z szacunkiem, wielką literą: Internet. Można też ją pisać małą literą: internet, gdy traktujemy tę nazwę jako „ogólną nazwę nowego medium – tak jak prasę, radio czy telewizję" (opinia Rady Języka Polskiego).

O budowie i działaniu internetu, o jego historii i wpływie na nasze życie, rozpatrując aspekty biznesowe, społeczne i techniczne, można napisać kilka grubych książek. Skupię się wyłącznie na przedstawieniu najważniejszych założeń technicznych.

Obecny internet składa się z miliardów urządzeń (komputerów, tabletów, smartfonów) i, przynajmniej teoretycznie, każda para urządzeń może się skomunikować. Z oczywistych powodów nie można zapewnić, aby między każdą parą urządzeń istniało bezpośrednie połączenie (kabel elektryczny, światłowód lub łącze radiowe). W wymianie danych pośredniczą inne urządzenia sieciowe, a obsługuje ją IP (ang. *Internet Protocol*) – podstawowy protokół internetowy służący do przekazywania danych z urządzenia do urządzenia. W użyciu są dwie wersje IP: 4 i 6. Aby móc się komunikować za pomocą IP, każde urządzenie, a właściwie jego interfejs sieciowy, musi mieć przyznany adres IP. Jeśli urządzenie ma kilka interfejsów sieciowych, to mają one na ogół różne adresy. Można też przypisać więcej niż jeden adres do jednego interfejsu. W IP 4 adresy są liczbami 32-bitowymi, a w IP 6 – 128-bitowymi. To właśnie zbyt mała pula dostępnych adresów w wersji 4 była głównym powodem opracowania wersji 6, a przy okazji poprawiono drobne niedociągnięcia i wprowadzono możliwość szyfrowania i cyfrowego podpisywania przesyłanych danych. Wewnętrznie IP używa wyłącznie binarnej reprezentacji adresów, ale w innych sytuacjach – dla wygody użytkowników – adres IP 4 zapisuje się jako cztery liczby dziesiętne z przedziału 0 do 255, reprezentujące po 8 bitów adresu, rozdzielone kropkami, np. 193.0.96.13. Adres IP 6 zapisuje się jako osiem 16-bitowych liczb w notacji szesnastkowej, rozdzielonych dwukropkami, np. fe80::222:19ff:fe8f:7c87 (podwójny dwukropek oznacza pominięcie w zapisie kolejnych liczb o wartości 0). Urządzenie może jednocześnie używać obu wersji IP, jeśli tylko ma przyznane oba adresy.

IP przesyła dane w porcjach, nazywanych pakietami albo datagramami. Pakiet IP składa się z nagłówka i właściwych danych. Nagłówek rozpoczyna się numerem wersji IP, aby rozróżnić jego format, gdyż każda z wersji posługuje się własnym formatem. Mimo różnic w formatach nagłówki IP 4 i IP 6 zawierają analogiczne pola: całkowity rozmiar pakietu (IP 4) lub rozmiar przesyłanych danych (IP 6), adres nadawcy, adres odbiorcy. IP korzysta do przekazywania pakietów między urządzeniami (węzłami sieci) z łączących je interfejsów sieciowych – łączy. Najczęściej spotykane współcześnie technologie łączy sieciowych to Ethernet, WiFi, DSL i LTE. Każda technologia łącza określa maksymalny rozmiar pakietu, jaki może przenosić, oznaczany skrótem MTU (ang. *maximum transmission unit*). Typowa wartość MTU wynosi 1500 oktetów. Oktet oznacza 8 bitów – jest to jednostka wprowadzona, aby uniezależnić się od rozmiaru bajtu, który, gdy opracowywano standardy internetowe, nie we wszystkich komputerach miał 8 bitów. Jeśli rozmiar pakietu miałby przekroczyć MTU, protokół przewiduje fragmentację pakietu, czyli jego podział na porcje nieprzekraczające MTU, a po przesłaniu wszystkich fragmentów złożenie w całość u odbiorcy.

Zwykły użytkownik internetu ma do czynienia z węzłami, które wysyłają tylko własne pakiety i odbierają jedynie pakiety do nich adresowane. Takich końcowych węzłów jest większość. Aby zapewnić komunikację między nimi, muszą istnieć węzły tranzytowe, nazywane ruterami (ang. *router*), a czasem bramami (ang. *gateway*). Sieć IP podzielona jest

na podsieci. Podsieć buduje się za pomocą jednej ze wspomnianych wyżej technologii łączy sieciowych. Wszystkie węzły w podsieci mają wspólny prefiks adresu IP. Ten prefiks definiuje się, podając adres IP i liczbę wspólnych bitów (maskę podsieci). Przykładowo do podsieci 193.0.96.0/24 należą adresy, które mają wspólne początkowe 24 bity z adresem 193.0.96.0, czyli adresy 193.0.96.0 do 193.0.96.255. Ze względów historycznych adresu 193.0.96.0 nie używa się. Adres 193.0.96.255 jest adresem rozgłaszania: na niego wysyła się pakiety, które mają być dostarczone do wszystkich węzłów w tej podsieci. Węzły w obrębie podsieci mogą przekazywać sobie pakiety IP bezpośrednio, korzystając z zastosowanej technologii sieciowej. Aby przekazywać pakiety IP między podsieciami, muszą one mieć wspólny węzeł – wspomniany wyżej ruter, który w każdej z łączonych podsieci ma interfejs sieciowy z adresem należącym do tej podsieci. Aby pakiet dotarł od nadawcy do odbiorcy, musi zwykle przejść przez wiele ruterów. Istotną rolę we właściwym przekazywaniu pakietów odgrywają tablice tras. Każdy węzeł sieci IP musi mieć zdefiniowaną tablicę tras. Wiersz tablicy tras zawiera:

- docelową podsieć;
- adres rutera, do którego należy przesłać pakiet, aby osiągnąć tę podsieć, albo informację, że docelowy węzeł jest w tej samej podsieci i możliwe jest bezpośrednie dostarczenie pakietu;
- nazwę interfejsu, przez który należy wysłać pakiet.

Algorytm wyznaczania trasy porównuje adres docelowy pakietu z celami umieszczonymi w tablicy tras. Napotkawszy zgodność, wysyła pakiet przez podany interfejs sieciowy bezpośrednio do węzła docelowego lub do kolejnego rutera. Tablica tras węzła końcowego jest bardzo prosta. Dla węzła o adresie 193.0.96.13 może wyglądać tak:

Cel	Ruter	Interfejs
193.0.96.0/24	bezpośrednio	eth0
inny	193.0.96.1	eth0

Rozważany węzeł ma tylko jeden (ethernetowy) interfejs sieciowy: eth0. Wszystkie pakiety są wysyłane przez ten interfejs. Pierwszy wiersz oznacza, że pakiety do własnej podsieci należy wysyłać bezpośrednio. Drugi wiersz mówi, że inne pakiety należy wysyłać do wskazanego rutera, który będzie wiedział, co z nimi zrobić. Tablica tras rutera zawiera więcej wpisów. Dla rozważanego rutera mogłaby ona wyglądać tak:

Cel	Ruter	Interfejs
193.0.96.0/24	bezpośrednio	eth0
193.0.97.0/24	bezpośrednio	eth1
89.73.136.0/28	bezpośrednio	eth2
inny	89.73.136.2	eth2

Ruter ten ma trzy interfejsy sieciowe: eth0, eth1, eth2. Każdy z tych interfejsów jest w innej podsieci i dla każdej podsieci tablica zawiera wiersz definiujący zakres adresów w tej podsieci i określający, że dostarczanie do tej podsieci jest bezpośrednie. Ostatni wiersz opisuje, co zrobić z pakietami o adresach docelowych niepasujących do żadnej ze znanych podsieci: w tym przykładzie należy je wysyłać do rutera 89.73.136.2.

Algorytm dostarczania pakietów IP jest zawodny. Dostarczenie pakietu jest możliwe, jeśli istnieje w sieci ścieżka od węzła źródłowego do węzła docelowego, taka że wszystkie rutery na tej ścieżce działają i mają poprawne tablice tras oraz wszystkie łącza są sprawne i nie są przeciążone przesyłaniem innych pakietów. Tablice tras ruterów są częściowo konfigurowane ręcznie przez administratorów, a częściowo automatycznie za pomocą protokołów wymiany informacji o trasach. Struktura internetu nie jest statyczna: węzły i łącza między nimi pojawiają się i znikają. Skutkuje to również odpowiednimi zmianami w tablicach tras. Istotną cechą algorytmu wyznaczania tras w internecie jest brak globalnej informacji adresowej: poszczególne rutery znają tylko swoje najbliższe otoczenie. Lokalność tablic tras może doprowadzić do powstania cyklu – zamkniętej ścieżki, w której pakiet, raz do niej wpadłszy, krążyłby w nieskończoność. Kolejne pakiety trafiające w taki cykl doprowadziłyby niechybnie do wysycenia przepustowości łączy i zablokowania dostarczania pakietów. W celu uniknięcia takiej sytuacji nagłówek IP zawiera jeszcze jedno, niewspomniane dotychczas, pole określające maksymalny czas przebywania pakietu w sieci. Nadawca pakietu ustala wartość początkową tego pola, np. 64, a każdy ruter przetwarzający ten pakiet zmniejsza tę wartość o jeden i jeśli jest ona nadal dodatnia, przesyła pakiet dalej. Jeśli wartość tego licznika osiągnie zero, ruter porzuca pakiet. Dzięki temu żaden pakiet nie może krążyć w sieci w nieskończoność.

Na bazie IP działają protokoły transportowe internetu. Dwa podstawowe to UDP i TCP. W rzeczywistości dane wymieniane są nie między urządzeniami, a między programami uruchamianymi na tych urządzeniach. UDP i TCP rozszerzają IP o dodatkowy poziom adresowania procesów (programów realizujących poszczególne usługi sieciowe). Dodatkowo TCP wprowadza kontrolę przepływu i zapewnia niezawodność dostarczania danych za pomocą potwierdzania ich dostarczenia i retransmisji danych zgubionych. Na bazie UDP lub TCP działają protokoły aplikacyjne: do tłumaczenia nazw domenowych na adresy IP (DNS), do przesyłania zawartości stron www (HTTP), do przesyłania poczty elektronicznej (SMTP, POP3, IMAP), do konfigurowania węzłów (DHCP) i wiele innych. Specyfikację protokołów internetowych można poznać oraz prześledzić historię ich rozwoju, czytając dokumenty RFC (ang. *Request for Comments*), dostępne, a jakże, w internecie.

Delta i fizyka cząstek elementarnych (I): Model Standardowy jaki jest, każdy widzi

Piotr CHANKOWSKI[*]

Rzeczy należy przedstawiać tak prosto, jak tylko to jest możliwe. Ale nie prościej.
nieważne kto, ważne, że słusznie!

Od swych narodzin z początkiem roku 1974 *Delta* asystowała burzliwemu rozwojowi fizyki cząstek elementarnych. Na jej łamach regularnie pojawiały się doniesienia z „frontu" oraz artykuły przybliżające jej Czytelnikom wybrane zagadnienia tej fascynującej dziedziny fizyki. Nic więc dziwnego, że do jubileuszowego pięćsetnego numeru Δ^1_{16} Redakcja zamówiła artykuł podsumowujący, co się wydarzyło w fizyce cząstek elementarnych, zwanej dziś częściej fizyką wysokich energii, przez ponad 40 lat istnienia *Delty*. Artykuł taki Czytelnikom *Delty* się jak najbardziej należy także z tego powodu, że 4 lipca 2012 roku zamknął się pewien długi rozdział badań nad oddziaływaniami cząstek elementarnych. Tego dnia ogłoszono odkrycie w eksperymentach prowadzonych w CERN-ie przy akceleratorze LHC rezonansu o masie 125 GeV, którego wszystkie charakterystyki są, w przedziałach osiągniętej dokładności doświadczalnej, takie jak przewidywanego przez teorię tzw. bozonu Higgsa.

Dzięki tym badaniom opracowany został spójny obraz struktury materii na odległościach do 10^{-19} m i zidentyfikowane zostały jej podstawowe „cegiełki" – punktowe (jak się wydaje), czyli prawdziwie elementarne cząstki (Δ^1_{74}). Stworzona i przetestowana została teoria oddziaływań fundamentalnych, zwana już od lat Modelem Standardowym. W ramach jednolitej struktury matematycznej opisuje ona trzy znane rodzaje oddziaływań cząstek elementarnych: silne, elektromagnetyczne i słabe (nie uwzględnia tylko oddziaływań grawitacyjnych). Teoria ta opiera się na kilku fundamentalnych ideach fizycznych, które wszystkie w zasadzie zostały sformułowane jeszcze przed powstaniem *Delty*, w przełomowych dla fizyki wysokich energii latach 1957–1973. Dlatego, aby osadzić we właściwym kontekście odkrycia, jakich dokonywano w fizyce wysokich energii za czasów istnienia *Delty*, konieczne jest bardziej całościowe ujęcie tematu zadanego mi przez Redakcję. W jakimś sensie prawie wszystko, co zdarzyło się w tej dziedzinie po roku 1974, a dotyczyło formowania się naszego zrozumienia świata cząstek dostępnego badaniom laboratoryjnym, miało charakter potwierdzenia idei teoretycznych sformułowanych w owych przełomowych latach lub nieco wcześniej. Oczywiście, po roku 1974 pojawiło się też wiele nowych idei teoretycznych, niektóre rewolucyjne, o których wspomnę w tym artykule. Trzeba jednak wyraźnie powiedzieć, że na razie żadna z tych idei nie została potwierdzona doświadczalnie i badanie ich konsekwencji oraz szukanie związanych z tymi ideami zjawisk będzie przypuszczalnie jeszcze zadaniem dla dzisiejszych młodych Czytelników *Delty*.

Aby lepiej zrozumieć, jaką rolę w formowaniu Modelu Standardowego i jego potwierdzaniu spełniły odkrycia dokonane po powstaniu *Delty*, dobrze jest najpierw pokrótce przedstawić tę teorię. Jak zapewne wszystkim Czytelnikom *Delty* wiadomo, podstawowymi składnikami materii (przynajmniej, jeśli nie próbujemy wnikać głębiej niż na odległości rzędu 10^{-19} m) są kwarki i leptony – punktowe cząstki o spinie równym $\hbar/2$. Jak wszystkie cząstki o spinie połówkowym, zwane fermionami, podlegają one zakazowi Pauliego (Δ^{10}_{78}). Grupują się one w trzy rodziny po cztery cząstki każda (zob. Δ^5_{05}, Δ^{12}_{12}): jeden kwark o ładunku $-1/3$ (w jednostkach $e > 0$), jeden o ładunku $2/3$, lepton o ładunku -1 i elektrycznie obojętne neutrino. I tak, pierwsza rodzina to kwarki dolny d i górny u oraz elektron e^- i jego neutrino ν_e, druga to kwarki dziwny s i powabny c oraz mion μ^- i neutrino mionowe ν_μ i wreszcie trzecia to kwarki piękny b i top t oraz leptony τ^- i ν_τ. Każdy z naładowanych fermionów może być lewo lub prawoskrętny, tj. mieć spin skierowany bądź zgodnie, bądź przeciwnie do kierunku jego pędu. Każdy z nich ma do pary odpowiadającą mu antycząstkę o takim samym spinie i przeciwnym ładunku elektrycznym. Każdy z kwarków to właściwie trzy kwarki różniące się pewną wewnętrzną cechą zwaną *kolorem*; trzy zaś antykwarki rozróżnia *antykolor*. Rodzaje kwarków nazywa się *zapachami*. Odpowiadające sobie cząstki kolejnych rodzin różnią się tylko masą (i z definicji zapachem). Cząstki i ich antycząstki mają

Pisząc Δ^n_{XY}, odwołujemy się do numeru n *Delty* z roku $19XY$ lub $20XY$; w przypadku pisma o mniej niż stuletniej tradycji jest to oznaczenie jednoznaczne. Pełna lista przywoływanych artykułów jest na stronie `www.deltami.edu.pl`.

Cząstki elementarne jako obiekty mikroświata podlegają prawom mechaniki kwantowej (zob. Δ^4_{75}, Δ^9_{76}, Δ^2_{78}). Przewidywania kwantowych teorii mają charakter statystyczny i polegają na podaniu prawdopodobieństw zajścia pewnych procesów. Każdemu zdarzeniu elementarnemu przypisuje się liczbę zespoloną $\mathcal{A}$ – tzw. amplitudę prawdopodobieństwa. Prawdopodobieństwo zajścia zdarzenia jest dane przez $|\mathcal{A}|^2$. Jeśli cały proces składa się z ciągu zdarzeń o amplitudach $\mathcal{A}_i$, $i = 1, \ldots, n$, to amplitudą całego procesu jest $\mathcal{A} = \mathcal{A}_1 \cdot \ldots \cdot \mathcal{A}_n$. Jeśli proces może zajść na m sposobów, z których każdy ma amplitudę $\mathcal{A}_i$, to amplitudą całego procesu jest $\mathcal{A} = \mathcal{A}_1 + \ldots + \mathcal{A}_m$. Właśnie ta reguła, która odróżnia kwantową probabilistykę od klasycznej, prowadzi do charakterystycznych dla mechaniki kwantowej zjawisk interferencyjnych.

Zwyczajem fizyków cząstek elementarnych energię E, pęd p i masę m podajemy w tych samych jednostkach, traktując prędkość światła c jako równą jedności. Bez tego wielkościami o tych samych mianach są E, pc i mc^2.

[*]Wydział Fizyki,
Uniwersytet Warszawski

takie same masy. Jeśli zaś chodzi o neutrina i antyneutrina, sprawa nie jest wciąż jasna: przez długie lata (kiedy uważano neutrina za bezmasowe) przyjmowano, że istnieją tylko lewoskrętne neutrina i prawoskrętne antyneutrina. Dziś, gdy wiadomo już, że masy neutrin nie są zerowe, bardziej prawdopodobne jest, że to, co dotąd nazywano lewoskrętnym neutrinem i prawoskrętnym antyneutrinem jest po prostu jedną cząstką istotnie obojętną. Szerzej sprawę tę omówię w dalszej części tego artykułu. (Niejasność ta nie ma jednak wpływu na strukturę najważniejszych oddziaływań cząstek).

Uniwersalnym językiem teoretycznym opisu cząstek elementarnych jest relatywistyczna kwantowa teoria pola, według której cząstki są „kwantami", tj. elementarnymi wzbudzeniami pewnych pól. (Zrozumienie tego także jest jednym z ważnych osiągnięć fizyki wysokich energii; był bowiem okres, gdy wydawało się, iż kwantowa teoria pola nie nadaje się do opisu oddziaływań cząstek elementarnych.) Pola w strukturze tej teorii są reprezentowane przez operatory działające na wektory pewnej przestrzeni Hilberta reprezentujące stany układu pól. Operatory te spełniają pewne równania, ale o „fizyce" decydują nie tylko one, lecz także charakter stanu o najniższej energii układu pól (tj. reprezentującego go wektora przestrzeni Hilberta). Stan ten nazywa się próżnią. To ona w dużej mierze determinuje rodzaj elementarnych wzbudzeń układu pól, które utożsamiamy z cząstkami.

W pewnym uproszczeniu kwantowa teoria pola opisuje oddziaływania cząstek jako elementarne akty, w których jedne cząstki znikają, a na ich miejsce powstają inne. Najprostsze oddziaływanie jednej cząstki z drugą polega więc na wymienieniu między nimi trzeciej (wirtualnej, tj. takiej, której energia E i pęd nie spełniają relatywistycznego związku $E^2 = \mathbf{p}^2 + m^2$) cząstki. Np. od czasów Diraca, Heisenberga i Pauliego wiadomo, że mający niezerowy ładunek punktowy elektron (fermion o spinie $\hbar/2$) może w elementarnym akcie wyemitować lub pochłonąć foton, zmieniając przy tym swoją energię E i pęd $\mathbf{p}$. Każdy taki akt charakteryzuje się pewną stałą sprzężenia, którą w przypadku oddziaływań fotonu jest e – ładunek elementarny. W kwantowej teorii pola stała sprzężenia jest miarą prawdopodobieństwa tego, jak „chętnie" cząstka emituje lub pochłania foton – mnoży ona amplitudę takiego zdarzenia. Wyemitowany foton może zostać pochłonięty przez inną naładowaną elektrycznie cząstkę, co w efekcie daje oddziaływanie tych cząstek na odległość, lub zostać zarejestrowany przez detektor (rejestracja przez detektor to też w gruncie rzeczy oddziaływanie fotonu z atomami detektora). Foton – bezmasowa cząstka o spinie $1\hbar$ – jest więc nośnikiem oddziaływań elektromagnetycznych lub, inaczej mówiąc, bozonem pośredniczącym tych oddziaływań (Δ^{11}_{90}).

W podobny sposób nośnikami oddziaływań silnych pomiędzy kwarkami są gluony – bezmasowe bozony o spinie $1\hbar$. O ile jednak fotony nie niosą ładunku elektrycznego (są elektrycznie obojętne), gluony nie są „kolorowo obojętne": w pewnym uproszczeniu (wbudowana w kwantową teorię pola teoria grup ujmuje to precyzyjnie) gluon ma kolor i antykolor (jest np. czerwono-antyniebieski). W elementarnym akcie oddziaływania wskutek pochłonięcia czerwono-antyniebieskiego gluonu znika kwark (np. u lub d) niebieski i powstaje kwark tego samego typu (u lub d), ale czerwony. Charakteryzująca oddziaływania silne stała g_s jest dużo większa niż e. Ponieważ gluony nie są kolorowo obojętne, możliwe są też oddziaływania gluonów ze sobą.

Opisane wyżej elementarne oddziaływania fotonów z naładowanymi fermionami i gluonów z kolorowymi kwarkami są niechiralne, tj. nie zależą od skrętności: lewo i prawoskrętny fermion oddziałują jednakowo „chętnie".

Oprócz fotonów i gluonów nośnikami oddziaływań są też bozony W^+, W^- (antycząstka W^+) i Z^0 – masywne (odpowiednio 80 i 91 razy cięższe niż proton) cząstki o spinie $1\hbar$. Są one nośnikami oddziaływań słabych. Bozony Z^0 oddziałują ze wszystkimi fermionami (i antyfermionami): w elementarnym akcie fermion emituje lub pochłania Z^0, nie zmieniając przy tym swojej „tożsamości". Jednak w odróżnieniu od oddziaływań z fotonami czy gluonami oddziaływania z bozonami Z^0 zależą silnie od skrętności: fermiony lewo- i prawoskrętne oddziałują inaczej. Mówimy wobec tego, że oddziaływania Z^0 mają nietrywialną strukturę chiralną. Ogólną stałą sprzężenia charakteryzującą oddziaływania bozonów Z^0 (jest ona modyfikowana jeszcze przez czynniki odróżniające skrętność) jest $e/\sin 2\theta_W$, gdzie kąt θ_W jest zwany kątem Weinberga ($\sin^2\theta_W \approx 0{,}23$).

Spin jest wewnętrznym momentem pędu cząstki. Według zasad mechaniki kwantowej cząstki mogą mieć spin $s \geqslant 0$ albo całkowity, albo połówkowy (w jednostkach $\hbar$). Rzut spinu cząstki na wybrany kierunek może przyjmować wartości $-s$, $-s+1$, …, $s-1$, s. W przypadku cząstek elementarnych wyróżnionym kierunkiem jest zawsze kierunek ich pędu.

Cząstka o spinie $\hbar/2$ spolaryzowana prawoskrętnie

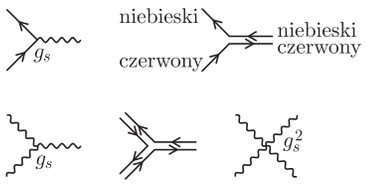
i lewoskrętnie

Osobliwością cząstek bezmasowych o spinie s jest to, że ich skrętność może przyjmować tylko skrajne wartości $-s$ i $+s$. Cząstki o spinie $1\hbar$, takie jak foton, nie mogą zatem mieć skrętności równej zeru.

Idea, że oddziaływania polegają na znikaniu i pojawianiu się *ex nihilo* cząstek pochodzi w gruncie rzeczy od Enrico Fermiego, który jako pierwszy (w roku 1934) opisał w ten sposób rozpady β jąder: według jego teorii w procesie rozpadu znikał np. neutron, a na jego miejsce powstawały proton, elektron i antyneutrino; wcześniej, przed odkryciem neutronu przez Jamesa Chadwicka w roku 1932, sądzono, że po prostu protony i elektrony są składnikami jąder.

Oddziaływanie elementarne („wierzchołek oddziaływania") elektrodynamiki kwantowej cząstek o spinie $\hbar/2$ i oddziaływanie wymienne.

Mierzalnymi wielkościami charakteryzującymi cząstki elementarne i ich oddziaływania są masy, spiny, liczby kwantowe (takie jak izospin czy dziwność), czasy życia, przekroje czynne i szerokości rozpadów. Ostatnie dwie grupy wielkości wyznacza się teoretycznie, obliczając kwantowomechaniczne amplitudy $\mathcal{A}$ odpowiednich procesów. Wygodnym narzędziem służącym do tego celu są diagramy Feynmana, które pozwalają łatwo wypisać (co nie znaczy jeszcze obliczyć!) w porządku od najbardziej do coraz mniej istotnych przyczynki do takich amplitud prawdopodobieństwa. Diagramy te otrzymuje się, łącząc ze sobą na wszystkie możliwe sposoby odpowiednie linie elementarnych wierzchołków oddziaływania i dołączając do tychże wierzchołków linie reprezentujące cząstki występujące na początku reakcji i na jej końcu. Każdemu elementowi tak otrzymanego diagramu Feynmana odpowiadają określone wyrażenia analityczne, które zestawione razem w sposób jednoznacznie podyktowany strukturą diagramu dają odpowiadający mu przyczynek do amplitudy $\mathcal{A}$. Przekrój czynny czy szybkość rozpadu zależy od amplitudy $\mathcal{A}$ procesu (czynnik dynamiczny) i od dostępnej przestrzeni fazowej (czynnik kinematyczny).

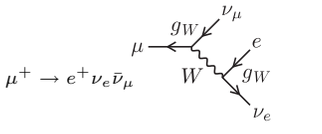


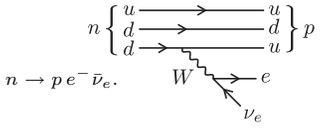
Oddziaływania silne kwarków i gluonów.

Chiralność (prawa i lewa) nie jest właściwością fermionu jako cząstki fizycznej; jest to cecha charakteryzująca sposób przekształcania się przy zmianie układu odniesienia pól, których wzbudzeniami są fermiony. Jeśli jednak masa fermionu jest zerowa, jego stan o określonej skrętności i stan jego antycząstki o przeciwnej skrętności są jednoznacznie związane z kwantowym polem o określonej chiralności.

Podział na cząstki i nośniki ich oddziaływań jest, oczywiście, tylko pewnym umownym sposobem mówienia o procesach elastycznych, w których cząstki końcowe są takiego samego rodzaju, jak cząstki początkowe. Np. w przypadku rozpraszania $e^-\gamma \to e^-\gamma$ można powiedzieć, że nośnikiem oddziaływania elektronu z fotonem jest sam elektron.

Słabe rozpady



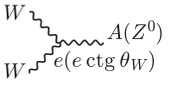


Macierz CKM jest unitarna, tzn. spełnia warunek

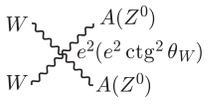
$$\sum_{i=u,c,t} V_{ij}^* V_{ik} = \begin{cases} 1 & \text{gdy } j = k, \\ 0 & \text{gdy } j \neq k, \end{cases}$$

gdzie $k = d, s, b$.

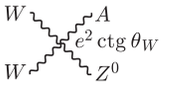
Wierzchołki oddziaływania



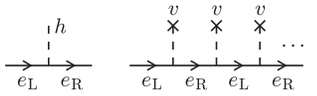
$W^+W^-A(Z^0)$



$W^+W^-AA(Z^0Z^0)$



$W^+W^-AZ^0$.



Sprzężenia fermionów do h^0 i do kondensatu.

Najbardziej skomplikowane są oddziaływania bozonów W^+ i W^- (oddziałują z nimi wszystkie fermiony i antyfermiony). Po pierwsze, oddziaływania te również w sposób charakterystyczny zależą od skrętności: gdyby masa fermionu była ściśle zerowa (albo gdy jego energia jest na tyle duża, że w porównaniu z nią można jego masę spoczynkową pominąć), z bozonami $W^\pm$ oddziaływałyby tylko lewoskrętne fermiony i prawoskrętne antyfermiony. Zatem oddziaływania bozonów $W^\pm$ również mają nietrywialną strukturę chiralną. Chiralny charakter sprzężeń bozonów $W^\pm$ i Z^0 do fermionów jest odpowiedzialny za niezachowanie parzystości w procesach słabych (łamanie symetrii względem odbicia lustrzanego, Δ^{10}_{87}, Δ^{12}_{95}).

Ponieważ bozony $W^\pm$ są naładowane, kwark typu dolnego musi, wyemitowawszy bozon W^- (lub pochłonąwszy W^+), przejść w kwark typu górnego, a elektron w neutrino itp. Oddziaływania bozonów $W^\pm$ z kwarkami mają także nietrywialną strukturę zapachową: wprawdzie kwark d, emitując bozon W^-, najchętniej przechodzi w kwark u, może on jednak przejść, trochę mniej chętnie, w kwark powabny c, a nawet, choć już bardzo niechętnie, w kwark t. Stałą sprzężenia bozonów $W^\pm$ do leptonów jest $e/\sqrt{2}\sin\theta_W$. Siła zaś ich oddziaływania z kwarkami jest dodatkowo osłabiana przez czynniki V_{ud}, V_{us}, etc. określające, jak „chętnie” kwark u przechodzi w kwarki d, s itd. Czynników takich jest, jak łatwo policzyć, 9; razem tworzą one tzw. macierz Cabibbo–Kobayashiego–Maskawy (CKM). Ma ona wyraźnie hierarchiczną strukturę: preferowane są, przy oddziaływaniu z $W^\pm$, przejścia w obrębie tej samej rodziny (np. s w c), zmiana rodziny na sąsiednią (np. u w s) jest mniej prawdopodobna, a najrzadsze są przejścia z rodziny pierwszej do trzeciej (np. u w b). Okazuje się, że przy trzech rodzinach kwarków fazy elementów macierzy CKM (jako liczb zespolonych) są określone przez tylko jeden parametr – kąt δ. Różna od zera wartość tego kąta jest odpowiedzialna za niezachowywanie w niektórych procesach uwarunkowanych oddziaływaniem słabym parzystości kombinowanej CP (Δ^4_{89}).

Ponieważ bozony $W^\pm$ mają ładunek elektryczny, oddziałują one z fotonami (bozon W może w elementarnym akcie wyemitować lub pochłonąć jeden lub dwa fotony). Istnieją także oddziaływania $W^\pm$ z Z^0 oraz z Z^0 i fotonem. Podobnie jak leptony, foton, kwarki i gluony, bozony $W^\pm$ i Z^0 są, przynajmniej na ile nam dziś wiadomo, cząstkami punktowymi (niezłożonymi).

Ostatnią cząstką niezłożoną (?) jest świeżo zarejestrowany bozon Higgsa h^0 – bezspinowa neutralna cząstka o masie 125,3 GeV. Pole, którego jest ona wzbudzeniem, pełni bardzo ważną rolę. Teoria mówi, że wytwarza ono przenikający całą przestrzeń, stały kondensat v mający wymiar masy ($v \approx 246$ GeV), analogiczny pod pewnymi względami do kondensatu Bosego–Einsteina (zob. Δ^{10}_{96}), za którego doświadczalne badanie Nagrodę Nobla w roku 2001 otrzymali E.A. Cornell, W. Ketterle i C.E. Wieman (Δ^1_{02}). Występowanie tego kondensatu jest właściwością stanu próżni układu pól kwantowych modelu standardowego. Wszystkie cząstki z wyjątkiem fotonu zmuszone są nieustannie oddziaływać z owym kondensatem, co jest źródłem ich mas (zjawisko zmieniania się masy cząstek wskutek oddziaływań jest dobrze znane z fizyki ciała stałego: elektrony poruszające się w sieci krystalicznej można efektywnie traktować jak cząstki swobodne oddziałujące tylko ze wzbudzeniami sieci – fononami – jeśli przypisze się im masy inne niż masa elektronu w próżni). Poszczególne fermiony sprzęgają się z różną siłą do pola Higgsa i tym samym ich masa jest ściśle proporcjonalna do stałych y_f, zwanych stałymi Yukawy, charakteryzujących ich sprzężenia do h^0. Pole Higgsa, a tym samym i bozon h^0, oddziałuje też z bozonami pośredniczącymi $W^\pm$ i Z^0, nadając im niezerowe masy (Δ^6_{99}).

Chociaż nie możemy wchodzić tu w matematyczne szczegóły kwantowej teorii pola, która jest jedną z najbardziej skomplikowaną z teorii opisujących świat fizyczny, aby umożliwić lepsze zrozumienie struktury modelu standardowego, postaram się jednak krótko przybliżyć zasady, na których się on opiera. Mimo, a może właśnie z powodu wyjątkowego charakteru tego numeru *Delty*, potraktuję Czytelników poważnie i, nawiązując do motta tego artykułu, postaram się w kolejnych odcinkach pokazać bogactwo struktury teoretycznej ukrytej za prostym fenomenologicznym opisem cząstek i ich oddziaływań. Dopiero wtedy będzie można bowiem w pełni docenić rozwój fizyki wysokich energii w minionym sześćdziesięcioleciu.

Postępy kosmologii po roku 1974

*Andrzej KRASIŃSKI**

1. Stan początkowy. W momencie ukazania się pierwszego numeru *Delty* kosmologia opierała się na następujących obserwacjach (o), konkluzjach (k) i postulatach (p):

(I) (o) Inne galaktyki, poczynając od pewnej minimalnej odległości, oddalają się od naszej. Kierunek ruchu jest radialny, a prędkość v w przybliżeniu proporcjonalna do odległości d (prawo Hubble'a).

(II) (k) W przeszłości średnia gęstość (a więc również temperatura) materii we wszechświecie musiała być większa niż obecnie, tym większa, im dalej w przeszłość patrzymy. Był taki okres w historii wszechświata, w którym temperatura i gęstość były zbyt wysokie, aby mogły istnieć atomy i cała materia była zjonizowana. Gdy temperatura spadła poniżej wartości potrzebnej do jonizacji atomów, musiało zostać wyemitowane promieniowanie, które powinno dotrwać do naszych czasów.

(III) (o) Kosmiczne mikrofalowe promieniowanie tła zostało zaobserwowane w roku 1965. Ma ono widmo charakterystyczne dla ciała doskonale czarnego o średniej temperaturze 2,73 K i dochodzi do Ziemi ze wszystkich kierunków. Odchylenia od średniej w poszczególnych kierunkach podzielone przez średnią temperaturę, $\Delta T/T$, były wówczas niewykrywalne przy błędzie pomiaru 0,01.

(IV) (p) Wszechświat wydaje się w przybliżeniu izotropowy wokół nas. *Założono* więc, że wszechświat jest izotropowy wokół każdego obserwatora. Postulat ten, pod nazwą *zasady kosmologicznej*, jest do dziś dogmatem astronomii.

Punkt (III) wymaga komentarza. Izotropię promieniowania tła na poziomie 10^{-2} uznano za „zdumiewająco dokładny" dowód izotropii wszechświata. Okazało się potem, że oddziaływanie promieniowania tła z materią jest bardzo słabe i fluktuacje mogły ujawnić się dopiero na poziomie $\Delta T/T \approx 10^{-5}$. Takie właśnie fluktuacje zaobserwowano.

2. Odkrycie pustek w rozkładzie galaktyk (1978). Pierwszą poprawkę do opisanego wyżej stanu wniosło odkrycie „dziur" w przestrzennym rozkładzie galaktyk (S.A. Gregory i L.A. Thompson 1978). Do tamtego momentu zakładano, że elementarną „komórką" wszechświata jest pojedyncza galaktyka i że galaktyki są równomiernie rozłożone w przestrzeni, zgodnie z zasadą kosmologiczną. Okazało się, że przestrzenny rozkład galaktyk bardziej przypomina pianę na powierzchni wody w wannie, z galaktykami rozmieszczonymi na powierzchniach pęcherzyków o typowym promieniu około 60 Mpc. Wnętrza pęcherzyków są *prawie* puste – średnia gęstość materii w pustce wynosi od kilku do kilkunastu procent średniej gęstości w całym wszechświecie. Ogłoszono to jako wielkie odkrycie, chociaż z pewnych prac, opublikowanych 44 lata wcześniej, wynikało, że powszechnie używane w astronomii jednorodne i izotropowe modele kosmologiczne są niestabilne ze względu na powstawanie zagęszczeń i rozrzedzeń (R.C. Tolman 1934, N.R. Sen 1934). Gdyby prace te zostały w porę zrozumiane, odkrycie pustek nie byłoby niespodzianką.

Skąd wzięła się sprzeczność pomiędzy wcześniejszą wiarą a nowym odkryciem? Przed pracą Gregory'ego i Thompsona obserwacje sięgały tylko do niezbyt dalekich galaktyk i *w przybliżeniu* potwierdzały zasadę kosmologiczną. Astronomowie wierzyli, że ta nieduża objętość jest reprezentatywną próbką całego wszechświata, a swoją wiarę głosili jako rzeczywistą wiedzę.

Odkrycie to wymaga jeszcze jednego komentarza. Nie istnieje metoda bezpośredniego pomiaru odległości do najdalszych galaktyk. Przy *ocenianiu* odległości do nich *zakłada się*, że prawo Hubble'a jest spełnione i *oblicza* z niego odległość. Występuje więc paradoks: gdy zakładamy, że wszechświat jest przestrzennie jednorodny (bo tylko w takim prawo Hubble'a obowiązuje), to z analizy obserwacji wychodzi nam, że materia w nim jest rozłożona niejednorodnie. Jeśli dopuścimy, że prawo Hubble'a nie obowiązuje, to jesteśmy bezradni (przynajmniej tymczasowo) wobec problemu wyznaczania odległości, ale przyznajemy na starcie, że wszechświat nie jest jednorodny. Tak czy inaczej,

Rozwiązanie zadania F 895.
(a) Liczba elektronów równa jest, oczywiście, liczbie protonów w atomach naszego ciała. Każdy gramoatom pierwiastka to $N_A \approx 6{,}022 \cdot 10^{23}$ atomów. Gramoatom to liczba gramów pierwiastka równa (z bardzo dobrym przybliżeniem sumie liczb protonów i neutronów jądra atomu). Ciało człowieka zbudowane jest głównie z atomów tlenu, węgla wodoru, azotu. Poza wodorem wymienione pierwiastki występują niemal wyłącznie w postaci izotopów o równej liczbie protonów i neutronów, a więc w każdym ich gramoatomie mamy $N_A/2$ protonów. Wodór to niemal wyłącznie izotop ^{1}H najczęściej związany w cząsteczkach wody (stanowiącej składnik żywych komórek). W cząsteczce wody mamy 10 protonów i 8 neutronów, co oznacza, że jeśli pominiemy niewielką różnicę mas protonu i neutronu, to $5/9 = 0{,}55\ldots$ masy wody przypada na protony. Z dokładnością do 10% możemy więc przyjąć, że średnio 1 g naszego ciała zawiera około 0,5 g protonów, a więc około $N_A/2 \approx 3 \cdot 10^{23}$ protonów i tyle samo elektronów.

Poza wymienionymi w rozwiązaniu inne pierwiastki stanowią łącznie mniej niż 4% masy człowieka.

(b) Stosunek liczby protonów do liczby wszystkich nukleonów w jądrze jest dla większości naturalnie występujących izotopów bliski 0,5 i nieznacznie maleje ze wzrostem liczby atomowej do około 0,39 dla ^{238}U. Wyjątek (patrz (a)) stanowi wodór, który niemal wyłącznie występuje jako izotop ^{1}H, ale stanowi on niewielką część masy otaczających nas substancji (np. tylko 10% masy wody). Zatem dla otaczającej nas materii wynik jest taki sam, jak dla naszego ciała.

*Centrum Astronomiczne im. Mikołaja Kopernika

zasada kosmologiczna jest w kłopocie. Oficjalne stanowisko kosmologów jest następujące: zasada kosmologiczna obowiązuje, ale w większej skali. Elementarna komórka wszechświata jest większa niż pojedyncza galaktyka. Jaki jest jej rozmiar? Tu zapada kłopotliwe milczenie. Tak daleko, jak sięgają obserwacje rozkładu galaktyk, widać rozmaite struktury i nie widać powtarzalności w ich przestrzennym rozkładzie.

3. Modele inflacyjne (1981). Niektórzy kosmologowie zauważyli pozorne paradoksy, wynikające z używanych wcześniej modeli wszechświata. Jednym z nich był „problem płaskości": nawet jeśli uśredniona po przestrzeni gęstość masy ρ różni się od tzw. gęstości krytycznej ρ_{kr} o czynnik 100 w obecnej chwili, to w chwili $t_i = 10^{-34}$ sekund po Wielkim Wybuchu ułamek $(\rho - \rho_{\mathrm{kr}})/\rho$ musiał być mniejszy niż 10^{-55}. Stan początkowy wszechświata musiał więc być niezwykle dokładnie dopasowany do krzywizny przestrzennej bliskiej zera. Drugim był „problem horyzontu": wskutek skończonej prędkości światła w tej samej chwili t_i pojedyncza cząstka materii mogła otrzymać sygnał od ograniczonej liczby innych cząstek, nazwijmy tę liczbę n_i. Obecny obserwator, kilkanaście miliardów lat po Wielkim Wybuchu, mógł otrzymać sygnał od większej liczby cząstek, N_0, przy czym $n_i/N_0 = 10^{-83}$. Jak to się stało, że obecnie promieniowanie tła jest tak dokładnie izotropowe, skoro przed jego emisją tylko niewielkie podzbiory cząstek mogły oddziaływać między sobą? Przecież oddziaływanie było konieczne dla wyrównania temperatur.

Gęstość krytyczna to taka, przy której przestrzeń stałego czasu jest zawsze płaska (tak astronomowie nazywają przestrzenie euklidesowe, czyli o zerowej krzywiźnie).

Modele inflacyjne (Alan Guth, 1981) proponują rozwiązanie tych problemów, postulując, że w okresie między mniej więcej 10^{-34} a 10^{-32} sekund po Wielkim Wybuchu wszechświat rozszerzał się w tempie wykładniczym i w tym czasie każda początkowa odległość powiększyła się około 10^{26} razy. Umożliwiło to kontakt, przed emisją promieniowania tła, pomiędzy wszystkimi widocznymi dziś na niebie obiektami.

Jeśli Czytelnikom podane wyżej rozumowania wydają się naciągane, proszę nie wątpić w siłę własnego rozumu. W chwili t_i średnia gęstość materii musiała być większa niż $10^{68}\,\mathrm{g/cm^3}$, czyli 10^{54} razy większa niż w jądrze atomowym. Takich gęstości nie osiągnięto do dzisiaj w żadnym akceleratorze. Jeśli więc trzymamy się tradycji, że fizyka jest nauką empiryczną, to modele inflacyjne nie są teoriami fizycznymi. Do podobnego wniosku doszedł niedawno jeden z twórców idei inflacji, Paul Steinhardt, używając innego argumentu: modele inflacyjne mają tyle wolnych parametrów, że można je przystosować do każdych danych eksperymentalnych, a wobec tego nie są falsyfikowalne.

Modele te zdobyły ogromną popularność dzięki nieustającej kampanii reklamowej, prowadzonej przez autorów i entuzjastów, i z tego powodu musiały być wspomniane w niniejszym artykule. Ostrzegam jednak Czytelników, że jest to „odkrycie" z zakresu metafizyki. Wcześniejsze twierdzenia kosmologii (np. przepowiednia istnienia promieniowania tła) były oparte na wynikach doświadczeń laboratoryjnych. Twierdzenia modeli inflacyjnych można byłoby sprawdzić *wyłącznie* poprzez obserwacje kosmologiczne interpretowane przy użyciu spekulacji niemożliwych do sprawdzenia w laboratorium.

4. Odkrycie fluktuacji temperatury w promieniowaniu tła (1992). Na przełomie lat 80. i 90. ubiegłego wieku dwa zespoły astronomów (ich kierownikami byli John Mather i George Smoot) przeprowadziły dokładne pomiary temperatury promieniowania tła dla różnych kierunków. Ich wynikiem ubocznym było precyzyjne potwierdzenie, że promieniowanie to ma widmo ciała doskonale czarnego. Wynikiem głównym było wykrycie kierunkowych fluktuacji temperatury o maksymalnej amplitudzie około $70\,\mu\mathrm{K}$, co odpowiada $\Delta T/T \approx 2{,}5 \cdot 10^{-5}$. Odkrycie to umożliwiło dalsze badania własności materii wszechświata w momencie emisji promieniowania tła, między innymi rozchodzących się w niej fal akustycznych. Smoot i Mather otrzymali za nie Nagrodę Nobla w roku 2006.

5. Przyspieszająca ekspansja wszechświata? (1998, 1999). Gwiazda, która wyczerpała zapasy swojego „paliwa" termojądrowego, zaczyna się zapadać – ciśnienie słabnącego promieniowania nie może zrównoważyć siły grawitacji. Jeżeli

Energia uwalniana w wybuchu supernowej jest w przybliżeniu równa energii, jaką wypromieniuje Słońce w ciągu całego swojego „życia”.

jakiś inny mechanizm nie powstrzyma zapadania się gwiazdy, to wśród różnych możliwych wariantów dalszego jej losu jest gwałtowny wybuch, uwalniający wielką energię, która jest wyświecana w ciągu kilku tygodni lub kilku miesięcy. Wybuch taki, nazywany gwiazdą supernową, jest zjawiskiem bardzo rzadkim. Ostatnią supernową w naszej Galaktyce zaobserwowano bezpośrednio w roku 1604, a potem wykryto ślady po dwóch innych. Z obserwacji supernowych w innych galaktykach wynika, że w naszej Galaktyce średnio powinny zachodzić trzy takie wybuchy w ciągu stu lat.

Ewolucja gwiazdy prowadząca do wybuchu supernowej może przebiegać inaczej. W pierwszym stadium powstaje biały karzeł w układzie podwójnym. Jeśli gwiazda-towarzysz wyrzuca materię, to jej część opada na powierzchnię białego karła, doprowadzając w końcu do wybuchu. Ten rodzaj supernowych nazwano typem Ia. Ponieważ powstają one zawsze w takich samych warunkach, przyjmuje się, że ich maksymalna jasność absolutna jest zawsze taka sama. Mierząc strumień promieniowania supernowej docierający do Ziemi, można więc wyznaczyć *odległość jasnościową* d_L do niej. Można też zmierzyć przesunięcie ku czerwieni w jej widmie, przeliczyć je na prędkość ucieczki gwiazdy od nas, i *obliczyć* odległość d drugim sposobem, z prawa Hubble'a.

Wyniki takich pomiarów dla dużej liczby supernowych typu Ia opublikowały w latach 1998 i 1999 dwa zespoły astronomów, kierowane przez Adama Riessa i Saula Perlmuttera. Wyszło im, że $d_L > d$ we wszystkich przypadkach: supernowe były „pociemnione” względem tego, czego oczekiwano na podstawie używanego przedtem modelu ewolucji wszechświata. Przymierzając do swoich wyników różne nowe modele (ale tylko takie, w których gęstość materii jest stała w przestrzeni i może się zmieniać jedynie z upływem czasu), doszli oni do wniosku, że najlepsze dopasowanie daje model, w którym obecnie przestrzeń rozszerza się ruchem przyspieszonym. Jest to możliwe tylko wtedy, gdy istnieje oddziaływanie odpychające, przeważające nad przyciąganiem grawitacyjnym. Źródło tego oddziaływania nazwano „ciemną energią” i ogłoszono, że jest to „największa zagadka współczesnej astronomii”.

Wprowadzanie nowego bytu nie jest jednak konieczne. Wystarczy dopuścić do konkurencji ogólniejsze modele wszechświata, w których gęstość materii nie jest stała w przestrzeni. Najprostszy z nich, nazywany modelem Lemaître'a–Tolmana, pozwala wyjaśnić wyniki obserwacji supernowych Ia na dwa sposoby. W pierwszym wybuch początkowy nie zachodzi równocześnie dla wszystkich cząstek wszechświata. Cząstki bliższe obserwatora są z Wielkiego Wybuchu wyrzucane później niż dalsze, wobec tego w momencie obserwacji są „młodsze” i oddalają się od obserwatora z większą prędkością. W drugim sposobie cząstki bliższe obserwatora „rodzą się” z większą prędkością początkową, dając ten sam efekt w obserwacjach. W obydwu przypadkach złudzenie rosnącej z czasem prędkości ekspansji powstaje wskutek zmniejszania się tej prędkości z odległością od obserwatora. Przy takim opisie „ciemna energia” jest niepotrzebna – wszechświat rozszerza się ruchem opóźnionym. Jedyne odstępstwo od tradycyjnej kosmologii w tym modelu jest takie, że prędkość ucieczki galaktyk nie jest dokładnie proporcjonalna do ich odległości od nas. Większość astronomów wierzy jednak w ciemną energię, a odkrycie z lat 1998/99 zostało wyróżnione Nagrodą Nobla dla Riessa, Perlmuttera i Briana Schmidta w roku 2011.

6. Wiedza a przekonanie. Przez wszystkie etapy historii kosmologii przewija się jeden wspólny motyw: ubieranie niewiedzy w pozory wiedzy. Następujące potem zdemaskowanie niewiedzy jest przedstawiane jako zaskakujące odkrycie. Tak było w roku 1928, gdy z obserwacji Hubble'a wynikło, że wszechświat się rozszerza. Przedtem astronomowie *wiedzieli*, że jest niezmienny w czasie. Tak było w roku 1978, gdy odkryto pustki. Przedtem astronomowie *wiedzieli*, że przestrzeń jest równomiernie wypełniona galaktykami. Tak było w roku 1992, gdy odkryto fluktuacje temperatury promieniowania tła. Przedtem astronomowie *wiedzieli*, że promieniowanie to jest izotropowe ze zdumiewającą dokładnością. Teraz astronomowie *wiedzą*, że wszechświat rozszerza się ruchem przyspieszonym i nie chcą słuchać, że obserwacje supernowych typu Ia można wyjaśnić inaczej. Pewnie czeka nas kolejne zaskoczenie...

Rozwiązanie zadania F 896.
W obu przypadkach (kondensatora i przewodnika) przebieg linii sił pola elektrycznego jest taki sam: wektor natężenia pola elektrycznego $\vec{E}$ w każdym punkcie powierzchni każdej z elektrod jest do tej powierzchni prostopadły, a jego wartość jest proporcjonalna do napięcia U między elektrodami. Powierzchniowa gęstość ładunku w każdym punkcie elektrody kondensatora jest równa $\varepsilon_0 E$, gdyż przenikalność elektryczna powietrza jest praktycznie równa przenikalności próżni. Normalna składowa gęstości prądu jest także proporcjonalna do wartości pola E i jest równa E/ϱ. W związku z tym, przy tym samym napięciu U, całkowity ładunek zgromadzony na powierzchni elektrod $Q = CU$ jest proporcjonalny do całkowitego prądu $I = U/R$, który popłynie po wypełnieniu kondensatora roztworem soli. Otrzymujemy więc:

$$R = \frac{\varepsilon_0 \varrho}{C}.$$

Po podstawieniu danych liczbowych $R \approx 0{,}0133\ \Omega$.

Lekkość bytów kosmologicznych

Krzysztof TURZYŃSKI

Z czego składa się wszechświat? Jeżeli wierzyć temu, co setki kosmologów piszą w najpoważniejszych czasopismach naukowych, znana nam materia tzw. barionowa odpowiada za zaledwie 5% gęstości energii we wszechświecie, a pozostała część to tzw. ciemna materia i ciemna energia. O tych tajemniczych substancjach niewiele da się obecnie powiedzieć, poza tym, że ciemna materia zachowuje się jak pył niewidzialnych, masywnych cząstek, ciemna energia zaś ma pewne unikalne, ale bardzo konkretne własności, które powodują przyspieszone rozszerzanie się wszechświata.

Powyższe stwierdzenia są dla wielu przejawem triumfu myśli ludzkiej przejawiającej się w wydzieraniu przyrodzie jej tajemnic dzięki postępowi technik obserwacyjnych połączonemu z bardzo wnikliwą analizą teoretyczną tych obserwacji. Są też i tacy, którzy sądzą, że odważne twierdzenia współczesnej kosmologii są zwykłą hucpą. Jak osądzić, gdzie leży prawda i czy środowisko naukowców jest w stanie wycofywać się ze swoich twierdzeń, jeśli te okazują się błędne lub nie dają się należycie uzasadnić? Przyjrzyjmy się tym kwestiom na przykładzie ciemnej materii.

Klasyczny argument na rzecz istnienia ciemnej materii pochodzi z badania krzywych rotacji galaktyk i wynika z obserwacji poczynionych przez Verę Rubin od początku lat sześćdziesiątych XX wieku. Sądząc po natężeniu emitowanego światła, masa typowej galaktyki spiralnej skupiona jest w jej centrum, można więc w przybliżeniu traktować ruch obiegającej to centrum gwiazdy jako wywoływany przez pojedynczą centralną masę. Jeśliby więc siła grawitacyjna owej masy M działająca na gwiazdę o masie m w odległości r od centrum wyrażała się wzorem Newtona $F_g = \mathrm{G}Mm/r^2$ i stanowiła zarazem siłę dośrodkową powodującą ruch gwiazdy z prędkością v po okręgu, $F_r = mv^2/r$, to prędkość v powinna być odwrotnie proporcjonalna do pierwiastka z odległości r. Tak nie jest – obserwowana zależność $v(r)$ wydaje się dążyć do stałych, ale niezerowych wartości przy wzroście r. Aby to wyjaśnić, można założyć istnienie nieświecącej i nieoddziałującej ze światłem materii (zwanej ciemną materią) stanowiącej źródło dodatkowego przyciągania grawitacyjnego i umożliwiającej gwiazdom na szybsze, niżby można oczekiwać, okrążanie centrów galaktyk bez obawy ucieczki w kosmiczną przestrzeń. Idea to nieco szalona, ale jakoś trzeba przecież wyjaśnić obserwowaną zależność $v(r)$, skoro przez tyle dekad nie udało się znaleźć jakiegoś błędu w obserwacjach i ich interpretacji. Można ewentualnie wymyślić jeszcze jakąś inną szaloną ideę, na przykład taką, że newtonowskie prawo grawitacji nie stosuje się w tak wielkich skalach odległości...

Uwierzeniu w jedną z takich szalonych idei może pomóc fakt, że w latach trzydziestych XX wieku Fritz Zwicky, badając rozkłady prędkości galaktyk w gromadzie galaktyk w gwiazdozbiorze Warkocza Bereniki, również zauważył, że nie są one zgodne z rozkładem świecącej materii. Obecnie można niekiedy dzięki zjawisku soczewkowania grawitacyjnego ocenić rozkład masy w gromadzie galaktyk niezależnie od rozkładu natężenia światła. Najbardziej znanym przykładem jest gromada 1E0657-558 w gwiazdozbiorze Kila, zwana Pociskiem. Powstała ona w wyniku zderzenia dwóch gromad galaktyk; ów kosmiczny kataklizm znacznie spowolnił materię świecącą (przede wszystkim gaz emitujący promieniowanie X), ale nie ciemną materię, która oddziałuje przede wszystkim grawitacyjnie, i obserwowane rozkłady obu rodzajów materii wykazują wyraźnie rozsunięcie w przestrzeni. Te same obserwacje próbowano także interpretować przy użyciu modyfikacji oddziaływań grawitacyjnych, ale próby te nie wydają się prowadzić w tak prosty sposób do konkluzji jak hipoteza istnienia ciemnej materii. Tym bardziej że astronomowie w ciągu ostatniej dekady wzbogacili swą kolekcję zderzających się gromad galaktyk o jeszcze kilka, może nieco mniej spektakularnych obiektów...

Ciemna materia musi być rozłożona we wszechświecie w sposób niejednorodny, toteż szacowanie jej średniej gęstości w obserwowalnym wszechświecie jest

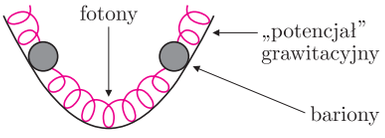
Rozwiązanie zadania M 1481.
Każdy wiersz i kolumnę naszej tablicy będziemy nazywali *linią*. Niech m będzie najmniejszą liczbą, dla której istnieje linia złożona z liczb nie większych od m. Możemy zakładać, że tą linią jest pierwszy wiersz, a jego pierwszym wyrazem jest m.

Wykażemy najpierw, że w każdej kolumnie, począwszy od drugiej, istnieją takie dwa jej *kolejne* wyrazy a i b, że $a \leqslant m-1$ i $b \geqslant m+1$. Dla ustalenia uwagi weźmy drugą kolumnę. Jej pierwszy wyraz nie może być większy od $m-1$. Niech b będzie najwyżej położonym wyrazem drugiej kolumny, który jest większy od m (musi taki istnieć wobec definicji m). Wyraz położony nad b jest szukanym a.

W ten sposób otrzymaliśmy $n-1$ par liczb $a_2 < m < b_2, \ldots, a_n < m < b_n$. Największa spośród liczb b_i musi więc wynosić co najmniej $m+n-1$. W takim razie a_i oraz b_i są poszukiwanymi liczbami.

zadaniem trudnym. Nie powinno zatem dziwić, że najdokładniejsze oszacowania gęstości ciemnej materii pochodzą z zupełnie innego źródła. Jest nim mikrofalowe promieniowanie tła, uwolnione w procesie rekombinacji przed miliardami lat – w chwili, gdy wszechświat stał się nazbyt chłodny, by fotony mogły jonizować pierwotne atomy, ale wciąż jeszcze był w miarę jednorodny. Od tego czasu fotony owe przemierzają wszechświat w zasadzie bez zakłóceń, zwiększając jedynie swą długość fali w miarę rozszerzania się wszechświata, i z tego powodu stanowią bezcenne źródło wiedzy o wczesnych etapach jego rozwoju. Bardzo ważne jest przy tym, że mikrofalowe promieniowanie tła jest z bardzo dobrym przybliżeniem izotropowe (identyczne dochodzi ze wszystkich kierunków), jego widmo jest najdoskonalszą realizacją widma ciała doskonale czarnego, jaką kiedykolwiek znała fizyka, a drobne niejednorodności jego natężenia, na poziomie $1 : 100\,000$, mają bardzo ciekawe własności statystyczne.

Zanim przejdziemy do ich omówienia, musimy zastanowić się nad kilkoma kwestiami technicznymi związanymi z owymi kosmicznymi fluktuacjami. Po pierwsze, zaburzenia takie możemy „składać" z zaburzeń o kształcie sinusoidalnym – dla odpowiednio małych amplitud tych zaburzeń we wczesnym wszechświecie każde z nich będzie ewoluowało niezależnie od pozostałych. Po drugie, większa gęstość (i temperatura) materii jest związana z silniejszą grawitacją. Zgodnie z ogólną teorią względności fotony wyemitowane z miejsc gęstszych są bardziej energetyczne, ale muszą stracić więcej energii na pokonanie silniejszej grawitacji; szczegółowy rachunek pokazuje, że pierwszy z wymienionych efektów jest silniejszy. Różnice w natężeniu (i temperaturze) mikrofalowego promieniowania tła dochodzącego z różnych kierunków pozwalają zatem na określenie różnic gęstości obszarów wszechświata, z których fotony te zostały wyemitowane. Wreszcie, w „normalnie" rozszerzającym się wszechświecie maksymalny rozmiar obszaru powiązanego przyczynowo rośnie szybciej niż rozmiary sinusoidalnych zaburzeń rozciągane wskutek rozszerzania się wszechświata. Oznacza to, że dane sinusoidalne zaburzenie o określonej długości ma najpierw długość przekraczającą rozmiar obszaru powiązanego przyczynowo; skoro odległe części tego zaburzenia początkowo „nic o sobie nie wiedzą", to dopiero w pewnym momencie ewolucji wszechświata, odpowiadającym odwróceniu powyższej nierówności, zaburzenie takie może zacząć ewoluować.

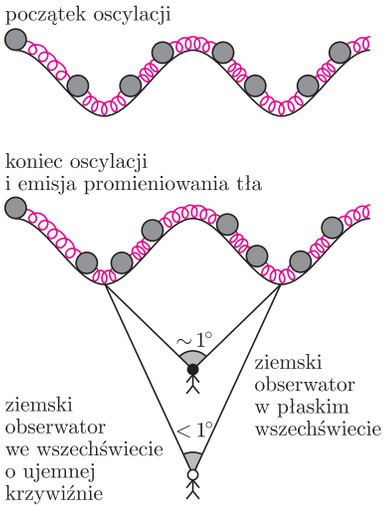


Rys. 1. Układ mechaniczny odpowiadający zaburzeniom kosmologicznym. Ciężkie kulki to materia barionowa, sprężynki to fotony, zaś „dołek", w którym się one znajdują, to „potencjał" grawitacyjny. Bariony dążą do skupiania się pod wpływem oddziaływań grawitacyjnych, czemu przeciwstawia się ciśnienie fotonów.

Pojedyncze zaburzenie sinusoidalne odpowiada zaburzeniu gęstości kilku składników: materii barionowej składającej się przede wszystkim z protonów (równoważące dodatni ładunek protonów elektrony mają około 2000 razy mniejszą masę i możemy je w bilansie masy pominąć), fotonów oraz ewentualnie ciemnej materii – a także odpowiadającego im zaburzenia grawitacyjnego. Ewolucję takiego układu możemy lepiej zrozumieć, korzystając z analogii zaproponowanej przez Wayne'a Hu z Uniwersytetu w Chicago – równania opisujące dynamikę każdego ze składników mają bowiem taką samą postać jak równania ruchu bardzo prostego układu fizycznego przedstawionego na rysunku 1. Pozostaje pytanie, co lub kto zapewnia warunki początkowe dla tych równań – czyli kształt zaburzeń na skalach przekraczających rozmiar obszarów przyczynowo powiązanych. Uchylanie się od odpowiedzi na to pytanie wydaje się mało ambitne intelektualnie, zwłaszcza że istnieje klasa teorii, które pozwalają podać pewien zakres przewidywań dla warunków początkowych. Są to teorie inflacji z wolnym toczeniem, zaproponowane ponad trzy dekady temu przez Andreia Lindego (notabene różne od zarzuconych obecnie z powodu niezgodności z doświadczeniem pionierskich koncepcji Alana Gutha). W teoriach tych pierwotne zaburzenia są odpowiednio rozciągniętymi wskutek przyspieszonego rozszerzania się bardzo wczesnego wszechświata fluktuacjami kwantowymi; kształt wszystkich pierwotnych zaburzeń opisywany jest prostą funkcją zależną od kilku stałych liczbowych.

Jedno zaburzenie ma szczególnie prostą, ale też ważną historię. Jego ewolucja zaczyna się w dobrze określonym momencie, gdy jego rozmiar zrównuje się z rozmiarem obszaru przyczynowo powiązanego. Od tej pory powinny zachodzić oscylacje gęstości barionów i fotonów – gdyby nie fakt, że po jednym półokresie takich oscylacji, w chwili odpowiadającej maksymalnemu ściśnięciu barionów w jednych miejscach zaburzenia i maksymalnemu rozrzedzeniu w drugich, doszło

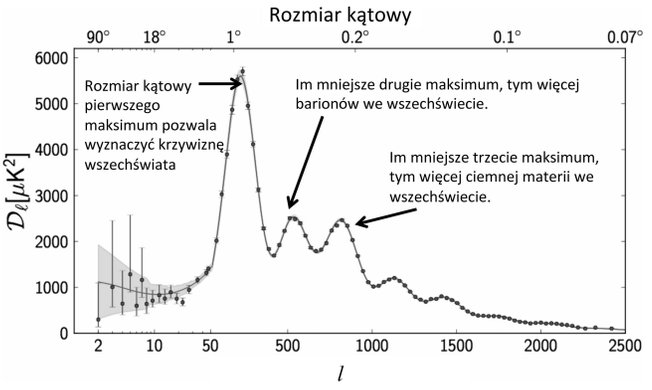
Teorie inflacji przewidują, że oprócz opisywanych tu korelacji zaburzeń temperatury mikrofalowego promieniowania tła istnieją także korelacje jego spolaryzowanych składowych. Są one wynikiem występowania tzw. fal grawitacyjnych. Choć omówienie tego zjawiska wykracza poza ramy tego artykułu, należy odnotować, że jego odkrycie dodatkowo wzmacniałoby przekonanie o zajściu inflacji. W marcu 2014 roku zespół BICEP2 poinformował o zaobserwowaniu takiego sygnału, ale, jak się okazało później, było to wynikiem błędnej identyfikacji spolaryzowanego promieniowania pochodzącego z dysku naszej Galaktyki.



Rys. 2. Ewolucja zaburzenia, dla którego rekombinacja zachodzi po półokresie oscylacji gęstości. Zaburzenia o określonym rozmiarze możemy zobaczyć w różnych odległościach kątowych w zależności od krzywizny wszechświata określającej tor fotonów w przestrzeni.

do rekombinacji i wyemitowania fotonów mikrofalowego promieniowania tła. W efekcie dla pewnego określonego rozmiaru zaburzenia powinno się dać zaobserwować w mikrofalowym promieniowaniu tła wyraźną korelację – miejsca cieplejsze powinny być odseparowane o określony kąt od innych cieplejszych miejsc (a zimniejsze od zimniejszych). Kształt ramion tego kąta odpowiada biegowi promieni świetlnych w rozszerzającym się wszechświecie – okazuje się, że pozwala to na bardzo dokładne oszacowanie, czy wszechświat odpowiada trójwymiarowej (płaskiej) przestrzeni euklidesowej, czy też należy go modelować jako przestrzeń trójwymiarową o dodatniej lub ujemnej krzywiźnie.

Równie istotne są zaburzenia, dla których rekombinacja zachodzi po jednym i po półtora okresu oscylacji. W przypadku tych pierwszych, im więcej barionów, tym silniejszemu ściśnięciu i słabszemu późniejszemu rozrzedzeniu one ulegają, co daje się zaobserwować jako zmniejszenia antykorelacji zaburzeń na skalach o połowę mniejszych niż dyskutowane poprzednio. Te drugie odpowiadają zaś ponownemu maksymalnemu ściśnięciu barionów, którego skuteczność zależy od tego, czy „potencjał" grawitacyjny ulegnie zanikowi od czasu pierwszego ściśnięcia (tak byłoby, gdyby rozrzedzone pół okresu wcześniej bariony i fotony stanowiły główne źródło grawitacji), czy też nie (jeśli źródłem grawitacji jest przede wszystkim ciemna materia, nieoddziałująca z fotonami, a więc nieoscylująca); zanik „potencjału" grawitacyjnego usuwa przeszkody w rozrzedzaniu się barionów i pozwala na zwiększenie amplitudy omawianych oscylacji w porównaniu z poprzednimi.



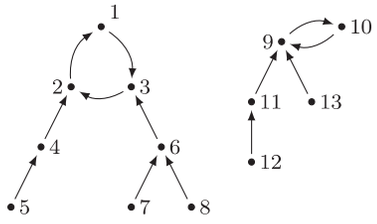
Rys. 3. Korelacje i antykorelacje zaburzeń temperatury mikrofalowego promieniowania tła obserwowane przez satelitę Planck. Źródło: ESA.

Nie samym jednak mikrofalowym promieniowaniem tła żyją kosmologowie. Wspomniane wyżej pierwotne zaburzenia gęstości stanowią nie tylko źródło jego nieizotropowości, ale także zarodzie, z których wskutek przyciągania grawitacyjnego powstają miliardy lat później galaktyki i gromady galaktyk. Oznacza to, że rozkład takich struktur we wszechświecie powinien być ściśle związany z własnościami mikrofalowego promieniowania tła. Symulacje formowania się struktur kosmicznych prowadzone przy użyciu superkomputerów wskazują, że tak właśnie jest i, co więcej, że proces ten jest czuły na szczegóły ewolucji wszechświata takie jak to, czy wszechświat rozszerza się z przyspieszeniem, czy z opóźnieniem, albo jaki procent materii we wszechświecie stanowi ciemna materia.

Powyższe rozważania pozwalają, moim zdaniem, na wyciągnięcie trzech ostrożnie optymistycznych wniosków. Po pierwsze, podobnie jak w innych spotykanych w fizyce sytuacjach (np. w doświadczeniach przy akceleratorze LHC) nie sposób oddzielić aspektów teoretycznych i empirycznych badań wszechświata (dane obserwacyjne pozwalają na testowanie teorii, ale muszą być zarazem interpretowane w ramach tej teorii, a nie w sposób od niej niezależny). Nie jest to jednak sytuacja beznadziejna, gdyż sieć wzajemnych powiązań między różnymi aspektami ewolucji wszechświata jest tak gęsta, że niesprzeczność schematu teoretycznego z danymi obserwacyjnymi stanowi ważny argument za jego poprawnością. Po drugie, schemat ten jest wyjątkowo oszczędny w proponowaniu nowych bytów – potrzebuje zaledwie jednego rodzaju w miarę stabilnych cząstek tworzących ciemną materię, jednego pola odpowiedzialnego za inflację i zadawane przez nią warunki początkowe dla zaburzeń gęstości oraz jednej stałej (kosmologicznej). Można porównać te propozycje z żądaniami fizyki cząstek elementarnych sprzed półwiecza (nowe pole Higgsa pozwalające na tzw. spontaniczne naruszenie symetrii cechowania, nowe cząstki – kwarki – budujące hadrony), które doprowadziły do rewolucji w postrzeganiu fundamentalnych składników materii i wysypu Nagród Nobla. Po trzecie zaś, mimo nieustających wysiłków fizyków teoretycznych, jak dotąd nie pojawiła się żadna inna idea, która zapewniałaby przy użyciu podobnie skromnych środków spójny schemat teoretyczny pozwalający na interpretację i przewidywanie równie szerokiej klasy zjawisk.

Informatyczny kącik olimpijski (89): Darmowe rozmowy

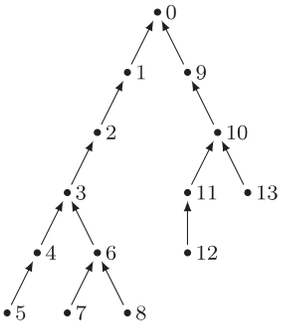
W tym miesiącu rozwiążemy zadanie *Darmowe rozmowy* z Obozu Naukowo-Treningowego im. Antoniego Kreczmara w roku 2011. Firma telekomunikacyjna, chcąc poinformować swoich klientów o nowej promocji, zleciła jednemu ze swoich pracowników, aby osobiście zadzwonił on do niektórych klientów. Klientów jest n, a ponadto każdy z nich może zadzwonić do jednej ustalonej osoby za darmo. Pracownik wychodzi z założenia, że promocja jest tak świetna, że każdy klient, który się o niej dowie, będzie chciał się podzielić tą wiedzą z kimś innym, ale że ludzie są z natury oszczędni, poinformuje on tylko tę osobę, do której może zadzwonić bezpłatnie. Pracownik ma czas wykonać k telefonów do klientów. Należy wyznaczyć, do których powinien zadzwonić, aby zmaksymalizować liczbę osób, które dowiedzą się o promocji.



Rys. 1. Przykładowy graf o $n = 13$ wierzchołkach. Dla $k = 2$ najbardziej opłaca się zadzwonić do klienta 12 (co spowoduje, że o promocji dowiedzą się klienci 12, 11, 9 i 10) oraz jednego z klientów 5, 7 lub 8 (co poinformuje dodatkowych pięciu klientów).

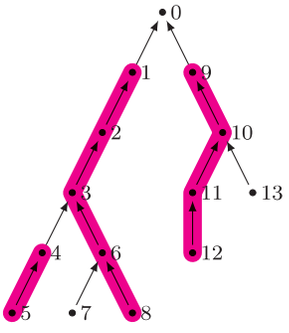
Zbiór klientów możemy przedstawić jako graf skierowany o n wierzchołkach, w którym istnieje krawędź od wierzchołka i do wierzchołka j, jeśli klient i może za darmo zadzwonić do klienta j (rys. 1). Zatem zadzwonienie do klienta i spowoduje, że klienci odpowiadający wszystkim wierzchołkom osiągalnym z wierzchołka i dowiedzą się o promocji.

Graf skierowany, w którym z każdego wierzchołka wychodzi dokładnie jedna krawędź, ma dość specyficzną strukturę: każda jego spójna składowa jest cyklem z podoczepianymi drzewami. W przypadku naszego zadania możemy tę strukturę jeszcze uprościć, konstruując skierowane drzewo o tej własności, że z optymalnego rozwiązania dla drzewa łatwo odtworzymy optymalne rozwiązanie dla pierwotnego grafu. Mianowicie każdą składową zastępujemy pojedynczą ścieżką o tej samej długości co cykl w tej składowej, a do końca tej ścieżki podczepiamy wszystkie drzewa ze składowej. Na końcu zaś wszystkie ścieżki podczepiamy do nowego wierzchołka 0 (rys. 2). Pokazanie odpowiedniości między rozwiązaniami dla drzewa i pierwotnego grafu pozostawimy jako nietrudne ćwiczenie dla Czytelników.



Rys. 2. Drzewo skonstruowane na podstawie grafu z rysunku 1.

W tym momencie nasze zadanie jest następujące: chcemy wybrać k wierzchołków w skierowanym drzewie tak, aby liczba wierzchołków z nich osiągalnych była jak największa. Na początek poczyńmy dwie oczywiste obserwacje: wybierając wierzchołki, wystarczy ograniczyć się do liści w drzewie (w szczególności bez straty ogólności możemy założyć, że k jest nie większe niż liczba liści). Ponadto w przypadku $k = 1$ należy wybrać ten z liści, który leży w najdalszej odległości od korzenia drzewa. Okazuje się, że również dalej działa podejście zachłanne: kolejne liście opłaca się wybierać tak, aby leżały jak najdalej od zbioru wierzchołków już zaznaczonych (rys. 3).



Rys. 3. Kolejne liście znajdowane przez algorytm zachłanny to, na przykład, 8, 12, 5, 7 i 13. Kolorem zaznaczono wierzchołki osiągalne dodawane w kolejnych fazach algorytmu.

Pomysł ten możemy zaimplementować następująco: wykonujemy k faz algorytmu. Zakładamy, że na początku i-tej fazy mamy zaznaczony w drzewie zbiór S_i wierzchołków osiągalnych z liści wybranych w poprzednich fazach. W fazie obliczamy odległości pozostałych wierzchołków do zbioru S_i, wybieramy liść o największej odległości i zaznaczamy wszystkie wierzchołki z niego osiągalne. Pojedynczą fazę wykonujemy w czasie $O(n)$, zatem cały algorytm działa w czasie $O(kn)$.

Rozwiązanie to można przyspieszyć. Wierzchołki dodawane w kolejnych fazach tworzą ścieżki. Każda krawędź takiej ścieżki wchodząca do danego wierzchołka wychodzi z jednego z tych jego synów, których poddrzewa mają największą głębokość. Możemy zatem obliczyć wszystkie te ścieżki w czasie $O(n)$, przeglądając drzewo od liści w górę, dla każdego wierzchołka pamiętając głębokość jego poddrzewa. Następnie wybieramy k najdłuższych ścieżek, sortując ich długości przez zliczanie.

A jak udowodnić poprawność rozwiązania zachłannego? Niech R_j będzie zbiorem wierzchołków, które leżą w odległości j od najbliższego liścia. W szczególności R_0 jest zbiorem liści i z tego zbioru chcemy zaznaczyć pewne k wierzchołków. Poruszając się w górę drzewa z tych wierzchołków, zaznaczymy ich rodziców, którzy znajdują się w zbiorze R_1, przy czym opłaca nam się tak wybrać liście, aby zbiór tych rodziców był jak największy. Oczywiście, będzie on miał rozmiar co najwyżej $\min(|R_1|, k)$. W ogólności, ze zbioru R_j zaznaczymy co najwyżej $\min(|R_j|, k)$ wierzchołków. Załóżmy, że zbiór S_i jest optymalnym rozwiązaniem dla $i = k$, to znaczy, że dla każdego j w zbiorze R_j zaznaczamy dokładnie $\min(|R_j|, i)$ wierzchołków. Jeśli liść wybrany w i-tej fazie algorytmu leży w odległości ℓ, to znaczy, że z każdego ze zbiorów $R_0, \ldots, R_{\ell-1}$ zaznaczymy po jednym wierzchołku, natomiast wszystkie wierzchołki w zbiorach $R_\ell, R_{\ell+1}, \ldots$ są już zaznaczone (więc ich rozmiary są nie większe niż i). Wynika z tego, że zbiór S_{i+1} jest też optymalny, bo dla każdego j w zbiorze R_j zaznaczymy $\min(|R_j|, i + 1)$ wierzchołków.

Co ciekawe, powyższy dowód daje nam prostsze rozwiązanie w przypadku, gdy interesuje nas tylko maksymalna *liczba* klientów, którzy dowiedzą się o promocji. Wystarczy bowiem w czasie $O(n)$ wyznaczyć rozmiary zbiorów R_j.

Tomasz IDZIASZEK

Klub 44

Liga zadaniowa Wydziału Matematyki, Informatyki i Mechaniki, Wydziału Fizyki Uniwersytetu Warszawskiego i Redakcji *Delty*

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 przesyłać w oddzielnych kopertach, umieszczając na kopercie dopisek: **Klub 44 M** lub **Klub 44 F**. Oceniamy zadania w skali od 0 do 1 z dokładnością do 0,1. Ocenę mnożymy 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`

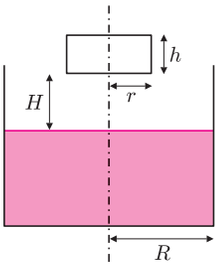
Termin nadsyłania rozwiązań: 31 III 2016

Zadania z fizyki nr 610, 611

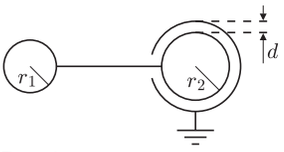
Redaguje Elżbieta ZAWISTOWSKA

610. Mokre koło o promieniu R obraca się ruchem jednostajnym w płaszczyźnie pionowej wokół nieruchomej osi. Prędkość punktów na obwodzie koła wynosi v. Znaleźć granicę obszaru suchego.

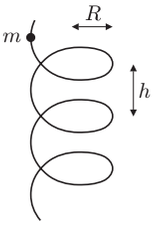
611. Do naczynia w kształcie walca o promieniu R, częściowo wypełnionego cieczą, wpada klocek w kształcie walca o promieniu r i wysokości h (rys. 1). W chwili początkowej odległość dolnej powierzchni klocka od powierzchni cieczy wynosi H, a jego prędkość jest równa zeru. Ile ciepła wydzieli się do chwili, gdy ustanie ruch klocka i cieczy? Gęstość klocka wynosi ρ, gęstość cieczy $\rho_c > \rho$.



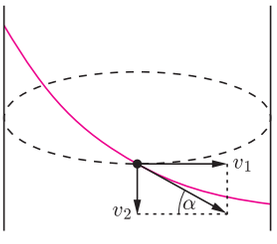
Rys. 1



Rys. 2



Rys. 3



Rys. 4

Czołówka ligi zadaniowej **Klub 44 F** po uwzględnieniu ocen rozwiązań zadań 594 ($WT = 2{,}65$), 595 ($WT = 4{,}00$), 596 ($WT = 2{,}20$), 597 ($WT = 3{,}25$), 598 ($WT = 3{,}82$), 599 ($WT = 3{,}40$), 600 ($WT = 4{,}00$) i 601 ($WT = 3{,}25$) z numerów 3–6/2015

Tomasz Rudny	Warszawa	37,68
Tomasz Wietecha	Tarnów	29,64
Marian Łupieżowiec	Gliwice	28,11
Jacek Konieczny	Poznań	27,92
Michał Koźlik	Gliwice	26,32
Ryszard Woźniak	Kraków	22,51

Rozwiązania zadań z numeru 9/2015

Przypominamy treść zadań:

602. Dwie przewodzące kule o promieniach r_1 i r_2, połączone przewodzącym drutem, znajdują się w dużej odległości od siebie. Kula o promieniu r_2 otoczona jest uziemioną sferą przewodzącą z małym otworkiem (rys. 2). Odległość sfery od kuli wynosi d i jest dużo mniejsza od promienia kuli. Kule naładowano ładunkiem Q. Wyznacz rozmieszczenie ładunku na kulach.

603. Po ustawionej pionowo sztywnej spirali zsuwa się z zerową prędkością początkową mały koralik o masie m. Promień spirali wynosi R, skok spirali (odległość między sąsiednimi zwojami) wynosi h (rys. 3). Znaleźć wartość przyspieszenia koralika na końcu n-tego zwoju. Tarcie zaniedbać.

602. Oznaczmy ładunki na kulach o promieniach r_1 i r_2 odpowiednio przez q_1 i q_2. Zachodzi związek

$$Q = q_1 + q_2. \tag{1}$$

Kule połączone drutem tworzą jeden przewodnik, więc ich potencjały są jednakowe:

$$\frac{q_1}{r_1} = \frac{q_2}{r_2} + \frac{q}{r_2 + d}, \tag{2}$$

gdzie q jest ładunkiem indukowanym na uziemionej sferze. Potencjał sfery jest równy zeru:

$$\frac{q}{r_2 + d} + \frac{q_2}{r_2 + d} = 0.$$

Stąd mamy $q = -q_2$. Podstawiając to do (2) i uwzględniając warunek $d \ll r_2$, otrzymujemy związek:

$$\frac{q_1}{r_1} = \frac{q_2}{r_2} - \frac{q_2}{r_2 + d}.$$

Uwzględniając (1), otrzymujemy:

$$q_1 = \frac{Q r_1 d}{r_2 d + r_2^2}.$$

603. Ruch koralika jest złożeniem ruchu po okręgu o promieniu R i ruchu w kierunku pionowym. Prędkość koralika v w danej chwili można rozłożyć na składowe – poziomą $v_1 = v\cos\alpha$ i pionową $v_2 = v\sin\alpha$, gdzie α jest kątem, jaki tworzy z poziomem styczna do spirali (rys. 4). Przyspieszenie koralika jest sumą wektorową składowej prostopadłej do toru, związanej z ruchem po okręgu, która wynosi

$$a_n = \frac{v^2\cos^2\alpha}{R},$$

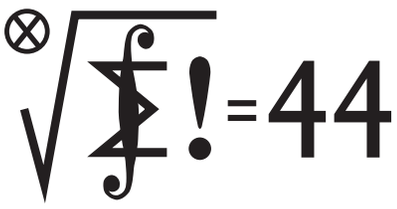
oraz składowej stycznej do toru a_s. Składową styczną można znaleźć, rozwijając myślowo zwój spirali na płaszczyźnie. Otrzymamy wtedy równię pochyłą nachyloną do poziomu pod kątem α, o podstawie $2\pi R$ i wysokości h. Składowa styczna do toru wynosi

$$a_s = \mathrm{g}\sin\alpha = \frac{gh}{\sqrt{h^2 + 4\pi R^2}}.$$

Prędkość koralika po przebyciu n zwojów otrzymujemy, korzystając z zasady energii mechanicznej: $v^2 = 2ghn$. Szukana wartość przyspieszenia jest równa

$$a = \sqrt{a_n^2 + a_s^2} = \frac{gh\sqrt{h^2 + 4\pi^2R^2 + 64\pi^2n^2R^2}}{h^2 + 4\pi^2R^2}.$$

Klub 44



Termin nadsyłania rozwiązań: 31 III 2016

Czołówka ligi zadaniowej **Klub 44 M** po uwzględnieniu ocen rozwiązań zadań 703 ($WT = 3{,}00$) i 704 ($WT = 1{,}05$) z numeru 6/2015

Paweł Najman	Kraków	42,85
Marek Spychała	Warszawa	42,75
Grzegorz Karpowicz	Wrocław	38,86
Jędrzej Garnek	Poznań	37,64
Krzysztof Maziarz	Kraków	35,37
Jerzy Cisło	Wrocław	35,00
Janusz Fiett	Warszawa	34,33
Franciszek S. Sikorski	Warszawa	33,77

Zadania z matematyki nr 713, 714

Redaguje Marcin E. KUCZMA

713. Dany jest czworokąt wypukły $ABCD$, w którym boki AB i CD nie są równoległe. Rozważamy okrąg, przechodzący przez punkty A i B, styczny do prostej CD w punkcie P oraz okrąg, przechodzący przez punkty C i D, styczny do prostej AB w punkcie Q. Zakładamy, że punkty P i Q leżą na odcinkach CD i AB oraz że wspólna cięciwa tych okręgów przechodzi przez środek odcinka PQ. Udowodnić, że proste AD i BC są równoległe.

714. Niech $d(m)$ oznacza liczbę dodatnich dzielników liczby naturalnej $m \geqslant 1$

(a) Wykazać, że istnieje nieskończenie wiele par różnych liczb naturalnych m, n, spełniających równanie $d(m)/m = d(n)/n$.
(b) Czy istnieje para liczb naturalnych względnie pierwszych $m, n > 1$, spełniających równanie $d(m)/m = d(n)/n$?

Zadanie 714 zaproponował pan Witold Bednarek z Łodzi.

Rozwiązania zadań z numeru 9/2015

Przypominamy treść zadań:

705. Niech A_0 będzie ustalonym wierzchołkiem $(n+1)$-kąta foremnego. Numerujemy pozostałe wierzchołki $A_1, \ldots, A_n$ w dowolnej kolejności. Każdemu bokowi A_iA_j przyporządkowujemy liczbę $|i-j|$. Niech S będzie sumą $n+1$ liczb, przyporządkowanych wszystkim bokom. Dla zadanej liczby naturalnej n:

(a) Obliczyć najmniejszą osiągalną wartość sumy S.
(b) Wyjaśnić, ile jest sposobów ponumerowania n wierzchołków (poza A_0), przy których S osiąga ową minimalną wartość.

706. Wyznaczyć wszystkie liczby naturalne $n \geqslant 1$, dla których istnieje wielomian W stopnia n, o współczynnikach całkowitych, ze współczynnikiem wiodącym równym 1, i taki, że równanie $W(x)^2 = 1$ ma $2n$ pierwiastków całkowitych (niekoniecznie różnych).

705. (a) Pewien wierzchołek otrzymuje nazwę A_n. Idąc od A_0 do A_n wzdłuż brzegu wielokąta, w wybranym kierunku, mijamy kolejno wierzchołki $A_{i_1}, \ldots, A_{i_k}$. Przechodzimy przez A_n, dalej mijamy wierzchołki $A_{j_1}, \ldots, A_{j_m}$, i wracamy do A_0. Numery $i_1, \ldots, i_k$ oraz $j_1, \ldots, j_m$ tworzą permutację zbioru $\{1, \ldots, n-1\}$. Liczby, przyporządkowane wszystkim bokom, sumują się do wartości

$$S = \big(|0-i_1| + |i_1-i_2| + \ldots + |i_{k-1}-i_k| + |i_k-n|\big) + \big(|n-j_1| + |j_1-j_2| + \ldots + |j_{m-1}-j_m| + |j_m-0|\big) \geqslant n+n = 2n.$$

Równość w tym szacowaniu jest osiągalna; ma ona miejsce wtedy i tylko wtedy, gdy $i_1 < \ldots < i_k$ oraz $j_1 > \ldots > j_m$. Zatem $2n$ to szukane minimum.

(b) Zbiór $I = \{i_1, \ldots, i_k\}$ może być dowolnym podzbiorem zbioru $\{1, \ldots, n-1\}$ (również pustym, wtedy pierwszy składnik rozpisanej sumy S ma postać $|0-n|$). Zauważmy teraz, że już sam *wybór* zbioru I determinuje ponumerowanie, realizujące równość $S = 2n$; liczby ze zbioru I, uporządkowane rosnąco, trzeba przypisać kolejnym wierzchołkom (przy obieganiu wielokąta od A_0 w wybranym kierunku), następny wierzchołek trzeba nazwać A_n, a dalszym wierzchołkom dać niewykorzystane numery, uporządkowane malejąco.

Konkluzja: jest tyle możliwości optymalnego ponumerowania n wierzchołków, ile podzbiorów ma zbiór $\{1, \ldots, n-1\}$, to znaczy 2^{n-1}.

706. Przykładami wielomianów, o jakich mowa, stopni $n = 1$ oraz $n = 2$, mogą być $W(x) = x$ oraz $W(x) = x^2 + x - 1$. Wykażemy, że nie istnieje wielomian o podanych własnościach, stopnia $n \geqslant 3$.

Przypuśćmy, że W jest takim wielomianem. Zestaw wszystkich $2n$ pierwiastków wielomianu $W(x)^2 - 1$ rozdzielamy na ciąg $\alpha_1 \leqslant \ldots \leqslant \alpha_n$ pierwiastków wielomianu $W(x) - 1$ oraz ciąg $\beta_1 \leqslant \ldots \leqslant \beta_n$ pierwiastków wielomianu $W(x) + 1$. Wówczas

$$(1) \qquad \prod_{i=1}^{n}(x-\alpha_i) - \prod_{i=1}^{n}(x-\beta_i) = \big(W(x)-1\big) - \big(W(x)+1\big) = -2.$$

Podstawiając $x = \beta_n$ mamy $\prod_{i=1}^{n}(\beta_n - \alpha_i) = -2$, skąd wynika, że najmniejszy z czynników tego iloczynu jest liczbą ujemną: $\beta_n - \alpha_n < 0$. Wobec tego α_n jest liczbą większą od wszystkich β_i. Widzimy ponadto, że liczby α_i nie mogą być wszystkie równe, bo liczba -2 nie jest iloczynem n równych liczb całkowitych. Zatem $\alpha_1 < \alpha_n$.

Podstawiając z kolei w równaniu (1) $x = \alpha_n$ dostajemy $\prod_{i=1}^{n}(\alpha_n - \beta_i) = 2$. Jest to iloczyn dodatnich liczb całkowitych; największa musi być dwójką, a pozostałe jedynkami – to znaczy,

$$(2) \qquad \beta_1 = \alpha_n - 2; \qquad \beta_i = \alpha_n - 1 \quad \text{dla } i = 2, \ldots, n.$$

Wracamy do równania (1) i podstawiamy $x = \alpha_1$; otrzymujemy równość $\prod_{i=1}^{n}(\alpha_1 - \beta_i) = 2$. Zgodnie ze wzorami (2), przepisujemy ją w postaci

$$(3) \qquad (\alpha_1 - \alpha_n + 2)(\alpha_1 - \alpha_n + 1)^{n-1} = 2.$$

Skoro $n - 1 \geqslant 2$, czynnik $(\alpha_1 - \alpha_n + 1)$ musi być równy ± 1. Gdyby był równy 1, znaczyłoby to, że $\alpha_1 = \alpha_n$, wbrew wcześniejszemu spostrzeżeniu. Gdyby był równy -1, w pierwszym nawiasie wzoru (3) mielibyśmy 0. Równość (3) doprowadziła do sprzeczności.

Wielomiany o postulowanych własnościach istnieją więc tylko dla $n = 1$ i $n = 2$. (Nietrudno znaleźć ich ogólną postać – zostawiamy to jako ćwiczenie).

Prosto z nieba: Ekstremalne życie

Czy fakt obecności przeróżnych form życia na Ziemi jest czymś wyjątkowym, czy też wręcz przeciwnie – zjawiskiem powszechnym, o którym nie wiemy jedynie dlatego, że dopiero zaczynamy podbój przestrzeni kosmicznej? Możliwość występowania życia na innych planetach, a także kometach, asteroidach, w atmosferach gwiazd, obłokach międzygwiazdowych, a nawet we wczesnej fazie istnienia wszechświata (jako, że w czasie między Wielkim Wybuchem a obecnie chłodnymi i pustymi przestrzeniami międzygalaktycznymi trwała przez pewien czas chwila, w której temperatura była wszędzie bliska 300 K...) rozpala i tak już bujną wyobraźnię astrobiologów.

Zejdźmy jednak na chwilę z nieba na Ziemię, by zastanowić się, czy badając warunki występujące w jej najbardziej nieprzyjaznych zakątkach, możemy się czegoś nauczyć o potencjalnym życiu poza Ziemią. W głębinach oceanów pod ogromnym ciśnieniem lub pod polarnymi lodowcami znajdziemy ekstremalnie wytrzymałe bakterie, które ewoluowały przez miliony lat, radząc sobie świetnie w tych warunkach.

Niedawno odkryto m.in. nieznane wcześniej szczepy bakterii żyjące w Jeziorze Asfaltowym (jeziorze gorącego, płynnego asfaltu) na wyspie Trynidad w pobliżu miasta La Brea.

Jeśli chodzi o zwierzęta, sztandarowym przykładem ekstremalnego twardziela jest ośmionogi niesporczak (*Tardigrada*), pospolicie występujący miniorganizm o rozmiarze około 1 mm, który potrafi przeżyć w otwartej przestrzeni kosmicznej bez wody i pożywienia, w ciśnieniach przekraczających 5000 atmosfer, we wrzącej wodzie i pod wpływem zabójczego dla innych organizmów promieniowania jonizującego.

Mając wybór, niesporczaki preferują zazwyczaj miejsca dużo mniej ekstremalne: różnego rodzaju mchy i porosty.

Astrobiolodzy teoretyzują, że w warunkach podobnych do marsjańskich (pustyni zimniejszej i bardziej suchej od Atakamy w Chile) potencjalnie istniejące tam wielokomórkowe życie byłoby możliwe w przypadku, gdyby niezbędną do życia wodę (wypełniającą przestrzenie międzykomórkowe) częściowo zastępował nadtlenek wodoru (H_2O_2). Naturalnie przeciwdziała on zamarzaniu i ma działanie higroskopijne (przyciąga wodę), co mogłoby być wykorzystywane w czasie marsjańskich nocy do pozyskiwania wody z atmosfery.

W jeszcze niższych temperaturach i z dala od Słońca życie na księżycach planet gazowych, np. na Tytanie, musiałoby korzystać ze związków innych niż woda. Tytan jest pokryty oceanami ciekłego metanu. Hipotetyczne metanowe organizmy pozyskiwałyby energię z łączenia wodoru z atmosferycznym acetylenem (C_2H_2) w produkcji metanu. Niskie temperatury sprawiałyby także, że tempo życia oraz ewolucja organizmów przebiegałaby w skali czasowej dużo dłuższej niż na Ziemi. O tym, czy jest tak w istocie, przekonamy się, oczywiście, dopiero po wysłaniu odpowiedniej sondy, np. projektowanej przez NASA „łodzi podwodnej", która ma odkryć tajemnice największego metanowego zbiornika na Tytanie, Jeziora Krakena.

Michał BEJGER

Niebo w styczniu

Już 2 stycznia Ziemia znajdzie się w peryhelium, czyli w tym punkcie swojej orbity, w którym jest najbliżej Słońca. Od naszej macierzystej gwiazdy będzie nas dzielić wtedy około 147 milionów kilometrów. Dla porównania w najodleglejszym punkcie orbity Ziemia znajduje się od niej około 152 milionów kilometrów. Błędne jest przekonanie, że w trakcie lata Ziemia jest najbliżej Słońca, a w zimie najdalej. Sytuacja jest dokładnie odwrotna, natomiast na pory roku i ich zmiany wpływa nie orbita naszej planety, a nachylenie osi dobowej rotacji Ziemi do płaszczyzny jej ruchu orbitalnego wokół Słońca. Oś ta tworzy z płaszczyzną orbity Ziemi (płaszczyzną ekliptyki) kąt około 66,5 stopnia. W trakcie ruchu rocznego po orbicie Ziemia jest najsilniej nachylona półkulą północną w kierunku Słońca pod koniec czerwca, czyli w trakcie naszego lata. Natomiast w czasie zimy panującej na terenach Azji i Ameryki Północnej oraz Europy promienie Słońca padają bardziej pionowo na półkulę południową, dlatego właśnie wtedy lato panuje na terenach Australii, Afryki i Ameryki Południowej.

Pozostając w temacie zmian pór roku, warto spojrzeć na niebo nad ranem 20 stycznia, gdy gwiazda Aldebaran (α Tauri) znajdzie się w odległości 0,5° w kierunku południowym od Księżyca i będzie można ją podziwiać nad zachodnim niebem. Ten najjaśniejszy ($0{,}85^m$) obiekt konstelacji Byka jest układem podwójnym odległym od nas o 66 lat świetlnych. Aldebaran razem z trzema innymi gwiazdami: Antaresem, Regulusem i Formalhaut został w XVIII wieku nazwany „królewskimi gwiazdami Persji" przez francuskiego pisarza Charlesa Françoisa Dupuisa, badającego perskie astronomiczne odkrycia z 3000–2500 roku p.n.e. Na ich podstawie Dupuis stwierdził, że Aldebaran i Antares wyznaczają wiosenne i jesienne przesilenia, a Regulus i Formalhaut letnie i zimowe równonoce, gdyż właśnie te gwiazdy dzielą nocne niebo na cztery równe części odpowiadające kolejnym porom roku. Antares (α Scorpii) to najjaśniejszy ($1{,}05^m$) obiekt gwiazdozbioru Skorpiona, a 20 stycznia nad ranem będzie można znaleźć go 6° w kierunku południowo-zachodnim od Saturna. Trzecią z „królewskich gwiazd Persji", najjaśniejszego z gwiazdozbioru Lwa Regulusa ($1{,}35^m$), można obserwować bez trudu całą noc. Fomalhaut, będąca najjaśniejszym obiektem gwiazdozbioru Ryb Południowych nie jest obecnie dostępna do obserwacji.

W trakcie styczniowych obserwacji warto pamiętać o komecie C/2013 US10 (Catalina), wspomnianej w grudniowym numerze *Delty*. Obecnie prognozowana jasność komety może przekroczyć nawet $4{,}9^m$, co powoduje, iż Catalina będzie widoczna gołym okiem, stanowić też będzie doskonały cel dla miłośników astrofotografii. Na początku stycznia kometa będzie znajdować się na tle gwiazdozbioru Wolarza, by stopniowo przesuwać się wzdłuż konstelacji Psy Gończe i Wielkiej Niedźwiedzicy, a na koniec stycznia znaleźć się na obszarze Smoka. Dokładne położenia można znaleźć w Internecie, na stronie Heavens Above. By najlepiej zaplanować obserwacje, warto pamiętać, że nów Księżyca w tym miesiącu wypada 10, natomiast pełnia 24 stycznia.

Karolina BĄKOWSKA

Z armaty do muchy

Joanna JASZUŃSKA

Poniższe zadania łączy to, że do rozwiązania każdego z nich można użyć pewnego Bardzo Znanego Twierdzenia, udowodnionego całkiem niedawno. Oczywiście to, że *można* strzelać z armaty do muchy nie oznacza, że zawsze *trzeba*...

n i k wszędzie oznaczają dodatnie liczby całkowite.

1. Udowodnij, że dla $n > 2$ liczba $\sqrt[n]{2}$ jest niewymierna.

2. Wykaż, że 56 nie jest trzecią potęgą liczby naturalnej.

3. W dwóch urnach jest po k kul, każda z kul jest biała lub czarna. Z każdej z urn n-krotnie losujemy kulę ze zwracaniem. Dla jakich wartości n, k i dla jakiego układu kolorów kul prawdopodobieństwo wylosowania samych białych kul z pierwszej urny jest równe prawdopodobieństwu wylosowania z drugiej urny wszystkich kul jednego koloru?

4. Znajdź wszystkie trójki dodatnich liczb całkowitych x, y, z, dla których $xy(x^2 + y^2) = 2z^4$.

5. Znajdź wszystkie pary liczb całkowitych x, y, dla których $x^3 - 6y^2 = 2$.

6. Czy istnieje wielomian o współczynnikach całkowitych, który nie jest różnowartościowy na zbiorze liczb rzeczywistych, ale jest różnowartościowy na zbiorze liczb wymiernych?

7. Niech

$$f(x) = \frac{3987}{3987x+1} + \frac{4365}{4365x+1} + \frac{4472}{-4472x+1},$$

a $f^{(k)}$ oznacza k-tą pochodną f. Czy $f^{(11)}(0) = 0$?

Rozwiązania

Dowód powstał dopiero pod koniec XX w. Jest zbyt długi i skomplikowany, by zmieścić się na tym marginesie.

Słynne *Wielkie Twierdzenie Fermata* (*WTwF*) z XVII w. głosi, że *dla $n > 2$ równanie $x^n + y^n = z^n$ nie ma rozwiązań w dodatnich liczbach całkowitych* x, y, z. Łatwo je uogólnić dla liczb wymiernych $x, y, z \neq 0$; proszę spróbować!

Więcej o WTwF znaleźć można w tym numerze *Delty* na stronach 4–7.

R1. Załóżmy, że $\sqrt[n]{2} = p/q$, gdzie $0 < p, q \in \mathbb{N}$. Wtedy $2 = p^n/q^n$, zatem $2q^n = p^n$, czyli $q^n + q^n = p^n$, sprzecznie z WTwF. □

R2. Gdyby $56 = n^3$, to $n^3 = 56 = 64 - 8 = 4^3 - 2^3$, czyli $n^3 + 2^3 = 4^3$, sprzecznie z WTwF. □

R3. Niech b_1 i b_2 oznaczają liczby białych kul odpowiednio w pierwszej i drugiej urnie. Prawdopodobieństwo, że z pierwszej urny n-krotnie wylosowano białą kulę równe jest $(b_1/k)^n$. Podobnie wyznaczamy odpowiednie prawdopodobieństwa dla drugiej urny i równość z treści zadania przybiera postać $(b_1/k)^n = (b_2/k)^n + ((k - b_2)/k)^n$, czyli $b_1^n = b_2^n + (k - b_2)^n$.

Jeśli $n > 2$, to z WTwF musi być $b_1 = b_2$ i $k - b_2 = 0$ lub $b_1 = k - b_2$ i $b_2 = 0$. To prowadzi do rozwiązań $b_1 = b_2 = k$ lub $b_1 = k$ i $b_2 = 0$.

Jeśli $n = 2$, równanie spełniają wszystkie trójki pitagorejskie i dla każdej z nich są dwa rozwiązania.

Jeśli $n = 1$, to prawdopodobieństwo, że wszystkie kule wylosowane z drugiej urny są jednego koloru jest równe 1, więc rozwiązaniem jest $b_1 = k$. □

R4. Dany warunek równoważny jest równości $(x + y)^4 = (x - y)^4 + (2z)^4$. Na mocy WTwF, skoro $x, y, z > 0$, oznacza to, że $x - y = 0$, czyli $x = y$. Wówczas $(2x)^4 = (2z)^4$ i w rezultacie $x = y = z$. □

R5. Przekształcając dane równanie, uzyskujemy $x^3 = 6y^2 + 2 = (1 + y)^3 + (1 - y)^3$. Na mocy WTwF musi być $x = 0$, $1 + y = 0$ lub $1 - y = 0$. To daje rozwiązania $(x, y) = (2, -1)$ lub $(x, y) = (2, 1)$. □

R6. Tak. Niech $W(x) = x^{18} - 8x^9$. Wówczas $W(0) = W(\sqrt[3]{2})$. Przypuśćmy, że $W(r) = W(s)$ dla pewnych liczb wymiernych $r \neq s$. Równanie $x^{18} - 8x^9 - W(r) = 0$ ma wtedy dwa różne pierwiastki wymierne r, s. Stąd także równanie $y^2 - 8y - W(r) = 0$ ma dwa różne pierwiastki wymierne r^9, s^9. Wobec tego z wzorów Viète'a $r^9 + s^9 = 8$, czyli $(r^3)^3 + (s^3)^3 = 2^3$.

Z WTwF dla liczb wymiernych r^3, s^3 znaczy to, że $r^3 = 0$ i $s^3 = 2$ lub $s^3 = 0$ i $r^3 = 2$, co na mocy zadania 1 prowadzi do sprzeczności, bo r i s są wymierne. □

R7. Niech

$$g(x) = \frac{a}{ax+1}, \quad \text{wówczas} \quad g^{(k)}(x) = (-1)^k \cdot k! \cdot \left(\frac{a}{ax+1}\right)^{k+1}.$$

Stąd

$$f^{(11)}(x) = -11! \cdot \left(\left(\frac{3987}{3987x+1}\right)^{12} + \left(\frac{4365}{4365x+1}\right)^{12} - \left(\frac{-4472}{-4472x+1}\right)^{12}\right),$$

czyli warunek $f^{(11)}(0) = 0$ równoważny jest warunkowi $3987^{12} + 4365^{12} - 4472^{12} = 0$. To zaś jest niemożliwe na mocy WTwF. □

Zadanie 6 pochodzi z LXIV Olimpiady Matematycznej, a opisane tu rozwiązanie przedstawił jej uczestnik.